The Software Alliance

BSA

アジア太平洋地域サイバーセキュリティダッシュボード

安全なグローバルサイバースペースへの道筋

galexia

目次

エグゼクティブサマリー

デジタル経済がもたらす機会を最大化し、ステークホルダーとの協働を最大限に活用するためには、政府は、法と規則を上手く組み合わせ、サイバーセキュリティに対し明確な指針を示すよう、適切に機関と仕組みを創設することが必要です。また、これらのステップは、政府から民間企業までの全ての関係者が協力して行う、システムの防護、サイバー攻撃の阻止、軽減及び対処に役立つものです。

これらの目標達成のために創設される機関及びフレームワークは、安定かつ明確なものである必要があると同時に、テクノロジーが絶え間なく進化する脅威環境に対応できるだけの柔軟性を有していることも重要です。

この調査 — 初の BSA アジア太平洋地域 サイバーセキュリティダッシュボード — は、調査対象となった 10 ヶ国の政府関係者に対して、その法、規則及び政策を評価する機会を提供します。

イノベーションのスピードが加速していることは、我々の周りのいたるところで顕著です。習慣から今でも「電話」と呼ぶ、ポケットに入る非常にパワフルなマイクロコンピューターから、生活の中で日に日に増加するセンサー製品まで、イノベーションは、世界経済のほぼすべてのセクターに革命をもたらしています。農業、製造業から通信及び公益事業まで、ソフトウェア主導型技術は、世界中の人々に新たな製品、サービス及び便益をもたらしています。

テクノロジーからの恩恵が増すのと並行して、脅威のリスクも増大しているのは不幸なことです。ハッカーなどの攻撃者が、犯罪目的あるいは重大な混乱や破壊を発生させるべく、脆弱性をついて、テクノロジーにより繋がった世界を手玉に取ろうとします。この事実は、サイバー空間で利用するシステムにレジリエンスと進化を可能とする柔軟性を組み込み、将来的な安全性を確保することが極めて重要であることを示しています。

政府は、採択し実行するサイバーセキュリティ政策を通じて、サイバー攻撃に対するいわば防波堤の構築を促進することができます。このような政策は、実際の攻撃インシデントの被害を軽減することや、将来新たに発現する脅威に対処することにも役立ちます。このためには、適切な法的フレームワーク、そしてこれを実行するための必要なインフラストラクチャーといった二つの要素が不可欠です。

本ダッシュボードは、調査対象となった国の政策に焦点を当てていますが、ダッシュボードを構成する質問は、成熟したサイバーセキュリティ環境を有する地域内又は世界のいずれかの国における進捗度を測る基準となり得るものです。

本ダッシュボードに関連する詳細な調査結果は、以下の URL からオンライン上で入手できます。— www.bsa.org/APACcybersecurity

本ダッシュボードから得られた要点は、以下のとおりです。

- アジア太平洋地域において、サイバーセキュリティ管理は、重要な課題と認識されているものの、本調査が含む 10 ヶ国における、包括的な国のサイバーセキュリティ戦略の策定、セキュリティ及び重要インフラストラクチャー防護に必要な法的フレームワークの実行は遅々としています。
- 公式な官民パートナーシップの欠如により、民間でのサイバーセキュリティ経験から学びを得るための機会が設けられていません。
- コンピューター緊急事態対応チーム（CERT）の設置及び国のサイバーセキュリティ教育キャンペーンの実施において、本地域は、強固さと一貫性を示しています。
- 特に、中国、インドネシア及び韓国といった一部の国におけるサイバーセキュリティ対応について、国際的なアプローチと異なる現地基準と現地テスト要件が課せられており、効果的なサイバーセキュリティへの障害となっています。

本ダッシュボードは、地域全体のサイバーセキュリティ向上に向けた多くの機会を明らかにするとともに、特定国におけるサイバー政策環境にかかる不足を指摘します。

本ダッシュボードは、サイバーセキュリティを高め、かつサイバーレジリエンスを向上するために必要な基本的ステップを詳細に検討します。つまり、政策立案者は、適切な政策的、法的及び運用上のフレームワークを確立し、様々なステークホルダーコミュニティとの協力を促進し、有益なサイバーセキュリティ情報を共有し、かつ重要インフラストラクチャー防護の優先対応をすべきです。これらの目標達成は、急を要し、本ダッシュボードは、その達成に必要な協議や討論の促進を目的としています。

本ダッシュボードに関連する詳細な調査結果は、以下の URL からオンライン上で入手できます。— **www.bsa.org/APACcybersecurity**. 政府関係者は、www.bsa.org/EUcybersecurity から入手可能な最近発行された EU サイバーセキュリティダッシュボードの結果を検討することで、世界を視野に入れてサイバー政策環境を把握することができます。

サイバーセキュリティ政策は、管理の対象であるセクターとほぼ同じ速度で進化するため、本ダッシュボードの進化も必要です。国の政府及び意志決定者が政策を進化させ、ギャップ解消に努めるのに合わせて、本ウェブサイトも、該当する地域での進捗を反映すべく更新されます。是非、これらの結果を検討され、変更に関する情報について BSA | The Software Alliance にご連絡ください。

手法

本サイバーセキュリティ調査は、6 テーマ、31 項目の評価に基づいています。各項目には、「はい」、「いいえ」、「一部該当」又は「該当なし」の回答がなされます。本調査では総合ランキングや合計点を出すことは行いません。

本分析は、公開情報に基づく机上調査の結果であり、国の政府機関との直接的面談に基づくものではありません。調査及び概要資料には、可能な限り詳細情報へのリンクを含めます。

調査期間は、2015 年 1 月 1 日に終了しており、調査した公開情報は、この日付までにおいて正確なものです。ICT インフラストラクチャー上の特定のデータの適時性については、本調査の中で別途記載します。

