

## 【ドイツ】 情報セキュリティ法の制定

海外立法情報課 渡辺 富久子

\* 情報セキュリティ法が制定され、重要インフラにおける情報システムのセキュリティ対策が強化された。ウイルスプログラムの拡散を防ぐための法改正も行われた。

### 1 制定の背景

インターネットの普及につれて、情報セキュリティの強化が重要な課題になっている。現在出回っているコンピュータウイルスは2億5千万種を超え、毎日30万種が増えている。また、コンピュータウイルスの1つであるボット（注1）に感染したコンピュータはドイツで100万台を超え、これはアメリカ、中国に次いで多い数字である。（注2）

現在、EUにおいても情報セキュリティ強化のための指令案が検討されているところであるが、問題の重要性に鑑み、ドイツは先駆けて情報セキュリティ法（注3）を制定した。

### 2 情報セキュリティ法の概要

情報セキュリティ法は、連邦情報技術安全庁法（以下「BSI法」）（注4）等の関連法律を改正する法律であり、一部を除き2015年7月25日から施行されている。以下に、主要な規定の概要を紹介する。

#### (1) 重要インフラにおける情報システムの保護

重要インフラ（エネルギー、情報技術、通信、運輸、衛生、水、食糧、金融）の事業者は、情報システムの障害を回避するために、最新の技術基準を遵守して組織的及び技術的な対策を講じなければならない。さらに、重要インフラの事業者は、監査や認証等を受け、最新の技術基準を遵守して対策を講じていることを連邦情報技術安全庁（以下「BSI」）に対して2年ごとに証明しなければならないとされている。具体的にどのような施設を重要インフラとみなすかは、法規命令により別途定められる。（BSI法第8a条）

BSIは、重要インフラの事業者のための連邦のセンターとして位置付けられる。BSIは、この任務を遂行するために、ウイルスプログラムや情報セキュリティに対する攻撃等の情報を収集及び評価し、その重要インフラに対する影響を分析し、重要インフラの情報セキュリティに関する現況の情報を継続的に更新し、これらの情報を重要インフラの事業者並びに連邦及び州の管轄官庁に対して遅滞なく報告しなければならない。（第8b条第2項）

重要インフラの事業者は、重大な情報システムの障害があり、当該重要インフラの機能停止に至るおそれがある場合又は機能停止に至った場合には、これをBSIに対して報告しなければならない。BSIは、当該報告を分析し、得られた知見を他の重要インフラの事業者に提供する。また、BSIは、重要インフラの事業者から重大な情報システムの障害について報告があった場合において、必要なときには、IT製品及び情報システムの製造者に対して協力を求めることができる。（第8b条第4項及び第6項）

これらの重要インフラの情報システムに係る規定は、従業員 10 人未満及び年間売上額が 200 万ユーロ未満の事業者には適用されない。また、通信法、エネルギー事業法及び原子力法の同様の規定が適用される事業者にも適用されない。(第 8c 条)

## (2) BSI の権限強化

BSI は、IT 製品の安全性の欠陥及びウイルスプログラムについての警告を公衆又は関係機関に発することができるが、これに加えて、データの消失又はデータへの不正アクセスがあった場合にも警告を発することができるようになった(第 7 条)。

さらに、BSI は、販売中の又は販売予定の IT 製品及び情報システムの安全性を検査することができるようになった。BSI は、検査を第三者に委託することもできる。(第 7a 条)

## (3) テレメディア法及び通信法の改正

業としてウェブサイトを経営する者は、そのウェブサーバに不正アクセスがなされないように技術的及び組織的な対策を講じなければならない(テレメディア法第 13 条第 7 項)。この措置は、十分に保護されていないウェブサーバを通じたウイルスプログラムの拡散を防ぐことを目的としている。

インターネット接続事業者は、利用者のインターネット接続機器が攻撃の足場として悪用されていることを確認した場合には、当該利用者にその旨を通知し、可能な範囲において、これを防御する方法を教示しなければならない(通信法第 109a 条第 4 項)。

## (4) 連邦刑事庁の捜査権限の拡大

連邦刑事庁は、他者にとって重要な意味を有するデータの改変及びコンピュータを対象とした破壊の捜査権限を有するが、これに加えて、データ探知、データ窃盗、データ探知及びデータ窃盗の予備並びにコンピュータによる詐欺についても捜査権限を有することになった(連邦刑事庁法第 4 条第 1 項第 1 文第 5 号)。

注(インターネット情報は 2015 年 9 月 14 日現在である。)

(1) ボットとは、感染したコンピュータを、ネットワークを通じて外部から操作するために作成されたプログラムである。感染したコンピュータは、外部からの指示により、スパムメール送信活動、攻撃活動、ネットワーク感染活動、ネットワークスキャン活動を行う。情報処理推進機構ウェブサイトを参照。<<https://www.ipa.go.jp/security/antivirus/bot.html>>

(2) Deutscher Bundestag, *Plenarprotokoll 18/95*, S.9037.

(3) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324).

(4) 連邦情報技術安全庁(Bundesamt für Sicherheit in der Informationstechnik)は、連邦内務省の下部機関であり、国家レベルの情報セキュリティを所管する。

## 参考文献

・ Deutscher Bundestag, *Drucksache 18/4096*, 5121.