PARLIAMENT OF AUSTRALIA

サイバーセキュリティ法制パッケージ 2024 に関するアドバイザリー報告書

情報・安全保障に関する議会合同委員会

2024 年 11 月

キャンベラ

© 2024 オーストラリア連邦

ISBN 978-1-76092-720-2（印刷版）
ISBN978-1-76092-720-2（HTML 版）

本報告書に含まれるすべての資料は、クリエイティブ・コモンズ 表示 - 非営利 - 改変禁止 4.0 オーストラリア ライセンスの下でプロバイダ提供されている。本資料は、以下の条件で共有、複製、再配布することができる：

- 非営利目的である
- 前頁に記載された委員会が認可される。
- 委員会は、その資料の使用を保証する代表者ではない。
- いかなる変更も明確に識別される。
- ライセンスに準拠した使用を制限するために、追加の法的または技術的な制限が適用されることはない。

素材がリミックス、変形、または構築された場合、変更された素材を配布することはできない。

このライセンスの詳細は、クリエイティブ・コモンズのウェブサイト https://creativecommons.org/licenses/by-nc-nd/4.0/。

内容

略語.....vi

メンバー ix

参考資料 x

勧告リスト.....xi

1.序文.....1

調査の実施.....1

報告書の構成 1

調査の背景.....2

サイバーセキュリティ法制パッケージ 2

2.サイバーセキュリティ法案 2024 4

サイバーセキュリティ法案の背景と目的 4

パート 1：予備 4

治外法権.....5

サイバー・セキュリティ・インシデント.....5

サイバーセキュリティインシデントが発生した場合に許可されるサイバーセキュリティ目的.....6

パート 2：スマートデバイスのセキュリティ標準 7

パート 3：ランサムウェアの報告義務 11

パート 4：重大なセキュリティ・インシデントの調整 16

パート 5：サイバーインシデント審査会 19

パート 6：規制権限 21

パート 7：その他.....21

3.情報サービスおよびその他の法改正（サイバー・セキュリティ）法案 2024.....22

スケジュール 1：特定のサイバー・セキュリティ情報の限定的利用 23

スケジュール 2：情報公開法の改正 27

4.重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 2024 28

スケジュール 1：重要インフラ資産」の定義に「データ保管システム」を含める。 29
別表 2：社会保険労務士法第 3 条 A の改正 31
別表 3：情報の利用および開示 32
日程 4：重要インフラ・リスクマネジメント・プログラムの変更を要請する新たな方向性 。.....34
スケジュール 5：重要な電気通信資産のセキュリティ規制 36
スケジュール 6：国家的に重要なシステムの宣言の通知 38

5.委員会への証拠提出.....40

立法パッケージに関する一般的見解 40

照会期間 41
これまでの協議プロセス.....41
今後の見直しの必要性 43

特定の条項に関する見解 44

標準セキュリティ基準 44
ランサムウェア報告義務.....49
サイバーインシデント審査会.....52
限定使用規定.....56
SOCI 法改正.....61

重要なデータ・ストレージ・システム 61
オールハザード」インシデントへの対応：結果管理の権限.....63
SOCI 法パート 4 情報共有規定.....67
重要インフラのリスクマネジメント・プログラムに対する指示権限 69
電気通信分野のセキュリティ規制 71

大臣による追加修正案.....72

6.委員会のコメントと勧告.....74

包括的なコメント 74
審査プロセス 75
スマートデバイスのセキュリティ標準.....76
ランサムウェア報告.....77

サイバーインシデント審査会 80
限定使用規定 81
SOCI 法改正 82
法定審査 83

委員会連合メンバーの追加コメント 87
A.提出書類リスト 91
B.公聴会の証人リスト 94

2024 年 10 月 31 日（木 94
2024 年 11 月 1 日（金 95

報告書

0

附属書

委員会連合メンバーの追加コメント.....95

附属書 A.List of submissions.....101

附属書 B.List of witnesses at public hearings.....105

略語

ACCC	オーストラリア競争・消費者委員会
ACCAN	オーストラリア・コミュニケーション消費者行動ネットワーク
ACSC	オーストラリア・サイバーセキュリティセンター
AICD	オーストラリア会社取締役協会
APRA	オーストラリア健全性規制庁
ASD	オーストラリア通信総局
アスファー	オーストラリア退職年金基金協会
ASIO	オーストラリア安全保障情報機構
ASIO 法	*1979* 年オーストラリア治安情報機関法
オーダ	.au ドメイン管理
BCA	オーストラリア・ビジネス評議会
BSA	BSA｜ソフトウェア・アライアンス
EM	覚書
ERP 請求書	重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 2024
CIRB	サイバーインシデント審査会
CIRMP	重要インフラのリスクマネジメント・プログラム
CISA	サイバーセキュリティ・インフラセキュリティ庁

コスボア	オーストラリア中小企業団体協議会
刑法	*1995* 年刑法別表第 1
CTIS	サイバー脅威インテリジェンスの共有
サイバーセキュリティ法案	サイバーセキュリティ法案 2024
情報公開法	*1982* 年情報公開法
IIER-A	統合経済研究所-オーストラリア
IoT	モノのインターネット
ISA 法案	インテリジェンス・サービスおよびその他の法改正（サイバー法
IS 法	2001 年安全保障情報サービス法（ISS 法）第 2024 号法案
法制審議会	オーストラリア法評議会
LPP	法律専門家の特権
NCSC	国家サイバー・セキュリティ・コーディネーター
プライバシー法	*1988* 年プライバシー法
PSPF	防御セキュリティポリシー・フレームワーク
PSTI 法	*2022* 年製品安全・電気通信インフラ法（英国）
SOCI 法	*2018* 年重要インフラ安全法
SoNS	国家的に重要なシステム
SLACI ビル	2020 年安全保障法制改正案（重要インフラ法案

SLACI 法	*2021* 年安全保障法制改正（重要インフラ）法
SLACIP 法	2022 年安全保障法制改正（重要インフラ保護）法
電気通信法	*1997* 年電気通信法
TIA 法	1979 年電気通信（傍受およびアクセス）法
TSSR	電気通信セクターの安全保障改革

メンバー

椅子

ラフ・チッコーネ上院議員	ALP, VIC

副議長

アンドリュー・ウォレス議員	フィッシャー, クイーンズランド州

メンバー

サイモン・バーミンガム上院議員	LP、SA
シャロン・クレイドン議員	ニューサウスウェールズ州ニューキャッスル
ルーク・ゴズリング議員	ソロモン、NT
アンドリュー・ヘイスティ議員	カニング（ワシントン州
ゾーイ・マッケンジー議員	フリンダース, VIC
ブレンダン・オコナー議員	ゴートン, VIC
ジェームズ・パターソン上院議員	LP, VIC
マリエル・スミス上院議員	ALP、SA
メリル・スワンソン議員	ニュー・サウス・ウェールズ州パターソン
ジェス・ウォルシュ上院議員	ALP, VIC

参考資料

トニー・バーク内務大臣兼サイバーセキュリティ担当大臣は、2024 年 10 月 9 日、サイバーセキュリティ法制パッケージを同委員会に付託し、調査・報告するよう、同委員会に書簡を送った。

勧告リスト

勧告 1

6.11 委員会は、本報告書の勧告を実施することを条件として、サイバーセキュリティ法案 2024、情報サービス等法改正（サイバーセキュリティ）法案 2024、重要インフラ等安全保障法改正（対応強化・予防）法案 2024 を国会で可決することを勧告する。

勧告 2

6.27 当委員会は、オーストラリア政府に対し、サイバーセキュリティ法案 2024 の報告義務の対象となるさまざまな企業にとって、ランサムウェアの報告メカニズムが可能な限り使いやすく、アクセスしやすいものとなるよう確保すること、およびオーストラリア政府が引き続き、すべての企業に対するサイバーセキュリティインシデント報告要件の重複を最小限に抑えるための作業を優先することを勧告する。

勧告 3

6.30 当委員会は、オーストラリア政府に対し、ランサムウェアの報告義務について企業を教育し、 法律の解釈に関する明確なガイダンスを提供するために、内務省とオーストラリア信号局 に十分なリソースを確保するよう勧告する。

勧告 4

6.32 当委員会は、提案されているランサムウェア報告義務が、ランサムウェアインシデントが報告事業体のオーストラリ ア国内での業務に関連する範囲にのみ適用されるよう、サイバーセキュリティ法案 2024 を修正することを勧告する。

勧告 5

6.39 委員会は、サイバーセキュリティ法案 2024 の説明文書を修正し、サイバーインシデント審査委員会の常任委員は公務員であるとの記述を削除することを勧告する。

勧告 6

6.42 委員会は、サイバーセキュリティ法案 2024 を改正し、見直しの職務権限を承認する前に、大臣がサイバーインシデント審査委員会に諮問することを義務付けることを勧告する。

勧告 7

6.48 委員会は、「限定的使用」条項によって与えられる防御を、サイバーセキュリティ法案 2024、情報サービスおよびその他の法改正（サイバーセキュリティ）法案 2024、および関連する説明文書の中でより明確に表現し、内務省がガイダンスを作成することで、産業界に十分理解されるようにすることを勧告する。

勧告 8

6.51 委員会は、サイバーセキュリティ法案 2024 および情報サービスおよびその他の法改正（サイバーセキュリティ）法案 2024 を改正し、以下をより明確にすることを勧告する：

- **ランサムウェア報告義務に基づく情報開示は、その後の法律専門家特権の放棄には当たらない。**
- **本規定は、報告事業体が訴訟手続きに関して有するいかなる権利、特権、免責にも制限または影響を与えない。**

勧告 9

6.55 委員会は、重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 2024 の実施を支援するための行政ガイダンス資料において、内務省は、重要インフラの安全保障法 2018 に導入された重要定義の意図する解釈と適用に関して、明確なガイダンスと事例を提供するよう勧告する。

勧告 10

6.60 委員会は、サイバーセキュリティ法案 2024 を改正し、委員会が（決議すれば）2027 年 12 月 1 日以降、実務上可能な限り速やかに、サイバーセキュリティ法 2024 の運用、有効性、影響の見直しを開始することができると規定することを勧告する。

勧告 11

6.69 委員会は、重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）第 60A 条で義務付けられている同法の運用に関する独立レビューを、2025 年 11 月 1 日までに開始するよう大臣に勧告する。

勧告 12

6.70 委員会は、重要インフラ安全保障法 2018（SOCI 法）の既存の第 60B 条を改正し、情報・安全保障に関する国会合同委員会が（その決議がなされれば）、同委員会が 2026 年 12 月 2 日までに見直

しを開始する限り、SOCI 法の運用、有効性、影響を見直すことができると規定することを勧告する。

勧告 13

6.73 委員会は、重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）を改正し、第 60AAA 条における以下の要件を廃止することを勧告する。

内務省が委員会に 6 ヶ月ごとの協議報告書を提出する。

1.序文

1.1　2024 年 10 月 9 日、トニー・バーク内務大臣兼サイバーセキュリティ担当大臣は、サイバーセキュリティ法制パッケージを委員会に付託し、調査・報告するよう書簡で要請した。

1.2　サイバーセキュリティ法制パッケージには、サイバーセキュリティ法案（2024 年）、情報サービスおよびその他の法改正（サイバーセキュリティ）法案（2024 年）、重要インフラ安全保障およびその他の法改正（対 応および予防の強化）法案（2024 年）が含まれる。

1.3　大臣は、2024 年春の会期中にタイムリーに改革案を可決できるよう、遅くとも 2024 年 11 月 18 日までに委員会の報告書を完成させるよう要請した。

調査の実施

1.4　委員会は 2024 年 10 月 10 日に調査内容を発表し、2024 年 10 月 25 日までに付託事項に対応する提出を求めた。

1.5　委員会は 64 件の提出書類と 4 件の補足書類を受理した。**附属書 A は**、提出された書類の一覧である。

1.6　委員会は 2024 年 10 月 31 日と 11 月 1 日に公聴会を開催した。附属書 B は公聴会に出席した証人のリストである。

1.7　提出書類のコピー　、公聴会の記録、各法案とその説明メモへのリンクは、委員会のウェブサイトからアクセスできる。[1]

報告書の構成

1.8　本報告書は 6 章で構成されている：

- 第 1 章の残りの部分では、事前協議や改革の目的など、サイバーセキュリティ法制パッケージが導入された背景について述べる。
- 第 2 章では、サイバーセキュリティ法案 2024 の条項を概説する。
- 第 3 章では、2024 年インテリジェンス・サービス等法改正案（サイバーセキュリティ法案）の条項の概要を説明する。
- 第 4 章では、重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案（2024 年）の条項について概説する。

[1] www.aph.gov.au/pjcis。

- 第 5 章では、3 つの法案に関して委員会が受け取った証拠をまとめている。
- 第 6 章では、委員会のコメントと国会への勧告が述べられている。

調査の背景

1.9 サイバー脅威からオーストラリアを守り、重要インフラのレジリエンスを確保することは、 オーストラリアの国家安全保障にとってますます重要になっている。現代のテクノロジーは、個人、企業、政府にとって新たな機会を追求し、効率化を図るための数え切れないほどの機会を提供する一方で、新たな脆弱性も生み出している。悪意のあるサイバー・アクターは、軽犯罪者から敵対的な国家に至るまで、これらの脆弱性を悪用する方法を常に模索している。大量の個人情報が流出した最近の有名なサイバーインシデントに対する反応からも明らかなように、オーストラリアの組織がサイバー脅威からより確実に身を守れるようにすることは、政府やより広範なコミュニティにとって、ますます優先度の高い課題となっている。

1.10 2023 年 11 月、当時の内務・サイバーセキュリティ大臣であったクレア・オニール議員は、*2023-2030* 年オーストラリア・サイバーセキュリティ　戦略を発表した。同戦略は、オーストラリアを 2030 年までに「サイバーセキュリティの世界的リーダー」とすることを目 的とし、6 つの「サイバーシールド」（強固な企業と市民、安全な技術、世界レベルの脅威共有とブロッ キング、保護された重要インフラ、ソブリン能力、レジリエンス地域とグローバルリーダーシップ） から構成されている。[2]この戦略では、これらの盾を強化するために、「産業界との共同設計」によるさまざまな法改正を行うことを明記している。[3]

1.11 2023 年 12 月、総務大臣は法改正案に関するコンサルテーション・ペーパーを公表し、パブリックコメント を求めた。[4]コンサルテーション・ペーパーに記載された変更点は、現在サイバーセキュリティ法制パッケージで実施されているものが大部分であった。内務省は、このコンサルテーション・ペーパーに対して 130 件以上の書面提出を受け、法案の策定に役立てた。[5]2024 年 9 月 4 日、内務省は立法パッケージ案の的を絞ったエクスポージャードラフトを発表した。このエクスポージャー・ドラフトに対して 61 件の書面提出があり、200 人以上が参加する「非公開のバーチャル・タウンホール」が 2 回開催された。[6]

サイバーセキュリティ法制パッケージ

1.12 サイバーセキュリティ法制パッケージを構成する 3 法案は、2024 年 10 月 9 日に衆議院に提出された。

---

[2] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略、2023 年 11 月、6-7 頁。

[3] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略、2023 年 11 月、9 頁。

[4] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略：2023 年 12 月、立法改革コンサルテーションペーパー。

[5] サイバーセキュリティ法案 2024、説明資料（EM）、9 頁。

[6]サイバーセキュリティ法案 2024、EM、9 頁。

1.13　今回の法案は、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略に基づく 7 つのイニシアチブを実施するためのもので、「オーストラリアを国際的なベストプラクティスに沿わせ」、オーストラリアが「サイバーセキュリティのグローバルリーダーになるための軌道に乗せる」ための法的ギャップに対処することを目的としている。[7]これらには以下のような施策が含まれる：

- スマートデバイスの最低限のサイバーセキュリティ標準を義務付ける
- 特定の企業に対し、身代金の支払いを報告するランサムウェア報告義務を導入する。
- 国家サイバーセキュリティ調整官とオーストラリア通信総局に「限定的使用」義務を導入する。
- サイバーインシデント審査委員会を設置する。[8]

1.14　サイバーセキュリティ法制パッケージは、*2018* 年重要インフラ安全保障法（SOCI 法）の改革も導入している：

- 業務上重要なデータを保持するシステムに関する既存の義務を明確にする。
- 重要インフラに対する「オールハザード」インシデントの影響をよりよく管理するための政府支援策を強化する。
- 産業界とガバナンスの情報共有を簡素化する。
- 政府が事業体に対し、リスクマネジメント・プログラムの重大な欠陥に対処するよう指示する権限を導入する。
- 電気通信の安全に関する規制を SOCI 法に整合させる。[9]

1.15　パッケージの各法案の主な条項については、第 2 章、第 3 章、第 4 章で詳述する。

[7] 内務省、「画期的なサイバーセキュリティ法パッケージの序文」、メディアリリース、2024 年 10 月 9 日。

[8] 内務省、「画期的なサイバーセキュリティ法パッケージの序文」、メディアリリース、2024 年 10 月 9 日。

[9] 内務省、「画期的なサイバーセキュリティ法パッケージの序文」、メディアリリース、2024 年 10 月 9 日。

2.サイバーセキュリティ法案 2024

サイバーセキュリティ法案の背景と目的

2.1　サイバーセキュリティ法案 2024（Cyber Security Bill）は、「現代の全経済的なサイバーセキュリティ問題」のための法的枠組みを確立し、オーストラリア政府が「新しく出現するサイバーセキュリティ脅威を特定し、それに対応する」ことができるようにすることを目的としている。[1]

2.2　説明文書によると、サイバーセキュリティ法案は以下を目指す：

> オーストラリア国民と企業にさらなる保護を提供し、現存するサイバーリスクの低減を構築し、政府による脅威環境の可視化を改善することで、様々な施策を通じて保護、インシデント対応手順、将来の政策に反映させる。[2]

2.3　サイバーセキュリティ法案の施策には以下が含まれる：

- インターネットまたはネットワークに接続可能なスマートデバイス（俗にモノのインターネット（IoT）デバイスと呼ばれる）のセキュリティ標準を義務付ける権限を確立する。
- サイバーインシデントの影響を受けた事業体がランサムウェアの要求を受け、そのサイバーセキュリティインシデントに関連して支払いや給付を行うことを選択した場合、報告義務を導入する。
- サイバーセキュリティインシデント発生時に国家安全保障局（NCSC）に提供されたサイバーセキュリティインシデント情報が、規制当局を含む他の政府機関でどのように使用され共有されるかを制限する「限定的使用」義務を設ける。
- 重要なサイバーセキュリティインシデントについて、インシデント発生後のレビューを行うサイバーインシデント・レビュー委員会を設置する。[3]

2.4　サイバーセキュリティ法案は 7 つの部分からなる。

パート 1：予備

2.5　サイバーセキュリティ法案のパート 1 は、提案されている第 1 条から第 11 条で構成され、域外適用、定義、「サイバーセキュリティインシデント」および「許可されたサイバーセキュリティ目的」という用語の意味を含む予備的事項を定めている。パート 1 は、本法案が勅許を得た翌日から開始される。

---

[1] サイバーセキュリティ法案 2024、説明資料（EM）、2 頁

[2] サイバーセキュリティ法案 2024、EM、.2 頁

[3] サイバーセキュリティ法案 2024、EM、.2 頁

治外法権

2.6 提案されている第 5 条は、いったん成立すれば、この法律はオーストラリア国内外に適用され ることを規定している。これは、オーストラリアの排他的経済水域と大陸棚を含む、 オーストラリアのすべての外部領土をカバーする。また、オーストラリア国外にも管轄権が及ぶ。[4]

2.7 本条は、サイバーセキュリティインシデントを含む、オーストラリア国外で発生した事業体お よび事象に同法を適用することを可能にし、国際法の下でオーストラリアと十分な関連性を持つことを条 件として、特定の事業体を同法の対象とすることを認める。これには、同法パート 3 の報告義務の対象となる報告事業体や、オーストラリア国外に所在する 関連する接続可能な製品の製造者および供給者が含まれる。[5]

2.8 説明文書には次のように記されている：

> サイバー・セキュリティ・インシデントは国家の境界を問わないため、この法律の域外適用が必要である。多くのインシデントが一つの法域で発生し、他の複数の法域にまたがる可能性がある。オーストラリアに所在する事業体は、サイバーセキュリティインシデントの対象となる他の法域に所在する事業体からサービスを調達することがある。事業体がオーストラリアと他の法域の両方で事業を行い、サイバーセキュリティインシデントの影響を受けることもある。本法がサイバーセキュリティ事件の複数法域の状況に関与するためには、様々な規定の域外適用が不可欠である。
>
> 本法の各パートは、必要な場合、オーストラリアとの関連性がどのようなものであるかを明示している。これは、本法パート 2 におけるセキュリティ標準が適用される関連接続可能製品の取得という文脈におけるオーストラリアとの関連性と、本法パート 3 におけるランサムウェアによる支払いの報告に関連する関連性とは、文脈が異なるためである。[6]

サイバー・セキュリティ・インシデント

2.9 サイバーセキュリティ法案で提案されている「サイバーセキュリティインシデント」の定義は、法律のパート 3、パート 4、パート 5 にわたって使用され、以下のような特定の運用規定を盛り上げるために使用されている：

- パート 3 におけるサイバーセキュリティインシデント後の報告事業体に対するランサムウェアの支払い報告義務
- パート 4 の重要なサイバーセキュリティインシデントに関連して収集された任意情報に関する NCSC の役割と責任

[4] サイバーセキュリティ法案 2024、EM、14 頁[18]。

[5] サイバーセキュリティ法案 2024、EM、14 頁 [19].

[6] サイバーセキュリティ法案 2024、EM、14-15 頁 [20]-[21].

- パート 5 では、特定のサイバーセキュリティインシデントに関するレビューを実施し、政府に勧告を行うサイバーインシデント・レビュー委員会の役割を説明する。[7]

2.10 提案された　第 9 条(1)は、サイバーセキュリティインシデントとは、*2018* 年重要インフラ安全保障法（SOCI 法　　）におけるサイバーセキュリティインシデントの意味に含まれる種類の 1 つ以上の行為、事象または状況であるとプロバイダに定めている。サイバーセキュリティインシデントは、SOCI 法第 12M 条において、以下を含む 1 つ以上の行為、事象または状況として定義されている：

- コンピュータ・データまたはコンピュータ・プログラムへの不正アクセス（第 12M 条(a)
- コンピュータ・データまたはコンピュータ・プログラムの不正な改変（第 12M 条(b)
- コンピュータとの間またはコンピュータからの電子通信の不正な障害（第 12M 条(c)
- コンピュータ、コンピュータ・データ、コンピュータ・プログラムの可用性、信頼性、セキュリティ、または動作を不正に損なうこと（第 12M 条(d)）。[8]

2.11　提案された第 9 項(1)(b)は、SOCI 法の第 12 項 M(c)が規定するサイバーセキュリティインシデントの定義の一部である「コン ピュータとの間の電子通信の不正な障害」は、サイバーセキュリティ法に基づくサイバーセキュリティインシデ ントから「そのような通信の単なる傍受」を除外しないことを規定している。[9]

2.12　提案されている第 9 項(2)は、連邦の立法権に対する憲法上の制限を考慮し、サイバーセキュリティ法 の目的におけるサイバーセキュリティインシデントの定義を制限するもので、例えば、サイバーセ キュリティインシデントは、重要インフラ資産、企業、電信サービスの利用、オーストラリアの国家安 定または安全に対する脅威を伴うものでなければならない。

サイバーセキュリティインシデントが発生した場合に許可されるサイバーセキュリティ目的

2.13　提案されている「許可されたサイバーセキュリティ目的」の定義は、パート 4 において、NCSC に提供された情報の使用と開示に関連して使用される。

2.14　提案されている第 10 条は、以下の各項をサイバーセキュリティインシデントの「許可されたサイバーセキュリティ目的」とすることをプロバイダに定めている：

- サイバーセキュリティインシデントへの対応、低減または解決に関連する英連邦団体（英連邦の執行機関でない限りにおいて）の機能の遂行。

[7] サイバーセキュリティ法案 2024、EM、.20 頁[67].

[8] サイバーセキュリティ法案 2024、EM、.20 頁 [68].

[9] サイバーセキュリティ法案 2024、EM、20 頁[69]。*2018* 年重要インフラ安全保障法（SOCI 法）第 5 条は、「単なる傍受」は SOCI 法上の電子通信の障害とはみなされないと規定している。

- サイバーセキュリティインシデントへの対応、低減または解決に関連する国家団体の機能の遂行。[10]

- サイバーセキュリティインシデントに関するパート 4 に基づく NCSC の機能の遂行

- サイバーセキュリティインシデントについて、英連邦の大臣および他の大臣に通知し、助言すること。

- サイバーセキュリティインデントが、オーストラリアもしくはその国民の社会的もしくは経済的安定、オーストラリアの防衛、または国家安全保障に重大な損害を与えた、または与えようとしている、もしくは与えることが合理的に予想される重大なリスクを防止または低減すること。

- 重要インフラ資産に対する重大なリスクを防止または低減する。[11]

- 情報機関の機能の遂行[12]

- 英連邦の執行団体の機能を果たす。[13]

パート 2：スマートデバイスのセキュリティ標準

2.15 サイバーセキュリティ法案のパート 2 では、特定の状況下でオーストラリア国内で入手される、インターネットに直接または間接的に接続できる製品（「関連接続可能機器」）に対して、義務的なセキュリティ標準を規定する規則を認める枠組みを確立している。

2.16 パート 2 は、公布によって定められた 1 日、または同法が勅許を得た後 12 ヶ月が経過した時点で開始される。パート 2 は 4 つのディビジョンから構成される。

2.17 パート 1 は予備的事項を扱う。提案されている第 12 条は、パート 2 の簡略化されたアウトラインを提供し、提案されている第 13 条は、どの製品がパート 2 の規則で定められた強制的なセキュリティ標準の対象となり得るかを定める適用規定である。[14]

---

[10] 提案されている第 8 条において「国の団体」とは、国もしくは準州の大臣もしくは部局、または国もしくは準州が公的目的のために設立した団体であって、王室の認可を受けていない団体を含むと定義されている。

[11] 重要インフラ資産」は、SOCI 法と同じ意味を持つ。

[12] 情報機関」は第 8 条案で定義され、オーストラリア犯罪情報委員会、オーストラリア地理院、 オーストラリア秘密情報局、オーストラリア安全保障情報局、オーストラリア信号長官、国防情 報局、国家情報長官室を含む。

[13] サイバーセキュリティ法案 2024、EM、.21-22 [75].連邦の執行団体」は第 8 条案で定義されており、オーストラリア連邦警察、オーストラリア健全性規 制局（Australian Prudential Regulation Authority）、オーストラリア証券投資委員会（Australian Securities and Investments Commission）、国家反汚職委員会（National Anti-Corruption Commission）の検査官、検察長官事務所（Office of the Director of Public Prosecutions）、国家反汚職委員会（National Anti-Corruption Commissioner）、スポーツ・インテグリティ・オーストラリア（Sport Integrity Australia）、および「刑事犯罪に対する罰則または制裁を課す法律の管理、またはそれに基づく機能の実行に責任を負う範囲での、他の連邦の団体」を含む：サイバーセキュリティ法案 2024、提案された条項 8。

[14]サイバーセキュリティ法案 2024、EM、23 頁[86]。

- 提案された第 13 項(1)は、パート 2 が、以下の開始日以降に製造または供給された「関連する接続可能な製品」にのみ適用されることを規定している。

- 第 13 条(2)項で定義される、規則で除外されない「インターネット接続可能な製品」または「ネットワーク接続可能な製品」を含む。

- 提案されている第 13 条(3)は、規則が製品のクラスが免除されること、または特定の製品が免除されることを規定することができると規定している。これにより、免除される製品は、関連する接続可能な製品とはみなされず、パート 2 の対象とはならない。

- 提案されている第 13 条 4 項は、「インターネット接続可能な製品」を、インターネット上でデータを送受信するためにインターネット・プロトコル・スイートの一部を構成する通信プロトコルを使用してインターネットに接続できる製品と定義している。

  - インターネット接続可能な製品の定義は、インターネット・ルーターのような有線接続（例えばイーサネットポート経由）、またはスマートテレビのような無線接続（例えば Wi-Fi や携帯電話接続経由）を通じて、インターネットに直接接続できる機器を幅広く捉えている。

- 提案されている第 13 条 5 項では、「ネットワーク接続可能な製品」を、電気的または電磁気的エネルギーを伴う伝送によってデータの送受信が可能な製品であって、インターネット接続可能な製品ではないものと定義している。

  - 大まかに言えば、ネットワーク接続可能な製品とは、インターネットに直接接続することはできないが、インターネット接続可能な製品を通じて（例えば Bluetooth 接続を通じて）インターネットに接続することができる製品を指す。第 13 条(6)から第 13 条(9)は、定義に該当する、または該当しない製品の種類をさらに技術的に明確にしている。

- 提案された第 13 条(10)は、第 13 条(4)から(9)の目的上、接続に電線またはケーブルが使用されているからといって、製品が他の製品に直接接続されているとみなされないことを明確にするものである。[15]

2.18 パート 2 は、事業体に対してセキュリティ標準の遵守を求める主要な運用条項からなる第 14 項から第 16 項の案で構成される。

- 提案されている第 14 条は、関連する接続可能な製品の特定クラスに関する規則で規定されるセキュリティ標準に関する一般規則制定権をプロバイダする。[16]提案されている第 87 条に基づき、規則は大臣が作成する立法文書の形をとる。

- 提案された第 15 条は、関連する接続可能製品を供給または製造しようとする事業体に対し、第 14 条に基づき作成されたセキュリティ標準に準拠する幅広い義務を規定する。[17] .

[15] サイバーセキュリティ法案 2024、EM、.23-25 頁 [86]-[99].

[16] サイバーセキュリティ法案 2024、EM、26 頁[100]。

[17] サイバーセキュリティ法案 2024、EM、.27 頁 [109].

- o 遵守義務は、事業体が「製品がオーストラリアで取得されることを認識している、または認識することが合理的に期待できる」状況において適用される。[18]

- 提案されている第 16 条は、事業体に対し、関連する接続可能な製品の供給に関連するセキュリティ標準への準拠を表明した文書を提供し、保持する義務を課すものである。[19] 。

  - o コンプライアンスに関する声明文の詳細要件は、規則で定めることが提案されている。[20]

2.19 第 3 章は第 17 節から第 20 節までで構成され、順守通知、停止通知、リコール通知、リコール通知に従わない場合の公示など、執行の枠組みを定める。

- 提案されている第 17 条は、第 15 条または第 16 条に基づく義務が遵守されない場合に事業体に与えられる可能性のある、最初のタイプの通知について規定している。

  第 17 条は、事業体が義務を遵守していないと長官が合理的に判断した場合、あるいは事業体が義務を遵守していない可能性を示唆する情報を長官が把握した場合、長官が事業体に遵守通知を出す権限を与えている。[21]

  - o 提案されている第 17 条(1)から第 17 条(4)は、順守通知を行うために存在しなければならない条件、通知に含まれなければならない詳細、事業体に順守通知を行う前に長官が従わなければならない手順に関する手続き上の公平性、および順守違反または順守違反の可能性のある特定の事例に関して、事業体に対して順守通知を 1 回のみ発行できることを定めている。[22]

- 提案されている第 18 条は、事業体が第 15 条または第 16 条に基づく義務を遵守していない場合に発行される 2 種類目の通知について規定している。第 18 条は、事業体が第 17 条に基づいて発行された遵守通知を遵守していないと長官が合理的に判断した場合、長官が事業体に対して停止通知を発行する権限を与えるものである。[23]

  - o 提案された第 18 項(1)は、第 18 項に基づく停止通告を行うためには、長官は、遵守通告を受けた事業 体が遵守通告を遵守していないこと、または事業体がとった行動が遵守違反の是正に不十分であることを 合理的に納得しなければならないと規定している。[24]説明文書には次のように記されている：

    何かを「合理的に納得」するということは、意思決定者が特定の行政行為を行う前に必要とされる心的状態の一般的な閾値である。この閾値は、停止通告を出すことが必要または望ま

[18] サイバーセキュリティ法案 2024、15 条 1 項。

[19] サイバーセキュリティ法案 2024、EM、28 頁[116]。

[20] サイバーセキュリティ法案 2024、16 条 5 項。

[21] サイバーセキュリティ法案 2024、EM、30 頁[128]。

[22] サイバーセキュリティ法案 2024、EM、30-31 頁 [129]-[132].

