規則(EU) 2019/881 （Cybersecurity Act）

［参考訳・改訂版］

2019 年 9 月 16 日
明治大学法学部教授
夏 井 高 人

＊＊＊

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.15-69）のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Eur-lex の Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[2019 年 6 月 8 日確認]

規則(EU) 2019/881（Cybersecurity Act）は、ENISA（the European Union Agency for Cybersecurity）に関する EU の基本法令であった規則(EU) No 526/2013（OJ L 165, 18.6.2013, p. 41–58）を全面改正し、同規則と置き換わる ENISA の新基本法令である。

規則(EU) 2019/881（Cybersecurity Act）は、2019 年 6 月 27 日から適用（施行）される。

規則(EU) 2019/881（Cybersecurity Act）は、前文、条文及び別紙の 3 つの部分で構成されている。この参考訳においては、規則(EU) 2019/881（Cybersecurity Act）の前文、条文及び別紙の全文を訳出した。

この参考訳においては、原則として直訳とした。直訳のままでは日本語として意味の通らない部分や非常にわかりにくい部分に関しては、やむを得ず意訳とした。

この参考訳は、あくまでも規則(EU) 2019/881（Cybersecurity Act）の私的な和訳であり、関連分野の研究者のための参考として提供するものである。確定訳ではなく、現時点における検討結果の一部を示すものであるので、今後、必要に応じて改訂・修正が加えられる可能性がある。誤記等があるときは、随時、法と情報雑誌上においてその正誤を公表する。

規則(EU) 2019/881（Cybersecurity Act）の最初の版の参考訳は、法と情報雑誌 4 巻 7 号（2019 年 7 月）に掲載して公表した。ところが、参考訳の Web 公開の要請が余りにも多く、そのためには可能な限り完全に近い訳文とするための見直し作業を要すると判断した。しかし、筆者一人の力だけでは誤記や誤訳等の完全な発見と訳文の見直しを実施することは不可能なことであり、かつ、諸般の事情により継続集中して翻訳作業等に打ち込むことが物理的に不可能な状況となったため、唐亀侑久氏（株式会社ラック）の助力を得て、誤記、誤訳及び訳漏れの精査を実施した。そして、他の法令等の翻訳作業を全て停止または放棄し、2019 年 8 月及び 9 月に予定していた法と情報雑誌の発行を見送ることとした上で、更に時間をかけて見直しと修正の作業を実施した。

この改訂版は、以上のような見直し作業を経て作成されたものではあるが、この改訂版もまた私訳を公開しているものであって、確定版ではなく、公式訳でもない。また、この参考訳・改訂版中においては、日本国政府の関係各省庁等が通常使用している訳語とは別の訳語を意図的に維持している部分もある。

他の翻訳作業等に深刻な支障が生ずるため、今後、この参考訳・改訂版を更に見直しする予定はない。この参考訳・改訂版を使用する者は、各自の自己責任において訳文を精査し、各人の考えに従って調整・補充等を実施した上で使用すべきである。

この参考訳に訳注はない。脚注は、全て原注である。

規則(EU) 2019/881（Cybersecurity Act）は、欧州連合の情報セキュリティのための基本業務を遂行するための基本的な役割を ENISA に対して与えている。ENISA が担うべき EU のネットワーク及び情報のセキュリティそれ自体に関する基本法令は、NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1-30）である（規則(EU) 2019/881（Cybersecurity Act）の前文(15)、前文(24)、前文(25)、前文(28)、前文(29)、前文(31)、前文(35)、前文(39)、前文(46)、前文(65)、前文(92)、第 5 条ないし第 9 条参照）。

NIS 指令(EU) 2016/1148 に関しては、夏井高人「NIS 指令(EU)2016/1148 の構造と機能」法律論叢 91 巻 6 号 243～291 頁(2019)において詳論したとおりである。

規則(EU) 2019/881（Cybersecurity Act）は、形式的には ENISA の権限と職務を定める法令である。しかし、他の関連法令がそうであるのと同じように、EU の情報セキュリティに関する法令は、それだけで孤立して存在しているわけではない。逆に、情報セキュリティの分野、個人データ保護の分野及び電子通信の分野の各法令は、相互に密接な関係にある。それゆえ、規則(EU) 2019/881（Cybersecurity Act）を正確に理解するためには、情報セキュリティと直接の関係をもつ NIS 指令(EU) 2016/1148 だけではなく、個人データ保護及び電子通信と関連する主要な法令全部に精通していなければならず、その逆もまた真である。それゆえ、例えば、EU の個人データ保護法制のみの法学専門家や電子通信法制のみの法学専門家が成立することはあり得ない。関連分野全体に精通していなければならないのである（規則(EU) 2019/881（Cybersecurity Act）の前文(15)参照）。

加えて、ENISA 以外の EU の関連機関（Europol、Eurojust、EPPO、OLAF 等）及び構成国の関連行政機関の間で行われる関連通信及びそのための通信インフラ（SIS 等）を規律する様々な法令に関する基本的な知識・理解も必須である。そのような通信関連法令には、指令(EU) 2018/1972（OJ L 321, 17.12.2018, p.36-214）が含まれる。

以上のような EU の法令間の相互関係に関しては、夏井高人「情報社会の素描－EU の関連法令を中心として－(1)」法律論叢 90 巻 4・5 号 135～181 頁 (2018)の中で詳論したとおりである。また、NIS 指令(EU) 2016/1148 に関しては、夏井高人「NIS 指令(EU) 2016/1148 の構造と機能」法律論叢 91 巻 6 号 243～291 頁(2019)において詳論したとおりである。

規則(EU) 2019/881（Cybersecurity Act）の前文(15)にある「Cybersecurity Strategy of the European Union」とは、欧州委員会及び欧州連合対外関係安全保障政策上級代表の共同通知「Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace」（JOIN(2013) 1 final）のことを指す。

規則(EU) 2019/881（Cybersecurity Act）の前文(15)にある「European Agenda on Security」とは、欧州委員会通知「European Agenda on Security」（COM(2015) 185 final）のことを指す。

規則(EU) 2019/881（Cybersecurity Act）の前文(26)にある「European Digital Competence Framework for Citizens」に関する情報は、下記のサイト上で提供されている。

European Digital Competence Framework for Citizens (DigComp)
https://ec.europa.eu/social/main.jsp?catId=1315&langId=en
[2019 年 6 月 9 日確認]

EU 全体の危機管理体制の中における ENISA の役割を的確に把握するためには、その危機管理体制全体の概要を理解することが必須の前提となる。そのような EU の危機管理体制全体の概要を示す公式文書として、委員会勧告(EU) 2017/1584（OJ L 239, 19.9.2017, p.36-58）があり、この分野における学術研究及び実務において必読の文書の 1 つとなっている（規則(EU) 2019/881（Cybersecurity Act）の前文(32)及び前文(34)参照）。

前文(40)の中にある委員会通知とは、「Digital Education Action Plan」（COM(2018) 22 final）のことを指す。ただし、その内容を正確に理解するためには、この委員会通知に添付されている委員会スタッフ作業文書「Evaluation of the EU Strategy on adaptation to climate change」（SWD(2018) 461 final）も併せて精読する必要性がある。

ENISA によるサイバーセキュリティ上の業務遂行は、当然のことながら、個人データの処理を含む場合が多々あり得る。そのような場合において、規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39-98）及び一般データ保護規則(EU) 2016/679（GDPR）（OJ L 119, 4.5.2016, p.1-88）が基本法令として適用されるが（規則(EU) 2019/881（Cybersecurity Act）の前文(63)、前文(74)参照）、それらの規則以外にも多数の個人データ保護法令が存在する。それゆえ、特に、複合的な問題に関し、EU のどの個人データ保護法令のどの条項が適用されるべきかについては、法解釈上の重要な検討課題の 1 つである。

そのような種類の問題を解決するため、そして、その適正な運用を確保するため、EDPS を含め、EU 及び構成国の個人データ保護監督機関との協議と合意が非常に大きな重要性をもっている（規則(EU) 2019/881（Cybersecurity Act）の前文(44)、前文(62)参照）。特に、犯罪捜査と関連する個人データに関しては、データ主体のアクセスの権利が基本的に制限されており、原則として、監督機関を介した間接アクセスのみが認められることから、その場合における監督機関の個人データ保護権限の実効性等に関して慎重な検討を要する。

これらの諸点に関しては、EU の多数の関連法令のより正確な理解を含め、今後、更に調査研究が深められなければならない。

規則(EU) 2019/881（Cybersecurity Act）の法案である Cybersecurity Act 提案 COM(2017) 477 の段階においては、「ICT products and services（ICT products and ICT services）」のセキュリティの重要性が示されていたが、最終的に採択された規則(EU) 2019/881（Cybersecurity Act）においては、「ICT processes」が加えられ、「ICT products, ICT services and ICT processes」と表現が改められている。

この「ICT processes」とは、ICT が通信ネットワーク上で実行・処理される流れそれ自体のことを指すものと考えられ、第 5 世代通信技術（5G）を基礎とする IoT における非常に高度なセキュリティを意識したものである（規則(EU) 2019/881（Cybersecurity Act）の前文(65)ないし前文(76)参照）。

一般に、IoT にあっては、それを構成する技術及び IoT を介して提供されるサービスだけではなく、プロセスとしての IoT それ自体の防護を考えなければならない。例えば、個別の機器のハッキングや虚偽情報の流布のようなサイバー攻撃だけではなく、IoT システム全体の包括的な攪乱または破壊やハイジャックのようなサイバー攻撃が想定される。

そして、あくまでも一般論としては、IoT が社会に普及すればするほど、公法と私法の境界または官と民の境界が消滅し、全体として統合された総動員型の包括的防護が不可欠になるという社会力学的関係が成立することになる。そこにおいては、国防、安全保障、警察活動及び市民の個別的な自己防衛との間の境界も消滅し、社会内のほぼ全ての部面において国家統制が貫徹されることになるであろう。このような変化は、IoT とその防御にとって本質的または本源的なものであるので、そのような意味での国家統制を回避するための合理的な方法が存在し得ない。以上を前提とした上で、IoT があまねく普及した社会におけるそのような方向性が「民主主義」という基本理念と整合性を保つことが可能であるか否かは、現代の政治哲学及び法哲学における最大の検討課題の 1 つである。

規則(EU) 2019/881（Cybersecurity Act）の前文中においては、全体として、ICT 製品、ICT サービス及び ICT プロセスの安全性に関し、何らかの認証が行われているとしても、完全な認証なるものが存在し得ない以上、その認証があるという事実のみでそれらの ICT 製品、ICT サービス及び ICT プロセスの安全性が保障されることにはならないという趣旨のことが強調されている。そこでは、基本的に、利用者自身の認識向上の必要性も強調されているが、それは、古典的な「買主注意せよ（Augen auf, Kauf ist Kauf）」の原則への回帰現象の一部としても理解可能であるかもしれない。一般に、ある情報またはデータの真正性及び正確性についても認証による保証が求められることがあるが、その場合でも基本的には同じである。

それらのことを踏まえた上で、一般に、ある認証を実施する機関・組織の適正性に関する検証が疎かにされている場合、認証制度及びその運用それ自体が社会全体の中における深刻な脆弱性要素となっているという一般原則が常に肯定される。

例えば、一般に、認証に用いられるシステム及びデータそれ自体の健全性が持続的に検証・監査されていない場合、当該システム及びデータのマネジメントが要求水準を満たすものではない場合には、その認証の価値はゼロである。当該システムの構成要素である部品（IC チップ）やソフトウェアの中に不法な機能が最初から含まれている場合において、そのような不法な機能をもつ部品やソフトウェアの存否に関する検証及び監視が徹底的に行われていない場合等には、そうである。そのような致命的な状況が発生することを避けるため、一般的には、異なる側面からの多重的な常時監視が導入されることがある。

また、当該システムを運営する機関・組織それ自体またはその職員等が仮想敵国のスパイまたは手先であるような場合には、「笑えない冗談」のような致命的な状況が現出し得ることになる。それゆえ、当該システムの重要性または機密性の性質及び程度に比例して、相応のクリアランスが必然的に求められることになる。

加えて、当該運営主体である機関・組織それ自体が、国際条約または国内法によって禁止されている行為を実施する機関・組織である場合、そのこと自体で認証それ自体の価値が損なわれることはな

いにしても、刑事訴訟の基本原則の 1 つである「毒樹の果実」の理論を応用し、そのような機関・組織による認証結果を用いることもまた違法行為になると判断し、または、その認証結果は、例外なく、全て無効であると判断すべき場合があり得る。そのような認証結果の無効化の可能性及び必要性は、規則(EU) 2019/881（Cybersecurity Act）及び委員会勧告(EU) 2017/1584 においても当然の前提とするところである。

それゆえ、あくまでも一般論としては、そのような文脈が妥当し得る全てのプロセスにおいて、相互監視が必要となる。トップダウンだけでは足りない。なぜならば、認証制度全体の要となっている認証機関が「悪の根源」であることがあり得るからであり、また、その認証機関を監督する行政機関等も当該認証機関と表裏一体の関係になっていることがあり得るからである。

規則(EU) 2019/881（Cybersecurity Act）の前文(66)の中にある 2016 年の委員会通知とは、2016 年 7 月 5 日の委員会通知「Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry」（COM(2016) 410 final）のことを指す。同前文(66)の中にある 2017 年の委員会通知とは、2017 年 5 月 10 日の委員会通知「the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All」（COM(2017) 228 final）のことを指す。いずれの委員会通知も、この分野において必読の政策文書の 1 つである。

セキュリティ認証のための証明書及び宣言書等の真正性の証明に関しては、「eIDAS」と略称される電子識別規則 (EU) No 910/2014（OJ L 257, 28.8.2014, p.73-114）が全面的に適用される。規則(EU) 2019/881（Cybersecurity Act）の実際の運用においては、電子識別規則 (EU) No 910/2014 の遵守を常に念頭に置かなければならないし、eIDAS を遵守する真正性の証明がない場合には、セキュリティの保証における互換性も確保できない。

それゆえ、規則(EU) 2019/881（Cybersecurity Act）を正確に理解するためには、電子識別規則 (EU) No 910/2014 も併せて精読・理解しなければならない。

（この参考訳を作成するに際し考慮した事項）

「connectivity」は、通常は、ある通信システムと別の通信システムとの間で齟齬なく通信が確立され得ることを意味する。しかし、規則(EU) 2019/881（Cybersecurity Act）においては、ある機器もしくはサービスまたは経済活動等がインターネットのような情報通信ネットワークに接続され得ることを意味するものとして、この語が用いられている。

例えば、IoT のために用いられる Cyber-physical Objects は、それ自体としては、IC チップとセンサーを組み合わせた機器の一種に過ぎないが、無線または有線により相互に自動接続する機能や自動的にネットワークを構築する機能をもっており、そのような自動的なネットワーク構築を可能とする機能をもっているという点が、特定の IoT のシステム全体の中において、それらの Cyber-physical Objects が全体としての Cyber-physical System を組成する細胞的な構成要素となるための本質的部分を構成している。

そこで、この参考訳においては、原則として、「connectivity」を「ネット接続性」と訳すことにした。

「policy」は、「law」と対比して述べられるときは「政策」を意味する。しかし、情報セキュリティのためのマネジメントシステムの一部として「policy」が用いられるときは、当該マネジメントシステムにおける「基

本方針」のことを意味する。
そこで、この参考訳においては、とりあえず、文脈により、「policy」を「政策」または「基本方針」と訳し分けることにした。ただし、この点に関しては、更に詳細な検討を要する。

「cyber-hygiene」に関しては、様々な訳語が提案されている。
この参考訳においては、とりあえず、「cyber-hygiene」を「サイバー衛生」と訳すことにしたが、より適切な訳語が他に存在する場合には、それによるべきである。

「peer review」と「peer-assessment」は、どちらも、制度の相互的な自己評価及び見直しのことを意味するものと解される。ただ、規則(EU) 2019/881（Cybersecurity Act）においては、構成国の制度と関係することを示す場合には「peer review」を用い、EU の欧州サイバーセキュリティ認証制度の構成国による運用と関係することを示す場合には「peer-assessment」を用いているようである。
以上のような明示の相違が存在することを理解した上で、この参考訳においては、意味として均等であることを重視し、「peer review」及び「peer-assessment」をいずれも「相互評価」と訳すことにした。

規則(EU) 2019/881（Cybersecurity Act）の第 15 条第 1 項(q)の「working arrangements」は、「practical arrangements」の誤りではないかと疑われるが、原文のまま訳すことにした。

機密情報の取扱いに関する規則(EU) 2019/881（Cybersecurity Act）の第 27 条第 4 項第 2 文にある「In that case ENISA」は「In that case, the Management Board」の誤りではないかと考えられるが、明示せずに「Executive Board」による採択で足りるという趣旨であるかもしれず、あるいは、ENISA の意思決定機関が「Management Board」であることから、当然解釈として、採択するのは「Management Board」であるとの趣旨とも解され、必ずしも判然としない。規則(EU) 2019/881（Cybersecurity Act）の前文及び他の条項の中においてもその趣旨を明確に示す部分はない。
以上のような問題があるが、この参考訳においては、原文のまま訳すことにした。

規則(EU) 2019/881（Cybersecurity Act）の脚注番号に関しては、原文に合わせ、頁毎のふり直しではなく、連続番号とした。この参考訳の脚注番号は、原文の脚注番号と一致している。

以上のほかは、後掲 Cybersecurity Act 提案 COM(2017) 477 の参考訳、後掲 ENISA 規則(EU) No 526/2013 の参考訳、後掲委員会勧告(EU) 2017/1584 の参考訳、後掲規則(EU) 2018/1725 の参考訳の各冒頭部分で述べたとおりである。

（訳出済みの関連法令等及び参考文献）

Cybersecurity Act 提案 COM(2017) 477 の参考訳は、法と情報雑誌 4 巻 1 号 1～81 頁にある。ENISA 規則(EU) No 526/2013 の参考訳は、法と情報雑誌 3 巻 7 号 263～292 頁にある。NIS 指令(EU) 2016/1148 の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 120～163 頁にある。指令(EU) 2015/1535 の参考訳は、法と情報雑誌 3 巻 7 号 1～20 頁にある。
規則(EU) 2018/1241 による改正後の Europol 規則(EU) 2016/794 の参考訳は、法と情報雑誌 4 巻 4

号 8～68 頁にある。Eurojust 規則(EU) 2018/1727 の参考訳は、法と情報雑誌 4 巻 5 号 1～60 頁にある。EPPO 理事会規則(EU) 2017/1939 の参考訳は、法と情報雑誌 3 巻 1 号 1～91 頁にある。

一般データ保護規則(EU) 2016/679（GDPR）の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU) 2018/1725 の参考訳は、法と情報雑誌 4 巻 1 号 1～81 頁にある。規則(EC) No 45/2001 の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 111～146 頁にある。e プライバシー指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。

電子識別規則 (EU) No 910/2014 の参考訳は、法と情報雑誌 2 巻 10 号 147～196 頁にある。欧州電子通信法指令(EU) 2018/1972 の参考訳は、法と情報雑誌 4 巻 2 号 1～212 頁にある。指令 98/48/EC の参考訳は、法と情報雑誌 3 巻 7 号 51～66 頁にある。指令 98/34/EC の参考訳は、法と情報雑誌 3 巻 7 号 21～39 頁にある。指令 98/48/EC による一部改正後の指令 98/34/EC の参考訳は、法と情報雑誌 3 巻 7 号 67～75 頁にある。理事会決定 87/95/EEC の参考訳は、法と情報雑誌 3 巻 11 号 115～126 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。

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。

この参考訳を作成するに際しては、上記各参考訳の冒頭部分に掲記した各参考文献のほか、小林良樹『インテリジェンスの基礎理論（第 2 版）』（立花書房、2014）、国立研究開発法人科学技術振興機構研究開発戦略センター「科学技術・イノベーション動向報告～EU 編～（2015 年度版）」（2016 年 3 月）、徳田昭雄「EU におけるオープン・イノベーション政策の新しい展開－共同技術イニシアティブ ARTEMIS の事例－」多国籍企業研究 4 号 99～118 頁 (2011)、Jason Staggs & Sujeet Shenoi (Eds.), Critical Infrastructure Protection XII, Springer (2018)、Henry Prunckun (Ed.), Cyber Weaponry: Issues and Implications of Digital Arms, Springer (2019)、Babak Akhgar & Ben Brewster (Eds.), Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities, Springer (2016)、Frances Cleary & Massimo Felici (Eds.), Cyber Security and Privacy: 4th Cyber Security and Privacy Innovation Forum, CSP Innovation Forum 2015, Brussels, Belgium April 28-29, 2015, Revised Selected Papers, Springer (2015)、Chong Li & Meikang Qiu, Reinforcement Learning for Cyber-Physical Systems: with Cybersecurity Case Studies, CRC Press (2019)、Song Guo & Deze Zeng (Eds.), Cyber-Physical Systems: Architecture, Security and Application, Springer (2018)、ENISA, Review of Cyber Hygiene practices, December 2016 を参考にした。

＊＊＊

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（Cybersecurity 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、及び、とりわけ、その第 114 条に鑑み、
欧州委員会からの提案に鑑み、
構成国の議会に立法案を送付した後、
欧州経済社会委員会の意見書に鑑み[1]、
地域委員会の意見書に鑑み[2]、
通常の立法手続に従って審議し[3]、
以下のとおりであるので、この規則を採択する。

(1) ネットワーク及び情報システム並びに電気通信ネットワーク及びサービスは、社会にとって重要な役割を演じており、経済成長のバックボーンとなってきた。情報通信技術（ICT）は、日々の社会活動を支援する複雑なシステムを支え、医療、エネルギー、金融及び輸送のような重要な諸部門において動いている我々の経済を維持し、そして、とりわけ、域内市場の稼働を支えている。

(2) 欧州連合全域にわたる市民、組織及び企業によるネットワーク及び情報システムの利用は、現在、広く普及している。デジタル化及びネット接続性は、不断にその数を増加させ続けている製品及びサービスの中心的な機能となり続けており、また、次の 10 年間において、モノのインターネット（IoT）の登場と共に、極めて多数の接続されたデジタル機器が EU 全域にわたり配置されるものと予想されている。インターネットに接続される機器の数が増加し続ける一方、安全性及び回復力がバイデザインで十分に構築されているわけではなく、不十分なサイバーセキュリティをもたらしている。この文脈において、認証の利用が限定的なものであることは、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ機能に関し、個人、組織及び企業のユーザが不十分な情報しかもっていないということを導いており、そのことは、デジタルソリューションへの信頼を損ねている。ネットワーク及び情報システムは、我々の全ての側面における生活の支援を可能とするものであり、欧州連合の経済成長を牽引している。それらは、デジタル単一市場を達成するための礎石である。

(3) デジタル化及びネット接続性の増加は、サイバーセキュリティ上のリスクを増加させており、サイバー脅威に対して社会全体をより脆弱なものとし、子どものような脆弱な人々を含め、個人が直面する危険を悪化させている。それらのリスクを削減するため、（委員会勧告 2003/361/EC[4]に定義する中小企業(SME)から重要インフラの運営者に至るまで）市民、組織及び企業によって利用されるネットワーク及び情報システム、通信ネットワーク、デジタル製品、デジタルサービス及びデ

[1] OJ C 227, 28.6.2018, p.86.
[2] OJ C 176, 23.5.2018, p.29.
[3] 欧州議会の 2019 年 3 月 12 日付け意見書（官報未登載）及び理事会の 2019 年 4 月 9 日付け決定
[4] マイクロ企業及び中小企業の定義に関する 2003 年 5 月 6 日の委員会勧告（(OJ L 124, 20.5.2003, p.36）

ジタル機器をサイバー脅威に対してより良く防護するため、欧州連合内のサイバーセキュリティを向上させるために必要となる全ての行動が執られる必要性がある。

(4) 欧州議会及び理事会の規則(EU) No 526/2013[5]によって設置されたものとしての欧州連合ネットワーク情報セキュリティ局（ENISA）は、関連情報を公衆が利用できるようにすることによって、欧州連合内のサイバーセキュリティ産業の発展、とりわけ、中小企業及びスタートアップの発展に貢献している。ENISA は、欧州連合の外からのサイバーセキュリティ製品及びサービスへの依存を削減することに貢献するため、並びに、欧州連合内の供給網を強化するため、大学及び研究機関との間の緊密な協力に努めなければならない。

(5) サイバー攻撃が増加しており、サイバー脅威及びサイバー攻撃に対してより脆弱なものである接続された経済と社会は、より強力な防衛を要求している。しかしながら、サイバー攻撃がしばしば国境を越えるものであるのに、サイバーセキュリティ機関及び法執行機関の職務権限とそれらによる政策上の対応は、ほとんど全て国内的なものである。大規模インシデントは、欧州連合全域にわたり、重要サービスの提供を破壊し得る。このことは、欧州の結束と共助のための専用の政策及びより広範な法律文書を基礎とする欧州連合レベルの効果的かつ調整された対応と危機管理を要求する。更に、欧州連合の信頼性のあるデータを基礎とし、並びに、欧州連合レベル及びグローバルレベルの将来の発展、検討課題及び脅威の組織的な予測を基礎として、欧州連合内のサイバーセキュリティ及び回復力の状態を継続的に評価することは、政策決定者、産業界及び利用者にとって、重要なことである。

(6) 欧州連合が直面するサイバーセキュリティ上の検討課題が増加していることに照らし、従前の欧州連合の活動を基礎とし得るものであり、かつ、諸目標の相互強化を育成し得るような、包括的なセットの措置を求める需要が存在する。それらの諸目標は、構成国及び企業の能力及び準備を更に増加させること、並びに、構成国と欧州連合の機関、組織、事務局及び部局を横断する情報共有及び調整を向上させることを含む。更に、全ての規模のサイバー脅威に対応する国内能力を維持すること、及び、それを更に拡大することの重要性を考慮に入れつつ、サイバー脅威の国境を越える性質に鑑み、とりわけ、国境を越える大規模なインシデント及び危機の場合において、構成国の行動を補完し得る欧州連合レベルの能力を増加させる必要性がある。

(7) サイバーセキュリティ上の問題に関する市民、組織及び企業の意識を向上させるための追加的な努力も必要である。更に、インシデントが、デジタルサービスプロバイダとデジタル単一市場への信頼を損ねるものであることに鑑み、信頼は、高度なサイバーセキュリティ認証によっても ICT 製品、ICT サービスまたは ICT プロセスが完全に安全なものであることを保証できないものとせざるを得ない ICT 製品、ICT サービスまたは ICT プロセスの安全性のレベルに関する情報を透明性のある態様によって提供することにより、更に強化されなければならない。信頼の向上は、サイバーセキュリティ上の要求事項及び国内市場及び諸部門を横断する評価基準を定める欧州連合全域にわたる認証によって促進され得る。

