ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 11 巻第 1 号（通巻第 72 号・2026 年 1 月）

法と情報研究会　編

本 号 目 次

規則(EU) 2025/38（サイバー結束法）
[参考訳]

2026 年 1 月 14 日
明治大学法学部教授
夏 井 高 人

Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)（OJ L, 2025/38, 15.1.2025）のテキスト（英語版）に基づき，その和訳を試みた。

規則(EU) 2025/38 の原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/reg/2025/38/oj
[2025 年 12 月 20 日確認]

規則(EU) 2025/38（サイバー結束法）の参考訳は，あくまでも原文を読む際の参考として提供しているものであり，個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

＊＊＊

この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p. 1）の参考訳・再訂版（法と情報雑誌 6 巻 6 号 467～548 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・再訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，NIS 指令(EU) 2016/1148 の参考訳・再訂版における訳文とは異なっている箇所がある。

この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，指令(EU) 2022/2555（NIS2 指令）（OJ L 333, 27.12.2022, p. 80-152）の参考訳（法と情報雑誌 8 巻 4 号 1～206 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，指令(EU) 2022/2555（NIS2 指令）の参考訳における訳文とは異なっている箇所がある。

この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，指令(EU) 2022/2557（OJ L 333, 27.12.2022, p. 164-198）の参考訳（法と情報雑誌 8 巻 4 号 207～303 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この

規則(EU) 2025/38（サイバー一結束法）の参考訳の中には，指令(EU) 2022/2557 の参考訳における訳文とは異なっている箇所がある。

この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，規則(EU) 2024/2847（サイバー回復力法）（OJ L, 2024/2847, 20.11.2024, p. 1–81）の参考訳（法と情報雑誌 10 巻 2 号 1～246 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，規則(EU) 2024/2847（サイバー回復力法）の参考訳における訳文とは異なっている箇所がある。

この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，規則(EU) 2019/881（サイバーセキュリティ法）（OJ L 151, 7.6.2019, p.15-69）の参考訳・改訂版（法と情報雑誌 4 巻 8 号 16～86 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，規則(EU) 2019/881（サイバーセキュリティ法）の参考訳・改訂版における訳文とは異なっている箇所がある。

この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，規則(EU) 2022/2554（OJ L 333, 27.12.2022, p. 1–79）の参考訳（法と情報雑誌 10 巻 5 号 1～234 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2025/38（サイバー結束法）の参考訳の中には，規則(EU) 2022/2554 の参考訳における訳文とは異なっている箇所がある。

Eur-lex 上で検索可能な規則(EU) 2025/38（サイバー結束法）の HTML 版の原文の末尾には「A statement has been made with regard to this act and can be found in OJ C, C/2025/308, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/308/oj」と記載されているが，この文は，規則(EU) 2025/38（サイバー結束法）を構成する要素の一部ではない。

―解 説―

1. 規則(EU) 2025/38（サイバー結束法）について

1.1 総 説

規則(EU) 2025/38（サイバー結束法）は，EU の現行法令である。

規則(EU) 2025/38（サイバー結束法）の中には，それ自体の適用（application）の日を定める条項はない。それゆえ，規則(EU) 2025/38（サイバー結束法）の発効の日から（別紙を含め）同規則の全ての条項が適用となったと解される。
規則(EU) 2025/38（サイバー結束法）の発効の日は，2025 年 2 月 4 日である。

規則(EU) 2025/38（サイバー結束法）は，ロシアによるウクライナに対する軍事侵攻によって明らかにされた軍事上の作戦行為または謀略行為の一部としての相手国の不可欠インフラ（critical infrastructure）等に対するサイバー攻撃の脅威とその被害の大きさの認識を踏まえた上で，欧州連合におけるサイバーセキュリティを強化するために採択された法令である。

規則(EU) 2025/38（サイバー結束法）では，規則(EU) 2022/2555（NIS2 指令）及び指令(EU) 2022/2557 によって導入されたサイバーな脅威及びインシデントと関連する情報の伝達と共有のための基本的な仕組みを更に拡充し，また，規則(EU) 2024/2847（サイバー回復力法）及び規則(EU) 2022/2554 を基礎とする不可欠インフラ等の回復力を強化するための関係諸機関の間における相互支援と相互補助を支援する新たな仕組みが導入されている。

規則(EU) 2025/38（サイバー結束法）は，このような性質をもつサイバー攻撃によって発生するインシデントを，大きなサイバーセキュリティインシデント（significant cybersecurity incidents）及び大規模なセキュリティインシデント（large-scale cybersecurity incidents）という 2 の態様に分類する考え方を基礎としている。
規則(EU) 2025/38（サイバー結束法）は，それらのインシデントの異なる特性に応じたサイバーな脅威（cyber threats）とインシデントの検出（detection），対応準備（prepare），インシデント対応（response）に必要となる欧州連合レベルの支援を定めている。

規則(EU) 2025/38（サイバー結束法）においては，DEP と関係をもつ第三国（DEP-associated third countries）との関係においては，欧州連合及び構成国との関係において使用される大規模なセキュリティインシデントと識別するために，大規模と均等なサイバーセキュリティインシデント（large-scale-equivalent cybersecurity incidents）という概念が使用されている。
つまり，大規模と均等なサイバーセキュリティインシデントという概念は，DEP と関係をもつ第三国と関連する文脈の中においてのみ使用されている。

1．2 規則(EU) 2025/38（サイバー結束法）の 3 つの柱

規則(EU) 2025/38（サイバー結束法）は，欧州サイバーセキュリティ警報システム（European Cybersecurity Alert System），サイバーセキュリティ緊急メカニズム（Cybersecurity Emergency Mechanism）及び欧州サイバーセキュリティ見直しメカニズム（European Cybersecurity Incident Review Mechanism）という 3 つの柱によって構成されている。

1．2．1 欧州サイバーセキュリティ警報システム

欧州サイバーセキュリティ警報システムは，規則(EU) 2025/38（サイバー結束法）の第Ⅱ章（Chapter Ⅱ）の中で定められている。

欧州サイバーセキュリティ警報システムは，サイバーセキュリティインシデントと関連する情報伝達及び情報共有のための任意ベース（voluntary basis）の仕組みである。

構成国は，当該構成国内のサイバーセキュリティインシデントと関連する情報伝達及び情報共有のための集中的な単一の拠点としての国内サイバーハブ（National Cyber Hubs）を設置する（同規則の前文(14)参照）。
CSIRT や国内サイバー危機管理当局等の欧州連合の既存の法令を基礎とするサイバーセキュリティインシデントと関連する情報伝達及び情報共有の仕組みが既に存在するため，それらの既存の組織をもって国内サイバーハブとすることもできる（同規則の第 4 条第 2 項参照）。
既存の仕組みと新設の仕組みの両者を包摂する国家制度または国家機能としての「国内サイバーハブ」という概念は，サイバーセキュリティと関連する情報の情報伝達と情報共有のための単一の国内拠点の総称であることになる。
既存の国内組織が規則(EU) 2025/38（サイバー結束法）に基づく国内サイバーハブとなっている場合，例えば，CSIRTs 及び国内サイバー危機管理当局等に関しては，その根拠法令となっている指令(EU) 2022/2555（NIS2 指令）の関連情報の正確かつ十分な理解を要する。

国内サイバーハブは，各構成国のための情報拠点である。複数の国内サイバーハブ間の情報伝達及び情報交換のためには，国境を越えるサイバーハブ（Cross-Border Cyber Hubs）が必要となる（同規則の前文(15)参照）。
ここでいう国境とは，欧州連合の構成国間の域内国境のことを意味し，第三国との間の域外国境のことを意味しない。第三国が関与する場合には，別の仕組みが準備されている。

少なくとも 3 つ以上の国内サイバーハブの相互運用ネットワーク（多国間プラットフォーム）として，コンソーシアム合意（consortium agreement）によって，組織される（規則(EU) 2025/38（サイバー結束法）の第 5 条参照）。

「国境を越えるサイバーハブ」という概念は，構成国間の国際的な制度または機能としての側面を示

す概念である。国境を越えるサイバーハブの制度または機能を運用するための運用主体は，コンソーシアム合意によって構成されるホスティングコンソーシアム（Hosting Consortium）である。

国境を越えるサイバーハブの運用のために必要な資金及び資源等は，規則(EU) 2021/887（OJ L 202, 8.6.2021, p. 1）によって設置されたサイバーセキュリティインシデントに対する対応等のための欧州連合の基金及び資源（EU サイバーセキュリティリザーブ及び他の関連法令を基礎とする基金及び資源）から，欧州サイバーセキュリティ産業，技術及び調査研究能力拠点（the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)）によって選抜された構成国に対して拠出または供与される（規則(EU) 2025/38（サイバー結束法）の第 9 条参照）。

現実には，既存の仕組みを国内サイバーハブとする例が一般的であろうと予測される。そうであるとすれば，国境を越えるサイバーハブ及びホスティングコンソーシアムは，ECCC によって運用される欧州連合の基金等を分配するための受け口として機能するために用意された仕組みであると理解することが可能である。
そして，国境を越えるサイバーハブ及びホスティングコンソーシアムが合意ベースのものである以上，（会計管理や監査を含め）現実の資金等の分配やその流れに関しては，コンソーシアム合意の具体的な内容を知ることによって正確な理解を得ることができ，また，それを知ることなしにしは正確な理解を得ることができない。

1. 2. 2 サイバーセキュリティ緊急メカニズム

サイバーセキュリティ緊急メカニズムは，規則(EU) 2025/38（サイバー結束法）の第 III 章（Chapter III）の中で定められている。

サイバーな脅威とインシデントの対応準備，それに対する対応及びそれからの復旧は，インシデントの影響を受けた法主体（affected entities）が自身で行うのが基本であり，また，インシデントの影響を受けた法主体の復旧に対する支援は，当該法主体が拠点をもつ構成国が行うのが基本である。
しかし，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントの場合，関係する構成国や DEP と関係をもつ第三国に対して迅速に支援が行われないと EU 全体の情報ネットワークの復旧が遅延し，安全保障上でも問題が生ずることとなりかねない。
そのような深刻な事態の発生を避け，欧州連合の支援によってインシデントによる影響を迅速に解消し，復旧できるようにするための制度または機能として，規則(EU) 2025/38（サイバー結束法）によって EU サイバーセキュリティリザーブ（EU Cybersecurity Reserve）が設置される（同規則の第 14 条参照）。

欧州連合の一般予算の中からの資金拠出（contribution）による支援は，基本的に，欧州委員会と ECCC によって，助成金（grants）という方式によって行われる。EU サイバーセキュリティリザーブを基礎とするインシデントからの最初の回復を支援するための資金拠出も同じである。これらの欧州連合の一般予算からの資金拠出においては，ECCC が重要な役割を担う。

そのため，EU のデジタル経済（digital economy）の基本方針と欧州連合の一般予算からの資金拠出の骨格を定める規則(EU) 2021/694（OJ L 166, 11.5.2021, p. 1–34）が一部改正される（規則(EU) 2025/38（サイバー結束法）の第 22 条参照）。

EU 域内におけるサイバー攻撃等による被害が深刻なものであり，そのような被害からの復旧のために巨額の資金を要するときは，支援対象の優先順位を定め，合理的かつ比例的な支援を実施する必要がある。
規則(EU) 2025/38（サイバー結束法）の下においては，このような意味での優先順位の判断とその決定においては，欧州委員会と ENISA が主導的な役割を演ずる（同規則の前文(43)，前文(45)，第 14 条第 4 項，第 16 条第 4 項参照）。

1．2．3 欧州サイバーセキュリティ見直しメカニズム

欧州サイバーセキュリティ見直しメカニズムは，規則(EU) 2025/38（サイバー結束法）の第 IV 章（Chapter IV）の中で定められている。

欧州サイバーセキュリティ見直しメカニズムは，規則(EU) 2025/38（サイバー結束法）の運用上で行われる個々のサイバーな脅威とインシデントの評価及びその評価を基礎とする個々の支援に関し，同規則の目的を達成することに貢献したか否かという観点から見直すための仕組みである。
ENISA は，個々のインシデントそれ自体とそれに対する支援等の対応を見直し及び評価し，その結果をまとめたインシデント見直し報告書を作成し，提出する（同規則の第 21 条参照）。

一般に，EU の規則（Regulation）や指令（Directive）のような法令は，EU の基本条約に定める基本方針を実現するための手段としてのマネジメントシステムの一種として理解できる。

それゆえ，EU の法令は，その立法～運用（適用）～評価（見直し）～改正等の仕組みは，そのような意味でのマネジメントシステムのマネジメントサイクルの中に位置づけて理解できる。
EU 法という社会システムは，衒学的または政治的なイデオロギー重視の観念法学の教義によって説明されるべきではない。それは，合理的なマネジメントシステムとしての機能（functioning）する構造体（structure）として，認識・理解されるべきである。

このことを踏まえた上で，欧州サイバーセキュリティ見直しメカニズムは，マネジメントシステムとしての欧州サイバーセキュリティ警報システム及び EU サイバーセキュリティリザーブを基礎として実施された個々の行為に関するマネジメントサイクル中の見直し（評価）の部分に相当する。
欧州サイバーセキュリティ見直しメカニズムの下における ENISA による見直し及び評価の結果は，それ以降における個々のインシデント評価や支援の判断に反映されることになる。

なお，マネジメントシステムとしての規則(EU) 2025/38（サイバー結束法）全体に関するマネジメントサイクル中の見直し（評価）の部分に相当する行為は，欧州委員会によって実施される（同規則の前文

(60)参照)。
欧州委員会は，規則(EU) 2025/38（サイバー結束法）の全体を見直し及び評価し，その結果をまとめた報告書を提出する（同規則の第 25 条参照）。

1．3 欧州サイバーセキュリティ認証制度

規則(EU) 2025/38（サイバー結束法）の中では，マネージドセキュリティサービス（managed security services）のための欧州サイバーセキュリティ認証制度（European cybersecurity certification scheme）への言及がある（同規則の第 17 条第 2 項(j)参照）。

欧州サイバーセキュリティ認証制度を定める EU の基本法令は，規則(EU)2019/881（サイバーセキュリティ法）である。

同規則の第 2 条第 9 号は，欧州サイバーセキュリティ認証制度に関し，「欧州連合レベルで定められ，かつ，個々の ICT 製品，ICT サービスまたは ICT プロセスの認証または適合性評価に適用される規定，技術上の要求事項，標準及び手続の包括的なセット（comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes）」のことを意味すると定めており，また，同規則の第 48 条及び第 49 条は，欧州委員会が ENISA に対して同認証制度の案の策定を委任し，この案を基礎として欧州委員会が同制度を採択する旨を定めている。

しかしながら，規則(EU)2019/881（サイバーセキュリティ法）は，法解釈上では，マネージドセキュリティサービスを包摂するものと解されているけれども，条文の文言それ自体としては，マネージドセキュリティサービスに関する認証制度の明示の言及がない。
そこで，マネージドセキュリティサービスのための欧州サイバーセキュリティ認証制度の制定と関連する欧州委員会の権限を明確化するため，規則(EU) 2025/37（OJ L, 2025/37, 15.1.2025）による規則(EU)2019/881（サイバーセキュリティ法）の一部改正が行われた。この規則(EU) 2025/37 による規則(EU)2019/881（サイバーセキュリティ法）の一部改正は，2025 年 2 月 4 日に発効している。

一部改正後の規則(EU)2019/881（サイバーセキュリティ法）の第 2 条第 14 号 a は，マネージドセキュリティサービスに関し，「インシデントの取扱い，ペネトレーションテスト，セキュリティ監査，並びに，専門家の助言を含め，技術上の支援と関連するコンサルティングのような，サイバーセキュリティ上のリスクマネジメントと関連する活動を遂行することまたはその活動のための補助を提供することによって組成され，サードパーティに対して提供されるサービス（service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits and consulting, including expert advice, related to technical support）」と定義している。

ただし，2026 年 1 月 7 日現在，マネージドセキュリティサービスのための欧州サイバーセキュリティ認証制度は，まだ公表されていない。

2. 参考訳作成における基本方針

この参考訳においては，規則(EU) 2025/38（サイバー結束法）の前文，条文及び別紙（ANNEX）の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし，原文を表示することが無意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。

この参考訳は，あくまでも規則(EU) 2025/38（サイバー結束法）の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

この参考訳の訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

原文中にある誤記と疑われる箇所に関しては，赤色字で示すことにした。この原文中の誤記と疑われる箇所は，形式的なミスという意味で誤記であるものと意味的な誤りを含むことになるために誤記であるもの両者を含む。
ただし，原文中に存在する誤記と疑われる箇所の全てが赤色字で表示されているという趣旨ではない。判断を保留した箇所が存在する。
原文中に誤りがあると判断した場合，原則として，そのまま直訳とした。しかし，そのまま直訳にしたのでは正しく法解釈された法規範を適正に示したことにならない場合，合理的に法解釈した結果を反映した訳文とすることにし，その箇所を灰色字で示すことにした。

なお，規則(EU) 2025/38（サイバー結束法）の中で示されている引用法令の出典を示す箇所の表記において「ELI:」が付されているものがある。しかし，その場合の「ELI:」の表記はそれが存在しなくても典拠である EU 官報の該当号の特定性に欠けることが全くないので，法情報学及び立法学の観点からすると，それらの「ELI:」の表記は，余事記載という意味で誤記の一種であると解し，そのような意味で，赤色字で示し，かつ，訳文の中ではその部分を消去することにした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

3. 参考訳作成において留意した事項

Critical

この規則(EU) 2025/38（サイバー結束法）の参考訳においては，情報通信やインフラの属性等との関係においては，「critical」を「不可欠」と訳すことにした。
同様に，「high criticality」に関し，指令(EU) 2022/2555（NIS2 指令）の中では「高度な重要性」と訳したが，規則(EU) 2025/38（サイバー結束法）の参考訳においては，「高度な不可欠性」と訳すことにした。

Essential

この規則(EU) 2025/38（サイバー結束法）の参考訳においては，情報通信やインフラの属性等との関係においては，「essential」を「必須」と訳すことにした。

Objectives

「objectives」は，一般的には，「目的」または「目標」のことを指す。
しかし，規則(EU) 2021/694 及び同規則を一部改正する規則(EU) 2025/38（サイバー結束法）においては，デジタル欧州計画に基づき EU の多年度予算の中から支出可能な領域または事項を限定するための概念として「objectives」が使用されている。
規則(EU) 2021/694 の中では，「general objectives」として示された上で，5 つの分野の「specific objectives」として定義され，それぞれの「specific objectives」に固有の条項が定められている（規則(EU) 2021/694 の第 3 条参照）。

一般に，EU 法の条文においては，目的や到達目標を示す語として，「goal」，「aims」または「end」を使用することが多い。
規則(EU) 2021/694 及び同規則を一部改正する規則(EU) 2025/38（サイバー結束法）の「general objectives」は，「goal」，「aims」または「end」と同じような意味で用いられていると解することにした。
これに対し，「specific objectives」に関しては，個別の達成目標であることには間違いないけれども，むしろ，目標の具体的な内容に重点を置いたものと理解されることから，「目的」または「目標」ではなく，「対象」と理解すべきである。

以上を踏まえた上で，この規則(EU) 2025/38（サイバー結束法）の参考訳においては，「general objectives」を「一般的な目的」と訳し，また，「specific objectives」を，「個別対象」と訳すことにした。

Operational objectives

一般に，「operational objectives」は，本来は，軍事用語であり，（戦略レベル，戦術レベルではなく）作戦レベルにおける個別の作戦目標または当該作戦によって実現されるべきものとして命ぜられる事項または行動の結果のことを意味する。規則(EU) 2021/694 の参考訳の検討時点においては，開発され

る技術等の「dual-use」も視野に入れているため（規則(EU) 2021/694 の第 6 条第 1 項(f)参照），軍事用語と同じように「作戦目標」と訳すことも検討した。しかし，日本語においては，軍事用語と非軍事用語とが別の語として截然と分けられる慣習のようなものがある。その分だけ日本人は同一の内容について複数の語彙をもち，学習上及び運用上の負担が大きいけれども，事実は事実として受け止めるしかない。基本的には非軍事用途を想定した訳語の方が適切であると判断し，民間企業においても理解しやすいような訳語を選択するのが妥当である。とはいえ，非軍事用語として「operational objectives」に対応する適切な日本語を見出すことができない。
そこで，関連する諸般の事情を考慮した上で，この規則(EU) 2025/38（サイバー結束法）の参考訳においては，規則(EU) 2021/694 の参考訳の検討の際と同様，個別対象（specific objectives）を実現するための個別作業の細目という意味で，「operational objectives」を「運用事項」と訳すことにした。

Prepare for

サイバーな脅威またはインシデントとの関係において「prepare for」が使用されている場合，それは，「～に対する準備態勢を整える」ということを意味している。

ただし，このように訳すと説明的過ぎる訳文となってしまう欠点があるため，この規則(EU) 2025/38（サイバー結束法）の参考訳においては，文脈に応じて，「対応準備」等と簡略な表現を用いて訳出することにした。

Reserve

「reserve」は，本来は軍事用語の一種であり，「予備役」のことを意味する。緊急時に備えて一定レベルのスタンバイ状態に置かれている個人または組織が，その必要性が現実化した際に直ちに投入可能なような状態にあることを示す。

この規則(EU) 2025/38（サイバー結束法）の参考訳においては，他に適切な訳語を見いだせないため，「リザーブ」とカタカナ表記することにした。

4. 関連参考訳等

規則(EU)2021/694 の参考訳は，法と情報雑誌 6 巻 1 号 1～104 頁にある。

デジタルの権利及び基本原則に関する欧州宣言の参考訳は，法と情報雑誌 9 巻 1 号 200～229 頁にある。

規則(EU)2019/881（サイバーセキュリティ法）の参考訳・改訂版は，法と情報雑誌4 巻 8 号 16～86 頁にある。指令(EU)2022/2555（NIS2 指令）の参考訳は，法と情報雑誌 8 巻 4 号 1～206 頁にある。規則(EU)2022/2554 の参考訳は，法と情報雑誌 10 巻 5 号 1～234 頁にある。規則(EU) 2024/2847（サイバー回復力法）の参考訳は，法と情報雑誌 10 巻 2 号 1～246 頁にある。指令 2013/40/EU の参考訳・改訂版は，法と情報雑誌 2 巻 8 号 164～185 頁にある。
委員会勧告(EU)2017/1584 の参考訳は，法と情報雑誌 3 巻 7 号 293～327 頁にある。

規則(EU)No 182/2011 の参考訳は，法と情報雑誌 3 巻 5 号 168～179 頁にある。

この参考訳の校正等に関し，唐亀侑久氏（株式会社ラック）の助力を得た。

＊＊＊

サイバーな脅威とインシデントを検出し，それに対して準備し及び対応するための欧州連合内の結束と能力を強化するための措置を定め並びに規則(EU) 2021/694 を改正する欧州議会及び理事会の 2024 年 12 月 19 日の規則(EU) 2025/38（サイバー結束法）

Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)

欧州議会及び欧州連合の理事会は，
欧州連合の機能に関する条約，とりわけ，同条約の第 173 条第 3 項及び第 322 条第 1 項(a)に鑑み，
欧州委員会からの提案に鑑み，
立法案を国内議会に送付した後，
欧州会計検査院の意見書に鑑み[1]，
欧州経済社会委員会の意見書に鑑み[2]，
地域委員会の意見書に鑑み[3]，
通常の立法手続に従って審議し[4]，

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a), thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the Court of Auditors[(1)],
Having regard to the opinion of the European Economic and Social Committee[(2)],
Having regard to the opinion of the Committee of the Regions[(3)],
Acting in accordance with the ordinary legislative procedure[(4)],

Whereas:

---

[1] 2023 年 4 月 18 日付けの意見書（官報未搭載）.
Opinion of 18 April 2023 (not yet published in the Official Journal).
[2] OJ C 349, 29.9.2023, p. 167.
[3] OJ C, C/2024/1049, 9.2.2024
[4] 欧州議会の 2024 年 4 月 24 日付け意見書（官報未搭載）及び理事会の 2024 年 12 月 2 日付け決定.
Position of the European Parliament of 24 April 2024 (not yet published in the Official Journal) and decision of the Council of 2 December 2024.

(1) 構成国の公行政，事業者及び市民の部門と国境を横断する相互接続及び相互依存が不断に増加していること，それと同時に，あり得る脆弱性を導入していることに照らし，情報通信技術の利用及びそれへの依存は，経済活動及び社会の全ての部門における基本的な諸側面となっている。

The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity and society in light of the ever increasing interconnectedness and interdependence of Member State public administrations, businesses and citizens across sectors and borders, simultaneously introducing possible vulnerabilities.

(2) サイバー諜報活動，ランサムウェアまたは破壊の目的のためのサプライチェーン攻撃を含め，サイバーセキュリティインシデントの大きさ，頻度及び影響は，欧州連合及びグローバルなレベルで増加している。サイバーセキュリティインシデントは，ネットワーク及び情報システムの稼動を妨げる大きな脅威を表している。急速に進化する脅威の様相を考慮すると，不可欠なインフラに対する大きな破壊または損害を生じさせるあり得る大規模なサイバーセキュリティインシデントの脅威は，欧州連合のサイバーセキュリティ枠組みの強化された準備態勢を要求する。現在の地政学的な緊張に関与する関係者の多角性に鑑みると，その脅威は，ウクライナに対するロシアの侵略戦争を越えて進んでおり，また，継続しそうである。サイバー攻撃は，地方，地域または国内の公共サービス及びインフラを頻繁に標的としているが，地方当局の限られた資源のゆえの場合を含め，地方当局が特に脆弱であるので，そのようなインシデントは，公共サービスの提供を妨げ得る。サイバーセキュリティインシデントは，高度の不可欠性のある部門または他の不可欠な部門を含め，経済活動の遂行を妨げ，大きな金銭的な損失を生み出し，利用者の信頼を損ね，欧州連合の経済と民主主義のシステムに対して大きな損害を生じさせることもあり得るのであり，また，健康もしくは生命に脅威を及ぼす結果をもつことさえあり得る。更に加えて，サイバーセキュリティインシデントが，しばしば，急速に発生して進化し，特定の地理的領域内に収まることがなく，また，多数の国々を横断して同時に発生しまたは容易に拡散するので，サイバーセキュリティインシデントは，予測できない。公的部門，民間部門，学術，市民社会及びメディアの間において緊密な協力をもつことが重要である。

The magnitude, frequency and impact of cybersecurity incidents, including supply chain attacks for the purposes of cyberespionage, ransomware or disruption, are increasing at Union and global level. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale cybersecurity incidents causing significant disruption or damage to critical infrastructure demands a heightened preparedness of the Union's cybersecurity framework. That threat goes beyond Russia's war of aggression against Ukraine, and is likely to persist given the multiplicity of actors involved in current geopolitical tensions. Such incidents can impede the provision of public services as cyberattacks are frequently targeted at local, regional or national public services and infrastructure, with local authorities being particularly vulnerable, including due to their limited resources. They can also impede the pursuit of economic activities, including in sectors of high criticality or other critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy and the democratic systems of the Union, and could even have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve quickly, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries. It is important to have close cooperation between

the public sector, the private sector, academia, civil society and the media.

(3) 欧州の将来に関する会議の 3 つの異なる提案の中で勧告されているように，デジタル単一市場におけるサイバーセキュリティのレベルを強化することによって，デジタル経済全体にわたり欧州連合内の製造業及びサービス業の競争力のある地位を強化する必要があり，また，製造業及びサービス業のデジタル変革を支援する必要がある。増加しつつあり，壊滅的な社会的及び経済的影響をもち得るサイバーな脅威に抗する市民，マイクロ企業，小企業と中規模企業及びスタートアップを含め事業者，並びに，不可欠なインフラを運営している法主体の回復力を増やす必要がある。それゆえ，サイバーな脅威とインシデントのより速い検出及びそれらへのより速い対応を支援するサイバーセキュリティの技能を開発するため，インフラ及びサービス並びに構築能力への投資が必要である。加えて，構成国は，大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントへのより良い対応準備とそれに対する対応における補助並びにそれからの最初の回復における補助を必要としている。現行の構造体を基礎としかつ既存の構造体の間で緊密に協力して，欧州連合は，それらの分野における欧州連合の能力，とりわけ，サイバーな脅威とインシデントに関するデータの収集及び分析に関する能力も増加させるべきである。

It is necessary to strengthen the competitive position of industry and services in the Union across the digital economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market as recommended in three different proposals of the Conference on the Future of Europe. It is necessary to increase the resilience of citizens, businesses, including microenterprises, small and medium-sized enterprises and startups, and entities operating critical infrastructure, against increasing cyber threats, which can have a devastating societal and economic impact. Therefore, investment is needed in infrastructure and services and building capabilities to develop cybersecurity skills that will support a faster detection of and a faster response to cyber threats and incidents. In addition, Member States need assistance in better preparing for and responding to, as well as assistance in the initial recovery from, significant cybersecurity incidents and large-scale cybersecurity incidents. Building on the existing structures and in close cooperation with them, the Union should also increase its capacities in those areas, in particular as regards the collection and analysis of data on cyber threats and incidents.

