経済産業省

資料５

サプライチェーンサイバーセキュリティ等に関する海外の動き

経済産業省　商務情報政策局
サイバーセキュリティ課

1．米国における近年の動き

- NIST SP800-171
- NIST Cybersecurity Framework
- ボットネット及びその他の自動化・分散化した脅威に対する対策

2．欧州における近年の動き

（Cybersecurity Certification Framework等）

3．ASEANにおける状況

１．米国における近年の動き

- NIST SP800-171
- NIST Cybersecurity Framework
- ボットネット及びその他の自動化・分散化した脅威に対する対策

米国における近年の動き

● **サイバーセキュリティの視野は、『特定機能の防御（重要インフラ中心）』から『サプライチェーンリスク管理』へ拡大。**

2010.11	米国大統領令(E.O.13556)発出	米国政府全体として、CUI(*1)のセキュリティ強化の取組を開始
2014.02	**Cybersecurity Framework vesion1.0**公表	サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載
2015.06	**NIST SP800-171**策定	非政府機関の情報システム等におけるCUIの保護を目的としたサイバーセキュリティ対策の要件を規定
2016.10	**DFARS Clause252.204-7012**発行	CDI(*2)を保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求
2017.01	**Cybersecurity Framework version1.1 draft1**公表	**サプライチェーンのリスク管理（Supply Chain Risk Management）**などを追記
2017.05	米国大統領令(E.O.13800)発出	連邦ネットワーク及び重要なインフラストラクチャに対するサイバーセキュリティの強化を指示
2017.12	**Cybersecurity Framework version1.1 draft2**公表	draft1公表後のパブリックコメントを踏まえ**サプライチェーンのリスク管理の重要性の強調**や**サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk)**を追記 関係業界は肯定的に受け止め
2018.01	E.O.13800を受けた中間報告を公表	**ボットネット及びその他の自動化・分散化した脅威**に対応するためのエコシステムの強靭性の強化に関する報告書

(*1) Controlled Unclassified Information；管理対象となるが秘密指定されていない情報
(*2) Covered Defense Information

NIST SP800-171

- **NIST SP800-171は、CUIの保護を目的に14個のカテゴリと109の項目から構成。**
- **SP800-171の遵守状況に関する政府機関による第三者認証制度はなく、自己宣言という形で準拠したか否かについて判断する自己認証を採用。**

2010.11	米国大統領令(E.O.13556)発出	米国政府全体として、CUIのセキュリティ強化の取組を開始
2015.06	**NIST SP800-171**策定	非政府機関の情報システム等におけるCUIの保護を目的としたサイバーセキュリティ対策の要件を規定
2016.10	**DFARS Clause252.204-7012** 発行	CDIを保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求。

NIST SP800-171における14個のカテゴリ

(1) アクセス制御：システムへのアクセスが出来る人／機能を制限すること
(2) 意識向上と訓練：セキュリティポリシーを遵守すること
(3) 監査と責任追跡性：システムの監査を行うとともに責任の追及が出来ること
(4) 構成管理：システムを構成する機器に求められるセキュリティ構成設定を確立すること
(5) 識別と認証：システム利用者、デバイスを識別すること
(6) インシデント対応：インシデントの追跡、報告が出来ること
(7) メンテナンス：組織のシステムのメンテナンスを行うこと
(8) 記録媒体保護：CUIをセキュアに格納するとともにアクセスできる者を制限すること
(9) 人的セキュリティ：システムへのアクセスを行う個人を審査すること
(10) 物理的保護：組織のシステム、装置等への物理的アクセスを制限すること
(11) リスクアセスメント：情報資産のリスクを適切に評価すること
(12) セキュリティアセスメント：セキュリティ管理策を定期的に評価すること
(13) システムと通信の保護：システムの鍵となる通信を監視し、制御し、保護すること
(14) システムと情報の完全性：タイムリーに情報及びシステムフローを識別すること

NIST SP800-171

- **2016年10月、DFARS Clause252.204-7012が発行され、CDIを保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求。**