(8) サイバーセキュリティは、単に技術のみと関連する問題ではなく、人間の行動が均等に重要な場合の問題でもある。それゆえ、「サイバー衛生」、すなわち、市民、組織及び企業によって実装され、かつ、実施されると、サイバー脅威のリスクに彼らが晒されることをミニマム化する単純で日常的な手段が強力に推進されなければならない。

---

[5] 欧州連合ネットワーク情報セキュリティ局（ENISA）に関する及び規則(EC) No 460/2004 を廃止する欧州議会及び理事会の 2013 年 5 月 21 日の規則(EU) No 526/2013（OJ L 165, 18.6.2013, p.41）

(9) 欧州連合のサイバーセキュリティの構造を強化する目的のために、国境を越えるインシデントを含め、サイバー脅威に対して構成国が包括的に対応するための能力を維持し、発展させることが重要である。

(10) 企業及び個々の消費者は、彼らの ICT 製品、ICT サービスまたは ICT プロセスの安全性が認証される保証のレベルに関する正確な情報をもつべきである。それと同時に、全面的にサイバー安全性のある ICT 製品及び ICT サービスなど存在しないので、サイバー衛生の基本原則が推進されなければならず、かつ、優先されなければならない。IoT 機器の可用性が増加していることに鑑み、ICT 製品、ICT サービス及び ICT プロセスの安全性への信頼を強化するために民間部門がとり得る一定幅の任意の手段が存在する。

(11) 現代の ICT 製品及び ICT システムは、しばしば、統合化されており、かつ、ソフトウェアモジュール、ライブラリまたはアプリケーションプログラムインタフェイスのような 1 または複数の第三者の技術及びコンポーネントに依拠している。第三者のコンポーネントの中で発見される脆弱性が ICT 製品、ICT サービス及び ICT プロセスの安全性をも害し得るものであるので、この「依存」として表現される依拠は、付加的なサイバーセキュリティ上のリスクを示し得る。多くの場合において、そのような相互依存関係を識別し、文書化することは、ICT 製品、ICT サービス及び ICT プロセスのエンドユーザが、例えば、利用者のサイバーセキュリティ脆弱性管理及び復旧手順を向上させることによって、彼らのサイバーセキュリティリスクマネジメント活動を向上させることを可能にしている。

(12) ICT 製品、ICT サービスまたは ICT プロセスに関与する組織、製造者またはプロバイダは、設計及び開発の最も早い段階において、サイバー攻撃が予測され、かつ、その攻撃の影響が想定され、かつ、ミニマム化されるような方法（「セキュリティバイデザイン」）で、可能な最も高度な度合いで、それらの製品、サービス及びプロセスの安全性を防護するための措置を実装することが奨励されなければならない。ICT 製品、ICT サービスまたは ICT プロセスのライフタイムを通じて、悪意ある加害行為からの危害のリスクを削減するために恒常的に進化する設計プロセス及び開発プロセスによって、安全性が確保されなければならない。

(13) 事業者、組織及び公的部門は、初めて利用する者が、可能な最も安全な設定によるデフォルトの初期設定を受けることができるようにし（「セキュリティバイデフォルト」）、そのことによって、ICT 製品、ICT サービスまたは ICT プロセスを適切に初期設定しなければならないという利用者の負担を軽減する態様で、事業者、組織及び公的部門によって設計される ICT 製品、ICT サービスまたは ICT プロセスを初期設定すべきである。セキュリティバイデフォルトは、利用者の側において、拡張的な初期設定または特別の技術上の理解または非直観的な行動を要求するものであってはならず、かつ、その実装の際、容易で信頼できるように稼働するものでなければならない。ケースバイケースで、リスク分析及び使いやすさの分析により、そのようなバイデフォルトの設定を実現できないとの結論を導くときは、利用者は、最も安全な設定を選択することが推奨されるべきである。

(14) 欧州議会及び理事会の規則(EC) No 460/2004[6]は、欧州連合内における高度かつ実効的なレベルのネットワーク及び情報セキュリティを確保するという到達目標に貢献する目的、並びに、市民、

[6] 欧州ネットワーク情報セキュリティ局を設置する欧州議会及び理事会の 2004 年 3 月 10 日の規則(EC) No 460/2004（OJ L 77, 13.3.2004, p.1）

消費者、企業及び行政機関の利益のためにネットワーク及び情報セキュリティの文化を発展させるという目的をもって、ENISA を設置した。欧州議会及び理事会の規則(EC) No 1007/2008[7]は、ENISA の任務を 2012 年 3 月まで延長した。欧州議会及び理事会の規則(EC) No 580/2011[8]は、ENISA の任務を 2013 年 9 月 13 日まで更に延長した。規則(EU) No 526/2013 は、ENISA の任務を 2020 年 6 月 19 日まで延長した。

(15) 欧州連合は、サイバーセキュリティを確保し、デジタル技術の信頼を増加させるための重要な手立てを既に講じてきた。2013 年、サイバー脅威及びサイバーリスクに対する欧州連合の政策上の対応をガイドするため、欧州連合のサイバーセキュリティ戦略が採択された。欧州のオンラインの市民をより良く防護するための仕事の中で、2016 年、指令(EU) 2016/1148[9]という形態により、サイバーセキュリティの分野における欧州連合における最初の立法行為が採択された。指令(EU) 2016/1148 は、サイバーセキュリティの分野における国内の能力に関する要件を設け、構成国の間における戦略上及び業務遂行上の協力を拡大するための最初の仕組みを定め、そして、エネルギー、輸送、水道供給、銀行、金融市場インフラ、医療、デジタルインフラ及びデジタルサービスプロバイダ（検索エンジン、クラウドコンピューティングサービス及びオンライン市場）のような、経済及び社会にとって重要な部門を横断するセキュリティ措置及びインシデント通報に関する義務を導入した。

同指令の実装を支援する重要な役割が ENISA に割当てられた。加えて、サイバー犯罪に対抗して実効的に闘うことは、セキュリティに関する欧州アジェンダの中で重要な優先事項の 1 つであり、高いレベルのサイバーセキュリティを達成するという狙い全体に貢献するものである。欧州議会及び理事会の規則(EU) 2016/679[10]並びに欧州議会及び理事会の指令 2002/58/EC[11]及び指令(EU) 2018/1972[12]のような他の法的行為もまた、デジタル単一市場における高いレベルのサイバーセキュリティに貢献する。

(16) 2013 年の欧州連合サイバーセキュリティ戦略の採択及び ENISA の任務の直近の改訂以降、グローバルな環境がより不確実なものとなり、かつ、より安全ではなくなったので、政策の文脈全体が大きく変化した。その変化を背景として、かつ、助言及び専門知識の拠点として、協力及び能力開発の促進者としての ENISA の役割の積極的な発展の過程において、並びに、欧州連合の新たなサイバーセキュリティ政策の枠組み内において、ENISA の評価の間に認識されたように、現在の任務が十分なものではないので、変化したサイバーセキュリティのエコシステムにおける ENISA の役割を定めるため、並びに、急激に変容したサイバー脅威の状況から生じているサイバーセキュリティ上の検討課題に対する欧州連合の対応に効果的に ENISA が貢献することを確

---

7 その期間に関し、欧州ネットワーク情報セキュリティ局を設置する規則(EC) No 460/2004 を改正する欧州議会及び理事会の 2008 年 9 月 24 日の規則(EC) No 1007/2008（OJ L 293, 31.10.2008, p.1）

8 その期間に関し、欧州ネットワーク情報セキュリティ局を設置する規則(EC) No 460/2004 を改正する欧州議会及び理事会の 2011 年 6 月 8 日の規則(EU) No 580/2011（OJ L 165, 24.6.2011, p.3）

9 欧州連合全域にわたるネットワーク及び情報システムの共通の高いレベルの安全性のための措置に関する指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1）

10 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p.1-88).

11 電子通信部門における個人データの処理及びプライバシー保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC（OJ L 201, 31.7.2002, p.37）

12 欧州電子通信法を定める欧州議会及び理事会の 2018 年 12 月 11 日の指令(EU) 2018/1972（OJ L 321, 17.12.2018, p.36）

保するため、ENISA の任務は、見直される必要性がある。

(17) この規則によって設置されるものとしての ENISA は、規則(EU) No 526/2013 によって設置されたものとしての ENISA を承継しなければならない。ENISA は、就中、助言及び専門知識を提供することにより、並びに、欧州連合の情報と知識のセンターとして活動することにより、この規則によって、及び、それ以外のサイバーセキュリティの分野における欧州連合の法的行為によって ENISA に与えられた職務を実施しなければならない。ENISA は、構成国と民間の利害関係者との間のベストプラクティスの交換を促進し、欧州委員会及び構成国に対して政策上の示唆を提供し、サイバーセキュリティ上の事柄と関連する欧州連合の部門別の政策上の取り組みのための拠点として活動し、並びに、構成国間、及び、構成国と欧州連合の機関、組織、事務局及び部局との間の業務遂行上の協力を育成しなければならない。

(18) 国家元首または政府レベルで会合し、構成国の代表者間の一般協定によって行われた決定 2004/97/EC, Euratom[13]の枠組み内において、構成国の代表は、ENISA が、ギリシア政府によって定められるギリシア内の都市にその本拠地をもつことを決定した。ENISA のホスト構成国は、ENISA の円滑かつ効率的な業務遂行のために可能な最善の条件を確保しなければならない。ENISA が適切な場所に置かれること、就中、適切な移動手段と ENISA の職員に同伴する配偶者及び子どものための施設を提供することは、ENISA の職務の適正かつ効率的な遂行のため、職員の採用及び維持確保のため、そして、ネットワーク活動の効率性を拡大するために不可欠なことである。ENISA の運営会議の承認を得た後、ENISA とホスト構成国との間で締結される協定の中で必要な手配が定められなければならない。

(19) 欧州連合が直面しているサイバーセキュリティ上のリスク及び検討課題が増加していることに鑑み、ENISA の拡大された役割及び職務を反映するため、そして、欧州連合のデジタルエコシステムを防護する組織のエコシステムの中における ENISA の重要な立場を反映するため、ENISA に割当てられる資金及び人的資源は、この規則によって ENISA に与えられる職務を、ENISA が実効的に遂行できるように増加されるべきである。

(20) ENISA は、高いレベルの専門知識を開発及び維持しなければならず、また、ENISA の独立性、ENISA が提供する助言の品質、ENISA が伝達する情報の品質、ENISA の業務遂行手続の透明性、ENISA の業務遂行手法の透明性、並びに、ENISA の職務を実施する際におけるその説明責任により、単一市場の信頼及び信用を構築する拠点として業務遂行しなければならない。ENISA は、欧州連合の機関、組織、事務局及び部局並びに構成国と全面的に協力してその職務を実施し、仕事の重複を避け、かつ、その波及効果を向上させつつ、国内の仕事を積極的に支援し、かつ、欧州連合の仕事に積極的に貢献しなければならない。加えて、ENISA は、民間部門の利害関係者及びそれ以外の関連する利害関係者からの入力を基礎とし、それらと協力しなければならない。職務のセットは、ENISA の業務遂行における柔軟性を許容しつつ、ENISA がその目標をどのように達成すべきかを定めるものとすべきである。

(21) 構成国間における業務遂行上の協力に対して適切な支援を提供できるようにするため、ENISA は、その技術上及び人的な能力及び技能を更に強化しなければならない。ENISA は、そのノウハウ及び能力を増加させなければならない。ENISA 及び構成国は、任意に、ENISA に対して国

[13] 欧州連合の一定の事務局及び部局の本拠地の所在地に関し、国家元首または政府レベルで会合し、構成国の代表者間の一般協定によって行われた 2003 年 12 月 13 日の決定 2004/97/EC, Euratom（OJ L 29, 3.2.2004, p.15）

内専門家を派遣し、専門家のプールを構築し、そして、職員を交換するための計画を策定し得る。

(22) サイバーセキュリティの局面における欧州連合の政策及び法律の関連性を拡大するため、並びに、国内レベルにおけるそれらの政策及び法律の実装の一貫性を可能とするため、ENISA は、サイバーセキュリティの分野及びその部門固有の側面において、政策及び法律の策定、改訂及び見直しと関連する欧州連合の全ての事項に関し助言し、意見を提供し、及び、分析することにより欧州委員会を補佐しなければならない。サイバーセキュリティと関連する事項が含まれている場合、ENISA は、欧州連合の部門固有の政策上及び法律上の取り組みのための助言及び専門知識の拠点として行動しなければならない。ENISA は、欧州議会に対し、継続的に、ENISA の活動を通知しなければならない。

(23) オープンインターネットのパブリックコア、すなわち、グルーバルな公共財であるオープンインターネットの主要なプロトコル及びインフラは、インターネット全体の基本的な機能を提供し、かつ、その正常な運用を支えている。ENISA は、重要なプロトコル（特に、DNS、BGP 及び IPv6）、（全てのトップレベルドメインの運用のような）ドメイン名システムの運用並びにルートゾーンの運用を含め、ただし、これらに限定されることなく、オープンインターネットのパブリックコアの安全性及びその機能の安定性を支援しなければならない。

(24) ENISA の基礎となる職務は、関連する法的枠組みの一貫性のある実装、とりわけ、サイバー回復力を増加させるために重要なものである指令(EU) 2016/1148 及びそれ以外のサイバーセキュリティの側面を含む関連法律文書の効果的な実装を促進することである。急速に進化するサイバー脅威の状況に照らし、サイバー回復力を構築するためのより包括的で政策横断的なアプローチによって構成国が支援されなければならないことは、明らかである。

(25) ENISA は、サイバー脅威及びインシデントを防止し、検知し、それに対応するための能力及び準備を構築及び拡大するためのそれらの仕事において、並びに、ネットワーク及び情報システムのセキュリティとの関連において、構成国並びに欧州連合の機関、組織、事務局及び部局を補助しなければならない。とりわけ、ENISA は、コンピュータセキュリティインシデント対応チーム（「CSIRT」）の欧州連合内における高度に共通のレベルの成熟を達成するため、指令(EU) 2016/1148 に定める国内及び欧州連合の CSIRT の発展及び拡大を支援しなければならない。構成国の業務遂行能力と関連して ENISA によって実施される活動は、指令(EU) 2016/1148 に基づく構成国の義務を遵守するために構成国によって執られる行動を積極的に支援するものでなければならず、それゆえ、構成国の活動に取って代わるものであってはならない。

(26) ENISA は、欧州連合レベルにおいて、ネットワーク及び情報システムのセキュリティに関し、並びに、構成国レベルにおいて、要請に応じて、とりわけ、サイバーセキュリティに関し、戦略の策定及びそのアップデートの補佐もしなければならず、また、そのような戦略の伝達を促進し、かつ、それらの戦略の実装の進捗状況を追跡調査しなければならない。ENISA は、公的組織の需要を含め、訓練及び訓練教材の需要に応えるため、並びに、それが適切なときは、広範に、欧州連合及び構成国自身の訓練能力の開発において構成国と欧州連合の機関、組織、事務局及び部局を補助するため、市民のためのデジタル能力枠組みを基礎とする「訓練指導者の訓練」の需要に応えるための貢献も行わなければならない。

(27) ENISA は、サイバーセキュリティの意識向上及び教育の分野において、構成国間における緊密な調整及びベストプラクティスの交換を容易にすることによって、構成国を支援しなければならない。そのような支援は、国内教育連絡部局のネットワークの構築及びサイバーセキュリティ訓練プ

ラットフォームの構築によって構成され得る。国内教育連絡部局のネットワークは、国内連絡官ネットワーク内で運営され得るものであり、かつ、構成国内における将来の調整のための出発点であり得る。

(28) ENISA は、その職務の執行において、就中、構成国による重要サービスの運営者の指定に関し、専門知識、助言を提供することにより、また、ベストプラクティスの交換を容易にすることにより、並びに、リスク及びインシデントと関連する国境を越える依存との関係において、指令(EU) 2016/1148 によって設けられた協力グループを補助しなければならない。

(29) 公的部門及び民間部門の間の協力並びに民間部門内の協力を強化するため、とりわけ、重要インフラの防護を支援するため、ENISA は、利用可能なツール及び手続に関するベストプラクティス及び指針を提供することにより、並びに、情報共有と関連する法的問題に対してどのように対処すべきかに関する指針を提供することにより、例えば、部門別の情報共有分析センターの構築を容易にすることを通じて、とりわけ、指令(EU) 2016/1148 の別紙 II に列挙する部門の部門内情報共有及び部門間情報共有を支援しなければならない。

(30) ICT 製品、ICT サービス及び ICT プロセスにおける脆弱性の潜在的な負の影響が持続的に増加しているので、そのような脆弱性を発見し、それを解消することは、サイバーセキュリティ上のリスク全体の削減において重要な役割を果たす。脆弱な ICT 製品、脆弱な ICT サービス及び脆弱な ICT プロセスの組織、製造者またはプロバイダと、脆弱性を発見するサイバーセキュリティ調査研究コミュニティ及び政府との間において協力することは、ICT 製品、ICT サービス及び ICT プロセスの脆弱性の発見及び解消の両者の比率を大きく増加させることが証明された。調整された脆弱性情報開示は、情報システムの保有者に対して脆弱性が通報され、詳細な脆弱性情報が第三者または公衆に対して開示される前に、その脆弱性を組織が診断し、解消できるようにする構造化された協力のプロセスを定める。そのプロセスは、それらの脆弱性の公表に関し、発見者及び組織との間の調整も定める。調整された脆弱性情報開示基本方針は、サイバーセキュリティを拡大するための構成国の仕事において重要な役割を果たし得る。

(31) ENISA は、情報交換のための共通の手順、言語及び用語を定めることに貢献するため、CSIRT からの、並びに、欧州連合の機関、組織及び部局のためのコンピュータ緊急対応チームの組織化及び業務遂行に関する欧州議会、欧州理事会、欧州連合の理事会、欧州委員会、欧州連合司法裁判所、欧州中央銀行、欧州会計検査院、欧州対外行動局、欧州経済社会委員会、欧州地域委員会及び欧州投資銀行の間の覚書 [14]によって設置された欧州連合の機関、組織及び部局のための機関間コンピュータ緊急対応チーム（CERT-EU）からの任意に共有された国内報告書を集約及び分析しなければならない。その過程において、ENISA は、業務遂行レベルにおける任意の技術情報の交換のための根拠を定める指令(EU) 2016/1148 の枠組み内において、同指令によって設置されたコンピュータセキュリティインシデント対応チームネットワーク（「CSIRT ネットワーク」）に民間部門も含めなければならない。

(32) ENISA は、サイバーセキュリティと関連する国境を越える大規模なインシデント及び危機の場合における欧州連合レベルの対応に貢献しなければならない。この職務は、この規則に定める ENISA の任務、並びに、大規模サイバーセキュリティインシデント及び危機に対する EU の調整された対応に関する委員会勧告(EU) 2017/1584[15]及び 2018 年 6 月 26 日の理事会決議の文脈に

[14] OJ C 12, 13.1.2018, p.1.

[15] 大規模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）

おいて構成国によって合意されるべきアプローチに従って遂行されなければならない。この職務は、関連情報を収集すること、CSIRT ネットワークと技術コミュニティとの間の調整者として行動すること、及び、危機管理に関して責任を負う意思決定者の間の調整者として行動することを含めるものとし得る。更に、ENISA は、1 または複数の構成国から要請があった場合、技術的な観点からのインシデントの対応において、構成国間における関連する技術ソリューションの交換を容易にすることにより、及び、公共通信の中に入力を提供することにより、構成国間の業務遂行上の協力を支援し得る。ENISA は、定期サイバーセキュリティ演習を通じて、そのような協力の手配をテストすることにより、業務上の協力を支援しなければならない。

(33) 業務遂行上の協力の支援において、ENISA は、構造化された協力により、CERT-EU の利用可能な技術上及び業務遂行上の専門知識を利用できるものとしなければならない。そのような構造化された協力は、ENISA の専門知識に基づくものとし得る。それが適切なときは、これら 2 つの組織の間において、そのような協力の実務上の実装を定めるため、及び、活動の重複を避けるための専用の覚書が締結されなければならない。

(34) CSIRT ネットワーク内の業務遂行上の協力を支援する ENISA の職務の遂行において、ENISA は、インシデントを防止し、検知し、及び、それに対応するための構成国の能力をどのようにして向上させるかに関する助言を提供することによる場合、重大な影響もしくは大きな影響をもつインシデントの技術上の取扱いを容易にすることによる場合、または、サイバー脅威及びインシデントが分析されることを確保することによる場合のように、構成国の要請により、構成国に対して支援を提供できるものとしなければならない。ENISA は、とりわけ、構成国間における技術ソリューションの任意の共有を支援することにより、または、構成国によって任意に共有される技術ソリューションのような、結合された技術情報を作成することにより、重大な影響または大きな影響をもつインシデントの技術上の取扱いを容易にしなければならない。勧告(EU) 2017/1584 は、構成国が誠実に協力すること、並びに、構成国の間において、及び、ENISA との間において、不適切な遅滞なく、サイバーセキュリティと関連する大規模なインシデント及び危機情報を共有することを勧告している。そのような情報は、業務遂行上の協力を支援する ENISA の職務の遂行において、ENISA を更に助けるものとなるであろう。

(35) 欧州連合の状況認識を支援するための技術レベルの継続的な協力の一部として、ENISA は、構成国と緊密に協力しつつ、公衆が利用可能な情報、ENISA 自身の分析結果、並びに、構成国の CSIRT、指令(EU) 2016/1148 に定めるネットワーク及び情報システムのセキュリティに関する国内連絡部局（「連絡部局」）、Europol の欧州サイバー犯罪センター（EC3）、CERT-EU、及び、それが適切なときは、欧州対外行動局の欧州連合情報センター（EU INTCEN）によって ENISA との間で共有された報告書を基礎として、インシデント及びサイバー脅威に関する詳細な EU サイバーセキュリティ技術状況報告書を継続的に準備しなければならない。この報告書は、理事会、欧州委員会、欧州連合対外関係安全保障政策上級代表及び CSIRT ネットワークが利用できるようにされなければならない。

(36) 関係する構成国の要請により実施される重大な影響または大きな影響をもつインシデントの事後的な技術調査は、将来のインシデントの防止に焦点を絞るものとすべきである。関係する構成国は、ENISA が事後的な技術調査を効果的に支援できるようにするため、必要な情報及び補助を提供しなければならない。

(37) 構成国は、インシデントと関係のある事業者に対し、それらの事業者の機微の商業情報及び公共

の安全と関連する情報を保護するための権利を妨げることなく、ENISA に対して必要な情報及び補助を提供することによって協力することを招請できる。

(38) サイバーセキュリティの分野における検討課題をより良く理解するため、そして、構成国及び欧州連合の機関、組織、事務局及び部局に対して戦略上の長期的な助言を提供するため、ENISA は、現在のリスク及び生じつつあるリスクを分析する必要がある。その目的のために、ENISA は、構成国、及び、しかるべく、統計機関及びその他の機関と共同して、関連する公衆が利用可能な情報または任意に共有された情報を収集し、先端技術の分析を遂行し、また、ネットワーク及び情報セキュリティ、とりわけ、サイバーセキュリティに対する技術革新の予想される社会的影響、法的影響、経済的影響及び規制上の影響に関するトピックを絞った評価を提供しなければならない。更に、ENISA は、サイバー脅威、脆弱性及びインシデントの分析を遂行することによって、生じつつあるサイバーセキュリティ上のリスクを特定し、インシデントを防止する上で、構成国並びに欧州連合の機関、組織、事務局及び部局を支援しなければならない。

(39) 欧州連合の回復力全体を増加させるため、ENISA は、助言を提供すること、指針を発行すること及びベストプラクティスを交換することにより、とりわけ、指令(EU) 2016/1148 の別紙 II に列挙する部門を支援するため、インフラのサイバーセキュリティの分野における専門知識を開発し、かつ、同指令の別紙 III に列挙するデジタルサービスのプロバイダによって利用される専門知識を開発しなければならない。サイバーセキュリティ上のリスク及び可能な解消策に関するより良く構成された情報へのより容易なアクセスを確保するため、ENISA は、欧州連合の「情報ハブ」、すなわち、欧州連合及び国内の機関、組織、事務局及び部局からもたらされるサイバーセキュリティに関する情報を公衆に提供するワンストップのポータルを開発及び維持しなければならない。サイバーセキュリティ上のリスク及び可能な解消策に関するより良く構成された情報へのアクセスを容易にすることは、構成国が、構成国の能力を強化し、構成国の実務を揃え、そして、サイバー攻撃に対する構成国の回復力を増加させることを助け得るものでもある。

(40) ENISA は、教育を向上させることによる EU 全域の意識向上キャンペーンによる場合を含め、サイバーセキュリティ上のリスクの公衆の意識を向上させること、並びに、市民、組織及び企業を対象として、個人利用者向けのグッドプラクティスに関する指針を提供することに貢献しなければならない。ENISA は、市民、組織及び企業の準備及び回復力の全体的なレベルを向上させるため、重大なインシデントに関する公衆が利用可能な情報を収集及び分析することにより、及び、市民、組織及び企業のための指針をとりまとめて刊行することにより、市民、組織及び企業のレベルにおけるサイバー衛生及びサイバーリテラシを含め、ベストプラクティス及びソリューションを向上させることにも貢献しなければならない。また、ENISA は、例えば、運用指針及び勧告を提供することにより、適用可能な認証制度に関する適切な情報を消費者に対して提供することにも努めなければならない。更に、ENISA は、2018 年 1 月 17 日の委員会通知の中で定められたデジタル教育行動計画に沿って、かつ、構成国並びに欧州連合の機関、組織、事務局及び部局と協力して、個人のより安全なオンライン行動及びデジタルリテラシを向上させるため、フィッシング攻撃、ボットネット、金融詐欺及び銀行詐欺、データ詐欺のインシデントのようなサイバー犯罪を含め、サイバー空間における潜在的な脅威の認識を向上させるため、並びに、基本的な多要素本人確認、パッチあて、暗号化、匿名化及びデータ保護の助言を向上させるため、エンドユーザに向けた継続的なアウトリーチキャンペーン及び公共教育キャンペーンを立案準備しなければならない。

(41) ENISA は、機器の安全性及びサービスの安全な利用に関するエンドユーザの意識を向上させる

上で中心的な役割を果たさなければならず、かつ、欧州連合レベルにおけるセキュリティバイデザイン及びプライバシーバイデザインを促進しなければならない。その目標の遂行において、ENISA は、ベストプラクティス及び経験、特に、学術機関及び IT セキュリティ研究者のベストプラクティス及び専門知識を活用できるようにしなければならない。

(42) サイバーセキュリティ部門において業務遂行する企業及びサイバーセキュリティソリューションの利用者を支援するため、ENISA は、需要サイド及び供給サイドの両者に関し、サイバーセキュリティ市場における主要動向の継続的な分析及び情報提供を遂行することにより、「市場観測所」を開発及び維持しなければならない。

