NIS 指令の委員会実装規則(EU) 2018/151

[参考訳]

2018 年 5 月 4 日
明治大学法学部教授
夏　井　高　人

＊＊＊

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact（OJ L 26, 31.1.2018, p.48-51）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:32018R0151&from=EN
[2018 年 5 月 3 日確認]

実装規則(EU) 2018/151 は、NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1-30）の第 16 条第 8 項に基づき、同指令の適用のための細目的な仕様を定める実装規則である。

実装規則(EU) 2018/151 は、前文及び条文で構成されている。この参考訳においては、実装規則(EU) 2018/151 の前文及び条文の全文を訳した。

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、あくまでも実装規則(EU) 2018/151 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。

実装規則(EU) 2018/151 は、例えば、インターネット上でコンテンツを提供するサービスプロバイダやクラウドコンピューティングサービスのプロバイダ等だけに適用される法令ではない。適用対象となるのは、主として、NIS 指令の別紙 III に定める重要インフラ及び重要な施設管理業務（特に、金融関係、交通・運輸関係等）で用いられる情報システムの運用者やそのサービスのプロバイダである。その意味で、実装規則(EU) 2018/151 は、国防関係、テロ対策を含む警察活動の関係においても、税関当局

や入管当局を含む行政機関との関係においても、そして、金融活動及びグローバルな商取引との関係においても、非常に大きな重要性をもつ EU の法令の 1 つであると言える。

一般に、情報セキュリティに関する基本的な素養をもつことは、現代の全ての法領域において、法律実務に携わる者にとって必須の素養である。それと同時に、情報セキュリティと関連する重要な関連法令を正確かつ迅速に認識・理解できることは、全ての法学研究者にとって必要不可欠なものである。その素養・知識・能力を欠く場合、例えば、民法の条項の一般的な解釈論において、「安全配慮義務」のような法概念だけではなく、「債務の本旨に従った履行」あるいは「過失」といったような普通の法概念の具体的な内容を全く想像できないような事態に陥ることが十分にあり得る。

（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。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。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。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。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 の参考訳は、法と情報雑誌 3 巻 2 号 199～332 頁にある。データ駆動型経済通知 COM(2014) 442 final の参考訳は、法と情報雑誌 3 巻 4 号 129～147 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を参考にした。

＊＊＊

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るリスクを管理するために デジタルサービスプロバイダによって考慮に入れられるべき要素の、並びに、 重大な影響をもつインシデントであるか否かを判定するためのパラメータの 更に詳細な仕様との関連において、 欧州議会及び理事会の指令(EU) 2016/1148 の適用のための規則を定める 2018 年 1 月 30 日の委員会実装規則(EU) 2018/151

欧州委員会は、
欧州連合の機能に関する条約に鑑み、
欧州連合内のネットワーク及び情報システムの共通の高いレベルの安全性のための措置に関する欧州議会及び理事会の 2016 年 7 月 16 日の指令(EU) 2016/1148[1]、並びに、とりわけ、その第 16 条第 8 項に鑑み、
以下のとおりであるので、この規則を採択する。

(1) 指令(EU) 2016/1148 に従い、デジタルサービスプロバイダは、それらの措置が適切なレベルの安全性を確保するものであり、かつ、同指令に定める要素を考慮に入れるものである限り、彼らのネットワーク及び情報システムの安全性に示されたリスクを管理するために適切かつ比例的であると彼らが判断する技術上の措置及び組織上の措置を自由に講ずることができる。
(2) 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。
(3) 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。
(4) 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低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。
(5) 人的資源に関する基本方針は、セキュリティ関連の技能の開発及び注意喚起と関係する側面を含め、技能のマネジメントを参照し得る。業務遂行の安全性に関する一群の適切な基本方針を定

[1] OJ L 194, 19.7.2016, p.1.

める場合、デジタルサービスプロバイダは、変化のマネジメント、脆弱性のマネジメント、業務遂行上及び管理上の業務の定式化、並びに、システムマッピングの側面を考慮に入れることが推奨される。

(6) セキュリティのアーキテクチャに関する基本方針は、とりわけ、ネットワークとシステムの分離、並びに、管理上の業務遂行のような重要な業務遂行のための特に安全な措置で構成され得る。ネットワークとシステムの分離は、デジタルサービスプロバイダに対し、顧客、顧客グループ、デジタルサービスプロバイダまたは第三者に帰属するデータの流れ及びコンピュータ資源のような、諸要素の間の区別を可能にし得るものである。

(7) 物理環境の安全性と関連して講じられる措置は、窃盗、火災、浸水またはそれ以外の気象の影響、電気通信または電源の喪失のようなインシデントによって生ずる損害から組織のネットワーク及び情報システムの安全を確保するものでなければならない。