手法及び項目についての詳細な記述は、**www.bsa.org/APACcybersecurity** で入手できます。

強力な法的サイバーセキュリティフレームワークの構成要素

確かな法的基盤の構築

政府は、確かな国のサイバーセキュリティ戦略に基づき、包括的な法的及び政策的フレームワークを策定し、かつこれを最新のものとして維持すべきです。このフレームワークは、以下の主要な原則のもとに構築すべきです。

- **リスクベース及び優先順位設定：**サイバー脅威は、様々な態様、規模、また異なる重要度で到来します。客観的なリスク評価に基づく — 重要資産及び重要セクターを最優先とする — 優先順位設定をすることが、損害可能性が最大となるこれらの分野に注力するサイバー防御を可能にするための有効な出発点となります。
- **技術的中立性：**サイバーセキュリティ防御に対する技術的中立アプローチは、市場で最も安全かつ有効なソリューションへのアクセスを確保するために不可欠です。一定の技術のみの使用義務を指定する要件や政策は、セキュリティコントロールやベストプラクティスの進化を制限し、単一障害点を作り出す可能性があり、セキュリティを弱体化します。
- **実施可能性：**どのような戦略も、最も多くの重要資産群にとって採用可能であり、かつ最も広範囲の当事者が実施可能であって始めて有効なものとなります。民間事業者に対する政府による過度の監督、あるいはサイバーリスク運用管理における不当にわずらわしい規制による干渉は、貴重なリソースを細かな行政規則順守に割かなければならないこととなり、多くの場合、有効でスケーラブルな防御をする上で最も非生産的な結果を招きます。
- **柔軟性：**サイバーリスク管理は、専門分野横断的な機能であって、「画一的な」アプローチは存在しません。業界、システム及びビジネスがそれぞれ固有の問題に直面するため、それぞれの当事者が、それぞれ固有のニーズに対処するための柔軟性を有していなければなりません。
- **プライバシーと人権の尊重：**セキュリティ要件は、プライバシー及び人権保護の必要性との間で十分なバランスを持ったものであるべきです。要件及び義務の釣り合いが取れており、基本的権利に対して厳密に必要である限度を超えた侵害をするものでないこと、適正な手続きに従うこと、及び適切な司法的監督がなされることは、すべて、サイバーセキュリティフレームワーク策定上の重要考慮事項です。

セキュリティの主要な責任を有する運用組織の設立

政府は、サイバーセキュリティインシデント防止を推進し、かつこれに対する対応に責任を有する運用組織を設置すべきです。コンピューターセキュリティ運用、緊急事態、及びインシデント対応チームの設置が主要要素となります。

信頼関係の醸成と協業

いかなる国又は政府も、孤立してサイバーセキュリティリスクに対処することはできません。非政府団体並びに国際的パートナー及び同盟国との連携が、サイバーセキュリティに関する有効なアプローチをとる上での不可欠な要素です。

- **民間企業との提携：**インフラストラクチャーの大部分は民間企業が所有しており、有効な官民連携が不可欠です。また、協業により情報、経験及びそれぞれの立場における視点の共有が進み、リスク管理効率が向上します。信頼関係を築き、これを阻害する法律上の障害を回避するための努力が必要です。
- **孤立ではなくグローバル：**サイバー脅威がグローバルであることを考えると、有効なサイバーセキュリティ政策及び戦略は、国際的な見地を維持し、またパートナー及び同盟国との協業の上に築かれる必要があります。また、地域間及び世界的な情報共有及び保護を最大化するために、国際的、任意、及び市場主導型の標準を活用すべきです。

サイバーセキュリティリスクについての教育及び認知度向上

サイバーセキュリティの確立において、人、プロセス及び技術が等しく重要です。最高の技術を有していても、適切に使用できなければ有効なものとはなりません。明確に策定されたサイバーセキュリティの優先順位、原則、政策、プロセス及びプログラムについての認知度の向上、教育及びトレーニングを行うことが、サイバーセキュリティ戦略においての重要な要素です。

はじめに

頻発する大規模サイバーセキュリティインシデントは、アジア太平洋地域及び世界において、サイバーレジリエンスの全般的強化とサイバー攻撃からの重要インフラストラクチャー防護が極めて重要であることを明確に示しています。この目標を達成するために、官民のステークホルダーは、サイバー攻撃及びインシデントを有効に防止し、軽減し、かつこれに対応するための能力を備える必要があります。

あらゆる市場でのサイバーレジリエンスの向上への注目が増す中で、本調査 — 初の BSA アジア太平洋地域サイバーセキュリティダッシュボード — は、現行のサイバーセキュリティフレームワーク及び能力の状況について包括的に概観します。

以下に詳述するように、本ダッシュボードは、以下の 5 つの主要分野に焦点を当て、アジア太平洋地域内 10 ヶ国におけるサイバーセキュリティ政策環境を分析しています。

- サイバーセキュリティのための法的基盤
- 運用能力
- 官民パートナーシップ
- セクター毎のサイバーセキュリティ計画
- 教育

さらに、本ダッシュボードは、国の法制度が、世界的なサイバーセキュリティサービスプロバイダーに対して差別的であるか、不必要な制約や要件を課しているか、についての評価を目的とした一連のサイバー法指標を設け、調査しています。

法的基盤

政策立案者は、公共団体及び民間企業の両者が、益々繋がる世界におけるサイバーセキュリティ問題への対処能力を確保する上で、主要な役割を果たします。彼らは、適切な法的及び政策的フレームワークの確立だけでなく、サイバーセキュリティの認知度向上活動及びサイバーレジリエンス向上のための取り組みに関与する当事者との協業を通じてこれを達成することができます。

本フレームワークの主要要素であり、基礎となるのは、サイバーリスク管理とその取組みを支える立法のために重要な**国のサイバーセキュリティ戦略です。**強力なサイバーセキュリティ戦略は、キーとなる官民のステークホルダーと共同で作成、実施され、また随時更新される「生きた文書」であるべきです。またそれには、社会的価値、伝統及び法理を反映した原則と優先順位が明確に規定され、含まれているべきです。

