国際社会と協調するために、
日本の重要インフラ並びにそのサプライチェーンが今取り組むべきこと
～ICAM とセキュリティクリアランス制度の考察～

一般社団法人セキュア IoT プラットフォーム協議会
理事長　辻井 重男

2025 年 10 月

Copyright 2025 Secure IoT Platform Consortium

はじめに

毎年アメリカ合衆国議会で制定される国防政策の基本法である国防権限法(NDAA)は、国防予算法という枠を超え、サイバーセキュリティ、サプライチェーン管理、人的安全保障を網羅する包括的立法へと進化している。毎年必ず超党派で可決される「マストパス」法であり、様々なサイバーセキュリティの関連条項が制定されている。
またここで定められた様々なセキュリティ規格は、国防案件のみならず、重要インフラやサプライチェーンへも適用される。

ICAM(Identity, Credential, and Access Management)

重要インフラおよびサプライチェーンのセキュリティ確保のために、ICAM(Identity, Credential, and Access Management)による厳格な個人識別・認証・アクセス管理が定義され、米国内のみならず同盟国にも波及する国際的準拠条件になりつつある。
ICAM は、ゼロトラストの中核をなす構成要素であり、情報にアクセスするヒトに対する確かな身元確認による ID 発行、ID に基づく資格情報の発行とアクセス管理が求められている。さらにデジタルアイデンティティ(電子的な本人確認・認証)のための技術的・運用的ガイドラインを規定して、NIST SP 800-63 が制定されている。
また AI 技術や IoT 機器の普及により、「もの」(センサー、デバイス、アプリケーション等)にも固有のデジタルアイデンティティを付与することが不可欠となっており、機器やソフトウェア間通信においても、厳格な認証・認可を適用する必要がある。

セキュリティクリアランス制度

人間中心の仕組みにとどまらず、あらゆるエンティティ（人・機器・プロセス）を統合的、かつ、動的に管理するゼロトラスト型アクセスフレームワークへと進化している。
あわせて米国を中心に重要情報保全のためのセキュリティクリアランス制度が導入されている。日本においても 2024 年以降、政府/企業/研究機関を対象とするセキュリティクリアランス制度(機密情報保全法制)の導入議論が本格化してきており、2025 年 5 月 16 日に施行された「重要経済安全情報保護活用法」にて日本版セキュリティクリアランスの内容が定義されている。

セキュア IoT プラットフォーム協議会では、国際社会並びに我が国の状況を考慮し、本考察において、ICAM や日本版セキュリティクリアランス制度などグローバルの動きを統合的に捉え、現在日本企業や産業界に求められる視点を整理する。

Copyright 2025 Secure IoT Platform Consortium

① ICAM 強化によるアクセス管理

ICAM は、単なる認証技術ではなく、ゼロトラストを前提に「適切な主体(ヒト・モノ・AI プロセス)が」、「適切な理由で」、「適切な情報に」、「適切なタイミング」でアクセスしていることを国家安全保障レベルで統合管理する枠組みである。

米国国立標準技術研究所(NIST)の発行するゼロトラストアーキテクチャ（SP800-207)およびその実装ガイド(SP1800-35)を背景に、ICAM は従来の静的な認証管理から、動的なリスクベースのアクセス制御モデルへと発展してきている。
また国際的なセキュリティ規格や法令（NIST SP800 シリーズ、欧州 CRA など）でも必須項目として ICAM の考え方が採用され、セキュリティバイデザインの基本的アーキテクチャとなっている。

厳格な個人認証

ICAM では、対象者の身元の厳格な確認が求められ、ID は資格情報(IC カードなど)に関連付けられる。さらにセキュリティを強化するために、PIN などの 2 番目の要素がその資格情報に追加される。多要素認証には、「あなたが知っているもの(PIN 等)」、「あなたが持っているもの(IC カード、機器、トークン等)」、「あなた自身であるもの(指紋、静脈、顔等)」が含まれる。
さらに、組織は個人の特性を資格情報に関連付け、特定の個人がいつその情報にアクセスできるかを決定するポリシーを作成することが必要とされる。