[23] サイバーセキュリティ法案 2024、EM、31 頁[133]。

[24] サイバーセキュリティ法案 2024、EM、31 頁[134]。

しいと「納得」できる合理的な根拠があることを要件としている。合理的に納得する」とは、事業体が遵守通知を遵守していないこと、または事業体が義務不遵守を是正するためにとった行動が、不遵守を是正するには不十分であることを長官が納得しなければならず、この納得が客観的に合理的であることを要求する心的状態である。したがって、満足の根拠となる根拠は、長官の立場にある合理的な人物に同様の信念を抱かせることができるものでなければならない。[25]

- o 提案された第 18 条(2)項には、停止通告が詳述しなければならない事項が明記され、提案された第 18 条(3)項には、長官が事業体に停止通告を行う前に従わなければならない自然正義の要素が含まれている。長官は、通知を行う意図を事業体に通知し、通知を行う意図について表明するための特定期間を事業体に提供しなければならない。この特定期間は 10 日を下回ってはならない。事業体が通告の発出について意見表明を行うための特定期間のベストプラクティスは 10 営業日であるが、これは通告の内容によって変更可能である。[26]

- o 提案されたサブセクション 18(4)は、事業体の特定のコンプライアンス違反の事例に関して、1 つの事業体に対して 1 回のみ停止通知を発行できることを規定している。[27]

- 提案されている第 19 条は、事業体が義務を遵守しなかった場合に発行される可能性のある第 3 のタイプの通知について規定している。第 19 条は、事業体が第 18 条に基づき発行された停止通告に従わなかったと、長官が合理的に納得した場合、長官が事業体に対してリコール通告を発行する権限を与えるものである。提案されている第 18 条(1)から第 18 条(4)とほぼ同じ内容で、第 19 条(1)から第 19 条(4)には、長官がリコール通告を行うために合理的に満足しなければならない事項、リコール通告が詳述しなければならない事項、リコール通告に関して従わなければならない自然正義の要素、およびリコール通告は 1 回のみ発行できることが規定されている。28

- 提案された第 20 条は、リコール通知に従わなかった事業体の詳細を公表するための、大臣の裁量権を規定する。本条は、大臣が当該詳細を同省のウェブサイト、または大臣が適切と考えるその他の方法で公表することができると規定している。公表できる情報には、不順守事業体の身元、製品および不順守の詳細、不順守に関連する製品がもたらすリスクが含まれる。[29]

2.20 提案されている第 21 条から第 24 条で構成されるパート 4 は、以下を含む雑多な権限を定めている：

- 通知の撤回と変更（第 21 条案）

- 通知を行う決定の内部（部門）審査（第 22 条案）

---

[25] サイバーセキュリティ法案 2024、EM、32 頁[138]。

[26] サイバーセキュリティ法案 2024、EM、32 頁[142]。

[27] サイバーセキュリティ法案 2024、EM、33 頁[143]。

[28] サイバーセキュリティ法案 2024、EM、33 頁[144]-[149].

[29]サイバーセキュリティ法案 2024、EM、34 頁[150]。

- 事業体が要求に応じて製品を検査に提供し、そのために合理的な対価を支払うことを要求することを含め、セキュリティ標準及び準拠表明書への準拠を評価するための独立した検査を手配するためのプロバイダに関する規定（第 23 項案）。

パート 3：ランサムウェアの報告義務

2.21 サイバーセキュリティ法案のパート 3 はランサムウェアの報告義務を扱い、3 つのディビジョンで構成されている。パート 3 は、公布によって定められた 1 日、または同法が勅許を得た後 6 カ月が経過した時点で開始される。

2.22 パート 1 は、パート 3 の簡略化されたアウトラインを提供する。

2.23 提案されている第 26 条から第 28 条で構成される第 2 区分は、サイバーセキュリティインシデントにより影響を受け、インシデントまたはその影響から利益を得ようとする事業体（「強要する事業体」）に直接的または間接的に支払いまたは利益（「ランサムウェアの支払い」と呼ぶ）を提供した特定の事業体（「報告する事業体」）に報告義務を課すものである。[30]

2.24 提案されている第 26 項(1)は、5 つの規準を定めており、この規準がすべて満たされた場合、ランサムウェアの報告義務が強化される。以下の場合、義務は活性化される：

- インシデントが発生した、発生している、または差し迫っている。
- インシデントが第 9 条に定義されるサイバーセキュリティインシデントである。
- サイバーセキュリティインシデントが、第 26 項(2)に定義される報告事業体に直接的または間接的な影響を与えた、与えている、または与えることが合理的に予想される。
- インシデントまたは報告事業体への影響から利益を得るために、恐喝主体が報告事業体またはその他の事業体に対して要求を行う。
- 報告事業体が、要求に直接関連する支払いまたは利益（ランサムウェアによる支払い）を、恐喝事業体に提供するか、または他の事業体がその事業体に代わって提供したことを認識している。[31]

2.25 説明文書では、第 26 条(1)の要件は、恐喝した事業体がサイバーセキュリティインシデントに責任があるかどうかに関係なく満たされると助言している。さらに、報告事業体は、「自らが要求の対象でなくとも、他の事業体が最初のサイバーセキュリティインシデントの結果として要求を受けたことを認識している場合であっても、パート 3 に基づく報告義務を負う」。[32]解説文書は次のように説明している：

[30] サイバーセキュリティ法案 2024、EM、39 頁[178]。

[31] Cyber Security Bill 2024、EM、39-40 [182]-[186].

[32]サイバーセキュリティ法案 2024、EM、40 頁[187]。

このセクションは、サイバーセキュリティインシデントの責任事業体の身元が常に判明するとは限らず、場合によっては判明しないこともあるという現実を反映している。同様に、恐喝を行った事業体の身元も常に確認できるとは限らない。同じ事業体である場合もあれば、複数の事業体が連携している場合もあり、また、ある事業体が他の事業体によって引き起こされたインシデントを日和見的に悪用するような、全く関係のない事業体である可能性もある。いずれにせよ、報告義務は、取り決めにとらわれないことを意図しており、ある事業体がサイバーセキュリティインシデントを引き起こし、別の事業体または同じ事業体が、インシデントから利益を得るために、影響を受けた事業体に対して要求を行う状況を捕捉しようとするものである。[33]

2.26 提案されている第 26 条(2)は、第 26 条(1)の目的における「報告事業体」を定義している。事業体は、ランサムウェアの支払いが行われた時点で、以下の場合、報告事業体である、

a. 事業体である：

i. 前会計年度の年間売上高がその年度の売上高基準額を超えており、オーストラリアで事業を営んでいる。

ii. 英連邦の団体でも国の団体でもない。

iii. 重要インフラ資産の責任事業体でない。

b. その事業体は、[SOCI 法]パート 2B が適用される重要インフラ資産の責任主体である。[34]

2.27 提案された第 26 項(3)は、第 26 項(2)(a)(i)の目的における「売上高基準額」は、規則（[35]）によって規定された方法によって決定されることを規定している。 提案された第 87 条に従い、規則は大臣によって作成された立法文書の形をとる。

2.28 提案されている第 27 条は、第 26 条の規準が満たされている場合、ランサムウェアによる支払い後の報告事業体の報告義務を定める。[36] 。

- この報告書は、支払いを行ってから、あるいは支払いに気づいてから 72 時間以内に「指定された連邦団体」に提出することが義務付けられている。[37]

---

[33] サイバーセキュリティ法案 2024、EM、41 頁[189]。

[34] Cyber Security Bill 2024, proposed s. 26(2); Cyber Security Bill 2024、EM、. 41 [190].説明資料には、「SOCI 法のパート 2B は、責任ある事業体が、同部が適用される重要インフラ資産に関連する影響を及ぼすサイバーセキュリティインシデントを報告しなければならない独自の枠組みを定めている。ランサムウェアの報告義務を充実させることで、SOCI 法内の既存の規定で義務付けられている報告を捕捉するための補完的な報告枠組みが確保されることになる。これにより、報告負担が増加することはないが、報告要件がより大きな報告スキームの中に確実に取り込まれることになる」。

[35] サイバーセキュリティ法案 2024、EM、43 頁[194]。

[36] サイバーセキュリティ法案 2024、EM、44 頁[202]。

[37] サイバーセキュリティ法案 2024、27 条 1 項案。

- 「連邦指定機関」とは、第 8 条で定義され、内務省およびオーストラリア信号局（ASD）、または規則で指定された省庁または連邦機関を意味する。

- 指定英連邦団体に対する報告の要求される様式，方法及び内容は，提案されている第 27 条(2)から(4)に定められており，規則が定める要件によって補足されることがある。

2.29 事業体は、報告義務に違反した場合、60 罰単位の民事罰の責任を負う。[38]

2.30 提案されている第 28 条(1)項および第 28 条(2)項は、サイバーセキュリティインシデントの報告義務を「誠実に」遵守することから生じる可能性のある、守秘義務違反、その他の契約上の要件、その他の民事訴訟などによる責任の発生から報告事業体を保護するように設計されている。[39]説明文書には次のように記されている：

> このような責任からの保護は、企業が、強制的な要件に従うか、損害賠償訴訟に発展する可能性のある契約上の義務やその他の義務に従うかの二者択一を迫られないようにするために必要である。これには、特定の情報の契約上の守秘義務や、損害賠償をもたらす不法行為の疑いが含まれる。この報告義務を遵守する一方で、事業体に適切な保護が提供されなければ、制度への積極的な関与と包括的な情報のプロバイダ提供が妨げられることになる。第 27 条では、損害賠償請求の対象となりうる情報を可能な限り限定するため、情報の種類を正確に定義している。[40]

2.31 提案されている第 28 条(3)は、第 28 条の保護に依拠しようとする事業体は、その事項を証明する証拠責任を負うと規定している。[41]説明資料には次のように記載されている：

> 第 28 条(3)を定めるにあたり、「犯罪の構成、侵害通知及び執行権に関する連邦ガイド」（Commonwealth Guide to Framing Offences, Infringement Notices and Enforcement Powers）が考慮された。事業体が立証責任を負うのは、立証すべき事項が事業体特有の知識の範囲内にあるためであり、仮想的な原告が反証することは、事業体がこの事項を立証するよりも著しく困難である（場合によっては費用がかかる）。事業体は、第 27 条を遵守して誠実に行動していたかどうかを判断できる証拠を提出することができる唯一の立場にある。[42]

2.32 Part3 のディビジョン 3 は、提案されているセクション 29 から 32 で構成され、ランサムウェアの支払い報告に関する情報の保護を扱っている。

2.33 提案された第 29 条は、指定連邦団体によるランサムウェア支払い報告に含まれる情報の許可された記録、使用および開示の枠組みを提供する。[43]提案された第 29 条(1)は、報告事業体によるランサ

---

[38] サイバーセキュリティ法案 2024、27 条 5 項案。

[39] サイバーセキュリティ法案 2024、EM、48 頁 [223]-[225].

[40] サイバーセキュリティ法案 2024、EM、48 頁[226]。

[41] サイバーセキュリティ法案 2024、EM、48 頁[227]。

[42] サイバーセキュリティ法案 2024、EM、48 頁[227]。

[43] サイバーセキュリティ法案 2024、EM、48 頁[228]。

ムウェア支払報告で指定連邦機関に提供された情報は、以下の 1 つ以上の目的のために記録、使用、または開示される可能性があると規定している：

- 報告事業体、および報告事業体の代理を務める他の事業体を支援し、サイバーセキュリティインシデントに対応、低減または解決する。
- 本編またはパート 6（規制権限）に基づき、機能を遂行し、または権限を行使する。
- *1995* 年刑法法（*Criminal Code Act 1995*）別表第 1 の第 137.1 項または第 137.2 項に基づく、またはそれらに起因する手続。刑法のこれらの条項は、虚偽で誤解を招くような情報および文書、または連邦の事業体に提供された情報、または連邦の法律に従って作成された情報のプロバイダに対する犯罪を定めている。この例外が含まれることで、事業体が虚偽で誤解を招く文書や情報の提供に関して、これらの犯罪のいずれかに該当する場合、ランサムウェアの支払い報告書を訴訟手続きに関連する証拠として提出できるようになる。
- 刑法第 149 条第 1 項に対する違反に対する手続を行う。刑法のこの規定には、連邦公務員がその職務を遂行するのを妨害し、妨げ、威嚇し、または抵抗することに対する犯罪が含まれている。これにより、ランサムウェアの支払い報告書は、サイバーセキュリティ法に関連する英連邦公務員の職務執行妨害の訴訟手続きに証拠として含まれることになる。
- サイバーセキュリティインシデントへの対応、低減または解決に関する英連邦団体の機能の遂行。
- サイバーセキュリティインシデントへの対応、低減または解決に関連する国家団体の機能の遂行。
- サイバーセキュリティインシデントに関するパート 4 に基づく NCSC の機能の遂行
- サイバーセキュリティインシデントについて、大臣および連邦の他の大臣に通知し、助言すること。
- 情報機関の機能を遂行する。[44]

2.34 提案された第 29 条(2)は、指定連邦団体が、報告事業体に関連する、パート 3 の違反又は刑事犯罪以外の、 違反の罰則又は制裁の調査若しくは執行、又は調査若しくは執行の補助を目的として、情報を記録、使用又は開示することを制限する。これは、事業体から提供された情報が、民事規制の文脈で不利に使用されることを防ぐためである。[45]

[44] サイバーセキュリティ法案 2024、EM、48-49 頁 [229].

[45] サイバーセキュリティ法案 2024、EM、50 頁[231]。

2.35　提案された第 29 条(3)は、第 29 条(1)は、*1988* 年プライバシー法によって、またはプライバシー法の下で禁止または制限される範囲において、指定された連邦団体に情報を記録、使用または開示する権限を与えないと述べている。[46]

2.36　提案された第 29 項(4)は、ランサムウェアの支払い報告に含まれる情報の記録、使用または開示に関する一般的制限 が、SOCI 法第 2B 部（サイバーセキュリティ報告）に基づく要件、*1997* 年電気通信法に基づく要件、または規則で定められた法律に基づく要件として、事業体によって、または事業体に代わって、指定された連邦機関に既に提供されている範囲には適用されないことを規定する。

2.37　提案された第 30 条は、ランサムウェアの支払い報告でプロバイダが提供した情報の二次使用と開示に関する制限を含んでいる。[47]第 30 条は、報告事業体によりランサムウェア支払報告で提供された情報、第 29 項(1)または第 30 条に基づき他の事業体、連邦機関または州機関により取得された情報、および他の事業体、連邦機関または州機関により保有される情報に適用される。第 30 条(2)、第 30 条(3)および第 30 条(4)は、第 29 条(1)、第 29 条(2)および第 29 条(3)の指定連邦機関に適用される記録、使用および開示の制限を反映する。

2.38　提案されている第 30 条(5)項は、第 29 条(4)項と、個人情報、事業体の同意を得て開示される事業体情報、および国の憲法上の機能または権限の履行に関する追加的な例外を用いて、第 30 条の記録禁止に対する例外を規定している。

2.39　提案された第 30 条(6)項では、ランサムウェアの支払報告書の情報の無許可の二次使用または開示に対する民事罰の規定が導入される。[48]

2.40　提案された第 31 条は、法律専門家の秘匿特権の問題と、通常であれば法律専門家の秘匿特権によって保護されるランサムウェアの支払い報告書内の情報を政府に提供することとの相互関係について明確にすることを意図している。[49]同条項は、ランサムウェア情報を報告するという事実が、コロニアル調査や王立委員会の手続きなどの一部の例外を除き、その情報に関する事業体の法律専門家秘匿特権の主張に影響を与えないことを規定している。

2.41　提案された第 32 条も同様に、ランサムウェアの支払い報告において報告事業体が提供した情報が、刑事訴訟や民事訴訟において証拠として認められることを制限している。[50]

---

[46] サイバーセキュリティ法案 2024、EM、50 頁[233]。

[47] サイバーセキュリティ法案 2024、EM、50 頁[236]。

[48] サイバーセキュリティ法案 2024、EM、52 頁 [243]-[244].

[49] サイバーセキュリティ法案 2024、EM、53 頁[253]。

[50] サイバーセキュリティ法案 2024、EM、54 頁[259]。

パート 4：重大なセキュリティ・インシデントの調整

2.42　サイバーセキュリティ法案のパート 4 は、NCSC への自発的な情報提供を扱う。パート 4 は、同法が勅許を得た翌日から開始され、3 つのディビジョンから構成される。

2.43 パート 1 は予備的な事項を扱い、「重大なサイバーセキュリティインシデント」の定義を規定する第 34 章案を含む。以下の場合、サイバーセキュリティインシデントは重大なサイバーセキュリティインシデントである：

- インシデントが、オーストラリアもしくはその国民の社会的もしくは経済的安定、オーストラリアの防衛、または国家安全保障に重大な損害を与えた、または与えようとしている、もしくは与えると合理的に予想される重大なリスクがある場合。

- インシデントがオーストラリア国民にとって重大な関心事である、あるいはそうなることが合理的に予想される場合。[51]

2.44　提案された第 35 条から第 37 条で構成されるパート 2 は、NCSC との自発的な情報共有を扱う。[52]

- 提案されている第 35 条は、影響を受けた事業体または影響を受けた事業体に代わって行動する他の事業体が、本条に定める規準に従い、重大なサイバーセキュリティインシデントに関して、NCSC に自発的に情報を提供することを定めている。[53]

- 提案されている第 36 条は、NCSC が情報を収集・利用できる状況と目的の概要を示しており、インシデントがサイバーセキュリティインシデントか重大なサイバーセキュリティインシデントかを判断するためのものである。[54]

- 提案されている第 37 条は、「重大なサイバーセキュリティインシデントに対応するため、政府全体で行動の調整と優先順位付けを主導する」「重大なサイバーセキュリティインシデントへの政府全体の対応に関して、ガバナンスと政府全体に情報を提供し、助言する」など、NCSC の役割の概要を示している。ただし、第 37 条は「非網羅的な性格のものであり、[NCSC]の役割を列挙された事項に限定するものではない」とされている。[55]

    - NCSC は第 8 項で定義され、国家サイバーセキュリティ・コーディネーターと呼ばれる内務省の役 員、およびオーストラリア公務員の職員、連邦団体の役員または職員で、サイバーセキュリティ法に基づく機能の遂行と権限の行使に関連してコーディネーターがサービスを利用できる者を含む。

[51] サイバーセキュリティ法案 2024、EM、56 頁[270]-[271]。

[52] サイバーセキュリティ法案 2024、EM、56 頁。

[53] サイバーセキュリティ法案 2024、EM、56 頁[272]。

[54] サイバーセキュリティ法案 2024、EM、58 頁 [284].

[55] サイバーセキュリティ法案 2024、EM、59 頁[288]。

2.45 提案されている第 38 条から第 43 条までのディビジョンは、第 35 条(2)に基づき、重大なサイバーセキュリティインシデントに関連して提供された情報の保護を取り扱う。[56]

2.46 提案されている第 38 条は、NCSC による当該情報の使用および開示に関するパラメータを定めている。[57]

- 提案された第 38 条(1)の概要は、NCSC は、サイバーセキュリティインシデントに関連して、事業体（影響を受ける事業体）により、または事業体のために、第 35 条(2)に基づきプロバイダから提供された情報を、以下の 1 つ以上の目的のためにのみ、記録、使用または開示することができる、というものである：
  - NCSC および NCSC を支援するスタッフが、影響を受けた事業体、および影響を受けた事業体の代理を務める他の事業体を支援し、サイバーセキュリティインシデントに対応、軽減、または解決できるようにする。
  - 第 10 条（上記参照）で定義される「許可されたサイバーセキュリティ目的」。[58]
- 提案された第 38 条 2 項は、本法案のパート 4 以外の民法違反の調査または執行のために、NCSC が記録を作成し、情報を使用し、開示することを禁止する。[59]説明資料には、第 38 項(2)に関するさらなる詳細が記載されている：

> この小項目は、本編の意図が、提供された情報が法執行または規制目的のために記録、使用、開示されないことが保証される一方で、事業体がサイバーインシデント発生時に国家サイバーセキュリティ・コーディネーターと関わることを奨励することであることを補強するものである。刑法違反から保護することが本制度の意図ではないため、刑法違反に対する罰則や制裁を科す目的の開示を妨げるものではない。
>
> 特に、サイバーセキュリティインシデントとは関係のない重大な法律違反が明らかになった場合に、運用、規制、法執行機関が既存の法制化された機能を遂行することを制限することは、政府の意図するところではないことを強調しておかなければならない。本編は、法執行機関や規制当局が既存の権限を使ってこの情報を収集し、事業体に対する規制や法執行の目的で使用することを制限する意図はない。[60]

2.47 提案されている第 39 条は、その他のインシデント（すなわち、第 34 条で定義されている「重大なサイバーセキュリティインシデント」ではないインシデント）に関連して提供された情報の NCSC による使用と開示に関するパラメータを定めている。[61]説明文書は次のように定めている：

---

[56] サイバーセキュリティ法案 2024、EM、59 頁[290]。

[57] サイバーセキュリティ法案 2024、EM、59 頁[290]。

[58] サイバーセキュリティ法案 2024、EM、59 頁[291]。

[59] サイバーセキュリティ法案 2024、EM、60 頁[294]。

[60] サイバーセキュリティ法案 2024、EM、60 頁[295]-[296].

[61] サイバーセキュリティ法案 2024、EM、61 頁[301]。

第 39 条の意図は、インシデントに関連して国家サイバーセキュリティ・コーディネータに情報がプロバイダされたが、そのインシデントが重大なサイバーセキュリティインシデントであるかどうか、あるいはその可能性があるかどうかが不明確である場合、その情報は依然として限定された目的でのみ記録、使用、開示されることを保証することである。インシデントが重要なサイバーセキュリティインシデントではないため、許可されたサイバーセキュリティの目的は適用されず、したがって、これらの目的のために情報を共有する必要はない。インシデントの詳細が明らかになり、重大なインシデントと判断された場合は、第 35 条に記載されている規定が適用される。[62]

2.48 提案されている第 40 条では、情報の二次使用と開示について同様の制限を設けている。[63]

2.49 提案されている第 41 条は、法律専門家の秘匿特権の問題と、パート 4 に基づき通常保護される情報を NCSC にプロバイダすることとの相互関係を明確にすることを意図している。[64]提案されている第 42 条は、影響を受けた事業体から自発的に提供された情報の認容可能性に関す るものである。[65]説明文書では以下のように規定されている：

この規定の意図は、許可されたサイバーセキュリティ目的のために開示される可能性が大量にあるため、国家サイバーセキュリティ・コーディネーターへの情報提供が法律専門家秘匿特権の放棄に相当するとも相当しないとも、本編では定めていないことを明確にすることである。秘匿特権情報の防御を保証することはできないが、第 40 条に基づく二次使用と開示の制限、および第 42 条(2)に基づく認容可能性からの保護は、法律専門家の秘匿特権が放棄されないという保証がなくても開示を促すのに十分なレベルの防御を提供情報に与える。

許可されたサイバーセキュリティ目的の下で自発的にプロバイダが提供した情報を、規制当局が報告事業体に対する民事コンプライアンス訴訟のために使用することはできない。情報は、連邦法に基づく民事罰の違反に対する手続きにおいて、その事業体に対して認められることはない。[66]

2.50 提案された第 43 条は、長官が、特定人物が第 8 条に定義される NCSC の一員である、または過去に一員であった旨の証明書を発行することを規定している。このような人物は、パート 4 に基づき事業体が提供する情報に関連する限り、連邦裁判所または州もしくは準州の裁判所において証人として強制されることはない。[67]説明文書は次のように定めている：

サイバーセキュリティインシデントまたは重大なサイバーセキュリティインシデントへの対応の過程で、国家サイバーセキュリティコーディネーターが受け取った情報は、限定的使用義務の対象であると考えられる。したがって、国家サイバーセキュリティ・コーディネータ

[62] サイバーセキュリティ法案 2024、EM、63 頁[309]。

[63] サイバーセキュリティ法案 2024、EM、63 頁[310]。

[64] サイバーセキュリティ法案 2024、EM、65 頁[328]。

[65] サイバーセキュリティ法案 2024、EM、66 頁[334]。

[66] サイバーセキュリティ法案 2024、EM、67 頁 [241]-[242].

[67]サイバーセキュリティ法案 2024、EM、67 頁[343]。

ーが対応したサイバーセキュリティ・インシデントに関して証拠としてプロバイダから提供される可能性のある情報は、同法第 42 条によれば、一切認められない。本法における非可決規定は、セーフハーバーとして設計されたものではない。執行機関は、依然として自らの立法権に依拠することができる。さらに、この保護はコロニアル調査には適用されない。[68]

2.51 第 44 条案からなるディビジョン 4 は、パート 4 の運用が、サイバーセキュリティ法または連邦の他の法律に基づく情報提供の他の要件に影響しないことを規定している。[69]

パート 5：サイバーインシデント審査会

2.52 サイバーセキュリティ法案のパート 5 では、サイバーインシデント審査委員会（CIRB）を設置する。パート 5 は、公布によって定められた 1 日、または同法が勅許を得た後 6 カ月が経過した時点で開始される。パート 5 は 7 つのディビジョンからなる。

2.53 パート 1 は第 45 条案で構成され、パート 5 の簡略化されたアウトラインを提供する。[70]

2.54 提案されている第 46 条から第 54 条で構成されるパート 2 門は　、CIRB によるレビューを扱う。レビューの目的は、今後同様の性質のサイバーセキュリティインシデントを予防、検知、対応、または影響を最小化するために取り得る措置について、政府および産業界に対応勧告を行うことである。[71]

2.55 CIRB は、サイバーセキュリティインシデントまたは一連の関連するサイバーセキュリティインシデントに関して、以下の者の書面による照会に基づき、レビューを実施させることができる：

a. 大臣

b. NCSC である；

c. インシデントまたは一連のインシデントによって影響を受けた事業体、または

d. CIRB のメンバーである。[72]

2.56 提案された第 46 条(2)は、以下の場合のみ見直しを行うことができると定めている。

a. インシデントまたは一連のインシデントが、第(3)項に定める規準を満たすと CIRB が納得した場合；

a. インシデントまたは一連のインシデント、および緊急対応が終了した後。

---

[68] サイバーセキュリティ法案 2024、EM、68 頁[347]。

[69] サイバーセキュリティ法案 2024、EM、68 頁[348]。

[70] サイバーセキュリティ法案 2024』EM, p. 70 [355]-[360].

[71] Cyber Security Bill 2024、EM、.70-81 [361]-[439].

[72]サイバーセキュリティ法案 2024、第 46 条案。

b. 大臣がレビューの職務権限を承認した場合。

2.57 第 46 条(3)に規定された審査が必要なインシデントの規準には、オーストラリアの社会的・ 経済的安定、国防、国家安全保障を「著しく害する」インシデント（または一連のインシデント）である場合、 あるいは「著しく害する」と合理的に予想されるインシデントである場合、斬新で複雑な手法や技術に関連するインシデントである場合、あるいは「オーストラリア国民にとって重大な関心事」 であると合理的に予想されるインシデントである場合が含まれる。

2.58 提案された第 46 条(4)項は、各レビューは、議長、レビューの職務権限に明記された CIRB の常任委員、およびレビューを補佐するために任命された専門家パネルのメンバーで構成されるレビューパネルによって実施されることをプロバイダとして規定している。

2.59 提案された第 48 条から第 50 条は、CIRB に事業体に対して情報または書類の提出を要求する権限、または要求する通知を発行する権限を与える。事業体は、文書提出を要求する通知に従わない場合、民事罰の責任を負う。[73]

2.60 提案された第 51 条から第 54 条には、CIRB が作成するドラフトおよび最終レビュー報告書の要件が規定されている。最終レビュー報告書には、「機微なレビュー情報」[74] を含んではならない：

- レビューの対象となったサイバーセキュリティインシデントに関して、責任の所在を明らかにする；
- このようなサイバーセキュリティインシデントに関連する事業体の責任を決定する手段を提供する；
- 個人の識別（本人の同意がある場合を除く。
- 事業体が審査対象であるという事実から、不利な推論が導き出されることを許容する。[75]

2.61 最終審査報告書（修正箇所を除く）の公表が義務付けられている。[76]

2.62 提案されている第 55 条から第 59 条で構成されるディビジョン 3 は、ランサムウェア報告書や NCSC に自発的に提供された情報（上記参照）に関するものと同様の限定使用規定を含む、審査に関する情報の保護を扱う。

2.63 提案されている第 60 条から第 63 条で構成されるディビジョン 4 は、CIRB の設置、機能、権限を扱う。CIRB は、議長 1 名と、少なくとも 2 名、ただし 6 名以下の常任委員で構成されることが義務付けられている。[77]第 63 条は、サイバーセキュリティ法の他の規定および連邦の他の法律に従

[73] サイバーセキュリティ法案 2024、第 50 条案。

[74] サイバーセキュリティ法案 2024、53 条案。

[75] サイバーセキュリティ法案 2024、52 条案。

[76] サイバーセキュリティ法案 2024、52 条 6 項案。

[77]サイバーセキュリティ法案 2024、第 61 条案。

い、CIRB は完全な裁量権を有し、その機能の遂行および権限の行使においていかなる者の指示にも従わないと定めている。

2.64 提案されている第 64 条から第 69 条で構成されるディビジョン 5 は、CIRB 議長および委員の任命条件を扱う。議長およびその他の常任委員は大臣が任命する。[78]

2.65 ディビジョン 6 は、第 64 条から第 69 条までで構成され、専門家パネル、補助スタッフ、コンサルタントを扱う。[79]専門家パネルのメンバーは、審査に協力するため、CIRB が審査の職務権限に従って任命する。[80]オーストラリア公務員の職員、または他の英連邦団体の役員もしくは職員は、CIRB を補佐するスタッフとして利用することができ、CIRB の指示に従う。[81]

2.66 提案されている第 73 条から第 77 条で構成されるディビジョン 7 は、その手続き、責任からの保護、年次報告など、CIRB に関するその他の事項を扱う。[82]

パート 6：規制権限

2.67 パート 6 は、4 つのディビジョンと提案されている第 78 条から第 83 条で構成され、民事罰規定、強制執行可能な約束、差止命令を含む規制権限を扱い、*2014* 年規制権限（標準規定）法（*Regulatory Powers (Standard Provisions) Act 2014* ）の監視、調査、執行手続の対象となる様々な民事罰やその他の違反規定を定める□[83]□パート 6 は、同法が勅許を受けた翌日から開始される。

パート 7：その他

2.68 第 84 条から第 87 条で構成されるパート 7 は、長官による上級行政官へのパート 2 の機能または権限の委譲や、 大臣の規則制定権の確立など、雑多な事項を扱う。[84]パート 7 は、本法が勅許を得た翌日から開始される。

[78] サイバーセキュリティ法案 2024、EM、90-93 [498]-[519].

[79] サイバーセキュリティ法案 2024、EM、93-95 [520]-[536].

[80] サイバーセキュリティ法案 2024、第 70 条案。

[81] サイバーセキュリティ法案 2024、第 71 条案。

[82] サイバーセキュリティ法案 2024、EM、95-99 [535]-[565].

[83] サイバーセキュリティ法案 2024、EM、99-110 [567]-[634].

[84] サイバーセキュリティ法案 2024、EM、110-113 [635]-[658].