このアジア太平洋地域内 10 ヶ国を対象とするサイバーセキュリティのための法的フレームワーク調査結果は、多様な回答を示しています。具体的には、オーストラリア、インド、日本、シンガポール及び台湾といった国は、セキュリティ、分類及び重要インフラストラクチャー防護の各要件について、立法及び政策手段によって裏付けられた、詳細かつ包括的なサイバーセキュリティ戦略を備えています。しかし、インドネシアは、未だサイバーセキュリティ

**政策立案者は、公共団体及び民間企業の両者が、益々繋がる世界における
サイバーセキュリティ問題への対処能力を確保する上で、主要な役割を果たします。**

戦略を策定していません。他の国 — 中国、マレーシア、韓国及びベトナム — では、一部でサイバーセキュリティ措置を実施していますが、国のサイバーセキュリティ戦略は未だ開発中です。

政府は、最優先で防御すべき重要サービス及びインフラストラクチャーについて調査し、それらについて明確な優先順位を設定すべきです。すべての資産、システム、ネットワーク、データ及びサービスが等しく重要であるわけではありません。従って、意志決定者は、インフラストラクチャーを評価し、サイバーセキュリティインシデントがもたらす危険、損害又は破壊が国に与える影響を考慮して、重要サービス及び機能を提供しているものを特定すべきです。

重要インフラストラクチャーが特定されたら、脆弱性及びギャップを特定し対処するために、それらのサイバーレジリエンスを評価する必要があります。民間企業が開発したベストプラクティスでは、多くの場合、重要システムのサイバーレジリエンスをテストするための体系的な社内及び第三者監査が含まれています。

サイバーセキュリティ関連情報を共有することが、官民双方のステークホルダーにとって、サイバーレジリエンスを得るための有効なアプローチを構築する上で重要であることは言うまでもありません。情報共有をうまく行うことにより、ステークホルダー全体の認知度を高め、彼らがセキュリティに向き合う姿勢を、脅威状況の進化に応じて適合させることが可能となります。

ただし、情報を有効に共有するには情報保護が不可欠です。そして、そのための適切な情報分類要件が必要です。

政府は、官民パートナーシップを醸成し、業種固有の連携を支援することによって情報共有を促進すべきです。また、必要な人的及び技術リソース、運用組織を提供し、反トラスト請求、不当な開示要求又は損害賠償請求に対する適切な法的保護を与えるべきです。さらに、情報共有を阻害し得る政策及び法律上の障壁を特定し、これに対処すべきです。

運用組織

国にとって重要な情報ネットワーク及びシステムの機密性、完全性そして可用性を脅かす重大な事由に対処するために、インシデント対応機能を設置すべきです。コンピューター緊急事態対応チーム（CERT）及びコンピューターセキュリティインシデント対応チーム（CSIRT）は、サイバーレジリエンスの向上において重要な役割を果たします。

これらの団体は、攻撃を受けた被害者に対してインシデント対応サービスを提供し、政府、民間企業及び場合によってはより広範な一般公衆におけるステークホルダーに対し、脆弱性及び脅威に関する情報を共有し、その他、コンピューター及びネットワークの安全性の向上に資する手段を提供します。

アジア太平洋地域内でのサイバーセキュリティについての本調査の対象となった 10 ヶ国すべてが、サイバーセキュリティインシデントの報告及び対応の管理において重要な役割を担う CERT 機能を有しています。調査対象となった大部分の国は、国又は地域が実施するサイバーセキュリティ訓練に参加しており、サイバーセキュリティ管理に必要な運用組織設置に関してはわずかなギャップが残るのみです。

官民間の有効なパートナーシップは、一層重要です。なぜなら、交通、ヘルスケア、金融及びエネルギーを司る企業を含め、非政府組織が、日々、国民が依存する重要インフラストラクチャーの多くを管理・運営しているからです。

官民パートナーシップ

有効なサイバーセキュリティには、国内のすべてのステークホルダーとの連携と協調が必要です。官民間の有効なパートナーシップは、一層重要です。なぜなら、交通、ヘルスケア、金融及びエネルギーを司る企業を含め、非政府団体が、日々、国民が依存する重要インフラストラクチャーの多くを管理・運営しているからです。

サイバーセキュリティのために官民パートナーシップを確立することの重要性は、アジア太平洋地域で認識されていますが、その展開は、未だ初期段階です。日本とマレーシアは、サイバーセキュリティのための公式な官民パートナーシップの確立について、主導的立場にあり、他の多くの国でも強い関心があります。

業種固有のサイバーセキュリティ計画

サイバーセキュリティ防御の一定の要素がすべての分野に亘るものであり、様々な提言が国内及び国際組織から提供される一方で、特定の団体の事業上のニーズに個別的な、あるいは特定業種や特定業務における固有のリスクに対応するための手段提供についての指針も必要です。

サイバーセキュリティに対する業種固有の対応確立においては、一部関心が高まっていますが、アジア太平洋地域での実施は極めて限定的です。オーストラリア、マレーシア及びシンガポールがこの分野を主導しており、いずれ他の国々も独自の業種固有イニシアチブをもって追従すると思われます。

教育

法人であれ団体であれ、一ステークホルダーが単独でサイバースペースの安全を確保することはできませんし、全ての個人そして団体はサイバーセキュリティに協力する責任を有します。政府及びあらゆる規模の組織並びに消費者は、それぞれの役割を担い、システムの安全確保、教育及び認知度向上への取組みを進める必要があります。

これには、教育及び認知度向上キャンペーンに加えて、大学及びより早期の教育課程におけるサイバーセキュリティ教育プログラムの開発と展開への支援が必要です。

アジア太平洋地域では、一般市民に対するサイバーセキュリティの認知度向上を目指した革新的なプログラムを含めて、サイバーセキュリティ教育に対して多大なリソースを投じられてきました。インドネシア及び台湾など少数の国は、国による教育戦略やプログラムが未実施ですが、このギャップは、近い将来解決すべきです。

