委員会勧告(EU) 2017/1584

[参考訳]

2018 年 7 月 17 日
明治大学法学部教授
夏　井　高　人

＊＊＊

Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises（OJ L 239, 19.9.2017, p.36-58）のテキスト（英語版）に基づき、和訳を試みた。そのテキストは、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:32017H1584&from=EN
[2018 年 7 月 12 日確認]

委員会勧告(EU) 2017/1584 は、EU 全体に対して深刻な影響を及ぼすような大規模サイバー攻撃に対する構成国及び EU の機関との間の協調対応に関する欧州委員会の勧告書である。

委員会勧告(EU) 2017/1584 は、前文、勧告文並びに別紙（Annex）及び付録（Appendix）の 4 つの部分で構成されている。勧告の前文において「計画書（Blueprint）」として表現されている勧告の実質的内容部分は、委員会勧告(EU) 2017/1584 に添付された別紙の部分に収録されており、勧告文はその結論部分だけを示すものである。別紙の実質的内容の大部分は、CSIRT ネットワーク標準運営手順（CSIRTs Network's Standard Operating Procedures (SOP)）からの引用で構成されている。付録の部分には、委員会勧告(EU) 2017/1584 で用いられている用語の解説、ARGUS のフェーズ I 及びフェーズ II の解説、EEAS 及び EEAS CRM の解説、並びに、参考文献の一覧が収録されている。

この参考訳においては、委員会勧告(EU) 2017/1584 の前文、勧告文並びに別紙及び付録の全文を訳した。

ただし、別紙の図 1 及び図 2、並びに、付録 5 の文献標題及び付録 6 の図に関しては、事柄の性質上、原文のままとした。

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、あくまでも委員会勧告(EU) 2017/158 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。

この参考訳に訳注はない。脚注は、全て原注である。

日本国政府内においては、委員会勧告(EU) 2017/158 に示されているような統合的な危機管理体制を構築されておらず、危機管理体制に関するまとまった公式文書も存在しない。大規模自然災害の際を含め、緊急事態に対する対応は、その都度、アドホックに定められ、また、緊急事態が発生しているか否かに関する状況認識を得るための統合された情報伝達経路または統合された情報伝達手順は存在しない。

委員会勧告(EU) 2017/158 の署名者となっている Mariya Gabriel 氏（1979 年生）は、ブルガリア出身で、フランスのボルドー政治学院において学位を得た政治学者であると同時に、ブルガリアの保守系政党 GERB に所属する政治家であり、2017 年から欧州委員会の The Commissioner for Digital Economy and Society の任にある。

委員会勧告(EU) 2017/158 の中では、EU の機関等を示すために略称が用いられている。主要なものの正式名を併記すると、以下のとおりとなる。

略称	正式名称
DG HOME	The Directorate-General for Migration and Home Affairs
DG CNECT	The Directorate-General for Communications Networks, Content & Technology
DG HR	The Directorate-General for Human Resources and Security
DG DIGIT	The Directorate-General for Informatics
GSC	The General Secretariat of the Council
PSC	The Political and Security Committee
HRVP	The High Representative of the Union for Foreign Affairs and Security Policy
EEAS	The European External Action Service
SIAC	The Single Intelligence Analysis Capacity
Sitroom	The EU Situation Room
INTCEN	The EU Intelligence and Situation Centre
EUMS INT	EUMS Intelligence Directorate
EUMS	The European Union Military Staff
MS	Military Staff
EU HFC	The EU Hybrid Fusion Cell
ENISA	The European Network and Information Security Agency
CERT-EU	The Computer Emergency Response Team for the EU Institutions, bodies and agencies
ERCC	The Emergency Response Coordination Centre in the Commission
Europol	The European Union Agency for Law Enforcement Cooperation
EC3	The European Cybercrime Centre

以上の諸機関の中には軍事のみと関係する機関とそうではない機関とが含まれている。これは、大規模サイバーセキュリティインシデント（large-scale cybersecurity incidents）及び危機（crises）が複数の異なる性質をもつものであることがあり、その性質に応じて対応すべき機関・部署が異なるからである。例

えば、そのインシデントがサイバー戦（Cyberwar）の性質をもつものである場合、軍事及び外交という側面が重要になる。他方、そのインシデントがサイバー戦ではないけれどもそれと同様の危険性をもつ特定の勢力・団体または個人等からのサイバー攻撃に該当するような場合、軍事的側面と警察（治安維持）の側面が重要になる。そのインシデントが、規模においていかに大規模であっても、個人または特定の組織・団体によるサイバー犯罪（Cybercrime）の一種である場合には、主として各構成国の警察機関が共働して対応すべきことになる。更に、そのインシデントが（大規模自然災害を含め）軍事または外交とは異なる性質をもつ要素により発生している場合、それぞれのインシデントの性質に即して、適切な機関・部署が対応すべきことになる。

それゆえ、EU のサイバー危機管理体制は、初動の段階における事象の監視と分析を重視し、想定される要因に即して意思決定機関を分岐させているのである。

その監視において、仮にあるパケットが攻撃用パケットであることだけは判別できたとしても、その攻撃の意図や攻撃者が確定できない場合には、全ての事態を想定した対処が必要となる。このような場合、警察と軍事と諜報活動を明確に分け、相互の情報交換のない縦割りの組織活動では全く対処できない。このような事態は、「戦時と平時が常に共存する状況」の下においては不可避なことであり、グローバルな情報社会が維持・継続される限り、それを解消する方法が全くない（このような問題構造に関しては、夏井高人「情報社会の素描－EU の関連法令を中心として－(2・完)」法律論叢 90 巻 6 号 165～211 頁(2018)で述べたとおりである）。しかし、それでもなお、国家機関としては、当該パケットの性質を分析し、仕訳けし、それぞれの性質に即した対応（response）を検討しなければならない。EU においては、このような種々の要素が混在したような状態で出現する脅威類型を「ハイブリッドな脅威（hybrid threats）」として理解している。EU における「ハイブリッドな脅威」の概念は、2016 年頃から明示で用いられているが、これは、以前から提示してきた私見である「戦時と平時が常に共存する状況」の中で中心的な位置づけとなる現象を示す概念である（夏井高人「サイバー犯罪の研究（5）－サイバーテロ及びサイバー戦に関する比較法的検討－」法律論叢 86 巻 2・3 号 85～133 頁(2013)参照）。そして、EU の初動体制では、軍や諜報機関を含めた関連機関の間における情報交換、そして、構成国の CSRIT（Computer Security Incident Response Teams）からの情報提供とその迅速な分析が重視され、そのための合理的なエスカレーションの仕組みが構築されているのである。

ただし、TFEU 及び TEU に基づき、軍事及び警察に関する権限は、基本的に、構成国の国家主権の一部として維持されており、その原則を維持したままで情報共有及び調整（coordination）が実現されなければならないという非常に大きな困難が存在している。

委員会勧告(EU) 2017/158 は、以上のような（場合によっては相互に矛盾する）政治的な諸要素を考慮に入れた上で、迅速に判断系統の分岐を実現し、適切な意思決定が実施されることをめざすものであると考えることができる。

委員会勧告(EU) 2017/158 の前文は、NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1-30）が大規模サイバーセキュリティインシデント（large-scale cybersecurity incidents）を想定していなかった旨を述べている。

これは、大規模サイバーセキュリティインシデントそれ自体を想定していなかったという趣旨ではなく、情報通信関連産業とは無関係の産業部門を含め、社会全体を崩壊させかねない全面的な攻撃や危機の発生の場合の対処を想定していなかったという趣旨であると解される。

NIS 指令(EU) 2016/1148 は、情報ネットワーク及び情報システムそれ自体の安全を確保することを目的としており、その防護のための法制度としては十分なものであると言える。しかし、情報ネットワーク及び情報システムに対する攻撃が手段的なものであり、それによって社会全体（または、少なくとも社会の中枢機能）の破壊が意図されているような場合、情報ネットワーク及び情報システムの安全確保のための対応だけでは本質的な解決にならないことは、明らかである。

委員会勧告(EU) 2017/158 は、それゆえ、情報ネットワーク及び情報システムの安全確保のために NIS 指令(EU) 2016/1148 によって確立された CSIRT ネットワークの仕組みをフルに活用し、かつ、同指令に基づく ENISA の統括機能（調整機能）を多角的に活用することを前提とした上で、更に、軍や諜報機関との関係を整理し、その指揮命令系統または統括（調整）を明確化することにより、最終的な意思決定権者の所在を含め、EU の機関全体としての意思決定のための構造と手順を構築しようとしていると考えることができる。

別紙（Annex）の中で欧州サイバー犯罪センター（European Cybercrime Centre (EC3)）の「法的枠組み」として触れられている具体的な内容を示す公式文書は、委員会通知 COM(2012) 140 final である。

別紙（Annex）の中で触れられている ENISA 規則(EU) No 526/2013 を廃止し、情報通信技術サイバーセキュリティ認証を設ける 2017 年 9 月 13 日の規則案（「サイバーセキュリティ法（Cybersecurity Act）」）とは、COM(2017) 477 final のことを指す。この規則案は、2018 年中に採択される見込みである。

原文に添付の図は、カラーで印刷されている。しかし、この参考訳においては、諸般の事情により、白黒印刷とすることにした。

（この参考訳を作成するに際し考慮した事項）

「Coreper」は、EU の常駐代表委員会の別名であり、固有名詞である。常駐代表委員会は、EU の外務（External）及び法務・内務（Justice and Home Affair）に属する事項に関し、非常に重要な役割を果たす機関であるとされている。

この参考訳においては、「Coreper」を「コレペール」とカタカナ表記することにした。

「IPCR Arrangements」は、「IPCR 手順」と訳すことにした。また、IPCR 手順の段階 5（Step 5）にある「contributions」は、危機管理における意思決定のための情報提供による貢献のことを意味するので、「情報」と訳すことにした。

なお、「Integrated Political Crisis Response arrangements (IPCR)」と関連する EU の基本法令として、理事会決定 2014/415/EU（OJ L 192, 1.7.2014, p.53-58）がある。

「solidarity」は、一般的には「連帯」と訳されている。

しかし、現実の EU においては、事実の問題として、「統治」は存在するが「連帯」はない。また、政治的・経済的な連携は存在するが、しばしばほころび、構成国の財政破綻問題や離脱問題等を生じさせている。今後も「連帯」はないであろうし、戦時においても、現実には統一 EU 軍が存在しない以上、真

の意味における「連帯」はない。構成国軍の合同軍と NATO 軍との「連携」及び「統括（調整）」が存在するだけである。社会理念としても、ベルリンの壁が崩壊した後、相当の変化を経て、既に「連帯」の理念それ自体が希薄化しているのではないかと思われる。その現実の証左は、主要な EU 構成国各国における右翼勢力の台頭、そして、中国の経済力（投資）の影響及びロシアの（直接・間接の）政治的影響の増大という事実である。現在の EU に「連帯」があるとすれば、それは、「資本（Capital）」に対する信仰を共通にしているという意味での連帯のみではないかと考えられる。しかし、もともと資本に対する信仰は、利己的・排他的な本質をもつものであり、全ての関係者が勝者になることなどあり得ないことを当然の前提とするものであるので、哲学的な意味における「連帯」とは程遠いものではないかと思われる。

加えて、TFEU の第 222 条に定める「solidarity」条項の実装に関する理事会決定 2014/415/EU を見ても、「solidarity」は、極めて政治的な危機管理（crisis management）上の実務的手順の一種として理解されていることを認識することができる。