3.情報サービスおよびその他の法改正（サイバー・セキュリティ）法案 2024

3.1 本章では、2024 年情報サービス等法改正案（サイバーセキュリティ）法案（ISA 法案）の主な施策の概要を説明する。

3.2 ISA 法案は、*2001* 年情報サービス法（IS 法）を改正し、特定のサイバーセキュリティ情報の使用と伝達に制限を設けることを提案している□[1]□ISA 法案には、サイバーセキュリティ法案 2024 に起因する一定の修正も含まれている。

3.3 ISA 法案は、サイバーセキュリティ法案 2024 のパート 4 で国家サイバーセキュリティ・コーディネー ター（NCSC）に課される限定的使用義務と同様に、オーストラリア通信総局（ASD） に「限定的使用」義務を法制化することを意図している。[2]同大臣の第 2 読会演説にある通りである：

> ISA 法案における限定的使用義務は、政府がサイバーセキュリティインシデントへの準備と対応を支援するために設立した機関に、産業界が関与し、情報を提供できることを法的に保証するものである。... 本法案における限定使用義務は、ASD が許可された目的でのみこの情報をオンシェアすることができ、オンシェアされた取得者は許可された目的でのみその情報を使用できることを明確にする。この義務は、産業界にとってのセーフハーバーではない。組織が既存の法律や規制上の義務を遵守することを免除するものではない。[3]

3.4 IS 法の改正案は、ASD が許可されたサイバーセキュリティ目的のためにのみ、限定されたサイバーセキュリティ情報をオンシェアすることを概説している。ISA 法案説明資料には以下のように記載されている：

> 産業界と ASD の間の関与と情報の流れが減少することは、ASD が包括的な国家サイバー脅威状況を維持し、タイムリーなサイバーセキュリティ技術的アドバイスと支援を提供する能力を妨げるため、オーストラリアの国家サイバーセキュリティ態勢にとって重要な脅威となる。[4]

3.5 ISA 法案は、ASD がサイバーセキュリティインシデントに関連する特定の情報（「限定的サイバーセ キュリティ情報」と呼ばれる）を伝達することができる、「許可されたサイバーセキュリティ目的」と 呼ばれる限定的な目的を規定している。ISA 法案は、ASD が、影響を受ける事業体に対す

---

[1] インテリジェンス・サービスおよびその他の法改正（サイバー・セキュリティ）法案 2024（ISA 法案）、説明資料（EM）、21 頁。

[2] トニー・バーク下院議員（芸術担当大臣、内務大臣、サイバーセキュリティ担当大臣、移民・多文化問題担当大臣、下院議長）、下院ハンサード、2024 年 10 月 9 日、47 頁。

[3] トニー・バーク下院議員（芸術担当大臣、内務大臣、サイバーセキュリティ担当大臣、移民・多文化問題担当大臣、下院議長）、下院ハンサード、2024 年 10 月 9 日、48 頁。

[4] ISA 法案、EM、3 頁。

る連邦、州または準州の法律違反（刑事犯罪を除く） を調査または執行する目的で、限定的なサイバーセキュリティ情報を伝達することを妨げる。[5]

3.6 ISA 法案はまた、特定の民事・刑事訴訟手続きにおいて、限定的なサイバーセキュリティ情報の認容性に特定の制限を設けることを意図しており、サイバーセキュリティ情報の提供は、その情報に関連する法律専門家の秘匿特権の主張に影響を与えないことを明記している。[6]

3.7 ISA 法案第 2 章では、*1982* 年情報公開法（FOI 法）を改正し、サイバーセキュリティ法案 2024 のパート 4 に規定された目的のために NCSC に提供された、または NCSC が受領した文書に対する情報公開請求の免除を含めることが提案されている。[7]

3.8 規定のより詳細な概要は以下の通りである。

スケジュール 1：特定のサイバー・セキュリティ情報の限定的利用

3.9 ISA 法案のスケジュール 1 は、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略 の主要なイニシアチブである、サイバーセキュリティインシデントに関する政府への産業界 の関与を促進することを目的としたディビジョン 1A を IS 法のパート 6 に挿入することを提案している。ISA 法案の説明文書で説明されているように、ASD に報告された情報がオンシェアされず、その後取得者により許可されたサイバーセキュリティ目的以外の理由で使用されないという保証を、法的メカニズムを通じて事業体に提供することで、産業界の関与が促進される。[8]

3.10 IS 法に新しいディビジョン 1A を挿入することは、この目的をサポートすることになる：

- 事業体またはその代表者を通じて ASD に自発的にプロバイダから提供される、または ASD が取得または作成するサイバーセキュリティ情報に関して、明確な法的義務を定める。[9]

- ASD は許可されたサイバーセキュリティ目的のためにのみ限定的なサイバーセキュリティ情報をオンシェアすることを明確にし、ASD によって限定的なサイバーセキュリティ情報がオンシェアされた場合、受信当事者がどのように限定的なサイバーセキュリティ情報を使用するかを規定する [10]

- 連邦、州、準州の裁判手続において、限定的なサイバーセキュリティ情報に対する防御を提供し、一定の例外を除き、影響を受けた事業体に対する裁判手続において、その情報が認められないようにする。[11]

---

[5] ISA 法案、EM、21 頁。

[6] ISA 法案、EM、21 頁。

[7] ISA 法案、EM、2 頁。

[8] ISA 法案、EM、2 頁。

[9] ISA 法案、EM、3 頁。

[10] ISA 法案、EM、3 頁。

[11] ISA 法案、EM、3 頁。

3.11　説明文書には次のように記されている：

> 法案のスケジュール 1 は、ASD との早期かつオープンなエンゲージメントを促進するために事業体に保証を提供することと、効果的かつ効率的な規制環境を阻害しないことによって、より広範な公共の利益を保護することの間で適切なバランスをとっている。[12]

3.12　IS 法第 41BA 条案は、サイバーセキュリティ情報が限定的使用義務の対象となる場合について概説している。これには、ディビジョン全体で使用されている重要用語である「限定的サイバーセキュリティ情報」を構成するものが含まれる。[13]

3.13　限定的なサイバーセキュリティ情報」とは、ASD によって取得または作成された、以下に関連する情報を含むと定義される：

- 発生した、または発生しつつあるサイバーセキュリティインシデント。
- サイバーセキュリティインシデントが発生する可能性がある。[14]

3.14　説明文書には次のように記されている：

> この広範な適用可能性により、悪用が発生したインシデント情報に加え、システム上の脆弱性の発見に関連する情報を保護するための限定的使用義務が認められる。[15]

3.15　提案された 41BA(2)項では、影響を受ける事業体から、または影響を受ける事業体の代理として、自発的に ASD に提供された情報、ASD の技術プログラムなどを通して影響を受ける事業体の同意を得て ASD が取得または作成した情報、または NCSC が取得し、サイバーセキュリティ法案 2024 における限定的使用義務に基づき ASD に開示された情報に対して、ディビジョンの適用が制限される。[16]

3.16　限定的なサイバーセキュリティ情報」は、特定の義務的報告義務を遵守して連邦に提供された情報、すでに公開された情報、および非識別化された情報も明確に除外する。[17]

3.17　提案された第 41BA 条(4)は、「サイバーセキュリティインシデント」を以下のように定義している：

> a.　1 つまたは複数の行為、出来事、または状況：

[12] ISA 法案、EM、4 頁。

[13] ISA 法案, EM, p. 8 [12].

[14] ISA 法案、sch 1、項目 2（41BA(1)案）。

[15] ISA 法案, EM, p. 9 [3].

[16] ISA 法案, EM, p. 8 [15].

[17] ISA 法案、sch 1、項目 2（41BA(3)案）。

i. 重要インフラ安全保障法（*Security of Critical Infrastructure Act 2018*）におけるサイバーセキュリティインシデントの意味に含まれる種類のものである。

ii. 同法におけるこの文言の意味において、コンピュータとの、またはコンピュータからの電子通信の不正な障害に関与するが、この文言はそのような通信の単なる傍受を除外しないかのようである。

b. コンピュータ、コンピュータデータまたはコンピュータプログラムにおいて、意図しないまたは予期しない脆弱性が発見され、その脆弱性が悪用された場合、(a)にいうサイバーセキュリティインシデントが発生する。[18]

3.18 提案された第 41BA 条(5)は、連邦機関、連邦執行機関、事業体および州機関の意味について規定している。これらの用語は、サイバーセキュリティ法案 2024 によって与えられる意味と同じである。[19]

3.19 提案されている IS 法第 41BB 条は、限定的なサイバーセキュリティ情報は、許可されたサイバーセキュリティ目的のためにのみ ASD によってコミュニケーションされることができると規定し、ASD による限定的なサイバーセキュリティ情報のコミュニケーションに特定の制限を課している。

3.20 提案されているサブセクション 41BB(1)は、局長および ASD のスタッフに対して、同サブセクションに規定されている 1 つ以上の許可されたサイバーセキュリティ目的のために、ASD のスタッフでない者に限定されたサイバーセキュリティ情報を伝達することのみを制限するものである□[20]□これらの目的は、サイバーセキュリティ法案 2024（第 2 章参照）に規定されている許可されたサイバーセキュリティ目的と同様であるが、IS 法（[21]）に基づく ASD の機能、および情報セキュリティ監察官の機能の遂行に関する特定の目的が追加されている。[22]

3.21 提案されたサブセクション 41BB(2)は、限定的なサイバーセキュリティ情報の民事または規制措置のための使用とコミュニケーションを制限し、ASD に自発的に提供された、または ASD によって取得もしくは準備された限定的なサイバーセキュリティ情報のみに適用される。[23]

3.22 提案されている第 41BC 条は、連邦団体、州団体または連邦法人による限定的なサイバーセキュリティ情報の二次利用および通信に同様の制限を課している。本条はまた、本条違反に対する民事罰も定めている。[24]

---

[18] ISA 法案, EM, p. 9 [19].

[19] ISA 法案, EM, p. 11 [27].

[20] ISA 法案, EM, p. 11 [29].

[21] ISA 法案、sch 1、項目 2（41BB(1)(a)案）。

[22] ISA 法案、sch 1、項目 2（41BB(1)(g)案）。

[23]ISA 法案, EM, p. 14 [42]-[43].

[24] ISA 法案, EM, p. 14 [45].

3.23 提案されている第 41BD 条は、国に対する第 41BC 条の適用に関するものであり、国にはその各能力の権利において拘束力があるが、犯罪に対して訴追される責任はないとプロバイダが規定している。提案されている第 41BD 条は、限られたサイバーセキュリティ情報の国家機関への伝達を可能にする同意メカニズムも導入している。[25]

3.24 提案された第 41BE 条は、法律専門家の秘匿特権に関するものである。41BE 条(1)は、事業体が限定的なサイバーセキュリティ情報を ASD に提供した場合、特定の訴訟手続きにおいて誰もが行うことができる法律専門家の秘匿特権の主張に影響を与えないことを明記している。[26]

3.25 提案されている第 41BF 条は、一定の例外を除き、影響を受けた事業体に対する刑事訴訟または民事訴訟において、限定的なサイバーセキュリティ情報を認めることを制限している。同条項は、ASD、連邦の団体、または国の団体が保有する限定的なサイバーセキュリティ情報は、特定の状況下では認められないことを明記している。[27]

- 提案されている第 41BF 条(1)は、第 41BF 条が適用される限定的なサイバーセキュリティ情報の種類を定めている。

- 提案されたサブセクション 41BF(2)は、虚偽または誤解を招く情報または連邦公務員に対する妨害行為を扱う限定的な例外を除き、限定的なサイバーセキュリティ情報は、連邦、州または準州の刑事手続において、影響を受けた事業体に対する証拠として認められないと規定している。28限定的なサイバーセキュリティ情報はまた、民事罰（ディビジョン 1A の民事罰規定を除く）の違反に関する民事訴訟手続き、他の連邦、州または準州の違反に関する訴訟手続きにおいても認められない。

- 準州法（コモン・ローを含む）、または連邦、州、準州の法廷における手続。29

- 提案されたサブセクション 41BF(3)は、限定的なサイバーセキュリティ情報の容認に関する制限は、オーストラリアにおけるコロニアル調査または王立委員会、あるいは連邦職員に対して要求される令状、禁止令状、差し止め命令を含む、原裁判管轄権を行使する連邦裁判所における訴訟手続きには適用されないと規定している。[30]

3.26 提案されている第 41BG 条は、ASD の局長および職員が、元職員および現職員を問わず、限定的なサイバーセキュリティ情報に関して、特定の裁判所命令に従うことを強制されることを防ぐものである。[31]

---

[25] ISA 法案、 EM, 17 [58].

[26] ISA 法案、EM、17 頁[62]。

[27] ISA 法案 EM, 18 [64].

[28] ISA 法案、 EM, 18 [66].

[29] ISA 法案、sch 1、項目 2（41BF(2)(b)-(d)案）。

[30] ISA 法案、EM, 19 [69].

[31] ISA 法案、EM, 19 [70].

3.27　提案されている第 41BH 条は、非法人である事業体に対して、許可や権利がどのように付与され行使されるか、また義務や義務がどのように課され履行されるかについて規定している。提案されたセクションはまた、ディビジョン 1A に違反した非法人に民事罰規定を適用する。[32]

スケジュール 2：情報公開法の改正

3.28　情報公開法第 7 条は、特定の個人および団体をその運用から除外している。

3.29　ISA 法案スケジュール 2 は　、サイバーセキュリティ法案 2024 の提案されたパート 4 に規定された目的のために NCSC に提供された、または NCSC が受領した文書は、情報公開法の運用から免除されると規定する、情報公開法に新しい第 7 項（2H）を挿入することを提案している。[33]

3.30　ISA 法案の説明文書にはこうある：

> *1982* 年情報公開法（*Freedom of Information Act 1982*）第 7 条に新たに（2H）項が追加され、同制度下で収集された情報に対する補完的な追加保護措置が提供される。*1982* 年情報公開法（*Freedom of Information Act 1982*）パート 4 には一連の強力な適用除外があるが、それらは完全ではなく、サイバーインシデント中に提供される可能性のあるあらゆる種類の情報を捕捉するには不十分である。事業体が、サイバーセキュリティインシデントへの対応、軽減、解決に関連する情報を、既存の適用除外に該当しないコーディネータに提供することはあり得るが、その事業体が、1982 年情報公開法に基づく関連要求を通じて情報が公開情報になることを懸念した結果、自発的な情報提供を拒否することはあり得る。
>
> ...サイバーセキュリティ法 *2024* のパート 4 に基づき取得された情報に対するこの特例の目的は、事業体がこのような条件付き免除が適用されるかどうかのアセスメントを受ける必要がなく、情報が政府によって秘密裏に取り扱われることを完全に確信できるようにすることである。[34]

[32] ISA 法案, EM, p. 19 [71].

[33] ISA 法案, EM, p. 19 [1].

[34] ISA 法案、EM、p. 20 [4]-[5]。

4.重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 2024

4.1 本 章では、重要インフラ等安全保障法改正案（対応強化・予防）2024（ERP 法案）の主要施策の概要を説明する。

4.2 ERP 法案には、主に *2018* 年重要インフラ安全保障法（SOCI 法）のほか、*1997* 年電気通信法（Telecommunications *Act*）、*1979* 年電気通信（傍受およびアクセス）法（TIA Act）、*1979* 年オーストラリア安全保障情報機構法（ASIO Act）など 、多くの改正が含まれている。

4.3 ERP 法案に含まれる改正案は、*2023-2030* 年オーストラリア・サイバーセキュリティ 戦略のシールド 4 を実施するためのものである。シールド 4 は重要インフラの保護に関するもので、2030 年までに「我々が日常的に頼っ ている重要インフラの数々が、サイバー攻撃をよりよく防ぎ、対応し、レジリエンスできなければならな い」状態にオーストラリアを置くことを目的としている。[1]

4.4 2030 年ビジョンを達成するために 、オーストラリア政府は次のことを行うとしている：

- 重要インフラ規制の範囲を明確にする
- 重要インフラのサイバーセキュリティ義務とコンプライアンスを強化する。
- ガバナンスのサイバーセキュリティを向上させる - 重要インフラに圧力をかけ、脆弱性を特定する。[2]

4.5 ERP 法案には 6 つのスケジュールが含まれている：

- スケジュール 1 は、SOCI 法における「重要インフラ資産」の定義を修正し、「ビジネス上重要なデータ」を保存または処理するデータストレージシステムを含めるものである。
- スケジュール 2 は、現在、重大なサイバーセキュリティインシデントに対応して大臣に一定の指示を出す権限を与えている SOCI 法のパート 3A を改正し、その適用範囲をサイバーセキュリティインシデントからすべての重大インシデントへと拡大するものである。
- スケジュール 3 は、SOCI 法における保護情報の定義を修正し、現行の開示と情報共有の規定を明確にするものである。

[1] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略、2023 年 11 月、38 頁。

[2] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略、2023 年 11 月、40 頁。

- 別表 4 は、「重大な欠陥」が確認された場合、内務省長官または関連する英連邦の規制当局が、関連事業体に対し、SOCI 法パート 2A がすべての重要インフラ資産に義務付けている重要インフラリスクマネジメントプログラムの変更を命じる権限を新たに導入するものである。

- スケジュール 5 は、電気通信分野の安全保障改革を SOCI 法に統合し、電気通信法から重複する条項を削除するものである。

- スケジュール 6 は、SOCI 法のパート 6A を改正し、国家的に重要なシステムの利権保有者の変更に関する報告義務を簡素化するものである。

スケジュール 1：重要インフラ資産」の定義に「データ保管システム」を含める。

4.6 SOCI 法のパート 1 第 2 節は 、同法で使用される用語の定義を定めている。現在、SOCI 法第 9 条は、資産が第 9 項(1)(a)から第 9 項(1)(f)に概説される資産の分類に含まれる場合、その資産は「重要インフラ資産」であると規定している。また、第 51 条に基づき大臣が宣言した資産、または規則で定められた資産も重要インフラ資産とすることができる。第 9(2)項はまた、第 9(1)項に列挙された資産のいずれかを、重要インフラ資産でないとして規則で規定することを認めている。

4.7 ERP 法案のスケジュール 1 は、9 項(7)を追加することで、「重要インフラ資産」の定義を修正する：データ保管システム」である。この改正案では、資産に関連して使用される「ビジネス上重要なデータ」を保管または処理する特定のデータ保管システムは、重要インフラ資産の一部とみなされる。ある資産が SOCI 法第 9 条の意味における重要インフラ資産である場合、データストレージシステムはその重要インフラ資産の一部であると判断される：

a. 重要インフラ資産の責任事業体がデータ保管システムを所有または運用している；

b. データストレージシステムが、重要インフラ資産に関連して使用されている、または使用される予定である；

c. ビジネスクリティカルなデータが、データストレージシステムに保存されているか、データストレージシステムで処理されている（他の情報もデータストレージシステムに保存されているか、データストレージシステムで処理されているかは問わない）；

d. ハザードの発生がデータ保管システムに影響を及ぼす重大なリスクがある場合、ハザードの発生が重要インフラ資産に関連する影響を及ぼす重大なリスクもある。[3]

[3] 重要インフラ等安全保障法改正案（対応強化・予防）法案 2024（ERP 法案）、sch.1、項目 3。

4.8 業務上　　重要なデータとは、SOCI 法ではすでに定義されている用語である：

a. 少なくとも 20,000 人の個人に関する個人情報（*1988* 年プライバシー法の意味における）。

b. 重要インフラ資産に関連する研究開発に関する情報。

c. 重要インフラ資産の運用に必要なシステムに関する情報。

d. 重要インフラ資産の運用に必要な情報。

e. 重要インフラ資産に関連するリスクマネジメントおよび事業継続に関する情報（どのように説明されているかは問わない）。[4]

4.9　ERP 法案の説明文書によると、データ保管システムの規準が第 9 項(7)案に盛り込まれた目的は、業務上重要な データを保管するすべての非運用システムを対象とするのではなく、脆弱性が重要インフラに関連する影 響を与える可能性のあるシステムのみを対象とすることを明確にすることである。[5]関連する影響」はすでに SOCI 法第 8 条 G で定義されており、基本的にはインシデントが資産の可用性、完全性、信頼性、または資産に関する、あるいは資産によって保持される情報の機密性に直接的または間接的に与える影響を対象としている。

4.10　説明文書では、SOCI 法第 9 項(7)の規準を満たすデータ保管システムの例を 2 つ挙げている：

- 情報技術と運用技術システム間のネットワーク分離が不十分な場合、業務上重要なデータを保管するデータ保管システム
- ネットワーク設計図、暗号化キー、アルゴリズム、運用システムコード、戦術、技術、手順などの運用データを保持するデータストレージシステム。[6]

4.11　この改正案の効果は、SOCI 法の現行パート 2（重要インフラ資産の登録）に基づき責任事業体に課され る義務、第 2A 部に基づく重要インフラリスクマネジメントプログラム、および第 2B 部に基づく通知 義務が、当該重要インフラ資産に関連する適格データストレージシステムにも及ぶことである。[7] .

4.12　別表 1 の改正は、主要な重要インフラ資産に対する責任主体が、自らが所有または運用するデータ保管システムに対する責任主体であることも明確にする。[8]責任事業体がデータストレージシステム

---

[4] *2018* 年重要インフラ安全保障法（SOCI 法）第 5 条。

[5] ERP 法案、説明資料（EM）、p.8 [19]。

[6] ERP 法案、EM、p.8 [19]。

[7] ERP 法案、sch.1、項目 4。

[8] ERP 法案、EM、p.9 [31]。

をサードパーティにアウトソーシングした場合、そのサードパーティがデータストレージシステムに責任を持つことになる。[9]

4.13 説明文書によると、この改正は「データ保管システムとビジネス上重要なデータの保護を強化する」ものである。[10]内務省は次のように定義の拡大を正当化している：

> 現在、SOCI 法は、重要インフラ資産の主要機能がデータ保存・処理である場合、データ保存・処理資産に積極的なセキュリティ義務を課している。しかし、これらの義務は、「ビジネス・クリティカル・データ」を保有する他の重要インフラ資産に関連する二次システムの適切な保護には及ばない。[11]

別表 2：社会保険労務士法第 3 条 A の改正

4.14 SOCI 法のパート　3A は、オーストラリア政府が深刻なサイバーセキュリティインシデントに対応 するための制度を定めている。サイバーセキュリティインシデントが重要インフラ資産に「関連する影響」を及ぼした、及ぼし ている、または及ぼす可能性がある場合、大臣は、インシデントに対応するために、内務省長官に対し て、当該資産に関連する事業体に対して以下の指示を 1 つ以上出す権限を与えることができる：

- 関連事業体に対し、長官に情報を提供するよう求める情報収集指示。
- 当該事業体に対し、特定の行為または事柄を行うこと、または行わないことを要求する行為指示。
- 介入要請とは、オーストラリア信号局（ASD）が「認可された機関」として、1 つまたは複数の指定された行為や事柄を行うことを要求するものである。

4.15 現行の Part 3A では、これらの措置は「重大なサイバーセキュリティインシデント」に対応する場合にのみ適用される。しかし、ERP 法案の Schedule 2 で提案されている改正案では、この制度は、深刻なサイバーセキュリティインシデントだけでなく、すべての深刻なインシデントに適用されるように拡大される。深刻なインシデント」は、SOCI 法では定義されておらず、説明文書では、通常の意味を持つように意図されていると助言されている。[12]そのため、別表 2 は、SOCI 法の第 3A 部を改正し、内務省長官が、「すべての危険」インシデントに対応して、大臣から権限を与えられた場合、情報を収集したり、事業体に対して、何かをするよう指示したり、何かをしないよう指示したりできるようにする。[13] 。

---

[9]ERP 法案、EM、p.8 [20]。

[10] ERP 法案、EM、p.7 [16]。

[11] ERP 法案、EM、p.8 [18]。

[12] ERP 法案、EM、p.13 [50]。

[13] ERP 法案、EM、p.7 [11]。

4.16　しかし、大臣が ASD に介入を要請する権限を与えることは、引き続き重大なサイバーセキュリティインシデントに限定される。[14]ERP 法案では、パラグラフ 35AB(10)(aa)を追加し、介入要請を許可する前に、大臣がインシデントが「サイバーセキュリティインシデント」であると納得しなければならないという追加要件を導入することで、これを実現している。従って、介入権の拡大は提案されておらず、現行法と同様、サイバーセキュリティインシデントに対応する場合にのみ利用可能である。

4.17　別表 2 は、個人情報の提供を指示される事業体に関するパート 3A 内の別の改正を行う。提案されている新しい第 35AB 条(9A)は、(2)(c)または(d)項（「措置指示」に関する）で言及される指示は、特定事業体に対し、当該事業体が保有する特定個人情報（*1988* 年プライバシー法の意味における）を、特定目的のために他の特定事業体に開示するよう求めることができると述べている。第 35AB 条(9B)は、大臣が *1988* 年プライバシー法を管理する大臣の同意を得なければ、この趣旨の大臣認可を与えることができないことを規定する。

4.17　別表 2 はまた、サイバーセキュリティインシデントからすべての重大インシデントへの対応体制の適用拡大を反映するため、SOCI 法にさまざまな派生的修正を加えている。

別表 3：情報の利用および開示

4.　19SOCI 法のパート 4 は、情報の収集と利用をガバナンスしている。現行法では、長官は重要インフラ資産の報告事業体または運用者に対して、特定の情報または文書の提供を求めることができる。[15]防御情報」は SOCI 法第 5 条で定義されており、現在、特に、SOCI 法に基づく権限の行使、または義務や機能の遂行の過程で人が入手した情報が含まれる。

4.20　保護された情報の記録作成、使用または開示は、特定の状況下では許可されるが、そうでない 場合は違反となる。[16]自己負罪に対する特権は、社会保障法パート 4 に基づく情報または文書の提供要求に関しては適用されない。[17]

4.21　SOCI 法に基づく現行の保護情報規定は、重要インフラを運用する民間事業体に対し、公務員に課されるのと同様の情報共有制限を適用するよう設計された。[18]しかし、説明文書によると、政府内および産業界からのフィードバックは、以下のようなものであった。

> SOCI 法は、場合によっては、政府、責任ある事業体、およびその従業員が通常の業務において 情報を使用または開示する能力、あるいは関連リスクを効果的に軽減する能力を不必要

[14] ERP Bill, EM, p. 17 [82]-[83]; ERP Bill, sch. 2, item 19.

[15] 社会保障法パート 4 パート 2（長官が情報または文書を入手する権限）。2（情報または文書を入手する長官の権限）。

[16] 社会保険法第 45 条（保護された情報の不正使用または開示の罪）。

[17] 社会保険法第 40 条

[18] ERP 法案、EM、P.23 [124]。

に制限 する可能性がある。このような制限は、リスクの高い事象や一刻を争う事象への対応を妨げる効果がある。[19]

4.22 ERP 法案のスケジュール 3 は、現行の「保護された情報」の定義を置き換え、「関連情報」のサブセットとして定義する新しいセクション 5A を導入する。[20] 。

4.23 「関連情報」には、SOCI 法に基づく権限の行使、または義務や職務の遂行の過程で、人が 入手または生成した文書や情報、または SOCI 法を遵守する目的で事業体が入手、生成、採用した情 報が含まれる。[21]提案された第 5A(3) 項(c)～(p)は、第 5A(3) 項(a)および(b)の関連情報のより一般的な定義に合致する文書または情 報の種類の既存の非網羅的なリスト（SOCI 法の「保護された情報」の定義の現行第 5 項(b)～(bl)）を事実上複製し、 SOCI 法第 32 項(2)に基づく大臣の指示に関連する文書への明確な言及を追加する。[22] 。

4.24 提案された サブセクション 5A(1)は、危害に基づくアプローチを適用する「保護される情報」の定義を新設し、「関連情報」とする。

a. その開示が国家の安全保障またはオーストラリアの防衛を脅かすか、または脅かすと合理的に予想される場合。

b. その開示がオーストラリアまたはその国民の社会的または経済的安定を損なうか、または損なうと合理的に予想される場合。

c. 商業上の機密情報を含む、または機密情報である。

d. 開示されることにより不利益を被る、または被る可能性があると合理的に予想される。

重要インフラ資産の可用性、完全性、信頼性、またはセキュリティに関わる。[23]

4.25 ERP 法案のスケジュール 3 はまた、「SOCI 法に基づくより効果的かつタイムリーな情報共有を可能にするため」に、SOCI 法パート 4 全体の開示規定を明確化する。[24]これには以下の改正が含まれる：

- 関連事業体が、資産の継続的運用に関連する、または資産に対するリスクを軽減する目的で、保護された情報を記録、使用または開示できることを明確にする；

[19] ERP 法案、EM、P.23 [125]。

[20] ERP 法案第 3 章第 8 節（5A 条項案）。

[21] ERP 法案第 3 章第 8 節（5A(3)案）。

[22] ERP 法案第 3 章第 8 節（5A(3)(m)案）。

[23] ERP 法案、sch.3、項目 8（提案された条文 5A(1)）。

[24]ERP 法案、EM、P.23 [123]。

- オーストラリア公共サービス(APS)職員」の定義と、長官が APS 職員に対し、例えば事業体への文書の電子メール送信など、職務の過程で保護情報の開示を行う権限を与えることを可能にする規定を導入する；

- 保護情報の定義に含まれる「商業上の機密情報」の定義を導入し、政府機関が商業上の機密情報をセキュリティ上の機密情報と同様に扱うことを重要インフラの所有者や運営者に安心させる。

- 長官が、加盟国、州、準州の大臣、省庁の長、またはその職員に対して、保護された情報の開示を許可する。[25]

4.26 「認可された APS 職員」は、「第 44A 条に基づく認可が有効な省内の APS 職員」と定義される。[26] 商業上の秘密情報」は以下のように定義される。

a. 企業秘密に関する情報

b. その他の情報のうち、その情報が伝達された場合に破壊されるか減少する、あるいは破壊されることが合理的に予想される商業的価値を持つもの。[27]

日程 4：重要インフラ・リスクマネジメント・プログラムの変更を要請する新たな方向性 。

4.27 SOCI 法パート 2A は、重要インフラ資産の責任事業体に対し、重要インフラリスクマネジメントプログラム（CIRMP）を策定し、遵守することを求めている。[28]

4.28 ERP 法案のスケジュール 4 は、パート 2A を改正し、1 つ以上の「重大な欠陥」が確認された場合、「関係当局者」 に責任事業体の CIRMP の変更を命じる権限を与える新しい権限（提案されている第 30 条 AI）を導入する。この改正は、重要インフラのリスクマネジメント義務を執行するために規制当局が現在利用可能な権限におけるギャップに対処することを意図している。[29]

4.29 「重大な欠陥」とは、国家安全保障、オーストラリアの防衛、またはオーストラリアもしくはその国民の社会的もしくは経済的安定性にリスクをもたらす 欠陥と定義されるであろう。30 .