追加サイバー法指標

この調査は、サイバーセキュリティの管理にマイナスの影響を及ぼしうる、アジア太平洋地域 10 ヶ国での多くの追加サイバー法指標を特定しています。これは、サイバーセキュリティ製品のための適切な国際標準の開発及び使用を妨げる現地の要件や、サイバーセキュリティベンダーの国籍に対する制限が含まれます。また、国際標準に対する実績が実証済みであるサイバーセキュリティ製品に対し、追加的負担となる不必要な現地のテスト要件もこれに含まれます。

真のセキュリティへの道のりを妨げる障害

一部の政府では、今日、本来のセキュリティ懸念に対する必要性を超えて、様々な政策を正当化するためにサイバーセキュリティを引き合いに出しています。このような政策は概してサイバーセキュリティを向上するのではなく、逆に弱体化させる結果を招きます。また、意図的かどうかを問わず、商品やサービスを提供するグローバル企業に対する不当な市場参入障壁を課すこととなります。

不必要又は不当な要件

適切なサイバーセキュリティ政策をとることで、組織は可能な限り広範な、最新サイバーセキュリティソリューションの選択肢の中から選び、開発及び採用をすることが可能となります。また、これにより、直面する特定のリスク軽減において最も有効なセキュリティ対策を実施することが可能となります。

しかし、一部の政府は、選択肢を制限し、費用を増大させ、企業が最も適切なサイバーセキュリティツールを使用することを妨げる、様々な要件を課しています。国独自の認証条件や現地のテスト要件、現地コンテンツの強制、ソースコードや暗号キー等の機微情報の開示要件及び知的財産の外国人による所有の制限などがこれに含まれます。

標準の変更

技術標準は、サイバーセキュリティを実現し拡張するために不可欠な役割を果たします。業界の参加によって開発され、かつ市場全体で受け入れられている国際的に認識された技術標準に準拠することにより、企業が、より新しく、より安全な商品をより迅速に開発・販売することが可能となります。

ところが、一部の政府は、国固有の規則を課すことがサイバーセキュリティ向上に通じると主張し、国固有の標準を課しています。しかし、実際の効果は反対です。政府が課す標準は、セキュリティを補強するというよりはむしろ、イノベーションを止め、消費者や企業に対し、ニーズに合わない可能性の高い製品の使用を強制することを招きます。

データローカライゼーション規則

グローバルなクラウドコンピューティングサービスの進歩により、世界中あらゆる規模の企業が、かつては大企業しか利用できなかった強力なリソースを利用することができるようになりました。しかし、クラウドモデルは、複数の場所、ひいては複数の国でのデータの保管及び処理を可能とするネットワークに基づくものです。データが複数国間を自由に移転することを認めることによって、クラウドプロバイダーは、信頼性、レジリエンス及び24 時間体制のサポートサービスを含む多くの利点を提供することができます。

データは特定の場所にあってより安全である、という誤った仮定に基づいて、一部の国では、国境を超えたデータ移転を禁止するあるいは著しく阻害する規則を課しています。データの自由な移転を不必要に制限する政策は、費用を増大させ、かつ新興のクラウドによって可能となるサービスへのアクセスを妨げることにより、クラウドコンピューティング最大の利点を弱体化させます。

国内技術の優先

最新の製品及びサービスは、多くの異なった国の研究・設計センターをまたがるグローバルな協力を通じて開発されています。国は、任意の技術移転、改良された製品及びサービスの迅速な開発及び展開を促進するために国境を越えた協力体制を促すインセンティブを提供すべきです。

しかし、一部の国は、外国との競争を回避することが、国内優良企業保護、国内テクノロジー業界促進、かつサイバーセキュリティ向上につながると考え、反対のアプローチを採用しています。国内で生まれた技術も、本来は世界的なイノベーションの一部です。外国との競争の回避は、企業や政府機関が世界レベルの製品及びサービスを購入することを否定することであり、サイバーセキュリティが減じられる結果を招きます。さらに、このような政策は、国内テクノロジー企業がグローバルリーダーと協働する価値のある機会を剥奪し、その国際競争力を低下させ、世界的イノベーションを妨げることとなります。