(8) 電力、燃料または冷却のようなサプライの安全性は、とりわけ、第三者である契約者及び下請け契約者並びにそれらのマネジメントを含むサプライチェーンの安全性を包含し得る。重要なサプライのトレーサビリティは、それらのサプライの淵源を識別し、記録するためのそのデジタルサービスプロバイダの能力を示すものである。

(9) デジタルサービスの利用者には、オンライン市場またはクラウドコンピューティングサービスの顧客または加入者、または、キーワード検索を実行するためのオンライン検索エンジン Web サイトの訪問者である自然人及び法人を含めるものとしなければならない。

(10) インシデントの影響の大きさを定義する際、この規則に定める事例は、重大なインシデントの非網羅的なリストとして考えられなければならない。教訓は、指令(EU) 2016/1148 の第 13 条の(i)及び(m)に示すリスク及びインシデントに関するベストプラクティス情報の収集、並びに、インシデント通知のための書式に関する意見交換と関連して、この規則の実装及び協力グループの作業によって示される。その結果は、指令(EU) 2016/1148 の第 16 条第 3 項に基づいて提供されるデジタルサービスに関する通知義務の契機となり得る通知パラメータの量的閾値に関する包括的な運用指針となり得る。それが適切なときは、欧州委員会は、この規則に定める現行の閾値の見直しを検討し得る。

(11) 職務権限を有する機関が、潜在的な新たなリスクの情報提供を受けることができるようにするため、デジタルサービスプロバイダは、新たな攻撃手法、攻撃ベクターまたは脅威アクター、脆弱性及びハザードのような、彼らにとって従前知られていなかった特徴をもつインシデントを任意に報告することが奨励され得る。

(12) この規則は、指令(EU) 2016/1148 の移行期間の期間満了の翌日に適用されなければならない。

(13) この規則に定める措置は、指令(EU) 2016/1148 の第 11 条第 3 項に示すネットワーク及び情報システム安全性委員会の意見に従うものである。

第 1 条　対象事項

この規則は、デジタルサービスプロバイダが指令(EU) 2016/1148 の別紙 III に示すサービスを提供する過程において使用するネットワーク及び情報システムの一定のレベルの安全性を判断し、それを確保するための措置を講ずる際、デジタルサービスプロバイダによって考慮に入れられるべき諸要素をより詳しく定め、かつ、それらのサービスの提供に対してインシデントが重大な影響をもつか否かを判断するために考慮に入れられるべきパラメータをより詳しく定める。

第 2 条　安全性の要素

1. 指令(EU) 2016/1148 の第 16 条第 1 項の(a)に示すシステム及び施設の安全性とは、ネットワーク及び情報システムの安全性並びにそれらの物理環境の安全性を意味し、以下の諸要素を含める：

(a) 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、それは、情報システムのマッピング、及び、情報セキュリティの管理に関する一群の適切な基本方針を確立することを意味し、リスク分析、人的資源、業務遂行の安全性、セキュリティのアーキテクチャ、セキュアデータ及びシステムライフサイクルマネジメント、並びに、それが適切なときは、暗号及びそのマネジメントを含める；

(b) 物理環境の安全性、それは、例えば、システム停止、人的エラー、悪意ある活動または自然災害に対処する全ハザードのリスクベースのアプローチを用い、デジタルサービスプロバイダのネットワーク及び情報システムの安全性をそれが損なわれることから保護するための一群の措置の可用性のことを意味する；

(c) サプライの安全性、それは、アクセシビリティを確保するための、及び、それが適用可能なときは、サービス提供において使用される重要なサプライのトレーサビリティを確保するための適切な基本方針を確立すること、及び、それを維持することを意味する；

(d) ネットワーク及び情報システムのアクセス管理、それは、ネットワーク及び情報システムの管理上の安全性を含め、ネットワーク及び情報システムへの物理的アクセス及び論理的アクセスが、業務上の要求事項及びセキュリティ上の要求事項に基づいて承認され、かつ、制限されることを意味する。

2. 指令(EU) 2016/1148 の第 16 条第 1 項の(b)に示すインシデントの取扱いに関し、デジタルサービスプロバイダによって講じられる措置は、以下のものを含める：

(a) 異常事態の適時かつ適切な覚知を確保するために維持管理され、テストされる検出プロセス及び手続；

(b) インシデント報告、並びに、そのプロバイダの情報システムの弱点及び脆弱性の識別に関するプロセス及び基本方針；

(c) 定められた手続に従った対応、及び、講じられた措置の結果報告；

(d) インシデントの深刻度の評価、インシデント分析から得られる知識の文書化、及び、証拠として提供され、そして、継続的な改善プロセスを支援し得る関連情報の収集。

3. 指令(EU) 2016/1148 の第 16 条第 1 項の(c)に示す事業継続性のマネジメントとは、破壊的なインシデントの後に、受容可能な予め定められたレベルのサービス提供を維持するため、または、適切に修復するための組織の能力のことを意味し、かつ、以下のものを含める：