(43) ENISA は、国際機関との間において、かつ、サイバーセキュリティの分野における関連する国際協力の枠組み内において、協力するための欧州連合の仕事に貢献しなければならない。とりわけ、ENISA は、それが適切なときは、OECD、OSCE 及び NATO のような諸機関と協力するために貢献すべきである。そのような貢献は、共同サイバーセキュリティ演習及び共同インシデント対応調整を含め得る。それらの活動は、全ての構成国の安全保障及び国防政策の特性を妨げることなく、欧州連合の一体性の原則、互恵性の原則及び意思決定の自律性の原則を全面的に尊重して実施されなければならない。

(44) ENISA の諸目標を全て達成することを確保するため、ENISA は、CERT-EU、EC3、欧州防衛局（EDA）、欧州グローバルナビゲーション衛星システム局（欧州 GNSS 局）、欧州電子通信規制機関（BEREC）、自由、安全及び法務の領域における欧州大規模 IT システム運用管理局（eu-LISA）、欧州中央銀行（ECB）、欧州銀行監督局（EBA）、欧州データ保護委員会、エネルギー規制当局協力局（ACER）、欧州連合航空安全局（EASA）、並びに、サイバーセキュリティに関与する EU の他の部局を含め、欧州連合の関連する監督機関との間で、並びに、欧州連合の他の職務権限を有する機関、欧州連合の機関、組織、事務局及び部局との間で連絡を取らなければならない。ENISA は、ノウハウ及びベストプラクティスを交換するため、データ保護を取り扱う機関との間においても連絡を取らなければならず、かつ、それらの機関に対して影響をもち得るサイバーセキュリティ上の問題に関する助言を提供しなければならない。国内法執行機関及び欧州連合の法執行機関並びにデータ保護監督機関の各代表は、ENISA 諮問グループに出席できるものとしなければならない。それらの機関の仕事に対して影響をもち得るネットワーク及び情報セキュリティ上の問題に関する法執行機関との間の連絡において、ENISA は、既存の情報伝達経路及び確立されたネットワークを尊重しなければならない。

(45) 関連分野において調査研究に従事する学術機関との間でパートナーシップを構築することができ、かつ、消費者団体及びそれ以外の団体からの入力のための適切な経路が存在しなければならず、それらの入力は、考慮に入れられなければならない。

(46) ENISA は、CSIRT ネットワークの事務局としてのその役割において、指令(EU) 2016/1148 に示すとおり、CSIRT ネットワークの関連職務との関係における業務遂行上の協力において、構成国の CSIRT 及び CERT-EU を支援しなければならない。更に、ENISA は、CSIRT によって管理または防護されており、かつ、複数の CSIRT が関与する、または、関与することがあり得るネットワークまたはインフラのインシデント、攻撃または破壊が発生した場合において、CSIRT ネットワークの標準作業手順を適切に考慮に入れつつ、関連 CSIRT の間の協力を促進し、支援しなければならない。

(47) インシデント対応における欧州連合の準備を増加させるため、ENISA は、継続的に、欧州連合レ

ベルのサイバーセキュリティ演習を立案準備しなければならず、また、構成国の要請に応じて、そのような演習の立案準備の際、構成国並びに欧州連合の機関、組織、事務局及び部局を支援しなければならない。隔年で、技術的要素、運営上の要素または戦略的要素を含む包括的な大規模演習が立案準備されなければならない。加えて、ENISA は、継続的に、インシデント対応における欧州連合の準備を増加させるという同じ目的をもち、より包括的ではない演習を立案準備できるものとすべきである。

(48) ENISA は、この分野における欧州連合の政策を支援するため、サイバーセキュリティ認証に関する ENISA の専門知識を更に開発し、維持しなければならない。ENISA は、既存のベストプラクティスを基礎としなければならず、かつ、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ保証の透明性を増加させるため、そして、それによって、デジタル単一市場への信頼及びデジタル単一市場が競争的であることを強化するため、欧州連合レベルのサイバーセキュリティ認証枠組み（欧州サイバーセキュリティ認証枠組み）の構築及び維持管理に貢献することによる場合を含め、欧州連合内のサイバーセキュリティ認証の普及を促進しなければならない。

(49) 公的部門及び民間部門の両者において、効率的なサイバーセキュリティ政策は、十分に開発されたリスク評価手法を基礎とするものでなければならない。リスク評価手法は、それらの手法を効率的に適用するためにはどのようにすれば良いかに関する共通の実務がないまま、異なるレベルで用いられている。公的部門及び民間部門の組織におけるリスク評価に関するベストプラクティス及びリスク管理ソリューションの相互運用性に関するベストプラクティスを向上させ、発展させることは、欧州連合内のサイバーセキュリティのレベルを向上させることとなる。その目的のために、ENISA は、欧州連合レベルの利害関係間の協力を支援し、かつ、ソフトウェアと共にネットワーク及び情報システムを構成する電子製品、システム、ネットワーク及びサービスのリスク管理及び測定可能な安全性のための欧州標準及び国際標準の策定及び普及と関連する利害関係者の仕事を容易にしなければならない。

(50) 全てのインターネット利用者が、彼ら自身の個人的なサイバーセキュリティを確保するために必要となる手立てを講ずることができるようにするため、ENISA は、構成国、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダに対し、それらの一般的な安全性標準を高めることを推進し、また、そのようにするインセンティブを与えなければならない。とりわけ、ICT 製品、ICT サービスまたは ICT プロセスの製造者及びプロバイダは、全ての必要なアップデートを提供し、サイバーセキュリティ標準に適合しない ICT 製品、ICT サービスまたは ICT プロセスをリコール、廃棄または回収しなければならず、他方で、輸入業者及び流通業者は、それらの事業者が欧州連合の市場に置く ICT 製品、ICT サービス及び ICT プロセスが、適用可能な要求事項を遵守し、かつ、欧州連合の消費者に対してリスクを示さないことを確保しなければならない。

(51) ENISA は、職務権限を有する機関と協力して、域内市場内において提供される ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティのレベルに関する情報を提供できなければならず、また、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダに向けて、それらの製造者及びプロバイダに対し、サイバーセキュリティを含め、ICT 製品、ICT サービス及び ICT プロセスの安全性を向上させることを要求する警告を発さなければならない。

(52) ENISA は、欧州連合の機関、組織、事務局及び部局に対し、並びに、関連する場合、その要請により、構成国に対し、サイバーセキュリティの分野における調査研究の必要性及び優先度に関する助言をするため、現在進行中の調査研究、開発及び技術評価活動、とりわけ、欧州連合の

様々な調査研究の取り組みによって実施される活動を全面的に考慮に入れなければならない。調査研究の必要性及び優先度を判断するため、ENISA は、関係する利用者グループと協議しなければならない。より個別的には、欧州研究会議、欧州イノベーション工科大学院及び欧州連合セキュリティ研究機関との間の協力が構築され得る。

(53) ENISA は、欧州サイバーセキュリティ認証制度を準備する際、標準化機関、とりわけ、欧州標準化機関と継続的に協議しなければならない。

(54) サイバー脅威は、グローバルな問題である。共通の行動規範を定める必要性を含め、サイバーセキュリティの標準、行動規範の採択、国際標準の利用、及び、情報共有を促進すること、ネットワーク及び情報セキュリティの問題の対応における迅速な国際的共働活動を推進すること、並びに、そのような問題に対する共通のグローバルなアプローチを向上させるためのより緊密な国際協力の必要性が存在する。その目的のために、ENISA は、それが適切なときは、欧州連合の機関、組織、事務局及び部局に対して必要な専門知識及び分析を提供することにより、欧州連合の更なる関与、並びに、第三国及び国際機関との間の協力を支援しなければならない。

(55) ENISA は、ENISA の任務の範囲内にある事項に関する助言及び補助を求める構成国並びに欧州連合の機関、組織、事務局及び部局からのアドホックな要請に対し、対応できなければならない。

(56) 各独立部局の活動を合理化し、その職務遂行能力を改善することを目的とし、EU の独立部局に関する機関間作業グループにより 2012 年 7 月に合意された共同声明及び共通アプローチを遵守するため、ENISA の統治に関する一定の基本原則を実装することが賢明であり、かつ、推奨される。この共同声明及び共通アプローチの中にある勧告は、ENISA の業務計画、ENISA の評価、並びに、ENISA の報告及び行政実務の中においても、しかるべく反映されなければならない。

(57) 構成国の代表及び欧州委員会の代表によって構成される運営会議は、この規則に従い、ENISA の業務遂行の一般的な指示を決定し、かつ、ENISA がその職務を実施することを確保しなければならない。運営会議は、予算を策定し、その予算の実行を確認し、適切な財務規則を採択し、ENISA によって行われる決定のための透明性のある作業手続を定め、ENISA の単一業務計画書を採択し、運営会議自身の手続規則を採択し、長官を任命し、並びに、長官の任期の延長及びその終了に関して決定するために必要となる権限を与えられなければならない。

(58) ENISA が適正かつ効率的に稼働するため、欧州委員会及び構成国は、運営会議の構成員に任命される者が適切な専門的知識及び経験をもつことを確保しなければならない。欧州委員会及び構成国は、運営会議の仕事の継続性を確保するため、運営会議におけるそれらそれぞれの代表者の交替を抑制するための努力も行われなければならない。

(59) ENISA が円滑に稼働するためには、ENISA の長官が、その能力及び文書化された行政上及び運営上の技能、並びに、サイバーセキュリティと関連する職務能力及び経験を基礎として任命されることを必要とする。長官の職務は、完全に独立して実施されなければならない。長官は、欧州委員会との事前協議を経た上で、ENISA の年次業務計画の提案書を準備しなければならず、かつ、その業務計画の適正な執行を確保するために必要となる全ての手立てを講じなければならない。長官は、ENISA の年次業務計画の実装を含み、運営会議に送付される年次報告書を準備し、ENISA の収入及び支出の見積書を作成し、かつ、予算を実行しなければならない。更に、長官は、とりわけ、科学的性格、技術的性格、法的性格または社会経済的性格をもつ個別の事項に対処するため、アドホックな作業グループを設置するオプションをもたなければならない。とり

わけ、欧州サイバーセキュリティ認証制度の個別の候補（「制度候補」）の準備との関係において、アドホックな作業グループが設置されることは、重要であると考えられる。長官は、そのアドホックな作業グループの構成員が、ジェンダーバランスを確保し、そして、当の個別の問題により、産業界、利用者、及び、ネットワーク及び情報セキュリティの学術上の専門家を含め、構成国の行政機関、欧州連合の機関、組織、事務局及び部局並びに民間部門の間における適切なバランスを確保することを狙いとし、最高度の専門性に従って選任されることを確保しなければならない。

(60) 執行会議は、運営会議の効果的な稼働に貢献しなければならない。運営会議の決定と関連する準備作業の一部として、執行会議は、関連する情報を仔細に検討し、利用可能なオプションを検討し、かつ、運営会議の関連決定を準備するための助言及び解決策を提示しなければならない。

(61) ENISA は、民間部門、消費者団体及びそれ以外の関連利害関係者との間の継続的な対話を確保するため、諮問組織として、ENISA 諮問グループをもつものとしなければならない。長官の提案に基づき運営会議によって設置される ENISA 諮問グループは、利害関係者と関係する問題に焦点を絞らなければならず、かつ、ENISA の注意を彼らに向けさせなければならない。ENISA 諮問グループは、とりわけ、ENISA の単年度作業計画案に関して協議を受けるものとしなければならない。ENISA 諮問グループの構成、及び、このグループに割当てられる職務は、ENISA の仕事における利害関係者の十分な代表を確保するものでなければならない。

(62) ENISA 及び欧州委員会が関連利害関係者との協議を容易にすることを助けるため、利害関係者サイバーセキュリティ認証グループが設置されなければならない。利害関係者サイバーセキュリティ認証グループは、ICT 製品及び ICT サービスの需要側及び供給側の両者についてバランスのとれた比率により、とりわけ、中小企業、デジタルサービスプロバイダ、欧州の標準化機関及び国際的な標準化機関、国内認定機関、データ保護監督機関、欧州議会及び理事会の規則(EC) No 765/2008[16]による適合性評価機関、並びに、学術団体及び消費者団体を含め、産業界を代表する構成員によって構成される。

(63) ENISA は、利益相反の防止及び管理に関する規則をもたなければならない。ENISA は、欧州議会及び理事会の規則(EC) 1049/2001[17]に定める文書への公衆のアクセスに関する欧州連合の関連条項も適用しなければならない。ENISA による個人データの処理は、欧州議会及び理事会の規則(EU) 2018/1725[18]に服さなければならない。ENISA は、情報の取扱い、とりわけ、機密ではない機微の情報及び欧州連合機密情報（EUCI）の取扱いに関し、欧州連合の機関、組織、事務局及び部局に適用される条項及び国内立法を遵守しなければならない。

(64) ENISA の全面的な自律性及び独立性を保障するため、並びに、予想外の緊急の職務を含め、追加的職務を ENISA が遂行できるようにするため、ENISA は、その収入が主として欧州連合からの拠出及び ENISA の仕事に参加する第三国からの拠出によって賄われる十分かつ自律的な予算を与えられるものとしなければならない。ENISA の増加する職務の全てを遂行し、その目的

16 製品のマーケティングと関連する認定及び市場調査の要件を定め、規則(EEC) No 339/93 を廃止する欧州議会及び理事会の 2008 年 7 月 9 日の規則(EC) No 765/2008（OJ L 218, 13.8.2008, p.30）

17 欧州議会、理事会及び欧州委員会の文書への公衆のアクセスに関する欧州議会及び理事会の 2001 年 5 月 30 日の規則(EC) No 1049/2001（OJ L 145, 31.5.2001, p.43）

18 欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39）

を達成するための十分な能力を ENISA がもつことを確保するために適切な予算であることが最も重要なことである。ENISA の職員の大半は、ENISA の任務の業務遂行上の実装に直接に従事するものとしなければならない。ホスト構成国及びそれ以外の構成国は、ENISA の予算に対して任意の拠出を行うことができるものとすべきである。欧州連合が関係する一般予算の負担となる補助金に関する限り、欧州連合の予算手続が、なお適用されなければならない。更に、欧州会計検査院は、透明性及び説明責任を確保するため、ENISA の会計を監査しなければならない。

(65) サイバーセキュリティ認証は、ICT 製品、ICT サービス及び ICT プロセスの信頼及び安全性を増加させる上で重要な役割を果たす。デジタル単一市場、並びに、とりわけ、データ経済及び IoT は、そのような製品、サービス及びプロセスが一定レベルのサイバーセキュリティを提供しているとの一般公衆の信頼が存在する場合においてのみ、繁栄し得る。ネット接続された自律型自動車、電子医療機器、工場自動制御システム及びスマートグリッドは、認証が既に広範に使用されている部門、または、近未来において使用される見込みのある部門の一例に過ぎない。指令(EU) 2016/1148 によって規律される諸部門もまた、サイバーセキュリティ認証が不可欠なものとなる部門である。

(66) 2016 年の通知「欧州のサイバー回復力システムを強化し、競争力があり革新的なサイバーセキュリティ産業を育成する」の中で、欧州委員会は、高品質であり、適正な価格であり、かつ、相互運用性のあるサイバーセキュリティ製品及びソリューションの必要性の概要を示した。単一市場内における ICT 製品、ICT サービス及び ICT プロセスの供給は、地理的に非常に断片化したままである。これは、欧州のサイバーセキュリティ産業が、広範に、国内政府の需要を基礎として発展してきたことによるものである。加えて、相互運用性のあるソリューション（技術標準）、実務及び欧州連合全域にわたる認証の仕組みが欠けていることは、他のギャップの中でも特に、サイバーセキュリティの分野における単一市場を害し続けている。このことは、国内レベル、欧州連合レベル及びグローバルなレベルにおいて欧州の企業が競争的であることを困難にしている。このことは、個人及び企業がアクセスをもつ実行可能で使い易いサイバーセキュリティ技術の選択肢を狭めるものでもある。同様に、デジタル単一市場戦略の実装の中間見直しに関する 2017 年の通知「全てのためにネット接続されたデジタル単一市場」の中で、欧州委員会は、ネット接続された製品及びシステムの安全性の必要性を強調し、そして、欧州連合内における ICT セキュリティ認証をどのように立案準備するかに関する原則を定める欧州 ICT セキュリティ枠組みを創設することが、インターネットへの信頼を維持し、域内市場の現在の断片化と闘うことを可能とする旨を示唆した。

(67) 現在、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ認証は、限定された範囲内においてのみ、利用されている。その認証が存在している場合、その認証の大半は、構成国レベルで、または、産業主導の制度枠組み内で行われている。その過程において、国内サイバーセキュリティ認証機関が発行した証明書は、原則として、別の構成国内では承認されない。そして、会社は、例えば、国内調達手続に参加するため、その会社が業務遂行する複数の構成国において、その会社の ICT 製品、ICT サービス及び ICT プロセスの認証を受けなければならないかもしれず、そのことは、それによって、その会社の費用負担を追加することとなる。更に、例えば、IoT の分野において、新たな制度が出現しつつあるけれども、サイバーセキュリティ上の横断的な問題に対する一貫性のある全体的なアプローチは存在しないように思われる。既存の制度は、製品の包摂範囲、保証のレベル、実体的な基準及び現実の利用の面において、欧州連合内における相互承認の仕組みを損なう重大な欠点と相違を示している。

(68) 欧州連合内における証明書の相互承認を確保するための幾つかの努力が尽くされてきた。しかしながら、それらは、部分的にしか成功していない。この点に関する最も重要な事例は、現在の上級官吏グループー情報システムセキュリティ（SOG-IS）の相互承認協定（MRA）である。この協定は、セキュリティ認証の分野における協力及び相互承認のための最も重要なモデルを提示するものではあるが、SOG-IS は、幾つかの構成国のみが関与している。域内市場の観点からすると、そのことが、SOG-IS MRA の実効性を狭めてきた。

(69) それゆえ、共通のアプローチを採択することが必要であり、そして、策定されるべき欧州サイバーセキュリティ認証制度のための主たる横断的要求事項を定め、ICT 製品、ICT サービスまたは ICT プロセスの欧州サイバーセキュリティ証明書及び EU 適合性宣言書が全ての構成国において承認され、利用できるようにする欧州サイバーセキュリティ認証枠組みを構築することが必要である。そのようにする際、既存の国内制度及び国際制度を基礎とし、かつ、相互承認制度、とりわけ、SOG-IS を基礎とすること、そして、そのような制度に基づく既存の制度から新たな欧州サイバーセキュリティ認証枠組みに基づく制度への円滑な移行を可能とすることが重要である。欧州サイバーセキュリティ認証枠組みは、二重の目的をもつべきである。第 1 に、それは、欧州サイバーセキュリティ認証制度の下で証明された ICT 製品、ICT サービス及び ICT プロセスへの信頼を増加させることを助けるものでなければならない。第 2 に、それは、国内サイバーセキュリティ認証制度との抵触または重複の累積を避けることを助けるものでなければならず、そして、デジタル単一市場における事業者の業務遂行の費用負担を削減するものでなければならない。欧州サイバーセキュリティ認証制度は、非差別のものでなければならず、かつ、それらの標準が、この点に関する欧州連合の正当な目的を満たすために効果的でない場合、または、不適切な場合を除き、欧州標準または国際標準を基礎とするものでなければならない。

(70) 異なる構成国内の異なる強度レベルを基礎とする「認証ショッピング」を防止するため、欧州サイバーセキュリティ認証枠組みは、全ての構成国において統一的な態様で構築されなければならない。

(71) 欧州サイバーセキュリティ認証制度は、国際レベル及び国内レベルで既に存在しているものを基礎とし、かつ、それが必要なときは、フォーラム及びコンソーシアムからの技術仕様、現在の力点及び弱点の評価と修正からの学習を基礎としなければならない。

(72) 産業界がサイバー脅威を先回りするための柔軟なサイバーセキュリティソリューションが必要であり、また、それゆえ、すぐに陳腐化してしまうリスクを避けるような方法で、全ての認証制度が設計されなければならない。

(73) 欧州委員会は、個別のグループの ICT 製品、ICT サービス及び ICT プロセスに関する欧州サーバーセキュリティ認証制度を採択する権限を与えられなければならない。それらの制度は、国内サイバーセキュリティ認証機関によって実装及び監督されなければならず、かつ、それらの制度の下で発行された証明書は、欧州連合全域を通じて有効であり、かつ、承認されるものでなければならない。産業界またはそれ以外の民間団体によって運営される認証制度は、この規則の適用範囲外にあるものとしなければならない。ただし、そのような制度を運営する組織は、欧州委員会に対し、欧州サイバーセキュリティ認証制度としてそれらを承認するための基礎として、そのような制度を検討することを提案できるものとしなければならない。

(74) この規則の条項は、ICT 製品、ICT サービス及び ICT プロセスの認証に関する個別の規定を定める欧州連合の立法を妨げてはならない。とりわけ、規則(EU) 2016/679 は、管理者及び処理者

による同規則の遵守を説明する目的のために、認証方法並びにデータ保護シール及びデータ保護マークを設けるための条項を定めている。そのような認証方法並びにデータ保護シール及びデータ保護マークは、データ主体が、関連 ICT 製品、ICT サービス及び ICT プロセスのデータ保護のレベルを直ちに評価できるものでなければならない。この規則は、そのような業務遂行が ICT 製品、ICT サービス及び ICT プロセスの中に組み込まれている場合を含め、規則(EU) 2016/679 に基づくデータ処理業務の認証を妨げない。

(75) 欧州サイバーセキュリティ認証制度の目的は、その制度の下で認証を受けた ICT 製品、ICT サービス及び ICT プロセスが、それらの製品、サービス及びプロセスのライフサイクルを通して、それらの製品、サービス及びプロセスによって提供され、または、それらを介して記録保存され、送信されもしくは処理されるデータの可用性、真正性、完全性及び機密性、または、それらの製品、サービス及びプロセスによって提供され、または、それらを介してアクセス可能な関連機能もしくはサービスの可用性、真正性、完全性及び機密性を防護することを狙いとする所定の要求事項に遵守することを確保するものでなければならない。この規則の中において、全ての ICT 製品、ICT サービス及び ICT プロセスと関連するサイバーセキュリティ上の要求事項の詳細を定めることは不可能なことである。ICT 製品、ICT サービス及び ICT プロセス並びにそれらの製品、サービス及びプロセスと関連するサイバーセキュリティの需要は、非常に多様であるので、全ての場合に有効なサイバーセキュリティ上の一般的な要求事項を開発することは、非常に困難である。それゆえ、認証の目的のための広く一般的なサイバーセキュリティの概念を採用する必要性があり、その概念は、欧州サイバーセキュリティ認証制度を設計する際に考慮に入れられる必要のある個別のセットのサイバーセキュリティの目標によって補完されなければならない。個々の ICT 製品、ICT サービス及び ICT プロセスにおいてそのような諸目標が達成されるための手配は、例えば、適切な標準を利用できないときは、標準または技術仕様を指示することにより、欧州委員会によって採択される個々の認証制度のレベルに応じて、別途、詳細に定められるものとしなければならない。

(76) 欧州サイバーセキュリティ認証制度の中で用いられる技術仕様は、欧州議会及び理事会の規則(EU) No 1025/2012[19]の別紙 II に定める要求事項を尊重しなければならない。ただし、保証レベル「高度」を示す欧州サイバーセキュリティ認証制度においてそれらの技術仕様が使用されなければならない適正に正当化される場合においては、それらの要求事項からの幾つかの免脱が考慮される必要性がある。そのような逸脱の理由は、公衆に利用可能なものとされなければならない。

(77) 適合性評価は、ICT 製品、ICT サービスまたは ICT プロセスと関連する個別の要求事項が満たされたか否かを評価するための手続である。その手続は、評価される ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダではない独立の第三者によって実施される。欧州サイバーセキュリティ証明書は、ICT 製品、ICT サービスまたは ICT プロセスの評価を無事に終えた後、発行されなければならない。欧州サイバーセキュリティ証明書は、その評価が適正に実施されたことの確認であると理解されなければならない。保証レベルにより、欧州サイバーセキュリティ認証制度は、その欧州サイバーセキュリティ証明書が民間組織と公的組織のいずれから発行さ

[19] 欧州標準化に関する、並びに、理事会指令 89/686/EEC、理事会指令 93/15/EEC、欧州議会及び理事会の指令 94/9/EC、指令 94/25/EC、指令 95/16/EC、指令 97/23/EC、指令 98/34/EC、指令 2004/22/EC、指令 2007/23/EC、指令 2009/23/EC、指令 2009/105/EC を改正し、理事会決定 87/95/EEC、欧州議会及び理事会の決定 No 1673/2006/EC を廃止する欧州議会及び理事会の 2012 年 10 月 25 日の規則(EU) No 1025/2012（OJ L 316, 14.11.2012, p.12）

れなければならないかを示さなければならない。適合性評価及び認証は、それ自体としては、認証された、ICT 製品、ICT サービス及び ICT プロセスがサイバーセキュアであることを保証できない。それらは、むしろ、ICT 製品、ICT サービス及び ICT プロセスがテストを受けたこと、並びに、それらの ICT 製品、ICT サービス及び ICT プロセスが、例えば、技術標準のような、いずれかにおいて定められた一定のサイバーセキュリティ上の要求事項を遵守していることを証明するための手続上の手法及び技術上の手法である。

(78) 欧州サイバーセキュリティ証明書の利用者による適切な認証及び関連セキュリティ要求事項の選択は、その ICT 製品、ICT サービスまたは ICT プロセスと関係するリスクの評価を基礎としなければならない。従って、保証レベルは、ICT 製品、ICT サービスまたは ICT プロセスの予定された利用と関係するリスクのレベルに見合うものでなければならない。

(79) 欧州サイバーセキュリティ認証制度は、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダの責任のみの下において実施される適合性評価（「自己適合性評価」）を定め得る。そのような場合、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダ自身が、その ICT 製品、ICT サービスまたは ICT プロセスの欧州サイバーセキュリティ認証制度の遵守を確保するために確認を全て実施することで十分なものとしなければならない。自己適合性評価は、単純な設計及び製造の仕組みのような、公衆に対して低度のリスクを示し、複雑性が低度の ICT 製品、ICT サービスまたは ICT プロセスに関し、適切なものであると理解されなければならない。更に、自己適合性評価は、その ICT 製品、ICT サービスまたは ICT プロセスが保証レベルの「基本」に対応する場合に限り、その ICT 製品、ICT サービスまたは ICT プロセスに許容されるものとしなければならない。

(80) 欧州サイバーセキュリティ認証制度は、ICT 製品、ICT サービスまたは ICT プロセスの自己適合性評価と認証の両者であることを許容し得る。そのような場合、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダが評価について責任を負う ICT 製品、ICT サービスまたは ICT プロセスと、第三者によって認証される ICT 製品、ICT サービスまたは ICT プロセスとの間の相違を、消費者またはそれ以外の利用者が明確に理解できる手段を定めなければならない。