(4) 欧州連合は，脆弱性を削減し，かつ，リスクに抗して不可欠なインフラと法主体の回復力を増加させるための多数の措置，とりわけ，欧州議会及び理事会の規則(EU) 2019/881[5]，欧州議会及び理事会の指令 2013/40/EU[6]及び指令(EU) 2022/2555[7]並びに委員会勧告(EU) 2017/1584[8]という措置を講じている。加えて，不可欠なインフラの回復力を強化するための欧州連合全域で調整されたアプローチに関する 2022 年 12 月 8 日の理事会勧告は，構成国に対し，域内市場において必須のサービスを提

[5] ENISA（欧州連合サイバーセキュリティ局）に関する及び情報通信技術のサイバーセキュリティ認証に関する並びに規則(EU)No 526/2013 を廃止する欧州議会及び理事会の 2019 年 4 月 17 日の規則(EU)2019/881（サイバーセキュリティ法）(OJ L 151, 7.6.2019, p. 15).
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

供するために用いられる不可欠なインフラの回復力を拡大するため，措置を講ずること，並びに，相互に，欧州委員会とそれ以外の適格な行政機関と及び関係する法主体と協力することを勧奨している。

The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructure and entities against risks, in particular Regulation (EU) 2019/881 of the European Parliament and of the Council [5], Directives 2013/40/EU [6] and (EU) 2022/2555 [7] of the European Parliament and of the Council and Commission Recommendation (EU) 2017/1584 [8]. In addition, the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take measures, and to cooperate with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

(5) ある構成国から別の構成国へ及び第三国から欧州連合へのインシデントの急速な波及という明確なリスクをもつ増加するサイバーセキュリティリスク及び全体として複雑な脅威の様相は，とりわけ，既存の構造体の実現能力を強化することによって，サイバーな脅威とインシデントをより良く検出し，それに対して準備し，それに対して対応し及びそこから復旧するための欧州連合レベルの結束を強化することを要求する。更に加えて，欧州連合のサイバーポスチャーの発展に関する 2022 年 5 月 23 日の理事会決議は，欧州委員会が，サイバーセキュリティのための新たな緊急対応基金の提案書を提示することを勧奨している。

The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spillover of incidents from one Member State to others and from a third country to the Union, require the strengthening of solidarity at Union level to better detect, prepare for, respond to, and recover from, cyber threats and incidents, in particular by reinforcing the capabilities of existing structures. Moreover, the Council conclusions of 23 May 2022 on the development of the European Union's cyber posture invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity.

---

[6] 情報システムに対する攻撃に関する及び理事会枠組み決定 2005/222/JHA を置換える欧州議会及び理事会の 2013 年 8 月 12 日の指令 2013/40/EU (OJ L 218, 14.8.2013, p. 8).
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

[7] 欧州全域の共通の高いレベルのサイバーセキュリティのための措置に関する，規則(EU) No 910/2014 及び指令(EU) 2018/1972 を改正し並びに指令(EU) 2016/1148 を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2555（NIS2 指令）(OJ L 333, 27.12.2022, p. 80).
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

[8] 大規模なサイバーセキュリティインシデント及び危機に対する調整された対応に関する 2017 年 9 月 13 日の委員会勧告(EU) 2017/1584 (OJ L 239, 19.9.2017, p. 36).
Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

(6) EU のサイバー防衛政策に関する欧州委員会及び外交及び安全保障政策に関する欧州連合上級代表から欧州議会及び理事会宛の 2022 年 11 月 10 日の共同通知は，セキュリティオペレーションセンター（SOCs）の EU インフラの配置を促進すること，信頼できる民間プロバイダからのサービスをもつ EU レベルのサイバーリザーブの段階的な構築を支援すること，そして，EU リスクマネジメントを基礎として，潜在的な脆弱性に関し，不可欠な法主体を試すことによって，EU の共通の検出能力，状況認識能力及び対応能力を強化するという目的をもつ EU のサイバー結束の取組みを公報した。

The Joint Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 10 November 2022 to the European Parliament and the Council on EU Policy on Cyber Defence announced an EU Cyber Solidarity Initiative with the objectives of strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operation Centres (SOCs), supporting gradual building of an EU-level cyber reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments.

(7) 欧州連合全域におけるサイバーな脅威とインシデントの検知と状況認識を強化し，大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントの防止と対応のための構成国と欧州連合の準備態勢と実現能力を高めることで結束を強化することが必要である。それゆえ，調整された検出能力及び状況認識能力を構築するため，欧州連合の脅威検出能力及び情報共有能力を強化するサイバーハブの汎欧州のネットワーク（「欧州サイバーセキュリティ警報システム」）が設けられるべきであり；大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントに対して準備すること，それらに対して対応すること，それらの影響を緩和すること及びそれらからの復旧を開始することにおいて，構成国の要請に応じて構成国を支援するため，並びに，大きなサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対して対応することにおいて，構成国以外のユーザを支援するため，サイバーセキュリティ緊急メカニズムが設けられるべきであり；また，個々の大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントを見直し及び評価するため，欧州のサイバーセキュリティインシデントの見直しメカニズムが設けられるべきである。この規則によってとられる活動は，構成国の権限を適正に尊重して行われるべきであり，かつ，それら全てが指令(EU) 2022/2555 によって設置された CSIRTs ネットワーク，欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）または協力グループ（NIS 協力グループ）によって行われる活動を補うものでありかつそれらの活動と重複すべきではない。それらの活動は，欧州連合の機能に関する条約（TFEU）の第 107 条及び第 108 条を妨げない。

It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to prevent and respond to significant cybersecurity incidents and large-scale cybersecurity incidents. Therefore a pan-European network of cyberhubs (the 'European Cybersecurity Alert System') should be established to build coordinated detection and situational awareness capabilities, reinforcing the Union's threat detection and information-sharing capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States upon their request in preparing for, responding to, mitigating the impact of and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents and to support other users in responding to significant cybersecurity incidents and large-scale-

equivalent cybersecurity incidents; and a European Cybersecurity Incident Review Mechanism should be established to review and assess specific significant cybersecurity incidents or large-scale cybersecurity incidents. The actions taken pursuant to this Regulation should be conducted with due respect for Member States' competences and should complement and not duplicate the activities conducted by the CSIRTs network, the European cyber crisis liaison organisation network (EU-CyCLONe) or the Cooperation Group (NIS Cooperation Group), all established pursuant to Directive (EU) 2022/2555. Those actions are without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union (TFEU).

(8) それらの目的を達成するため，一定の分野において，欧州議会及び理事会の規則(EU) 2021/694[9]を改正する必要がある。とりわけ，デジタル単一市場の回復力，完全性及び信頼性を保証すること，サイバー攻撃及びサイバーな脅威を監視し及びそれらに対応する能力を強化すること，そして，サイバーセキュリティに関する国境を越える協力及び調整を強化することを狙いとするデジタル欧州計画（DEP）の個別対象 3 の下にある欧州サイバーセキュリティ警報システム及びサイバーセキュリティ緊急メカニズムと関係する新たな運用事項の追加に関し，この規則は，規則(EU) 2021/694 を改正すべきである。欧州サイバーセキュリティ警報システムは，サイバーな脅威を予測すること及びそれに対して防護することにおいて，構成国を支援する上で重要な役割を果たし得るのであり，また，EU サイバーセキュリティリザーブは，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントの影響に対して対応すること及びそれを緩和することにおいて，構成国，欧州連合の機関，組織，事務局及び部局並びに DPE と関係をもつ第三国を支える上で重要な役割を果たし得る。その影響は，相当の物的損害または非物的損害並びに公共の保安及び安全上の重大なリスクを含み得る。欧州サイバーセキュリティ警報システム及び EU サイバーセキュリティリザーブが果たし得る特定の役割に照らし，この規則は，必要かつ十分なツール，インフラ及びサービスまたは技術，専門知識及び能力が欧州連合内においては利用可能ではない現実のリスクが存在し，かつ，そのような法主体を包摂することの利益がセキュリティリスクを上回っている場合における，欧州連合内に拠点をもつけれども第三国から支配されている法人の参加に関し，規則(EU) 2021/694 を改正すべきである。欧州サイバーセキュリティ警報システム及び EU サイバーセキュリティリザーブを実装する活動に対して与えられ得る資金支援の細目的な条件が定められるべきであり，また，所期の目的を達成するために必要となる統治の仕組み及び調整の仕組みが定義されるべきである。それら以外の規則(EU) 2021/694 の改正は，新たな運用事項の下において提案された活動の記述及びそれらの新たな運用事項の実装を監視するための計測可能な指標を含めるべきである。

To achieve those objectives, it is necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[9] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards the addition of new operational objectives related to the European Cybersecurity Alert System and the Cybersecurity Emergency

[9] デジタル欧州計画を設ける及び決定(EU) 2015/2240 を廃止する欧州議会及び理事会の 2021 年 4 月 29 日の規則(EU) 2021/694 (OJ L 166, 11.5.2021, p. 1).
Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

Mechanism under Specific Objective 3 of the Digital Europe Programme (DEP), which aims to guarantee the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyberattacks and cyber threats and to respond to them, and at reinforcing cross-border cooperation and coordination on cybersecurity. The European Cybersecurity Alert System could play an important role in supporting Member States in anticipating and protecting against cyber threats, and the EU Cybersecurity Reserve could play an important role in supporting Member States, Union institutions, bodies, offices and agencies, and DEP-associated third countries in responding to and mitigating the impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents. That impact could include considerable material or non-material damage and serious public security and safety risks. In light of the specific roles that the European Cybersecurity Alert System and the EU Cybersecurity Reserve could play, this Regulation should amend Regulation (EU) 2021/694 as regards the participation of legal entities that are established in the Union but are controlled from third countries, where there is a real risk that the necessary and sufficient tools, infrastructure and services, or technology, expertise and capacity, are not available in the Union and the benefits of including such entities outweigh the security risk. The specific conditions under which financial support may be granted for actions implementing the European Cybersecurity Alert System and the EU Cybersecurity Reserve should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of those new operational objectives.

(9) サイバーな脅威とインシデントに対する欧州連合の対応を強化するため，国際組織との協力及び信頼でき，志を同じくする国際パートナーとの協力が重要である。この文脈において，信頼でき，志を同じくする国際パートナーは，欧州連合の創生を鼓舞した諸原則，すなわち，民主主義，法の支配，人権及び基本的自由の普遍性及び不可分性，人間の尊厳の尊重，平等と結束の原則，国際連合憲章及び国際法の諸原則の尊重を共有し，かつ，欧州連合またはその構成国の安全保障上の必須の利益を損ねることがないことを共有する諸国であると理解されるべきである。そのような協力は，この規則によってとられる活動，とりわけ，欧州サイバーセキュリティ警報システム及び EU サイバーセキュリティリザーブとの関係においても利益があり得る。規則(EU) 2021/694 は，一定の可用性及び安全保障上の条件に服して，欧州サイバーセキュリティ警報システム及びサイバーセキュリティ緊急メカニズムに関する入札が，安全保障上の要件に服して，第三国から支配されている法人に対して開かれることを定めるべきである。この方法における調達を開くことの安全保障上のリスクを評価する際，それらの諸原則及び価値が欧州連合の安全保障上の必須の利益と関連している場合，志を同じくする国際パートナーとの間で欧州連合が共有している諸原則及び価値を考慮に入れることが重要である。加えて，そのような安全保障上の要件が規則(EU) 2021/694 の下における判断の下にあるときは，法主体の組織構造と意思形成プロセス，データ及び機密情報または機微の情報のセキュリティ，並びに，その活動の結果が，適格のない第三国による支配または制限に服さないことを確保することのような，複数の要素が考慮に入れられ得る。

To strengthen the Union's response to cyber threats and incidents, cooperation with international organisations as well as with trusted, like-minded international partners is vital. In that context, trusted, like-minded international partners should be understood to be the countries that share the principles that inspired the Union's creation, namely democracy, the rule

of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law, and that do not undermine the essential security interests of the Union or its Member States. Such cooperation could also be beneficial with regard to the actions taken pursuant to this Regulation, in particular the European Cybersecurity Alert System and the EU Cybersecurity Reserve. Regulation (EU) 2021/694 should provide, subject to certain availability and security conditions, for tenders for the European Cybersecurity Alert System and the EU Cybersecurity Reserve to be open to legal entities controlled from third countries, subject to security requirements. When assessing the security risk of opening the procurement in this way, it is important to take into account the principles and values which the Union shares with like-minded international partners, where those principles and values are related to essential security interests of the Union. Additionally, where such security requirements are under consideration under Regulation (EU) 2021/694, several elements could be taken into account, such as an entity's corporate structure and decision-making process, the security of data and classified or sensitive information and ensuring that the action's results are not subject to control or restrictions by non-eligible third countries.

(10) この規則の下における活動の資金拠出は，規則(EU) 2021/694 の中で定められるべきであり，それは，DPE の個別対象 3 の中で掲げられている活動のための適格な基本法行為のままであるべきである。個々の活動と関係する参加のための個別の条件は，規則(EU) 2021/694 に従い，適格な作業計画の中で定められるべきである。

The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for the actions enshrined within Specific Objective 3 of the DEP. Specific conditions for participation concerning each action are to be provided for in the relevant work programmes, in accordance with Regulation (EU) 2021/694.

(11) TFEU の第 322 条を基礎として欧州議会及び理事会によって採択された横断的な資金提供の諸原則は，この規則に対して適用される。それらの諸原則は，欧州議会及び理事会の規則(EU, Euratom) 2024/2509[10] の中で定められており，とりわけ，欧州連合の予算の確定及び実装のための手続を決定しており，また，資金提供の関係者の責任に関する点検を定めている。TFEU の第 322 条を基礎として採択された諸原則は，欧州議会及び理事会の規則(EU, Euratom) 2020/2092[11]の中で設けられている欧州連合の予算の保護のための条件付けの一般的な制度も含んでいる。

Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply

[10] 欧州連合の一般予算に対して適用可能な資金提供上の諸原則に関する欧州議会及び理事会の 2024 年 9 月 23 日の規則(EU, Euratom) 2024/2509 (OJ L, 2024/2509, 26.9.2024,).
Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.9.2024,).

[11] 欧州連合の予算の保護のための条件付けの一般的な制度に関する欧州議会及び理事会の 2020 年 12 月 16 日の規則(EU, Euratom) 2020/2092 (OJ L 433 I, 22.12.2020, p. 1).
Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 433 I, 22.12.2020, p. 1).

to this Regulation. Those rules are laid down in Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council[10] and determine, in particular, the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of Article 322 TFEU also include a general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council[11].

(12) 防止の措置と対応準備の措置は，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントの対応における欧州連合の回復力を拡大するために必須であるが，そのようなインシデントの発生，機会及び大きさは，その性質上，予測できない。適切な対応を確保するために要求される資金源は，年によって大きく異なっていることがあり得るのであり，また，即時に利用できるようにされることが可能であるべきである。それゆえ，予測可能性という予算原則と新たな需要に対して迅速に対処する必要性との両立は，作業計画の資金上の実装の適応を要求する。そのため，規則(EU, Euratom) 2024/2509 の第 12 条第 4 項によって認められる未使用予算の繰り越しに加え，未使用予算の繰り越しを認めることが適切であるが，次年度に限り，かつ，EU サイバーセキュリティリザーブ及び相互補助を支援する活動に限る。

While prevention and preparedness measures are essential to enhance the resilience of the Union in addressing significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, the occurrence, timing and magnitude of such incidents are, by their nature, unpredictable. The financial resources required to ensure an adequate response can vary significantly from year to year and should be capable of being made available immediately. Reconciling the budgetary principle of predictability with the necessity to react rapidly to new needs therefore requires adaptation of the financial implementation of the work programmes. Consequently, it is appropriate to authorise the carry-over of unused appropriations, but only to the following year and only to the EU Cybersecurity Reserve and the actions supporting mutual assistance, in addition to the carry-over of appropriations authorised pursuant to Article 12(4) of Regulation (EU, Euratom) 2024/2509.

(13) サイバーな脅威とインシデントをより実効的に防止し，評価し，それに対応し及びそれから復旧するため，当該インフラに影響を与えるサイバー攻撃の場合における当該脅威の地理的な分布，相互関係及び潜在的な影響を含め，欧州連合の領域上にある不可欠の資産及びインフラに対する脅威に関するより包括的な知識が構築される必要がある。サイバーな脅威を識別すること，緩和すること及び防止することへの積極的なアプローチは，高度な検出を可能とする能力の増加を含む。欧州サイバーセキュリティ警報システムは，それぞれ 3 つ以上の国内サイバーハブを束ねてグループ化されており，複数のものが相互運用される国境を越えるサイバーハブによって構成されるべきである。そのインフラは，国内及び欧州連合のサイバーセキュリティ上の利益と需要を満たすものであり，それが適切なときは匿名化された適格なデータ及び情報の高度な収集のための最新の技術及び分析ツールを梃入れするものであり，調整されたサイバー検出と管理能力を拡大するものであり，かつ，リアルタイムの状況認識を提供するものであるべきである。そのインフラは，サイバーな脅威とインシデントを防止することを狙いとし，そして，欧州連合のサイバー危機管理に関して職責を負う欧州連合の法主体及びネットワーク，とりわけ，EU-CyCLONe を補うこと及び支援することを狙いとして，データ及び情報の検出，集約及び分析を向上させることにより，サイバーポスチャーの向上に資するべき

である。

To more effectively prevent, assess, respond to and recover from cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructure on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyberattacks affecting that infrastructure. A proactive approach to identifying, mitigating and preventing cyber threats includes an increased capacity of advanced detection capabilities. The European Cybersecurity Alert System should consist of several interoperating Cross-Border Cyber Hubs, each grouping together three or more National Cyber Hubs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state-of-the-art technology for advanced collection of relevant data and information, anonymised where appropriate, and analytics tools, enhancing coordinated cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to improve the cyber posture, by increasing detection, aggregation and the analysis of data and information with the aim of preventing cyber threats and incidents and thus complementing and supporting Union entities and networks responsible for cyber crisis management in the Union, in particular EU-CyCLONe.

(14) 欧州サイバーセキュリティ警報システムへの構成国の参加は，任意である。各構成国は，当該構成国におけるサイバーな脅威検出活動を調整することを職務としてもつ国内レベルの単一の法主体を指定すべきである。それらの国内サイバーハブは，欧州サイバーセキュリティ警報システムに参加するための国内レベルの基点及びゲートウェイとして活動すべきであり，また，公的法主体及び民間法主体からのサイバーな脅威情報が，実効的かつ効率化された態様で，国内レベルで共有され及び収集されることを確保すべきである。国内サイバーハブは，公的法主体と民間法主体との間の協力及び情報共有を強化し得るのであり，また，適格な産業の情報共有分析拠点（ISACs）を含め，適格な部門のコミュニティ及び部門横断のコミュニティとの間の適格なデータ及び情報の交換の支援もし得る。公的法主体と民間法主体との間の緊密かつ調整された協力は，欧州連合のサイバー回復力を強化することのための中心である。そのような協力は，能動的なサイバー防護を向上させるためのサイバーな脅威情報の共有という文脈においては，とりわけ価値がある。そのような協力と情報共有の一部として，国内サイバーハブは，特定の情報を要請し及び受領し得る。それらの国内サイバーハブは，この規則によって，そのような要請を履行することを義務づけられることがなく，かつ，その権限を与えられることもない。早期の段階における潜在的なサイバーな脅威とインシデントの迅速な検出を拡大し，それによって，状況認識を向上させるため，それが適切なときは，かつ，欧州連合法及び国内法に従って，要請されまたは受領される情報は，マネージドセキュリティサービスプロバイダのような，当該構成国内における高度の不可欠性のある部門または他の不可欠な部門において業務運営する法主体からのテレメトリーデータ，センサーデータ及び履歴データを含み得る。国内サイバーハブが指令(EU) 2022/2555 の第 8 条第 1 項により適格な構成国によって指定されまたは設置される職務権限のある当局ではない場合，国内サイバーハブが，そのようなデータの要請及び受領との関係において，当該職務権限のある当局との間で調整することが重要である。

Participation in the European Cybersecurity Alert System is voluntary for Member States. Each Member State should designate a single entity at national level tasked with coordinating cyber threat detection activities in that Member State. Those National Cyber Hubs should act as a reference point and gateway at national level for participation in the European

Cybersecurity Alert System and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner. National Cyber Hubs could strengthen the cooperation and information sharing between public and private entities and could also support the exchange of relevant data and information with relevant sectoral and cross-sectoral communities, including relevant industry Information Sharing and Analysis Centers (ISACs). Close and coordinated cooperation between public and private entities is central to strengthening the Union's cyber resilience. Such cooperation is particularly valuable in the context of sharing cyber threat intelligence to improve active cyber protection. As part of such cooperation and information sharing, National Cyber Hubs could request and receive specific information. Those National Cyber Hubs are neither obliged nor empowered by this Regulation to enforce such requests. Where appropriate and in accordance with Union and national law, the information requested or received could include telemetry, sensor and logging data from entities, such as managed security service providers, that operate in sectors of high criticality or other critical sectors within that Member State, in order to enhance rapid detection of potential cyber threats and incidents at an earlier stage, thereby improving situational awareness. If the National Cyber Hub is not the competent authority designated or established by the relevant Member State pursuant to Article 8(1) of (EU) 2022/2555, it is crucial that it coordinates with that competent authority in respect of requests for and receipt of such data.

(15) 欧州サイバーセキュリティ警報システムの一部として，多数の国境を越えるサイバーハブが設けられるべきである。国境を越える脅威の検出と情報共有及び運営管理の受益が全面的に達成され得ることを確保するため，それらの国境を越えるサイバーハブは，少なくとも 3 つの構成国の国内サイバーハブを束ねるべきである。国境を越えるサイバーハブの一般的な目的は，とりわけ，公的なまたは民間の様々な情報源からの適格な情報の，それが適切なときは匿名化され，信頼できかつ安全な環境の中における共有を介して，また，最新のツールの共有と共同利用，及び，信頼できかつ安全な環境の中における検出能力，分析能力及び防止能力の共同開発を介して，サイバーな脅威を分析し，防止し及び検出する能力を強化すること，そして，高品質のサイバーな脅威情報の作成を支援することにあるべきである。国境を越えるサイバーハブは，既存の SOCs，CSIRTs，及び，CSIRTs ネットワークを含め，他の適格な関係者を基礎とし，かつ，それらを補って，新たな付加的な能力を提供すべきである。

As part of the European Cybersecurity Alert System, a number of Cross-Border Cyber Hubs should be established. Those Cross-Border Cyber Hubs should bring together National Cyber Hubs from at least three Member States to ensure that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-Border Cyber Hubs should be to strengthen capacities to analyse, prevent and detect cyber threats and to support the production of high-quality cyber threat intelligence, in particular through the sharing of relevant information, anonymised where appropriate, in a trusted and secure environment, from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and the joint development of detection, analysis and prevention capabilities in a trusted and secure environment. Cross-Border Cyber Hubs should provide new additional capacity, building upon and complementing existing SOCs, CSIRTs and other relevant actors, including the CSIRTs network.

(16) 国内サイバーハブの設置またはその実現能力の拡大への関心表明の募集の後，欧州議会及び理

事会の規則(EU) 2021/887[12] によって設置された欧州サイバーセキュリティ産業，技術及び調査研究能力拠点（ECCC）によって選抜された構成国は，ECCC と共同して，適格なツール，インフラまたはサービスを購入すべきである。そのような構成国は，そのツール，インフラまたはサービスを運用するための助成金を受ける適格をもつべきである。国境を越えるサイバーハブの設置またはその実現能力の拡大への関心表明の募集の後に ECCC によって選抜された少なくとも 3 つの構成国によって構成されるホスティングコンソーシアムは，ECCC と共同して，適格なツール，インフラまたはサービスを購入すべきである。ホスティングコンソーシアムは，そのツール，インフラまたはサービスを運用するための助成金を受ける適格をもつべきである。適格なツール，インフラまたはサービスを購入するための調達手続は，そのような関心表明の募集の後，ECCC 及び選抜された構成国の適格な契約当局によって，共同して実施されるべきである。そのような調達は，規則(EU, Euratom) 2024/2509 の第 168 条第 2 項及び ECCC の財務規則を遵守すべきである。それゆえ，民間の法主体は，ECCC と行動でツール，インフラもしくはサービスを購入することへの関心表明の募集に参加する適格またはそれらのツール，インフラもしくはサービスを運用するための助成金を受ける適格をもってはならない。ただし，構成国は，欧州連合法及び国内法に従い，当該構成国が適切であると考える別の方法により，当該構成国の国内サイバーハブ及び国境を越えるサイバーハブの設置，拡大及び運用において，民間の法主体を含め得るべきである。民間の法主体は，国内サイバーハブに対する支援を提供する目的のために，規則(EU) 2021/887 による欧州連合の資金を受ける適格も与えられ得る。

A Member State selected by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) established by Regulation (EU) 2021/887 of the European Parliament and of the Council[(12)] following a call for expressions of interest to set up, or enhance the capabilities of, a National Cyber Hub, should, jointly with the ECCC, purchase relevant tools, infrastructure or services. Such a Member State should be eligible to receive a grant to operate the tools, infrastructure or services. A Hosting Consortium, consisting of at least three Member States, which has been selected by the ECCC following a call for expressions of interest to set up or enhance the capabilities of a Cross-Border Cyber Hub should purchase relevant tools, infrastructure or services jointly with the ECCC. The Hosting Consortium should be eligible to receive a grant to operate the tools, infrastructure or services. The procurement procedure to purchase the relevant tools, infrastructure or services should be carried out jointly by the ECCC and relevant contracting authorities of the Member States selected, following such calls for expressions of interest. Such procurement should comply with Article 168(2) of Regulation (EU, Euratom) 2024/2509, and the ECCC's Financial Rules. Private entities should not therefore be eligible to participate in the calls for expressions of interest to purchase tools, infrastructure or services jointly with the ECCC, or to receive grants to operate those tools, infrastructure or services. However, the Member States should be able to involve private entities in the setting up, enhancement and operation of their National Cyber Hubs and Cross-Border Cyber Hubs in other ways which they deem appropriate, in accordance with Union and national law. Private entities could also be eligible to receive Union funding pursuant to Regulation (EU) 2021/887 for the purpose of providing

[12] 欧州サイバーセキュリティ産業，技術及び調査研究能力拠点並びに国内調整拠点のネットワークを設ける欧州議会及び理事会の 2021 年 5 月 20 日の規則(EU) 2021/887 (OJ L 202, 8.6.2021, p. 1).
Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).

support to National Cyber Hubs.

(17) 欧州連合におけるサイバーな脅威の検出及び状況認識を拡大するため，関心表明の募集の後に国内サイバーハブを設置するためまたはその実現能力を拡大するために選抜される構成国は，国境を越えるサイバーハブへの参加の申込みを行うべきである。ツール，インフラもしくはサービスが獲得される日または補助金の資金を受ける日のいずれか早い方の日から 2 年以内に，構成国が国境を越えるサイバーハブに参加しないときは，その構成国は，その構成国の国内サイバーハブの実現能力を拡大するための欧州サイバーセキュリティ警報システムの枠組み内における欧州連合の別の支援活動に参加する適格を与えられてはならない。そのような場合，構成国からの法主体は，当該法主体が当該計画の中で定められている適格性基準に適合していることを条件として，サイバー検出及び情報共有のための能力に関する募集を含め，DEP の下にある別のトピックスまたは欧州連合の別の基金計画に関する提案の募集に参加したままであり得る。

In order to enhance the detection of cyber threats and situational awareness in the Union, a Member State which, following a call for expressions of interest, is selected to set up, or enhance the capabilities of, a National Cyber Hub should commit to applying to participate in a Cross-Border Cyber Hub. If a Member State is not a participant in a Cross-Border Cyber Hub within two years of the date on which the tools, infrastructure or services are acquired or on which it receives grant funding, whichever occurs sooner, it should not be eligible to participate in further Union support actions within the framework of the European Cybersecurity Alert System to enhance the capabilities of its National Cyber Hub. In such cases, entities from Member States could still participate in calls for proposals on other topics under the DEP or other Union funding programmes, including calls on capacities for cyber detection and information sharing, provided that those entities meet the eligibility criteria established in those programmes.

(18) CSIRTs は，指令(EU) 2022/2555 に従い，CSIRTs ネットワーク内において情報を交換する。欧州サイバーセキュリティ警報システムは，CSIRTs ネットワークの実現能力を強化できるようにする欧州連合の状況認識を構築することに貢献することによって CSIRTs ネットワークを補う新たな実現能力を組成すべきである。国境を越えるサイバーハブは，CSIRTs ネットワークとの間で緊密に調整し及び協力すべきである。国境を越えるサイバーハブは，公的な法主体及び民間の法主体からのサイバーな脅威に関する，それが適切なときは匿名化された，データをプールすること及び適格な情報を共有することによって，専門家の分析及び共同で獲得したインフラ及び最新のツールを介してそのようなデータ及び情報の価値を拡大する活動をすべきであり，また，欧州連合の技術上の主権，欧州連合のオープンな戦略の自律性，競争力があること及び回復力に貢献し及び欧州連合の実現能力の発展に寄与する活動をすべきである。

CSIRTs exchange information within the CSIRTs network in accordance with Directive (EU) 2022/2555. The European Cybersecurity Alert System should constitute a new capability that is complementary to the CSIRTs network by contributing to building a Union situational awareness allowing the reinforcement of the capabilities of the CSIRTs network. Cross-Border Cyber Hubs should coordinate and cooperate closely with the CSIRTs network. They should act by pooling data and sharing relevant information, anonymised where appropriate, on cyber threats from public and private entities, enhancing the value of such data and information through expert analysis and jointly acquired

infrastructure and state-of-the-art tools, and contributing to the Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience and to the development of Union capabilities.

