欧州委員会

ブリュッセル、2025 年 2 月 24 日

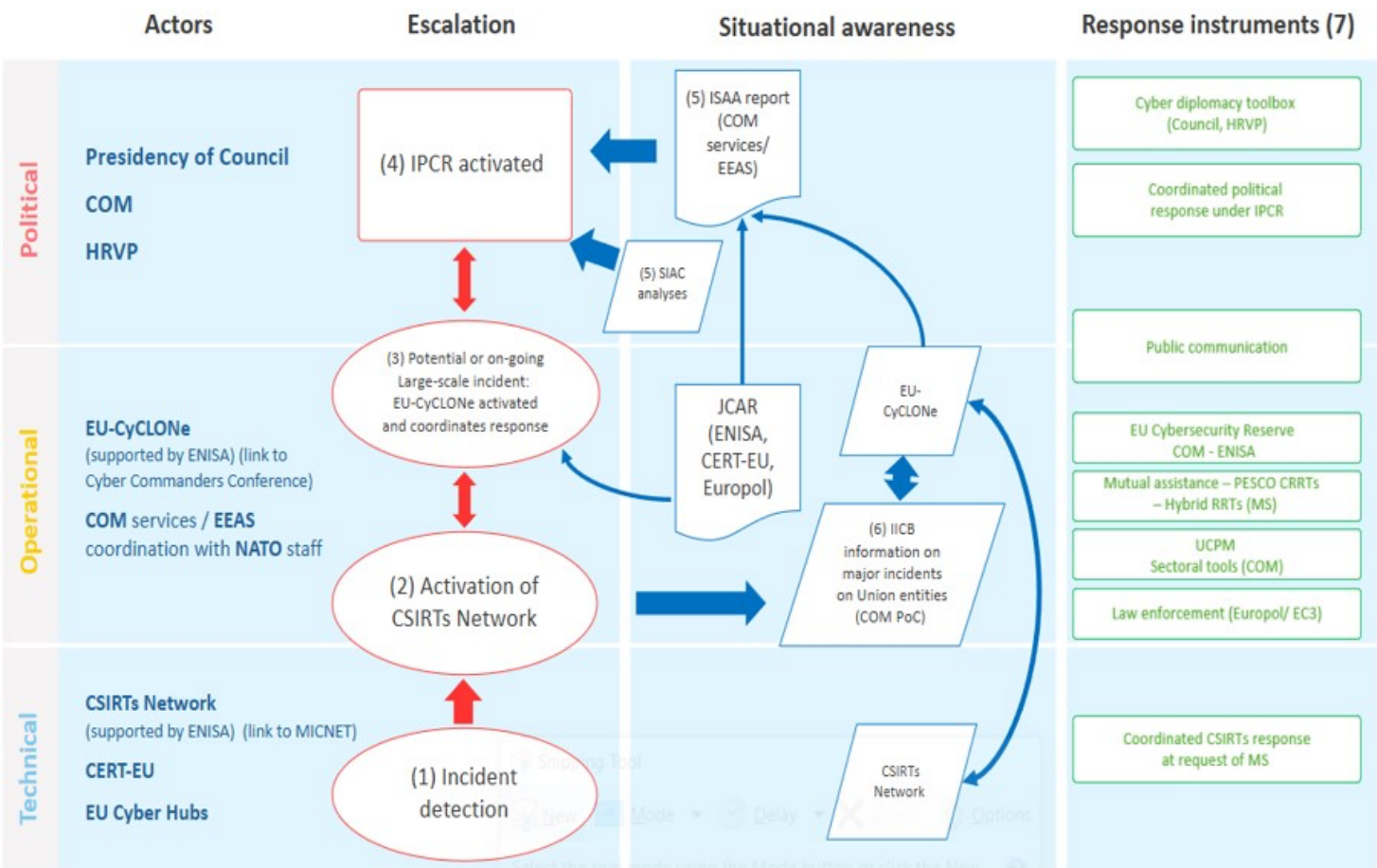
COM(2025) 66 final

附属書 1～3

サイバーセキュリティ危機管理に関する EU の青写真に関する欧州理事会勧告の提案の附属書

附属書 I - サイバーセキュリティ危機に対応するための EU の青写真

下図は、以下の附属書 II の関連する EU 危機メカニズムに従って、EU サイバーセキュリティ危機において誰が誰と話し合うかという、EU サイバー青写真を図示し要約したものである。このような危機は、必然的に 1 つ以上の重要な部門に現実の影響を及ぼすことになるため、サイバー・コミュニティと部門および市民保護の対応メカニズムとの緊密な連携が必要となる。サイバーインシデントは、より広範なハイブリッドキャンペーンの一部である可能性があり、したがってサイバー対応は、欧州連合の準備戦略に沿って他の行動と調整されるべきである。



(1) CSIRI や国境を越えたサイバーハブが大規模サイバーセキュリティインシデントを検知する。

(2) CSIRTS ネットワークは、内部手順に従ってエスカレーションを行う。

(3) EU-CyCLONe は、大規模なインシデントが発生した場合の作戦対応を調整する。

(4) 理事会議長国は、加盟国、欧州委員会および上級代表者と協議の上、EU（IPCR）危機管理体制を作動させるか停止させるかを決定する。

(5) IPCR が発動された場合、欧州委員会のサービスと EEAS が作成した ISAA 報告書が協議に反映される。EU-CyCLONe および JCAR は、ISAA にインプットを提供すべきである。理事会は SIAC の分析からも情報を得る。

(6) CERT- EU は、EU の事業体に影響を及ぼす危機への業務上の対応を担当する。関連情報は、欧州委員会を窓口として、IICB から EU-CyCLONe に提供される。

(7) EU 理事会、EU-CyCLONe および CSIRTs ネットワークは、それぞれ政治レベル、運用レベルおよび技術レベルでの対応を統括する。

附属書 I- 関連する EU レベルのアクター（事業体およびネットワーク）及び危機管理メカニズム

(1)　サイバー危機管理のライフサイクル全体にわたって関連する組合レベルのアクター

レベル／段階	準備	検知	対応	回復
政治	• 評議会 • 委員会 • EEAS		• 理事会 • 欧州委員会 • 欧州委員会	