[25] ERP 法案、EM、p.24 [130]。

[26] ERP 法案第 3 章第 2 節。

[27] ERP 法案第 3 章第 2 節。

[28] 社会保険法第 30AA 条、第 30AC 条、第 30AD 条 30AA、30AC および 30AD。

[29] ERP 法案、EM、35 頁[211]。

[30] ERP 法案、sch.4、項目 3（提案された条文 30AI(3)）。

4.30 「関連当局」とは、内務省長官、または内務省長官が存在する場合は、資産の安全保障に関連する機能を有す る「関連連邦規制当局」と定義される。31関連する連邦規制当局」は、すでに SOCI 法第 5 条で定義された用語であり、SOCI 法第 61 条に基づき大臣が作成する規則に明記されなければならない。

4.31 改正案では、責任事業体に対して指示を与える前に、関係当局はまず、関係当局が指示を与えること を検討している旨を記載した文書による通知を行い、特定された重大な欠陥を明記し、責任事業体に対して、 通知を受け取ってから 14 日以内に関係当局に文書による提出を行うよう求める。当該職員は、通知に応じて受領した書面による提出物、及び通知に対応して責任事業体により取られた、又は取られることが提案された行動を考慮しなければならない。32

4.32 提案された 第 30AI 条(4)は、第 30AI 条(1)に基づいて下される指示の内容に関する必須要件を規定している。説明文書によると、「この権限が適切かつ慎重な範囲内で行使されることを確実にするため」、[33] 、この提案された条項に基づく指示は、以下の要件を満たさなければならない：

- 重大な欠陥を特定する
- 責任事業体に対し、事業体の重要インフラリスクマネジメントプログラムを変更し、欠陥に対処するよう求める。
- 責任事業体がそのプログラムを変更しなければならない期間を指定する。この期間は、指示が与えられた日から少なくとも 14 日間でなければならない。

4.33 責任事業体は、第 30AI 条(1)に基づき行われた指示を遵守し、SOCI 法第 30AG 条に基づき関連する連邦規制当局または長官に提出する年次報告書に、指示の内容および対応策を含めなければならない。[34]

4.34 内務省長官は、SOCI 法第 60 条に既に規定されているその他の義務的報告要件とともに、提案されている第 30 条 AI に基づき事業体に対して当該会計年度に下された指示の件数も、大臣への定期報告書に記載しなければならない。[35]

4.35 説明書によると、以下の通りである：

> 規制当局がこのような指示を出すことができれば、CIRMP の義務が、準備、予防、低減活動を重要インフラ資産の通常業務に組み込むという意図を確実に達成するのに役立つ。[36]

---

[31] ERP 法案、sch.4、項目 3（30AI(2)案。

[32] ERP 法案 Sch.4 第 3 項（30AI(6)-(7)案）。30AI(6)-(7)）。

[33] ERP 法案、EM、37 頁[224]。

[34] ERP 法案（Sch.4）第 2 項（30AG(2)(db)案）、第 3 項（30AI(5)案）。

[35] ERP 法案、sch.4、項目 5（提案された条項 60(2)(gaa)）。

[36] ERP 法案、EM、35 頁[212]。

4.36　説明文書では、提案されている指示権限は最後の手段としてのみ使用されるべきであると付け加えている：

> この新しい小項目は、第 30AI 条に基づく指示を出すかどうかを検討する際に、規制当局が用いなければならない協調的アプローチを法律に明記したものである。すなわち、規制当局は責任ある事業体と協力してリスクに対処するよう努めるべきであり、協議が必要な結果を得られなかった場合にのみ、指示権を行使すべきである。[37]

スケジュール 5：重要な電気通信資産のセキュリティ規制

4.37　ERP 法案のスケジュール　5 は、SOCI 法に新しいパート 2D を導入し、「重要な電気通信資産に対する強化されたセキュリティ規制」を規定する。[38]

4.38 この　改正は、現在電気通信法第 14 部に含まれている電気通信分野の安全保障改革（TSSR）の要素を SOCI 法に移管するものであり、ERP 法案によって大部分が廃止されることになる。[39]
。

4.39　2022 年に行われた電気通信法第 14 部の法定見直しの中で、委員会は TSSR 制度と SOCI 法（[40]）との間の「重大なクロスオーバー」を指摘し、「TSSR の廃止または重複する義務の無効化」を求める様々な声があることを 指摘した。[41]委員会は最終的に、作業部会を設置して協議するよう勧告した：

> 改正重要インフラ安全保障法（*Security of Critical Infrastructure Act 2018*）の下で発動される可能性のある重複する安全保障義務について、発動前に合意された見解に達する。合意され、発動された場合、電気通信事業体に対する規制の重複を避けるため、*1997* 年電気通信法第 14 編の重複する義務またはその他の仕組みは廃止されるか、関連する仕組みによって無効化されるべきである。[42]

4.40　説明文書によると、別表 5 は、TSSR の現行の安全保障および関連義務を SOCI 法に「格上げ、強化、明確化」するものである。[43]これには、現在 TSSR がスパイ行為と妨害行為に焦点を当てているのを、SOCI 法に基づく「すべての危険」を含むように拡大することが含まれる。[44]

4.41　現在、電気通信法第 313 条 1A 項に含まれる「防御義務」は、通信事業者および運送サービス・プロバイダに対し、その電気通信ネットワークおよび施設を無許可の干渉または無許可のアクセスか

---

[37] ERP 法案、EM、38 頁[233]。

[38] ERP 法案第 5 章第 27 節。

[39]ERP 法案第 5 章 46 節。

[40] 国会情報・安全保障合同委員会、*1997* 年電気通信法第 *14* 条の見直し-電気通信分野の安全保障改革、2022 年 2 月、3 頁。

[41] 国会情報・安全保障合同委員会、*1997* 年電気通信法第 *14* 条の見直し-電気通信分野の安全保障改革、2022 年 2 月、49 頁。

[42] 国会情報・安全保障合同委員会、*1997* 年電気通信法第 *14* 条の見直し-電気通信分野の安全保障改革、2022 年 2 月、50 頁。

[43] ERP 法案、EM、39 頁[241]。

[44] ERP 法案、EM、39 頁[244]。

ら保護するために「最善を尽くす」ことを求めている。ERP 法案は、この義務を SOCI 法第 30EB 条に置き換え、重要な電気通信資産の責任事業体に対し、以下の目的のため、「合理的に実行可能な限り」その資産を保護することを義務付ける。

a. そして

b. ハザードの発生が資産に関連する影響を及ぼす重大なリスクがある場合、そのハザードから資産を保護すること。[45]

4.42 第 30EB 条の新たな義務の範囲となる特定の重要電気通信資産は、規則で定めることが提案されている。[46]提案されている義務には、違反した場合、1,500 罰金単位の民事罰が含まれる。[47]

4.43 SOCI 法第 30EC 条（案）は、規則が定める重要な電気通信資産の責任事業体に対し、その電気通信サービ スまたはシステム（第 30EE 条（案）に規定）に、資産を保護する義務を果たす能力に「重大な悪影響を及ぼす 可能性がある」一定の変更または変更案を、長官に通知するよう求めるものである。[48]提案された第 30ED 条は、長官に対し、通知された変更を評価し、事業体に対し以下のいずれかを助言することを求めるものである：

a. 資産に「安全保障を害するようなリスク」があり、そのリスクを排除または低減するための措置を必要とする。

b. そのようなリスクはない。

これらの通知とアセスメントの要件は、電気通信法第 314A 条と第 314B 条にある既存の要件に類似しており、これらは廃止される。[49]

4.44 SOCI 法第 30EF 条案は、電気通信法第 315A 条をほぼそのまま踏襲するもので、内務大臣は、「安全保障を害する」と大臣が見なす特定のサービスを、通信事業者または運送サービス・プロバイダ に「使用もしくは提供しない、または使用もしくは提供を中止する」よう求める指示を出すことができる。オーストラリア安全保障情報機構（ASIO）による不利な安全保障評価が、このような指示が出される前提条件となる。[50]提案されている第 30EF 条には、違反した場合の 2,000 罰金単位の民事罰が盛り込まれている。[51]また、事業体はこのような指示を遵守するために善意で行った行為について、損害賠償請求訴訟やその他の手続きに対して責任を負わないことも規定されている。[52] 。

---

[45] ERP 法案第 5 章第 27 節（30EB 条案）。

[46] ERP 法案、sch.5、項目 27（提案された条文 30EB(1)）。

[47] ERP 法案第 5 章第 27 節（30EB(2)案）。

[48] ERP 法案、sch.5、項目 27（提案された条文 30EC）。

[49]ERP 法案第 5 章 46 節。

[50]*1997* 年電気通信法 315A 条 3 項、ERP 法案 Sch.5 項 27 号（30EF 条 3 項案）。

[51] ERP 法案第 5 章第 27 節（30EF(5)案）。

[52] ERP 法案第 5 章第 27 節（第 30EF 条(6)-(7)案）。

4.45 現行の電気通信法から廃止されるその他の TSSR の構成要素-内務大臣のその他の指示決定権限、[53] 内務省長官の情報収集権限、[54] 、セキュリティ能力計画に関する要件[55] -は、SOCI 法の提案されたパート 2D には再現されていない。しかし、現行の SOCI 法のリスクマネジメント・プログラムに関する指示決定権、情報収集権、要件は、これらの規定とほぼ同等である。

4.46 別表 5 は、現行の SOCI 法年次報告書において、提案されている第 30EC 条に基づき長官に通知された件数、および提案されている第 30EF 条に基づき大臣が発行した指示の件数の報告を義務付けることを提案している。[56]

4.47 電気通信法のパート 14 から TSSR 関連セクションが削除されたことを反映し、ERP 法案の Schedule 5 には、電気通信法、TIA 法、ASIO 法の他の部分に対する結果的な改正も盛り込まれている。[57] 。

4.48 ASIO 法に関連して、ERP 法案は第 38A 条を改正し、電気通信法第 315A 条および第 315B 条への言及を削除し、SOCI 法第 30EF 条を挿入する。ASIO 法第 38A 条は、不利な、あるいは適格なセキュリティ・アセスメントが電気通信法または SOCI 法に基づく指示に関連する場合、大臣はアセスメントを受け取ってから 14 日以内に、アセスメントのコピーを添付した書面による通知を被評価者に与えなければならないと規定している。大臣は、その開示が安全保障の利益を害するような事項をアセスメントから除外しなければならない。[58]これは ASIO が行う他の不利な、あるいは適格な安全保障評価とは異なるものであり、大臣が「国家の安全保障に不可欠」であると証明した場合には、さらに通知を保留することができる。[59]

スケジュール 6：国家的に重要なシステムの宣言の通知

4.49 SOCI 法の現行のパート 6A では、内務大臣は重要インフラ資産を国家的に重要なシステム（SoNS）であると私的に宣言することができる。[60] .

4.50 SOCI 法の 52B(3)(a)項 では、ある資産が SoNS として宣言された後、大臣はその宣言から 30 日以内に、その資産に関する各報告事業体に通知しなければならないと定めている。資産の「報告事業体」とは、現在以下のいずれかと定義されている：

a. その資産の責任事業体、[61] または

---

[53] *1997* 年電気通信法 315B 条。

[54] *1997* 年電気通信法 315C-315G。

[55] *1997* 年電気通信法 314C-314E。

[56] ERP 法案第 5 章 28 節。

[57] ERP 法案、第 5 章、項目 29-59。

[58] *Australian Security Intelligence Organisation Act 1979*, s. 38A(3).

[59] *Australian Security Intelligence Organisation Act 1979*, s. 38(2)(a).

[60] 社会保険法 52B 条 1 項。

[61] 責任事業体」は、SOCI 法第 12L 条第 5 項が定める意味を有する。

b. 資産に関する直接の利害関係者である。[62]

4.51 現在、社会保険法第 52 条 D は、SoNS の報告事業体を変更する場合、長官に通知することを義務づけている。第 52D 条(4)はまた、内務省長官が第 52B 条(1)に基づく SoNS の宣言を追加報告事業体に通知することを義務づけている。

4.52 ERP 法案の Schedule 6 は、第 52B 条と第 52D 条を改正し、直接の利害関係者が報告事業体でなくなった場合、または資産に関する別の報告事業体を知った場合、長官に通知する義務を削除し、また大臣が SoNS の宣言を各直接の利害関係者に通知する義務を削除する。直接権益保有者は、現行通り、SOCI 法パート 2 の重要インフラ資産登録義務を通じて、変更を報告することが求められる。

4.53 ERP 法案の Schedule 6 の項目 4 は、パラグラフ 52B(3)(a)の「資産の報告事業体」を「資産の責任事業体」に置き換えることで、SoNS として資産を宣言した場合、大臣が直接の利害関係者に通知するという要件を削除するものである。[63]従って、大臣は資産の各報告主体に通知する必要はなくなり、代わりに資産を SoNS と宣言してから 30 日以内に資産の責任主体に通知することだけが求められることになる。

4.54 ERP 法案の Schedule 6 の第 5 項は、第 52D 条を廃止し、責任事業体が資産の責任事業体でなくなった場合に、その事業体がその事業停止から 30 日以内に長官に通知することのみを要求する新しい第 52D 条に置き換えるものである。これにより、SoNS として宣言された資産の直接権益保有者の変更について長官に通知するという既存の要件は削除されることになる。

4.55 提案された第 52 条 D 項は、責任事業体が届出義務を遵守しなかった場合、引き続き 150 ペナルティ・ユニットの民事罰を科す。SOCI 法第 52 条 D 項の改正の効果は、SoNS として宣言された資産の直接の利害関係者が変更された場 合、そのすべての事例を長官に通知するという要件を削除することである。

[62] 直接権益保有者」は第 8 項で定義され、（その事業体の関連会社とともに）資産に 10%以上の権益を保有する事業体、または、その事業体が直接または間接に資産に影響を与え、支配する立場にある権益を保有する事業体を含む。 [63]

[63]ERP 法案、EM、82 頁[560]。

5.委員会への証拠提出

5.1 本 章では、サイバーセキュリティ法制パッケージを構成する 3 つの法案に関して、委員会が受け取った証拠を要約する。

立法パッケージに関する一般的見解

5.2 参加者の間では、サイバーセキュリティ法制パッケージの根底にある意図に対する基本的な支持が強かった。[1]また、内務省による法制化に向けた協議アプローチに対する評価も広まった。

5.3 同時に 、いくつかの規定が広範に適用される可能性があること、また、その実施を支援するために、規則や内務省からのガイダンスを通じて、さらなる洗練が必要であることについて、提出者の間で共通の懸念があった。[2]また、重複する報告義務の可能性を含め、影響を受ける事業体に課されるコンプライアンスと報告負担の増加についても、幅広い懸念があった。[3]

5.4 提出者は 、新たな義務が理解され、効果的に実施されるよう、段階的な実施を支持するとともに、同省および規制当局による業界との継続的な協議および関与を強く勧めた。[4]

---

[1]例えば、Australian Industry Group, *Submission 11*, p. 1; CISO Lens, *Submission 12*, p. 5; Customer Owner Banking Association, *Submission 15*, p. 1; BSA | The Software Alliance, *Submission 20*; Australasian Higher Education Cybersecurity Services, *Submission 22*; Interactive Games & Entertainment Association, *Submission 23*; Geomastery Advisory, *Submission 24*, p. 1; Universities Australia, *Submission 25*, p. 1; Global Shield, Submission 30, p. 1; Goodcestestors Policy, *Submission 32*, p. 2; Business Council Australia, Submission 37, p. 1; Global Shield, Submission 30, p. 1; Goodcestors Policy, Submission 32, p. 2; Business Council Australia, *Submission 37*, p. 21; Universities Australia, *Submission 25*, p. 1; Global Shield, *Submission 30*, p. 1; Good Ancestors Policy, *Submission 32*, p. 2; Business Council of Australia, *Submission 37*, p. 1; Governance Institute of Australia Ltd, *Submission 42*, p. 1; Amazon Web Services, Submission 43, p.1; Amazon Web Services, *Submission 43*, p.1; Consumer Electronics Suppliers Association, *Submission 45*, p.2; Association of Superannuation Funds of Australia, *Submission 46*, p.1; Council of Small Business Organisations Australia, *Submission 48*, p.3; Tech Council of Australia, *Submission 49*, p.1; PEXA, *Submission 51*; Infoblox, *Submission 52*; Information Technology Industry Council, *Submission 54*, p. 1; Prashant Singh, Indian Australian Technology Forum, *Submission 56*; Palo Alto Networks, *Submission 57*, p. 1; Law Council of Australia, *Submission 62*, p. 5; Mr Greg Peak, *Submission 14*, p. 2.

[2]例えば、マッコーリー大学（提出書類 *4*、p.1）、DLC Legal（提出書類 *7*、p.4）、Group of Eight（提出書類 *10*、p.4）、Social Cyber Institute（提出書類 *18*、p.3）、Internet Association of Australia（提出書類 *38*、p.1）、Association of Superannuation Funds of Australia（提出書類 *46*、p.3）を参照のこと。

[3]例えば、DLC Legal, *Submission 7*, p. 4; Customer Owner Banking Association, *Submission 15*, p. 1-2; Universities Australia, *Submission 25*, p. 1; Medicines Australia, *Submission 29*; CyberCX, *Submission 41,* p. 3; Governance Institute of Australia, *Submission 42,* p. 2; Consumer Electronics Suppliers Association, *Submission 45*, p. 2 を参照のこと。

[4]例えば、DLC Legal, *Submission 7*, p. 4, 9; Australasian Higher Education Cybersecurity Services, *Submission 22*, p. 2; Universities Australia, *Submission 25*, p. 2; HackerOne, *Submission 33*, p. 2; Samsung Electronics Australia, *Submission 40*, p. 5; Council of Small Business Organisations of Australia, *Submission 48*, p. 3; Tech Council of Australia, *Submission 49*, p. 1; Eclypsium, Inc, *Submission 50*, p. 4 を参照のこと。

5.5 これらの　　一般的な見解は、本章を通してより詳細に検討される。

照会期間

5.6　立法パッケージに対する高い支持にもかかわらず　　、輸入事業者の多くは、委員会の調査期間が短かったことに懸念を表明し、重要かつ複雑な法案群に関する書面提出を準備するために、利害関係者に与えられた期間がわずか 2 週間であったことを指摘した。[5]

5.7　この懸念の一例として、全国レベルで法律専門職を代表するオーストラリア法 律審議会（Law Council of Australia）は、「協議の複雑さとフィードバック提供のための限られた時間枠」 のため、サイバーセキュリティ法制パッケージの「すべての側面について詳細なコメントを提供 することはできない」と助言した。[6]法制審議会はその提出書類の中で、時間枠について懸念を表明した：

> [T]法制審議会は、本パッケージの表決から書面提出期限まで 2 週間強の期間が与えられたことに失望している。我々は、本法案の複雑な性質を強調するものであり、高度に専門的な分野において広範な影響と結果をもたらすものである。現在の協議期間では、法律が可能な限り効果的かつ効率的に機能するよう、利害関係者と有意義でしっかりとした協議を行うことはできない。[7]

これまでの協議プロセス

5.8　サイバーセキュリティ法制パッケージは、2023-*2030* 年オーストラリア・サイバーセキュリティ　戦略に関 する 2023 年 12 月のコンサルテーション・ペーパーで予告された改革をほぼ実施するものである□[8]□このコンサルテーションペーパーは 2024 年 3 月 1 日まで提出が可能であった。[9] 同省はまた、2024 年 9 月 4 日に法律案のターゲットとなるエクスポージャードラフトを公表した。公開草案の提出期間は 2024 年 9 月 11 日に終了し、61 件の書面提出があり、2 回の非公開のバーチャルタウンホールには 200 人以上が出席した。[10]

5.9　調査参加者は　　、法案序文に先立ち内務省が行った協議プロセスには概ね満足していた。[11]業界代表者団体を含むさまざまな提出者を通じて、内務省がそのプロセスを通じて十分な協議を行っ

---

[5] 例えば、オーストラリア大学最高経営責任者ルーク・シーヒー氏（委員会ハンサード、キャンベラ、2024 年 10 月、48 頁）、ソーシャル・サイバー・インスティテュート（提出書類 *18*、8 頁）、オーストラレーシア高等教育サイバーセキュリティ・サービス（提出書類 *22*、4-5 頁）、インタラクティブ・ゲーム＆エンターテインメント協会（提出書類 *23*、3 頁）、ジオマスタリー・アドバイザリー（提出書類 *24*、2 頁）、オーストラリア水道サービス協会および水道セクター・サービス・グループ（提出書類 *36*、3 頁）、オーストラリア法評議会（提出書類 *62*、6 頁）などを参照のこと。

[6] オーストラリア法評議会、提出書類 *62*、6 頁。

[7] オーストラリア法評議会、提出書類 *62*、6 頁。

[8] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略：2023 年 12 月、立法改革コンサルテーションペーパー。

[9] サイバーセキュリティ法案 2024、説明資料（EM）、9 頁。

[10]サイバーセキュリティ法案 2024、EM、9 頁。

[11] 例えば、Akash Mittal 氏（豪州情報セキュリティ協会議長）、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、2-3 頁、Mike Bareja 氏（豪州ビジネス協会デジタルテクノロジー、AI、サイバー、未来産業担当ディレクター）、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、33 頁、Water Services Association and Australia and Higher Education Cybersecurity

たという点で一般的なコンセンサスが得られた。多くの提出者は、法律の構成や提案された実施プロセスにはまだ改善の余地があると考えたが、ほとんどの提出者は、サイバーセキュリティ法制パッケージには驚くようなものはなかったという意見で一致した。

5.10 委員会の公聴会では、多くの提出者が内務省の協議プロセスを賞賛した。例えば、サイバーセキュリティ連合は次のように述べている：

> また、現在のオーストラリア・サイバーセキュリティ戦略の策定に至るまでの産業界との協議や、今回の法制化を支える協議プロセスに関するオーストラリア政府の姿勢を称賛したい。サイバーセキュリティ連合は、政策や法律の策定に関して世界的に多くの政府と関わっているが、 オーストラリアはこの点で模範的な国である。他の政府との議論では、内務省が採用している協議や共同設計のアプローチを参考にすることが多い。[12]

5.11 Australian Institute of Company Directors (AICD)も同様に、法制化パッケージの策定にあたって取られた協議アプローチに感謝の意を表明した：

> 我々は、これらの改革に関して、内務省が産業界と緊密に協力し、協議していること、そして、エコシステムのすべての部分が協力し合わなければ、真の意味で集団的なレジリエンスを構築することはできないことを認識する「チーム・オーストラリア」のアプローチを強く求め、支持していることを改めて表明する。[13]

5.12 オーストラリア情報セキュリティ協会の会長は次のように述べている：

> 私の経験では、この部局との関係は終始良好だった。法案に盛り込まれた内容については、ドラフトが発表されたときも驚かなかった。本当によくコミュニケーションされていた。[14]

5.13 同様に、ユニバーシティーズ・オーストラリアは、政府全体の協力的なアプローチを評価した：

> 私は、政治の両側面において、この問題への関与は素晴らしいものだと感じている。特にこの委員会を通じて、超党派性が非常に高い。[15]

5.14 しかし、すべての提出者がサイバーセキュリティ法制パッケージが国会に提出されるまでの協議プロセスに満足していたわけではない。Geomastery Advisory の提出文書には次のように記されている：

Service、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、48 頁を参照のこと。33; Ms Nikki Peever, Director, Cybersecurity, Australasian Higher Education Cybersecurity Service, *Committee Hansard*, Canberra, 31 October 2024, p. 48; Water Services Association of Australia and Water Sector Services Group, *Submission 36*, p. 3.

[12] アリ・シュワルツ、サイバーセキュリティ連合コーディネーター、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、9 頁。

[13] Australian Institute of Company Directors, Head, Policy, Mr Christian Gergis, *Committee Hansard*, Canberra, 31 October 2024, p. 35.

[14] アカシ・ミッタル、オーストラリア情報セキュリティ協会議長、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、3 頁。

[15] ルーク・シーヒー（オーストラリア大学最高経営責任者）、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、48 頁。

> オーストラリアにおけるコンサルテーションは、一般的に英国や欧州連合（EU）で行なわれているコンサルテーションにはるかに及ばない。... 産業界が法案の成果を支持したからといって、その成果を達成するための方法を支持することにはならない。[16]

5.15 オーストラリア・インターネット協会は、協議に参加する機会には感謝しているが、以前の協議で提供されたすべてのフィードバックが今回の法制化パッケージで対処されているわけではないとコメントした。[17]

今後の見直しの必要性

5.16 調査参加者の中には、サイバーセキュリティ法制パッケージの構成要素を将来的に見直すべきとの意見もあった。

5.17 法制審議会は、サイバーセキュリティ法 2024 が成立した場合、3 年後に見直すべきであると勧告し、次のように述べている：

> [今回の見直しに際して［法制審議会］などから提起された問題を考慮すると、サイバーセキュリティ法案には、この枠組みが実際にどのように運用されているかを評価するため、3 年後に実施する法定見直しを盛り込むことが賢明であると考える。[18]

5.18 Macquarie Technology Group は、第 60A 条で義務付けられている *2018* 年重要インフラ安全保障法（SOCI 法）の独立レビューが既にまもなく開始される予定であることを強調した。[19]同委員会は、同委員会の提出文書で提起された事項（データストレージシステムに関連して後述）に対処するための法改正が同委員会のレビューの結果として行われない場合、必要とされる独立レビューの一環として関連する勧告を行うべきであると勧告した。[20]

5.19 SOCI 法第 60 条 B は、同法第 60 条 A に基づく独自の見直しと同様、*2021* 年安全保障法制改正（重要インフラ）法（SLACI 法）が勅許を受けた後 3 年が経過する前に見直しを開始する限り、同委員会に SOCI 法の法定見直しを実施する権限を与えている。この期間は 2024 年 12 月 2 日に満了する。

5.20 内務省は、SLACI 法および *2022* 年安全保障法制改正（重要インフラ保護）法（SLACIP 法）に関する協議の実施、進捗、結果について、SOCI 法第 60AAA 条で義務付けられている通り、委員会に定期的に報告してきたと指摘した。[21]この報告義務は、委員会が第 60B 条に基づくレビューの実施を開始するまで有効である。[22]しかし、SLACI 法および SLACIP 法に関する協議が終了

---

[16] Geomastery Advisory, *Submission 24*, p. 1.

[17] Internet Association of Australia, *Submission 38*, p. 1.

[18] ジョン・キーブズ氏（オーストラリア法審議会ビジネス法部会執行委員）、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、2 頁。

[19] マッコーリー・テクノロジー・グループ、提出書類 *31* 号、8 頁。

[20] マッコーリー・テクノロジー・グループ、提出書類 *31* 号、2 頁。

[21] 内務省提出資料 *59*、5 頁。

[22] *2018* 年重要インフラ安全保障法（*Security of Critical Infrastructure Act 2018*）第 60AAA 条(4)。

したことを受け、同省は委員会に対し、この継続的な報告義務の有用性と価値を検討するよう提案した。[23]

特定の条項に関する見解

5.21 サイバーセキュリティ法制パッケージの背後にある取り組みには大きな支持が寄せられたが、提出者からは、パッケージ内の 3 法案の以下の分野に関連して具体的なコメントが寄せられた。本章では、提出者が提起したすべての問題やコメントを取り上げるわけではないが、特定された主なテーマを反映することを目指す。

標準セキュリティ基準

5.22 サイバーセキュリティ法案 2024（Cyber Security Bill）の第 14 条は、関係大臣が「関連する接続可能な製品」のセキュリティ標準を義務付ける規則を作成できるようにするもので、これにはモノのインターネット（IoT）製品やスマートデバイスなど、インターネット接続可能な製品やネットワーク接続可能な製品が含まれる。[24]

5.23 ほとんどの　提出者は、関連する接続可能な製品に必須のセキュリ ティ標準を導入することを支持している。[25][26]例えば、CyberCX は次のように提出した：

> セキュア・バイ・デザイン標準の序文は、まず第一に、消費者向け IoT 機器の基本的な設計上の弱点を突いた攻撃からユーザーをより良く防御する効果をもたらすべき論理的な措置である。これによりオーストラリアは、他の主要市場、すなわち欧州連合（EU）や米国で行われている標準規制と歩調を合わせることになる。[27]

5.24 オーストラリア法評議会を代表するアニー・ハガー（Annie Haggar）氏は、スマートデバイスのセキュリティ標準の序文を、他の品目に関する既存の標準と比較した：

> 私は、この法案で導入される変更の中で最も重要で、最もインパクトのあるものだと考えている。チャイルドシートの標準を導入するように、オーストラリア社会の安全に最も直接的で大きな影響を与えるだろう。標準を満たさないチャイルドシートはオーストラリアでは買

[23] 内務省提出資料 *59*、5 頁。

[24] Cyber Security Bill 2024、EM、. 3; Cyber Security Bill 2024, proposed s. 13.

[25] UpGuard, *Submission 47*, p.1; CISO Lens, *Submission 12*, p.6; CyberCX, *Submission 6*, p.2; Information Technology Industry Council, *Submission 54*, p.2; Business Council of Australia, *Submission 37*, p.6; Australian Communications Consumer Action Network, *Submission 21*, p.3; Rebecca Trapani, *Submission*.

[26] Association of Superannuation Funds of Australia, *Submission 46*, p. 10; Office of Victorian Information Commissioner, *Submission 60*, p. 3; Institute for Integrated Economic Research-Australia, *Submission 1*, p. 1; DLC Legal, *Submission 7*, p. 4; Mr Mark Piddington, *Submission 26*, p. 1; HackerOne, *Submission 33*, p. 1; Samsung Electronics Australia, *Submission 40*, p. 1.

[27] CyberCX, *Submission 6*, p. 2.

えない。自転車のヘルメットも同様で、一定の標準が必要だ。これは非常に重要な措置である。[28]

5.25 オーストラリアが製品に標準規格を義務付けることについては、基本的に強い支持があったが、提出者 は、この 規定に関連する規則を制定する際には、国際標準規格を採用するよう政府に求めた。29

5.26 例えば 、オーストラリア統合経済研究所（IIER-A）は、「脅威の変化に応じて柔軟に変更できる」国際標準 を 採用することは「賢明」であるが、「複数の標準を採用するのではなく、一つの標準を設定し、その遵守を 強化することが有用であろう」と述べた。[30]同様に、BSA｜ザ・ソフトウェア・アライアンス（BSA）は、政府は「他の志を同じくする国々と乖離したアプローチを避けるためにあらゆる努力を払う」べきだと提出した。[31]Infoblox は次のように提出した：

> 国際標準に合わせることは、影響を受ける事業体にとって遵守することが有益であるだけでなく、オーストラリアが国際的な相互運用性と一貫性を維持するためにも必須である。[32]

5.27 コンシューマー・エレクトロニクス・サプライヤー・オーストラリアは、「オーストラリアの要件を主要な海外市場の要件に合わせる」ことで、「オーストラリアの特注ソリューションの必要性を最小限に抑え、技術の進歩に対する規制の将来性を確保する」 ことを勧告した。[33]

5.28 どの国際標準を採用すべきかに関して、Samsung Electronics Australia、Amazon Web Services、 IIER-A など複数の提出者は、いかなる規則策定においても、 英国の *Product Security and Telecommunications Infrastructure Act 2022* (PSTI Act)標準の 使用を支持した。[34]

5.29 同省は、PSTI 法などの国際標準に沿った規則を意図していると提出した：

> 本編に基づく規則は、ETSI EN 303 645 標準などの国際標準をモデルとして、英国の製品セキュリ ティおよび電気通信インフラ法（*Product Security and Telecommunications Infrastructure Act 2022*）などの立法的アプローチと整合させることを意図している。国

---

[28] アニー・ハガー（オーストラリア法審議会未来委員会委員）、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、2 頁。

[29] 例えば、Information Technology Industry Council, *Submission 54*, p.2、Business Council of Australia, *Submission 37*, p.6、Samsung Electronics Australia, *Submission 40*, pp.1, 3、DLC Legal, *Submission 7*, p.6、Interactive Games & Entertainment Association, *Submission 23*, p.4、Consumer Electronics Suppliers Association, *Submission 45*, p.2 を参照のこと。

[30] オーストラリア統合経済研究所（Institute for Integrated Economic Research-Australia）, *Submission 1*, p. 1.

[31] BSA｜The Software Alliance, *Submission 20*, p. 2.

[32] Infoblox, *Submission 52*, p. 4.

[33] コンシューマー・エレクトロニクス・サプライヤー・アソシエーション、*Submission 45*, p. 3.

[34] Amazon Web Services, *Submission 43*, p. 3; Samsung Electronics Australia, *Submission 40*, p. 2; Institute for Integrated Economic Research-Australia, *Submission 1*, p. 1; HackerOne, *Submission 33*, p. 1; Consumer Electronics Suppliers Association, *Submission 45*, p. 2; Information Technology Industry Group, *Submission 54,* p. 2.

際標準は固定的なものではなく、新たな技術的助言、業界や消費者の期待、技術の進歩に基づいて更新される可能性があることに留意すべきである。[35]

5.30 内務省は、「産業界と協議を続け、法の設計が目的に適合していることを確認する」ために、この措置に 1 年間の段階的導入期間を設けたと助言した。[36]しかし、より長い実施期間が必要と考える提出者もいた。[37]例えば、オーストラリア商工会議所（Australian Chamber of Commerce and Industry）は以下のように提出した：

> 同法では製品要件が大幅に変更されるため、12 ヶ月の移行期間では、事業者が開始日に確実に遵守できるようにするには不十分である。[38]

5.31 サムスン　電子オーストラリアは、サムスンを含む民生用電子機器製造事業者は通常、グローバルな 計画、設計、製造プロセスに従っており、製品によっては「一般的に少なくとも 18～24 ヶ月のリードタイ ムを要する」バリエーションがあると助言した。[39]サムスンは、PSTI 法および規制の規則と異なる場合、オーストラリアにおける新規格の開始時 期を延長する必要があることを示唆した。[40]

5.32 法制審議会の Haggar 氏は、一部のインターネット接続製品のセキュリティ標準は、ファームウェアやソフトウエアの更新によって比較的迅速にアップグレードできるだろうと示唆した。[41]しかし、輸入事業者が、新基準が開始されたときにオーストラリアで販売できなくなる可能性のある、すでに在庫として存在する製品への対処方法を検討する時間を確保することが重要であると彼女は注意を促した。[42]

5.33 また、いくつかの　提出者は、セキュリティ標準の義務化が無差別に適用された場合、 オーストラリア市場の技術再販業者やイノベーターに冷や水を浴びせる可能性があるとの 懸念を表明した。[43]例えば、Rebecca Trapani は、「準拠の負担は、豪州市場でのプレゼンス維持のメリットを上回 る可能性がある」と提出した。[44]同様に、Geomastery Advisory 社は、サイバーセキュリティ法案がセキュリティ標準を義務付けようとしていることを「行き過ぎ」とみなし、次のように提案した：

---

[35] 内務省提出資料 *59*、8 頁。

[36] ピーター・アンスティ内務省サイバー・テクノロジー安全保障政策担当第一次官補、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、30 頁。

[37] Samsung Electronics Australia, *Submission 40*, p. 4; Governance Institute of Australia, *Submission 42,* p. 4.