(19) 国境を越えるサイバーハブは，適格なデータ及びサイバーな脅威情報を広範にプールできるようにし，かつ，コンピュータ緊急対応チーム（CERTs），CSRITs，ISACs 及び不可欠インフラの運用者のような広範で多様なセットの利害関係者の間において脅威情報を拡散できるようにする中心点として活動すべきである。ホスティングコンソーシアムの構成者は，そのコンソーシアム合意の中で，関係する国境を越えるサイバーハブの参加者の間で共有される適格な情報を定めるべきである。国境を越えるサイバーハブ内の参加者間で交換される情報は，例えば，ネットワークとセンサー，脅威情報フィード，侵害の測定機器からのデータ，及び，インシデント，サイバーな脅威，ニアミス，脆弱性，手法と手順，敵対的な戦術，脅威関係者固有の情報，サイバーセキュリティ警報に関する文脈化された情報，並びに，サイバー攻撃を検出するためのサイバーセキュリティツールの設定に関する推奨事項を含み得る。加えて，国境を越えるサイバーハブは，相互に，協力協定にも入るべきである。そのような協力協定は，とりわけ，情報共有の基本原則及び相互運用性を定めるべきである。相互運用性，とりわけ，情報共有のフォーマット及びプロトコルと関係する協力協定の文言は，規則(EU) 2019/881 によって設置された欧州連合サイバーセキュリティ局（ENISA）から発行される相互運用性の運用指針によって導かれるべきであり，かつ，それゆえ，その運用指針をその文言の出発点として採用すべきである。その運用指針は，その運用指針が国境を越えるサイバーハブによって早期の段階で考慮に入れら得ることを確保するため，迅速に発行されるべきである。その運用指針は，国際的な技術標準及びベストプラクティス，並びに，設けられた国境を越えるサイバーハブの稼動状況を考慮に入れるべきである。

Cross-Border Cyber Hubs should act as central points allowing for a broad pooling of relevant data and cyber threat intelligence, and enable the spreading of threat information among a large and diverse set of stakeholders, such as Computer Emergency Response Teams (CERTs), CSIRTs, ISACs and operators of critical infrastructure. The members of a Hosting Consortium should specify in the consortium agreement the relevant information to be shared among the participants of the Cross-Border Cyber Hub concerned. The information exchanged among participants in a Cross-Border Cyber Hub could include, for instance, data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, cyber threats, near misses, vulnerabilities, techniques and procedures, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks. In addition, Cross-Border Cyber Hubs should also enter into cooperation agreements with each other. Such cooperation agreements should, in particular, specify information-sharing principles and interoperability. Their clauses concerning interoperability, in particular information-sharing formats and protocols, should be guided by and therefore take as their starting point interoperability guidelines issued by the European Union Agency for Cybersecurity established by Regulation (EU) 2019/881 (ENISA). Those guidelines should be issued swiftly to ensure that they can be taken into account by Cross-Border Cyber Hubs at an early stage. They should take into account international standards and best practices, and the functioning of any established Cross-Border Cyber Hubs.

(20) 国境を越えるサイバーハブ及び CSIRTs ネットワークは，諸活動の相乗効果及び補完性を確保するため，緊密に協力すべきである。その目的のために，国境を越えるサイバーハブ及び CSIRTs ネット

ワークは，協力及び適格な情報の共有に関する手続上の覚書を合意すべきである。その覚書は，サイバーな脅威及び大きなサイバーセキュリティインシデントに関する適格な情報を共有すること，国境を越えるサイバーハブの間で使用される最新のツールの経験，とりわけ，人工知能及びデータ分析の技術の経験が CSIRTs ネットワークの間で共有されることを確保することを含み得る。

Cross-Border Cyber Hubs and the CSIRTs network should cooperate closely to ensure synergies and complementarity of activities. For that purpose, they should agree on procedural arrangements on cooperation and the sharing of relevant information. This could include the sharing of relevant information on cyber threats and significant cybersecurity incidents and ensuring that experience with state-of-the-art tools, in particular artificial intelligence and data analytics technology, used within the Cross-Border Cyber Hubs, is shared with the CSIRTs network.

(21) 適格な当局間において共有された状況認識は，大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントと関連する欧州連合全域の準備態勢と調整のための欠くことのできない前提条件である。指令(EU) 2022/2555 は，大規模なサイバーセキュリティインシデント及び危機の運用レベルにおける調整された運営管理を支援するため，また，構成国並びに欧州連合の機関，組織，事務局及び部局の間における適格な情報の定期的な交換を確保するため，EU-CyCLONe を設けた。指令(EU) 2022/2555 は，全ての構成国間における迅速かつ実効的な運用上の協力を促進するため，CSIRTs ネットワークも設けた。国境を越えるサイバーハブが潜在的なまたは進行中の大規模なサイバーセキュリティインシデントと関連する情報を獲得する状況において，状況認識を確保するため及び結束を強化するため，国境を越えるサイバーハブは，CSIRTs ネットワークに対して適格な情報を提供すべきであり，かつ，EU-CyCLONe に対して早期警戒として連絡すべきである。とりわけ，状況の相違により，共有される情報は，技術情報，攻撃者または潜在的な攻撃者の性質と動機に関する情報，及び，潜在的なまたは進行中の大規模なサイバーセキュリティインシデントに関するより高度なレベルの非技術情報を含み得る。その過程において，知る必要性の原則に対し，及び，共有される情報の潜在的に機微な性質に対し，注意が払われるべきである。指令(EU) 2022/2555 は，欧州議会及び理事会の決定 No 1313/2013/EU[13]によって設けられた欧州連合市民保護の仕組み（UCPM）における欧州委員会の職責，及び，理事会実装決定(EU) 2018/1993[14]による EU 統合政治的危機対応覚書（IPCR 覚書）に関する分析報告書を提供する欧州委員会の職責も繰り返している。国境を越えるサイバーハブが，潜在的なまたは現在進行中の大規模なサイバーセキュリティインシデントと関連する適格な情報及び早期警戒を EU-CyCLONe 及び CSIRTs ネットワークとの間で共有するときは，当該情報が，それらのネットワークを介して，構成国の当局及び欧州委員会との間で共有されることが重要である。その点に関して，指令(EU) 2022/2555 は，EU-CyCLONe の目的が，大

[13] 欧州連合の市民保護の仕組みに関する欧州議会及び理事会の 2013 年 12 月 17 日の決定 No 1313/2013/EU (OJ L 347, 20.12.2013, p. 924).
Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

[14] EU 統合政治的危機対応覚書に関する 2018 年 12 月 11 日の理事会実装決定(EU) 2018/1993 (OJ L 320, 17.12.2018, p. 28).
Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28).

規模なサイバーセキュリティインシデント及び危機の運用レベルにおける調整された運営管理を支援すること，そして，構成国並びに欧州連合の機関，組織，事務局及び部局の間における適格な情報の定期的な交換を確保することにあると定めている。EU-CyCLONe の職務は，そのようなインシデント及び危機の共有された状況認識を開発することを含んでいる。EU-CyCLONe が，その目的及びその職務に沿って，適格な構成国の代表及び欧州委員会に対してそのような情報が迅速に提供されることを確保することは，極めて重要なことである。その目的のために，EU-CyCLONe の手続規則が適切な条項を含めることが不可欠である。

Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant cybersecurity incidents and large-scale cybersecurity incidents. Directive (EU) 2022/2555 established EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies. Directive (EU) 2022/2555 also established the CSIRTs network to promote swift and effective operational cooperation among all Member States. To ensure situational awareness and strengthen solidarity, in situations where Cross-Border Cyber Hubs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to the CSIRTs network and inform, as an early warning, EU-CyCLONe. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level, non-technical information about a potential or ongoing large-scale cybersecurity incident. In that context, due regard should be paid to the need-to-know principle and to the potentially sensitive nature of the information shared. Directive (EU) 2022/2555 also reiterates the Commission's responsibilities in the Union Civil Protection Mechanism (UCPM) established by Decision 1313/2013/EU of the European Parliament and of the Council [13], and its responsibility for providing the analytical reports for the EU Integrated Political Crisis Response Arrangements (IPCR Arrangements) pursuant to Council Implementing Decision (EU) 2018/1993 [14]. Where Cross-Border Cyber Hubs share relevant information and early warnings related to a potential or ongoing large-scale cybersecurity incident with EU-CyCLONe and the CSIRTs network, it is imperative that that information be shared through those networks with Member States' authorities as well as with the Commission. In that respect, Directive (EU) 2022/2555 provides that EU-CyCLONe's purpose is to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies. EU-CyCLONe's tasks include developing a shared situational awareness of such incidents and crises. It is of paramount importance that EU-CyCLONe ensure, in line with that purpose and its tasks, that such information is provided immediately to the relevant Member State representatives and to the Commission. To that end, it is crucial that EU-CyCLONe's rules of procedure include appropriate provisions.

(22) 欧州サイバーセキュリティ警報システムに参加している法主体は，しかるべく，データのフォーマット，分類法，データの取扱い及びデータ分析ツールに関するものを含め，その法主体間における高いレベルの相互運用性を確保すべきである。それらの法主体は，安全な通信経路，ミニマムなレベルのアプリケーション層のセキュリティ，状況認識ダッシュボード及び諸指標も確保すべきである。共通分類法の採択及び検出されたサイバーな脅威とリスクの原因を記述するための状況報告書のためのテンプレートの開発は，指令(EU) 2022/2555 の実装の過程において行われた既存の作業を考慮に

入れるべきである。

Entities participating in the European Cybersecurity Alert System should ensure a high level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analytics tools. They should also ensure secure communications channels, a minimum level of application layer security, a situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the causes of detected cyber threats and risks, should take into account existing work done in the context of the implementation of Directive (EU) 2022/2555.

(23) 様々な情報源からのサイバーな脅威に関する適格なデータ及び情報を大規模ベースで，信頼できかつ安全な環境の中において交換できるようにするため，欧州サイバーセキュリティ警報システムに参加している法主体は，最新で高度に安全なツール，機器及びインフラ並びに高い技能をもつ担当者を具備すべきである。このことは，とりわけ，最新の人工知能技術及びデータ分析技術を使用することによって，集団的な検出能力及び当局及び適格な法主体に対する適時の警報を向上させることを可能にすべきである。

In order to enable the exchange of relevant data and information on cyber threats from various sources, on a large-scale basis, in a trusted and secure environment, entities participating in the European Cybersecurity Alert System should be equipped with state-of-the-art, highly secure tools, equipment and infrastructure, as well as skilled personnel. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, in particular by using the latest artificial intelligence and data analytics technologies.

(24) 適格なデータ及び情報を収集すること，分析すること，共有すること及び交換することによって，欧州サイバーセキュリティ警報システムは，サイバーセキュリティ，競争力及び回復力の分野における欧州連合の技術上の主権及びオープンな戦略上の自律性を拡大すべきである。高品質のキュレートされたデータをプールすることは，高度な人工知能技術及びデータ分析技術の開発にも貢献し得る。人間による監視及びその目的のための高度な技能をもつ労働力は，高品質なデータの実効的なプールのために必須なままである。

By collecting, analysing, sharing and exchanging relevant data and information, the European Cybersecurity Alert System should enhance the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, competitiveness and resilience. The pooling of high-quality, curated data could also contribute to the development of advanced artificial intelligence and data analytics technologies. Human oversight and, to that end, a skilled labour force remains essential for the effective pooling of high-quality data.

(25) 欧州サイバーセキュリティ警報システムは，民間のプロジェクトではあるが，サイバー防衛のコミュニティは，不可欠なインフラの防護のために開発された民間のより強力な検出能力及び状況認識能力から受益し得る。

While the European Cybersecurity Alert System is a civilian project, the cyber defence community could benefit from

stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure.

(26) 欧州サイバーセキュリティ警報システムの参加者の間における情報共有は，既存の法律上の諸要件，及び，とりわけ，欧州連合と国内のデータ保護法，並びに，情報の交換を規律している欧州連合の競争に関する規定を遵守すべきである。情報の受領は，個人データの処理が必要である限り，データ主体の権利及び自由を守り，述べられた目的のためにその個人データが必要ではなくなったときは速やかにそのデータを破壊し，かつ，そのデータを利用している法主体に対してデータが破壊されたことを連絡する技術上の措置及び組織上の措置を実装すべきである。

Information sharing among participants of the European Cybersecurity Alert System should comply with existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information. The recipient of the information should implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects, and destroy the data as soon as they are no longer necessary for the stated purpose and inform the entity making the data available that the data have been destroyed.

(27) 機密性及び情報セキュリティを維持することは，欧州サイバーセキュリティ警報システムの過程における情報の共有もしくは交換を推進するためであるか，サイバーセキュリティ緊急メカニズムの下にある支援を申込んでいる法主体の利益を維持するためであるか，または，欧州サイバーセキュリティインシデント見直しメカニズムの下における報告書が，そのインシデントによって影響を受けた法主体に対して負の影響をもつことなしに学習された有用な教訓を得ることができることを確保するためであるかの別を問わず，この規則の 3 つの柱全てにとって極めて重要なことである。それらの仕組みにおける構成国及び法主体の参加は，それらの仕組みのコンポーネント間における信頼関係に依拠している。欧州連合の規定または国内規定により情報が機密のものであるときは，この規則の下におけるその情報の共有または交換は，その共有または交換の目的のために適格でありかつ比例的であるところに限定されるべきである。その共有または交換は，関係する法主体のセキュリティ及び商業上の利益を保護することを含め，当該情報の機密性も維持すべきである。この規則による情報の共有または交換は，非開示の合意またはトラフィックライトプロトコル（TLP）のような情報伝達に関するガイドを用いて起き得る。TLP は，情報の別の目的による拡散と関連する制限に関する情報を提供するための手段として理解されなければならない。TLP は，ほとんど全ての CSIRTs 及び幾つかの ISACs において用いられている。それらの一般的な要件に加え，欧州サイバーセキュリティ警報システムに関しては，ホスティングコンソーシアムの合意は，関係する国境を越えるサイバーハブ内における情報共有のための条件に関する細目的な規定を定めるべきである。その合意は，とりわけ，欧州連合法及び国内法に従っている場合に限り，情報が共有されることを要求し得る。

Preserving confidentiality and information security are of paramount importance for all three pillars of this Regulation, whether for encouraging the sharing or exchange of information in the context of the European Cybersecurity Alert System, preserving the interests of the entities applying for support under the Cybersecurity Emergency Mechanism, or ensuring that reports under the European Cybersecurity Incident Review Mechanism can yield useful lessons learned without having a negative impact on the entities affected by the incidents. The participation of Member States and entities

in those mechanisms depend on relationships of trust between their components. Where information is confidential pursuant to Union or national rules, its sharing or exchange under this Regulation should be limited to that which is relevant and proportionate to the purpose of the sharing or exchange. That sharing or exchange should also preserve the confidentiality of that information, including protecting the security and commercial interests of any entities concerned. Information sharing or exchange pursuant to this Regulation could take place using non-disclosure agreements, or guidance on information distribution such as the traffic light protocol (TLP). The TLP is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all CSIRTs and in some ISACs. In addition to those general requirements, when it comes to the European Cybersecurity Alert System, Hosting Consortia agreements should lay down specific rules regarding the conditions for information sharing within the Cross-Border Cyber Hub concerned. Those agreements could, in particular, require that information be shared only in accordance with Union and national law.

(28) EU サイバーセキュリティリザーブの設置に関し，個別の機密性の規定が必要である。危機の過程において及び機微の部門の中で業務運営している法主体との関係において，支援が要求され，評価され及び提供される。EU サイバーセキュリティリザーブが実効的に機能するために，ユーザと法主体が，要求の評価及び支援の配置においてその法主体の役割を果たすために個々の法主体とって必要となる全ての情報を共有でき，かつ，その全ての情報に対するアクセスを遅滞なく提供できることは，必須である。従って，この規則は，EU サイバーセキュリティリザーブの運用のために必要な場合に限り，全てのそのような情報が使用されまたは共有されること，並びに，欧州連合法及び国内法によって秘密であるとされまたは機密とされている情報が，当該法律に従う場合に限り使用されまたは共有されることを定めるべきである。加えて，ユーザは，それが適切なときは，制限の細目を別途定めるために，TLP のような情報共有プロトコルを利用できるべきである。ユーザはこの点に関して裁量権をもつけれども，そのような制限を適用する際，そのユーザが，とりわけ，要求されたサービスの遅延した評価または供給と関連してあり得る結果を考慮に入れることが重要である。効率的な EU サイバーセキュリティリザーブをもつため，ユーザが要求を提出する前に，契約している当局が，そのユーザに対し，そのあり得る結果を明確にすることが重要である。それらの安全確保は，EU サイバーセキュリティリザーブのサービスの要求及び提供に限定され，かつ，EU サイバーセキュリティリザーブの調達における場合のような，別の過程における情報交換に対しては影響を与えない。

In respect of the deployment of the EU Cybersecurity Reserve, specific confidentiality rules are necessary. Support will be requested, assessed and provided in a crisis context and in respect of entities operating in sensitive sectors. For the EU Cybersecurity Reserve to function effectively, it is essential that users and entities are able to share, and provide access, without delay, to all information that is necessary for each entity to play its part in the assessment of requests and the deployment of support. Accordingly, this Regulation should provide that all such information is to be used or shared only where necessary for the operation of the EU Cybersecurity Reserve, and that information that is confidential or classified pursuant to Union and national law is to be used and shared only in accordance with that law. Additionally, users should be able, where appropriate, to use information-sharing protocols such as the TLP to further specify limitations. Whilst users have discretion in this regard, it is important that when applying such limitations, they take into account the possible consequences, in particular with regard to delayed assessment or delivery of the requested services. In order to have an efficient EU Cybersecurity Reserve, it is important that the contracting authority clarify those consequences to the user

before it submits a request. Those safeguards are limited to the request and provision of EU Cybersecurity Reserve services and do not affect information exchange in other contexts, such as in the procurement of the EU Cybersecurity Reserve.

(29) 構成国に影響を与えているリスクの増加及びインシデントの数を考慮し，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対する欧州連合の回復力を向上させるため，そして，準備態勢，インシデント対応及び必須サービスの最初の復旧のための緊急の資金支援を介して，構成国の活動を補うため，危機支援の法律文書，すなわち，サイバーセキュリティ緊急メカニズムを定める必要がある。インシデントからの全面復旧は，インシデントによって影響を受けた法主体の稼動をそのインシデントの前からある状態へと修復する包括的な過程であり，また，大きな費用を伴う長い過程であり得るので，EU サイバーセキュリティリザーブからの支援は，システムの基本的な機能性の修復を導く復旧過程の最初の段階に限定されるべきである。サイバーセキュリティ緊急メカニズムは，定義された状況の下においてかつ明確な条件の下で，迅速かつ実効的な補助を配置できるようにすべきであり，また，資源がどのように使用されたかを注意深く監視及び評価できるようにすべきである。インシデント及び危機を防止すること，それに対して準備すること及び対応することの主たる職責は構成国にあるが，サイバーセキュリティ緊急メカニズムは，欧州連合条約（TEU）の第 3 条第 3 項に従い，構成国間の結束を促進する。

In view of the increasing risks and number of incidents affecting Member States, it is necessary to set up a crisis support instrument, namely the Cybersecurity Emergency Mechanism, to improve the Union's resilience to significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, incident response and initial recovery of essential services. As the full recovery from an incident is a comprehensive process of restoring the functioning of the entity affected by the incident to the state from before the incident and could be a long process that entails significant costs, the support from the EU Cybersecurity Reserve should be limited to the initial stage of the recovery process, leading to the restoration of basic functionalities of the systems. The Cybersecurity Emergency Mechanism should enable the rapid and effective deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to incidents and crises lies with the Member States, the Cybersecurity Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union (TEU).

(30) サイバーセキュリティ緊急メカニズムは，構成国に対し，構成国自身の措置及び資源を補う支援を提供すべきであり，また，大きなサイバーセキュリティインシデント及び大規模サイバーセキュリティインシデントに対する対応及びそれらからの最初の復旧の場合において，ENISA の任務に従って ENISA から提供されるサービス，CSIRTs ネットワークからの調整された対応と補助，EU-CyCLONe からの緩和支援，並びに，TEU の第 42 条第 7 項及び理事会決定(CFSP) 2017/2315[15]によって設置され

[15] 常設の構造化された協力体制（PESCO）を設置し及び参加構成国のリストを決定する 2017 年 12 月 11 日の理事会決定(CFSP) 2017/2315 (OJ L 331, 14.12.2017, p. 57).

た常設の構造化された協力体制（PESCO）のサイバー緊急対応チームの文脈におけるものを含め構成国間の相互補助のような，既存の他の支援の選択肢を提供すべきである。サイバーセキュリティ緊急メカニズムは，欧州連合全域にわたる及び DEP と関係をもつ第三国におけるそのようなインシデントの対応準備，それに対する対応及びそれからの復旧を支援するために特化された手段が利用可能であることを確保する必要性に対処すべきである。

The Cybersecurity Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in the case of response to, and initial recovery from, significant cybersecurity incidents and large-scale cybersecurity incidents, such as the services provided by ENISA in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) TEU and the permanent structured cooperation (PESCO) Cyber Rapid Response Teams established pursuant to Council Decision (CFSP) 2017/2315[15]. It should address the need to ensure that specialised means are available to support preparedness for, response to and recovery from such incidents across the Union and in DEP-associated third countries.

(31) この規則は，欧州連合レベルの危機対応を調整するための手続及び枠組み，とりわけ，指令(EU) 2022/2555，欧州議会及び理事会の決定 No 1313/2013/EU[16]によって設けられた欧州連合市民保護の仕組み，IPCR 覚書及び委員会勧告(EU) 2017/1584[17]を妨げない。サイバーセキュリティ緊急メカニズムの下において提供される支援は，サイバーセキュリティ緊急メカニズムの民間という性質を考慮に入れた上で，サイバー緊急対応チームを介するものを含め，共通の外交及び安全保障政策及び共通の安全保障及び国防政策の文脈において提供される補助を補い得る。サイバーセキュリティ緊急メカニズムの下において提供される支援は，ある構成国から別の構成国に対して提供される補助，または，欧州連合と構成国間のもしくは TFEU の第 222 条に示す状況における共同対応の一部をなすものを含め，TEU の第 42 条第 7 項の文脈において実装される活動を補い得る。この規則の実装は，それが適切なときは，サイバー外交ツールボックスの下にある措置の実装との間で調整され得るべきである。

This Regulation is without prejudice to procedures and frameworks to coordinate crisis responses at Union level, in particular Directive (EU) 2022/2555, the Union Civil Protection Mechanism established by Decision No 1313/2013/EU of the European Parliament and of the Council[16], the IPCR Arrangements and Commission Recommendation (EU)

Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States (OJ L 331, 14.12.2017, p. 57).

[16] 欧州連合の市民保護の仕組みに関する欧州議会及び理事会の 2013 年 12 月 17 日の決定 No 1313/2013/EU (OJ L 347, 20.12.2013, p. 924).

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

[17] 大規模なサイバーセキュリティインシデント及び危機に対する調整された対応に関する 2017 年 9 月 13 日の委員会勧告(EU) 2017/1584 (OJ L 239, 19.9.2017, p. 36).

Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

2017/1584[17]. Support provided under the Cybersecurity Emergency Mechanism can complement assistance provided in the context of the common foreign and security policy and the common security and defence policy, including through the Cyber Rapid Response Teams, taking into account the civilian nature of the Cybersecurity Emergency Mechanism. Support provided under the Cybersecurity Emergency Mechanism can complement actions implemented in the context of Article 42(7) TEU, including assistance provided by one Member State to another Member State, or form part of the joint response between the Union and Member States or in situations referred to in Article 222 TFEU. The implementation of this Regulation should also be coordinated with the implementation of measures under the Cyber Diplomacy Toolbox, where appropriate.

(32) この規則の下において提供される補助は，国内レベルにおいては，構成国によってとられる活動を支援するものでありかつそれを補うものであるべきである。その目的のために，欧州委員会，ENISA，構成国，及び，それが適格なときは，ECCC の間の緊密な協力及び意見聴取が確保されるべきである。サイバーセキュリティ緊急メカニズムの下における支援を要請する際，構成国は，支援を求める必要性を正当化する適格な情報を提供すべきである。

Assistance provided under this Regulation should be in support of, and complementary to, the actions taken by Member States at national level. To that end, close cooperation and consultation between the Commission, ENISA, the Member States and, where relevant, the ECCC should be ensured. When requesting support under the Cybersecurity Emergency Mechanism, Member States should provide relevant information justifying the need for support.

(33) 指令(EU) 2022/2555 は，構成国に対し，1 または複数のサイバー危機管理当局を指定または設置すること，及び，当該当局が，実効的かつ効率的な態様で当該当局の職務を遂行するための十分な資源をもつことを確保することを要求している。指令(EU) 2022/2555 は，構成国に対し，危機の場合において配置され得る実現能力，資産及び手続を特定すること，並びに，大規模なサイバーセキュリティインシデント及び危機の管理のための目標と手立てを定める大規模なサイバーセキュリティインシデント及び危機の国内対応計画を採択することも要求している。構成国は，明確に定義されたプロセスに従ったインシデントの取扱いの職責を負い，少なくとも同指令の適用範囲の下にある部門，副部門及びタイプの法主体を包摂する 1 または複数の CSIRTs を設けること，並びに，CSIRTs が，CSIRTs の職務を実効的に遂行するための十分な資源をもつことを確保することも要求される。この規則は，指令(EU) 2022/2555 の義務の構成国による遵守を確保することにおける欧州委員会の役割を妨げない。サイバーセキュリティ緊急メカニズムは，準備態勢を強化することを狙いとする活動に対する補助，並びに，大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントの影響を緩和するため，最初の復旧を支援するため，または，高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体から提供されるサービスの基本的な機能性を復旧するためのインシデント対応活動に対する補助を提供すべきである。

Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure that they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as

to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident-handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entity under the scope of that Directive, and to ensure that they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cybersecurity Emergency Mechanism should provide assistance for actions aiming to reinforce preparedness as well as incident response actions to mitigate the impact of significant cybersecurity incidents and large-scale cybersecurity incidents, to support initial recovery or to restore the basic functionalities of the services provided by entities operating in sectors of high criticality or entities operating in other critical sectors.

(34) 一貫性のあるアプローチを促進しかつ欧州連合及びその域内市場を横断してセキュリティを強化するための対応準備活動の一部として，演習及び訓練による場合を含め，指令(EU) 2022/2555 によって識別された高度の不可欠性のある部門において業務運営している法主体のサイバーセキュリティの調整された態様の試験及び評価に対し，支援が提供されるべきである。その目的のために，欧州委員会は，ENISA，NIS 協力グループ及び EU-CyCLONe からの意見聴取を経た上で，欧州連合レベルの調整された準備態勢試験のための資金支援を受ける適格があるべき適格な部門または副部門を定期的に指定すべきである。その部門または副部門は，指令(EU) 2022/2555 の別紙 I の中で列挙された高度の不可欠のある部門から選抜されるべきである。調整された準備態勢試験は，共通のリスクシナリオ及び手法を基礎とすべきである。部門の選抜及びリスクシナリオの開発は，欧州委員会，外交政策及び安全保障政策に関する欧州連合の上級代表（「上級代表」）及び NIS 協力グループによって，適格な民間及び軍の組織と部局及び EU-CyCLONe を含め設けられているネットワークと調整して実施される欧州連合のサイバーポスチャーの開発に関する理事会決議の中で求められている，リスク評価及びリスクシナリオ，並びに，ヌヴェールの閣僚共同要請によって要請され，欧州委員会及び ENISA の支援を受け，欧州議会及び理事会の規則(EU) 2018/1971 [18]によって設けられた電子通信に関する欧州規制当局の組織と協力し，NIS 協力グループによって実施される通信ネットワーク及びインフラのリスク評価，指令(EU) 2022/2555 の第 22 条によって実施される不可欠なサプライチェーンの欧州連合レベルで調整されたセキュリティリスク評価，並びに，欧州議会及び理事会の規則(EU) 2022/2554 [19]の中で定められたデジタル業務運営上の回復力試験のような，適格な欧州連

[18] 電子通信に関する欧州規制当局の組織（BEREC）及び BEREC の支援のための部局（BEREC Office）を設置し，並びに，規則(EU) 2015/2120 を改正し及び規則(EC) No 1211/2009 を廃止する欧州議会及び理事会の 2018 年 12 月 11 日の規則(EU) 2018/1971 (OJ L 321, 17.12.2018, p. 1).

Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009 (OJ L 321, 17.12.2018, p. 1).

[19] 金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009, 規則(EU) No 648/2012, 規則(EU) No 600/2014, 規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014

合全域のリスク評価とリスクシナリオを，重複を避けるべき必要性を含めて，考慮に入れるべきである。部門の選抜は，不可欠なインフラの回復力を強化するための欧州連合全域で調整されたアプローチに関する理事会勧告も考慮に入れるべきである。

As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in sectors of high criticality identified pursuant to Directive (EU) 2022/2555 in a coordinated manner, including through exercise and training. For that purpose, the Commission, after consulting ENISA, the NIS Cooperation Group and EU-CyCLONe, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated preparedness testing at Union level. The sectors or subsectors should be selected from the sectors of high criticality listed in Annex I to Directive (EU) 2022/2555. The coordinated preparedness testing should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture conducted by the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including EU-CyCLONe, as well as the risk assessment of communications networks and infrastructure requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications established by Regulation (EU) 2018/1971 of the European Parliament and of the Council [18], the Union level coordinated security risk assessments of critical supply chains to be conducted pursuant to Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council [19]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

(35) 加えて，サイバーセキュリティ緊急メカニズムは，高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体の調整された準備態勢試験によって包摂されていない，他の対応準備活動に対する支援及び他の部門における対応準備の支援を提供すべきである。それらの活動は，様々なタイプの国内対応準備活動を含み得る。

In addition, the Cybersecurity Emergency Mechanism should provide support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated preparedness testing of entities operating in sectors of high criticality or entities operating in other critical sectors. Those actions could include various types of national preparedness activity.

(36) 構成国が対応準備活動を支援するための補助金を受けるときは，高度の不可欠性のある部門内にある法主体は，任意ベースで，当該活動に参加できる。そのような活動の後，対応準備活動から最大限に受益するために，参加法主体が，個別の措置から帰結する推奨事項を実装するための修復

and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

計画を作成することは，グッドプラクティスである。その活動の一部として，参加法主体がそのような修復計画を作成及び実装することを構成国が要求することは重要なことであるが，構成国は，そのような要求を執行することを義務づけられてはおらず，かつ，この規則によってその権限を与えられてもいない。そのような要求は，指令(EU) 2022/2555 に従った法主体の要件及び職務権限のある当局の監督権限を妨げない。

When Member States receive grants to support preparedness actions, entities in sectors of high criticality can participate in those actions on a voluntary basis. It is good practice that following such actions, participating entities draw up a remediation plan to implement any resulting recommendations of specific measures to benefit to the fullest extent from the preparedness action. While it is important that Member States request as part of the actions, that participating entities draw up and implement such remediation plans, Member States are neither obliged nor empowered by this Regulation to enforce such requests. Such requests are without prejudice to requirements for entities and supervisory powers for competent authorities in accordance with Directive (EU) 2022/2555.

