NIS指令（EU）2016／1148の構造と機能

法律論叢第91巻第6号（2019.2）

【論　説】

NIS指令(EU) 2016/1148の構造と機能

夏　井　高　人

目　次

1　はじめに

2013年2月7日、EUの欧州委員会及び対外関係及び安全保障に関する欧州連合上級代表（High Representative）は、欧州議会、理事会、欧州経済社会委員会及び地域委員会に宛て、「欧州連合のサイバーセキュリティ戦略：オープン、安全かつ防護されたサイバー空間」と題する通知（JOIN(2013) 1 final）を提出した。この通知は、2000年以降におけるインターネットの利用の急激な拡大、そして、

その社会全体に与える影響の増加を踏まえ、サイバーセキュリティのための基本法制の確立を求めるものである。

この通知においては、その冒頭部分において、問題意識として、とりわけ、「日々の生活、基本的な権利、社会における相互関係及び経済」が「シームレスに働く情報技術及び通信技術に依存している」こと、サイバー空間がオープンかつ自由であるためには、「EUがオフラインにおいて維持しているのと同じ規範、基本原則及び価値観がオンラインにも適用されなければならない」こと、「基本的な権利、民主主義及び法の支配は、サイバー空間においても保護されなければならない」こと、「情報通信技術は、経済成長のバックボーンとなってきており、全ての経済部門が依拠する重要な資源である」こと、デジタル単一市場（Digital Single Market）(1)を推進することにより、EUのGDPを大きく増大させ得ること、「デジタル世界は、経済的利益をもたらすと同時に、脆弱性をもつものでも」あり、「（意図的なまたは事故による）サイバーセキュリティ上のインシデントが警戒すべきペースで増加しており、水道、医療、電気及び移動のサービスのような我々に与えられる重要なサービスの供給に対して打撃を与え得るものである」こと、「EUの経済は、民間部門及び個人に対するサイバー犯罪活動によって既に害を受けている」こと、「サイバー犯罪者は、情報システムに侵入するため、重要なデータを盗み出すため、または、企業を恐喝するために、これまで以上に巧妙な手口を用いるようになっている」こと、「サイバー空間における経済情報探知活動（economic espionage）及び国家が背後に存在する活動（state-sponsored activities）は、EUの政府及び企業に対する新たな類型の脅威を示している」ことを強調し、更に、対外関係において、EUの市民を調べ、コントロールするために、サイバー空間を濫用する可能性を示唆している(2)。このような状況認識を踏まえ、共同通知JOIN(2013) 1 finalは、EU全域においてサイバーセキュリティを確立するための基本政策及びそれを実現するための基本法制を構築することの重要性及び必要性を強調している。

共同通知JOIN(2013) 1 finalを踏まえ、2013年2月7日、欧州委員会は、欧州全域にわたる高度で共通の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ための措置に関する指令の提案書COM(2013) 48 final（以下「NIS指令案」という。）を提出した。この文書は、説明覚書（Explanatory Memorandum）の部分と法案文(3)の2つの部分で構成されている。NISは、「network and information

security」の略称である。この NIS 指令案には、提案の基礎となる影響評価結果を示す委員会スタッフ作業文書 SWD(2013) 32 final(4) 及びその要旨（Executive Summary）である委員会スタッフ作業文書 SWD(2013) 31 final が添付されている。

NIS 指令案の説明覚書は、その冒頭部分において、提案趣旨に関し、「この指令案の狙いは、高度で共通のレベルのネットワーク及び情報セキュリティ（NIS）を確保することにある。これは、インターネット並びに社会と経済が稼働することを下支えする民間のネットワーク及び情報システムのセキュリティを向上させることを意味する。これは、構成国に対し、その準備を増強し、構成国相互の協力関係を向上させることを要求することにより、また、電力、輸送のような重要インフラの事業者及び情報社会サービス（電子商取引プラットフォーム、ソーシャルネットワーク等）の主要なプロバイダ並びに行政機関に対し、セキュリティ上のリスクを管理するための適切な手立てを採択し、職務権限を有する国内機関に対して重大なインシデントを報告することを要求することにより、達成される」と述べ、更に、「この提案は、欧州委員会と欧州連合の対外関係及び安全保障政策に関する上級代表の欧州のサイバーセキュリティに関する共同通知と結合されて提出される。その戦略の目標は、基本的な権利及びそれ以外の EU の中心的な価値観を促進及び保護しつつ、安全かつ信頼性のあるデジタル環境を確保することにある。この分野における戦略に基づく更なる活動は、認識を向上させること、サイバーセキュリティ製品及びサービスのための域内市場を発展させること、並びに、R&D 投資を促進することに焦点を当てている。これらの活動は、サイバー犯罪に対する闘いをステップアップさせること、そして、EU のための国際的なサイバーセキュリティ政策を構築することを狙いとする別の行動によって補完される」と述べている。

ここでいう「欧州のサイバーセキュリティに関する共同通知」とは、前述の共同通知 JOIN(2013) 1 final のことを指す。サイバー犯罪対策に関する法令としては、Europol 規則 (EU) 2016/794（OJ L 135, 24.5.2016, p.53-114）(5) が採択された。Europol の中に設置された欧州サイバー犯罪対策センター（European Cyber Crime Centre (EC3)）(6) がその中心的な役割を果たす（説明覚書 1.3 参照）。ここでいうサイバー犯罪とは、欧州評議会（Council of Europe）のサイバー犯罪条約（ETS No.185）(7) に定める犯罪のことを指す(8)。

サイバー犯罪条約の加盟者（Party）としての EU において EU レベルで同条約を実装するための刑事実体法としての法令は、指令 2013/40/EU（OJ L 218, 14.8.2013, p.8-14）(9) である。同指令は、同条約の第 2 条（違法アクセス）、第 3 条（違法傍受）、第 4 条（データ妨害）、第 5 条（システム妨害）、第 6 条（機器の濫用）、第 11 条（未遂及び幇助・教唆）、第 12 条（法人の責任）、第 13 条（制裁措置）、第 23 条（管轄権）及び第 24 条（国際協力）に対応する法令である。同指令の前文 (15) は、「理事会の 2008 年 11 月 27 日及び 28 日の決定は、欧州評議会の 2001 年のサイバー犯罪に関する条約の内容を考慮に入れた上で、構成国及び欧州委員会と共に、新たな戦略が策定されるべきであることを指示した。同条約は、情報システムに対する攻撃を含め、サイバー犯罪との闘いのために参照される法的枠組みである。この指令は、同条約の上に構築される。可能な限り速やかに、全ての構成国によって、同条約の批准手続が完了されることは、先決的であると考えられなければならない」と述べている (10) 。ここでいう理事会決定とは、「Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime: 2987th JUSTICE and HOME AFFAIRS Council meeting, Brussels, 27-28 November 2008」のことを指す。EU の構成国は、同指令を国内法の中に実装しなければならない。指令 2011/93/EU（OJ L 335, 17.12.2011, p.1-14）(11) は、児童ポルノ犯罪の処罰に関して定めている。同指令は、サイバー犯罪条約の第 9 条（児童ポルノ関連犯罪）に対応するものともなっている。また、資金洗浄及びテロリスト資金提供 (12) に関する指令 (EU) 2015/849（OJ L 141, 5.6.2015, p.73-117）(13) 及び指令 (EU) 2017/1371（OJ L 198, 28.7.2017, p.29-41）も関連法令である。これらの指令は、サイバー犯罪条約の第 7 条（コンピュータ関連偽造）及び第 8 条（コンピュータ関連詐欺）との関係をもつ。なお、指令 (EU) 2015/849 は、指令 (EU) 2018/843（OJ L 156, 19.6.2018, p.43-74）(14) によって大規模に改正された (15) 。

他方、サイバー犯罪条約の加盟者としての EU において EU レベルで同条約を実装するための刑事手続法としての法令は、COM(2018) 225 final (16) として提案されている。なお、構成国の国境を越える捜査協力に関しては、欧州捜査命令（EIO）に関する指令 2014/41/EU（OJ L 130, 1.5.2014, p.1-36）(17) 及び犯罪と関連する物件等の没収に関する指令 2014/42/EU（OJ L 127, 29.4.2014, p.39-50）(18) がある。指令 2014/41/EU の中には、犯罪捜査のための通信傍受に関する条項も含ま

れている。COM(2018) 225 final は、サイバー犯罪条約の第 16 条（コンピュータデータの応急保全）、第 18 条（提出命令）に対応するものである。指令 2014/41/EU は、同条約の第 19 条（捜索・押収）、第 21 条（通信内容の傍受）、第 26 条（国際共助の一般原則）、第 28 条（自発的情報提供）、第 29 条（応急保全の共助）、第 31 条（アクセスの共助）、第 32 条（同意によるアクセス）と関係している(19)。

加えて、EU のサイバーセキュリティ政策に関しては、説明覚書の 1.3 に関連国際機関との関係の説明があるとおり、NIS 指令案が提出された時点までに 2 国間または多国間で様々な交渉が行われ、関連する会合が開催された(20)。

したがって、NIS 指令案及び共同通知 JOIN(2013) 1 final は、資金洗浄、テロリスト犯罪及び後述のハイブリッド脅威を含め、上述の関連諸法令及び政策文書と併せて精読されなければならない(21)。

その後、NIS 指令案は、長期間にわたる審議と主要条項案の修正を経た上で(22)、「欧州連合内におけるネットワーク及び情報システムの高度で共通の安全性のため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 (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union)」(OJ L 194, 19.7.2016, p.1-30)(23)（以下「NIS 指令 (EU) 2016/1148」という。）として採択された。同指令は、2016 年 8 月 8 日に発効した(24)。また、その後、後述のとおり、同指令の付属法令として、委員会実装規則 (EU) 2018/151 (OJ L 26, 31.1.2018, p.48-51)(25) が採択された。

ところで、一般に、情報セキュリティと関連する事項は、情報社会を規律するための法令の全体構造の中では、個人データ保護及びプライバシー保護に関する法令と同様、横断的なプロトコルとしての機能を果たしている(26)。それゆえ、これらの情報社会の法におけるプロトコル層を構成する諸法令は、様々な場面において交錯することになり、しかも、それぞれの法令の保護法益が実質的に相反的な関係となる場合がしばしばあるため、それらの法令に基づく諸手続間の調整が必要となる。

その調整は、EU 全体の危機管理体制の中における一貫性のある調整手順の下で統括された様々な部分的な調整が含まれるが、その調整の際に適用される法原則を探究することには学術的な意味がある(27)。とりわけ、情報セキュリティ上のリ

スク及びインシデントの報告（通知）を合理化・迅速化すればするほど、当該報告の中に含まれ得る個人データ保護が希薄化するという一般的な関係が成立し得るため、その場合に適用される法原則を明らかにし、かつ、危機管理のための情報伝達及び情報共有という一般的な利益（General Interest）または公共の利益（Public Interest）を優先すべき場合においても必須のものとして適用される機密性保護[28]のための安全性確保措置（Safeguards）の仕組みを理解することは、日本国における対応法令の構築・解釈・運用においても大きく資するものとなると考えられる。

本稿は、以上のような問題意識に基づき、NIS指令(EU) 2016/1148の基本構造及び機能、特にEU全体の危機管理体制の中における役割を検討した上で[29]、民間のプロバイダ等による重大なインシデントの報告（通知）の際におけるEUの個人データ保護法制との関係及びそれ以外の法令に対する影響または波及効果について示唆することを目的とする[30]。

2　NIS指令(EU) 2016/1148の目的・定義、構造及び機能並びに関連細則

2．1　目的・定義

NIS指令(EU) 2016/1148の第1条第1項は、同指令の目的に関し、「この指令は、域内市場の稼働を向上させるため、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性に関する高度で共通のレベルを達成するための措置を定める」と規定している。

このような目的を設定することについて、前文(1)は、「ネットワーク及び情報のシステム及びサービスは、社会において非常に重要な役割を果たしている。その信頼性と安全性は、経済活動及び社会活動にとって重要であり、とりわけ、域内市場が機能する上で重要である」と述べ、前文(3)は、「ネットワーク及び情報システム、そして、基本的にはインターネットは、物品、サービス及び人々の国境を越える移動を容易にする上で重要な役割を果たしている。そのような多国籍的な性

質のゆえに、これらのシステムに重大な混乱が生ずると、それが意図的なものであるか偶発的なものであるかを問わず、その混乱が発生した地域とは無関係に、個々の構成国及び欧州連合全体に悪影響を及ぼし得る。ネットワーク及び情報システムの安全性は、それゆえ、域内市場が円滑に稼働する上で重要なものである」と述べている。

すなわち、NIS 指令(EU) 2016/1148 におけるネットワーク及び情報システムの安全性確保は、それ自体が自己目的になっているのではなく、域内市場の円滑な稼働を保証し、企業、行政機関及び消費者の信頼を確保するための手段の一部として、その技術的側面及びマネジメントの側面に着目した政策論であるということができる(31)。NIS 指令(EU) 2016/1148 の保護法益は、そのようなものとして理解されなければならない(32)。

NIS 指令(EU) 2016/1148 の適用対象である「ネットワーク及び情報システム（network and information system）」の定義は、第 4 条(1)で与えられており、(a)指令 2002/21/EC の第 2 条(a)の意味における電子通信ネットワーク；(b)機器または相互接続された機器もしくは関連機器のグループであって、その中の 1 もしくは複数のものがプログラムによってデジタルデータの自動処理を実行するもの；または、(c)(a)及び(b)に含まれる構成要素の運用、使用、保護及び維持管理のために、それらの構成要素によって記録保存され、処理され、検索されまたは送信されるデジタルデータのいずれかを意味する。