「EU には連帯が存在する」との観念は、幻想の一種である。「solidarity」は、基本的には、本来、国防及び軍の指揮権と関係する概念である。

以上を踏まえた上で、この参考訳においては、「solidarity」を「連携」と訳すことにした。

欧州委員会の「President」は、通常は、「委員長」と訳されている。

しかし、欧州議会の「President」と欧州連合の理事会の「President」は、共に「議長」と訳されており、かつ、欧州議会の「President」、欧州連合の理事会の「President」及び欧州委員会の「President」は、政治力学的にも法的に同格であり、欧州委員会の「President」だけを別格とすべき正当な根拠を見出し難い。

加えて、欧州委員会の中には様々な部署が存在しており、その中にはその部署のトップの職名を「Commissioner」とするところが複数存在する。この「Commissioner」は、それをカタカナ表記するのであれば「コミッショナー」であるが、それをもし和訳するとすれば、「委員長」である（付録の 3.のフェーズ II 参照）。

それゆえ、この参考訳においては、欧州委員会の「President」を「議長」と訳すことにした。

以上のほかは、後掲各参考訳の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）

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。NIS 指令の委員会実装規則(EU) 2018/151 の参考訳は、法と情報雑誌 3 巻 5 号 192～198 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。

EES 規則(EU) 2017/2226 の参考訳は、法と情報雑誌 3 巻 3 号 201～300 頁にある。安全な欧州連合第 11 次進捗状況報告書（COM/ 2017/0608 final）の参考訳は、法と情報雑誌 2 巻 11 号 156～176 頁にある。ハイブリッドな脅威報告書（JOIN (2017) 30）の参考訳は、法と情報雑誌 2 巻 8 号 91～119 頁にある。サイバーセキュリティ通知 JOIN(2017) 450 final の参考訳は、法と情報雑誌 2 巻 12 号 113～147 頁にある。

サイバー犯罪条約（ETS No.185）の説明書の参考訳は、法と情報雑誌 1 巻 6 号 1～132 頁にある。

指令 2013/40/EU の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 164～185 頁にある。指令(EU) 2015/849 の参考訳は、法と情報雑誌 3 巻 2 号 140～198 頁にある。指令(EU) 2017/1371 の参考訳は、法と情報雑誌 3 巻 1 号 92～109 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。Europol 規則(EU) 2016/794 の参考訳は、法と情報雑誌 2 巻 3 号 1～101 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の各文献等のほか、防衛基盤整備協会「情報セキュリティの現状と動向について－サイバー演習の実施要領と事例－（平成 26 年度）」（平成 27 年 2 月）、福井千衣「EU のテロリズム対策」外国の立法 228 号 68～81 頁 (2006)、佐藤智美「欧州連合（EU）の危機管理演習（CME/CMX）と軍事演習（MILEX）の概要－多国間主義に基づいた危機管理における協力体制」陸戦研究 663 号 15～45 頁 (2008)、小林正英「地域紛争と危機管理における国連および EU と NATO の役割」慶應法学 5 号 129～154 頁 (2006)、Artur Gruszczak, Intelligence Security in the European Union: Building a Strategic Intelligence Community, Palgrave Macmillan (2016)、Kristi Raik & Pauli Järvenpää, A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity, RKK ICDS (2017)、Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee & Madeline McCue, Addressing Hybrid Threats, Swedish Defence University (2018)、Ursula C. Schroeder, The Organization of European Security Governance: Internal and External Security in Transition, Routledge (2011) を参考にした。

＊＊＊

大規模サイバーセキュリティインシデント及び危機への協調対応に関する

2017 年 9 月 13 日の委員会勧告(EU) 2017/1584

欧州委員会は、
欧州連合の機能に関する条約、及び、とりわけ、その第 292 条に鑑み、

(1) 我々の企業及び市民は、かつてない程度に、部門を越え、国境を越えて、相互接続され、相互依存しており、情報通信技術の利用及びそれへの依存は、経済活動の全ての部門において、基本的な構成要素となっている。域内市場に対し、より広くは、欧州連合の経済、民主主義及び社会が依拠しているネットワーク及び情報システムに対し重大な混乱を発生させる潜在力をもつ影響を複数の構成国または欧州連合全域の組織に及ぼすサイバーセキュリティインシデントは、構成国及び欧州連合の機関が、十分に事前準備しなければならないシナリオの 1 つである。

(2) そのインシデントによって生ずる混乱が関係する構成国自身では手に負えないほどに拡大するものである場合、または、そのインシデントが、欧州連合の政治レベルにおける適時の調整及び対応を必要とする技術的または政治的重要性のある広範な影響のように、複数の構成国に影響を及ぼすものである場合、サイバーセキュリティインシデントは、欧州連合のレベルにおける危機として判断され得る。

(3) サイバーセキュリティインシデントは、ネットワーク及び情報システム並びに通信システムを超える様々な部門の活動に影響を与える広範囲な危機の引き金となり得る；適切な対応は、サイバーな軽減対策活動と非サイバーな軽減対策活動によらなければならない。

(4) サイバーセキュリティインシデントは、予測不可能であり、しばしば、非常に短い期間の間に発生して進化するものであり、それゆえ、影響を受けた組織、及び、そのインシデントに対応し、その影響を軽減することについて職責を負う組織は、それらの組織の対応を迅速に調整しなければならない。更に、サイバーセキュリティインシデントは、しばしば、特定の地理的場所だけにあるのではなく、多数の国々で同時に発生し、または、多数の国々を横断して容易に拡散し得るものである。

(5) 大規模サイバーセキュリティインシデント及び欧州レベルの危機への効果的な対応は、全ての関係する利害関係者の間における迅速かつ効果的な調整を要し、かつ、個々の構成国の準備体制及び能力、並びに、欧州連合の能力によって支援された調整された共同活動に依拠する。それゆえ、インシデントに対する適時かつ効果的な対応は、事前に構築され、かつ、可能な範囲内で、十分に訓練され、国内レベル及び欧州連合レベルにおける重要な活動主体の明確に定義された役割と責任をもつ調整手続及び調整の仕組みによることになる。

(6) 重要情報インフラ保護に関する 2011 年 5 月 27 日の理事会決議[1]において、理事会は、EU の構成国に対し、「構成国間の協調を強化すること、そして、国内の危機管理上の経験と結果に基づ

[1] 重要情報インフラ保護に関する欧州理事会決議「到達点及び次のステップ：グローバルなサイバーセキュリティに向けて」document 10299/11、ブリュッセル、2011 年 5 月 27 日

き、かつ、ENISA と協力して、2012 年の次期サイバー欧州演習の枠組み内でテストされるべき欧州のサイバーインシデント協力メカニズムの発展に貢献すること」を勧奨した。

(7) 2016 年の通知「欧州のサイバー回復力システム及び競争力のある革新的なサイバーセキュリティ産業の促進」[1]は、構成国に対し、NIS 指令 [2]の協力の仕組みを最大限に行うこと、及び、大規模サイバーインシデントのための準備体制と関連する国境を越える協力を拡大することを推奨している。この通知は、「計画書」の中で定められるサイバー環境の様々な要素を横断する危機対応協力の共同のアプローチが、準備体制を向上させ得ること、そして、そのような計画書が、既存の危機管理の仕組みの波及効果及び一貫性を確保するものでなければならないことも付け加えた。

(8) 上述の通知に関する理事会決議 [3]の中で、構成国は、欧州委員会に対し、行政組織及びそれ以外の関連利害関係者による判断のために、そのような計画書を送付することを求めた。しかしながら、NIS 指令は、大規模サイバーセキュリティインシデント及び危機の場合における欧州連合の協力枠組みを定めていない。

(9) 欧州委員会は、コンピュータセキュリティインシデント対応チーム（CSIRT）、NIS 指令によって設置された協力活動グループ及びサイバー問題に関する理事会横断作業部会からの構成国代表、並びに、欧州対外行動局（EEAS）、ENISA、Europol/EC3、理事会事務総局（GSC）からの代表との間で 2017 年 4 月 5 日及び 7 月 4 日にブリュッセルで開催された 2 つの別の協議ワークショップにおいて、構成国と協議した。

(10) 欧州連合レベルの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協調対応のための、この勧告に添付された現在の計画書は、上述の協議の産物であり、かつ、通知「欧州のサイバー回復力システム及び競争力のある革新的なサイバーセキュリティ産業の促進」を補完する。

(11) この計画書は、大規模サイバーセキュリティインシデント及び危機への対応における構成国と EU の機関、組織、事務局及び部局（以下「EU の機関」として示す。）との間の協力の目標及びモード、並びに、既存の危機管理の仕組みを既存のサイバーセキュリティ組織が EU レベルでどのように全面的に利用するかを示し、これを定めるものである。

(12) 前文(2)の意味におけるサイバーセキュリティ危機への対応に際し、理事会内における欧州連合の政治レベルの対応の調整は、統合政治危機対応（IPCR）手順 [4]を用いることになる；欧州委員会は、ARGUS[5]のハイレベル部門横断協調プロセスを用いるであろう。その危機が、重要な対外的局面または共通の安全保障及び防衛政策（CSDP）の局面を伴う場合、欧州対外行動局（EEAS）の危機対応メカニズム（CRM）[6]が発動されることになる。

(13) 一定の分野において、部門別の EU レベルの危機管理の仕組みは、サイバーセキュリティインシデントまたは危機の場合において協力を定めている。例えば、欧州グローバルナビゲーション衛星システム（GNSS）の枠組みの中で、理事会決定 2014/496/CFSP[6]は、理事会、上級代表、欧州

---

[1] COM(2016) 410 final, 5 July 2016

[2] 欧州連合内におけるネットワーク及び情報システムの安全の高いレベルの共通の措置に関する欧州議会及び理事会の 2016 年 7 月 6 日の指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1）

[3] Document 14540/16、2016 年 11 月 15 日

[4] より多くの情報は、EU レベルの危機管理、協力の仕組み及び活動主体に関する別紙の 3.1 節の中で見出され得る。

[5] 前項に同じ。

[6] 欧州グローバルナビゲーション衛星システムの設置、運用及び使用の欧州連合の安全への影響の側面

委員会、欧州 GNSS 局及び構成国の、サイバー攻撃の場合を含め、欧州連合に対する脅威、構成国に対する脅威、または、GNSS に対する脅威に対処するために定められた運営責任の連鎖内のそれぞれの役割を既に定めている。それゆえ、この勧告は、そのような仕組みを妨げてはならない。

(14) 構成国は、構成国に影響を与える大規模サイバーセキュリティインシデント及び危機の場合における対応について基本的な責任を負う。しかしながら、欧州委員会、上級代表及びそれ以外の EU の機関及び部署は、欧州連合法から生ずる、または、サイバーセキュリティインシデント及び危機が、単一市場内の全ての部門の経済活動、欧州連合の安全保障及び国際関係、並びに、機関それ自体に対して影響を与え得るということから生ずる重要な役割をもつ。

(15) 欧州連合レベルにおいて、サイバーセキュリティ危機への対応に関与する鍵となる活動主体は、新たに設置された NIS 指令の構造及び仕組み、すなわち、コンピュータセキュリティインシデント対応チーム（CSIRT）ネットワーク、並びに、関連する部局及び組織、すなわち、欧州連合ネットワーク情報セキュリティ局（ENISA）、Europol の欧州サイバー犯罪センター（Europol/EC3）、EU 情報活動分析センター（INTCEN）、EU 軍参謀本部情報部（EUMS INT）及び SIAC（単一情報分析部）として共に作業をする状況分析室（Sitroom）、（INTCEN を基礎とする）EU ハイブリッドフュージョンセル、EU の機関のためのコンピュータ緊急対応チーム（CERT-EU）、並びに、欧州委員会内の緊急対応コーディネートセンターを含む。

