# 全世界（広域）ASEAN・インド太平洋地域におけるサイバーセキュリティ分野官民連携強化に係る情報収集・確認調査

# ファイナルレポート

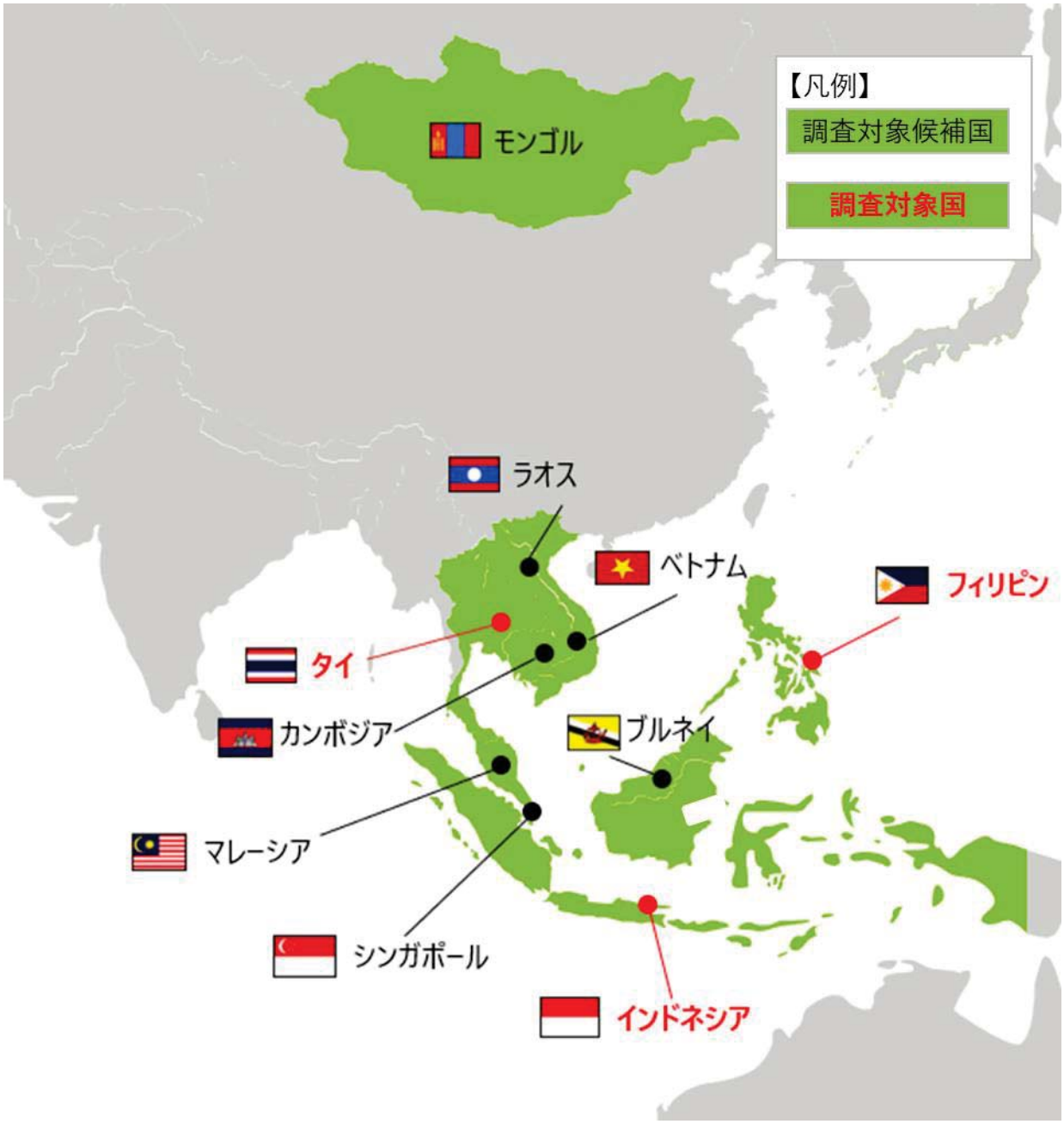
**2026 年 2 月**

**独立行政法人**
**国際協力機構（JICA）**

**有限責任監査法人トーマツ**

**デロイト トーマツ サイバー合同会社**

| |
|---|
| ガ平 |
| JR |
| 26-009 |


【凡例】
調査対象候補国
調査対象国
モンゴル
ラオス
ベトナム
フィリピン
タイ
カンボジア
ブルネイ
マレーシア
シンガポール
インドネシア

**調査対象国**

# 目次

# 図目次

# 表目次

# 略語表

| 略語 | 英語（原文） | 日本語訳（説明） |
|---|---|---|
| AD | Active Directory | アクティブディレクトリ |
| AI | Artificial Intelligence | 人工知能 |
| AJCCA | ASEAN Japan Cybersecurity Community Alliance | ASEAN 日本サイバーセキュリティコミュニティアライアンス |
| AJCCBC | ASEAN-Japan Cybersecurity Capacity Building Centre | 日 ASEAN サイバーセキュリティ能力構築センター |
| ASEAN | Association of Southeast Asian Nations | 東南アジア諸国連合 |
| ASM | Attack Surface Management | 攻撃対象領域管理 |
| BGP | Border Gateway Protocol | ボーダーゲートウェイプロトコル |
| BSSN | Badan Siber dan Sandi Negara | 国家サイバー・暗号庁（インドネシア） |
| CASB | Cloud Access Security Broker | クラウドアクセスセキュリティブローカー |
| CII | Critical Information Infrastructure | 重要情報インフラ |
| CRC | Cybersecurity Regulatory Committee | 規制委員会（タイ） |
| CSIRT | Computer Security Incident Response Team | コンピュータセキュリティインシデント対応チーム |
| CVE | Common Vulnerabilities and Exposures | 共通脆弱性識別子 |
| CVSS | Common Vulnerability Scoring System | 共通脆弱性評価システム |
| DDoS | Distributed Denial of Service | 分散型サービス拒否攻撃 |
| DJID (SDPPI) | Directorate General of Resources and Equipment of Post and Information Technology | 郵便・情報通信技術資源機器総局（インドネシア） |
| DPA | Data Privacy Act | データプライバシー法（フィリピン） |
| DX | Digital Transformation | デジタルトランスフォーメーション |
| EDR | Endpoint Detection and Response | エンドポイント検知・対応 |
| EMC | Electromagnetic Compatibility | 電磁両立性 |
| FIRST | Forum of Incident Response and Security Teams | インシデント対応・セキュリティチームフォーラム |
| FQDN | Fully Qualified Domain Name | 完全修飾ドメイン名 |
| GCI | Global Cybersecurity Index | グローバルサイバーセキュリティ指標 |
| GDP | Gross Domestic Product | 国内総生産 |
| GDPR | General Data Protection Regulation | EU 一般データ保護規則 |
| GovNet | Government Network | 政府ネットワーク（フィリピン） |
| GUI | Graphical User Interface | グラフィカルユーザーインターフェース |
| ICS | Industrial Control Systems | 産業用制御システム |
| ICSCoE | Industrial Cyber Security Center of Excellence | 産業サイバーセキュリティセンター |
| ICT | Information and Communication Technology | 情報通信技術 |
| idCARE.UI | Indonesia Cyber Awareness and Resilience Center of Universitas Indonesia | インドネシア大学サイバー意識・レジリエンスセンター |
| idNSA | Indonesia Network Security Association | インドネシアネットワークセキュリティ協会 |
| IDS | Intrusion Detection System | 侵入検知システム |

| | | |
|---|---|---|
| IPA | Information-technology Promotion Agency | 情報処理推進機構 |
| IPS | Intrusion Prevention System | 侵入防止システム |
| IR | Incident Response | インシデント対応 |
| ITE 法 | Information and Electronic Transactions Law | 電子情報・取引法（インドネシア） |
| JICA | Japan International Cooperation Agency | 独立行政法人国際協力機構 |
| KOMINFO | Ministry of Communication and Information Technology | 情報通信省（インドネシア） |
| MFA | Multi-Factor Authentication | 多要素認証 |
| MIC | Ministry of Information and Communications | 情報通信省 |
| MoPS | Ministry of Public Security | 公安省 |
| MPLS | Multi-Protocol Label Switching | マルチプロトコル・ラベル・スイッチング |
| NCERT | National Computer Emergency Response Team | 国家コンピュータ緊急対応チーム（フィリピン） |
| NCIAC | National Cybersecurity Inter-Agency Committee | 国家サイバーセキュリティ省庁間委員会（フィリピン） |
| NCO | National Cybersecurity Office | 国家サイバー統括室 |
| NCSA | National Cyber Security Agency | 国家サイバーセキュリティ庁（タイ） |
| NCSC | National Cyber Security Committee | 国家サイバーセキュリティ委員会（タイ） |
| NCSP | National Cybersecurity Plan | 国家サイバーセキュリティ計画 |
| NDA | Non-Disclosure Agreement | 秘密保持契約 |
| NISC | National center of Incident readiness and Strategy for Cybersecurity | 内閣サイバーセキュリティセンター |
| NTC | National Telecommunications Commission | 国家電気通信委員会（フィリピン） |
| ODA | Official Development Assistance | 政府開発援助 |
| OJT | On the Job Training | 職場内訓練 |
| OSINT | Open Source Intelligence | オープンソースインテリジェンス |
| OT | Operational Technology | 運用技術（産業システム） |
| PDP 法 | Personal Data Protection Law | 個人情報保護法（インドネシア） |
| PH-CERT | Philippine Computer Emergency Response Team | フィリピンコンピュータ緊急対応チーム |
| Playbook | Incident Response Playbook | インシデント対応手順書 |
| PoC | Proof of Concept | 概念実証 |
| RDP | Remote Desktop Protocol | リモートデスクトッププロトコル |
| SASE | Secure Access Service Edge | セキュアアクセスサービスエッジ |
| SD-WAN | Software-Defined Wide Area Network | ソフトウェア定義広域ネットワーク |
| SIEM | Security Information and Event Management | セキュリティ情報イベント管理 |
| SNI | Standar Nasional Indonesia | インドネシア国家規格 |
| SOC | Security Operation Center | セキュリティオペレーションセンター |
| SSH | Secure Shell | セキュアシェル |
| STI | Science, Technology and Innovation | 科学技術イノベーション |
| TISA | Thailand Information Security Association | タイ情報セキュリティ協会 |
| VNA | Vietnam News Agency | ベトナム通信社 |
| VPN | Virtual Private Network | 仮想プライベートネットワーク |

| | | |
|---|---|---|
| WAF | Web Application Firewall | ウェブアプリケーションファイアウォール |
| XDR | Extended Detection and Response | 拡張検知・対応 |

# 第 1 章　調査サマリー

本報告書は、ASEAN・インド太平洋地域におけるサイバーセキュリティ分野の官民連携強化を目的に、日本企業の製品・サービスの現地展開可能性や、産業システム（OT）の実態と課題を多角的な視点から実証・調査したものである。日本のサイバーセキュリティ製品が持つ技術力や現地適合性、そして産業システムで顕在化している制度・運用面のギャップ、現場のニーズについて、調査対象国における実証事業やワークショップを通じて把握した。

第 2 章　調査の背景では、デジタル化の進展によるサイバー空間の脅威拡大と、開発途上国の体制・人材不足がもたらす被害深刻化の現状について述べている。

第 3 章　調査の概要では、ASEAN9 か国とモンゴルを対象に、日本企業のサイバーセキュリティ製品・サービスの情報収集、調査対象国における実証事業、産業システムのワークショップなどの多角的手法を導入した調査プロセスの全体像について説明している。

第 4 章　本邦サイバーセキュリティ製品に関する情報では、日本国内に展開するサイバーセキュリティ製品・サービスの特徴や現地展開状況、実証事業の成果についてとりまとめている。日本国内に展開するサイバーセキュリティ製品・サービスに関する情報収集を行い、国内 63 社・315 製品に関する情報収集および整理を行った。また、調査対象国は、ASEAN9 か国およびモンゴルの中から、インドネシア、タイ、フィリピンの 3 か国を選定し、株式会社インターネットイニシアティブ（インドネシア）、株式会社網屋（タイ）、株式会社マクニカ（フィリピン）の 3 社に実証事業を含めた調査の再委託を行った。現地政府機関や重要インフラ事業者に対する実証事業を通じて、運用効率化、リスク低減、法令遵守、現地適合性、人材習熟度、運用負荷などの観点から、本邦サイバーセキュリティ製品・サービスの調査対象国における有効性や競争力について具体的に調査した。

第 5 章　産業システム（OT）向けサイバーセキュリティ対策状況では、調査対象国であるタイ・フィリピン・インドネシアの政府機関・重要情報インフラ事業者を対象とした OT セキュリティのワークショップの実施を通じて、OT 分野における制度整備と現場実装のギャップ、共通する運用課題などに関する調査結果をまとめた。

第 6 章　提言・まとめでは、本調査を実施した成果として、JICA 及び実証事業実施企業３社、OT ワークショップを実施した国立大学法人名古屋工業大学との意見交換の内容や、本調査を踏まえた提言・まとめについて報告している。

# 第 2 章　調査の背景

デジタル化の進展に伴い、ヒト、モノ、カネ、行政機関を含めた組織やインフラシステムの多くがサイバー空間で繋がっており、サイバーセキュリティのリスクも甚大化している。多くの開発途上国各国ではサイバーセキュリティの対策体制・能力の不足と人材不足がリスクを増大させており、世界的に猛威を振るったランサムウェアによる被害、重要インフラ（エネルギー、金融、通信、保健等）等に深刻な被害、サプライチェーンを通じた機密情報漏洩、偽情報による社会的混乱、個人情報漏洩等深刻な被害が多発している。このような状況の下、開発途上国でのデジタル社会推進における各国のセーフガードとして、また、国を越えて被害を及ぼすサイバー空間の地域レベルの安全性強化のため、数多くの開発協力機関や政府が開発途上国におけるサイバーセキュリティ能力強化にかかる支援を行っている。

日本政府は 2021 年に「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針[1]」を策定し、国際的なサイバーセキュリティ上のリスクを低減する観点より、重要インフラ防護、サイバー犯罪対策、国際的ルール作り、信頼醸成措置推進、人材育成等に関する国際協力を進めている。また、日本が主導する日 ASEAN サイバーセキュリティ政策会合[2]では、2024 年度より「産官学セッション」が追加され、産業界や学術界との連携が重視されてきている。上記方針等を踏まえ、JICA では「サイバーセキュリティとデジタルトラストサービスに関する日 ASEAN 能力構築プログラム強化プロジェクト[3]」等の技術協力を通じて、開発途上国の政府関係者や重要インフラ事業者等向けのサイバーセキュリティ能力強化を実施している。

かかる状況下、同協力の実施に際し、各国政府向けのサイバーセキュリティ対応能力強化に加え、重要インフラ事業者向けのサイバーセキュリティ対策強化等において、本邦企業や研究機関の知見・経験の活用が期待されている。しかしながら、これまでの JICA の取り組みでは、産業界や学術界との連携が限られており、本邦企業によるサイバーセキュリティにかかる製品の海外での提供実績や展開に関心をもっている本邦企業を十分に把握できていない状況である。

[1] サイバーセキュリティ戦略本部 cs-tojyokokushien2021.pdf
[2] 経済産業省 第 18 回日 ASEAN サイバーセキュリティ政策会議を開催しました （METI/経済産業省）
[3] JICA サイバーセキュリティとデジタルトラストサービスに関する日 ASEAN 能力向上プログラム強化プロジェクト | ODA 見える化サイト

# 第 3 章　調査の概要

## 3.1. 調査目的

JICA はグローバル・アジェンダ「デジタル化の促進」の一環として「自由で安全なサイバー空間の実現[4]」を重要テーマに位置付けた「サイバーセキュリティ・クラスター戦略」を策定し、開発途上国の政府関係者や重要インフラ事業者向けの能力強化を実施している。また、JICA は民間技術の活用を通じた課題解決の重要性を認識しているが、サイバーセキュリティ分野においては、本邦企業や研究機関の知見や経験の活用が限定的であり、企業による製品の海外展開や実績把握が十分に進んでいない状況にある。これらを踏まえて、本調査では、日本国内のサイバーセキュリティ分野における本邦民間企業や研究機関・大学の取り組みを把握すると共に、ASEAN 諸国への展開可能性の検討を行った。

## 3.2. 調査の対象

### 3.2.1 業務実施の範囲

本調査は後述の「3.2.2 業務実施の方法」に示す事項の調査を行い、報告書等を作成するものとした。調査対象候補国は、ASEAN 9 か国（インドネシア、カンボジア、シンガポール、タイ、フィリピン、ブルネイ、ベトナム、マレーシア、ラオス）、モンゴルを対象とした。

### 3.2.2 業務実施の方法

本調査は、計画段階、調査実施段階、調査結果のまとめ段階に分けて進めた。調査実施段階においては、本邦セキュリティ企業、製品情報収集を行ったうえで、本邦企業製品の実証事業を行う活動と、産業システム（OT）向けサイバーセキュリティ対策に関する情報収集を行う活動を並行して進めた。全体の流れは下記作業フローの通りである。

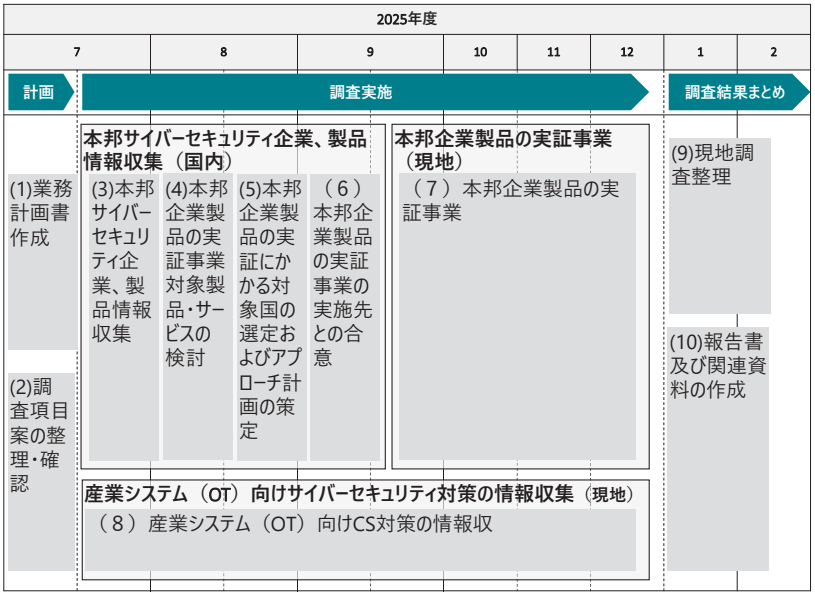



**図 1　本調査の作業フロー**

**表 1　本調査の作業項目と内容**

| 項番 | 項目 | 活動内容 |
|---|---|---|
| （1） | 業務計画書作成 | 本調査の業務計画書（日）を作成し、ガバナンス・平和構築部 STI・DX 室と確認を行った。 |

[4] JICA digital_text.pdf

| | | |
|---|---|---|
| (2) | 調査項目案の整理・確認 | ● 本邦サイバーセキュリティ企業、製品情報収集および本邦企業製品の証事業（国内・現地）<br>● 産業システム（OT）向けサイバーセキュリティ対策の情報収集（現地） |
| (3) | 本邦サイバーセキュリティ企業、製品情報収集（国内） | 本邦で提供されているサイバーセキュリティ製品およびサービスにおいて、開発途上国向け（政府向け・重要インフラ向け）に有用と思われるものをオンラインやオフラインにて、製品等の情報を関係者からヒアリングする等の調査を行い、ロングリストを作成した。 |
| (4) | 本邦企業製品の実証事業対象製品・サービスの検討 | 上記（３）で作成したリストを踏まえ、実証事業を行う候補製品/サービスを検討した。 |
| (5) | 本邦企業製品の実証にかかる対象国の選定およびアプローチ計画の策定 | 調査対象候補国及び機関のサイバーセキュリティに関する情報、サイバーセキュリティツールや重要インフラにおけるサイバーセキュリティにおけるニーズや現状をデスクトップ及びオンラインで情報収集を行い、調査国候補及び実証実施候補企業を抽出した。 |
| (6) | 本邦企業製品の実証事業の実施先との合意 | 上記（５）に基づき、実証事業の公募と実施企業の選定を行った。 |
| (7) | 本邦企業製品の実証事業 | 実証事業では国内での準備期間を設け、調査計画を策定した。 |
| (8) | 産業システム（OT）向けサイバーセキュリティ対策の情報収集 | ASEAN の多くの国が重要情報インフラの特定を終わった状況において、現状の OT サイバーセキュリティの検討状況、需用についての情報収集のためのワークショップ開催を通じて確認を行った。 |
| (9) | 現地調査整理 | 上記（７）（８）の調査結果については、各調査が完了した際に結果をした。 |
| (10) | 報告書および関連資料の作成 | 最終報告書及び関連資料の作成を行った。 |

調査実施段階における本邦企業製品の情報収集・実証事業については製品情報収集や対象国の選定を踏まえて、実証企業の選定や企業による実証活動を進めた。

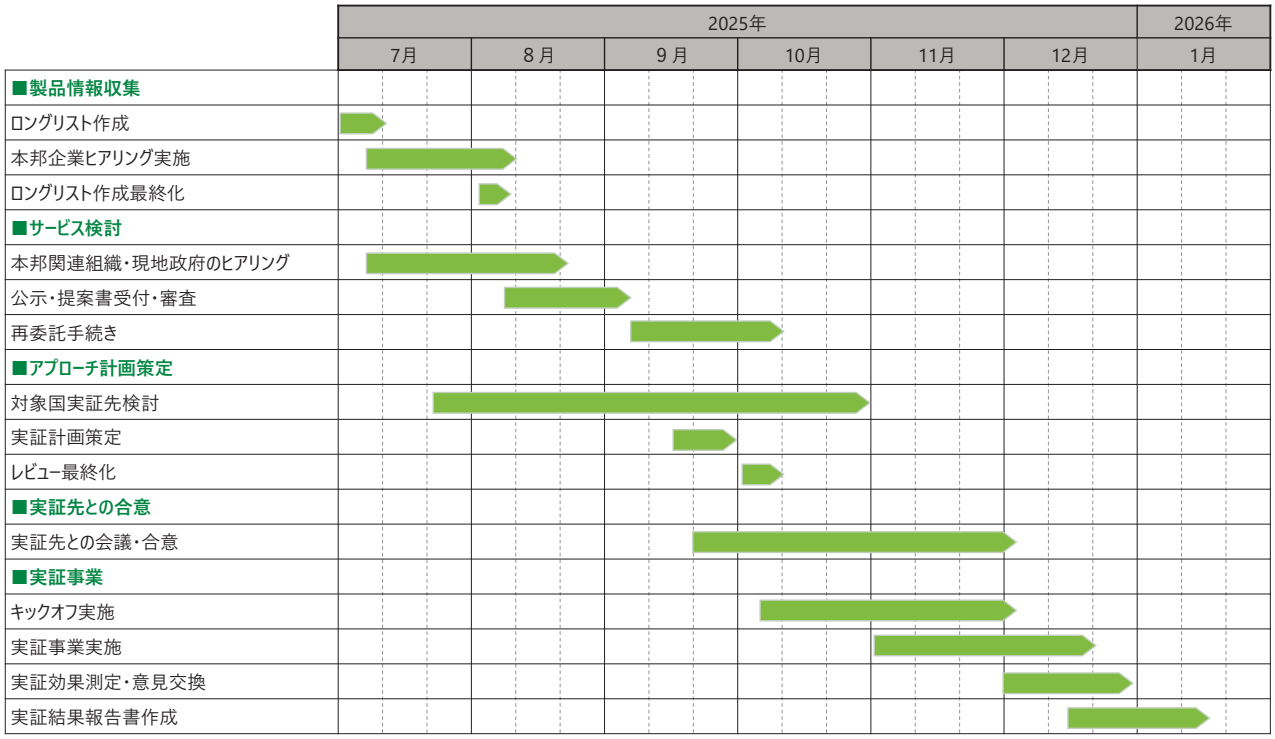



**図 2　本邦企業製品の情報収集・実証事業に関する詳細スケジュール**

産業システム（OT）向けサイバーセキュリティ対策の情報収集においては、対象３か国でのワークショップ実施を活動の中心として進めた。

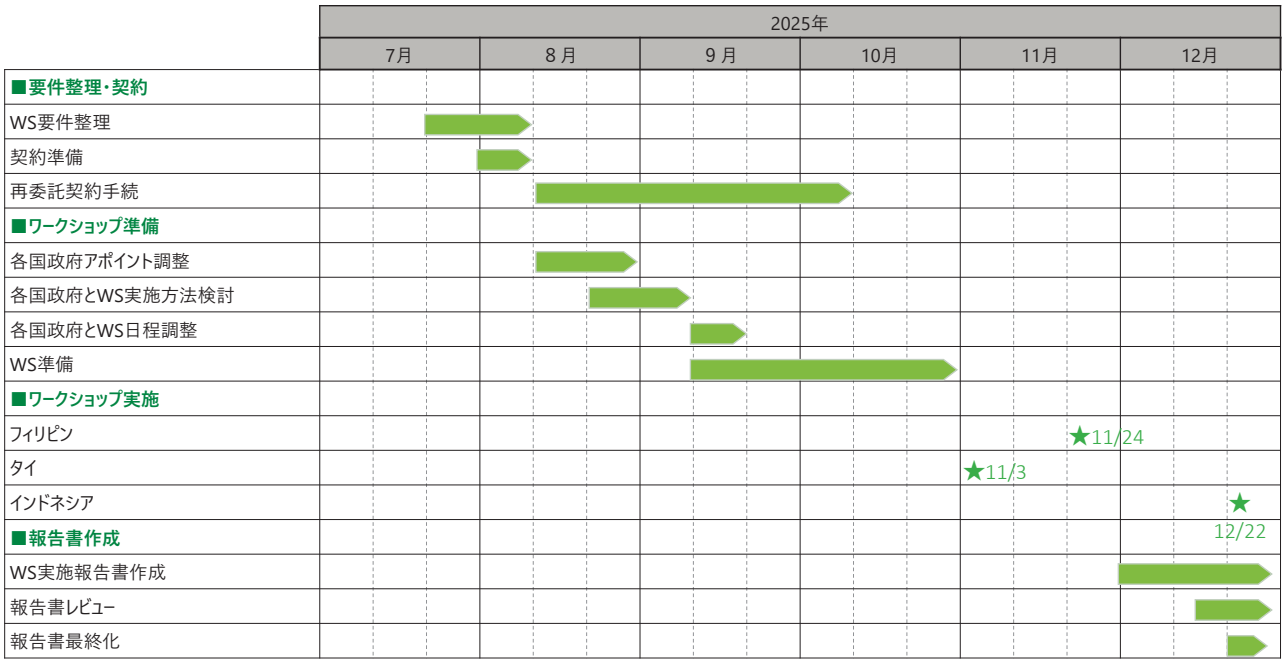



**図 3　産業システム（OT）向けサイバーセキュリティ対策の情報収集に関する詳細スケジュール**

### 3.3. 調査実施のスケジュール

調査期間は 2025 年 7 月 1 日～2026 年 2 月 27 日である。

# 第 4 章　本邦サイバーセキュリティ製品に関する情報

## 4.1. 全体の概要

本事業は、日本のサイバーセキュリティ製品・サービスの ASEAN 諸国およびモンゴルにおける展開可能性、現地ニーズ、現状を把握するための調査を目的とする。本調査では、日本のサイバーセキュリティ製品・サービスの実証事業を通じ、現地政府機関や重要インフラ事業者向けの実証事業の可能性、製品・サービスの有効性、現地適合性を検討する。また、日本国内の民間企業や研究機関、学術機関が有する産業システム（OT）のサイバーセキュリティ対策や人材育成・研修に関する知見、ならびに官民連携による先進的な技術・ノウハウについて、現地での展開可能性やニーズを、ワークショップの開催等を通じて評価する。近年、開発途上国ではランサムウェア、重要インフラへの攻撃、個人情報漏洩等のリスクが高まっており、体制整備や人材育成の課題が顕在化している。本事業は、日本政府の方針や JICA が実施するサイバーセキュリティ能力構築プロジェクト等と連携し、調査結果を今後の国際協力や事業展開の検討材料とするものである。

調査対象国の選定では、①日本政府・JICA の協力実績、②企業の海外展開意向、③名目 GDP、④ Global Cybersecurity Index[5]（GCI）を指標とし、インドネシア、タイ、フィリピンの 3 カ国を選定した。各国の国家戦略や法規制の分析から、重要インフラ保護や個人情報保護法などの遵守が重要であることを確認した。

日本のサイバーセキュリティ製品・サービスに関するデスクトップ調査の結果、日本国内のセキュリティベンダーは、ネットワーク監視、エンドポイント防御[6]、ASM[7]、ゼロトラスト[8]、クラウドセキュリティ、AI/自動化、脆弱性診断、CSIRT[9]支援、教育・訓練など、多様な分野で事業を展開していることを確認した。また、日本国内の官公庁や重要インフラへの導入実績に加え、ASEAN 各国をはじめとする海外の政府機関や重要インフラ事業者への導入実績も確認できた。

実証事業の製品・サービス選定は、現地課題への有効性や体制、法令遵守、インフラ統合性、運用性など多面的に評価し、株式会社インターネットイニシアティブ（インドネシア）、株式会社網屋（タイ）、株式会社マクニカ（フィリピン）の3社を採択した。現地の実運用環境で、ログ監視・異常検知（SIEM[10]）、リモートアクセス管理（ゼロトラスト/特権 ID 管理）、ASM の観点から、運用効率化やリスク低減、長期的な持続性を検証した。また、現地法令やデータ保護・プライバシー要件への対応、インフラとの統合、現地スタッフの運用習熟度も評価した。

実証の結果、日本製品は現地のセキュリティ強化に有効であり、現地ニーズや規制にも十分に適合することが確認された。専門人材不足や運用負荷が高い ASEAN 市場では、AI や自動化、クラウド型サービス、運用支援体制の重要性が再認識された。今後は、国際標準対応や現地規制への柔軟

---

[5] Global Cybersecurity Index 2024 を参照。GCI は国際電気通信連合（ITU）が各国のサイバーセキュリティ能力を評価し、法律、技術、組織、能力構築、協力の 5 つの分野でランク付けするグローバルな指標。

[6] PC やスマートフォン等の端末（エンドポイント）をサイバー攻撃やマルウェアから保護するセキュリティ対策。

[7] Attack Surface Management：攻撃対象領域管理。インターネット上の公開資産を把握・管理し、外部からの攻撃リスクを低減する手法。

[8] ネットワーク内外を問わず、すべてのアクセスを常に検証するセキュリティモデル。

[9] CSIRT（Computer Security Incident Response Team）の略称であり、サイバーセキュリティインシデントへの対応や調査・復旧を専門に行う組織。

[10] Security Information and Event Management：セキュリティ情報・イベント管理。複数のログを統合的に管理し、脅威検知・分析を支援するシステム。

な対応、現地パートナーとの連携、人材育成支援を通じて、持続的な市場展開が期待される。

本事業により、日本のサイバーセキュリティ製品・サービスが ASEAN を含むグローバル市場で競争力と信頼性を有することが示され、海外展開の基盤となる知見とモデルケースが確立された。

### 4.2. 本邦企業製品の実証にかかる調査対象国の選定

調査対象国の選定にあたり、サイバーセキュリティ分野での国際協力案件の実効性や持続可能性を高める上で特に重要と考えられる、A)本国の協力実績（サイバーセキュリティ分野）、B)本邦企業の意向、C)名目 GDP、D)GCI（Global Cybersecurity Index）の成熟度の 4 つの選定軸を設定した。

A)本国の協力実績では、日本の政府機関（NCO[11]、総務省、経済産業省等）や JICA がこれまでに相手国と積み重ねてきた協力事業の有無や内容を指す。特に表 2 に記載した JICA が過去に取り組んだ具体的なサイバーセキュリティ関連の協力実績は、対象国とのさらなる連携を進める上での基盤となり、プロジェクトの成功可能性を高める要因としても重要である。

表 2　日本国政府機関が実施したサイバーセキュリティ関連の取り組み（2020 年以降）

| 対象国 | プロジェクト名称 | 実施主体 | 支援携帯 | 実施期間 | 実施概要 | 相手国政府関連機関 |
|---|---|---|---|---|---|---|
| インドネシア | サイバーセキュリティ人材育成プロジェクト | JICA | 技術協力 | 2019年5月～2024年5月 | インドネシア大学と連携し、サイバーセキュリティ専門人材の育成、オープンソースツールの開発、モンゴルなど他国との連携強化 | 情報通信省、インドネシア大学 |
| ベトナム | サイバーセキュリティに関する能力向上プロジェクト | JICA | 技術協力 | 2019年6月~2021年11月 | 情報通信省傘下の情報セキュリティ局を対象に、サイバー攻撃への対応能力向上、子供のオンライン保護政策の支援、啓発活動の実施 | 情報通信省 情報セキュリティ局 |
| モンゴル | サイバーセキュリティ人材育成プロジェクト | JICA | 技術協力 | 2023年1月～2026年12月 | モンゴル国の安全なデジタル社会推進のため、産学官連携でサイバーセキュリティ教育と人材育成を強化 | デジタル開発通信省、モンゴル科学技術大学情報通信技術校 |
| ASEAN全体（タイ中心） | サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクト | JICA<br>総務省<br>外務省 | 技術協力 | 2023年3月～2027年2月 | ASEAN加盟国の政府職員や重要インフラ機関向けに、サイバーセキュリティのトレーニングや演習を、日本政府がタイ政府と共に設立した、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）で実施 | タイ国家サイバーセキュリティ庁（NCSA）、ASEAN加盟国の関係機関 |
| カンボジア | サイバーセキュリティ能力向上プロジェクト | JICA | 技術協力 | 2023年5月～2026年10月 | 郵政通信省内のICTセキュリティ局を中心に、サイバーセキュリティ能力向上のための研修やセミナーを提供し、同局とCII産業や他の政府省庁間のサイバーセキュリティに関する組織間の連携を強化 | 郵政通信省、ICT総局・ICT セキュリティ局 |
| フィリピン | サイバーセキュリティ能力向上プロジェクト（個別専門家派遣） | JICA | 技術協力 | 2023年10月～2025年9月 | フィリピンの情報通信技術省サイバーセキュリティ局のサイバーセキュリティ能力向上を目的に、研修や普及啓発活動、重要インフラセクターとの連携強化を支援 | 情報通信技術省サイバーセキュリティ局 |
| インドネシア、カンボジア、フィリピン | JICA在外技術研修「サイバー防御演習」 | JICA | 研修 | 2025年1月～2025年2月 | インドネシア、カンボジア、フィリピンを対象としたサイバーセキュリティ研修を実施。サイバー攻撃防御の演習設計及び実施者の育成を行い、各国の技術的能力を強化する。JICAが実施中のサイバーセキュリティ関連事業と協力・連携して行われている | インドネシア：情報通信省（MIC）<br>フィリピン：情報通信技術省（DICT）<br>カンボジア：郵政通信省（MPTC） |

B) 本邦企業の意向は、サイバーセキュリティ分野における日本企業の海外展開ニーズや戦略を反映するものである。調査対象国の選定にあたっては、企業が進出意欲を持つ国を対象とすることで、実証事業を通じて蓄積したノウハウや知識を今後の自社展開にも活用が可能となる。

C) 名目 GDP[12]は、調査対象国の経済規模を示す指標であり、名目 GDP が大きい国ほど市場規模が大きく、ICT インフラやサイバーセキュリティ分野への投資余力も高いと考えられる。経済成長が著しい国では、デジタル化の進展に伴いサイバーセキュリティ対策の需要も増大しており、協力案件の波及効果が期待できる。