[38] オーストラリア商工会議所、提出書類 *5*、p. 1.

[39] Samsung Electronics Australia, *Submission 40*, p. 4.

[40] Samsung Electronics Australia, *Submission 40*, p. 4.

[41] アニー・ハガー（オーストラリア法審議会未来委員会委員）、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、8 頁。

[42] アニー・ハガー（オーストラリア法審議会未来委員会委員）、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、2、8 頁。

[43] Rebecca Trapani, *Submission 6*, pp.3-4; Geomastery Advisory, *Submission 24*, p. 3.

[44] Rebecca Trapani, *Submission 6*, pp.

過度に規制されれば、オフショア製造事業者は（すでに起きているように）単に供給を停止することが容易になり、オーストラリアの消費者から多大な利益を、産業界からは重要な部品を奪うことになるかもしれない。[45]

5.34 Tech Council of Australia は、ハードウェア製品に特化した新興企業への潜在的な悪影響を懸念した。同協議会は次のように述べた：

> 標準の適用に閾値がないため、消費者へのエクスポージャーが大きくないにもかかわらず、新機種を開発・反復している新興企業が規制負担を負う可能性がある。この負担は、成長段階の微妙な段階にあるそれらの事業がもたらすリスクに不釣り合いであろう。... 我々は、政府に対し、これらのビジネスに対する規制環境が、同等の国・地域よりも負担が重くならないようにすることを奨励する。[46]

5.35 何人かの　提出者は、サイバーセキュリティ法案パート 2 で使用されている定義が明確でない、あるいは、法律自体、あるいは施行に関する　規則や付随するガイダンスを通じて　、より洗練されたものにすることが有益であるとコメントした。

5.36 例えば　、Quokka は「製品」の定義が不明確であり、スマートデバイスとそのコンパニオンアプリの組 み合わせであることを明確にするために修正されるべきであると提出した。47Quokka のその根拠は、「ほとんどの場合、コンパニオンアプリがなければ、実際に使用可能な製品は存在しない」というものであった。48Quokka はさらに、スマートデバイスのコンパニオンアプリは「消費者のスマートフォン上の他のアプリよりもはるかに高いセキュリティリスクを持つことが多い」と提出した。49 。

5.37 サムスン　電子オーストラリアは、英国の PSTI 法規制と同様に、ノートパソコンと一部のタブレット製品が 関連する接続製品の定義から除外されることを明確にするため、「法案および/または規則、あるいは[説明資料] の中で明確化が必要である」と提出した。50

5.38 その他は　、特定の技術が規則内に明確に含まれることを懸念していた。例えば、VOICE Australia は、接続された自家用車は規則に　明示的に含ま　れるべきであると提出した□[51]□同様に、DLC Legal は、インターネットに接続された自動車はセキュリティ標準の対象となるべきだとし、次のように述べた：

> ほとんどの最新型自動車の接続機能は、他のすべての「関連接続可能な製品」と同じか、それ以上のリスクにさらされている。[51]

---

[45] Geomastery Advisory, *Submission 24*, p. 3.

[46] Tech Council of Australia, *Submission 49*, p. 1.

[47] クオッカ、提出書類 *19* 号、p.1.

[48] Quokka, *Submission 19*, p. 2.

[49] Quokka, *Submission 19*, p. 3.

[50] Samsung Electronics Australia, *Submission 40*, pp.

[51] VOICE Australia, Submission 2, pp. 1-2[51]　DLC Legal, *Submission 7*, p. 6.

5.39 内務省は、「除外に基づくアプローチ」をとり、機器のサイバーセキュリティに対処する法律がすでにある場合、それは規則上除外される可能性が高いと提出した：

> 提案されている規則の形式は、各セキュリティ標準に対する機器の適用範囲について、除外ベースのアプローチをとる。一般的に、以下のような場合、デバイスは除外される：これらのデバイスのサイバーセキュリティに適切に対処できる既存の法律がある、これらのデバイスについてより高い、または特注の標準を開発するための作業が政府全体で進行中である、または、これらのデバイスの複雑さにより、この規則の下で義務付けられると、より低い標準が満たされるリスクがある。各標準の除外機器リストは、さらに機器を除外したり、機器を標準の適用範囲に戻したりするために修正することができる。[52]

5.40 また、提出者の中には、提案されたセキュリティ標準に脆弱性開示プログラムまたはこれに類するものを含めることを特に主張する者もいた。[53]例えば、HackerOne は次のように述べている：

> オーストラリアの新しい IoT セキュリティ標準の重要な要素として脆弱性開示プログラム（VDP）の統合を強く提唱している。これは、英国の PSTI 法で取られたアプローチと同じである。[54] 。

5.41 一部の提出者は、標準がどのように施行されるかについて懸念を表明し、規制の施行を担当する他の制度との相互作用に関連する提案を行った。オーストラリア・コミュニケーション・コンシューマー・アクション・ネットワーク（Australian Communications Consumer Action Network：ACCAN）は、スマートデバイスのセキュリティ標準を施行するための対策案に関連して、いくつかの提案を行った。[55]ACCAN は、消費者が非準拠の機器に気づかない可能性を懸念し、内務省に以下を勧告した：

> 関連するコネクテッドデバイスの透明性と消費者の可視性を改善するため、コンプライアンス通知、停止通知、リコール通知の公開登録簿を設置する。[56]

5.42Rebecca Trapani と Mark Piddington の両氏は、これらの法律案がオーストラリア消費者法とどのように交差するのかについて、より大きな配慮がなされるべきであると提 出した。両氏は、セキュリティ標準の監督はオーストラリア競争・消費者委員会（ACCC）が行うべきであると提案した。[57]レベッカ・トラパニ氏はまた、「義務付けられたサイバーセキュリティ基準の実施を監督する」オンブズマンを設置すべきであると提案した。[58]

---

[52] 内務省提出資料 *59*、10 頁。

[53] HackerOne, *Submission 33*; Access Now, *Submission 53*, p. 6; Governance Institute of Australia, *Submission 42*, p. 2; Samsung Electronics Australia, *Submission 40*, p. 2.

[54] HackerOne, *Submission 33*, p. 1.

[55] オーストラリアコミュニケーション消費者行動ネットワーク、提出書類 *21*。

[56] Australian Communications Consumer Action Network, *Submission 21*, p. 6.

[57] Rebecca Trapani, *Submission 6*, p. 3; Mr Mark Piddington, *Submission 26*, p. 1.

[58] Rebecca Trapani, *Submission 6*, p. 7.

ランサムウェア報告義務

5.43　サイバーセキュリティ法案は、第 26 項(2)に基づいて策定される規則で定める特定の年間売上高 の閾値を満たす事業体に対し、サイバーセキュリティインシデントに関連してランサムウェアやサイバー恐喝による金銭または現物給付の支払いを行った場合に、内務省およびオーストラリア信号局（ASD）に報告することを義務付ける報告義務を設けることを提案している。[59]

5.44 提出者は　この取り組みを支持した。[60] しかし、報告事業体の適切な売上高閾値については見解が分かれており、報告要件によって事業者が過度の負担を強いられないようにすることについての一般的な懸念があった。

5.45　売上高の閾値は規則で規定されるため 、実際の金額はサイバーセキュリティ法案では定義されていない。しかし、サイバーセキュリティ法案の説明資料には、報告事業体にとって適切な閾値は年間売上高 300 万ドル以上であるという政府の現在の見解が示されている。[61]内務省によると、この閾値は *1988* 年プライバシー法（*Privacy Act 1988*）における現行の中小企業の定義と一致しており、規則発効時の協議の出発点として使用される。[62]

5.46 一部の　提出者、特に中小企業の代表者は、提案された基準額が低すぎると考えた。[63]オーストラリア中小企業団体協議会（COSBOA）は、「300 万ドルという閾値は、現在の環境下でビジネスの基本的な日常業務の運営に既に苦慮している中小企業の集団をあまりにも広く捕捉することになる」と提出した。[64]COSBOA は、プライバシー法の 300 万ドルの基準額は 20 年以上前の序文以来、指標化されておらず、「(オーストラリア税務局の)200 万ドルのマイクロビジネスの定義の方が参照しやすい」と述べた。[65]

5.47　一方、300 万ドルの閾値を規則で導入すること、または一部の提出者の場合は、より低い閾値を導入することを支持する意見もあった。[66]BSA は、300 万ドルの閾値を支持する理由を次のように提出した：

> ランサムウェアのデータ収集のサンプル数を増やすことは、脅威の特定などに重要であることは言うまでもない。サイバーセキュリティが単なる「大きな技術的問題」ではなく、あらゆる規模のエンタープライズに影響を与えるものであることを強調している。... また、プ

---

[59] サイバーセキュリティ法案 2024、EM、5 頁。

[60] 例えば、CISO Lens, *Submission 12*, p. 6; CyberCX, *Submission 6*, p. 2; Palo Alto Networks, *Submission 57*, p. 1; Customer Owner Banking Association, *Submission 15*, p. 1; auDA, *Submission 16*, p. 4; Australian Information Security Association, *Supplementary Submission 44.1,* p. 1 を参照のこと。

[61] サイバーセキュリティ法案、EM-添付資料 A、126 頁。

[62] 内務省提出資料 *59*、11 頁。

[63] 例えば、Customer Owner Banking Association, *Submission 15*, p.2、Council of Small Business Organisations Australia, *Submission 48*, p.1 などを参照のこと。

[64] オーストラリア中小企業団体協議会、提出書類 *48*、p.1.

[65] オーストラリア中小企業団体協議会、提出書類 *48*、p. 2.

[66] auDA, *Submission 16*, p. 4.

ライバシー法に基づく「中小企業」の定義とも一致する。これは、異なる法律間の調和を促進するものである。[67]

5.48 .au ドメイン管理局（auDA）は、最低売上高アプローチではなく、義務的義務にリスクベースアプローチを採 用することを含め、より多くの事業体を捕捉するために報告義務を拡大すべきであると考えた。これには、 診療所のような機密情報を日常的に取り扱う小規模事業者も含まれる。[68] auDA は次のように提出した：

> 中小企業はオーストラリア経済のかなりの割合を占めており、中小企業を義務から除外することは、多くの攻撃が報告されないだけでなく、悪意ある行為者にとってより魅力的なターゲットになる可能性がある。[69]

5.49 内務省は、提案された 300 万ドルの売上高基準は、受け取った「フィードバックのバランス」に基づいたものであると述べ、[70] 、その提案は以前提案されていた 1,000 万ドルという 数値から引き下げられたと助言した。[71]

5.50 ランサムウェアの報告を要求時点で義務付けるか、支払い時点でのみ義務付けるかという問題は、委員会の公聴会で詳細に議論された。[72]当初の提案では、両時点で報告を義務付ける予定であったが、利害関係者からのフィードバックや、企業に過度な報告義務を負わせることへの懸念から、内務省は支払い時のみ報告を義務付けることを選択した。内務省は次のように説明している：

> 報告されることを望む情報の種類を決定する際に、我々は、支払の下でも要求の下と同じ情報が対象となり、要求を受けてから支払を行うまでの時間は、その情報の有用性を低下させるほど重要ではないことを発見した。[73]

---

[67] BSA｜ザ・ソフトウェア・アライアンス、アジア太平洋地域シニア・ポリシー・マネージャー、シェン・ホン・タム氏、委員会ハンサード、キャンベラ、2024 年 10 月 31 日木曜日、20 頁。

[68] auDA, *Submission 16*, pp.

[69] auDA, *Submission 16*, p. 4.

[70] ハミッシュ・ハンスフォード内務省サイバー・インフラ安全保障担当副長官、委員会ハンサード、キャンベラ、2024 年 11 月 1 日（金）、35 頁。

[71] ジェシカ・ロビンソン内務省サイバーセキュリティ法担当局長、委員会ハンサード、キャンベラ、2024 年 11 月 1 日（金）、35 頁。

[72] アカシ・ミッタル（オーストラリア情報セキュリ ティ協会会長）、委員会ハンサード、キャンベラ、2024 年 10 月 31 日（木）、p.4; シェン・ホン・タム（BSA｜ザ・ソフトウェ ア・アライアンス、シニア・ポリシー・マネージャー）、 委員会ハンサード、キャンベラ、2024 年 10 月 31 日（木）、p.21 オーストラレーシア高等教育サイバーセキュリティサービス、サイバーセキュリティ担当ディレクター、ニッキー・ピーバー氏（委員会ハンサード、キャンベラ、2024 年 10 月 31 日木曜日、50 頁）。

[73] ジェシカ・ロビンソン内務省サイバーセキュリティ法担当局長、委員会ハンサード、キャンベラ、2024 年 11 月 1 日（金）、35 頁。

5.51 オーストラリア商工会議所（Australian Chamber of Commerce and Industry）[74]、このアプローチを歓迎した。[75]豪州情報セキュリティ協会は、ランサムウェア攻撃への対応に際して、組織の意思決定に影響を与えうる 要因がいくつかあることから、支払前にランサムウェア攻撃を報告することは、引き続き任意であるべき であることに同意した。[76]

5.52 委員会に提出された証拠では、追加的な報告要件の賦課と規制負担の増大が一貫して問題として挙げら れている。[77]例えば、IIER-A は規制負担を「重大な懸念」とみなし、[78] と CyberCX は、新たな報告要件を既存の義務と整合させ、ReportCyber のような既存の報告システムを活用するなどして、報告手続きを可能な限り使いやすいものにすることの重要性を強調した。可能な限り、重複する情報要求を排除し、報告の時間枠を統合すべきである。[79]

5.53 一部の提出者の間では、企業に報告義務を課すことで、今度は政府が影響を受ける事業体とサイバー脅威情報をより多く共有することを求めるべきだという意見もあった。例えば IIER-A は、サイバー脅威情報の共有は、すべての重要インフラセクターにおいて「欠けている要素」であり続けると考えた。[80]DLC Legal も同様にサイバー脅威情報の共有を支持し、「重要インフラに責任を持つすべての事業体を含めるべきであり、ひいては重要インフラ事業体間でのサイバー脅威情報の共有を義務付けるべきである」と提出した。[81]。

5.54 Customer Owned Banking Association は、ランサムウェア報告措置の採用を支持する一方で、提案されている措置が、オーストラリア健全性規制庁（APRA）によって銀行にすでに課せられている義務と重複することを懸念し、APRA が ASD および Australian Cyber Security Centre と情報を共有できるような取り決めを行うべきであるとした。[82]

5.55 高等教育セクターの提出　　者も、新たな報告義務を懸念していた。例えば、オーストラリア大学（Universities Australia）は、「この立法パッケージが示唆する追加的な報告義務は、すでに広範かつ多面的なサイバーセキュリティ報告環境に追加されるものである」と提出した。[83]マッコーリー大学も提出した：

---

[74] Department of Premier and Cabinet, Tasmanian Government, *Submission 8,* p. 2, The Group of Eight, *Submission 10,* p. 2, Cyber CX, *Submission 41,* p. 2, Association of Superannuation Funds of Australia, *Submission 46,* p. 3, Palo Alto Networks, *Submission 57,* p. 1、

[75] Australian Chamber of Commerce and Industry, *Submission 5*, p.1.

[76] Australian Information Security Association, *Supplementary Submission 44.1,* p. 1.

[77] 例えば、Institute for Integrated Economic Research-Australia, *Submission 1*, p.1、Customer Owner Banking Association, *Submission 15*, p.1、Universities Australia, *Submission 25*, p.1、Medicines Australia, *Submission 29*、Consumer Electronics Suppliers Association, *Submission 45*, p.3 を参照のこと。

[78]オーストラリア統合経済研究所、提出資料 *1*、p.1

[79]CyberCX, *Submission 41*, p. 3.

[80] オーストラリア統合経済研究所（Institute for Integrated Economic Research-Australia）, *Submission 1*, p. 1.

[81]DLC Legal, *Submission 7,* p. 4.

[82] カスタマー・オーナー銀行協会、提出書類 *16*、p. 2.

[83] Universities Australia, *Submission 25*, p. 1.

マッコーリーは、事業体がインシデント情報を連邦と共有するために、インシデントの性質に応じて、連邦の異なる機関に属する少なくとも 4 つのインシデント通知チャネルを特定した。[84]

5.56 オーストラリア保険審議会は、サイバーセキュリティ法案第 26 条を改正し、報告義務はランサムウェアやサイバー恐喝の支払いを弁済する可能性のあるサイバー保険会社には 適用されず、恐喝された事業者にのみ適用される　ことを明確にするよう勧告した。[85]

5.57 法制審議会と豪州ビジネス協会（BCA）は、提案されているランサムウェア報告制度の域外 運用から生じる潜在的な問題を特定した。提案されている第 26 条の現在の構成は、第 5 条と合わせて読むと、オーストラリアで事業を行ってい る事業体であれば、売上高の閾値を満たした場合に報告が義務付けられることになる。これは、オーストラリアでの売上高だけでなく、事業全体の売上高と連動することになり、多くのグローバルデジタルビジネスは年間売上高が 300 万ドルを超えることになる。[86]法制審議会は次のような例を示している：

> 米国（または米国の顧客）のみに限定されたサイバーインシデントに見舞われ、豪州の事業への影響がない場合でも、そのインシデントに関連して行われた身代金の支払いを報告しなければならない場合があるようだ。[87]

5.58 法制審議会は、サイバーセキュリティ法案の域外適用の根拠と「サイバーセキュリティインシデントの 多地域的背景」に関与する必要性を認めたが、「事業体のオーストラリアでの事業とサイバーセ キュリティインシデントとの間に十分な関連性」があることを確認するために法案を修正する可能性を 提案した。[88]法制審議会と BCA は、サイバーセキュリティ法案第 26 項を修正し、第 26 項(1)(c)の最後に「オーストラリアで事業を行う限りにおいて」という文言を挿入することを提案した。[89]

5.59 BCA と法制審議会は、法律専門家の秘匿特権に関しても懸念を表明しているが、これについては本章の限定的使用規定との関連で後述する。

サイバーインシデント審査会

5.60 サイバーセキュリティ法案は、オーストラリアで発生した重大なサイバーセキュリティインシデ ントについて、無過失でインシデント後のレビューを実施する明確な権限を持つ独立した諮問 団体と

---

[84] マッコーリー大学、提出書類 *4*、p. 1.

[85] オーストラリア保険審議会、提出書類 *9.1*, p. 1.

[86] オーストラリアビジネス協会（Business Council of Australia）、提出書類 *37* 号、5 頁； オーストラリア法律審議会（Law Council of Australia）、提出書類 *62* 号、13 頁。

[87] オーストラリア法評議会、提出書類 *62*、13 頁。

[88]オーストラリア法評議会、提出書類 *62*、13 頁。

[89] オーストラリア法曹協会（Law Council of Australia）、提出書類 *62* 号、13 頁； オーストラリアビジネス協会（Business Council of Australia）、提出書類 *37* 号、5 頁。

して、サイバーインシデント・レビュー委員会（CIRB）の設立を提案している。このようなレビューの後、CIRB は政府と産業界の双方に勧告を発表する。[90]

5.61 CIRB の設置、特に「無過失」方式については、基本的には広く支持されていた。[91]しかし、調査の過程で提出された証拠によると、提出者は提案されている CIRB の構成に懸念を抱いていた。[92]、CIRB の独立性と、提案されている大臣の関与、特に見直しの付託事項の決定における大臣の役割との間に矛盾があること、[93]、理事会の監督と説明責任に関する規定が不十分であることが指摘された。[94]

5.62 提案されている CIRB の構成について、法案の説明文書は次のように述べている：

> 委員会は、委員長、常任委員、専門家パネルの 3 つで構成される。また、理事会の機能と管理業務を補助するため、内務省から支援スタッフが割り当てられる。[95]
>
> 委員長は、この法律を管理する大臣によって任命され、理事会を指導し、法律内で与えられた権限に応 じて決定を下す役割を担う。委員長に欠員が生じた場合、大臣は委員長の職務を代行する委員長代行を任命することができる。
>
> 常任委員は、大臣によって任命された公務員が務める。委員長と常任委員を合わせて、理事会の中核となる。任期は、法案が成立した時点で最長 4 年と定められている。
>
> 理事会の第 3 の構成要素は、専門家パネルである。専門家パネルは、個々の審査ごとに、サイバーセキュリティ、法律、または分野ごとに高いレベルの専門知識と経験を有する業界の専門家から選ばれる。[96]

5.63 一部の　　提出者は、CIRB を公的委員と民間委員の混合で構成した方がよいと提案した。[97]例えば、Palo Alto Networks 社は、政府に対して次のように勧告した：

---

[90] サイバーセキュリティ法案、EM, p. 8.

[91] Institute for Integrated Economic Research-Australia, *Submission 1*, p. 2; .au Domain Administration Ltd (auDA), *Submission 16*, p. 5; Active Cyber Defence Alliance, *Submission 17*, p. 5; Geomastery Advisory, *Submission 24*, p. 5; Universities Australia, *Submission 25*, p. 2; Law Council of Australia, *Submission 62*, p. 15.

[92] 例えば、DLC Legal, *Submission 7,* p. 5; Active Cyber Defence Alliance, *Submission 17,* p. 5; Universities Australia, *Submission 25,* p. 2; Business Council of Australia, *Submission 37,* p. 5; CyberCX, *Submission 41,* p. 4-5; Governance Institute of Australia, *Submission 42,* p. 5; Information Technology Industry Council, *Submission 54,* p. 3; Palo Alto Networks, *Submission 57,* p. 2 を参照のこと。

[93] DLC Legal, *Submission 7*, p. 6; アクティブ・サイバーディフェンス・アライアンス, *Submission 17*, p. 4; Universities Australia, *Submission 25*, p. 2.

[94] BSA | The Software Alliance, *Submission 20*, pp.4-5; Internet Association of Australia, *Submission 38*, p. 4.

[95]サイバーセキュリティ法案、EM, p. 8.

[96] サイバーセキュリティ法案、EM, p. 8.

[97] ニッキー・ピーバー（オーストラレーシア高等教育サイバーセキュリティ・サービス、サイバーセキュリティ・ディレクタ ー）およびルーク・シーヒー（オーストラリア大学最高経営責任者）、委員会ハンサード、キャンベラ、2024 年 10 月 31 日（木）、48 頁。

サイバーセキュリティ企業やインシデント対応企業を専門家パネルに限定するのではなく、CIRB の常任メンバーとして加える。これらの企業は常任メンバーとして、複数のセクター（政府、通信、エネルギーなど）にまたがるサイバーセキュリティのリスク、準備、インシデントに関する広範かつ日常的なマネジメントから引き出されたリアルタイムの洞察を継続的に提供することができる。これらの企業の存在により、CIRB は、新たな脅威や敵が使用する進化する戦術、技術、手順（TTPs）、国際的なサイバー・ベスト・プラクティスをリードする洞察について、一貫したグローバルかつ経済全体の視点から恩恵を受けることができる。[98]

5.64CISO　　レンズは、サイバーセキュリティリスクの複雑性を理解する上で、委員長と常任委員をサポートする専門家パネルに選出される人物は、その関連領域で　豊富な経験を持つ真の専門家でなければならない、と提出した。99また、CISO レンズは、委員長、常任委員、専門家パネルの利益相反リスクをマネジメントすることは、理事会の信頼性と、民間業界が理事会のレビューの結果と勧告を受け入れる意欲を高める上で重要であるとコメントしている。100

5.65　委員会はこうした懸念を内務省に伝えたが、内務省は、CIRB の提案モデルは、産業界と政府双方のメンバーで構成される米国のサイバー安全審査委員会（Cyber Safety Review Board）からの学習に基づいていると説明した：

> 我々がここでやろうとしているのは、APS 会員となった独立専門家が関与する可能性のある理事会を構成し、理事会の一員として個人に適用される完全な免責と責任を負わせることである。つまり、事実上、「これは理事会のメンバーとしてのあなたの仕事です。アメリカの経験から学んだ重要な教訓は、ある分野では産業界がさまざまな調査において対立していることを考えると、実際には、対立していない人や利益相反の取り決めをしている人がいる特定の調査において、最大限の柔軟性を持たせるために、調査委員を急増させることができるようにするのがよいということである。そうすることで、最大限の柔軟性を持たせることができる。[101]

5.66　サイバーセキュリティ法案の説明文書によると：

> サイバーセキュリティ担当大臣は、理事会の議長および常任メンバーの任免に関連し、また個々のレビューの職務権限を承認する。それ以外の点では、理事会は独立した組織であり、その機能の遂行において、サイバーセキュリティ担当大臣を含め、いかなる個人または団体からの指示にも服さない。[102]

---

[98] Palo Alto Networks, *Submission 57*, p. 2.

[99] CISO Lens, *Submission 12*, p. 8.

[100]CISO Lens, *Submission 12*, p. 8.

[101] ハミッシュ・ハンスフォード内務省サイバー・インフラ安全保障担当副長官、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、p.26。

[102] サイバーセキュリティ法案、EM, p. 8.

5.67DLC Legal は、CIRB がサイバーセキュリティ法案のもとで独立性を与えられている一方で、レビューの職務権限について大臣の承認が必要であることは、「この独立性の社会的認識を損なうリスク」があるという懸念を表明し、多くの提出者もこれに同意した。[103]DLC Legal は、大臣承認の要件を例外的な状況に限定することを勧告した。[104]

5.68 この 懸念は、ソーシャル・サイバー・インスティテュート（Social Cyber Institute）も同じで、大臣は職務権限の設定に一切関与すべきではないか、あるいは単にレビューの開始を「通知」されるべきであると主張した。[105]と指摘している：

> CIRB がサイバーセキュリティインシデントのレビューを進めたいのに、崇高な意図であれ悪意ある意図であれ、そのレビューのための職務権限を承認しない大臣によって妨げられるというシナリオは十分に想像できる。別の大臣が、レビューが無意味になる時点まで職務権限の承認を遅らせるかもしれない。
>
> そうでなければ独立した団体の運営を妨げるような権力を大臣に与えてはならない。[106]

5.69 この 問題は法制審議会からも同様に提起されたが、法制審議会は、CIRB の常任委員および各審査を引き受ける専門家パネリストを決定する際に、大臣が考慮しなければならない事項を定めた規則の下で提供される行政ガイダンスによって対処できるのではないかと提案した：

> このような考慮事項には、任命者の独立性、提案された審査に関連する個人の知識や専門性についての満足度などが含まれる。
>
> あるいは、審査に参加する常任理事会メンバーの指名（および専門家パネル・メンバーの選任）は、理事会議長が決定する事項とすることもでき、この場合、独立性が束縛されるとの認識を回避できる可能性が高い。[107]

5.70 グループ・ オブ・エイト・オーストラリアはさらに、CIRB に関する大臣の責任について懸念を表明し、政府が支援権限を行使した場合、CIRB はサイバーセキュリティインシデントに対する政府自身の対応を審査する可能性があると指摘した。[108]

5.71 一部の 提出者は、CIRB 議長が事業体に対して文書提出を強制することを認める第 49 条案に反対した。[109]例えば、オーストラリア・インターネット協会は、提案された第 49 条の権限につい

---

[103] DLC Legal, *Submission 7*, p. 6.また、アクティブ・サイバーディフェンス・アライアンス（Active Cyber Defence Alliance）、*Submission 17*, p. 6; ソーシャル・サイバー・インスティテュート（Social Cyber Institute）、 *Submission 18*, p. 2; ニッキー・ピーバー（Ms Nikki Peever, Director, Cybersecurity, Australasian Higher Education Cybersecurity Service）、委員会ハンサード（*Committee Hansard*, Canberra, Thursday 31 October 2024, p. 49）も参照のこと。

[104] DLC Legal, *Submission 7*, p. 6.

[105] ソーシャルサイバー研究所、提出書類 *18* 号、p.2.

[106] ソーシャルサイバー研究所、提出書類 *18* 号、p.2.

[107] オーストラリア法評議会、補足提出資料 *62.1*, p. 1.

[108] Group of Eight Australia, *Submission 10*, p. 6.

[109] 例えば、BSA | The Software Alliance, *Submission 20*, p.2 を参照のこと。

て、「CIRB がこの権限を行使する前に考慮しなければならない一定の考慮事項を定める規定に従うべきである」と提出した。[110]

限定使用規定

5.72 サイバーセキュリティ法案（Cyber Security Bill）および情報サービス法改正法案（Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024）（ISA Bill）の「限定的使用」条項は、国家サイバーセキュリティ調整官（National Cyber Security Coordinator : NCSC）または ASD（それぞれ）に自発的に提供された情報に関連するもので、調査参加者からは概ね歓迎された。[111]要するに、これらの措置は、サイバーセキュリティインシデントに関連してオーストラリア企業から NCSC または ASD に提供された特定の情報は、限られた許可された目的でのみ使用および開示されることを規定し、情報を合法的に受領した二次機関による使用または開示にも同様の制限を設けるものである。

5.73 内務省は、この規定はサイバーセキュリティインシデント発生時に、政府機関への「タイムリーで十分な情報提供」に対する障壁を取り除くことを意図していると助言した：

> 事業体によっては、提供した情報が規制当局に提供され、将来の規制当局や法執行手続 きで不利な証拠として使用されることを恐れて、日常的に顧問弁護士を同伴して政府と直接関 わっており、サイバーセキュリティ・インシデントへの対応と復旧が法律問題として扱われ ている状況もある。タイムリーな情報の欠如は、政府がサイバーセキュリティインシデントに対応し、インシデントの 軽減を支援する方法を制限し、影響を受けた事業体にさらなる損害をもたらす、より深刻な結 果につながる可能性がある。[112]

5.74ASD は　　、ISA 法案についてコメントし、「産業界と政府間の豊富なサイバーセキュリティ関連情報の自由な流れを可能にする」助けとなる、高いレベルの信頼に裏打ちされたパートナーシップの重要性について議論した。[113]ASD は、事業体が技術的なサイバーセキュリティインシデント情報をタイムリーに ASD と共有することをためらったり、共有したがらない傾向が増えていることを観察しており、それは「主に ASD と共有された情報が政府の他の部署によって規制措置に利用されることを懸念しているため」であり、「オーストラリアの国家サイバーセキュリティ態勢に重大なリス

---

[110] Internet Association of Australia, *Submission 38*, p. 4.

[111] 例えば、Institute for Integrated Economic Research-Australia, *Submission 1*, p.2; Macquarie University, *Submission 4*, p.1; Department of Premier and Cabinet (Tasmania), *Submission 8*, p.2。オーストラリア産業グループ、提出書類 *11*、2 頁; CISO レンズ、提出書類 *12*、7 頁; アクティブ・サイバーディフェンス・アソシエーション、提出書類 7 頁; BSA | The Software Alliance、提出書類 *20*、2 頁; オーストラリア会社取締役協会、提出書類 *27*、3、2 頁; メディシンズ・オーストラリア、提出書類 *29*、1 頁; サイバーセキュリティ連合、提出書類 *34*、3 頁; サイバー CX、提出書類 41、4 頁 4; Governance Institute of Australia, *Submission 42*, p. 2; Australian Information Security Association, *Submission 44*, p. 3; Consumer Electronics Suppliers Association, *Submission 45*, p. 3; UpGuard, *Submission 47*, pp.2-3; Council of Small Business Organisations Australia, *Submission 48*, p. 3; Law Council of Australia, *Submission 62*, pp.14-15.

