【イタリア】サイバーセキュリティの強化等に関する法律の制定

海外立法情報課長　芦田　淳

＊2024 年 6 月、サイバー攻撃等への対処を強化するための措置を設けるとともに、サイバー犯罪への対応を見直すため、刑法典等の関係法令を改正する法律が制定された。

1　概要

本稿では、2024 年 6 月 28 日法律第 90 号「国家のサイバーセキュリティの強化及びサイバー犯罪に関する規定」[1]（以下「90 号法」）を取り上げる。サイバー攻撃の増加等を踏まえ、同法の基となった法律案は 2024 年 2 月に中道右派政権により提出され、同年 5 月に下院、同年 6 月に上院において可決された。ただし、可決に際して、野党からは、中央行政機関、地方自治体、公共交通機関に新たな負担をもたらす（後述）にもかかわらず、新たな役割に対応するために必要な財源が措置されていないとの批判がなされた[2]。成立した 90 号法は、全 2 章 24 か条から成り、同年 7 月 17 日から施行されている。その第 1 章（第 1 条～第 15 条）は主にサイバー攻撃等への対処を強化するための規定、第 2 章（第 16 条～第 24 条）はサイバー犯罪への対応を見直す規定となっており、その主な内容は次のとおりである。

2　90 号法の主な内容

（1）中央行政機関、地方自治体及び関係事業者に対する義務付け

（ｉ）ネットワーク等に係るインシデントの報告

中央行政機関及び一定規模以上の地方自治体等[3]のほか、当該機関等の内部で情報サービス、輸送サービス、排水処理サービス及び廃棄物処理サービスを提供する主体は、ネットワーク、情報システム及び情報サービスに影響を及ぼすインシデントについて、それを認識した時点から 24 時間以内に国家サイバーセキュリティ庁[4]に通知し、72 時間以内に入手可能な全ての情報について同庁に報告を行うものとする（第 1 条[5]）。5 年間にわたり繰り返し報告を怠った者に対して、国家サイバーセキュリティ庁は、2 万 5000～12 万 5000 ユーロ[6]の過料を科すものとする。また、同庁は、報告の遅延又は不履行が確認されてから 12 か月以内に、レジリエンス（耐性）を強化する措置が実施されたか否か等を検証する目的で、検査を行うことができる。

＊　本稿におけるインターネット情報の最終アクセス日は、2024 年 12 月 4 日である。

1　L. 28 giugno 2024, n.90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. 以下、法令の法文に関しては、イタリア共和国の法令ポータルサイト（Normattiva website <http://www.normattiva.it/>）を参照した。

2　*ANSA*, 20 giugno 2024.

3　ここでいう一定規模以上の地方自治体等とは、州（トレント自治県及びボルツァーノ自治県を含む。）、大都市、人口が 10 万人を超えるコムーネ（基礎的自治体）、州都であるコムーネ、10 万人以上の利用者がいる公共交通機関の運営会社、大都市の域内で運営される郊外公共交通機関の運営会社及び地方保健公社（保健サービスを提供する独立機関）を指す。なお、イタリアの地方自治体は、基本的に「州・自治県－県・大都市－コムーネ」の 3 つの階層に分かれている。

4　国家サイバーセキュリティ庁（Agenzia per la cybersicurezza nazionale）は、2021 年 6 月 14 日緊急法律命令第 82 号「サイバーセキュリティに関する緊急規定、国家サイバーセキュリティアーキテクチャの定義及び国家サイバーセキュリティ庁の設立」に基づいて設立された、サイバーセキュリティ分野における国の利益を保護するための機関である。“Chi siamo.” Agenzia per la cybersicurezza nazionale website <https://www.acn.gov.it/portale/chi-siamo>

5　以下、特に断りがない限り、条名は 90 号法のものである。

6　1 ユーロは約 164 円（令和 6 年 12 月分報告省令レート）。

（ⅱ）脆弱（ぜいじゃく）性への対応

国家サイバーセキュリティ庁は、(i) の報告義務を負う者等に対して、サイバーセキュリティ上の潜在的な脆弱性を通知する（第 2 条）。通知された者は、15 日以内に対応措置を講じるものとする。対応措置の不履行又は遅延は、技術的又は組織的な理由がある場合を除いて、(i) と同額の過料により処罰される。

（ⅲ）サイバーセキュリティ担当者の決定

(i) の報告義務を負う者は、情報のセキュリティに係る方針及び手続の策定等に携わるサイバーセキュリティ担当者を定め、国家サイバーセキュリティ庁に通知するものとする（第 8 条）。

(2) 関連する行政機関職員の転職制限

国家サイバーセキュリティ庁の職員であって、同庁の職務としてその費用により、所定の専門訓練課程に参加した者は、当該課程の終了日から 2 年間、サイバーセキュリティ関連業務を遂行するために民間団体に雇用されることは原則としてできない（第 12 条）。この規定に違反して締結された契約は、無効とする。また、各種情報機関の長又はその次席の地位にあった者等は、一部の例外を除いて、その任期終了から 3 年間、外国の機関及びイタリアの特定分野（防衛、安全保障、エネルギー、輸送及び通信）に関わる民間団体において職務を行ったり、役職に就いたりしてはならない（第 13 条）。

(3) 行政機関等による調達に係る規制

戦略的な国の利益の保護に関連して使用される所定の情報財[7]及び情報サービスを調達する際に行政機関及び公共サービス事業者等が考慮すべき要素（データの機密性、完全性及び可用性を保障するために、調達の対象である情報財等が適合すべき一連の基準及び技術的規制）について、首相令により定めるものとする（第 14 条）。

(4) サイバー犯罪への対応強化

90 号法は、関連法令の改正により、サイバー犯罪への対応を強化している。刑法典[8]に関しては、例えば、情報システム及びデータ通信システムへの不正なアクセスについて規定した同法典第 615 条の 3 を改め、公務員等が、職権を濫用して、又はその職務等に含まれる義務に反して不正なアクセスを行った場合等の刑罰について、従来は 1～5 年の懲役であったところ、2～10 年の懲役とした（第 16 条）。さらに、当該アクセスが軍事上の利益、公の秩序、公の安全、健康、市民保護又は公の利益に係る情報システム又はデータ通信システムに関するものであれば、従来は 3～8 年の懲役により処罰していたところ、4～12 年の懲役により処罰することとした。また、上述した刑法典第 615 条の 3 等で規定された行為により、又は当該行為を行うと脅迫することにより、他人に何かを行わせ、又は行わせないようにして、自己又は他人のために不当な利益を得、他人に損害を与えた者に対して、6～12 年の懲役及び 5,000～1 万ユーロの罰金により処罰するという規定を新たに設けた（刑法典第 629 条の改正）。

また、刑事訴訟法典[9]に関しては、上述した刑法典第 615 条の 3 に規定された犯罪等であって、公の利益に係る情報システム等に関するものについて、通常は 18 か月である予備捜査[10]の最長期間を 2 年とする改正（刑事訴訟法典第 407 条の改正）等を行っている（第 17 条）。

---

7 情報財（beni informatici）とは、ソフトウェア、データベース等を指す。
8 R.D. 19 ottobre 1930, n. 1398, Approvazione del testo definitivo del Codice Penale.
9 D.P.R. 22 settembre 1988, n.447, Approvazione del codice di procedura penale.
10 予備捜査（indagini preliminari）とは、犯罪の通報に根拠があるか否かについて、検察官又は司法警察が行う捜査をいう。