運用	• EU-CyCLONe • ENISA • 欧州委員会 • 欧州刑事警察機構		• EU-CyCLONe • 欧州委員会 • ENISA • CERT-EU（EU 事業体に影響を及ぼすインシデント用） • 欧州刑事警察機構	• ENISA
技術	• CSIRTs ネットワーク • 国境を越えたサイバーハブ • CERT-EU	• CSIRTs ネットワーク • 国境を越えたサイバーハブ • CERTEU	• CSIRTs ネットワーク • CERT-EU	• CSIRTs ネットワーク • CERT-EU

(2) サイバー危機管理に関連する EU レベルの関係者（アルファベット順）の役割と能力

アクター	レベル	役割と能力	参照
CERT-EU	技術／運用	EU 事業体に影響を及ぼす重大インシデントへの対応と管理を調整する。 CSIRTs ネットワークのメンバーである。 EUCyCLONe において欧州委員会を支援する。 サイバーセキュリティ情報交換およびインシデント対応調整のハブとして機能し、EU 事業体およびカウンターパート間のインシデント、サイバー脅威、脆弱性、ニアミスに関する情報交換を促進する。 EU 事業体を代表して、EU サイバーセキュリティ予備軍の展開を要請する。 技術協定に基づき、NATO サイバーセキュリティセンターと協力する。	規則（EU、Euratom）2023/2841
EU 理事会議長国	政治	欧州連合機能条約第 222 条に基づき連帯条項が発動される場合を除き）加盟国の要請に応じて、適宜、影響を受ける加盟国、欧州委員会および人事部と協議の上、IPCR を発動するか非発動にするかを決定し、いつ一方の発動モードから他方の発動モードにエスカレーションまたはデスカレーションするかを決定する。	欧州連合条約第 16 条 EU 理事会実施決定(EU) 2018/1993
国境を越えたサイバーハブ	技術	3 つ以上の国のサイバーハブで構成され、国境を越えたハブ内でサイバー脅威、ニアミス、侵害の指標、サイバーアラートに関連する関連情報の交換を確保する。 CSIRTs ネットワークと密接に協力し、情報を共有する。 EU-CyCLONe および CSIRTs Network を通じて、加盟国当局および欧州委員会に、潜在的または進行中の大規模サイバーセキュリティインシデントに関連する情報を提供する。	規則(EU) 2025/38
CSIRTs ネットワーク	技術	インシデント、ニアミス、サイバー脅威、リスク、脆弱性に関する関連情報を交換する。 インシデントの影響を受ける可能性のあるメンバーの要請により、ネットワークは、インシデント及び関連するサイバー脅威に関連する情報を交換し、議論する。	指令(EU) 2022/2555 の第 15 条