[112] 内務省提出資料 *59*、12 頁。

[113] オーストラリア通信総局（ASD）、提出書類 *61*、5 頁。

ク」をもたらしていると助言した。[114]ASD は、この規定が「オーストラリアの国家サイバーセキュリティ体制に重大なリスク」を与えると考えた：

> ASD が全オーストラリア国民にサイバーセキュリティのアドバイスと支援を提供するという役割にとって基本的に重要な情報である ASD に自発的に報告した情報が、規制措置のために利用されたり、民事訴訟で不利な証拠として使用されたりすることがないことを、産業界にさらに保証する。[115]

5.75 オーストラリア産業グループは、以下のように法案に盛り込まれた条項を支持した：

> 企業がサイバーインシデントに対処している最中には、これらの事業体との関わりが機密であり、さらなる悪影響につながらないことを確信する必要がある。[116]

5.76 AICD も同様に、同規定は「必要な情報の共有と、自発的に提供された情報が他の規制目的のために提供されることがないという企業への安心感の提供との間で適切なバランスをとっている」と考えている。[117]

5.77 他の提出者は、本規定の趣旨を支持しつつも、その趣旨に沿うには十分でない可能性を示唆した。例えば、Internet Association of Australia は、NCSC が任意情報を他機関と共有する権限が付与される状況の幅が広いため、本規定は「事業体が NCSC と情報を共有することを促すのに十分な保証を与えるものではない」と主張した。[118]同様の理由で、auDA は、提案されている限定的な使用義務は「詳細な情報を共有することへの既存のためらいを減らすことは考えにくく、すでに消極的な利害関係者とのオープンな関与を促進するという目的を達成することはほとんどない」と提出した。[119]

5.78CyberCX は 、NCSC と ASD に提供される情報の使用について、「業界の参加をより促進し、企業に不当な損害を与えかねない予期せぬ結果を回避するため」に、いくつかの追加的な制約を設けることを提案した。[120]また、電子監視法における禁止事項と同様に、情報の共有に一般的な禁止事項を適用し、対象を限定した適用除外を設けるモデルを主張した。[121]CyberCX のシニア・マネージャーであるウィリアム・ストルツ博士は、委員会に対し、組織が自発的に政府と情報を共有することで不利益を被ることがあってはならないと述べた：

> [例えば、あなたがデータセンター事業者で、非常に積極的で善良な企業市民であり、できる限り自主的に政府に報告すると決めた場合、その報告が、例えば英連邦との商業的関係に

---

[114] ASD, *Submission 61*, p. 5.

[115] ASD, *Submission 61*, p. 4.

[116] Australian Industry Group, *Submission 11*, p. 2.

[117] Australian Institute of Company Directors, *Submission 27*, p. 4.

[118]Internet Association of Australia, *Submission 38*, pp.

[119] auDA, *Submission 16*, p. 5.

[120] CyberCX, *Submission 41*, p. 4.

[121] CyberCX, *Submission 41*, p. 4.

おいてあなたに悪影響を及ぼさないこと、また、そのような洞察が政府内部で広く共有されないこと。[122]

5.79 オーストラリア退職年金基金協会(ASFA)は、「関連インシデントに関する情報が NCSC に提供された場合、規制措置や強制措置は講じられない」とする明示的な規定を勧告した。[123] 。

5.80 しかし、内務省はその提出書類の中で、限定的使用規定に基づいて提供された情報は「大半の民事訴訟ま たは刑事訴訟では」認められないが、同規定は事業体に「セーフハーバー」を提供することを意図したものでは なく、「業務、規制、または法執行機関が、影響を受けた事業体から直接情報を入手し、法制化された機能を実行するために、既存の権限を使用することを制限するものではない」と説明している。[124]

5.81 Geomastery Advisory は、この「セーフハーバー」規定の欠如を指摘し、限定的使用規定が、刑事訴追のために提供された情報の使用を妨げないことに懸念を表明した。[125]この規定は「不十分」であり、「産業界と政府との間に必要なレベルの信頼関係は生まれない」と主張している。[126] 。

5.82 The Water Services Association of Australia and the Water Sector Services Group （オーストラリア水道サービス協会と水道セクターサービスグループ）も同様に、「セーフハーバー」の欠如を懸念していた。同協会は、「機密性が高く、犯罪を誘発したり、評判に影響を与える可能性のある情報の公開に関 する制限」を求めている 。 [127]

5.83 BSA はこれとは対照的に、一般規定には概ね満足しており、[128] 、自発的に 提供された情報がほとんどの法的手続きで認められるとは考えていないと報告した。[129]しかし、BSA は、NCSC または ASD が、提供された情報を共有するために、影響を受けた事業体の同意を求め、「なぜ情報を共有しなければならないのか、また、どの特定の機関と共有しなければならないのか」を説明することを義務付けるべきであると提案した。[130]Tech Council of Australia も同様の指摘をしており、「特に州や連邦団体が関与するマルチステークホルダーシナリオでは、企業が自社のデータがどのように使用されるかを理解することが不可欠である」と主張している。[131]

5.84 ソーシャル・サイバー・インスティテュートは、限定使用の機構を「適切かつ的を射たもの」と評した。しかし、法案が「セーフハーバー」制度を創設するとの不正確な報道がなされたことを指摘

---

[122]委員会ハンサード、キャンベラ、2024 年 10 月 31 日、17 頁。

[123] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、*Submission 46*, pp.7-9.

[124] 内務省提出資料 *59*、13 頁。

[125] Geomastery Advisory, *Submission 24*, p. 3.

[126] Geomastery Advisory, *Submission 24*, p. 3.

[127] Water Services Association of Australia and Water Sector Services Group, *Submission 36*, p. 5.

[128] BSA｜ザ・ソフトウェア・アライアンス、アジア太平洋地域シニア・ポリシー・マネージャー、シェン・ホン・タム氏、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、20 頁。

[129] BSA｜ザ・ソフトウェア・アライアンス、 *Submission 20.1*, p. 1.

[130] BSA | The Software Alliance, *Submission 20*, pp.4, 5; Mr Shen Hong Tham, Senior Policy Manager, AsiaPacific, BSA | The Software Alliance, *Committee Hansard*, Canberra, 31 October 2024, pp.20-21.

[131] オーストラリア技術評議会、提出書類 *49*、p. 2.

し、同協会は、そうでないことを明確に法令に明記することと、「本法案の実施段階において、限定的使用規定をめぐる国のサイバーセキュリティに関する説明に対する大幅な教育と改善」を求めた。[132]同様に、マッコーリー大学も次のように提出した：

> これらの変更が産業界にとってどのような意味を持つかを伝え、通知の仕組みに対する信頼を築き、さまざまなセクターで全面的に採用されるようにするためには、コミュニケーションによる多大なアウトリーチ活動が必要となる。[133]

5.85 オーストラリア情報セキュリティ協会（Australian Information Security Association）の報告によると、同協会が「サイ バーセキュリティ法制パッケージのうち、最も好影響をもたらすと思われる具体的なイニシアチブはどれ か」を会員に調査したところ、限定的使用義務は「パッケージの他の構成要素に比べて最も支持されなかった」。[134]同協会はこれを、業界やメディアにおける明確性の欠如といくつかの誤った解釈によるものだとし、次のように提出した：

> セーフハーバー条項や民事罰の可能性がないため、組織はこれが何を意味するのかについてもっとよく知るべきである。この枠組みを、国家サイバーセキュリティ調整官やその他の規制団体が、サイバーインシデント中に共有された情報を、結果管理のために自社に不利になるように利用するための手段と見なすべきではない。[135]

5.86 サイバーセキュリティ法案では、「重大なサイバーセキュリティインシデント」に関連して NCSC に提供される情報と、その他のインシデントに関する情報とを区別しており、後者については許可される使用と開示がより限定されている。[136]ASUFA は、NCSC に提供される情報には、限定的な使用による保護が適用されることを「明白に」し、「重大なサイバーインシデントと非重大なサイバーインシデントの違い、およびこれらのうちどれを NCSC に報告する必要があるか」について、説明文書でさらにガイダンスを示すよう勧告した。[137]ASFA はまた、インシデントが「政府全体の対応」を必要とすると NCSC が判断できる状況をより明確にし、サードパーティーのサービスプロバイダーとの関係で法的責任がどのように機能するかについて、さらなる規制ガイダンスを求めた。[138]AICD も同様に、「情報」がどのように定義されるかを含め、この法律がどのように解釈され、実施されるかについてのガイダンスを添えるよう勧告した。[139]

5.87 ほとんどの水道事業者が州または地方政府の管理下にあることを指摘　　し、水道セクターは「管轄区域との協議・調整 義務」を盛り込むことを支持した。[140] これはサイバーセキュリティ法

---

[132] ソーシャルサイバー研究所、提出書類 *18* 号、7 頁。

[133] マッコーリー大学、提出書類 *4*、p. 1.

[134] Australian Information Security Association, *Submission 44*, p. 3.

[135] Australian Information Security Association, *Submission 44*, p. 3.

[136] サイバーセキュリティ法案 38(1), 39(2).

[137] オーストラリア退職年金基金連合（Association of Superannuation Funds of Australia）、提出書類 *46*、8 頁。

[138] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、提出書類 *46*、9 頁。

[139] Australian Institute of Company Directors, *Submission 27*, p. 5.

[140] オーストラリア水道サービス協会および水道セクターサービスグループ、提出書類 *36*、4-5 頁。

案の第 11 条案で対処されたようである。[141]タスマニア州首相・内閣府（Department of Premier and Cabinet）からの提出文書によると、提案されている第 11 条の仕組みが「実際にどのように運用されるか」について、「内務省とのさらなる関与」を歓迎するとしている。[142]

5.88 法曹会は提出書類の中で、法律専門家の秘匿特権（LPP）に関連するサイバーセキュリティ法案の限定的使用規定の潜在的な運用について懸念を示した。この懸念は、NCSC に自発的に提供された情報、および法案のランサムウェア報告義務やサイバーインシデント審査委員会に提供された情報に関連している。[143]法制審議会は、サイバーセキュリティ法案の第 31 条、第 42 条、第 57 条は、情報提供は「法律専門家の秘匿特権の主張に影響を与えない」と明確に規定しているが、LPP の対象となる情報は依然として報告可能であるという説明文書の示唆により、「混乱が生じる可能性がある」と提出した。[144]法制審議会は次のように説明している：

> LPP の適用と権利放棄は複雑であり、多くの場合、事実に固有である。この制度の下で提案されている情報の共有、特に自発的な開示に関連して、開示が情報の機密性と矛盾するとみなされ、秘匿特権の放棄に相当する可能性があるかどうかという重大な問題が生じる。[145] 。

5.89 曖昧さを取り除くため、法制審議会はサイバーセキュリティ法案を修正し、LPP の対象として特定された資料は報告義務の対象外であることを明確にし、法案に「情報の開示はその後の秘匿特権の放棄にはならない旨の明示的な記述を一貫して盛り込む」ことを勧告した。[146] 。

5.90 BCA はその提出書類の中で同様の点を指摘し、「会社による最初の開示も、その後の他の事業体への開示も、法律専門家秘匿特権の主張に影響しないという趣旨の、より明確な声明」を主張した。[147]

5.91 法制審議会はまた、本条項は「本条項とは別に、報告事業体が被告として有するいかなる権利、特権、免責にも制限や影響を与えるものではない」とする法案の小条項についての懸念を強調した。法制審議会は、これらの条項は重要ではあるが、「十分とは言えず、事業体が被告となる手続だけでなく、すべての手続を対象とする必要がある」と主張した。[148]

---

[141] サイバーセキュリティ法案の提案されている第 11 条は、情報が州（または準州）の機関に開示されるのは、情報が開示されるパートの規定がその管轄区域に適用されることについて、その州または準州の大臣が書面による明示的な同意を与えた場合に限られるとプロバイダが規定している。

[142] タスマニア州首相・内閣府（Department of Premier and Cabinet）, *Submission 8*, p. 3.

[143] オーストラリア法評議会、提出書類 *62*、6-7 頁。

[144] オーストラリア法評議会、提出書類 *62*、7 頁。

[145] オーストラリア法評議会、提出書類 *62*、8 頁。

[146] オーストラリア法評議会、提出書類 *62*、8 頁。

[147] オーストラリアビジネス協会、提出書類 *37*、p.6.

[148] オーストラリア法評議会、提出書類 *62*、8 頁。

SOCI 法改正

重要なデータ・ストレージ・システム

5.92 重要インフラ等セキュリティ法改正案（対応と予防の強化）法案 2024（ERP 法案）のスケジュール 1 は、SOCI 法の「重要インフラ資産」の定義を改正し、「データストレージシステム」を含める。データストレージシステムは、提案されている第 9 項(7)に規定されている 4 つの規準を満たす場合、重要インフラ資産の一部として扱われる。データ・ストレージ・システム」は SOCI 法や ERP 法案の定義用語ではないため、通常の意味を持つものとする。[149]

5.93 多くの提出者は、重要インフラ資産の定義をさらに明確化し、その定義にデータ保管システムを含めることを支持した□[150]□例えば、DLC Legal は、「この拡大は、重要インフラセキュリティの文脈でデータシステムの重要性が増していることを認めるものである」と述べている。[151]Telstra もこの変更案を歓迎し、「これらは、オーストラリアの重要インフラや国家安全保障に影響を与えないシステムの捕捉を防ぐ重要な制限である」と提出した。[152]

5.94 CyberCX は、SOCI 法第 9 条の改正への支持を表明し、公聴会で次のように述べた：

> 法制化の焦点は、インフラとは対照的に、これらの重要なサービスの運用に不可欠なデータとは何かということであり、したがって、重要インフラや国家重要システム事業体へのデータサービス提供に不可欠と思われるサードパーティを捕捉するという適用は、賢明なものである。[153]

5.95 しかし、提出者の中には、改正の背後にある意図を支持しつつも、さらなる明確化が必要であると考える者もいた。例えば、Australasian Higher Education Cybersecurity Services は、「データ保管システムに関する修正案は、要件の明確化に役立たない。154同様に、オーストラリア大学協会（Universities Australia）は、「大学は、SOCI 法におけるデータ保存要件の改正を実施するための支援を受ける必要がある。155

5.96 Ausgrid は ERP 法案で提案された規制改正を支持したが、「ビジネス・クリティカル・データ（business critical data）」の定義の改正案により、（SOCI 法が）対象とするデータ・ストレー

---

[149] 重要インフラ等安全保障法改正案（対応強化・予防）2024（ERP 法案）、EM、9 頁[26]。

[150] UpGuard, *Submission 47*, p. 2; BSA | The Software Alliance, *Submission 20*, p. 2; Institute for Integrated Economic Research-Australia, *Submission 1*, p. 2; DLC Legal, *Submission 7*, p. 7; Macquarie Technology Group, *Submission 31*, p. 2; Council of Small Business Organisations of Australia, *Submission 48*, p. 3.

[151] DLC Legal, *Submission 7*, p. 7.

[152] Telstra, *Submission 35*, pp.

[153] ウィリアム・ストルツ博士、サイバーCX シニアマネージャー、委員会ハンサード、2024 年 10 月 31 日、16 頁。

[154] Australian Higher Education Cybersecurity Service, *Submission 22*, p. 4.

[155] Universities Australia, *Submission 25*, p. 2.

ジ・システムの種類が拡大する可能性がある」　ため、改正によって財務上および非財務上 の影響が生じる可能性を懸念した（156 ）。

5.97　メディシンズ・オーストラリアはこう付け加えた：

> SOCI 法の改正は、医療重要インフラのサプライチェーン内の企業にコストとコンプライアンスの負担を増やし続けている。[157]

5.98　何人かの提出者は、「データ保管システム」の通常の意味に依存するのではなく、その定義を法律に盛り込むべきであるとコメントした。ソーシャル・サイバー・インスティテュートによると、定義がないことは問題であり、「重要インフラ資産に関連して使用される、考え得るあらゆる形態のデータストレージを捕捉するのに十分な広さである」という：[158]

> 例えば、データ保管システムには、ビジネスクリティカルな情報を含むサーバーやネットワークだけでなく、その資産の従業員が持つモバイルデバイスや USB ドライブも含まれる。提案されている法第 9 条(7)に含まれる閾値テストが満たされている限り、ストレージシステムは捕捉される。[159]

5.99　ASFA は別表 1 に関して、「ビジネスクリティカルなデータ」、「ハザード」、「重大なリスク」という用語が、データ保管システムの文脈でどのように適用されるかについて、追加ガイダンスを提供するよう勧告した。[160]ASFA は次のように勧告した：

> また、「ビジネス・クリティカル・データ」の定義を一律にするのではなく、業種ごとに定義することも検討すべきである。[161]

5.100 マッコーリー・テクノロジー・グループは、「ビジネスクリティカルなデータ」の定義と、政府以外の事業 体がアクセスする政府データなど、その定義に含まれる、あるいは含まれないデータの種類についても懸念を表明し た。162 。

5.101 他の提出者は、特にサードパーティが運用するデータ保管システムに関連して、重要インフラ資 産の一部であるデータ保管システムの「責任主体」が誰であるかについて曖昧になる可能性に関 する懸念を提起した。提案されているパラグラフ 9(7)(a)では、責任主体は「データストレージシステムを所有または運用」する事業体であるとプロバイダが規定している。ソーシャル・サイバー・インスティテュートの提出資料によると、重要インフラ資産ではデータの保存や処理をサードパーテ

---

[156] アウスグリッド、提出書類 *58*

[157] Medicines Australia, *Submission 29,* p. 1.

[158] ソーシャルサイバー研究所、提出書類 *18* 号、p.4.

[159]ソーシャルサイバー研究所、提出書類 *18* 号、4 頁。

[160] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、提出書類 *46*、11 頁。

[161] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、提出書類 *46*、12 頁。

[162] マッコーリー・テクノロジー・グループ、提出書類 *31* 号、2 頁。

ィに委託するのが一般的であり、誰がその責任を負うかについて契約上の争いに発展する可能性がある。[163]BCA は次のように勧告した：

> 法案では、システム（サービスとしてのクラウド・ホスティング・プラットフォームなど）がサードパーティによって提供されているが、責任事業体の資産の一部を形成している場合、「によって運営される」とは何を意味するのかを明確にすべきである。[164]

オールハザード」インシデントへの対応：結果管理の権限

5.102 現在、SOCI 法のパート 3A では、1 つ以上の重要インフラ資産に関連する影響を及ぼした、及ぼしている、または及ぼす可能性のある深刻なサイバーセキュリティインシデントに対して、 大臣が重要インフラ資産の責任事業体に対して、情報提供や行動をとるよう指示を与える権限 を付与することができる。

5.103 ERP 法案で提案されている改正案は、サイバーセキュリティインシデントだけでなく、あらゆる重大インシデントに対応できるよう、Part 3A の情報収集・行動指示権限の適用範囲を拡大するものである。これは、重要インフラのリスクマネジメントに対する「オールハザード」アプローチへの内務省の移行を反映したものである。[165] 。

5.104 ERP 法案の説明文書によると

> 別表 2】に含まれる改正の目的は、SOCI 法第 3A 部にある既存の政府支援の枠組みを通じて、複数の資産に関わるインシデントとその結果の管理を促進することである。対象となるインシデントは、重要インフラ資産の可用性、完全性、信頼性に影響を与える限り、自然または人為的なものである。これには、サイバーハザードや情報ハザード、物理的ハザードや自然ハザード、人的ハザード、サプライチェーンハザードなど、あらゆるタイプのハザードによるインシデントが含まれる。[166]

5.105 多くの提出者は、サイバーセキュリティインシデントだけでなく、すべてのインシデントを含む結果管理権限の拡大を基本的に支持することを表明した。[167]

---

[163] ソーシャルサイバー研究所、提出書類 *18* 号、4 頁。

[164] オーストラリアビジネス協会、提出書類 *37*、p.4.

[165] 内務省提出資料 *59*、23 頁。

[166] ERP 法案、EM、p.11 [38]。

[167] Department of Premier and Cabinet (Tasmania), *Submission 8*; CyberCX, *Submission 41*, p. 6; Social Cyber Institute, *Submission 18*, p. 5; CISO Lens, *Submission 12*, p. 9; DLC Legal, *Submission 7*, p. 7; Global Shield, *Submission 30*, pp.

5.106 しかし、これらの改正の意図に対する支持にもかかわらず、AICD、[168] the Governance Institute of Australia、[169] the BCA、[170] ASFA、[171] およびその他数社[172] を含む多くの提出者が、拡大された権限の広範な性質について懸念を表明した。

5.107 何人かの提出者は、権限が例外的な状況でのみ行使されることをより明確にすべきだと勧告した。[173]AICD は、結果管理権限が「非常に危機的な状況」で展開される最後の手段であるという政策意図にもかかわらず、現在の権限の枠組みは「ほとんど自由」であると提出した。[174]AICD は、拡大された結果管理権限の目的と使用方法について、追加的な実例も含め、説明文書でさらに詳細な情報を提供するよう勧告した。[175]

5.108 BCA は、いかなる指示も比例的であるべきであり、対処しようとするインシデントに適合させるべきであると勧告した。[176]

5.109 内務省は、ERP 法案の Schedule 2 は、「権限の範囲と目的を限定するために既存の Part 3A の枠組みが適用されることを保証する」ことで、これらの問題に対する利害関係者のフィードバックを反映している、と提出した。[177]同省は提出した：

> 州、準州、連邦の既存の規制制度では現実的かつ効果的な対応が不可能であり、事業体がインシデントに対応するためのあらゆる合理的な手段を講じる意思がないか、講じることができないと大臣が納得しない限り、この権限は使用できないため、最終手段であることに変わりはない。[178]

5.110 また、ERP 法案には再現されていない説明文書の文言についても懸念があった。AICD は、説明文書では「マルチアセット」インシデントで権限が活用されるとしているが、ERP 法案の草案では「権限の使用は複数の重要資産を対象とするインシデントに限定されていない」と提出した。[179]同様に、グループ・オブ・エイトも、ERP 法案では「マルチアセットインシデント」という用語は使用

---

[168] AICD, *Submission 27*, p. 8.

[169] オーストラリア・ガバナンス機構、提出書類 *42* 号、7 頁。

[170] オーストラリアビジネス協会、提出書類 *37*、p.4.

[171] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、提出書類 *46*、13 頁。

[172] Social Cyber Institute, *Submission 18*, p. 5; auDA, *Submission 16*, p. 6; Group of Eight, *Submission 10*, p. 2; Institute for Integrated Economic Research-Australia, *Submission 1*, p. 2; Internet Association of Australia, *Submission 38*, p. 2.

[173] オーストラリア・ガバナンス機構、提出書類 *42* 号、7 頁; タスマニア州首相・内閣府、提出書類 *8* 号、3 頁; グループ・オブ・エイト、提出書類 *10* 号、5 頁; オーストラリアビジネス協会、提出書類 *37* 号、4 頁; auDA、提出書類 *16* 号、6 頁。

[174] Australian Institute of Company Directors, *Submission 27*, p. 8.

[175] Australian Institute of Company Directors, *Submission 27*, p. 8; *Committee Hansard*, 31 October 2024, p. 33.

[176] オーストラリアビジネス協会、提出書類 *37*、p.4.

[177]内務省提出資料 *59*、18 頁。

[178] 内務省提出資料 *59*、18 頁。

[179] Australian Institute of Company Directors, *Submission 27*, p. 8.

されておらず、「（結果管理権限が）主に「マルチアセットインシデント」の管理に対処することを意図しているかどうかについては、さらなる限定が必要かもしれない」[180] 。

5.111 The Internet Association of Australia は、「インシデント」という用語が ERP 法案で定義されていないため、 「このような「インシデント」が発生した場合に、どのような状況で長官または大臣が特定の権限を発動 できるのかが不明確」であることを懸念している。[181]また、オーストラリア・インターネット協会は、ERP 法案で使用されている「重大インシデント」と「インシデント」の区別が明確でないため、さらなる混乱を招きかねないとの懸念を示した。[182]

5.112 何人かの提出者は、行動指示が、財務的、法的な影響を含め、責任主体に重大な影響を及ぼす可 能性があると述べた。[183]BCA は、ERP 法案は、責任事業体が明示的な指示を実行した結果、否定的な結果が発生した場合の 責任の取り決めを明確にすべきであると提出した。[184]BCA は、このような指示を出す前に、以下の点を明確に考慮すべきであると勧告した：

- その方向性を実施する際に事業体に課されるコスト負担と、よりコスト負担の少ない、同様の結果を達成する代替措置があるかどうか、
- 将来の商業的実行可能性
- 短期的な方向性が永続的な影響を及ぼすことはない。[185]

5.113 同様に、オーストラリア政府ガバナンス協会（Governance Institute of Australia）は、同協会の会員が「自由裁量がなく、広範囲に及ぶ可能性がある」ディレクション権限の範囲を懸念しているとし、次のように提出した：

> 政府またはガバナンスの裁量で重要インフラ事業体の操業を停止させる指示は、事業体にとって非常 にコストがかかる可能性があり、極めて例外的な災害シナリオにおいて行使されるべきであ るため、実際には問題があるかもしれない。事業体が長期にわたって操業停止となった場合、取締役は会社法 588G 条に基づき、事業体が支払能力を維持できるようにする責任を負う。事業の支払能力を脅かす可能性のある政府のガバナンスが、このシナリオの下で取締役の義務とどのように関係するかは明らかではない。[186]

5.114 サイバーセキュリティ連合は、これらの権限が「影響を受けていない事業体が、最初に影響を受けた事業体のセキュリティの欠点に基づいてセキュリティ態勢を変更する」よう指示するために使用

---

[180] Group of Eight, *Submission 10*, p.5（強調は省略）。

[181] Internet Association of Australia, *Submission 38*, p. 2.

[182] Internet Association of Australia, *Submission 38*, p. 2.

[183] CISO Lens, *Submission 12*, p. 9; Insurance Council of Australia, *Submission 9: Attachment 1*, p. 2; Cybersecurity Coalition, *Submission 34*.

[184] オーストラリアビジネス協会、提出書類 *37*、p.4.

[185] オーストラリアビジネス協会、提出書類 *37*、p.4.

[186] オーストラリア・ガバナンス機構、提出書類 *42* 号、7 頁。

される可能性があることを懸念しており、「ほとんどの状況において、事業体はリスクに関する判断を下し、自らのネットワークを管理するのが最も適切である」と述べている。[187] 。

5.115 内務省は、利害関係者からの上記のような意見を考慮し、これらの権限が実際にどのように使われるかを導くための方針と手続きの準備に取り組んでいると提出した。[188]

5.116 [189]ガバナンス・インスティテュート・オブ・オーストラリア（The Governance Institute of Australia）[190] 、 情報技術産業協議会（the Information Technology Industry Council）[191] 、サイバーセキュリティ連合（the Cybersecurity Coalition）[192] 、いくつかの提出者は、結果管理権限の使用に対する監視の欠如について懸念を表明した。例えば、BSA は、「新たな広範な権限を導入しない限りにおいて、本修正案を支持する」[193] が、「SOCI 法 Part 3A に基づく広範な権限の行使に対する独立した監視メカニズムが欠如していることを懸念している」と提出した。[194]BSA は次のように助言した：

> SOCI 法はセーフガードをプロバイダとして提供してはいるが、権限を行使する前に関連大臣が政府内および影響を受ける事業体に協議することを義務付けているに過ぎない。そのため、これらの広範な権限には、潜在的な悪用を抑止するための独立したチェック機能はない。また、影響を受ける事業体がこれらの権限の行使に異議を申し立てる手段もない。一般的な問題として、たとえ国家安全保障のためであっても、広範な権限を導入する政策は、事業体の製品やサービスに影響を及ぼす場合、利用者の信頼を損なう可能性がある。したがって、これらの権限は厳格なチェックとバランスに従うべきである。[195]

5.117 同様に、Palo Alto Networks は、SOCI 法の「パート 3A のメリットレビューの除外について懸念」 を抱いていると提出した。[196]Palo Alto Networks は次のように述べている：

> 提案されている結果管理権限の幅広さと特殊性を考慮し、我々は引き続き、*1977* 年行政決定（司法審査）法による立法化された不服申し立てと審査権を提唱する。[197]

5.118 内務省はパート 3A の監督権や上訴権については直接触れなかったが、提出書類の中で社会保障法のその他の保護措置を強調している：

---

[187] サイバーセキュリティ連合、提出書類 *34*、6-7 頁。この見解は auDA も共有している（*Submission 16*, p. 6）。

[188] 内務省提出資料 *59*、18 頁。

[189] オーストラリア・ガバナンス機構、提出書類 *42*、8 頁。

[190] DLC Legal, *Submission 7*, p. 8.

[191] 情報技術産業協会、提出資料 *54*、p.1.

[192] サイバーセキュリティ連合、提出書類 *34*、7 頁。

[193] BSA｜The Software Alliance, *Submission 20*, p. 6.

[194] BSA｜The Software Alliance, *Submission 20*, p. 2.

[195] BSA｜ザ・ソフトウェア・アライアンス、アジア太平洋地域シニア・ポリシー・マネージャー、シェン・ホン・タム氏、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、19 頁。

[196] Palo Alto Networks, *Submission 57*, p. 3.

[197] Palo Alto Networks, *Submission 57*, p. 3.

> SOCI 法の既存の保護措置に加え、行動指針がプライバシー法で定義される個人情報の開示を必要とする場 合、プライバシー法を管理する大臣は同意しなければならない。[198] …
>
> 同省は引き続き、SOCI 法の運用について、議会と国民に透明性と説明責任を提供することに全力を尽くす。第 3A 部に基づいて下された大臣認可のコピーは、認可後 48 時間以内に情報・安全保障監察総監にプロバイダされなければならない。さらに SOCI 法第 60 条に基づき、長官は国会に提出するため、第 3A 部に基づく認可を含む各会計年度の SOCI 法の運用に関する報告書を大臣に提出しなければならない。[199]

SOCI 法パート 4 情報共有規定

5.119 ERP 法案の別表 3 に含まれる SOCI 法パート 4 の改正案は、SOCI 法における開示規定を明確にすることを意図している。

5.120 SOCI 法の下での情報共有の明確化と、商業データに対するより大きな防御の導入については、基本的な 支持が得られた。[200]例えば、Department of Premier and Cabinet（タスマニア州）は以下のように提出した：

> *2018* 年重要インフラ安全保障法（Cth）における保護された情報の使用と開示に関する不明瞭な規定が情報共有に消極的な姿勢を生み、協力と相互運用性を低下させていると指摘し、特定の目的での情報共有に関する保証を提供する動きを支持する。[201]

5.121 しかし、SOCI 法第 4 条に基づく保護情報の開示には、サイバーセキュリティ法案によって導入されようとしているのと同じように、限定的な使用義務を課すべきだという意見もあった。ガバナンス機構（The Governance Institute of Australia）が提出した：

> 政府事業体間の情報共有を可能にするために、SOCI 法に定義される保護情報の開示を許可する場合、当該事業体は、対象となる事象に関連する当該情報の共有に関連する限定的使用義務を行使することも要求すべきである。[202]

5.122 タスマニア州首相・内閣府（Department of Premier and Cabinet: Tasmania）は、情報開示の規定 に緊急事態管理が含まれることを支持する一方、次のように述べた、

---

[198] 内務省提出資料 *59*、18 頁。

[199] 内務省提出資料 *59*、18-19 頁。

[200] Amazon Web Services, *Submission 43*; Department of Premier and Cabinet (Tasmania), *Submission 8*, p. 4; CyberCX, *Submission 41*, p. 6; Group of Eight, *Submission 10*, p. 6; Institute for Integrated Economic Research-Australia, *Submission 1*, p. 2; DLC Legal, *Submission 7*, p. 8.

[201]タスマニア州首相・内閣府（Department of Premier and Cabinet）, *Submission 8*, p. 4.

[202] オーストラリア・ガバナンス機構、提出書類 *42* 号、7 頁。

[政府は政府全体の重要インフラ政策に責任を負っており、状況によっては緊急時の政策機能にも責任を負っているため、これらの規定をファースト・ミニスターにも拡大すべきである。[203]

5.123 Amazon Web Services は、一部の保護情報の潜在的な機微性が高いため、「保護情報」を受領する者は、保護セキュリティポリシーフレームワーク（PSPF）の下で SECRET に分類される情報の取り扱い要件に見合ったレベルでその情報を取り扱うことを要求されるべきだと提出した。[204]そのために、Amazon Web Services は以下のことを勧告している：

本規則は、政府による保護情報の適切な取扱いに関する要件を、データ消去の期限を確認するデータライフサイクルを含む関連する詳細とともに明示する。[205]

5.124 ASFA は、使用されている用語が「広範であり、無数の解釈の余地がある」と指摘した上で、「（権限を与えられた APS 職員が）その他の「保護された情報」を開示できる正確な状況を概説する詳細な規則とガイダンスを設けるべきである」と勧告した（[206]）。

5.125 ビクトリア州情報コミッショナー事務所は、ERP 法案と現行の SOCI 法で定義された用語である「保護された情報」と、PSPF セキュリティ分類システムで使用されている防御の定義との「混同の可能性」を懸念していると提出した[207]。

5.126 内務省は、「これらの規定は、危害に基づくテストの適用方法、および保護された情報が開示される場合について、利害関係者が理解できるようにガイダンス資料によってサポートされる」と提出した。[208]

5.127 ERP 法案は、プライバシー法を管理する大臣の許可を得て、特定の状況において SOCI 法に基づく個人情報の共有を大臣が指示できるようにすることを提案している。アクセス・ナウが提出した：

我々は、オーストラリア情報コミッショナー事務局（Office of Australian Information Commissioner）が、個人情報の開示を求めるあらゆる指示に関するものを含め、SOCI 法とプライバシー法の相互作用に関するガイダンスの作成に関与することを勧告する。[209]

5.128 多くの提出者は、SOCI 法に基づき取得した保護情報を他の政府機関と共有する前に、影響を受ける事業体の同意を求めるべきであると勧告した。BSA が提出した：

BSA は、保護された情報を共有する前に、内務長官の認可を必要とすることを支持するが、さらに、内務長官は、他の政府機関と情報を共有するために、影響を受ける事業体の同意を

---

[203] タスマニア州首相・内閣府（Department of Premier and Cabinet）, *Submission 8*, p. 4.