D) GCI（Global Cybersecurity Index）の成熟度は、サイバーセキュリティ分野における各国の政策・法制度・インフラ・人的資源等の整備状況を総合的に評価した国際指標である。GCI スコアが中程度以上の国は、既に一定の基盤が整っていることから、より効果的な事業実施が見込まれる。

これら 4 つの軸をもとに、表 3 に示す通り各国を総合的に評価した結果、インドネシアが最も高評価となった。続いて、タイ、フィリピン、ベトナムの 3 か国が次点となった。その中から、本邦

[11] National Cybersecurity Office の略称。2025 年 7 月に内閣官房組織令に基づき、内閣サイバーセキュリティセンターを改組し、内閣官房に「国家サイバー統括室」を設置。

[12] World Bank Grope GDP.pdf

企業の意向や協力実績、各国の制度環境等を総合的に勘案し、フィリピン及びタイを調査対象国として選定した。

**表 3　調査対象国の選定における評価**

| 評価クライテリア | | ◎：JICA技術協力支援<br>○：本邦政府機関事業<br>△：会議体ASEAN-日本サイバーセキュリティ政策会議など)<br>×：実績無し | ◎：全社意向有り<br>○：一部企業意向有り<br>×：全社意向なし | ◎：対象国1位～4位<br>○：対象国5位～7位<br>×：対象国8位～10位 | ◎T1：Role-modeling<br>○T2：Advancing<br>△T3：Establishing<br>×T4：Evolving<br>×T5：Building | | 5：最優先<br>4：高優先<br>3：中優先<br>2：低優先<br>1：非優先 | |
|---|---|---|---|---|---|---|---|---|
| 国名 | ODA支援対象国 | A) 本国の協力実績<br>サイバーセキュリティ) | B) 本邦企業の意向 | C) GDP<br>Millions of US dollars) | D) GCIの成熟度<br>総評5段階) | 点数 20点中) 評価指標 | 総評対象国優先度)<br>優先度 | 理由 |
| インドネシア | 対象 | サイバーセキュリティ人材育成プロジェクトJICA) | 製造業が多い | 世界16位／対象国1位<br>$1,371,171 | T1<br>100 | 20 法<br>20 技術<br>20 組織<br>20 能力構築<br>20 協力 | 5 | A～Dいずれも懸念なし |
| フィリピン | 対象 | サイバーセキュリティに関する能力向上プロジェクトJICA) | 英語圏<br>サイバーセキュリティコンテンツへのニーズが高い | 世界33位／対象国4位<br>$437,146 | T2<br>93.49 | 20 法<br>19.11 技術<br>19.51 組織<br>17.17 能力構築<br>17.7 協力 | 4 | A～Dいずれも大きな懸念はない<br>Dは他国と比較してやや劣勢 |
| ベトナム | 対象 | サイバーセキュリティに関する能力向上プロジェクトJICA) | 製造業が多い<br>一部企業が慎重 | 世界34位／対象国5位<br>$429,717 | T1<br>99.74 | 20 法<br>20 技術<br>20 組織<br>19.74 能力構築<br>20 協力 | 4 | A～Dいずれも大きな懸念なし<br>Bについては一部企業が慎重な姿勢<br>Cについては上位と比較しやや劣勢 |
| タイ | 対象 | サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクトJICA) | 外資製品や製造業が多い<br>親日 | 世界26位／対象国2位<br>$514,969 | T1<br>99.22 | 20 法<br>20 技術<br>19.22 組織<br>20 能力構築<br>20 協力 | 4 | A～Dいずれも大きな懸念なし<br>Aについては実施国であるものの、ASEAN全体が対象であるため、優先度を下げた |
| マレーシア | 対象 | 日本国政府の取り組みの非幹事国 | 一部企業現地拠点あり | 世界37位／対象国6位<br>$399,705 | T1<br>98.82 | 20 法<br>20 技術<br>18.82 組織<br>20 能力構築<br>20 協力 | 3 | AはJICAの技術協力プロジェクト実績がなく、現地政府の調査協力が懸念 |
| モンゴル | 対象 | サイバーセキュリティ人材育成プロジェクトJICA) | 特段コメントなし | 世界121位／対象国8位<br>$20,325 | T3<br>56.36 | 19.18 法<br>6.64 技術<br>13.62 組織<br>10.43 能力構築<br>6.49 協力 | 3 | AはJICA技術協力プロジェクト実績有り<br>B～Dに懸念有り |
| カンボジア | 対象 | サイバーセキュリティに関する能力向上プロジェクトJICA) | フランス製品が多い | 世界42位／対象国7位<br>$363,494 | T4<br>37.02 | 11.82 法<br>4.56 技術<br>8.3 組織<br>6.12 能力構築<br>6.22 協力 | 2 | AはJICA技術協力プロジェクト実績有り<br>B～Dに懸念有り<br>Dはモンゴルと比較し、GCIが劣勢 |
| ラオス | 対象 | 日本国政府の取り組みの非幹事国 | 中国企業の存在が強い | 世界134位／対象国9位<br>$15,843 | T4<br>33.74 | 10.38 法<br>6.18 技術<br>5.52 組織<br>2.05 能力構築<br>9.61 協力 | 1 | A～Dいずれも懸念有り |
| シンガポール | 非対象 | 日本国政府の取り組みの非幹事国 | 市場が成熟 | 世界30位／対象国3位<br>$501,428 | T1<br>99.86 | 20 法<br>20 技術<br>20 組織<br>19.86 能力構築<br>20 協力 | 1 | ODA支援対象国ではない |
| ブルネイ | 非対象 | 日本国政府の取り組みの非幹事国 | 市場が小さい | 世界138位／対象国10位<br>$15,128 | T3<br>70.38 | 17.2 法<br>14.89 技術<br>11.35 組織<br>10.76 能力構築<br>16.18 協力 | 1 | ODA支援対象国ではない |

特に、JICA の過去の協力実績が豊富な国（A 軸が高い国）では、現地政府機関と迅速に連携できる可能性が高く、調査や事業の推進において円滑な情報収集や関係者調整が可能となる。これにより、本事業の実現可能性が高まると判断した。この点を踏まえ、ベトナムについては、2025 年 2 月 28 日付でサイバーセキュリティ関連の国の管理・監督責任が情報通信省（Ministry of Information and Communications：MIC）から公安省（Ministry of Public Security：MoPS）に移管され、サイバーセキュリティ製品・サービスに関する事業許可や輸入許可等、10 の行政手続きが MoPS の管轄となった[13]。本事業期間を踏まえたうえで、新たな主管当局との調整には一定の時間を要すると見込まれ、事業期間内で十分な協力体制を構築することが難しい可能性があるため、調査対象国の優先度を下げることとした。また、ODA 支援対象国ではないシンガポールおよびブルネイについては、ODA 事業の目的を踏まえ、調査対象国の優先度を下げることとした。

### 4.3. 調査対象国における国家戦略及び法規制

調査対象国における各国の国家戦略および法規制は下記の通りである。

[13] ベトナム通信社 Cybersecurity protection function handed over to public security ministry

### 4.3.1インドネシアにおけるサイバーセキュリティ関連の国家戦略及び法規制

**(1)** 国家戦略

インドネシアは、サイバーセキュリティの強化を国家戦略の重要課題と位置付けている。国家としてサイバー空間の安全保障を体系的に推進するため、2023 年に大統領規則（Perpres）第 47 号/2023[14]を制定した。戦略の柱は下記の通りである。

- サイバーセキュリティガバナンスの強化：
  国家サイバー・暗号庁（BSSN）を中心に、サイバーセキュリティ政策の統括と調整を行う。各省庁や地方自治体、重要インフラ事業者との連携体制を構築する。
- 重要情報インフラの保護：
  エネルギー、金融、通信、運輸、保健医療などの重要インフラの保護を強化する。重要インフラ事業者に対し、最低限のサイバーセキュリティ基準やインシデント報告義務を課す。
- インシデント対応能力の向上：
  サイバー攻撃や情報漏洩発生時の迅速な対応体制（CSIRT の設置・連携）を整備する。インシデントの記録・分析・共有を推進する。
- 人材育成・啓発
  サイバーセキュリティ分野の人材育成プログラムを拡充する。国民や企業への啓発活動を強化する。
- 国際協力：
  ASEAN をはじめとする国際機関や他国との情報共有・共同訓練・技術協力を促進する。

[14] インドネシア監査庁（BPK） PERPRES No. 47 Tahun 2023

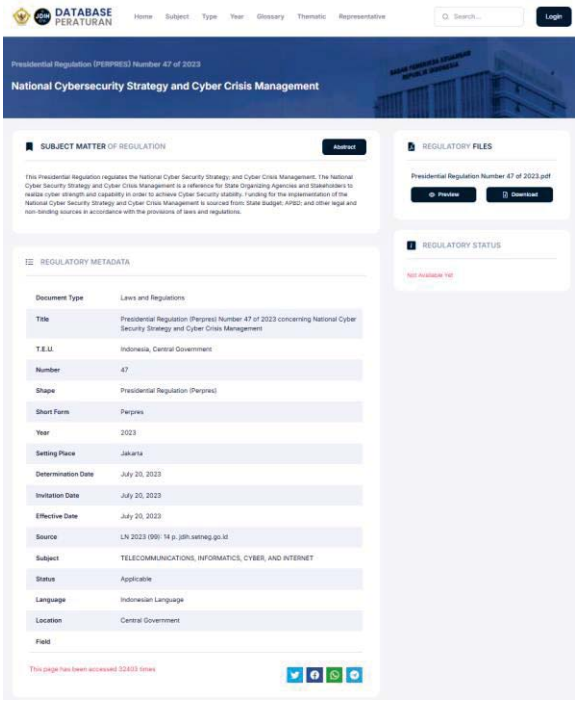
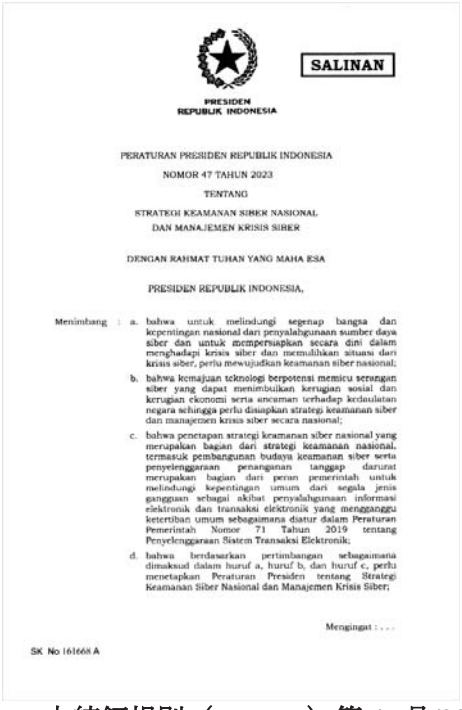



**図 4　インドネシア監査庁（BPK）法令情報システム ウェブサイト**


SALINAN

PRESIDEN
REPUBLIK INDONESIA

PERATURAN PRESIDEN REPUBLIK INDONESIA
NOMOR 47 TAHUN 2023
TENTANG
STRATEGI KEAMANAN SIBER NASIONAL
DAN MANAJEMEN KRISIS SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melindungi segenap bangsa dan kepentingan nasional dari penyalahgunaan sumber daya siber dan untuk mempersiapkan secara dini dalam menghadapi krisis siber dan memulihkan situasi dari krisis siber, perlu mewujudkan keamanan siber nasional;

b. bahwa kemajuan teknologi berpotensi memicu serangan siber yang dapat menimbulkan kerugian sosial dan kerugian ekonomi serta ancaman terhadap kedaulatan negara sehingga perlu disiapkan strategi keamanan siber dan manajemen krisis siber secara nasional;

c. bahwa penetapan strategi keamanan siber nasional yang merupakan bagian dari strategi keamanan nasional, termasuk pembangunan budaya keamanan siber serta penyelenggaraan penanganan tanggap darurat merupakan bagian dari peran pemerintah untuk melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Presiden tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber;

Mengingat : . . .

SK No 161668 A

**図 5　大統領規則（Perpres）第 47 号/2023**

**(2)** 法規制

A) サイバーセキュリティ法（電子情報・取引法（ITE 法）（No.11/2008）[15]）

i. 全体概要

サイバー犯罪や電子取引の規制を定める基本法である。サイバー犯罪の取り締まりや電子商取引の法的基盤を提供しており、個人情報保護やデータ漏洩への対応も強化している。

ii. 重要情報インフラの定義

インドネシアのサイバーセキュリティ政策の中心である国家サイバー・暗号庁（BSSN）は、BSSN 規則 No.8/2020 において、重要情報インフラを、国家の安全保障、経済の安定、公共の健康や安全の維持にとって重要であり、その機能が妨害・損傷・破壊された場合、社会全体や国家に重大な影響を及ぼす情報システム・ネットワーク・資産を指す、としている。

iii. 関連する重要情報インフラのセクター

BSSN および関連ガイドラインでは、以下の分野が重要情報インフラに該当するとされている。

- 政府・行政機関（国家データセンター、住民データベース等）
- エネルギー分野（電力管理システム、石油・ガスの運用ネットワーク等）
- 金融サービス（銀行システム、決済インフラ、証券取引システム等）
- 通信・情報分野（通信事業者のネットワーク、インターネット基幹設備等）
- 保健医療（病院の情報システム、医療データベース等）

[15] インドネシア監査庁（BPK） UU No. 11 Tahun 2008

- 運輸・物流（航空管制システム、鉄道管制システム、港湾システム等）
- 水資源・給水
- 食料供給管理システム
- 防衛・治安関連システム

B) 当該国の販売において留意すべき法規制

i. 個人データ保護法（個人情報保護法（PDP 法）（Law No.27/2022）[16]）

インドネシア PDP 法は、2022 年に成立し、個人データの保護・セキュリティ対策・インシデント対応を厳格に義務付けている。サイバーセキュリティ製品はこれらの法令遵守を支援する重要なツールとなるため、販売にあたっては、PDP 法対応機能の説明・現地規制の確認・顧客のコンプライアンス支援がポイントとなる。

ii. 輸出関連規制

インドネシア向けサイバーセキュリティ製品の輸出について、インドネシア側における規制は、主に以下が関連する。

- 通信機器認証[17]：

サイバーセキュリティ製品輸出の際には、インドネシア情報通信省（KOMINFO）[18]による型式認証（DJID (SDPPI)[19]認証）または、SNI（インドネシア国家規格）の取得[20]を求められる場合がある。また、無線機能を持つ機器（Wi-Fi 付きファイアウォール等）は、SDPPI 認証が必須である[21]。

- 暗号技術の規制：

インドネシアでは暗号技術について、BSSN の認可が必要な場合がある[22]。特に、政府機関・重要インフラ向けに提供する場合は、BSSN の承認や追加審査が求められることがある。

- 輸入許可：

一部のサイバーセキュリティ製品は、輸入許可（Import Permit）や事前登録が必要となる場合がある[23]。

### 4.3.2 タイにおけるサイバーセキュリティ関連の国家戦略及び法規制

**(1)** 国家戦略

タイ王国国家戦略（2018-2037）[24]におけるサイバーセキュリティ政策は、国家安全保障と発展の中核として位置づけられている。国家安全保障戦略では、サイバー攻撃など多様な脅威への備えとして、専門人材の育成や先端技術・ビッグデータ活用を推進し、政府・民間・

---

[16] インドネシア監査庁（BPK） UU No. 27 Tahun 2022

[17] 一般財団法人日本品質保証機構 インドネシア | 国際認証サービス | 電気製品・医療機器・車載機器の認証・試験 | 日本品質保証機構（JQA）

[18] 2024 年 10 月、KOMINFO（情報通信省）から KOMDIGI（通信デジタル省）に名称が変更されている（インドネシア -「SDPPI」から「DJID」へ、無線認証当局の名称変更」| ニュースリリース | JQA）。

[19] 2025 年 1 月、SDPPI（情報通信資源規格総局）は、DJID（デジタルインフラ総局）に名称が変更されている（インドネシア -「SDPPI」から「DJID」へ、無線認証当局の名称変更」| ニュースリリース | JQA）。

[20] インドネシア国家標準化庁（BSN） https://bsn.go.id

[21] インドネシア監査庁（BPK） Permenkominfo No. 3 Tahun 2024

[22] インドネシア監査庁（BPK） Peraturan BSSN No. 8 Tahun 2020

[23] インドネシア共和国商業省 Peraturan - JDIH Kementerian Perdagangan RI、JETRO view_interface.php

[24] タイ国家戦略室 National_Strategy_Summary.pdf

市民・国際機関が連携した統合的な対処体制を構築している。国際協力や情報インフラの強化にも重点を置き、ASEAN 諸国などと連携し、全国規模の情報収集・分析体制を整備している。競争力強化戦略では、デジタル・AI・データ分野を成長産業と位置づけ、科学技術や物流を含むデジタル基盤の強化を進めている。行政分野では、デジタル技術による迅速・透明なサービス提供と、戦略実施状況の全国的なモニタリング・評価体制を整備し、政策の透明性と実効性を高めている。さらに、生涯学習やデジタルプラットフォームを活用した人材育成、社会のデジタル化にも力を入れている。これらを通じて、タイ王国はサイバーセキュリティを軸に、脅威対応力、産業振興、行政改革、人材育成を一体的に推進し、安全で強靭なデジタル社会の実現を目指している。

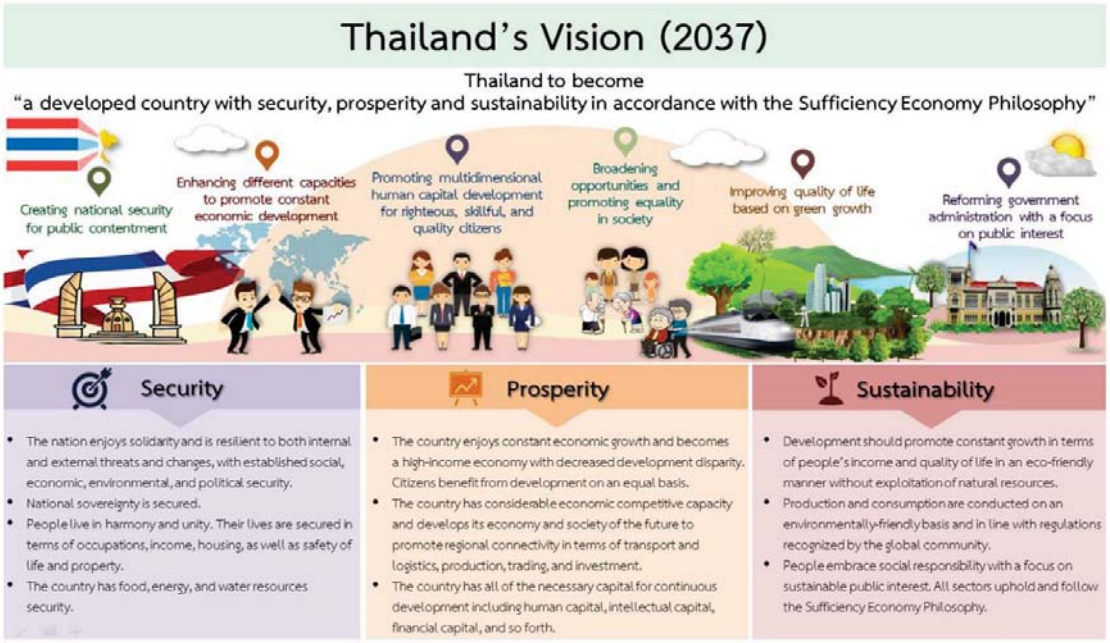



**図 6　Thailand's Vision 2037**

**(2)** 法規制

A)　サイバーセキュリティ法（Cybersecurity Act, B.E. 2562 (2019)[25]）

i. 全体概要

タイ王国のサイバーセキュリティ法は、国の安全や公共秩序に関わるサイバー脅威から政府及び民間の情報システムを保護する枠組みを定めている。同法では、サイバーセキュリティの維持を国内外の脅威に対する予防・対処・リスク軽減措置全般と定義し、脅威にはコンピュータやデータへの不法侵害も含まれる。国家サイバーセキュリティ委員会（NCSC）、規制委員会（CRC）、事務局が設置され、政策策定や基準設定、監視・対応支援などを担う。政策は、統合管理、能力強化、重要情報インフラ保護、協力、人材育成、啓発、法整備を目的とし、関連組織はこれに沿った標準や実践規範を整備する義務がある。事務局は調整窓口として、情報共有や訓練、基準策定支援、インシデント対応を行う。各組織は責任者の届出、基準遵守、毎年のリスク評価と対応計画、重大インシデントの迅速報告を義務付けられる。脅威の深刻度に応じて CRC が情報収集や技術

[25] タイデジタル経済社会省 3572-Cybersecurity-Act-B-E-2562--2019-

的措置を指示し、違反には罰則が科される。

ii. 重要情報インフラの定義

本法第 3 条により、重要情報インフラとは、政府機関または民間組織が国家安全、公共の安全、国家経済の安全、または公共利益に資するインフラの維持に関連して業務で使用するコンピュータまたはコンピュータシステムであると定義されている。

iii. 関連する重要情報インフラのセクター

委員会は、本法第 49 条に基づき、委員会は通知を通じて、どの組織が重要情報インフラに該当するか、その特徴や条件を定める権限を持つ。

（1）国家安全保障
（2）重要な公共サービス
（3）銀行・金融
（4）情報技術・電気通信
（5）交通・物流
（6）エネルギー及び公益事業
（7）公衆衛生
（8）委員会が定めるその他

B) 当該国の販売において留意すべき法規制

i. 個人データ保護法（Personal Data Protection Act B.E. 2562 (2019)[26]）

タイの個人データ保護法（PDPA）は、タイ国内で個人データを収集・利用・開示する事業者のみならず、国外事業者であってもタイ国内の個人データを取り扱う場合には適用される（Section 5）。個人データとは、直接または間接的に個人を特定できる全ての情報を指し、死亡した者に関する情報は含まれない（Section 6）。データの管理者および処理者の役割は明確に規定されている（Section 6）。個人データをタイ国外へ移転する場合、移転先国が PDPA と同等の保護水準を有しない場合は、データ主体の明示的な同意または他の合法的根拠が必要である（Section 28）。データ主体には、アクセス、訂正、削除、利用停止などの権利が認められている（Section 30-34）。個人データの収集・利用・開示には原則として同意取得が必須であり、同意なしの処理は違法である（Section 19）。これら規則に違反した場合、最大 500 万バーツの行政罰、刑事罰、民事損害賠償が科される（Section 84, Section 79, Section 77）。タイでの事業展開に際しては、PDPA の規制遵守体制を構築することが求められる。

ii. 輸出関連規制

タイ向けサイバーセキュリティ製品の輸出について、タイ側における規制は、主に以下が関連する。

・ 輸出入品規制法（1979 年）（EXPORTAND IMPORT OF GOODS ACT, B.E. 2522[27]）

輸出入される全ての物品について、国家の安全、経済安定、公共の利益等を理由に、商務大臣の通知により輸出入禁止や許可制、品質・原産地証明の提出義務、課徴金の支払い、指定港での通関などの規制が課されることを定めている。違反には重い罰則が科されるため、日本からサイバーセキュリティ製品を輸出する際は、事

[26] タイデジタル経済社会省 3577-Personal-Data-Protection-Act-B-E--2562--2019-
[27] World Trade Organization Import Licensing Notification Portal

前に対象品目に該当するか否か、必要な許認可や書類、商務省や関係機関の最新通知を十分に確認し、適切な手続きの実施が重要である。

- 大量破壊兵器の拡散に関連する物品の管理に関する法律(Control of Item in Relation to the Proliferation of Weapons of Mass Destruction Act B.E. 2562[28])

  タイが国連安保理決議等の国際的要請に基づき、大量破壊兵器(WMD)拡散に利用され得る物品や技術の移転を管理する枠組みである。本法律は、デュアルユース製品（民生・軍事両用）のうち、WMD 関連に転用可能なものを規制対象とし、該当リストや通知、キャッチオール規定に基づき管理する。サイバーセキュリティ製品も、機能や用途によっては対象となる場合があるため、製品仕様や用途の明確な整理が実務上重要となる。

- タイ電気通信事業法（The Act on Organization to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunication Services, B.E. 2553（2010）[29]）

  この法律は、タイの国家放送通信委員会（NBTC）の設立や権限、無線通信機器や放送機器、電気通信サービスの規制を定めたものである。NBTC は、無線通信機器の技術基準や型式認証（Type Approval）、周波数の割り当て、認証ラベルの表示義務などを規定し、市場に流通する機器の安全性と電波利用の適正を担保する役割を持つ。また、NBTC が発出する通知や規則により、型式認証の手続きや提出書類、試験基準、ラベル表示、罰則などが詳細に定められており、認証は NBTC のウェブサイトや通知に基づいて進められる。サイバーセキュリティ製品であっても、無線通信機能を持つ場合は NBTC 関連法規への適合が販売の前提条件となる。

### 4.3.3 フィリピンにおけるサイバーセキュリティ関連の国家戦略及び法規制

**(1)** 国家戦略

フィリピン国では、国家としてデジタル分野での最先端としてのポジションを担うべく、サイバーセキュリティの強化を国家の重要課題と位置付けている。国家として安全なデジタル空間を創出するため、2024 年に国家サイバーセキュリティ計画(National Cybersecurity Plan:NCSP 2023-2028[30])を策定した。電力、通信、金融、交通、保健分野等の重要インフラの保護、軍組織を含む公的機関のネットワーク保護や各サプライチェーンの保護を提唱している。また、一般市民が安心してデジタル技術を活用できるよう、啓発教育活動を官民また一般向けに行っている。本計画では主なフレームワークとして、以下を掲げている。

- 政府ネットワークの防御強化：

  政府ネットワーク（GovNet）の防御強化（IDS/IPS、セキュア BGP、受動要素の導入）で、国・地方の 3,900 超の機関を保護する。またサイバーセキュリティ局の再編により、国家 CSIRT（NCERT）を強化し、国家 SOC（NSOC）を新設することにより、脅威タイプや脆弱性、対処法を収載する「国家サイバー脅威データベース」を構築する。並行して民間事業者と連携し、ネットワーク区画の防護も図る。

---

[28] タイ商務省貿易交渉局（DTN） กรมเจรจาการค้าระหว่างประเทศ | Department of Trade Negotiations

[29] タイデジタル経済社会省 The Act on Organization to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunication Services, B.E. 2553（2010）

[30] フィリピン情報技術省 NCSP 2023-2028 - FINAL-DICT

・ サイバーセキュリティ人材能力強化

10 月を「サイバーセキュリティ啓発月」とし、全府省庁でサイバー衛生の活動を実施する。ICT アカデミー再設立とサイバーセキュリティ・センターオブエクセレンスで高度教育と研究を推進し、職種索引の更新や資格基準の策定、業界認定の公務資格化も進める。奨学金や国際トレーニングの提供、国内外のハッキング大会でタレント育成を推進する。

・ 省庁横断型の政策枠組み制定

省庁横断の調整機能として NCIAC（National Cybersecurity Inter-Agency Committee）を強化し、政策調整と紛争解決を促進する。また重要情報インフラ（CII）保護のための大統領令を推進し、インシデントの義務的開示やセキュリティ研究者保護などの立法を後押しし、二国間・多国間の国際協力を拡大し、国際標準を取り入れる。

上記の３項目を達成すべく、NCSP は以下６項目を主な柱として明示している。[31]

・ サイバーセキュリティ法の制定:

サイバーセキュリティのための法制度と政策枠組みを強化することに重点を置き、オンライン上の脅威から守るため、明確な法律と規制を整備することを目指す。

・ 重要情報インフラ（CII）の保護と防御:

電力網、金融サービス、交通などの重要なシステムをサイバー攻撃から守る取り組みであり、脆弱性評価、インシデント対応計画、サイバーセキュリティ認証といった措置を含む。例えば、銀行にサイバーセキュリティ監査を義務付けたり、重要インフラ運用者が侵入検知システムを実装・維持したりすることである。

・ サイバー空間におけるプロアクティブ防御:

脅威に対して受け身ではなく、先手を打って対処する重要性を強調し、被害が出る前に脅威を特定し、予防するための措置を含む。この柱の重要な要素として、監視とインシデント対応を支援する国家サイバーセキュリティ・オペレーションセンターの設置があげられる。

・ サイバーセキュリティ人材の強化:

効果的なサイバーセキュリティには、強力な人材基盤が不可欠であるという認識に基づき、奨学金や、Lumify Work Philippines のようなサイバーセキュリティ・センター・オブ・エクセレンスを通じた教育・訓練を活用して、専門家が技能と能力を育成する環境を整える。

・ 国民のサイバーセキュリティ意識と教育:

サイバーセキュリティのベストプラクティスを広めるため、啓発キャンペーン（ナショナル・サイバーセキュリティ・マンスなど）や教育プログラムを実施し、すべての人がオンラインの脅威から自分自身を守れるようになることを目指す。

[31] フィリピン情報技術省 Achieving Cyber Resilience via the National Cyber Security Plan | Lumify Work Philippines

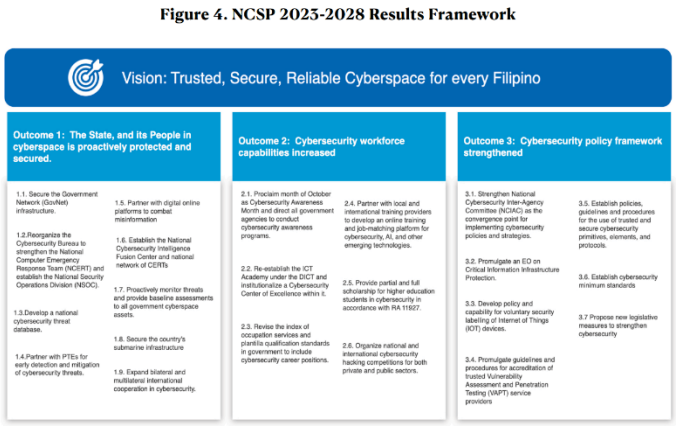



図 7　フィリピン国家サイバーセキュリティ計画（NCSP 2023-2028）フレームワーク

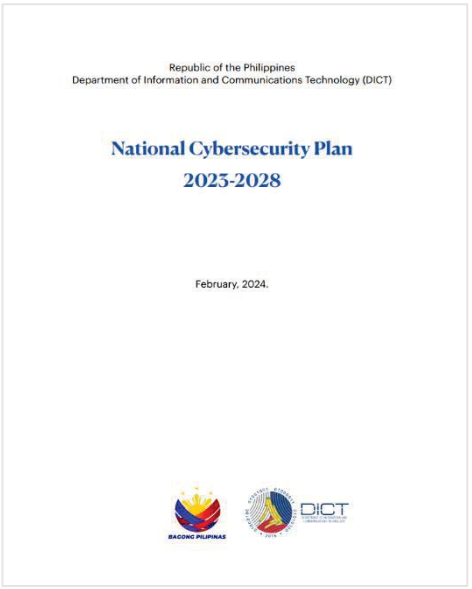



図 8　フィリピン国家サイバーセキュリティ計画（NCSP 2023-2028）

**(2)** 法規制

A) サイバーセキュリティ法（Cybercrime Prevention Act of 2012, Republic Act No. 10175[32]）

i. 全体概要

本法律はサイバー空間での犯罪防止・取り締まりをするための法的枠組みを提供する法律であり、違法アクセス、データ干渉、システム干渉などをサイバー犯罪と定義し、操作協力や執行の基盤を整理するものである。これらはオンライン上の不正行為に対処するための基本法として位置づけられている。実務面では E-commerce Act（RA8792）等の他法と併用され、官民のオンラインサービスに対するサイバー犯罪対応を補完する役割も持つ。

ii. 重要情報インフラの定義

本法第３条において、重要情報インフラの定義として、社会や経済の機能に不可欠なサービスの継続に重要であり、障害や破壊が国家安全保障、経済、公共の安全・健康に深刻な影響を与え得るコンピュータシステムや資産（物理・仮想を含む）を指すものと明示がある。

iii. 関連する重要情報インフラのセクター

本法では、CII に該当する具体的な産業セクター名の列挙については記載が見られず、第３条において、社会・経済に不可欠なサービスを提供する分野を包括的にとらえている。どのセクターが CII にあたるかは、当該分野のシステムや資産が停止・破壊された場合に国家安全保障、経済、公共の安全・健康に「深刻な影響」を及ぼすかという基準で判断される、公共性・重要性の高い分野が対象となる。他方、「テロ防止、禁止および処罰に関する法律」（共和国法第 11479 号）の第３条[33]においては、重要インフラストラクチャには、通信、水およびエネルギー供給、緊急サービス、食料安全保障、燃料

[32] The Official Gazette Republic Act No. 10175 | Official Gazette of the Republic of the Philippines
[33] The LAWPHil Project Republic Act No. 11479

供給、銀行および金融、交通、ラジオおよびテレビ、情報システムおよび技術、化学および原子力分野などに影響を与える資産またはシステムが含まれるが、これらに限定するものではないと記載がある。

B) 当該国の販売において留意すべき法規制

i. 個人データ保護法（Data Privacy Act, Republic Act No.10173：DPA[34]）

フィリピンの DPA 法は 2012 年に成立し、個人のプライバシーの保護とイノベーションと成長のための情報の自由な流通を確保すべく、フィリピン国内で個人情報を処理する主体に加え、国内設置の機器を用いる処理や、フィリピン国民の個人情報の処理に対して、厳格な遵守枠組みを定めている。外国法に従って外国で収集された情報をフィリピンで処理する場合には、一定の適用除外が認められるが、国内部分には情報セキュリティ措置の義務が課される。DPA は、処理の基本原則として「透明性」「正当目的」「比例性」を掲げ、これらに沿った処理を要求しており、サイバーセキュリティ製品はこれらの法令遵守を支援する重要なツールとなるため、販売にあたっては、DPA 法対応機能の説明・現地規制の確認・顧客のコンプライアンス支援がポイントとなる。

i. 輸出関連規制

フィリピン向けサイバーセキュリティ製品の輸出について、フィリピン側における規則は主に以下が該当する。

**(3)** NTC 認証[35]：

通信機器並びに無線通信を利用するすべての電化製品については、NTC(National Telecommunications Commision)による認可が必要であり、フィリピン国内での使用に関して、他の電子機器や通信ネットワークに対して悪影響を及ぼさないこと(Electromagnetic Comapatibility:EMC)と技術的な規格に適合していることを確認する必要がある。電子通信機器、無線デバイス、ブルートゥース機器、ラジオ周波を利用する無線機器等多くの電子機器が該当し、事前に確認する必要がある。[36]

**(4)** 輸入許可：

一部のサイバーセキュリティ製品は、輸入許可（Import Permit）や事前登録が必要となる場合がある。

### 4.4. 本邦製品の情報・海外展開の状況

本邦で提供されているサイバーセキュリティ製品およびサービスにおいて、開発途上国向け（政府向け・重要インフラ向け）に有用と思われる製品・サービスに関し、各社のホームページを中心に 2025 年 7 月時点での情報を収集した。本調査項目は「企業情報」「製品・サービス情報」「政府または重要インフラへの導入実績」の 3 分類で構成した。企業情報には本社所在地、資本金、現地拠点、海外展開状況などを記載し、企業の事業基盤や展開地域を明示し、製品・サービス情報では、提供形態、多言語対応、主な機能や特徴などを整理し、具体的なサービス内容を示した。導入実績については、政府機関や重要インフラ事業者への導入事例などを記載した。

---

[34] National Privacy Communication Republic Act 10173 - Data Privacy Act of 2012 - National Privacy CommissionNational Privacy Commission

[35] National Telecommunication Commision National Telecommunications Commission - National Capital Region