(16) 技術レベルのサイバーインシデントへの対応における構成国間の協力は、NIS 指令によって設置された CSIRT ネットワークから提供される。ENISA は、そのネットワークのために事務局を提供し、かつ、CSIRT 間の協力を積極的に支援する。国内 CSIRT と CERT-EU は、必要があるときは、1 または複数の構成国に影響を与えるサイバーセキュリティインシデントへの対応を含め、任意ベースで、協力し、かつ、情報交換する。構成国の CSIRT の代表からの要請により、構成国の CSIRT は、討議を行うことができ、かつ、それが可能なときは、当該同じ構成国の国家主権の及ぶ範囲内で識別されたインシデントに対して協調対応することを定めることができる。関連手続は、CSIRT ネットワークの標準運営手順（SOP）[1]の中で定められることになるであろう。

(17) CSIRT ネットワークは、リスク及びインシデントの分類、早期警戒、共助、調整のための基本原則及び書式と関連するものを含め、構成国が国境を越えるリスク及びインシデントに対応する場合における業務遂行上の協力のフォームの細目を討議し、開発し、定めることも職務とする。

(18) NIS 指令の第 11 条によって設けられた協力活動グループは、CSIRT ネットワークの活動に関する戦略的運用指針を提供すること、及び、構成国の能力及び準備体制を討議すること、並びに、任意ベースで、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戦略と CSIRT の実効性を評価すること、そして、ベストプラクティスを指定することを職務とする。

(19) 協力活動グループ内の専門ワークストリームは、NIS 指令の第 14 条第 7 項により、重要サービスの運営者が第 14 条第 3 項によりインシデントの通知を要求される状況、並びに、そのような通知のためにフォーマット及び手続に関するインシデント通知運用指針を準備しているところである [2]。

に関する、並びに、共同活動 2004/552/CFSP を廃止する 2014 年 7 月 22 日の理事会決定 2014/496/CFSP（OJ L 219, 25.7.2014, p.53）

[1] 2017 年までに採択された部分を除き、未完成である。

[2] この運用指針は、2017 年末までに完成される予定である。

(20) 報告、評価、研究、調査及び分析を介して得られるリアルタイムの状況、リスク状態及び脅威の認識と理解は、十分な情報提供に基づく判断を可能とするために重要である。この（全ての関連する利害関係者による）「状況認識」は、効果的な協調対応のために重要である。状況認識は、原因、並びに、インシデントの影響及び発生源に関する要素を含む。これは、適切なフォーマットにより、インシデントを表現するための共通の分類を使用し、かつ、適切に安全な方法による関係者間の情報交換及び情報共有によるものであることが認識されている。

(21) サイバーセキュリティへの対応は、インシデントの技術的な要因を共働で調査する複数の組織を伴い得る技術的措置を定めること（例：マルウェア分析）、または、その組織が影響を受けたか否かを組織が評価し得るための方法を定めること（例：痕跡）から、そのような措置の適用に関する運用上の決定、そして、インシデントによっては、政治レベルで、悪意あるサイバー活動への共同対応のための枠組み [1]、または、ハイブリッドな脅威に対抗するための EU の作戦手順書 [2]のような、上記以外の手段の使用に関する決定まで、種々の形態を採り得る。

(22) デジタルサービスへの欧州の市民及び企業の信頼は、デジタル単一市場の繁栄にとって重要なものである。それゆえ、危機管理広報は、サイバーセキュリティインシデント及び危機の負の影響の軽減において部分的に重要な役割を演ずる。広報は、第三国から活動する（潜在的な）侵略者の行動に影響を与える手段としての共同外交対応のための枠組みの過程においても利用され得る。サイバーセキュリティインシデント及び危機の負の影響の軽減のための広報と侵略者に影響を与えるための広報を揃えることは、政治的対応を実効的なものとするために重要である。

(23) （例えば、パッチの適用、または、脅威を避けるための補完的な行動の実施により）利用者及び組織レベルで彼らがどのようにインシデントの影響を軽減させ得るかに関する情報を公衆に提供することは、大規模サイバーセキュリティインシデント及び危機を軽減するための効果的な手段の 1 つであり得る。

(24) 欧州委員会は、コネクティングヨーロッパファシリティ（CEF）を通じて、生起しつつあるサイバー脅威及びインシデントへの準備体制、協力及び対応についての構成国の CSIRT のレベルを向上させるため、MeliCERTes として知られる参加構成国 CSIRT 間のコアサービスプラットフォーム協力メカニズムを開発中である。欧州委員会は、国内レベルにおける CSIRT の業務遂行能力を向上させるため、CEF の下で賞を与えられる提案の競争的な募集を通じて、構成国内の CSIRT に共同で資金提供している。

(25) EU レベルのサイバーセキュリティ演習は、構成国及び民間部門の中における協力を強化し、向上させるために重要である。その目的のために、2010 年以来、ENISA は、定期的な汎欧州サイバーインシデント演習（「サイバー欧州」）を組織している。

(26) 欧州理事会、欧州委員会議長及び北大西洋条約機構事務総長の共同宣言の実装に関する理事会決議 [3]は、とりわけ、サイバー防衛演習及びサイバー欧州を含め、それぞれの演習における相互の職員参加を通じて、サイバー演習における協力強化を求めている。

---

[1] 悪意あるサイバー活動への EU の共同外交対応のための枠組みに関する理事会決定（「サイバー外交ツールボックス」）、Doc.9916/17

[2] ハイブリッドな脅威への対抗のための EU の作戦手順の共同作業文書「EU 作戦書」、SWD(2016) 227 final、2016 年 7 月 5 日

[3] ST 15283/16、2016 年 12 月 6 日

(27) 継続的に進化している脅威の様相、及び、近時のサイバーセキュリティインシデントは、欧州連合が直面しているリスクの増加を示すものであり、構成国は、更に遅滞することなく、かつ、いかなる場合においても、2018 年末までに、この勧告に基づいて行動しなければならない。

以上のとおりであるので、この勧告を採択する:

(1) 構成国及び EU の機関は、その中で記述された運用上の基本原則を伴う計画書の中に提示される協力の目標及び方式を統合する EU サイバーセキュリティ対応枠組みを構築しなければならない。
(2) EU サイバーセキュリティ対応枠組みは、とりわけ、関連する活動主体、EU の機関及び構成国の機関を、全ての必要なレベル（技術レベル、運営レベル、戦略／政治レベル）で定め、かつ、それが必要なときは、EU の危機管理の仕組みの文脈内におけるそれらの機関の協力の方法を定める標準的な運営手続を開発しなければならない。不適切な遅滞のない情報交換、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の間における対応の協調に重点が置かれなければならない。
(3) その目的のために、構成国の職務権限を有する機関は、情報共有及び協力手順の細目を定めることに向けて、共に作業しなければならない。
(4) 構成国は、その構成国の国内危機管理の仕組みがサイバーセキュリティインシデント対応に適切に対応することを確保し、かつ、EU の枠組みの文脈内における EU レベルの強力のために必要な手続を定めなければならない。
(5) EU の既存の危機管理の仕組みに関し、計画書に沿って、構成国は、欧州委員会の関連部署及び EEAS と共に、その構成国の国内危機管理及びサイバーセキュリティ組織及び手続を、EU の既存の危機管理の仕組み、すなわち、IPCR 及び EEAS CRM への統合に関する実務上の実装運用指針を定めなければならない。とりわけ、構成国は、EU の危機管理の仕組みの過程において、その構成国の危機管理機関とその構成国の EU レベルの代表との間で効率的な情報の流れを可能とするための適切な構造が設けられることを確保しなければならない。
(6) 構成国は、コネクティングヨーロッパファシリティ（CEF）のサイバーセキュリティデジタルサービスインフラ（DSI）計画によって提供される機会を全面的に利用しなければならず、かつ、現在構築中のコアサービスプラットフォーム協力メカニズムが、必要な機能を提供し、かつ、サイバーセキュリティ危機の間においても協力を求める構成国の要求を満たすものであることを確保するため、欧州委員会と協力しなければならない。
(7) 構成国は、ENISA の補佐を受け、かつ、この分野における従前の作業を基礎として、危機の間における構成国の技術上及び運営上の協力を更に拡大するために、サイバーセキュリティインシデントの技術上の原因及びその影響を記述するための状況報告書に関する共通の分類及びテンプレートの開発及び採択において協力しなければならない。この点に関し、構成国は、インシデント通知運用指針に関して協力活動グループ内において目下進行中の作業、及び、とりわけ、国内通知のフォーマットと関連する側面を考慮に入れなければならない。
(8) 枠組み内に定める手続は、テストされなければならず、かつ、それが必要なときは、国内演習、地域演習及び欧州連合演習、並びに、サイバー外交演習、及び、NATO サイバーセキュリティ演

習への構成国の参加から学んだ教訓に従って、見直されなければならない。とりわけ、その手続は、ENISA によって組織されるサイバー欧州演習の過程においてテストされなければならない。サイバー欧州 2018 は、そのような最初の機会を提供する。

(9) 構成国及び EU の機関は、その政治的対応を含め、かつ、必要があるときは、しかるべく民間部門の組織の関与と共に、国内レベル及び欧州レベルで、大規模サイバーセキュリティインシデント危機への構成国の対応を継続的に実践しなければならない。

2017 年 9 月 13 日にブリュッセルにおいて行われた。

欧州委員会として
委員会委員 Maria Gabriel

別 紙

大規模な国境を越えるサイバーセキュリティインシデント及び危機への協調対応のための計画書

イントロダクション

この計画書は、関係する構成国自身では手に負えないほどに拡大する混乱を生じさせ、または、そのインシデントが、欧州連合の政治レベルにおける適時の政策調整及び対応を必要とする技術的または政治的重要性のある広範かつ重大な影響のように、複数の構成国または EU の機関に影響を及ぼすサイバーセキュリティインシデントに適用される。

そのような大規模サイバーセキュリティインシデントは、サイバーセキュリティ「危機」として判断される。

サイバーな要素をもつ EU 全域の危機の場合、欧州連合の政治レベルにおけるその対応の調整は、統合政治危機対応（IPCR）手順を用い、理事会によって実施される。

欧州委員会内において、調整は、ARGUS 緊急警報システムに従って行われる。

その危機が対外的な局面または共通の安全保障及び国防政策（CSDP）の側面を伴う場合、EEAS 危機対応メカニズムが発動される。

計画書は、これらの十分に構築された危機管理の仕組みが、既存の EU レベルのサイバーセキュリティ組織、及び、構成国間の協力の仕組みをどのように全面的に利用すべきであるかを記述する。

そのようにする際、計画書は、一群の運用基本原則（比例性、補完性、相補性及び情報の機密性）を考慮に入れ、3 つのレベル（戦略的／政治レベル、運営レベル及び技術レベル）における協力のコア目標（効果的な対応、状況認識の共有、広報メッセージ）、仕組み及び関与する活動主体並びにそのコア目標に適合するための活動を提示する。

計画書は、危機管理ライフサイクルの全体（防止／軽減、手配、対応、回復）を包摂しないが、対応には焦点を当てる。ただし、計画書は、一定の活動、とりわけ、状況認識の共有の達成と関連する活動には対応する。