(37) サイバーセキュリティ緊急メカニズムは，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントの影響を緩和するため，最初の復旧を支援するため，または，必須のサービスの稼動を復旧するためのインシデント対応活動に対する支援も提供すべきである。それが適切なときは，サイバーセキュリティ緊急メカニズムは，市民に対するインシデントの影響に対応するための包括的なアプローチを確保するため，UCPM を実装すべきである。

The Cybersecurity Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, to support initial recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impact of incidents on citizens.

(38) サイバーセキュリティ緊急メカニズムは，指令(EU) 2022/2555 の第 11 条第 3 項(f)に示す CSIRTs による場合を含め，ある構成国から，大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントによる影響を受けている別の構成国に対して提供される技術上の補助を支援するべきである。そのような補助を提供する構成国は，相互補助の枠組みの中で専門家チームを派遣することと関連する費用を負担することの要請書を提出することが認められるべきである。要請適格費用は，サイバーセキュリティ専門家の旅費，宿泊費及び日当を含み得る。

The Cybersecurity Emergency Mechanism should support technical assistance provided by one Member State to another Member State that is affected by a significant cybersecurity incident or large-scale cybersecurity incident, including by CSIRTs as referred to in Article 11(3), point (f), of Directive (EU) 2022/2555. Member States providing such assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

(39) 大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントの検出，それに対する準備及びそれに対する対応において民間事業者が果たす必須の役割に鑑み，大規模なサイバーセキュリティインシデント及び危機並びに大規模と均等なサイバーセキュリティインシデント及び危機の場合において報酬なしに事業者がサービスを提供することによるそのような事業者との間の任意のプロボノ協力の価値を認識することが重要である。ENISAは，EU-CyCLONeと協力して，そのようなプロボノの取組みの発展を監視し得るのであり，また，民間事業者の信頼性，民間事業者の経験及び機微の情報を安全な態様で取り扱う能力と関係するものを含め，この規則の下において信頼できるマネージドセキュリティサービスプロバイダに対して適用可能な基準を当該事業者が遵守することを促進し得る。

Given the essential role that private undertakings play in the detection of, preparedness for and response to large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, it is important to recognise the value of voluntary pro bono cooperation with such undertakings, whereby they offer services without remuneration in the case of large-scale cybersecurity incidents and crises and large-scale-equivalent cybersecurity incidents and crises. ENISA, in cooperation with EU-CyCLONe could monitor the evolution of such pro bono initiatives and promote their compliance with the criteria applicable to trusted managed security service providers under this Regulation, including in relation to the trustworthiness of private undertakings, their experience as well as the ability to handle sensitive information in a secure manner.

(40) サイバーセキュリティ緊急メカニズムの一部として，EU サイバーセキュリティリザーブは，構成国，欧州連合の機関，組織，事務局もしくは部局または DEP と関係をもつ第三国に対して影響を与える大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントの場合における対応を支援し及び復旧活動を開始するため，信頼できるマネージドセキュリティサービスプロバイダからのサービスで組成され，段階的に定められるべきである。EU サイバーセキュリティリザーブは，サービスの可用性及び準備態勢を確保すべきである。それゆえ，EU サイバーセキュリティリザーブは，例えば，スタンバイ状態にあり，連絡を受けて直ちに配置可能な能力を含め，事前に確約されているサービスを含めるべきである。EU サイバーセキュリティリザーブからのサービスは，国内レベルにおける当該法主体自身の活動の補完として，高度に不可欠な部門において業務運営している影響を受けた法主体または他の不可欠な部門において業務運営している影響を受けた法主体に対する補助の提供において，国内当局を支援することに資するべきである。EU サイバーセキュリティリザーブからのサービスは，類似の条件の下で，欧州連合の機関，組織，事務局及び部局を支援することにも資することができるべきである。EU サイバーセキュリティリザーブは，調査研究及び技術革新への投資のインセンティブを提供することによる場合を含め，マイクロ企業及び小企業と中規模企業並びにスタートアップを含め，デジタル経済全体にわたり欧州連合内の製造業及びサービス業の競争上の地位を強化することにも貢献し得る。EU サイバーセキュリティリザーブのためのサービスを調達する際，ENISA の欧州サイバーセキュリティ技能枠組みを考慮に入れることが重要である。EU サイバーセキュリティリザーブからの支援を要請する際，ユーザは，当該ユーザの申請書の中に，影響を受けた法主体及び潜在的な影響と関連する適切な情報，要請される EU サイバーセキュリティリザーブからのサービスに関する情報及び影響を受けた法主体に対して国内レベルで提供される支援に関する情報を含めるべきである。それらの

情報は，申請者からの要請を評価する際に考慮に入れられるべきである。影響を受けた法主体にとって利用可能な別の形態の支援との間の補完性を確保するため，その要請書は，それが利用可能なときは，インシデント対応及び最初の復旧サービスのために準備された契約上の手立てに，並びに，そのようなタイプのインシデントに潜在的に適用されている保険契約に関する情報も含めるべきである。

As part of the Cybersecurity Emergency Mechanism, an EU Cybersecurity Reserve should gradually be set up, consisting of services from trusted managed security service providers to support response and initiate recovery actions in the case of significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents affecting Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries. The EU Cybersecurity Reserve should ensure the availability and readiness of services. It should therefore include services that are committed in advance, including for instance capacities that are on stand-by and deployable at short notice. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in sectors of high criticality or to affected entities operating in other critical sectors as a complement to their own actions at national level. The services from the EU Cybersecurity Reserve should also be able to serve to support Union institutions, bodies, offices and agencies, under similar conditions. The EU Cybersecurity Reserve could also contribute to strengthening the competitive position of industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, including by providing incentives for investment in research and innovation. It is important to take into account ENISA's European cybersecurity skills framework when procuring the services for the EU Cybersecurity Reserve. When requesting support from the EU Cybersecurity Reserve, users should include in their application appropriate information regarding the affected entity and potential impact, information about the requested service from the EU Cybersecurity Reserve, and the support provided to the affected entity at the national level, which should be taken into account when assessing the request from the applicant. To ensure complementarity with other forms of support available to the affected entity, the request should also include, where available, information on contractual arrangements in place for incident response and initial recovery services, as well as insurance contracts potentially covering such a type of incident.

(41) 欧州連合の資金の実効的な利用を確保するため，EU サイバーセキュリティリザーブの下において事前に確約されたサービスは，当該サービスが確約されている期間内においては当該事前に確約されたサービスがインシデント対応のために利用されない場合には，適格な契約に従い，インシデントの防止及び対応と関連する対応準備のサービスへと転換され得るべきである。それらのサービスは，ECCC によって運営管理される対応準備活動にとって補完的なものであるべきであり，かつ，その活動と重複してはならない。

In order to ensure the effective use of Union funding, pre-committed services under the EU Cybersecurity Reserve should be convertible, in accordance with the relevant contract, into preparedness services related to incident prevention and response in the event that those pre-committed services are not used for incident response during the time for which they are pre-committed. Those services should be complementary to and should not duplicate the preparedness actions to be managed by the ECCC.

(42) 構成国のサイバー危機管理当局及び CSIRTs からのまたは欧州連合の機関，組織，事務局及び部局の代わりに CERT-EU からの EU サイバーセキュリティリザーブの支援を求める要請は，契約当局によって評価されるべきである。EU サイバーセキュリティリザーブの運営管理及び業務運営を ENISA が受任したときは，その契約当局は，ENISA である。DEP と関係をもつ第三国からの支援を求める要請は，欧州委員会によって評価されるべきである。支援を求める要請の提出及び評価を容易にするため，ENISA は，安全なプラットフォームを設定し得る。

Requests for support from the EU Cybersecurity Reserve from Member States' cyber crisis management authorities and CSIRTs, or CERT-EU on behalf of Union institutions, bodies, offices and agencies, should be assessed by the contracting authority. Where ENISA has been entrusted with the administration and operation of the EU Cybersecurity Reserve, that contracting authority is ENISA. Requests for support from DEP-associated third countries should be assessed by the Commission. To facilitate the submission and assessment of requests for support, ENISA could set up a secure platform.

(43) 複数の競合する要請が受領されている場合，それらの要請は，この規則の中で定められた基準に従って，優先順位が決められるべきである。この規則の一般的な目的に照らし，それらの基準は，インシデントの規模と深刻度，影響を受けた法主体のタイプ，影響を受けた構成国及びユーザに対するインシデントの潜在的な影響，インシデントの潜在的に国境を越える性質及び波及のリスク，並びに，対応及び最初の復旧を補助するためにユーザによって既に講じられた措置を含むべきである。同目的に照らし，かつ，構成国ユーザからの要請が，専ら，欧州連合全域にわたり高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体を支援することを意図するものであることに鑑み，それらの基準が複数の要請に対して均等として評価されることを導くときは，構成国ユーザからの要請に対し，より高い優先順位を与えるのが適切である。構成国が，適格なホスティングの合意の下において，欧州連合の機関，組織，事務局及び部局を防護するため及び補助するための措置を講じなければならないかもしれない義務を妨げない。

Where multiple concurrent requests are received, those requests should be prioritised in accordance with criteria laid down in this Regulation. In light of the general objectives of this Regulation, those criteria should include the scale and severity of the incident, the type of entity affected, the potential impact of the incident on the Member States and users affected, the potential cross-border nature of the incident and risk of spillover, and the measures already taken by the user to assist the response and initial recovery. In light of those objectives and given that requests from Member State users are exclusively intended to support, across the Union, entities operating in sectors of high criticality or entities operating in other critical sectors, it is appropriate to give higher priority to requests from Member State users where those criteria lead to two or more requests being assessed as equal. This is without prejudice to any obligations that Member States may have under relevant hosting agreements to take measures to protect and assist Union institutions, bodies, offices and agencies.

(44) 欧州委員会は，EU サイバーセキュリティリザーブの実装に関し，総括的な職責をもつべきである。サイバーセキュリティ支援活動について ENISA によって得られた豊富な経験に鑑み，ENISA は，EU サイバーセキュリティリザーブを実装するために最も適した部局である。それゆえ，欧州委員会は，EU サイバーセキュリティリザーブの業務運営及び運営管理を，部分的に，または，それが適切であると

欧州委員会が判断するときはその全体について，ENISA に委任すべきである。その委任は，規則(EU, Euratom) 2024/2509 の下において適用可能な規定に従って実施されるべきであり，かつ，とりわけ，履行される拠出合意の署名のための適格な条件に服するべきである。拠出合意の署名の前を含め，ENISA に対して委任されない EU サイバーセキュリティリザーブの業務運営及び運営管理の諸側面は，欧州委員会による直接の運営管理に服するべきである。

The Commission should have overall responsibility for the implementation of the EU Cybersecurity Reserve. Given the extensive experience gained by ENISA with cybersecurity support action, ENISA is the most suitable agency to implement the EU Cybersecurity Reserve. Therefore, the Commission should entrust ENISA, partially or, where the Commission considers it to be appropriate, entirely with the operation and administration of the EU Cybersecurity Reserve. The entrustment should be carried out in accordance with the applicable rules under Regulation (EU, Euratom) 2024/2509 and in particular should be subject to the relevant conditions for signing a contribution agreement being fulfilled. Any aspects of the operation and administration of the EU Cybersecurity Reserve not entrusted to ENISA should be subject to direct management by the Commission, including prior to the signing of the contribution agreement.

(45) 構成国は，EUサイバーセキュリティリザーブの創立，配置及び配置後において鍵となる役割をもつ。規則(EU) 2021/694 は，EU サイバーセキュリティリザーブを実装する活動のための適格な基礎法行為であるので，EU サイバーセキュリティリザーブの下にある活動は，規則(EU) 2021/694 の第 24 条に示す作業計画の中で定められるべきである。同条第 6 項により，その作業計画は，審議手続に従った実装行為により，欧州委員会によって採択されるべきである。更に，欧州委員会は，NIS 協力グループとの間で調整し，EU サイバーセキュリティリザーブの優先順位及び発展を判断すべきである。

Member States should have a key role in the constitution, deployment and post-deployment of the EU Cybersecurity Reserve. As Regulation (EU) 2021/694 is the relevant basic act for actions implementing the EU Cybersecurity Reserve, the actions under the EU Cybersecurity Reserve should be provided for in the work programmes referred to in Article 24 of Regulation (EU) 2021/694. Pursuant to paragraph 6 of that Article, those work programmes are to be adopted by the Commission by means of implementing acts in accordance with the examination procedure. Furthermore, the Commission, in coordination with the NIS Cooperation Group, should determine the priorities and the evolution of the EU Cybersecurity Reserve.

(46) EU サイバーセキュリティリザーブの枠組み内で締結される契約は，事業者対事業者の関係に対し及び影響を受けた法主体またはユーザとサービス提供者との間の既存の義務に対して影響を与えてはならない。

The contracts established within the framework of the EU Cybersecurity Reserve should not affect the business-to-business relationship and existing obligations between the affected entity or users and the service provider.

(47) EU サイバーセキュリティリザーブの文脈においてサービスを提供する民間のサービスプロバイダを選抜する目的のために，構成国の当局，高度の不可欠性のある部門で業務運営している法主体及び他の不可欠な部門において業務運営している法主体の需要に適合することを確保するため，当

該プロバイダを選抜するための入札の募集の中に含められるべきミニマムの基準及び要件のセットを定める必要がある。構成国の個別の需要に対処するため，EU サイバーセキュリティリザーブのためのサービスを調達する際，契約当局は，それが適切なときは，この規則に定めるものに付加して，選抜の基準及び要件を策定すべきである。地域レベル及び地方レベルで能動的なより小さなプロバイダの参加を奨励することが重要である。

For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria and requirements that should be included in the call for tenders to select those providers, so as to ensure that the needs of Member States' authorities, entities operating in sectors of high criticality and entities operating in other critical sectors are met. In order to address the specific needs of Member States, when procuring services for the EU Cybersecurity Reserve, the contracting authority should, where appropriate, develop selection criteria and requirements additional to those laid down in this Regulation. It is important to encourage the participation of smaller providers, active at regional and local level.

(48) EU サイバーセキュリティリザーブへの包摂のためにプロバイダを選抜する際，契約当局は，EU サイバーセキュリティリザーブが，全体としては，ユーザの言語の要件に適応できるプロバイダを包摂することを確保することを狙いとすべきである。その目的のために，契約当局は，入札条件を準備する前に，EU サイバーセキュリティリザーブの潜在的なユーザが特定の言語要件をもつか否かを調査し，EU サイバーセキュリティリザーブの支援サービスが，欧州連合の機関の公用語または構成国の公用語中の，ユーザまたは影響を受けた法主体によって理解される見込みのある言語によって提供され得るようにすべきである。EU サイバーセキュリティリザーブの支援サービスの提供のために複数の言語がユーザから要求され，かつ，当該ユーザのためのそれらの複数の言語で当該サービスが調達された場合，そのユーザは，EU サイバーセキュリティリザーブの支援の要請の中で，その要請を生じさせている特定のインシデントとの関係において，どの言語でそのサービスが提供されるべきかを指定できるべきである。

When selecting providers for inclusion in the EU Cybersecurity Reserve, the contracting authority should aim to ensure that the EU Cybersecurity Reserve, when taken as a whole, contains providers that are able to accommodate users' language requirements. To that end, the contracting authority should, before preparing tender specifications, inquire whether the potential users of the EU Cybersecurity Reserve have specific language requirements, so that EU Cybersecurity Reserve support services can be provided in a language from among the official languages of the Union institutions or of the Member States, likely to be understood by the user or affected entity. In the case that more than one language is required by a user for the provision of EU Cybersecurity Reserve support services and those services have been procured in those languages for that user, the user should be able to specify, in the request for EU Cybersecurity Reserve support, in which of those languages the services should be provided in relation to the specific incident giving rise to the request.

(49) EU サイバーセキュリティリザーブの設置を支援するため，欧州委員会が，ENISA に対し，サイバーセキュリティ緊急メカニズムによって包摂される分野において，規則(EU) 2019/881 によるマネージドセキュリティサービスのための候補サイバーセキュリティ認定制度を準備することを要請することが重要で

ある。

To support the establishment of the EU Cybersecurity Reserve, it is important that the Commission requests ENISA to prepare a candidate cybersecurity certification scheme for managed security services pursuant to Regulation (EU) 2019/881, in the areas covered by the Cybersecurity Emergency Mechanism.

(50) 共有された状況認識を促進し，欧州連合の回復力を拡大し並びに大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントに対する実効的な対応を実現可能にするというこの規則の目的を支援するため，欧州委員会または EU-CyCLONe は，CSIRTs ネットワークの支援を得て，かつ，関係する構成国の承諾を得て，ENISA に対し，特定の大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントと関係するサイバーな脅威，既知の悪用可能な脆弱性及び緩和の活動を見直すこと及び評価することを要請できるべきである。インシデントの見直し及び評価の完了後，ENISA は，関係する構成国，民間部門からの代表を含め適格な利害関係者，欧州委員会並びに欧州連合の他の適格な機関，組織，事務局及び部局と共働して，インシデントの見直しの報告書を準備すべきである。民間部門からの代表を含め適格な利害関係者との間の共働を基礎として，特定のインシデントに関する見直しの報告書は，そのインシデントが起きた後において，インシデントの原因，影響及び緩和を評価することを狙いとすべきである。この規則によって求められる最高度の職業上の完全性，公平性及び必要な技術上の専門知識という条件を満たすマネージドセキュリティサービスプロバイダによって共有されている入力及び教訓に対し，特に注意が払われるべきである。その報告書は，EU-CyCLONe，CSIRTs ネットワーク及び欧州委員会に対して配られるべきであり，かつ，EU-CyCLONe，CSIRTs ネットワーク及び欧州委員会の仕事並びに ENISA の仕事を情報伝達するために利用されるべきである。インシデントが DEP と関係をもつ第三国と関係しているときは，欧州委員会は，上級代表に対しても，その報告書を提供すべきである。

In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing the Union's resilience and enabling effective response to significant cybersecurity incidents and large-scale cybersecurity incidents, the Commission or EU-CyCLONe should be able to request ENISA, with the support of the CSIRTs network and with the approval of the Member States concerned, to review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with the Member State concerned, relevant stakeholders, including representatives from the private sector, the Commission and other relevant Union institutions, bodies, offices and agencies. Building on the collaboration with stakeholders, including from the private sector, the review report on specific incidents should aim to assess the causes, impact and mitigation of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered to EU-CyCLONe, the CSIRTs network and the Commission and should be used to inform their work as well as that of ENISA. Where the incident relates to a DEP-associated third country, the Commission should also provide the report to the High Representative.

(51) サイバー攻撃の予測できないという性質及びサイバー攻撃がしばしば特定の地理的な領域の中に

収まることなく高度の波及のリスクを呈しているということを考慮に入れた上で，近隣諸国の回復力及び大きなサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対して実効的に対応するための近隣諸国の能力を強化することは，欧州連合，及び，とりわけ，その域内市場及び産業界の全体としての保護に貢献する。そのような活動は，欧州連合のサイバー外交に対して更に貢献し得る。それゆえ，DEP と関係をもつ第三国は，当該第三国が DEP と関係をもつ合意の中でそのことが定められているときは，当該第三国の領土の全部または一部において，EU サイバーセキュリティリザーブからの支援を要請できるべきである。DEP と関係をもつ第三国に対する資金提供は，適格なパートナーシップ及び当該の国々に関する資金提供文書の枠組みの中で，欧州連合によって支えられるべきである。支援は，大きなサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントに対する対応及びそれからの最初の復旧の分野におけるサービスを包摂すべきである。

Taking into account the unpredictable nature of cyberattacks and the fact that they are often not contained in a specific geographical area and pose a high risk of spillover, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents contributes to the protection of the Union, and in particular its internal market and industry, as a whole. Such activities could further contribute to the Union's cyber diplomacy. Therefore, DEP-associated third countries should be able to request support from the EU Cybersecurity Reserve, in all or part of their territories, where this is provided for in the agreement through which the third country is associated to the DEP. The funding for DEP-associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and initial recovery from significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents.

(52) この規則の中で EU サイバーセキュリティリザーブ及び信頼できるマネージドセキュリティサービスプロバイダに関して定められた諸条件は，DEP と関係をもつ第三国に対して支援を提供する際，適用されるべきである。DEP と関係をもつ第三国は，高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体であり，かつ，その法主体のために当該第三国が EU サイバーセキュリティリザーブからの支援を要請する場合，及び，検出されたインシデントが業務運営上の大きな混乱を導き，または，欧州連合内への波及効果をもち得る場合においては，EU サイバーセキュリティリザーブからの支援を要請できるべきである。DEP と関係をもつ第三国は，当該第三国が DEP と関係をもつ合意の中でそのような支援が特に定められている場合に限り，支援を受ける適格をもつべきである。加えて，そのような第三国は，3 つの基準が満たされている限り，適格をもち続けるべきである。第一に，その第三国は，当該合意の適格な諸条件を全面的に遵守しているべきである。第二に，EU サイバーセキュリティリザーブの補完的な性質に鑑み，その第三国は，大きなサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントに対して対応準備するための適切な手立てを講じているべきである。第三に，EU サイバーセキュリティリザーブからの支援の提供は，当該の国に対する欧州連合の基本政策及び当該の国との間の全体的な関係と一貫性があり，かつ，セキュリティの分野における欧州連合の他の基本政策と一貫性があるべきである。第三の基準の遵守についての欧州委員会の評価の過程において，欧州委員会は，そのような支援を与えることを共通の外交及び安全保障政策と揃えることに関し，上

級代表から意見聴取すべきである。

The conditions set for the EU Cybersecurity Reserve and trusted managed security service providers in this Regulation should apply when providing support to DEP-associated third countries. DEP-associated third countries should be able to request support from the EU Cybersecurity Reserve where the entities targeted and for which they request support from the EU Cybersecurity Reserve are entities operating in sectors of high criticality or entities operating in other critical sectors and where the incidents detected lead to significant operational disruptions or might have spillover effects in the Union. DEP-associated third countries should only be eligible to receive support where the agreement through which they are associated to the DEP specifically provides for such support. In addition, such third countries should remain eligible only so long as three criteria are fulfilled. First, the third country should be complying in full with the relevant terms of that agreement. Second, given the complementary nature of the EU Cybersecurity Reserve, the third country should have taken adequate steps to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents. Third, the provision of support from the EU Cybersecurity Reserve should be consistent with the Union's policy towards and overall relations with that country and with other Union policies in the field of security. In the context of its assessment of the compliance with that third criterion, the Commission should consult the High Representative for the alignment of the granting of such support with the common foreign and security policy.

(53) DEP と関係をもつ第三国に対する支援の提供は，共通の外交及び安全保障政策及び共通の安全保障及び国防政策の文脈におけるものを含め，第三国との間の関係及び欧州連合の安全保障政策に対して影響を与え得る。従って，理事会に対し，そのような支援が提供され得る期間を承認し及び指定する実装権限が与えられることが適切である。理事会は，欧州委員会の 3 つの基準の評価を適正に評価に入れた上で，欧州委員会の提案を基礎として行為すべきである。そのような実装行為の改正に対し及び改正または廃止の提案に対し，同じことが適用されるべきである。例外的な状況において，3 つ目の基準との関係において状況の大きな変化があったと理事会が判断するときは，理事会は，欧州委員会の提案を待つことなく，理事会自身の発意により，実装行為を改正または廃止するために行為できるべきである。そのような大きな変化は，緊急の措置を要することがあり得るが，第三国との関係に対してとりわけ重要な意味をもち得るが，欧州委員会による事前の詳細な評価を要しないことがあり得る。更に，欧州委員会は，DEP と関係をもつ第三国からの支援の要請及びそのような第三国に対して与えられる支援の実装に関し，上級代表と協力すべきである。欧州委員会は，そのような要請及び支援に関して ENISA から提供された見解も考慮に入れるべきである。欧州委員会は，理事会に対し，その結果に関して行われた適格な判断を含め，要請の評価の結果に関して及び配置されるサービスに関して，連絡すべきである。

The provision of support to DEP-associated third countries may affect relations with third countries and the Union's security policy, including in the context of the common foreign and security policy and the common security and defence policy. Accordingly, it is appropriate for the Council to be granted implementing powers to authorise and specify the period during which such support can be provided. The Council should act on the basis of a Commission proposal, taking due account of the Commission's assessment of the three criteria. The same should apply to renewals and to proposals to amend or repeal such acts. Where, in exceptional circumstances, the Council considers there to have been a significant change of circumstances in respect of the third criterion, the Council should be able to act on its own initiative to amend or

repeal an implementing act, without awaiting a Commission proposal. Such significant changes are likely to require urgent action, to have particularly important implications for relations with third countries, and not to require detailed assessment in advance by the Commission. Moreover, the Commission should cooperate with the High Representative in respect of requests for support from DEP-associated third countries and the implementation of support granted to such third countries. The Commission should also take into account any views provided by ENISA in respect of such requests and support. The Commission should inform the Council about the outcome of the assessment of the requests, including relevant considerations made in that regard, and the services that are deployed.

(54) サイバー技能アカデミーに関する 2023 年 4 月 18 日の委員会通知は，高度な技能をもつ職業人の払底を認めている。この規則の目的を追求するためには，そのような技能が必要である。欧州連合は，サイバー攻撃を防止，検出及び抑止するため，並びに，欧州連合の最も不可欠なインフラを含め，欧州連合をそのような攻撃に抗して防護し，かつ，欧州連合の回復力を確保するための技能と能力をもつ職業人を緊急に必要としている。その目的のために，民間部門からの者を含め利害関係者，学術及び公的部門の間における協力を推進することが重要である。頭脳流出を避けるため，または，ある地域で他の地域よりも技術の格差が拡大することを避けるための安全確保の創設を促進するため，教育及び訓練への投資に関し，欧州連合の全領土内において，相乗効果をつくり出すことは，同様に重要なことである。デジタル統治の設計における女性の存在と参加を促進するため，サイバーセキュリティ就労者におけるジェンダー格差を削減することに重点を置いて，サイバーセキュリティ技能の格差を埋めることが急務である。

The Commission communication of 18 April 2023 on the Cyber Skills Academy acknowledged the shortage of skilled professionals. Such skills are needed to pursue the objectives of this Regulation. The Union urgently needs professionals with the skills and competences to prevent, detect and deter cyberattacks and defend the Union, including its most critical infrastructure, against such attacks and ensure its resilience. To that end, it is important to encourage cooperation among stakeholders, including from the private sector, academia and public sector. It is equally important to create synergies, in all territories of the Union, for investment in education and training to promote the creation of safeguards to avoid a brain drain or the widening of the skills gap in some regions more than in others. It is urgent that the cybersecurity skills gap, with a particular focus on reducing the gender gap in the cybersecurity workforce to promote women's presence and participation in the design of digital governance, be closed.

(55) デジタル単一市場における技術革新を推進するため，そのいずれもがこの規則の目的である構成国の回復力及び欧州連合のオープンな戦略上の自律性を増加させることに貢献するという観点から，サイバーセキュリティにおける調査研究及び技術革新を強化することが重要である。民間部門，市民社会及び学術からの者を含め，異なる利害関係者間の協力と調整を強化するため，相乗効果は，必須である。

In order to boost the innovation in the Digital Single Market, strengthening research and innovation in cybersecurity is important, with a view to contributing to increasing the resilience of Member States and the open strategic autonomy of the Union, both of which are objectives of this Regulation. Synergies are essential to strengthen cooperation and coordination among the different stakeholders, including from the private sector, civil society and academia.

(56) データ侵害及び識別名の盗取または操作を含め，サイバーセキュリティ上のリスク及びサイバー犯罪に抗して欧州連合の民主主義，人々，事業者及び公的機関の諸利益を保護するため，この規則は，「デジタル 10 年のためのデジタルの権利及び基本原則に関する欧州宣言」と題する欧州議会，理事会及び欧州委員会の 2022 年 1 月 26 日の共同宣言の中で行われた確約を考慮に入れるべきである。

This Regulation should take into account the commitment set out in the Joint Declaration of 26 January 2022 of the European Parliament, the Council and the Commission entitled 'European Declaration on Digital Rights and Principles for the Digital Decade' to protect the interests of the Union's democracies, people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation.

(57) この規則の一定の非本質的な要素を補完するため，TFEU の第 290 条に従い，EU サイバーセキュリティリザーブに対して要請される対応サービスのタイプ及び数の細目を定めるための法行為を採択する権限は，欧州委員会に対して委任されるべきである。欧州委員会の準備作業の間，専門家レベルのものを含め，欧州委員会が適切な意見聴取を実施すること及びそれらの意見聴取がより良い立法に関する 2016 年 4 月 13 日の機関間合意[20]の中で定められた基本原則に従って実施されることは，特に重要なことである。とりわけ，委任される行為の準備への平等な参加を確保するため，欧州議会及び理事会は，構成国の専門家と同時に全ての文書を受領し，かつ，構成国の専門家は，委任される行為の準備を取扱う欧州委員会の専門家グループの会合へのアクセスを自動的にもつ。

In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to specify the types and number of response services required for the EU Cybersecurity Reserve. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[20]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(58) この規則の実装のための統一的な条件を確保するため，EU サイバーセキュリティリザーブの支援サービスを割当てるための詳細な手続上の手立ての細目を別途定めるための実装権限は，欧州委員会に対して与えられるべきである。その権限は，欧州議会及び理事会の規則(EU) No 182/2011[21]に従って行使されるべきである。

---

[20] OJ L 123, 12.5.2016, p. 1.