[36] National Telecommunication Commision Wireless Data Networks And Devices

表 4　本邦サイバーセキュリティ企業・製品調査に関する調査項目

| 調査項目 | | 概要説明 |
|---|---|---|
| 企業情報 | 企業名 | 製品・サービスを提供する企業の名称 |
| | 本社所在地 | 企業の本社が所在する国・都市 |
| | 資本金 | 企業の資本金額。企業規模や事業基盤の目安となる |
| | 会社概要 | 企業の業種、主な事業内容、特徴などの簡単な紹介 |
| | 企業URL | 企業の公式ウェブサイトURL |
| | 法人形態 | 日本法人か海外法人かなど、企業の法人形態 |
| | 現地拠点 | 調査対象地域における拠点有無や拠点所在地 |
| | 海外展開実績 | 海外での事業展開や実績の有無 |
| | 海外展開実績（地域別） | 各国・地域（例: タイ、インドネシア等）での展開状況 |
| | 海外展開実績のソース情報 | 海外展開実績の根拠となる情報源やURL |
| | 備考 | その他特記事項や補足情報 |
| 製品・サービス情報 | 製品・サービスカテゴリ | 製品・サービスの分類（例：監視、Webサーバ保護、アクセス制御等） |
| | 製品・サービス名 | 製品やサービスの正式名称 |
| | 製品・サービス概要 | 製品やサービスの主な機能や特徴を簡潔に説明 |
| | 提供方法 | クラウド型、オンプレミス、ハイブリッド等、提供形態 |
| | 多言語対応可否・対応言語 | 多言語対応の有無と対応言語 |
| | 製品URL | 製品またはサービスの公式ウェブサイトURL |
| 政府または重要インフラへの導入実績 | 導入実績（政府） | 政府機関への導入実績、代表的な導入事例やケーススタディ |
| | 導入実績（重要インフラ） | 電力・ガス・水道・交通・通信等、重要インフラ事業者への導入実績 |

上記調査項目に基づき、日本国内で提供されているサイバーセキュリティ製品およびサービスの調査を実施した。結果、全体で 63 社、315 件の製品・サービス情報を収集し、ロングリストに取りまとめた。日本国内で事業展開するセキュリティベンダーは、ネットワーク監視、エンドポイント防御、Web アプリケーション保護、アクセス管理、認証・ID 管理、脆弱性診断、データ保護、IoT セキュリティなど、多様な分野にわたる製品・サービスを提供している。また、クラウド型、オンプレミス型、ハイブリッド型など複数の提供方法があり、企業規模や業種を問わず幅広いニーズに対応している。加えて、脅威インテリジェンス、サイバー演習、CSIRT 運用支援、ペネトレーションテスト、セキュリティコンサルティング、教育・訓練などの運用支援サービスも多数存在する。多言語対応や海外拠点の設置進んでおり、国内外の顧客に対応する体制が構築されている。

**(1)** 企業情報に関する特徴

日本国内に展開するセキュリティベンダーは、日本発の大手 IT 企業や専門ベンダー、外資系グローバル企業などが混在している。資本金規模や法人形態は様々であり、海外展開状況については、ASEAN 諸国（シンガポール、タイ、ベトナム、インドネシア、フィリピン等）をはじめ、北米、欧州、中東、アフリカなど、世界各地に拠点設置や現地パートナー連携の実績が多数確認できた。多言語対応や現地法人設立、パートナー契約などを通じて、国内市場のみならずグローバル市場へのサービス提供体制を整えている企業が多いことが特徴である。

**(2)** 製品・サービスの技術に関する特徴

製品・サービスにおいては、統合監視（SOC、SIEM）、エンドポイント防御（EDR/XDR）、ゼ

ロトラスト、クラウドセキュリティ、脅威インテリジェンス、SASE[37]、ASM、AI/自動化技術など、先進領域に対応するものが多く確認できた。これらはAIや自動化技術による脅威検知・運用効率化、クラウドネイティブなセキュリティ、サンドボックス型脅威分析、API 連携による認証・ID 管理、IoT セキュリティ設計など、最新技術動向を反映した製品が主流である。クラウド型・オンプレミス型・ハイブリッド型といった提供形態も幅広く、企業規模や業種ごとに柔軟な導入が可能であることが特徴である。また、脆弱性診断、ペネトレーションテスト、サイバー演習、CSIRT 運用支援、セキュリティコンサルティング、教育・訓練などの運用支援サービスも充実しており、単なる製品販売にとどまらず、運用体制の強化を総合的にサポートできる点も特徴である。

**(3)** 政府・重要インフラへの導入実績に関する特徴

多くのベンダーの製品・サービスが、官公庁、自治体、電力・ガス・水道・交通などの重要インフラ、金融機関、教育機関などに導入された事例が多数確認できた。特に、統合監視（SOC、SIEM）、EDR/XDR、ゼロトラスト、WAF、CASB、DDoS 対策、認証・ID 管理などの分野は、政府機関や重要インフラでの導入が顕著である。これらの導入実績は、社会インフラの安全確保やサイバー攻撃対策の基盤として、セキュリティサービスが広く活用されていることを示している。地域や業種を問わず、幅広い公共・重要インフラ分野での採用が進んでいる点が特徴である。

さらに、日本国内だけでなく、海外でも政府機関や重要インフラ分野への導入実績が多数確認できる。大手 IT ベンダーやグローバルセキュリティベンダーは、アジア・ASEAN 諸国や欧米など各地域で現地拠点を持ち、現地の政府機関や社会インフラ事業者にサービスを提供している。こうしたベンダーは国際標準に準拠したサービスを展開しており、グローバルに導入実績が広がっている点が特徴である。

[37] Secure Access Service Edge の略称。ネットワーク機能とセキュリティ機能をクラウドで統合した新しいアーキテクチャ。

### 4.5. 本邦企業製品の実証にかかる実証候補企業へのインタビューの実施

ロングリストをもとに、2025 年 7 月下旬から 8 月上旬にかけて、日本国内でサイバーセキュリティ製品・サービスを保有し、ASEAN 地域に拠点を有する、あるいは国際展開に関心を持つ 9 社に対し事前ヒアリングを実施し、各社の事業内容、現地展開の実績や意欲、予算面の課題、現地でのコネクションの有無等を確認した。ヒアリングの結果、想定していた本調査の予算ではコスト面で懸念があること、また企業ごとに現地販売体制の強さに差があることが判明した。以下にインタビュー結果の概要を記載する。

#### 4.5.1 株式会社網屋

**(1)** 会社概要

株式会社網屋[38]（以降、網屋）は、セキュリティ、情報通信、ソフトウェア分野を主軸とする企業で、従業員数は 202 名（2025 年 12 月末時点）、資本金は 6,247 万円（2025 年 9 月時点）である。1996 年 12 月設立、東京都中央区に本社を置き、主力事業は統合ログ管理製品「ALog」などのセキュリティソリューションの開発・販売である。

**(2)** 海外展開可能性のある製品とその特長・優位性

ALog[39]は、独自のログ翻訳変換技術と AI による不正予兆検知を搭載した統合ログ管理（SIEM[40]）製品である。多種多様な IT システムから自動でログを収集し、専門知識不要で分かりやすく管理・分析できる。国内外で 6,000 契約以上の導入実績があり、国産 SIEM 分野で No.1 の実績を誇る。

主な特長は、①自動化機能（オンプレ・クラウド問わず自動収集、豊富なテンプレート/プラグイン）、②AI によるログマッピング（時刻フォーマット定義のみで柔軟に対応、正規表現自動抽出）、③アラート通知・レポート解析（テンプレート選択で自動レポート、即時アラート[41]）、④AI リスクスコアリング[42]（普段との違いを自動分析しリスク度合いをスコア化）、⑤特許取得の翻訳変換ロジック（ログを見やすく・正しく・小さく変換、データ容量を 200 分の 1 に圧縮）、⑥低コスト（翻訳変換後のデータ容量で課金、欧米競合より圧倒的低コスト）、

---

[38] 網屋 会社概要 | 会社情報 | 株式会社 網屋

[39] 網屋 カンタン SIEM ALog シリーズ | 株式会社 網屋

[40] SIEM（Security Information and Event Management）とは、ファイアウォールや IDS／IPS、プロキシーなどから出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことで、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントを検知することを目的とした仕組み。

[41] アラートとは、システムが異常やリスクを検知した際に、担当者へ通知する警告メッセージのこと。

[42] AI などの技術を使って、検知したイベントや操作の危険度を数値化（スコア化）し、優先度の高いリスクを抽出・通知する仕組み。

⑦エージェントレス方式[43]（既存システムに負荷をかけず導入可能）、⑧多様な通信プロトコル対応（SMB[44], SSH[45], Syslog[46], WebAPI[47]）である。


**図 9　ALog によるアラート通知・レポート解析イメージ**

**(3)** 海外への事業展開の状況

ASEAN（タイ、ベトナム、シンガポール、マレーシア、インドネシア）を中心に、台湾、中国、英国、米国などで事業展開している。拠点は現地代理店やパートナーを通じて展開し、現地技術サポート体制も整備している。ASEAN 各国では重要インフラ事業者への導入実績があり、マレーシア政府機関、インドネシア大手自動車会社、台湾大手金融機関・政府機関などに納入実績がある。海外売上は 2022 年 57 件、2023 年 64 件、2024 年 72 件と着実に拡大している。

### 4.5.2　株式会社インターネットイニシアティブ

**(1)** 会社概要

株式会社インターネットイニシアティブ[48]（以降、IIJ）は、電気通信業を主軸とする企業で、従業員数は 5,221 名（2025 年時点、連結）、資本金は 230 億 3,700 万円（2025 年時点）である。1992 年 12 月設立、本社は東京都千代田区富士見に所在する。事業内容は、インターネット接続サービス、WAN サービス及びネットワーク関連サービスの提供、ネットワーク・システムの構築・運用保守、通信機器の開発及び販売など多岐にわたる。

**(2)** 海外展開可能性のある製品とその特長・優位性

---

[43] エージェントレス方式とは、監視対象のシステムに専用のソフトウェア（エージェント）をインストールすることなく、標準的な通信プロトコル（例：SMB、SSH、Syslog など）を利用して情報を収集する方法。

[44] Windows などのコンピュータ間でファイルやプリンタなどの共有を行うための通信プロトコルです。ログ収集などにも利用される。

[45] SSH（Secure Shell）は、ネットワーク上で安全にリモートアクセスやデータ転送を行うための通信プロトコルであり、主に Linux やネットワーク機器のログ収集で使われる。

[46] Syslog (System Logging Protocol)は、ネットワーク機器やサーバからログ情報を送信するための標準的な通信プロトコルであり、多くの機器でサポートされており、ログ管理の自動化に利用される。

[47] API（Application Programming Interface）は、ソフトウェア同士が機能やデータをやり取りするための仕組みです。クラウドサービスのログ取得などで利用される。

[48] インターネットイニシアティブ 会社概要 | IIJ について | IIJ

Safous Privileged Remote Access（特権リモートアクセスサービス）[49]は、重要な社内システムや産業用システムに対する安全なリモート接続と特権アカウント管理を一体的に提供するソフトウェアである。従来の VPN（Virtual Private Network） ではなく、インターネットを使ったゼロトラスト通信に基づいてユーザやデバイスを都度検証し、最小限の権限で業務システムへアクセスさせることで、セキュリティレベルを格段に向上させている。近年の大規模なランサムウェア攻撃は、VPN の脆弱性を突かれるケースと特権アカウントの漏洩・不正利用という二つの原因に集約されているといわれており、Safous は、この二大リスクを同時に低減するアプローチを実現する。

主な特徴は、①ゼロトラストアーキテクチャ（VPN を介さず、利用者や機器を「常に検証」する仕組み）、②特権アカウントの安全管理（パスワードを金庫（Vault ）で保護し、必要なときに一時的に権限を払い出して、利用後は自動的に無効化）、③ エージェントレス接続（ユーザ端末に専用ソフトをインストールする必要がなく、Web ブラウザ経由で安全に接続可能）、④多要素認証（MFA）、⑤最小権限アクセス制御（事前に、どのシステムに対し、どのような作業範囲を、どの時間帯に、誰の承認を得てアクセスさせるかを登録）、⑥セッション記録・監査（誰が、いつ、どのシステムに、何を操作したかを動画やログで記録）である。

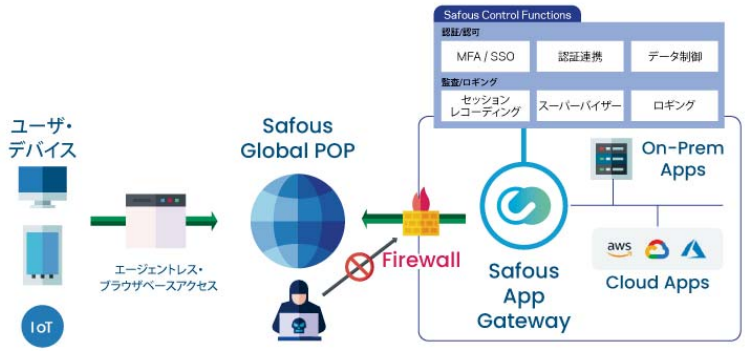



**図 10　Safous Privileged Remote Access の製品概要イメージ**

**(3)** 海外への事業展開の状況

ASEAN（タイ、インドネシア等）において、事業展開を行っている。拠点は現地代理店やパートナーを通じて展開し、現地技術サポート体制も整備されている。ASEAN 各国では重要インフラ事業者への導入実績があり、タイ国立研究機関、インドネシア大手金融機関、インドネシア食品製造企業などに納入実績がある。Safous Privileged Remote Access の海外販売・導入実績は計約 2,500 ライセンスに達している。今後も現地のニーズに応じて、IT/OT 混在環境へのセキュリティ製品導入を拡大していく方針である。

### 4.5.3　株式会社マクニカ

**(1)** 会社概要

株式会社マクニカ[50]（以降、マクニカ）は、半半導体・電子部品・サイバーセキュリティ等

[49] インターネットイニシアティブ IIJ Safous 特権リモートアクセス - ゼロトラストセキュリティに基づいたセキュアアクセスサービス

[50] マクニカ 企業概要 - 会社情報 - マクニカ

を扱う技術商社である。従業員数は 5,071 名（2025 年 3 月時点）、資本金は 111 億 9,426 万円（2025 年 3 月時点）である。1972 年設立され、本社は横浜市に所在する。主力事業は、半導体・集積回路などの電子部品の輸出入、販売、開発、加工、電子機器並びにそれらの周辺機器及び付属品の開発、輸出入、販売である。

**(2)** 海外展開可能性のある製品とその特長・優位性

Macnica ASM[51]（Attack Surface Management：攻撃対象領域管理）は、インターネット上で公開されている情報を利用し、攻撃者の視点から外部公開資産を特定・評価するサービスである。このサービスは「パッシブスキャン型」（対象システムに直接負荷をかけず、公開情報をもとに調査する方式）で実施される。

サービス提供の流れは以下である。まず、①ドメイン調査では、公式に公開されているドメインだけでなく、登録者名やメールアドレス、電話番号などのキーワードを指定し、リバース Whois や証明書情報などのオープンソースデータを活用して、組織が把握していない関連ドメインも抽出・発見する。次に、②サブドメインや FQDN・IP 調査では、見つかったドメインを起点に、サブドメインや IP アドレスなど外部公開システムを幅広く探索する。最後に、③リスク調査では、発見した資産に存在する脆弱性を特定し、既知の脆弱性データベースや特許出願中の技術を使って、各 IP で稼働しているサービスや製品、開いているポートを確認し、外部から悪用される可能性のある脆弱性を洗い出す。主な特徴は、以下の３点である。

A) 外部公開資産の網羅的発見：OSINT（Open Source Intelligence：公開情報を活用した情報収集）を使い、インターネット上で公開されている資産を自動と手作業の両方で特定
B) ノイズ除去と精度向上：抽出の過程で混入する他社資産や誤検知（ノイズ）を、アナリストが目視で確認・除外し、最終的なリストを作成
C) 攻撃者視点のリスク評価：発見された資産に関わる脆弱性の中から、ランサムウェアなどの重大なインシデント（被害につながる出来事）に直結しやすい「クリティカル脆弱性」（重大度が高い脆弱性）を、アナリストが選別・判定して通知）

[51] マクニカ Macnica Attack Surface Management - セキュリティ事業 - マクニカ

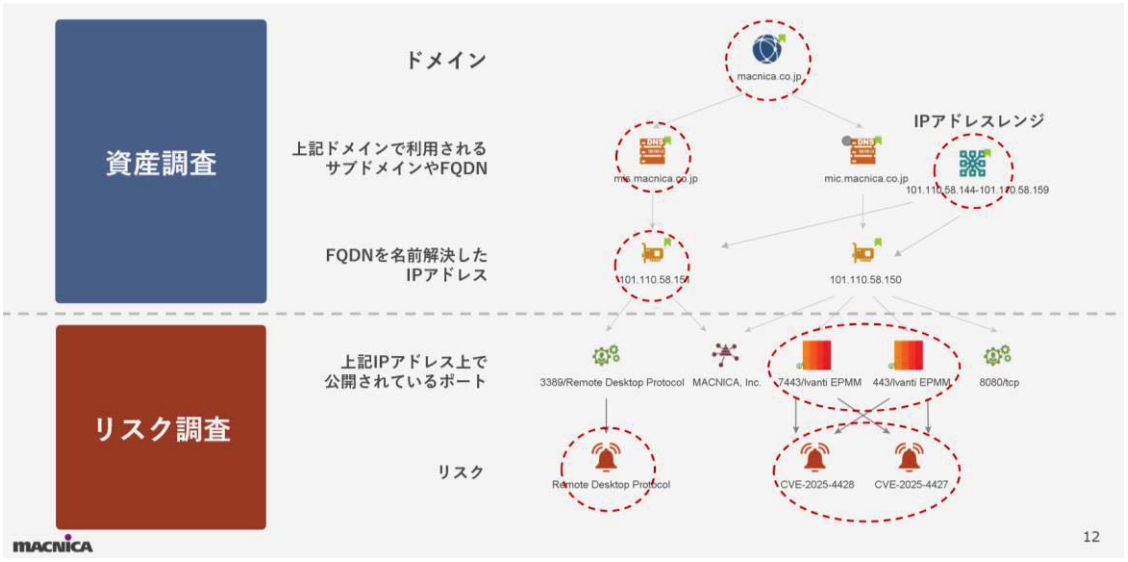



**図 11　Macnica ASM 調査プロセスのイメージ**

**(3)** 海外への事業展開の状況

Macnica ASM は、国内において重要インフラを含めて約 60 社に導入実績が有るが、海外企業への導入実績は 2025 年 12 月時点ではない。グループとして ASEAN 諸国（タイ、フィリピン、インドネシアを含む）へのコネクションがあり、シンガポール、中国、台湾、韓国、アメリカ、イギリス、ブラジル等にも海外子会社を有している[52]。グループ企業と連携して販路の拡大を行っているが、現地法人ごとに販売する商材ドメインと製品が異なる。また、サイバーセキュリティのディストリビューション事業にて、本事業の対象国のタイ、フィリピン、インドネシアに現地子会社の Netpoleon Solutions Pte Ltd. が強いコネクションを有している.

### 4.5.4　　トレンドマイクロ株式会社

**(1)** 会社概要

トレンドマイクロ株式会社[53]（以降、トレンドマイクロ）は、コンピュータ及びインターネット用のセキュリティ関連製品を開発して販売するサイバーセキュリティ会社である。従業員数は 6,869 名（2024 年 12 月時点）、資本金は 199 億 2,600 万円（2024 年 12 月時点）である。1989 年 10 月に台湾出身の創業者により設立され、本社は東京都新宿区に所在する。主力事業は、コンピュータ及びインターネット用セキュリティ関連製品・サービスの開発・販売である。

**(2)** 海外展開可能性のある製品とその特長・優位性

Deep Discovery Inspector（DDI）[54]は、組織の内部ネットワークに潜む脅威を可視化し、標的型攻撃や情報窃取型マルウェアなどの不審な通信を検知するセキュリティアプライアンスである。DDI は通信パケットの情報から挙動分析を行い、ネットワーク上の不審なふるまいや要注意アプリケーションの検出、C&C サーバへの接続検知、サンドボックスによるファイルの動的

[52] マクニカ 拠点情報 - 会社情報 - マクニカ
[53] トレンドマイクロ 会社概要 | トレンドマイクロ (JP)
[54] トレンドマイクロ Deep Discovery™ Inspector | トレンドマイクロ (JP)

解析などの機能を有している。通常の設置ではコアスイッチのミラーポート設定を行い、DDI はコアスイッチを経由する通信のコピーデータを解析する。そのため、設置にかかる手間が少なく、また万が一 DDI に障害が発生した場合でも、ネットワークへの影響が少ない。

DDI は、トレンドマイクロの管理するクラウドコンソールに検知情報をフィードバックすることで、他ソリューションのログ等と統合管理ができ、攻撃の全体像の可視化や顧客の管理・運用負荷の削減に寄与する。また、Trend Service One Complete というセキュリティアナリストによるソリューションの運用支援を提供しており、クラウドコンソールを監視するサービスがある。一方、顧客の都合でクラウドコンソールに検知状況等をアップロードできない場合、DDI にログインしてコンソールを直接確認することで、検知情報を確認することができる。この場合、コンソールにアクセスするために現地へ訪問し、直接状況を確認しながら、きめ細やかなサポートや迅速な対応を行うことができる。

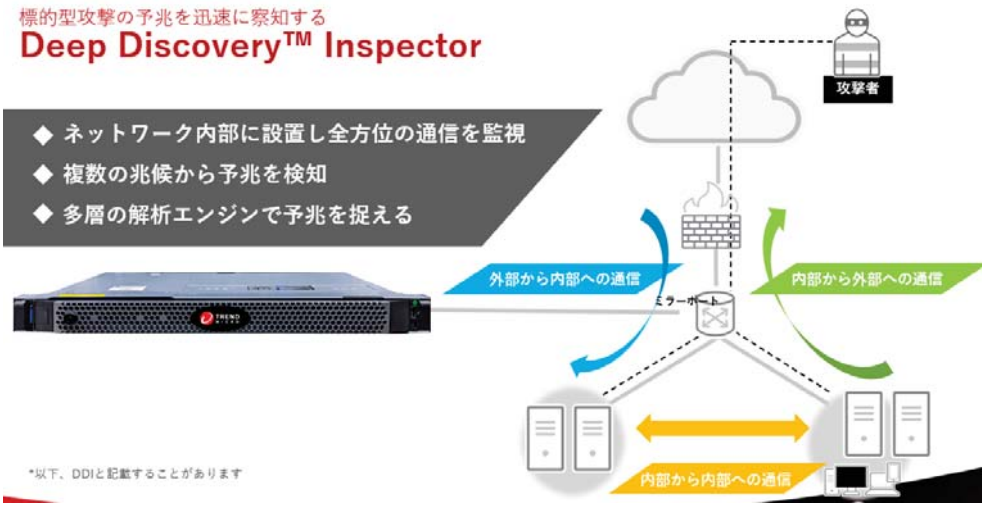



**図 12　Deep Discovery Inspector の製品概要イメージ**

**(3)** 海外への事業展開の状況

調査希望対象国となっているインドネシア、タイ、フィリピンには、トレンドマイクロの営業拠点があり営業担当者とエンジニアが在籍している。営業拠点がある国では、DDI を含めたソリューションの販売実績があり、主に当該国の政府機関及び重要インフラ事業者（主に金融）に導入されている場合が多い。また、販売形態としては、海外でも日本と同様のライセンス体系になっており、新規購入時に初年度のソフトウェア利用料とハードウェアサポートがセットで含まれる。次年度以降は、DDI のソフトウェア更新費用を支払うことで使用を継続することが可能である。

### 4.5.5　株式会社 SYNCHRO

**(1)** 会社概要

株式会社 SYNCHRO[55]（以降、SYNCHRO）は、製造業およびサイバーセキュリティ製品開発を主軸とする企業である。従業員数は 38 名、資本金は 3 億 1,517 万円（2026 年 1 月現在）である。2001 年 4 月設立で東京都千代田区に本社を置いている。具体的な事業概要としては、①手の甲静脈認証システム「VPⅡ」シリーズを中心に入退室管理システムの製造・販売・設置・保守、②排他的 IP ネットワーキング技術「KATABAMI」の各種 IoT 機器への組込み・開発・販売・保守、③①「VPⅡ」②「KATABAMI」によるリアル&サイバー両空間からのトータルアクセスコントロールで差別化を図ったソリューションシステムの企画・設計・開発・保守のワンストップエンジニアリング実践に基づく、セキュアな次世代型サービスプラットフォーム構築事業がある。

**(2)** 海外展開可能性のある製品とその特長・優位性

KATABAMI シリーズ[56]は、SYNCHRO が開発した国産サイバーセキュリティ製品群であり、主に以下の 4 製品で構成されている。①KATABAMI VDP dawn は、安価な機器に装着することでネットワーク上の接続機器を自動的に洗い出す。②KATABAMI VDP は、遠隔からオフィス内部（LAN 内）の脆弱性診断を実施する。③KATABAMI Isolator は、脆弱性が解消できないが業務上利用継続が必要な機器をネットワークから安全に隔離する。④KATABAMI CRA は、ランサムウェアが入り込めない通信経路を構築しデータを保管する。

脆弱性診断サービス②KATABAMI VDP とそれに付随する対策アドバイスの特長としては、机上での一般論に留まらず、対象企業を実際に診断した結果をレポートするという「個別具体的な課題解決」であるということがある。診断結果レポートは、脆弱性評価において世界的に活用されている FIRST（Forum of Incident Response and Security Teams） の「共通脆弱性評価システム CVSS（Common Vulnerability Scoring System） v3 概説」に基づき作成する。さらに、各脆弱性への対応策も個別に説明するため、対象企業の意識喚起とセキュリティ知識の習得にも寄与できる。加えて、ランサムウェアなどのサイバー攻撃を受けた際に、リストアップ可能なバックアップデータを遠隔地に（VPN ではない分離されたネットワークに）保管する対策も有効である。このサービスは④KATABAMI CRA として日本国内では提供済みである。

[55] SYNCHRO 会社概要・沿革・アクセス – 株式会社 SYNCHRO
[56] SYNCHRO KATABAMI – 株式会社 SYNCHRO

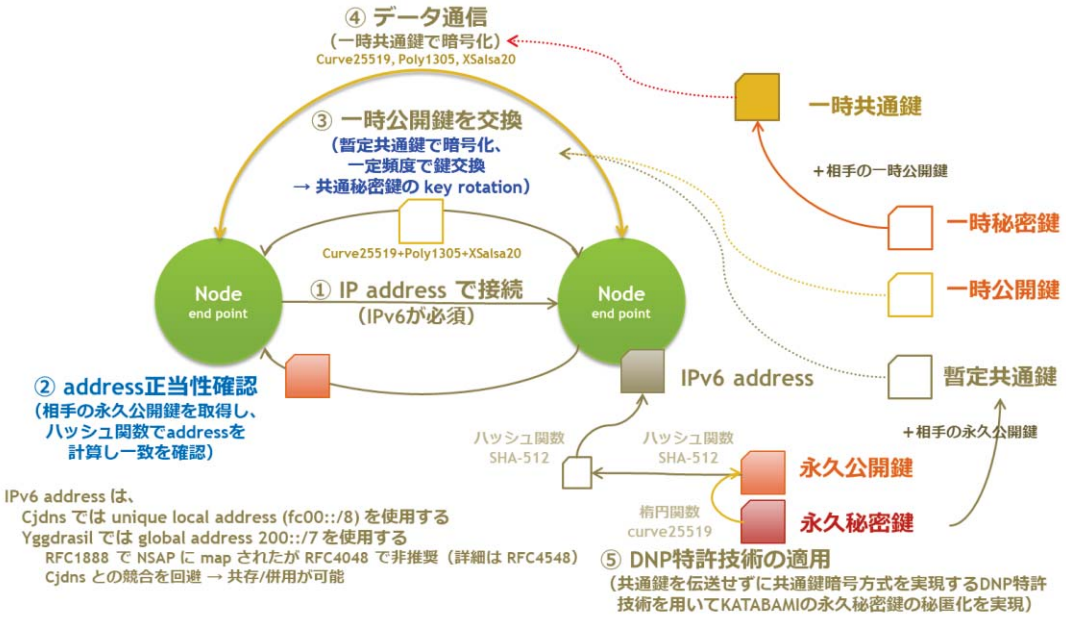



**図 13　KATABAMI 通信の概念図**

**(3)** 海外への事業展開の状況

国内では原子力関連組織や新聞社などの重要インフラ分野を含め、20 件の導入実績がある。海外販売・導入実績は、ベトナムのシステム開発企業 1 件となっている。今後は ASEAN の現地重要インフラ事業者との連携を強化し、事業拡大を目指している。例えば、インドネシアでは災害対策研究センターや発電所、フィリピンでは産業機器用スイッチメーカーなどと経営層レベルでのコネクションを有している。

### 4.5.6　GMO サイバーセキュリティ by イエラエ株式会社

**(1)** 会社概要

GMO サイバーセキュリティ by イエラエ株式会社[57]（以降、GMO）は、情報通信業を主軸とし、従業員数は 302 名（2025 年時点）、資本金は 1 億円（2025 年時点）である。2013 年 2 月設立され、本社は東京都渋谷区に所在する。主要事業には、脆弱性診断（サイバーセキュリティ診断）、ペネトレーションテスト、セキュリティインシデント/フォレンジック対応支援、セキュリティ訓練/資格取得支援、SOC、セキュリティコンサルティング、ASM/脆弱性診断ツール「GMO サイバー攻撃ネット de 診断」の開発/運営、WAF の自動運用サービス「GMO サイバーセキュリティ WAF エイド」の開発/運営、価格調査ツール「プライスサーチ」の開発/運営がある。

**(2)** 海外展開可能性のある製品とその特長・優位性

GMO サイバー攻撃ネット de 診断 ASM[58]は、Attack Surface Management（ASM：攻撃対象領

[57] GMO サイバーセキュリティ by イエラエ株式会社 会社情報 | 脆弱性診断（セキュリティ診断）の GMO サイバーセキュリティ by イエラエ

[58] GMO サイバーセキュリティ by イエラエ株式会社 GMO サイバー攻撃ネット de 診断 ASM| GMO サイバーセキュリティ by イエラエ株式会社

域管理）ツールである。インターネット上に公開されている組織の資産（IP アドレス、ドメイン、サブドメイン、Web アプリケーション、ネットワーク機器など）を自動的かつ継続的に探索・把握し、脆弱性や設定不備の有無を検出・管理することを目的としている。従来の人手による台帳管理やスポット診断に比べ、ASM は自動化と継続的モニタリングによって攻撃者に先んじてリスクを発見できる。

主な特長・優位性は、①外部資産の自動探索（インターネット上に存在する公開資産を自動的にクローリングし、組織が把握していない資産も検出可能）、②脆弱性・リスク評価（検出資産に対して脆弱性スキャンを実施し、国際標準（CVE、CVSS スコア）に基づいて分類。優先度付与と修正指針の提示）、③継続的モニタリング（定期的な自動監視（週次・月次）で新たな露出資産や構成変更を検知し、リアルタイムにアラート通知）、④レポーティングと可視化（ダッシュボードで組織全体の外部攻撃対象面を俯瞰。非技術者でも理解しやすいレポートを経営層や監督機関へ提供可能）、⑤人材不足補完（専門人材が不足している組織でも、ASM の自動化により効率的な資産管理が可能）である。


**図 14　ASM 診断フロー**

**(3)** 海外への事業展開の状況

国内では情報通信や金融業界を主とする重要インフラ企業に対して累計 30 社以上の提供実績がある。また、モンゴル国ウランバードル市に海外展開を行っている。ASEAN への事業拡大を目指しており、本調査対象国であるインドネシア、タイ、フィリピンの企業・政府系機関とトップレベル（責任者）でのコネクションを有する。

### 4.5.7　　ヤマハ株式会社

**(1)** 会社概要

ヤマハ株式会社[59]（以降、ヤマハ）は、楽器、音響機器、及び関連サービス分野を主軸とする企業である。連結従業員数は 18,949 名（2025 年時点）で、資本金は 285 億 3,400 万円（2025

[59] ヤマハ 会社概要 - 企業情報 - ヤマハ株式会社

年時点）である。創業は 1887 年、設立は 1897 年 10 月であり、静岡県浜松市に本社を置いている。また、リコーダーやピアニカなどの教育用楽器から、ピアノ、ギター、ドラム、バイオリンなど 100 種類以上の楽器を世界中に提供するとともに、ネットワーク機器事業を展開する中でサイバーセキュリティ製品も提供している。

**(2)** 海外展開可能性のある製品とその特長・優位性

ヤマハは、UTM（Unified Threat Management：統合脅威管理）アプライアンス製品やセキュリティ機能を持つルーター製品を取り扱っている。UTX100/UTX200 は中小規模企業に必要とされるセキュリティ機能を 1 台で提供することができる UTM アプライアンス[60]である。設置するだけの簡単導入で複数のセキュリティ対策を高コストパフォーマンスで実現することが可能である。従来のネットワークセキュリティ機器に標準搭載されていたファイアウォール機能に加え、マルウェアや標的型攻撃などの脅威に対抗するために、アプリケーションコントロール、URL フィルタリング、侵入防止（IPS）、アンチウイルス、アンチボット、アンチスパム機能を搭載している。メーカー専用サポート窓口による設定支援や先出しセンドバックまで含んだサポートサービスがセキュリティーライセンスに付属しており、ヤマハルーター/スイッチとの組合せも一括サポートも行う。

UTX100/UTX200 は、チェックポイント社（Check Point）の高い信頼性を有するコアエンジンを採用しつつ、ヤマハ独自の機能拡張を加えてヤマハならではの付加価値を追及した、より安心して利用できる製品となっている。これらの製品は、重要インフラ向けの導入実績はないものの、主にレストランやコンビニ等のチェーンストア拠点での利用が多い。

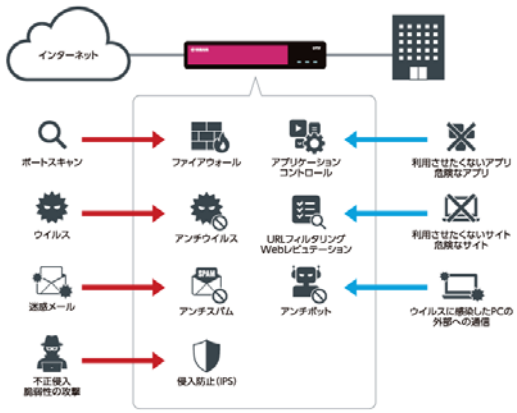



**図 15　UTX100 のセキュリティ機能のイメージ**

**(3)** 海外への事業展開の状況

ヤマハのサイバーセキュリティ製品である UTM アプライアンス製品は、海外展開は行っていない。ネットワーク製品全般の国内販売は SCSK 株式会社が担当しており、海外では現地販売子会社が楽器や音響システムを中心に一部のスイッチ製品を販売している（インドネシア、シンガポール、タイ、フィリピン、ベトナム、マレーシア、アジア、オセアニア、北米、中南米、欧州、中東に現地法人あり）。今後の海外展開については、SCSK 株式会社が一部のルーター

[60] ヤマハ UTX100 特長

製品をインドネシアで発売を開始した他は、具体的な計画の公表は行っていない。

### 4.5.8 SCSK セキュリティ株式会社

**(1)** 会社概要

SCSK セキュリティ株式会社[61]（以降、SCSK セキュリティ）は、サイバーセキュリティ対策に特化した SCSK グループの専門事業会社で、資本金は 5,000 万円（SCSK 株式会社 100%出資）である。2023 年 8 月設立され、東京都江東区に本社を置く。主力事業は、セキュリティサービス開発・販売（コンサルティング、脆弱性診断/評価、トレーニング等）、セキュリティ製品販売である。