[204] Amazon Web Services, *Submission 43*, p. 2.

[205] Amazon Web Services, *Submission 43*, p. 2.

[206] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、提出書類 *46*、13 頁。

[207] ビクトリア州情報コミッショナー事務所、提出書類 *60*、p.2。

[208]内務省提出資料 *59*、20 頁。

[209] Access Now, *Submission 53*, p. 7.

求め、その過程で、影響を受ける事業体に対して、なぜ情報を共有しなければならないのか、どの政府機関と共有するのかを説明することを勧告する。[210]

5.129 また、提出者の中には、保護された情報の取得と共有に関して、大臣と長官にもっと透明性を求めるべきだという意見もあった。アクセス・ナウは、情報収集の指示と個人の権利の透明性に関する勧告を行った。政府は、これらの権限の行使について、行使されたことを認めるだけでなく、そのような指示が人々のプライバシーやその他の権利に与える影響について声明を出すよう求められるべきだと考えた。[211]

5.130 アクセス・ナウはまた、人々の個人情報が関係する場合、そのような情報を収集する認可機関に対し て、救済または是正を求める専用の権利を持つべきであると提出した。米国のサイバーセキュリティ・インフラセキュリティ庁（CISA）は、CISA 内のプライバシーポリシーの遵守を確保し、救済や是正に関連するガイダンスを個人に提供するために、プライバシー局を設置している。[212]今すぐアクセスすることをお勧めする：

> 個人情報保護法（[213]）に基づき、プライバシー侵害や個人情報の開示に起因する損害が発生した場合、人々が明確で利用しやすい救済手段を持つことを勧告する。

重要インフラのリスクマネジメント・プログラムに対する指示権限

5.131 ERP 法案は、SOCI 法の第 2A 部を改正し、重大な欠陥が特定された場合、「関係当局者」に責任事業体の重要インフラリスクマネジメントプログラム（CIRMP）の変更を命じる権限を与える新 たな権限を導入することを提案している。重大な欠陥」という用語は、提案されている第 30AI 条(3)項において、重大なリスクをもたらす欠陥と定義される：

a. 国家安全保障

b. オーストラリアの防衛

c. オーストラリアまたはその国民の社会的または経済的安定に寄与する。

5.132 内務省によると、現在、規制当局がリスクマネジメントプログラムに重大な欠陥があると識別した場合、裁判以外にそのプログラムを是正する権限はない。[214]今回提案された権限は、関係当局が CIRMP の是正を指示できるようにすることで、SOCI 法のこのギャップに対処することを意図している。

---

[210] BSA｜ザ・ソフトウェア・アライアンス、投稿 *20*、2-3 頁。

[211] Access Now, *Submission 53*, p. 7. [212]

[212]Access Now, *Submission 53*, p. 7.

[213] Access Now, *Submission 53*, p. 8.

[214] 内務省提出資料 *59*、20 頁。

5.133 提案されている権限には、関係当局が CIRMP を変更する指示を出す前に、いくつかの前提 条件が含まれている。関係当局はまず責任ある事業体と協議し、その協議プロセスに応じて提出された 書面や行動を考慮しなければならない。[215]内務省によると

> これらのセーフガードは、事業体が著しく、あるいは故意に義務を遵守していないような稀な状況において、この権限が最後の手段として留保されることを保証するものであり、必要な場合に政府が介入できるようにするものである。[216]

5.134 ほとんどの場合、提出された意見書はこの修正案を支持するものであったが、CIRMP の実施と将来的な欠陥への対処に関しては、ガバナンスが継続的な協議と教育に関与し続ける必要性を強調した。[217]

5.135 ガバナンス協会（The Governance Institute of Australia）は、同協会のメンバーに対し、「コンプライアンスと執行 は最後の手段として、責任ある事業体に対する継続的な教育と関与に取り組む規制姿勢の保守を奨励す る」とし、このような方向性は「重大かつ重大な欠陥」が確認された「例外的な状況」においてのみ 行われるべきであると提出した。[218]

5.136 内務省は、責任事業体の CIRMP の欠陥を是正するために、協議的なアプローチを取るつもりであると提出した：

> 可能な限り、【サイバー・インフラ・セキュリティセンター】は産業界と協力し、規制対象事業体がリスクを理解し、効果的にマネジメントできるよう努める。[219]

5.137 また、「重大な欠陥」の定義が不十分であったり、定義が広すぎるという懸念を表明した提出者もいた。[220]例えば、ASFA は次のように勧告している：

> 重大な欠陥」を構成するような状況の例について、さらなるガイダンスを提供する必要がある。[221]

5.138 サイバーセキュリティ連合はまた、重大な欠陥の定義は「非常に広範に読み取ることができる- オーストラリア政府、経済的または個人的な損害に影響を与えるもの」であると考えた。[222]Global Shield は、何が重大な欠陥にあたるかをより明確にする一つの方法として、「重要イ ンフラ資産所

---

[215] ERP 法案第 4 章第 3 節。

[216] 内務省提出資料 *59*、21 頁。

[217] CyberCX, *Submission 41*, p. 6; Department of Premier and Cabinet (Tasmania), *Submission 8*, p. 4; Governance Institute of Australia Ltd, *Submission 42*, p. 8; Institute for Integrated Economic Research- Australia, *Submission 1*, p. 2; Global Shield, *Submission 30*, p. 3.

[218] Governance Institute of Australia Ltd, *Submission 42*, p.8（強調部分あり）。

[219]内務省提出資料 *59*、20 頁。

[220] Association of Superannuation Funds of Australia, *Submission 46*, p. 14; BSA | The Software Alliance, *Submission 20*, p. 6; Mr Ari Schwartz, Coordinator, Cybersecurity Coalition, *Committee Hansard*, Canberra, 31 October 2024, p. 12; HackerOne, *Submission 33*, p. 2; Global Shield, *Submission 30*, p. 3.

[221] オーストラリア退職年金基金協会（Association of Superannuation Funds of Australia）、提出書類 *46*、14 頁。

[222] アリ・シュワルツ、サイバーセキュリティ連合コーディネーター、委員会ハンサード、キャンベラ、2024 年 10 月 31 日、12 頁。

有者がリスクマネジメントプログラムをより効果的に実施し、潜在的な欠陥に 積極的に対処できるようにするための国家リスクアセスメント」の創設を提案した。[223]

5.139 一方、BSA は、このような審査・救済権の序文にはまったく同意せず、次のように述べている。「政府がこの権力を必要とする明確な証拠はなく、効果的なチェック機能が欠如していることに懸念を抱いている」[224] 。

5.140 内務省は委員会の公聴会で、新権限の根拠を次のように説明した：

> また、インフラ資産に重大な欠陥があった場合、リスクマネジメントプログラムを是正する権限がないとの意見もあった。そのため、オーストラリア経済や安全保障に危害を及ぼしかねないような重大なコンプライアンス違反があった場合、そのリスクマネジメント・プログラムを是正することができるようにするために、このような権限が求められているのである。これが権限と政策的根拠の背景である。そして、「これは深刻な欠陥であり、実際に我々の経済に害を及ぼしている」と事業体と共に判断し、実施する。それがすべての根拠だ[225]

電気通信分野のセキュリティ規制

5.141 提出者が電気通信セクターの規制に関する改革案についてコメントした範囲では、改革案と、電気通信法（Telecommunications Act）第 14 条の要件を SOCI 法（SOCI Act）に統合する取り組みを概ね支持していた。[226]Palo Alto Networks は、この改革案は「電気通信セクターのサイバーセキュリティに関する規制の複雑さを合理化する」ものであると述べた。[227]Telstra は、SOCI 法のパート 22 において TSSR を拡張セキュリティ要件に置き換える案を支持し、この変更により「重複が解消され、要件を満たす上での確実性が増す」と提出した。[228]

5.142 IIER-A は改正案を支持したが、「衛星ベースの設備」、「海底ケーブル」、「電気通信サービ ス」、「電気通信システム」の意味の明確化を求めた。229

5.143 ERP 法案の Schedule 5 で提案された改革に関連して懸念されたのは、「重要な電気通信資産」の定義の変更である。ERP 法案は、「施設」という用語を削除し、「資産」という用語に置き換えることで、重要な電気通信資産の定義を修正する。Telstra の見解では、「施設」という用語は電気通信分

---

[223] グローバル・シールド、提出書類 *30* 号、p.3.

[224] BSA｜The Software Alliance, *Submission 20*, p. 3.

[225] ハミッシュ・ハンスフォード内務省サイバー・インフラ安全保障局次官、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、28 頁 ; オーストラリア統合経済研究所、提出資料 *1*、2 頁。

[226] BSA | The Software Alliance, *Submission 20*, p. 3; Palo Alto Networks, *Submission 57*, p. 3; Aussie Broadband, *Submission 39*; Institute for Integrated Economic Research-Australia, *Submission 1*, p. 3.

[227]Palo Alto Networks, *Submission 57*, p. 3.

[228] Telstra, *Submission 35,* p. 2.

[229] オーストラリア統合経済研究所（Institute for Integrated Economic Research-Australia）, *Submission 1*, p. 3.

野でよく理解されており、Telstra は、この変更によって SOCI 法で使用されている文言と一致することになるとしても、実際には定義の変更は必要ないと主張した。230 。

5.144 Telstra は、「重要な電気通信資産」の定義が ERP 法案の提案通りに修正された場合、説明文書を次のように更新す べきであると勧告した：

- 二次データ保管資産は、SoCI 法第 9 条第 7 項の規準を満たす場合にのみ、重要な電気通信資産として捕捉されることを明確にする。
- [電気通信ネットワークの一部を直接構成するものではないが、その機能をサポートする資産や、車両供給事業の遂行に不可欠な資産に関する例を［削除する]。[231]

5.145 オーストラリア・インターネット協会は、提案されている「重要な電気通信資産」の定義は「広すぎる」し、電気通信部門のセキュリティ義務を統合するという政府の意向に沿うものではないと提出した。[232]同協会は、このような定義は「『キャリッジ・サービス』の定義が同様に広範であることから、様々な電気通信システムを不必要かつ不適切に捕捉する可能性が高い」と考えた。[233]

5.146 オージー・ブロードバンド社は、電気通信法と SOCI 法の同等条項の解釈の仕方によっては、異なる条項が影響を与える可能性があることも強調した：

> 例えば、法案第 30EB 条(2)の要件は、プロバイダが「最善を尽くす」という既存の義務とは対照的に、責任ある事業体は「合理的に実行可能な限り」資産を保護しなければならないと定めている。オージー・ブロードバンドは、この新しい要件における「合理的に実行可能な範囲」の尺度について、さらなるガイダンスや明確化された規則を歓迎する。[234]

5.147 一方、Paul Wilkins 氏は委員会に対し、電気通信法 313 条（1A）項および（2A）項に基づき、通信事業者およびキャリッジ・サービス・プロバイダに「最善の努力」を求める現行の義務は、「せいぜい恣意的な標準」であると述べた。ウィルキンス氏は、定義がないため「各キャリアによる個別の解釈が可能となり、統一された標準、アーキテクチャ、プロセスの開発が妨げられる」と考えた。[235]

大臣による追加修正案

5.148 2024 年 11 月 7 日、トニー・バーク内務大臣兼サイバーセキュリティ担当大臣は、検事総長と大臣がサイバーセキュリティ法制パッケージに含まれる修正案と交差する追加の問題を特定したことを通知するため、委員会に書簡を送った。同大臣の書簡には以下のように記されている：

---

[230] Telstra, *Submission 35*, p. 3.

[231] Telstra, *Submission 35*, p. 3.

[232] Internet Association of Australia, *Submission 38*, p. 2.

[233] Internet Association of Australia, *Submission 38*, p. 2.

[234] Aussie Broadband, *Submission 39*, p. 1.

[235] Paul Wilkins, *Submission 13: Attachment 1*, p. 5.

オーストラリアの重要インフラのセキュリティを確保するための政府の取り決めの一環として、 オーストラリア安全保障情報機構（ASIO）には、重要インフラの所有や運用など に関する政府の決定に情報を提供するためのセキュリティ評価を提供する権限が与えられている。

1979 年オーストラリア安全保障情報機構法（ASIO 法）は、ASIO が不利な安全保障評価または適格な安全保障評価を行ったことを申請者に通知する手順、および開示が安全保障の利益を害する情報の保護に関連するプロセスを規定している。特筆すべきは、ASIO 法第 38 条がこれらの手続きを一般的に規定している一方で、ASIO 法第 38A 条が 1997 年電気通信法と 2018 年重要インフラ安全保障法に関連する特定の状況について規定していることである。

2004 年のコミュニケーション法改正法（第 1 号）において ASIO 法第 38 条 A が序文化されて以来、ASIO 法パート 4 は継続的な法改正の対象となってきた。これらの改革の累積的効果により、ASIO 法第 38A 条は冗長となり、ASIO 法第 38 条の一般的かつ広範に一貫した運用が注目されている。

疑義を避けるため、アセスメント総長と私は、最近および将来の不利な、あるいは適格なセキュリティ評価に関する通知要件と情報保護規定の運用を明確にするための法改正にメリットがあると考えている。このような変更により、オーストラリアの重要インフラに対する脅威を管理するための効果的かつ適切なプロセスが維持され、より広範な立法パッケージを補完することができる。委員会が同意するのであれば、報告書に記載することを検討していただきたい。

5.149 具体的な修正点の詳細は委員会に提供されていなかった。

6.委員会のコメントと勧告

6.1　本章では、サイバーセキュリティ法制パッケージを構成する 3 法案に関する委員会のコメントと勧告を掲載する。

包括的なコメント

6.2　サイバーセキュリティと重要インフラの防御は、オーストラリアの国家安全保障と経済レジリエンスにとってますます重要な要素となっている。近年の出来事で示されたように、サイバーセキュリティインシデントは、何百万人ものオーストラリ ア国民のプライバシーと安全を脅かし、以前には不可能だった規模の詐欺や恐喝を可能にする可能性がある。さらに深刻なのは、敵対する国家が、重要インフラを破壊し、紛争時に豪州の国益に大きな損害を与える潜在的手段として、サイバー脆弱性を見なすようになっていることである。安全保障総局長が 2024 年の年次脅威アセスメントで警告したとおりである：

> テロリストとスパイの共通点は多くないが、破壊工作はそのひとつだ。ASIO は、両者が破壊工作について話し、破壊工作について研究し、時には破壊工作のための偵察を行うのを目の当たりにしている。
>
> 破壊工作のベクトルとして、最も即効性があり、低コストで、潜在的な影響力が大きいのはサイバーである。重要インフラ・ネットワークは相互に接続され、依存し合っているため、脆弱性と潜在的なアクセスポイントが増加している。
>
> ASIO は、ある国家がオーストラリアや他の国の重要なインフラをスキャンしようと何度も試み、水、輸送、エネルギーネットワークをターゲットにしていることを把握している。
>
> 偵察は非常に洗練されており、一流の技術を駆使してネットワークをマッピングし、脆弱性をテストし、デジタルのドアをノックし、デジタルの鍵をチェックする。[1]

6.3　こうした脅威に対してオーストラリアのサイバーセキュリティを強化することは、オー ストラリアの継続的な安全と繁栄にとって不可欠である。この目的のため、当委員会は、2030 年までに豪州がサイバーセキュリティの世界的リーダー となるために、豪州のサイバー防衛を強化し、サイバーレジリエンスを構築するという、サイバーセ キュリティ法制パッケージと、より広範な *2023-2030* 年豪州サイバーセキュリティ戦略の意図を 支持する。この意図と、サイバーセキュリティ法制パッケージを構成する 3 つの法案で採られている一般的なアプローチは、調査参加者のほぼ全 体的な支持を得た。

6.4　同時に、委員会は、提出書類を提出したり公聴会に出席したりした一部の組織や個人から提起された懸念、特に、明確なガイダンスの重要性と、法案実施中の継続的な協議に関する懸念に耳を傾け

[1] マイク・バージェス安全保障総局長、「総局長年次脅威アセスメント 2024」、2024 年 2 月 28 日、https://www.asio.gov.au/director-generals-annual-threat-assessment-2024、2024 年 11 月 3 日閲覧。

た。委員会は、各法案が、使用制限規定を除く主要な措置について、6 ヶ月から 12 ヶ月の実施期間を認めていることに留意する。以下に詳述するように、当委員会は内務省に対し、これらの期間を利用して、規定の意図する運用に関する明確なガイダンス資料、教育、助言による産業界のサポートを確保するよう奨励する。

審査プロセス

6.5 立法パッケージに対する基本的な支持は強かったが、調査参加者の中には、委員会のレビューが短期間で行われたことに懸念を表明する者もいた。委員会はこうした懸念に同情する。当委員会はつい最近、政府に対し、要求された法案レビューの期間に関して「現実主義を貫く」よう要請した：

> 委員会は、複雑な法案の審査期間が極端に短いことは、委員会とそのスタッフにプレッシャーを与えるだけでなく、収集できる証拠の質と量を低下させ、主要な利害関係者との関係を損なう可能性さえあることに留意する。
>
> 健全な民主的プロセスと適切な国家安全保障の監視のためには、可能な限り、委員会がその仕事をうまくこなすのに必要な適切な時間と空間を提供する必要がある。[2]

6.6 今回の例では、法案が国会に提出されてから、大臣が報告するよう要請するまでの期間は 6 週間未満であった。これは、150 頁を超える複雑な法案を一括して提出したにしては異例の短さである。

6.7 それにもかかわらず 、当委員会は、調査参加者の間で法案に対する幅広い支持が得られたこと、また、国会に序文が提出される前に広範かつ厳密な協議プロセスが行われたことに留意する。この「ベストプラクティス」の協議プロセスにより、導入された法案には利害関係者が驚くようなものは（あったとしても）ほとんどなく、したがって委員会が解決すべき問題は、そうでなかった場合よりも少なかった。提出者の中には、パッケージの側面について基本的に異論を唱える者もいたが、委員会に持ち込まれた事項の大半は、実施や細部に関するものであった。

6.8 厳しい時間枠にもかかわらず 、委員会は産業界、ピーク団体、市民社会、個人から 60 を超える質の高い書面提出を受け、2 日間の公聴会を開催した。委員会は、結論と勧告を策定するにあたり、これらの貢献を考慮に入れた。委員会は、調査を支援するために建設的な努力を払ってくれたすべての関係者に感謝の意を表する。

6.9 さらに、同委員会は、オーストラリアのサイバーレジリエンスを強化し、*2023-2030* 年オーストラリア・サイ バーセキュリティ戦略を実施することが、政府と今国会の緊急優先事項であることを認め、同委員会は、 47th 国会の会期が終了する前に立法パッケージを可決することが、その実施の遅延を避けるために必要であると考 える。

6.10 これを踏まえ、当委員会は、本報告書の残りの部分に含まれる勧告を条件として、法案の緊急可決を支持する。

---

[2] 国会情報・安全保障合同委員会『*2022-2023* 年委員会年次活動報告』2024 年 2 月、15 頁。

勧告 1

6.11　委員会は、本報告書の勧告を実施することを条件として、サイバーセキュリティ法案 2024、情報サービス等法改正（サイバーセキュリティ）法案 2024、重要インフラ等安全保障法改正（対応強化・予防）法案 2024 を国会で可決することを勧告する。

スマートデバイスのセキュリティ標準

6.12　サイバーセキュリティ法案 2024（Cyber Security Bill）が提案したスマートデバイスのセキュリティ標準の義務化序文は、立法パッケージの中で最も強く支持された施策の一つであった。当委員会も同様に、この措置を強く支持する。自動車から台所用品、その他の家庭用機器に至るまで、オーストラリア国民は、購入する製品が安全、セキュリティ、プライバシーを確保するための最低限の標準を満たしていることを期待できるはずである。カメラやマイクを内蔵する機器が増えるにつれ、このことはますます重要になっている。

6.13　委員会は、特定のクラスの機器に適用される標準、これらの標準の導入の段階的な変更、適用除外など、この措置の詳細の多くが規則で規定されることが提案されていることに留意する。これは、技術環境の変化やベストプラクティス標準に対応して技術仕様を迅速に更新し、各クラスの製品に関連する特定のセキュリティ要件に対応する柔軟性をオーストラリア政府に与えるものであり、適切である。委員会は、規則が強制的な協議要件、[3] および議会による不許可手続きの　対象となることに留意する。

6.14　調査への参加者は、製造事業者とサプライヤーが適応するための時間を確保するため、新基準の段階的な導入 アプローチを主張した。内務省は委員会への証拠提出の中で、改革に 1 年間の段階的導入期間を設け、その間に産業界と協議を続け、規則の実施が目的に適うものであることを確認する方法を説明した。内務省は、この規則に対するアプローチ案をまとめた説明文書を公表した。この文書では、セキュリティ標準はまず一般消費者向け接続可能製品に適用され、将来的には必要に応じて規則の適用を検討するという内務省の意向が概説されている。[4] 。

6.15　委員会は、この段階的アプローチを支持し、標準が各クラスの製品に適した方法で適用されるよう、関係者との協議を継続することを奨励する。

6.16　委員会は、標準規格を同等の国際規格に合わせるという政府の意図も支持する。[5] 世界の他地域で適用されている規格と大きく乖離した規格は、ある種の製品の供給者にとって大きな問題となり、その製品がオーストラリアの主流市場から撤退し、海外からの並行輸入を促進する可能性さえある。

6.17　委員会は、少数の提出者から、自動車のセキュリティ標準がサイバーセキュリティ法案やその解説書で明示的に扱われていないという懸念があることを認める。しかし、委員会は、サイバーセキュリティ法案のパート 2 は、規則で特に除外されていない限り、「関連する接続可能な製品」の定義を

[3] サイバーセキュリティ法案 2024、第 87 条案。

[4] Department of Home Affairs, *Submission 59*, p. 29.[5]内務省提出資料 *59*, p. 8.

満たすすべての製品に適用されることを意図していることに留意する。また委員会は、以下の場合にのみ機器が除外されるという内務省の助言にも留意する：

> これらの機器のサイバーセキュリティに適切に対処できる既存の法律がある、ガバナンス全体でこれらの機器についてより高い、あるいは特注の標準を策定する作業が進行中である、あるいは、これらの機器の複雑性から、この規則の下で義務化されることは、より低い標準を満たすリスクとなる。[5]

6.18 接続可能な機器のセキュリティを向上させることが最重要目標であることに変わりはないが、当委員会は、同省が産業界と協力して、実施と執行に合理的なアプローチを適用することを奨励する。

6.19 Part 2 で使用されるいくつかの定義の解釈に関する一部の提出者からの懸念に言及し、委員会は、内務省によるアウトリーチや教育とともに、企業が各業種に関連する提案された新要件を十分に理解できるよう、明確なガイダンスを作成する必要性を強調する。サイバーセキュリティ法制パッケージの他の側面と同様に、内務省は規定の施行に「教育第一」のアプローチを適用すべきである。

ランサムウェア報告

6.20 当委員会は、サイバーセキュリティ法案で提案されている、企業によるランサムウェアの支払いに関する報告義務の導入を支持する。ランサムウェアやその他のデジタル恐喝は、豪州の企業とその生産性だけでなく、より広範な地域社会にとっても根強いセキュリティ上の脅威である。新たな報告義務は、企業による支払いの程度を明らかにし、この種の深刻なサイバー犯罪と闘う政府の取り組みに情報を提供するのに役立つだろう。

6.21 提案されている報告義務に適用されるべき年間売上高の閾値については、調査への寄稿者の間でも意見が分かれた。個人情報保護法（*Privacy Act 1988*）の中小企業の定義に沿った 300 万ドルという売上高の閾値案は低すぎ、中小企業にとって遵守は負担が大きすぎると考える投稿者もいた。他の投稿者は、ランサムウェアによる支払いの程度を政府がより詳細に把握できるようにするために、提案されている閾値を低くするか、あるいは削除するべきだと考えている。また、報告義務の目的を達成するのに十分なデータを提供することと、中小企業の規制負担を最小限に抑えることのバランスが適切であるとして、提案されている売上高の閾値を支持する意見もあった。

6.22 委員会は、このような異なる見解を認める。しかし、当委員会は、正確な売上高基準額は、当委員会が見直すことを命じられた一次法ではなく、規則で設定されることに留意する。ルールは、サイバーセキュリティ法で規定された強制的な協議要件の対象となり、国会による不許可となる。

6.23 また、ランサムウェアの支払いだけを報告対象とすべきか、企業が受け取ったランサムウェアの要求も報告対象とすべきか（要求が支払いにつながったかどうかにかかわらず）についても、意見が分かれた。当委員会は、ランサムウェアの要求の報告を義務付けることで、政府機関が問題の程度をより完全に把握できることに留意している。しかし、企業の規制負担を最小限に抑えるた

[5] 内務省提出資料 *59*、10 頁。

め、ランサムウェアの支払いの報告のみを義務付けるというサイバーセキュリティ法案のアプローチを支持している。

6.24 この点について当委員会は、提案されている売上高基準以下の中小企業や個人、その他の組織 を含む企業が、ランサムウェアの要求を報告し、任意ベースでオーストラリア・サイバー・セキュリティ・センター（ACSC）に支援を求めることができる既存の仕組みがあることに留意する。[6]当委員会は、組織がこれらのサービスを利用することを奨励し、ACSC が義務的な報告とともに任意ベースで受け取った情報を、脅威の状況の広範な分析に役立てることを奨励する。

6.25 委員会は、新たなランサムウェアの報告義務が、一部の事業体、特に重要インフラ安全保障法 *2018*（SOCI 法 ）に基づきサイバーセキュリティインシデントを報告する義務を有する事業体の報告義務と重複する懸念を認める。当委員会は、SOCI 法に基づく広範な報告義務が、SOCI 法の事業体がサイバーセキュリティ法に基づきランサムウェアの支払いに関する個別の報告を行う必要性を必ずしも排除すべきではないと考えているが、政府からの重複した情報要請を回避し、報告ツールを合理化する必要性は明らかである。より広く言えば、委員会は、ランサムウェアの報告義務の成功には、報告を促進するために使用されるツールが、そのツールを使用する様々な企業にとって、見つけやすく、使いやすく、理解しやすいものであることが不可欠であると考えている。

6.26 委員会は、報告プロセスの合理化がすでに *2023-2030* 年オーストラリア・サイバーセキュリ ティ 戦略のイニシアチブであることに留意している□[7]□当委員会は、cyber.gov.au の「ワンストップ・ショップ」報告施設が、中小企業を含め、可能な限りユーザーフレンドリーでアクセスしやすいものとなるよう、さらなる作業が進行中であると理解している。[8]

勧告 2

6.27 当委員会は、オーストラリア政府に対し、サイバーセキュリティ法案 2024 の報告義務の対象となるさまざまな企業にとって、ランサムウェアの報告メカニズムが可能な限り使いやすく、アクセスしやすいものとなるよう確保すること、およびオーストラリア政府が引き続き、すべての企業に対するサイバーセキュリティインシデント報告要件の重複を最小限に抑えるための作業を優先することを勧告する。

6.28 委員会は、内務省がコンプライアンスに対して「教育第一」のアプローチを取る意向であることを知り、安心した。[9]当委員会は、提案されているランサムウェア報告義務の対象となる企業に教育と明確なガイダンスを提供することの重要性を強調する。

6.29 従って、委員会は、内務省が提案されている 6 ヶ月間の規定実施期間中およびそれ以降も、教育とガイダンスに十分なリソースを割くことが重要であると考える。当委員会はまた、オーストラリア

[6] Australian Signals Directorate (ASD), 'Ransomware', https://www.cyber.gov.au/threats/typesthreats/ransomware, viewed 6 November 2024.

[7] オーストラリア政府、*2023-2030* 年オーストラリア・サイバーセキュリティ戦略、25 頁。

[8] アシュリー・ベル内務省サイバー政策・プログラム担当次官補、委員会ハンサード、キャンベラ、2024 年 11 月 1 日、25 頁。

[9] Cyber Security Bill 2024, Explanatory Memorandum (EM), p. 47 [222].

ビジネス協会やオーストラリア中小企業団体協議会などの　　代表的なビジネス団体に対し、その会員を教育し、情報を提供するための　　サポートを提供することを奨励する。

勧告 3

6.30　当委員会は、オーストラリア政府に対し、ランサムウェアの報告義務について企業を教育し、 法律の解釈について明確なガイダンスを提供するために、内務省とオーストラリア信号局 に十分なリソースを確保するよう勧告する。

6.31　委員会は、オーストラリアビジネス協会（Business Council of Australia）およびオーストラリア法 律審議会（Law Council of Australia）が提起した、サイバーセキュリティ法案の域外適用規定が、 オーストラリアを拠点とする事業体との関連性がない海外のインシデントにもランサムウ ェアの報告義務を不用意に拡大する可能性があるという懸念に留意する。当委員会は、オーストラリア法審議会がサイバーセキュリティ法案第 26 項(1)(c)にこの問題に対処する小修正を提案したことに留意する。10委員会は、政府がこの提案を検討し、ランサムウェア報告義務がランサムウェアインシデントが報告事業体のオーストラリアでの事業に関連する範囲にのみ適用されるよう、適宜法案を修正することを勧告する。

勧告 4

6.32　当委員会は、提案されているランサムウェア報告義務が、ランサムウェアインシデントが報告事業体のオーストラリ ア国内での業務に関連する範囲にのみ適用されるよう、サイバーセキュリティ法案 2024 を修正することを勧告する。

6.33　委員会はまた、産業界に追加的な報告義務を課す代わりに、政府によるサイバー脅威情報の産業界への 共有を強化すべきであるという、調査への複数の寄稿者から表明された意見も認める。当委員会は、原則としてこの考え方を支持する。政府が入手できる情報が改善されれば、政府機関が産業界のパートナーや、場合によってはより広範な一般市民に対して、サイバー脅威の存在とそれらの脅威から身を守る方法を警告することを期待するのは合理的である。

6.34　当委員会は、ACSC が近年、最近設立された双方向のサイバー脅威情報共有（Cyber Threat Intelligence Sharing: CTIS）プラットフォームを含め、脅威情報の提供をすでに拡大していることを承知している。CTIS プラットフォームは、企業が脅威情報を豪州情報局（Australian Signals Directorate: ASD）や他の業界パートナーと共有し、またそのような情報を受け取ることができるようにすることを目的としている。[11]ACSC はまた、cyber.gov.au のウェブサイトとそれに付随する電子メール・アラート・サービスを通じ て、より一般的なサイバーセキュリティ・アラートとア

[10] オーストラリア法評議会、提出書類 *62*、13 頁。

[11] ASD, 'Join Cyber Threat Intelligence Sharing service through Sentinel', https://www.cyber.gov.au/aboutus/view-all-content/news-and-media/join-the-cyber-threat-intelligence-sharing-service-through-sentinel, viewed 6 November 2024.