サイバーセキュリティインシデントが、より広い危機の発端またはその一部において、他の部門に影響を与え得るものであることに注意することが重要である。サイバーセキュリティ危機が物理的な世界に対して影響を及ぼすと予想されることに鑑み、適切な対応は、サイバーな軽減対策活動及び非サイバーな軽減対策活動の両者によらなければならない。サイバー危機対応活動は、EU レベル、国内レベルまたは部門レベルの他の危機管理の仕組みと統合されなければならない。

最後に、計画書は、欧州グローバルナビゲーション衛星システム（GNSS）計画[1]のために設けられるもののような、部門または政策に固有の既存の仕組み、手順または法律文書を置き換えるものではなく、かつ、それらを妨げてはならない。

[1] 決定 2014/496/CFSP

指針となる基本原則

目標達成に向けた作業において、必要な活動を定め、それぞれの活動主体または仕組みに対して役割及び責任を割り当てる際、以下の運営基本原則が適用された。また、将来の実装運用指針を準備する際においても、以下の運営基本指針が尊重される必要がある。

比例性: 構成国に影響を与えるサイバーセキュリティインシデントの大多数は、国内「危機」と判断され得るものよりも下にあるもので、欧州「危機」よりもずっと下のものである。そのようなインシデントへの対応における構成国内の協力の基盤は、NIS 指令 [1]によって設けら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（CSIRT）ネットワークから提供される。国内 CSIRT は、必要があるときは、CSIRT ネットワークの標準運営手順（SOP）に沿って、1 または複数の構成国に影響を与えるサイバーセキュリティインシデントへの対応を含め、日々の業務において、任意に協力し、情報交換する。それゆえ、計画書は、それらの SOP を全面的に利用するものでなければならず、かつ、追加的なサイバーセキュリティ危機の特別の職務は、その中に反映されなければならない。

補完性: 補完性の原則は、鍵である。構成国は、構成国に影響を与える大規模サイバーセキュリティインシデントまたは危機の場合における対応に関する第一次的な責任をもつ。しかしながら、欧州委員会、欧州対外行動局、並びに、それら以外の EU の機関、事務局、部局及び組織は、重要な役割をもつ。その役割は、IPCR 手順の中で明確に定められているが、欧州連合法からも生ずるものであり、または、サイバーセキュリティインシデント及び危機が、単一市場内の全ての部門の経済活動、欧州連合の安全保障及び国際関係、並びに、機関それ自体に対して影響を及ぼし得るということからも生じ得るものである。

相補性: 計画書は、新たな NIS 指令の構造及び仕組み、すなわち、CSIRT ネットワーク、並びに、関連する部局及び組織、すなわち、欧州連合ネットワーク情報セキュリティ局（ENISA）、Europol の欧州サイバー犯罪センター（Europol/EC3）、EU 情報活動分析センター（INTCEN）、EU 軍参謀本部情報部（EUMS INT）及び SIAC（単一情報分析部）として共に作業をする状況分析室（Sitroom）；（INTCEN を基礎とする）EU ハイブリッドフュージョンセル；EU 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（CERT-EU）をその中に統合する EU レベルの既存の危機管理の仕組み、すなわち、統合政治危機対応（IPCR）手順、ARGUS 及び EEAS 危機管理メカニズムを全面的に考慮に入れる。そのようにする場合、計画書は、それら相互の活動及び協力が、最大限の相補性と最小限の重複を達成することも確保しなければならない。

情報の機密性: 計画書の文脈の中で交換される全ての情報は、安全に関する適用可能な法令 [2]、個

[1] 指令 (EU) 2016/1148

[2] 欧州委員会における安全に関する 2015 年 3 月 13 日の委員会決定(EU, Euratom) 2015/443（OJ L 72, 17.3.2015, p.41）及び EU 機密情報の保護のための安全規則に関する 2015 年 3 月 13 日の委員会決定(EU, Euratom) 2015/444（OJ L 72, 17.3.2015, p.53）；欧州対外行動局のための安全規則に関する 2013 年 4 月 19 日の外務及び安全保障政策に関する欧州連合上級代表決定（OJ C 190, 29.6.2013, p.1）。EU 機密情報の保護

人データの保護に関する適用可能な法令、並びに、トラフィックライトプロトコル [1]を遵守しなければならない。機密情報の交換に関し、適用される機密区分制度の別に拘らず、利用可能な認定されたツールが使用されるものとする [2]。個人データの処理に関しては、計画書は、適用可能な EU の法令、とりわけ、一般データ保護規則[3]、e プライバシー指令[4]、及び、「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個人の保護並びにそのデータの支障のない移動に関する」規則[5]を尊重する。

コア目標

計画書に基づく協力は、上述の 3 つのレベル（政治、運営及び技術）のアプローチに従う。各レベルにおいて、協力は、情報交換及び共同活動を含めることができ、かつ、以下のコア目標の達成を狙いとする。

- 効果的な対応を可能にする。対応は、インシデントの技術的な要因を共働で調査する複数の組織を伴い得る技術的措置を定めること（例：マルウェア分析）、または、その組織が影響を受けたか否かを組織が評価し得るための方法を定めること（例：痕跡）から、そのような措置の適用に関する運用上の決定、そして、インシデントによっては、政治レベルで、悪意あるサイバー活動への EU 外交対応（「サイバー外交ツールボックス」）、または、ハイブリッドな脅威に対抗するための EU の作戦手順書のような、上記以外の手段の使用に関する決定まで、種々の形態を採り得る。
- 状況認識を共有する。全ての関連する利害関係者によって、3 つのレベル（技術、運用、政治）でそれが広がるので、事件を十分に良く理解することは、協調対応のために重要なことである。状況認識は、原因、並びに、インシデントの影響及び発生源に関する技術的要素を含む。サイバーセキュリティインシデントは、広範な種類の部門（金融、電力、輸送、医療等）に影響を与え得るものであるので、適切な情報が、適切なフォーマットで、適時の態様で、全ての関連する利害関係者に到達することは、必須のことである。
- 鍵となるメッセージの広報に同意する[6]。危機管理広報は、サイバーセキュリティインシデント及び

のための安全規則に関する 2013 年 9 月 23 日の理事会決定 2013/488/EU（OJ L 274, 15.10.2013, p.1）。

[1] https://www.first.org/tlp/

[2] 2016 年 6 月現在、これらの送受信経路は、CIMS（機密情報管理システム）、ACID（暗号化アルゴリズム）、RUE（RESTREINT UE/EU RESTRICTED 指定文書の作成、交換及び記録保存のための安全システム）及び SOLAN を含めていた。それ以外の、例えば、機密情報送受信手段は、PGP または S/MIME を含む。

[3] 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）

[4] 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の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（プライバシー及び電子通信に関する指令）（OJ L 201, 31.7.2002, p.37）

[5] 欧州共同体の機関及び組織による個人データの処理と関連する個人の保護並びにそのデータの支障のない移動に関する欧州議会及び理事会の 2000 年 12 月 18 日の規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1）－見直し中

[6] 広報が、公衆全体に対するインシデントに関する広報と、重要部門及びまたは影響を受けた部門へのより

危機の負の影響の軽減において重要な役割を演ずるが、（潜在的な）侵略者の行動に影響を与える手段としても利用され得る。サイバーセキュリティインシデント及び危機の負の影響の軽減のための広報と侵略者に影響を与えるための広報を揃えることは、政治的対応を実効的なものとするために重要である。とりわけ、（例えば、パッチの適用、または、脅威を避けるための補完的な行動の実施により）公衆がどのようにインシデントの影響を軽減させ得るかに関する正しく活動し得る情報を供給することは、サイバーセキュリティにおいて重要である。

技術、運営、戦略／政治の各レベルにおける構成国間及び構成国と EU の活動主体との間の協力

EUレベルの大規模サイバーセキュリティインシデントまたは危機への効果的な対応は、効果的な技術上、運営上及び戦略上／政治上の協力によって異なる。

各レベルにおいて、活動主体は、以下の 3 つのコア目標の達成に関し、特別の活動を遂行しなければならない：

- 協調対応;
- 状況認識共有;
- 広報。

インシデントまたは危機を通じて、より低いレベルは、より高いレベルに対して警告を発し、情報提供し、かつ、それを支援することになる;より高いレベルは、より低いレベルに対し、しかるべく、ガイダンス[1]及び決定を提供する。

技術レベルの協力

活動範囲:

- サイバーセキュリティ危機の間におけるインシデントの取扱い[2]
- 脅威及びリスクの継続的な分析を含め、インシデントの監視及び調査。

技術的または運用的な情報の広報の両者を指しえることに、以後、注意することが重要である。この広報は、機密の供給経路の使用及び特別な技術的ツール／プラットフォームの使用を要求することがあり得る。いずれの場合においても、構成国内の運営者及びより広い公衆へ連絡することは、各構成国の特権であり、かつ、責任である。それゆえ、上記に示す補完性の原則に沿って、構成国及び国内 CSIRT は、その構成国の領土内において、その構成国の選挙民それぞれに対して供給される情報について、最終的な責任をもつ。

[1] 「活動許可」－サイバーセキュリティ危機に照らし、適切な軽減対策活動を実施するため、反応時間が短いことが生死を分ける重要性をもつ。これらの短い反応時間を提供するため、特別のインシデントにおいてそれが要求されていない場合、より高いレベルまたは EU の機関と協議をもつことなく、通常要求される全ての公式経路を経て行うことなく、迅速に活動するための構成国の許可を与える任意の「活動許可」が、ある構成国から別の構成国に対して発せられ得る（例えば、CSIRT は、別の構成国の CSIRT に対して脆弱性情報を転送するために、より高いレベルと協議することを要するものとしてはならない）。

[2] 「インシデントの取扱い」とは、インシデントの検知、分析及び抑制、並びに、そのインシデントへの対応を支援する全ての活動のことを意味する。

潜在的な活動主体

技術レベルにおいて、計画書における協力のための中心的な仕組みは、議長国によって主宰され、ENISA から事務局の提供を受ける CSIRT ネットワークである。

- 構成国:
  - 職務権限を有する機関及び NIS 指令によって設けられる単一連絡部局
  - CSIRT
- EU の組織／事務局／部局
  - ENISA
  - Europol/EC3
  - CERT-EU
- 欧州委員会
  - ERCC（DG ECHO 内に所在する 24/7 運用サービス）及び（インシデントの特別の性質により、DG CNECT と DG HOME との間で選択される）指定された主務部署、事務総局（ARGUS 総局）、DG HR（安全保障総局）、DG DIGIT（IT 安全保障運営総局）。
  - 上記以外の EU の部局に関し [1]、欧州委員会または EEAS 内のそれぞれの親 DG（最初の連絡先）
- EEAS
  - SIAC（単一情報分析部：EU INTCEN 及び EUMS INT）
  - EU 状況分析室及び指定された地理別の部署または課題別の部署
  - （ハイブリッドな文脈におけるサイバーセキュリティに関しー EU INTCEN の一部である）EU ハイブリッドフュージョンセル

状況認識共有:

- 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、一般に利用可能な情報、ENISA 自身の分析、（任意ベースで）構成国の CSIRT によって、または、NIS 指令の単一連絡部局、Europol の欧州サイバー犯罪センター（EC3）及び CERT-EU、並びに、それが適切なときは、欧州対外行動局（EEAS）の EU 情報活動分析センター（INTCEN）によって、ENISA との間で共有される報告に基づき、継続的に、インシデント及び脅威に関する EU サイバーセキュリティ技術状況報告書を準備する。その報告は、理事会、欧州委員会、HRVP 及び CSIRT ネットワークの関連する事項のために利用可能とされなければならない。
- 大きなインシデントの場合、CSIRT ネットワークの議長は、ENISA の補佐を受けて、EU サイバーセキュリティインシデント状況報告書 [2]を作成し、その報告書は、輪番議長国の CSIRT を介して、議長国、欧州委員会及び HRVP に提出される。