アジア太平洋地域サイバーセキュリティダッシュボード

✔ はい　✖ いいえ　◑ 一部該当

#	質問
	法的基盤
1.	国のサイバーセキュリティ戦略が整備されていますか？
2.	国のサイバーセキュリティ戦略が採択されたのは何年ですか？
3.	重要インフラストラクチャー防護（CIP）戦略又は計画が整備されていますか？
4.	書面による情報セキュリティ計画の制定を義務付ける立法・政策がありますか？
5.	「システム」の棚卸及びデータの分類を義務付ける立法・政策がありますか？
6.	セキュリティ施策・要件のリスクレベルに対するマッピングを義務付ける立法・政策はありますか？
7.	（少なくとも）年１回のサイバーセキュリティ監査を義務付ける立法・政策がありますか？
8.	政府のサイバーセキュリティ能力についての公開報告書を義務付ける立法・政策がありますか？
9.	各機関に対して最高情報責任者（CIO）又は最高セキュリティ責任者（CSO）の設置を義務付ける立法 / 政策がありますか？
10.	サイバーセキュリティインシデントの所定の報告を義務付ける立法・政策がありますか？
11.	立法・政策は、「重要インフラストラクチャー防護」（CIP）についての適切な定義を含むものですか？
12.	官民によるサイバーセキュリティソリューションの調達要件は、追加の現地要件を課すことなく、国際的な認定又は認証スキームに基づくものですか？
	運用組織
1.	国のコンピューター緊急事態対応チーム（CERT）又はコンピューターセキュリティインシデント対応チーム（CSIRT）が存在しますか？
2.	コンピューター緊急事態対応チーム（CERT）が設置されたのは何年ですか？
3.	ネットワーク及び情報セキュリティ（NIS）のための国の管轄官庁がありますか？
4.	サイバーセキュリティインシデントデータ収集のためのインシデント報告プラットフォームはありますか？
5.	国のサイバーセキュリティ訓練が実施されていますか？
6.	サイバーセキュリティインシデントに対応するための国のインシデント管理の仕組み（NIMS）が存在しますか？
	官民パートナーシップ
1.	サイバーセキュリティについて定義された官民パートナーシップ（PPP）が存在しますか？
2.	業界ごとに組織化されていますか（事業又は業界ごとのサイバーセキュリティ評議会が存在する等）？
3.	新たな官民パートナーシップが計画中又は進行中ですか（その場合、どの分野に焦点を当てていますか）？
	業界固有のサイバーセキュリティ計画
1.	サイバーセキュリティに対処する官民共同計画がありますか？
2.	業界ごとにセキュリティの優先順位が定義されていますか？
3.	なんらかの業界サイバーセキュリティリスク評価が実施されていますか？
	教育
1.	若年層に対し、サイバーセキュリティについての一般知識を向上させ、サイバーセキュリティ認知度を増すための教育戦略が存在しますか？
	追加サイバー法指標
1.	サイバーセキュリティサービスは、ベンダーの国籍に基づく差別を行う法が課されることなく運営することができますか？
2.	サイバーセキュリティサービスは、特定の技術の使用を義務付ける法又は政策が課されることなく運営することができますか？
3.	サイバーセキュリティサービスは、国際的なテスト要件を超えた追加的な現地テスト要件が課されることなく運営することができますか？
4.	サイバーセキュリティサービスは、ソースコードその他の専有情報の提出を義務付ける法又は政策が課されることなく運営することができますか？
5.	サイバーセキュリティサービスは、サービスプロバイダーに対してサーバーを対象国内に設置することを要求する法又は政策が課されることなく運営することができますか？
6.	サイバーセキュリティサービスは、クロスボーダーのデータ移転に対する不必要な制限（登録要件等）が課されることなく運営することができますか？

オーストラリア	中国	インド	インドネシア	日本	マレーシア	シンガポール	韓国	台湾	ベトナム
✔	◑	✔	✖	✔	◑	✔	◑	✔	◑
2009	–	2013	–	2013	–	2013	–	2013	–
✔	✔	✔	✖	✔	◑	✔	◑	✔	✖
◑	✖	✖	◑	✔	✖	◑	◑	✖	◑
✔	✔	◑	✔	✔	✔	✔	✔	✔	✔
✔	✔	◑	◑	✔	◑	✔	✔	✔	◑
✖	✖	✖	◑	✖	✖	◑	◑	✔	✖
◑	◑	◑	✖	✖	◑	✖	✖	◑	✖
✔	✖	◑	✖	◑	◑	◑	✖	✔	✖
✔	✖	✔	✖	◑	✖	✖	✖	✖	✖
✔	✖	✔	✖	✔	✔	✔	✔	✔	✖
✔	✖	◑	✖	✔	✔	✔	◑	N/A	N/A
✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2010	2002	2004	2007	1996	1997	1997	1996	1998	2005
✔	◑	✔	✔	✔	✔	✔	✔	✔	✖
✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
◑	✔	✔	✖	✔	✔	◑	✔	✔	✖
✔	✖	◑	✖	◑	✔	✖	◑	✔	✖
✖	✖	◑	◑	✔	✔	✔	◑	◑	◑
◑	◑	✔	◑	✔	◑	◑	◑	◑	✔
✖	✖	◑	✖	✔	–	✖	✖	◑	✖
◑	✖	✖	✖	✖	✔	◑	✖	✖	✖
✖	✖	✖	✖	✖	✖	◑	✖	◑	✖
✖	✖	✖	✖	✖	✖	◑	✖	✖	✖
✔	◑	✔	✖	✔	✔	✔	◑	✔	◑
◑	✖	◑	✖	✔	◑	✔	◑	✔	✖
✔	◑	✔	✔	✔	✔	✔	✔	✔	✖
✔	✖	✖	✖	✔	✔	✔	✖	✔	✔
✔	✖	✔	✖	✔	✔	✔	✔	✔	✔
◑	◑	✔	✖	✔	✔	✔	✔	✔	✖
✔	◑	✔	◑	✔	✔	✔	◑	◑	✔

有益なサイバー脅威情報共有のための適切なフレームワーク整備

サイバーセキュリティインシデント又は漏洩は、政府及び民間企業、並びに個人に多大な影響を及ぼす可能性があります。注目を集める漏洩事件は、世界中の政府に対して、いかにしてこれらのインシデントを最善の方法で防止、検知し、かつ対応するかを検討することを促しています。

適切な時点での適切な情報の交換及び共有 — 並びにこれを可能とする当事者間の協業 — は、リスクを削減・軽減し、サイバーインシデントに対応するための最良の方法と考えられます。

従って、問題は、どのような方法がステークホルダー間での有益かつ有効な情報共有達成手段として最良かということになります。一部の国では、強制的なインシデント通知システムを考えていますが、これだけでは、集団での認知度及び準備度の問題に対処するには十分ではありません。これに関しては、信頼に基づく任意の情報交換が、情報共有の成功のために最も有効な手段であることが証明されています。

このような有益な情報共有の実現は、容易ではありません。かかる交換を促進する必要な環境が整備されて初めて、達成可能になります。このような環境の基本的要素の一部は以下のようなものです。

- **信頼関係の醸成：**サイバー脅威情報共有やインシデント報告には、その効果的な機能のためのセーフガード及びインセンティブが必要となります。これらの要素は、このような制度の運用に必要な信頼の確保に役立ちます。これは、情報の共有によって、これを提供する組織に、不当な責任、公辱、訴訟又は制裁が生じないことの保証を含みます。
- **高度の機密性の確保：**重要インフラストラクチャーに影響を及ぼすインシデント又はサイバー脅威について共有される情報の機微性を考慮して、インフラストラクチャー運営者と監督官庁との間の通信の機密性及びセキュリティが、当該官庁による透明性のある報告義務を除き、尊重かつ維持されることの約束が不可欠です。