ドバイザリーを一般市民に提供している。[12]委員会は、これらの既存サービスの有効性についての証拠は得られなかったが、利害関係者からの フィードバックに応じて、ACSC が双方向の情報共有を強化する方法を模索し続けることを奨励する。

サイバーインシデント審査会

6.35 当委員会は、サイバーセキュリティ法案で提案されている、豪州で発生した重大なサイ バーセキュリティインシデントの事後レビューを行う独立したサイバーインシデント・レ ビュー委員会（CIRB）の設置を支持する。最近のインシデントから、重大なサイバーセキュリティインシデントの後に学ぶべき重要な教訓 があることが明らかになっており、CIRB はそうした教訓を独立に確認し、政府、産業界、一般市民 にフィードバックするためのメカニズムを提供することになる。

6.36 CIRB は不要と考える回答者もいたが、ほとんどの回答者は少なくとも基本的には支持を表明した。しかし委員会は、CIRB の構成と構成案、および個々のレビューの職務権限を承認する際の大臣の役割について、懸念を表明した寄稿者が多数いたことを認める。

6.37 サイバーセキュリティ法案のパート 5 では、CIRB は常設メンバーと専門家パネルで構成され、専門家パネルのメンバーは各レビューを支援するために任命されることが提案されている。しかし、サイバーセキュリティ法案の説明文書の中で、CIRB の常任委員は公務員であるとの記述に懸念を示す意見が複数あった。[13]当委員会はこのような懸念を認め、各 CIRB レビューにおいて、政府内外から幅広い専門家が参加することが重要であることに同意する。

6.38 当委員会は、サイバーセキュリティ法案には、CIRB の常任メンバーを公務員のみ で構成することを求めるような記述はないことに留意する。ASD のような法定機関の代表者を含む上級公務員が CIRB に参加し、その権限を行使することは適切であるが、委員会は政府外部の代表者も参加させたいという意見も聞いている。この主張の是非を説明し、十分に検討するために、政府とその他の者による更なる協議を可能にするため、委員会は説明文書を修正し、現在の記述を削除することを勧告する。

勧告 5

6.39 委員会は、サイバーセキュリティ法案 2024 の説明文書を修正し、サイバーインシデント審査委員会の常任委員は公務員であるとの記述を削除することを勧告する。

6.40 委員会はまた、サイバーセキュリティ法案では CIRB の各審査の職務権限について大臣の承認が必要であるため、CIRB の独立性が損なわれるとの意見もあることを認めた。委員会は謹んで同意しない。本法案は、CIRB に各レビューの実施方法と報告方法に関する独立性を与えているが、大臣が、CIRB とその専門家パネルの特定のメンバーに関しても含め、各レビューの職務権限が適切であることを確認する役割を持つことは適切である。これにより、民主的に選出され、サイバーセキュリテ

[12] ASD、「Alerts and Advisories」、https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories、2024 年 11 月 6 日閲覧。

[13] サイバーセキュリティ法案 2024、EM、8 頁。

ィ政策に責任を持つ公職者である大臣は、レビューがインシデントに関連して進行中の他のレビューの仕組みや調査と重複しないこと、またレビューに関与する CIRB の常任メンバーや専門家パネルのメンバーが利害の対立を持たないことを確認することができる。

6.41 とはいえ　、委員会は、大臣が職務権限を承認する前に CIRB と緊密に協議することを期待する。この協議が確実に行われることを保証するため、委員会はサイバーセキュリティ法案を改正し、このような協議を義務化することを勧告する。

勧告 6

6.42　委員会は、サイバーセキュリティ法案 2024 を改正し、見直しの職務権限を承認する前に、大臣がサイバーインシデント審査委員会に諮問することを義務付けることを勧告する。

限定使用規定

6.43　委員会は、サイバーセキュリティ法案および情報サービスおよびその他の法改正（サイバーセキュリティ）法案 2024（ISA 法案）における「限定的使用」条項の意図に対する強い支持に留意する。これは、サイバーセキュリティインシデントに関する情報を政府機関に自発的に開示する事業体に対して、開示した情報が将来的に自分たちの利益に反して使用されることがないことをより確実にするためのものである。委員会はまた、この防御がさらに強化されることを懸念する投稿者もいることを指摘している。

6.44　調査に参加した一部の　プロバイダは、サイバーインシデントに関する情報を国家サイバーセキュリティコーディネー ター（NCSC）または ASD に提供した場合、事業体は将来の規制措置や強制措置から保護されるべきだと提案した。しかし、委員会は、事業体がインシデントを関連当局に報告したという理由だけで、インシデントに関する法的責任を免れるような「セーフハーバー」を設けることは、この規定の意図するところではないことに留意する。むしろ、限定的使用規定の意図は、インシデント報告書そのものが事業体に対するいかなる訴訟でも認められず、事業体の報告書が規制当局によってコンプライアンス措置のために使用されないことを保証することにある。

6.45　調査への投稿者の中には、情報の使用や共有に関する追加的な制約を求めたり、政府機関が情報を共有する前に影響を受ける事業体と協議することを要求したりした者もいた。

6.46　委員会は、この枠組みは適切なバランスのとれた実行可能な枠組みであると考える。

6.47 それにもかかわらず、一部の利害関係者から提起された懸念と、本規定の運用と意図に関連する明らかな混乱に留意し、当委員会は、業界パートナーが限定的使用の防御の範囲を理解できるようにするための一層の努力が必要であると考える。そのためには、説明文書において、実例を用いるなどして、本規定の限界をより明確に示すとともに、本規定が実際にどのように運用されることを意図しているのかを企業が理解できるよう、今後ガイダンスや教育を行うことが必要であろう。

勧告 7

6.48 委員会は、「限定的使用」条項によって与えられる防御を、サイバーセキュリティ法案 2024、情報サービスおよびその他の法改正（サイバーセキュリティ）法案 2024、および関連する説明文書の中でより明確に表現し、内務省がガイダンスを作成することで、産業界に十分理解されるようにすることを勧告する。

6.49 委員会は、法律専門家秘匿特権（LPP）の対象となる可能性がある情報が規定によって適切に保護されるかどうかについて、オーストラリアビジネス協会およびオーストラリア法制審議会から提起された懸念に留意する。委員会は、サイバーセキュリティ法案または ISA 法案のいずれかに基づき政府に開示された情報に関して、LPP を放棄する意図はないと理解している。委員会は、この意図を明確にするために法案が修正されることを支持する。

6.50 委員会はまた、既存の権利、特権および免除の法案による防御が、事業体が被告となる訴訟手続だけ でなく、すべての訴訟手続にも及ぶことを保証するための、オーストラリア法評議会の小修正の提案に 留意する。委員会は、この問題に対処するための小修正の挿入を支持する。

勧告 8

6.51 委員会は、サイバーセキュリティ法案 2024 および情報サービスおよびその他の法改正（サイバーセキュリティ）法案 2024 を改正し、以下をより明確にすることを勧告する：

- **ランサムウェア報告義務に基づく情報開示は、その後の法律専門家特権の放棄には当たらない。**
- **本規定は、報告事業体が訴訟手続に関して有するいかなる権利、特権、免責にも制限または影響を与えない。**

SOCI 法改正

6.52 委員会は、重要インフラ等安全保障法改正案（対応と予防の強化）法案 2024（ERP 法案）によって導入される SOCI 法の大幅な変更に留意する。多くの提出者は、以下の改正案を含むこれらの変更への支持を表明した：

- 重要インフラ資産」の定義に、「ビジネスクリティカルなデータ」を保持するデータストレージシステムを含める。
- SOCI 法の既存の情報収集と行動指示の権限を拡大し、重大なサイバーセキュリティインシデントだけでなく、あらゆる重大インシデントに対応できるようにする。
- 情報共有規定と関連する管理プロセスを明確にする
- 事業体に対し、重要インフラリスクマネジメント計画の重大な欠陥に対処するよう求める新たな指示権を導入する。

- *1997* 年電気通信法（*Telecommunications Act 1997*）の電気通信部門安全保障改革（TSSR）条項を SOCI 法に統合する。

6.53 しかし、第 5 章で概説したように、調査参加者のなかには、規定の一部について異議を唱える者もいた。他の参加者は、ERP 法案によって SOCI 法に導入されたいくつかの重要な用語の潜在的な適用範囲に懸念を示し、改正がどのように解釈され適用されることを意図しているかに関連して、より明確な説明を求めた。これは、「データ保管システム」、「業務上重要なデータ」、「重大なリスク」、「責任ある事業体」、「インシデント」、「重大なインシデント」、「重大な欠陥」などの用語に関するものであった。

6.54 委員会は、様々な権限が実際にどのように使用されるかを導くための方針、手順、ガイダンス資料の作成に 取り組んでいるという内務省の助言を歓迎する。委員会は、同省が業界と協議の上、これらの資料の中に、上記の用語が事業体によってどのように解釈され、適用されることを意図しているのかについて、例を挙げて明確なガイダンスを含めることを奨励する。

勧告 9

6.55 委員会は、重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 2024 の実施を支援するための行政ガイダンス資料において、内務省は、重要インフラの安全保障法 *2018* に 導入された重要定義の意図する解釈と適用に関して、明確なガイダンスと事例を提供するよう勧告する。

6.56 調査参加者の中には、SOCI 法の現行の運用について幅広い懸念を表明した者もいた。これには、SOCI 法の既存の部分に関する定義の明確性の欠如に関する懸念、SOCI 法を遵守するための事業体への財政的影響と規制上の賦課金に関する懸念、SOCI 法の下で利用可能な指示権限の範囲に関する懸念、これらの権限に関連する独立した認可、監督メカニズム、またはメリット・レビューの不在に関する懸念が含まれる。

6.57 今回の調査の一環として、こうした広範な懸念に対処しようとするのは、当委員会の意図するところではない。ERP 法案は、SOCI 法の下で利用可能な権限を修正し、場合によっては拡大するものであるが、SOCI 法の現行の運用を根本的に変更する勧告の是非は、別個の広範な見直しで検討するのが最善であろう。当委員会は、法制化された独立審査と、当委員会による SOCI 法の法定審査に関する勧告を以下に行う。

法定審査

6.58 当委員会は、サイバーセキュリティ法の最初の運用期間終了後、法的な見直しを求める声 を支持する。スマートデバイスのセキュリティ標準、ランサムウェア報告義務、サイバーインシデント審査委員会に関するサイバーセキュリティ法案の措置は、オーストラリアの文脈では全く新しいものであり、法律が効果的であり、産業界に不必要な義務や重複する義務を負わせていないことを確認するために評価されるべきである。同様に、NCSC や ASD との自発的な情報共有を向上させるために、限定的使用規定が意図したとおりに機能しているかどうかも見直されるべきである。

6.59 委員会は、およそ 3 年後に見直しを開始することが適切であるというオーストラリア法 律審議会の提案に同意する。この見直しは、サイバーセキュリティ法が意図したとおりに運用され、その目的を効果的に 達成し、合理的かつ適切に実施されているかどうかをアセスメントする機会となる。

勧告 10

6.60 委員会は、サイバーセキュリティ法案 *2024* を改正し、委員会が（決議すれば）2027 年 12 月 1 日以降、実務上可能な限り速やかに、サイバーセキュリティ法 *2024* の運用、有効性、影響の見直しを開始することができると規定する ことを勧告する。

6.61 委員会はまた、ERP 法案によって大幅な改正が提案されている SOCI 法が、その運用について広範な議会または独立機関による見直しが行われることなく、6 年間運用されてきたことを意識している。

6.62 委員会は以前、2021 年 9 月に SOCI 法の法定見直しを完了した。[14]しかし、この見直しは、SOCI 法にパート 3A を導入する 2020 年安全保障法制改正（重要インフラ）法案（SLACI 法案） の序文と重なったため、当時の委員会は現行の SOCI 法の運用を効果的に見直すことができなかった。[15]

6.63 当時の委員会は、3 年後に委員会が SOCI 法のさらなる法定見直しを実施できるよう法改正を勧告した。[16]その結果、委員会は現在、SOCI 法第 60 条 B の下、2021 年安全保障法制改正（重要インフラ）法（SLACI 法） が勅許を受けた後 3 年経過する前に見直しを開始する限り、SOCI 法の運用、有効性、影響を見直す権限を与えられている。この期間は 2024 年 12 月 2 日に満了するため、現在の委員会は早急に法定見直しを開始する必要がある。

6.64 委員会は、SOCI 法の広範で総合的な見直しが引き続き必要であると考える。上述したように、今回の調査における証拠によって、第 3A 部の権限に関連する独立した認可・審査メカニズムの欠如など、SOCI 法の側面について引き続き懸念があることが示された。これらの懸念は、第 3A 部によって導入された権限をさらに拡大する ERP 法案に広く関連していた。しかし、委員会は、これらの懸念に対処するには、サイバーセキュリティ法制パッケージに関する現在の調査よりも長い期間をかけて行われる SOCI 法の全体的な見直しの方が適していると考えている。

6.65 とはいえ、2021 年に起きたように、ERP 法案を通じて SOCI 法に大幅な改正が導入されたことは、SOCI 法が再び流動的な状態にあることを意味する。ERP 法案が導入する重要な変更の多くは、6 ヶ月または 12 ヶ月の実施期間が経過するまで開始される予定はない。17今後 6 ヶ月以内に

---

[14] 情報・安全保障に関する国会合同委員会、安全保障法制改正（重要インフラ）法案 *2020* および重要インフラ安全保障法 *2018* の法定見直しに関する諮問報告書、2021 年 9 月。

[15] 国会情報・安全保障合同委員会、安全保障法制改正（重要インフラ）法案 *2020* および重要インフラ安全保障法 *2018* の法定見直しに関する諮問報告書、2021 年 9 月、59 頁［4.10］。

[16] 国会情報・安全保障合同委員会、安全保障法制改正（重要インフラ）法案 *2020* および重要インフラ安全保障法 *2018* の法定見直しに関する諮問報告書、2021 年 9 月、60 頁［4.16］。

[17] 重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 2024 年第 2 項（「開始」）。

予想される選挙も複雑な要因である。その結果、委員会は、2024 年 12 月 2 日の期限までに開始するとしても、有意義な法定見直しを実施する態勢が整っていない。

6.66 委員会は、ERP 法案によって導入された変更の影響が十分にアセスメントされるような時期に、法定見直しの期日を次の国会の開 会後まで延期すべきであると考える。従って委員会は、SOCI 法第 60 条 B によって可能となる法定見直しの開始日を 2 年延長し、2026 年 12 月 2 日とすることを提案する。

6.67 委員会はまた、2022 年 3 月に当時の委員会が勧告し、委員会自身の法定見直し（18 ）に情報を提供することを意図していた、社会保険法第 60 条 A に基づく独立した見直しがまだ行われていない ことに留意する。第 60A 条は、2023 年 4 月 2 日に同条が施行されてから 12 ヵ月後に独立したレビューを開始させ、レビュー開始後 12 ヵ月以内に国会に上程するための報告書を大臣に提出させることを大臣に義務付けていた。しかし、法案には独立審査を開始する期限が明記されていないため、当委員会は、独立審査はまだ開始されていないと理解している。

6.68 2022 年当時の委員会は、独立レビューの早期完了を想定していたが、ERP 法案によって導入された変更がまだ発効していない今、独立レ ビューを間近に開始するメリットはほとんどないだろう。しかし、委員会の次回の法定見直しに間に合わせるため、委員会は、2025 年 11 月 1 日までに独立見直しを開始することを勧告する。

勧告 11

6.69 委員会は、重要インフラ安全保障法（*Security of Critical Infrastructure Act 2018*）第 60A 条で義務付けられている同法の運用に関する独立レビューを、2025 年 11 月 1 日までに 開始するよう大臣に勧告する。

勧告 12

6.70 委員会は、重要インフラ安全保障法 *2018*（SOCI 法）の既存の第 60B 条を改正し、情報・安全保障に関する国会合同委員会が（その決議がなされれば）、同委員会が 2026 年 12 月 2 日までに見直しを開始する限り、SOCI 法の運用、有効性、影響を見直すことができると規定する ことを勧告する。

6.71 委員会は、内務省が SLACI 法および *2022* 年安全保障法制改正（重要インフラ保護）法（SLACIP 法）に関連して同省が実施した協議の実施、進捗状況および結果に関連する 6 ヶ月ごとの報告書を、SOCI 法第 60AAA 条で義務付けられている通り、また委員会の以前の勧告に従って、委員会に提供してきたことに留意する。この報告義務は、委員会が SOCI 法の法定見直しを開始した時点で期限切れとなっていた。

6.72 SLACI 法および SLACIP 法の施行が完了したとの同省の助言に留意し、委員会は、第 60AAA 条はその目的を果たし、もはや同省がこれらの定期報告書を提供し続ける必要はないと考える。したが

[18] 国会情報・安全保障合同委員会、安全保障法制改正案（重要インフラ保護）法案に関する諮問報告書、*2022* 年 3 月。

って委員会は、第 60AAA 条を廃止することを勧告する。この勧告を行うにあたり、委員会は *2001* 年情報サービス法第 30 条に基づき、委員会の機能遂行を目的として内務省にブリーフィングを要請する　　常設の権限を有していることに留意する。

勧告 13

6.73　委員会は、重要インフラ安全保障法 2018 を改正し、内務省が委員会に 6 ヶ月ごとの協議報告書を提出するという第 60AAA 条の要件を廃止すことを勧告する。

ラフ・チッコーネ上院議員
議長
14 2024 年 11 月

委員会連合メンバーの追加コメント

当委員会の連合メンバー（連合メンバー）は、本法案の政策意図と本報告書の勧告を支持する。本法案によって導入される改革は、重要インフラの安全保障（SOCI）体制と 2016 年と 2020 年の連続する国家サイバーセキュリティ戦略の立役者であった前連立ガバナンスによる、世界をリードするアプローチの論理的延長を示すものである。

しかし、連合メンバーは、多くの利害関係者と同様、本調査の対象となった法案や他の多くの法案について、政府が急ぎすぎるプロセスを続け、国会での精査時間が限られているため、意図しない結果や法案の作成ミスを見落とすリスクが高まっていることについて、引き続き重大な懸念を抱いている。

重要インフラの安全保障およびその他の法改正（対応と予防の強化）法案 *2024*

前連立政府は 2018 年に重要インフラ安全保障法（SOCI 法）を導入し、重要インフラ資産を所有、運営、または直接の利害関係を有する事業体の法的義務を概説し、深刻なサイバーセキュリティ脅威または攻撃に対する政府の支援権限を盛り込んだ。前連立政府は 2021 年に SOCI 法を改正し、2022 年にも SOCI 法を改正して、特定の資産に対するリスクマネジメントプログラムの義務化など、国家的に重要な重要インフラ資産やシステムに対するセキュリティ義務を強化した。

連合メンバーは、重要インフラ等安全保障法改正案（対応と予防の強化）法案 2024 のアプローチを歓迎する。この法案は、前政権が導入した SOCI 改革を控えめかつ論理的に拡張したものである。

限定使用規定

連合メンバーは、サイバーセキュリティ法案および情報サービスおよびその他の法改正（サイバーセキュリティ）法案 2024（ISA 法案）における使用制限条項を歓迎する。この条項は、事業体に対して、サイバーインシデントについて政府に開示した情報が、将来、事業体の利益に反して使用されないという保証を提供するものである。

オーストラリア情報局のレイチェル・ノーブル前局長は 2022 年 11 月、このコンセプトを公に支持した：

> 純粋に *ASD* の観点から言えば、セーフハーバーのコンセプトは非常に優れたアイデアだと思う。なぜなら、あなたの指摘する曖昧な部分、つまり、もし私が政府を相手にしているのであれば、その情報を他の政府部門に渡すのか渡さないのか？私の許可なくそのようなことが起こらないことを、どうすれば確認できるのか？そのため、オペレーションという観点からは、インシデントが発生し、まだ人々を水から救い出し、救命ボートに乗せようとしているとき、民間企業にとって、少なくとも *ASD* とのオペレーション上の関わりは、他の政府機関であろうと、例えば集団訴訟で見られるようなプロセスを精査する他の人々であろうと、他者の調査から除外されるという絶対的な信頼があることは、我々にとっても非常に魅力的である。[1]

[1] レイチェル・ノーブル豪州通信局長、外務・国防・通商法制委員会ハンサード、上院予算案、キャンベラ、2024 年 11 月 8 日、15 頁。

連合は、2023 年 3 月 22 日に限定使用義務の法制化を初めて要求したが、連合メンバーは、もしオーストラリア政府がこの改革をより迅速に進めていれば、その間に見られた、ASD とタイムリーに情報を共有しようという産業界の意欲の低下に対して、一定の効果があったかもしれないと指摘している。

スマートデバイスのセキュリティ標準

サイバーセキュリティ法案 2024 で提案されたスマートデバイスの標準規格は、歓迎すべきものであり、長年の懸案であった。この提案は、前連立ガバナンスが 2021 年 7 月 13 日に発表したディスカッションペーパー「オーストラリアのサイバーセキュリティ規制とインセンティブの強化 - オーストラリアのサイバーセキュリティ戦略 2020 のイニシアティブ」において初めて提案されたものである。

中国製のカメラやドローン、インターネットに接続されたソーラー・インバーターが英連邦政府の敷地内で何百台も使用されていることが相次ぐ監査で明らかになり、インターネット接続機器の国家安全保障上のリスクが明らかになったため、こうした改革の必要性は近年ますます高まっている。

ガバナンス政府にはこの提案を練り上げ、洗練させる十分な時間があり、この作業がようやく結実したことを歓迎する。

サイバーインシデント審査会

連合メンバーは、サイバーインシデント審査会の法制化を歓迎する。連合は当初、2023 年 10 月 19 日にこの構成を要求し、教訓から恩恵を受ける可能性のある組織の集合的な利益のために、重大なサイバーインシデント後に冷静で客観的な調査を実施するメカニズムの必要性を指摘した。これは、米国政府が 2021 年にサイバー安全審査委員会の設立を発表した後のことである。もしオーストラリア政府がもっと早く同様の組織を設立していれば、メディセキュア社のデータ流出事件や今年初めに発生したクラウドストライク社の障害などの重大インシデントの事後調査を支援できたかもしれない。

とはいえ、連合メンバーは、遅ればせながら CIRB が設立されたことを歓迎し、サイバーセキュリティ法案 2024 の説明文書を修正し、サイバーインシデント審査委員会の常任委員は公務員のメンバーであるという記述を削除し、大臣が適切と判断した場合には政府外部の代表者を加える柔軟性を持たせるという勧告案を支持する。

時間枠の圧縮は、意図しない結果を招くリスクがある。

当委員会の連合メンバーは、本法案の政策意図と本報告書の勧告を支持するが、アルバネーゼ労働党政権が急ぎすぎたプロセスと限られた国会精査の時間により、本法案の意図しない結果や起草ミスを見落とすリスクを高めていることに、引き続き大きな懸念を抱いている。

クレア・オニール前内務・サイバーセキュリティ大臣は、2023-2030 年オーストラリア・サイバーセキュリティ戦略（サイバー戦略）の策定を 2022 年 12 月 8 日に発表した。サイバー戦略は 2023 年 11 月 22 日に発表され、2023 年 12 月 19 日に内務省はサイバー戦略から生じる法改正に関するコンサルテーション・ペーパーを発表し、これが今回の法案に反映された。

内務省は 9 月 4 日から 2024 年 9 月 11 日にかけて、立法改革パッケージ案の的を絞ったエクスポージャー・ドラフトを諮問した。政府は 2024 年 10 月 9 日に法案を下院に提出し、同日 PJCIS に付託した。PJCIS の報告書は 2024 年 11 月 18 日までに提出される予定であり、政府は国会が召集される前に法案を可決する意向であると理解している。

つまり、利害関係者が法案を提出する期間はわずか 2 週間しかなく、PJCIS が法案を検討し報告する期間はわずか 1 カ月強しかなかった。これらの改革が 2 年近く前から進められてきたことを考えると、政府が年内にこの法案を通過させようと躍起になっている間に、国会での精査の時間を短縮しようとしたのは不可解である。

委員長の報告書は、オーストラリア法審議会のコメントを引用しながら、こうした懸念を指摘している。

複数の関係者が同様の懸念を示した。

ソーシャル・サイバー・インスティテュートはこう述べている：

> 最大限の敬意を表するが、コストと時間の面でビジネスに重大な影響を及ぼす本法案のような巨大な法改正を、わずか *12* 営業日のパブリックコンサルテーションのプロバイダとして導入することは、単純に適切ではない。*PJCIS* は間違いなく、*3* つの複雑な法案を消化し、このような短い期間内に自分たちの立場をまとめることのできる、最も熱心で鋭い目を持つ利害関係者からのみ提出を受けるだろう。
>
> 政府が自らの立場を検討する時間が長かったために、この状況はさらに悪化している。説明文書によれば、このパッケージは *2023* 年 *12* 月から *2024* 年 *3* 月にかけて出された協議文書と、*2024* 年 *9* 月 *4* 日から *11* 日までの「的を絞った協議」に由来する。したがってアルバネーゼ政府には、*2024* 年 *3* 月 *1* 日から *9* 月 *4* 日まで、そして *9* 月 *11* 日から *10* 月 *9* 日まで、少なくとも *222* 日間、この法律のドラフトを検討する時間があった。わずか *2* 週間で、この法律案に関する詳細な産業界や利害関係者のフィードバックを求めるのは、サイバーセキュリティをめぐる産業界との「広範な協議」を擁護しようとする政府の行動とは矛盾している。[2]

.auDA も同様の懸念を共有している：

> 全体として、これらの改革に関する協議プロセスは、サイバーセキュリティという重要な分野における産業界と政府との親善を深めるために、より多くの時間を割くことが有益であると考える。
>
> よりサイバーセキュアなオーストラリアへの道のりは、政府と産業界の真のパートナーシップでなければならず、すべての関係者と協議し、意見を聞くために十分な時間を取ることによってのみ達成される。[3]

オーストラレーシア高等教育サイバーセキュリティサービスも同様だ：

---

[2] ソーシャルサイバー研究所、投稿 *18*、p8-9。

[3] au Domain Administration Ltd (auDA), *Submission 18*, p. 7.

> しかし、合計 *300* 頁を超える読み物である *3* つの法案に *2* 週間しか回答期間を設けられないのは、改革パッケージの徹底的な検討と協議には不十分である。産業界が有意義な意見を述べるための十分な機会を確保するため、関連する協議（法的検討、グループ協議、提出書類の草案作成など）の時間を確保できるような回答期限を検討していただきたい。この重要なサイバーセキュリティ法制に適切な時間枠は、最低 *4* 週間であろう。[4]

政府は、こうした懸念にまったく無関心であり、このような非常に複雑で重大な法案を適切に精査するためには、限られた調査期間では不十分であることは明白である。委員長の報告書は、この調査を通じてすでに指摘された数多くの懸念や潜在的な問題を網羅しており、より綿密な精査を行えば、さらなる検討が必要な領域がさらに明らかになるのは当然である。

連合は、この性急なアプローチに繰り返し警告を発してきた。この性急なプロセスの結果、将来、予期せぬ事態が発生した場合、それはすべて政府に責任がある。

アンドリュー・ウォレス議員　　サイモン・バーミンガム議員

副議長

アンドリュー・ヘイスティ議員　　ゾーイ・マッケンジー議員

ジェームズ・パターソン上院議員

[4] Australasian Higher Education Cybersecurity Service (AHECS), *Submission 22*, p 4-5.

A.提出書類リスト

1 オーストラリア統合経済研究所

2 良心のエンパワーメントのためのベトナム海外イニシアティブ（VOICE）オーストラリア

3 オーストラリア・リスク政策機構

4 マッコーリー大学

5 オーストラリア商工会議所

6 レベッカ・トラパニ

7 DLC リーガル

8 タスマニア州首相・内閣府

9 オーストラリア保険審議会

- 9.1 提出書類 9 の補足

10 グループ・オブ・エイト

11 オーストラリア産業グループ

12 CISO レンズ

13 ポール・ウィルキンス

14 グレッグ・ピーク氏

15 消費者金融協会

16 .au ドメイン管理株式会社

17 アクティブ・サイバーディフェンス・アライアンス

18 ソーシャルサイバー機構

19 クオッカ

20 BSA｜ソフトウェア・アライアンス

- 20.1 提出書類 20 の補足

21 オーストラリア・コミュニケーション消費者行動ネットワーク

22 オーストラリア高等教育サイバーセキュリティサービス

23 インタラクティブ・ゲーム＆エンターテインメント協会

24 ジオマスタリー アドバイザリー

25 オーストラリアの大学

26 マーク・ピディントン

27 オーストラリア会社取締役協会

28 デパートメント 13 インターナショナル社

29 メディシンズ・オーストラリア

30 グローバル・シールド

31 マッコーリーテクノロジーグループ

32 良き先祖のポリシー

33 ハッカーワン

34 サイバーセキュリティ連合

35 テルストラ

36 オーストラリア水道協会および水道セクター・グループ

37 オーストラリア・ビジネス評議会

38 オーストラリア・インターネット協会

39 オージー・ブロードバンド

40 サムスン電子オーストラリア

41 サイバーCX

42 オーストラリア・ガバナンス機構株式会社

43 アマゾン・ウェブ・サービス

44 オーストラリア情報セキュリティ協会

- 44.1 提出書類 44 の補足

45 コンシューマー・エレクトロニクス供給協会

46 オーストラリア退職年金基金協会（The Association of Superannuation Funds of Australia Ltd.

47 アップガード

48 オーストラリア中小企業団体協議会

49 オーストラリア技術評議会

50 株式会社エクリプシアム

51 ペクサ

52 インフォブロックス

53 今すぐアクセス

54 情報技術産業協議会

55 ノティオン・デジタル・フォレンジック

56 プラシャント・シン、インド・オーストラリア・テクノロジー・フォーラム

57 パロアルトネットワークス

58 アウスグリッド

59 内務省

60 ビクトリア州情報コミッショナー事務所

61 オーストラリア通信総局

62 オーストラリア法評議会

- 62.1 提出書類 62 の補足

63 コンフィデンシャル

64 コンフィデンシャル

B.公聴会の証人リスト

2024 年 10 月 31 日（木

委員会室 2R1

キャンベラ

オーストラリア情報セキュリティ協会

- アカシ・ミッタル（議長

サイバーセキュリティ連合

- アリ・シュワルツ（コーディネーター

サイバー*CX*

- ウィリアム・ストルツ博士（シニア・マネージャー

BSA｜ソフトウェア・アライアンス

- APAC シニア・ポリシー・マネージャー シェン・ホン・タム氏

パロアルトネットワークス

- サラ・スローン オーストラリア・ニュージーランド・インドネシア ガバメント・アフェアーズ・公共政策部長

オーストラリア会社取締役協会

- クリスチャン・ゲルギス政策部長
- サイモン・ミッチェル シニア・ポリシー・アドバイザー

オーストラリア・ビジネス評議会

- マイク・バレヤ、デジタルテクノロジー、AI、サイバー、未来産業担当ディレクター

オーストラリア中小企業団体協議会

- ルーク・アハテルストラット CEO

マッコーリー大学

- ロス・マクレナン博士、研究サービス担当副学長

オーストラリア高等教育サイバーセキュリティサービス

- サイバーセキュリティ担当ディレクター、ニッキー・ピーバー氏

オーストラリアの大学

- 最高経営責任者 ルーク・シー氏

2024 年 11 月 1 日（金

委員会室 2R1

キャンベラ

オーストラリア法評議会

- ジョン・キーブス ビジネス法部門エグゼクティブ・メンバー
- アニー・ハガー、フューチャーズ委員会メンバー
- ネイサン・マクドナルド 政策担当副本部長

オーストラリア・コミュニケーション消費者行動ネットワーク

- 最高経営責任者 キャロル・ベネット
- ガレス・ダウニング博士（副最高経営責任者

オーストラリア通信総局

- デール・ファース A/g 事務局長
- ステファニー・クロウ、オーストラリア政府サイバーセキュリティ局次長兼オーストラリア・サイバーセキュリティセンター長
- スティーブン・マクグリン、チーフ・カウンセル、法務・コンプライアンス・戦略担当事務局長代理

内務省

- ミシェル・マクギネス CSC 中将、国家サイバー・セキュリティ・コーディネーター、国家サイバー・セキュリティ局
- ヘイミッシュ・ハンスフォード、サイバー・インフラ・セキュリティ担当副長官
- サリー・ファイファー重要インフラ・パートナーシップ・政策担当第一次官補
- ピーター・アンスティ第一次官補（サイバー・テクノロジー・セキュリティ政策担当） - アシュレイ・ベル次官補（サイバー政策・プログラム部門担当
- 重要インフラ・セキュリティ政策部次官補、エミリー・グラント氏
- 重要インフラ戦略政策課長 シルパ・マニア氏
- ジェシカ・ロビンソン、サイバーセキュリティ法セクション・ディレクター
- セキュア・テクノロジー・セクション ディレクター ジョージナ・パポウツシ氏