(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の継続性を確保するための業務影響分析に基づく危機管理計画を確立すること、及び、それを使用すること、それは、例えば、演習を通じて、継続的に評価され、テストされる;
(b) 災害からの復旧能力、それは、例えば、演習を通じて、継続的に評価され、テストされる。

4. 指令(EU) 2016/1148 の第 16 条第 1 項の(d)に示す監視、監査及び試験は、以下に関する基本方針を確立すること、及び、それを維持管理することを含める;
(a) ネットワーク及び情報システムが意図されたとおりに運用されているか否かを評価するための観察または計測の予め計画された手順の実施;
(b) 基準または一群の運用指針が守られているか否か、記録が正確か否か、並びに、効率性及び実効性の目標に適合しているか否かを点検する検査及び確認;
(c) データを保護し、意図した機能を維持する、ネットワーク及び情報システムのセキュリティの仕組みの流れを明らかにするためのプロセス。

5. 指令(EU) 2016/1148 の第 16 条第 1 項の(e)に示す国際標準とは、欧州議会及び理事会の規則(EU) 1025/2012[1]の第 2 条第 1 項の(a)に示す国際標準化機関によって採択された標準のことを意味する。欧州議会及び理事会の規則(EU) 1025/2012 の第 19 条により、既存の国内標準を含め、ネットワーク及び情報システムの安全性に関して欧州で承認され、または、国際的に承認された標準及び仕様を使用することもできる。

6. デジタルサービスプロバイダは、職務権限を有する機関が、第 1 項、第 2 項、第 3 項、第 4 項及び第 5 項に定める安全性の諸要素の遵守を確認できるようにするため、それらのプロバイダが、十分な文書を利用可能なものとすることを確保する。

第 3 条 インシデントの影響が重大であるか否かを判断するために考慮に入れられるパラメータ

1. インシデントによる害を受けた利用者の数、とりわけ、指令(EU) 2016/1148 の第 16 条第 4 項の(a)に示すプロバイダ自身のサービスの提供のためのサービスに依拠する利用者の数に関し、デジタルサービスプロバイダは、以下のいずれかを推計すべき立場にあるものとする:
(a) そのサービスの提供に関する契約を締結し、害を受けた自然人及び法人の数;または、
(b) とりわけ、過去のトラフィックデータを基礎とするサービスを利用し、害を受けた利用者の数。

2. 指令(EU) 2016/1148 の第 16 条第 4 項の(b)に示すインシデントの持続期間とは、可用性、真正性、完全性または機密性の面において、サービスの本来の提供が阻害されてから、回復の時までの間の期間のことを意味する。

3. 指令(EU) 2016/1148 の第 16 条第 4 項の(c)に示すインシデントによって害を受けた領域に関する地理的な範囲内にある限り、そのインシデントがデジタルサービスプロバイダは、特定の構成国内においてそのプロバイダのサービスの提供に害を与えたか否かを判断すべき立場にあるものとする。

---

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

4. 指令(EU)2016/1148 の第 16 条第 4 項の(d)に示すサービスの機能を阻害する範囲は、インシデントによって害された以下の 1 または複数の特性との関連において計測されるものとする：すなわち、データまたは関連サービスの可用性、真正性、完全性または機密性である。
5. 指令(EU) 2016/1148 の第 16 条第 4 項の(e)に示す経済活動及び社会活動に対する影響の範囲に関し、デジタルサービスプロバイダは、その顧客との契約関係の性質、または、それが適切なときは、害を受けた利用者の潜在的な数に基づき、そのインシデントが、健康、安全または財産上の損害のような、利用者にとって重大な物的損失または非物的損失を生じさせたか否かを判断できる。
6. 第 1 項、第 2 項、第 3 項、第 4 項及び第 5 項の目的のために、デジタルサービスプロバイダは、そのプロバイダがアクセスをもたない追加的な情報の収集を要求されるものとしてはならない。

第 4 条 インシデントの重大な影響

1. 以下のいずれかの状況が生じたときは、インシデントは、重大な影響をもつものとみなされる：
(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 万利用者を超えて利用不可能となり、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。
2. 指令(EU) 2016/1148 の第 11 条第 3 項に基づく職務の遂行の過程で協力グループによって収集されたベストプラクティス、及び、同指令の第 11 条第 3 項の(m)に基づく意見交換に基づき、欧州委員会は、第 1 項に定める閾値を見直すことができる。

第 5 条 発効

1. この規則は、EU 官報上で公示された翌日から 20 日目の日に発効する。
2. この規則は、2018 年 5 月 10 日から適用される。

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

2018 年 1 月 30 日にブリュッセルにおいて行われた。

欧州委員会
議長 Jean-Claude Juncker