DFARS Clause252.204-7012における要求事項

（1）主なセキュリティ要求事項

- **NIST SP800-171のセキュリティ要求事項を満たすこと。**
- **外部のクラウドサービスプロバイダ**を利用して、保護対象防衛情報を保存・処理・送信しようとする場合には、米国のクラウドの基準Fed RAMP（NIST SP800-53を満たした事業者が提供するクラウドサービス）の要求事項と**同等の基準**を満たしており、そのサービスプロバイダが、サイバー事案報告等の要求事項を満たしていることを要請。

（2）サイバー事案報告の要求

- 契約業者が、保護対象防衛情報に影響を及ぼす等のサイバー事案を発見した場合には、国防省にサイバー事案を**速やかに報告**。
- 保護対象防衛情報の漏えいの証拠を調査。
- 国防省が実施するフォレンジック分析に必要な追加情報又は機器へのアクセスを受け入れること。

（3）下請け契約の扱い

- 契約業者は、**下請け業者の業務に必要な情報が、保護対象防衛情報であるか否かを判断し、該当する場合には、DFARS Clause 252.204-7012に基づく保護を要求**する。

NIST Cybersecurity Framework

- **2017年、NIST（アメリカ国立標準技術研究所）のCybersecurity Frameworkの改訂ドラフト版が公表され、『サプライチェーンリスク管理』を追記。**

2014.02	**Cybersecurity Framework vesion1.0**公表	サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載
2017.01	**Cybersecurity Framework version1.1 draft1**公表	**サプライチェーンのリスク管理（Supply Chain Risk Management）**などを追記
2017.12	**Cybersecurity Framework version1.1 draft2**公表	draft1公表後のパブリックコメントを踏まえ**サプライチェーンのリスク管理の重要性の強調**や**サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk)**を追記 関係業界は肯定的に受け止め

Cybersecurity Frameworkにおける5つの分類

特定：最初に、組織としてサイバーセキュリティに関する方針を決定する”、“どのようなリスクがあるかを特定する”等

防御：リスクの多寡に応じて適切な予防策を講じる

検知：防御策を監視することで突破されそうになった（あるいはされた）ことをいち早く察知する

対応：異常が検知され必要な暫定処置を講じる

復旧：恒久措置を施し元通りの状態に回復させる

特定

防御

検知

対応

復旧

ID.AM　資産管理
ID.BE　ビジネス環境
ID.GV　ガバナンス
ID.RA　リスクアセスメント
ID.RM　リスク管理戦略
ID.SC　サプライチェーン管理

ID.SCが新規に追加され、サプライチェーン全体で対策を実施することや、必要に応じて監査を行うことを要求

NIST Cybersecurity Framework

- **特に、Cybersecurity Framework version1.1 draft2では、**
  - **『サプライチェーンリスク管理（Supply Chain Risk Management）』**
  - **『サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk)』**

の重要性がより強調された。

『サプライチェーンリスク管理』に関して、draft2でSection3.3の本文を改訂。

Supply chains are a complex, globally distributed, …. Given these complex and interconnected relationships, **supply chain risk management (SCRM) is a critical organizational function.**…. **A primary objective of cyber SCRM is to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable** due to poor manufacturing and development practices within the cyber supply chain. "

サプライチェーンは、複雑で、グローバルに広がっており、…。これらの複雑な相互作用の関係のもと、**サプライチェーンリスクマネジメント(SCRM)は、重要な組織としての役目である。**…。**サイバーSCRMの主目的は、**「サイバーサプライチェーンにおける不十分な製造や開発の実施により、**潜在的に悪意のある機能、偽物もしくは脆弱性がある製品やサービス」を特定、評価、軽減することである。**

『サイバーセキュリティリスクの自己評価』に関して、draft2でSection4.0のタイトル及び本文を改訂。

4.0 **Self-Assessing Cybersecurity Risk** with the Framework
…. Self-assessment and measuring should improve decision making about investment priorities.

