【台湾】情報通信安全管理法の制定

海外立法情報課長　岡村　志嘉子

＊2018 年 5 月 11 日、台湾で、国内の情報通信の安全確保、情報通信の安全に対する国民意識の向上、国の情報通信安全環境の整備等を目的とする情報通信安全管理法が制定された。

1　背景と経緯

(1) 情報通信の安全に関する政策

インターネットが急速に社会に浸透する中で、台湾政府は今世紀に入り、情報通信の安全に関する各種施策を強化してきた。2001 年 1 月には、行政院の下に行政院副院長を長とする国家情報通信安全タスクフォースが設置された。同タスクフォースは、国家情報通信インフラ建設及び安全対策について 4 年毎の整備計画を策定し､国家レベルの統一的な施策を主導している。

近年、台湾においても、金融機関が国外からサイバー攻撃を受けるなど、情報通信の安全リスクが高まっている。2016 年 5 月に発足した蔡英文政権は、同年 8 月、同タスクフォースの事務部門であった情報通信安全弁公室の組織を強化拡充し、情報通信安全処を発足させた。情報通信安全処の設置目的は、デジタル経済時代において、情報通信の安全を国の安全の重要な構成要素と位置付け、十分な専門要員を配置することにより業務の専門性を向上させ、国として情報通信の安全に関する統一的な取組を強化することである。

2016 年 11 月には、「デジタル国家・イノベーション経済発展計画（2017～2025 年）」が閣議決定され、国内のデジタル経済の規模拡大、ブロードバンドによるインターネット利用を国民の基本的権利として保障すること等の目標が掲げられた。情報通信の安全確保は、同発展計画の実現に当たっての重要な鍵とみなされている。2017 年 11 月には、上述のタスクフォースが新たな 4 か年整備計画として「国家情報通信安全発展計画（2017～2020 年）」を策定した。その中では、基幹ネットワークの安全性向上、重要インフラの安全防護体制の強化、高度専門人材の養成等と並んで、法整備が早期に達成すべき重点項目の 1 つに挙げられている。

(2) 立法動向

情報通信の安全について、台湾の現行法においては、刑法のコンピューター使用妨害罪や個人情報保護法の規定が適用されるが、その適用範囲は限定的であった。そのため、公的機関だけでなく民間も含め、情報通信の安全確保について全般にわたって規定する法律を早期に制定することが課題となっており、情報通信安全処を中心として検討が進められてきた。

2017 年 4 月 27 日、情報通信の安全環境を官民が協力して国として一体的に構築することを目指す情報通信安全管理法案が閣議決定され、立法院に送られた。同法案は、審議の過程で、過度の私権制限や企業秘密の侵害等への懸念が多く出されたため、それらの規定を修正又は削除した上で、2018 年 5 月 11 日に可決された。施行規則等の制定において私権制限の妥当性について十分な検討を求める附帯決議も、同時に採択された。情報通信安全管理法[1]（全 5 章 23 か条）は、同年 6 月 6 日に公布された。施行日は、今後、行政院により定められる。

＊　本稿におけるインターネット情報の最終アクセス日は、2018 年 7 月 13 日である。

[1] 「資通安全管理法」『總統府公報』7367 號 <https://lis.ly.gov.tw/lgcgi/ttspdf2?7367:8-15>

2　情報通信安全管理法の構成と主な内容

(1) 構成

第 1 章：総則（第 1 条～第 9 条）、第 2 章：公務機関の情報通信安全管理（第 10 条～第 15 条）、第 3 章：特定非公務機関の情報通信安全管理（第 16 条～第 18 条）、第 4 章：罰則（第 19 条～第 21 条）、第 5 章：附則（第 22 条～第 23 条）。

(2) 立法目的と適用範囲

国の情報通信安全政策を積極的に推進し、国の情報通信安全環境の構築を加速し、国の安全を保障し、公共の利益を守ることを目的とする（第 1 条）。

この法律は、公務機関（法に従い公権力を行使する中央・地方機関又は公法人で、軍事機関と情報機関を除く。）と特定非公務機関（重要インフラの提供者、重要インフラ以外のインフラを提供する公営事業等）に適用される（第 3 条）。

(3) 重要インフラの定義と重要インフラ提供者の義務

重要インフラとは、その機能の停止又は低下が国の安全、公共の利益、国民生活又は経済活動に重大な影響を及ぼすおそれがあるものをいい、主務官庁が定期的に見直し、それを公告する（第 3 条）。また、重要インフラの提供者の指定は、関係官庁、民間団体、専門家等による検討を経て決定される（第 16 条）。重要インフラが具体的に何を指すのかについては、条文には明記されていないが、情報通信安全処は、エネルギー、水資源、通信、交通、銀行・金融、緊急救援・医療、中央・地方政府機関、ハイテクパークの 8 分野であると説明している[2]。

重要インフラの提供者は、情報通信安全維持計画を策定・実施し、当該計画の実施状況を主務官庁に届け出なければならない（第 16 条）。

(4) 政府の義務

情報通信の安全性向上のため、政府は、民間及び産業界との一体的な取組により、①情報通信の安全に係る専門人材の養成、②情報通信安全技術の開発、集積、応用、産学協力及び国際協力、③情報通信の安全に関連する産業の振興、④情報通信の安全に関連するハード・ソフト技術の規格化、認証体制等の整備を推進しなければならない（第 4 条）。

また、各主務官庁に対しては、国家情報通信安全情勢報告の定期的公表と立法院への報告（第 5 条）、公務機関及び特定非公務機関に対する情報通信安全責任の等級区分指定（第 7 条）、情報通信安全情報共有メカニズムの構築（第 8 条）等が義務付けられている。

(5) 情報通信の安全に関わる事件の通報義務と罰則

公務機関及び特定非公務機関は、情報通信の安全に関わる事件に対応するため、通報・緊急対応計画を策定しなければならない（第 14 条、第 18 条）。事件を知ったとき、公務機関の場合は上級機関又は監督機関に加えて主務官庁への通報が（第 14 条）、特定非公務機関の場合は主務官庁への通報が（第 18 条）それぞれ義務付けられている。

公務機関の職員がこの法律の規定に違反したときは、情状に応じ関係規定により処分される（第 19 条）。特定非公務機関は、情報通信安全維持計画等の策定・実施を怠り、期限までに改めなかったときは 10 万台湾ドル[3]以上 100 万台湾ドル以下の過料（第 20 条）、通報すべき事件を通報しなかったときは 30 万台湾ドル以上 500 万台湾ドル以下の過料(第 21 条)に処される。

---

[2] 行政院資通安全處「資通安全管理法與發展藍圖」2017.9.22. <https://s.itho.me/egov/2017/A-1320.pdf>

[3] 1 台湾ドルは約 3.7 円（平成 30 年 7 月分報告省令レート）。