(81) 自己適合性評価を実施する ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダは、適合性評価手続の一部として、EU 適合性宣言書を発行し、かつ、それに署名し得るものとしなければならない。EU 適合性宣言書は、特定の ICT 製品、ICT サービスまたは ICT プロセスが、欧州サイバーセキュリティ認証制度の要求事項を遵守していることを述べる文書である。EU 適合性宣言書を発行し、それに署名することにより、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダは、その ICT 製品、ICT サービスまたは ICT プロセスが欧州サイバーセキュリティ認証制度の法律上の要求事項を遵守することについて責任を負う。国内サイバーセキュリティ認証機関及び ENISA に対し、EU 適合性宣言書の副本が提出されなければならない。

(82) ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダは、関連する欧州サイバーセキュリティ認証制度に定める期間内、職務権限を有する国内サイバーセキュリティ認証機関に対し、EU 適合性宣言書、技術文書、並びに、その ICT 製品、ICT サービスまたは ICT プロセスの欧州サイバーセキュリティ認証制度の適合性と関連する他の全ての情報を利用できるようにしなければならない。技術文書は、その制度に基づき適用される要求事項を指示しなければならず、かつ、その自己適合性評価と関連する範囲内において、その ICT 製品、ICT サービスまたは

ICT プロセスの設計、製造及び運用を包摂しなければならない。技術文書は、ICT 製品または ICT サービスが当該制度に基づいて適用される要求事項を遵守しているか否かの評価が可能であるようにまとめられなければならない。

(83) 欧州サイバーセキュリティ認証枠組みの統治は、構成国の関与、及び、利害関係者の適切な関与を考慮に入れ、かつ、欧州サイバーセキュリティ認証制度の企画及び提案、要請、準備、採択及び見直しの間における欧州委員会の役割を定める。

(84) 欧州委員会は、欧州サイバーセキュリティ認証グループ（「ECCG」）及び利害関係者サイバーセキュリティ認証グループの協力を得て、かつ、広範かつオープンなコンサルテーションの後、欧州サイバーセキュリティ認証制度のための欧州連合導入作業計画を準備しなければならず、また、拘束力のない文書の方式により、その計画を公表しなければならない。欧州連合導入作業計画は、産業界、国内機関及び標準化機関が、とりわけ、将来の欧州サイバーセキュリティ認証制度を予め準備することを可能にする戦略文書でなければならない。欧州連合導入作業計画は、個別の基礎に基づく準備に関して欧州委員会が ENISA に対して提示する予定の制度候補を求める要請の多年度概要を含めるものとしなければならない。欧州委員会は、ICT 標準化のための欧州委員会の導入計画及び欧州標準化機関に対する標準化の要請を準備する間、欧州連合導入作業計画を考慮に入れなければならない。新たな技術の急速な導入及び採用、未知のサイバーセキュリティ上のリスクの発生、並びに、立法の発展及び市場の発展に照らし、欧州委員会または ECCG は、ENISA に対し、欧州連合導入作業計画の中に含まれていない制度候補を準備することを要請する権限をもつものとしなければならない。そのような場合、欧州委員会及び ECCG は、この規則の全体的な狙い及び諸目標、並びに、ENISA の計画及び資源利用に関する継続性を確保すべき必要性を考慮に入れた上で、そのような要請の必要性の評価もしなければならない。

そのような要請を受けた後、ENISA は、不適切な遅滞なく、特定の ICT 製品、ICT サービス及び ICT プロセスの制度候補を準備しなければならない。欧州委員会は、当の個別の市場、とりわけ、SME、技術革新、当該市場への参入の障壁、及び、エンドユーザの費用負担に対するその要請の積極の影響及び負の影響を評価しなければならない。欧州委員会は、ENISA によって準備された制度候補を基礎として、実装行為により、欧州サイバーセキュリティ認証制度を採択する権限を与えられなければならない。この規則に定める一般的な目的及びセキュリティ上の諸目標を考慮に入れた上で、欧州委員会によって採択される欧州サイバーセキュリティ認証制度は、個々の制度の対象事項、適用範囲及び機能に関するミニマムのセットの要素を指示しなければならない。それらの諸要素は、就中、適用対象となる ICT 製品、ICT サービス及び ICT プロセスの類型を含め、サイバーセキュリティ認証の適用範囲及び対象、例えば、標準または技術仕様の指示によるサイバーセキュリティ要求事項の詳細仕様、個別の評価基準及び評価手法、並びに、予定する保証のレベル（基本、標準または高度）、そして、該当するときは、評価のレベルを含めるものとしなければならない。ENISA は、ECCG からの要請を拒否できるものとすべきである。そのような決定は、運営会議によって行われ、かつ、適正な理由を付すこととしなければならない。

(85) ENISA は、欧州サイバーセキュリティ認証制度に関する情報を提供し、その制度を公表する Web サイトを維持管理しなければならず、その Web サイトは、就中、制度候補の準備の要請書、並びに、準備段階において ENISA によって実施されるコンサルテーションプロセスの中で受け取ったフィードバックを含めるものとしなければならない。その Web サイトは、この規則に基づいて発行される欧州サイバーセキュリティ証明書及び EU 適合性宣言書の取消し及び失効に関する情

報を含め、この規則に基づいて発行される欧州サイバーセキュリティ証明書及び EU 適合性宣言書に関する情報も提供しなければならない。その Web サイトは、欧州サイバーセキュリティ認証制度によって置き換えられた国内サイバーセキュリティ認証制度も表示しなければならない。

(86) 欧州サイバーセキュリティ認証制度の保証レベルは、ICT 製品、ICT サービスまたは ICT プロセスが特定の欧州サイバーセキュリティ認証制度のセキュリティ要求事項に適合しているとの信頼の基礎となるものである。欧州サイバーセキュリティ認証枠組みの一貫性を確保するため、欧州サイバーセキュリティ認証制度は、同制度の下で発行される欧州サイバーセキュリティ証明書及び EU 適合性宣言書の保証レベルを指示できるものとすべきである。個々の欧州サイバーセキュリティ証明書は、「基本」、「標準」または「高度」のいずれかの保証レベルを示し得るが、EU 適合性宣言書は、「基本」の保証レベルのみを示し得る。保証レベルは、ICT 製品、ICT サービスまたは ICT プロセスの評価の対応する厳格さ及び深さを提供し得るものであり、また、技術上の監視、インシデントを緩和または防止することをその目的とする技術的管理策を含め、その ICT 製品、ICT サービスまたは ICT プロセスと関係する技術仕様、標準及び手順を指示することによって特徴付けられ得る。個々の保証レベルは、認証が適用される異なる部門ドメインの間において一貫性のあるものでなければならない。

(87) 欧州サイバーセキュリティ認証制度は、使用される評価手法の厳格さ及び深さにより、複数の評価レベルを示し得る。評価レベルは、いずれか 1 つの保証レベルに対応するものでなければならず、かつ、保証内容の適切な組み合わせによって関連付けられなければならない。全ての保証レベルに関し、ICT 製品、ICT サービスまたは ICT プロセスは、制度によって示されるような多数の安全性機能を含めるべきものであり、それは、安全で即時に使用できる設定、署名されたコード、安全なアップデート及び攻撃の軽減、スタックメモリまたはヒープメモリ全部の防護を含み得る。これらの諸機能は、実効的なソフトウェア及びハードウェアの仕組みが信頼性をもって組み込まれることを確保するためのセキュリティに的を絞った開発アプローチ及び関連ツールを使用して開発されたものでなければならず、かつ、そのように維持管理されなければならない。

(88) 「基本」レベルの保証に関し、その評価は、少なくとも、保証内容に従うことによってガイドされなければならない：その評価は、少なくとも、適合性評価機関による ICT 製品、ICT サービスまたは ICT プロセスの技術文書の見直しを含めなければならない。証明書が ICT プロセスを含む場合、ICT 製品または ICT サービスの設計、開発及び維持管理のために使用されるプロセスもまた、技術上の見直しに服さなければならない。欧州サイバーセキュリティ認証制度が自己適合性評価を定める場合、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダが、その ICT 製品、ICT サービスまたは ICT プロセスが認証制度を遵守するものであることの自己評価を実施したことで十分なものとしなければならない。

(89) 「標準」レベルの保証に関し、その評価は、「基本」レベルの保証の要求事項に加え、少なくとも、その ICT 製品、ICT サービスまたは ICT プロセスのセキュリティ機能がその技術文書を遵守するものであることを確認することによってガイドされなければならない。

(90) 「高度」レベルの保証に関し、その評価は、「標準」レベルの保証の要求事項に加え、少なくとも、十分な技能と資源をもつ者によって実行される巧妙なサイバー攻撃に対するその ICT 製品、ICT サービスまたは ICT プロセスのセキュリティ機能の耐性を評価する実効性のあるテストによってガイドされなければならない。

(91) 欧州サイバーセキュリティ認証及び EU 適合性宣言書に依ることは、欧州連合法または欧州連合

法に従って採択された構成国法が別異に定める場合を除き、任意のままとしなければならない。整合化された欧州連合法が存在しない場合、欧州議会及び理事会の指令(EU) 2015/1535[20]による欧州サイバーセキュリティ認証制度に基づく義務的な認証を定める国内技術規則を採択できる。構成国は、公共調達の過程において、欧州議会及び理事会の指令 2014/24/EU[21]の過程において、欧州サイバーセキュリティ認証に依らせることもできる。

(92) 幾つかの場合において、欧州連合内のサイバーセキュリティのレベルを向上させるため、一定の ICT 製品、ICT サービスまたは ICT プロセスに関し、特定のサイバーセキュリティの要求事項を課し、それらの認証を義務的なものとすることが、将来において必要となることがあり得る。欧州委員会は、域内市場における安全な ICT 製品、ICT サービス及び ICT プロセスの可用性に対する採択された欧州サイバーセキュリティ認証制度の影響を継続的に監視しなければならず、かつ、欧州連合内における ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダによる認証制度の利用のレベルを継続的に評価しなければならない。欧州サイバーセキュリティ認証制度の実効性、及び、特定の制度が義務とされるべきか否かは、重要サービスの運営者によって使用されるネットワーク及び情報システムの安全性を考慮に入れた上で、欧州連合のサイバーセキュリティ関連立法、とりわけ、指令(EU) 2016/1148 に照らし、評価されなければならない。

(93) 欧州サイバーセキュリティ証明書及び EU 適合性宣言書は、エンドユーザが説明を受けた上で選択を行うことを助けるものでなければならない。それゆえ、認証を受けた ICT 製品、ICT サービス及び ICT プロセスまたは EU 適合性宣言書の発行を受けた ICT 製品、ICT サービス及び ICT プロセスは、予定されるエンドユーザの予想される技術レベルに合わせて調整される構成された情報提供を伴うものとすべきである。全てのそのような情報は、オンラインで利用可能でなければならず、また、それが適切なときは、物理媒体で利用可能でなければならない。エンドユーザは、認証制度の参照番号、保証レベル、その ICT 製品、ICT サービスもしくは ICT プロセスと関係するサイバーセキュリティ上のリスクの記述、並びに、発行機関または発行組織に関する情報へのアクセスをもたなければならず、または、欧州サイバーセキュリティ証明書の複製物を入手できるものとしなければならない。加えて、エンドユーザは、ICT サービスまたは ICT プロセスの製造者またはプロバイダのサイバーセキュリティ上のサポートの基本方針、すなわち、そのエンドユーザが、どれだけの期間にわたり、サイバーセキュリティ上のアップデートまたはパッチを受けることを期待できるかについて、情報提供を受けるものとしなければならない。該当するときは、エンドユーザが、その ICT 製品、ICT サービスのサイバーセキュリティを維持または向上させるために実装可能な行動または設定に関する指針、並びに、（自動的な通報に加え）サイバー攻撃の場合において通報し、サポートを受けるための連絡部局の連絡先情報が提供されなければならない。その情報は、定期的にアップデートされ、かつ、欧州サイバーセキュリティ制度に関する情報を提供する Web サイト上において利用できるようにされなければならない。

(94) この規則の諸目的を達成するため、及び、域内市場の断片化を避けるため、欧州サイバーセキュリティ認証制度に包摂される ICT 製品、ICT サービスまたは ICT プロセスの国内サイバーセキュリティ認証制度またはその手続は、その実装行為により欧州委員会によって定められる日から、

[20] 技術規則の分野及び情報社会サービス関連法令の分野における情報提供手続を定める欧州議会及び理事会の 2015 年 9 月 9 日の指令(EU) 2015/1535（OJ L 241, 17.9.2015, p.1）

[21] 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）

その有効性を終了させなければならない。更に、構成国は、既存の欧州サイバーセキュリティ認証制度によって既に包摂されている ICT 製品、ICT サービス及び ICT プロセスに関し、新たな国内サイバーセキュリティ認証制度を導入してはならない。ただし、構成国は、国家安全保障の目的のための国内サイバーセキュリティ認証制度を採択または維持することを妨げられるものとしてはならない。構成国は、欧州委員会及び ECCG に対し、新たな国内サイバーセキュリティ認証制度を策定する予定を通知しなければならない。その代わりに欧州サイバーセキュリティ認証制度を求める戦略上の意図に照らし、欧州委員会及び ECCG は、域内市場の適正な稼働に対する新たな国内サイバーセキュリティ認証制度の影響を評価しなければならない。

(95) 欧州サイバーセキュリティ認証制度は、欧州連合内における整合化されたサイバーセキュリティ実務を助けることを意図している。それらの制度は、欧州連合内におけるサイバーセキュリティのレベルを増加させることに貢献する必要がある。欧州サイバーセキュリティ認証制度の設計は、サイバーセキュリティの分野における発展を考慮に入れるものであり、かつ、それを許容するものでなければならない。

(96) 欧州サイバーセキュリティ認証制度は、現行のソフトウェア及びハードウェアの開発手法、並びに、とりわけ、個々の欧州サイバーセキュリティ証明書に対するソフトウェアまたはファームウェアの頻繁なアップデートの影響を考慮に入れなければならない。欧州サイバーセキュリティ認証制度は、当該証明書のセキュリティ上の要求事項の遵守に関するアップデートのあり得る負の影響を考慮に入れた上で、その ICT 製品、ICT サービスまたは ICT プロセスが認証の更新を受けなければならないこと、または、特定の欧州サイバーセキュリティ証明書の適用範囲が減縮されることをアップデートが要求し得る条件を指示しなければならない。

(97) 欧州サイバーセキュリティ認証制度が採択された後、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダは、彼らが選択する欧州連合内のいずれかの地の適合性評価機関に対し、彼らの ICT 製品または ICT サービスの認証を求める申請書を提出できるようにしなければならない。この規則に定める一定の指定された要求事項を適合性評価機関が適合しているときは、適合性評価機関は、国内認定機関によって認定されるものとしなければならない。認定は、最長 5 年間で発行されなければならず、また、その適合性評価機関がその要件に適合し続けている限り、同じ条件で更新され得るものとしなければならない。国内認定機関は、認定のための条件に適合しない場合、もしくは、適合しなくなった場合、または、適合性評価機関がこの規則に違反している場合、適合性評価機関の認定を制限し、停止し、または、取消さなければならない。

(98) 欧州サイバーセキュリティ認証制度の発効により失効した国内標準への国内立法中の参照は、混乱の発生原因となり得る。それゆえ、構成国は、欧州サイバーセキュリティ認証制度の採択をその構成国の国内立法の中に反映させなければならない。

(99) 欧州連合全域にわたる均等な標準を達成するため、相互承認を容易にするため、そして、欧州サイバーセキュリティ証明書及び EU 適合性宣言書の全体的な受容を促進するため、国内サイバーセキュリティ認証機関の間における相互評価の制度を設ける必要性がある。相互評価は、ICT 製品、ICT サービス及び ICT プロセスの欧州サイバーセキュリティ証明書の遵守を監督するための手続、自己適合性評価を実施する ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダの義務を監視するための手続、適合性評価機関、並びに、「高度」の保証レベルの証明書を発行する組織の職員の専門性が適切であることを監視するための手続を含めるものとしなければならない。欧州委員会は、実装行為により、相互評価のための少なくとも 5 年間の計画

を策定し、相互評価制度の運用のための基準及び手法を定め得るものとすべきである。

(100) 欧州サイバーセキュリティ認証の枠組み内にある全ての国内サイバーセキュリティ認証機関を通じて設けられる一般的な相互評価制度を妨げることなく、一定の欧州サイバーセキュリティ認証制度は、ICT 製品、ICT サービス及び ICT プロセスについて欧州サイバーセキュリティ認証制度の下における「高度」の保証レベルの保証をもつ欧州サイバーセキュリティ証明書を発行する組織のための相互評価の仕組みを含めることができる。ECCG は、そのような相互評価の仕組みの実装を支援しなければならない。相互評価は、とりわけ、関係する組織が整合化された態様で彼らの職務を実施しているか否かを評価しなければならず、また、異議申立ての仕組みを含めることができる。相互評価の結果は、公衆が利用できるものとしなければならない。関係する組織は、彼らの実務及び専門性を調整するための適切な措置をしかるべく採択できる。

(101) 構成国は、この規則から生ずる義務の遵守を監督するため、1 または複数の国内サイバーセキュリティ認証機関を指定しなければならない。国内サイバーセキュリティ認証機関は、既存の機関または新たな機関とすることができる。構成国は、他の構成国と合意した上で、当該別の構成国の領土内にある 1 または複数の国内サイバーセキュリティ認証機関を指定できるものとすべきである。

(102)国内サイバーセキュリティ認証機関は、EU 適合性宣言書との関係において、その構成国それぞれの領土内に設けられた ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダの義務を監視し、かつ、強制しなければならず、専門知識及び関連情報を提供することにより、適合性評価機関の監視及び監督において、国内認定機関を補助しなければならず、欧州サイバーセキュリティ認証制度に定める追加要求事項にその機関が適合するときは、適合性評価機関がその職務を遂行することを承認しなければならず、かつ、サイバーセキュリティ認証の分野における関連する発展を監視しなければならない。国内サイバーセキュリティ認証機関は、その機関から発行される欧州サイバーセキュリティ証明書との関係において、または、その証明書が「高度」の保証レベルを示すときは、適合性評価機関から発行される欧州サイバーセキュリティ証明書との関係において、自然人または法人から申立てられた異議申立ても取扱わなければならず、適切な範囲内において、その異議申立ての対象事項を調査しなければならず、かつ、合理的な期間内に、その異議申立人に対し、その調査の進捗状況及び調査結果を通知しなければならない。更に、国内サイバーセキュリティ認証機関は、ICT 製品、ICT サービス及び ICT プロセスの、この規則の要求事項または個別のサイバーセキュリティ認証制度のあり得る不遵守に関する情報交換による場合を含め、別の国内サイバーセキュリティ認証機関またはそれ以外の行政機関と協力しなければならない。欧州委員会は、例えば、規則(EC) No 765/2008 によって市場調査機関が既に使用している市場調査の情報通信システム（ICSMS）及び食品ではない危険な製品に関する緊急警報システム（RAPEX）のような、一般的な電子情報支援システムを利用できるようにすることにより、その情報交換を容易にしなければならない。

(103) 欧州サイバーセキュリティ認証枠組みの一貫性のある適用を確保するため、国内サイバーセキュリティ認証機関の代表またはそれ以外の関連国内機関の代表によって構成される ECCG が設置されなければならない。ECCG の主要な職務は、欧州サイバーセキュリティ認証枠組みの一貫性のある実装及び適用を確保するための欧州委員会の仕事において、欧州委員会に対して助言し、欧州委員会を補佐すること、サイバーセキュリティ認証制度候補の準備に際し、ENISA を補佐し、ENISA と緊密に協力すること、適正に正当化される場合において、ENISA に対し、制度候

補を準備するよう要請すること、並びに、制度候補に関し、ENISA 宛の意見書を採択すること、並びに、既存の欧州サイバーセキュリティ認証制度の維持及び見直しに関し、欧州委員会宛の意見書を採択することでなければならない。ECCG は、適合性評価機関の認定及び欧州サイバーセキュリティ証明書の発行について職責を負う様々な国内サイバーセキュリティ認証機関の間におけるグッドプラクティス及び専門知識の交換を容易にしなければならない。

(104)意識を向上させるため、及び、将来の欧州サイバーセキュリティ認証制度の受容を容易にするため、欧州委員会は、例えば、サイバーセキュリティ上のグッドプラクティスに関し、または、認証された ICT 製品、ICT サービス及び ICT プロセスの利用の積極的な効果に着目する責任あるサイバーセキュリティ行動に関し、一般的または部門別のサイバーセキュリティ運用指針を発行できる。

(105) 取引を更に容易にし、かつ、ICT のサプライチェーンがグローバルなものであることを更に認識させるため、欧州サイバーセキュリティ証明書に関する相互承認協定は、欧州連合の機能に関する条約（TFEU）の第 218 条に従い、欧州連合によって締結され得る。欧州委員会は、ENISA 及び欧州サイバーセキュリティ認証グループからの助言を考慮に入れた上で、関連する交渉の開始を勧告できる。個々の欧州サイバーセキュリティ認証制度は、第三国との間のそのような相互承認協定に関する個別の条件を定めなければならない。

(106) この規則の実装に関する統一的な条件を確保するため、欧州委員会に対し、実装権限が与えられなければならない。それらの実装権限は、欧州議会及び理事会の規則(EU) No 182/2011[22]に従って行使されなければならない。

(107) ICT 製品、ICT サービスまたは ICT プロセスの欧州サイバーセキュリティ認証制度の実装行為の採択、ENISA による調査の実施のための協定に関する実装行為の採択、国内サイバーセキュリティ認証機関の相互評価に関する計画の実装行為の採択、並びに、国内サイバーセキュリティ認証機関から欧州委員会に対する認定適合性評価機関の通知の状況、フォーマット及び手続に関する実装行為の採択には、審議手続が使用されなければならない。

(108) ENISA の業務遂行は、定期的かつ独立の評価に服さなければならない。その評価は、ENISA の目標、その仕事の実際、及び、その職務の関連性、とりわけ、欧州連合レベルの業務遂行上の協力と関連する ENISA の職務に関するものとしなければならない。その評価は、欧州サイバーセキュリティ認証枠組みの影響、実効性及び効率性も評価しなければならない。見直しが行われる際、欧州委員会は、助言及び専門知識の拠点としての ENISA の役割がどのように強化され得るかを評価しなければならず、また、そのような製品、サービス及びプロセスが欧州連合内に入る場合、欧州連合の法令を遵守しない第三国の ICT 製品、ICT サービス及び ICT プロセスの評価の支援の役割を ENISA に対して与えることの可否も評価しなければならない。

(109) この規則の目的は、構成国によっては十分に達成され得ず、その規模及び効果のゆえに、欧州連合のレベルにおいてより良く達成され得るものであるので、欧州連合は、欧州連合条約（TEU）の第 5 条に定める補完性原則に従い、措置を採択できる。同条に定める比例性原則に従い、この規則は、その目的を達成するために必要なところを越えることがない。

(110) 規則(EU) No 526/2013 は、廃止されなければならない。

---

[22] 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則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）

第 I 款 総則的な条項

第 1 条 対象事項及び適用範囲

1. 欧州連合内における高いレベルのサイバーセキュリティ、サイバー回復力及び信頼を狙いとしつつ、域内市場の適正な稼働を確保するため、この規則は:
   (a) ENISA(欧州連合サイバーセキュリティ局)の目的、職務及び組織上の事項を定め;かつ、
   (b) 欧州連合内における ICT 製品、ICT サービス及び ICT プロセスの十分なレベルのサイバーセキュリティを確保する目的のため、並びに、欧州連合内におけるサイバーセキュリティ認証制度に関する域内市場の断片化を避けるため、欧州サイバーセキュリティ認証制度を設置するための枠組みを定める。

   第 1 副項(b)に示す枠組みは、任意的認証または義務的認証と関連する他の欧州連合法の個別の条項を妨げることなく、適用される。
2. この規則は、公共の安全、防衛、国家安全保障及び刑事法の分野における国の活動と関係する構成国の職務権限を妨げない。

第 2 条 定義

この規則の目的のために、以下の定義が適用される:

(1) 「サイバーセキュリティ」とは、ネットワーク及び情報システム、そのようなシステムの利用者、並びに、サイバー脅威による影響を受けるその他の者の防護のために必要となる活動のことを意味し;
(2) 「ネットワーク及び情報システム」とは、指令(EU) 2016/1148 の第 4 条(1)に定義するネットワーク及び情報システムのことを意味し;
(3) 「ネットワーク及び情報システムの安全性に関する国内戦略」とは、指令(EU) 2016/1148 の第 4 条(3)に定義するネットワーク及び情報システムの安全性に関する国内戦略のことを意味し;
(4) 「重要サービス運営者」とは、指令(EU) 2016/1148 の第 4 条(4)に定義する重要サービス運営者のことを意味し;
(5) 「デジタルサービスプロバイダ」とは、指令(EU) 2016/1148 の第 4 条(6)に定義するデジタルサービスプロバイダのことを意味し;
(6) 「インシデント」とは、指令(EU) 2016/1148 の第 4 条(7)に定義するインシデントのことを意味し;
(7) 「インシデント対応」とは、指令(EU) 2016/1148 の第 4 条(8)に定義するインシデント対応のことを意味し;
(8) 「サイバー脅威」とは、ネットワーク及び情報システム、そのようなシステムの利用者及び影響を受けるその他の者に対し損害、危殆またはそれ以外の負の影響を与え得る可能性のある状況、出来事または行動のことを意味し;
(9) 「欧州サイバーセキュリティ認証制度」とは、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のことを意味し；

(10) 「国内サイバーセキュリティ制度」とは、国内行政機関によって策定及び採択され、かつ、特定の制度の適用範囲の下にある 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のことを意味し；

(11) 「欧州サイバーセキュリティ証明書」とは、当該 ICT 製品、ICT サービスまたは ICT プロセスが欧州サイバーセキュリティ認証制度に定める個々の安全性の要求事項を満たしていると評価されたことを証明する関係機関から発行される文書のことを意味し；

(12) 「ICT 製品」とは、ネットワーク及び情報システムの構成要素または構成要素グループのことを意味し；

(13) 「ICT サービス」とは、その全部において、または、主として、ネットワーク及び情報システムによる情報の送信、記録保存、検索または処理によって構成されるサービスのことを意味し；