**(2)** 海外展開可能性のある製品とその特長・優位性

SCSK セキュリティは製品のインプリメンテーション、コンサルティング、分析業務に強みを持つ。取り扱うサイバーセキュリティ製品は国産に加えて、海外の製品を代理店として販売している。F5 ネットワークス社の代理店として販売している BIG-IP (Advanced) Web Application Firewall[62]（以下、BIG-IP ASM（Application Security Manager））は、Web サーバが利用するポートのトラフィックを監視し、悪意あるユーザから Web アプリケーションとその背後にあるデータを守る Web アプリケーションファイアウォール （WAF）である。入力フォームを備えた Web アプリケーションには、多少なりとも脆弱性が存在することが多い。脆弱性診断を実施してセキュリティホールを発見し、アプリケーション自体を修正する方法もあるが、アプリケーションの数が多い場合はコストや工期の面で現実的ではないことがある。こうした課題に対し、BIG-IP ASM は Web サーバの手前に配置することで、脆弱性を狙ったリクエストをブロックし、アプリケーションやその背後のデータを守ることができる。また、SCSK セキュリティの豊富な WAF 導入実績とノウハウに基づく「SCSK WAF 導入運用支援サービス」と組み合わせることで、サイトごとに最適なポリシーチューニングも行え、より強固な Web システムの構築を支援する。

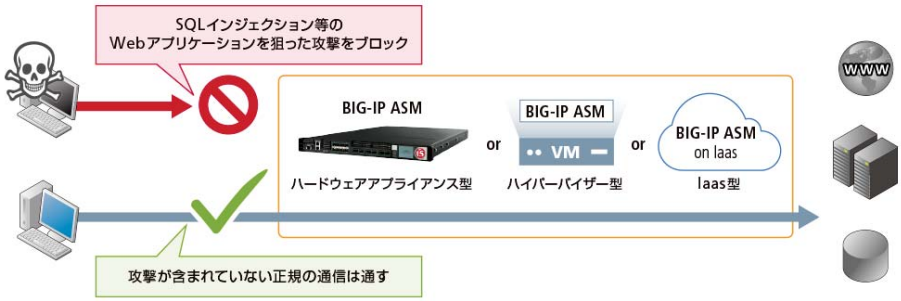



**図 16　BIG-IP ASM の製品概要イメージ**

日本の重要インフラの導入実績として、政府系機関・電力会社等に提供しており、トレンドマイクロ社のティッピングポイント（IPS）や Splunk を国内の政府機関向けに、IBM の QRadar を国内電力会社向けに SIEM ソリューションとして構築・提供している。

**(3)** 海外への事業展開の状況

[61] SCSK セキュリティ企業情報 – SCSK セキュリティ株式会社
[62] SCSK セキュリティオンプレミス型 WAF「F5 BIG-IP ASM」概要 – SCSK セキュリティ株式会社

SCSK グループではイギリス、ドイツ、中国、シンガポール、インドネシア、ミャンマー、米国に海外ネットワークを有しており、現地での顧客対応にも強みを持つ。ASEAN 諸国においては、海外現地法人をインドネシアのジャカルタに設置した（SCSK Global Indonesia が 2019 年に設立）。

### 4.5.9 KDDI 株式会社

**(1)** 会社概要

KDDI 株式会社[63]（以降、KDDI）は、電気通信事業を主軸とする大手総合通信会社で、従業員数は約 64,636 名（2025 年 3 月時点）、資本金は 1,418 億 5,200 万円（2025 年 3 月時点）である。1984 年 6 月設立、東京都港区に本社を置く。主力事業は「au」ブランドによる携帯電話サービス、専用線、プロバイダ、固定電話サービス、衛星電話サービスなどの提供である。

**(2)** 海外展開可能性のある製品とその特長・優位性

KDDI は、市販のセキュリティ製品を活用して運用・監視サービスの提供を行っている。具体的には、「KDDI マネージドセキュリティサービス[64]」において、KDDI のログ分析基盤と KDDI の情報セキュリティ分野のグループ会社である LAC のノウハウを組み込んだ自動分析エンジンを活用し、ゼロトラスト環境に必要なセキュリティ監視・運用を提供するサービスを提供している。ログ分析基盤やセキュリティ人材、運用ノウハウを一括で利用できるため、新たなセキュリティ監視システムや人的リソースを準備することなく、ゼロトラストセキュリティを導入できる。リアルタイムログ分析・検知では、24 時間 365 日リアルタイムでログ分析・検知を行い、重要なアラートを顧客に通知する。特に重要なアラートについては、セキュリティアナリストによる追加分析・対策支援を行い、海外からの英語問い合わせに対し、英語窓口による的確なサポートも可能である。また、導入後はダッシュボード上で、生成 AI を活用した AI 分析・レポート機能によりセキュリティ状況をリアルタイムかつ直感的に可視化でき、アラート数の多い端末やユーザも簡単に確認できる。さらに、指定した期間に対して生成 AI が自動で要約レポートを作成し、表示されたアラート情報や要約レポートはお客さまの任意のタイミングでダウンロード可能なため、セキュリティレポートの作成にも手間をかけずに活用できる。

[63] KDDI 企業情報 | KDDI 株式会社
[64] KDDI KDDI マネージドセキュリティサービス｜マネージド・アウトソース/ゼロトラスト｜法人向け｜KDDI 株式会社

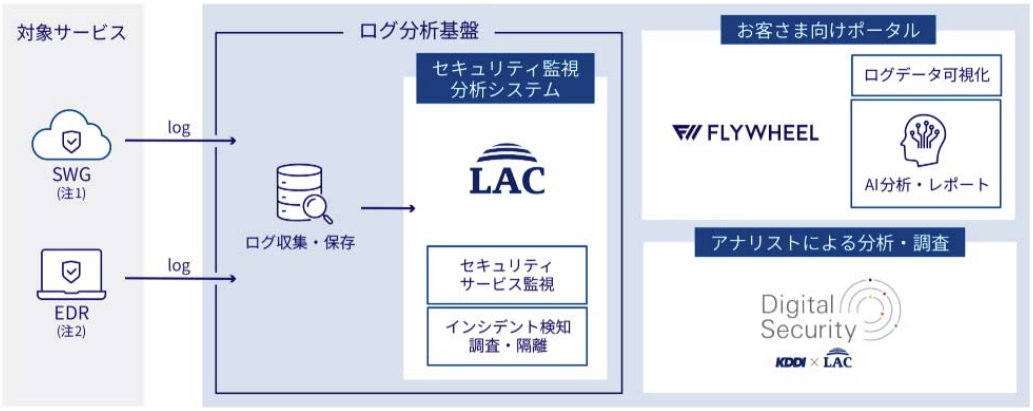



**図 17　KDDI マネージドセキュリティサービスの概要**

**(3)** 海外への事業展開の状況

アジア、オセアニア、ヨーロッパ、中東、北アメリカ、南アメリカの世界各国にグループの拠点を有している。ASEAN 地域では、カンボジア、インドネシア、マレーシア、ミャンマー、フィリピン、シンガポール、タイ、ベトナムに現地拠点があり、これらの国の通信系インフラ事業者や電力会社と強力なコネクションを有している。

## 4.6. 実証事業を行う製品・サービスの選定経緯

### 4.6.1 実証事業を行う製品・サービスの選定方法

事前ヒアリングを行った 9 社に対し、2025 年 8 月 7 日付で公募要領を送付し、8 月 26 日を応募締切日として案内した。実証事業を行う製品・サービスの選定にあたっては、日本国内でサイバーセキュリティ製品・サービスを有し、かつ海外展開への意欲および実績を有する法人を対象に公募した。

公募要領では、対象国をタイ、インドネシア、フィリピンの 3 カ国とし、各国の政府関連組織または重要インフラ事業者から各国 1 組織を実証先として選定し、2025 年 9 月から 2026 年 1 月までの期間に実証事業を実施することとした。現地の実情やニーズに応じて実証方法の調整や改善を行うこと、ならびにデータ保護・プライバシー対応、現地インフラとの統合性、運用性および技術習得の容易性等、多面的な観点から製品・サービスの有効性や持続性を検証することを求めた。さらに、実証の成果や検証結果については報告書として提出することを要件とした。

選定方針として、サイバーセキュリティ分野で十分な技術力・業務遂行能力を有し、事業期間内に業務を完了できる組織体制を持つ日本法人を再委託候補とした。また、前述の「4.4 本邦企業製品の実証にかかる実証候補企業へのインタビューの実施」の結果も踏まえ、実証事業の性質上、価格競争を重視すると参加企業が減少する恐れがあると判断し、JICA と協議のうえ「質に基づく選定」を重視する方針とした。

審査基準は、応募資格の有無、実施目的の適合性（調査目的との合致）、課題解決への貢献可能性（提案製品・サービスの現地課題に対する有効性）、実証計画の妥当性・実現性（具体的なアプローチやスケジュール、体制、現地コネクションの有無）、経費見積の妥当性を総合的に評価・審査した。また、企業ごとに現地コネクションや体制構築の難易度が異なるため、各企業が希望する

国を選択できる方式とし、応募した国ごとに評価・選定した。

#### 4.6.2 実証事業を行う再委託先の選定経緯

募集期間において 9 社中 6 社から応募資料一式を受領し、その後、本調査団及び JICA にて応募企業に対する審査を実施した。審査では、各社の提案内容が本事業の目的や現地課題に合致しているか、提案製品・サービスが現地課題に対して有効でインパクトが期待できるか、実証計画やスケジュール、体制が現実的かつ実行可能であるか、現地政府機関や重要インフラ事業者とのコネクションがあるか、経費見積が妥当かという観点から総合的に評価した。

最終的に 3 社（株式会社網屋、株式会社インターネットイニシアティブ、株式会社マクニカ）を国別に採択することを決定した。各社への採択通知は 2025 年 9 月 5 日に実施し、全社から本事業参画の意向確認を得た。

採択企業及び調査対象国は以下のとおりである。

- 株式会社網屋（タイ）
- 株式会社インターネットイニシアティブ（インドネシア）
- 株式会社マクニカ（フィリピン）

主な選定理由は、実証計画の実現可能性と現地での実施体制が確立されていること、現地の課題解決に有効な製品・サービスであること、現地政府機関や重要インフラ事業者とのコネクションを有していること、海外市場での競争力・持続性・独自性を備えていること、本調査事業を通じて現地市場参入や社会的意義が期待できること点などが高く評価された。

### 4.7. 製品・サービス実証計画及び実証結果

これらのプロセスを経て選定された 3 社と調査団にて、キックオフ会議を実施し、各調査対象国における実証計画の策定、現地パートナーとの合意形成、製品導入・効果測定、調査報告書作成等の実施内容についてすり合わせを行った。なお、各社から提出された調査結果報告に基づく、製品・サービス実証計画及び実証結果は下記の通りである。

#### 4.7.1. 株式会社網屋（タイ）

（1） 対象国及び実証製品・技術・サービス

- 対象国
  タイ
- 実証を行う製品・サービス名
  ALog
- 製品・サービスの概要（特徴・機能・通信の流れ等）

ALog は、独自のログ翻訳変換技術と AI による不正予兆検知を組み合わせることで、多様な IT システムから集めた膨大かつ複雑なログデータも、専門知識がなくても簡単に管理できる SIEM 製品である。6,000 件以上の導入実績を持ち、国産 SIEM 市場でトップシェアを誇る。自動化機能により、クラウドやオンプレミスなど多様な環境から自動的にログを収集し、AI がログの分析やリスクスコア化、異常時の即時アラート通知を実現する。特許取得の翻訳変換技術でログを見やすく圧縮し、データ容量を大幅に削減することでコストも抑えられる。エージェントレス方式を採用し、既存システムへの負荷も最小限で、安全かつ効率的な運用が可能であ

る。

加えて ALog は、追加ソフトなしで多様なシステムから自動でログを収集し、ダッシュボードで状況把握や即時アラート通知が可能である。AI によるリスク検知や自動レポート生成で、監査や運用の効率化、セキュリティ強化、運用負荷の軽減を実現する。主な特徴および機能は、4.5.1 の通りである。

■ALog機能概要

ALogは、様々なITシステムのログを収集・分析・保管するログマネジメント製品です。
ホストが出力する複雑なイベントログ(生ログ)を解析し、実際にユーザーが実行した操作パターン(アクセスログ)に分析変換します。

システムイメージ（ログ収集・分析）

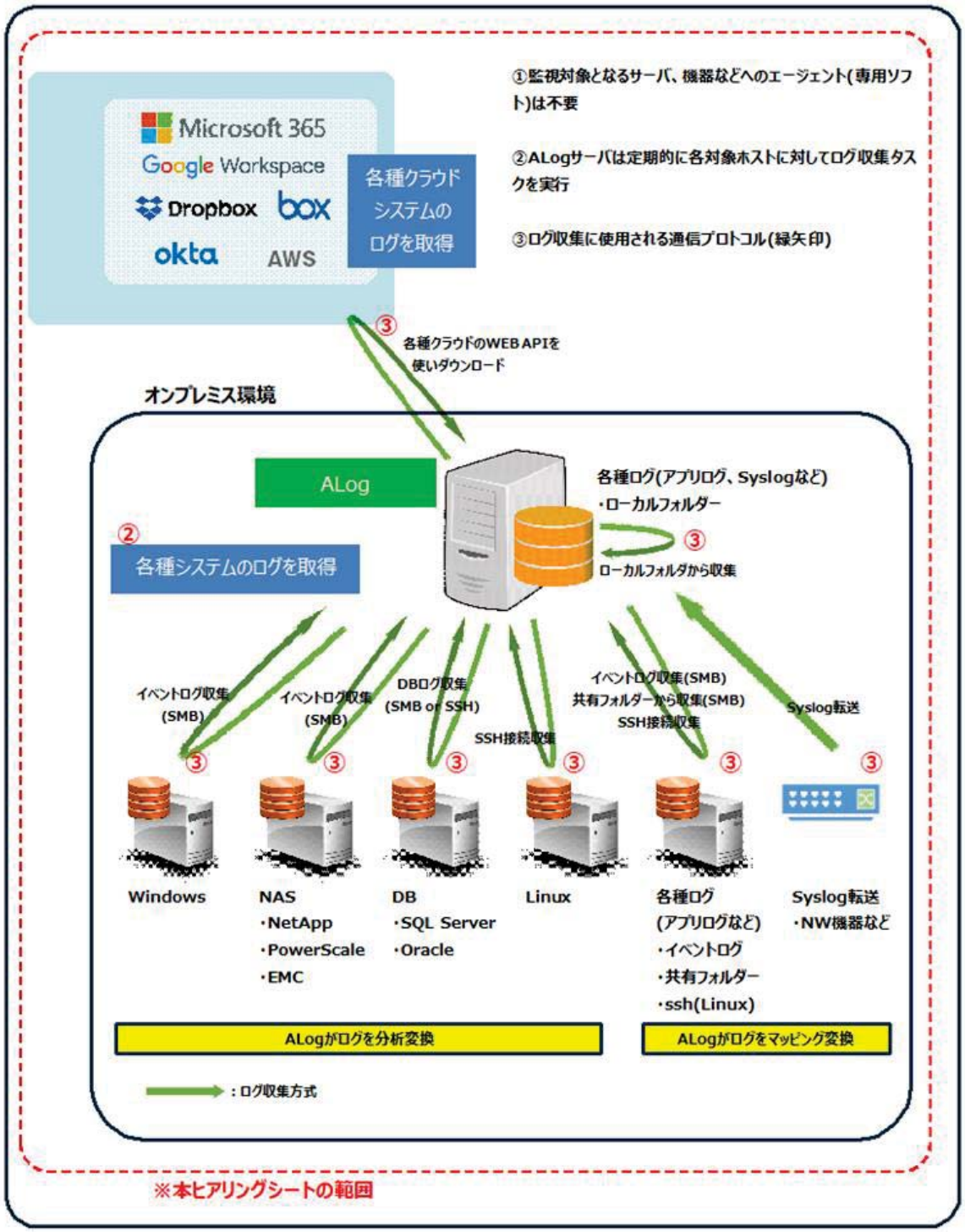



図 18　ALog のシステムイメージ(ログ収集・分析)

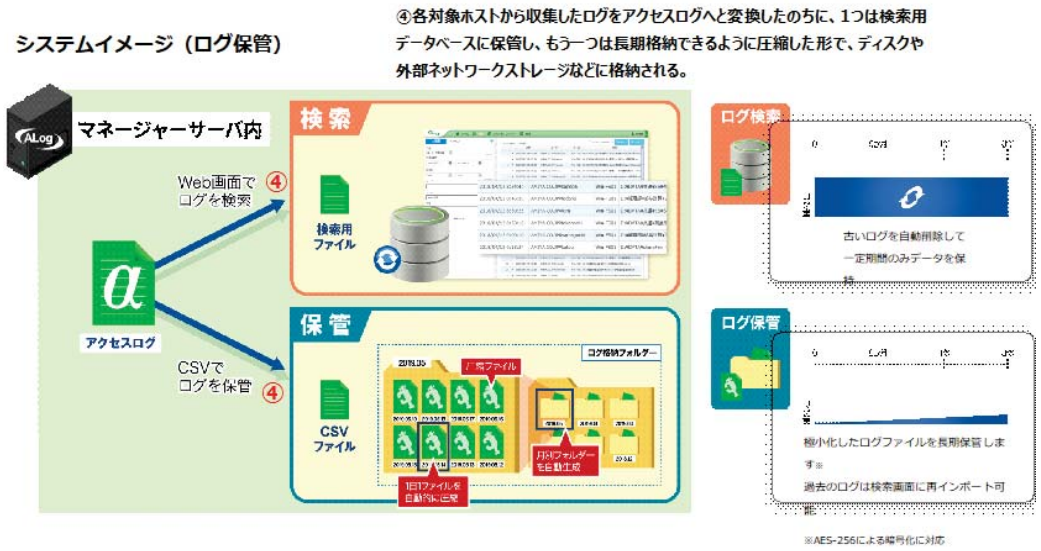



**図 19　ALog のシステムイメージ(ログ保管)**

- 有効性仮説・期待される成果（定量・定性／短期・長期）

ALog 導入により、短期的には重要ログの検知漏れゼロやアラート検知時間の 50%削減を目標とし、テストシナリオによる検証でログの正確性や対応速度を定量評価する。長期的には、インシデント対応の自動化により人員工数を半減し、年間 1080 時間の効率化やサイバー攻撃検知率 50%以上向上を実現する。多様なログ収集と AI による異常検知・リスク可視化により、運用負荷軽減と迅速なインシデント対応が可能となり、セキュリティ強化と事業継続性向上に貢献する。

■定量的成果（短期・長期）

【短期】

ALog 導入の短期目標は、重要ログの検知漏れゼロとアラート検知数・平均検知時間の 50%削減である。評価は、機密ファイルアクセスや権限変更、不正ログインなどのテストシナリオを用いて、ALog が正確にログを集約・表示できているかを目視で確認する。OS やネットワーク機器、クラウドサービスなど対象範囲を明確にし、収集状況もモニタリングする。導入前後で同一シナリオを実施し、アラート対応時間や検知数、誤検知・検知漏れの影響も含めて効果を定量的に評価することで、ALog 導入による運用効率化とセキュリティ強化の実効性を総合的に判断する。

【長期】

ALog 導入により、従来 4 名体制で行っていた 24 時間 365 日のインシデント対応業務を自動化し、2 名分の人員工数を削減できる。1 アラートあたり 30 分かかっていた対応も、ALog の自動判定で 50%削減され、月 180 時間の作業が 90 時間に短縮される。実際の SOC 運用ログや担当者ヒアリングをもとに、導入前後の平均対応時間差を年換算し、年間 1080 時間の効率化が見込める。さらに、従来は一部ログしか分析していなかったが、ALog 導入により複数システムを横断的に分析でき、サイバー攻撃検知率も既存運用比で 50%以上向上する。疑似攻撃シナリオを用いた検証や MDR サービスの顧客満足度も評価に活用し、改善効果を数値で測定する。

■定性的成果

【短期】

ALog は、多様な機器からのログ収集・可視化が可能である。必要なのは時刻フォーマット定義のみであり、AI が正規表現のマッピング候補を自動抽出するため、ログフォーマットの変更や設定も容易に行うことができる。また、AI によるリスクスコアリング機能を搭載しており、データの特徴を分析して不正アクセスや情報漏洩のリスクを 10 段階で可視化・通知できる。普段との違いを検知し、サイバー攻撃の兆候も早期に把握可能である。

【長期】

セキュリティインシデントに備えることで、有事の際に迅速な対応とセキュリティの可視化を強化できる。インシデント発生時も、ALog による適切なログ管理によりセキュリティ状況を可視化でき、早期検知や正確な調査が可能となる。その結果、スムーズなインシデント対応が実現し、事業復旧の遅延や会社の信用失墜を防ぐことが可能となる。

（2） 実証事業の内容

・ 実証の目的

ALog は現在、シンガポール、マレーシアなど、東南アジアを中心としたアジア各国や欧米、その他の地域で販売されている。今後は、ASEAN 各国の重要インフラ事業者市場を拡大する方針である。これにより、メイドインジャパンのセキュリティ製品としての知名度を高め、品質の高さを認知させるとともに、現地重要インフラ事業者のセキュリティ可視化強化に貢献することを目指す。サイバー攻撃や人為的要因による個人情報漏洩などのインシデント発生時に、いかに迅速に検知・対応できるかが重要であり、ALog 導入により限られたリソースでも効率的な検知・対応が可能となる。サイバーセキュリティリスクへの対応策として、ALog はアクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを提供するものである。

・ 実証スコープ・重点実証項目

A) ALog の現地での有効性、持続性、現地適合性

① 有効性（サイバーセキュリティとコンプライアンス）

ALog は PC や Active Directory、Firewall など複数のログを統合・横断的に分析することで、サイバー攻撃や内部不正の予兆を早期に検知し、セキュリティレベルを大きく向上させることができる。また、タイの個人情報保護法（PDPA）にも対応しており、ログから迅速に原因を特定し、証拠を保全することで、法令が定める情報漏洩時の通知義務を確実に果たせる。

② 持続性（長期的な運用サポート）

ALog は現地で製品トレーニングを受けた認定代理店による技術サポートを継続的に受けられるため、システムの安定稼働と長期利用が可能である。ログ圧縮機能や柔軟な価格体系により、事業拡大やログ増加にも無駄なく適応できる運用を実現できる。

③ 現地適合性（人材・スキルへの対応）

ALog は独自のログ翻訳技術により、専門知識がなくても「いつ、誰が、何をしたか」を分かりやすく自動変換できるため、現地のセキュリティ専門家不足を補うこと

ができる。また、オンプレミス版とクラウド版の両方を提供しており、現地のインフラや要件に応じて最適な導入方法の選択が可能となる。

B) 法規制遵守、統合性と運用性の実証

タイの PDPA における 72 時間以内の通知義務や、データ主体への速やかな通知義務にも対応できる。ALog は不審なアカウント操作や特権ユーザのログオン、不正アクセス、ランサムウェアの被害範囲などを監視し、レポートサンプルを作成することで、法規制の遵守と実際の運用性を実証する。

C) スコープ

ALog の現地導入および運用検証においては、ファイルアクセス、認証、ネットワーク、PC、メール、プロキシ、VPN など多様なログの取得とレポーティング、異常検知時のアラート設定を行う。これにより、少人数の IT セキュリティスタッフでも迅速かつ的確な対応が可能であることを検証する。

・ 実証方法（項目・方法・期間・渡航回数など）

A) 実証期間および現地渡航

実証事業の体制は、日本側に業務責任者 1 名、業務主任者 1 名（プロジェクトマネジメントおよび実証先との交渉を担当）、業務補佐 1 名（IT エンジニア）を配置し、さらにタイ現地側に業務補佐 1 名（IT エンジニア）を加えた計 4 名体制で実施する。実証は 1〜2 ヶ月間行い、現地渡航は 2 回（初回は導入と設定、中間〜最終は調整・効果測定・報告）を予定している。日常監視やアラート対応は現地 IT エンジニアが担当し、日本側がリモートでサポートを行う。

B) 現地環境に合わせた導入内容

サーバ、ネットワーク機器、ストレージ、クラウドサービスを対象に ALog を導入する。事前に現地インフラの棚卸しやログ出力の確認、セキュリティポリシーのヒアリングを実施し、導入目的を整理する。

C) ログ収集設定・アラート閾値調整

認証、操作、ネットワーク、クラウドの各種ログを収集し、ALog 標準テンプレートでアラート閾値を初期設定する。現地業務に合わせ実証期間中に設定をチューニングし、擬似イベントで検知精度を検証する。

D) 調査項目ごとの検証・測定・評価方法

現状の対策や運用体制、課題、発生背景をヒアリングやドキュメントレビューで確認する。現地ニーズや製品要望もアンケートやインタビューで把握し、ALog の有効性・持続性・適合性・ニーズ合致度をテストやヒアリングで評価する。データ保護・プライバシー対応、現地インフラとの統合性、運用性・技術習得、障害対応力も検証する。

E) 現地担当者への運用トレーニング

現地 IT スタッフ向けに 2 時間程度のオンラインまたはハンズオン形式でトレーニングを実施し、操作やレポート作成の習熟度を確認する。トレーニング後は満足度調査やインタビューを行う。

F) 評価指標とフィードバック

平均検知時間の 50%削減、サイバー攻撃検知率 50%以上向上、月 90 時間以上の運用工数削減を数値目標とする。進捗や効果は定量・定性指標で評価し、週次レビューや最終レポートで現地チームと共有する。

・ 実証スケジュール

スケジュールは下記の通り。

2025 年 9 月中旬～下旬　実証計画策定

2025 年 10 月上旬～中旬　実証先選定（イベント出展・現地含む）、実証先決定

2025 年 10 月中旬～下旬　実証先とのキックオフ実施（現地渡航）

2025 年 10 月中旬～11 月上旬　実証先調査・要件整理、対象システム選定・監査設定確認

2025 年 10 月下旬～11 月下旬　ALog 導入・ログ収集設定、運用検証実証実施（現地）

2025 年 11 月上旬～12 月上旬　実証運用、効果測定

2025 年 12 月上旬～12 月中旬　結果分析、報告書作成、実証先への報告、トレーニング実施

2025 年 12 月下旬　調査報告書（ドラフト版）提出

2026 年 1 月中旬　調査報告書（最終版）提出

2026 年 1 月下旬　最終報告会・意見交換会実施

（3） リスクと対応策

・ 外部要因リスク

サーバの現地調整の遅延、技術トラブルなどは、現地にパートナー及び網屋エンジニアが常駐しているため迅速な連携解決が可能である。対応スキームは下記の図の体制で対応する。

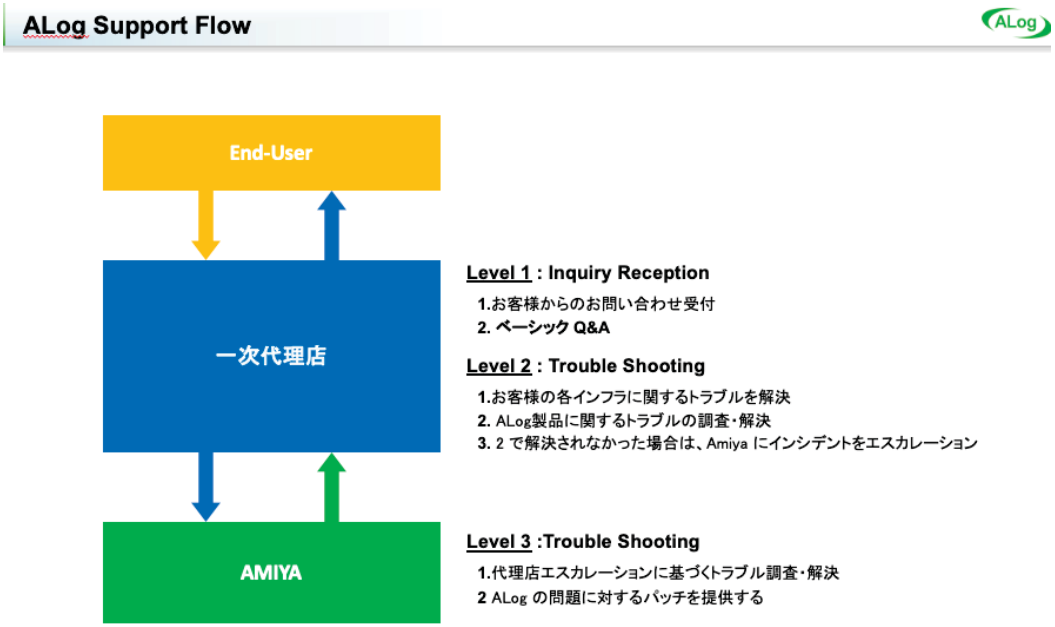



**図 20　ALog サポートフロー**

・ 法規制リスク（データ越境／個人情報保護／輸出入）

A) データ越境

当該製品は、現地サーバに格納されたデータへのアクセス履歴を監視する製品であり、データを直接国外に送信することはないため、データ越境の懸念は生じない。

B) 個人情報保護

当該製品は、個人情報の取り扱いが現地法に適合している。

C) 輸出入

本実証で使用したソフトウェア（ALog および関連コンポーネント）は、開発元である株式会社網屋の公式サイトから現地サーバへインターネット経由で直接ダウンロードして導入する。そのため、CD-ROM や USB メモリなどの物理媒体による国際輸送や通関手続きは発生しない。

・ その他留意事項

A) システム運用リスク

ALog のログ収集対象が増えるとネットワークやサーバに負荷がかかり、遅延や欠損が発生する可能性がある。収集間隔の調整やサーバスペックの見直し、分散処理で対応できる。また、OS やクラウドサービスの仕様変更による一時的な収集停止には、ベンダーパッチや定期的な検証が有効である。

B) セキュリティリスク

ログ収集に高権限アカウントが必要なため、不正利用リスクがある。用途を限定し、強固なパスワードポリシーを導入することで対策する。

C) 障害・災害リスク

ALog サーバが停止するとログ収集が中断するため、定期的なバックアップや迅速な復旧体制が必要である。電源障害や空調トラブルには UPS や適切なラック環境で対応する。

D) 技術トラブル

ハードウェア故障、ネットワーク断、ソフトウェア不具合、データ損失、セキュリティインシデントなどが想定される。

E) 冗長構成・復旧策

クラスタやフェイルオーバーは標準で備えていないが、設定ファイルやログのバックアップを定期的に実施することで、障害時も新環境で迅速に復旧できる。外部ストレージへの二重保管も推奨される。

（４） 実証先の概要

・ 名称・所在地

組織名：Faculty of ICT, Mahidol University

所在地：999 Phutthamonthon Sai 4 Road, Salaya,Nakhon Pathom 73170, Thailand

ウェブサイト： https://www.ict.mahidol.ac.th/en/

・ 実証先の業務内容

Mahidol大学はバンコクに本部を置くタイ王国の国立大学であり、1888年創立、1943年に大学として設置された。前身はタイ初の国立医科大学であり、現在は 17 学部など多くの組織を持つ総合大学である。世界大学ランキング 2025 ではタイ国内 2 位に位置している。同大学はシリラート病院医学部バリュードリブンケアセンターと連携し、医療イノベーションを推進するプログラムを実施している。さらに、2026 年にはサイバーセキュリティセンターの設立が予定されている。サイバー攻撃によって機能が停止した場合、機密情報の漏洩等重大な影響が生じる可能性がある。

Mahidol 大学 ICT 学部[65]は、学部長である Dr. Pattanasak Mongkolwat 氏を中心に、6名のアドバイザー、4名の副学部長、12名の学部長補佐によって構成されている。学科は6つの部門で組織されている。今回の PoC（概念実証）は、これらの部門のうち、17 名で構成される「Office of Technology Support（技術支援部門）」の協力のもとに実施した。特に、「Technology Infrastructure Division（技術インフラ部門）」の教授陣が中心となって PoC を推進した。

図 21　Mahidol University 外観

・　実証環境

A) 実証環境の定義（本番環境での実施）

本実証は、導入効果および既存システムへの影響を正確に検証するため、教職員や学生が日常的に利用している本番環境で実施した。テスト用の擬似データではなく、実際の業務や授業に伴うアクセス操作ログを分析対象としたことで、実運用に即したログ収集の安定性と検知精度を評価することができた。

B) 使用機器・ソフトウェア一覧

本実証で使用したハードウェアおよびソフトウェアの仕様は、以下の通りである。

[65] Mahidol University ICT 学部 People – Faculty of ICT, Mahidol U.