アクター	レベル	役割と能力	参照
		ネットワークはまた、要請を受けた加盟国の管轄内で識別されたインシデントに対して、協調的な対応を実施することもできる。 加盟国から EU サイバーセキュリティ・リザーブへの要請に関する情報を受け取る。	
サイバー司令官会議		加盟国の国家レベルのサイバー指揮官が、現在進行中のサイバー空間での作戦や大規模なサイバーインシデントを緩和するための戦略について協力し、重要な情報を交換するためのフォーラム。欧州連合理事会の持ち回り議長国が主催し、欧州防衛庁（EDA）、欧州対外活動庁（EEAS）、EU 軍参謀本部（EUMS）が後援している。	サイバー防衛共同コミュニケーション
欧州委員会	運用／政治	域内市場の円滑な機能の確保 IPCR メカニズムに分析報告書（ISAA）をプロバイダとして提供する。 緊急対応調整センターおよび共通緊急コミュニケーション・情報システムの管理を含む、一般的な準備活動 EU-CyCLONe のオブザーバーであり、大規模なインシデントが発生する可能性がある場合、または発生しつつある場合に加盟する。 CSIRTS ネットワークのオブザーバー EU サイバーセキュリティ・リザーブの実施に関する全体的な責任を負う。 大規模インシデントに関する関連情報を EUCyCLONe と共有するための、機関間サイバーセキュリティ委員会の窓口となる。 ガリレオ・セキュリティ・モニタリング・センターの戦略的監督。(GSMC）IPCR の起動または停止に関する決定について、理事会議長から諮問を受ける。欧州委員会の業務は、EEAS とともに ISAA 報告書を作成する。	欧州連合条約第 17 条 実施 決定 (EU) 2018/1993 欧州議会および理事会の決定 No.1313/2013/EU 指令（EU）2022/2555 規則(EU) 2025/38 規則 (規則（EU, Euratom） 2023/2841
欧州サイバーセキュリティ機関（ENISA）	技術/運用	CSIRTs ネットワークと EU-CyCLONe の事務局を提供する。 国境を越えた大規模なインシデントや危機に対する共通の対応策の策定を支援する： 各国の情報源からの報告を集約し、分析する。	NIS 2 指令（EU）2022/2555 規則（EU）2019/881