ICAM の要求事項

ICAM を設計するためには以下の要件を満たすことが必要となる。

●ID management
- 信頼された発行者から ID が発行されているか
- 有効期限が設定できるか 資格情報が改ざんされないか

●Credential management
- 多要素認証が保証できるか
- PIN を使用してハードウェアトークンを実装できるか

●Access management
- 上記要件を満たすアクセス管理が実行できるか
- TLS、IPsec+IKE(Internet Key Exchange)は日本国内行政で横断的な推奨技術

この 3 つの要求事項の実現のためには、PKI(公開鍵基盤)による厳格なコントロールが効果的であり、最もリーズナブルな方式であると考えられる。

Copyright 2025 Secure IoT Platform Consortium

さらなる要求事項

TLS や IPsec+IKE は通信経路の暗号化における基本技術として引き続き有用であるが、ゼロトラストでは「経路暗号」より「ID 証明の信頼」が中核となる。そのためよって、“人・モノ・IoT”といった多主体環境においては、それだけでは不十分である。

特に IoT や AI プロセス(AI エージェント)など「非人間エンティティ」には、デバイス単位のデジタル証明(Device Attestation)やセキュアエレメントを用いた FIDO2 準拠の認証器が必要である。これらの方式は、公開鍵暗号をベースで、より軽量で分散的な信頼モデルを提供し、オンライン上での相互認証・ハードウェア署名・セキュアブート検証を自律的に実施可能である。

したがって、現代の ICAM 設計においては以下の組み合わせが推奨される。

・PKI による証明書ベースの信頼を基盤

・FIDO2、WebAuthn、Device Identity Attestation

・ゼロトラスト連携による継続的認証監視(マルチレイヤ型の統合認証アーキテクチャ)

SIOTP 協議会では、マルチレイヤ型の統合認証アーキテクチャに関するこれらの観点を、推進していく所存である。

Copyright 2025 Secure IoT Platform Consortium

② 重要インフラ/サプライチェーンに対するセキュリティ対策と ICAM

NDAA では、国家安全保障の観点において、防衛案件のみならず、特にセキュリティ対策が重視される重要インフラやハードウェア/ソフトウェア/通信/契約/研究開発/データアクセスを含む総合的なサプライチェーンに対する情報保全が求められている。

米国国防権限法(NDAA) 2025

2025 年に発布された NDAA では、国家安全保障の基盤として、重要インフラおよび防衛産業基盤を含むサプライチェーン全体のレジリエンス強化を制度化。敵対国に依存しない調達体制の確立し、産業基盤・サプライチェーンのあらゆる段階で外国の影響を排除することを政策目標として明記されている。これに基づき連邦調達や契約におけるセキュリティ要求事項が強化されている。

例えばサプライチェーンでは、モノの流れだけではなく、情報/資格/人材/アクセス権を含む複合的に統制する形式が必要だと考えられ、重要インフラ、サプライチェーン保護の観点においては、前述の ICAM のフレームワークを基盤とするが重要となってきている。これにより人・モノ・AI システムなどあらゆる主体のアクセスをゼロトラスト原則で統制することが不可欠となる。

この流れは米国内だけではなく我が国においてもその対応が迫られているところである。

国防省セキュリティ能力成熟度モデル(CMMC)

米国国防総省(DoD)では、防衛サプライチェーン全体のサイバーセキュリティ強化を目的とした認証フレームワークとしてセキュリティ能力成熟度モデル(CMMC: Cybersecurity Maturity Model Certification)を導入。2025 年 9 月の最終規則(48 CFR 改正)により契約条項として義務化可能となり、2025 年 11 月 10 日から新規契約における CMMC 条項の適用が開始される。これは単なる準拠義務化ではなく、認証(資格)保持が契約受注の有力な前提条件となり、上位契約者から下請けへの同一サイバー要件(flow-down)の適用が本格化することが想定される。