**表 5　実証環境の仕様（ハード・ソフトウェア）**

| 役割 | ホスト名 | 詳細 | 備考 |
|---|---|---|---|
| ALog 管理サーバ | ALog Server | OS:Microsoft Windows Server<br>ソフトウェア:<br>ALog V1.1.5<br>ALog Syslog Receiver V1.0.3 | 対象サーバ/機器よりログを収集後、分析しアラートやレポートを生成 |
| 対象サーバ 1（AD） | AD 1 | Windows Server<br>Active Directory | ログインやアカウント権限に関する管理を行い、そのログを生成 |
| 対象サーバ 2（AD） | AD 2 | Windows Server<br>Active Directory | ログインやアカウント権限に関する管理を行い、そのログを生成 |
| 対象サーバ 3 （AD） | AD 3 | Windows Server<br>Active Directory | ログインやアカウント権限に関する管理を行い、そのログを生成 |
| 対象サーバ 4 | File Share | Windows Server | ファイルを格納し、それに関するログを生成 |
| 対象 NW 機器 | NW 機器 | 中規模拠点向け次世代ファイアウォール | VPN や Thread(脅威)に関するログを生成、及び ALog 管理サーバに転送 |

C) システム構成およびログ収集の仕組み

上表は、本実証で使用したシステム接続構成と各機器の役割を示している。黒枠内が監視対象範囲（オンプレミス環境）であり、ユーザは PC から認証サーバやファイルサーバ、ネットワーク機器を経由してシステムを利用している。ALog 管理サーバは、これらのサーバやネットワーク機器から出力されるログを収集し、エージェントレス方式でイベントログを一元的に取得している。ネットワーク機器からは Syslog 形式でログが転送される。収集されたログは ALog 内部で自動的に分かりやすい形式に変換・蓄積され、管理者は PC のブラウザから一括して検索・分析できる。

（5） 対象国・実証先におけるサイバーセキュリティ上の課題

- 現状の対策状況

  Mahidol 大学 ICT 学部は、シリラート病院医学部とのシリラート病院患者のための献血共同プロジェクトを推進しており、極めて機密性の高い情報を多数保有している。情報の秘匿性を維持するため、運用は外部委託せず、内部スタッフによる自律的な管理を徹底している。大学全体の共通セキュリティサービスを利用しているが、特定部門におけるアクセス監視やログ管理の詳細な可視化には課題が残る。サイバー攻撃による情報漏洩が発生した場合、連携プロジェクトの運営に深刻な支障をきたすリスクがある。
- 現状の運用体制・管理方法

ICT 学部の技術インフラ部門が全ての運用・管理を担当しており、アウトソーシングは行っていない。技術インフラ部門は 19 名で構成され、技術設備部門、システムエンジニアリングおよび保守ユニット、建築・景観ユニット、教室および実験室サポートユニット、技術基盤事業部、通信ネットワーク管理ユニット、コンピュータシステム管理ユニット、情報・システム部門、オーディオビジュアル・デジタル学習メディア開発部門の各ユニットが存在する。

- 主な課題・制約

  最大の課題は予算の制約であり、新たなセキュリティ製品の購入が困難な状況である。また、教員が IT システムやセキュリティ管理を兼務しているため、人的リソースに余裕がない。

- 発生背景

  過去に重大なセキュリティインシデントは発生しておらず、現時点でセキュリティリスクは高くないと認識されている。

（6） 対象国・実証先におけるサイバーセキュリティ製品・サービスのニーズ

- ニーズの種類

  予算が限られているため、現時点では新規のセキュリティ製品やサービスを導入する計画は存在しない。大学では共通プラットフォームおよび独自開発のアプリケーションを用いている。2026 年中に新設されるサイバーセキュリティセンターにて、各種セキュリティ対策を一元的に集約・管理する方針である。そのため、将来的には共通プラットフォームや独自アプリケーション、業務システムを監視・管理できるセキュリティ製品・サービスの導入ニーズがあると考えられる。

- 製品・サービスニーズ

  予算の制約があるため、現状では新規導入の予定はない。しかし、大学内の他学部と共通プラットフォームを利用しているため、独自アプリケーションの監視が可能なソリューションが必要である。

- ニーズの根拠

  大学の他学部が共通プラットフォームを利用していることから、独自アプリケーションの監視ができるソリューションが必須である。

（7） 対象国・実証先におけるサイバーセキュリティ製品・サービスの有効性・持続性・適合性・ニーズ検証

- 有効性

  <u>概要</u>

  ALog 製品は、認証基盤、ファイル共有、ネットワーク境界など複数の重要システムに対し、安定したログ収集と監査証跡管理を実現することができる。一定の検証期間において、長期休暇期間を含む連続稼働を実施したが、ログの欠損や収集停止は一切発生せず、主要な操作（ファイル操作、認証、権限変更、外部通信など）を網羅的に記録・再現できることが確認された。

具体的な確認実績

- 認証基盤（Active Directory）では、ログイン認証の成否や監査ポリシー変更など、管理者の操作履歴を正確に記録し、不正アクセスや内部不正の予兆も監査可能であることを実証した。
- ファイルサーバでは、ファイルの作成・削除・リネーム操作をユーザ単位で特定できる。特にリネーム操作はランサムウェア対策に有効であり、異常検知のためのデータ収集基盤が確立されている。
- 境界防御では、トラフィックログや脅威情報を ALog で統合管理でき、外部製品との連携による相関分析基盤が確立されている。
- 事前に定義したリスクシナリオ（不正ログイン、連続認証失敗、監査設定変更、重要ファイルの名称変更・削除）に対して、全ての検知アラートが即時発報され、検知漏れはゼロ（検知率 100%）であった。
- 実証期間中に発生した 14 件のリスク判定ログについて、高・中・低リスクの判定が適切に行われ、誤検知は発生しなかった。


**図 22　リスクアセスメント結果**

- 不正アクセスなどのインシデント発生時、管理者が AD・ファイルサーバの操作追跡に要する調査時間は、従来手法では 120 分であったが、ALog を利用することで 5 分に短縮された。これにより、約 96%の工数削減が実現している。ログ収集やデータ解読、相関分析、レポート出力など各工程で大幅な効率化が達成されている。

評価

ALog は、重要システムの監査証跡やリスク検知において非常に高い有効性を示している。ログ収集の安定性、操作履歴の網羅性、リスク検知精度、誤検知の抑制、外部製品との連携効率、運用負荷の削減といった全ての観点で、期待水準を十分に満たす結果が得られた。特に、限られた人員と予算環境下でも高精度なリスク検知と運用効率化を両立できる点は大きな特長である。現場担当者からも「非常に有用」との評価が得られて

おり、限られたリソース環境下においても実運用に十分適しているセキュリティ監査・管理基盤であると評価できる。

また、本実証実験を通じて、ログ調査における「スキル依存」と「時間消費」という2大課題が解消されることが確認された。従来、120分を要していた「生ログの翻訳と相関分析」にはWindows Event IDに関する高度な専門知識が不可欠であったが、ALogの導入によりこの工程が自動化され、専門知識を持たない管理者でもわずか5分で正確な事実確認が可能となった。さらに、1件あたり115分の削減は、年間100件の調査・レポート作成が発生すると仮定した場合、年間約192時間の工数削減に相当する。この余剰時間をより高度なセキュリティ監視や教育など戦略的業務へ充てることが可能となり、大学全体のセキュリティ運用レベル向上に寄与する高い投資対効果（ROI）が期待できる。

・ 持続性

本実証の結果、製品への関心は非常に高いものの、現時点では導入計画がなく、背景には現地組織の限られた予算状況がある。単独予算での導入は短期的には難しく、財政面での調整が継続利用の前提となっている。

Mahidol大学は外部委託を行わず、インフラ部門による自律運用体制を維持している。ALogは運用効率性が高く、担当者の工数を大幅に削減できることから、追加人員コストをかけずに長期運用を維持できる可能性が高い。

また、PoC期間中の検証では、学内リソースのみで基本的な運用が可能であることが確認された。しかし、複雑なセキュリティ事象やシステム更新時の対応には、現地技術パートナーによる遠隔支援体制の確立が持続利用のための重要な条件となる。

・ 適合性

ALogは、Mahidol大学の技術インフラ部門において、専門のセキュリティアナリストを配置しなくても高度な監査が可能であり、現地の限られた人材リソースや技術基盤に高く適合している。アンケート調査でも、製品のGUIや使いやすさに関して最高評価が得られており、利用者からの満足度も非常に高い。加えて、システム構成など機密情報の提供に制限がある現地環境においても、外部製品との自動マッピング機能が有効に機能することが確認された。検証シナリオにおいても検知率100%を達成しており、現地環境で十分に機能する製品であると評価できる。

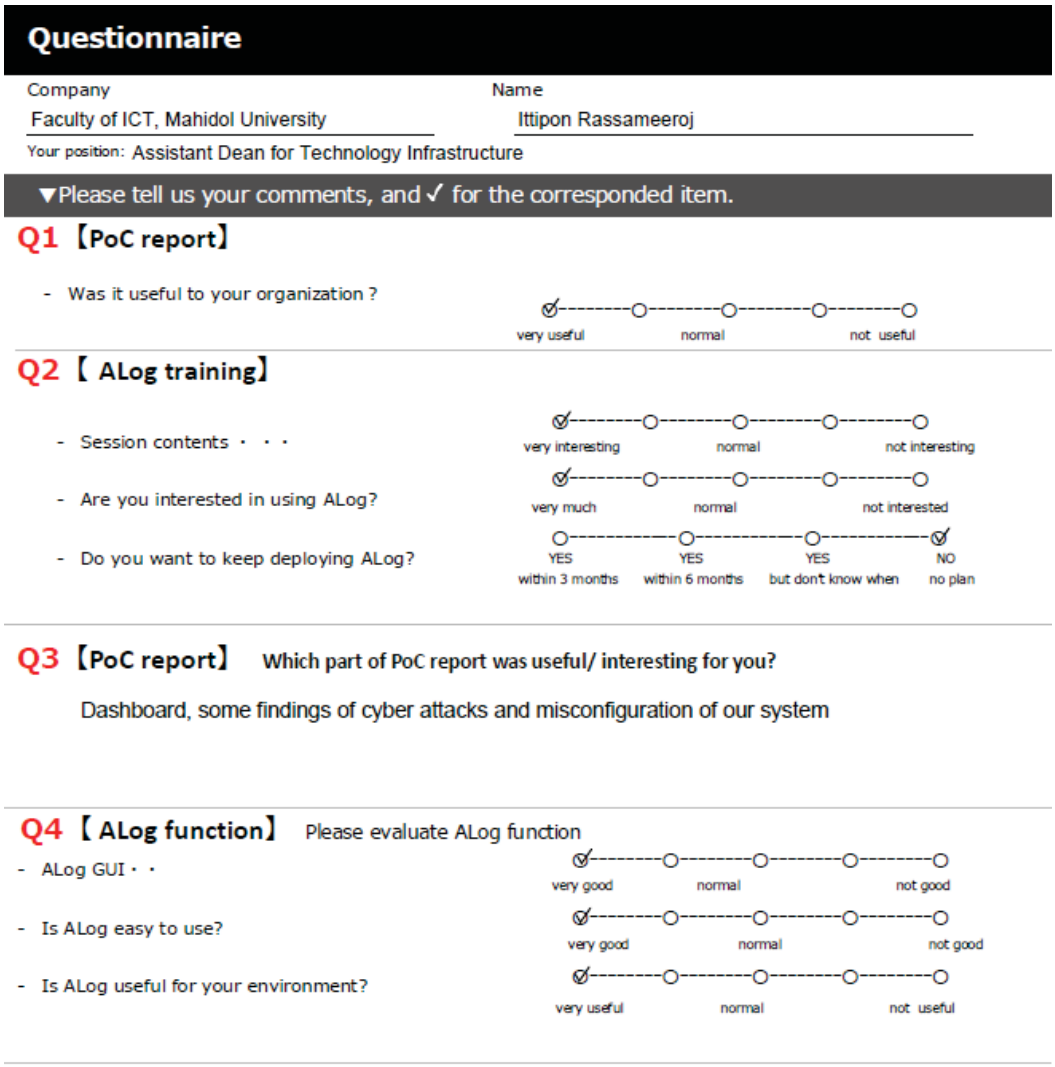



**図 23　Mahidol 大学による評価アンケート結果**

・　ニーズ検証

実証を通じて、ALog は Mahidol 大学の抱える「現状のセキュリティ不足」や「詳細なデータアクセス監査」「境界防御製品との連携」といった潜在的課題に合致していることが明らかとなった。特にダッシュボード機能やサイバー攻撃・システム設定ミスの発見は、現場担当者から最も有益と評価された。現場の技術的ニーズと ALog の機能は整合しているが、ALog の価値をさらに訴求することが導入促進の鍵となる。総じて、ALog は「非常に有用」と評価され、現場の運用担当者にとって実用的なリスク可視化プラットフォームとして機能している。

（８）　対象国・実証先におけるデータ保護・プライバシー対応の評価

・　データ保護（法規制適合）

GDPR[66]は、EU における個人情報とプライバシー保護を強化するための規則であり、前述の

[66] 「General Data Protection Regulation」の略で、「EU 一般データ保護規則」のこと。

通りタイでも PDPA（個人情報保護法）が施行されている。ALog は、GDPR 第 25 条「データ保護バイデザイン及びデータ保護バイデフォルト[67]」に対応可能なソリューションである。具体的には、技術的・組織的措置を講じることで、個人データの最小化や仮名化など、データ主体の権利保護を実現できる。また、ALog はデータ越境の懸念がなく、現地サーバでデータを管理するため、越境リスクや輸出入規制にも該当しない。これらにより、ALog は現地法規制に適合したデータ保護体制の構築が可能である。

- データ保護対策

実証先においては、重要なサーバ群（AD 等）を外部ネットワークから隔離した内部セグメントで運用し、ALog サーバとの通信もネットワーク機器によって厳格に制御しているため、外部からの不正アクセスやデータ流出リスクは極めて低い。アクセス権は許可された担当者のみに限定され、記録媒体によるデータ持ち出しも禁止することで人的漏洩リスクも管理されている。ログ管理については、ALog の改ざん防止機能を本番運用時に有効化することで、ログの真正性を技術的に担保できる。データの保持期間や削除・廃棄は実証先のセキュリティポリシーに従って実施されるため、適切な管理が保証されている。

- プライバシー保護

実証先においては、個人情報は、現地の法律に従って適切に管理されている。NDA（秘密保持契約）を締結し、個人情報の扱いや運用方法も明確にしている。また、個人情報や機微情報の取り扱いを慎重に運用し、利用者への通知や同意取得を徹底している。プライバシーポリシーに基づき、個人情報保護が確実に実施されている。

- プライバシーリスク

Mahidol 大学では、全学部共通の IT インフラ基盤を使用している。各学部のデータやネットワークは論理的に隔離されているため、他学部の職員が無断でアクセスできない。タイの個人情報保護法（PDPA）に沿った統制も行われている。

加えて、ALog 導入に関しては、以下のリスクが検証され、対策が講じられている。

- ✓ 越境データ転送リスク：ログデータは国内のオンプレミス環境で管理され、外部への転送はない。
- ✓ データ機密性リスク：PoC（試験運用）段階では平文保存だが、本番運用では暗号化保存を行い、漏洩や改ざんリスクを排除する。
- ✓ 管理者濫用リスク：管理画面へのアクセスを限定し、管理者の操作履歴も記録・監査する。
- ✓ 業務影響（負荷）リスク：ログ収集によるサーバ負荷は有意に増加せず、業務に支障はない。

（9） 現地インフラとの統合性の評価

[67] 個人データの取り扱いにおいて、最初から（設計段階から）データ保護を組み込むことと、必要最小限のデータのみを処理することを義務付けている。

- インフラ環境

  本実証は、実証先の本番環境で実施した。既存ネットワーク構成を変更せず、ALog を導入・統合した。監視対象は Windows Server（Active Directory やファイルサーバ）およびネットワーク機器である。サーバ層は SMB プロトコルを用いたエージェントレス方式、ネットワーク層は Syslog によるログ転送で対応した。ALog Manager は現地の仮想化基盤上にインストールした。特別なエージェントの導入は不要であり、既存の通信ポート設定と標準権限のみでスムーズに導入できた。

- 統合性

  ALog SIEM と現地インフラの統合は正常に完了した。導入直後から Windows イベントログおよびネットワーク機器のトラフィックログが遅延なく収集された。異なる規格のログは ALog の標準テンプレートで共通形式に正規化され、Web コンソールで一元管理可能となった。重要操作に対するアラート通知も正常に動作し、従来の個別確認作業から ALog による一元的な効率運用への移行が実現できた。

- 統合上の課題

  実証期間中に技術的なトラブルは発生しなかった。構築初期には、ALog サーバと監視対象間の SMB および Syslog 通信の疎通を確認し、必要なポート設定を実施して解決した。運用検証期には、ALog が脆弱性スキャナではなくログ管理製品であることを定義し、CVE 対応はログパターンやアラート設定で実施する方針とした。セキュリティ製品による検知と ALog による挙動調査の役割分担を明確にした運用設計で合意した。

（１０）運用性および技術習得の容易性の評価

- 運用性

  ALog は、外部委託を行わない現地運用体制に適した直感的な操作性を持つ。ログの検索や集計がブラウザベースの GUI で容易に行えるため、利用者から「Very good」との高評価を得た。実証期間中のハンズオン演習では、管理者がアラート通知を受信し、短時間で原因特定や監査証跡の抽出ができることを確認した。ダッシュボードは「誰が・いつ・何をしたか」を自動で表示し、異常の早期発見に寄与している。利用者アンケートでもダッシュボード機能やサイバー攻撃・設定ミスの発見が有益であると評価された。

- 技術習得

  現地担当者は、座学とハンズオンによる研修を受け、ALog の基礎運用を短期間で習得した。実習では、管理画面での操作やアラート、レポート出力などを体験し、参加者は 3 時間程度で異常検知ができるレベルに到達した。研修内容は「非常に興味深い」と評価された。今後の課題として、障害発生時の対応訓練や中長期運用タスクの定着度確認が残るが、基本操作の習得が容易であるため、動画マニュアルや現地業務に合わせた設定テンプレートの拡充で、さらなる技術習得の効率化が期待できる。

- 利用者の評価

  Mahidol 大学の現地ステークホルダーによるアンケートでは、「非常に有用」や「非常に良い」など高い評価を得た。特に、専門的な知識がなくても攻撃の予兆や設定ミスを発

見できる点が評価された。製品機能面には高い満足度があるが、継続利用の課題として「限定的な予算」が挙げられている。今後は、部局特化型でコスト効率の良い導入形態が求められている。

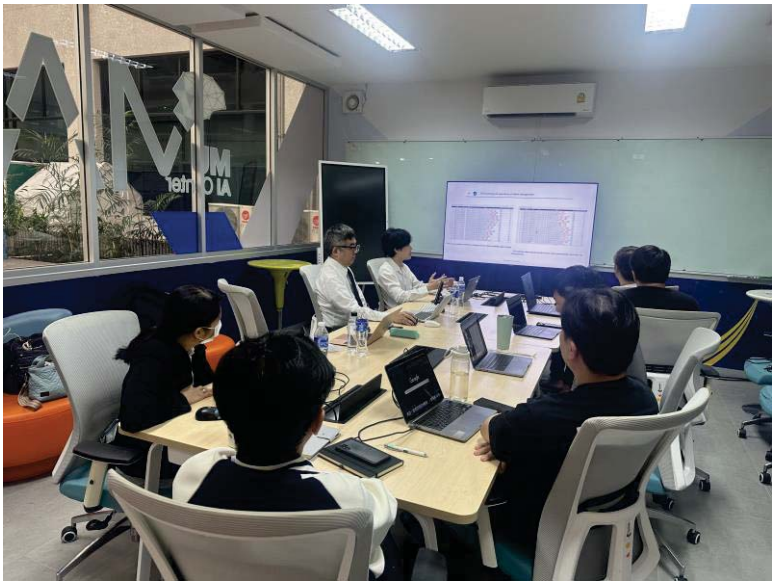


**図 24　Faculty of ICT, Mahidol University の教授への PoC 報告会の様子**

（１１）提言・まとめ

- 改善案・推奨事項

  ALog SIEM は、現状の機能をさらに強化することで、他社 SIEM との差別化と運用効率の向上が可能である。特に、ログ相関機能の自動化・テンプレート化、アラートの視認性向上、標準的なアクションテンプレートの実装、誤検知抑制機能の強化、CVE 対応支援の明確化が必要である。さらに、導入・運用時には「自動判断型 SIEM ではなく、可視化・証跡管理に強い SIEM」であることを明示し、統合レポートや閾値の意味、他セキュリティ製品との役割分担、通信仕様説明を標準化するべきである。これにより、ALog は監査・インシデント対応・証跡管理において、ユーザが正確かつ迅速に判断できる SIEM としての価値を最大化できる。

- 総括

  タイ市場において、ALog SIEM は現地のサイバーセキュリティ課題や法規制、IT 人材・予算面の制約に極めて適合している。専門知識不要で使える設計、圧倒的なコスト優位性、PDPA（個人情報保護法）への高い親和性、現地パートナー・実績の存在により、導入・運用のハードルが低い。特に、IT 人材不足や高価な他社製品の導入が困難な現場に対して、ALog は最適かつ現実的な選択肢である。教育・医療・政府分野での展開も容易であり、市場拡大の基盤が既に整っている。日本国内での豊富な実績を活かし、タイ市場でも同様の成功が見込める。


**図 25　網屋及び Faculty of ICT, Mahidol University 学部長および教授と撮影**

### 4.7.2. 株式会社インターネットイニシアティブ（インドネシア）

（１） 対象国及び実証製品・技術・サービス

- 対象国：インドネシア
- 実証を行う製品・サービス名：
  Safous Privileged Remote Access（特権リモートアクセスサービス）
- 製品・サービスの概要（特徴・機能・通信の流れ等）：

Safous は、重要な社内システムや産業用システムに対する安全なリモート接続と特権アカウント[68]管理を一体的に提供するソフトウェアである。従来の VPN（Virtual Private Network） ではなく、インターネットを使ったゼロトラスト通信[69]に基づき、ユーザやデバイスを都度検証し、最小限の権限で業務システムへアクセスさせることで、セキュリティレベルを向上させることが可能となる。主な特徴および機能は、4.5.2 の通りである。

- 有効性仮説・期待される成果（定量・定性／短期・長期）

インドネシアにおけるサイバーセキュリティの課題として、OT/IT 混在領域へのサイバー攻撃が挙げられる。サイバー攻撃の主要因であるランサムウェアは、「VPN をはじめとしたリモートアクセスの脆弱性を突いて侵入」し、「システム書き換えのできる特権 ID に昇格」してシステムを改ざんする、という手法をとっている。また、現在の OT/IT 混在領域では、「誰が、

[68] システム管理や設定変更など、通常ユーザより強い権限を持つアカウント。乗っ取られると甚大な被害につながる。

[69] 「何も信用しない」前提で、ネットワークやユーザを常に認証・検証し、最小限の権限のみを与えるセキュリティモデル。

いつ、どのシステムに、どのような作業を、どの時間に、誰の認可を得て行ったのか」が可視化されておらず、結果として無法地帯を生み出している。

これらのリスクに対し、Safous を導入することにより、重要インフラを管理する側が、リモートアクセスしてくるユーザに対して事前に、どのシステムに対し、どの様な作業範囲を、どの時間帯に、誰の承認を得てアクセスさせるかを登録できるほか、さらにその登録者に対し MFA（Multi-Factor Authentication：多要素認証）をかけることで、なりすまし、PW/ID の使いまわしによる不正アクセス、許可システム以外へのアクセス、許可範囲を超えた作業、契約外の作業を完全に抑止することが可能となる。

これらの必要性に応じたアクセス管理やログの記録といった機能は、いずれの国においても求められていることであり、ガイドラインや法律はあるものの実効性のある対策ができていないインドネシアの制度面での課題の解決につながるものである。

■定量的成果

【短期】

- なりすましや VPN 機器の脆弱性等のリモートアクセスに起因するサイバー攻撃：ゼロ
- セキュリティを担保しつつ、VPN のような輻輳が生じないこと
- セキュリティ対策実施率（対象システム全体）
- ゼロトラスト経由率（Safous 経由のリモート接続比率）

【長期】

- なりすましや VPN 機器の脆弱性等のリモートアクセスに起因するサイバー攻撃：ゼロ
- 導入拠点数、アカウント数の増減に応じた設定やネットワーク設定の事務工数
- 生産設備におけるダウンタイム の縮減（平均復旧時間の短縮、設備の稼働率の向上）
- 設備現場へのリモートメンテナンス実現による、現場訪問回数と人件費の削減

■定性的成果

【短期】

- 統制の即時可視化：重要システムへのアクセス状況(ログイン/オペレーション/ログオフ)が人単位で見える化。責任所在が明確化。
- 標準ルールの定着：案件・期間・対象に限定した一時アクセスが運用の基本となり、終了と同時に権限失効。
- 監査対応の即応性：だれが・いつ・どこで・何を行ったかの記録を即時提示可能。内部・外部監査の負担が軽減。
- 影響の局所化：万一の侵入時も到達範囲が限定され、サービス停止の連鎖が抑制される。
- 遠隔運用の実感：離島・オフショア・僻地を含め、現場に赴かず状況確認・一次対応が可能で、現場の俊敏性が向上。

【長期】

- “止めない”運用文化の定着：常時開放・共有の慣行を廃し、必要な者に・必要な時点に・必要最小限だけの原則が組織標準として浸透。
- コスト構造の改善：出張・待機・緊急対応の恒常コストが低位安定。人員増を抑えつつ拠点拡大にも対応。
- 監査・法令適合の持続性：国内保管の証跡と一貫した手続により、監査・認証・顧客査察への継続的適合が容易。

- 安全なデジタル化の拡大：安全な接続を前提に設備の追加・更新（Industrial 4.0）を推進でき、つながるほど運用リスクが下がる状態を維持。
- レジリエンス向上：検知・遮断・復旧のサイクルが成熟し、重大障害の発生頻度と影響度が継続的に低下。

（2） 実証事業の内容

・ 実証の目的

本実証では、先進的な導入事例をモデルケースとして構築し、それを契機に他拠点や類似組織への普及を加速させていくことを目指す。

Safous は、新興国を中心としたグローバル市場において、セキュリティ投資への意識や体制が十分でない地域でも導入しやすいよう設計、開発された製品であり、特に、セキュリティの第一歩として最も重要な「アクセス管理」を中核機能としている。

アクセス管理は、ASEAN 諸国で深刻化しているランサムウェア攻撃への有効な防御策であり、今後オンライン化が進む OT 領域において、特に政府機関や重要インフラ事業者は、多拠点に分散して有している重要な制御システムに関し、多様なレベルに対しアクセス権限を付与する必要があるため、Safous の適合性が高いと考えられる。

・ 実証スコープ・重点実証項目

本実証においては、以下 3 点について確認する。

① 有効性・持続性および現地ニーズ

ランサムウェア攻撃の脅威や IT/OT 混在環境での安全なネットワーク接続が相手方にとって重点課題として認識されているか。組織として課題解消のための製品導入のリーダーシップがとられているか。当社製品の市場価格が妥当と認識されているか。

② データ保護、プライバシー対応

Safous 自体が製品として現地法制に適合していることは確認済みだが、導入候補先の規制対応ニーズにどの程度対応できているか（現地法制に基づき重要インフラ事業者として課されているセキュリティ措置への充足性）を確認する。

③ 現地インフラとの親和性および運用・技術習得容易性

Safous 導入のハードルやリードタイムは小さいが、相手方が重要インフラ事業者である場合、政治的・組織文化的背景から、導入にあたって幅広い社内外のステークホルダーの理解醸成が必要となるケースも想定される。また、OT 領域ではセキュリティのみならず IT ツール自体に不慣れな担当者がアサインされるケースもあるため、意思決定や習熟に必要なリードタイムを見極める必要がある。

・ 実証方法（項目・方法・期間・渡航回数など）

実証項目は、以下の通りである。

- 対象国・実証先におけるサイバーセキュリティ上の課題
- 対象国・実証先におけるサイバーセキュリティ製品・サービスのニーズ
- 対象国・実証先におけるサイバーセキュリティ製品・サービスの有効性・持続性・適合性・ニーズ検証
- 対象国・実証先におけるデータ保護・プライバシー対応の評価
- 現地インフラとの統合性の評価

・　運用性および技術習得の容易性の評価

主として実証先のヒアリングにより、上記実証項目についての情報収集、評価を行う。手順は、以下の通りである。

①　関係者や候補先と具体的な実証拠点を決定

②　※本実証では傘下企業の OT 領域への導入を見据えた製品評価のため、現時点では BKI の OT 領域への接続性を持った IT 領域(IT/OT 混在エリア)に導入し、当該拠点のシステムやインフラの現況を調査し、IT/OT 双方のサイバーセキュリティに責任を持つ担当者に対し製品内容や導入方法の説明を実施

③　実際の導入、ユーザ（従業員、ベンダー等）への説明

④　ある程度実証期間が経過した時点から、実証先の経営陣、拠点の主任、セキュリティ担当者、ユーザ等から幅広くヒアリングし、ユーザエクスペリエンスを収集

実証期間については、実際の導入からヒアリング終了までの製品評価の期間を 2 か月程度と想定している。また、上記①、②の段階で 1 回、④の段階で 1 回の計 2 回の渡航を想定している。

・　実証スケジュール（マイルストーン含む）

スケジュールは下表の通り。

2025 年 10 月上旬　実証先との会議・合意、実証先システム調査及び導入計画
2025 年 10 月中旬　先方とのキックオフ実施、インストール機器調達
2025 年 10 月下旬　セキュリティ製品導入作業
2025 年 11 月上旬　実証先チームへの製品及び運用レクチャー
2025 年 12 月上旬　実証効果測定・意見交換
2025 年 12 月下旬　調査報告書（ドラフト版）を提出
2026 年 1 月中旬　調査報告書（最終版）を提出
2026 年 1 月下旬　最終報告会・意見交換会を実施

（3）　リスクと対応策

・　外部要因リスク：

意思決定者の交代等による実証先候補の導入意欲の低下、外国技術の導入規制、類似製品の採用等による導入検討の終了。

・　法規制リスク（データ越境／個人情報保護／輸出入）：データ越境／個人情報保護／輸出入の何れも該当なし

・　その他留意事項：なし

（4）　実証先の概要

・　名称・所在地

企業名：PT Biro Klasifikasi Indonesia（BKI）

所在地：Jl. Yos Sudarso 38-40, Tanjung Priok, Jakarta – 14320

・　実証先の業務内容

本実証先である BKI は、インドネシアにおける船級・検査・認証を担う国営企業であり、海

事産業の安全性確保および国際条約（SOLAS[70]、MARPOL[71]等）に基づく規制の実装を担う中核的な主体である。また、船級・検査・認証業務を通じ、海事産業における安全性・品質の担保を行うだけでなく、国際条約や国内規制に基づく要求事項を現場運用へ落とし込み、監督可能な形で実装する役割を担っている。

同社では、インドネシアにおける海事領域のデジタル化施策の一環として DX ソリューションの導入を推進しており、この一端として、Chikarang 地域に新設されたデータセンター（以下「SMV データセンター」という。）において、海事領域におけるデータ収集、監視システム、デジタルサービスの統合基盤（以下「海事情報プラットフォーム」という。）を構築する取り組みを進めている。同プラットフォームが取り扱う情報には、船舶の運航・機器運用に関するデータ、沿岸インフラの稼働状況、監視映像等の複数種別が含まれる想定であり、将来的に対象範囲が拡大するほど、アクセス管理、操作記録、ログ保全などの統制要件は不可欠となる。

SMV データセンターは新設施設として運用を開始した段階にあり、海事情報プラットフォームの将来的な利用を見据え、ネットワーク構成の標準化、資産情報（用途・所有・接続関係）の整理、運用手順（変更管理・承認・監査対応）等を段階的に整備しているところである。

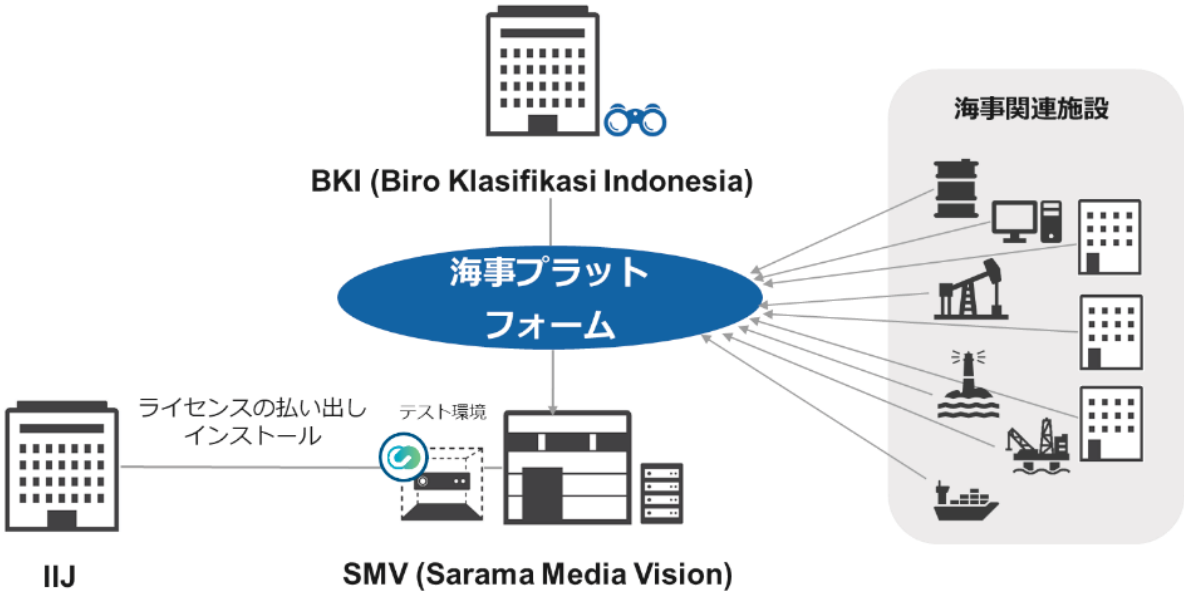



**図 26　実証先関係概要**

・　実証環境

本実証では、当初 BKI のデジタル TIC 運営部門をカウンターパートとし、BKI が新設したデータセンター（SMV）における海事情報プラットフォームの本番運用環境に対し Safous を導入、プラットフォーム運用や海事企業からのデータ収集のセキュリティを確保する想定であった。しかし、SMV の海事情報プラットフォームでは、本番環境への新規製品導入にあたり、技術適

[70] SOLAS 条約（海上人命安全条約 / International Convention for the Safety of Life at Sea）：船舶の構造・設備・運航等に関する国際的な安全基準を定めた条約であり、海上における人命の安全確保を目的として国際海事機関（IMO）により採択されたもの。

[71] MARPOL 73/78 条約（国際海洋汚染防止条約 / International Convention for the Prevention of Pollution from Ships）：船舶からの油、有害液体物質、廃棄物、排気ガス等による海洋汚染の防止を目的として定められた国際条約であり、国際海事機関（IMO）により採択されたもの。

合性の確認に加えて、運用責任者の明確化、アクセス権限設計、ログ保全方針、インシデント時の追跡性（証跡）といった統制観点での検討・承認が前提となり、本番運用環境に対して Safous を導入することができない状況であった。これらの統制要件が整備途上である段階では、段階的な検証環境を設け、接続要件および監査性（操作記録・ログ取得）の成立性を先行確認するアプローチが合理的であるため、今回は SMV データセンターのステージング環境へ Safous を導入し効果測定する形で実証を行った。

（5） 対象国・実証先におけるサイバーセキュリティ上の課題

- 現状の対策状況

調査の結果、SMV データセンターは新規施設としての基盤整備が進行中の段階にあり、海事情報プラットフォームとして求められる統制レベルとの間に、いくつかのギャップが存在することが確認された。これらはいずれも海事情報プラットフォームとして通常期待されるセキュリティレベルを満たしているとはいえず、基礎的な管理策が広範に欠落していることが明らかとなった。

- 現状の運用体制・管理方法：非公開情報
- 主な課題・制約：海事情報プラットフォーム構想の進展に対して、現行のセキュリティ水準が著しく不十分である等の課題が確認された。
- 発生背景

課題の背景は、セキュリティ意識の欠如、適したインフラエンジニアの不在という質的な問題及び量的なリソース不足が挙げられる。サイバーセキュリティに関する規制においてデータ、アプリケーション、ネットワーク、データセンター設備、運用管理体制を対象とした情報セキュリティ管理および技術標準・手続きやセキュリティ監査に関する技術基準が定められ、「実装 → 監査 → 改善」のサイクルを継続的に回すことが求められているものの、エンフォースメントがなされておらず結果としてサイバーセキュリティ製品の導入は進んでいない。さらに、海事情報プラットフォームの構想が先行する一方で、それを支えるネットワーク設計、資産管理、運用手順、監査対応といった基盤整備が移行期にあることも背景要因である。この移行期においては、統制が確立しないまま遠隔接続を許可することが困難であり、結果としてリモートアクセスを禁止せざるを得ない状況が生じている。

（6） 対象国・実証先におけるサイバーセキュリティ製品・サービスのニーズ

- ニーズの種類：
  - ネットワークおよびデータセンター基盤の基本的なセキュリティ対策の確立
  - Maritime Data Center[72]化に向けた統制レベルの引き上げ
  - 古い資産を含むシステム群の可視化および統制

これらのニーズは、今般の実証先のような単一データセンターの運用効率化にとどまらず、将来的に海事情報プラットフォームを国家的に運用する主体として必要不可欠な統制要件に基づくものである。

- 製品・サービスニーズ：非公開情報

[72] 一般用語ではないが、BKI 関係者が好んでこの表現を使うことから、そのままの記載としている。

・　ニーズの根拠

製品・サービスニーズについては、単なる利便性向上ではなく、海事情報プラットフォームを継続運用するうえで不可欠な統制要件（監査性、追跡性、説明責任）に基づく。

（7）　対象国・実証先におけるサイバーセキュリティ製品・サービスの有効性・持続性・適合性・ニーズ検証

・　有効性：ステージング環境における実証の結果、Safous は以下の点で高い有効性を示した。

■定量的効果

・　重要度の高いアプリケーションを定義し、管理者の特権アクセスの権限設定及び管理を可能とした
・　Safous 経由の接続はいずれも安定しており、遅延や接続障害は確認されなかった
・　多要素認証の導入により、なりすましリスクを排除
・　アクセスログ・操作記録（セッション録画）を取得でき、従来ゼロであった可視性が確立された

■定性的効果

【短期】

・　誰が・いつ・どこへアクセスし・何を行ったかを明確化
・　権限の一時付与と自動失効により、不要権限の恒常保持を防止作業証跡の提示が容易となり、監査対応負荷を軽減