アクター	レベル	役割と能力	参照
		技術、運用、政治レベル間の情報の流れを確保する。 インシデントハンドリングの促進 公的コミュニケーションに関して EU 事業体を支援する。 インシデント対応能力をテストする。 サイバー連帯法の規定に従い、EU サイバーセキュリティ準備金の一部または全部を運用・管理する。 特定の重要なまたは大規模なサイバーインシデントについて、脅威、既知の脆弱性、緩和措置をレビューし、アセスメントする。 インシデントレビュー報告書を作成する。	規則（EU）2025/38 規則（EU）2024/2847
欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）	運用	大規模サイバーセキュリティインシデントと危機の運用レベルでの協調的管理を支援する。 加盟国および欧州連合の機構、団体、事務所、機関間の関連情報の定期的な交換を確保する。 大規模なサイバーセキュリティインシデントや危機の管理を調整し、そのようなインシデントや危機に関する政治レベルでの意思決定を支援する。 関連する大規模サイバーセキュリティインシデントと危機の結果と影響をアセスメントし、可能な緩和策を提案する。 ENISA とともに、EU サイバーセキュリティ準備金への支援要請の提出を容易にするためのテンプレートを作成する。 加盟国から EU サイバーセキュリティ・リザーブへの要請に関する情報を受け取る。 国境を越えたサイバーハブまたは CSIRTs Network から、潜在的または進行中の大規模サイバーセキュリティインシデントに関連する情報を受け取る。	指令（EU）2022/2555 規則（EU）2025/38
欧州外務・安全保障政策上級代表は欧州対外活動庁の支援を受ける。	政治	ハイブリッドおよびサイバー分野における対外安全保障上の脅威に対処するための欧州連合の取り組みを主導し、調整する。 欧州連合のハイブリッド外交およびサイバー外交のツールボックスを活用し、対外的脅威を抑止	理事会決定 2010/427/EU

アクター	レベル	役割と能力	参照
		し、これに対応するためのサイバー外交およびサイバー防衛手段に対応する。 ツールボックスを活用する。 CSDP の関与も含め、外部パートナーとの連携を図る。 準備態勢を提供する。 例えば、実践的な演習、トレーニングおよびネットワークを通じて、ハイブリッドおよびサイバー脅威に対する加盟国の状況認識および対応能力を提供する。 特に欧州連合の共通安全保障・防衛政策（CSDP）の下で、欧州連合の宇宙資産の安全保障と防衛への影響を扱う。 IPCR の活性化または非活性化の決定について、理事会議長国から諮問を受ける。EEAS は欧州委員会のサービスとともに ISAA 報告書を作成する。	
欧州刑事警察機構	運用	サイバー犯罪の防止と抑止のため、加盟国の所轄当局に運用面および技術面での支援を提供する。	規則（EU）2016/794（すべての改正を含む
サイバーセキュリティ機関間委員会		EU 事業体のための機関間サイバー危機管理計画を承認する。CERTEU の提案に基づき、EU 事業体に関する重大インシデントに対するインシデント 対応協力に関するガイドラインまたは勧告を採択する。	規則（EU、Euratom）2023/2841
軍事コンピュータ緊急対応チーム運用ネットワーク（MICNET）	技術	軍事 CSDP ミッションおよび作戦で使用されるものを含め、同盟内の防衛システムに影響を及ぼすサイバー脅威に対して、より強固で協調的な対応を促進する。	サイバー防衛共同コミュニケーション 2022
単一情報分析能力（SIAC）		(1)民間情報およびオープンソース情報を扱い、外交政策、テロリズム、ハイブリッド脅威に関する戦略的情報を提供する EU 情報状況センター（EU INTCEN）と、(2)CSDP ミッションのための軍事情報を扱い、EU の防衛および危機管理活動を支援する EU 軍参謀本部情報局（EUMS INT）で構成される。 上級代表の認可を受ける。	欧州連合条約第 38 条および第 42 条から第 46 条 理事会共同行動 2001/555/CFSP 理事会決定 2010/461/CFSP

