シンガポール法律コラム

第２５回　シンガポールにおける最近のサイバー犯罪対策などについて

2025 年 12 月
One Asia Lawyers Group 代表
シンガポール法・日本法弁護士
伊奈　知芳

1. シンガポールのサイバー法制の全体像

皆さん、こんにちは。One Asia Lawyers Group のシンガポールメンバーファーム Focus Law Asia LLC です。シンガポールにおいては、政府が早くから「スマート・ネーション構想（Smart Nation）」を掲げ、行政・企業・市民生活のデジタル化を強力に推進してきていますが、一方で、オンライン詐欺、ランサムウェア被害、AI を活用したディープフェイク詐欺など、多様なサイバー犯罪やオンラインでの有害行為も年々増加しています。こうした背景も踏まえ、2024 年 9 月には「Singapore Cyber Landscape 2024/2025」も発表され[1]、各種法制度の強化や官民連携・国際協力などによる対策を推進していく方針が示されています。

そこで、以下では、主要法令の概要と最新動向、企業実務における留意点を整理します。

2. Cybersecurity Act 2018（2024 年改正）

2.1 基本的枠組み

Cybersecurity Act は、2018 年に施行され、国家レベルの重要インフラ（Critical Information Infrastructure, CII）を保護することを目的に制定されました。管轄機関は Cyber Security Agency of Singapore（CSA）であり、電力、金融、通信、運輸、医療、政府情報システムなど、社会機能を支える事業者に対し、一定のサイバー防御義務を課しています。

CII 事業者は CSA に指定されると、システムの保護、リスク管理体制の維持、定期監査、インシデント報告などの義務を負います。また、重大なサイバーインシデント発生時には CSA 長官が調査・介入する権限を持っています。

2.2 2024 年改正の概要

同法においては 2024 年に改正が行われ、これにより、デジタル化の進展やサプライチェーンの多層化に対応するための制度が大幅に拡充されました。これは 2025 年 10 月 31 日から施行されますが、主な改正点は次の通りです[2]。

[1] https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2024-2025/
[2] https://www.csa.gov.sg/legislation/cybersecurity-act/

(1) 適用対象の拡大

国家レベルのサイバー上の脅威を一時的に「重大な懸念」として指定し、政府が迅速に介入・対応できるようにする制度である「System of Temporary Cybersecurity Concern（STCCs）」や国の経済や社会の中核を支える基幹的なデジタルインフラ（例：クラウドサービス、データセンター、国の通信ネットワークなど）を政府が指定し、特別なサイバーセキュリティ要件を課すことができるとする「Foundational Digital Infrastructure（FDI）」など、新たなカテゴリが導入され、クラウド基盤やデータセンター、通信網の一部も同法による規制対象に含まれるようになりました。

(2) Entities of Special Cybersecurity Interest（ESCI）事業者の新設

CII ほど国家的影響は大きくないものの、一定規模以上のデジタルサービスを提供する民間企業を「ESCI 事業者」として登録し、インシデント報告やリスク管理の一定義務を課しています。

2.3 サプライチェーン全体への監視拡大

下請けやクラウドプロバイダなどを経由したリスクにも対応するため、委託先・外部ベンダーへのリスク管理責任が明確化されました。

2.4 CSA の権限強化と柔軟運用

上記の STCCs、FDI、ESCI 等は、CSA 長官が状況に応じて、通知等により各種事業者を指定できる枠組みであり、これにより当局が突発的な状況にも従前以上に機動的に関与できるようになることが期待されます。

この改正により、SaaS 事業者やクラウドベンダーも新たに規制対象となる可能性があるため、企業は、自社が上記カテゴリのいずれかに該当しないかどうかを確認する必要があります。

3. Computer Misuse Act 1993（CMA）

CMA は 1993 年に制定され、サイバー犯罪取締りの基本法として位置付けられています。同法はもともと、不正アクセスやデータ改ざんを禁止する刑事法でしたが、その後の改正で攻撃ツールや不正認証情報の販売・仲介行為、ボットネット運用など、周辺的な関与行為も犯罪に含まれるようになりました。

特に 2021 年以降の改正では、以下の行為が新たに明示的に禁止されています。

- 他人の認証情報（ID・パスワード）を不正に取得・保有・販売する行為
- マルウェア、ハッキングツール、フィッシングキットの配布・提供
- 攻撃代行やアクセス権限の不正譲渡