  時により、一般公衆に対してインシデントを知らせることが必要となる場合もあります。このような場合、攻撃対象の増加、インシデントの影響の増幅、パニックの発生あるいは不当な公辱を招くことを回避するために、開示前に、侵害の被害を受けた企業と当該官庁との間での綿密な対話を確保するためのあらゆる注意がはらわれるべきです。
- **相互関係の確保：**民間企業が国の多くの重要インフラストラクチャーの所有及び運営をしていますが、情報共有は、民間企業から政府への該当する情報の一方向の提供と見られるべきではありません。これは、信頼と相互利益に基づいた、真のかつ相互の情報交換とみなすべきです。
- **要件の明確性と複数法域における一貫性：**強制的な通知要件は、かつてないほど多くの地域を対象とするものであるため、相反する法律上の義務に直面する可能性が増しています。様々な組織が異なった国及び地域に亘る複数のセクターで事業運営を行っているため、何をいつ誰に対して報告するかという問題は、重要な法令遵守上の課題となっています。従って、強制通知制度を導入すべき場合であっても、異なった通知義務間や、様々な国及び地域間で、可能な限り高い一貫性を保つようにすることが不可欠です。

アジア太平洋地域サイバーセキュリティ国別サマリー

以下のサマリーは、上記の条件に基づいた、主要なサイバーセキュリティ立法及び政策、並びに各法域内で現在運営している主要団体に焦点を当てた、サイバーセキュリティ環境を概説するものです。調査対象となった各国についてのより詳細な情報については、www.bsa.org/APACcybersecurity で入手可能な国別サマリーをご参照ください。

オーストラリア

法的基盤：オーストラリアのサイバーセキュリティ戦略は、2009 年に採択され、現在改訂作業中です。改訂版の戦略は、2015 年後半に発表予定です。オーストラリアは、情報分類について強力な法的フレームワークを有しますが、情報セキュリティを、議会立法ではなく、ガイドラインや類似の政策文書を通じて施行しており、専用の情報セキュリティ法あるいは機密情報法は存在しません。

運用組織： 2014 年に発足したオーストラリアサイバーセキュリティセンター（Australian Cyber Security Centre）は、サイバーセキュリティ及び情報セキュリティに従事する多くの機関を統括するハブとなっています。しかしながら、責任の分離については幾分か混乱が残っています。CERT オーストラリアとオーストラリアシグナルディレクトレート（the Australian Signals Directorate）の両機関がインシデント報告サービスを運営しています。

官民パートナーシップ：オーストラリアは、サイバーセキュリティための公式な官民パートナーシップを有しませんが、CERT オーストラリアが認知度向上プログラム及び重要インフラストラクチャー防護において民間企業と協働しています。また、サイバーセキュリティ戦略審査プロセスにおいて民間企業に対する諮問が行われています。

業界固有のサイバーセキュリティ計画：オーストラリアにおいて、サイバーセキュリティに対処する官民共同計画は存在しません。重要インフラストラクチャーレジリエンス戦略（Critical Infrastructure Resilience Strategy）が信頼される情報共有ネットワーク（Trusted Information Sharing Network）（TISN）の主要な部分として「業界団体」の参加を強調していますが、TISN は、業界固有の計画を作成することを意図したものではありませんでした。

教育：オーストラリアは、すべての年齢グループについて包括的サイバーセキュリティ教育戦略を整備しており、教育資材及びイニシアチブに多額の投資を行っています。

追加サイバー法指標：オーストラリアは、おおむね、技術プロバイダーに対して国固有の制約（例えば、強制的な技術要件、現地テスト要件、及びソースコード共有の要件）を課していませんが、調達分野において一部制約及び負担が存在します。

中国

法的基盤：現在、中国はサイバーセキュリティ戦略を有していませんが、いくつかの政府政策は、サイバーセキュリティについての助言を含んでいます。中国においてサイバーセキュリティにフォーカスした一つの特定の法は存在しませんが、2010 年国家機密法（State Secrets Law 2010）等の異なった法の下でサイバーセキュリティを対象とする多くの規定が存在します。

運用組織：中国の CERT、CNCERT/ CC. は、2002 年に設置されました。国の情報セキュリティは、様々な異なった政府機関によって取り扱われており、その運営及び目的について一般に入手可能な情報が極めて少ない場合があります。

官民パートナーシップ：サイバーセキュリティの分野において中国で官民パートナーシップに関する活動はほとんどありません。

業界固有のサイバーセキュリティ計画：中国では、サイバーセキュリティに対処する官民共同計画は存在しません。

教育：中国では国のサイバーセキュリティ教育戦略は整備されていませんが、一部の臨時の教育イニシアチブが CERT 及び産業情報技術省（Ministry of Industry and Information Technology）によって取られています。

追加サイバー法指標：中国は、サイバーセキュリティサービスプロバイダーに対して広範囲の法律的及び政策的制約を課しています。

インド

法的基盤：インドのサイバーセキュリティ政策（National Cyber Security Policy）は、2013 年に採択されました。これは、高度の原則並びに的を絞った目標及び提案の両方を含む詳細な計画です。しかしながら、計画は、完全に実施されておらず、サイバーセキュリティを支える法的フレームワークは弱いままとなっています。

運用組織：国の CERT である CERT-In は、情報セキュリティに関する高度の政策協議に関与しています。

官民パートナーシップ：インドにおいて民間企業を代表する団体は、充実しており、サイバーセキュリティに関して積極的です。また、CERT-In は、民間企業と連携していますが、専用の官民パートナーシップは存在しません。

業界固有のサイバーセキュリティ計画：インドでは、サイバーセキュリティに対処する官民共同計画は存在しません。サイバーセキュリティに係る官民パートナーシップについて協議しかつ提言を行うために共同ワーキンググループが設置されています。ワーキンググループのメンバーには業界の代表者が含まれています。