[1] インシデントの性質及び異なる活動部門（金融、輸送、電力、医療等）に対する影響の相違により、EU の関連する部局または組織が関与することになる。

[2] EU サイバーセキュリティインシデント状況報告書は、国内 CSIRT から提供される国内報告書の合綴である。報告書のフォーマットは、CSIRT ネットワーク SOP の中で示される。

- *上記以外の EU の全ての部局*のそれぞれの親 DG に対する報告。その DG は、順次、欧州委員会の主務部署に対して報告する。
- *CERT-EU* は、CSIRT ネットワーク、（しかるべく）EU の機関及び部局、並びに、（発動されているときは）ARGUS に対し、技術報告書を提供する。
- *Europol/EC3*[1]及び *CERT-EU* は、CSIRT ネットワークに対し、技術的な痕跡の専門的な法科学分析結果及びそれ以外の技術情報を提供する。
- EEAS SIAC： EU ハイブリッドフュージョンセルは、INTCEN の代わりに、関連する EEAS の部署に対し、報告する。

対応:

- *CSIRT ネットワーク*は、IP アドレス、痕跡[2]等のような、インシデントに関する技術的な詳細及び分析を交換する。そのような情報は、遅滞なく、かつ、遅くともインシデントが検知された時から 24 時間以内に、ENISA に対して提供されなければならない。
- CSIRT ネットワーク標準運営手順に従い、原因及び可能な技術的軽減対策措置を判定するため、インシデントと関連する利用可能な技術的痕跡及びそれ以外の技術情報を分析するための彼らの努力において、その構成員と協力する。
- ENISA は、その専門知識に基づき、かつ、その任務に従い、CSIRT の技術的な活動において、CSIRT を補佐する[3]。
- 構成国の CSIRT は、ENISA 及び欧州委員会の補佐を受け、その技術的対応活動上で協力する。
- EEAS SIAC： EU ハイブリッドフュージョンセルは、INTCEN の代わりに、変動する最初の証拠を集めるための収集プロセスを設ける。

広報:

- CSIRT は、技術的な助言[4]及び脆弱性警告[5]を作成し、それらをそれぞれのコミュニティに配布し、かつ、それぞれの場合において適用可能な承認手続に従い、公衆に対して提供する。
- ENISA は、CSIRT ネットワークの共通の連絡の作成及び供給を容易にする。
- ENISA は、CSIRT ネットワーク及び欧州委員会報道官との間で、その広報活動を調整する。
- ENISA と EC3 は、構成国間で合意された状況認識共有に基づき構成国の広報活動を調整する。
- その危機が対外的な局面または共通の安全保障及び防衛政策（CSDP）の局面を伴う場合、その

[1] EC3 の法的枠組みに定める条件及び手続に従い、かつ、それに基づく。

[2] コンピュータ法科学における「痕跡（IOC）」は、コンピュータへの介入を高い信頼をもって示すネットワーク上またはオペレーティングシステム内で観察される痕跡である。典型的な IOC は、ウイルスのシグネチャ及び IP アドレス、マルウェアファイルの MD5 ハッシュ、ボットネットコマンド及び管理サーバの URL またはドメイン名である。

[3] ENISA、欧州サイバーセキュリティ局に関する、及び、規則(EU) No 526/2013 を廃止する、並びに、情報通信技術サイバーセキュリティ認証に関する 2017 年 9 月 13 日の規則案（「サイバーセキュリティ法」）

[4] インシデントの原因及び可能な軽減策に関する技術的な性質の助言

[5] IT システムに対して負の影響を与えるために悪用されつつある技術上の脆弱性に関する情報

広報は、EEAS 及び HRVP 報道官との間で調整されなければならない。

運用レベルの協力

活動範囲:

- 政治レベルの意思決定の準備
- サイバーセキュリティ危機の管理の調整（しかるべく）
- EU レベルの結果及び影響の評価、並びに、可能な軽減対策活動の提案。

潜在的な活動主体

- 構成国:
  - 職務権限を有する機関及び NIS 指令によって設けられる単一連絡部局
  - CSIRT、サイバーセキュリティ部局
  - （複数部門のインシデントまたは危機の場合）上記以外の国内部門当局
- EU の組織／事務局／部局
  - ENISA
  - Europol/EC3
  - CERT-EU
- 欧州委員会
  - （ARGUS プロセスの）事務総局の（副）事務総長
  - DG CNECT/HOME
  - 欧州委員会安全保障機関
  - （複数部門のインシデントまたは危機の場合）上記以外の総局
- EEAS
  - 危機対応及び SIAC（EU INTCEN 及び EUMS INT）の事務総局の（副）事務総長
  - EU ハイブリッドフュージョンセル
- 理事会
  - GSC または PSC[1]の支援を受け、かつ、（発動されているときは）IPCR 手順の支援を受け、議長国（サイバー問題に関する横断作業部会またはコレペール[2]の議長）

状況認識:

- 政治／戦略状況報告書の作成の支援（例：IPCR 発動の場合における ISAA）

[1] 政治及び安全保障委員会は、欧州連合条約の第 38 条に示す共通の対外政策及び安全保障政策を取り扱う欧州連合の理事会の委員会の 1 つである。

[2] 常駐代表委員会またはコレペール（欧州連合の機能に関する条約 TFEU の第 240 条）は、欧州連合の理事会の仕事の準備について職責を負う。

- *サイバー問題に関する理事会横断作業部会*は、コレペールまたは PSC の会合をしかるべく準備する
- IPCR が発動された場合:
  - 議長国は、構成国の関連する利害関係者、機関、部局、非 EU 諸国のような第三者及び国際機関の参加を招請し、コレペールまたは PSC のための議長国の準備を支援するためのラウンドテーブルを求めることができる。これらは、ボトルネックを識別するための危機管理会合であり、分野横断的な問題に関する行動のための提案書を作成する。
  - 欧州委員会の主務部署または ISAA 主務部署としての EEAS は、ENISA、CSIRT ネットワーク、Europol/EC3、EUMS INT、INTCEN 及びそれ以外の全ての活動主体の貢献を受けて、ISAA 報告書を準備する。ISAA 報告書は、技術的なインシデントと危機管理評価（脅威分析、リスク評価、非技術的な結果及び影響、インシデントまたは危機の非サイバー的な側面等）との相関性に基づく EU 全域の評価を示すものとし、それは、運営レベル及び政治レベルの必要に応じて個別化される。
- ARGUS が発動された場合:
  - CERT-EU 及び EC3[1]は、欧州委員会内における情報交換に直接的に貢献する。
- EEAS 危機対応メカニズムが発動された場合:
  - SIAC は、その情報収集を強化し、全ての情報源の情報を集約し、かつ、インシデントに関する分析及び評価を準備する。

（政治レベルからの要請に基づく）対応:

- 結果及び影響を軽減させるための（NIS 指令の）単一連絡部局及び職務権限を有する国内機関の国境を越える協力。
- 全ての技術的な軽減対策措置を発動し、かつ、標的とされた情報システム上の攻撃の影響を停止させ、または、これを軽減させるために必要な技術的能力を調整する。
- **CSIRT ネットワーク SOP** に従い、共同対応または共働対応に向けて、協力し、かつ、技術的な能力を調整する。
- 関連する第三者と協力する必要性を評価する。
- （発動されている場合）ARGUS プロセス内における意思決定。
- （発動されている場合）IPCR 手順に基づく決定及び調整の準備。
- （発動されている場合）第三国及び国際機関との連絡、並びに、CSDP の任務及び業務遂行の保護、EU の使節団の保護を狙いとする措置に関するものを含め、EEAS 危機対応メカニズムを介する EEAS の意思決定を支援すること。

広報:

- インシデントと関連する公開メッセージに同意する。
- その危機が対外的な局面または共通の安全保障及び防衛政策（CSDP）の局面を伴う場合、その

[1] EC3 の法的枠組みに定める条件及び手続に従い、かつ、それに基づく。

広報は、EEAS 及び HRVP 報道官との間で調整されなければならない。

戦略／政治レベルの協力

潜在的活動主体

- 構成国に関し、サイバーセキュリティについて職責を負う大臣
- 欧州理事会に関し、議長
- 理事会に関し、輪番の議長国
- 「サイバー外交ツールボックス」内の措置の場合、PSC 及び横断作業部会
- 欧州委員会に関し、議長、または、委任を受けた副議長／コミッショナー
- 外務安全保障政策に関する欧州連合の上級代表／欧州委員会の副議長。

活動範囲: 悪意あるサイバー活動への EU の共同外交対応のための枠組みに基づく措置を含め、危機のサイバーな側面及び非サイバーな側面の両者の戦略的及び政治的管理。

状況認識共有:

- 欧州連合の機能に関する危機によって生じた混乱の影響の識別。

対応:

- インシデントの性質及び影響に応じた追加的な危機管理メカニズム／手段の発動。これらは、例えば、市民保護メカニズムを含め得る。
- 悪意あるサイバー活動への EU の共同外交対応のための枠組み内の措置。
- 例えば、それが適用可能となった後のサイバーセキュリティ緊急対応基金[1]の発動のような、影響を受けた構成国に対する緊急支援を利用可能とすること。
- それが適切なときは、国連（UN）、欧州安全保障協力機構（OSCE）及び特に NATO のような、国際機関との協力及び調整。
- 国家安全保障上及び国防上の意味合の評価。

広報:

公衆に向けた共通の広報戦略に基づく決定。

[1] サイバーセキュリティ緊急対応基金は、共同通知「回復力、抑止及び防衛：EU のための強力なサイバーセキュリティの構築」JOIN(2017) 450/1 の下で提案されている活動である。

IPCR 手順の枠組み内における EU レベルの構成国との協調対応

EU レベルの相補性の原則に従い、本節は、とりわけ、コア目標、並びに、構成国の機関、CSIRT ネットワーク、ENISA、CERT-EU、Europol/EC3、INTCEN、EU ハイブリッドフュージョンセル及び IPCR プロセス内のサイバー問題に関する理事会横断作業部会の職責及び活動を述べ、それに焦点を当てる。活動主体は、EU レベルまたは国内レベルで定められた手続に沿うものと推定される。

図 1 に示すように、EU の危機管理メカニズムの発動とは無関係に、（必要があるときは）補完性原則及び比例性原則に従うインシデント／危機を通じて、国内レベルの活動及び CSIRT ネットワーク内の協力が行われる。