4.0 フレームワークを用いた**サイバーセキュリティリスクの自己評価**
…。自己評価と測定により投資の優先順位の決定を改善すべきである。

ボットネット及びその他の自動化・分散化した脅威に対する対策

- **2017年5月、トランプ大統領が「サイバーセキュリティ強化のための大統領令」に署名。**
- **2018年１月、大統領令を踏まえた報告書案を公表（セキュリティ確保のためのエコシステムの形成を強調）。**
- **2018年５月、本報告書を大統領に報告予定。**

大統領令

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure（連邦ネットワーク及び重要なインフラストラクチャに対するサイバーセキュリティの強化に関する大統領令）　2017年5月11日
①連邦政府のネットワーク　②重要インフラ　③国家／国民のためのサイバーセキュリティ(ボットネット対策含む)に関して各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示

報告書案

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats（ボットネットおよびその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性の強化に関する報告書）　2018年1月5日

報告書の概要：自動化・分散化した脅威（ボットネット）に対処する**５つの目標**を設定

1. 適応可能、持続可能かつ安全な技術市場環境の実現に向けた明確な道筋の明確化
2. 進化する脅威に動的に対応するためのインフラのイノベーションの促進（エコシステムのすべてのドメインでの対応）
3. ネットワークのエッジにおけるイノベーションの促進による、悪意ある行為の防止、検出、影響の緩和
4. 国内外のセキュリティ、インフラ、運用技術の各コミュニティ間の連携の構築
5. エコシステム全体にわたる啓発・教育の強化

２．欧州における近年の動き

（Cybersecurity Certification Framework等）

欧州における近年の動き

- 欧州では、**重要インフラは最新のサイバーセキュリティ対応を実装することが求められ**（NIS Directive）、**ネットワークに接続する機器のセキュリティに関して認証・確認のための自主的フレームワーク（Cybersecurity Certification Framework）を整備**することを掲げている

【欧州】

- **単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入を検討**

  ⇒方向性：規制ではなく、自主的な仕組み　　産業界：国際標準に基づく自己適合宣言を主張している。

- 2016年、ＥＵ各国の重要インフラ事業者（エネルギー、交通、銀行、金融等）に対して、**セキュリティ対策を義務化。その際セキュリティ関連国際標準を考慮することを指示。（NIS 指令）**
- 2018年から、EUの顧客データを扱う企業に対して、データ処理制限、流出などの際の通知義務などをEU域外においても義務化。（EU一般データ保護規則：GDPR）

【ドイツ】

- ＮＩＳ指令に先立ち、2015年にＩＴセキュリティ法を制定し、重要インフラ事業者（エネルギー、交通、ICTs、交通、金融・保険、健康、水、食糧）に対して以下を要求。

  ①サイバーセキュリティに係る**最低限の基準を満たしていることについて情報セキュリティ庁の証明を得ること**
  ②**２年ごとにセキュリティ監査等を受けること**
  ③**サイバー攻撃と思われる事象が発生した場合に情報セキュリティ庁へ報告すること**

- 現在、small office and homes のルーターのテクニカルガイドラインを作成中（任意制度）

欧州における近年の動き

・2017年9月13日、**ユンカー欧州委員会委員長の施政方針演説でサイバーセキュリティに関する言及があり**、これを受けたデジタル単一市場の施策の一環として、新たに**サイバーセキュリティ認証フレームワークの導入を検討していく旨公表**。併せて、サイバーセキュリティに関するENISA規則※の修正提案を承認。
・同年11月20日には、ENISAが、**「IoTのベースラインセキュリティの推奨事項」を発表**。

※Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

1．欧州委員会がENISAの評価の中間報告をもとに複数のオプションを提案（2017年7月7日）
　①ENISAの今後の組織と戦略の方向性
　②欧州デジタル単一市場におけるサイバーセキュリティ認証フレームワーク（Cybersecurity Act）

2．パブリックコメント（2017年7月7日 - 2017年8月4日）

3．インパクトアセスメント発表（2017年9月8日）
　欧州委員会がENISAの過去の実績を評価するとともに、提案内容について、パブリックコメント、有識者の意見、関係者へのアンケート等を元に各オプションを採用した場合の影響を評価