【長期】

・　「必要な者に・必要な時に・必要最小限のアクセスを付与する」運用文化への転換
・　オンサイト依存から、遠隔一次対応を含む柔軟なオペレーションへの移行可能性
・　将来の Maritime Data Cener におけるベンダー統制・多拠点展開への適合性

・　持続性

Safous はエージェントレス方式であるため、運用負荷が軽く、担当者が 1 名であっても維持可能である。また ID/アクセス管理が集中化されるため、本番環境の整備が進んだ後も継続的に利用できる構造である。

・　適合性

Safous のアクセス制御、承認ワークフロー、監査証跡管理は、将来の Maritime Data Center の要件と強く一致しており、既存文化（監査重視・証跡重視）とも親和性が高い。

・　ニーズ検証

事前に抽出された課題（アクセス管理、可視化、監査対応等）に対し、Safous は実証範囲においてすべて対応可能であることを確認した。

本実証で確認された運用モデル将来的に海事情報プラットフォーム全体へ展開可能な統制・監査モデルとしても有効であると評価できる。

（8）　対象国・実証先におけるデータ保護・プライバシー対応の評価

・　データ保護（法規制適合）

インドネシアでは、電子政府システム（SPBE）[73]に対する情報セキュリティマネジメント及び技術基準が BSSN により複数の規則として発行されている。特に以下が、本実証先である SMV データセンターに関連する主な規制である。

・Peraturan BSSN No.4 Tahun 2021

「SPBE における情報セキュリティ管理および技術標準・手続き」を定めたもので、データ、アプリケーション、ネットワーク、データセンター設備、運用管理体制が対象範囲に含まれる。

・Peraturan BSSN No.8 Tahun 2024

SPBE のセキュリティ監査に関する技術基準を定めており、「実装 → 監査 → 改善」のサイクルを継続的に回すことが求められる。

Safous は、アクセス管理、承認ワークフロー、操作記録、最小権限の原則等を備えており、上記規制が求める「アクセス制御」「認証管理」「監査証跡」の部分において実装上の適合性が高いことが確認された。

- データ保護対策

  Safous によりデータセンターにおける基本的なデータ保護対策の大部分を補完できることが確認され、有効であることが確認された。

- プライバシー保護

  本実証で利用した Safous は、利用者のメールアドレス、認証ログ、操作記録など最低限の識別情報のみを扱うが、いずれも 導入先（SMV データセンター）のゲートウェイ内に保存され、外部へ送信されない構造である。インドネシア 個人情報保護法（PDP Law）の原則である、目的制限、データ主体保護、アクセス制御にも適合しており、プライバシー保護の観点から、製品自体にリスクとなる構造的懸念は認められなかった。

- プライバシーリスク

  非公開情報

（9） 現地インフラとの統合性の評価

- インフラ環境

  SMV データセンターは、物理環境としては電力や通信の冗長性が確保され十分な可用性を有している。

- 統合性

  ステージング環境において Safous は安定稼働し、RDP[74]、SSH[75]、Web アプリ等の接続を問題なく制御できた。特別なエージェントを必要としない点は、最新ソフトウェアの

[73] 電子政府システム（SPBE：Sistem Pemerintahan Berbasis Elektronik）：行政サービスおよび政府内部業務の効率化・透明性向上を目的として、情報通信技術を活用し政府業務を電子的に実施するためのインドネシア政府の国家的枠組みである。各省庁・政府機関に対し、行政手続、データ管理、公共サービス等のデジタル化および相互連携を推進する指針を定めている。

[74] RDP（Remote Desktop Protocol）：遠隔地から Windows パソコンやサーバを操作するための通信方式である。 本報告書では、Safous を経由して Windows サーバへリモート接続する操作を指して用いている。

[75] SSH（Secure Shell）：暗号化された通信を使って、遠隔からサーバや機器に接続するための通信方式である。 本報告書では、Linux サーバや管理用サーバ等に対する SSH プロトコルによるリモートアクセス操作を意味している。

インストールの難しいレガシー機器[76]が多く存在する可能性のある現地環境との高い適合性を示すものである。

・　統合上の課題

Safous は、シンプルかつ迅速にネットワーク全体の安全性を確保するためのソリューションであり、今回の実証を通じて海事情報プラットフォームの基盤に Safous を導入することについては統合上の課題は確認されなかった。

（１０）運用性および技術習得の容易性の評価

・　運用性

Safous の管理コンソールはブラウザのみで操作可能であり、アクセス権限設定、アプリケーション登録、セッション記録の確認などが統合的に実施できる。既存の未整備環境においても短期間で統制を確立できる点が評価された。

・　技術習得

ステージング環境を用いたレクチャーにより、担当者は ID 設定、アクセス条件の作成、ログ確認などの基本操作を短期間で習得できた。当初想定していたとおり一般的な IT 管理者であれば、約 1 週間で運用を自走可能と判断される。

・　利用者の評価

管理者からは、属人化していたアクセス統制が整理され、作業責任の明確化や操作記録の取得が可能になった点が高く評価された。一方、承認フローや Firewall の導入等のネットワークセキュリティの整備については今後の課題として認識されている。総合評価として、Safous の導入は現地運用体制の強化に明確な効果を示した。

（１１）提言・まとめ

・　改善案・推奨事項

本実証を通じて得られた知見を踏まえ、SMV/BKI に対して以下の改善策を提言する。

①　基盤セキュリティおよびネットワーク統制の段階的整備

海事情報プラットフォームは、将来的に船舶、港湾、沿岸インフラ、オフショア施設など複数の OT 環境と接続されることが想定されているため、包括的なネットワーク統制の確立が必要であるが、これらは一括導入ではなく、現行の運用体制および承認プロセスを踏まえた段階的な整備が望ましい。

②　資産管理および構成情報の可視化

非公開情報

③　アクセス管理・承認フローの標準化

[76] 導入から時間が経過しているものの、現在も業務で使われているシステムや機器を指す。例として、WindowsXP のようなすでにサポートが終了しているが今なお使われているシステムや機器が挙げられる。OT で使われるシステムや機器は止められないこと、安定稼働すること、を第一にすることが多く、IT のような頻繁なシステムのアップグレードはされないことが多い。本報告書では、最新のソフトウェアやエージェントの導入が難しい可能性のある現地環境の機器を想定している。

複数の内部担当者や外部ベンダーが関与する運用形態を前提とした場合、個別 ID に基づくアクセス管理、最小権限の原則、承認フローの明確化が重要となる。Safous を用いたアクセス統制および操作記録の取得は、こうした運用を実装するための有効な手段であり、今後は標準的な運用手順として整理することが望まれる。

④ 監査証跡およびログ管理の確立
海事情報プラットフォームは、将来的に説明責任や監査対応が求められる基盤となることが想定されるため、アクセスログ、操作記録、承認履歴といった監査証跡を一元的に管理し、必要に応じて提示可能な状態を維持する運用を確立することが重要である。

⑤ 海事情報プラットフォーム拡張を見据えた統制モデルの整備
将来的な対象拡大を見据え、個別システムごとに異なる統制を導入するのではなく、共通のアクセス統制・監査モデルを基盤として整備することが、持続的な運用の観点から有効である。

・ 総括

本実証を通じ、Safous は SMV データセンターのように基盤整備が進行中の環境においても、アクセス管理、可視化、監査証跡の確立を短期間で実現できる有効な手段であることが確認された。また、PoC フェーズとしての評価は十分に得られており、技術面および運用面の双方において実装可能性が示された。

今後 BKI では海事企業のセキュリティ対策を進める観点から、各社に対して Safous の導入を働きかける方針である。一方で、海事情報プラットフォームの参加者の経営体力やセキュリティに対する意識は様々であり、プラットフォーム上の特に重要性の高い施設を運用するエネルギー関連の公的機関等に対する Safous の導入について、日本政府や国際機関からの導入支援の可能性について質問を受ける場面もあった。

海事施設は重要インフラとして日本においても攻撃対象として認知されており、2023 年にはランサムウェアによるサイバーインシデントにより港湾機能が停止したことは記憶に新しいところである。これを受け、国土交通省は、港湾・海事分野の事業者に対して継続的な注意喚起を行い、可視性の確保、アクセス統制、操作記録の重要性を強調している。すなわち、OT 環境におけるセキュリティ対策では、境界防御やシステム停止を前提とした対策のみでは不十分であり、「どの資産が存在し、誰が、いつ、どのようにアクセスしたか」を継続的に把握・統制できる仕組みが必要である、ということである。

Safous により確立される ID ベースのアクセス統制および監査証跡の運用モデルは、こうした OT セキュリティの考え方とも整合しており、SMV データセンターに限定されず、海事情報プラットフォームの対象拡大に応じて横展開可能な基盤となり得る。関係者や対象施設が増加した場合であっても、統制と可視性を維持しながら段階的に安全な運用範囲を拡大できる点は、今後の持続的かつ安全な海事情報プラットフォーム運用において重要な示唆を与えるものである。

### 4.7.3. 株式会社マクニカ（フィリピン）

（1） 対象国及び実証製品・技術・サービス

・ 対象国

フィリピン

- 実証を行う製品・サービス名
  Macnica Attack Surface Management (ASM)
- 製品・サービスの概要（特徴・機能・通信の流れ等）
  Macnica ASM（Attack Surface Management：攻撃対象領域管理）は、インターネット上で公開されている情報を利用し、攻撃者の視点から外部公開資産を特定・評価するサービスである。このサービスは「パッシブスキャン型」（対象システムに直接負荷をかけず、公開情報をもとに調査する方式）で実施される。
- 有効性仮説・期待される成果（定量・定性／短期・長期）
  ■定量的評価
  【短期】
  短期的には、Macnica ASM を実証事業とした場合、以下のような定量的成果が得られると想定される。まず、従来認識されていなかった外部公開資産が多数検出されることが期待される。過去の導入事例では、既知資産の 1.5 倍以上の IT 資産が新たに発見されたケースもあり、フィリピン政府機関/重要インフラ企業においても未把握資産が検出されることが想定される。次に、重大な脆弱性（Critical/High）が明らかになり、即時の遮断やパッチ適用などの対応が可能となる。これにより、インシデントを未然に防ぐ可能性が高まる。また、リスクの深刻度に基づき、対処すべき資産や脆弱性が整理され、短期間で「まず何をすべきか」が明確になる。その結果、各機関が迅速に対策ロードマップを策定することが可能となる。さらに、実証終了時点で、検出資産数・脆弱性件数・対応状況などを定量的に報告するため、潜在的な被害の回避が期待できる。
  【長期】
  長期的な観点（Macnica ASM を正式導入後）では、継続的な監視を実施することで、新規資産や構成変更に伴うリスクを即座に検知し、攻撃面の可視化が常時維持される。これにより、脆弱性の放置を防止し、インシデント発生率の逓減が実現される。また、資産台帳や対応履歴が自動的に蓄積されることで、DICT や第三者監査への報告が容易になり、将来的な法制度や報告義務等にも対応可能となる。さらに、手動調査や外部診断の代替として、ASM の年間サービス料で広範囲の監視が可能となり、インシデント対応費用や人的工数の削減が継続的に実現される。最後に、重大インシデントを「起こさなかった」ことによる潜在的な金銭・社会的損失の回避効果も蓄積され、長期的なコストメリットが得られることが期待できる。

  ■定性的評価
  【短期】
  短期的には、「何が見えていなかったか」が明らかになることで、担当者・管理者の不安が解消され、セキュリティへの関心と危機感が組織内に浸透することに寄与する。次に、専門家によるリスク精査により、誤検知やノイズが排除され、担当者は重要事項に集中できるようになる。これにより、初期段階から業務負荷が軽減され、運用効率が向上することが期待される。また、ASM レポートを通じて、IT 部門・経営層・外部ベンダー間の情報共有が活性化され、セキュリティを共通課題として認識する土壌が形成される。さら

に、実証期間中の報告会を通じて、関係者のスキル向上と実践的な知識習得が可能となり、双方向の学習機会が実現される。

【長期】

長期的観点（Macnica ASM を正式導入後）では、継続的な可視化と対応により、セキュリティが日常業務に組み込まれ、属人化から脱却し、「守るべきものを守る」文化が根付くことに寄与出来る。また、ASM ポータルにより、対応状況が組織内外で可視化され、説明責任が果たしやすくなる。DICT 等の政府機関との情報連携を強化することに寄与する。さらに、レポートの共有を通じて、他機関・民間企業との情報交換が活性化され、好事例の展開や遅れている組織への支援など、協調的な防衛体制が構築されることに貢献出来ると考える。

（２） 実証事業の内容

・ 実証の目的

フィリピンの政府機関／重要インフラ事業者を対象に、マクニカが提供する Macnica ASM（External Attack Surface Management：EASM）をトライアル提供し、当該国のサイバーセキュリティ上の課題に対する有効性と持続可能性を実証することを目的とする。現地の実情に即した形で ASM を適切に適用し、対象組織の安全なサイバー空間の実現に資する具体的効果を明らかにする。

ASM は、攻撃者視点で外部攻撃面を継続的に可視化し、リスクを優先度付けして通知する目的のため、人材・体制が限られる官庁・重要インフラにおいても、運用負荷を抑えつつ実効的な外部攻撃面管理を可能にする。当社は、本実証を通じて、フィリピンにおける①有効性・持続性（技術・社会環境適合性と財政的持続性）、②現地ニーズおよび受容性、③データ保護・プライバシー要件への適合、④既存システム／運用との統合性、⑤運用性・技術習得の容易性という五つの検証観点を、実際の調査結果と実証先ヒアリングに基づいて明確化する。これにより、制度・運用要件に整合し、短期実装から長期定着までを見通した導入モデルを検討する。

さらに、実証過程を通じて、未知資産の可視化、高リスク資産の削減、是正プロセスの定着に関するアドバイザリ、現地担当者へのナレッジ移転を重点成果として示す。これらは、フィリピンの重要インフラ保護の底上げに直結するとともに、日本発ソリューションの再現性ある展開モデルとして横展開可能な知見を提供することに貢献する。当社は、本実証の遂行を通じて、JICA が掲げる官民連携の深化と国際競争力の向上に実質的に貢献することを目指す。

・ 実証スコープ・重点実証項目

① 有効性・持続性：対象組織において、外部に公開されている資産の把握状況を明確化し、ASM によるリスク低減効果を定量的に評価する。指標としては、未知資産の新規発見比率や高リスク資産の削減状況などを用いる。

② 現地ニーズ適合性：当社で定義した優先ユースケース（要注意プロダクト）を基に実証を行い、その後、対象組織に対して「追加で優先的に通知したいリスクや要望があるか」をヒアリングし、現地特有のニーズを把握する。

③ データ保護・プライバシー対応：Macnica ASM の利用規約を基準とし、対象国のデータ保護・プライバシー要件に対する適合性を評価します。追加の技術的措置（暗号化や保持期間設定等）は実施せず、規約ベースでの適合性確認に留める。

④ 運用プロセスの適合性：リスク通知から資産特定、管理者特定、是正処置に至る一連のフローが適切に機能するかを机上検証し、その過程で顧客側の要因（例：既存の CTEM(Continuous Threat Exposure Management)製品や既存導入済みサイバーセキュリティ機器・資産管理ツール等）がどのように影響するかを特定する。

⑤ 運用上の課題と改善策：実証を通じて現地での運用課題や注意点を抽出し、対象組織と協議のうえ、あるべき対応策やベストプラクティスを整理する。

・ 実証方法（項目・方法・期間・渡航回数など）

本実証は、「準備 → 計画確定 → キックオフ（現地） → 調査 → 先行通知・是正支援 → 報告書作成・現地報告会 → 取りまとめ → 提出・最終報告」の順で実施する。キックオフおよび実証先への調査報告会は対面で現地訪問し、それ以外はオンラインを基本とする。なお、本事業はポータル等の提供や継続運用サービスは行わず、調査結果を整理した文書レポートの提供を成果とする。

・ 実証スケジュール（マイルストーン含む）

A. 事前準備および実証体制の構築

2025 年 9 月 5 日から 10 月 20 日までの約 1 か月半にわたり、事前準備として業務委託契約の締結や進捗管理を行い、内部キックオフ会議の開催と資料作成、契約・コンプライアンス条件の最終確認と調整、実証協力同意書（MOU）の雛形作成（実証先候補の抽出と社内合意、実証先への打診・調整・確定、調査対象スコープの策定、プロジェクト計画の策定、サイバーセキュリティのディストリビューション事業において活動している、現地子会社である Netpoleon 側の体制調整を実施する。

**B.** 関係各省とのキックオフ・検証目的のすり合わせ

2025 年 10 月 20 日から 24 日までの 5 日間で、関係各省とのキックオフの実施を行う

**C.** 実証事業開始（ASM 調査）

2025 年 10 月 23 日から 12 月 5 日までの約 1 か月にわたり、シード情報整理、OSINT ディスカバリ、アナリスト検証・ノイズ除去、リスク評価、優先度付け、クリティカルリスク通知・是正支援、実証先報告レポート骨子作成を実施する

**D.** 実証先向け調査報告および事務局向けレポート作成

2025 年 12 月 8 日から 12 月 26 日までの約 3 週間にわたり、実証先別報告レポートの作成、コンプライアンス・翻訳レビュー、現地報告会の実施、最終報告書の統合・品質チェックを経て、12 月 26 日に最終ドラフトを提出・登録する

E. 最終報告書提出および報告会

2026 年 1 月 6 日から 1 月 19 日までの約 2 週間で、最終報告書を執筆する。その後、最終報告書を提出・登録し、完了報告を行い、最後に JICA 向けの最終報告会で発表する。

（3） リスクと対応策

・ 外部要因リスク

契約レビューが、越境条項の追加確認によって長引く場合があるため、「個人データを扱わないこと」を前提にしたMOU（覚書）案を提示する。本実証では、OSINT（公開情報を活用した調査）を中心とし、提供するのは文書レポートのみで、個人を特定できる情報は一切扱わない措置を取る。

・ 法規制リスク（データ越境／個人情報保護／輸出入）

個人情報保護リスク：個人情報保護法では、情報の利用目的を限定し、収集を最小限にし、安全に管理することが求められる。これに対応するため、本実証では個人を特定できる情報は収集しない方針とし、報告書には組織や資産レベルの情報のみを記載する。
WHOISなどで個人名が含まれる場合は、削除または匿名化する。追加の技術的な仕組みは導入せず、Macnica ASMの利用規約を基準に適合性を確認する。

・ その他留意事項

特になし

（4） 実証先の概要

・ 名称・所在地

A組織（国家行政機関群）
B組織（フィリピン大手通信事業者）

・ 実証先の業務内容

【A組織】

フィリピン政府の情報通信政策を統括する中枢機関を中心に、保健、エネルギー、運輸、水道といった重要インフラを所管する複数の省庁および関連政府機関で構成されるグループである。国家レベルでのデジタルインフラ整備、サイバーセキュリティ戦略策定、国際連携を担っている。これらの機関は、国民生活に直結するサービスを提供するため、外部攻撃面の管理は国家安全保障上の重要課題である。

【B組織】

B組織は、フィリピン国内で最大規模の通信インフラを提供する民間企業であり、固定通信、モバイル通信、データセンターサービスを含む広範なICTサービスを展開している。従業員数は約8,000名、国内外の利用者に対して高可用性のネットワークを提供している。

・ 実証環境

【A組織】

本実証では、A組織群（総数：5機関）の公開資産 に対するリスク評価を通じて、政府機関におけるASMの適用可能性を検証し、将来的な制度設計や標準化への示唆を得ることを目的とした。

【B組織】

VPN機器やクラウド接続サービスなど、外部公開資産の規模が大きいことから、攻撃対象領域の管理は喫緊の課題と推定された。過去には、国際的なサイバー攻撃キャンペーンの標的となった事例も報告されており、外部攻撃面の 可視化とリスク低減は事業継続性に直結する重要テーマである。本実証では、同社の外部公開資産の網羅的把握と、脆弱性管理プロセスの改善可能性を検証することを目的とした。

（５） 対象国・実証先におけるサイバーセキュリティ上の課題

【A 組織の課題】

第一に、資産管理の不統一が顕著である。中央部門は各政府機関の資産に対する直接的な管理権限を持たず、管理は各機関に委任されている。現状、共通の管理マニュアルや標準化された対応手順は整備されておらず、ドメイン管理は取得時の申請管理に留まっている。さらに、サイバーセキュリティに関するシステム運用基準や違反規定が未策定であるため、中央部門は推奨事項の提示にとどまり、強制力を伴う統制が実現できていない。この構造的な制約は、外部公開資産の可視性を低下させ、攻撃者による未管理資産の悪用リスクを高めている。

第二に、法制度の未整備が課題である。現行体制では、サイバーセキュリティ関連法規制は国家計画に基づく基本方針に留まり、各機関に対して脆弱性管理やインシデント対応を義務付ける法的枠組みが存在しない。このため、対応の実効性は各機関の判断に依存し、中央部門が迅速な是正措置を強いることが困難な状況にある。

第三に、人材不足とスキルの不均衡が深刻である。中央部門には約 79 名が所属しているが、各機関の ICT 担当者のスキルレベルは不明確であり、標準化されたスキル評価制度は存在しない。加えて、現行の人材育成は外部機関によるトレーニングに依存しており、体系的な教育プログラムは未整備である。インシデントレスポンスを担うチームは約 14 名で構成されているが、週次で 10〜15 件のインシデント報告を受ける状況下で、対応人数とスキルの不足が運用負荷を増大させている。

第四に、運用負荷の集中が課題である。脆弱性診断および登録テスト領域、ならびにインシデントレスポンス業務が最も負荷の高い領域として確認されている。特に、脆弱性診断は月次スキャンを基盤とする手作業中心の運用であり、検知結果の確認や対象機関との調整に時間を要している。また、インシデント対応においては、報告を受けた後 15 分以内に一次連絡を行う標準を維持しているものの、対象機関からのレスポンスが遅延するケースが多く、対応完了までの期間は機関によって大きくばらつきがある。最後に、技術的自動化の遅れが指摘される。現行体制では、脆弱性管理に 統合脆弱性統合管理ツールを利用しているが、資産管理や脆弱性対応の自動化は未達であり、外部公開資産の完全な可視化や迅速な対応を阻害している。加えて、古いソフトウェアや未使用機器の残存が散見され、これらの除去プロセスも手作業に依存している。総じて、A 組織は国家レベルのサイバーセキュリティ戦略を担う中核機関として一定の機能を有しているものの、資産管理の統一性、法制度の強制力、人材育成、運用効率化、技術的自動化といった領域において、構造的な課題が残存している。

【B 組織の課題】

第一に、資産インベントリの完全性確保に関する課題である。同社は本社、複数のグループ会社、Internet Service Provider (ISP：インターネットサービス事業者) 事業領域を含む広範な資産を管理しているが、現行の管理モデルは分散型であり、IT 部門、ネットワーク部門、セキュリティチームがそれぞれ異なるツールを利用している。IT 部門・ネットワーク部門はそれぞれ運用する統合資産管理ツール（ITSM/ITAM）セキュリティチームは ログ統合システム（SIEM）を使用して情報を統合しているが、ドメインや IP アドレスの自動所属判別（どの子

会社資産かの判定）は依然として困難である。特に ISP 領域では、IP レンジの判別に手作業によるグルーピングが必要となり、完全な自動化には至っていない。ヒアリングでは、B 組織が「複雑なツリー構造」と表現しており、資産管理の精度向上 が最優先課題であることが確認された。

第二に、運用負荷の高さが顕著である。SOC は 24 時間 365 日の監視体制を維持しており、脆弱性スキャン、アラート対応、レポート作成、エビデンス収集などの業務が集中している。特にゼロデイ脆弱性発覚時には、追加調査や緊急対応が必要となり、人的リソースへの負担が増大する。ヒアリングによれば、週末や深夜帯も監視を止めない 24365 体制を維持しており、シフト勤務による継続対応が求められている。また、レポート作成やエビデンス収集は手作業が多く、運用負荷をさらに高めている。自動化プレイブックの開発や SIEM 連携は進行中であるが、現状では人手依存の業務が残っている。

第三に、規制対応の複雑性が課題として挙げられる。同社は ISO 27001 や PCI DSS(Payment Card Industry Data Security Standard）など国際標準を遵守しているが、マルチテナント環境における PCI DSS 準拠は ASM 導入時 に専用 SaaS 構成を必要とするなど、運用設計に制約を与えている。さらに、グループ会社ごとにインベントリが分散しているため、監査対応やインシデント対応時に迅速な情報集約が難しい点が指摘されている。法令変更によるログ保持期間の延長や新規規制への対応は、今後の運用負荷増加要因となる可能性があるとコメントされた。総じて、B 組織は外部攻撃面管理において高い成熟度を有しているものの、資産管理の完全性、運用負荷軽減、規制対応効率化といった領域において課題が残存している。これらの課題は、分散管理モデルと事業規模の大きさに起因するものであり、今後の改善に向けては、自動化の深化と情報集約プロセスのさらなる強化が必要である。

（６） 対象国・実証先におけるサイバーセキュリティ製品・サービスのニーズ

【フィリピンでの一般的なサイバーセキュリティに関するニーズ】

フィリピンではサイバーセキュリティが重要な課題になりつつあるものの、老朽化したインフラ、限られたリソース、十分に浸透していないサイバーセキュリティ意識等の問題が深刻であり、これらの脆弱性がランサムウェア攻撃やフィッシング、データ漏洩といったサイバー脅威にさらされやすくしている。これらの脅威に対し、強固なサイバーセキュリティ対策の重要性は高まっており、フィリピンのサイバーセキュリティ市場は 2028 年までに 13%成長し、3 億 8710 万ドルに達すると見込まれており、パンデミックでの影響やデジタル決済、フィンテックプラットフォームでの加速も重なり、ソフトウェアの売上は 2028 年までに 12 億 6,000 万ドルに達する指標もある。新規の参入市場としては、情報・ネットワークセキュリティ、IT 監査、コンサルティング、デジタルフォレンジクス、脅威インテリジェンス、ソフトウェア開発がニーズとしてあげられる。[77]

【A 組織の現地ニーズ】

A 組織の現地ニーズは、Macnica ASM 導入検討に関連する外部攻撃面の可視化強化、脆弱性管理の高度化、運用効率化、ならびに意思決定支援のためのレポート品質向上に集中している。 第一に、中央部門が資産管理権限を持たず、各機関に管理が委任されているため、外

[77] International Trade Association Philippines - Digital Economy

部公開資産の全体把握が難しく、ASM 導入による資産の網羅的な検知・分類と可視性の強化が最優先課題となっている。

第二に、現行の脆弱性診断は統合脆弱性統合管理ツールによる月次スキャンに依存しており、検知精度や対応速度に制約がある。ASM には不足機能の補完やゼロデイ脆弱性への即時通知、影響範囲の明確化が求められている。

第三に、現行体制では、脆弱性診断や様々なインシデント対応において手作業が多く、週次で各機関からエスカレーションされた 10〜15 件のインシデント対応を行う状況下で、人的リソースへの負担が大きい。Macnica ASM 導入により、検知結果の自動化やアラート精度向上で運用効率化とインシデント予防が期待されている。

第四に、意思決定支援のためのレポート品質向上が強く求められている。各機関を説得し、是正措置を実施させるためには、技術的根拠に加え、意思決定層が理解しやすい情報を含むレポートが必要である。特に、重大リスクの理由を明確に説明し、視覚的要素を強化したレポート構成が期待されており、ASM 情報を既存報告プロセスに統合することで、意思決定者が迅速かつ適切な判断を下せる環境を整備することが可能となる。

また、A 組織における一般的な重要ニーズとして、ハクティビストによる Web サイト改ざんへの対策が挙げられる。A 組織は国民や関係機関に対する情報発信の正確性・信頼性を担保する責務を負っており、Web 改ざんの発生は国家機関としての権威性および社会的信用に直接的な悪影響を及ぼす重大なリスクである。関係者からは「Web 改ざん検知は組織の権威性確保に直結する重要要素であり、徹底した対策が必要である」とのコメントが確認された。これらの背景として、慢性的なサイバーセキュリティ人材不足がある。A 組織ではインシデント対応体制を 30 名規模に拡大することを検討しているが、必要なスキルを持つ人材不足しており、採用と育成に課題があると確認がとれた。なお、この課題は、フィリピン市場全体に共通する構造的なニーズでもある。

【B 組織の現地ニーズ】

B 組織におけるニーズは、Macnica ASM 導入検討に関連する機能要件、運用改善、 UI・通知機能、レポート品質、統合性、ならびに規制対応に関する内容を中心にヒアリングを行った。最初に挙げられたニーズとしては、 Macnica ASM の SIEM や SOAR（Security Orchestration, Automation and Response）[78]との API 連携、コード管理対応、アセット単位での自動テスト機能の選択利用が求められている。また、AWS マーケットプレイスでのライセンス購入やテナント管理、迅速な脆弱性通知・アラート機能も重要な機能として確認できた。

第二に、現行ツールに対する不満点から導かれる改善ニーズとして、資産管理・分類の自動化が強く求められている。具体的には、サブドメインや IP アドレスのグルーピング・分類が手作業で煩雑であること、ISP 領域の IP 判別が難しいこと、誤検知（フォルスポジティブ）の除外作業が負担となっていることが指摘された。さらに、脆弱性検知の遅延や通知内容の不足（影響資産数や詳細情報がメールのみで提供される点）も改善対象である。

第三に、ASM 導入後に期待される運用改善として、資産追加時の即時検知・通知、サーバレスやクラウド資産の可視化、ゼロデイ脆弱性対応の迅速化、アラートの信頼性・精度向上

[78] Security Orchestration, Automation and Response: サイバーセキュリティの運用を自動化し、セキュリティチームが迅速に脅威に対応できるようにするプラットフォーム。

が挙げられる。SOC チームの運用負荷軽減を目的とした検知結果の自動化・統合管理、コード管理ツールによる再利用性確保も重要なニーズである。

第四に、UI および通知機能に関する要望として、資産の状態やリスクを一目で把握できるダッシュボード、アラートの即時通知、資産追加やリスク検出時の自動アラート、グループ分けやフィルタリング機能など、直感的で分かりやすい操作性が求められている。また、アラートの詳細情報（影響アセット数、推奨対応策等）の明示も必要とされている。ただし、B 組織においては、自社でダッシュボードを開発し統合しているため、Macnica ASM 自体の UI に関しては強い要望ではない。

第五に、IT 部門や事業部門に分かりやすい根拠付きレポートや既存ツールで検知できない資産の報告、脆弱性・リスクの優先度付きリスト、自動レポート出力が求められた。特に FQDN・IP・オープンポートの一覧化や重大リスクの証拠、PoC の記載が重視されおり、また規制対応では PCI DSS 維持のため独立運用やベンダーリスクアセスメントが必要であった。全体として、外部攻撃面の可視化強化、自動化・統合による運用負荷軽減、UI やレポート品質向上、規制対応が中心的なニーズである。

（7） 対象国・実証先におけるサイバーセキュリティ製品・サービスの有効性・持続性・適合性・ニーズ検証

- 有効性

  POC 実証では、外部攻撃面の可視化に有効性が認められた。

  A 組織は Macnica ASM のレポートにより、従来把握できていなかった資産や VPN・FW 機器のリスクを認識でき、React2Shell 脅威の早期警告も得ることができた。

  また B 組織では、既存の高度な SOC 体制により外部攻撃面の管理は成熟していたが、Macnica ASM のレポートはその精度を検証し、未把握資産がほぼ存在しないことを確認する材料となった。さらに、React2Shell[79] 脅威に関する情報は、ゼロデイ対応の重要性を再認識させる効果を持ち、ASM が提供する脅威インテリジェンスの価値を示した。他方、今回の評価はレポート提出に限定されており、ASM のリアルタイム検知能力やポータル機能の実効性は検証できていない。

[79] React2Shell: Web サイト上で本来は想定していない JavaScript の実行経路を悪用し、最終的に OS コマンド実行（Shell 実行）へ到達してしまう脆弱性の総称的な呼び方。

### 表 6　A 組織における脆弱性評価のリスク検出結果

※表 A-3：リスク検出結果（A 組織）

| リスクレベル | リスクアラート数 *()内はホスト数 | 備考 |
|---|---|---|
| Critical | 14 アラート（3 IPs） | 極めてリスクの高い脆弱性。これらは攻撃者に頻繁に悪用されるもので、ネットワークへの侵入を許す恐れがある。即時の対応が必要。 |
| High | 13 アラート（7 IPs） | RDP (3389/tcp) や SMB (445/tcp) など、攻撃者の標的になりやすいポートの外部露出。 |
| Medium | 116 アラート（83 IPs） | FTP、SSH、SNMP、LDAP、SQL などのポートの露出。直ちに致命的とは限らないが、一般的にインターネットへ公開すべきではない。 |
| | 96 アラート（78 IPs） | 数年間アップデートされていない、あるいはサポートが終了したソフトウェア（Apache、PHP、MySQL など）が稼働しているサーバ。 |
| 要注意プロダクト（攻撃者の標的になりやすい製品） | 25 IPs | 外部に公開されている VPN 機器や Exchange Server。これらは一般的な攻撃対象であるため、常に最新バージョンに更新されていることを確認する必要がある。 |

### 表 7　A 組織に付随する 4 機関における各リスク分布

| 項目＼対象 | 中央部門 | 機関 1 | 機関 2 | 機関 3 | 機関 4 |
|---|---|---|---|---|---|
| Critical | 4(1) | 10(2) | 0 | 0 | 0 |
| High | 1(1) | 5(2) | 1(1) | 6(1) | 0 |
| Medium | 39(29) | 57(46) | 43(30) | 73(45) | 0 |
| 合計 | 44 | 72 | 44 | 79 | 0 |

### 表 8　B 組織における脆弱性評価のリスク検出結果

※表 B-1：資産発見結果（B 組織）

| 項目 | 調査結果 | 備考 |
|---|---|---|
| ドメイン数 | 54 ドメイン | xxx.ph などのドメインの総数 |
| FQDN 数 | 1907 件 | 上記のドメインに関連付けられた FQDN（完全修飾ドメイン名）のうち、名前解決（IP アドレスの特定）が可能だったものの件数 |
| IP アドレス数 | 1026 件 | 調査の過程で、サブドメインや FQDN を IP アドレスに紐付けた件数 |
| Netblock 数 | 3601 件 ※ | 対象組織が所有している可能性が高いと判断された IP アドレスレンジの件数 |

**表 9　B 組織に付随する子会社における各リスク分布**

| 項目＼対象 | 本社 | 子会社 1 | 子会社 2 |
|---|---|---|---|
| Critical | 0 | 0 | 0 |
| High | 9(2) | 0 | 0 |
| Medium | 45(27) | 5(4) | 0 |
| 合計 | 54 | 5 | 0 |

・　持続性

持続性については、両組織とも ASM の情報提供を既存の報告プロセスに組み込むことは可能と評価した。

A 組織では、月次レポートへの統合が容易であり、Macnica ASM の提供情報は現行体制を補完する形で活用できると考えられる。一方で、人的リソースやスキル不足が課題であり、ASM 運用に関する教育プログラムの整備が必要である。コスト面では、A 組織は 39 百万ペソ（約 1 億 350 万円）の予算を既存脆弱性統合管理ツールに確保しており、Macnica ASM 導入は財政的に許容範囲内であるが、入札形式や随意契約条件（2 百万ペソ以 下）など調達プロセスの制約を考慮する必要がある。

B 組織では、Macnica ASM は既存の SOC 体制に統合可能であり、Splunk や SOAR との API 連携を通じて自動化を強化できる見込みであるが、Macnica ASM の API 連携機能は現在限定的であるため、追加の機能開発が必要である。コスト面では、ASM 導入は既存予算枠内で対応可能とされ、財政的な障壁は軽微である。