(3) 関連する EU レベルの危機管理メカニズム

メカニズム	水平的／セクター別／サイバー別	内容	参照
ARGUS	水平	欧州委員会は、多部門にまたがる新たな危機や、欧州連合レベルでの行動を必要とする予見可能な脅威、差し迫った脅威について、関連情報を交換することができる。	欧州委員会コミュニケーション (2005)662
EEAS 危機対応センター（CRC）	水平	EEAS における危機関連のあらゆる問題の一元的な窓口であり、EU 代表部の職員の安全を脅かす緊急事態や、在外 EU 市民に影響を及ぼす危機に対する 24 時間 365 日の常設の危機対応能力である。これは、安全保障、領事、状況認識の専門家を結集するとともに、EU 代表部の現場の献身的な専門家に依存している。	安全保障と防衛の戦略的羅針盤-市民、価値観、利益を防御し、国際平和と安全保障に貢献する欧州連合のために（2022 年 3 月 21 日）
重要インフラの青写真	水平	国境を越えた重要な関連性を持つ重要インフラの障害に対する欧州連合レベルでの対応を調整する。	理事会勧告 C/2024/4371
サイバーセキュリティ警報システム	サイバー特化	サイバー脅威に関する検知、分析、データ処理能力を強化し、域内のインシデントを防止するための高度な連合能力を確保する。	規則（EU）2025/38（サイバー連帯法） OJ L series, 15.1.2025
サイバー外交ツールボックス（悪質なサイバー活動に対する EU の共同外交対応の枠組み）	サイバー特化	悪質なサイバー活動に対する EU 共同の外交対応で、紛争予防、サイバーセキュリティ脅威の緩和、国際関係の安定拡大に貢献する。	2017 年 6 月 19 日理事会結論 実施指針 10289/23 を改定する、 08.06.2023
欧州サイバー予備軍	サイバー特化	サイバーセキュリティの専門家とリソースを危機時に動員し、加盟国、EU 機構、団体または機関における対応努力を支援する。	規則（EU）2025/38
国境を越えた電気の流れのサイバーセキュリティの側面に関するセクター別規則に関するネットワークコード	セクター別	電力セクターにおけるサイバーセキュリティ・リスクアセスメントの反復的プロセスを確立し、危機マネジメントに特化した規定を含み、CSIRTs ネットワークおよび EU-CyCLONe にリンクしている。	欧州委員会委任規則（EU）2024/1366
EU サイバー防衛調整センター	水平	最初の目的は、サイバー空間における悪質な活動、特に軍事的な CSDP ミッションや	サイバー防衛共同コミュニケーション 2022

メカニズム	水平的／セクター別／サイバー別	内容	参照
		作戦に関する、EU と加盟国の共有状況認識を強化することである。	
ハイブリッド・ツールボックス	水平	あらゆる種類のハイブリッドの脅威に対応するために EU レベルで利用可能なものの概要と、その協調的な利用、領域を超えた行動の一貫性を確保するための一連の規定を含む。ハイブリッド・ツールボックスは、包括的な状況認識と得られた教訓に基づく意思決定を確実にするのに役立つ。	2022 年 6 月 22 日、ハイブリッドキャンペーンに対する EU の協調的対応の枠組みに関する理事会結論
ハイブリッド緊急対応チーム（EU HRRTs）	水平	EU ハイブリッド緊急対応チームは、EU ハイブリッド・ツールボックスの一環として、加盟国、共通安全保障・防衛政策ミッションおよび活動、 、ハイブリッドの脅威やキャンペーンに対抗するために、関連する分野別の国および EU の文民・軍人の専門知識を活用し、個別的かつ的を絞った短期支援を提供する。	EU ハイブリッド緊急対応チームの実質的設立のための指導枠組み（2024 年 5 月 21 日）
IPCR	水平	テロ行為を含む重大かつ複雑な危機に対し、EU 政治レベルでの迅速かつ協調的な意思決定を支援する。 発動・解除の決定は理事会議長国が行い、理事会は（連帯条項が発動された場合を除き）影響を受ける加盟国、欧州委員会、人事部と協議する。 GSC、欧州委員会の各局および EEAS は、議長国と協議のうえ、情報共有モードで IPCR を作動させることに合意することもできる。 協議は、欧州委員会業務部と EEAS が作成した ISAA 報告書に基づいて行われる。 この報告書は、関連する情報に基づいている。この報告書は、特にウェブ・プラットフォームを通じて加盟国（関連する各国の危機センターなど）から提供される関連情報と分析、および欧州連合機関（EEAS）から提供される分析に基づいている。	理事会実施決定（EU）2018/1993
EU 法執行緊急対応プロトコル	水平	迅速なアセスメント、重要情報の安全かつタイムリーな共有、捜査の国際的側面の効	大規模サイバーセキュリティインシデントと危機への