4．ユンカー欧州委員会委員長による施政方針演説の中で、サイバーセキュリティについて言及
欧州委員会がインパクトアセスメントを元にしたENISAの修正提案を承認（2017年9月13日発表）
　※提案（**Cybersecurity Package**）の承認であって、提案内容をそのまま採択したわけではない

　①ENISAを恒久的な機関として機能を強化
　　・当初噂されていたEUのセキュリティ庁ではない
　　・EUにおけるセキュリティの標準化や認証に関する業務が含まれることになった
　②セキュリティについて各国、セクター別の支援を行い、認証及び表示の枠組みについて既存の認証メカニズムに基づいて構築することを提案
　　・直接的な運用認証制度は導入しない
　　・新たな技術標準の開発は行わない
　⇒次頁　詳細

5．ENISAが「IoTのベースラインセキュリティの推奨事項」を発表（2017年11月20日）
　一般的な課題を抽出し、関係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）やベストプラクティスを紹介するレポート。

欧州のCybersecurity Certification Frameworkのポイントと欧州委員会にて承認された提案

欧州のCybersecurity Certification Frameworkのポイント	○ICT機器とサービスについて、**サイバーセキュリティ認証フレームワーク(Cybersecurity Certification Framework)を構築し、欧州内におけるサイバーセキュリティ認証制度を確立する**ことで、欧州におけるデジタル単一市場の信頼性、セキュリティを確保する。 ○欧州サイバーセキュリティ認証フレームワークは、**法の定めがない限り自主的なもの(voluntary)であり、直ちに事業者に規制を課すようなものではない**。
欧州委員会にて承認された提案	ICT機器及びサービスのための欧州Cybersecurity Certification Frameworkを確立し、サイバーセキュリティ認証の分野におけるENISAの本質的な機能及び任務を規定する。 現在の提案は、欧州のサイバーセキュリティ認証制度を支配する規則の全体的な枠組みを定めている。 この提案では、**直接的な運用認証制度を導入するのではなく、特定のICT機器/サービスのためのサイバーセキュリティ認証制度をENISAが作成**する。 この認証制度では、**製品が遵守する必要のある技術要件及び評価手順に関して既存の基準を使用し、技術標準自体を開発しない。**（例えば、現在、**SOG-IS MRA**スキームで国際CC規格に照らしてテストされているスマートカードなどの機器に関するEU全体の認定は、このスキームをEU全体で有効にすることを意味する。） 欧州のサイバーセキュリティ認証制度が採用されると、ICT機器の製造業者またはICTサービスの提供者は、自らの選択した適合性評価機関に自社の機器またはサービスの認証申請書を提出することができる。適合性評価機関は、指定された特定の要件を満たしていればその証明書を発行する。 **監視、監督、執行の任務は加盟国に委ねられている。**加盟国は、1つの認証監督当局を提供しなければならない。この権限は、適合性評価機関のコンプライアンスと、自国の地域に設置された適合性評価機関が発行した証明書と、この規則及び関連する欧州のサイバーセキュリティ認証制度の要件とを監督することを任される。

EU Cybersecurity Packageへの反応概要

2017年9月13日に発表された「Cybersecurity Package」に対して、意見募集が12月6日まで行われ、欧米の32の事業者・団体から意見が提出された。

サイト：「https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en」

ENISAの機能拡大

概ね賛同されたが、各国の規制機関との関係性、サイバーセキュリティ認証フレームワーク策定における機能について、詳細が明確でないと懸念する意見がある

サイバーセキュリティ認証フレームワーク

デジタル単一市場の形成に資するという面では概ね賛同されたが、認証の範囲、策定方法と策定に関わる関係者の選択、既存の規制との関係性、グローバルとの断絶の懸念、事業者（特に中小企業）の負担増大への懸念等について、詳細が不明であることから多数の意見が寄せられている。