(14) 「ICT プロセス」とは、ICT 製品または ICT サービスの設計、開発、供給または維持管理のために実施される活動のセットのことを意味し；

(15) 「認定」とは、規則(EC) No 765/2008 の第 2 条(10)に定義する認定のことを意味し；

(16) 「国内認定機関」とは、規則(EC) No 765/2008 の第 2 条(11)に定義する国内認定機関のことを意味し；

(17) 「適合性評価」とは、規則(EC) No 765/2008 の第 2 条(12)に定義する適合性評価のことを意味し；

(18) 「適合性評価機関」とは、規則(EC) No 765/2008 の第 2 条(13)に定義する適合性評価機関のことを意味し；

(19) 「標準」とは、規則(EU) No 1025/2012 の第 2 条(1)に定義する標準のことを意味し；

(20) 「技術仕様」とは、ICT 製品、ICT サービスまたは ICT プロセスに適合するための技術上の要求事項を記述する文書、または、ICT 製品、ICT サービスまたは ICT プロセスと関連する適合性評価手続を記述する文書のことを意味し；

(21) 「評価レベル」とは、ICT 製品、ICT サービスまたは ICT プロセスが、特定の欧州サイバーセキュリティ認証制度のセキュリティ上の要求事項に適合しているとの信頼の基礎を意味し、ICT 製品、ICT サービスまたは ICT プロセスが評価されたレベルを示すものであるが、そのようなレベルであることは、その ICT 製品、ICT サービスまたは ICT プロセスの安全性を計測するものではなく；

(22) 「自己適合性評価」とは、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダによって実施され、当該 ICT 製品、ICT サービスまたは ICT プロセスが特定の欧州サイバーセキュリティ認証制度の要求事項に適合するか否かを評価する行動のことを意味する。

第 II 款　ENISA（欧州連合サイバーセキュリティ局）

第 I 章　任務及び目的

第 3 条　任務

1. ENISA は、サイバーセキュリティの向上において、構成国、欧州連合の機関、組織、事務局及び部局を積極的に支援することによる場合を含め、欧州連合全域にわたる高いレベルの共通のサイバーセキュリティを達成する目的のためにこの規則に基づき ENISA に対して割当てられた職務を実施する。ENISA は、欧州連合の機関、組織、事務局及び部局のために、並びに、それら以外の欧州連合の利害関係者のために、サイバーセキュリティに関する助言及び専門知識の拠点として行動する。

   ENISA は、この規則に基づき ENISA に対して割当てられた職務を実施することにより、域内市場の断片化を削減することに貢献する。
2. ENISA は、サイバーセキュリティと関連する構成国の法律、規則及び行政規則を近似化させるための措置を定める欧州連合の法的行為によって ENISA に対して割当てられた職務を実施する。
3. その職務を実施する際、ENISA は、構成国の諸活動との重複を避けつつ、かつ、構成国の既存の専門知識を考慮に入れた上で、独立して行動する。
4. ENISA は、技術上及び人的な能力及び技能を含め、この規則に基づき ENISA に対して割当てられた職務を遂行するために必要となる ENISA 自身の資源を開発する。

第 4 条　目的

1. ENISA は、ENISA の独立性、ENISA が提供する助言及び補助の科学的品質及び技術的品質、ENISA が提供する情報、ENISA の業務遂行手法の透明性、業務手段、並びに、ENISA の職務を実施する際における ENISA の説明責任によって、サイバーセキュリティに関する専門知識の拠点である。
2. ENISA は、サイバーセキュリティに関する部門別の政策を含め、サイバーセキュリティと関連する欧州連合の政策の策定及び実装において、欧州連合の機関、組織、事務局及び部局並びに構成国を補助する。
3. ENISA は、欧州連合の機関、組織、事務局及び部局、並びに、構成国、公的及び民間の利害関係者のネットワーク及び情報システムの防護を向上させるため、サイバー回復力及び対応能力を開発し、向上させるため、並びに、サイバーセキュリティの分野における技能及び能力を開発するため、それらを補助することにより、欧州連合全域にわたる能力構築及び準備体制を支援する。
4. ENISA は、サイバーセキュリティに関する事柄に関し、欧州連合レベルの情報共有及び協力を含め、構成国、欧州連合の機関、組織、事務局及び部局、並びに、関連する民間の利害関係者または公的利害関係者の間の協力を促進する。
5. ENISA は、サイバー脅威の防止及びサイバー脅威への対応において、とりわけ、国境を越え

るインシデントの発生の際において、構成国の活動を支援するため、欧州連合レベルのサイバーセキュリティ能力を向上させることに貢献する。

6. ENISA は、域内市場の断片化を避けるため、欧州サイバーセキュリティ認証の利用を促進する。ENISA は、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティの透明性を向上させ、それによって、デジタル域内市場における信頼及びデジタル域内市場の競争力を強化するため、この規則の第 III 款に従い、欧州サイバーセキュリティ認証枠組みの構築及び維持に貢献する。

7. ENISA は、市民、組織及び企業の間におけるサイバー衛生及びサイバーリテラシを含め、高いレベルのサイバーセキュリティの意識を向上させる。

第 II 章 職務

第 5 条 欧州連合の政策及び法律の策定及び実装

ENISA は、以下の活動によって、欧州連合の政策及び法律の策定及び実装に貢献する:

(1) サイバーセキュリティの分野における欧州連合の政策及び法律の策定及び見直しに関し、並びに、サイバーセキュリティと関連する事項が含まれている場合において、部門別の政策及び法律の取り組みの策定及び見直しに関し、とりわけ、ENISA の独立の意見及び分析を提供することにより、並びに、準備作業を実施することにより、補助し、助言すること;

(2) 意見書、運用指針を発すること、リスク管理、インシデント通報及び情報共有のようなトピックスに関する助言及びベストプラクティスを提供することによる場合、並びに、この点に関する職務権限を有する機関の間のベストプラクティスの交換を容易にすることによる場合を含め、特に指令(EU) 2016/1148 との関係において、一貫性をもってサイバーセキュリティと関連する欧州連合の政策及び法律を実装するため、構成国を補助すること;

(3) オープンインターネットのパブリックコアの一般的な可用性または完全性を維持することと関連するサイバーセキュリティ政策の策定及び普及において、構成国並びに欧州連合の機関、組織、事務局及び部局を補助すること;

(4) ENISA の専門知識及び補助を提供することにより、指令(EU) 2016/1148 の第 11 条による協力グループの仕事に貢献すること;

(5) 以下を支援すること:

(a) とりわけ、助言を提供すること及び技術上の運用指針を発することにより、並びに、職務権限を有する機関の間におけるベストプラクティスの交換を容易にすることにより、電子識別子及び信頼サービスの分野における欧州連合の政策の策定及び実装;

(b) 専門知識及び助言を提供することによる場合、並びに、職務権限を有する機関の間におけるベストプラクティスの交換を容易にすることによる場合を含め、拡大されたレベルの電子通信の安全性の向上;

(c) 欧州データ保護委員会に対し、要請に応じて助言を提供することによる場合を含め、データ保護及びプライバシーと関連し、欧州連合の政策及び法律のサイバーセキュリティ上の特定の側面の実装において、構成国;

(6) 以下と関連する法的枠組みの実装状態に関する年次報告書を準備することにより、欧州連

合の政策活動の継続的な見直しを支援すること:

(a) 指令(EU) 2016/1148 の第 10 条第 3 項により協力グループに対して連絡部局から提供される構成国のインシデント通知に関する情報提供;

(b) 欧州議会及び理事会の規則(EU) 910/2014[23]の第 19 条第 3 項により監督機関から ENISA に対して提供される、信頼サービスプロバイダから受け取るセキュリティ侵害及び完全性喪失の通知の要旨;

(c) 指令(EU) 2018/1972 の第 40 条により職務権限を有する機関から ENISA に対して提供される、公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダから送信されるセキュリティ上のインシデント通知。

第 6 条 能力開発

1. ENISA は:

(a) 情報及び専門知識を構成国に提供することにより、サイバー脅威及びインシデントの防止、検知及び分析を向上させ、並びに、それらに対応する能力を向上させるための仕事において、構成国を補助し;

(b) 任意ベースの脆弱性開示基本方針の策定及び実装において、構成国並びに欧州連合の機関、組織、事務局及び部局を補助し;

(c) とりわけ、CERT-EU に対する適切な支援を通じて、サイバー脅威及びインシデントの防止、検知及び分析を向上させ、並びに、そのようなサイバー脅威及びインシデントに対応するための欧州連合の機関、組織、事務局及び部局の能力を向上させるためのそれらの機関、組織、事務局及び部局の仕事において、それらの機関、組織、事務局及び部局を補助し;

(d) 指令(EU) 2016/1148 の第 9 条第 5 項により要請された場合、国内 CSIRT の構築において、構成国を補助し;

(e) 指令(EU) 2016/1148 の第 7 条第 2 項により要請された場合、ネットワーク及び情報システムの安全性に関する国内戦略の策定において、構成国を補助し、並びに、ベストプラクティスを向上させるため、欧州連合全域にわたるそれらの戦略の伝達を向上し、並びに、その実装の進捗状況を注視し;

(f) サイバーセキュリティと関連する欧州連合の戦略の策定及び見直し、それらの戦略の伝達の向上及びそれらの戦略実装の進捗状況の追跡において、欧州連合の機関を補助し;

(g) 最新技術に関し、個々の CSIRT が共通のセットのミニマムの能力をもち、かつ、ベストプラクティスに従って業務遂行することを確保するため、対話と情報交換を向上させることによる場合を含め、国内 CSIRT 及び欧州連合の CSIRT の能力のレベルの向上において、それらの CSIRT を補助し;

(h) 少なくとも 2 年に 1 度、第 7 条第 5 項に示す欧州連合レベルのサイバーセキュリティ演習を継続的に立案準備することにより、及び、その演習の評価プロセス及びその演習から学んだ教訓を基礎とする政策上の勧告を行うことにより、構成国を補助し;

[23] 域内市場における電子商取引のための電子識別及び信頼サービスに関する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014（OJ L 257, 28.8.2014, p.73）

(i) それが適切なときは、利害関係者と協力して、サイバーセキュリティと関連する訓練を提供することにより、関連行政機関を補助し;

(j) とりわけ、構成国による重要サービスの運営者の指定に関し、リスク及びインシデントと関連する国境を越える相互依存関係と関係する場合を含め、指令(EU) 2016/1148 の第 11 条第 3 項(1)により、ベストプラクティスの交換において、協力グループを補助する。

2. ENISA は、利用可能なツール、手続に関し、並びに、情報共有と関連する法的問題にどのように対応するかに関し、ベストプラクティス及び運用指針を提供することにより、とりわけ、指令(EU) 2016/1148 の別紙 II に列挙する諸部門において、各部門内の情報共有及び諸部門間の情報共有を支援する。

第 7 条 欧州連合レベルの業務遂行上の協力

1. ENISA は、構成国、欧州連合の機関、組織、事務局及び部局の間、及び、利害関係者の間における業務遂行上の協力を支援する。

2. ENISA は、共通の関心事に対処するため、CERT-EU を含め、欧州連合の機関、組織、事務局及び部局との間において、サイバー犯罪を取り扱う行政機関との間において、並びに、プライバシー及び個人データの保護を取り扱う監督機関との間において、以下の手段による場合を含め、業務遂行レベルで協力し、かつ、波及効果を構築する:

(a) ノウハウ及びベストプラクティスの交換;

(b) サイバーセキュリティと関連する事項に関する助言の提供及び運用指針の発行;

(c) 欧州委員会との協議を経た上で、個別の職務の執行のための実務上の覚書の作成。

3. ENISA は、指令(EU) 2016/1148 の第 12 条第 2 項により、CSIRT ネットワークの事務局を提供し、かつ、その権能において、その構成員の間における情報共有及び協力を積極的に支援する。

4. ENISA は、以下によって、CSIRT ネットワーク内における業務遂行上の協力に関し、構成国を支援する:

(a) インシデントの防止、検知及び対応のための構成国の能力をどのようにして向上させるかに関し助言すること、並びに、1 または複数の構成国の要請により、個別のサイバー脅威との関係において助言を提供すること;

(b) 1 または複数の構成国の要請により、重大または大きな影響のあるインシデントを評価する場合において、とりわけ、構成国間における関連情報及び技術ソリューションの任意の共有を支援することによる場合を含め、専門知識の提供及びそのようなインシデントの技術上の取扱いを容易にすることによって、補助すること;

(c) 公衆が利用可能な情報またはその目的のために構成国から任意に提供される情報を基礎として、脆弱性及びインシデントを分析すること;並びに、

(d) 1 または複数の構成国の要請により、指令(EU) 2016/1148 の意味における重大または大きな影響のあるインシデントに関する事後の技術的調査との関係において、支援を提供すること。

これらの職務を遂行する際、ENISA 及び CERT-EU は、波及効果からの利益を享受するため、及び、活動の重複を避けるため、構造化された協力に従事する。

5. ENISA は、欧州連合レベルのサイバーセキュリティ演習を継続的に立案準備し、その要請に

より演習を立案準備する際、構成国並びに EU の機関、組織、事務局及び部局を支援する。欧州連合レベルのサイバーセキュリティ演習は、技術上の要素、運営上の要素及び戦略的な要素を含めることができる。2 年に 1 度の間隔で、ENISA は、大規模な包括的演習を立案準備する。

ENISA は、それが適切なときは、欧州連合レベルのサイバーセキュリティ演習にも参加する関連組織と共に、部門別のサイバーセキュリティ演習にも貢献し、また、部門別のサイバーセキュリティ演習の立案準備を助ける。

6. ENISA は、構成国と緊密に協力し、公衆が利用可能な情報、ENISA 自身の分析調査、並びに、とりわけ、構成国の CSIRT または指令（EU）2016/1148 によって設置される連絡部局により共有される報告書、および、EC3 および CERT-EU の双方から任意ベースに共有される報告書を基礎として、インシデントおよびサイバー脅威に関する継続的で詳細な EU サイバーセキュリティ技術状況報告書を準備する。

7. ENISA は、主として以下により、サイバーセキュリティと関連する大規模で国境を越えるインシデントまたは危機に対する欧州連合レベル及び構成国レベルの共同対応を発展させることに貢献する：

(a) パブリックドメインである国内情報源、または、共通の状況認識を確立することに貢献するために任意ベースで共有された国内情報源からの報告を集約し、分析すること；

(b) CSIRT ネットワークと欧州連合レベルの技術上及び政策上の意思決定権者との間における効率的な情報の流れ及びエスカレーションの仕組みの提供を確保すること；

(c) 要請に応じて、とりわけ、構成国間における技術ソリューションの任意の共有を支援することによる場合を含め、そのようなインシデントまたは危機の技術上の取扱いを容易にすること；

(d) そのようなインシデントまたは危機と関連する広報活動において、欧州連合の機関、組織、事務局及び部局を支援すること、並びに、要請に応じて、構成国を支援すること；

(e) 欧州連合レベルのそのようなインシデントまたは危機への対応のための共同計画をテストすること、並びに、構成国の要請に応じて、国内レベルのそのような計画のテストにおいて、構成国を支援すること。

第 8 条 市場、サイバーセキュリティ認証及び標準化

1. ENISA は、この規則の第 III 款に定めるとおり、以下によって、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ認証に関する欧州連合の政策の策定及び実装を支援及び促進し；

(a) 標準化の分野と関連する発展を常に監視し、かつ、その標準が存在しない場合、第 54 条の(c)により、欧州サイバーセキュリティ認証制度の策定において使用されるための適切な技術仕様を勧告すること；

(b) 第 49 条に従い、ICT 製品、ICT サービス及び ICT プロセスの欧州サイバーセキュリティ制度候補（「制度候補」）を準備すること；

(c) 第 49 条第 8 項に従い、採択された欧州サイバーセキュリティ認証制度を評価すること；

(d) 第 59 条第 4 項による相互評価に参加すること；

(e) 第 62 条第 5 項による ECCG の事務局の提供において、欧州委員会を補助すること。

2. ENISA は、第 22 条第 4 項による利害関係者サイバーセキュリティ認証グループの事務局を提供する。
3. ENISA は、国内サイバーセキュリティ認証機関及び産業界と協力し、公式の、構成され、かつ、透明性のある態様により、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ上の要求事項に関し、運用指針をとりまとめて公表し、かつ、グッドプラクティスを策定する。
4. ENISA は、運用指針をとりまとめて発行することにより、及び、構成国の要請に応じて構成国に対して支援を提供することにより、評価及び認証プロセスと関連する能力開発に貢献する。
5. ENISA は、リスク管理並びに ICT 製品、ICT サービス及び ICT プロセスの安全性に関する欧州標準及び国際標準の開発及び採用を容易にする。
6. 構成国及び産業界と共働して、重要サービスの運営者及びデジタルサービスプロバイダの安全性の要求事項と関連する技術分野に関し、並びに、指令(EU) 2016/1148 の第 19 条第 2 項により、構成国の国内標準を含め、既在の標準に関し、助言及び運用指針を作成する。
7. ENISA は、欧州連合内のサイバーセキュリティ市場を育成するという観点から、需要サイド及び供給サイドの両者において、サイバーセキュリティ市場の主要動向の継続的な分析を実施し、提供する。

第 9 条 知識及び情報

ENISA は:

(a) 先端技術の分析を実施し、かつ、サイバーセキュリティの技術革新による社会的影響、法的影響、法的影響、経済的影響及び規制上の影響に関し、トピックを絞った評価を提供し;
(b) 最新の傾向を判断し、インシデントの防止を助けるため、サイバー脅威及びインシデントの長期的な戦略分析を実施し;
(c) 構成国の機関の専門家及び利害関係者の専門家と共同して、ネットワーク及び情報システムのセキュリティに関し、とりわけ、指令(EU) 2016/1148 の別紙 II の列挙する部門を支えるインフラ及び同指令の別紙 III に列挙するデジタルサービスのプロバイダによって使用されるインフラに関し、助言、運用指針及びベストプラクティスを提供し;
(d) 専用のポータルを通じて、欧州連合の機関、組織、事務局及び部局から提供されるサイバーセキュリティに関する情報、並びに、構成国、民間の利害関係者及び公的な利害関係者から任意に提供されるサイバーセキュリティに関する情報を蓄積し、組織化し、かつ、公衆が利用できるようにし;
(e) 重大なインシデントに関する公衆が利用可能な情報を収集及び分析し、かつ、欧州連合全域にわたり、市民、組織及び企業に対して運用指針を提供するための報告書をとりまとめる。

第 10 条 意識向上及び教育

ENISA は:

(a) サイバーセキュリティ上のリスクの公衆の認識を向上させ、サイバー衛生及びサイバーリテラシを含め、市民、組織及び企業を主たる対象として、個人ユーザのためのグッドプラクティスに関する運用指針を提供し;

(b) 構成国、欧州連合の機関、組織、事務局及び部局並びに産業界と共同して、欧州連合内におけるサイバーセキュリティ及びその可視性を増加させるための継続的な普及支援を立案準備し、かつ、広範で公開の討議を奨励し；
(c) サイバーセキュリティの認識を向上させ、サイバーセキュリティ教育を促進するための構成国の仕事において、構成国を補助し；
(d) サイバーセキュリティの認識向上及び教育に関し、緊密な調整を支援し、かつ、構成国間におけるベストプラクティスの交換を支援する。

第 11 条 調査研究及び技術革新

ENISA は、調査研究及び技術革新に関し、：
(a) 新たな先端情報通信技術に関するものを含め、現在のリスク及びサイバー脅威及び発生しつつあるリスク及びサイバー脅威に対して実効的に対応できるようにするため、並びに、リスク防止技術を実効的に利用するため、サイバーセキュリティの分野における需要及び優先順位の調査研究に関し、欧州連合の機関、組織、事務局及び部局並びに構成国を補助し；
(b) 欧州委員会が ENISA に対して関連権限を委任したときは、調査研究及び技術革新の基金計画の実装のフェーズに関与し、または、受益者としてそれに関与し；
(c) サイバーセキュリティの分野において、欧州連合レベルで、戦略的な調査研究及び技術革新のアジェンダに貢献する。

第 12 条 国際協力

ENISA は、以下により、サイバーセキュリティと関連する問題に関する国際協力を促進するため、第三国及び国際機関との間において、関連する国際協力の枠組み内の範囲内において、欧州連合の仕事に貢献する：
(a) それが適切なときは、国際的な演習の立案準備にオブザーバーとして関与すること、及び、そのような演習の結果を分析し、運営会議に対して報告すること；
(b) 欧州委員会の要請に応じて、ベストプラクティスの交換を容易にすること；
(c) 欧州委員会の要請に応じて、欧州委員会に対して専門知識を提供すること；
(d) 第 62 条に基づいて設置される ECCG と共働して、第三国との間におけるサイバーセキュリティ認証の相互承認のための協定と関係する事項に関し、欧州委員会に対して助言し、欧州委員会を支援すること。

第 III 章 ENISA の組織

第 13 条 ENISA の構成

ENISA の行政組織及び運営組織は、以下によって構成される：
(a) 運営会議；
(b) 執行会議；

(c) 長官;
(d) ENISA 諮問グループ;
(e) 国内連絡官ネットワーク。

第 1 節 運営会議

第 14 条 運営会議の構成

1. 運営会議は、各構成国から任命される各 1 名の構成員、及び、欧州委員会から任命される 2 名の構成員によって構成される。全ての構成員は、議決権をもつ。
2. 運営会議の各構成員は、代理者をもつ。その代理者は、構成員が不在の場合において、その構成員を代理する。
3. 運営会議の構成員及びその代理者は、それらの者の業務運営上、行政上及び予算上の技能を考慮に入れた上で、サイバーセキュリティの分野における彼らの知識を基礎として任命される。欧州委員会及び構成国は、運営会議の仕事の継続性を確保するため、運営会議内における欧州委員会及び構成国の代表の交代を抑制するための努力を尽くす。欧州委員会及び構成国は、運営会議内におけるジェンダーバランスを達成することを目指す。
4. 運営会議の構成員及びその代理者の任期は、4 年とする。その任期は、更新され得る。

第 15 条 運営会議の権能

1. 運営会議は:
   (a) ENISA の業務遂行の一般的指示を決定し、かつ、この規則に定める規定及び基本原則に従って ENISA が業務遂行することを確保し;ENISA の仕事と、構成国によって実施される活動及び欧州連合レベルで実施される活動の一貫性も確保し;
   (b) 意見を得るために欧州委員会に対してそれを送付する前に、第 24 条に示す ENISA の単一計画書案を採択し;
   (c) 欧州委員会の意見を考慮に入れた上で、ENISA の単一計画書を採択し;
   (d) 単一計画書の中に含まれる多年度計画及び単年度計画の実装を監督し;
   (e) ENISA の年次予算を採択し、かつ、第 IV 章に従い、ENISA の予算に関するそれ以外の権能を行使し;
   (f) ENISA の業務遂行指標に ENISA がどのように適合しているかに関する検討及び記述を含め、ENISA の活動に関する統合された年次報告書を評価及び採択し、翌年の 7 月 1 日までに、欧州議会、理事会、欧州委員会及び欧州会計検査院に対し、その報告書及び評価書の両者を送付し、かつ、その年次報告書を公表し;
   (g) 第 32 条に従い、ENISA に適用される財務規則を採択し;
   (h) 実装される措置の費用対効果分析を考慮に入れた上で、不正行為のリスクと比例的な不正行為防止戦略を採択し;
   (i) その構成員と関係する利益相反の防止及び管理に関する規則を採択し;
   (j) 欧州不正対策局（OLAF）の調査結果である判断及び勧告、並びに、様々な内部監査報告

書または外部監査報告書及び評価結果書の適切な事後対応を確保し；

(k) 第 19 条第 7 項により、個別の職務の委任に関する暫定的な決定のための規定を含め、運営会議の手続規則を採択し；

(l) ENISA の職員に関し、本条第2項に従い、欧州連合の官吏の職員規則（「官吏の職員規則」）及びその他の公務員の雇用条件（「その他の公務員の雇用条件」）によって与えられる権限、及び、雇用契約の締結権限に関する欧州連合のその他の公務員の雇用条件によって与えられる権限、任命権限に関する、及び、雇用契約の締結権限を授与する権限に関する理事会規則(EEC, Euratom, ECSC) No 259/68[24]に定める権限（「任命権限」）を行使し；

(m) 官吏の職員規則第 110 条に定める手続に従い、官吏の職員規則及びその他の公務員の雇用条件を実装する規則を採択し；

(n) 第 36 条に従い、長官を任命し、かつ、それが適切なときは、彼もしくは彼女の任期を延長し、または、彼もしくは彼女を解任し；

(o) 彼または彼女の職務の遂行において全面的に独立しており、欧州委員会の会計事務職員とすることのできる会計事務職員を任命し；

(p) ENISA の活動の必要性を考慮に入れ、かつ、良好な予算運営に配慮した上で、ENISA の内部組織構成を定めること、及び、それが必要なときは、それらの内部組織構成を修正することに関する全ての決定を行い；

(q) 第 7 条に関する作業覚書の締結を承認し；

(r) 第 42 条に従い、業務協定の作成または締結を承認する。

2. 運営会議は、官吏の職員規則第 110 条に従い、官吏の職員規則第 2 条第 1 項及びその他の公務員の雇用条件第 6 条に基づき、関連任命権限を長官に委任する決定、及び、その権限の委任が停止され得る条件を定める決定を採択する。長官は、それらの権限を再委任できる。

3. 例外的な状況がそのように要求する場合、運営会議は、長官に対する任命権限の委任を一時的に停止し、及び、長官によるその権限の再委任を一時的に停止し、かつ、その権限を運営会議自らが行使し、または、その構成員のいずれかに対し、もしくは、長官以外の職員に対し、その権限を委任する決定を採択できる。

第 16 条 運営会議の議長

運営会議は、構成員の 3 分の 2 の多数決により、その構成員の中から議長及び副議長を選任する。その任期は、4 年とし、1 度だけ更新され得る。ただし、その任期中のいかなる時といえども、議長及び副議長が、運営会議の構成員資格を失ったときは、その議長及び副議長の任期は、当該の日に自動的に終了となる。議長が彼または彼女の職務を遂行できないときは、副議長は、職務上のものとして、議長に置き換わる。

第 17 条 運営会議の会合

1. 運営会議の会合は、その議長によって招集される。

[24] OJ L 56, 4.3.1968, p.1.