そして、指令 2002/21/EC（OJ L 108, 24.4.2002, p.33-50）(33) の第 2 条(a)は、「電子通信ネットワーク」について、「送受信システム、並びに、適用可能なときは、交換機器またはルーティング機器及びそれら以外の資源であって、アクティブではないネットワーク要素を含め、運搬される情報の種類に拘らず、有線により、無線により、光学的手段により、または、それら以外の電磁的な手段により、信号の伝送を許容するものを意味し、衛星ネットワーク、固定（インターネットを含め、回線交換、パケット交換）及び移動体地上ネットワーク、信号の送受信の目的のために使用される範囲内で送電線システム、ラジオ放送及びテレビ放送のために使用されるネットワーク、ケーブルテレビネットワークを含む」と定義している。これは、指令 2002/21/EC が採択される前の時代においては、「電気通信ネットワーク（telecommunication network）」として理解されていたものとほぼ同じ

ものを指す。結局、NIS 指令 (EU) 2016/1148 における「ネットワーク及び情報システム」とは、電子通信ネットワーク、または、電子通信ネットワークを構成する機器もしくはデータのことを意味する。

他方、NIS 指令 (EU) 2016/1148 の適用対象である「デジタルサービス（digital service）」の定義は、第 4 条 (5) で与えられており、その定義は、指令 (EU) 2015/1535[34] の第 1 条第 1 項の (b) の定義を引用している。

指令 (EU) 2015/1535 の第 1 条第 1 項の (b) は、「サービス」について、「情報社会サービス、換言すると、通常、対価を得るために、隔地者間で、電子的な手段により、かつ、サービスを受ける者の個別の要求に応じて提供されるサービスのことを意味する。この定義の目的のために：(i)「隔地者間で」とは、当事者が同時に現在することなく、そのサービスが提供されることを意味し；(ii)「電子的な手段により」とは、（デジタル圧縮を含め）処理のための電子装置及びデータの記録保存によって、サービスが最初に送られ、その到達地において受領され、かつ、有線により、無線により、光学的な手段により、または、それ以外の電磁的な手段によって、その全体が送信され、運搬され、受領されることを意味し；(iii)「サービスを受ける者の個別の要求に応じて」とは、個別の要求に関するデータの送信を介してそのサービスが提供されることを意味する。この定義の適用のないサービスの指示リストは、別紙 I に定める」と定義している。要するに、「デジタルサービス」とは、「情報社会サービス（information society service）」のことを指す。

2. 2 構造

NIS 指令 (EU) 2016/1148 の第 1 条第 2 項は、第 1 条第 1 項の目的を実現するための手法として、以下のとおりの 5 つの柱を掲げている。

(a) 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を採択すべき構成国の義務を定め；
(b) 構成国間における戦略上の協力と情報交換を支援し、容易にし、かつ、構成国間における信頼と秘密を発展させるための協力グループを創設し；
(c) 構成国間における信頼と秘密の発展に寄与し、かつ、迅速かつ効果的な

業務遂行上の協力活動を促進するための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」）を創設し；

(d) 重要サービス運営者及びデジタルサービスプロバイダに適用される防護義務及び通知義務を定め；

(e) 職務権限を有する国内機関、連絡部局並びにネットワーク及び情報システムの安全性に関する職務を有する CSIRT を設置すべき構成国の義務を定める。

(a)及び(b)に関し、NIS 指令(EU) 2016/1148 の前文(4)は、「欧州のサイバー危機に対する協力活動のための基本原則を確立することを含め、意見交換及び良いポリシー実務の交換を行う欧州連合構成国フォーラム内における大きな発展に基づき、ネットワーク及び情報システムの安全性に関する構成国間の戦略的な協力活動を支援し、容易にするため、構成国の代表、欧州委員会及び欧州連合ネットワーク及び情報セキュリティ局（「ENISA」）によって構成される協力活動グループが設置されなければならない。このグループが効果的かつ包括的なものであるために、全ての構成国が、その領土内にあるネットワーク及び情報システムの高いレベルの安全性を確保するためのミニマムの能力と戦略をもつことが重要である。加えて、リスク管理の文化を促進し、かつ、重大なインシデントの大部分が報告されることを確保するために、重要サービス運営者及びデジタルサービスプロバイダに対し、防護義務と通知義務が適用されるべきである」と述べている。

(c)及び(e)に関し、NIS 指令(EU) 2016/1148 の前文(32)は、「職務権限を有する機関また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」）は、インシデント通知を受領しなければならない。連絡部局は、職務権限を有する機関または CSIRT としても活動するのでない限り、直接にはインシデント通知を受領しない。しかしながら、職務権限を有する機関または CSIRT は、影響を受ける他の構成国の連絡部局に対してインシデント通知を転送することについて、連絡部局の職務も遂行できるものとしなければならない」と述べ、また、前文(34)は、「構成国は、ネットワーク及び情報システムのインシデント及びリスクを防止し、検出し、対応し、そして、削減させるために、技術上の能力及び組織上の能力の両者の面において、十分に具備するものとしなければならない。構成国は、コンピュータ

緊急対応チーム（「CERT」）としても知られ、インシデント及びリスクに対処するための効果的で互換性のある能力を保障し、かつ、欧州連合レベルの効果的な協力を確保するための基本的な要求事項を遵守し、よく機能する CSIRT をもつ。全ての種類の重要サービス運営者及びデジタルサービスプロバイダがそのような能力及び協力からの利益を享受するために、構成国は、指定された CSIRT によってそれらの全ての種類がカバーされることを確保しなければならない。サイバーセキュリティに関する国際協力の重要性に鑑み、CSIRT は、この指令によって設けられる CSIRT ネットワークに加え、国際協力ネットワークにも参加できるものとしなければならない」と述べている。NIS 指令 (EU) 2016/1148 における CSIRT は、CERT と同様、各構成国の情報セキュリティ政策や法執行等とは無関係に活動する組織・団体ではなく、構成国の機関として機能する組織である。それゆえ、CSIRT ネットワークもまた、単なる任意団体または親睦団体ではない。CSIRT は、各構成国の監督機関の目であり、耳であり、鼻である。そして、CSIRT ネットワークは、それらを連絡する神経網である。

(d) に関し、NIS 指令 (EU) 2016/1148 の前文 (52) は、「重要サービス運営者及びデジタルサービスプロバイダは、それらが使用するネットワーク及び情報システムの安全性を確保しなければならない。これらは、その内部 IT スタッフによって管理され、または、その防護をアウトソースして管理されている基本的に私的なネットワーク及び情報システムである。防護義務及び通知義務は、そのネットワーク及び情報システムの維持管理を内部者によって遂行しているかアウトソースしているかに拘りなく、関連する重要サービス運営者及びデジタルサービスプロバイダに対して適用されなければならない」と述べ、また、前文 (57) は、「重要サービス運営者（とりわけ、その物理的なインフラとの直接のリンク）とデジタルサービスプロバイダ（とりわけ、その国境を越える性質）との間の根本的な相違に鑑み、この指令は、これら 2 つのグループの組織と関連する整合性のレベルに関して、異なるアプローチを採用しなければならない。重要サービス運営者について、構成国は、関連する運営者を指定し、この指令に定めるものよりも厳格な義務を負わせることができるものとしなければならない。適用範囲内にある全てのデジタルサービスプロバイダに対してこの指令を適用しなければならないため、構成国は、デジタルサービスプロバイダを指定できない。加えて、この指令及びそれに基づいて採

択される実装行為は、防護義務及び通知義務に関し、デジタルサービスプロバイダの高いレベルの整合性を確保しなければならない。このことは、デジタルサービスプロバイダが欧州連合内において統一的な方法で、それらが直面するかもしれないリスクの性質及び程度と比例的な方法で取り扱われることを可能とするものとしなければならない」と述べている。ここでいう通知義務を負う重要サービス運営者（operators of essential services）(35) は、NIS 指令(EU) 2016/1148 の別紙Ⅱに定める産業部門の区分に応じ、構成国によって指定される（第5条第1項）。その指定の際の指定基準は、以下のとおりである（第5条第2項）。

(a) その組織が、不可欠な社会的活動及びまたは重要な経済的活動の維持にとって重要なサービスを提供し；
(b) ネットワーク及び情報システムに依拠して当該サービスが提供され；かつ
(c) 当該サービスの提供に対して、インシデントが重大な破壊的効果をもち得ること。

第5条第2項(c)の「破壊的効果（disruptive effect）」の重大性の判断基準は、以下のとおり、第6条第1項において示されている。

(a) 関係する組織によって提供されるサービスに依存する利用者の数；
(b) 当該組織によって提供されるサービスに関し、別紙Ⅱに示す他の部門との依存関係；
(c) 程度及び持続時間の面における経済活動及び社会活動または公共の安全に対してそのインシデントがもち得る影響；
(d) 当該組織の市場占有率；
(e) インシデントによって悪影響を受ける可能性のある地域に関する地理的な広がり；
(f) 当該サービス提供の代替手段の利用可能性を考慮に入れた上で、その組織が十分なレベルでそのサービス提供を維持継続することの重要性。

NIS指令(EU) 2016/1148の別紙Ⅱは、6つの部門（Sector）に区分され、それぞれ更に細目的な副部門（Subsector）に区分されている。このような区分に関し、前文(28)は、「部門横断的な要因に加え、あるインシデントが重要サービスの提供に対して破壊的な効果をもつか否かを判定するために、部門別の要因も検討されなければならない。そのような要因は、電力の供給者に関しては、国内で生産される電力の量及び割合を；石油の供給に関しては、1日当たりの生産量；空港及び航空会社を含め、航空運輸、鉄道輸送及び港湾に関しては国内輸送量の割合及び1年当たりの輸送人員または貨物輸送の数量；銀行及び金融市場インフラに関しては、総資産またはGDPに対する総資産の割合に基づく全体的な重要性(36)；医療部門に関しては、1年当たりの医療機関で医療行為を受けた患者数；水道に関しては、浄水処理と供給の分量、例えば、病院、公共機関、個人を含め、水の供給を受ける利用者の数と種類、並びに、同一の地理的地域をカバーする代替的な水の供給源を含めることができる」と述べている。

また、前文(10)は、「海上輸送部門においては、欧州連合の法令に基づく企業、船舶、港湾施設、港湾及び船舶交通業務のための防護義務は、無線システム及び通信システム、コンピュータシステム及びネットワークを含む全ての運用業務を包摂している。従うべき義務的手続の部分は、全てのインシデントの報告義務を含んでいることから、それらの義務がこの指令の対応する条項と少なくとも均等である限り、特別法として理解されるべきである」と述べ(37)、前文(13)は、「業務運営上のリスクは、銀行及び金融市場インフラの部門における健全性の規律と監督にとって、極めて重要な部分である。これは、ネットワーク及び情報システムの安全性、完全性及び回復性を含め、全ての運用を包摂する。これらのシステムと関連する義務は、この指令に基づいて定められる義務をしばしば上回るもので、欧州連合の多数の法令によって定められている。それらの法令は、以下のものを含む：信用機関の活動へのアクセス及び信用機関及び投資企業に対する信頼性監督に関する規則並びに信用機関及び投資企業の信頼性確保義務に関する規則は、業務遂行上のリスクと関連する義務を含んでいる；金融商品の市場に関する規則は、投資企業及び規則の適用のある市場に対するリスク評価と関連する義務を含んでいる；OTCデリバティブ、清算機関及び取引情報蓄積機関に関する規則は、清算機関及び取引情報蓄積機関に対するリスク評価と関連する義務を含んでいる；そして、欧州連合内に

おける証券決済の向上及び中央証券決済機関に関する規則は、業務遂行上のリスクと関連する義務を含んでいる。更に、インシデント通知義務は、金融部門における通常の監督実務の一部分となっており、しばしば監督業務マニュアルの中に収録されている。構成国は、構成国が特別法を適用する場合には、これらの規則や義務を考慮しなければならない」と述べている。そして、前文(15)は、「オンライン市場は、消費者及び商人が、オンラインで商人と売買契約またはサービス契約を締結できるようにするものであり、その契約の履行を完結させる場となるものである。それは、利用者が最終的に契約を締結する相手である第三者のサービスを媒介者として提供するだけのオンラインサービスを含めるものではない。それゆえ、それは、特定の製品やサービスの価格を他の商人のそれと比較し、そして、製品を購入しようとする好みの商人のところへと利用者をリダイレクトするだけのオンラインサービスを含めるものではない。オンライン市場によって提供されるコンピュータ処理サービスは、送信、データの集積または利用者のプロファイリングの処理を含み得る。第三者からのアプリケーションまたはソフトウェアプログラムのデジタル配信が可能なオンライン販売店として機能するアプリケーション販売店は、オンライン市場の一種として理解されるべきである」と述べ、前文(16)は、「オンライン検索エンジンは、原則として、全ての Web サイトについて、利用者が何らかの事柄に関するクエリーに基づいて検索を実行できるようにするものである。それは、選択的に、特定の言語による Web サイトに焦点を当てるものであり得る。この指令が定めるオンライン検索エンジンの定義は、その検索機能が外部の検索エンジンによって提供されるものであるか否かを問わず、特定の Web サイトのコンテントに限定された検索機能を含めるものではない。のみならず、それは、特定の製品やサービスの価格を他の商人のそれと比較し、そして、製品等を購入しようとする好みの商人のところへと利用者をリダイレクトするオンラインサービスを含めるものでもない」と述べている(38)。