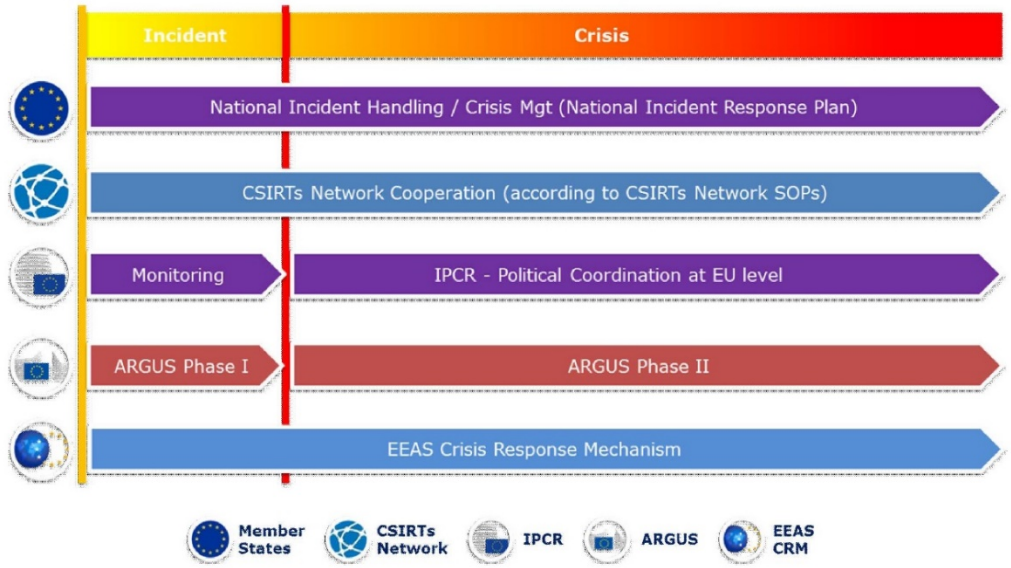

図 1 EU レベルのサイバーセキュリティインシデント／危機の対応

以下に示す全ての活動は、関係する協力の仕組みの標準的な運用手続／規則に従って、かつ、個々の活動主体及び機関の定められた任務及び職務権限に沿って、実施されなければならない。これらの手続／規則は、可能な最善の調整、及び、大規模サイバーセキュリティインシデント及び脅威への効果的な対応を達成するために、幾つかの追加または修正を必要とすることがあり得る。

ある特定のインシデントの間、以下に示す全ての活動主体が行動を執ることを要求されるというわけではない。ただし、計画書、及び、協力メカニズムの適切で標準的な運営手順は、それらの活動主体の潜在的な関与を想定するものでなければならない。

サイバーセキュリティインシデントまたは危機がもち得る社会に対する影響が異なるものであることに鑑み、全てのレベルにおける部門活動主体の関与に関する高い程度の柔軟性及び適切な対応は、サイバーな軽減対策活動及び非サイバーな軽減対策活動の両者によることになる。

サイバーセキュリティ危機管理－IPCR におけるサイバーセキュリティの統合

IPCR SOP[1]に示す IPCR 手順は、以下に示す段階を順に履むものとする（それらの段階の中の幾つかのものは、状況によって異なる）。

各段階において、我々は、サイバーセキュリティ固有の活動及び活動主体を指示する。読者の便宜にため、各段階において、計画書に固有の活動に続けて IPCR SOP からの文が提供される。

この段階を追うアプローチは、必要な能力及び手続においてサイバーセキュリティ危機への効果的な対応を妨げている既存の**ギャップ**を明確に識別することもできる。

（以下の [2]）図 2 は、IPCR プロセスを図示するものであり、新たに導入される要素は、青色で強調されている。

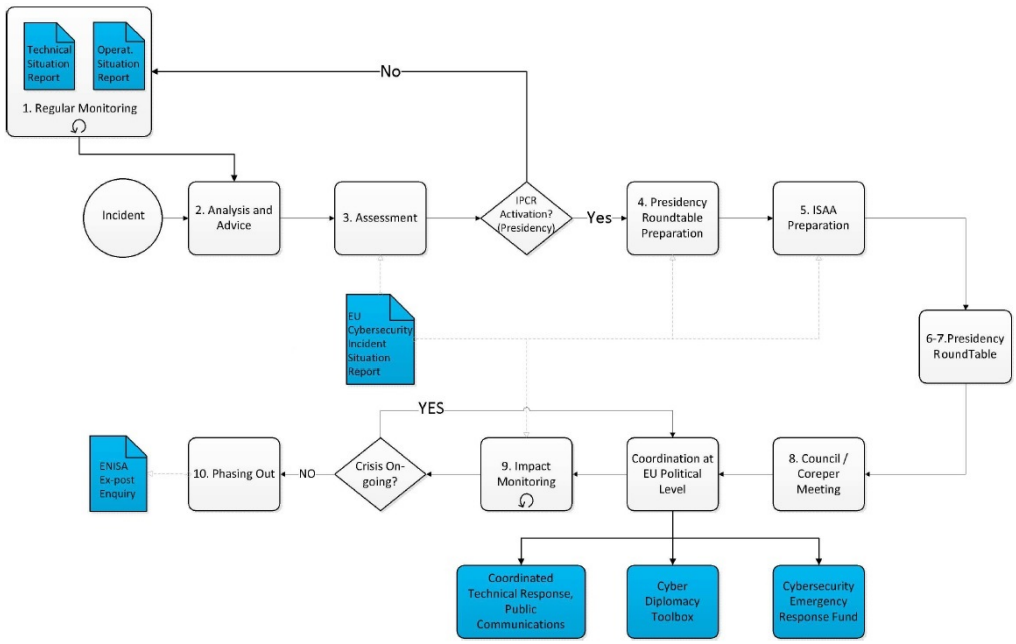

図 2：IPCR におけるサイバーセキュリティ固有の要素

注記：認識可能な危機の閾値よりも下のところにあるように設計されているサイバードメインにおけるハイブリッドな脅威の性質に鑑み、EU は、防止措置及び準備体制構築措置を実施する必要がある。EU ハイブリッドフュージョンセルは、関連インシデントを迅速に分析し、適切な調整組織に通知するための職務をもつ。フュージョンセルからの定期的な報告は、準備体制を拡大するための部門別の政策決定への情報提供に貢献し得る。

[1] 議長国の友グループによって合意され、2015 年 10 月にコレペールによって注記された文書 12607/15「IPCR 標準運営手順」による。

[2] より大きな版の図を付録の中に見つけることができる。

- **段階 1－部門別監視及び警報**：既存の、継続的な部門別状況報告及び警報は、理事会議長国に対し、拡大しつつある危機及びその展開の可能性に関する徴候を提供する。
  - **識別されたギャップ**：現在のところ、EU レベルのサイバーセキュリティインシデント（及び脅威）に関する継続的かつ調整されたサイバーセキュリティ状況報告及び警報は、存在しない。
  - **計画書：EU サイバーセキュリティ状況監視／報告**
    - サイバーセキュリティインシデント及び脅威に関する**継続的な EU サイバーセキュリティ技術状況報告書**は、インシデント及び脅威に関し、ENISA によって、一般に利用可能な情報、ENISA 自身の分析、（任意ベースで）構成国の CSIRT によって、または、NIS 指令の単一連絡部局、Europol の欧州サイバー犯罪センター（EC3）及び CERT-EU、並びに、欧州対外行動局（EEAS）の EU 情報活動分析センター（INTCEN）によって、ENISA との間で共有される報告に基づき、提供されることになる。この報告書は、理事会、欧州委員会、CSIRT ネットワークの関連する事項のために利用可能とされなければならない。
    - EU ハイブリッドフュージョンセルは、SIAC の代わりに、**EU サイバーセキュリティ運営状況報告書**をまとめなければならない。この報告書は、悪意あるサイバー活動への EU の共同外交対応のための枠組みも支援する。
    - 両者の報告書は、それらの利害関係者自身の状況認識に資するため、意思決定に情報提供するため、そして、国境を越える地域協力を容易にするため、EU 及び国内の利害関係者に対して供給される。

インシデントが検知された後

- **段階 2－分析と助言**：利用可能な監視及び警報に基づき、欧州委員会の関連部署、EEAS 及び GSC は、IPCR の発動可能性に関して議長国に助言する準備をするため、（全面または情報共有モードの）拡大可能性に関し、相互の情報提供を維持する。
  - **計画書**：
    - 欧州委員会に関し、DG CNECT、DG HOME、DG HR.DS 及び DG DIGIT は、ENISA、EC3 及び CERT-EU によって支援される。
    - EEAS。状況分析室の仕事及び情報資源を策定する EU ハイブリッドフュージョンセルは、サイバー脅威を含め、EU 及びそのパートナーに影響を与える現実のハイブリッドな脅威及び潜在的なハイブリッドな脅威に関する状況認識を提供する。それゆえ、EU ハイブリッドフュージョンセルの分析及び評価が、構成国、パートナーである国または組織に対する直接の脅威が存在することを示す場合、（最初の段階で）INTCEN は、定められた手続に従い、運営レベルに情報提供する。そして、運営レベルは、監視モードの危機管理手順（例：EEAS 危機対応メカニズムまたは IPCR 監視ページ）の発動の可能性を含め、政治戦略的レベルのための勧告を準備する。
    - CSIRT ネットワークの議長は、ENISA の補佐を受け、EU サイバーセキュリティインシデント状況報告書[1]を準備し、それは、輪番の議長国を介して、議長国、欧州委員会及

[1] EU サイバーセキュリティ状況報告書は、国内 CSIRT から提供される国内報告書の合綴である。報告書の

び HRVP に対して提示される。

- **段階 3－IPCR 発動に関する評価／決定**：議長国は、政治的調整、情報交換、または、EU レベルの意思決定の必要性を検討する。その目的のために、議長国は、非公式のラウンドテーブルを招集できる。議長国は、コレペールまたは理事会の関与を要する領域の最初の識別を実施する。これは、統合状況認識及び分析（ISAA）の作成のためのガイダンスの基礎を構成する。議長国は、危機の特性、そのあり得る結果、及び、関連する政治上の必要性に照らし、関連する理事会作業部会及びまたはコレペール及びまたは PSC の会合を招集することの適切性に関し、判断する。
  - **計画書**：
    - ラウンドテーブル参加者：
      - 欧州委員会の関連部署及び EEAS は、それぞれの職務権限のある分野に関し、議長国に対して助言する。
      - 各国からの専門家（CSIRT、サイバーセキュリティの職務権限を有する機関、その他）による支援を受けるサイバー問題に関する横断作業部会内の構成国の代表。
      - 最新の EU サイバーセキュリティインシデント状況報告書に基づく ISAA 報告のための政治的／戦略的ガイダンス、及び、ラウンドテーブル参加者から提供される追加的な情報。
      - 関連する作業部会及び委員会：
        - サイバー問題に関する横断作業部会内。

欧州委員会、EEAS 及び GSC は、全面的に合意し、かつ、議長国に参与し、あり得る全面発動のための基礎を準備するために、危機ページを生成することにより、情報共有モードによる IPCR の発動を決定することもできる。

- **段階 4－IPCR 発動／情報収集及び情報交換**：（情報共有モードまたは全面発動のいずれかの）発動に基づき、ISAA へのフィード及び政治レベルの討議の準備に貢献する側面に焦点を当て、特定の情報の交換ができるようにする IPCR Web プラットフォーム上に危機ページが生成される。ISAA 主務部署（欧州委員会の関連部署または EEAS のいずれか）は、事案の状況によって異なる。

- **段階 5－ISAA 作成**：ISAA 報告書の作成が開始される。欧州委員会／EEAS は、ISAA SOP に概要が示される ISAA 報告書を発し、また、IPCR Web プラットフォーム上において、更に情報交換を促進することができ、または、情報提供を求める特別の要求を発することができる。ISAA 報告書は、議長国によって決定され、かつ、そのガイダンスの中で定められているとおり、そして、議長国によって決定される議題に関し、戦略上の状況認識と情報提供を受けた上での討議を可能とするため、政治レベル（コレペールまたは理事会）の必要性に応じて個別化される。ISAA SOP に従い、サイバーセキュリティ危機の性質によって、ISAA 報告書が欧州委員会の関連部署（CNECT、DG HOME）または EEAS のいずれによって準備されるのかが決定されることになる。