メカニズム	水平的／セクター別／サイバー別	内容	参照
		果的な調整を通じて、国境を越えた大規模なサイバー攻撃への即時対応を行う EU 法執行当局を支援するためのツールである。	EU 協調対応に関する理事会結論（2018 年 6 月 26 日）。
PESCO サイバー迅速対応チーム（CRRT）	サイバー特化	専門チームを展開し、重大なサイバーインシデントに迅速に対応するとともに、脆弱性アセスメントや選挙監視などの予防措置を実施する。 加盟国主導で、一部はコネクティング・ヨーロッパ・ファシリティの資金援助を受けている。	欧州連合条約第 42 条(6)、第 46 条、第 10 議定書。
宇宙脅威対応アーキテクチャ（STRA）	分野別 (サイバー関連を含む宇宙脅威）。	欧州連合宇宙計画の下で構築され提供されるシステムの展開、運用、使用から生じる脅威を回避するために、理事会および上級代表者が行使すべき責任に関する宇宙脅威対応アーキテクチャー(STRA)	理事会決定（CFSP）2021/698
システム的サイバーインシデント調整枠組み（EU-SCICF）	分野別	金融セクターにおける潜在的なシステミック・サイバー・イベントに対処・管理するためのコミュニケーションと調整の枠組みを開発中である。規則（EU）2022/2554 に基づく欧州監督当局（ESA）の役割のひとつである、国境を越えた情報通信技術（ICT）に関連する重大なインシデントや、EU の金融セクター全体にシステミックな影響を及ぼす関連脅威が発生した場合に、EU レベルでの効果的な協調対応を徐々に可能にすることを基礎とする。	関連当局のための汎欧州システミック・サイバーインシデント調整枠組みに関する 2021 年 12 月 2 日の欧州システミック・リスク理事会勧告（ESRB/2021/17）
欧州連合国民保護メカニズム（UCPM）	水平	災害の予防、準備、対応を改善するための市民保護協力を確保する。	決定 1313/2013
CISE - 共通情報共有環境	7 つのセクターをカバーする海事に特化したもの。	CISE - 海上監視を担当する EU/EEA 当局のシステムを結ぶネットワークである。CISE は、シームレスかつ自動化された方法で、国境や異なるセクターを越えた関連情報の交換を可能にする。	安全保障と防衛のための戦略的羅針盤-市民、価値観、利益を防御し、国際平和と安全保障に貢献する欧州連合のために（2022 年 3 月 21 日）。

(4) 指令(EU) 2022/2555 および EU レベルのセクター危機メカニズム（該当する場合）に基づく、重要度の高いセクターおよびその他の重要セクター

セクター	サブセクター	該当するセクター危機メカニズム
エネルギー	電力	電力調整グループ
	地域冷暖房	n/a
	石油	石油調整グループ 欧州連合オフショア 認可グループ (EUOAG)
	ガス	ガス調整グループ
	水素	n/a
輸送	航空	欧州航空危機 コーディネーション・セル（EACCC）
	鉄道	n/a
	水	欧州漁業管理機関 (EFCA) セーフシーネット（SSN） 統合海上サービス（IMS） 長距離識別追跡データセンター（LRIT） EMSA 海事支援サービス
	道路	n/a
	水平	緊急輸送計画（COM(2022) 211）により設置された輸送連絡網
バンキング		EU-SCICF
金融市場インフラ		EU-SCICF 欧州金融安定化メカニズム
健康		早期警戒・対応システム（EWRS） 保健緊急事態対応施設（HEOF） 組織・細胞・血液成分迅速警戒システム（RATC/RAB） 公衆衛生緊急枠組み