他方で、NIS 指令 (EU) 2016/1148 の前文(22)は、「この指令に示す部門及び副部門に該当する事業を営む組織が重要サービスと重要でないサービスの両方を運営することがあり得る。例えば、航空運輸部門では、空港は、滑走路の管理のように、構成国によって重要であると判断され得るサービスを提供するが、ショッピングエリアの提供のように、重要ではないと判断され得る多数のサービスも提供して

いる。重要サービス運営者は、重要であると判断される当該サービスとの関係においてのみ、特別の防護義務に服さなければならない。運営者の指定の目的のために、構成国は、重要であると判定するサービスのリストを作成しなければならない」とも述べている。

以上を前提とした上で、NIS 指令 (EU) 2016/1148 は、第 1 条第 2 項に定める 5 つの柱に基づき、それを実現するための構造を定める条項を設けている。それらの条項を第 1 条第 2 項に定める 5 つの柱に従って整理すると、以下のとおりとなる。

	関連する条項
(a)	第 7 条（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）
(b)	第 10 条（国内レベルにおける協力活動） 第 11 条（協力活動グループ）
(c)	第 12 条（CSIRT ネットワーク）
(d)	第 14 条（重要サービス運営者の防護義務及びインシデント通知） 第 15 条（実装及び執行） 第 16 条（デジタルサービスプロバイダの防護義務及びインシデント通知） 第 17 条（実装及び執行） 第 18 条（裁判管轄及び地的管轄） 第 19 条（標準化） 第 20 条（任意の通知）
(e)	第 8 条（構成国の職務権限を有する機関及び連絡部局） 第 9 条（コンピュータセキュリティインシデント対応チーム（CSIRT））

2．3　機能（インシデント通知）

一般に、情報セキュリティのマネジメントにおいて、インシデントの報告（通知）は、より上位の判断権限をもつ者または組織に向けたエスカレーション（escalation）のために実施される。

NIS 指令 (EU) 2016/1148 において想定されている重要サービス運営者及びデジタルサービスプロバイダは、それぞれ独立した民間法人または公的機関（行政機関等）である。それゆえ、重要サービス運営者及びデジタルサービスプロバイダそれぞれが標準的な情報セキュリティの措置を構ずるべきことは当然のことである。そして、重要サービス運営者及びデジタルサービスプロバイダは、当該組織内におけるエスカレーションとしてインシデントの報告が行われるべきことも当然のこ

とである(39)。

NIS 指令(EU) 2016/1148 が定めるインシデント報告（通知）は、そのような個々の法主体内における報告ではない。それは、複数の構成国にまたがって当該インシデントの影響が発生する場合、あるいは、EU 全域において当該インシデントの影響が発生する場合のような広域の影響の有無、範囲及び程度を可及的速やかに判断して当該インシデントに対応し、あるいは、現実の被害が発生した場合において、可能な限り速やかな復旧、すなわち、回復力（resilience）の構築と実現を目的として、EU レベルで実施すべきインシデント報告を定めるものである。

インシデント報告（通知の重要性）について、NIS 指令(EU) 2016/1148 の前文(40)は、「インシデントに関する情報は、一般市民及び企業、とりわけ、中小企業にとって、その重要性を増加させている。幾つかの事例では、そのような情報は、構成国のレベルで、Web サイトを介して、特定の国の言語を用い、国内の場面におけるインシデント及びその発生に主に焦点を当てて、既に提供されている。企業が次第に国境を越えて業務を遂行し、市民がオンラインサービスを利用していることに鑑み、インシデントに関する情報は、欧州連合のレベルで、集約された形態で提供されるべきである。CSIRT ネットワークの事務局は、企業の利益と必要性に特に焦点を絞って、欧州連合内で発生した大きなインシデントに関する一般的な情報を一般市民が利用できるようにする Web サイトを管理運営し、または、既存の Web サイト上にその専用ページをホストすることが望まれる。CSIRT ネットワークに参加する CSIRT は、機密情報または機微の情報が含まれないようにしつつ、任意に、その Web サイト上で公表されるべきインシデント情報を提供することが求められる」と述べている。

行政機関が重要サービス運営者である場合及び適用範囲外の行政機関について、NIS 指令(EU) 2016/1148 の前文(45)は、「この指令は、重要サービス運営者として指定される行政組織に対してのみ適用される。それゆえ、構成国は、この指令の適用範囲外にある行政組織のネットワーク及び情報システムの安全性を確保すべき責任を負う」と述べている。また、重要サービス運営者及びデジタルサービスプロバイダがインシデント通知義務に服するだけではなく、任意かつ積極的に情報提供すべきことに関し、前文(44)は、「ネットワーク及び情報システムの安全性を確保すべき責任は、広範囲にわたって、重要サービス運営者及びデジタルサービスプ

ロバイダが負っている。リスク評価及び直面しているリスクに適切に対応するための防護策の実装を含め、リスク管理の文化は、適切な規則上の義務及び産業界における任意のプラクティスによって促進され、開発されるべきである。信頼できるレベルにある活動領域を設けることは、協力活動グループ及び CSIRT ネットワークが効果的に機能するため、そして、全ての構成国による効果的な協力を確保するためにも重要である」と述べている（第 20 条参照）。

サイバー攻撃からの回復力の重要性及び回復力の増強のための情報セキュリティの基本戦略の変化に関し、共同通知 JOIN(2017) 450 final (40) は、「EU は、既に、これらの検討課題の多くに関して作業を行っている：様々な作業の流れを一緒に描くべき時が来た。2013 年、EU は、サイバー回復力を向上させるため、一連の重要な作業行程を開始するサイバーセキュリティ戦略を示した」、「EU の政策の適用範囲、並びに、その処理におけるツール、構造及び能力に鑑み、EU は、サイバーセキュリティに適切に対処している。構成国は、国内のセキュリティについて職責を負うものであるが、脅威の規模及び国境を越える性質は、構成国に対してインセンティブを提供し、そして、EU レベルの能力を構築しつつ、それと同時に、構成国がより拡大されより改善された国内のサイバーセキュリティの能力を開発及び維持することを支援する EU の活動を強く要求するものでもある。回復力を構築し、サイバー攻撃に対する EU のより良い対応を提供する必要のある優先性をサイバーセキュリティに対して与えるため、このアプローチは、全ての関係者（EU、構成国、産業界及び個人）を活性化させるように設計されている。このアプローチは、EU 及びその構成国に対する全ての形態のサイバーインシデントを検知し、調査することを助け、そして、犯罪者の訴追を含め、適切に対応するための具体的な手立てを提供する。それは、グローバルな場においてサイバーセキュリティを効果的に向上させるための EU の対外活動を可能とするであろう。その結果は、EU が、現在ある脅威及び将来の脅威の両者に対処することを通じて、欧州の繁栄、社会及び価値観、並びに、基本的な権利及び自由を保護するため、事後的な対応というアプローチから事前の活動というアプローチへとシフトすることとなるであろう」、「欧州連合ネットワーク情報セキュリティ局（ENISA）は、EU のサイバー回復力の強化において重要な役割と職責をもつが、その現在の任務によって義務とされてはいない。それゆえ、欧州委員会は、局の恒常的な任務を含め、意欲的な改正

案を提示しているところである。これは、ネットワーク及び情報システムの安全性に関する指令（「NIS 指令」）及びサイバーセキュリティ認証枠組みの実装を含め、ENISA が、構成国、EU の機関及び重要な分野にある企業に対して支援を提供できることを確保するものとなるであろう」と述べている。ここでいう 2013 年のサイバーセキュリティ戦略とは、JOIN(2013) 1 final のことを指す。また、欧州委員会の提案とは、後述の Cybersecurity Act（COM(2017) 477）のことを指す。

要するに、共同通知 JOIN(2017) 450 final に示されているとおり、EU の情報セキュリティの基本戦略は、インシデント情報の伝達を受けて事後的に対応するという消極的な対応から、リスクの徴候を可能な限り早期に収集し、それに基づいて事前に対抗策を構築して攻撃を待ち構える、または、事前に回復力を準備しておき、迅速に反撃に移るという積極姿勢に転じたと考えることが可能である。ENISA をはじめとする EU の関連各機関は、あるインシデント情報を入手した場合、当該インシデントの発生場所に限定した分析だけではなく、そのインシデントが別のインシデントの徴候またはリスクの徴候として理解すべきものであるか否かについて、（後述のとおり、構成国の軍及び諜報機関から得られる機密情報を含め）他の関連情報と総合して戦略的に分析するのである(41)。NIS 指令(EU) 2016/1148 に基づくインシデント通知というエスカレーションの仕組みは、そのために用いられる。

以上を踏まえた上で、NIS 指令(EU) 2016/1148 が定める枠組み内において、重要サービス運営者及びデジタルサービスプロバイダ、並びに、職務権限を有する機関または CSIRT は、以下のとおりに行動しなければならない。

(a) 重要サービス運営者

（防護措置義務）

重要サービス運営者は、その業務遂行の用に供するネットワーク及び情報システムの安全性に対して示されたリスクを管理するための適切かつ比例的な技術上及び組織上の措置を講ずることを確保する。それらの措置は、最新技術を考慮した上で、示されたリスクに適切に対応するレベルのネットワーク及び情報システムの安全性を確保するものとする（第 14 条第 1 項）。

重要サービス運営者は、そのサービスの継続性を確保するために、その重要サービスの提供のために用いられるネットワーク及び情報システムの安全性

に悪影響を及ぼすインシデントの影響を抑止し、ミニマム化するための適切な措置を講ずる（第14条第2項）。

（通知義務）

重要サービス運営者は、不適切な遅滞なく、職務権限を有する機関またはCSIRTに対し、その運営者が提供する重要サービスの継続性に重大な影響をもつインシデントについて通知する。その通知は、職務権限を有する機関またはCSIRTがそのインシデントの国境を越える影響を判断するための情報を含めるものとする（第14条第3項）。

インシデントの影響の重大性を判断するために、とりわけ、重要サービスの混乱により影響を受ける利用者の数、インシデントの持続時間、及び、インシデントによって悪影響を受ける地域に関する地理的な広がりというパラメータが考慮に入れられるものとする（第14条第4項）。

(b) デジタルサービスプロバイダ

（防護措置義務）

デジタルサービスプロバイダが、欧州連合内において別紙Ⅲに示すサービスを提供する過程でそのプロバイダがその用に供するネットワーク及び情報システムの安全性に対して示されたリスクを特定し、管理するための適切かつ比例的な技術上及び組織上の措置を講ずることを確保する。最新技術を考慮した上で、それらの措置は、示されたリスクに適切に対応するレベルのネットワーク及び情報システムの安全性を確保し、かつ、システム及び施設の安全性、インシデント対応、事業継続性管理、監視、監査及びテスト、国際標準への準拠という要素を考慮に入れるものとする（第16条第1項）。

デジタルサービスプロバイダが、そのサービスの継続性を確保するために、欧州連合内において提供されるオンライン市場、オンライン検索エンジンまたはクラウドコンピューティングサービスのデジタルサービス（別紙Ⅲ）のネットワーク及び情報システムの安全性に悪影響を及ぼすインシデントの影響を抑止し、ミニマム化するための適切な措置を講ずる（第16条第2項）。

（通知義務）

デジタルサービスプロバイダは、欧州連合内において提供するオンライン市

場、オンライン検索エンジンまたはクラウドコンピューティングサービスのデジタルサービス（別紙Ⅲ）の提供に重大な影響をもつインシデントについて、不適切な遅滞なく、職務権限を有する機関または CSIRT に対し、その運営者が提供する重要サービスの継続性に重大な影響をもつインシデントについて通知する（第 16 条第 3 項）。

（インシデントの重大性の判断基準）

インシデントの影響の重大性を判断するために、インシデントにより影響を受ける利用者の数、とりわけ、そのサービスに利用者自身のサービスが依拠する利用者の数、インシデントの持続時間、及び、インシデントによって悪影響を受ける地域に関する地理的な広がり、そのサービスの機能の混乱が及ぶ範囲、経済活動及び社会活動に及ぼす影響の範囲というパラメータが考慮に入れられるものとする（第 16 条第 4 項）。

(c) 職務権限を有する機関または CSIRT

（インシデント情報の受領）

職務権限を有する機関または CSIRT は、インシデント通知を受け取る。CSIRT はその通知を受け取らないものと構成国が定める場合、その CSIRT は、その職務を遂行する上で必要な範囲内で、第 14 条第 3 項及び第 5 項により重要サービス運営者から通知されるインシデントに関するデータ及び第 16 条第 3 項及び第 6 項によりデジタルサービスプロバイダから通知されるインシデントに関するデータへのアクセスが認められる（第 10 条第 2 項）。

（他の構成国に対するインシデント情報の提供）

重要サービス運営者からの通知の中で提供される情報に基づき、職務権限を有する機関または CSIRT は、そのインシデントが当該構成国の重要サービスの継続性に重大な影響をもつときは、他の影響を受ける構成国に対して、情報提供する（第 14 条第 5 項）。

それが適切である場合、とりわけ、デジタルサービスプロバイダから通知を受けたインシデントが複数の構成国と関係するものであるときは、職務権限を有する機関または CSIRT は、他の影響を受ける構成国に対し、情報提供する（第 16 条第 6 項）。

（公衆に対するインシデント情報の提供）

重要サービス運営者から通知を受けたインシデントを抑止し、または、進行中のインシデントへの対処のために、公衆の注意喚起が必要な場合、職務権限を有する機関または CSIRT は、通知元である重要サービス運営者との協議を経た上で、公衆に対し、個々のインシデントに関して情報提供することができる（第 14 条第 6 項）。

