【オーストラリア】2018年重要インフラ安全保障法の改正

海外立法情報課長　内海　和美

＊2022年4月、豪州のサイバーセキュリティ対策を強化するため、2018年重要インフラ安全保障法を改正し、重要インフラの所有者等に新たな義務を課す法律が制定された。

1　背景及び改正経緯

豪州では、2020-21年度のサイバー犯罪の発生件数は67,500件以上（前年度比13%増）、自己申告による損失額は330億豪ドル[1]以上であり、報告されたサイバーセキュリティ・インシデント（以下「インシデント」）の4分の1が豪州の重要インフラ又は重要サービスに関連しているとされる[2]。

増加するサイバーセキュリティへの脅威に対応するため、2018年4月11日、2018年重要インフラ安全保障法[3]（以下「2018年法」）が制定され、同年7月11日施行された。重要インフラの大部分は、民間企業や州・準州政府によって所有・運営されているが、連邦政府がこれらのサイバーセキュリティに関与することを目的とする。2021年12月2日、2018年法を改正する法律（2021年保安法改正（重要インフラ）法[4]。以下「2021年法」）が制定された（翌3日施行）。2021年法は、2020年12月10日に下院へ提出された当初案[5]には、①重要インフラ資産の対象拡大、②リスク管理プログラムの導入、③政府へのインシデント報告義務、④国家的重要システムに指定された重要インフラ資産を有する事業体等へのサイバーセキュリティ強化義務、⑤深刻なインシデントに対応するため、政府へ新たな権限（情報収集、行動指示等）の付与等が盛り込まれていた（下線は次節参照）。しかし、豪州法制審議会（Law Council of Australia）が、法案に対し「大臣や次官への委任立法の数、範囲、重大性から見て、本法案は極めて異例」[6]と懸念を示したため、法案を分割し、サイバーセキュリティへの脅威への対応の観点から緊急性の高い①、③及び⑤を先に成立させ（2021年法）、残りは後日の成立を期すこととなった。

2022年4月1日、2018年法を改正し、主に②及び④を新たに規定する法律（2022年保安法改正（重要インフラ保護）改正法[7]。以下「2022年法」）が制定された（翌2日施行）。2022年法は、2018年法に「第2A章：重要インフラリスク管理プログラム」、「第2AA章：重要イン

＊　本稿におけるインターネット情報の最終アクセス日は、2022年9月7日である。

1 1豪ドルは、約94円（令和4年9月分報告省令レート）。

2 Australian Cyber Security Centre, “ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021,” p.10. <https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>

3 Security of Critical Infrastructure Act 2018, No.29, 2018. <https://www.legislation.gov.au/Details/C2022C00160>

4 Security Legislation Amendment (Critical Infrastructure) Act 2021, No.124, 2021. <https://www.legislation.gov.au/Details/C2021A00124>

5 Security Legislation Amendment (Critical Infrastructure) Bill 2020. <https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6657_first-reps/toc_pdf/20182b01.pdf;fileType=application%2Fpdf>

6 Parliamentary Joint Committee on Intelligence and Security, “Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018,” 2021.9, p.29. <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024715/toc_pdf/AdvisoryreportontheSecurityLegislationAmendment(CriticalInfrastructure)Bill2020andStatutoryReviewoftheSecurityofCriticalInfrastructureAct2018.pdf;fileType=application%2Fpdf>

7 Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, No.33, 2022. <https://www.legislation.gov.au/Details/C2022A00033>

フラリスク管理プログラムの対象外である資産に関連する報告義務」、「第 2C 章 : サイバーセキュリティ強化義務」、「第 6A 章 : 内務大臣による国家的重要システム（system of national significance: SoNS）の指定」を追加し、併せて付随する改正を加えた。

2　2022 年法の概要

（1）重要インフラリスク管理プログラム

一つ以上の重要インフラ資産[8]（critical infrastructure asset. 以下「重要資産」）を所有・運営する事業体・個人（以下「責任事業体等」）は、①重要資産に影響を及ぼす可能性のあるハザードを特定し、②当該ハザードが発生するリスクを最小化又は排除し、③当該ハザードが重要資産に及ぼす影響を軽減する目的で、リスク管理プログラムを書面により策定・維持し、さらに当該プログラムの遵守・定期的見直し・更新の義務を負う（第 30AC 条～第 30AH 条）。これらの義務に反した場合、200 ペナルティユニット[9]（penalty unit: PU）以下の民事罰が科される。

（2）サイバーセキュリティ強化義務

内務大臣は、書面により、重要資産のうち国家的重要性を有すると認めた特定の資産を、SoNS として非公開で指定（privately declare）することができる。「国家的重要性」の判断に際しては、豪州の社会的・経済的安定性、防衛、国家安全保障に留意しなければならない。同大臣は、指定後 30 日以内に、当該資産の責任事業体等に指定の事実を通知しなければならない（第 52B 条）。SoNS の責任事業体等へは、サイバーセキュリティ強化義務が課される。主な内容は、次のとおりである。

（ⅰ）インシデント対応計画の策定（第 2C 章第 2 節）

SoNS の責任事業体等は、SoNS に影響を与える可能性のあるインシデントへの対応計画を策定・維持し、さらに当該計画の遵守・定期的見直し・更新の義務を負う。これらの義務に反した場合、200PU 以下の民事罰が科される。

（ⅱ）サイバーセキュリティ訓練の実施（第 2C 章第 3 節）

内務次官は、書面による通知により、SoNS 及び 1 種類以上のインシデントに関してサイバーセキュリティ訓練（以下「訓練」）を実施するよう要求することができる。訓練は、インシデントへの適切な対応能力、準備態勢、SoNS への影響を軽減する能力のテストを目的とし、インシデントの全種類に対応する訓練と、1 種類以上に対応する訓練の 2 種類がある。責任事業体等は、訓練後 30 日以内に評価報告書を作成し、写しを同次官に提出しなければならない。

（ⅲ）脆弱（ぜいじゃく）性評価の実施（第 2C 章第 4 節）

全種類又は 1 種類以上のインシデントに対する SoNS の脆弱性を評価するため、内務次官は、責任事業体等に脆弱性評価の実施を要求することができる。要求に従わない場合、200PU 以下の民事罰が科される。責任事業体等は、評価後 30 日以内に報告書を作成し、写しを同次官に提出しなければならない。

(i)～(iii)は、SoNS の責任事業体等に全てが自動的に適用されるわけではなく[10]、義務遵守に掛かるコスト、合理性、均衡性（手段と目的の均衡）が考慮される（第 30CB 条第 4 項ほか）。

---

[8] 電気通信、放送、ドメインネームシステム、銀行、金融市場インフラ、電力、ガス、液体燃料、港湾、航空、公共交通、防衛産業等の重要資産を指す（2018 年法第 9 条）。資産とは、システム、ネットワーク、設備、コンピュータ、コンピュータ機器・プログラム・データ、施設等と定義される（同法第 5 条）。

[9] 1PU は、222 豪ドル（2020 年 7 月 1 日以降）。なお、200PU は個人の場合。法人は個人の 5 倍の額となる。

[10] Cyber and Infrastructure Security Centre, “The Enhanced Cyber Security Obligations Framework,” 2022.5, p.1.