セクター	サブセクター	該当するセクター危機メカニズム
		化学物質インシデント迅速警戒システム（RASCHEM） 欧州感染症サーベイランスポータル 医療緊急事態への準備と対応（HERA） 医療情報システム（MediSys） 医療機器不足に関する執行運用グループ（MDSSG） ファーマコビジランス・ラピッドアラート EU 保健タスクフォース（EUHTF）
飲料水		n/a
廃水		n/a
デジタルインフラ		n/a
ICT サービス管理		n/a
行政		n/a
宇宙		宇宙脅威対応アーキテクチャ（STRA）
郵便・宅配便サービス		n/a
廃棄物管理		n/a
化学製品の製造、生産、販売		化学物質インシデント迅速通報システム（RASCHEM）
食品の製造、加工、流通		欧州作物モニタリングシステム 世界農業生産異常ホットスポット検知（ASAP） 欧州植物衛生情報システムネットワーク（EUROPHYT） EU 獣医緊急チーム（EUVET） 食品と飼料のための迅速警報システム（RASFF） 欧州食料安全保障危機準備・対応メカニズム（EFSCM） 域内市場緊急・レジリエンス法（IMERA）
製造事業者	医療機器	n/a
	コンピュータ、電子、光学製品	n/a

セクター	サブセクター	該当するセクター危機メカニズム
	機械・設備	n/a
	自動車、トレーラー、セミトレーラーの製造事業者	n/a
	その他の輸送機器の製造事業者	n/a
デジタルプロバイダー		n/a
研究		n/a

附属書 3 - 指針となる原則

2017 年のサイバーセキュリティ青写真で示された原則は、引き続き関連するものである。

比例性： 加盟国に影響を及ぼすサイバーセキュリティインシデントのほとんどは、国家的または連合的危機とみなされるようなものではない。サイバーインシデントが発生した場合、加盟国は CSIRTs ネットワークおよび EU-CyCLONe の中で、それぞれの手続きに沿って協力する。

補完性：加盟国は、自国に影響を及ぼす大規模なサイバーセキュリティインシデントや危機が発生した場合の対応について、第一義的な責任を負う。欧州委員会、欧州対外活動庁、ENISA、CERT-EU、欧州刑事警察機構、その他すべての関連事業体は、危機のライフサイクル全体を通じて重要な役割を担う。この役割は、IPCR の取り決めに定められているが、EU 法に由来するものでもあり、サイバーセキュリティのインシデントと危機が、単一市場内の経済活動の 1 つまたは複数の部門、EU の安全保障と国際関係、さらには機構自体にどのような影響を及ぼすかを反映している。

補完性：この勧告は、EU レベルの既存の危機管理メカニズム、すなわち、IPCR の取り決め、ARGUS、EEAS 危機対応メカニズムを十分に考慮している。相乗効果を最大化し、重複を最小化するために 2017 年以降に採択されたルールに基づき、CSIRTs ネットワークと EU-CyCLONe の役割が変更されたこと、および EU 法執行緊急対応プロトコルが採択されたことを考慮に入れている。

情報の機密性本勧告に関連するすべての情報交換は、セキュリティ、個人データ保護、機密情報分類のためのトラフィックライト・プロトコル制度に関する適用規則を遵守しなければならない。機密情報の交換については，適用される分類スキームにかかわらず，利用可能な認定ツールを使用す ることが望ましい。パーソナルデータの処理に関しては、特に、欧州議会及び理事会規則（EU）2016/679[1] 、欧州議会及び理事会指令 2002/58/EC[2] 、欧州議会及び理事会規則（EU）2018/1725[3] 、適用される EU 規則を尊重しなければならない。

[1]個人データの処理に関する自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日付欧州議会および理事会規則（EU）2016/679 および指令 95/46/EC の廃止（一般データ保護規則）（OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj）。

[2]電子通信分野におけるパーソナルデータの処理およびプライバシーの保護に関する 2002 年 7 月 12 日付欧州議会および理事会指令 2002/58/EC（プライバシーおよび電子通信に関する指令）（OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj）。

[3]欧州連合機関、団体、事務所および機関によるパーソナルデータの処理に関する自然人の保護、ならびに当該データの自由な移動に関する 2018 年 10 月 23 日付欧州議会および理事会規則（EU）2018/1725、ならびに規則（EC）No 45/2001 および決定 No 1247/2002/EC の廃止（OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj）。