デジタルサービスプロバイダから通知を受けたインシデントを抑止し、または、進行中のインシデントへの対処のために、公衆の注意喚起が必要な場合、または、そのインシデントが公共の利益にかかわるものである場合、職務権限を有する機関または CSIRT、並びに、それが適切なときは、関係する別の構成国の職務権限を有する機関または CSIRT は、関係する通知元であるデジタルサービスプロバイダとの協議を経た上で、公衆に対し、個々のインシデントに関して情報提供することができ、または、そのデジタルサービスプロバイダに対し、そのようにすることを要求することができる（第 16 条第 7 項）。

（連絡部局に対するインシデント情報の提供）

職務権限を有する機関または CSIRT は、この指令によって送付されるインシデント通知に関し、連絡部局に対して情報提供する（第 10 条第 3 項）。

(d) CSIRT ネットワーク

（情報共有）

CSIRT ネットワークは、構成国の CSIRT の代表及び CERT-EU によって構成される。欧州委員会は、CSIRT ネットワークにオブザーバーとして参加する。ENISA は、事務局を提供し、かつ、CSIRT 間における協力を積極的に支援する（第 12 条第 2 項）。

インシデントによって悪影響を受けている可能性のある構成国からの CSIRT 代表の要請があるときは、当該インシデント及びそれに伴うリスクと関連する非商業的な機微の情報の交換及び意見交換をする。ただし、構成国の CSIRT は、インシデントの調査を妨げるリスクがあるときは、その意見交換への参加を拒否することができる（第 12 条第 3 項 (b)）。

（任意の共助）

構成国の CSIRT 代表の要請があり、かつ、それが可能なときは、当該同一の構成国の領土内で特定されたインシデントに対する共同対応を指示する（第 12 条第 3 項(d)）。

構成国間の任意の共助に基づき、構成国に対する国境を越えるインシデントに対処する支援を提供する（第 12 条第 3 項(e)）。

(e) 連絡部局

（他の構成国の連絡部局へのインシデント情報の提供）

職務権限を有する機関または CSIRT の要請があるときは、連絡部局は、他の影響を受ける構成国の連絡部局に対し、重要サービス運営者からの通知を送付する（第 14 条第 5 項）。

（情報共有）

連絡部局は、2018 年 8 月 9 日までに、それ以降は 1 年毎に、協力活動グループに対し、通知の数及び通知されたインシデントの性質、第 14 条第 3 項及び第 5 項並びに第 16 条第 3 項及び第 6 項に従って講じられた措置を含め、受領した通知に関する概要報告書を送付する（第 10 条第 3 項）。

(f) 協力活動グループ

（共同対応）

協力活動グループは、構成国の代表、欧州委員会及び ENISA によって構成される（第 11 条第 1 項）。

以上のとおり、重要サービス運営者またはデジタルサービスプロバイダから個々のインシデント情報を受け取るのは、各構成国の職務権限を有する機関（行政機関）または CSIRT である。しかし、NIS 指令(EU) 2016/1148 の第 12 条第 2 項により、CERT-EU 及び ENISA は、CSIRT ネットワークを介して、重要サービス運営者またはデジタルサービスプロバイダから通知されるインシデント情報を収集し、更に、EU の他の関連機関及び組織と情報共有することが可能である(42)。

2．4　委員会実装規則 (EU) 2018/151

NIS 指令 (EU) 2016/1148 の第 16 条第 8 項は、デジタルサービスプロバイダからのインシデント通知と関連するリスク要素の評価要素（同条第 1 項）及びインシデントの重大性を判断するためのパラメータ（同条第 4 項）を更に追加するため、欧州委員会が実装行為を採択するものと定めている。その実装行為として、2018 年 1 月 30 日、委員会実装規則 (EU) 2018/151 が採択された。同実装規則は、2018 年 5 月 10 日に適用（施行）となった。

同実装規則の前文 (2) は、「適切かつ比例的な技術上の措置及び組織上の措置を判断する際、デジタルサービスプロバイダは、リスクベースのアプローチを用い、体系化された方法で情報セキュリティと取り組まなければならない」と述べ、また、前文 (3) は、「システム及び施設の安全性を確保するため、デジタルサービスプロバイダは、評価手続及び分析手続を遂行しなければならない。これらの活動は、ネットワーク及び情報システム、物理環境の安全性、サプライの安全性及びアクセス管理という体系的なマネジメントと関係するものでなければならない」と述べ、そして、前文 (4) は、「ネットワーク及び情報システムの体系的なマネジメントの範囲内でリスク分析を行う場合、デジタルサービスプロバイダは、例えば、重要な資産に対する脅威及びその脅威がいかに業務遂行を阻害するかを判断することにより、そして、現在の能力と資源の要求事項に基づき、それらの脅威をどのようにして最も良く削減させるかを判断することにより、特別のリスクを識別し、そして、その大きさを計量することが推奨される」と述べている。

委員会実装規則 (EU) 2018/151 の第 2 条は、NIS 指令 (EU) 2016/1148 の第 16 条第 1 項の (a) ないし (d) のリスク要素を更に詳細に定めている。そして、同実装規則の第 4 条第 1 項は、以下の場合には、重大なインシデントがあったものとみなす旨を定めている。

(a) デジタルサービスプロバイダから提供されるサービスが、1 時間あたり 500 万人を超える利用者が利用不可能となり、それによって、欧州連合内において害を受けた利用者の数を示す利用者利用時間が 60 分間になった場合；

(b) デジタルサービスプロバイダから提供され、または、そのプロバイダのネットワーク及び情報システムを介してアクセス可能な、記録保存され、送信され、もしくは、処理されたデータ、または、関連サービスの完全性、真正性または機密性の喪失を帰結するインシデントが、欧州連合内における 10 万を超える利用者を害する場合；

(c) そのインシデントが、公衆の安全、公共の安全または生命の喪失のリスクを生じさせた場合；

(d) 当該利用者に生じた損害が 100 万ユーロを超過するときは、そのインシデントが欧州連合内の少なくとも 1 の利用者に対して物的な損害を生じさせた場合。

3　EU の危機管理体制の中における NIS 指令の位置づけ

3．1　委員会勧告 (EU) 2017/1584

ある攻撃または脅威が EU それ自体または EU 内の相当多数の構成国に向けられている場合、その攻撃に対する危機管理は、EU 自身が行わなければならない。しかし、EU の機関及び組織の構造は複雑であり、権限も様々に分掌されているため、その調整のための何らかの規範が必要となる。2017 年 9 月 13 日に発せられた委員会勧告 (EU) 2017/1584（OJ L 239, 19.9.2017, p.36-58）(43) は、そのような意味での規範を確立するための文書である。

委員会勧告 (EU) 2017/1584 により EU の危機管理の職務に関与する主要な EU の機関及び組織は、以下のとおりである。

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

委員会勧告 (EU) 2017/1584 の前文 (6) は、「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の協力の仕組みの発展に貢献すること』を勧奨した」と述べ、前文 (9) は、「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」と述べ、前文 (14) は、「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」と述べ、前文 (15) は、「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」と述べ、前文(16)は、「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）の中で定められることになる」と述べ、前文(17)は、「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」と述べ、前文(18)は、「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」と述べ、そして、前文(19)は、「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」と述べている。前文(19)と関連して、2017 年 2 月、ENISA は、「Incident notification for

DSPs in the context of the NIS Directive」を公表した。この運用指針は、現時点において最も詳細な運用指針である。

委員会勧告(EU) 2017/1584 の勧告本文は 9 項目だけの簡素なものである。勧告本文は、下記のとおりである。

(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 レベルの協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）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。

委員会勧告(EU) 2017/1584 には「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」が別添されている。EU の機関及び組織における危機管理は、この計画書に従って実施される。計画書は、比較的長文のものであるが、その「イントロダクション」の部分は、計画書全体の要約となっている。「イントロダクション」は、下記のとおりである。

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。

頁数の関係から詳細は省略するが、この計画書では、NIS 指令(EU) 2016/1148 によって構築された CSIRT 及び CSIRT グループ並びに ENISA との連携の仕組みを基礎とし、これらを最大限活用することにより、サイバー危機（Cyber crisis）に対し、①当該危機の発展段階または脅威度と比例するモード（情報共有モード、監視モード、全面発動モード）に対応して、②危機管理行動の適用範囲における EU レベル、構成国レベルまたは部門レベルにおいて、かつ、③危機管理行動の性質における技術レベル、運営レベル、戦略／政治レベルに即した行動が決定される。最高度のモード及びレベルにおいては、EU の対外行動及び NATO との合同活動も選択肢の中に含まれる(44)。

CSIRT 及び CSIRT グループに期待されているのは、構成国レベルにおける認識の向上（注意喚起）のための日常的な周知活動・広報活動、日常的な情報収集、そして、収集した情報の ENISA への提供である。

なお、計画書が想定する危機管理は、サイバー攻撃だけに限定されない。大規模自然災害等によって発生する EU の危機に対する対応も含まれる。ネットワーク及び情報システムのリスク及びインシデントが人為的な攻撃だけに限定されることがなく、大規模自然災害による場合も含まれ得ることは、ONP 指令(45) の当時から EU（EC、EEC）において一貫して採用されている基本政策の一部である。

3．2　理事会決定 2014/496/CFSP との関係

委員会勧告(EU) 2017/1584 は、EU 内において既に確立されている危機管理体制に関しては重複を避ける姿勢を示している。特に明示されているのは欧州グローバルナビゲーション衛星システム（GNSS）計画である(46)。

理事会決定 2014/496/CFSP（OJ L 219, 25.7.2014, p.53-55）(47) は、GNSS における危機管理を定めている(48)。理事会決定 2014/496/CFSP は、リスボン条約

に基づく EU の機関及び組織の組織変更に伴う修正を実装するための改正法令である。この分野における EU の従前の法令は、2004 年 7 月 12 日の理事会共同行動 2004/552/CFSP（OJ L 246, 20.7.2004, p.30-31）であった(49)。

理事会決定 2014/496/CFSP は、GNSS と関連する危機管理の最終意思決定機関が理事会であることを定めた上で、緊急の場合においては、上級代表（HR）が暫定措置を講ずることが可能な危機管理体制を構築している。

理事会決定 2014/496/CFSP の前文(6)は、「そのシステムと関連する出来事が欧州連合に対する脅威、構成国に対する脅威または GNSS に対する脅威を構成するか否かに関する情報及び専門知識は、グローバルナビゲーション衛星システム局（「GSA」）、構成国及び欧州委員会から理事会及び HR に対して提供されなければならない。加えて、第三国もそのような情報を提供できる」と述べ、前文(7)は、「Galileo 安全監視センター（「GSMC」）の運営者としての理事会、HR、GSA それぞれの役割は、欧州連合、構成国または GNSS に対する脅威に対処するために構築される運営上の職責の連鎖の中で明確にされなければならない」と述べ、そして、前文(8)は、「この点に関し、脅威の基本的な指示は、全体として GNSS によって取り扱われる主要な一般的脅威を含むシステム固有セキュリティ要求事項書、及び、セキュリティ適格性認証プロセスの中で定められるセキュリティリスク登録簿を含むシステムセキュリティ計画に含められている。これらの文書は、特にこの決定によって取り扱われる脅威を識別するため、及び、この決定の実装に関する運営上の手続を完了するための指示を提供する」と述べている。

3．3　ハイブリッド脅威及びセキュリティユニオン

2018 年 6 月 13 日、欧州連合対外行動局（EEAS）は、「Europe that Protects: Countering Hybrid Threats」と題する文書を公表した。

この文書は、「EU 及びその構成国は、重大かつ切迫した脅威と直面し続けている。それは、テロリスト攻撃、化学攻撃、サイバー攻撃または虚偽情報キャンペーンを招来する過激化のような、従来存在しなかった形態をとるようになってきている(50)。これら全ての活動は、あることにおいて共通している。すなわち、彼らは、我々の社会を不安定にし、損ね、そして、我々の欧州の価値観を衰退させることを求めている」との状況認識を述べた上で、「ハイブリッドな脅威は、特定の政

治的な目的を達成するために国家または非国家の行為者によって統合された態様で使用され得る在来型の活動と非在来型の活動、軍事的な活動と非軍事的な活動を結合したものである」と述べ、ハイブリッドな脅威（Hybrid Threats）を定義している(51)。

このようなハイブリッドな脅威の存在を明確に認識し、具体的な対応策すなわち行動計画を明示した公式政策文書は、2016 年 4 月 6 日の共同通知「ハイブリッドな脅威への対抗に関する共同枠組み：欧州連合の対応」（JOIN(2016) 18 final）である。この文書は、欧州委員会の長（President）である Jean-Claude Juncker 氏による EU の関連機関の共同による対応が必要であるとの強い主張に基づき、EU の外務理事会、上級代表及び構成国との緊密な協議を経て作成された。

JOIN(2016) 18 final が示す枠組みの下において、EU の関連機関及び構成国は、欧州委員会及び上級代表の支援を受け、ハイブリッドな脅威に対抗するための監視措置を講ずる（行動 1）。EEAS の EU 諜報及び情報センター（EU INTCEN）内に設置された EU Hybrid Fusion Cell は、ハイブリッドな脅威と関連する情報を分析し、関連機関に伝達する（行動 2）。研究拠点（Centre of Excellence）(52) は、EU 及び NATO と協力し、ハイブリッドな脅威の戦略分析と調査研究を実施する（行動 3）。欧州委員会と構成国は、共同して、重要インフラ(53) に対するハイブリッドな脅威への防護を実施する（行動 5）。重要インフラには、エネルギー部門（行動 6、行動 13）、輸送部門（行動 7、行動 15）、宇宙部門（行動 8）、公衆衛生及び食品部門（行動 10）、金融部門（行動 14、行動 16）が含まれる。