2. 運営会議は、少なくとも年 2 回の通常会合をもつ。議長からの要請がある場合、欧州委員会からの要請がある場合、または、構成員の 3 分の 1 以上からの要請がある場合、運営会議は、特別会合をもつ。
3. 長官は、運営会議の会合に参加するが、議決権をもたない。
4. ENISA 諮問グループの構成員は、議長からの招請により、運営会議の会合に参加できるが、議決権をもたない。
5. 運営会議の構成員及びその代理者は、運営会議の手続規則に従い、運営会議の会合の際、助言者または専門家の補助を受けることができる。
6. ENISA は、運営会議の事務局を提供する。

第 18 条 運営会議の議決規則

1. 運営会議は、その構成員の多数決によりその決定を行う。
2. 単一計画書の採択、年次予算の採択、及び、長官の任命、任期の延長または解任に関しては、運営会議の構成員の 3 分の 2 の多数を要する。
3. 各構成員は、1 個の議決権をもつ。構成員が不在のときは、その構成員の代理者は、その構成員の議決権を行使する資格をもつ。
4. 運営会議の議長は、議決に参加する。
5. 長官は、議決に参加しない。
6. 運営会議の手続規則は、より詳細な議決の手配、とりわけ、構成員が他の構成員の代わりに行動できる状況を定める。

第 II 節 執行会議

第 19 条 執行会議

1. 運営会議は、執行会議の補助を受ける。
2. 執行会議は:
   (a) 運営会議によって採択される決定を準備し;
   (b) 運営会議と共に、OLAF の調査からもたらされる判断及び勧告、並びに、様々な内部監査報告書または外部監査報告書及び評価結果書の適切な事後対応を確保し;
   (c) 第 20 条に定める長官の職責を妨げることなく、第 20 条による業務管理上の事柄及び予算上の事項に関し、運営会議の決定の実装において、長官を補佐し、長官に助言する。
3. 執行会議は、5 名の構成員によって構成される。執行会議の構成員は、運営会議の構成員の中から任命される。構成員中の 1 名は、執行会議を主宰することもできる運営会議の議長とし、他の 1 名は、欧州委員会の代表中のいずれかの者とする。執行会議の構成員の任命は、執行会議のジェンダーバランスを確保することを目指す。長官は、執行会議に参加するが、議決権をもたない。
4. 執行会議の構成員の任期は、4 年とする。その任期は、更新される。

5. 執行会議は、少なくとも 3 か月に 1 回、会合する。執行会議の議長は、その構成員の要請に応じて、追加会合を招集する。
6. 運営会議は、執行会議の手続規則を定める。
7. 緊急性のゆえに必要があるときは、執行会議は、とりわけ、任命権限の委任の停止及び予算上の事柄を含め、業務運営管理上の事項に関し、運営会議の代わりに、一定の暫定的な決定を行うことができる。そのような暫定的な決定は、不適切な遅滞なく、運営会議に対して通知される。その場合、運営会議は、その決定が行われた時から遅くとも 3 か月以内に、その暫定的な決定を承認するか、または、破棄するかを決定する。執行会議は、運営会議の構成員の 3 分の 2 の承認を要する決定を運営会議の代わりに行ってはならない。

第 III 節 長 官

第 20 条 長官の職責

1. ENISA は、ENISA の長官によって運営され、長官は、彼または彼女の職務の遂行において独立している。長官は、運営会議に対して説明責任を負う。
2. 長官は、そのようにすることを求められるときは、彼または彼女の職務の遂行に関し、欧州議会に対して報告する。理事会は、彼または彼女の職務の遂行に関して報告させるため、長官を招請できる。
3. 長官は、以下について職責を負う:
   (a) ENISA の日々の管理運営;
   (b) 運営会議によって採択された決定を実装すること;
   (c) 単一計画書を準備し、かつ、欧州委員会に対してそれを送付する前に、承認を得るため、運営会議にそれを提出すること;
   (d) 単一計画書を実装すること、並びに、それに関して運営会議に報告すること;
   (e) ENISA の活動に関する統合された年次報告書を準備すること、及び、評価及び採択を得るため、それを運営会議に提出すること;
   (f) 遡及的評価の結果に関する事後対応の行動計画を準備すること、及び、2 年毎に、欧州委員会に対し、進捗状況に関する報告をすること;
   (g) 内部監査報告書または外部監査報告書の判断、及び、OLAF による調査結果に事後対応する行動計画を準備すること、並びに、欧州委員会に対して年 2 回、及び、運営会議に対して継続的に、進捗状況に関して報告すること;
   (h) 第 32 条に示す ENISA に適用される財務規則案を準備すること;
   (i) ENISA の収入及び支出の見積書を作成すること、並びに、ENISA の予算を実行すること;
   (j) 詐欺、汚職及びそれ以外の違法行為に対する防止措置を適用することにより、効果的な点検により、及び、不規則行為が検知されたときは、不正に支払われた金額を回復することにより、並びに、それが適切なときは、効果的であり、比例的であり、かつ、抑止力のある行政制裁及び金銭制裁により、欧州連合の財政上の利益を防護すること;
   (k) ENISA のための不正行為防止戦略を準備すること、及び、承認を得るため、それを運営会議に提出すること;

(l) 関連利害関係者との間の継続的な対話を確保するため、産業界及び消費者団体との間の接触を発展させ、維持すること;

(m) 欧州連合の基本方針の策定及び実装における一貫性を確保するため、サイバーセキュリティと関連する各機関の活動に関し、欧州連合の機関、組織、事務局及び部局との間で意見及び情報を交換すること;

(n) この規則によって長官に割当てられた上記以外の職務を実施すること。

4. 必要があるときは、かつ、ENISA の目的及び職務の範囲内において、長官は、構成国の職務権限を有する機関からの専門家を含め、専門家で構成されるアドホック作業グループを設置できる。長官は、運営会議に対し、そのことについて事前に通知する。とりわけ、作業グループの組織構成に関する手続、長官による作業グループの専門家の任命、及び、作業グループの業務遂行は、ENISA の内部運営規則の中で定められる。

5. 必要があるときは、効率的かつ実効的な態様で ENISA の職務を実施する目的のために、かつ、適切な費用対効果分析を基礎として、長官は、1 または複数の構成国に 1 または複数の地方事務所を設置することを決定する。地方事務所を設置することを決定する前に、長官は、ENISA の本拠地のある構成国を含め、関係する構成国の意見を求め、かつ、欧州委員会及び運営会議の事前同意を得る。長官と関係構成国との間の協議過程の間に合意が得られない場合、その案件は、討議のために理事会にもちこまれる。地方事務所全部の職員の総数は、ミニマムのものであることを維持し、かつ、ENISA の本拠地が所在する構成国に所在する ENISA の職員の総数の 40％を超過してはならない。個々の地方事務所の職員の員数は、ENISA の本拠地が所在する構成国に所在する ENISA の職員の総数の 10％を超過してはならない。

地方事務所を設置する決定は、不要な費用支出と ENISA の業務運営機能の重複を避ける態様で、その地方事務所において実施されるべき活動の範囲を定める。

第 IV 節 ENISA 諮問グループ、利害関係者サイバーセキュリティ認証グループ及び国内連絡官ネットワーク

第 21 条 ENISA 諮問グループ

1. 運営会議は、長官からの提案に基づいて審議し、ICT 産業界、公衆が利用可能な電子通信ネットワークまたは電子通信サービスのプロバイダ、消費者団体、SME、重要サービス運営者、サイバーセキュリティにおける学術上の専門家のような関連利害関係者を代表する承認を受けた代表、指令(EU) 2018/1972 に基づき指定される職務権限を有する機関の代表及び欧州標準化機関の代表、並びに、法執行機関の代表及びデータ保護機関の代表によって構成される ENISA 諮問グループを、透明性のある態様により、設置する。運営会議は、適切なジェンダーバランス及び地理的バランス並びに異なる利害関係者間のバランスを確保することを目指す。

2. ENISA 諮問グループの手続、とりわけ、ENISA 諮問グループの構成に関する手続、第 1 項に示す長官からの提案、ENISA 諮問グループ構成員の任命及び ENISA 諮問グループの業務遂行は、ENISA の内部運営規則の中で定められ、かつ、公表される。

3. ENISA 諮問グループは、長官が議長となり、または、ケースバイケースで、長官から指名された者が議長となる。

4. ENISA 諮問グループの構成員の任期は、2 年半とする。運営会議の構成員は、ENISA 諮問グループの構成員となることができない。欧州委員会及び構成国からの専門家は、ENISA 諮問グループの会合に出席する資格をもち、その仕事に関与する。長官によって適切であると判断された上記以外の組織の代表であって、ENISA 諮問グループの構成員ではない者は、ENISA 諮問グループの会合に出席し、その仕事に関与するために、招請され得る。
5. ENISA 諮問グループは、この規則の第 III 款の各条項の適用を除き、ENISA の職務の遂行に関し、ENISA に対して助言する。ENISA 諮問グループは、とりわけ、ENISA の単年度事業計画の提案書の作成に関し、及び、その単年度事業計画と関連する事柄に関する利害関係者との間の連絡を確保することに関し、長官に対して助言する。
6. ENISA 諮問グループは、運営会議に対し、継続的に、その活動に関して情報提供する。

第 22 条 利害関係者サイバーセキュリティ認証グループ

1. 利害関係者サイバーセキュリティ認証グループが設置される。
2. 利害関係者サイバーセキュリティ認証グループは、関連利害関係者を代表する承認を受けた専門家の中から選任された構成員によって構成される。欧州委員会は、透明性のある公募の後、ENISA からの提案に基づき、異なる利害関係者間のバランス並びに適切なジェンダーバランス及び地理的バランスを確保して、利害関係者サイバーセキュリティ認証グループの構成員を選任する。
3. 利害関係者サイバーセキュリティ認証グループは:
   (a) 欧州サイバーセキュリティ認証枠組みと関連する戦略上の問題に関し、欧州委員会に対して助言し;
   (b) 要請に応じて、市場、サイバーセキュリティ認証及び標準化と関連する ENISA の職務と関係する一般的な事項及び戦略上の事項に関し、ENISA に対して助言し;
   (c) 第 47 条に示す欧州連合導入作業計画において、欧州委員会を補助し;
   (d) 第 47 条第 4 項により欧州連合導入作業計画に関する意見書を発し;並びに、
   (e) 緊急の場合において、第 47 条及び第 48 条に示されているとおり、欧州連合導入作業計画に含まれていない追加的な認証制度の必要性に関し、欧州委員会及び ECCG に対して助言を提供する。
4. 利害関係者サイバーセキュリティ認証グループは、欧州委員会の代表及び ENISA の代表が共同議長となり、その事務局は、ENISA から提供される。

第 23 条 国内連絡官ネットワーク

1. 運営会議は、長官からの提案に基づいて審議し、全ての構成国の代表（国内連絡官）によって構成される国内連絡官ネットワークを設置する。各構成国は、国内連絡官ネットワークへの 1 名の代表を任命する。国内連絡官ネットワークの会合は、専門家構成毎に分けて開催され得る。
2. 国内連絡官ネットワークは、とりわけ、ENISA と構成国との間の情報交換を容易にし、かつ、ENISA の活動、判断及び勧告の欧州連合全域にわたる利害関係者への伝達において、ENISA を支援する。

3. 国内連絡官ネットワークは、ENISA の単年度事業計画の実装の過程において、ENISA と国内専門家との間の協力を国内レベルで容易にするための連絡部局として行動する。
4. 国内連絡官は、彼らそれぞれの構成国の運営会議代表と緊密に協力しなければならないが、国内連絡官ネットワークそれ自身は、運営会議またはそれ以外の欧州連合のフォーラムの仕事と重複してはならない。
5. 国内連絡官ネットワークの権能及び手続は、ENISA の業務遂行内部規則の中で定められ、かつ、公表される。

第 V 節 業務遂行

第 24 条 単一計画書

1. ENISA は、単年度事業計画及び多年度事業計画を含め、ENISA の計画された全ての活動を含める単一計画書に従い、業務を遂行する。
2. 長官は、毎年、委員会委任規則(EU) No 1271/2013[25]の第 32 条に従い、かつ、欧州委員会によって定められる運用指針を考慮に入れた上で、対応する資金計画及び人員計画をもつ多年度事業計画及び単年度事業計画を含む単一計画書案を作成する。
3. 運営会議は、毎年 11 月 30 日までに、第 1 項に示す単一計画書を採択し、遅くとも翌年の 1 月 31 日までに、欧州議会、理事会及び欧州委員会に対し、その計画書及び当該文書の後にアップデートされた版を送付する。
4. 単一計画書は、欧州連合の一般予算の最終的な採択の後に確定し、必要があるときは、しかるべく補正される。
5. 単年度事業計画は、業務遂行の指標を含め、目標の細目及び所期の結果によって構成される。単年度事業計画は、活動ベースの予算及び運営の原則に従い、予算付けられる活動の記述、並びに、個々の活動に割当てられる資金及び人員の表示を含める。単年度事業計画は、第 7 項に示す多年度事業計画と一貫性のあるものとする。単年度事業計画は、前予算年と比較し、追加、変更または削除された職務を明確に表示する。
6. 運営会議は、ENISA に対して新たな職務が与えられる場合、採択された単年度事業計画を修正する。単年度事業計画の大きな修正は、当初の単年度事業計画と同じ手続によって採択される。運営会議は、単年度事業計画の大きくない修正を行う権限を長官に委任できる。
7. 多年度事業計画は、目的、所期の結果及び業務遂行指標を含め、全体的な戦略計画を定める。多年度事業計画は、多年度の予算及び人員を含む資金計画を定める。
8. 資金計画は、年次で、最新のものに改められる。それが必要な場合、とりわけ、第 67 条に示す評価結果に対応する必要がある場合、戦略計画は、最新のものに改められる。

[25] 欧州議会及び理事会の(EU, Euratom) No 966/2012 に示す組織のための枠組み財政規則に関する 2013 年 9 月 30 日の委員会委任規則(EU) No 1271/2013（OJ L 328, 7.12.2013, p.42）

第 25 条 利害関係の宣言

1. 運営会議の構成員、長官、及び、構成国から一時的に派遣される官吏は、それぞれ、職務専念の宣言、並びに、彼らの独立性を損なうと判断され得る直接または間接の利害関係の有無を示す宣言を行う。その宣言は、正確かつ完全であり、毎年、書面により行われるものとし、必要があるときは、最新のものに改められる。
2. 運営会議の構成員、長官、及び、アドホック作業グループに参加する外部専門家は、それぞれ、遅くとも各会合の開始の時点において、正確かつ完全に、その議題にある事項との関係において彼らの独立性を損なうと判断され得る利害関係の宣言を行い、かつ、そのような事項に関する討議及び議決への参加を控える。
3. ENISA は、ENISA の内部運営規則の中で、第 1 項及び第 2 項に示す利害関係の宣言に関する規定のための実務上の手配を定める。

第 26 条 透明性

1. ENISA は、高いレベルの透明性をもって、かつ、第 28 条に従い、ENISA の活動を実施する。
2. ENISA は、公衆及び利害関係者が、とりわけ、ENISA の仕事の結果に関し、適切であり、客観的であり、信頼性があり、かつ、容易にアクセス可能な情報の提供を受けることを確保する。ENISA は、第 25 条に従って行われる利害関係の宣言も公表する。
3. 運営会議は、長官からの提案に基づいて審議し、利害関係者が ENISA の活動中の幾つかの手続にオブザーバー参加することを承認できる。
4. ENISA は、ENISA の内部運営規則の中で、第 1 項及び第 2 項に示す透明性の規定を実装するための実務上の手配を定める。

第 27 条 秘密

1. 第 28 条を妨げることなく、ENISA は、秘密の取扱いを求める理由を付した要請と関係して ENISA が処理または受理する第三者の情報を外部に明かしてはならない。
2. 運営会議の構成員、長官、ENISA 諮問グループの構成員、アドホック作業グループに参加する外部専門家、及び、構成国から一時的に派遣される官吏を含む ENISA の職員は、その職務を終えた後においても、TFEU の第 339 条に基づく守秘義務を遵守する。
3. ENISA は、ENISA の内部運営規則の中で、第 1 項及び第 2 項に示す秘密の規定を実装するための実務上の手配を定める。
4. ENISA の職務の遂行のために要求されるときは、運営会議は、機密情報を ENISA が取り扱うことを許容する決定を行う。その場合において、ENISA は、欧州委員会の関連部署と合意した上で、委員会決定(EU, Euratom) 2015/443[26]及び委員会決定(EU, Euratom) 2015/444[27]に定める防護基本原則を適用する安全規則を採択する。その安全規則は、機密情報の交換、処理及び記録保

[26] 委員会の防護に関する 2015 年 3 月 13 日の委員会決定 (EU, Euratom) 2015/443（OJ L 72, 17.3.2015, p.41）
[27] EU 機密情報の防護規則に関する 2015 年 3 月 13 日の委員会決定 (EU, Euratom) 2015/444（OJ L 72, 17.3.2015, p.53）

存に関する条項を含める。

第 28 条 文書へのアクセス

1. 規則(EC) No 1049/2001 は、ENISA が保有する文書に適用される。
2. 運営会議は、2019 年 12 月 28 日までに、規則(EC) No 1049/2001 を実装するための覚書を採択する。
3. 規則(EC) No 1049/2001 の第 8 条に従って ENISA によって行われる決定は、TFEU の第 228 条に基づく欧州オンブズマンへの不服申立て、または、TFEU の第 263 条に基づく欧州連合司法裁判所における訴訟に服し得る。

第 IV 章 ENISA の予算の作成及び構成

第 29 条 ENISA の予算の作成

1. 長官は、毎年、翌会計年度のための ENISA の収入及び支出の見積書案を作成し、かつ、運営会議に対し、人員計画書案と共に、それを送付する。収入と支出は、均衡するものとする。
2. 運営会議は、毎年、その見積書案に基づき、翌会計年度のための ENISA の収入及び支出の見積書を作成する。
3. 運営会議は、毎年 1 月 31 日までに、欧州委員会及び第 42 条第 2 項に従って欧州連合が協定を締結した第三国に対し、見積書を送付し、その見積書は、単一計画書案の一部となる。
4. 欧州委員会は、その見積書に基づき、人員計画に関して欧州委員会が必要と判断する見積り、及び、一般予算にかかる補助金の額をその一般予算案の中に入れ、その一般予算は、TFEU の第 314 条に従い、欧州議会及び理事会に対して送付される。
5. 欧州議会及び理事会は、ENISA に対する欧州連合からの拠出金の配分を承認する。
6. 欧州議会及び理事会は、ENISA の人員計画を採択する。
7. 運営会議は、単一計画書と共に、ENISA の予算を採択する。ENISA の予算は、欧州連合の一般予算の最終的な採択の後に確定する。それが必要なときは、運営会議は、欧州連合の一般予算に従い、ENISA の予算及び単一計画書を補正する。

第 30 条 ENISA の予算の構成

1. 他の資金源を妨げることなく、ENISA の収入は、以下によって構成される：
   (a) 欧州連合の一般予算からの拠出金；
   (b) 第 32 条に示す ENISA の財務規則に従い、個別の支出事項に割当てられる収入；
   (c) 委任覚書の方式による欧州連合の基金、または、第 32 条に示す ENISA の財務規則及び欧州連合の政策を支える関連法律文書の条項によるアドホックな資金供与；
   (d) 第 42 条に示す ENISA の仕事に関与する第三国からの拠出金；
   (e) 金銭または物品による構成国からの任意の拠出。

   第 1 副項の(e)に基づき任意の拠出を提供する構成国は、その拠出をした結果として特定の権

利または役務を主張してはならない。

2. ENISA の支出は、職員、行政上の支援及び技術上の支援、インフラ及び業務遂行上の支出、並びに、第三者との間で締結した契約から生ずる支出を含める。

第 31 条 ENISA の予算の実行

1. 長官は、ENISA の予算の実行について職責を負う。
2. 欧州委員会の内部監査者は、ENISA に対し、欧州委員会の部署に対する権限と同じ権限を行使する。
3. ENISA の会計事務職員は、翌会計年（N+1 年）の 3 月 1 日までに、欧州委員会の会計事務職員及び欧州会計検査院に対し、当の会計年（N 年）の仮決算書を送付する。
4. 欧州議会及び理事会の規則(EU, Euroatom) 2018/1046[28]の第 246 条により、ENISA の仮決算書に関する欧州会計検査院の意見書を受理した後、ENISA の会計事務職員は、彼または彼女の責任において、ENISA の最終決算書を作成し、かつ、意見を得るため、運営会議に対してその最終決算書を提出する。
5. 運営会議は、ENISA の最終決算書に関する意見書を送付する。
6. 長官は、N＋1 年の 3 月 31 日までに、欧州議会、理事会、欧州委員会及び欧州会計検査院に対し、予算運営及び財務運営に関する報告書を送付する。
7. ENISA の会計事務職員は、N＋1 年の 7 月 1 日までに、欧州議会、理事会、欧州委員会の会計事務職員及び欧州会計検査院に対し、運営会議の意見書と共に、ENISA の最終決算書を送付する。
8. ENISA の会計事務職員は、ENISA の最終決算書の送付と同じ日に、欧州会計検査院に対し、欧州委員会の会計事務職員宛の宣誓書副本と共に、それらの最終決算書に適用される宣誓書も送付する。
9. 長官は、N+1 年の 11 月 15 日までに、EU 官報上において ENISA の最終決算書を公示する。
10. 長官は、N＋1 年の 9 月 30 日までに、欧州会計検査院に対し、欧州会計検査院の意見書に対する回答書を送付し、運営会議及び欧州委員会に対しても、その回答書の副本を送付する。
11. 長官は、規則(EU, Euroatom) 2018/1046 の第 261 条第 3 項に従い、欧州議会の要求に応じて、欧州議会に対し、関係する会計年度の年次免責手続の円滑な適用のために必要となる全ての情報を送付する。
12. 欧州議会は、理事会からの勧告に基づき、長官に対し、N＋2 年の 5 月 15 日よりも前に、N 年の予算の実行に関する年次免責を与える。

第 32 条 財務規則

ENISA に適用される財務規則は、欧州委員会との協議を経た上で、運営会議によって採択さ

[28] 欧州連合の一般予算に適用される財務規則に関する、規則(EU) No 1296/2013、規則(EU) No 1301/2013、規則(EU) No 1303/2013、規則(EU) No 1304/2013、規則(EU) No 1309/2013、規則(EU) No 1316/2013、規則(EU) No 223/2014、規則(EU) No 283/2014 及び決定 No 541/2014/EU を改正する、並びに、規則(EU, Euratom) No 966/2012 を廃止する欧州議会及び理事会の 2018 年 7 月 18 日の規則(EU, Euroatom) 2018/1046（OJ L 193, 30.7.2018, p.1）

れる。その財務規則は、そのような相違が ENISA の業務遂行のために必要であり、かつ、欧州委員会が事前にその同意を与えた場合を除き、委任規則(EU) 1271/2013 と相違するものであってはならない。

第 33 条 不正行為との闘い

1. 欧州議会及び理事会の規則(EC) 883/2013[29]に基づく詐欺、汚職及びそれ以外の違法行為との闘いを容易にするため、ENISA は、2019 年 12 月 28 日までに、欧州不正対策局（OLAF）による内部調査に関する欧州議会、欧州連合の理事会及び欧州共同体の委員会の間の 1999 年 5 月 25 日の機関間合意 [30]に加入する。ENISA は、同合意の別紙に定める雛形を用いて、ENISA の全ての従業者に適用される適切な条項を採択する。
2. 欧州会計検査院は、文書及び現場における検査に基づき、ENISA から欧州連合の資金提供を受けた全ての受益者、契約者及び再契約者に対する監査の権限をもつ。
3. OLAF は、ENISA からの資金供与または資金付けされる契約との関係において、欧州連合の財政上の利益を害する詐欺、汚職またはそれ以外の違法行為が存在するか否かを判断するため、規則(EU) No 883/2013 並びに理事会規則(Euratom, EC) No 2185/96[31]に定める条項及び手続に従い、現場における検査及び調査を含め、調査を実施できる。
4. 第 1 項、第 2 項及び第 3 項を妨げることなく、ENISA の、第三国及び国際機関との間の協力協定、契約、供与合意及び供与決定は、それらそれぞれの機関の職務権限に従い、そのような監査及び調査の実施を欧州会計検査院及び OLAF に対して明示で授権する条項を含める。

第Ⅴ章 職 員

第 34 条 総則的な条項

官吏の職員規則及びその他の公務員の雇用条件、並びに、官吏の職員規則及びその他の公務員の雇用条件を有効にするための欧州連合の機関間の合意によって採択された規則は、ENISA の職員に対して適用される。

第 35 条 特権及び免除

TEU 及び TFEU に附属する欧州連合の特権及び免除に関する議定書第 7 号は、ENISA 及びその職員に適用される。

---

[29] 欧州不正対策局（OLAF）によって実施される調査に関する、並びに、欧州議会及び理事会の規則（EC） No 1073/1999 及び理事会規則(Euratom) No 1074/1999 を廃止する欧州議会及び理事会の 2013 年 9 月 11 日の規則(EU, Euratom) No 883/2013（OJ L 248, 18.9.2013, p.1）

[30] OJ L 136, 31.5.1999, p.15.