[21] 欧州委員会の実装権限の行使の構成国による管理のための仕組みに関する規定及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011 (OJ L 55, 28.2.2011, p. 13).
Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify further the detailed procedural arrangements for allocating the EU Cybersecurity Reserve support services. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[21].

(59) 諸条約の下にある欧州連合の年次予算と関連する諸規定を妨げることなく，欧州委員会は，ENISA の予算編成上及び人員配置上の必要性を評価する際，この規則から生ずる義務を考慮に入れるべきである。

Without prejudice to the rules relating to the Union's annual budget under the Treaties, the Commission should take into account the obligations arising from this Regulation when assessing the budgeting and staffing needs of ENISA.

(60) 欧州委員会は，定期的に，この規則の中で定められた措置の評価を実施すべきである。最初のそのような評価は，この規則の発効の日の後の最初の 2 年間に，その後は，TFEU の第 312 条によって設けられた多年度資金提供枠組みの改訂のタイミングを考慮に入れた上で，4 年毎に行われるべきである。欧州委員会は，欧州議会及び理事会に対し，行われた進捗状況に関する報告書を提出すべきである。欧州サイバーセキュリティ警報システムの中で共有される情報の範囲を含め，要求される異なる要素を評価するため，欧州委員会は，既に利用可能な情報または任意に提供された情報のみを基礎とすべきである。地政学上の進展を考慮に入れた上で，かつ，2027 年よりも前にこの規則の中で定められた措置の継続性及び更なる発展を確保するため，欧州委員会が，2028 年から 2034 年までの多年度資金提供枠組みの中にある適切な予算を割当てるべき必要性を評価することが重要である。

The Commission should carry out an evaluation of the measures laid down in this Regulation on a regular basis. The first such evaluation should take place in the first 2 years after the date of entry into force of this Regulation and at least every 4 years thereafter, taking into account the timing of the revision of the multiannual financial framework established pursuant to Article 312 TFEU. The Commission should submit a report on progress made to the European Parliament and to the Council. In order to assess the different elements required, including the extent of information shared within the European Cybersecurity Alert System, the Commission should base itself exclusively on information that is readily available or voluntarily provided. Taking into consideration geopolitical developments and in order to ensure continuity and further development of the measures laid down in this Regulation beyond 2027, it is important that the Commission assess the necessity to allocate an appropriate budget in the multiannual financial framework for 2028 to 2034.

(61) この規則の目的，すなわち，デジタル経済全体にわたり欧州連合内の製造業及びサービス業の競争上の地位を強化すること並びにサイバーセキュリティの分野における欧州連合の技術上の主権及びオープンな戦略上の自律性に貢献することは，その活動の規模及び影響のゆえに，構成国によっては十分に達成され得ず，欧州連合レベルにおいてより良く達成され得るので，欧州連合は，TEU の第 5 条の中で定められた補完性の原則に従い，措置を採択できる。同条の中で定められた比例性の原則に従い，この規則は，その目的を達成するために必要なところを超えることがない，

Since the objectives of this Regulation, namely to reinforce the competitive position of industry and services in the Union across the digital economy and to contribute to the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

以上のとおりであるので, この規則を採択する:

HAVE ADOPTED THIS REGULATION:

第 I 章 総則的な条項
Chapter I General Provisions

第 1 条 対象事項及び目的
Article 1 **Subject-matter and objectives**

1. この規則は，とりわけ，以下のものを設けることによって，サイバーな脅威とインシデントを検出し，その対応準備をし及びそれに対して対応するための欧州連合内の能力を強化するための措置を定める：

This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cyber threats and incidents, in particular by establishing:

(a) 調整された検出能力及び共通の状況認識能力を構築及び拡大するためのサイバーハブの汎欧州ネットワーク（欧州サイバーセキュリティ警報システム）；

a pan-European network of cyber hubs (European Cybersecurity Alert System) to build and enhance coordinated detection and common situational awareness capabilities;

(b) 大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントに対して対応準備すること，それらに対して対応すること，それらの影響を緩和すること及びそれらからの復旧を開始することにおいて構成国を支援するため，並びに，大きなサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対して対応することにおいて構成国以外のユーザを支援するためのサイバーセキュリティ緊急メカニズム；

a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, mitigating the impact of and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents and to support other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents;

(c) 大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントを見直すため及び評価するための欧州サイバーセキュリティインシデント見直しメカニズム。

a European Cybersecurity Incident Review Mechanism to review and assess significant cybersecurity incidents or large-scale cybersecurity incidents.

2. この規則は，マイクロ企業及び小企業と中規模企業並びにスタートアップを含め，デジタル経済全体にわたり欧州連合内の製造業及びサービス業の競争上の地位を強化すること，また，デジタル単一市場における技術革新を推進することによる場合を含め，サイバーセキュリティの分野における欧州連合の技術上の主権及びオープンな戦略上の自律性に貢献することという一般的な目的を追求

する。この規則は，欧州連合レベルの結束を強化すること，サイバーセキュリティのエコシステムを強化すること，構成国のサイバー回復力を拡大すること，並びに，サイバーセキュリティとの関係において，就労者の技能，ノウハウ，能力及びコンピテンシーを開発することによって，それらの目的を追求する。

This Regulation pursues the general objectives of reinforcing the competitive position of industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, including by boosting innovation in the Digital Single Market. It pursues those objectives by strengthening solidarity at Union level, reinforcing the cybersecurity ecosystem, enhancing Member States' cyber resilience and developing the skills, knowhow, abilities and competencies of the workforce in relation to cybersecurity.

3. 第 2 項に示す一般的な目的の達成は，以下の個別対象を通じて追求される：

The achievement of the general objectives referred to in paragraph 2 shall be pursued through the following specific objectives:

(a) 欧州連合の共通の調整された検出能力及びサイバーな脅威とインシデントの共通の状況認識を強化すること；

to strengthen common coordinated Union detection capacities and common situational awareness of cyber threats and incidents;

(b) 欧州連合のサイバーセキュリティインシデント対応支援を DEP と関係をもつ第三国のために利用できるようにする可能性を含め，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントを取扱うための調整された準備態勢試験並びに拡大された対応能力及び復旧能力を開発することによって，欧州連合全域にわたり高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体の準備態勢を強化すること及び結束を強化すること；

to reinforce preparedness of entities operating in sectors of high criticality or entities operating in other critical sectors across the Union and strengthen solidarity by developing coordinated preparedness testing and enhanced response and recovery capacities to handle significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents, including the possibility of making Union cybersecurity incident response support available for DEP-associated third countries;

(c) 習んだ教訓の描出及びそれが適切なときは推奨事項を含め，大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントを見直すこと及び評価することによって，欧州連合の回復力を拡大すること及び実効的なインシデント対応に貢献すること。

to enhance the Union's resilience and contribute to effective incident response by reviewing and assessing significant cybersecurity incidents or large-scale cybersecurity incidents, including drawing lessons learned and, where appropriate, recommendations.

4. この規則の下における活動は，構成国の権限を適正に尊重して実行され，かつ，CSIRTs ネットワーク，EU-CyCLONe 及び NIS 協力グループによって実施される活動に対して補完的なものとする。

The actions under this Regulation shall be conducted with due respect to the Member States' competences and shall be complementary to the activities carried out by the CSIRTs network, EU-CyCLONe and the NIS Cooperation Group.

5. この規則は，国の領土の完全性を確保すること，法と秩序を維持すること及び国家安全保障を防護すること含め，構成国の必須の機能を妨げない。とりわけ，国家安全保障は，各構成国の単独の職責のままである。

This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

6. 欧州連合の規定または国内規定によって機密である情報のこの規則の下における共有または交換は，その共有または交換の目的にとって適格でありかつ比例的であるところに限定される。そのような情報の共有または交換は，その情報の機密性を維持し，かつ，関係する法主体のセキュリティ及び商業上の利益を保護する。当該情報の開示が国家安全保障，公共の保安または国防という構成国の必須の利益に反し得るような情報の供給を伴ってはならない。

The sharing or exchange of information under this Regulation that is confidential pursuant to Union or national rules shall be limited to that which is relevant and proportionate to the purpose of that sharing or exchange. Such sharing or exchange of information shall preserve the confidentiality of the information, and protect the security and commercial interests of the entities concerned. It shall not entail the supply of information the disclosure of which would be contrary to the Member States' essential interests of national security, public security or defence.

第 2 条 定義

Article 2 **Definitions**

この規則の目的のために，以下の定義が適用される：

For the purposes of this Regulation, the following definitions apply:

(1) 「国境を越えるサイバーハブ」とは，書面によるコンソーシアム合意によって設置され，少なくとも 3 つの構成国の国内サイバーハブを 1 つの調整されたネットワーク構造に束ね，かつ，とりわけ，

それが適切なときは匿名化された適格なデータ及び情報の交換を介して，並びに，最新のツールの共有，並びに，サイバー検出能力，分析能力，防止能力及び防御能力の信頼できる環境の中における共同開発を介して，サイバーな脅威の監視，検出及び分析を拡大し，インシデントを防止し及びサイバーな脅威情報の作成を支援するために設計された多国間プラットフォームのことを意味し；

‘Cross-Border Cyber Hub’ means a multi-country platform, established by a written consortium agreement that brings together in a coordinated network structure National Cyber Hubs from at least three Member States, and that is designed to enhance the monitoring, detection and analysis of cyber threats to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment;

(2) 「ホスティングコンソーシアム」とは，国境を越えるサイバーハブを設置すること及び国境を越えるサイバーハブのためのツール，インフラまたはサービスの獲得に貢献すること及び国境を越えるサイバーハブの業務運営に同意した参加構成国によって構成されるコンソーシアムのことを意味し；

‘Hosting Consortium’ means a consortium composed of participating Member States, that have agreed to establish and to contribute to the acquisition of tools, infrastructure or services for, and the operation of, a Cross-Border Cyber Hub;

(3) 「CSIRT」とは，指令(EU) 2022/2555 の第 10 条によって指定されまたは設置された CSIRT のことを意味し；

‘CSIRT’ means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555;

(4) 「法主体」とは，指令(EU) 2022/2555 の第 6 条第 38 号の中で定義された法主体のことを意味し；

‘entity’ means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555;

(5) 「高度の不可欠性のある部門において業務運営している法主体」とは，指令(EU) 2022/2555 の別紙 I の中で列挙されたタイプの法主体のことを意味し；

‘entities operating in sectors of high criticality’ means the types of entity listed in Annex I to Directive (EU) 2022/2555;

(6) 「他の不可欠な部門において業務運営している法主体」とは，指令(EU) 2022/2555 の別紙 II の中で列挙されたタイプの法主体のことを意味し；

‘entities operating in other critical sectors’ means the types of entity listed in Annex II to Directive (EU) 2022/2555;

(7) 「リスク」とは，指令(EU) 2022/2555 の第 6 条第 9 号の中で定義されたリスクのことを意味し；

‘risk’ means risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;

(8) 「サイバーな脅威」とは，規則(EU) 2019/881 の第 2 条第 8 号の中で定義されたサイバーな脅威のことを意味し；

‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(9) 「インシデント」とは，指令(EU) 2022/2555 の第 6 条第 6 号の中で定義されたインシデントのことを意味し；

‘incident’ means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

(10) 「大きなサイバーセキュリティインシデント」とは，指令(EU) 2022/2555 の第 23 条第 3 項の中で定められた基準を満たすインシデントのことを意味し；

‘significant cybersecurity incident’ means an incident fulfilling the criteria set out in Article 23(3) of Directive (EU) 2022/2555;

(11) 「大きなインシデント」とは，欧州議会及び理事会の規則(EU, Euratom) 2023/2841[22]の第 3 条第 8 号の中で定義された大きなインシデントのことを意味し；

‘major incident’ means a major incident as defined in Article 3, point (8), of Regulation (EU, Euratom) 2023/2841 of the European Parliament and the Council[(22)];

(12) 「大規模なサイバーセキュリティインシデント」とは，指令(EU) 2022/2555 の第 6 条第 7 号の中で定義された大規模なサイバーセキュリティインシデントのことを意味し；

‘large-scale cybersecurity incident’ means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;

(13) 「大規模と均等なサイバーセキュリティインシデント」とは，欧州連合の機関，組織，事務局及び

[22] 欧州連合の機関，組織，事務局及び部局における共通の高いレベルのサイバーセキュリティのための措置を定める欧州議会及び理事会の 2023 年 12 月 13 日の規則(EU, Euratom) 2023/2841 (OJ L, 2023/2841, 18.12.2023).
Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023).

部局の場合においては，大きなインシデントのことを意味し，また，DEP と関係をもつ第三国の場合においては，関係する DEP と関係をもつ第三国の当該インシデントに対して対応するための能力を超過するレベルの混乱を生じさせるインシデントのことを意味し；

‘large-scale-equivalent cybersecurity incident’ means, in the case of Union institutions, bodies, offices and agencies, a major incident and, in the case of DEP-associated third countries, an incident which causes a level of disruption that exceeds the capacity of the DEP-associated third country concerned to respond to it;

(14) 「DEP と関係をもつ第三国」とは，規則(EU) 2021/694 の第 10 条によるデジタル欧州計画への当該第三国の参加を認める欧州連合との間の合意の当事者である第三国のことを意味し；

‘DEP-associated third country’ means a third country which is party to an agreement with the Union allowing for its participation in the Digital Europe Programme pursuant to Article 10 of Regulation (EU) 2021/694;

(15) 「契約当局」とは，欧州委員会，または，第 14 条第 5 項によって EU サイバーセキュリティリザーブの業務運営及び運営管理が ENISA に対して委任された範囲内では，ENISA のことを意味し；

‘contracting authority’ means the Commission or, to the extent that the operation and administration of the EU Cybersecurity Reserve has been entrusted to ENISA pursuant to Article 14(5), ENISA;

(16) 「マネージドセキュリティサービスプロバイダ」とは，指令(EU) 2022/2555 の第 6 条第 40 号の中で定義されたマネージドセキュリティサービスプロバイダのことを意味し；

‘managed security service provider’ means a managed security service provider as defined in Article 6, point (40), of Directive (EU) 2022/2555;

(17) 「信頼できるマネージドセキュリティサービスプロバイダ」とは，第 17 条に従って EU サイバーセキュリティリザーブの中に含められるために選抜されたマネージドセキュリティサービスプロバイダのことを意味する。

‘trusted managed security service providers’ means managed security service providers selected to be included in the EU Cybersecurity Reserve in accordance with Article 17.

第 II 章 欧州サイバーセキュリティ警報システム
Chapter II The European Cybersecurity Alert System

第 3 条 欧州サイバーセキュリティ警報システムの設置
Article 3 Establishment of the European Cybersecurity Alert System

1. サイバーな脅威との関係における検出能力，分析能力及びデータ処理能力を拡大するための欧州連合の高度な能力の開発並びに欧州連合内におけるインシデントの防止を支援するため，国内サイバーハブ及び国境を越えるサイバーハブによって任意ベースで組成されているインフラの汎欧州ネットワークである欧州サイバーセキュリティ警報システムが設置される。

A pan-European network of infrastructure that consists of National Cyber Hubs and Cross-Border Cyber Hubs joining on a voluntary basis, the European Cybersecurity Alert System, shall be established to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union.

2. 欧州サイバーセキュリティ警報システムは：

The European Cybersecurity Alert System shall:

(a) 適格な法主体，とりわけ，CSIRTs，CSIRTs network，EU-CyCLONe 及び指令(EU)2022/2555 の第 8 条第 1 項によって指定されまたは設置された職務権限のある当局を支援すること及びそれらとの間で協力すること並びにそれらの実現能力を強化することによって，サイバーな脅威に対するより良い防護及び対応に貢献し；

contribute to better protection from and responses to cyber threats by supporting and cooperating with, and reinforcing the capabilities of, relevant entities, in particular CSIRTs, the CSIRTs network, EU-CyCLONe and competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555;

(b) 国境を越えるサイバーハブ内の様々な情報源からのサイバーな脅威とインシデントに関する適格なデータ及び情報をプールし，並びに，CSIRTs ネットワークにとって適格なときは，国境を越えるサイバーハブを介して，分析されまたは集約された情報を共有し；

pool relevant data and information on cyber threats and incidents from various sources within the Cross-Border Cyber Hubs and share analysed or aggregated information through Cross-Border Cyber Hubs, where relevant with the CSIRTs network;

(c) 最新のツール及び先進技術の利用を通じて，高品質な実用的情報及びサイバー脅威情報を収集し及びその作成を支援し，並びに，当該実用的情報及びサイバー脅威情報を共有し；

collect and support the production of high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools and advanced technologies, and share that information and cyber threat intelligence;

(d) 欧州連合全域にわたりサイバーな脅威及び共通の状況認識の調整された検出を拡大することに貢献し，並びに，それが適格なときは，法主体に対する具体的な推奨事項を提供することによる場合を含め，警報を発することに貢献し；

contribute to enhancing the coordinated detection of cyber threats and common situational awareness across the Union, and to the issuing of alerts, including, where relevant, by providing concrete recommendations to entities;

(e) 人工知能及びデータ分析ツールのような高度なツール及び技術の開発に貢献することを含め，欧州連合内のサイバーセキュリティコミュニティに対してサービス及び活動を提供する。

provide services and activities for the cybersecurity community in the Union, including contributing to the development of advanced tools and technologies, such as artificial intelligence and data analytics tools.

3. 欧州サイバーセキュリティ警報システムを実装する活動は，デジタル欧州計画（DEP）からの資金提供によって支援され，かつ，規則(EU) 2021/694，とりわけ，同規則の個別対象 3 に従って実装される。

Actions implementing the European Cybersecurity Alert System shall be supported by funding from the Digital Europe Programme (DEP) and implemented in accordance with Regulation (EU) 2021/694, in particular Specific Objective 3 thereof.

第 4 条 国内サイバーハブ

Article 4 National Cyber Hubs

1. 構成国が欧州サイバーセキュリティ警報システムに参加することを決定するときは，その構成国は，この規則の目的のために国内サイバーハブを指定し，または，それが適用可能なときは，設置する。

Where a Member State decides to participate in the European Cybersecurity Alert System, it shall designate or, where applicable, establish a National Cyber Hub for the purposes of this Regulation.

2. 国内サイバーハブは，構成国の権限の下において活動する単一の法主体であるものとする。国内サイバーハブは，CSIRT，または，それが適用可能なときは，指令(EU) 2022/2555 の第 8 条第 1 項によって指定されもしくは設置された国内サイバー危機管理当局もしくはそれ以外の職務権限のある当局またはそれら以外の法主体であり得る。国内サイバーハブは：

A National Cyber Hub shall be a single entity acting under the authority of a Member State. It may be a CSIRT or, where applicable, a national cyber crisis management authority or other competent authority designated or established pursuant

to Article 8(1) of Directive (EU) 2022/2555, or another entity. The National Cyber Hub shall:

(a) サイバーな脅威及びインシデントに関する情報を収集すること及び分析することに関し，国内レベルの他の公的組織及び民間組織の基点及びそれらへのゲートウェイとして活動するための能力並びに第 5 条に示す国境を越えるサイバーハブに貢献するための能力をもち；かつ

have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a Cross-Border Cyber Hub as referred to in Article 5; and

(b) インシデントを防止することを狙いとして，とりわけ最新の技術を用いることにより，サイバー脅威情報のような，サイバーな脅威とインシデントと関連するデータ及び情報を検出すること，集約すること及び分析することが可能であるものとする。

be capable of detecting, aggregating, and analysing data and information relevant to cyber threats and incidents, such as cyber threat intelligence, by using in particular state-of-the-art technologies, with the aim of preventing incidents.

3. 本条第 2 項に示す機能の一部として，国内サイバーハブは，指令(EU) 2022/2555 の第 3 条に示す必須法主体及び重要法主体の部門別コミュニティ及び部門横断コミュニティを含め，サイバーな脅威とインシデントの検出及び防止の目的のために適格なデータ及び情報を交換するため，民間部門の法主体との間で協力し得る。それが適切であるときは，かつ，欧州連合法及び国内法に従って，国内サイバーハブによって要求されまたは受領される情報は，テレメトリーデータ，センサーデータ及び履歴データを含み得る。

As part of the functions referred to in paragraph 2 of this Article, National Cyber Hubs may cooperate with private sector entities to exchange relevant data and information for the purpose of detecting and preventing cyber threats and incidents, including with sectoral and cross-sectoral communities of essential and important entities as referred to in Article 3 of Directive (EU) 2022/2555. Where appropriate and in accordance with Union and national law, the information requested or received by National Cyber Hubs may include telemetry, sensor and logging data.

4. 第 9 条第 1 項によって選抜された構成国は，その構成国の国内サイバーハブの国境を越えるサイバーハブへの参加を申込むことを確約する。

A Member State selected pursuant to Article 9(1) shall commit to applying for its National Cyber Hub to participate in a Cross-Border Cyber Hub.

第 5 条 国境を越えるサイバーハブ

Article 5 **Cross-Border Cyber Hubs**

1. 少なくとも 3 つの構成国が，当該構成国のサイバーな検出活動及び脅威の監視活動を調整するために当該構成国の国内サイバーハブが共に作業することを確保することを確約しているときは，それらの構成国は，この規則の目的のためにホスティングコンソーシアムを設置し得る；

   Where at least three Member States are committed to ensuring that their National Cyber Hubs work together to coordinate their cyber-detection and threat monitoring activities, those Member States may establish a Hosting Consortium for the purposes of this Regulation.

2. ホスティングコンソーシアムは，第 4 項に従って国境を越えるサイバーハブを設置すること，並びに，国境を越えるサイバーハブのためのツール，インフラまたはサービスの獲得に貢献すること及びその業務運営に貢献することを合意した少なくとも 3 つの参加構成国によって構成される。

   A Hosting Consortium shall be composed of at least three participating Member States that have agreed to establish and contribute to the acquisition of tools, infrastructure or services for, and the operation of, a Cross-Border Cyber Hub, in accordance with paragraph 4.

3. 第 9 条第 3 項に従ってホスティングコンソーシアムが選抜されるときは，その構成者は，以下のとおりの書面によるコンソーシアム合意を締結する：

   Where a Hosting Consortium is selected in accordance with Article 9(3), its members shall conclude a written consortium agreement which:

   (a) 第 9 条第 3 項に示すホスティング及び利用合意を実装するための内部的な取決めを定め；

   sets out the internal arrangements for implementing the hosting and usage agreement referred to in Article 9(3);

   (b) そのホスティングコンソーシアムの国境を越えるサイバーハブを設置し；かつ

   establishes the Hosting Consortium's Cross-Border Cyber Hub; and

   (c) 第 6 条第 1 項及び第 2 項によって要求される特定の文言を含める。

   includes the specific clauses required pursuant to Article 6(1) and (2).

4. 国境を越えるサイバーハブは，第 3 項の中に示す書面によるコンソーシアム合意によって設置される多国間プラットフォームであるものとする。国境を越えるサイバーハブは，調整されたネットワーク構造の中で，当該ホスティングコンソーシアムの構成国の国内サイバーハブを束ねる。国境を越えるサ

イバーハブは，とりわけ，それが適切なときは匿名化された適格なデータ及び情報の交換を介して，並びに，最新のツールの共有と，信頼できる環境内におけるサイバーな検出能力，分析能力，防御能力及び防護能力の共同開発を介して，サイバーな脅威の監視，検出及び分析を拡大するため，インシデントを防止するため及びサイバー脅威情報の作成を支援するために設計される。

A Cross-Border Cyber Hub shall be a multi-country platform established by a written consortium agreement as referred to in paragraph 3. It shall bring together in a coordinated network structure the National Cyber Hubs of the Hosting Consortium's Member States. It shall be designed to enhance the monitoring, detection and analysis of cyber threats, to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment.

5. 国境を越えるサイバーハブは，対応するホスティングコンソーシアムの調整者としての構成者によって，または，そのホスティングコンソーシアムが法人格をもつときは，そのホスティングコンソーシアムによって，法律上の目的のために代表される。国境を越えるサイバーハブによるこの規則並びにホスティング及び利用合意を遵守する責任は，第 3 項に示す書面によるコンソーシアム合意の中で割当てられる。

A Cross-Border Cyber Hub shall be represented for legal purposes by a member of the corresponding Hosting Consortium acting as a coordinator, or by the Hosting Consortium if it has legal personality. Responsibility for compliance by the Cross-Border Cyber Hub with this Regulation and the hosting and usage agreement shall be allocated in the written consortium agreement referred to in paragraph 3.

6. 構成国は，ホスティングコンソーシアム構成者の合意によって既存のホスティングコンソーシアムに加わり得る。第 3 項に示す書面によるコンソーシアム合意並びにホスティング及び利用合意は，しかるべく修正される。このことは，当該ホスティングコンソーシアムによって既に共同で調達されたツール，インフラまたはサービスに対する欧州サイバーセキュリティ産業，技術及び調査研究能力拠点（ECCC）の保有の権利に対して影響を与えてはならない。

A Member State may join an existing Hosting Consortium with the agreement of the Hosting Consortium members. The written consortium agreement referred to in paragraph 3 and the hosting and usage agreement shall be modified accordingly. This shall not affect the ownership rights of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) over the tools, infrastructure or services already jointly procured with that Hosting Consortium.

第 6 条　国境を越えるサイバーハブ内及び国境を越えるサイバーハブ間の協力及び情報共有

Article 6　**Cooperation and information sharing within and between Cross-Border Cyber Hubs**

1. ホスティングコンソーシアムの構成者は，そのような情報共有が以下のとおりであるときは，その構成

者の国内サイバーハブが，第 5 条第 3 項に示す書面によるコンソーシアム合意に従い，サイバーな脅威，ニアミス，脆弱性，手法と手順，侵害指標，敵対的な戦術，脅威関係者固有の情報，サイバーセキュリティ警報と関連する情報及びサイバー攻撃を検出するためのサイバーセキュリティツールの設定に関する推奨事項のような，それが適切なときは匿名化された適格な情報を，その国境を越えるサイバーハブ内の構成者間で共有することを確保する：

Members of a Hosting Consortium shall ensure that their National Cyber Hubs share, in accordance with the written consortium agreement referred to in Article 5(3), relevant information, anonymised where appropriate, such as information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks, among themselves within the Cross-Border Cyber Hub where such information sharing:

(a) サイバーな脅威の検出を育成及び拡大し，また，インシデントを防止するため及びそれに対して対応するためまたはインシデントの影響を緩和するための CSIRTs ネットワークの実現能力を強化し；

fosters and enhances the detection of cyber threats and reinforces the capabilities of the CSIRTs network to prevent and respond to incidents or to mitigate their impact;

(b) 例えば，サイバーな脅威との関係における注意を喚起すること，そのような脅威の拡散能力を抑制することまたは阻止すること，様々な防御能力，脆弱性の修復と開示，脅威の検出，封じ込めの技法と防止の技法，緩和の戦略，対応の段階と復旧の段階を支援すること，または，公的法主体と民間法主体の間における脅威の共働的な調査研究を促進することを通じて，サイバーセキュリティのレベルを拡大する。

enhances the level of cybersecurity, for example through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, response and recovery stages or promoting collaborative threat research between public and private entities.

2. 第 5 条第 3 項に示す書面によるコンソーシアム合意は，以下のことを確定する：

The written consortium agreement referred to in Article 5(3) shall establish:

(a) そのホスティングコンソーシアムの構成者間における第 1 項に示す情報を共有することの確約及び当該情報が共有されるための条件；

a commitment to share among the members of the Hosting Consortium information as referred to in paragraph 1 and the conditions under which that information is to be shared;

(b) 第 1 項に示す，それが適切なときは匿名化された適格な情報の全参加者による共有を明確化しかつインセンティブを与える統治の枠組み；

a governance framework clarifying and incentivising the sharing by all participants of relevant information, anonymised where appropriate, as referred to in paragraph 1;

(c) 人工知能及びデータ分析ツールのような，高度なツール及び技術の開発に対する貢献のための対象。

targets for contribution to the development of advanced tools and technologies, such as artificial intelligence and data analytics tools.

書面によるコンソーシアム合意は，第 1 項に示す情報が欧州連合法及び国内法に従って共有されることを定め得る。

The written consortium agreement may specify that the information referred to in paragraph 1 is to be shared in accordance with Union and national law.

3. 国境を越えるサイバーハブは，相互に，国境を越えるサイバーハブ中における相互運用性及び情報共有の基本原則を定める協力協定を締結する。国境を越えるサイバーハブは，欧州委員会に対し，締結された協力協定に関して連絡する。

Cross-Border Cyber Hubs shall conclude cooperation agreements with one another, specifying interoperability and information-sharing principles among the Cross-Border Cyber Hubs. Cross-Border Cyber Hubs shall inform the Commission about the cooperation agreements concluded.

4. 国境を越えるサイバーハブ間における第 1 項に示す情報共有は，高いレベルの相互運用性によって確保される。そのような相互運用性を支援するため，ENISA は，欧州委員会と緊密に協力して，不適切な遅滞なく，かつ，いかなる場合においても 2026 年 2 月 5 日までに，国際的な技術標準とベストプラクティス及び設置された国境を越えるサイバーハブの稼動を考慮に入れた上で，とりわけ情報共有のフォーマット及び手順の細目を定める相互運用性の運用指針を発行する。国境を越えるサイバーハブの協力協定の中で定められる相互運用性の要件は，ENISA から発行される運用指針を基礎とする。

Information sharing as referred to in paragraph 1 between Cross-Border Cyber Hubs shall be ensured by a high level of interoperability. To support such interoperability, ENISA shall, in close consultation with the Commission, without undue delay and in any event by 5 February 2026, issue interoperability guidelines specifying in particular information-sharing formats and protocols, taking into account international standards and best practices, as well as the functioning of any established Cross-Border Cyber Hubs. Interoperability requirements provided for in the cooperation agreements of Cross-Border Cyber Hubs shall be based on the guidelines issued by ENISA.