JOIN(2016) 18 final が示す枠組みの下において、ハイブリッドな脅威に対抗するための EU の防衛力が増強され（行動 9）、サイバーセキュリティが強化される（行動 11）。

JOIN(2016) 18 final が策定された時点において、NIS 指令 (EU) 2016/1148 は、まだ採択されておらず、NIS 指令案の段階にあったが、この点に関し、JOIN(2016) 18 final は、「共同立法者によって採択されれば、指令の実効的な国内法化及び実装は、ハイブリッドな脅威に関する情報及びベストプラクティスの交換を介して構成国間のサイバーセキュリティに関する協力を強化する全構成国にわたるサイバーセキュリティ能力を助けることになる。とりわけ、指令は、任意ベースで業務遂行上の協力を遂行する 28 の国内 CSIRT（コンピュータセキュリティインシデ

ント対応チーム）及び CERT-EU のネットワークの設置を定めている」、「官民の協力及び EU 全域にわたるサイバーセキュリティへの取り組みを推進するため、欧州委員会は、NIS プラットフォームを構築し、リスク管理に関するベストプラクティスガイドを発行する。構成国は、国内インシデントを通知するためのセキュリティ上の要求事項及び書式を定めるが、欧州委員会は、とりわけ、欧州連合ネットワーク情報セキュリティ局（ENISA）を想定するリスク管理の取り組みの高度な収斂を推進する」と述べている。要するに、サイバーセキュリティにおける（特に技術的な面における）EU の中枢機関は ENISA であり、その業務遂行に必要な情報が ENISA に集められる。

JOIN(2016) 18 final が示す枠組みの下において、ハイブリッド攻撃からの回復力が強化され（行動 17）、第三国（特に近隣諸国）及び国際機関との協力関係の構築が推進される（行動 18）。そして、TFEU 第 222 条及び TEU 第 42 条第 7 項に基づき、構成国の連携によるサイバー防衛（行動 20、行動 21）及び NATO との合同的な対応（行動 22）が推進される。

以上のような政策に基づき、これらの EU の関連機関の連携した活動を容易にするため、IT システムとして eu-LISA が使用され(54)、欧州犯歴情報システム（ECRIS）に記録されている情報の利用の向上が推進されている(55)。

欧州委員会は、2017 年 6 月「セキュリティに関する欧州アジェンダ（A European Agenda on Security）」を公表したが、これは、JOIN(2016) 18 final に示された行動計画の達成状況及び情報セキュリティ政策上の最新の検討課題を報告するセキュリティユニオン進捗状況報告書（Security Union Progress Report）における検討結果を踏まえ、サイバー脅威に対する対抗策を更に推進するものである。

セキュリティユニオン進捗状況報告書は、2016 年 10 月 12 日に最初の報告書 COM(2016) 670 final が提出されて以来、2016 年 11 月 16 日の第 2 次進捗状況報告書 COM(2016) 732 final、2016 年 12 月 21 日の第 3 次進捗状況報告書 COM(2016) 831 final、2017 年 1 月 25 日の第 4 次進捗状況報告書 COM(2017) 41 final、2017 年 3 月 2 日の第 5 次進捗状況報告書 COM(2017) 203 final、2017 年 4 月 12 日の第 6 次進捗状況報告書 COM(2017) 213 final、2017 年 5 月 16 日の第 7 次進捗状況報告書 COM(2017) 261 final、2017 年 6 月 29 日の第 8 次進捗状況報告書 COM(2017) 354 final、2017 年 7 月 26 日の第 9 次進捗状況報告書 COM(2017)

407 final、2017 年 9 月 7 日の第 10 次進捗状況報告書 COM(2017) 466 final、2017 年 11 月 18 日の第 11 次進捗状況報告書 COM(2017) 608 final[56] 、2017 年 12 月 12 日の第 12 次進捗状況報告書 COM(2017) 779 final、2018 年 1 月 24 日の第 13 次進捗状況報告書 COM(2018) 46 final、2018 年 4 月 17 日の第 14 次進捗状況報告書 COM(2018) 211 final、2018 年 6 月 13 日の第 15 次進捗状況報告書 COM(2018) 470 final[57] と続き、2018 年 11 月の時点における最新の報告書は、2018 年 10 月 10 日の第 16 次進捗状況報告書 COM(2018) 690 final である。

第 11 次進捗状況報告書 COM(2017) 608 final の中で取り上げられている公共の場の安全の確保の必要性に対応するための行動計画は、「公共の場の防護を支援するための行動計画」COM(2017) 612 final として公表されている。これは、直接的には、欧州において現実に発生した自動車を突進させるテロ攻撃に対する対応策となっている。しかし、第 14 次進捗状況報告書 COM(2018) 211 final においても述べられているとおり、公共の場における安全の確保は、CBRN[58] 及び小型武器[59] との関係においても、同様に非常に重要な事項の 1 つである[60] 。

以上のほか、ハイブリッドな脅威と関連する EU の主要な政策文書として、共同報告書 JOIN (2017) 30 final[61] 、共同報告書 JOIN(2018) 14 final[62] 及び共同通知 JOIN(2018) 16 final[63] が公表されている。また、リスク対応準備規則案 COM(2016)862（2016/0377/COD）が提案されている。

3．4　委員会通知 COM(2018) 226 final

委員会通知 COM(2018) 226 final[64] は、欧州連合内における刑事手続の連携（共助）としての証拠の収集に際し、情報サービスを提供するサービスプロバイダの指定代理者（legal representatives）の指定等の手続を統一化するための法令（指令）の提案書である。

同通知における指定代理者は、EU 域内に本拠地または事業所をもたない第三国のプロバイダに対する刑事手続上の執行にとって必要となる送達等の法定の受理者である。この制度は、刑事手続上の送達の効果を EU 域内で発生させることにより、その後の刑事手続の続行を可能とすると同時に、当該刑事手続上の命令違反行為がある場合の制裁の要件の充足を容易にする。この制度は、規則 (EU) 2016/679（GDPR）（OJ L 119, 4.5.2016, p.1-88）[65] の第 27 条（欧州連合内に設けられて

いない管理者または処理者の代理者）に定める代理者である法人または自然人と同様の機能をもつ法的な仕組みである。

上述のとおり、サイバー攻撃の徴候及びハイブリッドな脅威の徴候を内容とする情報は、サイバー犯罪の捜査だけではなく、一般的な犯罪捜査の過程においても得られることがある。各構成国の刑事法務当局がそのような徴候を獲得した場合において、各構成国の関連する行政機関の連絡部局（contact point）を通じて Europol または ENISA に対し情報伝達が行われることがあり得る。このような情報の利用は、当該犯罪捜査の直接の目的からは逸れるものであるが、犯罪捜査に関してはそもそも GDPR の適用除外となっており、特別法である指令 (EU) 2016/680[(66)] を実装する構成国の国内法が適用される[(67)]。また、その徴候が差し迫った脅威（特にハイブリッドな脅威）の存在を示すものである場合には、当該情報の当初の目的外の利用は、一般的な利益または公共の利益を根拠とする適用除外となる。

委員会通知 COM(2018) 226 final の説明覚書は、立法提案の経過説明の中で、「2016 年 3 月 22 日、ブリュッセルにおける法務内務閣僚及び EU の機関の代表のテロリスト攻撃に関する共同声明 は、EU 及び構成国の立法の遵守を拡大するため、第三国及びサービスプロバイダとの協力を強化することにより、より迅速かつ効果的に電子証拠を保全し、確保するための方法を見出す必要性があることを優先的な事項として強調した」、「2016 年 6 月 9 日の理事会決議の中において、サイバー空間における法の支配を維持するために行動すべしとする彼らの決断を再確認し、そして、欧州委員会に対し、サイバー空間における刑事司法を向上させることに関する EU の共通のアプローチを優先的な事項として策定することを求めた」と述べている。ここでいう「法の支配（rule of law）」とは、法執行（law enforcement）の実効性確保のことを意味する。また、「刑事司法（criminal justice）」とは、警察当局及び検察当局による刑事法務のことを意味する。

また、同説明覚書は、サービスプロバイダに対して指定代理者の指定を義務化することの比例性に関し、「刑事手続における証拠の収集を求める決定を受け、遵守し、または、執行するという課題に関し、サービスの提供を妨げる既存の障碍または生じつつある障碍を除去するための整合性のあるアプローチを提案しようとするものである。選択されたアプローチは、課せられる負担と比例的であると判断される。インターネット及び情報社会サービスの重要性の増加及び存在を考慮し、現

在の障碍に対処するための可能な多数の選択肢が存在する。立法提案書に添付された影響評価書の中でより詳細に述べるとおり、これらの選択肢の中で、EU 内において活動する一定のサービスプロバイダに対して指定代理者の任命を義務付けることは、サービスプロバイダに対して不適切な負担を課すことなく、法的命令を与えることができるようにするための効果的な仕組みを提供するという目的を達成するものである」と述べている。ここでいう影響評価書とは、委員会スタッフ作業文書 SWD(2018) 118 のことを指す。

委員会通知 COM(2018) 226 final によって提案されている指令案（2018/0107 (COD)）の前文(7)は、「刑事手続における証拠の収集の目的のために構成国内の職務権限を有する機関から発令された決定の受領、遵守及び執行に関し、欧州連合内の一定のサービスプロバイダの指定代理者に関する整合性のある規定を定めることにより、サービスの支障のない提供を妨げる既存の障碍は、除去されなければならず、また、この点に関する格差のある国内アプローチを将来において課すことは、防止されなければならない。サービスプロバイダのための公平な場が確立されなければならない。更に、自由、安全及び正義という共通領域におけるより効果的な刑事法執行が促進されなければならない」と述べている。

同指令案の第 2 条(1)は、指定代理者とは、「第 1 条第 1 項、第 3 条第 1 項、第 3 条第 2 項及び第 3 条第 3 項の目的のために、サービスプロバイダによって、書面により、指定された法人または自然人のことを意味」すると定義している。

同指令案の第 1 条第 1 項は、「この指令は、刑事手続における証拠の収集の目的のために構成国の職務権限を有する機関から発令された決定及び命令の受領、遵守及び執行に関し、一定のサービスプロバイダの欧州連合内における指定代理者に関する規定を定める」と定めている。

同指令案の第 3 条第 1 項は、「欧州連合内においてサービスを提供するサービスプロバイダが設けられている構成国は、そのサービスプロバイダが、刑事手続における証拠の収集の目的のために構成国の職務権限を有する機関から発令された決定及び命令の受領、遵守及び執行に関し、欧州連合内における少なくとも 1 つの指定代理者を指定することを確保する。指定代理者は、そのサービスプロバイダが設けられ、または、サービスを提供する構成国中の 1 つに居住し、または、設けられる」と定めている(68)。

同指令案の第3条第2項は、「サービスプロバイダが構成国内に設けられていない場合、構成国は、その構成国の領土上においてサービスを提供するサービスプロバイダが、刑事手続における証拠の収集の目的のために構成国の職務権限を有する機関から発令された決定及び命令の受領、遵守及び執行に関し、欧州連合内における少なくとも1つの指定代理者を指定することを確保する。指定代理者は、そのサービスプロバイダがサービスを提供する構成国中の1つに居住し、または、設けられる」と定めている。

そして、同指令案の第3条第3項は、「刑事手続における証拠の収集のために、欧州連合の機能に関する条約の第5款第4章の適用範囲内で採択された欧州連合の法律文書に基づき、構成国の職務権限を有する機関から発令された決定及び命令の受領、遵守及び執行に関し、その法律文書に参加する構成国は、その構成国の領土上においてサービスを提供するサービスプロバイダが、それらの構成国の1つにおいて、少なくとも1つの指定代理者を指定することを確保する。指定代理者は、そのサービスプロバイダがサービスを提供する構成国中の1つに居住し、または、設けられる」と定めている。

同指令案の第3条にいう「職務権限を有する機関（competent authorities）」とは、法執行機関（law enforcement office）、すなわち、刑事法務を担当する警察当局及び検察当局のことを意味する(69)。ただし、構成国の国内法がそのように定める場合、機能論的には、裁判所の捜査判事（令状事務担当判事）も職務権限を有する機関である。捜査判事の法制論上の位置づけは、当該構成国の憲法(70)及び関連国内法令並びに法的伝統によって異なる。また、同指令案の第3条の「令状」は、上述の欧州捜査命令（EIO）を含む。

ところで、NIS指令(EU) 2016/1148の第4条(10)は、「代理者」について、「欧州連合内に設立されたのではないデジタルサービスプロバイダの代わりに行動するために明示で指定された自然人または欧州連合内に設けられた法人のことを意味し、この指令に基づく当該デジタルサービスプロバイダの義務に関し、そのデジタルサービスプロバイダに代わって、構成国の職務権限を有する機関または国内CSIRTによって指定されることがある」と定義し、第18条第2項は、欧州連合内で設立されたものではないが、オンライン市場、オンライン検索エンジンまたはクラウドコンピューティングサービスのサービス（同指令別紙Ⅲ）を欧州連