[31] 欧州共同体の財政上の利益を詐欺及びその他の非違行為から保護するために欧州委員会によって実施される現場における検査及び調査に関する 1996 年 12 月 11 日の理事会規則(Euratom, EC) No 2185/96（OJ L 292, 15.11.1996, p. 2）

第 36 条 長官

1. 長官は、その他の公務員の雇用条件の第 2 条(a)に基づき、ENISA の臨時職員として業務に従事する。
2. 長官は、公開かつ透明性のある選考手続の後、欧州委員会から提案された候補者名簿の中から、運営会議によって任命される。
3. 長官との間の雇用契約を締結する目的のために、ENISA は、運営会議の議長によって代表される。
4. 任命の前に、運営会議によって選ばれた候補者は、欧州議会の関連委員会において陳述を行い、その構成員の質問に返答するために招請される。
5. 長官の任期は、5 年とする。欧州委員会は、長官の任期が満了するまでに、長官の職務遂行の評価、ENISA の将来の職務及び検討課題を考慮に入れる評価を実施する。
6. 運営会議は、第 18 条第 2 項に従い、長官の任命、任期の延長または解任に関する決定に至る。
7. 運営会議は、第 5 項に示す評価を考慮に入れる欧州委員会からの提案に基づいて審議し、5 年を超えない範囲で、長官の任期を 1 回だけ延長できる。
8. 運営会議は、欧州議会に対し、長官の任期を延長する運営会議の予定を通知する。そのような延長の前の 3 か月以内に、長官は、招請されたときは、欧州議会の関連委員会において陳述を行い、議会構成員の質問に返答する。
9. 任期が延長されなかった長官は、同じ職位のための別の選考手続に参加してはならない。
10. 長官は、欧州委員会からの提案に基づいて審議する運営会議の決定による場合においてのみ、解任され得る。

第 37 条 派遣される国内専門家及びそれ以外の職員

1. ENISA は、ENISA によって雇用された職員ではない、派遣された国内専門家またはそれ以外の職員を使用できる。官吏の職員規則及びその他の公務員の雇用条件は、そのような職員には適用されない。
2. 運営会議は、国内専門家の ENISA への派遣に関する規則を定める決定を採択する。

第 VI 章 ENISA に関する総則的な条項

第 38 条 ENISA の法的地位

1. ENISA は、欧州連合の組織であり、かつ、法人格をもつ。
2. 各構成国において、ENISA は、国内法に基づき法人に対して与えられる最大限の法的能力を享受する。ENISA は、とりわけ、動産及び不動産を獲得または処分し、訴訟手続の当事者となることができる。
3. ENISA は、その長官によって代表される。

第 39 条 ENISA の法的責任

1. ENISA の契約上の法的責任は、当の契約に適用される法律によって規律される。
2. 欧州司法裁判所は、ENISA によって締結された契約中に含まれている仲裁条項による判断を与える管轄権をもつ。
3. 非契約上の法的責任の場合、ENISA は、構成国の法律に共通の一般原則に従い、その職務の遂行において ENISA またはその職員によって生じた損害を弁償する。
4. 欧州司法裁判所は、第 3 項に示す損害の弁償と関連する紛争の管轄権をもつ。
5. ENISA に対するその職員個人の法的責任は、ENISA の職員に適用される関連条件によって規律される。

第 40 条 言語の手配

1. 理事会規則第 1 号[32]は、ENISA に適用される。構成国、及び、構成国によって指定されたその他の組織は、その構成国が選択する欧州連合の機関の公用語により、ENISA に対して送信し、返信を受けることができる。
2. ENISA の稼働のために必要な翻訳サービスは、欧州連合の組織のための翻訳センターから提供される。

第 41 条 個人データの保護

1. ENISA による個人データの処理は、規則(EU) 2018/1725 に服する。
2. 運営会議は、規則(EU) 2018/1725 の第 45 条第 3 項に示す実装規定を採択する。運営会議は、ENISA による規則(EU) 2018/1725 の適用のために必要となる追加措置を採択できる。

第 42 条 第三国及び国際機関との協力

1. この規則に定める目的を達成するために必要な範囲内において、ENISA は、第三国の職務権限を有する機関もしくは国際機関またはそれら両者と協力できる。その目的のために、ENISA は、欧州委員会の事前承認により、第三国の機関及び国際機関との間で業務協定を締結できる。これらの業務協定は、欧州連合及びその構成国に対して課せられる法的義務をつくり出してはならない。
2. ENISA は、その点に関して欧州連合との間で協定を締結した第三国の参加に対し、開かれている。そのような協定の関連条項に基づき、協定は、とりわけ、それらの第三国の ENISA の仕事への関与の性質、範囲及び態様を定め、かつ、ENISA によって実施される取り組みへの参加、資金拠出及び職員と関連する条項を含む業務協定が締結される。職員と関連する事項に関し、それらの業務協定は、いかなる場合においても、官吏の職員規則及びその他の公務員の雇用条件を遵守する。

[32] 欧州経済共同体によって使用される言語を決定する理事会規則第 1 号（OJ 17, 6.10.1958, p.385/58）.

3. 運営会議は、ENISA が職務権限を有する事項に関し、第三国または国際機関との関係に関する戦略を採択する。欧州委員会は、長官との間で適切な作業覚書を締結することにより、ENISA の任務の範囲内において、かつ、既存の機関の枠組み内において、ENISA が業務遂行することを確保する。

第 43 条 機微の非機密情報及び機密情報の防護に関する安全規則

欧州委員会との協議を経た上で、ENISA は、決定(EU, Euratom) 2015/443 及び決定(EU, Euratom) 2015/444 に定めるとおり、機微の非機密情報及び EUCI に関する欧州委員会の安全規則に含まれる防護の基本原則を適用する安全規則を採択する。ENISA の安全規則は、そのような情報の交換、処理及び記録保存に関する条項を含める。

第 44 条 本拠地協定及び業務遂行条件

1. ホスト構成国において ENISA に対して提供される便宜、ホスト構成国内において適用される個別の法令と共に当該構成国によって長官、運営会議の構成員、ENISA の職員及びその家族に対して利用できるようにされる施設に関する必要な手配は、運営会議の承認を得た上で締結される ENISA とホスト構成国との間の本拠地協定の中で定められる。
2. ENISA のホスト構成国は、その場所へのアクセシビリティ、職員の子どものための適切な教育施設の存在、労働市場への適切なアクセス、職員の子ども及び配偶者の両者のための社会保険及び医療を考慮に入れた上で、ENISA の適正な稼働を確保するための可能な最善の条件を提供する。

第 45 条 行政上の監督

ENISA の業務遂行は、TFEU の第 228 条に従い、欧州オンブズマンによる監督を受ける。

第 III 款 サイバーセキュリティ認証枠組み

第 46 条 欧州サイバーセキュリティ認証枠組み

1. ICT 製品、ICT サービス及び ICT プロセスのためのデジタル単一市場をつくり出すという観点から、欧州連合内のサイバーセキュリティのレベルを向上させることより、域内市場の稼働のための条件を向上させ、また、欧州サイバーセキュリティ認証制度への欧州連合レベルの整合化されたアプローチを可能とするため、欧州サイバーセキュリティ認証枠組みが設けられる。
2. 欧州サイバーセキュリティ認証枠組みは、欧州サイバーセキュリティ認証制度を構築するための仕組みを定め、並びに、記録保存されるデータ、送受信されるデータもしくは処理されるデータ、または、それらの製品、サービス及びプロセスによって提供され、もしくは、それらを介してアクセス可能な機能もしくはサービスの可用性、真正性、完全性もしくは機密性をそれらのライフサイクルを通じて保護する目的のため、そのような制度に従って評価を受けた ICT 製品、ICT サー

ビス及び ICT プロセスが、指定されたセキュリティ上の要求事項を遵守していることをテストするための仕組みを定める。

第 47 条 欧州サイバーセキュリティ認証のための欧州連合導入作業計画

1. 欧州委員会は、将来の欧州サイバーセキュリティ認証制度のための優先順位を定める欧州サイバーセキュリティ認証に関する欧州連合導入作業計画（「欧州連合導入作業計画」）を公表する。
2. 欧州連合導入作業計画は、とりわけ、欧州サイバーセキュリティ認証制度の適用範囲内にあるものに含められることから利益を享受する ICT 製品、ICT サービス及び ICT プロセスまたはそれらの類型の一覧を含める。
3. 欧州連合導入作業計画の中に ICT 製品、ICT サービス及び ICT プロセスまたはそれらの類型を含めることは、以下の 1 または複数の基準を基礎として正当化される：
   (a) 特定の類型の ICT 製品、ICT サービスまたは ICT プロセスに適用され、かつ、とりわけ、断片化のリスクに関し、国内サイバーセキュリティ制度の可用性及び発展；
   (b) 欧州連合または構成国の関連する法律または政策；
   (c) 市場の需要；
   (d) サイバー脅威の状況における変化を確認すること；
   (e) ECCG からの特定の制度候補の準備の要請。
4. 欧州委員会は、欧州連合導入作業計画案に関する ECCG 及び利害関係者認証グループから発される意見書を適正に考慮に入れる。
5. 最初の欧州連合導入作業計画は、2020 年 6 月 20 日までに公表される。欧州連合導入作業計画は、少なくとも 3 年に 1 度アップデートされ、かつ、必要に応じて、より頻回にアップデートされる。

第 48 条 欧州サイバーセキュリティ認証制度に関する要請

1. 欧州委員会は、ENISA に対し、欧州連合導入作業計画を基礎とする制度候補を準備すること、または、欧州連合導入作業計画を基礎とする既存の欧州サイバーセキュリティ認証制度を見直すことを要請できる。
2. 適正に正当化される場合において、欧州委員会または ECCG は、ENISA に対し、欧州連合導入作業計画に含まれていない制度候補を準備すること、または、欧州連合導入作業計画に含まれていない既存の欧州サイバーセキュリティ認証制度を見直すことを要請できる。欧州連合導入作業計画は、しかるべくアップデートされる。

第 49 条 欧州サイバーセキュリティ認証制度の準備、採択及び見直し

1. 第 48 条による欧州委員会からの要請を受けた後、ENISA は、第 51 条、第 52 条及び第 54 条に定める要求仕様に適合する制度候補を準備する。
2. 第 48 条第 2 項による ECCG からの要請を受けた後、ENISA は、第 51 条、第 52 条及び第 54 条に定める要求仕様に適合する制度候補を準備できる。ENISA がそのような要請を拒否する場

合、ENISA は、その拒否の理由を与える。そのような要請を拒否するための全ての決定は、運営会議によって行われる。

3. 制度候補を準備する際、ENISA は、公式の、オープンで、透明性があり、かつ、包摂的なコンサルテーションプロセスにより、関連する全ての利害関係者と協議する。

4. 個々の制度候補に関し、ENISA は、ENISA に対して個別の助言及び専門知識を提供する目的のために、第 20 条第 4 項に従い、アドホックな作業グループを設ける。

5. ENISA は、ECCG と緊密に協力する。ECCG は、ENISA に対し、制度候補の準備と関係する補佐及び専門家の助言を提供し、かつ、制度候補に関する意見書を採択する。

6. ENISA は、第 3 項、第 4 項及び第 5 項に従って準備された制度候補を欧州委員会に対して送付する前に、ECCG の意見書を最大限考慮に入れる。ECCG の意見書は、ENISA を拘束してはならず、また、そのような意見書が欠けていることは、ENISA が欧州委員会に対して制度候補を送付することの妨げとしてはならない。

7. 欧州委員会は、ENISA によって準備された制度候補を基礎として、第 51 条、第 52 条及び第 54 条に定める要求事項に適合する ICT 製品、ICT サービス及び ICT プロセスのための欧州サイバーセキュリティ認証制度を定める実装行為を採択できる。これらの実装行為は、第 66 条第 2 項に示す審議手続に従い、採択される。

8. ENISA は、少なくとも 5 年毎に、利害関係者から受け取ったフィードバックを考慮に入れた上で、採択された個々の欧州サイバーセキュリティ認証制度を評価する。必要があるときは、欧州委員会または ECCG は、ENISA に対し、第 48 条及び本条に従い、改訂版の制度候補を策定する過程を開始することを要請できる。

第 50 条 欧州サイバーセキュリティ認証制度の Web サイト

1. ENISA は、有効ではなくなった欧州サイバーセキュリティ認証制度、取消されて失効した欧州サイバーセキュリティ証明書及び EU 適合性宣言書、並びに、第 55 条に従って提供されるサイバーセキュリティ情報へのリンクのリポジトリと関連する情報を含め、欧州サイバーセキュリティ認証制度、欧州サイバーセキュリティ証明書及び EU 適合性宣言書に関する情報を提供し、公表する専用の Web サイトを維持管理する。

2. それが適切なときは、第 1 項に示す Web サイトは、欧州サイバーセキュリティ認証制度によって置き換えられた国内サイバーセキュリティ認証制度も示す。

第 51 条 欧州サイバーセキュリティ認証制度のセキュリティ上の目的

欧州サイバーセキュリティ認証制度は、少なくとも以下のセキュリティ上の諸目的を適用可能な限り達成するように設計される：

(a) ICT 製品、ICT サービスまたは ICT プロセスの全ライフサイクルを通じて、事故によるまたは無権限の記録保存、処理、アクセスまたは開示に対し、記録保存され、送受信され、または、それら以外の処理をされるデータを防護すること；

(b) ICT 製品、ICT サービスまたは ICT プロセスの全ライフサイクルを通じて、事故によるまたは無権限の破壊、喪失もしくは改変または可用性の欠如に対し、記録保存され、送受信され、

または、それら以外の処理をされるデータを防護すること;

(c) 承認を受けた者、プログラムまたは機械装置のみが、それらのアクセス権が示すデータ、サービスまたは機能に対してアクセス可能であること;

(d) 既知の依存関係及び脆弱性を特定し、文書化すること;

(e) どのデータ、サービスまたは機能がアクセスされたか、使用されたか、または、それら以外の処理をされたか、いつ、及び、誰によってであるかを記録すること;

(f) どのデータ、サービスまたは機能がアクセスされたか、使用されたか、または、それら以外の処理をされたか、いつ、及び、誰によってであるかを点検可能であること;

(g) ICT 製品、ICT サービス及び ICT プロセスが既知の脆弱性を含んでいないこと;

(h) 物理的なインシデントまたは技術上のインシデントの場合において、適時の態様で、データ、サービス及び機能の可用性及びそれらへのアクセスが修復されること;

(i) ICT 製品、ICT サービス及び ICT プロセスが、バイデフォルト及びバイデザインで安全であること;

(j) ICT 製品、ICT サービス及び ICT プロセスが、周知の脆弱性を含んでいないアップデートされたソフトウェア及びハードウェアによって提供され、かつ、安全にアップデートする仕組みが提供されること。

第 52 条 欧州サイバーセキュリティ認証制度の保証レベル

1. 欧州サイバーセキュリティ認証制度は、ICT 製品、ICT サービス及び ICT プロセスに関し、以下の 1 または複数の保証レベルを指定できる:すなわち、「基本」、「標準」または「高度」である。保証レベルは、インシデントの蓋然性及び影響の面において、ICT 製品、ICT サービスまたは ICT プロセスの予定された使用と関係するリスクのレベルに見合うものとする。

2. 欧州サイバーセキュリティ証明書及び EU 適合性宣言書は、その欧州サイバーセキュリティ証明書または EU 適合性宣言書が発行された欧州サイバーセキュリティ認証制度の中で指示される保証レベルを示す。

3. 対応する安全機能、並びに、ICT 製品、ICT サービスまたは ICT プロセスが受けるべき評価の厳格さ及び深さは、各保証レベルに対応するセキュリティ上の要求事項は、関連する欧州サイバーセキュリティ認証制度の中で定められる。

4. 証明書または EU 適合性証明書は、目的がサイバーセキュリティインシデントのリスクを軽減し、または、それを防止することにある技術的管理策を含め、技術仕様、標準およびそれらと関連する手続を示す。

5. 「基本」レベルの保証を示す欧州サイバーセキュリティ証明書または EU 適合性宣言書は、当該証明書または当該 EU 適合性宣言書が発行された ICT 製品、ICT サービス及び ICT プロセスが、安全機能を含め、対応するセキュリティ上の要求事項に適合すること、並びに、それらの ICT 製品、ICT サービス及び ICT プロセスが、インシデント及びサイバー攻撃の既知の基本的なリスクをミニマム化することを意図するレベルにあると評価されたことの保証を提供する。実施されるべき評価活動は、少なくとも、技術文書の評価を含める。そのような評価が適切ではない場合、それと均等の効果をもつ代替的な評価活動が実施される。

6. 「標準」レベルの保証を示す欧州サイバーセキュリティ証明書は、当該証明書が発行された

ICT 製品、ICT サービス及び ICT プロセスが、安全機能を含め、対応するセキュリティ上の要求事項に適合すること、並びに、それらの ICT 製品、ICT サービス及び ICT プロセスが、既知のサイバーセキュリティ上のリスク、並びに、限定された技能及び資源をもつ行為者によって実行されるインシデント及びサイバー攻撃のリスクをミニマム化することを意図するレベルにあると評価されたことの保証を提供する。実施されるべき評価活動は、少なくとも以下のものを含める：すなわち、周知の脆弱性が存在しないことの証明を評価すること；その ICT 製品、ICT サービスまたは ICT プロセスが、必要な安全機能を正しく実装していることをテストし、説明すること。そのような評価が適切ではない場合、それと均等の効果をもつ代替的な評価活動が実施される。

7. 「高度」レベルの保証を示す欧州サイバーセキュリティ証明書は、当該証明書が発行された ICT 製品、ICT サービス及び ICT プロセスが、安全機能を含め、対応するセキュリティ上の要求事項に適合すること、並びに、それらの ICT 製品、ICT サービス及び ICT プロセスが、十分な技能及び資源をもつ行為者によって実行される最新のサイバー攻撃のリスクをミニマム化することを意図するレベルにあると評価されたことの保証を提供する。実施されるべき評価活動は、少なくとも以下のものを含める：すなわち、周知の脆弱性が存在しないことの証明を評価すること；その ICT 製品、ICT サービスまたは ICT プロセスが、最新の安全機能を正しく実装していることをテストし、説明すること；並びに、侵入テストを用い、高度な技能をもつ攻撃者に対するそれらの耐久性を評価すること。そのような評価が適切ではない場合、それと均等の効果をもつ代替的な評価活動が実施される。

8. 欧州サイバーセキュリティ認証制度は、使用される評価手法の厳格さ及び深さによって異なる複数の評価レベルを示し得る。それぞれの評価レベルは、保証レベルのいずれかに対応するものとし、かつ、保証内容の適切な組み合わせによって定義されるものとする。

第 53 条　自己適合性評価

1. 欧州サイバーセキュリティ認証制度は、その ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダのみの責任の下にある自己適合性評価を許容し得る。自己適合性評価は、保証レベル「基本」に対応する程度のリスクを示す ICT 製品、ICT サービス及び ICT プロセスとの関係においてのみ、許容される。

2. ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダは、その制度の中で定められた要求事項を満たすことが証明された旨の EU 適合性宣言書を発行できる。そのような宣言書の発行により、その ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダは、その ICT 製品、ICT サービスまたは ICT プロセスが当該制度に定める要求事項を遵守するものであることについての責任を保証する。

3. その ICT 製品または ICT サービスの製造者またはプロバイダは、対応する欧州サイバーセキュリティ認証制度の中に定められている期間内、第 58 条に示す国内サイバーセキュリティ認証機関に対し、その EU 適合性宣言書、技術文書、及び、その ICT 製品、ICT サービスまたは ICT プロセスがその制度の適合性と関連する他の全ての関連情報を利用できるようにする。国内サイバーセキュリティ認証機関及び ENISA に対し、その EU 適合性宣言書の副本が送付される。

4. EU 適合性宣言書の発行は、欧州連合法または構成国法の中で別異に定める場合を除き、任意のものとする。

5. EU 適合性宣言書は、全ての構成国において承認される。

第 54 条 欧州サイバーセキュリティ認証制度の構成要素

1. 欧州サイバーセキュリティ認証制度は、少なくとも、以下の諸構成要素を含める：
   (a) 適用対象となる ICT 製品、ICT サービス及び ICT プロセスのタイプまたは類型を含め、認証制度の対象事項及び適用範囲；
   (b) 制度の目的、並びに、選択された標準、評価手法及び保証レベルがその制度の利用予定者の需要にどのように対応するかについての明確な記述；
   (c) 評価に適用される国際標準、欧州標準または国内標準の参照、または、そのような標準が利用できない場合もしくは不適切な場合、規則(EU) No 1025/2012 の別紙 II に定める要求事項に適合する技術仕様の参照、または、そのような仕様が利用できない場合、欧州サイバーセキュリティ認証制度の中に定める技術仕様もしくはそれ以外のサイバーセキュリティ上の要求事項の参照；
   (d) 該当するときは、1 または複数の保証レベル；
   (e) その制度の下において自己適合性評価が許容されるか否かの表示；
   (f) 該当するときは、サイバーセキュリティ上の要求事項を評価する彼らの技術上の能力を保証するために適合性評価機関が服する特定の要求事項または追加的な要求事項；
   (g) 評価のタイプを含め、第 51 条に示すセキュリティ上の目的が達成されることを説明するために使用される個別の評価基準及び評価手法；
   (h) 該当するときは、証明のために必要であり、かつ、申請者から適合性評価機関に対して供給されなければならず、または、それ以外に利用できるようにされなければならない情報；
   (i) 制度がマークまたはラベルを定める場合、そのようなマークまたはラベルを使用し得るための条件；
   (j) サイバーセキュリティ上の個別の要求事項の継続的な遵守を説明するための仕組みを含め、ICT 製品、ICT サービス及び ICT プロセスが欧州サイバーセキュリティ証明書または EU 適合性宣言書の要求事項を遵守していることを監視するための規定；
   (k) 該当するときは、欧州サイバーセキュリティ証明書を発行し、維持し、継続し、更新し、並びに、証明書の適用範囲を拡張または削減するための条件；
   (l) 認証され、または、EU 適合性宣言書が発行されたが、その制度の要求事項を遵守していない ICT 製品、ICT サービス及び ICT プロセスの帰趨に関する規定；
   (m) ICT 製品、ICT サービス及び ICT プロセス中の事前に検出されなかったサイバーセキュリティ上の脆弱性がどのように報告され、また、取り扱われるかに関する規定；
   (n) 該当するときは、適合性評価機関による記録の保持に関する規定；
   (o) 同じタイプまたは類型の ICT 製品、ICT サービス及び ICT プロセスに適用される国内サイバーセキュリティ認証制度または国際サイバーセキュリティ認証制度の識別名、セキュリティ上の要求事項、評価基準及び評価手法並びに保証レベル；
   (p) 発行される欧州サイバーセキュリティ証明書及び EU 適合性宣言書の内容及びフォーマット；
   (q) ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダによって利用できる

ようにされる EU 適合性宣言書、技術文書及びそれ以外の全ての関連情報を利用できる期間;

(r) その制度に基づいて発行される欧州サイバーセキュリティ証明書の最長有効期間;

(s) その制度に基づいて発行され、修正され、または、取消された欧州サイバーセキュリティ証明書の開示の基本方針;

(t) 認証制度の第三国との間における相互承認の条件;

(u) 該当するときは、第 56 条第 6 項により保証レベル「高度」の欧州サイバーセキュリティ証明書を発行する機関または組織のための制度によって設けられる相互評価の仕組みに関する規定。そのような仕組みは、第 59 条に定める相互評価を妨げてはならない;

(v) 第 55 条に従って補足的なサイバーセキュリティ情報の供給及びアップデートにおいて、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダが服するフォーマット及び手続。

2. 欧州サイバーセキュリティ認証制度の個々の要件は、適用可能な法律上の要件、とりわけ、欧州連合の整合化された立法から生ずる要件と一貫性のあるものでなければならない。

3. 欧州連合の特定の法令がそのように定める場合、欧州サイバーセキュリティ認証制度の下で発行される証明書または EU 適合性宣言書は、当該法律上の要件を満たしていることの推定を説明するために使用され得る。

4. 欧州連合の整合化された立法が存在しない場合、構成国法は、欧州サイバーセキュリティ認証制度が、法律上の要件を満たしていることの推定を説明するために使用され得ることを定めることができる。

第 55 条 認証された ICT 製品、ICT サービス及び ICT プロセスに関する補足的なサイバーセキュリティ情報

1. 認証を受けた ICT 製品、ICT サービスもしくは ICT プロセスの製造者もしくはプロバイダ、または、EU 適合性宣言書が発行された ICT 製品、ICT サービス及び ICT プロセスの製造者もしくはプロバイダは、以下の補足的なサイバーセキュリティ情報を公衆が利用できるようにする:

(a) その ICT 製品または ICT サービスの安全な設定、インストール、設置、運用及び維持管理について、エンドユーザを補助するための案内及び推奨事項;

(b) とりわけ、サイバーセキュリティと関係するアップデートの可用性に関し、エンドユーザに対してセキュリティサポートが提供される期間;

(c) その製造者またはプロバイダの連絡先情報、並びに、エンドユーザ及びセキュリティリサーチャーから脆弱性情報を受け取るための承認された手法;

(d) その ICT 製品、ICT サービスまたは ICT プロセスと関連する公衆に開示された脆弱性を列挙するオンラインリポジトリの参照、並びに、関連するサイバーセキュリティアドバイザリの参照。

2. 第 1 項に示す情報は、電子的な方式によって利用できるものとし、かつ、少なくとも、対応する欧州サイバーセキュリティ証明書または EU 適合性宣言書が失効するまでは使用でき、かつ、必要に応じてアップデートされるものとする。

第 56 条 サイバーセキュリティ証明書

1. 第 49 条により採択される欧州サイバーセキュリティ認証制度に基づいて認証された ICT 製品、ICT サービス及び ICT プロセスは、その制度の要求事項に適合するものであると推定される。
2. サイバーセキュリティ認証は、欧州連合法または構成国法の中で別異に定められている場合を除き、任意のものとする。
3. 欧州委員会は、採択された欧州サイバーセキュリティ認証制度の効率性及び利用を評価し、また、欧州連合内の ICT 製品、ICT サービス及び ICT プロセスの十分なレベルのサイバーセキュリティを確保し、域内市場の稼働を向上させるため、関連する欧州連合法を通じて、特定の欧州サイバーセキュリティ制度が義務的なものとされなければならないか否かを継続的に評価する。そのような最初の評価は、2023 年 12 月 31 日までに実施され、かつ、その後の評価は、その後、少なくとも 2 年毎に実施される。それらの評価結果を基礎として、欧州委員会は、義務的な認証制度に含められるべき既存の認証制度の適用を受ける ICT 製品、ICT サービス及び ICT プロセスを特定する。

   優先順位にそって、欧州委員会は、指令（EU）2016/1148 の別紙 II に列挙される部門を重点化し、少なくとも最初の欧州サイバーセキュリティ認証制度の採択から 2 年後に評価されるものとする。

   その評価を準備する際、欧州委員会は：

   (a) ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダに対する措置の影響、及び、それらの措置の費用の面における利用者に対する措置の影響、並びに、対象とされる ICT 製品、ICT サービスまたは ICT プロセスの所期の拡大された安全性レベルから生ずる社会的利益または経済的利益を考慮に入れ；
   (b) 関連する構成国法及び第三国法の存在及び実装を考慮に入れ；
   (c) 全ての関連利害関係者及び構成国とのオープンで、透明性があり、かつ、包摂的なコンサルテーションプロセスを実施し；
   (d) とりわけ、SME を含め、ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダに対してあり得る措置の影響との関係において、実装の期限、移行措置及び移行期間を考慮に入れ；
   (e) 任意的な制度から義務的な制度へ移行する上で最も迅速かつ効率的な方法が実装されるべきことを提案する。
4. 第 60 条に示す適合性評価機関は、第 49 条に従い欧州委員会によって採択される欧州サイバーセキュリティ認証制度の中に含められる基準を基礎として、「基本」または「標準」の保証レベルを示し、本条による欧州サイバーセキュリティ証明書を発行する。
5. 適正に正当化される場合において、第 4 項からの特例により、欧州サイバーセキュリティ制度は、公的機関のみから当該制度から生ずる欧州サイバーセキュリティ証明書が発行され得ることを定めることができる。そのような公的機関は、以下のいずれかとする：
   (a) 第 58 条第 1 項に示す国内サイバーセキュリティ認証機関；または、
   (b) 第 60 条第 1 項により、適合性評価機関として認定される公的組織。
6. 第 49 条によって採択された欧州サイバーセキュリティ制度が「高度」の保証レベルを要求するときは、同制度に基づく欧州サイバーセキュリティ証明書は、国内サイバーセキュリティ認証機関

によってのみ、または、以下の場合においては、適合性評価機関によって、発行されなければならない:

(a) 適合性評価機関から発行される個々の欧州サイバーセキュリティ証明書に関し、国内サイバーセキュリティ認証機関からの事前の承認に基づく場合;または、

(b) そのような欧州サイバーセキュリティ証明書を発行する職務の適合性評価機関に対する国内サイバーセキュリティ認証機関からの一般的な委任に基づく場合。

7. ICT 製品、ICT サービスまたは ICT プロセスの認証を申請する自然人または法人は、当該機関が欧州サイバーセキュリティ証明書を発行する機関である場合、第 58 条に示す国内サイバーセキュリティ認証機関に対し、または、第 60 条に示す適合性評価機関に対し、その認証を行うために必要となる全ての情報を利用できるようにする。

8. 欧州サイバーセキュリティ証明書保有者は、第 7 項に示す機関または組織に対し、認証を受けた ICT 製品、ICT サービスまたは ICT プロセスに関して事後的に検知された脆弱性または不規則性であって、その認証と関連する要求事項の遵守に影響をもち得るものを通知する。当該機関または組織は、不適切な遅滞なく、関係する国内サイバーセキュリティ認証機関に対し、その情報を転送する。

9. 欧州サイバーセキュリティ証明書は、その欧州サイバーセキュリティ認証制度の中で定められた期間で発行され、また、関連する要求事項に適合し続けている限り、更新され得る。

10. 本条により発行される欧州サイバーセキュリティ証明書は、全ての構成国において承認される。

第 57 条 国内サイバーセキュリティ認証制度及び証明書

1. 本条第 3 項を妨げることなく、国内サイバーセキュリティ認証制度、並びに、欧州サイバーセキュリティ認証制度の適用のある ICT 製品、ICT サービス及び ICT プロセスに関する関連手続は、第 49 条第 7 項により採択される実装行為の中で定められる日にその効力を終了させる。欧州サイバーセキュリティ認証制度の適用のない ICT 製品、ICT サービス及び ICT プロセスに関する国内サイバーセキュリティ認証制度及び関連手続は、存続する。

2. 構成国は、有効な欧州サイバーセキュリティ認証制度が既に適用されている ICT 製品、ICT サービス及び ICT プロセスに関し、新たな国内サイバーセキュリティ認証制度を導入してはならない。

3. 国内サイバーセキュリティ認証制度に基づいて発行され、かつ、欧州サイバーセキュリティ認証制度の適用のある既存の証明書は、その期間が満了する日まで、その有効性を維持する。

4. 域内市場の断片化を避けるため、構成国は、欧州委員会及び ECCG に対し、新たな国内サイバーセキュリティ認証制度の策定予定を通知する。

第 58 条 国内サイバーセキュリティ認証機関

1. 各構成国は、その構成国の領土内の 1 もしくは複数の国内サイバーセキュリティ認証機関を指定し、または、別の構成国との合意により、指定元構成国における監督の職務について職責を負う当該別の構成国内の 1 もしくは複数の国内サイバーセキュリティ認証機関を指定する。

2. 各構成国は、欧州委員会に対し、指定された国内サイバーセキュリティ認証機関の識別名を通

知する。構成国が複数の国内サイバーセキュリティ認証機関を指定する場合、その構成国は、欧州委員会に対し、それらの個々の機関に割当てた職務に関しても通知する。

3. 第 56 条第 5 項(a)及び第 56 条第 6 項を妨げることなく、各国内サイバーセキュリティ認証機関は、その組織構成、資金の決定、法的構成及び意思決定において、それらの機関が監督する組織から独立であるものとする。

4. 構成国は、第 56 条第 5 項(a)及び第 56 条第 6 項に示す欧州サイバーセキュリティ証明書の発行と関係する国内サイバーセキュリティ認証機関の活動が、本条に定めるそれらの機関の監督活動と厳格に区分されていること、及び、それらの機関の活動が相互に独立して実施されることを確保する。

5. 構成国は、国内サイバーセキュリティ認証機関が、その権限を行使するために十分な資源をもつこと、及び、実効的かつ効率的な態様でその職務を実施することを確保する。

6. この規則の実効的な実装のため、国内サイバーセキュリティ認証機関が、積極的であり、実効的であり、効率的であり、かつ、安全な態様で、ECCG に参加することが適切である。

7. 国内サイバーセキュリティ認証機関は:

(a) 他の関連する市場調査機関と協力して、ICT 製品、ICT サービス及び ICT プロセスが、それらの機関それぞれの領土内で発行された欧州サイバーセキュリティ証明書の要求事項を遵守することを監視するため、第 54 条(j)による欧州サイバーセキュリティ認証制度の中に含まれる規定を監督及び執行し;

(b) それらの機関それぞれの領土内に設けられており、かつ、自己適合性評価を実施する ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダの義務の遵守及び執行を監視し、かつ、とりわけ、第 53 条第 2 項及び第 3 項並びに対応する欧州サイバーセキュリティ認証制度に定めるそのような製造者またはプロバイダの義務の遵守を監視し、及び、執行し;

(c) 第 60 条第 3 項を妨げることなく、この規則の目的のために、適合性評価機関の活動の監視及び監督において、国内認定機関を積極的に補助及び支援し;

(d) 第 56 条第 5 項に示す公的機関の活動を監視及び監督し;

(e) 該当するときは、第 60 条第 3 項に従い、適合性評価機関を承認し、また、適合性評価機関がこの規則の要件に違反する場合、既存の承認を制限し、停止し、または、取消し;

(f) 国内サイバーセキュリティ認証機関から発行された欧州サイバーセキュリティ証明書との関係において、第 56 条第 6 項により適合性評価機関から発行された欧州サイバーセキュリティ証明書との関係において、または、第 53 条に基づいて発行された EU 適合性宣言書との関係において、自然人または法人からの異議を取扱い、かつ、適切な範囲内で、そのような異議の対象事項を調査し、かつ、合理的な期間内に、その異議申立人に対し、その調査の進捗状況及びその結果を通知し;

(g) ENISA 及び ECCG に対し、本項の(b)、(c)及び(d)または第 8 項に基づいて行われた活動に関する年次の要旨報告書を提供し;

(h) ICT 製品、ICT サービス及び ICT プロセスの、この規則の要求事項または特定の欧州サイバーセキュリティ認証制度の要求事項の可能的な不遵守に関して情報交換することによる場合を含め、別の国内サイバーセキュリティ認証機関またはそれ以外の行政機関と協力し;並びに、

(i) サイバーセキュリティ認証の分野における関連する発展を監視する。

8. 各国内サイバーセキュリティ認証機関は、少なくとも、以下の権限をもつ：

(a) 適合性評価機関、欧州サイバーセキュリティ証明書保有者及び EU 適合性宣言書の発行者に対し、その職務の遂行のために必要となる全ての情報の提供を要求すること；

(b) 本款の遵守を確認する目的のために、監査の方式により、適合性評価機関、欧州サイバーセキュリティ証明書保有者及び EU 適合性宣言書の発行者の調査を実施すること；

(c) 適合性評価機関、欧州サイバーセキュリティ証明書保有者及び EU 適合性宣言書の発行者が、この規則の遵守及び欧州サイバーセキュリティ認証制度を遵守することを確保するため、国内法に従い、適切な措置を講ずること；

(d) 欧州連合の手続法または構成国の手続法に従って調査を実施する目的のために、適合性評価機関及び欧州サイバーセキュリティ証明書保有者の施設へのアクセスを獲得すること；

(e) そのような証明書がこの規則または欧州サイバーセキュリティ認証制度を遵守していない場合、国内法に従い、国内サイバーセキュリティ認証機関から発行された欧州サイバーセキュリティ証明書または第 56 条第 6 項により適合性評価機関から発行された欧州サイバーセキュリティ証明書を取消すこと；

(f) 第 65 条に示すとおり、国内法に従って制裁を課すこと、及び、この規則に定める義務の違反を直ちに解消することを要求すること。

9. 国内サイバーセキュリティ認証機関は、とりわけ、サイバーセキュリティ認証並びに ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティと関係する技術的な問題と関連する情報、経験及びグッドプラクティスを交換することにより、互いに協力し、及び、欧州委員会と協力する。

第 59 条 相互評価

1. 欧州サイバーセキュリティ証明書及び EU 適合性宣言書に関し、欧州連合全域にわたる均等な基準を達成するため、国内サイバーセキュリティ認証機関は、相互評価に服する。

2. 相互評価は、とりわけ、構成上、人的資源上及び手続上の諸要件、機密性並びに異議申立てに関し、良好かつ透明性のある評価基準及び評価手続を基礎として、実施される。

3. 相互評価は、以下のことを評価する：

(a) 該当するときは、第 56 条第 5 項(a)及び第 56 条第 5 項に示す欧州サイバーセキュリティ証明書の発行と関係する国内サイバーセキュリティ認証機関の活動が、第 58 条に定めるそれらの機関の監督活動と厳格に区分されているかどうか、並びに、それらの活動が相互に独立して実施されているかどうか；

(b) ICT 製品、ICT サービス及び ICT プロセスが、第 58 条第 7 項(a)による欧州サイバーセキュリティ証明書を遵守していることの監督及びそれを監視するための規定の執行のための手続；

(c) 第 58 条第 7 項(b)による ICT 製品、ICT サービスまたは ICT プロセスの製造者またはプロバイダの義務の監視及び執行のための手続；

(d) 適合性評価機関の活動の監視、承認及び監督のための手続；

(e) 該当するときは、第 56 条第 6 項により「高度」の保証レベルの証明書を発行する機関または組織の職員が、適切な専門知識をもっているかどうか。

4. 相互評価は、少なくとも 2 つの別の構成国のサイバーセキュリティ認証機関及び欧州委員会によって実施され、かつ、少なくとも 5 年に 1 度実施される。ENISA は、相互評価に関与できる。
5. 欧州委員会は、少なくとも 5 年間適用される相互評価のための計画を策定し、相互評価チームの構成、相互評価において使用される手法、及び、それと関連するスケジュール、頻度及びそれら以外の職務に関する基準を定める実装行為を採択できる。それらの実装行為を採択する際、欧州委員会は、ECCG の見解を適正に考慮に入れる。それらの実装行為は、第 66 条第 2 項に示す審議手続に従って採択される。
6. 相互評価の結果は、ECCG によって検討され、ECCG は、公衆が利用できるようにされ得る要旨を作成し、また、それが必要なときは、関係する機関によって執られるべき行動または措置に関する運用指針または勧告を発する。

第 60 条 適合性評価機関

1. 適合性評価機関は、規則(EC) No 756/2008 により指定された国内認定機関によって認定される。そのような認定は、その適合性評価機関が、この規則の別紙に定める諸要件に適合する場合に限り、発行される。
2. 第 56 条第 5 項(a)及び第 56 条第 6 項により国内サイバーセキュリティ認証機関から欧州サイバーセキュリティ証明書が発行される場合、その国内サイバーセキュリティ認証機関の認証組織は、本条第 1 項による適合性評価機関として認定される。
3. 第 54 条第 1 項(f)により、欧州サイバーセキュリティ認証制度が、特別の要求事項または追加的な要求事項を定めているときは、それらの要求事項に適合する適合性評価機関のみが、国内サイバーセキュリティ認証機関から、その制度に基づく職務を遂行することの承認を受ける。
4. 第 1 項に示す認定は、適合性評価機関に対して最長 5 年の期間で発行され、かつ、その適合性評価機関が本条に定める要求事項に適合し続けている限り、同じ条件で更新され得る。認定の条件に該当しない場合、もしくは、該当しなくなった場合、または、適合性評価機関がこの規則に違反する場合、国内認定機関は、合理的な期間内に、第 1 項によって発された適合性評価機関の認定を制限し、停止し、または、取消すための全ての適切な措置を講ずる。

第 61 条 通知

1. 個々の欧州サイバーセキュリティ認証制度に関し、国内サイバーセキュリティ認証機関は、欧州委員会に対し、第 52 条に示す特定の保証レベルをもつ欧州サイバーセキュリティ証明書を発行するために既に認可された適合性評価機関、及び、該当するときは、第 60 条第 3 項により既に承認を受けた適合性評価機関を通知する。国内サイバーセキュリティ認証機関は、欧州委員会に対し、不適切な遅滞なく、その後の変更を通知する。
2. 欧州サイバーセキュリティ認証制度が発効した時から 1 年後、欧州委員会は、EU 官報上において、当該制度に基づいて通知を受けた適合性評価機関のリストを公表する。
3. 欧州委員会が、第 2 項に示す期間の経過後に通知を受領したときは、当該通知の受領の日から2か月以内に、EU 官報上において、通知を受けた適合性評価機関のリストの修正を公示する。

4. 国内サイバーセキュリティ認証機関は、欧州委員会に対し、第 2 項に示すリストから、当該機関から通知を受けた適合性評価機関を削除することの要請書を送付できる。欧州委員会は、その国内サイバーセキュリティ認証機関の要請書を受理した日から 1 か月以内に、EU 官報上において、当該リストの対応する修正を公示する。
5. 欧州委員会は、本条第 1 項に示す通知の状況、フォーマット及び手続を定める実装行為を採択できる。それらの実装行為は、第 66 条第 2 項に示す審議手続に従って採択される。

第 62 条 欧州サイバーセキュリティ認証グループ

1. 欧州サイバーセキュリティ認証グループ（「ECCG」）が設置される。
2. ECCG は、国内サイバーセキュリティ認証機関の代表またはそれ以外の関連国内機関の代表によって構成される。ECCG の構成員は、複数の構成国を代表してはならない。
3. 利害関係者及び第三者は、ECCG の会合に出席し、その仕事に関与することを招請され得る。
4. ECCG は、以下の職務をもつ：
   (a) とりわけ、欧州連合導入作業計画、サイバーセキュリティ認証政策上の問題、政策上のアプローチの調整、及び、欧州サイバーセキュリティ認証制度の準備に関し、本款の一貫性のある実装及び適用を確保する仕事において、欧州委員会に助言し、これを補助すること；
   (b) 第 49 条による制度候補の準備との関係において、ENISA を補助し、ENISA に助言し、及び、ENISA と協力すること；
   (c) 第 49 条により ENISA によって準備される制度候補に関する意見書を採択すること；
   (d) 第 48 条第 2 項により制度の候補を準備することを ENISA に対して要請すること；
   (e) 既存の欧州サイバーセキュリティ認証制度の維持及び見直しに関し、欧州委員会宛の意見書を採択すること；
   (f) サイバーセキュリティ認証の分野における関連する発展を検討すること、並びに、サイバーセキュリティ認証制度に関する情報及びグッドプラクティスを交換すること；
   (g) 能力開発及び情報交換を通じて、とりわけ、サイバーセキュリティ認証と関係する問題に関する効率的な情報交換のための手法を構築することにより、本款に基づく国内サイバーセキュリティ認証機関の間の協力を容易にすること；
   (h) 第 54 条(u)により欧州サイバーセキュリティ認証制度の中で定められる規定に従って相互評価の仕組みを実装することを支援すること；
   (i) 既存の欧州サイバーセキュリティ認証制度の見直しをすること、並びに、それが適切なときは、ENISA に対し、国際的に承認された利用可能な標準との不適合または乖離に対処するために関連する国際的な標準化機関と交渉することの勧告を行うことによる場合を含め、欧州サイバーセキュリティ認証制度を国際的に承認された標準に揃えることを容易にすること。
5. 欧州委員会は、ENISA の補助を得て、ECCG を主宰し、かつ、欧州委員会は、第 8 条第 1 項(e)に従い、ECCG に対して事務局を提供する。

第 63 条 異議申立ての権利

1. 自然人及び法人は、欧州サイバーセキュリティ証明書の発行者に対し、または、第56条第6項

に従って行動する場合において、適合性評価機関から発行される欧州サイバーセキュリティ証明書と関連する異議申立ての場合、関連する国内サイバーセキュリティ認証機関に対し、異議申立ての権利をもつ。

2. 異議申立てを受けた機関または組織は、その申立人に対し、手続の進捗状況及び行われた決定を通知し、かつ、申立人に対し、第 64 条に示す効果的な司法救済の権利を通知する。

第 64 条 効果的な司法救済の権利

1. 行政上の救済またはそれ以外の非司法救済を妨げることなく、自然人及び法人は、以下に関し、効果的な司法救済の権利をもつ:
   (a) 該当するときは、不適切な発行との関係において、不発行またはそれらの自然人及び法人によって保有される欧州サイバーセキュリティ証明書の不承認を含め、第 63 条第 1 項に示す機関または組織によって行われた決定;
   (b) 第 63 条第 1 項に示す機関または組織への異議申立てに関する不作為。
2. 本条による手続は、司法救済が求められている機関または組織が所在する構成国の裁判所において行われる。

第 65 条 制裁

構成国は、本款の違反行為及び欧州サイバーセキュリティ認証制度の違反行為に対して適用される制裁に関する規定を定め、それらの規定が実装されることを確保するために必要となる全ての措置を講ずる。定められる制裁は、効果的であり、比例的であり、かつ、抑止力のあるものとする。構成国は、遅滞なく、欧州委員会に対し、それらの規定及びそれらの措置を通知し、かつ、それらに影響を与えるその後の改正を通知する。

第 IV 款 最終規定

第 66 条 委員会の手続

1. 欧州委員会は、委員会から補助を受ける。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。
2. 本項が参照されるときは、規則(EU) No 182/2011 の第 5 条第 4 項(b)が適用される。

第 67 条 評価及び見直し

1. 欧州委員会は、2024 年 6 月 28 日までに、かつ、その後は 5 年毎に、ENISA 及びその実際の仕事の影響、実効性及び効率性、ENISA の任務を修正する必要性の有無、並びに、そのような修正の財政上の影響の評価を実施する。その評価は、ENISA の活動に対する応答として ENISA に対して行われたフィードバックを考慮に入れる。ENISA に与えられた目的、任務及び職務に照らし、ENISA の業務遂行を継続することが正当化されなくなったと欧州委員会が判断する場合、

欧州委員会は、ENISA と関連する条項に関してこの規則が改正されることを提案できる。

2. その評価は、欧州連合内における ICT 製品、ICT サービス及び ICT プロセスの十分なレベルのサイバーセキュリティを確保するための諸目的と関係するこの規則の第 III 款の諸条項の影響、実効性及び効率性、並びに、域内市場の稼働の向上も評価する。
3. その評価は、基礎的なサイバーセキュリティ上の要求事項に適合しない ICT 製品、ICT サービス及び ICT プロセスが欧州連合の市場に入ることを防止するため、域内市場へのアクセスのためのサイバーセキュリティ上の基本的な要求事項が必要であるか否かを評価する。
4. 欧州委員会は、2024 年 6 月 28 日までに、かつ、その後は 5 年毎に、欧州議会、理事会及び運営会議に対し、欧州委員会の判断結果と共に、その評価報告書を送付する。その評価報告書の判断結果は、公表される。

第 68 条 廃止及び承継

1. 規則(EC) No 526/2013 は、2019 年 6 月 27 日に発効するものとして、廃止される。
2. 規則(EC) No 526/2013 への参照及び同規則によって設置されたものとしての ENISA への参照は、この規則及びこの規則によって設置されたものとしての ENISA への参照として解釈される。
3. この規則によって設置されたものとしての ENISA は、保有、合意、法的義務、雇用契約、資金拠出及び法的責任の全てに関し、規則(EC) No 526/2013 によって設置されたものとしての ENISA を承継する。規則(EC) No 526/2013 に従って採択された運営会議及び執行会議の全ての決定は、それらの決定がこの規則を遵守していることを条件として、有効なままである。
4. ENISA は、2019 年 6 月 27 日を始期として、不定期間で設置される。
5. 規則(EC) No 526/2013 の第 24 条第 2 項により任命された長官は、長官の任期の残任期間について、執務を続け、この規則の第 20 条に示す長官の責務を果たす。彼または彼女の契約のその他の条件は、不変のままとする。
6. 規則(EC) No 526/2013 の第 6 条により任命された運営会議の構成員及びその代理者は、彼らの任期の残任期間について、執務を続け、この規則の第 15 条に示す運営会議の構成員の権能を行使する。

第 69 条 発効

1. この規則は、EU 官報上で公示された翌日から 20 日目に発効する。
2. 第 58 条、第 60 条、第 61 条、第 63 条、第 64 条及び第 65 条は、2021 年 6 月 28 日から適用される。

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

2019 年 4 月 17 日にストラスブールにおいて行われた。

欧州議会として	理事会として
議長　A. Tajani	議長　G. Ciamba

別 紙

適合性評価機関によって適合性あるとされるための要件

認定を受けることを望む適合性評価機関は、以下の諸要件に適合するものとする：

1. 適合性評価機関は、国内法に基づいて設立され、かつ、法人格をもつ。
2. 適合性評価機関は、その機関が評価を行う組織または ICT 製品、ICT サービスもしくは ICT プロセスとは独立の第三者機関とする。
3. その機関が評価を行う ICT 製品、ICT サービスまたは ICT プロセスの設計、製造、提供、組立て、利用または維持管理に関与する事業者を代表する産業団体または職業団体に所属する機関は、独立であること及び利益相反が存在しないことが説明されることを条件として、適合性評価機関であると判断され得る。
4. 適合性評価機関、その機関のトップレベルの経営陣及び適合性評価の職務の実施について責任を負う者、または、それらの者の承認された代表は、評価対象である ICT 製品、ICT サービスまたは ICT プロセスの設計者、製造者、供給者、導入者、購入者、保有者、利用者または保守管理者であってはならない。この禁止は、その適合性評価機関の業務遂行のために必要な評価対象 ICT 製品の利用、または、私的目的のためのそのような ICT 製品の利用を排除してはならない。
5. 適合性評価機関、その機関のトップレベルの経営陣及び適合性評価の職務の実施について責任を負う者、または、そのような活動に従事する者を代表する者は、評価対象である ICT 製品、ICT サービスまたは ICT プロセスの設計、製造またはコンサルテーション、マーケティング、導入、利用または保守管理に直接に関与してはならない。適合性評価機関、その機関のトップレベルの経営陣及び適合性評価の職務の実施について責任を負う者は、その適合性評価活動との関係において、その判断の独立性または完全性と抵触し得る活動に従事してはならない。この禁止は、とりわけ、コンサルタントサービスに対して適用される。
6. 適合性評価機関が公的機関によって保有または運営される場合、国内サイバーセキュリティ認証機関及び適合性評価機関との間において、独立であること及び利益相反が存在しないことが確保されるものとし、かつ、そのことが文書化される。
7. 適合性評価機関は、その支部局及び下請者の活動がその機関の評価活動の秘密、客観性または公平性を害さないことを確保する。
8. 適合性評価機関及びその職員は、最高度の専門的完全性及びその分野における必要な技術能力をもって適合性評価活動を実施し、かつ、特に、それらの活動の結果に利害のある人または人々のグループに関し、金銭的な性質をもつ圧力または誘惑を含め、その機関の判断またはその機関の適合性評価活動の結果に影響を与え得る全ての圧力及び誘惑を受けてはならない。
9. 適合性評価機関は、それらの職務が適合性評価機関によって実施されるものであるか、または、その機関を代理する者によってその機関の責任の下で実施されるものであるかを問わず、この規則に基づいてその機関に対して割当てられた全ての適合性評価の職務を実施できるものとする。外部職員への下請けまたは外部職員のコンサルティングは、適正に文書化され、中間介在者が関与してはならず、かつ、就中、秘密及び利益相反に適用される書面によ

る合意に服する。当の適合性評価機関は、遂行される職務に関し、全面的に責任を負う。

10. いかなる時においても、個々の適合性評価手続、並びに、個々のタイプ、類型または二次類型の ICT 製品、ICT サービスまたは ICT プロセスに関し、適合性評価機関は、その必要性に応じた裁量により、以下のものをもつ:
    (a) 適合性評価の職務を遂行するための技術上の知識及び十分かつ適切な経験をもつ職員;
    (b) それらの手続の透明性及びそれらの手続の再現可能性を確保するため、適合性評価が実施される際に従う手続の記述。その文書は、第 61 条により指定された機関として実施される職務とその機関の別の活動とを区分する適切な基本方針及び手続を設ける;
    (c) 活動の遂行に関する手続。それは、事業者の規模、その事業者が業務遂行する部門、その組織構成、当の ICT 製品、ICT サービスまたは ICT プロセスの技術の複雑性の程度、及び、製造過程が大量生産であるかシリアルの生産であるかを適正に考慮に入れる。
11. 適合性評価機関は、適合性評価活動と関係する技術上の職務及び管理運営上の職務を適切な態様で遂行するために必要となる手段をもち、かつ、必要な全ての機器及び施設へのアクセスをもつ。
12. 適合性評価活動を実施することについて責任を負う者は、以下のものをもつ:
    (a) 全ての適合性評価活動を包摂する良好な技術上の訓練及び職業訓練;
    (b) それらの者が実施する適合性評価の要件についての十分な知識、及び、それらの評価を実施するための十分な権限;
    (c) 適用される要求事項及びテストの標準についての適切な知識及び理解;
    (d) 適合性評価が実施されたことを説明する証明書、記録及び報告書を作成するための能力。
13. 適合性評価機関の公平性、その機関のトップレベルの経営陣の公平性、適合性評価活動を実施することについて責任を負う者の公平性、及び、下請者の公平性が保証される。
14. トップレベルの経営陣の報酬及び適合性評価活動を実施することについて責任を負う者の報酬は、実施された適合性評価の数またはそれらの評価の結果に依るものであってはならない。
15. その構成国の国内法に従い、その構成国によって損害賠償責任が保証されている場合、または、構成国自身が適合性評価について直接に責任を負う場合を除き、適合性評価機関は、損害賠償責任保険を締結する。
16. 適合性評価機関、及び、その機関の職員、その機関の委員会、その機関の支部局、その機関の下請者、または、適合性評価機関の関係機関もしくは外部組織の職員は、そのような者が服する欧州連合法または構成国法によって開示が要求される場合を除き、及び、その活動が実施される構成国の職務権限を有する機関との関係における場合を除き、この規則に基づく、または、この規則に有効性を与える国内法の条項により、それらの者の適合性評価の職務を実施する際に獲得した全ての情報に関し、秘密を保持し、かつ、守秘義務を尊重する。知的財産権は、保護される。適合性評価機関は、この点の要件に関し、文書化された手続を、設ける。
17. 第 16 条の場合を除き、この別紙の要件は、適合性評価機関と、認証を申請する者または認証を申請するか否かを検討している者との間における技術情報及び規制上の指針の交換を妨げてはならない。

18. 適合性評価機関は、手数料に関し、SME の利益を考慮に入れた上で、一貫性があり、公正であり、かつ、合理的な諸条件のセットに従い、業務遂行する。
19. 適合性評価機関は、ICT 製品、ICT サービスまたは ICT プロセスの認証を遂行する適合性評価機関の認定に関し、規則(EC) No 765/2008 の下で整合化されている関連標準の諸要求事項に適合するものとする。
20. 適合性評価機関は、適合性評価の目的のために使用されるテストの研究施設が、テストを遂行する研究施設の認定に関し、規則(EC) No 765/2008 の下で整合化されている関連標準の要求事項に適合するものであることを確保する。