第 7 条 欧州連合レベルのネットワークとの間の協力及び情報共有

Article 7 **Cooperation and information sharing with Union-level networks**

1. 国境を越えるサイバーハブ及び CSIRTs ネットワークは，とりわけ，情報を共有する目的のために，緊密に協力する。その目的のために，国境を越えるサイバーハブ及び CSIRTs ネットワークは，協力と適格な情報の共有に関する，及び，第 2 項を妨げることなく，共有される情報のタイプに関する手続覚書に合意する。

   Cross-Border Cyber Hubs and the CSIRTs network shall cooperate closely, in particular for the purpose of sharing information. To that end, they shall agree on procedural arrangements on cooperation and sharing of relevant information and, without prejudice to paragraph 2, on the types of information to be shared.

2. 潜在的なまたは進行中の大規模なサイバーセキュリティインシデントと関連する情報を獲得するときは，国境を越えるサイバーハブ及び CSIRTs ネットワークは，国境を越えるサイバーハブが，共通の状況認識の目的のために，EU-CyCLONe 及び CSIRTs ネットワークを介して，不適切な遅滞なく，構成国の当局及び欧州委員会に対し，適格な情報及び早期警戒が提供されることを確保する。

   Where the Cross-Border Cyber Hubs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall ensure, for the purposes of common situational awareness, that relevant information as well as early warnings are provided to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs network without undue delay.

第 8 条 セキュリティ

Article 8 **Security**

1. 欧州サイバーセキュリティ警報システムに参加している構成国は，機密性及びデータセキュリティ並びに欧州サイバーセキュリティ警報システムのネットワークの物理的なセキュリティを含め，高いレベルのサイバーセキュリティを確保し，かつ，ネットワークを介して共有されるデータと情報のセキュリティを含め，ネットワークを脅威から防護する方法で，かつ，ネットワークのセキュリティ及びシステムのセキュリティを確保する方法で，そのネットワークが適切に運営管理されかつ管理されることを確保する。

   Member States participating in the European Cybersecurity Alert System shall ensure a high level of cybersecurity, including confidentiality and data security, as well as physical security of the European Cybersecurity Alert System network, and shall ensure that the network is adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including that of data and information shared through the network.

2. 欧州サイバーセキュリティ警報システムに参加している構成国は，構成国の行政機関または行政組織以外の法主体との間の欧州サイバーセキュリティ警報システム中における第 6 条第 1 項に示す情

報の共有が，欧州連合または構成国の安全保障上の利益に対して負の影響を与えないことを確保する。

Member States participating in the European Cybersecurity Alert System shall ensure that the sharing of information referred to in Article 6(1) within the European Cybersecurity Alert System with any entity other than a public authority or body of a Member State does not negatively affect the security interests of the Union or of the Member States.

第 9 条 欧州サイバーセキュリティ警報システムの資金提供

Article 9 **Funding of the European Cybersecurity Alert System**

1. 欧州サイバーセキュリティ警報システムへの参加を予定している構成国の関心表明の募集の後，ECCC は，第 4 条第 1 項によって指定されまたは設置された国内サイバーハブを設置しまたはその実現能力を拡大するためのツール，インフラまたはサービスの共同調達において ECCC に参加する構成国を選抜する。ECCC は，選抜された構成国に対し，そのようなツール，インフラまたはサービスの運用の資金提供のための助成金を供与し得る。欧州連合の資金拠出は，ツール，インフラまたはサービスの獲得費用の 50%まで及び運用費用の 50%までの負担とする。選抜された構成国は，残余の費用を負担する。ツール，インフラまたはサービスの獲得のための手続を開始する前に，ECCC と選抜された構成国は，そのツール，インフラまたはサービスの利用を規律するホスティング及び利用合意を締結する。

Following a call for expressions of interest for Member States intending to participate in the European Cybersecurity Alert System, the ECCC shall select Member States to take part with the ECCC in the joint procurement of tools, infrastructure or services in order to set up, or enhance the capabilities of, National Cyber Hubs designated or established pursuant to Article 4(1). The ECCC may award to the selected Member States grants to fund the operation of such tools, infrastructure or services. The Union financial contribution shall cover up to 50 % of the acquisition costs of the tools, infrastructure or services and up to 50 % of the operational costs. The selected Member States shall cover the remaining costs. Before launching the procedure for the acquisition of tools, infrastructure or services, the ECCC and the selected Member States shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructure or services.

2. ツール，インフラまたはサービスが獲得された日または当該構成国が助成金の資金提供を受けた日のいずれか早い方の日から 2 年以内に，構成国の国内サイバーハブが国境を越えるサイバーハブに参加しないときは，その構成国は，その構成国が国境を越えるサイバーハブに加わるまで，本章の下にある欧州連合の付加的な支援を受ける適格を与えられてはならない。

Where a Member State's National Cyber Hub is not a participant in a Cross-Border Cyber Hub within 2 years of the date on which the tools, infrastructure or services were acquired, or on which it received grant funding, whichever occurred sooner, the Member State shall not be eligible for additional Union support under this Chapter until it has joined a Cross-Border Cyber Hub.

3. 関心表明の募集の後，ツール，インフラまたはサービスの ECCC との共同調達に参加するホスティングコンソーシアムが ECCC によって選抜される。ECCC は，そのホスティングコンソーシアムに対し，そのツール，インフラまたはサービスの運用の資金提供をするため，助成金を供与し得る。欧州連合の資金拠出は，ツール，インフラまたはサービスの獲得費用の 75%まで及び運用費用の 50%までの負担とする。ホスティングコンソーシアムは，残余の費用を負担する。ツール，インフラまたはサービスの獲得のための手続を開始する前に，ECCC とホスティングコンソーシアムは，そのツール，インフラまたはサービスの利用を規律するホスティング及び利用合意を締結する。

Following a call for expressions of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools, infrastructure or services with the ECCC. The ECCC may award a grant to the Hosting Consortium to fund the operation of the tools, infrastructure or services. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools, infrastructure or services, and up to 50% of the operational costs. The Hosting Consortium shall cover the remaining costs. Before launching the procedure for the acquisition of tools, infrastructure or services, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructure or services.

4. ECCC は，少なくとも 2 年毎に，構成国内に拠点をもちまたは拠点をもつとみなされ，かつ，構成国によってまたは構成国の国民によって支配されている法人からのものを含め，国内サイバーハブ及び国境を越えるサイバーハブの実現能力並びにそれらのハブの実現能力を確立するためまたは拡大するために必要でありかつ十分な品質のツール，インフラまたはサービスのマッピングを準備する。マッピングを準備する際，ECCC は，CSIRTs ネットワーク，既存の国境を越えるサイバーハブ，ENISA 及び欧州委員会から意見聴取する。

The ECCC shall prepare, at least every 2 years, a mapping of the tools, infrastructure or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, and their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, the ECCC shall consult the CSIRTs network, any existing Cross-Border Cyber Hubs, ENISA and the Commission.

第 III 章 サイバーセキュリティ緊急メカニズム
Chapter III Cybersecurity Emergency Mechanism

第 10 条 サイバーセキュリティ緊急メカニズムの設置
Article 10 Establishment of the Cybersecurity Emergency Mechanism

1. サイバーな脅威に対する欧州連合の回復力の向上を支援し，並びに，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントの短期的な影響に対する結束の精神による対応準備及びその影響の緩和を支援するため，サイバーセキュリティ緊急メカニズムが設置される。

   A Cybersecurity Emergency Mechanism is established to support the improvement of the Union's resilience to cyber threats and the preparation for and mitigation of, in a spirit of solidarity, the short-term impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents.

2. 構成国の場合，サイバーセキュリティ緊急メカニズムの下における活動は，要請に応じて提供され，かつ，インシデントの対応準備，それに対する対応及びそれからの復旧のための構成国の努力と活動に対して補完的なものとする。

   In the case of the Member States, actions under the Cybersecurity Emergency Mechanism shall be provided upon request and shall be complementary to Member States' efforts and actions to prepare for, respond to and recover from incidents.

3. サイバーセキュリティ緊急メカニズムを実装する活動は，DEP からの資金提供によって支援され，かつ，規則(EU) 2021/694，とりわけ，同規則の個別対象 3 に従って実装される。

   The actions implementing the Cybersecurity Emergency Mechanism shall be supported by funding from the DEP and shall be implemented in accordance with Regulation (EU) 2021/694, in particular Specific Objective 3 thereof.

4. サイバーセキュリティ緊急メカニズムの下における活動は，基本的に，規則(EU) 2021/887 に従い，ECCC を介して実装される。ただし，この規則の第 11 条(b)に示す EU サイバーセキュリティリザーブを実装する活動は，欧州委員会及び ENISA によって実装される。

   The actions under the Cybersecurity Emergency Mechanism shall be implemented primarily through the ECCC in accordance with Regulation (EU) 2021/887. However, actions implementing the EU Cybersecurity Reserve as referred to in Article 11, point (b), of this Regulation shall be implemented by the Commission and ENISA.

第 11 条 活動のタイプ

Article 11 **Types of action**

サイバーセキュリティ緊急メカニズムは，以下のタイプの活動を支援する：

The Cybersecurity Emergency Mechanism shall support the following types of action:

(a) 対応準備活動，すなわち：

preparedness actions, namely:

(i) 第 12 条の中で定められる，欧州連合全体にわたり高度の不可欠性のある部門において業務運営している法主体の調整された準備態勢試験；

the coordinated preparedness testing of entities operating in sectors of high criticality across the Union as specified in Article 12;

(ii) 第 13 条の中で定められる，高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体の(i)以外の対応準備活動；

other preparedness actions for entities operating in sectors of high criticality or entities operating in other critical sectors, as specified in Article 13;

(b) 第 14 条の下において設置される EU サイバーセキュリティリザーブに参加している信頼できるマネージドセキュリティサービスプロバイダから提供される，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対する対応を支援する活動及びそれらからの復旧を開始する活動；

actions supporting response to and initiating recovery from significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, to be provided by trusted managed security service providers participating in the EU Cybersecurity Reserve established under Article 14;

(c) 第 18 条に示す相互補助を支援する活動。

actions supporting mutual assistance as referred to in Article 18.

第 12 条 法主体の調整された準備態勢試験

Article 12 **Coordinated preparedness testing of entities**

1. サイバーセキュリティ緊急メカニズムは，高度の不可欠性のある部門において業務運営している法主体の任意の調整された準備態勢試験を支援する。

   The Cybersecurity Emergency Mechanism shall support the voluntary coordinated preparedness testing of entities operating in sectors of high criticality.

2. 調整された準備態勢試験は，ペネトレーションテスト及び脅威評価のような，準備態勢活動によって組成され得る。

   The coordinated preparedness testing may consist of preparedness activities, such as penetration testing, and threat assessment.

3. 本条の下における対応準備活動に対する支援は，基本的に，助成金の方式により，かつ，規則(EU) 2021/694 の第 24 条に示す適格な作業計画の中で定められた条件に服して，構成国に対して提供される。

   Support for preparedness actions under this Article shall be provided to Member States primarily in the form of grants and subject to the conditions provided for in the relevant work programmes as referred to in Article 24 of Regulation (EU) 2021/694.

4. 欧州連合全域にわたり，この規則の第 11 条(a)(i)に示す法主体の調整された準備態勢試験を支援する目的のために，欧州委員会は，NIS 協力グループ，EU-CyCLONe 及び ENISA から意見聴取した上で，指令(EU) 2022/2555 の別紙 I の中で列挙された，高度の不可欠性のある部門の中から，助成金を供与するための提案の募集が発され得る部門または副部門を指定する。

   For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 11, point (a)(i), of this Regulation across the Union, the Commission shall, after consulting the NIS Cooperation Group, EU-CyCLONe and ENISA, identify the sectors or sub-sectors concerned from the sectors of high criticality listed in Annex I to Directive (EU) 2022/2555 for which a call for proposals to award grants may be issued. The participation of Member States in those calls for proposals is voluntary.

5. 第 4 項に示す部門または副部門を指定する際，欧州委員会は，欧州連合レベルの調整されたリスク評価及び回復力試験並びにそれらの結果を考慮に入れる。

   When identifying the sectors or sub-sectors referred to in paragraph 4, the Commission shall take into account coordinated risk assessments and resilience testing at Union level and the results thereof.

6. NIS 協力グループは，欧州委員会，上級代表及び ENISA と協力して，並びに，EU-CyCLONe は，その委任の及ぶ範囲内で，第 11 条(a)(i)に示す調整された準備態勢試験のための，及び，それが適切なときは，同条(a)(ii)に示すその他の対応準備活動のための共通のリスクシナリオ及び手法を開発する。

The NIS Cooperation Group in cooperation with the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and ENISA, and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated preparedness testing referred to in Article 11, point (a)(i), and, where appropriate, for other preparedness actions referred to in point (a)(ii) of that Article.

7. 高度の不可欠性のある部門において業務運営している法主体が，調整された準備態勢試験に任意に参加し，かつ，当該試験が，その参加法主体が復旧計画の中に統合され得るという個別の方策に関する推奨事項を帰結するときは，調整された準備態勢試験に関して職責を負う構成国の当局は，それが適切なときは，準備態勢を強化するという観点から，参加法主体による当該措置の事後対応を見直す。

Where an entity operating in a sector of high criticality participates voluntarily in coordinated preparedness testing and that testing results in recommendations for specific measures, which the participating entity could integrate into a remediation plan, the Member State authority responsible for the coordinated preparedness testing shall, where appropriate, review the follow-up of those measures by the participating entities with a view to reinforcing preparedness.

第 13 条　その他の対応準備活動

Article 13　**Other preparedness actions**

1. サイバーセキュリティ緊急メカニズムは，第 12 条の適用を受けない準備態勢活動を支援する。そのような活動は，第 12 条による調整された準備態勢試験のために指定されていない部門の法主体のための対応準備活動を含む。そのような活動は，脆弱性監視，リスク監視，演習及び訓練を支援し得る。

The Cybersecurity Emergency Mechanism shall support preparedness actions not covered by Article 12. Such actions shall include preparedness actions for entities in sectors not identified for coordinated preparedness testing pursuant to Article 12. Such actions may support vulnerability monitoring, risk monitoring, exercises and training.

2. 本条の下における対応準備活動に対する支援は，要請に応じて，かつ，基本的に，助成金の方式により，かつ，規則(EU)2021/694 の第 24 条に示す適格な作業計画の中で定められた条件に服して，構成国に対して提供される。

Support for preparedness actions under this Article shall be provided to Member States upon request and primarily in the form of grants and subject to the conditions provided for in the relevant work programmes as referred to in Article 24 of

Regulation (EU) 2021/694.

第 14 条 EU サイバーセキュリティリザーブの設置

Article 14 **Establishment of the EU Cybersecurity Reserve**

1. 大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントに対して対応することにおいて，または，それに対する対応のための支援を提供することにおいて，及び，そのようなインシデントからの復旧を開始することにおいて，要請に応じて第 3 項に示すユーザを補助するため，EU サイバーセキュリティリザーブが設置される。

   An EU Cybersecurity Reserve is established in order to assist, upon request, users as referred to in paragraph 3, in responding to, or providing support for a response to, significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents, and initiating recovery from such incidents.

2. EU サイバーセキュリティリザーブは，第 17 条第 2 項の中で定められた基準に従って選抜された信頼できるマネージドセキュリティサービスプロバイダからの対応サービスによって組成される。EU サイバーセキュリティリザーブは，事前に確約されたサービスを含め得る。信頼できるマネージドセキュリティサービスプロバイダの事前に確約されたサービスは，当該サービスが事前に確約されている期間内においては当該事前に確約されたサービスがインシデント対応のために利用されない場合，インシデントの防止及び対応と関連する対応準備サービスへと転換され得る。EU サイバーセキュリティリザーブは，要請により，全ての構成国，欧州連合の機関，組織，事務局及び部局並びに第 19 条第 1 項に示す DEP と関係をもつ第三国において配置可能であるものとする。

   The EU Cybersecurity Reserve shall consist of response services from trusted managed security service providers selected in accordance with the criteria laid down in Article 17(2). The EU Cybersecurity Reserve may include pre-committed services. The pre-committed services of a trusted managed security service provider shall be convertible into preparedness services related to incident prevention and response where those pre-committed services are not used for incident response during the time for which those services are pre-committed. The EU Cybersecurity Reserve shall be deployable, upon request, in all Member States, in Union institutions, bodies, offices and agencies, and in DEP-associated third countries as referred to in Article 19(1).

3. EU サイバーセキュリティリザーブから提供されるサービスのユーザは，以下の者によって構成される：

   The users of the services provided by the EU Cybersecurity Reserve shall consist of the following:

   (a) 指令(EU) 2022/2555 の第 9 条第 1 項及び第 2 項並びに第 10 条にそれぞれ示す構成国のサイバー危機管理当局及び CSIRTs；

Member States' cyber crisis management authorities and CSIRTs as referred to, respectively, in Article 9(1) and (2) and Article 10 of Directive (EU) 2022/2555;

(b) 規則(EU, Euratom) 2023/2841 の第 13 条に従う CERT-EU；

CERT-EU in accordance with Article 13 of Regulation (EU, Euratom) 2023/2841;

(c) 第 19 条第 8 項に従う DEP と関係をもつ第三国のコンピュータセキュリティインシデント対応チーム及びサイバー危機管理当局のような職務権限のある当局。

competent authorities such as computer security incident response teams and cyber crisis management authorities of DEP-associated third countries in accordance with Article 19(8).

4. 欧州委員会は，EU サイバーセキュリティリザーブの実装に関し，総括的な職責をもつ。欧州委員会は，NIS 協力グループと協力し，かつ，第 3 項に示すユーザの要請に沿って，EU サイバーセキュリティリザーブの優先順位及び発展を判断し，かつ，その実装を監督し，また，この規則の下にある他の支援活動と欧州連合の他の活動及び計画との間の補完性，一貫性，相乗効果及び連携を確保する。それらの優先順位は，見直され，かつ，それが適切なときは，2 年毎に改訂される。欧州委員会は，欧州議会及び理事会に対し，それらの優先順位及びその改訂を連絡する。

The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and the evolution of the EU Cybersecurity Reserve in coordination with the NIS Cooperation Group and, in line with the requirements of the users referred to in paragraph 3, shall supervise its implementation and shall ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as with other Union actions and programmes. Those priorities shall be reviewed and, if appropriate, revised every 2 years. The Commission shall inform the European Parliament and the Council of those priorities and any revisions thereof.

5. 本条第 4 項に示す EU サイバーセキュリティリザーブの実装に関する欧州委員会の総括的な職責を妨げることなく，かつ，規則(EU, Euratom) 2024/2509 の第 2 条第 19 号の中で定義された拠出合意に服して，欧州委員会は，EU サイバーセキュリティリザーブの業務運営及び運営管理の全部または一部を ENISA に委任する。ENISA に対して委任されない諸側面は，欧州委員会による直接の運営管理に服するままとする。

Without prejudice to the Commission's overall responsibility for the implementation of the EU Cybersecurity Reserve referred to in paragraph 4 of this Article and subject to a contribution agreement as defined in Article 2, point (19), of Regulation (EU, Euratom) 2024/2509, the Commission shall entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA. Aspects not entrusted to ENISA shall remain subject to direct management by the Commission.

6. ENISAは，少なくとも2年毎に，本条第3項(a)及び(b)に示すユーザによって需要されるサービスのマッピングを準備する。そのマッピングは，構成国内に拠点をもちまたは拠点をもつとみなされ，かつ，構成国によってまたは構成国の国民によって支配されている法人からのものを含め，そのようなサービスの可用性も含める。当該可用性のマッピングの中で，ENISA は，EU サイバーセキュリティリザーブの目的にとって適格な欧州連合のサイバーセキュリティ就労者の技能及び能力を評価する。マッピングを準備する際，ENISAは，NIS協力グループ，EU-CyCLONe，欧州委員会，及び，それが適用可能なときは，規則(EU,Euratom)2023/2841の第10条によって設置される機関間サイバーセキュリティ委員会（IICB）から意見聴取する。サービスの可用性のマッピングの中で，ENISAは，マネージドセキュリティサービスプロバイダを含め，適格なサイバーセキュリティ産業の利害関係者からも意見聴取する。ENISAは，本条第3項(c)に示すユーザの需要を特定するため，理事会に対する連絡の後，かつ，EU-CyCLONe，欧州委員会，及び，それが適格なときは，上級代表からの意見聴取を経た後，類似のマッピングを準備する。

ENISA shall prepare, at least every 2 years, a mapping of the services needed by the users referred to in paragraph 3, points (a) and (b), of this Article. The mapping shall also include the availability of such services, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. In mapping that availability, ENISA shall assess the skills and capacity of the Union cybersecurity workforce relevant to the objectives of the EU Cybersecurity Reserve. When preparing the mapping, ENISA shall consult the NIS Cooperation Group, EU-CyCLONe, the Commission and, where applicable, the Interinstitutional Cybersecurity Board established pursuant to Article 10 of Regulation (EU, Euratom) 2023/2841 (IICB). In mapping the availability of services, ENISA shall also consult relevant cybersecurity industry stakeholders, including managed security service providers. ENISA shall prepare a similar mapping, after informing the Council and after consulting EU-CyCLONe, the Commission and, where relevant, the High Representative, to identify the needs of users referred to in paragraph 3, point (c), of this Article.

7. 欧州委員会は，EU サイバーセキュリティリザーブに対して要請される対応サービスのタイプ及び数の細目を定めることによってこの規則を補完するため，第 23 条に従って委任される行為を採択する権限を与えられる。それらの委任される行為を準備する際，欧州委員会は，本条第 6 項に示すマッピングを考慮に入れるものとし，かつ，NIS 協力グループ及び ENISA との間で助言を交換し及び協力できる。

The Commission is empowered to adopt delegated acts in accordance with Article 23 to supplement this Regulation by specifying the types and the number of response services required for the EU Cybersecurity Reserve. When preparing those delegated acts, the Commission shall take into account the mapping referred to in paragraph 6 of this Article and may exchange advice and cooperate with the NIS Cooperation Group and ENISA.

第 15 条 EU サイバーセキュリティリザーブからの支援を求める要請

Article 15 **Requests for support from the EU Cybersecurity Reserve**

1. 第 14 条第 3 項に示すユーザは，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントに対する対応を支援するため及びそれらからの復旧を開始するため，EU サイバーセキュリティリザーブからのサービスを要請し得る。

   The users referred to in Article 14(3) may request services from the EU Cybersecurity Reserve to support response to and initiate recovery from significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents.

2. EU サイバーセキュリティリザーブからの支援を受けるため，第 14 条第 3 項に示すユーザは，それが適格なときは，技術上の直接の補助，及び，インシデントへの対応及び復旧の努力を補助するためのその他の資源の提供を含め，その支援が要請されるインシデントの影響を緩和するための全ての適切な措置を講ずる。

   To receive support from the EU Cybersecurity Reserve, the users referred to in Article 14(3) shall take all appropriate measures to mitigate the effects of the incident for which the support is requested, including, where relevant, the provision of direct technical assistance, and other resources to assist the response to the incident, and recovery efforts.

3. 支援を求める要請書は，以下のとおりに，契約当局に対して転送される：

   Requests for support shall be transmitted to the contracting authority as follows:

   (a) この規則の第 14 条第 3 項(a)に示すユーザの場合，指令(EU) 2022/2555 の第 8 条第 3 項によって指定されまたは設置された単一連絡部局を介して；

   in the case of the users referred to in Article 14(3), point (a), of this Regulation, via the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555;

   (b) 第 14 条第 3 項(b)に示すユーザの場合，当該ユーザによって；

   in the case of the user referred to in Article 14(3), point (b), by that user;

   (c) 第 14 条第 3 項(c)に示すユーザの場合，第 19 条第 9 項に示す単一連絡部局を介して。

   in the case of the users referred to in Article 14(3), point (c), via the single point of contact referred to in Article 19(9).

4. 第 14 条第 3 項(a)に示すユーザからの要請の場合，構成国は，CSIRTs ネットワークに対し，及び，そ

れが適切なときは，EU-CyCLONe に対し，本条によるインシデント対応及び最初の復旧の支援を求める当該構成国のユーザの要請を連絡する。

In the case of requests from the users referred to in Article 14(3), point (a), Member States shall inform the CSIRTs network, and, where appropriate, EU-CyCLONe, about their users' requests for incident response and initial recovery support pursuant to this Article.

5. インシデント対応及び最初の復旧の支援を求める要請書は，以下の事項を含める：

Requests for incident response and initial recovery support shall include:

(a) 影響を受けた法主体及び以下の者に対するインシデントの潜在的な影響に関する適切な情報：

appropriate information regarding the entity affected and the potential impact of the incident on:

(i) 第 14 条第 3 項(a)に示すユーザの場合は，他の構成国に対する波及のリスクを含め，影響を受けた構成国及びユーザ；

in the case of users referred to in Article 14(3), point (a), the Member States and users affected, including the risk of spillover to another Member State;

(ii) 第 14 条第 3 項(b)に示すユーザの場合は，影響を受けた欧州連合の機関，組織，事務局または部局；

in the case of the user referred to in Article 14(3), point (b), the Union institutions, bodies, offices or agencies affected,

(iii) 第 14 条第 3 項(c)に示すユーザの場合は，影響を受けた DEP と関係をもつ第三国；

in the case of users referred to in Article 14(3), point (c), the DEP-associated countries affected;

(b) 推定される需要の記載を含め，要請されるサービスの利用計画と併せ，要請されるサービスと関連する情報；

information regarding the requested service, together with the planned use of the requested support, including an indication of the estimated needs;

(c) 第 2 項に示す，支援が要請されるインシデントの緩和のために講じられた措置に関する適切な情報；

appropriate information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;

(d) それが適格なときは，影響を受けた法主体にとって利用可能な別の形態の支援に関する利用可能な情報。

where relevant, available information about other forms of support available to the entity affected.

6. ENISA は，欧州委員会及び EU-CyCLONe と協力して，EU サイバーセキュリティリザーブからの支援を求める要請書の提出を容易にするための雛型を策定する。

ENISA, in cooperation with the Commission and EU-CyCLONe, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.

7. 欧州委員会は，実装行為により，そのような要請書を提出すること及びその応答を供給することに関する覚書並びに第 16 条第 9 項に示す報告のための雛型を含め，EU サイバーセキュリティリザーブの支援サービスが要請される方法，並びに，本条，第 16 条第 1 項及び第 19 条第 10 項によって当該要請書が応答される方法に関する詳細な手続覚書を別途定め得る。それらの実装行為は，第 24 条第 2 項に示す審議手続に従って採択される。

The Commission may, by means of implementing acts, specify further the detailed procedural arrangements for the way in which the EU Cybersecurity Reserve support services are to be requested and the way in which those requests are to be responded to pursuant to this Article, to Article 16(1) and to Article 19(10), including arrangements for submitting such requests and delivering the responses and templates for the reports referred to in Article 16(9). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

第 16 条 EU サイバーセキュリティリザーブからの支援の実装

Article 16 **Implementation of the support from the EU Cybersecurity Reserve**

1. 第 14 条第 3 項(a)及び(b)に示すユーザからの要請の場合，EU サイバーセキュリティリザーブからの支援の要請は，契約当局によって評価される。応答は，遅滞なく，かつ，その支援の実効性を確保するため，いかなる場合においても要請書の提出から 48 時間以内に，第 14 条第 3 項(a)及び(b)に示すユーザに対して転送される。契約当局は，理事会及び欧州委員会に対し，その過程の結果を連絡する。

In the case of requests from users referred to in Article 14(3), points (a) and (b), requests for support from the EU Cybersecurity Reserve shall be assessed by the contracting authority. A response shall be transmitted to the users referred to in Article 14(3), points (a) and (b), without delay and in any event no later than 48 hours from the submission of the request to ensure effectiveness of the support. The contracting authority shall inform the Council and the Commission of

the results of the process.

2. EU サイバーセキュリティリザーブのサービスの要請及び提供の過程において共有される情報に関し，この規則の適用に関与する全ての当事者は：

As regards information shared in the course of requesting and providing the services of the EU Cybersecurity Reserve, all parties involved in the application of this Regulation shall:

(a) 当該情報の利用及び共有を，この規則の下における当該当事者の義務または権能を果たすために必要なところに限定し；

limit the use and sharing of that information to what is necessary to discharge their obligations or functions under this Regulation;

(b) 欧州連合法及び国内法によって秘密であるとされまたは機密とされている情報を，当該法律に従う場合に限り，利用及び共有し；かつ

use and share any information that is confidential or classified pursuant to Union and national law only in accordance with that law; and

(c) それが適切なときは，トラフィックライトプロトコルを含め，適格な情報共有プロトコルを利用し及びそれを尊重することによって，実効的であり，効率的でありかつ安全な情報交換を確保する。

ensure effective, efficient and secure information exchange, where appropriate by using and respecting relevant information-sharing protocols including the traffic light protocol.