フォーマットは、CSIRT ネットワーク SOP の中で示される。

IPCR の発動後、議長国は、政治的な調整及びまたは理事会内の意思決定プロセスを議長国が支援するために、ISAA が焦点を当てる特別の分野の概要を示す。議長国は、欧州委員会の関連部署／EEAS との協議を経た後、報告書の時機も決定する。

- **計画書**:
  - ISAA 報告書は、以下を含め、関連部署からの情報を含める:
    - EU サイバーセキュリティインシデント状況報告書の形式で、CSIRT ネットワーク。
    - EC3、状況分析室、EU ハイブリッドフュージョンセル、CERT-EU は、ISAA 主務部署及び IPCR ラウンドテーブルに対し、しかるべく、支援し、かつ、寄与を提供する。
    - 影響を受ける部門の別により、EU の各部門の部局及び組織。
    - （CSIRT 以外の）構成国の機関。
  - ISAA への入力の集約[1]:
    - 欧州委員会及び EU の部局。ARGUS IT システムは、ISAA のための内部バックボーンネットワークを提供する。EU の部局は、それぞれの職責のある DG にそれらの部署の情報を送付し、それらの DG は、順次、ARGUS の中へ関連情報をフィードする。欧州委員会の関連部署及び部局は、構成国及び国際機関の既存の部門別ネットワークから、並びに、それ以外の関連情報源から、情報を収集する。
    - EEAS の場合。EU 情報分析室は、EEAS の関連部署によって支援を受け、内部バックボーンネットワーク及び ISAA との単一連絡先を提供する。EEAS は、第三国及び関連国際機関から情報を収集する。

- **段階 6－非公式議長国ラウンドテーブルの準備**:議長国は、理事会の事務総局の補佐を受け、非公式ラウンドテーブルの時機、議題、参加者、及び、予想される結果（可能な成果物）を決定する。GSC は、議長国の代わりに、IPCR Web プラットフォーム上で関連情報を伝達し、とりわけ、会合の通知を発する。

- **段階 7－議長国ラウンドテーブル／EU 政治的調整の準備措置／意思決定**:議長国は、状況の見直しをするため、並びに、コレペールまたは理事会の注意を惹くための項目を準備し、見直しをするため、非公式のラウンドテーブルを招集する。また、非公式のラウンドテーブルは、コレペール／理事会に対して送付されるべき全ての活動提案書に関し、その作成、見直し及び討議をするための場ともなる。
  - **計画書**:
    - サイバー問題に関する理事会横断作業部会は、PSC またはコレペールを準備する。

- **段階 8－コレペールにおける政治的調整及び意思決定／理事会**:全てのレベルにおける対応活動の調整、例外的措置の決定、政治宣言等と関係するコレペール／理事会の会合の結論。これらの決定は、別の ISAA 報告書作成のための更新された政治／戦略ガイダンスを構成するもの

[1] ISAA SOP

でもある。

- **計画書**:
  - サイバーセキュリティ危機への対応を調整する政治的決定は、**対応**及び**広報**に関する上述の第 1 節「戦略／政治、運営及び技術の各レベルにおける協力」に示す（それぞれ対応する活動主体によって遂行される）活動を介して、実装される。
  - ISAA の作成は、これも上述の第 1 節に示される状況認識に関する技術、運営及び政治／戦略の各レベルにおける調整に基づき、継続される。

- **段階 9－影響の監視**：ISAA 主務部署は、ISAA 情報提供者の支援を受け、危機の拡大に関する情報、及び、行われた政治的決定の影響に関する情報を提供する。このフィードバックのループは、変化するプロセスを支援し、かつ、EU の政治レベルの関与を継続するか、または、ICPR を終了させるかの議長国の判断を支援する。

- **段階 10－終了**：発動に関するのと同じプロセスの後、議長国は、IPCR 発動を維持するか否かの可能性を検討するため、非呼応式のラウンドテーブル会合を招集できる。議長国は、発動の終了または、そのモードを下げることを決定できる。
  - **計画書**:
    - ENISA は、その任務の条項に従い、インシデントの事後的な技術調査に貢献し、または、それを実施するために招請され得る。

付 録

1. EU レベルの危機管理、協力メカニズム及び活動主体

危機管理のメカニズム

統合政治危機対応手順（IPCR）：2013 年 6 月 25 日に理事会によって承認された[1]統合政治危機対応手順（IPCR）は、重大な危機が発生した際、EU の政治レベルの適時な調整及び対応を容易にするために設計されている。IPCR は、2014 年 6 月 24 日に採択された連携条項の欧州連合による実装に関する理事会決定 2014/415/EU に定める連携条項（TFEU 第 222 条）の呼出しへの対応の政治レベルにおける調整を支援する。ICPR 標準運用手順（SOP）[2]は、発動プロセス及びその後に行われる活動を定める。

ARGUS：複数部門の重大な危機の場合における特別の調整プロセスのために、2005 年に欧州委員会によって設置された危機調整システム。ARGUS は、同じ名前をもつ一般緊急警報システム（IT ツール）によって支援される。ARGUS は、2 つのフェーズを予定しており、（複数部門の重大な危機の場合の）フェーズ II は、欧州委員会の議長またはその職責が割り当てられた委員長の承認の下で、危機調整委員会（CCC）の会合により発動される。CCC は、欧州委員会の危機対応を主導及び統括するため、欧州委員会の関連総局、官房及び他の EU の部署の代表を集める。CCC は、副事務総長によって主宰され、状況を検討し、選択肢を判断し、欧州委員会の責任の下で、EU のツール及び法律文書に関する発動可能な決定を行い、そして、その決定が実装されることを確保する[3][4]。

EEAS 危機対応メカニズム：EEAS 危機対応メカニズムは、対外的な性質または重要な対外的局面をもち、（ハイブリッドな脅威を含め）EU の利益または構成国の利益に潜在的または現実的に影響を与える危機及び緊急事態に対応するために構築された EEAS のためのシステムである。関連する委員会及び理事会事務総局の官吏のその会合への参加を確保することにより、その CRM は、欧州委員会によって管理される財政、貿易及び会社の法律文書の波及効果が外交、安全保障及び防衛の努力の間に及ぶことを促進する。危機セルは、危機のある間、発動され得る。

協力のメカニズム

CSIRT ネットワーク：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は、全ての国内

---

[1] 2013 年 6 月 24 日に理事会によって承認された「CCA 見直しプロセスの結了：EU 統合政治危機対応手順」に関する文書 10708/13

[2] 議長国の友グループによって合意され、2015 年 10 月にコレペールによって注記された文書 12607/15「IPCR 標準運営手順」

[3] 欧州委員会は「ARGUS」一般緊急警報システム上で提供する COM(2005) 662 final, 2005 年 12 月 23 日

[4] 「ARGUS」一般緊急警報システムに関しては、内部手続規則を改正する 2005 年 12 月 23 日の委員会決定 2006/25/EC, Euratom（OJ L 19, 24.1.2006, p. 20）

CSIRT 及び政府 CSIRT 並びに CERT-EU を集める。このネットワークの目的は、脅威及びサイバーセキュリティインシデントに関する CSIRT 内の情報共有を可能とし、それを拡大することであり、そして、サイバーセキュリティインシデント及び脅威への対応において協力することでもある。

サイバー問題に関する理事会横断作業部会：この作業部会は、理事会内におけるサイバー政策上の問題の戦略的かつ横断的な調整を確保するために設置されたものであり、立法活動及び非立法活動の両者に関与し得る。

活動主体

ENISA：欧州連合ネットワーク情報セキュリティ局は、2004 年に設置された。局は、汎欧州サイバーセキュリティ演習、国内サイバーセキュリティ戦略の策定、CSIRT の協力及び能力開発のような課題に関し、助言とソリューションを提供するため、構成国及び民間部門と緊密に連携して仕事をする。ENISA は、EU 全域において CSIRT と直接に共働し、かつ、CSIRT ネットワークの事務局である。

ERCC：（欧州委員会人道援助市民保護総局－DG ECHO の下にある）欧州委員会緊急対応調整センターは、24/7 ベースで、幅広い防止活動、準備活動及び対応活動を支援し、調整する。このセンターは、2013 年に発足し、IPCR の 24/7 連絡部局としての活動を含め、欧州委員会の危機対応のハブとして（EU の他の危機管理室と連絡をとりながら）活動する。

Europol/EC3：Europol 内に 2013 年に設置された欧州サイバー犯罪センター（EC3）は、EU 内のサイバー犯罪に対する法執行対応を支援する。EC3 は、構成国の捜査機関及び行政機関に対する犯罪情報の中央ハブとしての運営上及び分析上の支援を提供し、また、運営上の分析、調整及び専門知識並びに高度に専門的な技術及びデジタル法科学支援能力によって、構成国による運営及び捜査を支える情報を提供する。

CERT-EU：EU の機関、組織及び部局のコンピュータ緊急対応チームは、サイバー脅威に対する EU の機関、組織及び部局の保護を向上させる任務をもつ。CERT-EU は、CSIRT ネットワークの構成員である。CERT-EU は、NATO CIRC、幾つかの第三国、及び、サイバーセキュリティ分野の主要な商業上の活動主体との間で、サイバー脅威に関する情報共有に関し、技術的な協定を結んでいる。

EU の諜報機関は、**単一情報分析部**（SIAC）の SIAC 覚書に基づき、EU 情報活動分析センター（INTCEN）、EU 軍参謀本部（EUMS）、EU 軍参謀本部情報部（EUMS INT）で構成されている。SIAC の任務は、外務安全保障政策に関する欧州連合の上級代表、及び、欧州対外行動局（EEAS）に対し、情報分析、早期警戒及び状況認識を提供することである。SIAC は、外務安全保障政策（CFSP）、共通安全保障防衛政策（CSDP）及び対テロリズム（CT）の分野における EU の様々な意思決定機関に対し、並びに、構成国に対し、そのサービスを提供する。EU INTCEN 及び EUMS INT は、作戦機関ではなく、収集能力をもたない。作戦レベルの諜報活動は、構成国の責任に属する。SIAC は、単に戦略分析を取り扱うだけである。

EU ハイブリッドフュージョンセル：ハイブリッドな脅威への対抗に関する 2016 年 4 月の共同通知は、EU におけるハイブリッドな脅威に関する全ての情報分析のための中心点として、EU ハイブリッドフュージョンセル（EU HFC）を指定した：その任務は、機関間協議を通じて、2016 年 12 月に、欧州委員会から承認された。INTCEN を基礎として、EU ハイブリッドフュージョンセルは、SIAC の一部であり、それゆえ、EUMS INT と共同で仕事をし、かつ、軍常設機関の地位をもつ。ハイブリッドとは、サイバー攻撃、虚偽情報キャンペーン、スパイ活動、経済的圧力、代理戦、または、それ以外の破壊活動のような、国家または非国家の活動主体による、黙示／明示、軍用／民間用の道具及び梃子の多角的な組み合わせの意図的な使用のことを指す。EU HFC の仕事は、欧州委員会及び構成国の両者内において、統合化された対応／多様な課題に対応するために必要な政府全体のアプローチの提供するための拡大されたネットワーク上の連絡部局（PoC）の仕事に従事する。

EU Sitroom：EU 状況分析室は、EU 情報活動分析センター（EU INTCEN）の一部であり、EEAS に対し、危機の軽減及び効果的な対応を確保するための運営能力を提供する。それは、24/7 の能力をもち、世界規模の監視及び状況認識を提供する常設の軍民後方支援組織である。