③ 日本版セキュリティクリアランス制度

政府が保有する安全保障上重要な情報として指定された情報に対し、アクセスする必要がある者のうち、情報を漏らすおそれがないという信頼性を確認した者の中で取り扱うとする施策として、セキュリティクリアランス制度が制定されている。

我が国においても、国家安全保障上の秘密保持を規定した従来の「特定秘密保護法」に加えて、経済安全保障の文脈中で民間の持つ技術情報も対象とした「重要経済安保情報保護活用法」が 2025 年 5 月 16 日に施行された。

それにより以下の点が定義されることとなった。

・「経済安全保障情報」保護枠組みの創設
・企業や研究機関を含む対象の拡張
・防衛装備移転や共同研究との連携
・米欧との相互運用性の確保

<u>セキュリティクリアランス対象企業</u>

セキュリティクリアランス制度の対象企業は、重要経済安保情報にアクセスする必要がある民間企業。具体的には、電力、通信、鉄道、金融などの重要インフラ事業者や、半導体、AI、量子、バイオテクノロジーなどの重要物資/先端技術を扱う企業、そしてそれらを取り扱うサプライチェーン関連企業が想定される。

また重要物資のサプライチェーンに関わる企業、サイバー攻撃への防御策など、セキュリティ関連企業も含まれると考えられる。

また適合事業者の認定においては、当該企業の意思決定に外国の所有/支配/影響がないかを確認されることも重要な点である。

<u>欧米との連携と課題</u>

前述の ICAM を考慮すると、米国をはじめとする各国との連携が極めて重要な事項であり、重要経済安全情報を取り扱うためには、厳格な情報セキュリティマネジメントを実装するために、米国の CMMC や SP800 シリーズとの整合性を意識したガバナンスへの準拠を検討すべきだと考えられる。

企業は ICAM やゼロトラストアーキテクチャ によるアクセス制御を導入することにより、日米・欧州間の相互信頼を確立し、安全保障上の共同研究や技術移転を円滑化できるようになる。

一方で、日本企業が CMMC 準拠を進める際に、「個人情報保護法による常時モニタリング制限」、「労働法・雇用均等待遇規制による背景調査の制約」や「外為法や経済安保法による国外監査データ移転制限」などの課題が発生する可能性がある。

これらの課題に対しては、「本人同意の確保」、「匿名性の実施」、「法的透明性の担保」など運用上の調和が求められる。

Copyright 2025 Secure IoT Platform Consortium

また防衛、政府、企業間連携では、閉域環境ではなくパブリッククラウド環境での情報共有が基本となることを前提に、ICAM とセキュリティクリアランス制度の導入に向けて、適切な技術要件と運用モデルを考えることが必要である。ここでは ICAM 設計を説明する際に前述した、以下の要件を組み合わせたマルチレイヤ型の統合認証アーキテクチャの構築が推奨されることをあらためて記述する。

・PKI による証明書ベースの信頼を基盤
・FIDO2、WebAuthn、Device Identity Attestation
・ゼロトラスト連携による継続的認証監視

まとめ

ここまで説明してきたように、米国をはじめとするグローバルな動向に対応し、日本の産業界においても以下に備えることが重要である。

① ICAM 対応(ID/アクセス管理の高度化)
・多要素認証(MFA)/デジタル証明書/ゼロトラストインフラへの対応
・国際セキュリティ基準(CMMC、NIST SP シリーズ)への準拠
② セキュリティクリアランス制度への対応
・契約/共同研究/入札の要件化
・特定社員への制度対応が必須に

産業界全体で標準化・教育・評価体制を整備し、ICAM とセキュリティクリアランスへの対応によるゼロトラストレディな産業基盤の構築を進めることを強く提案する。
これらの対応は重要インフラを中心としたグローバルサプライチェーンに参加するための共通基盤要件であり参入条件になることが予想される。
そのためこの要件に対応できない国内企業は、国際的な契約・研究・調達プロジェクトから排除されることを十分に認識し、早急に業界団体一丸となって準備を始めることを提案する。

Copyright 2025 Secure IoT Platform Consortium