合内において提供するデジタルサービスプロバイダに関し、「欧州連合内における代理者を指定するものとする。代理者は、そのサービスが提供されている構成国の中のいずれか 1 つに設けられなければならない。デジタルサービスプロバイダは、代理者が設けられた構成国の裁判管轄に服するものとみなされる」と定めている。すなわち、EU の構成国ではない第三国の事業者[71] は、EU 域内に事業所（establishment）が存在しない場合には、その代理者をもたなければならない。そして、その事業者の EU 域内における事業所または代理者は、当該事業者の EU 域内における経済活動に伴う情報セキュリティ上の重大なインシデントに関し、その情報の通知義務を負うことになる。

以上を踏まえた上で、委員会通知 COM(2018) 226 final による指令案第 2 条 (1) における指定代理者、NIS 指令 (EU) 2016/1148 における代理者及び GDPR 第 27 条の代理者は、同一の自然人または法人が兼ねることが普通にあり得ることが当然に想定されているものと考えられる[72] 。そのような場合、委員会通知 COM(2018) 226 final による捜査令状の受領等、NIS 指令 (EU) 2016/1148 によるインシデント情報の通知、GDPR による個人データの侵害の通知は、同一の代理者によって実施される。そして、Europol や ENISA に集められた情報に基づく EU 全体の危機管理体制に関しては、既述のとおりである。

3．5　COM(2017) 477 final（Cybersecurity Act）

ENISA（European Union Agency for Network and Information Security）[73] に関する現行法令は、ENISA 規則 (EU) No 526/2013（OJ L 165, 18.6.2013, p.41-58）[74] である。COM(2017) 477 final（Cybersecurity Act）は、ENISA を「EU サイバーセキュリティ局（EU Cybersecurity Agency）」として改組し、その権限を拡大するための改正提案であり、2018 年 11 月現在、審議中である（2017/0225 (COD)）。

NIS 指令 (EU) 2016/1148 との関係では、Cybersecurity Act の中で使用される用語が NIS 指令 (EU) 2016/1148 の中で使用される用語と統一される（Cybersecurity Act の第 2 条）。また、ENISA は、特に NIS 指令 (EU) 2016/1148 との関係において、欧州連合のサイバーセキュリティの基本方針及び法律の一貫性のある実装について、構成国を補佐すること（Cybersecurity Act の第 5 条第 2 項）、NIS 指令 (EU)

2016/1148 の第 11 条に定める協力グループの仕事に貢献すること（Cybersecurity Act の第 5 条第 3 項）、構成国の連絡部局からのインシデント通知に関する報告書を提出することによって、欧州連合の政策決定活動を支援すること（Cybersecurity Act の第 5 条第 5 項(a)）、CERT-EU、構成国の CSIRT 及び CSIRT ネットワーク並びに協力グループを支援すること（Cybersecurity Act の第 6 条）、セキュリティ業務の遂行に関し、CERT-EU 及び利害関係者等との協力関係を強化すること（Cybersecurity Act の第 7 条）、CSIRT グループに対して事務局を提供すること（Cybersecurity Act の第 7 条第 2 項）、ICT 製品及び ICT サービスのセキュリティに関する技術標準、運用指針等の策定に関与すること（第 8 条）(75)、ネットワーク及び情報システムのセキュリティに関し、特に NIS 指令(EU) 2016/1148 の別紙Ⅱに掲げる重要インフラの安全性確保のために、構成国の専門家と協力して、助言、運用指針及びベストプラクティスを提供すること（Cybersecurity Act の第 9 条(c)）が予定されている。

これら Cybersecurity Act で予定されている方策は、NIS 指令(EU) 2016/1148 において既に定められているものであるが、ENISA の権限を定める現行の ENISA 規則(EU) No 526/2013 においては、ENISA に対する権限授与の根拠条項との関係が明確ではないため、少なくともこの点に関しては同規則の改正が不可避のものとなっている。それ以上に重要なことは、Cybersecurity Act が提案どおりに採択された場合、欧州連合におけるサイバーセキュリティの中枢機関としての戦略及び業務遂行の両面における ENISA の役割が格段に増加し、また、上述の EU 全体の危機管理体制の中における ENISA の重要性も増加するということである。

4　個人データ保護との関係

NIS 指令(EU) 2016/1148 が定めるインシデント情報の通知の中には当該インシデントと関連する自然人の個人データが含まれ得ることから、当該個人データの適正な法的保護が必要となる。それと同時に、ネットワーク及び情報システム上で発生するインシデントは、例えば、ハッキングによる利用者個人データの大量外部流出のように、直接的に、個人データの侵害を発生させ得る(76)。

NIS 指令 (EU) 2016/1148 の第 2 条第 1 項は、「この指令による個人データの処理は、指令 95/46/EC に従って行われる」と定めているが、2018 年 5 月 25 日以降は、個人データ保護指令 95/46/EC ではなく、GDPR が適用される。特に、構成国の行政機関、CSIRT 及び CSIRT ネットワークに関しては、GDPR が適用される。NIS 指令 (EU) 2016/1148 の第 8 条第 6 項は、「職務権限を有する機関及び連絡部局は、それが適切なときは、かつ、国内法に従い、国内の関連法執行機関及び国内個人データ保護機関と協議し、これらと協力する」と定めている。

また、NIS 指令 (EU) 2016/1148 の第 2 条第 2 項は、「この指令による欧州連合の機関及び組織による個人データの処理は、規則 (EC) No 45/2001 に従って行われる」と定めている。規則 (EC) No 45/2001（OJ L 8, 12.1.2001, p.1-22）(77) の改正案 COM(2017) 8 final(78) が提案されており、2018 年 11 月現在、審議中である（2017/0002 (COD)）(79)。

他方、電子通信と関係する個人データ保護に関しては、e プライバシー指令 2002/58/EC（OJ L 201, 31.7.2002, p.37-47）も適用される。同指令についても改正案 COM(2017) 10 final(80) が提案され、2018 年 11 月現在、審議中である（2017/0003 (COD)）(81)。

更に、第三国との関係に関しては、GDPR 及び規則 (EC) No 45/2001 に定める個人データの第三国移転に関する条項が適用されるほか、NIS 指令 (EU) 2016/1148 の第 13 条は、「欧州連合は、TFEU の第 218 条に従い、第三国または国際機関との間で、協力活動グループの活動の中の幾つかにそれらが参加することを認め、それを組織する国際協定を締結できる。そのような協定は、個人データの十分な保護を確保する必要性を考慮に入れるものとする」と定めている。

5　知的財産権保護との関係

NIS 指令 (EU) 2016/1148 の第 1 条第 5 項は、「TFEU の第 346 条を妨げることなく、営業秘密に関する法令のような欧州連合及び構成国の法令によって秘密のものとされる情報は、この指令の適用のためにそのような情報の交換が必要となる場合に限り、欧州委員会及びそれ以外の関連機関との間で交換される。交換される情

報は、その交換の目的と関連するものであり、かつ、必要十分なものに限定される。この情報交換は、情報の機密性を確保し、重要サービス運営者及びデジタルサービスプロバイダの安全及び商業的利益を保護するものとする」と定めている。

知的財産権の一種としての営業秘密保護に関する EU の基本法令は、指令 (EU) 2016/943（OJ L 157, 15.6.2016, p.1-18）(82) であるが、データベースの法的保護に関する *sui generis* の権利の適用関係も検討しなければならない(83)。

6 まとめ

以上で本稿における検討を終える。

本稿においては、NIS 指令 (EU) 2016/1148 の構造及び機能の分析を通じて、関連諸法令及び法令案との関係を考察し、EU 全体の危機管理体制の中におけるその位置づけを明確にできたと考える。その結果、NIS 指令 (EU) 2016/1148 の適用は、指令の条項それ自体の中に示されているところよりも広範なものであり、技術的な意味における情報セキュリティ上のインシデント対応だけではなく、サイバー犯罪捜査及びハイブリッド脅威への対応とも関連性をもつものであり、最悪の場合には軍事行動の契機ともなり得るものであること、NIS 指令における情報セキュリティ上のインシデント情報収集及び情報共有の仕組み（特にインシデント通知義務）は、そのようなものとして機能するものであることが明らかとなった。

NIS 指令 (EU) 2016/1148 と日本国の関連法令との関係、特に日本国の情報セキュリティ基本法とその附属法令、個人情報保護法令及び知的財産関連法令との関係に関しては、EU における ENISA を改組する Cybersecurity ACT を含む既述の改正法案及び European Electronic Communications Code（COM(2016) 590 final）の立法動向を踏まえた上で、他日を期すこととしたい。

加藤哲実先生の御厚情に感謝し、本稿をもって献呈論文とする。

以上（2018 年 11 月 23 日脱稿）(84)

（明治大学法学部教授）

注

(1) 夏井高人「データ駆動型経済通知 COM(2014) 442 final [参考訳]」法と情報雑誌 3 巻 4 号 129～147 頁 (2018) 参照。なお、法と情報雑誌に掲載して公表した私訳である参考訳の中には誤訳や誤記等が含まれている箇所並びに後の検討結果に基づき訳を改めた部分等が存在する。それらについては、気づき次第、同誌上において定期的に、及び、Web 上において可及的速やかに、正誤表の形式で公表しているほか、必要に応じて改訂版を作成し、公表している。

(2) 虚偽情報または情報攪乱の手法（disinformation）を用いた選挙妨害行為や扇動行為等を含め、外国政府による新たな類型のサイバーな謀略活動に関しては、後述のとおり、ハイブリッド脅威（Hybrid Threats）という概念によってまとめられ、この脅威への対抗政策が構築され、実施されている。ハイブリッド脅威は、サイバー空間における脅威だけで構成されるものではなく、国際条約によって禁止されている生物兵器、化学兵器、放射線兵器及び核兵器（CBRN）の使用や爆弾テロ攻撃等を含め、現実世界における謀略活動や攻撃を組み合わせた複合的な攻撃として理解されており、最悪の場合には、集団的防衛権の行使を含む軍事行動による対処が必要な場合があり得ることを当然のものとして想定するものである。このような意味でのハイブリッド脅威に対抗するため、EU は、NATO との連携を明確化し、後述の EU レベルの官民一体的なものとしての一元的な危機管理体制の構築、関連法制の整備及び関係機関等の訓練・教育の強化を進めると同時に、NATO と合同の模擬演習を重ねている。他方において、EU は、重要インフラ等と関係する企業の買収（多数株式の取得、不動産の購入等）を通じた外国からの脅威に対抗するため、監視措置及び規制措置の厳格化を進めている。ここでは、通常の経済取引や外国からの投資を手段とする謀略行為または侵略行為の可能性が明確に認識されている。同様のことは、映画、演劇、音楽、書籍、雑誌、その他の娯楽作品、SNS 等を含め、ごく普通の文化活動やスポーツ活動を通じた文化汚染活動による謀略行動についても言うことができる。このことは、ワイマール憲法が定める本来の目的に反して平和的な手段が外見上適法に濫用され、ナチス政権という独裁体制が成立したという歴史認識または歴史上の経験が基底にあるものと推察される。このことは、TFEU の第 222 条において、EU の基本的な価値観（特に、民主主義及び基本的な権利の尊重）を破壊する行為をテロリスト活動として位置づけ、EU の構成国による集団的防衛権の行使の法的正当性根拠としていることにも現れている。

　一般に、正常かつ平和的な手段の大半は、その濫用によって、本来の目的と相反する結果を生じさせるための手段として使用され得る。このことは、世界共通の事象として一般的な法制度に通有することであるので、今後の法政策学及び法解釈学は、「法制度の濫用」に対し、より大きな重点を置くものとしなければならない。そのためには、法制度それ自体が、自律的に価値を自動実現可能な仕組みなのではなく、あくまでも何らかの目的を実現するための社会的な手段（道具）の一種であることを明確に認識することが要求される。法哲学上及び法思想史上の概念を一応措くとして、社会制度としての法制度は、客観的には、広い意味でのマネジメントシステムの一種である。とりわけ、情報法制は、そうである。

(3) 法案文に関しては、夏井高人「ネットワーク情報セキュリティ指令案：NIS 指令案 [参考訳]」法と情報雑誌 1 巻 1 号 1～50 頁 (2016) 参照。

(4) 委員会スタッフ作業文書 SWD(2013) 32 final には、個人データ保護（data protection）に対する影響評価の側面に関しても多数の言及があり、貴重な政策文書の 1 つである。な

お、委員会スタッフ作業文書 SWD(2013) 32 final の別紙 11（ANNEX 11）には、情報セキュリティと交叉する法的側面において考慮すべき法的要素の分野リストがある。その中には、「異なるタイプのコンピュータ及びネットワークの濫用に関する定義及び刑事制裁」、「個人データ保護及びプライバシーを規律する欧州の法的枠組み」、「情報の自由（FoI）及び公的部門の情報の二次利用（PSI）立法」、「刑事手続」、「知的財産権」、「守秘義務」、「準拠法の決定」並びに「CERT の任務及び職務権限」が含まれている。

(5) 夏井高人「欧州連合法執行協力局（Europol）規則 (EU) 2016/794 [参考訳]」法と情報雑誌 2 巻 3 号 1～101 頁 (2017) 参照。なお、同規則により廃止された Europol 決定 2009/371/JHA に関しては、同「2009/371/JHA [参考訳]」同誌 2 巻 2 号 31～98 頁 (2017) 参照。