教育：一連のプロモーション活動及び教育イニシアチブを通じたサイバーセキュリティ認知を促すことは、2013 年インドサイバーセキュリティ政策（Indian National Cyber Security Policy 2013）の目標の一つであり、かかる政策は、サイバーセキュリティについての包括的な全国的認知度向上キャンペーンに対する約束も含みます。

追加サイバー法指標：インドは、サイバーセキュリティプロバイダーへのいくつかの法的及び政策的負荷を回避していますが、国際的なテスト体制の追加となる現地テスト要件を課し続けています。

インドネシア

法的基盤：インドネシアは、サイバーセキュリティ戦略策定の初期段階にあります。インドネシアにおけるサイバーセキュリティについての法的フレームワークは弱いものです。明確な機密セキュリティ法又は政策は存在せず、またセキュリティ施策は、異なった立法に亘って散在しています。特定のサイバーセキュリティ規定は整備されていません。

運用組織：国の CERT である ID.SIRTII/CC は、稼働の初期段階にあるようです。ID.CERT は、非政府 CERT ですが、より長い期間運営されています。

官民パートナーシップ：インドネシアでは、専門のサイバーセキュリティ官民パートナーシップは存在しませんので、CERT が民間企業のための主な連携団体として行為しています。業界の代表者の協会は存在しますが、そのいずれも特にサイバーセキュリティに特化したものではありません。

業界固有のサイバーセキュリティ計画：インドネシアは、サイバーセキュリティに対処するための官民共同計画を欠いています。

教育：インドネシアは、サイバーセキュリティ教育戦略を欠いています。

追加サイバー法指標：インドネシアは、サイバーセキュリティサービスプロバイダーに対して、差別的な調達優先、現地のテスト要件及びデータ移転の制限を含む、広範囲の負担の大きい法及び政策を課しています。

日本

法的基盤：2013 年に採択された日本のサイバーセキュリティ戦略は、対策案を特定するだけでなく、日本のサイバーセキュリティに関する様々なステークホルダーの役割を定めた包括的な文書です。サイバーセキュリティを支える法的フレームワークは、2014 年サイバーセキュリティ基本法の成立を受けて、地域内で最も強力なもののうちの一つです。また、日本は、機微情報の取り扱いに関する非常に強力なセキュリティ施策及び不正アクセスインシデントへのより強力な罰則を課す新たな特定秘密保護法を 2013 年 12 月に成立させました。

運用組織：日本におけるサイバーセキュリティに関連する運用組織は、完全に成熟しています。国の cert である JCERT/CC は、1996 年に設置され、強力なウェブでの存在感を維持しています。サイバーセキュリティ戦略本部も、2014 年サイバーセキュリティ基本法に基づき設置されています。

官民パートナーシップ：日本は、サイバーセキュリティについての成熟した官民パートナーシップの仕組みを有しています。これは、そのメンバーに重要な国のインフラストラクチャーに関わる政府及び民間企業からの代表者が含まれている、J-CSIP を含みます。

業界固有のサイバーセキュリティ計画：日本では、サイバーセキュリティに対処する官民共同計画は存在しません。

教育：日本の 2013 年サイバーセキュリティ戦略は、若年層に対してサイバーセキュリティについての教育を行う詳細かつ包括的な約束を記載しています。

追加サイバー法指標：日本は、サイバーセキュリティサービスプロバイダーに対する不当な法的及び規制上の制約を回避しています。

マレーシア

法的基盤：マレーシアは、単一のサイバーセキュリティ戦略を有してはいませんが、複数の政策及び戦略を集めたものをマレーシアのサイバーセキュリティ政策（Malaysia's Cyber Security Policy）と称しています。マレーシア政府は、2017 年までにこの政策群を完全に改訂し、強化する予定であることを発表しています。

運用組織：サイバーセキュリティマレーシア（CyberSecurity Malaysia）は、国の cert — MyCert — 及び報告サービスである Cyber999 を運営しています。また、これは、情報セキュリティについての最上位の機関として行為しています。

官民パートナーシップ：サイバーセキュリティマレーシアは、官民パートナーシップモデルにおけるサイバーセキュリティについての年次総会も兼ねた表彰イベントを組織しています。

業界固有のサイバーセキュリティ計画：官民の協力は、マレーシアのサイバーセキュリティ政策の主要原則であり、これは、セキュリティ上の懸念に対処するためにセクターベースのアプローチを使用し、この目的のために 10 の重要セクターを特定しています。

教育：サイバーセーフプログラムは、サイバーセキュリティに関する包括的な資料及び活動のパッケージを提供しています。

追加サイバー法指標：マレーシアの政府調達体制は、世界的なサイバーセキュリティプロバイダーに対する一定の制約を含みますが、これ以外では、この国は不当な法的及び規制上の負荷の多くを回避しています。

シンガポール

法的基盤：シンガポールは、2013 年に、5 か年計画である国のサイバーセキュリティマスタープラン（National Cyber Security Masterplan）を採択しており、重要インフラストラクチャー防護体制の開拓を継続しています。シンガポールは、一部、サイバーセキュリティのための広範囲の法的インフラストラクチャーを整備しています。新たなシンガポールサイバーセキュリティ局（Singapore Cybersecurity Agency）は、2015 年 4 月に稼働を開始します。

運用組織：SingCERT は、国のコンピューター緊急事態対応チームとして 1997 年に設立され、Infocomm Development Authority (IDA) は、サイバーセキュリティを含む情報通信政策のすべての側面のための高度な調整機関です。

官民パートナーシップ：シンガポールの政府機関は、サイバーセキュリティの分野において民間企業と密接に協働しており、官民パートナーシップの展開に対する公式な約束が存在します。

業界固有のサイバーセキュリティ計画：2008 年に立ち上げられた、Infocomm Security Masterplan 2 (MP2) には、シンガポール政府が、特に重要インフラストラクチャー所有者に関して、業界固有セキュリティプログラムの開発作業を行うことが記載されています。MP2 は、その後、MP2 の上に構築されてはいますが、セクターベースのプログラムに対する直接的な約束を含まない計画に引き継がれています。