また、今回の評価で明らかになった不足要素は以下の通りである。

・　ASM のリアルタイム検知能力や自動化機能の実証が未実施であること
・　資産分類や誤検知除外の完全自動化が未達であること
・　レポート品質が意思決定層向けに最適化されていないこと

戦略と技術の両面で施策検討が必要である。戦略面では、セキュリティ知識が不足している実務者向けの作業ガイドラインの策定・発信、運用人材育成のための製品トレーニングプログラム整備、レポートのビジュアル化やエグゼクティブ向け情報強化が重要であり、技術面では、資産分類や誤検知除外の自動化機能強化、SIEM や SOAR との API 連携機能開発が求められる。総合評価では、Macnica ASM は外部攻撃面の可視化や脅威情報提供に有効性があり、ゼロデイ脆弱性に関する情報提供の迅速性も競争力を示している。ただし、リアルタイム検知や運用統合の実証が未実施な点が、今後の課題である。持続性については、両組織とも財政・規制面の障壁が低く、長期運用が可能であり、標準化や連携機能開発、トレーニングプログラム整備を進めることで、ASM の海外市場での適応性と競争優位性が期待される。

・　適合性

今回の実証結果としてはレポート提出のみであるが、その内容は現地ニーズに対して一定の適合性を示した。具体的には、要注意プロダクト（VPN 機器、Firewall、 Exchange Server 等）に関するリスク情報を網羅し、React2Shell 脅威に関する早期通知を提供した点は高く評価された。また、資産検出結果は、A 組織において未把握資産の存在を明確化し、B 組織において既存管理精度を検証する材料となった。一方で、レポートの課題として以下が指摘された。

- 即時性の不足：通知はレポート提出時点に限定され、リアルタイム性が担保されていない
- 運用統合性の不明確さ：API 連携やコード管理ツール対応など、現行体制への統合方法が具体化されていない
- レポートの説得力不足：意思決定層向けのビジュアル要素や、リスク優先度の明示が不十分

これらのニーズへの適合を実現するために、改善点として、戦略レベルでは、運用標準化ガイドラインの策定、現地法規制対応を考慮したレポートテンプレートの提供が考えられる。技術的施策としては、資産分類・誤検知除外の内部自動化、SIEM や SOAR との API 連携 機能の開発と強化が考えられる。レポート品質向上を実施し、よりわかりやすいビジュアル化・リスク優先度の明示・エグゼクティブ向け要約の追加等を検討する必要がある。

- ニーズ検証

ニーズ検証については、ヒアリング結果から両組織に共通する現地ニーズは以下の通りである。

- 外部公開資産の完全な可視化と、未把握資産の早期検知
- ゼロデイ脅威（例：Reac2Shell）に対する迅速な通知と影響範囲の明確化
- 法規制対応（国家サイバーセキュリティ計画、PCI DSS 等）を担保するためのレポート品質
- 運用負荷軽減を目的とした自動化機能（資産分類、誤検知除外）
- 意思決定層向けの説得力あるレポート（ビジュアル化、リスク対応優先度の明示）

A 組織では、法制度の未整備と人材不足が顕著であり、ASM に対しては「外部攻撃面の可視化」「脅威通知の即時性」「標準化ガイドラインの提供」が強く求められた。

B 組織では、既存 SOC 体制の成熟度を前提に、Macnica ASM には「自動化の強化」「SIEMk や SOAR との API 連携」「レポート作成負荷の軽減」が期待されている。

総合評価として、Macnica ASM は、現地ニーズに対して「脅威情報提供」「資産検出精度」 「リスク通知」において一定の適合性を示したが、リアルタイム性、自動化連携機能、レポート品質の面で不足がある。これらの改善を実施することで、ASM は現地特有の脅威環境や制度要件により高い適応性を持ち、海外展開において競争優位性を確立できると考えられる。

（8） 対象国・実証先におけるデータ保護・プライバシー対応の評価

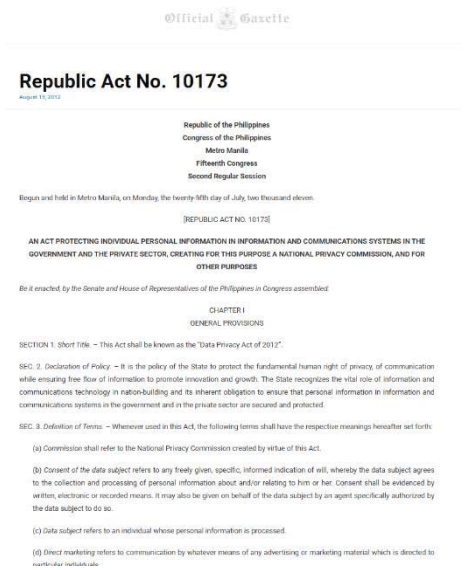
Macnica ASM は外部攻撃面管理のため公開情報を収集・分析するソリューションで、今回の実証はレポート提出のみである。


**図 27　マクニカの OSINT を活用したリバース Whois 調査図**

フィリピンの国家サイバーセキュリティ計画およびデータプライバシー法では、ASM が収集する情報は公開資産に限定されているため、個人情報のリスクは低く、法的懸念はないと評価された。利用規約も公開情報のみを対象としており、現地法への整合性は担保されている。他方、A 組織はデータ保持期間を 1 年程度と希望しており、導入後に保持期間を柔軟に設定する必要がある。また両組織において、将来、内部資産や認証情報を扱う場合には、暗号化やアクセス制御の強化が求められる可能性がある。総合的に、Macnica ASM 対象国のデータ保護・プライバシー要件に概ね適合しているが、保持期間設定や暗号化機能の不足は今後のリスクとなるため改善が必要であり、以下の改善が必要な可能性がある。

- データ保持期間設定機能の追加：現地要件に合わせ、1 年程度の保持期間を選択可能とする
- 暗号化オプションの提供：将来的な内部資産対応を見据え、データ暗号化機能を強化
- 監査ログの強化：法令遵守を証明するため、アクセス履歴やデータ処理記録の保持を義務化

なお、A 組織における情報セキュリティ及びコンプライアンス対応状況に関しては、国家サイバーセキュリティ計画（NCSP 2023–2028）ならびにデータプライバシー法を遵守しており、検討要件ごとに適合状況を確認している。



Official Gazette

Republic Act No. 10173

August 15, 2012

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

*Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:*

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SEC. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *Consent of the data subject* refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to

**図 28　フィリピン　データプライバシー法（The Data Privacy Act of 2012 (Republic Act No. 10173)）**

また、B 組織における情報セキュリティおよびコンプライアンス対応状況は、国際規格や業界標準の遵守を基盤として整備されていることが確認された。ヒアリング結果では、B 組織は ISO 27001 および ISMS（情報セキュリティマネジメントシステム）に準拠した管理体制を構築し、SWIFT に基づく自社規定による定期監査を実施している。決済関連では PCI DSS への適合が求められ、一部子会社は特定ブランドやチャネルで対応している。B 組織はセキュリティ製品導入時に秘密保持契約やベンダーリスクアセスメント、SOC2 などの第三者認証取得をベンダーに要求し、システム統合要件も確認しており、導入判断は法務・コンプライアンス部門も含めて総合的に行われる。日本ベンダーがフィリピン市場へ進出する際は、現地の要件や認証取得が採用の重要な基準となる。

（9） 現地インフラとの統合性の評価

実証を通じて、Macnica ASM はリスク通知から資産特定、管理者特定、是正処置までの基本的な機能要件を満たすことが確認されたが、海外市場での運用プロセス統合や性・拡張性には改善余地が大きい。資産識別機能は高く、既存の CTEM（Continuous Threat Exposure Management： 継続的脅威エクスポージャ管理）関連製品やセキュリティ機器との連携においても一定の互換性を確保している一方で、外部資産管理ツールとの API やデータ形式の違いが一元化の障壁となり、IT 資産管理ツールなど海外で一般的な IT 資産管理基盤との連携設計が不十分である。また、権限管理やグローバル企業で一般的な RBAC（Role-Based Access Control）や IAM（Identity and Access Management）との連携要件が未定義であり、グローバル展開時のリスク要因である。是正処置の、脆弱性検知から対応策提示までのプロセスを自動化し提示する機能はあるが、既存のインシデント対応ワークフローとの統合は限定的である。不足点として、以下の課題が認められる。

- グローバル標準の API およびデータフォーマットへの対応が不十分
- 責任者情報の管理モデルが国内仕様に依存しており、海外の権限管理体系との互換性が低い
- 是正処置のワークフローが Macnica ASM 内で閉じており、外部 SIEM や ITSM との連携設計が未成熟

課題改善の方向性として、国際標準に準拠した API 設計やデータモデルの再構築、主要 ITSM・SOAR 製品や RBAC・IAM との連携、モジュール化設計が必要であり、また脆弱性検知・評価ロジックの差別化による、競合リスク低減も重要である。総合的に、Macnica ASM の運用適合性はあるものの、グローバル展開には統合性、標準化、拡張性の強化と国際標準への迅速な対応が不可欠である。

## （１０）　運用性および技術習得の容易性の評価

Macnica ASM を運用統合した際の主な課題として、第一に現場担当者が是正策の理由や方法を十分に理解できず対応が遅れることがある。A 組織では、各省庁の ICT 担当者がセキュリティに関する知見を欠いており、メール通知のみでは対応が進まないとの指摘があった。これの是正策として、技術的指示に加え、リスクの背景、影響範囲、優先度、推奨対応手順を明示する実行可能なガイドラインを標準化することが求められる。さらに、意思決定者向けに経営インパクトを簡潔に示す要素を追加し、現場担当者が即時対応できる情報設計を行うことが不可欠である。

第二には、是正策の妥当性確認に必要な情報提供の不足し、追加調査や手動作業が発生することである。Macnica ASM は脆弱性検知と対応策提示を行うが、既存システムにおいては、提示された是正策が妥当であるかを確認するためのデータが十分に提供されていない。特に、API を通じてリスク根拠となる詳細情報を取得できない場合、現場担当者や承認者は追加の検証作業を手動で行う必要があり、対応の迅速性と正確性が損なわれるリスクがある。A 組織では、是正策の妥当性を確認するために複数の会議や追加調査が必要となり、対応までに時間を要する状況が指摘された。B 組織においても、SOC 担当者が Macnica ASM の提示情報だけでは十分な判断ができず、Splunk や他のツールから補足情報を収集する必要があることが確認されている。これらの課題に対して、ASM の API 機能を強化し、是正策の妥当性確認に必要なデータを包括的に提供することが求められる。具体的には、脆弱性の検知根拠、影響資産の詳細、推奨対応策の技術的背景を API 経由で取得可能とし、既存の承認フローや検証プロセスに統合することで、対応の迅速化と精度向上を実現する必要がある。

以上の課題を踏まえ、持続的な運用モデル確立の改善策として、情報設計の高度化と API 連携によるデータ提供の強化が不可欠である。情報設計の高度化により、現場担当者が即時対応可能な形式で是正策を提示し、経営層に対してはリスクの重要性を明確に伝えることができる。また、API 連携の強化により、妥当性確認に必要な情報を自動的に取得し、既存の承認プロセスに統合することで、対応の迅速性と正確性を確保することが可能となる。

## （１１）　提言・まとめ

本セクションでは、官民連携をさらに深化させ、日系の国産サイバーセキュリティ関連ベンダーの国際競争力を高めるための基盤整備について、政府において積極的に検討いただきたい

施策を提示する。これらの提言は、海外展開における構造的障壁を解消し、国産ベンダーがグローバル市場で持続的な競争力を確保するための制度・財政・技術面の支援を包括的に示すものである。まず、グローバル標準適合のための制度設計として、NIST SSDF や ISO/IEC 15408 (CC) 等の国際標準に適合した製品開発を促進するため、「国際標準適合ガイドライン」を策定が重要である。このガイドラインは、認証取得プロセスの簡素化、設計段階での要件組み込み、監査対応の効率化を目的とし、国産ベンダーの国際競争力強化に直結する。

次に、ASEAN・インド太平洋地域における法令対応を支援すべく各国の規制をまとめた「規制対応ハンドブック」提供と専門家による相談窓口やアドバイザリーサービスの設置が望ましい。このハンドブックは、データ越境規制、プライバシー保護要件、暗号化義務、監査基準を網羅し、製品設計・運用モデルに反映可能な形式で提示することが望ましい。

さらに開発スピード向上や海外展開時の初期投資負担軽減のため、補助金や税制優遇措置を導入し、現地営業・認証取得費用等への支援策を設計することが望ましい。

最後にサイバー分野に特化した市場情報発信や、進出企業間の人的ネットワーク構築やベストプラクティス共有・ビジネスマッチングを促進する仕組みを設計することも必要である。

# 第 5 章　産業システム（OT）向けサイバーセキュリティ対策状況

## 5.1. 全体の概要

本調査は産業システム（特に産業プラントや社会インフラなどの設備やシステムの制御や運用を行うオペレーショナルテクノロジー(OT)）にかかるニーズ把握である。本邦組織と連携したニーズ調査ワークショップの一部ないし全てにおいて、専門性を持つ本邦企業等への再委託契約を通じて実施した。

**・　OT ワークショップ実施の背景・目的**

世界的なデジタル化の進展に伴いサイバーセキュリティのリスクは増大し、特に対策体制や専門人材が不足する開発途上国において、その対応は深刻な課題となっている。この状況に対し、日本政府は 2021 年に「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」を策定し、国際協力を通じた能力構築支援を推進している。かかる政府方針に基づき、JICA は技術協力を通じて開発途上国の能力強化に努めてきたが、従来の取り組みは産業界や学術界との連携が限定的であるという課題を抱えている。加えて、ASEAN 諸国の多くが重要情報インフラの特定を完了した現在、産業システム（OT）のセキュリティ対策は喫緊の課題である。これらの背景を踏まえ、本ワークショップは、ASEAN 諸国における OT サイバーセキュリティ対策の検討状況及び具体的な需要を把握し、独立行政法人情報処理推進機構（IPA）等、日本の有する先進的な知見の展開可能性を検討するための基礎情報とすることを目的とした。

**・　ヒアリング実施**

本調査は、デスクトップ調査、オンラインヒアリング、現地インタビューを組み合わせて実施した。まず、デスクトップ調査により、産業サイバーセキュリティ分野の国内有識者及び対象国の関連組織を特定した。次いで、これらの候補者に対してヒアリングを行い、本調査への協力意向を確認した。その結果、ワークショップ実施にあたり協力機関となった現地組織に対しては、さらに現地インタビューを実施し、各国の現状及び課題に関する詳細な情報収集を行った。

**・　再委託先選定**

本調査は高度な専門性を要するため、再委託先の選定を実施した。候補者への事前インタビューにおいて、国内有識者である名古屋工業大学の佐々木弘志氏より参画の意向が示された。IPA 産業サイバーセキュリティセンター（ICSCoE）との連携も踏まえ、ICSCoE 修了生を擁する同大学ものづくり DX 研究所メンバーによる参画が決定したため、契約形態は特命随意契約とした。

同大学は、OT セキュリティ分野において国内随一の専門性と実績を有しており、佐々木氏をはじめとする産業界、学術界の専門家人材が多数在籍する。さらに、フィリピンや ASEAN 諸国など国外の重要インフラ事業者や政府機関との国際的なネットワーク有しており、国際会議やワークショップでの実績も豊富である。

本業務の遂行に不可欠なこれらの要件を総合的に勘案した結果、現状、業務を的確かつ迅速に遂行可能な組織は同大学のみであると判断した。

**・　OT ワークショップ実施対象国の決定**

OT ワークショップの実施対象国はタイ、フィリピン、インドネシアの 3 か国とした。その理由は、

「4.2 本邦企業製品の実証にかかる対象国の選定」に示した通り、既存の JICA 協力実績および現地政府との連携基盤を有することから、実証事業とワークショップを同時に展開することで現地ニーズの把握や技術導入効果の検証、現場課題の共有など効率的な実施が可能となるためである。

・ **ワークショップ実施対象国との調整**

対象国の関連組織に対してヒアリングを実施し、協力意向を確認した結果、以下の 3 組織を各国のカウンターパートとしてワークショップを実施した。

- タイ：国家サイバーセキュリティ庁 (National Cyber Security Agency: NCSA)
- フィリピン：情報通信技術省 (Department of Information and Communications Technology: DICT)
- インドネシア： インドネシア大学内に設置された、サイバーセキュリティ専門の研究・教育機関 (Indonesia Cyber Awareness and Resilience Center of Universitas Indonesia: idCARE.UI)

・ **OT ワークショップの実施**

現地ワークショップは、現地関連組織と連携し、再委託先の名古屋工業大学の佐々木弘志氏率いる同大学ものづくり DX 研究所チームにより実施された。ワークショップの基本構成は、①自己紹介（Lightning Talk）、②OT セキュリティ基礎講義、③グループワーク＆発表、④クロージング（時間配分は国ごとに調整）（表 13）とした。ワークショップを通じて、「重要インフラにおけるサイバーセキュリティ政策にかかる検討状況」「重要インフラ企業におけるサイバーセキュリティ対策状況」「政府機関および重要インフラにおける OT 研修の需用」「OT セキュリティにおける他援助機関の協力状況」について調査を行った。

**表 10 ワークショップの構成例（インドネシア）**

| Time (PM) | Program | In charge | Contents |
|---|---|---|---|
| 1:00~1:10 | Opening Remarks | idCARE.UI<br>idNSA | Opening remarks by Dr. Muhammad Salman (idCARE.UI),Dr. Rudi Lumanto (idNSA). |
| 1:10~2:30 | Lightning Talk from Participants | NITech | Self-Introduction and sharing OT Security challenges for the participants along the topic template shared in advance. |
| 2:30~2:40 | Break① | - | |
| 2:40~3:00 | OT Security Basics Lecture (First Half) | Mr.Fujihara from NITech | OT security basics lecture (about Why) by Nagoya Institute of Technology (NITech) |
| 3:00~3:30 | Break② | | For prayer time and break |
| 3:30~4:10 | OT Security Basics Lecture (Second Half) | Mr.Hasegawa<br>Mr.Nakayama<br>From NITech | OT security basics lecture (about How) and workshop guidance by Nagoya Institute of Technology (NITech) |
| 4:10~4:55 | OT Risk Workshop<br>Work-1 Risk Analysis | Mr.Nakayama from NITech | Group Work 35 min<br>Group Presentation (2 groups) 10 min<br>* Mr. Hasegawa and Mr. Fujihara will be held on the support |
| 4:55~5:05 | Break③ | - | |
| 5:05~5:50 | OT Risk Workshop<br>Work-2 Risk Response | Mr.Nakayama from NITech | Group Work 35 min<br>Group Presentation (2 groups) 10 min<br>* Mr. Hasegawa and Mr. Fujihara will be held on the support |
| 5:50~6:00 | Certificate Award Ceremony | idCARE.UI<br>idNSA | |
| 6:00~6:05 | Photo Session | All | |
| 6:05~6:20 | Closing Remarks | idCARE.UI<br>idNSA | Closing remarks by NITech, Dr. Rudi Lumanto (idNSA),Dr. Muhammad Salman (idCARE.UI) |

・ **報告書へのとりまとめ**

本報告書は、再委託先である名古屋工業大学から受領したワークショップの調査結果報告書と、別途実施したヒアリング調査の結果に基づき作成したものである。これら両調査の結果を精査し、抽出した成果や課題等の重要点を中心に構成している。なお、報告書の作成プロセスにおいては、事前に再委託先とアウトラインや方向性について協議し、情報の網羅性を確保するよう努めた。

## 5.2. ASEAN の重要情報インフラにおけるサイバーセキュリティ対策に関する情報

### 5.2.1ASEAN 全体における OT セキュリティの概観

東南アジア諸国連合（ASEAN）と東アジアの経済研究機関（以降、ERIA）が 2023 年に発行した報告書『Operational Technology Security in ASEAN[80]』によれば、ASEAN 地域では、ICT セキュリティに対する意識は向上しつつあるものの、OT セキュリティへの意識と準備は依然として不十分な状況である。ASEAN 全体として OT セキュリティに特化した統一的なイニシアチブはまだ見られず、各国の取り組み状況には差があるのが実情である。

国家レベルの取り組みでは、シンガポールとマレーシアが先行している。シンガポールは国際標準である IEC 62443[81]を国内規格として採用し、政府の調達要件と連動した製品認証制度を整備するなど、先進的な取り組みを進めている。マレーシアも 2023 年に IEC 62443 を国内規格として採択し、OT セキュリティに関するガイドラインの整備を開始した。しかし、他の多くの ASEAN 諸国では、国家レベルでの具体的な OT セキュリティに関するイニシアチブはまだ見られないのが現状である。

企業レベルにおいても、対策状況は一様ではない。グローバル企業や、過去に OT 関連のインシデントを経験した、あるいは重要インフラに関連する一部の現地企業は、国内基準の有無にかかわらず、自主的にグローバル標準を参照して対策を進める傾向がある。一方で、多くの ASEAN 諸国の現地企業は、OT セキュリティの重要性を認識していても、高コスト、専門家不足、あるいは政府による明確なガイドラインの欠如といった理由から、体系的な対策に着手できていない。さらに、OT セキュリティの重要性への理解不足から対策の優先順位が低い企業や、工場の自動化が進んでいないため OT 対策の必要性が低い企業も多数存在する。

このように、ASEAN 地域では OT セキュリティ対策が各国・各企業の自主的な取り組みに委ねられているのが現状である。しかし、グローバルサプライチェーンの拡大に伴い、地域全体で協調してサイバーレジリエンスを向上させることの重要性は増している。各国・各企業が個別最適の取り組みを続けるだけでは、グローバルなビジネス機会を損失するリスクも指摘されている。さらに、ERIA の見解として、地域的な合意に基づき各国政府が規制を整備し、その枠組みの下で企業の OT セキュリティ対策を段階的に成熟させていくという協調的アプローチが望ましいと結論づけている。

### 5.2.2各国の政策・制度的枠組み

#### (1) サイバーセキュリティ関連政策・戦略の比較分析

タイ、フィリピン、インドネシアの 3 か国は、いずれも国家レベルで重要インフラのサイバーセキュリティ強化に取り組んでおり、規制当局としてタイは国家サイバーセキュリティ庁（NCSA）、フィリピンは情報通信技術省（DICT）、インドネシアは国家サイバー・暗号庁（BSSN）が中心的な役割を担っている点で共通している。しかし、制度の成熟度と OT/ICS（Industrial Control Systems）への具体的な適用状況には差異が見られる。

---

[80] Economic Research Institute Operational Technology Security in ASEAN

[81]工場やインフラの「OT（制御システム）」に向けた、国際電気標準会議（IEC）が発行するサイバーセキュリティの国際規格。

**表 11　各国の重要インフラセキュリティ政策一覧**

| 比較項目 | タイ | フィリピン | インドネシア |
|---|---|---|---|
| 中核機関 | NCSA | DICT | BSSN |
| 重要インフラ指定・枠組み | Cybersecurity Act（2019）[82] CII 定義、リスク評価運用 | 重要インフラ保護の義務化に向け制度整備中（法案審議を含む[83]） | IIV（重要情報インフラ）枠組（大統領規則 82/2022 等）[84] |
| OT/ICS への適用状況 | CII 向け義務の明確化が進展（リスク評価等） | 国家計画は整備、実装は発展途上 | 国家計画は整備、実装は発展途上 |
| 参加者が言及した参照標準 | NIST CSF[85], NERC CIP[86] | 言及なし | IEC 62443[87]、NIST CSF |

上表の通り、タイは「Cybersecurity Act（2019）」を基盤に重要情報インフラ（CII）の枠組みを制度化し、リスク評価等の義務を明確化するなど、制度面の整備が先行している。一方、フィリピンは国家計画レベルでの方向性は示されているものの、OT 領域への実装は発展途上にある。インドネシアは BSSN を中心に複数の制度を整備しており、IEC 62443 等の国際標準への言及も確認されたが、実運用面での組織間の成熟度の差が課題となっている。

**(2)　CII/IIV 保護に関する法制度・ガイドラインの整備状況と課題**

各国で CII/IIV 保護に関する法制度・ガイドラインの整備が進められているが、共通の課題として、IT 中心に設計された制度・ガイドラインが、OT 特有の制約と衝突しやすい点が挙げられる。OT 環境では、安全性（Safety）と可用性（Availability）が最優先され、長期稼働するレガシー設備が多いため、IT で一般的なセキュリティパッチの頻繁な適用やシステムの再起動といった対策をそのまま適用することが困難である。このため、制度や方針が整備されていても、現場では「操業を止めずにどのように実装するか」といった実務上の問いに対する具体的な解決策が示されにくい状況が生じている。この「実装ギャップ」は、制度が現場で実効性を持ちにくい根本的な課題となっている。

### 5.2.3事前アンケート等から見る重要インフラ事業者の対策状況と課題

**(1)　事前アンケートの実施**

事前アンケート調査は、OT ワークショップ参加申込者を対象として実施したものである。目的は、各国のサイバーセキュリティおよび各組織の OT セキュリティの取り組み状況を把握し、ワークショップの議論を効果的に進めることである。調査対象の詳細は 5.4.1（表 14）を参照されたい。

事前アンケートでは、参加者の氏名と企業名を取得し、各国のサイバーセキュリティ関連法規制や政策、重要インフラの管轄当局、情報共有のためのプラットフォームや ISAC の有無について確認した。また、各組織の OT セキュリティについては、セクター間の成熟度認識、公式ポリシーやリスク管理フレームワークの導入状況、意思決定権者、監査・検査の頻度、過去のインシデント経

[82] Government Gazette cybersecrutiy-act-2019-en.pdf
[83] フィリピン上院 19th Congress - Senate Bill No. 1365 - Senate of the Philippines
[84] インドネシア監査庁（BPK）PERPRES No. 82 Tahun 2022
[85] NIST Cybersecurity Framework の略であり、 米国重要インフラ向けセキュリティフレームワークのこと。
[86] North American Electric Reliability Corporation Critical Infrastructure Protection の略であり、北米電力規制のこと。
[87] 産業用オートメーションおよび制御システムのサイバーセキュリティに関する国際標準規格。

験などを調査した。これらの設問を通じて、各国・組織の現状と課題を把握し、ワークショップの議論の質向上を図るものである。

**(2) OT セキュリティに関する組織体制・ガバナンスの現状**

事前アンケートの結果から、OT セキュリティに関する方針や枠組みの策定状況は国によって異なり、タイでは策定が進んでいる一方、インドネシアでは未策定が半数近くを占めるなど、ばらつきが見られた。最終意思決定者については、経営層または IT/CISO[88]が関与する傾向が共通して見られたが、タイでは IT/CISO、フィリピンでは経営委員会、インドネシアでは CISO に権限が集中するなど、国の政策が企業ガバナンス構造に反映されている点が特徴的である。しかし、これらのガバナンス体制が整備されていても、それが現場レベルで有効に機能しているかは別問題であり、方針と運用の間に乖離が存在する可能性が示唆される。

**(3) 技術的対策の導入状況と「一部実装」の課題**

技術的対策については、多くの組織でネットワーク分離（IT/OT 境界のファイアウォール設置）や基本的な監視、アクセス制御などが実施されている。一方で、OT 資産の網羅的な可視化や OT に特化した脅威検知・分析（OT-IDS 等）、OT 環境のログを活用する SIEM の導入などは進んでいない傾向が見られる。重要な課題は、多くの対策が「一部実装（Partially implemented）」にとどまっている点である。これは、事業者が対策を軽視しているのではなく、OT 特有の環境下で「何からどこまで実施すれば十分なのか」という判断基準を持てていない状態を示しており、結果として対策が断片的になり、リスク低減に結びついていない状況を生んでいる。

**(4) インシデント対応（IR）体制の整備状況と現場の不安**

インシデント対応計画についての事前アンケートの結果は以下の通りとなった。

**表 12　インシデント対応計画**

| 観点 | タイ | フィリピン | インドネシア | 共通的示唆 |
|---|---|---|---|---|
| 過去 3 年のインシデント経験 | 14% (2/14) | 7% (1/13) | 11% (2/19) | 経験値が低い |
| OT を含む IR 計画整備 | 57% (8/14) | 54% (7/13) | 32% (6/19) | 計画・訓練の不足が弱点 |
| 対応への自信 | 中〜低 | 中〜低 | 低〜中 | 訓練不足を反映 |

過去 3 年間にインシデントを経験した組織は 3 か国ともに少なく（7%〜14%）、経験値が低いことがうかがえる。OT を含むインシデント対応（IR）計画の整備率はタイ（57%）、フィリピン（54%）に比べてインドネシア（32%）が低く、3 か国全体で計画や訓練の不足が弱点となっている。これに伴い、インシデント対応への自信も「中〜低」レベルにとどまっている。現場からは「インシデントが起きたらどう対応すべきか分からない」「OT を含めた IR 計画がない、または机上の空論である」といった不安の声が共通して表明されており、計画の不在と訓練不足が現場の大きな不安要因となっていることが明らかである。

[88] Chief Information Security Officer の略であり、 最高情報セキュリティ責任者（経営層）のこと。

### 5.2.4OT 研修需要と他ドナー等による支援の現状・課題

#### (1) 事前アンケートに基づく OT 研修ニーズの分析

事前アンケートからは、OT 研修に対する強い需要が確認され、その内容は大きく 3 つの領域に分類できる。第一に、ネットワーク分離や監視といった技術を自組織の OT 環境にどう適用すべきかなど、「技術を『使える形』にするための研修」への需要。第二に、IT と OT 部門の役割分担やインシデント対応計画の策定・運用を担う人材を育成するための、「ガバナンス・運用を担う人材育成への需要」。第三に、座学よりもケーススタディやリスク分析、インシデント対応演習といった、自組織の課題解決に直結する「演習型・参加型研修への明確なニーズ」である。

#### (2) 他機関による支援の現状と限界

ASEAN・インド太平洋地域では、JICA を含む国際機関や各国政府、民間団体によりサイバーセキュリティ分野の研修・能力構築支援が実施されており、制度理解や基礎知識の普及において一定の成果を上げている。しかし、これらの支援には限界も確認されている。具体的には、研修が単発的・イベント型で提供されることが多く、組織内での運用定着まで伴走できていない点、支援内容が IT セキュリティ中心であり、OT 特有の可用性や安全性の制約を十分に扱えていない点、そして技術、人材、運用を統合的に扱うプログラム設計になっていない点が共通の課題として挙げられる。このため、既存の支援が現場の具体的な課題解決に必ずしも結びついていない状況がある。

### 5.2.5関係組織によるワークショップ協力意向・課題等

本項では、ワークショップ実施に先立ち、各国カウンターパート候補機関等に対して、本調査団が実施したヒアリング調査の結果を記述する。

#### (1) ASEAN Japan Cybersecurity Community Alliance

- 組織概要

ASEAN Japan Cybersecurity Community Alliance[89]（以降、AJCCA）は、日本と ASEAN 諸国のサイバーセキュリティ関連団体で構成される国際的な連携組織である。主な目的は、日 ASEAN 地域におけるサイバーセキュリティのガバナンスおよび運用に関する相互理解、交流、協力を深めることであり、サイバーレジリエンスの向上と能力強化を目指している。活動内容としては、サイバー脅威に関する情報交換、産官学連携の促進、持続可能なサイバーセキュリティ能力の向上・強化に取り組んでいる。構成員は、日本ネットワークセキュリティ協会（JNSA）をはじめとする日 ASEAN 各国のサイバーセキュリティ業界団体等 9 団体（設立時）が加盟している。

- ヒアリング内容

AJCCA の組織概要と強み、及び本プロジェクトにおける協力価値についてヒアリングを実施した。具体的には、サイバーセキュリティ案件は国家の機微情報に触れるため、同団体が介在することで、通常はアクセスが難しい現地の政府機関や重要インフラ企業が持つ実態情報へのアプローチが可能となる。これは、AJCCA が持つ各国機関との強固な信頼関

[89] SEAN Japan Cybersecurity Community Alliance (AJCCA) Landing - ASEAN Japan Cybersecurity Community Alliance (AJCCA)

係に基づくものであり、日系企業が単独で活動する上では得難い、本プロジェクトの成功に不可欠な価値であるとの見解を得た。

### (2) インドネシア

- **Badan Siber dan Sandi Negara（インドネシア国家サイバー暗号庁）**
  - 組織概要

Badan Siber dan Sandi Negara（以降、BSSN）は、2018 年 1 月 3 日に設立されたインドネシア政府の主要なサイバーセキュリティ機関であり、サイバーセキュリティ、サイバーインテリジェンス、暗号化、情報セキュリティ等を総合的に管轄している。BSSN は、警察や国家情報庁と連携し、サイバー犯罪対策、偽情報（フェイクニュース）やヘイトスピーチの拡散防止、過激思想のインターネット上での拡散抑止等、インドネシアのデジタル空間における安全保障を担っている。

  - ヒアリング内容

BSSN は、インドネシアにおける OT ワークショップの開催に対し協力の意向を示した。ワークショップの実施にあたっては、日本の民間企業で実際に導入されている完全自動化の OT サイバーセキュリティ製品のデモンストレーションを希望した。また、ワークショップの内容については OT 分野に焦点を当てるよう要望があった。さらに、ワークショップの差別化策として、日本企業におけるサイバーセキュリティ戦略の紹介の提案を受けた。ワークショップの成功に向けて、BSSN からは、より実効性を高めるための具体的な論点として「トレーニング証明書の発行要件の明確化」や「類似の取り組みとの差別化による参加企業の関心向上」について意見が共有された。これらの検討課題に対応していくことを前提に、関連機関や重要インフラ事業者への紹介を約束されるなど、協力に向けた建設的な対話が行われた。

- **Indonesia Network Security Association**
  - 組織概要

Indonesia Network Security Association（以降、idNSA）は、インドネシア国内におけるサイバーセキュリティおよびネットワークセキュリティの向上を目的とした業界団体である。セキュリティ専門家の育成、知識の共有、標準化の推進をビジョンおよびミッションに掲げ、セミナーの開催、トレーニングや認証プログラムの提供、コミュニティ活動等を主な事業内容としている。組織は会長をはじめとする役員・理事によって運営されており、インドネシア国内におけるサイバーセキュリティ分野のリーダー的存在である。また、AJCCA の主要構成団体として、ASEAN 地域全体の連携強化や日本（JNSA）との協力にも積極的に取り組んでいる。

  - ヒアリング内容

idNSA は OT 関連ワークショップの実施に前向きであり、インドネシア大学などと協議が可能。サイバーセキュリティ分野では AI ベースの製品がトレンドであり、PoC 実施時には MOU や NDA が必要となる場合があると助言があった。また、インドネシア市場の特性として、サイバーセキュリティ専門家に対する高い需要（約 150 万人の不足）があり、企業における意識向上の余地が大きい点が共有された。これは、本プロジェクトが提供する人

材育成や啓発活動が、現地のニーズに的確に応える大きな機会であることを示唆している。加えて、重要インフラ企業の予算が現状では他分野に優先されている傾向も指摘されたことから、費用対効果の高いソリューションの導入や、OT セキュリティ投資の重要性を訴求していく戦略が有効であるとの見解を得た。

### (3) フィリピン

- **Department of Information and Communications Technology（情報通信省サイバーセキュリティ局）**
  - ➢ 組織概要

    Department of Information and Communications Technology90（以降、DICT）は、フィリピンの ICT 分野における政策立案・推進を担う主要な行政機関である。ICT 開発戦略の策定、公共アクセスの改善、通信インフラの整備、サイバーセキュリティ対策、政府機関のデジタル化や産業振興の推進、さらに国際協力などを通じて、国民生活の向上と経済発展に寄与している。
  - ➢ ヒアリング内容

    DICT は OT 関連ワークショップの実施当たり協力の意向を示し、参加者呼びかけなどの開催にあたって必要な準備から、ワークショップ当日の運営についても協力する意向を確認した。