3. 第 16 条第 1 項及び第 19 条第 10 項の下における個々の要請の評価において，契約当局または欧州委員会は，しかるべく，第 15 条第 1 項及び第 2 項に示す基準が満たされているか否かを最初に評価する。該当する場合，欧州委員会は，それが適格なときは，第 1 条第 3 項(b)に示す目的及び以下の基準を考慮に入れて，支援の適切な期間及び性質を評価する：

In assessing individual requests under Article 16(1) and Article 19(10), the contracting authority or the Commission, as applicable, shall first assess whether the criteria referred to in Article 15(1) and (2) are fulfilled. If that is the case, it shall assess the duration and nature of support that is appropriate, having regard to the objective referred to in Article 1(3), point (b), and the following criteria, where relevant:

(a) インシデントの規模及び深刻度；

the scale and severity of the incident;

(b) 影響を受けた法主体のタイプ，指令(EU) 2022/2555 の第 3 条第 1 項に示す必須法主体に対して影響を与えるインシデントに対してより高い優先順位が与えられ；

the type of entity affected, with higher priority given to incidents affecting essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555;

(c) 影響を受けた構成国，欧州連合の機関，組織，事務局もしくは部局または DEP と関係をもつ第三国に対するインシデントの潜在的な影響；

the potential impact of the incident on the affected Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries;

(d) そのインシデントの潜在的な国境を越える性質及び他の構成国，欧州連合の機関，組織，事務局もしくは部局または DEP と関係をもつ第三国に対する波及のリスク；

the potential cross-border nature of the incident and the risk of spillover to other Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries;

(e) 第 15 条第 2 項に示す，対応及び最初の復旧の努力を補助するためにユーザによって講じられた措置。

the measures taken by the user to assist the response, and initial recovery efforts, as referred in Article 15(2).

4. 第 14 条第 3 項に示すユーザからの競合する要請がある場合において優先順位をつけるため，それが適格なときは，構成国と欧州連合の機関，組織，事務局及び部局との間の誠実な協力の原則をを妨げることなく，本条の第 3 項に示す基準が考慮に入れられる。同基準の下において複数の要請が均等であると評価されるときは，より高い優先順位は，構成国ユーザからの要請に対して与えられる。EU サイバーセキュリティリザーブの業務運営及び運営管理の全部または一部が第 14 条第 5 項によって ENISA に対して委任されたときは，ENISA 及び欧州委員会は，本項に従って要請の優先順位をつけるため，緊密に協力する。

To prioritise requests, in the case of concurrent requests from users referred to in Article 14(3), the criteria referred to in paragraph 3 of this Article shall be taken into account, where relevant, without prejudice to the principle of sincere cooperation between Member States and Union institutions, bodies, offices and agencies. Where two or more requests are assessed as equal under those criteria, higher priority shall be given to requests from Member State users. Where the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA pursuant to Article 14(5), ENISA and the Commission shall closely cooperate to prioritise requests in accordance with this paragraph.

5. EU サイバーセキュリティリザーブのサービスは，信頼できるマネージドセキュリティサービスプロバイダと，EU サイバーセキュリティリザーブの下における支援が提供されるユーザとの間の個別の合意

に従って提供される。それらのサービスは，信頼できるマネージドセキュリティサービスプロバイダ，ユーザ及び影響を受けた法主体の間の個別の合意に従って提供され得る。本項に示す全ての合意は，就中，法的責任の条件を含める。

The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the trusted managed security service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those services may be provided in accordance with specific agreements between the trusted managed security service provider, the user and the entity affected. All agreements referred to in this paragraph shall include, inter alia, liability conditions.

6. 第 5 項に示す合意は，構成国，及び，それが適切なときは，EU サイバーセキュリティリザーブの他のユーザからの意見聴取を経た上で ENISA によって準備される雛型を基礎とする。

The agreements referred to in paragraph 5 shall be based on templates prepared by ENISA, after consulting Member States and, where appropriate, other users of the EU Cybersecurity Reserve.

7. 欧州委員会，ENISA 及び EU サイバーセキュリティリザーブのユーザは，EU サイバーセキュリティリザーブの実装の枠組み内において提供されたサービスによって第三者に対して生じた損害に関し，契約上の法的責任を負ってはならない。

The Commission, ENISA and the users of the EU Cybersecurity Reserve shall bear no contractual liability for damage caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.

8. ユーザは，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントに対する対応を支援するため及びそれらからの復旧を開始するためにのみ，第 15 条第 1 項の下における要請に応答して提供される EU サイバーセキュリティリザーブのサービスを利用できる。ユーザは，以下の者との間の関係においてのみ，そのサービスを利用できる：

Users may use the EU Cybersecurity Reserve services provided in response to a request under Article 15(1) only in order to support response to and initiate recovery from significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents. They may use those services only in respect of:

(a) 第 14 条第 3 項(a)に示すユーザの場合は，高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体，及び，第 14 第 3 項(c)に示すユーザの場合は，均等な法主体；並びに

entities operating in sectors of high criticality or entities operating in other critical sectors, in the case of users referred to in Article 14(3), point (a), and equivalent entities in the case of users referred to in Article 14(3), point (c); and

(b) 第 14 条第 3 項(b)に示すユーザの場合は，欧州連合の機関，組織，事務局及び部局。

Union institutions, bodies, offices and agencies, in the case of the user referred to in Article 14(3), point (b).

9. 支援の終了から 2 か月以内に，支援を受けたユーザは，以下の者に対し，提供されたサービス，達成された結果及び学習された教訓に関する要旨報告書を提供する：

Within 2 months of the end of a support, users that have received support shall provide a summary report about the service provided, the results achieved and the lessons learned, to:

(a) 第 14 条第 3 項(a)に示すユーザの場合は，欧州委員会，ENISA，CSIRTs ネットワーク及び EU-CyCLONe；

the Commission, ENISA, the CSIRTs network and EU-CyCLONe in the case of users referred to in Article 14(3), point (a);

(b) 第 14 条第 3 項(b)に示すユーザの場合は，欧州委員会，ENISA 及び IICB；

the Commission, ENISA and the IICB in the case of the user referred to in Article 14(3), point (b);

(c) 第 14 条第 3 項(c)に示すユーザの場合は，欧州委員会。

the Commission in the case of users referred to in Article 14(3), point (c).

欧州委員会は，理事会及び上級代表に対し，本項第 1 副項(c)によって第 14 条第 3 項(c)に示すユーザから受領した要旨報告書を転送する。

The Commission shall transmit any summary report received from users referred to in Article 14(3) pursuant to the first subparagraph, point (c), of this paragraph, to the Council and the High Representative.

10. EU サイバーセキュリティリザーブの業務運営及び運営管理の全部または一部がこの規則の第 14 条第 5 項によって ENISA に対して委任されたときは，ENISA は，そのことに関し，定期的に，欧州委員会に対して報告しかつ欧州委員会から意見聴取する。その過程において，ENISA は，この規則の第 14 条第 3 項(c)に示すユーザから ENISA が受領した要請書を，また，本条の下における優先順位づけの目的のために要求されるときは，この規則の第 14 条第 3 項(a)または(b)に示すユーザから ENISA が受領した要請書を，欧州委員会に対して直ちに送付する。本項の義務は，規則(EU)2019/881 の第 14 条を妨げてはならない。

Where the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA pursuant to Article 14(5) of this Regulation, ENISA shall report to and consult the Commission on a regular basis in that

respect. In that context, ENISA shall immediately send to the Commission any requests it receives from users referred to in Article 14(3), point (c), of this Regulation and, where required for the purposes of prioritisation under this Article, any requests it has received from users referred to in Article 14(3), point (a) or (b), of this Regulation. The obligations in this paragraph shall be without prejudice to Article 14 of Regulation (EU) 2019/881.

11. 第 14 条第 3 項(a)及び(b)に示すユーザの場合においては，契約当局は，定期的に，かつ，少なくとも年 2 回，支援の利用及びその結果に関し，NIS 協力グループに対して報告する。

In the case of users referred in Article 14(3), points (a) and (b), the contracting authority shall report to the NIS Cooperation Group, on a regular basis and at least twice per year, about the use and the results of the support.

12. 第 14 条第 3 項(c)に示すユーザの場合においては，欧州委員会は，定期的に，かつ，少なくとも年 2 回，支援の利用及びその結果に関し，理事会に対して報告し，かつ，上級代表に対して連絡する。

In the case of users referred to in Article 14(3), point (c), the Commission shall report to the Council and inform the High Representative on a regular basis and at least twice per year, about the use and the results of the support.

第 17 条 信頼できるマネージドセキュリティサービスプロバイダ

Article 17 **Trusted managed security service providers**

1. EU サイバーセキュリティリザーブを設置する目的のための調達手続において，契約当局は，規則(EU, Euratom) 2024/2509 の中で定められた基本原則に従って，かつ，以下のとおりの基本原則に従って行動する：

In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in Regulation (EU, Euratom) 2024/2509 and in accordance with the following principles:

(a) 言語に関するもの，認証に関するものまたは認定に関するものを含め，そのようなサービスの提供のための国内要件をとりわけ考慮に入れた上で，EU サイバーセキュリティリザーブの中に含まれるサービスが，全体としては，EUサイバーセキュリティリザーブが全ての構成国において配置され得るサービスを含むようなものであることを確保し；

ensure that the services included in the EU Cybersecurity Reserve, when taken as a whole, are such that the EU Cybersecurity Reserve includes services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including on languages, certification or accreditation;

(b) 欧州連合及びその構成国の必須の安全保障上の利益の保護を確保し；

ensure the protection of the essential security interests of the Union and its Member States;

(c) 欧州連合内におけるサイバーセキュリティの技能の発展を促進することを含め，規則(EU) 2021/694 の第 3 条の中で定められた諸目的に対して貢献することによって，EU サイバーセキュリティリザーブが欧州連合の付加価値をもたらすことを確保する。

ensure that the EU Cybersecurity Reserve brings Union added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the Union.

2. EU サイバーセキュリティリザーブのためのサービスを調達する際，契約当局は，その調達文書の中に，以下のとおりの基準及び要件を含める：

When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following criteria and requirements:

(a) プロバイダは，そのプロバイダの担当者が，最高度の職業上の完全性，独立性，責任，及び，当該の者の特定の分野における活動を遂行するために必要な技術上の能力をもち，かつ，専門知識の耐性と継続性及び要求される技術上の資源を確保することを示す；

the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence and continuity of expertise as well as the required technical resources;

(b) プロバイダ並びに適格な子会社及び下請業者は，機密情報の保護に関する適用可能な規定を遵守し，かつ，それが適格なときは，相互の間の合意を含め，そのサービスと関連する秘密情報，及び，とりわけ，証拠，判断結果及び報告を保護するための適切な方策を設ける；

the provider, and any relevant subsidiaries and subcontractors, shall comply with applicable rules on the protection of classified information and shall have in place appropriate measures, including, where relevant, agreements between one another, to protect confidential information relating to the service, and in particular evidence, findings and reports;

(c) プロバイダは，そのプロバイダの統治構造が透明性のあるものであり，そのプロバイダの公平性及びそのプロバイダのサービスの品質を阻害しそうになく，または，利益相反を生じさせそうにないことの十分な証明を提供する；

the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;

(d) プロバイダは，構成国から要求されるときは，少なくともサービスの配置をする予定の担当者に

関し，適切なセキュリティクリアランスをもつ；

the provider shall have appropriate security clearance, at least for personnel intended for service deployment, where required by a Member State;

(e) プロバイダは，そのプロバイダの IT システムのための適格なレベルの安全性をもつ；

the provider shall have the relevant level of security for its IT systems;

(f) プロバイダは，要求されたサービスを支援するために必要となるハードウェア及びソフトウェアであって，既知の悪用可能な脆弱性を含んでおらず，最新のセキュリティアップデートを含んでおり，かつ，いかなる場合においても，欧州議会及び理事会の規則(EU) 2024/2847[23]の適用可能な条項を遵守するものを具備する；

the provider shall be equipped with the hardware and software necessary to support the requested service, which shall not contain known exploitable vulnerabilities, shall include the latest security updates and shall in any case comply with any applicable provision of Regulation (EU) 2024/2847 of the European Parliament and of the Council[23];

(g) プロバイダは，そのプロバイダが，適格な国内当局，高度の不可欠性のある部門において業務運営している法主体または他の不可欠な部門において業務運営している法主体に対して類似のサービスを供給する経験をもつということを示し得る；

the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities, entities operating in sectors of high criticality or entities operating in other critical sectors;

(h) プロバイダは，そのプロバイダがそのサービスを供給可能な構成国において短期間内にそのサービスを提供し得る：

the provider shall be able to provide the service within a short timeframe in the Member States where it can deliver the service;

(i) プロバイダは，該当するときは，そのプロバイダがそのサービスを供給可能な構成国または第

---

[23] デジタルの要素をもつ製品の横断的なサイバーセキュリティ要件に関する並びに規則(EU) No 168/2013 及び規則 (EU) 2019/1020 並びに指令 (EU) 2020/1828 を改正する欧州議会及び理事会の 2024 年 10 月 23 日の規則(EU) 2024/2847（サイバー回復力法）(OJ L, 2024/2847, 20.11.2024).

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024).

14 条第 3 項(b)及び(c)に示すユーザから要求される欧州連合の機関または構成国の 1 または複数の公用語でそのサービスを供給し得る；

the provider shall be able to provide the service in one or more official languages of the Union institutions or of a Member State as required, if any, by the Member States or users referred to in Articles 14(3), points (b) and (c), where the provider can deliver the service;

(j) 規則(EU) 2019/881 によるマネージドセキュリティサービスのための欧州サイバーセキュリティ認証制度が設けられた後，当該サービスのプロバイダは，その制度の適用の日から 2 年以内に，同制度に従って認証を受ける；

once an European cybersecurity certification scheme for managed security services pursuant to Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme within 2 years from the date of application of the scheme;

(k) プロバイダは，演習または訓練のような，インシデント対応と密接に関連する対応準備サービスへと転換され得る未使用のインシデント対応サービスの転換条件をその入札書の中に含める。

the provider shall include in the tender the conversion conditions for any unused incident response service that could be converted into preparedness services closely related to incident response, such as exercises or training.

3. EU サイバーセキュリティリザーブのためのサービスを調達する目的のために，契約当局は，それが適切なときは，構成国と緊密に協力して，第 2 項に示すものに加え，基準及び要件を策定し得る。

For the purpose of procuring services for the EU Cybersecurity Reserve, the contracting authority may, where appropriate, develop criteria and requirements in addition to those referred to in paragraph 2, in close cooperation with Member States.

第 18 条 相互補助を支援する活動

Article 18 **Actions supporting mutual assistance**

1. サイバーセキュリティ緊急メカニズムは，指令(EU) 2022/2555 の第 11 条第 3 項(f)に示す場合を含め，ある構成国から，大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントによる影響を受けた別の構成国に対する技術上の補助に対する支援を提供する。

The Cybersecurity Emergency Mechanism shall provide support for technical assistance from one Member State to another Member State affected by a significant cybersecurity incident or a large-scale cybersecurity incident, including in cases referred to in Article 11(3), point (f), of Directive (EU) 2022/2555.

2. 本条第 1 項に示す技術上の相互補助に対する支援は，助成金の方式により，かつ，規則(EU)

2021/694 の第 24 条に示す適格な作業計画の中で定められた条件に服して，提供される。

The support for the technical mutual assistance referred to in paragraph 1 of this Article shall be provided in the form of grants and subject to the conditions provided for in the relevant work programmes as referred to in Article 24 of Regulation (EU) 2021/694.

第 19 条 DEP と関係をもつ第三国に対する支援

Article 19 **Support to DEP-associated third countries**

1. DEP と関係をもつ第三国は，それによって当該第三国が DEP と関係をもつ合意が EU サイバーセキュリティリザーブへの参加を定めているときは，EU サイバーセキュリティリザーブからの支援を要請できる。その合意は，関係する DEP と関係をもつ第三国に対して本条第 2 項及び第 9 項の中で定められた義務を遵守することを要求する条項を含める。EU サイバーセキュリティリザーブへの第三国の参加の目的のために，DEP への第三国の部分的な関係樹立は，規則(EU) 2021/694 の第 6 条第 1 項(g)に示す運用事項に限定された関係樹立を含み得る。

A DEP-associated third country may request support from the EU Cybersecurity Reserve where the agreement through which it is associated to the DEP provides for participation in the EU Cybersecurity Reserve. That agreement shall include provisions requiring the DEP-associated third country concerned to comply with the obligations set out in paragraphs 2 and 9 of this Article. For the purposes of the participation of a third country in the EU Cybersecurity Reserve, the partial association of a third country to the DEP may include an association limited to the operational objective referred to in Article 6(1), point (g), of Regulation (EU) 2021/694.

2. 第 1 項に示す合意の締結から 3 か月以内に，かつ，いかなる場合においても，EU サイバーセキュリティリザーブからの支援を受ける前に，DEP と関係をもつ第三国は，欧州委員会に対し，少なくとも，大きなサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントの対応準備のために講じられた国内措置に関する情報，並びに，コンピュータセキュリティインシデント対応チームまたはそれと均等な法主体を含め，対応可能な国内法主体，その法主体の実現能力及びその法主体に割当てられる資源に関する情報を含め，当該第三国のサイバー回復力及びリスクマネジメントの実現能力に関する情報を提供する。DEP と関係をもつ第三国は，定期的に，かつ，少なくとも年 1 回，その情報のアップデートを提供する。欧州委員会は，第 11 項の適用を容易にする目的のために，上級代表及び ENISA に対し，その情報を提供する。

Within 3 months of the conclusion of the agreement referred to in paragraph 1 and in any event prior to receiving any support from the EU Cybersecurity Reserve, the DEP-associated third country shall provide to the Commission information about its cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents, as well as information on responsible national entities, including computer security incident response teams or equivalent entities, their capabilities and the resources allocated to them. The DEP-associated third country shall provide updates of that

information on a regular basis and at least once a year. The Commission shall provide the High Representative and ENISA with that information for the purposes of facilitating the application of paragraph 11.

3. 欧州委員会は，定期的に，かつ，少なくとも年 1 回，第 1 項に示す個々の DEP と関係をもつ第三国との関係において，以下の基準を評価する：

The Commission shall assess regularly, and at least once a year, the following criteria in respect of each DEP-associated third country referred to in paragraph 1:

(a) 当該条件が EU サイバーセキュリティリザーブへの参加と関連する限り，当該国が，第 1 項に示す合意の条件を遵守しているか否か；

whether that country is complying with the terms of the agreement referred to in paragraph 1, insofar as those terms relate to participation in the EU Cybersecurity Reserve;

(b) 第 2 項に示す情報を基礎として，当該国が，大きなサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントの対応準備のための適切な手立てを講じているか否か；並びに

whether that country has taken adequate steps to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents, based on the information referred to in paragraph 2; and

(c) 支援の提供が，当該国に向けた欧州連合の基本政策及び全体的な関係と一貫性があるか否か，そして，その支援の提供が，セキュリティの分野における欧州連合の他の基本政策と一貫性があるか否か。

whether the provision of support is consistent with the Union's policy towards and overall relations with that country and whether it is consistent with other Union policies in the field of security.

欧州委員会は，第 1 副項(c)に示す基準に関し，第 1 副項に示す評価を実行するときは，上級代表から意見聴取する。

The Commission shall consult the High Representative when conducting the assessment referred to in the first subparagraph, with regard to the criterion referred to in point (c) of that subparagraph.

DEP と関係をもつ第三国が第 1 副項に示す条件の全てに適合していると欧州委員会が結論づけるときは，欧州委員会は，理事会に対し，当該国に対する EU サイバーセキュリティリザーブからの支援の提供を認める第 4 項に従った実装行為を採択することの提案書を提出する。

Where the Commission concludes that a DEP-associated third country meets all of the conditions referred to in the first

subparagraph, the Commission shall submit a proposal to the Council to adopt an implementing act in accordance with paragraph 4 authorising the provision of support from the EU Cybersecurity Reserve to that country.

4. 理事会は，第3項に示す実装行為を採択できる。当該実装行為は，最長で1年間適用される。当該実装行為の適用期間は，更新され得る。単一の要請に応答する支援が提供され得る日数に関し，75 日を下回らない制限を含め得る。

The Council may adopt the implementing acts referred to in paragraph 3. Those implementing acts shall apply for a maximum of one year. They may be renewed. They may include a limit of no less than 75 days on the number of days for which support can be provided in response to a single request.

本条の目的のために，理事会は，即座に行動し，かつ，原則として，第 3 項第 3 副項によって欧州委員会の適格な提案の採択から 8 週間以内に，本項に示す実装行為を採択する。

For the purposes of this Article, the Council shall act expeditiously and shall, as a rule, adopt the implementing acts referred to in this paragraph within eight weeks of the adoption of the relevant Commission proposal pursuant to paragraph 3, third subparagraph.

5. 理事会は，欧州委員会の提案に基づいて行動し，いつでも，第4項によって採択した実装行為を改正または廃止できる。

The Council may amend or repeal an implementing act adopted pursuant to paragraph 4 at any time, acting on a proposal of the Commission.

理事会が，第3項第1副項(c)に示す基準に関して大きな変化があったと判断するときは，理事会は，1または複数の構成国の適正に根拠づけられた発意に基づいて行動し，第4項によって採択した実装行為を改正または廃止できる。

Where the Council considers there to have been a significant change concerning the criterion referred to in paragraph 3, first subparagraph, point (c), the Council may amend or repeal an implementing act adopted pursuant to paragraph 4 acting on the duly reasoned initiative of one or more Member States.

6. 本条の下にある理事会の実装権限の行使において，理事会は，第 3 項第 1 副項に示す基準を適用し，かつ，それらの基準についての理事会の評価を説明する。とりわけ，第 5 条第 2 副項によって理事会自身の発意に基づいて理事会が行動する場合，理事会は，同副項に示す大きな変化を説明する。

In the exercise of its implementing powers under this Article, the Council shall apply the criteria referred to in paragraph 3, first subparagraph, and shall explain its assessment of those criteria. In particular, where it acts on its own initiative pursuant to paragraph 5, second subparagraph, the Council shall explain the significant change referred to in that

subparagraph.

7. EU サイバーセキュリティリザーブから DEP と関係をもつ第三国に対する支援は，第 1 項に示す合意の中で定められた細目的な条件を遵守する。

Support from the EU Cybersecurity Reserve to a DEP-associated third country shall comply with any specific conditions laid down in the agreement referred to in paragraph 1.

8. EU サイバーセキュリティリザーブからサービスを受ける適格のある DEP と関係をもつ第三国からのユーザは，コンピュータセキュリティインシデント対応チームまたはそれと均等な法主体及びサイバー危機管理当局のような，職務権限のある当局を含む。

Users from DEP-associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as computer security incident and response teams or equivalent entities and cyber crisis management authorities.

9. EU サイバーセキュリティリザーブからの支援を受ける適格のある各 DEP と関係をもつ第三国は，この規則の目的のために単一連絡部局として行動する 1 つの当局を指定する。

Each DEP-associated third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single point of contact for the purposes of this Regulation.

10. 本条の下における EU サイバーセキュリティリザーブからの支援を求める要請は，欧州委員会によって評価される。契約当局は，本条第 4 項によって採択された当該国との関係においてそのような支援を認める理事会の実装行為が発効しているときに限り，かつ，その範囲内に限り，第三国に対して支援を提供し得る。応答は，不適切な遅滞なく，第 14 条第 3 項(c)に示すユーザに対して転送される。

Requests for support from the EU Cybersecurity Reserve under this Article shall be assessed by the Commission. The contracting authority may provide support to a third country only where, and for so long as, a Council implementing act authorising such support in respect of that country adopted pursuant to paragraph 4 of this Article is in force. A response shall be transmitted to the users referred to in Article 14(3), point (c), without undue delay.

11. 本条の下における支援を求める要請書の受領の後，欧州委員会は，理事会に対し，直ちに連絡する。欧州委員会は，当該要請の評価が理事会に対して連絡されることを保つ。欧州委員会は，受領した要請及び EU サイバーセキュリティリザーブから DEP と関係をもつ第三国に対して与えられる支援の実装に関し，上級代表とも協力する。加えて，欧州委員会は，それらの要請に関し，ENISA から提供される見解も考慮に入れる。

Upon receipt of a request for support under this Article, the Commission shall immediately inform the Council. The

Commission shall keep the Council informed of the assessment of the request. The Commission shall also cooperate with the High Representative about the requests received and the implementation of the support granted to DEP-associated third countries from the EU Cybersecurity Reserve. Additionally, the Commission shall also take into account any views provided by ENISA in respect of those requests.

第 20 条 欧州連合の危機管理の仕組みとの調整

Article 20 **Coordination with Union crisis management mechanisms**

1. 大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントが決定 No 1313/2013/EU の第 4 条第 1 号の中で定義された災害から生ずる場合またはその災害を帰結する場合，そのようなインシデントへの対応のためにこの規則の下において提供される支援は，同決定の下における活動を補完し，かつ，同決定を妨げない。

Where a significant cybersecurity incident, a large-scale cybersecurity incident or a large-scale-equivalent cybersecurity incident originates from or results in a disaster as defined in Article 4, point (1), of Decision No 1313/2013/EU, the support provided under this Regulation for responding to such incident shall complement actions under, and be without prejudice to, that Decision.

2. 実装決定(EU) 2018/1993 の下における EU 統合政治的危機対応覚書（IPCR 覚書）が発動されている場合における大規模サイバーセキュリティインシデントまたは大規模と均等なサイバーセキュリティインシデントの場合においては，そのようなインシデントへの対応のためにこの規則の下において提供される支援は，IPCR 覚書の下にある適格な手続に従って取り扱われる。

In the event of a large-scale cybersecurity incident or a large-scale-equivalent cybersecurity incident where the EU Integrated Political Crisis Response Arrangements under Implementing Decision (EU) 2018/1993 (IPCR Arrangements) are activated, support provided under this Regulation for responding to such incident shall be handled in accordance with the relevant procedures under the IPCR Arrangements.

第 IV 章 欧州サイバーセキュリティインシデント見直しメカニズム
Chapter IV European Cybersecurity Incident Review Mechanism

第 21 条 欧州サイバーセキュリティインシデント見直しメカニズム
Article 21 European Cybersecurity Incident Review Mechanism

1. 欧州委員会または EU-CyCLONe の要請があるときは，ENISA は，CSIRTs ネットワークの支援を得て，かつ，関係する構成国の承認を受け，特定の大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントと関係するサイバーな脅威，既知の悪用可能な脆弱性及び緩和の活動を見直し及び評価する。インシデントの見直し及び評価の完了後，かつ，将来のインシデントを避けるためまたは緩和するために習んだ教訓を描出することを狙いとして，ENISA は，EU-CyCLONe，CSIRTs ネットワーク，関係する構成国及び欧州委員会に対し，それらの職務の遂行において，とりわけ，指令(EU)2022/2555 の第 15 条及び第 16 条の中で定められた職務の遂行においてそれらを支援するため，インシデント見直し報告書を供給する。インシデントが DEP と関係をもつ第三国に対して影響をもつときは，ENISA は，理事会に対し，その報告書を提供する。そのような場合において，欧州委員会は，上級代表に対し，その報告書を提供する。

   At the request of the Commission or EU-CyCLONe, ENISA shall, with the support of the CSIRTs network and with the approval of the Member States concerned, review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident and with the aim of drawing lessons learned to avoid or mitigate future incidents, ENISA shall deliver an incident review report to EU-CyCLONe, the CSIRTs network, the Member States concerned and the Commission to support them in carrying out their tasks, in particular the tasks set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where an incident has an impact on a DEP-associated third country, ENISA shall provide the report to the Council. In such cases, the Commission shall provide the report to the High Representative.

2. 本条第 1 項に示すインシデント見直し報告書を準備するため，ENISA は，構成国の代表，欧州委員会，他の適格な欧州連合の機関，組織，事務局及び部局，マネージドセキュリティサービスプロバイダを含め，産業界，並びに，サイバーセキュリティサービスのユーザを含め，適格な全ての利害関係者と協力し，かつ，それらの者からのフィードバックを集める。それが適切なときは，ENISA は，CSIRTs と，及び，それが適格なときは，指令(EU)2022/2555 の第 8 条第 1 項によって指定されまたは設置された職務権限のある当局と協力した上で，大きなサイバーセキュリティインシデントまたは大規模なセキュリティインシデントによって影響を受けた法主体とも協力する。意見聴取を受けた代表は，潜在的な利益相反を開示する。

   To prepare the incident review report referred to in paragraph 1 of this Article, ENISA shall cooperate with and gather feedback from all relevant stakeholders, including representatives of Member States, the Commission, other relevant Union institutions, bodies, offices and agencies, industry, including managed security services providers, and users of cybersecurity services. Where appropriate, ENISA shall, in cooperation with CSIRTs and, where relevant, the competent

authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555, also cooperate with entities affected by significant cybersecurity incidents or large-scale cybersecurity incidents. Consulted representatives shall disclose any potential conflict of interest.

3. 本条第 1 項に示すインシデント見直し報告書は，主たる原因，既知の悪用可能な脆弱性及び学んだ教訓を含め，特定の大きなサイバーセキュリティインシデントまたは大規模なサイバーセキュリティインシデントの見直し及び分析を包摂する。ENISA は，その報告書が，機微の情報または機密情報の保護と関係する欧州連合法または国内法を遵守することを確保する。適格な構成国またはそれ以外のインシデントによって影響を受けている第 14 条第 3 項に示すユーザが，そのように要請するときは，その報告書に含まれているデータ及び情報は，匿名化される。その報告書は，まだパッチがあてられていない積極的に悪用された脆弱性に関する詳細を含めてはならない。

The incident review report referred to in paragraph 1 of this Article shall cover a review and analysis of the specific significant cybersecurity incident or large-scale cybersecurity incident, including the main causes, known exploitable vulnerabilities and lessons learned. ENISA shall ensure that the report complies with Union or national law concerning the protection of sensitive or classified information. If the relevant Member States or other users referred to in Article 14(3) that are affected by the incident so request, the data and information contained in the report shall be anonymised. It shall not include any details about actively exploited vulnerabilities that remain unpatched.

4. それが適切なときは，インシデント見直し報告書は，欧州連合のサイバーポスチャーの改善のための推奨事項を描出し，かつ，適格な利害関係者から学んだベストプラクティス及び教訓を含め得る。

Where appropriate, the incident review report shall draw recommendations to improve the Union's cyber posture and may include best practices and lessons learned from relevant stakeholders.