教育：2013 年に発表された国のサイバーセキュリティマスタープラン 2018（National Cyber Security Masterplan 2018）は、サイバーセキュリティ教育に対する強い約束を含むものです。

追加サイバー法指標：シンガポールは、サイバーセキュリティサービスプロバイダーに対する不当な法的及び規制上の制約を回避しています。

韓国

法的基盤：韓国は、サイバーセキュリティに対して国のセキュリティ及び防衛にフォーカスしたアプローチをとっています。このため、2011 年に発行されたこの国のサイバーセキュリティマスタープラン（Cyber Security Master Plan）は、サイバーセキュリティ戦略というよりは、むしろサイバー防衛戦略です。これらの法的フレームワークにはわずかなギャップが一部存在します。

運用組織：KrCERT/CC 及び KNCERT（政府のみ）の両団体が設立されたコンピューター緊急事態対応チームです。情報セキュリティの責任は、韓国インターネットセキュリティ局（Korea Internet and Security Agency）に集約されており、これは、多大なオンラインプレゼンスを有しています。

官民パートナーシップ：KrCERT/CC は、そのインシデント対応職務の一部として民間企業と連携していますが、韓国においてサイバー又は情報セキュリティのための公式な官民パートナーシップは存在しません。

業界固有のサイバーセキュリティ計画：韓国には、サイバーセキュリティに対処するための官民共同計画は存在しません。

教育：韓国情報セキュリティ局は、ユーザーによるインターネットの責任ある使用を促進することに責任を負っており、当局は、広範囲のオンライン及び放送による認知度向上キャンペーンを行っています。

追加サイバー法指標：韓国は、韓国固有のテスト規則を含めて、サイバーセキュリティサービスプロバイダーに対して一定の不当な制約を課しています。

台湾

法的基盤 : 台湾の情報及び通信セキュリティタスクフォース（National Information and Communication Security Taskforce）は、いくつかの情報セキュリティ政策及び戦略（National Information Security Policy and Strategy）文書を開発しています。現行の戦略は、2013 年から 2016 年までの期間を対象としています。

運用組織 : 台湾は、二つのコンピューター緊急事態対応チームを備えており、これらが共同で台湾ネットワークに亘るサイバーセキュリティインシデントをカバーしています。ネットワーク情報及びセキュリティに対する政府の責任は、防衛省（Ministry for National Defense）が負っています。

官民パートナーシップ : 台湾において、サイバーセキュリティについて定義された官民パートナーシップは存在しませんが、CERT が民間企業と密接に連携しています。

業界固有のサイバーセキュリティ計画 : 台湾において、サイバーセキュリティに対処するための官民共同計画は存在しません。

教育 : サイバーセキュリティ教育は、国の情報通信セキュリティタスクフォースによってコーディネートされています。教育省（Ministry of Education）もサイバーセキュリティ教育ウェブサイトを展開しています。

追加サイバー法指標 : 台湾は、サイバーセキュリティサービスプロバイダーに対する不当な制約の大部分を回避していますが、一定のクロスボーダーのデータ移転の制限を認めています。

ベトナム

法的基盤 : ベトナムにおいて国のサイバーセキュリティ戦略は整備されていませんが、2012-2015 国家抗犯罪マスタープラン（2012-2015 National Anti-Crime Master Plan）が一部サイバー犯罪を極めて限定的にその範囲に含めています。ベトナムにおける重要インフラストラクチャー防護のための法的インフラストラクチャーも限定的です。情報セキュリティ法（Law on Information Security）案は、施行されれば、この分野における改善につながります。

運用組織 : 国のコンピューター緊急事態対応チームである VNCERT は、2005 年に設立されました。ベトナムにおけるその他の運用組織は、極めて限定的ですが、これらのギャップは、情報セキュリティ法案に含まれている提案で取り上げられているかもしれません。

官民パートナーシップ : ベトナムは、サイバーセキュリティについて定義された官民パートナーシップを有していませんが、VNCERT は、民間企業と密接に連携しています。

業界固有のサイバーセキュリティ計画 : ベトナムには、サイバーセキュリティに対処するための官民共同計画は存在しません。

教育 : ベトナムは、サイバーセキュリティ能力構築のための技術的トレーニング及び教育コースをいくつか導入していますが、一般公衆向けの認知度向上キャンペーンや教育戦略は存在しません。

追加サイバー法指標 : ベトナムは、サイバーセキュリティサービスプロバイダーに対して一定の調達制限や技術命令を課しています。

BSA について

BSA | The Software Alliance (BSA | ザ・ソフトウェア・アライアンス) (www.bsa.or.jp) は、グローバル市場において世界のソフトウェア産業を牽引する業界団体です。BSA の加盟企業は世界中で最もイノベーティブな企業を中心に構成されており、経済の活性化とより良い現代社会を築くためのソフトウェア・ソリューションを創造しています。

ワシントン DC に本部を構え、世界 60 カ国以上で活動する BSA は、正規ソフトウェアの使用を促進するコンプライアンスプログラムの開発、技術革新の発展とデジタル経済の成長を推進する公共政策の支援に取り組んでいます。

GALEXIA について

Galexia (www.galexia.com) は、世界的及びクロスボーダーでの法的及び規制上の問題点にフォーカスして、プライバシー、アイデンティティ、サイバーセキュリティ及びクラウドの分野において、最前線で、国際的研究及び助言をしています。Galexia は、国々がサイバーセキュリティの問題に対処する際に生じる政策上の複雑さに関し専門知識を有しています。Galexia は、国のサイバーセキュリティ戦略、重要インフラストラクチャー防護及びサイバーセキュリティ管理及び警告システムの整備について助言します。

Galexia は、証拠に基づいた研究から明確かつ効果的な成果を生むために、国内外の企業及び政府を含む多様な顧客と密接に協働しています。Galexia は、研究及び分析に対するリアルタイムでのアクセスを提供する協調型クラウドベース報告ツールを利用しています。

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090