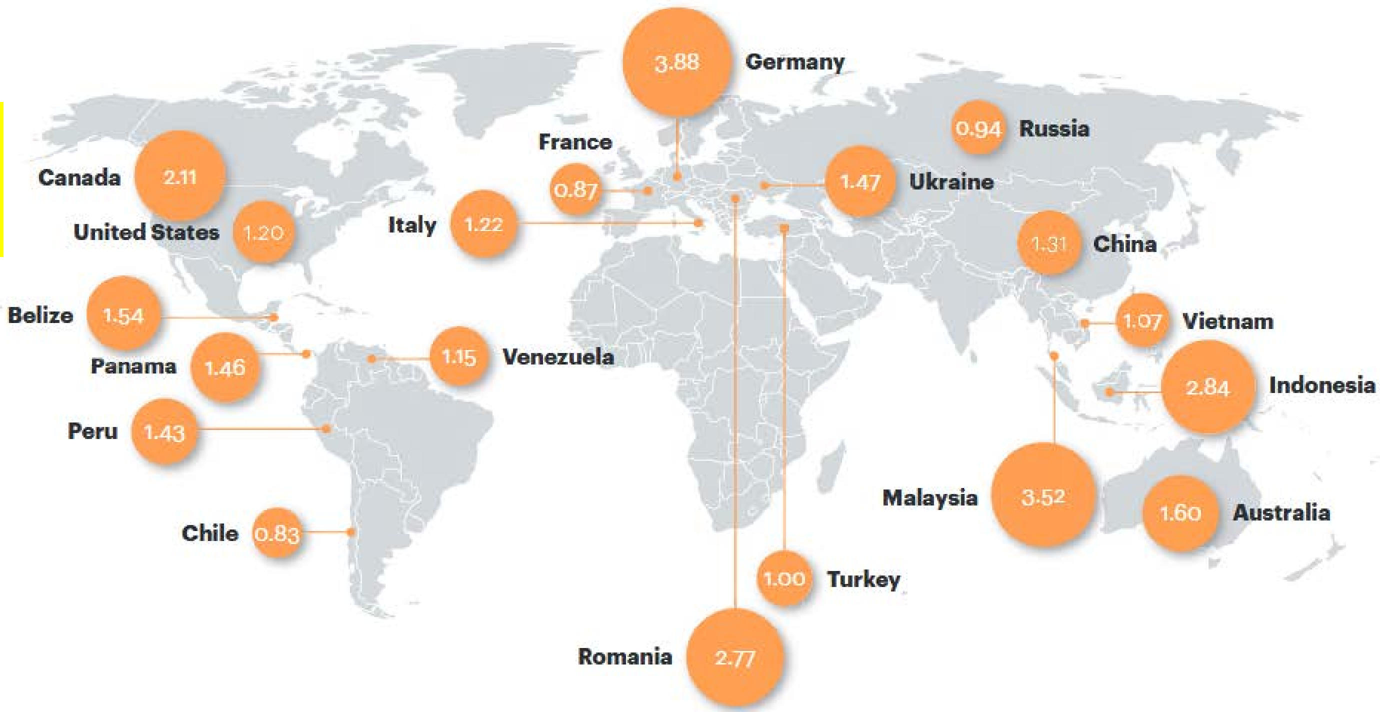
- **認証制度の範囲を明確化：BtoCとBtoB、IoTとIIoT、水平か垂直か、セクター等の分野的なものと、製品やサービスなのかプロセスやシステムなのか等の対象についての明確化**
- **国際標準へ準拠：ISO27000シリーズ、IEC62443シリーズ、CCが論点の中心だが、意見は分かれている**
- 策定の方法：WTO TBT協定、NLF等の手続きに則していることといった意見が複数
- 既存の規制の尊重：十分に機能している国家単位やセクター単位の既存の規制を尊重
- **策定に向けた議論のあり方：意見を表明している事業者・団体の多くは、ステークホルダーとして議論に加わることを強く希望しており、業界団体はセクターごとの自主的な仕様の策定を主張**
- **認証の方法：自己宣言をベースとして、重要インフラ等においてはリスクの大きさに合わせて外部（第三者）認証を追加すべきとする意見が多い**
- 認証のレベル：範囲や方法とも関連して、リスクベースで認証のレベルを設けるべきという意見と堅牢性を重視意見とに分かれている。ただし後者は主にセキュリティ認証を行っている企業や団体の意見であるため利益誘導の面があると思われる
- 啓発と教育：認証制度やその意味が利用者と事業者双方に認知されなければ意味が無いため、啓発と教育についての意見が多数見られた。