5. ENISA は，公衆が利用可能な版のインシデント見直し報告書を発行し得る。その版の報告書は，信頼できる公開情報，または，それ以外の関係する構成国の同意を得た信頼できる情報，及び，第 14 条第 3 項(b)または(c)に示すユーザと関連する情報に関しては，当該ユーザの同意を得た信頼できる情報のみを含める。

ENISA may issue a publicly available version of the incident review report. That version of the report shall include only reliable public information, or other reliable information with the consent of the Member States concerned and, as regards information relating to a user as referred to in Article 14(3), point (b) or (c), with the consent of that user.

第 V 章 最終規定
Chapter V Final Provisions

第 22 条 規則(EU) 2021/694 の改正
Article 22 Amendments to Regulation (EU) 2021/694

規則(EU) 2021/694 は，以下のとおり改正される:

Regulation (EU) 2021/694 is amended as follows:

(1) 第 6 条は，以下のとおり改正される:

Article 6 is amended as follows:

(a) 第 1 項は，以下のとおり改正される:

paragraph 1 is amended as follows:

(i) 以下の号が挿入される:

the following point is inserted:

「(aa) 欧州連合における状況認識及び欧州連合のサイバーな脅威の情報収集能力を拡大することに貢献する国内サイバーハブ及び国境を越えるサイバーハブの開発，配置及び運用を含め，欧州議会及び理事会の規則(EU) 2025/38[(*)] の第 3 条によって設置される欧州サイバーセキュリティ警報システム（『欧州サイバーセキュリティ警報システム』）の開発を支援し;

support the development of the European Cybersecurity Alert System established by Article 3 of Regulation (EU) 2025/38 of the European Parliament and of the Council [(*1)] (the "European Cybersecurity Alert System"), including the development, deployment and operation of National Cyber Hubs and Cross-Border Cyber Hubs that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;

[(*)] サイバーな脅威とインシデントを検出し，それに対して準備し及び対応するための欧州連合内の結束と能力を強化するための措置を定め並びに規則(EU) 2021/694 を改正する欧州議会及び理事会の 2024 年 12 月 19 日の規則(EU) 2025/38（サイバー結束法）(OJ L, 2025/38, 15.1.2025).」;

Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15.1.2025).' ;

(ii) 以下の号が付加される:

the following point is added:

「(g) 大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントに対して対応準備すること及びそれに対して対応することにおいて，国内の資源と実現能力及び欧州連合レベルで利用可能な他の形態の支援を補完して構成国を支援し，かつ，大きなサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対応することにおいて他のユーザを支援するための規則(EU) 2025/38 の第 14 条によって設置される EU サイバーセキュリティリザーブ（『EU サイバーセキュリティリザーブ』）を含め，同規則の第 10 条によって設置されるサイバーセキュリティ緊急メカニズムを設置し及び運用し;」;

establish and operate the Cybersecurity Emergency Mechanism established by Article 10 of Regulation (EU) 2025/38, including the EU Cybersecurity Reserve established by Article 14 of that Regulation (the "EU Cybersecurity Reserve"), to support Member States in preparing for and responding to significant cybersecurity incidents and large-scale cybersecurity incidents that is complementary to national resources and capabilities and other forms of support available at Union level, and to support other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents;';

(b) 第 2 項は，以下のとおりに置き換えられる:

paragraph 2 is replaced by the following:

「2. 個別対象 3 の下にある活動は，基本的に，欧州議会及び理事会の規則(EU) 2021/887(*)に従い，欧州サイバーセキュリティ産業，技術及び調査研究能力拠点及び国内調整拠点のネットワークを介して実装される。ただし，EU サイバーセキュリティリザーブは，欧州委員会によって，及び，規則(EU) 2025/38 の第 14 条第 6 項に従い，ENISA によって実装される。

The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres in accordance with Regulation (EU) 2021/887 of the European

Parliament and of the Council[*2]. However, the EU Cybersecurity Reserve shall be implemented by the Commission and, in accordance with Article 14(6) of Regulation (EU) 2025/38, by ENISA.

[*] 欧州サイバーセキュリティ産業，技術及び調査研究能力拠点及び国内調整拠点のネットワークを設ける欧州議会及び理事会の 2021 年 5 月 20 日の規則(EU) 2021/887 (OJ L 202, 8.6.2021, p. 1).」;

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).'.

(2) 第 9 条は，以下のとおり改正される:

Article 9 is amended as follows:

(a) 第 2 項(b), (c)及び(d)は，以下のとおり置き換えられる:

in paragraph 2, points (b), (c) and (d) are replaced by the following:

「(b) 個別対象 2－人工知能に対し，17 億 6080 万 6000 ユーロ;
(c) 個別対象 3－サイバーセキュリティ及び信頼に対し，13 億 7202 万 0000 ユーロ;
(d) 個別対象 4－高度なデジタル技能に対し，4 億 8264 万 0000 ユーロ;」;

(b) EUR 1 760 806 000 for Specific Objective 2 – Artificial Intelligence;
(c) EUR 1 372 020 000 for Specific Objective 3 – Cybersecurity and Trust;
(d) EUR 482 640 000 for Specific Objective 4 – Advanced Digital Skills;';

(b) 以下のとおりの項が付加される:

the following paragraph is added:

「8. 財政規則の第 12 条第 1 項からの特例により，規則(EU) 2025/38 による EU サイバーセキュリティリザーブの実装の過程における活動及び相互補助を支援する活動であって，この規則の第 6 条第 1 項(g)の中で定められた運用事項を追求する活動のための未使用の拠出及び決済の予算枠は，自動的に繰り越しとなり，かつ，次予算年の 12 月 31 日まで拠出され及び支払われ得る。欧州議会及び理事会は，財政規則の第 12 条第 6 項によって繰り越された予算枠の連絡を受ける。」;

By way of derogation from Article 12(1) of the Financial Regulation, unused commitment and

payment appropriations for actions in the context of the implementation of the EU Cybersecurity Reserve and the actions supporting mutual assistance pursuant to Regulation 2025/38, pursuing the objectives set out in Article 6(1), point (g), of this Regulation shall be automatically carried over and may be committed and paid up to 31 December of the following financial year. The European Parliament and the Council shall be informed of appropriations carried over pursuant to Article 12(6) of the Financial Regulation.';

(3) 第 12 条は，以下のとおり改正される:

Article 12 is amended as follows:

(a) 以下のとおりの項が挿入される:

the following paragraphs are inserted:

5a. 欧州連合内に拠点をもつけれども第三国から支配されている法主体と関係する限り，関係する活動との関係において以下の条件のいずれもが満たされているときは，欧州サイバーセキュリティ警報システムを実装する活動に対し，第 5 項は，適用されてはならない:

Paragraph 5 shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to any action implementing the European Cybersecurity Alert System where both of the following conditions are fulfilled in respect of the action concerned:

(a) 規則(EU)2025/38 の第 9 条第 4 項によって実施されるマッピングの結果を考慮に入れた上で，欧州サイバーセキュリティ警報システムの諸目的に対して適切に貢献するために当該活動にとって必要かつ十分なツール，インフラまたはサービスが，構成国内に拠点をもちまたは拠点をもつとみなされ，かつ，構成国によってまたは構成国の国民によって支配されている法主体からは利用可能ではなくなるという現実のリスクが存在し;

there is a real risk, taking into account the results of the mapping carried out pursuant to Article 9(4) of Regulation (EU) 2025/38, that the tools, infrastructure or services necessary and sufficient for that action to adequately contribute to the objective of the European Cybersecurity Alert System will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States;

(b) 欧州サイバーセキュリティ警報システム内にあるそのような法主体からの調達の安全保障上のリスクが，その利益と比例しており，かつ，欧州連合及びその

構成国の安全保障上の必須の利益を損ねることがない。

the security risk of procuring from such legal entities within the European Cybersecurity Alert System is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States.

5b. 欧州連合内に拠点をもつけれども第三国から支配されている法主体と関係する限り，関係する活動との関係において以下の条件のいずれもが満たされているときは，EU サイバーセキュリティリザーブを実装する活動に対し，第 5 項は，適用されてはならない：

Paragraph 5 shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to any action implementing the EU Cybersecurity Reserve where both of the following conditions are fulfilled in respect of the action concerned:

(a) 規則(EU) 2025/38 の第 14 条第 6 項によって実施されるマッピングの結果を考慮に入れた上で，EU サイバーセキュリティリザーブの機能を適切に遂行するために EU サイバーセキュリティリザーブにとって必要かつ十分な技術，専門知識または能力が，構成国内に拠点をもちまたは拠点をもつとみなされ，かつ，構成国によってまたは構成国の国民によって支配されている法主体からは利用可能ではなくなるという現実のリスクが存在し；

there is a real risk, taking into account the results of the mapping carried out pursuant to Article 14(6) of Regulation (EU) 2025/38, that the technology, expertise or capacity necessary and sufficient for the EU Cybersecurity Reserve to adequately perform its functions will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States;

(b) EU サイバーセキュリティリザーブ内にあるそのような法主体を含めることの安全保障上のリスクが，その利益と比例しており，かつ，欧州連合及びその構成国の安全保障上の必須の利益を損ねることがない。」；

the security risk of including such legal entities within the EU Cybersecurity Reserve is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States.';

(b) 第 6 項は，以下のとおりに置き換えられる：

paragraph 6 is replaced by the following:

「6. 安全保障上の理由により適正に正当化される場合においては，それらの法主体が，欧州連合及び構成国の安全保障上の必須の利益の防護を保証するため及び機密文書の情報の防護を確保するために，当該法主体によって満たされるべき要件を遵守する場合に限り，作業計画は，関係をもつ国の中に拠点をもつ法主体及び欧州連合の中に拠点をもつけれども第三国の支配下にある法主体が，個別対象 1 及び 2 に基づく活動の全部または一部に参加する適格があることも定め得る。それらの要件は，作業計画の中で定められる。

If duly justified for security reasons, the work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries may be eligible to participate in all or some actions under Specific Objectives 1 and 2 only if they comply with the requirements to be fulfilled by those legal entities to guarantee the protection of the essential security interests of the Union and the Member States and to ensure the protection of classified documents information. Those requirements shall be set out in the work programme.

第 1 副項は，欧州連合内に拠点をもつけれども第三国から支配されている法主体と関係する限り，個別対象 3 の下にある活動に対しても適用される：

The first subparagraph shall also apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to actions under Specific Objective 3:

(a) 第 5 項 a が適用される場合，欧州サイバーセキュリティ警報システムを実装するため；及び

to implement the European Cybersecurity Alert System where paragraph 5a applies; and

(b) 第 5 項 b が適用される場合，EU サイバーセキュリティリザーブを実装するため。」；

to implement the EU Cybersecurity Reserve where paragraph 5b applies.';

(4) 第 14 条第 2 項は，以下の通りに置き換えられる：

in Article 14, paragraph 2 is replaced by the following:

「2. 計画は，とりわけ，基本的な方式としての調達による場合または助成金及び賞金による場合を含め，財政規則の中で定められた方式のいずれかにより，資金を提供し得る。

The Programme may provide funding in any of the forms laid down in the Financial Regulation, including

in particular through procurement as a primary form, or grants and prizes.

活動の目的の達成が，革新的な物品及びサービスの調達を要求する場合，助成金は，欧州議会及び理事会の指令 2014/24/EU(*)及び指令 2014/25/EU(**)の中で定義された契約当局または契約法主体である受益者に対してのみ，供与され得る。

Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU(*) and 2014/25/EU(**) of the European Parliament and of the Council.

活動の目的を達成するために，大規模商業ベースではまだ利用可能となっていない革新的な物品またはサービスの供給を必要とする場合，契約当局または契約法主体は，同じ調達手続の中で，多角的な契約の供与が認められ得る。

Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure.

公共の保安上の適正に正当化される理由に関し，契約当局または契約法主体は，契約の履行地が欧州連合の領域内にあることを要求できる。

For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union.

EU サイバーセキュリティリザーブのための調達手続を実装する際，欧州委員会及び ENISA は，この規則の第 10 条に従って計画と関係をもつ第三国の代わりにまたはその名において調達するための中央購入組織として行動し得る。欧州委員会及び ENISA は，当該第三国に対し，資材及びサービスを購入すること，貯蔵すること及び再販売すること，または，貸与することを含め寄付することによって，卸売業者としても行動できる。欧州議会及び理事会の規則(EU, Euratom) 2024/2509(***)の第 168 条第 3 項からの特例により，単独の第三国からの要請は，欧州委員会または ENISA に対して法行為を委任するために十分なものとする。

When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in accordance with Article 10 of this Regulation. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council(***), the request from a single third country shall be sufficient to mandate the Commission or ENISA to act.

EU サイバーセキュリティリザーブのための調達手続を実装する際，欧州委員会及び ENISA は，欧州連合の機関，組織，事務局または部局の代わりにまたはその名において調達するための中央購入組織として行動し得る。欧州委員会及び ENISA は，欧州連合の機関，組織，事務局または部局に対し，資材及びサービスを購入すること，貯蔵すること及び再販売すること，または，貸与することを含め寄付することによって，卸売業者としても行動できる。規則(EU, Euratom) 2024/2509 の第 168 条第 3 項からの特例により，単独の欧州連合の機関，組織，事務局または部局からの要請は，欧州委員会または ENISA に対して法行為を委任するために十分なものとする。

When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies, offices or agencies. The Commission and ENISA may also act as a wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies, offices or agencies. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509, a request from a single Union institution, body, office or agency shall be sufficient to mandate the Commission or ENISA to act.

計画は，混合オペレーションの範囲内にある決済手段の方式によっても資金拠出を提供し得る。

The Programme may also provide financing in the form of financial instruments within blending operations.

(*) 公共調達に関する及び指令 2004/18/EC を廃止する欧州議会及び理事会の 2014 年 2 月 26 日の指令 2014/24/EU (OJ L 94, 28.3.2014, p. 65).

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

(**) 水道，エネルギー，輸送及び郵便サービス部門において業務遂行する組織による調達に関する並びに指令 2014/17/EC を廃止する 2014 年 2 月 26 日の指令 2014/25/EU (OJ L 94, 28.3.2014, p. 243).

Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

(***) 欧州連合の一般予算に対して適用可能な資金提供上の諸原則に関する欧州議会及び理事会の 2024 年 9 月 23 日の規則(EU, Euratom) 2024/2509 (OJ L, 2024/2509, 26.9.2024,).」;

Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.9.2024).';

(5) 以下のとおりの条が挿入される:

the following article is inserted:

「第 16 条 a 諸規定の抵触
'Article 16a **Conflicts of rules**

欧州サイバーセキュリティ警報システムを実装する活動の場合において，適用可能な規定は，規則(EU) 2025/38 の第 4 条，第 5 条及び第 9 条の中で定められた規定とする。この規則の条項と規則(EU) 2025/38 の第 4 条，第 5 条及び第 9 条との間の抵触の場合においては，後者が優越し，かつ，当該個々の活動に対して適用される。

In the case of actions implementing the European Cybersecurity Alert System, the applicable rules shall be those set out in Articles 4, 5 and 9 of Regulation (EU) 2025/38. In the case of a conflict between the provisions of this Regulation and Articles 4, 5 and 9 of Regulation (EU) 2025/38, the latter shall prevail and apply to those specific actions.

EU サイバーセキュリティリザーブの場合において，計画と関係をもつ第三国の参加のための特別の規定は，規則(EU) 2025/38 の第 19 条の中で定められている。この規則の条項と規則(EU) 2025/38 の第 19 条との間の抵触の場合においては，後者が優越し，かつ，当該個々の活動に対して適用される。」;

In the case of EU Cybersecurity Reserve, specific rules for the participation of third countries associated to the Programme are laid down in Article 19 of Regulation (EU) 2025/38. In the case of a conflict between the provisions of this Regulation and Article 19 of Regulation (EU) 2025/38, the latter shall prevail and apply to those specific actions.';

(6) 第 19 条は，以下のとおりに置き換えられる:

Article 19 is replaced by the following:

「第 19 条 助成金
'Article 19 **Grants**

計画の下における助成金は，財政規則の第 VIII 款に従って供与され及び運営管理され，かつ，財政規則の第 190 条の中で定められた共同資金提供の基本原則を妨げることなく，適格な費用の 100%まで包摂し得る。そのような助成金は，各個別対象について個別の

ものとして，供与され及び運営管理される。

Grants under the Programme shall be awarded and managed in accordance with Title VIII of the Financial Regulation and may cover up to 100 % of the eligible costs, without prejudice to the co-financing principle as laid down in Article 190 of the Financial Regulation. Such grants shall be awarded and managed as specified for each specific objective.

助成金の方式による支援は，提案の募集なしに，財政規則の第 195 条第 1 項(d)に従い，規則(EU) 2025/38 の第 9 条によって選抜された構成国及び規則(EU) 2025/38 の第 5 条に示すホスティングコンソーシアムに対し，ECCC から直接に供与され得る。

Support in the form of grants may be awarded directly by the ECCC without a call for proposals to the Member States selected pursuant to Article 9 of Regulation (EU) 2025/38 and the Hosting Consortium referred to in Article 5 of Regulation (EU) 2025/38, in accordance with Article 195(1), point (d), of the Financial Regulation.

サイバーセキュリティ緊急メカニズムのための助成金の方式による支援は，提案の募集なしに，財政規則の第 195 条第 1 項(d)に従い，構成国に対し，ECCC から直接に供与され得る。

Support in the form of grants for the Cybersecurity Emergency Mechanism may be awarded directly by the ECCC to Member States without a call for proposals, in accordance with Article 195(1), point (d), of the Financial Regulation.

規則(EU) 2025/38 の第 18 条の中で定められた相互補助を支援する活動に関しては，ECCC は，欧州委員会及び ENISA に対し，提案の募集なしに直接に助成金を求める構成国の要請に関して連絡する。

With regard to actions supporting mutual assistance provided for in Article 18 of Regulation (EU) 2025/38, the ECCC shall inform the Commission and ENISA about Member States' requests for direct grants without a call for proposals.

規則(EU) 2025/38 の第 18 条の中で定められた相互補助を支援する活動に関しては，かつ，財政規則の第 193 条第 2 項第 2 副項(a)に従い，その費用は，適正に正当化される場合においては，助成金の申請書が提出された時よりも前に当該費用がかかったとしても，適格であると判断され得る。

With regard to actions supporting mutual assistance provided for in Article 18 of Regulation (EU) 2025/38, and in accordance with Article 193(2), second subparagraph, point (a), of the Financial Regulation, the costs may, in duly justified cases, be considered to be eligible even if they were incurred before the grant application

was submitted.';

(7) 別紙 I 及び II は，この規則の別紙に従って改正される。

Annexes I and II are amended in accordance with the Annex to this Regulation.

第 23 条 委任の実行

Article 23 **Exercise of the delegation**

1. 本条の中で定められた条件に服して，委任される行為を採択する権限は，欧州委員会に対して与えられる。

The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 14 条第 7 項に示す委任される行為を採択する権限は，2025 年 2 月 5 日から 5 年間，欧州委員会に対して与えられる。欧州委員会は，その 5 年間の終了前の遅くとも 9 か月以内に，権限の委任との関係における報告書を作成する。権限の委任は，各期間の終了前の遅くとも 3 か月以内に欧州議会または理事会がそのような延長に反対しない限り，同一の期間で，黙示に延長される。

The power to adopt delegated acts referred to in Article 14(7) shall be conferred on the Commission for a period of 5 years from 5 February 2025. The Commission shall draw up a report in respect of the delegation of power not later than 9 months before the end of the 5-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than 3 months before the end of each period.

3. 第 14 条第 7 項に示す権限の委任は，欧州議会または理事会によって，いつでも，取消され得る。取消の決定は，当該決定の中で示された権限の委任を終了させる。その取消しは，EU 官報上の決定の公示の翌日に発効し，または，その決定の中で指定される後日に発効する。その取消しは，既に発効している委任される行為の有効性に影響を与えない。

The delegation of power referred to in Article 14(7) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following that of the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. 委任される行為を採択する前に，欧州委員会は，より良い立法に関する 2016 年 4 月 13 日の機関間合意の中で定められた基本原則に従い，各構成国から指定された専門家から意見聴取する。

Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance

with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. 委任される行為を採択した後直ちに，欧州委員会は，欧州議会及び理事会に対し，同時に通知する。
As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. 第 14 条第 7 項により採択された委任される行為は，欧州議会及び理事会に対するその行為の通知から 2 か月以内に欧州議会及び理事会のいずれからも異議が表明されなかったとき，または，その期間の満了前であっても，欧州議会及び理事会の両者が欧州委員会に対して異議がない旨を通知したときに発効する。その期間は，欧州議会または理事会からの提案により，2 か月まで延長される。

A delegated act adopted pursuant to Article 14(7) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of 2 months of the notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or of the Council.

第 24 条 委員会の手続
Article 24 **Committee procedure**

1. 欧州委員会は，規則(EU) 2021/694 の第 31 条第 1 項に示すデジタル欧州計画調整委員会によって補佐を受ける。この委員会は，規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by the Digital Europe Programme Coordination Committee referred to in Article 31(1) of Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項に対する参照が行われたときは，規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

第 25 条 評価及び見直し
Article 25 **Evaluation and review**

1. 2027 年 2 月 5 日までに及びその後は少なくとも 4 年毎に，欧州委員会は，この規則の中で定められた措置の稼動を評価し，かつ，欧州議会及び理事会に対し，報告書を提出する。

By 5 February 2027 and at least every 4 years thereafter, the Commission shall evaluate the functioning of the measures provided for in this Regulation and shall submit a report to the European Parliament and to the Council.

2. 第 1 項に示す評価は，とりわけ，以下の諸点を評価する：

The evaluation referred to in paragraph 1 shall assess, in particular:

(a) 設置された国内サイバーハブ及び国境を越えるサイバーハブの数，それが可能なときは，CSIRTs ネットワークの仕事に対する影響を含め，共有された情報の範囲，並びに，サイバーな脅威及びインシデントの欧州連合の共通の検出及び状況認識を強化することに対して及び最新の技術の開発に対してそれらのハブが貢献した範囲；共同で調達されるサイバーセキュリティのツール，インフラまたはサービスのための DEP 資金提供の利用；また，その情報が利用可能なときは，国内サイバーハブと，指令(EU) 2022/2555 の第 3 条に示す必須の法主体及び重要な法主体の部門別コミュニティ及び部門横断のコミュニティとの間の協力のレベル；

the number of National Cyber Hubs and Cross-Border Cyber Hubs established, the extent of information shared, including, if possible, the impact on the work of the CSIRTs network, and the extent to which those have contributed to strengthening common Union detection and situational awareness of cyber threats and incidents and to the development of state-of-the-art technologies; the use of DEP funding for cybersecurity tools, infrastructure, or services jointly procured; and, if the information is available, the level of cooperation between National Cyber Hubs and sectoral and cross-sectoral communities of essential and important entities as referred to in Article 3 of Directive (EU) 2022/2555;

(b) 訓練を含め，サイバーセキュリティ緊急メカニズムが支援する準備態勢の下における活動の利用及び実効性，DEP 資金提供を含め，大きなサイバーセキュリティインシデント，大規模なサイバーセキュリティインシデント及び大規模と均等なサイバーセキュリティインシデントに対する対応及びそれに対する最初の復旧，並びに，サイバーセキュリティ緊急メカニズムの実装からの学んだ教訓及び推奨事項；

the use and effectiveness of actions under the Cybersecurity Emergency Mechanism supporting preparedness, including training, response to and initial recovery from significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents, including the use of DEP funding and the lessons learned and recommendations from the implementation of the Cybersecurity Emergency Mechanism;

(c) DEP 資金提供の利用を含め，ユーザのタイプとの関係における EU サイバーセキュリティリザーブの利用及び実効性，そのサービスのタイプを含め，サービスの受入れ，要請に対する応答のための及び EU サイバーセキュリティリザーブが配置されるための平均期間，インシデントの防止及び対応と関連する対応準備サービスに転換されたサービスの割合，並びに，EU サイバーセキュリティリザーブの実装からの学んだ教訓及び推奨事項；

the use and effectiveness of the EU Cybersecurity Reserve in relation to types of user, including the use of DEP funding, the uptake of services, including their type, the average time for responding to the requests and for the EU Cybersecurity Reserve to be deployed, the percentage of services converted into preparedness services related to incident prevention and response and the lessons learned and recommendations from the implementation of the EU Cybersecurity Reserve;

(d) マイクロ企業及び小企業と中規模企業並びにスタートアップを含め，デジタル経済全般にわたる欧州連合内の製造業及びサービス業の競争力のある地位を強化することへのこの規則の貢献，並びに，就労者のサイバーセキュリティ上の技能及び能力を強化するという全体的な目的に対する貢献。

the contribution of this Regulation to strengthening the competitive position of the industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and the contribution to the overall objective of reinforcing the cybersecurity skills and capacities of the workforce.

3. 第 1 項に示す報告書を基礎として，欧州委員会は，それが適切なときは，欧州議会及び理事会に対し，この規則を改正するための立法提案書を提出する。

On the basis of the reports referred to in paragraph 1, the Commission shall, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.

第 26 条 発効

Article 26 **Entry into force**

この規則は，EU 官報上におけるその公示の 20 日後に発効する。

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

この規則は，その全体について拘束力があり，かつ，全ての構成国において直接に適用される。

This Regulation shall be binding in its entirety and directly applicable in all Member States.

2024 年 12 月 19 日にブリュッセルにおいて行われた。

Done at Brussels, 19 December 2024.

欧州議会として	理事会として
For the European Parliament	For the Council
長　R. METSOLA	長　BÓKA J.
The President　R. METSOLA	The President　BÓKA J.

別 紙
ANNEX

規則(EU) 2021/694 は，以下のとおりに改正される：

Regulation (EU) 2021/694 is amended as follows:

(1) 別紙 I の中において，「個別対象 3ーサイバーセキュリティ及び信頼」は，以下のとおりに置き換えられる：

in Annex I, the section 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:

「**個別対象 3ーサイバーセキュリティ及び信頼**

Specific Objective 3 – **Cybersecurity and Trust**

計画は，指令(EU) 2016/1148 の実装を支援することによる場合を含め，欧州連合のサイバーセキュリティ産業の潜在力及び競争力を強化することにより，並びに，市民及び事業者をサイバーな脅威から防護するための民間部門及び公的部門両者の実現能力を向上させることにより，欧州連合のデジタルな経済，社会及び民主主義を安全にするために必須の遂行能力の強化，構築及び獲得を刺激する。

The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union's digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.

この個別対象の下にある最初の活動，及び，それが適切なときは，後続の活動は，以下のものを包摂する：

Initial and, where appropriate, subsequent actions under this objective shall include:

1. 不可欠インフラ及びデジタル単一市場を最大限防護するために必須である高度なセキュリティの機器，インフラ及びノウハウへの構成国との共同投資。そのような共同投資は，欧州サイバーセキュリティ警報システムを形成する国内サイバーハブ及び国境を越えるサイバーハブを含め，サイバーセキュリティのための量子施設及びデータ資源，サイバー空間における状況認識への投資，並びに，欧州全域にわたり公的部門及び民間部門に対して利用できるようにされるその他のツールへの投資を含め得る。

   Co-investment with Member States in advanced cybersecurity equipment, infrastructure and know-how that are

essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace including National Cyber Hubs and Cross-Border Cyber Hubs forming the European Cybersecurity Alert System, as well as other tools to be made available to public and private sector across Europe.

2. デジタル単一市場内のサイバーセキュリティと信頼を強化する製品及びサービスを介する場合を含め，既存技術の処理能力の規模を拡大すること，構成国内の能力拠点をネットワーク化すること，及び，それらの処理能力が公的部門と産業界の需要に対応することを確実にすること。

Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.

3. 構成国を横断して，実効的で最新のサイバーセキュリティと信頼のソリューションの広範な配置を確保すること。そのような配置は，その設計からその商業化まで，製品のセキュリティと安全を強化することを含める。

Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.

4. 例えば，サイバーセキュリティ技能の計画を揃えることにより，それらの計画を個々の部門毎の需要に適応させることにより，そして，的を絞り特化された訓練へのアクセスを促進することにより，ジェンダーバランスを考慮に入れた上でのサイバーセキュリティ上の技能格差を解消することの支援。

Support closing the cybersecurity skills gap, taking into account gender balance by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.

5. 行政機関の間の相互補助に対する支援及び欧州連合レベルの信頼できるマネージドセキュリティサービスプロバイダのリザーブの設置を含め，国境を越えるサイバーセキュリティサービスの配置を介して，大きなサイバーセキュリティインシデント及び大規模なサイバーセキュリティインシデントの対応準備及びそれに対する対応における構成国間の結束を向上させること。」；

Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents and large-scale cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted managed security service providers at Union level.’;

(2) 別紙 II において，「個別対象 3－サイバーセキュリティ及び信頼」は，以下のとおりに置き換えられる：
in Annex II, the section 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:

「**個別対象 3－サイバーセキュリティ及び信頼**

Specific Objective 3 – **Cybersecurity and Trust**

3.1. 欧州サイバーセキュリティ警報システムの過程におけるものを含め，共同調達されたサイバーセキュリティのインフラもしくはツールまたはその両方の数

The number of cybersecurity infrastructure, or tools, or both jointly procured including in the context of the European Cybersecurity Alert System

3.2. 欧州サイバーセキュリティファシリティへのアクセスを得ている利用者及び利用者コミュニティの数

The number of users and user communities getting access to European cybersecurity facilities

3.3. サイバーセキュリティ緊急メカニズムの下におけるサイバーセキュリティインシデントに対する準備態勢及びそれに対する対応を支援する活動の数」。

The number of actions supporting preparedness for and response to cybersecurity incidents under the Cybersecurity Emergency Mechanism'.

2026 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 11 巻第 1 号（通巻第 72 号）
The Law and Information Magazine vol.11 no.1 (consecutive no.72)

2026 年 1 月 14 日発行
2026 年 2 月 25 日誤記等訂正版発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）