実務最新動向（ニューズメール 2024 年 2 月号）
シンガポール・サイバーセキュリティ法の改正案について

岩田合同法律事務所
弁護士　松田　章良
弁護士　山田　康平
弁護士　松田　大樹

1.　はじめに

シンガポールのサイバーセキュリティ庁（Cyber Security Agency of Singapore）（以下「CSA」といいます。）は、2023 年 12 月 15 日、サイバーセキュリティ法（CYBERSECURITY ACT 2018 No. 9 of 2018）の改正案（Proposed Cybersecurity (Amendment) Bill）（以下「改正案」といいます。）を公表し、併せてパブリック・コンサルテーションを開始しました[1]。パブリック・コンサルテーションは、2024 年 1 月 15 日に終了しており、近日中にその結果を踏まえた改正法が施行されるものとみられます。

近年、サイバー空間におけるサイバー攻撃の脅威がますます高まっていることを受けて、ASEAN を含むアジア各国においても、サイバーセキュリティに関連する法規制の整備・拡充が急速に進められています。最近では、中国やベトナムにおいて適用範囲が広範なサイバーセキュリティ法が制定されており、また、我が国においても、2022 年 5 月に経済安全保障推進法が成立し、電力や航空、金融など基幹インフラ設備へのサイバー攻撃を防止するための「基幹インフラ制度」が設けられたところです。

サイバーセキュリティを巡る状況が刻々と変化する中で、事業者が適切なサイバーセキュリティ対策を講じていくためには、各国のサイバーセキュリティに関する法規制を把握し、最新動向を理解しておくことが肝要といえます。そこで、本ニューズメールでは、シンガポールにおける近時の動向として、シンガポールのサイバーセキュリティ法の内容を概観した上で、今般公表された改正案のポイントをご紹介いたします。

[1] https://www.csa.gov.sg/News-Events/Press-Releases/2023/public-consultation-on-the-proposed-cybersecurity-(amendment)-bill

2. シンガポール・サイバーセキュリティ法の概要

シンガポールのサイバーセキュリティ法は、2018 年 3 月 2 日に成立しました。同法は、シンガポールにおける国家サイバーセキュリティの監督及び維持のための法的枠組みを設けるものであり、主として以下の 4 つの事項について規定しています[2]。

① サイバー攻撃に対する重要情報インフラ（Critical Information Infrastructure (CII)）の保護強化

重要情報インフラとは、重要サービス（essential service）の継続的提供のために必要な、その全部又は一部がシンガポールに所在するコンピュータ又はコンピュータシステム（以下総称して「システム」といいます。）であって、当該システムの損失や危殆化がシンガポールにおける重要サービスの可用性を低下させるものをいいます[3]。重要サービスは、エネルギー、水、銀行・金融、ヘルスケア、運輸（陸上、海上、航空）、情報通信、メディア、セキュリティ・緊急サービス、政府の各カテゴリーに分けて指定されています。サイバーセキュリティ長官（Commissioner of Cybersecurity）は、特定のシステムの所有者に対して通知することにより、当該システムを CII として指定することができ、当該システムの所有者は、当該 CII を保護するための各種の義務を負います。

② サイバーセキュリティに関する脅威・インシデントの防止・対処のための CSA の権限

サイバーセキュリティ長官に対し、サイバーセキュリティに関する脅威やインシデントを調査し、再発を防止するための権限を付与しています。

③ サイバーセキュリティに関する情報共有

政府やシステムの所有者が脆弱性を特定し、サイバー事件をより効果的に防止する観点から、CSA が事業者に対して情報を要請し、当該情報を保護・共有するための枠組みを設けています。

④ サイバーセキュリティサービス事業者に対するライセンス

CSA は、現在、ペネトレーションテストサービス又はセキュリティーオペレーションセンターによるモニタリングサービスの両方又は一方を提供するサイバーセキュリティサービス事業者に対してのみ、ライセンスを付与することとしています。

---

[2] CSA のウェブサイト（https://www.csa.gov.sg/legislation/cybersecurity-act）参照。

[3] https://www.csa.gov.sg/faq/cybersecurity-act

3. 改正案の概要

改正案は、クラウド・コンピューティングなどの新たな技術ツールやビジネスモデルの採用が増えていること等に照らし、シンガポールのサイバーセキュリティ法令が引き続きサイバースペースにおける新たな課題に対処できるようにすること等を目的とするものです。主要な改正点としては、以下の 3 点が挙げられます。

① 適用場面の拡大

サイバーセキュリティ法の適用は、従来、原則として、重要サービスの提供事業者が所有する CII に限られていましたが、今般の改正案は、その適用場面を拡大し、重要サービスの継続的な提供のために使用されている CII については、重要サービスの提供事業者が所有又は管理していない CII（non-provider-owned CII）に対しても、適用されることとされています。この結果、non-provider-owned CII を使用している重要サービスの提供事業者は、本改正により、大要、以下のような義務を負うこととなります。

・non-provider-owned CII に関する情報の提供

・サイバーセキュリティ長官の定める実施規範等の遵守

・non-provider-owned CII の実質的又は法的所有者の変更に係る通知

・non-provider-owned CII に関するインシデントの通知

・non-provider-owned CII がサイバーセキュリティ法等を遵守していることについての定期的な監査

・non-provider-owned CII に関する定期的なサイバーセキュリティリスクの評価

・サイバーセキュリティ訓練への参加

加えて、重要サービスの提供事業者は、CII の所有者やコンピューティングベンダーから法的拘束力のあるコミットメントを得ることも要求されることとなります。

その他、本改正により、シンガポールに所在する重要サービスのプロバイダーが、CII をオフショア化することによって、本法に基づく義務を回避できないようにするための改正もなされています。その結果、シンガポール国外に所在するシステムも、同法における（重要サービスの提供事業者が所有する）CII として指定される可能性があります。