３．ASEANにおける状況

ASEANにおける状況

- **ASEAN諸国は、サイバー攻撃の活動拠点となっている。**
  - **マレーシア、インドネシア、ベトナムは、遮断された不正なWEB活動の起点となっている比率が高く、マルウェアの攻撃に悪用されている。**
  - **ベトナムは、2015年12月から2016年11月までの間に、168万個のIPアドレスの遮断を記録した。さらに、2016年に発生したIoT機器に対する攻撃の起点に悪用された数が世界で5番目に多かった。**

Blocked suspicious Web activity, by country of origin (expected ratio = 1.0)

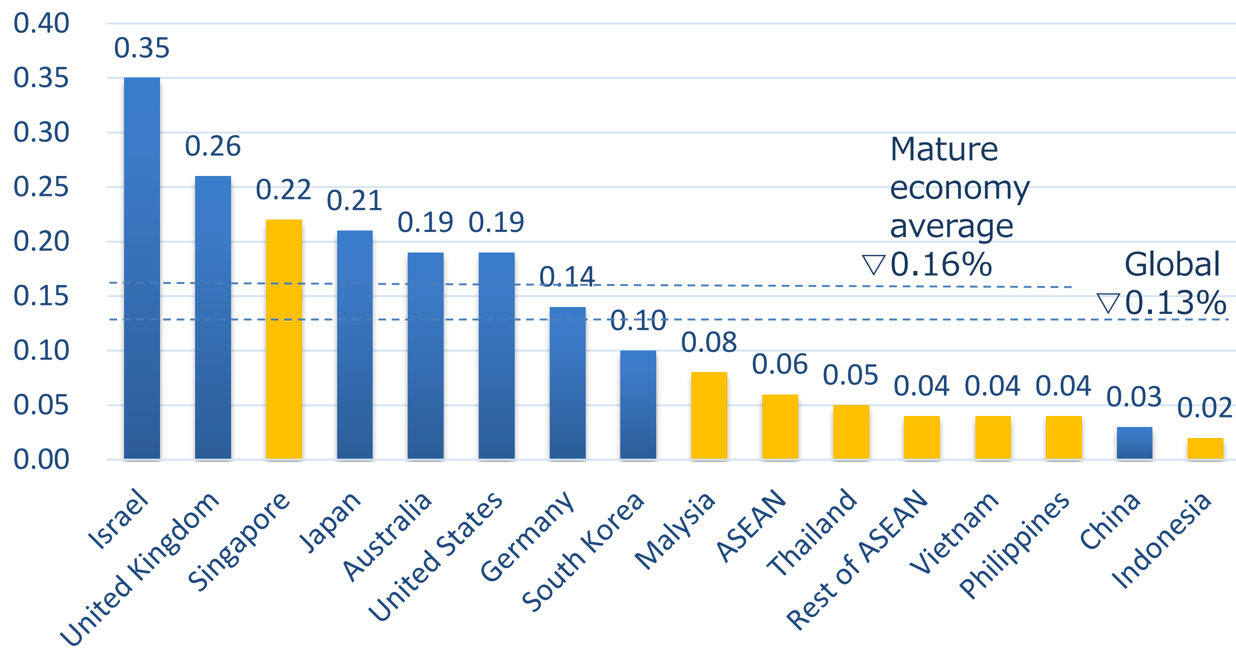


出典：「A.T. Kearney, “Cybersecurity in ASEAN—An Urgent Call to Action”」より引用

ASEANにおける状況

- **サイバーセキュリティに対するポリシーが不十分。**
  - ➢ **ASEAN地域におけるサイバーレジリエンスは、一般的に低いという評価 （特に、ポリシー、ガバナンス、サイバーセキュリティ能力）。**
  - ➢ **産業界もリスクを過少評価しており、結果として、サイバーセキュリティに対する投資が不足しているという指摘あり。**

Cybersecurity spending (% of GDP for 2017)



出典：「A.T. Kearney, “Cybersecurity in ASEAN—An Urgent Call to Action”」より引用