- **Philippine Computer Emergency Response Team**
  - ➢ 組織概要

    Philippine Computer Emergency Response Team91（以降、PH-CERT）は、フィリピンにおけるサイバーセキュリティ活動の最高機関である。主な役割は、サイバーセキュリティインシデントへの対応、国内各種 CERT との調整・報告、ネットワーク監視やセキュリティテスト、脆弱性評価などである。PH-CERT はフィリピン情報通信技術省（DICT）サイバーセキュリティ局の下位部門である国家コンピュータ緊急対応チーム（NCERT：National Computer Emergency Response Team）の通称であり、フィリピン初のサイバーセキュリティ関連非営利団体としても設立された。
  - ➢ ヒアリング内容

    PH-CERT は、OT 分野のワークショップ開催に協力する意向を示し、関係先の紹介や講演者の手配も可能。本プロジェクトに対して協力的であり、今後の発展にも期待を寄せている点について言及を受けた。

### (4) タイ

- **National Cyber Security Agency（国家サイバーセキュリティ局）**
  - ➢ 組織概要

    National Cyber Security Agency（以降、NCSA）は、タイ政府のサイバーセキュリティ対

[90] フィリピン情報通信省 Department of Information and Communications Technology
[91] 国家コンピュータ緊急対応チーム About Us | NCERT

策を統括する機関である。NCSA は、国家的なサイバーセキュリティ政策および戦略の策定、重要情報インフラの防御とサイバー攻撃への対応、サイバーセキュリティ意識向上と人材育成、さらに ASEAN 諸国等との国際協力を推進している。2019 年のサイバーセキュリティ法に基づき設立され、タイのデジタル環境の安全性と回復力確保に重要な役割を果たしている。

➢ ヒアリング内容

NCSA は、本プロジェクトにおける OT ワークショップの開催に対し、重要インフラ事業者の紹介を含め協力の意向を示した。また、タイにおけるサイバーセキュリティの課題 として、国内のサイバーセキュリティインシデントへの対応速度の遅さを課題として認識しており、特に、機微情報を多く扱うヘルスケア分野や、OT（Operational Technology）に関しては「エネルギー・公共事業」および「運輸・物流」分野での対策強化が必要であるとの見解が示された。

・ **Thailand Information Security Association**

➢ 組織概要

Thailand Information Security Association（以降、TISA）は、タイ国内の情報セキュリティ専門家、研究者、関連業界団体によって構成される非営利の主要協会である。TISA は、タイ国内外におけるサイバーセキュリティの推進、人材育成および標準化、国内外の業界団体との連携、情報共有を主な活動としている。特に、セミナーやワークショップの開催、ベストプラクティスや倫理規定の策定、日 ASEAN サイバーセキュリティ官民共同フォーラム等の国際協力活動への参加を通じて、サイバーセキュリティ分野の発展に貢献している。TISA は、2019 年に設立された国家サイバーセキュリティ庁（NCSA）と連携し、民間セクターを代表する主要なパートナー組織となっている。

➢ ヒアリング内容

TISA からは、タイ国内の現状として、政府主導のワークショップは主に NCSA が担っているという役割分担の実態が共有された。このため、本ワークショップの開催にあたっては、NCSA を主な連携パートナーとし、TISA には民間セクターの代表として専門的知見の提供や業界への働きかけといった形で協力いただく体制が、最も効果的であるとの助言を得た。また、タイの重要インフラにおけるサイバーセキュリティの主要な課題は OT セキュリティである点が共有され、タイの重要インフラにおけるサイバーセキュリティ投資は IT 分野が中心となる傾向にあり、OT セキュリティは今後の重点強化分野と認識されている。特に電力、水道、運輸といった分野では、OT セキュリティ対策の導入が大きな潜在的ニーズとなっており、本プロジェクトが貢献できる領域は非常に大きいとの見解が示された。また、従来の機器購入・設置型から、コンサルティングやインフラをテストする攻撃的サイバーセキュリティ、マネージドサービスプロバイダーの活用へと移行する動きがある。

## 5.3. OT サイバーセキュリティの検討状況およびニーズ情報

### 5.3.1 OT セキュリティに関する検討状況と認識されている課題

5.2 で分析した通り各国政府は OT セキュリティ強化を推進しているが、策定された政策が IT 中心

であり、現場への「実装ギャップ」が共通の課題となっている。 この状況下で、重要インフラ事業者は、DX 推進や遠隔保守の導入により IT と OT ネットワークの接続が進展し、これが新たな攻撃経路を生むリスクとして認識している。事業者が直面する共通の課題は、以下の 4 点に集約される。

1. IT-OT 統合に伴うリスクの顕在化
2. サポート切れ OS など長期稼働するレガシー設備と可用性の制約
3. OT を理解したセキュリティ人材の不足
4. インシデント発生時の対応への不安

これらの課題により、多くの事業者で技術対策が部分的な導入にとどまり、体系的なリスク低減に至っていない状況である。

### 5.3.2OT セキュリティに関するニーズ

#### (1) 技術導入・コンサルティングに関するニーズ

多くの事業者が技術対策を「一部実装」するにとどまり、「何からどこまでやれば十分なのか分からない」という課題を抱えていることから、技術導入の優先順位付けや全体設計に関するコンサルティングへの強いニーズが存在する。求められているのは、単なる製品導入の支援ではなく、OT 特有の可用性や安全性の制約、レガシー設備の存在を前提とした上で、リスクを評価し、資産の可視化やネットワーク分離といった影響の少ない対策から段階的に実装していくアプローチを共に検討するパートナーシップである。

#### (2) 人材育成・研修に関するニーズ

人材育成に関しては、技術者だけでなく、経営層や現場の運用部門を含む、組織横断的な研修へのニーズが高い。具体的には、OT 特有の制約を踏まえた技術の設計・運用能力、IT と OT の橋渡しができる能力、インシデント対応計画を策定・運用できる能力の育成が求められている。また、一方的な知識提供ではなく、自組織の課題に即して思考し、議論する演習型・参加型の研修プログラムへの期待が極めて高い。国別に見ると、タイでは実装・演習重視、フィリピンでは投資判断支援、インドネシアでは基礎から学ぶ体系的研修への需要が大きい。

#### (3) 国内・国際的な情報共有や演習への参加ニーズ

多くの組織が自組織単独でのインシデント対応や高度な脅威分析に限界を感じており、他組織の事例や知見を学ぶ機会を求めている。重要インフラへの脅威はセクター全体に影響を及ぼす性質を持つため、セクター内での情報共有や共同訓練を通じて業界全体の対応力を底上げすることへのニーズは高い。特に、インシデント対応計画が未整備であったり、対応への自信が低かったりする組織が多く、実践的な演習への参加を通じて、計画の実効性を高め、対応能力を向上させたいという明確な需要が存在する。

### 5.3.3課題・ニーズ解決に向けた日本からのアプローチ提示

本調査で明らかになった課題とニーズ、特に「IT 中心のセキュリティ概念が OT 現場に翻訳されていない」という問題に応えるため、ワークショップでは日本の先進的な知見に基づくアプローチを提示した。

#### (1) ワークショップにおける基礎講義の設計思想

実施した OT セキュリティ基礎講義は、単なる知識提供ではなく、政策・制度、現場課題、そし

て実装可能な対策をつなぐための「共通言語」と「思考の枠組み」を参加者に提供することを目的とした。これにより、多様な背景を持つ参加者間の共通理解を醸成し、続くグループワークの質を高めることを意図した。

### (2)　日本の知見の展開：経産省ガイドラインの活用

講義では、日本の経済産業省が策定した令和 4 年 11 月 16 日発行の「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(Ver1.0)」に基づくチェックリストの説明や OT 領域のソリューションとのマッピング（図 32）についての解説を行った。

| Sub Cat. | Item | OT security solutions for each term | |
|---|---|---|---|
| Asset management | 2-6<br>2-7 | Communication terminal visibility and control in the network | OT-IDS, Asset Management tool, NAC |
| Endpoint Protection | 3-1<br>3-2<br>3-3 | • Client protection and centralized management<br>• Apply virtual patches<br>• Application whitelist or blocking of designated communications | AV,EDR,. Whitelist (WL),. USB-Type AV |
| Network | 3-5<br>3-6<br>3-7 | • Segmentation and security measures with VLANs<br>• Secure remote maintenance<br>• Communication terminal visibility and control in the network | UTM,SW/AP FW, SRA,. Decoys, OT-IDS |
| Log | 3-8 | Communication log storage and reporting | Syslog Server SIEM, etc. |

**図 29　経産省チェックリストの項目とセキュリティ製品の対応表**

このチェックリストは、多くの事業者が抱える「何から始めるべきか分からない」という課題に対し、自組織の現状を可視化し、対策の優先順位付けを行うための実践的なツールとして機能した。これは、監査項目としてではなく、どこから着手すべきかを判断するための対話ツールとして位置づけられた点が特徴である。

### (3)　リスクベースアプローチと段階的導入の提示

本講義の中核として、技術対策を目的化せず、現場の事業リスク（安全、品質、事業継続など）を起点に考える「リスクベースアプローチ」が提示された（図 32）。

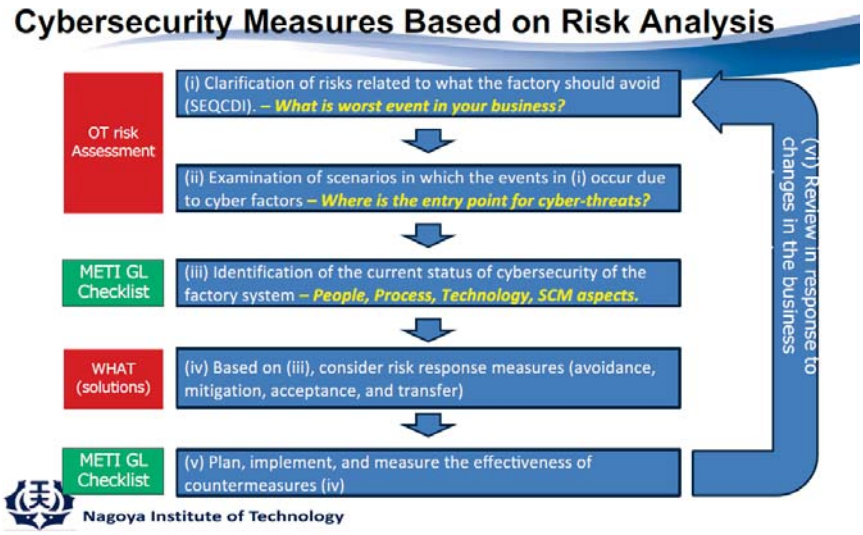



**図 30　OT セキュリティの現場リスクベースのアプローチ**

これは、まず安全、環境、品質、コスト、納期、情報（SEQCDI）の観点から「起きてほしくない事象」を具体的に言語化し、そこからサイバー要因との結び付けや対策を検討する手法である。さらに、技術導入に関しては、脅威検知の範囲と対応の自動化レベルで分類したモデル（Model X/Y/X+/Y+）が示された。このモデルにより、「高度な製品を入れられないから何もできない」のではなく、「今の環境でもできることから積み上げられる」という段階的な成熟度の考え方が共有された。これは、レガシー設備や予算に制約を抱える事業者にとって、現実的なアプローチとして有効であった。

## 5.4. ワークショップ実施による情報収集結果

### 5.4.1 ワークショップの実施概要

本ワークショップは、タイ、フィリピン、インドネシアの 3 か国を対象に、OT 分野におけるサイバーセキュリティ対策の現状評価、研修ニーズや政策課題の明確化、そして参加者の意識向上と能力強化を目的として開催された。実施概要の詳細は下記のとおりである。

**表 13　ワークショップ実施概要**

| 項目 | タイ | フィリピン | インドネシア |
|---|---|---|---|
| 実施国・都市 | タイ・バンコク | フィリピン・マニラ | インドネシア・ジャカルタ |
| 実施場所 | TK palace hotel & convention | The B Hotel | Universitas Indonesia (インドネシア大学) |
| 実施日時 | 2025 年 11 月 2 日 | 2025 年 11 月 24 日 | 2025 年 12 月 22 日 |
| 事前アンケート有効回答 | 14 名 | 12 名 | 19 名 |

| 項目 | タイ | フィリピン | インドネシア |
|---|---|---|---|
| 主な参加セクター（例） | 電力、交通、政府機関、通信、水道、石油・ガス | 電力（発電）、政府機関、水道 | 通信、製造、エネルギー、金融、政府機関 |
| 現地協力機関（主要） | NCSA | DICT | idNSA[92]、idCARE.UI[93] |
| 実施形式 | 対面 | 対面 | 対面 |

参加者は、各国の重要インフラ事業者および関連政府機関から招聘された IT・OT セキュリティ担当者であり、所属セクターは多岐にわたった。プログラムは、①自己紹介、②OT セキュリティ基礎講義、③グループワーク＆発表、④クロージングで構成され、参加者の共通理解を促しつつ、具体的な議論を引き出す設計とした。

### 5.4.2 各国ワークショップにおける主要な議論と示唆

・　タイ：「制度先行、運用・人材定着が課題」

タイでは、国家制度やガイドラインが比較的整備されている一方で、現場では OT を理解した人材が限られ、事故対応計画や訓練を含む運用面への定着が十分に進んでいない「制度先行、運用・人材定着が課題」という構造が示唆された。ワークショップでは参加者間の知識・経験差も見られたが、グループワークを通じてリスク検討の基本的な枠組みを理解するという目的は達成された。今後の協力としては、既存の枠組みを前提に、演習や運用テンプレートを通じて実効性を高める支援が有効であると考えられる。

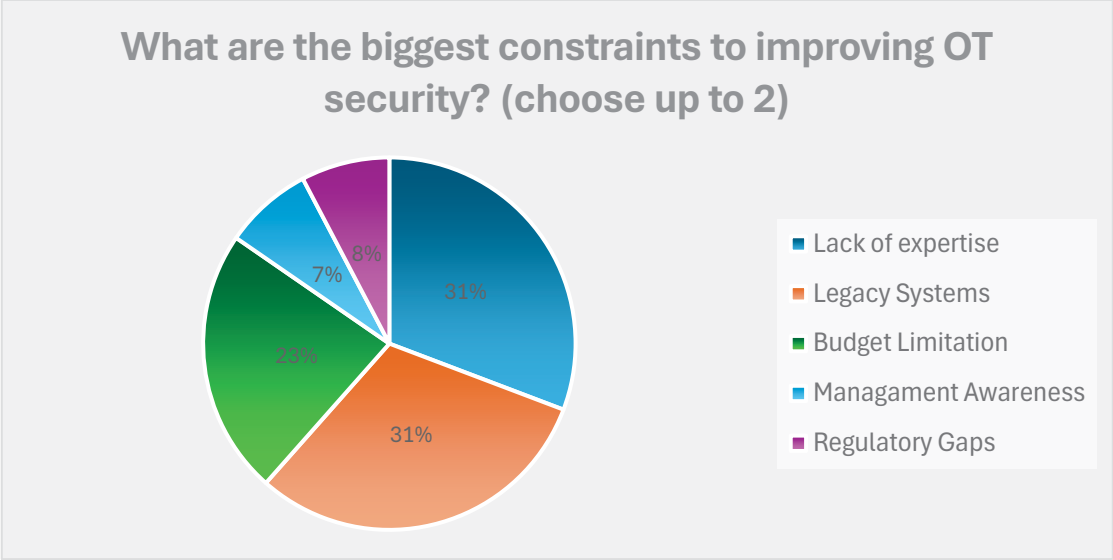



**図 31　OT セキュリティ向上の最大の課題に関する回答（タイ）**

・　フィリピン：「経営関与は高いが、予算・レガシー制約が壁」

フィリピンでは、経営層の関与や事業影響を意識した議論は活発であるものの、老朽化した設備や限られた予算が技術対策導入の障壁となっている「経営関与は高いが、予算・レガシー制約が壁」

[92] Indonesia Network Security Association の略称。
[93] Indonesia Cyber Awareness and Resilience Center, University of Indonesia の略称。

という状況が示唆された。ワークショップでは参加者全体のスキルレベルが高く、守るべき資産や優先順位を明確にした高度な議論が行われた。今後の協力としては、リスクの優先順位付けや可視化を通じて、投資判断の根拠を明確化する支援が求められる。

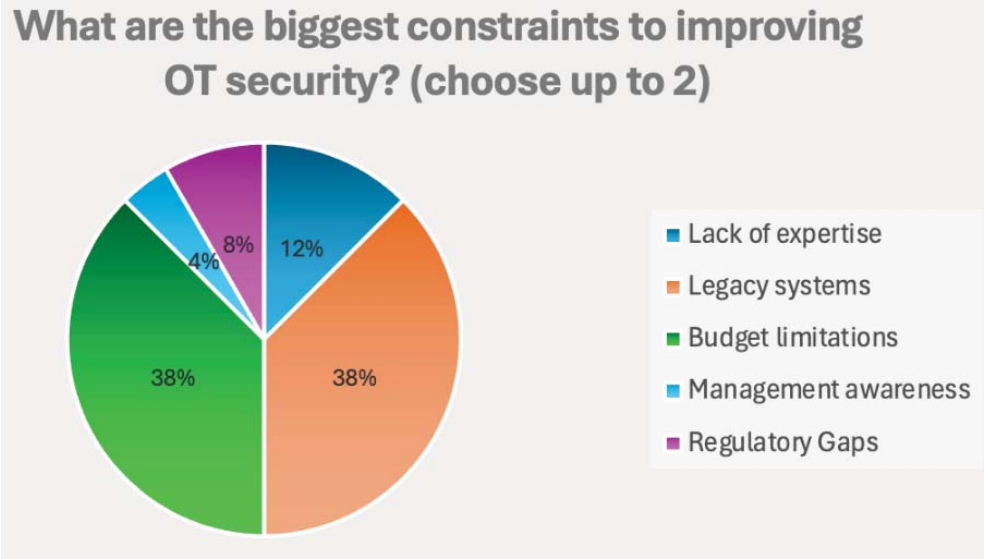



**図 32　OT セキュリティ向上の最大の課題に関する回答（フィリピン）**

・　インドネシア：「制度群は多いが、人材・計画不在が最大課題」

インドネシアでは、複数の制度や国際標準が参照されている一方で、OT を含むインシデント対応計画の整備率が低く（31.6%）、組織的な運用体制へ移行できていない「制度群は多いが、人材・計画不在が最大課題」という状況が示唆された。ワークショップでは IT・OT 双方に精通した参加者を中心に質の高い議論が展開された。今後の協力としては、基礎的なテンプレート（IR Playbook 等）と演習を重視し、組織としての対応能力を底上げする段階的な支援が不可欠である。

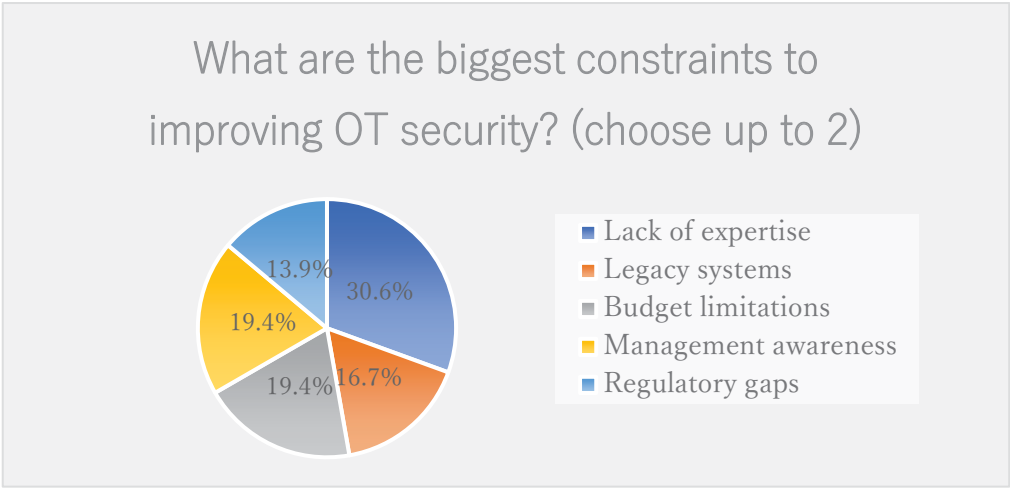



**図 33　OT セキュリティ向上の最大の課題に関する回答（インドネシア）**

### 5.4.3全体を通じた考察

・　3か国に共通して見られた課題・ニーズ

3 か国に共通する構造的課題として、国家レベルで政策整備が進む一方、OT 特有の制約を考慮した実装の具体像が現場に届いておらず、「政策と現場の間に存在する実装ギャップ」が確認された。これにより、事業者レベルでは「IT-OT 統合に伴うリスク」「レガシー設備」「人材不足」「インシデント対応への不安」といった共通の課題に直面している。これらの課題を背景に、技術を実用化するための研修、ガバナンスを担う人材の育成、そして実践的な演習型研修への強いニーズが共通して見られた。

・　今後の協力の方向性に関する提言

本調査結果を踏まえ、今後の協力は、日本の製造業等が持つ「稼働を止めずに守る」思想や、現場リスクを起点とするアプローチを活かすべきである。具体的な方向性として、以下の 3 点を提言する。第一に、単発のワークショップから、基礎・応用・定着といった段階を設けた「継続型プログラムへ発展」させること。第二に、「IR Playbook」や「演習シナリオ」といったテンプレートと演習を中核に据え、政策と現場を橋渡しすること。第三に、OT 環境の現実に即し、「可視化」から「監視」「制御」へと進む「段階的技術導入を前提とした支援」を行うことである。

# 第 6 章　提言・まとめ

## (1) 報告会の実施

### A)　全体概要

本プロジェクトの活動成果を総括し、今後の JICA によるプロジェクト形成への具体的な示唆を得るため、2026 年 1 月 28 日（水）に本邦での最終報告会を実施した。報告会は有限責任監査法人トーマツの丸の内二重橋オフィスにて開催され、本邦サイバーセキュリティ製品に関する状況として PoC を実施した 3 社の成果を共有する第一部（9:30〜11:00）と、産業システム（OT）向けのサイバーセキュリティ対策状況として OT ワークショップの成果を共有する第二部（11:00〜12:00）の二部構成で進行した。参加者は JICA ガバナンス平和構築部 STI・DX 室の担当者および有限責任監査法人トーマツの担当者に加え、第一部には PoC 実施企業である網屋、マクニカ、IIJ の各担当者、第二部には名古屋工業大学の担当者が出席し、議論を行った。

本報告会は、日本の民間企業や研究機関・大学が持つサイバーセキュリティ分野の知見や技術の現状を把握し、それらを ASEAN 諸国へ展開する可能性を検討することの成果として位置づけられるものである。本邦企業や研究機関の知見や活用は限定的であり、企業による現場ニーズ把握や製品の海外展開が十分に進んでいない状況があるという背景を踏まえ、プロジェクト期間中に得られた成果と課題を JICA へ共有し、将来のプロジェクト形成に資する多角的な意見交換を行うことを目的とした。議題としては、各再委託先である PoC 実施企業 3 社および名古屋工業大学から、それぞれの活動成果、認識された課題、そして今後の JICA プロジェクト形成における提言が共有された。各報告後には、JICA を交えた活発な意見交換会が実施された。

### B)　本邦サイバーセキュリティ製品に関する情報

PoC 実施企業 3 社との意見交換会では、JICA に対して本邦企業の現地展開を加速するためのイベント支援強化案が示された。具体的な提案として、ビジネスマッチングの場の提供、セキュリティカンファレンスの開催、政府関係者を招いたワークショップの機会創出が挙げられた。JICA 主催による「ジャパンパビリオン」形式のイベント開催への期待も示された。さらに、現地 IT 協会や産業界との連携を通じたローカルパートナーの発掘・育成支援の重要性が指摘された。

現場導入に関しては、現地法規制への適合や導入・維持費用が障壁となっており、制度面や費用面での環境整備が課題とされた。規制対応のためのガイドライン整備支援、導入インセンティブとなる現地導入費用補助、国際標準への適合支援が具体的な提案として挙げられた。特に費用補助については、実証先の政府機関からも要望があったと報告された。加えて、実証後の本格導入に向けた予算確保の課題や契約手続きの円滑化支援への期待が示された。

サイバーセキュリティ対策の持続的運用には、現地人材の育成や導入後の継続的なサポート体制の確立が不可欠とされた。現地の人材やリソース不足を背景に、サブスクリプション型の継続支援や現地担当者が自立できるための技術移転型支援の提案がなされた。JICA からは ASEAN 全域でのサイバーセキュリティ人材育成事例を取り上げ、現場向けの実践的トレーニングや主要大学・国家機関との連携によるコミュニティ形成の促進が有効との意見が示された。

さらに、日本発製品の強みを現地で訴求し、ブランド認知を高めるための広報・啓発活動の推

進も重要視された。日本の強みとして、技術力のみならず運用や統制を含めた設計力、説明責任を果たす姿勢が参加企業より挙げられた。現地の対面重視の文化を踏まえた信頼関係構築の重要性も指摘された。各国・分野ごとに異なる現場の成熟度や文化に柔軟に対応したレポート作成や運用補完、人材不足を補う実行支援のパターン化・知見共有も、今後の取り組みとして意義があるとの見解が述べられた。

**図 34　PoC 報告会の様子（各社報告および意見交換）**

C)　産業システム（OT）向けサイバーセキュリティ対策状況

OTワークショップを実施した名古屋工業大学との意見交換において、OTセキュリティ対策は単なる技術導入を目的とするものではなく、ビジネスリスク低減のためのツールとして捉える必要があるという指摘があった。現場の稼働や安全性を守ることが最優先事項であり、サイバー攻撃はその脅威の一つとして位置づけられる。このような視点の転換が、現場の理解や納得の促進、制度の形骸化防止につながると考えられる。また、セキュリティ対策そのものが目的化することへの懸念も示された。対策が目的化すると、システム停止のリスクがあってもガイドラインに従ってパッチを適用する判断に至る可能性がある。しかし、ビジネスリスクを低減する視点に立ち、その対策が適切かどうかを判断することが求められるとされる。

さらに、各国の成熟度に合わせた伴走型支援の重要性も指摘された。タイ、フィリピン、インドネシアでは、それぞれ人材育成、設備更新、計画策定など異なる課題が存在しているため、画一的な支援よりも現場に即した実装支援が望ましいとされる。インシデント対応計画の実効性を高めるための具体的なサポートや、経済産業省ガイドラインのチェックリストを活用した初期導入支援が有効であると考えられる。経済産業省のチェックリストは、NIST フレームワークなどに比べて項目が少なく、「組織（People）」の観点から始まるため、対策組織が未整備な状態でも現状把握がしやすい点が特徴として挙げられた。

その他、IT 中心の制度では「機密性」が重視される傾向があるが、OT 現場では「安全性」や「可用性」が最優先事項となる。このギャップを埋めるために、OT に特化したリスクベースアプローチの採用や、操業を止めずに実現可能な対策を現場目線で検討する必要がある。IT セキュリティの歴史的背景から「機密性」に意識が偏りやすいが、OT ではサイバー攻撃によるサービス停止が重大なリスクとなるため、「なぜこの対策が必要なのか」を現場が納得できる形で進めることが重要であるとされる。

テクノロジーのみならず、組織（People）やプロセス（Process）と一体となった支援が、日本ならではの差別化につながる可能性がある。制度と現場をつなぐ実践的な仕組みを提供することが、JICA の国際協力における強みとなり得る。例えば、ある工場がサイバー攻撃を受けた際に、IT システムの復旧ではなく手動で出荷情報を取得し生産を再開した事例が紹介された。このような対応は事前の計画や組織・体制の整備によって初めて実現可能であり、テクノロジーだけでなく組織・プロセス面の支援が有効であると考えられる。

以上を踏まえ、JICA が今後取り組む事項として、現場実装を重視した伴走型支援や、ビジネスリスク低減の視点導入、OT 特化のリスクベースアプローチの推進、組織・プロセスの包括的支援などが意見として挙げられた。


**図 35　OT ワークショップ報告会の様子（結果報告および意見交換）**

**(2)** 提言・まとめ

A)　本邦サイバーセキュリティ製品に関する情報収集

本実証事業における 3 社の取り組みは、日本のサイバーセキュリティ製品がグローバル市場で競争力を確保するための条件や課題を具体的に示している。

マクニカは、フィリピン市場において、米国やイスラエル系ベンダーの高い技術力やグローバル標準への対応が求められる厳しい競争環境に対応するため、現地法令や規制を踏まえた製品設計と迅速な市場投入を推進している。現地パートナーとの信頼関係やネットワークを活用し、フィリピン独自の文化や商習慣にも配慮した展開を進めているのが特徴である。一方、現地語対応や人材育成、ブランド認知度の強化などは今後の課題であり、現地に根ざした営業体制やアジャイルな製品開発、マーケティングの拡充が必要となる。今後も現地ニーズに即したソリューション提供と体制強化を重視し、持続的な市場展開を目指していく。

網屋の ALog SIEM は、タイ市場の制約条件（コスト重視、人材不足、個人情報保護法対応など）に即したプロダクト設計と運用モデルを提示している。高度な SIEM の導入が難しい中堅企業層に対し、専門知識不要、特許取得済みの圧縮技術、現地保存、自動化といった特徴が、現実的な導入・運用障壁の低減に寄与している。PDPA（タイ個人情報保護法）との親和性も高く、証跡管理や原因特定が容易な点は現地で高く評価されている。タイ市場では既にパートナー企業や教育機関との連携実績があり、今後の横展開の起点となりうる土壌が形成されている。ALog は「自動判断 SIEM」ではなく「人が判断しやすくする SIEM」としてポジショニングされており、現場課題に即した運用設計が現地ニーズと合致している。

IIJ は海事分野という重要インフラ領域で、Safous を活用したアクセス統制と監査証跡モデルの標準化を進めている。IT と OT が混在する環境において、可視性、説明責任、運用効率を同時に実現しており、段階的導入や共通化モデルの提示は今後の OT セキュリティの高度化やグローバル規制対応に向けた先行事例と位置付けられる。現状の課題（アクセス管理の不在、責任不明確、監査体制の欠如など）に対し、Safous 導入による改善効果が認められている。海事情報プラットフォームの拡張にも横展開可能な基盤となっており、国内外の重要インフラでのインシデントや規制強化の流れとも合致している。

以上の事例から、海外展開における成功要因として、現地法令・規制対応の徹底、現場課題から

逆算した UX や運用設計、現地人材・パートナーとの協働、段階的拡張を見据えた共通基盤構築が重要であると考えられる。今後は、官民一体となったグローバル認証・規制対応支援、現地営業体制の即応化、ローカル企業へのインセンティブ設計など、エコシステム型成長を支える制度・財政・技術面の基盤整備が求められる。

B)　産業システム（OT）向けサイバーセキュリティ対策状況

タイ、フィリピン、インドネシアの 3 か国を対象に産業システム向けサイバーセキュリティワークショップを実施した結果、いずれの国においても国家レベルでの政策や制度の整備は進んでいる一方、現場での実装には依然として課題が残ることが明らかになった。いわゆる「実装ギャップ」の主な要因としては、工場など産業インフラの現場では安全性や稼働の確保が最優先されており、長期間稼働するレガシー設備が多いことから、IT 分野を中心に設計された対策や制度をそのまま適用しにくい点が挙げられる。

このような背景から、インシデント対応計画の未整備や専門人材の不足、技術的対策の一部導入にとどまるなどの共通課題が顕在化している。効果的な対応策としては、リスクベースでのチェックリストやインシデント対応計画の標準化、現場での演習や研修の実施、また業界内での情報共有や共同訓練の推進が重要となる。あわせて、資産の可視化やネットワーク分離、監視といった技術的な対策を段階的かつ組み合わせて導入していくことが求められる。

国ごとの優先事項としては、タイは現場での運用定着と演習の充実、フィリピンはリスクに基づく優先順位付けと投資判断の根拠明確化、インドネシアは人材育成と計画整備の基盤構築が喫緊の課題である。今後の協力にあたっては、日本の「稼働を止めずに守る」という思想や、現場リスクを起点とするアプローチを活用し、政策と現場をつなぐ継続的な支援プログラムへの発展が期待される。

C)　総括

各国で政策整備が進む一方、OT 現場への実装が十分に進まないというギャップや、日本発サイバーセキュリティ製品のグローバル競争力強化について、同時に取り組む必要があると考えられる。現場でのギャップの背景には、安全性や可用性を優先する運用文化、レガシー設備の存在、人材や予算の不足などがあり、対策が部分的な導入にとどまっている状況が見受けられる。製品側では、現地法令への適合、運用起点の UX 設計、言語・人材対応、ブランド認知、共通基盤の不足などが課題として挙げられる。こうした状況に対しては、政策と現場を橋渡しする継続的な実装支援や、エコシステム型の市場展開支援を同時に進めることが有効と考えられる。

例えば、技術協力においては、開発途上国のシステム利用現場が即座に活用できるサイバーセキュリティの製品実装パッケージを本邦企業と共同で整備し、また、運用方法の指導も行いながら「止めずに守る」対策の定着を図ることが有効と考えられる。リスクベースのチェックリストやインシデント対応計画の標準テンプレートを現場の成熟度に応じてカスタマイズし、段階的な導入の仕組みを構築することが期待される。加えて、定期的なテーブルトップ演習や評価指標の共有、セクター横断の共同演習を制度として根付かせることも意義がある。IT と OT を統合した運用モデルや、資産可視化・分離・監視の段階的導入ガイドも併せて提供し、現場の実効性向上を目指すことが望ましい。さらに、現地法規制への対応手順や責任分担を官民コンソーシアムで策定し、主管庁

と協働して規制運用の定着を進める枠組みの構築も重要と考えられる。現地人材育成やコミュニティ形成についても、主要大学や国家機関と連携した技術移転の促進が期待される。

無償資金協力については、初期装備の不足を補い、現場が対策を迅速に開始できる環境を整備することが有効と考えられる。監視・可視化の基本機能を備えた機材の配備や、論理分離・ゲートウェイの整備、演習用ラボや地域訓練拠点の設置、非停止で導入可能なネットワーク中心対策への初期支援など、費用負担を抑えつつ効果を最大化する取り組みが期待される。また、現地導入費用の一部補助や持続的な運用支援の一環として、一定期間、現地サポートに係る運用費の補助等、維持費用の段階的支援、現地法規制対応ガイドラインの整備・普及への資金支援も有効な施策と考えられる。さらに、本格導入に向けた予算確保や契約手続きの円滑化についても、財政面からの支援が求められる。

本邦サイバーセキュリティ企業が、日本発の製品・サービスの現地での導入、運用体制の確立、および関係者との信頼関係の構築を一体的に推進する上で、中小企業・SDGs ビジネス支援事業（JICA Biz）の活用も選択肢の一つとして考えられる。製品・サービスの現地法令適合、国際認証取得、現地ビジネスパートナーおよびビジネスモデルの構築を伴走型で支援するとともに、重要情報インフラの特定セクターにおいて小規模実証を行い、効果を可視化する。さらに、その実証で得た運用・技術・商流等の知見をもとに、他セクターへの更なる実証を行い、横展開を図ることが期待される。加えて、現地 IT 協会や産業界との連携を通じて、現地パートナーの発掘・育成も推進されることが望ましいことから、顧客ニーズ検証の一環として、各種現地イベント、カンファレンスへの参加、ワークショップの開催を通じて、本邦サイバーセキュリティ企業（JICA Biz 採択企業）のブランド認知度の向上を図ることも考えられる。

総じて、日本がもつ「稼働を止めずに守る」という思想を軸に、制度・財政・技術の三位一体で重要インフラのレジリエンスと日本発ソリューションの競争力を同時に高める進め方が有効と考えられる。現場起点の実装を継続的に支え、政策と運用のギャップを段階的に解消していくことが、持続的な成果につながると期待される。


ジャイカ
JICA