② サイバーセキュリティ長官による監督対象範囲の拡大

サイバーセキュリティ長官の監督範囲が、CII の所有者のみならず、(i)主要な基盤デジタル・インフラ・サービス事業者（Major FDI (foundational digital infrastructure) service providers）、(ii)サイバーセキュリティに特別の利害を有する事業者（entity of special cybersecurity interest）、(iii)サイバーセキュリティ上

の一時的な懸念が生じているシステム（system of temporary cybersecurity concern）の所有者に拡大されており、当該(i)～(iii)に該当する者は、サイバーセキュリティ長官によって指定されます。

(i)のFDIサービスとしては、例えば、クラウド・コンピューティング・サービス事業者や、データセンター施設サービス事業者等が想定されており、これらの事業者がシンガポールに対し又はシンガポールから FDI サービスを提供しており、当該サービスの損失又は障害が当該サービスを利用している多数の企業又は組織に混乱を来たす場合には、当該事業者は主要な基盤的デジタル・インフラ・サービス事業者として指定される可能性があります。

③ サイバーセキュリティ長官による規制権限の強化

サイバーセキュリティ長官への報告対象となるインシデントの範囲が拡大され、また、サイバーセキュリティ長官に立入検査の実施を許可する権限が付与される等しています。

4. まとめ

上述のとおり、サイバーセキュリティを巡る状況は日々刻々と変化しており、それに伴って各国のサイバーセキュリティに関する規制も多様化・複雑化しているところです。自社グループに、シンガポールのサイバーセキュリティ法制に基づく規制が直接的に適用される事例は必ずしも多くないと思われますが、自社の取引先や、委託関係がある場合等に、同法制に基づく規制が関連する場合が生じ得るため、留意が必要です。

以　上

【執筆者】

弁護士　松田章良　TEL: +81 3 3214 6282　　E-MAIL: amatsuda@iwatagodo.com

岩田合同法律事務所パートナー弁護士（2008 年弁護士登録）。2006 年東京大学法学部卒業、2008 年 9 月長島・大野・常松法律事務所入所。2015 年コロンビア・ロースクール（LL.M.）卒業（Harlan Fiske Stone 賞）、同年 NY 州司法試験合格。2015 年 9 月岩田合同法律事務所入所。同年 11 月より 2021 年 8 月までシンガポールの DREW & NAPIER 法律事務所及び東京にて執務。2019 年 NY 州弁護士登録。

クロスボーダーの企業取引、紛争及び調査案件を主に取り扱っているほか、東南アジア地域を中心として、日本企業の海外進出・展開に係る案件を多く担当している。また、近時は日本・シンガポール・EUにおけるデータプロテクション（個人情報保護）に係る案件を多数取り扱うほか、AI やフィンテック分野を含む先進的なデータの利活用に係る案件を多く取り扱っている。

弁護士　山田康平　TEL: +81 3 3214 6208　　E-MAIL: kyamada@iwatagodo.com （東京）

TEL: +65 6531 4112　E-MAIL: kohei.yamada@drewnapier.com （シンガポール）

岩田合同法律事務所弁護士（2014 年弁護士登録）。2011 年東京大学法学部卒業、2013 年東京大学法科大学院修了、2014 年 12 月岩田合同法律事務所入所。2022 年コーネル・ロースクール（LL.M.）卒業、同年 NY 州司法試験合格。同年 9 月よりシンガポールの DREW & NAPIER 法律事務所にて執務。シンガポールの DREW & NAPIER 法律事務所は、Drew Network Asia を形成し、東南アジア 9 か国にわたり、リーガルアドバイスを提供している。

M&A 取引、会社法・金融商品取引法を始めとするコーポレート分野に関するアドバイスを主に取り扱っているほか、クロスボーダーの企業取引、紛争処理（訴訟・仲裁・調停）を多く担当している。現在は、シンガポールの DREW & NAPIER 法律事務所にても勤務しており、東南アジア地域への日本企業の海外進出・展開のサポート等を行っている。

弁護士　松田大樹　TEL: +81 3 3214 3215　　E-MAIL: taiki.matsuda@iwatagodo.com

岩田合同法律事務所弁護士（2020 年弁護士登録）。2017 年一橋大学法学部卒業、2019 年一橋大学法科大学院修了、2020 年 12 月岩田合同法律事務所入所。

会社法・金融商品取引法を中心として、コーポレート分野に関する法的助言を幅広く取り扱っているほか、M&A 取引や独占禁止法分野に関する案件を多く担当している。また、クロスボーダーの企業取引案件、日本企業の海外進出・展開に係る競争法案件等の取扱実績を有する。

岩田合同法律事務所

1902 年（明治 35 年）、故・岩田宙造弁護士により創立。一貫して企業法務の分野を歩んでいる、我が国において最も歴史のある法律事務所の一つです。創立当初より、政府系銀行、都市銀行、地方銀行、信託銀行、電力会社、大規模小売業、重電機メーカー、素材メーカー、印刷会社、製紙会社、不動産会社、建設会社、食品会社等、我が国を代表する企業等の法律顧問として、多数の企業法務案件に関与しております。日本人弁護士約 100 名が所属するほか、日本語対応も可能な中国法弁護士、フランス法弁護士、米国弁護士経験を有する米国人コンサルタント等も所属しております。

〒100-6315　東京都千代田区丸の内 2-4-1 丸ビル 15 階　www.iwatagodo.com/
お問い合わせ先: E-mail: newsmail@iwatagodo.com　Tel: +81-3-3214-6205