(6) 日本国における EC3 に対応する機関は、日本サイバー犯罪対策センター（JC3）である。

(7) サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」経済産業省（2002 年 4 月）、夏井高人「サイバー犯罪条約（ETS No.185）の説明書 [参考訳]」法と情報雑誌 1 巻 6 号 1～132 (2016) 参照。なお、同参考訳は、2001 年 5 月 1 日に Web 上で公開した「サイバー犯罪に関する条約草案の説明用覚書草案（仮訳）」の改訂版である。

(8) サイバー犯罪全般に関する研究結果は、夏井高人「サイバー犯罪の研究 (1)～(9・完)」として法律論叢誌上で公表した。

(9) 夏井高人「指令 2013/40/EU[参考訳・改訂版]」同誌 2 巻 8 号 164-185 頁 (2017) 参照。

(10) 指令 2013/40/EU にはサイバー犯罪条約の第 7 条（コンピュータ関連偽造）及び第 8 条（コンピュータ詐欺）が含まれていない。その理由は、明確ではないが、同指令 2013/40/EU の採択の時点において、EU の構成国が既にこれらの条項に相当する処罰条項を国内法中にもっていたからではないかと推定される。これは、EU における補完性原則と関連する事柄である。

(11) 植月献二「【EU】児童の性的搾取・児童ポルノ等の対策強化指令」外国の立法 250-1 号 6～7 頁 (2012) 参照。

(12) Europol は、毎年、the Internet Organised Crime Threat Assessment（IOCTA）を発行している。

(13) 夏井高人「指令 (EU) 2015/849 [参考訳]」法と情報雑誌 3 巻 2 号 140～198 頁 (2018) 参照。

(14) 夏井高人「指令 (EU) 2018/843 による改正後の指令 (EU) 2015/849 [参考訳]」同誌 3 巻 8 号 276～328 頁 (2018) 参照。

(15) 仮想通貨プラットフォームの監視及び規制も含まれる。この点に関しては、夏井高人「FinTech 通知 COM(2018) 109 final [参考訳]」同誌 3 巻 8 号 181～200 頁 (2018) 参照。

(16) 丸橋透「刑事における電子証拠の欧州提出命令及び欧州保全命令に関する欧州議会及び理事会の規則　提案書 COM/2018/225 final [参考訳]」同誌 3 巻 8 号 201～275 頁 (2018) 参照。

(17) 夏井高人「指令 2014/41/EU [参考訳]」同誌 3 巻 7 号 199～245 頁 (2018) 参照。

(18) 夏井高人「指令 2014/42/EU [参考訳]」同誌 3 巻 7 号 246～262 頁 (2018) 参照。

(19) データ保持指令 2006/24/EC（OJ L 105, 13.4.2006, p.54-63）は、トラフィックデータの応急保全を定めていたが、欧州司法裁判所の判決 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8

April 2014, ECLI:EU:C:2014:238 によって、同指令の採択の時から全部無効と判断され、失効した。なお、夏井高人「公衆が利用可能な通信サービスまたは公共通信ネットワークの提供と関係して生成または処理されるデータの保持並びに指令 2002/58/EC の改正に関する欧州議会及び理事会の 2006 年 3 月 15 日の指令（Directive 2006/24/EC）[参考訳]」法と情報雑誌 1 巻 5 号 47～65 頁 (2016)、同「指令 2002/58/EC [参考訳・改訂版]」同誌 2 巻 5 号 158～187 頁 (2017)、丸橋透「欧州連合の通信メタデータ保持法制の検討」法律論叢 91 巻 1 号 279～319 頁 (2018)、同「Tele2 Sverige AB 対スウェーデン郵政通信省（C-203/15）及び英国内務大臣対トム・ワトソン他（C-698/15）先決裁定事件欧州連合司法裁判所大法廷判決（2016 年 12 月 21 日）ECLI:EU:C: 2016:970 [参考訳]」法と情報雑誌 2 巻 1 号 1～40 頁 (2017) 参照。

(20) Europol は、サイバーセキュリティポリシーに関する説明文書として、「EU Policy Cycle SOCTA Empact」を公表している。なお、大沢秀介・荒井誠・横大道聡編『変容するテロリズムと法―各国における＜自由と安全＞法制の動向』（弘文堂、2017）参照。

(21) NIS 指令 (EU) 2016/1148 に含まれている諸概念を正確に理解するためには、かつての「電気通信（telecommunication）」の時代から「電子通信（electronic communication）」の時代への変化を踏まえた上で、それぞれの時代における「システム（system）」と「サービス（service）」及びこれに対応する「相互接続性（interconnectivity）」及び「相互運用性（interoperability）」を理解しなければならず、その上で、同指令における「ネットワーク」がかつての「telecommunication network」から「electronic communication network」へと変化し、同指令における「情報サービス（information service）」がかつての「telecommunication service」から「electronic communication service」へと変化した歴史的経緯、とりわけ、通信の自由化に伴うキャリアとサービスベンダとの分離（及びこれに伴う旧来の市場支配者である事業者等による独占の弊害の排除、新規事業者の市場参入の容易化のための接続強制等の法定）という歴史的現象を精密に踏まえた調査・検討・考察が不可欠のものとして求められる。NIS 指令 (EU) 2016/1148 の第 4 条の定義条項は、これらを十分に踏まえた上で理解されなければならない。本稿を執筆するに際し、EU における 1980 年代から今日に至るまでの間の EU の通信関連法令を網羅的に（前文及び別紙等を含め）全訳し、検討する作業を敢行した。これらの訳文の大部分は、法と情報雑誌に掲載して公表している。なお、研究の進展に対応して、従前の参考訳の訳文は、適宜改訂され得る。

(22) NIS 指令 (EU) 2016/1148 が採択されるまでの間に当初案から修正された点、及び、それと関連する議論は、それ自体として非常に興味深いものであり、比較法の分野だけではなく、国際政治学及び法社会学を含む関連諸学の観点からも研究の価値が十分にあると考えられるが、本稿においては、その検討を割愛する。なお、立法過程における審議経過は、Eur-lex 上で検索可能である。

(23) 夏井高人「NIS 指令 (EU) 2016/1148 [参考訳・改訂版]」法と情報雑誌 2 巻 8 号 120～163 頁 (2017)、島村智子「ネットワーク・情報システムの安全に関する指令（NIS 指令）―EU のサイバーセキュリティ対策立法―」外国の立法 277 号 1～32 頁 (2018) 参照。

なお、「Member State」を「構成国」ではなく「加盟国」と訳すことが誤りであり、EU 法及び構成国法の全ての翻訳文において早急に改められるべきものであることは、夏井高人「欧州共同体のオープンネットワーク提供（ONP）指令に基づく基本要件―通信の秘密条項及び個人データ保護と関連する規定の概要―」法律論叢 91 巻 2・3 号掲載予定の脚注 (3) で述べたとおりである。特に、「加盟国」との訳語は、シェンゲン協定と

関連する EU の法律文書及び欧州評議会の諸条約と関連する EU の法律文書の訳文において致命的な破綻をきたすことが不可避である。「micro enterprises」は、「零細企業」ではない。委員会勧告 2003/361/EC の定義に従い、「マイクロ企業」と訳さなければならない。同勧告の定義によれば、大人数の従業者を抱える比較的裕福な企業も「micro enterprises」に含まれ得る。「requirements」は、文脈に応じて、「要件」、「義務」または「要求事項」等と訳し分けなければならない。後述のとおり、「representative」（第 18 条）は、明らかに「代表者」ではない。「代理者」または「代理人」と訳すのが妥当である。現実には、各構成国内にある企業または法律事務所等が委任を受けて「representative」となっている例が多いようである。「subparagraph」は、「後段」ではなく、「副項」である。「後段」との訳語は、同一の項の中に 3 以上の「subparagraph」が存在する場合には必ず破綻する。ちなみに、「段」に相当する語は、「indent」である。また、同翻訳では「ANNEX」を「附属書」と訳しているが、誤りである。一般に、「ANNEX」は、当該文書の形態及び機能の別に従い、「別紙」、「別表」、「別冊」、「附属書」等と訳し分けなければならないが、NIS 指令 (EU) 2016/1148 における「ANNEX」は、明白に「別紙」である。そして、同指令の別紙Ⅱの表の中では関連法令が多数引用されており、それらの法令を全て丹念に精読し、理解した上で訳さなければ正確な訳を得ることができない。別紙Ⅱにおいて区分されているのは、「団体」ではなく、「組織（organisation）」である。「団体」と訳すと、「organisation」に該当する組織が構成国の行政機関または独立行政法人である場合に必ず破綻する。

一般に、EU の法令を翻訳する場合、条文のみの翻訳だけでは明らかに不完全である。特に、当該法令に前文が存在する場合、その前文の部分は、必ず条文と一緒に訳出されなければならない。このことは、EU 構成国の国内法及び EEA 諸国の国内法に関しても基本的には同じである。従来、「Member State」の訳語に関して深刻な問題があることが明確化されてこなかったのは、欧州及びアメリカ合衆国の法令の既存の訳文の圧倒的多数において、前文（recital or preamble）の訳が省略されていたことにも一因があると推測される。訳文の作成に際し、もし前文を含む全文並びに立法提案書、関連判例及び関連政策文書を可能な限り網羅的に真面目に精読した上で、前文を含む完全訳を作成することが励行されていたとすれば、このような問題が発生することはなかったであろう。

(24) 構成国における NIS 指令 (EU) 2016/1148 の実装期限は、2018 年 5 月 9 日である。また、構成国の実装法令を発効させる期限は、2018 年 5 月 10 日である。

(25) 夏井高人「NIS 指令の委員会実装規則 (EU) 2018/151 [参考訳]」法と情報雑誌 3 巻 5 号 192～198 頁 (2018) 参照。

(26) 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) 参照。

(27) 世界各国の危機管理体制に関しては、国立国会図書館調査及び立法考査局『主要国における緊急事態への対処：総合調査報告書』（2003 年 6 月）参照。

(28) EU の通信法制における「通信の秘密」に関しては、前掲「欧州共同体のオープンネットワーク提供（ONP）指令に基づく基本要件―通信の秘密条項及び個人データ保護と関連する規定の概要―」で詳論したとおりである。

(29) NIS 指令のもつ情報共有の仕組みと主要各国の同様の仕組みの比較研究として、田川義博・林紘一郎「サイバーセキュリティのための情報共有と中核機関のあり方―3 つのモデルの相互比較とわが国への教訓―」情報セキュリティ総合科学 9 号 17～44 頁 (2017) がある。

(30) 日本国のサイバーセキュリティ基本法（平成 26 年法律第 104 号）及び個人情報保護法（平成 15 年法律第 57 号・最終改正平成 30 年法律第 80 号）に対する影響に関しては、別稿において論ずることにする。

(31) 将来、人間が 1 人も存在しない人工知能（AI）だけで構成される世界が到来すると、人間が取引を行う市場を想定する必要性も消滅する結果、情報システムの安全性確保のための法制も必要なくなると考えられる。そのような時点においては、人工知能による防護処理のための技術のみが存在する。その結果、人間が存在しない世界においては、情報セキュリティそれ自体が自己目的化することはあり得る。一般に、不確定要素または不規則要素は、最大のリスク要素であるので、リスクの極小化を最優先で計算した場合、地球上で最も不確定要素または不規則要素をもつ人類を抹殺することが最適解であるという計算結果が算出されることはあり得ることである。特に、完全に自律的な人工知能システムであるというためには、既定の制約条件も自律的に修正または廃棄可能でなければならないので、そのようなシステムに対して何らかの制約条件を設定しても無駄である。換言すると、このような場合には、キルスイッチが成立しない。ただし、人間の尊厳を優先する場合、そのような最適解の是非は別である。このような視点からの検討は、現代における法社会学の重要な部分を構成し得る。

(32) 前述の NIS 指令案の説明覚書参照。

(33) 夏井高人「指令 2002/21/EC（枠組み指令）[参考訳]」法と情報雑誌 3 巻 7 号 76～108 頁(2018)、同「指令 2009/140/EC による改正後の指令 2002/21/EC [参考訳]」同誌 3 巻 9 号 31～58 頁(2018)、同「指令 2009/140/EC [参考訳]」同誌 3 巻 11 号 46～98 頁(2018)参照。

(34) 夏井高人「指令(EU) 2015/1535 [参考訳]」同誌 3 巻 7 号 1～20 頁(2018)、同指令 98/48/EC による一部改正後の指令 98/34/EC [参考訳] 同誌同号 67～75 頁(2018)参照。

(35)「operators」は、通常は、「事業者」である。しかし、NIS 指令(EU) 2016/1148 の第 5 条を国内法に実装する構成国においては、当該業務を遂行する組織が国営または公営のものであり得ることから、その訳語は、一般に民間企業のみを指す「事業者」は適切ではなく、「運営者」とすべきである（第 4 条(4)参照）。

(36) NIS 指令(EU) 2016/1148 の別紙Ⅱの表の 4 に掲げられている金融市場インフラの中には、指令 2014/65/EU（OJ L 173, 12.6.2014, p.349-496）及び規則(EU) No 648/2012（OJ L 201, 27.7.2012, p.1-59）が示されている。指令 2014/65/EU は、指令(EU) 2016/1034（OJ L 175, 30.6.2016, p.8-11）により、一部改正されている。規則(EU) No 648/2012 は、規則(EU) 2017/2402（OJ L 347, 28.12.2017, p.35-80）により、一部改正されている。これらに関しては、夏井高人「金融商品市場指令 2014/65/EU（MiFID Ⅱ）[参考訳]」法と情報雑誌 3 巻 3 号 1～175 頁(2018)、同「指令(EU) 2016/1034 [参考訳]」同誌同号 176～180 頁(2018)、同「OTC デリバティブ規則(EU) No 648/2012 [参考訳]」同誌 3 巻 8 号 1～96 頁(2018)、同「規則(EU) 2017/2402 による改正後の規則(EU) No 648/2012 [参考訳]」同誌同号 97～118 頁(2018)参照。