さらに、国外で行われた行為であっても、シンガポール国内に被害を及ぼす場合には CMA が適用されることとなっています。

4. Online Criminal Harms Act 2023（OCHA）

OCHA は 2023 年に施行され、オンライン詐欺や有害情報拡散への対策を目的としています。この法律では、プラットフォーム事業者や通信サービス提供者に対して、当局の指示に基づく迅速な削除・遮断・アクセス制御を義務付けています。

同法に基づき、Infocomm Media Development Authority（IMDA）や警察（Singapore Police Force、SPF）は、SNS やマーケットプレイス、メッセージングアプリなどに対し、有害投稿・詐欺広告・詐欺サイトへのリンク削除を命じることができます。また、検索結果からの除外命令や、支払処理ルートの遮断も可能です。

OCHA は刑事法（CMA）と行政法（Cybersecurity Act）の中間に位置付けられ、刑事訴追の前段階で被害の拡大を迅速に抑えるための柔軟な制度であると言えます。

5. Personal Data Protection Act 2012（PDPA）

PDPA は、ご案内の通り、個人情報の保護と適正な利用を定める法律であり、サイバーセキュリティ法制と密接に関連しています。第 24 条では、事業者に対し合理的なセキュリティ管理措置を講じる義務が明記されています。これは、単なる情報管理だけでなく、サイバー攻撃防御の技術的・組織的対策も含まれます。

2021 年改正により導入されたデータ侵害通知制度では、個人情報の漏えいが一定基準を超えた場合、72 時間以内に、Personal Data Protection Commission（PDPC）へ報告し、影響を受ける個人にも通知する必要があります。違反すると、企業売上高の 10%または 100 万シンガポールドルのいずれか高い方の課徴金が課される場合があります。

また、AI や自動化ツールの利用が進む中、データの「最小化」「仮名化・匿名化」「説明責任」など、Model AI Governance Framework と整合した管理が求められます（詳細は前回コラムをご参照ください。）。

6. 各企業において実務上求められる対策

以上のような各法令の状況を踏まえ、各企業としては、サイバー犯罪対策として以下のような対応をとることが考えられます。

(1) サイバーインシデント発生時の通報ラインを明確にする（CSA／PDPC／警察、など）
(2) サプライチェーン全体を含むリスクアセスメントを定期的に実施する
(3) ログ・監査証跡の完全性を確保し、フォレンジック対応を想定した体制を整える
(4) 社内訓練や疑似攻撃演習を通じて、実効的訓練文化を醸成する
(5) 有事の広報・対外説明をテンプレート化する

まとめ

現代の高度なデジタル化社会においては、データ漏洩を含む各種サイバーインシデントは、その発生のリスクを完全にはゼロにできない状況にあるといえ、サイバー犯罪に対する対応も、政府当局との間での「いたちごっこ」となる側面も否定できません。しかしながら、各企業におかれても、自社における被害の発生を可能な限り防ぎ、かつ、発生した被害を最小限に抑えるために、これらの規制の枠組みを把握し、各社の具体的な状況に合った対策を講じていく必要があると思われます。

※本稿は、シンガポールの週刊 SingaLife（シンガライフ）において掲載中の「シンガポール法律コラム」のために著者が執筆した記事を、ニューズレターの形式にまとめたものとなります。

＜著　者＞

伊奈　知芳

One Asia Lawyers Singapore Office

弁護士（日本）

弁護士登録後、日本における対中国クロスボーダー投資案件を主要業務とするブティック型法律事務所に約 8 年間勤務。同所入所直後より主に中国案件に関与し、2010 年より同所上海事務所代表として常駐。2013 年より同所主席代表弁護士として勤務する。
2015 年同所を退職後、シンガポール国立大学法学部大学院（LL.M.）へ留学。2016 年、同大学院を卒業（Master's Degree を取得）後、One Asia Lawyers の設立に参画。以後一貫してシンガポールをベースとし、東南アジア及び中国を中心とするクロスボーダーM&A 案件のほか、労務、 知財、コンプライアンスその他一般企業法務案件、およびシンガポール関わる国際離婚、相続案 件等に幅広く携わっている。特に、シンガポールを中心とした個人情報保護法制に関する案件については、講演・執筆活動も多数行っている。International Association of Privacy Professionals (IAPP) 会員、Certified Information Privacy Professional/Europe (CIPP/E)。

tomoyoshi.ina@oneasia.legal