関連する手段

悪意あるサイバー活動への EU の共同外交対応のための枠組み：2017 年に合意されたこの枠組みは、EU のサイバー外交のアプローチの一部であり、混乱の防止、サイバーセキュリティ脅威の軽減、及び、国際関係におけるより大きな安定性に貢献するものである。この枠組みは、それが必要なときは、抑止手段を含め、共通外交安全保障政策内の全ての措置を利用する。その枠組み内における措置の利用は、協力を推進し、そして、即時の脅威及び長期にわたる脅威の軽減を容易にし、かつ、責任のある加害者及び潜在的な侵略者の長期にわたる行動に影響を与えるものでなければならない。

2. IPCR 手順のサイバーセキュリティ危機調整－横断的調整レイヤ及び政治的エスカレーション

IPCR 手順は、技術的問題及び運営上の問題に対応するために使用され得る（そして、使用されてきた）ものであるが、常に、政治／戦略の確度から使用される。

エスカレーションの面において、IPCR は、IPCR 発動の最初の段階である「監視モード」から「情報共有モード」、そして、「IPCR 全面発動」へと遷移することにより、危機のレベルに応じて使用され得る。

全面モードの発動は、EU の理事会の輪番の議長国が決定することである。欧州委員会、EEAS 及び GSC は、情報共有モードの IPCR を発動できる。監視モード及び情報共有モードは、異なるレベルの情報交換の引き金となり、情報共有モードは、ISAA 報告書の作成を求める要求を発動させる。全面発動は、議長国をテーブルにつかせる IPCR ラウンドテーブル会合をツールボックスに加える（典型的には、コレペール II の議長、または、常駐代表部の特定分野の専門家レベルであるが、例外的に、大臣レベルでラウンドテーブルがもたれることがあった。）。

活動主体:

輪番の議長国（典型的にはコレペール議長）が主宰する。
欧州理事会に関しては、議長官房
欧州委員会に関しては、DSG/DG レベル及びまたは特定分野の専門家
EEAS に関しては、DSG/MD レベル及びまたは特定分野の専門家
GSC に関しては、事務総局官房、IPCR チーム及び職責を負う DG。

活動範囲: 政治レベルでそれらに対応するため、3 つのレベルそれぞれのボトルネックまたは欠点の状況及びエスカレートされる認識の共通の統合された像を生成すること、参加者の権限の範囲内にあるときは、そのテーブルにおいて決定を生成すること、または、コレペール II もしくは理事会宛に、行動の提案を生成すること。

状況認識共有:

（発動がない場合）: EU が予期しない危機に発展し得るような展開しつつある状況を追跡するため、IPCR の監視ページを生成し得る。

（IPCR 情報共有）: 欧州委員会の関連部署、EEAS 及び（IPCR 質問窓口を介する）構成国からの入力に基づき、ISAA 主務部署によって、ISAA 報告書が起草される。

（IPCR 全面発動）: ISAA 報告書に加え、公式 IPCR ラウンドテーブルは、欠点及びボトルネックを討議するため、軍参謀本部（MS）内の様々な活動主体、欧州委員会、EEAS、関連部局等を集める。

協力及び対応:

インシデントの性質及び影響の相違に応じて、追加的な危機管理のマネジメント／手段の発動／同期化。これらは、例えば、市民保護メカニズム、悪意あるサイバー活動への EU の共同外交対応のための枠組み、または、「ハイブリッドな脅威への対抗に関する共同枠組み」を含めることができる。

危機の連絡:

IPCR 危機報道ネットワークは、共通メッセージの作成を支援するため、または、最も効果的な広報ツールを練るため、欧州委員会内の関連部署、GSC 及びEEASとの協議を経た上で、議長国によって発動され得る。

3. ARGUS のサイバーセキュリティ危機管理－欧州委員会内の情報共有

欧州レベルの活動が要求される予期できない危機、すなわち、マドリッドのテロ攻撃（2004 年 3 月）、東南アジアの津波（2004 年 12 月）及びロンドンのテロ攻撃（2005 年 7 月）に直面し、欧州委員会は、2005 年、その名を冠する一般的な緊急警報システムによって支援される ARGUS 調整システムを設けた [12]。それは、リアルタイムで危機関連情報を共有できるようにするため、及び、迅速な意思決定を確保するため、複数の部門の重大な危機の場合において特別の**危機調整プロセス**を提供することを狙いとする。

ARGUS は、出来事の深刻度に応じて、2 つのフェーズを定める:

フェーズ I:は、限定された規模の危機に対し、「情報共有」のために使用される

フェーズ I で報告された近年の出来事の例は、ポルトガル及びイスラエルの山火事、2016 年のベルリン攻撃、アルバニアの洪水、ハイチのハリケーン・マシュー及びボリビアの干ばつを含む。事務総局は、その職務権限のドメインにおける状況が、正当化するため、または、情報共有からの利益を享受するために十分な深刻さをもつと事務総局が判断する場合、フェーズ I を開始できる。例えば、DG CNECT または DG HOME は、それぞれの機関の職務権限のドメインにおけるサイバー状況が、正当化するため、または、情報共有からの利益を享受するために十分な深刻さをもつとそれらの機関が判断する場合、フェーズ I を開始できる。

フェーズ II:は、複数部門の重大な危機、または、予測可能もしくは差し迫った欧州連合の脅威の場合において、引き金となる。

フェーズ II は、欧州委員会が、その職務権限のドメインにおける最高のレベルで、かつ、他の機関と協力して、迅速であり、調整され、かつ、一貫性のある対応を決定し、管理することができるようにする特別の調整手続の引き金となる。フェーズ II は、複数部門の重大な危機、または、予測可能もしくは差し迫った脅威のための措置である。現実の生活において発生したフェーズ II の出来事の例は、移民／難民危機（2015 年～現在）、福島の 3 重災害（2011 年）、及び、アイスランドのエイヤフィヤトラヨークトル火山の噴火（2010 年）である。

フェーズ II は、彼自身の発意により、または、欧州委員会の構成員の要請により、議長によって発動される。議長は、その危機と最も関係の深いサービスについて職責を負う委員長に対応する委員会に対してその政治的な職責を割り当てることができ、または、彼自身にその職責を維持することを決定することができる。

フェーズ II は、危機調整委員会（CCC）の緊急会合を予定する。その会合は、議長の権限に基づいて、または職責が割り当てられた委員長の権限に基づいて要求される。その会合は、ARGUS IT ツールを介し、事務総局によって招集される。CCC は、欧州委員会の関連総局、官房及び他の EU の部署

[1] 欧州共同体の委員会、2005 年 12 月 23 日、欧州委員会から欧州議会、理事会、欧州経済社会委員会及び地域委員会宛通知:欧州委員会は、「ARGUS」一般緊急警報システム上で提供する、COM(2005) 662 final

[2] 決定 2006/25/EC, Euratom

の代表を集め、欧州委員会の危機対応を主導及び統括するために設置された特別の運営上の危機管理組織の 1 つである。**CCC は、副事務総長によって主宰され、状況を検討し、選択肢を判断し、及び、決定を行い、また、**その職責との整合性及び一貫性を確保しつつ、**その決定及び活動が実装されることを確保する**。CCC に対する支援は、事務総局から提供される。

4. EEAS 危機対応メカニズム

EEAS の危機対応メカニズム（CRM）は、EU の対外的な局面を含むような重大な状況または深刻な事態の発生に基づき、発動される。CRM は、HRVP または事務総局との協議を経た上で、危機対応に関する DSG によって発動される。危機対応に関する DSG は、HRVP もしくは SG または他の DSG もしくは MD から、危機管理メカニズムを開始することを要請され得る。

CRM は、安全保障戦略内における危機対応において、EU の一貫性に貢献する。とりわけ、CRM は、欧州委員会によって管理される財政、貿易及び会社の法律文書の波及効果が外交、安全保障及び防衛の努力の間に及ぶことを促進する。

CRM は、同時発動の場合における波及効果を発揮させるため、欧州委員会の一般緊急対応システム（ARGUS）及び EU 統合政治危機対応手順（IPCR）と連携している。EEAS の状況分析室は、EEAS と、理事会及び欧州委員会の緊急対応システムとの間の連絡ハブとして活動する。

通常、CRM 実装と関連する最初の活動は、EEAS、当の危機によって直接に影響を受けた欧州委員会及び理事会の上級管理者の間における危機会合の要求である。危機会合は、その危機の短期的影響を評価し、即時の行動を執ることに合意することができ、または、危機セルの発動を合意し、または、危機プラットフォームの招集を合意する。

危機セルは、小規模なオペレーション室であり、EEAS 本部の意思決定への支援を提供するため、その危機への対応に関与する EEAS、欧州委員会及び理事会の関連部署の代表が状況を継続的に監視するためにそこに集まる。危機セルは、発動されると、1 日 24 時間、週 7 日の態勢で運用される。

危機プラットフォームは、その危機の中長期的な影響に関する評価を提供し、講じられるべき措置を合意するため、EEAS、欧州委員会及び理事会の関連部署を集める。危機プラットフォームは、HRVP もしくは事務総局によって、または、危機対応に関しては DSG によって主宰される。危機プラットフォームは、危機にある国または領域における EU の活動の実効性を評価し、措置の補正または追加を決定し、かつ、理事会に対する提案を討議する。危機プラットフォームは、アドホックな会合である;それゆえ、それは、恒常的には発動しない。

タスクフォースは、対応に関与する部署の代表で構成され、EU の対応の実装に従い、かつ、それを容易にするために発動され得る。タスクフォースは、EU の活動の影響を評価し、政策文書及び予備文書を準備し、危機アプローチのための政治的枠組み（PFCA）の準備に貢献し、そして、EU の対応の実装を容易にすることのできる上記以外の覚書を採択する。

5. 参考文献

以下は、計画書を準備する際に考慮に入れた文書の一覧である。

- The European Cyber Crises Cooperation Framework, Version 1, 17 October 2012.
- Report on Cyber Crisis Cooperation and Management, ENISA, 2014
- Actionable Information for Security Incident Response, ENISA, 2014
- Common practices of EU-level crisis management and applicability to cyber crises, ENISA, 2015
- Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, 2016
- EU Cyber Standard Operating Procedures, ENISA, 2016
- A good practice guide of using taxonomies in incident prevention and detection, ENISA, 2017
- Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final, 5 July 2016
- Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry — Council conclusions (15 November 2016), 14540/16
- Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (OJ L 192, 1.7.2014, p. 53)
- Finalisation of the CCA review process: the EU Integrated Political Crisis Response (IPCR) arrangements, 10708/13, 7 June 2013
- Integrated Situational Awareness and Analysis (ISAA) — Standard Operating Procedures, DS 1570/15, 22 October 2015
- Commission provisions on 'ARGUS' general rapid alert system, COM(2005) 662 final, 23 December 2005
- Commission Decision 2006/25/EC, Euratom of 23 December 2005 amending its internal Rules of Procedure (OJ L 19, 24.1.2006, p. 20)
- ARGUS Modus Operandi, European Commission, 23 October 2013
- Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), Doc. 9916/17
- EU operational protocol for countering hybrid threats 'EU Playbook', Doc. SWD(2016) 227
- EEAS Crisis Response Mechanism, 8 November 2016 (Ares(2017)880661) Joint Staff Working Document EU operational protocol for countering hybrid threats, 'EU Playbook', SWD(2016) 227 final, 5 July 2016
- Joint Communication to the European Parliament and the Council: Joint
- EEAS(2016) 1674 — Working Document of the European External Action Service — EU Hybrid Fusion Cell — Terms of Reference

6. IPCR プロセスにおけるサイバーセキュリティ固有の諸要素