(37) NIS 指令(EU) 2016/1148 の別紙Ⅱの表の 2 に掲げられている道路インフラの中には、指令 2010/40/EU（OJ L 207, 6.8.2010, p.1-13）が示されている。指令 2010/40/EU は、決定(EU) 2017/2380（OJ L 340, 20.12.2017, p.1-3）により、一部改正されている。指令 2010/40/EU に関しては、夏井高人「ITS 指令 2010/40/EU [参考訳]」法と情報雑誌 2 巻 9 号 27～47 頁(2017)参照。

(38) これらの重要インフラ及び重要サービスを標的とするハイブリッド攻撃に関しては、更

に後述する。

(39) 中尾康二・北原幸彦・竹田栄作・中野初美・原田要之助・山下真『ISO/IEC 27002:2013（JIS Q 27002:2014）情報セキュリティ管理策の実践のための規範：解説と活用ガイド』（日本規格協会、2015）296～300 頁参照。

(40) 夏井高人「サイバーセキュリティ通知 JOIN(2017) 450 final [参考訳]」法と情報雑誌 2 巻 12 号 113～147 頁 (2017) 参照。

(41) このことは、NIS 指令 (EU) 2016/1148 の正文及び直接の立法資料を読むだけでは理解できないものである。他の関連政策文書を網羅的に読み、全体の流れを掴まなければならない。

(42) 後述の委員会勧告 (EU) 2017/1584 の前文 (15) ないし (19) 参照。

(43) 夏井高人「委員会勧告 (EU) 2017/1584 [参考訳]」法と情報雑誌 3 巻 7 号 293～327 頁 (2018) 参照。

(44) Maria Mälksoo, Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO, European Security Vol.27, Issue 3, pp.374-392 (2018) 参照。

(45) 前掲「欧州共同体のオープンネットワーク提供（ONP）指令に基づく基本要件―通信の秘密条項及び個人データ保護と関連する規定の概要―」参照。

(46) 理事会決定 2014/496/CFSP に基づくその後の進捗状況等に関しては、委員会報告書 COM(2017) 616 final が参考になる。

(47) 夏井高人「理事会決定 2014/496/CFSP [参考訳]」法と情報雑誌 3 巻 11 号 171～177 頁 (2018) 参照。

(48) 空間情報それ自体に関しては、指令 2007/2/EC（OJ L 108, 25.4.2007, p.1-14）がある。日本国の関連法令として、地理空間情報活用推進基本法（平成 19 年法律第 63 号）がある。なお、夏井高人「INSPIRE 指令 2007/2/EC [参考訳]」同誌 2 巻 9 号 1～25 頁 (2017) 参照。

(49) 日本国の関連法令として、衛星リモートセンシング記録の適正な取扱いの確保に関する法律（平成 28 年法律第 77 号）、人工衛星等の打上げ及び人工衛星の管理に関する法律（平成 28 年法律第 76 号）、内閣衛星情報センター組織規則（平成 13 年 3 月 29 日内閣総理大臣決定）がある。

(50) サイバー攻撃だけに限定する場合であっても、特定のパケットが攻撃目的のパケットであるか否かを当該パケットそれ自体からは見極めることができない類型の攻撃が多々あり得る。この点に関しては、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。

(51) 一般に、ハイブリッドな脅威は、インターネットを介するサイバー攻撃の脅威が現実化した後に明確に認識されるようになったと考えられる。しかし、実際には相当古くからあった。国家による謀略活動の多くは一般的にハイブリッドなものである。戦時と平時を相互に排他的な関係にあるものとして理解することは不可能であり、戦時と平時が常に共存する状況にあると理解するほうが正しい。従来の国際法の分野において「戦時」として理解されていた現象は、戦時の要素が濃厚になっている状態または現実に物理的な戦闘が遂行されている状況を指すために用いられてきたと考えられる。しかし、平時から戦時に切り替わる、または、戦時から平時に切り替わるということはない。国家間の基本的な関係を左右する構成要素の濃度の変化があるだけである。一般に、国際条約は、そのような濃度を決定する要素の定量的な暫定的制限のための合意文書に過ぎず、定性

的な最終解決を得るための力をもち得ない。このことは、本源的には、個々の自然人が自己保存本能を維持し、かつ、他の自然人との交渉をもつ限り、それらの自然人の間において、少なくとも潜在的には何らかの軋轢と闘争が生じ得ることに起因するものである。法律論としても、ある者の権利行使は、その権利の行使を受ける者の何らかの利益の喪失を伴わない限り成立しない。ある社会内において許容される権利行使の範囲または閾値とその根拠となる社会的価値観を探究することもまた、法社会学の重要な任務の 1 つである。なお、加藤哲実『法の社会史―習俗と法の研究序説』（三嶺書房、1991）参照。

(52) 研究拠点は、フィンランドのヘルシンキ及びエストニアのリガにあり、NATO との協力関係を強化している。また、JOIN(2018) 14 final によれば、2017 年 9 月、欧州防衛局及び EU の理事会のエストニア大統領職は、政治レベルのサイバーセキュリティインシデントの調整活動及び攻撃的なサイバーキャンペーンの政治的影響の認識を向上させるため、CYBRID17 と命名された EU の防衛大臣のための戦略的机上サイバー演習を実施した。

(53) NIS 指令 (EU) 2016/1148 の別紙Ⅱ参照。

(54) eu-LISA の Web サイト上において、「eu-LISA Programming Document 2018-2020」及び「eu-LISA Strategy 2018-2022」が公表されている。

(55) 丸橋透「域内治安、国境及び移住分野の EU 中央情報システム間の相互運用性の枠組みを定める欧州議会と理事会の 2 つの指令案の影響評価書（委員会スタッフ作業文書）SWD/2017/ 0473 final 及びその要旨 SWD/2017/0474 final [参考訳]」法と情報雑誌 3 巻 2 号 199～332 頁 (2018) 及び同「入国／出国システム (EES) 規則 (EU) 2017/2226[参考訳]」同誌 3 巻 3 号 201～300 頁 (2018) 参照。

(56) 夏井高人「第 11 次進捗状況報告書（COM/ 2017/0608 final）[参考訳]」同誌 2 巻 11 号 156～176 頁 (2018) 参照。

(57) 夏井高人「第 15 次進捗状況報告書 COM(2018) 470 final [参考訳]」同誌 3 巻 10 号 85～106 頁 (2018) 参照。

(58) 田村圭「CBRN テロ対策の動向」保健医療科学 65 巻 6 号 533～541 頁 (2016)、齋藤智也・石金正裕・大曲貴夫・小林彩香・松井珠乃・奥谷晶子・森川茂「炭疽菌による生物テロへの公衆衛生対応」同誌同号 548～560 頁 (2016)、足達好正「CBRN テロ研究の現状と展望」防衛学研究 49 号 101～119 頁 (2013)、河本志朗「大規模イベントにおける CBRN テロ対策の取組と課題（テロ対策と大量破壊兵器の不拡散）」国際安全保障 44 巻 2 号 69～85 頁 (2016)、植月献二「EU における原子力の利用と安全性」外国の立法 244 号 39～55 頁（2010) 参照。

(59) 佐藤丙午「小型武器問題とミクロ軍縮―新しい国際規範の形成と国連の役割―」防衛研究所紀要 6 巻第 1 号 70～94 頁 (2003)、榎本珠良「武器移転規制と秩序構想―武器貿易条約（ATT）の実施における課題から―」国際武器移転史 1 号 53～76 頁 (2016) 参照。

(60) これらは、現時点において最も重視されている検討課題の 1 つである。CBRN のリスクに対処するための行動計画に関しては、2017 年 10 月 18 日の委員会通知 COM(2017) 610 final がある。小型武器（Small and Light Weapons (SALW)）に関しては、2006 年 1 月 13 日の理事会戦略文書（5319/06）及び 2015 年 10 月 22 日の理事会決定 (CFSP) 2015/1908（OJ L 278, 23.10.2015, p.15-25）がある。なお、医薬品、化粧品、サプリメント等を装った巧妙な CBRN 攻撃に対する警戒も必要である。

(61) 夏井高人「ハイブリッドな脅威報告書（JOIN (2017) 30）[参考訳]」法と情報雑誌 2 巻 8 号 91～119 頁 (2017) 参照。

(62) 夏井高人「ハイブリッドな脅威報告書 JOIN(2018) 14 final [参考訳]」同誌 3 巻 10 号 178

～198 頁 (198)。

(63) 夏井高人「ハイブリッドな脅威通知 JOIN(2018) 16/final [参考訳]」同誌 3 巻 9 号 281～295 頁 (2018) 参照。

(64) 夏井高人「委員会通知 COM(2018) 226 final [参考訳]」同誌 3 巻 7 号 328～357 頁 (2018) 参照。

(65) 夏井高人「規則 (EU) 2016/679（一般データ保護規則）[参考訳・再訂版]」同誌 3 巻 5 号 1～114 頁 (2018) 参照。

(66) 夏井高人「指令 (EU) 2016/680 [参考訳]」同誌 2 巻 1 号 41～140 頁 (2017) 参照。

(67) 夏井高人「EU の個人データ保護法令と他の関連立法との関係に関する検討」法律論叢 91 巻 4・5 号掲載予定参照。

(68)「居住し、または、設けられる」との表現は、指定代理者が自然人の場合には設立行為を観念することができず、居住しかあり得ないこと、そして、指定代理者が法人の場合には設立行為及び設立登記が通常であるが、構成国の国内法によっては設立行為が存在しない法人（例：法人格のある組合等）もあり得ることを前提とするものである。以下、第 3 条第 2 項及び同条第 3 項においても同じ。

(69) 夏井高人「EU の行政機関に適用される個人データ保護規則における基本概念―個人データ保護条約及び EU 一般個人データ保護規則との関係を含めて―」法律論叢 89 巻 2・3 号 181～245 頁 (2016) 参照。

(70) 主要国の憲法に関しては、宮沢俊義編『世界憲法集』（岩波文庫、1960）、高橋和之編『新版世界憲法集（第 2 版）』（岩波文庫、2007）がある。

(71) 例えば、Facebook や LINE のような、EU の構成国ではない国に本店が所在する SNS サービスのプロバイダも含まれ得る。

(72) 同一の支配の下にある親子事業者またはグループ企業等を除き、複数の異なる事業者が同一の自然人または法人を代理者に指定した場合には利益相反の問題が生じ得ることは当然の前提とした上で、同一の単一の事業者の代理者である限り、実質的にみて利益相反の問題が生ずることはあり得ないが、その場合においても、観念的には、法定の複数の義務の間における解釈・適用上の抵触問題はあり得る。しかし、いずれも強行法上の義務であるので、抵触は存在しないものとして扱われることになるのであろう。ただし、そのように解する場合であっても、異なる種類の複数の情報について、その送信（通知）の優先順位の問題は残る。

　なお、EU 法におけるこのような代理者の指定義務に関し、EU 法の域外適用の問題として議論されることがあるが、そのような見解は誤りである。EU 法は、EU 域内において事業活動を営む事業者に対して適用される。ただ、当該事業者の事業所が EU 域内に存在しない場合、法の適用（執行）が不可能となることがあり得ることから、EU 法の域内適用（域内執行）を確保するために代理者指定義務が定められているのである。

(73) ENISA は、ギリシアのクレタ島に本拠地を置き、アテネに支局をもつ。

(74) 夏井高人「ENISA 規則 (EU) No 526/2013 [参考訳]」法と情報雑誌 3 巻 7 号 263～292 頁 (2018) 参照。

(75) 夏井高人「先端デジタル技術の法的責任に関する欧州委員会スタッフ作業文書 SWD(2018) 137 final [参考訳]」同誌 3 巻 9 号 233～268 頁 (2018)、同「欧州のための人工知能通知 COM(2018) 237 final [参考訳]」同誌同号 198～232 頁 (2018) 参照。

(76) 脚注 72 参照。

(77) 夏井高人「規則 (EC) No 45/2001 [参考訳・改訂版]」法と情報雑誌 2 巻 5 号 111～146 頁

(2017) 参照。

(78) 夏井高人「規則 (EC) No 45/2001 の改正案 [参考訳]」同誌 2 巻 4 号 249～354 頁 (2017) 参照。

(79) 脚注 67 参照。

(80) 丸橋透・夏井高人「指令 2002/58/EC の改正案 [参考訳]」法と情報雑誌 2 巻 4 号 195～248 頁 (2017) 参照。

(81) 前掲「欧州共同体のオープンネットワーク提供（ONP）指令に基づく基本要件―通信の秘密条項及び個人データ保護と関連する規定の概要―」参照。

(82) 夏井高人「営業秘密指令 (EU) 2016/943 [参考訳]」法と情報雑誌 2 巻 9 号 489～514 頁 (2017) 参照。

(83) 夏井高人「欧州委員会スタッフ作業文書 SWD(2018) 146 final [参考訳]」同誌 3 巻 10 号 128～184 頁 (2018)、同「欧州データ空間通知 COM(2018) 232 final [参考訳]」同誌同号 107～127 頁 (2018) 参照。

(84) 本論文は、科学研究費補助金共同研究基盤研究 (A) 知的財産権と憲法的価値・科研費研究課題番号 15H01928 の研究成果の一部である。