ICSCoE TLP: WHITE

ゼロトラスト導入指南書

～情報系・制御系システムへのゼロトラスト導入～

2021 年 6 月
独立行政法人　情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム　４期生
ゼロトラストプロジェクト

はじめに

近年，新型コロナウイルス感染症（COVID-19)の蔓延によるリモートワーク利用の加速化やクラウド活用の増加により，社外から社内システムに接続する機会が増えてきている。

現状のセキュリティ対策は，境界型防御が主流であり，社内を信用できる領域，社外を信用できない領域として外部からの接続を遮断している。しかし，上記の社会変化から，社内のシステム環境へ社外から接続するということが行われていることから，境界型防御で考えていたセキュリティモデルではサイバー攻撃の脅威を防ぎきれない状況になってきている。

また，標的型メールによる社内端末のウイルス感染の事象も増加しているなど，社内が信用できる領域として考えることが困難な状況となってきている。

これらに対するセキュリティ対策として，「ゼロトラスト」という概念が提唱されている。これは，社内外すべてを信用できない領域として，全ての通信を検知し認証を行うという考え方であり，ゼロトラストを完全に導入すれば境界型防御をなくすことができるという考えもある。

しかし，ゼロトラストを導入しようと調査を進めると，多種多様な説明からはじまり，多数の文献，製品，機能などがあり，実際どのように検討し導入していけば良いのか，また導入することでどのようなメリット・デメリットがあるのか，境界型防御との相違点についてわからないのが現状である。

今回，上記の課題を解決すべく，「ゼロトラスト」を言葉で捉えるのではなく，文献調査を行うとともに，調査で抽出した技術要素の機能調査，機能検証を実施した。また，現在ゼロトラストを導入している企業についても調査し，実際の構築手順の情報や構築における課題等を事前に収集することで，機能検証を行う際の参考とした。加えて，境界型防御との相違点を検証の中で考察し，境界型防御とゼロトラストの機能を融合したハイブリット・セキュリティの考え方をまとめた。

また，一般的にはゼロトラストは情報系システムへの導入を前提として考えられており，制御系システムへの導入は難しい（メリットがない）と思われている。しかし，制御系システムについても，IoT 機器やクラウドなど，情報系システムとの接続要件が出てきていることから，ゼロトラストの導入を有効と考え，制御系システムへの導入検証および考察も実施した。

本書は，実際にゼロトラストを会社に導入していく際の手助けとなる「指南書」として，上記の内容をまとめる。

目次

1．本指南書の説明

1.1.　本指南書の目的

本書では，ゼロトラスト導入指南書として，自社でゼロトラストの導入を検討する担当者を対象に，導入検討や製品選定等を進める上での注意事項等をまとめた。導入検討の際の参考資料として活用することを目的としている。

なお，本書を利用するにあたって前提知識として，“情報処理技術者試験(IT　パスポート試験)の合格程度の水準”の知識が必要となる。

1.2.　本指南書の構成

1章 「本指南書の説明」では，指南書の目的や用語の定義および本書の免責事項について記載する。

2章 「ゼロトラストの概要」では，ゼロトラストに関係する文献の内容をもとに，ゼロトラストの歴史や基本的な考え方を説明する。

3章 「ゼロトラストの構成要素」では，ゼロトラストに用いられる技術要素の種類と各技術要素の機能を説明する。

4章 「ゼロトラストのモデルケース」では，今回検証した各ユースケースの説明および検証内容，検証で得た気づきを説明する。

5章 「制御系システムへのゼロトラスト導入検証」では，制御系システムへのゼロトラスト導入について検証と考察を行った結果を説明する。

6章 「導入方法」では，実際にゼロトラスト機能を実装する方法とそれに伴う費用を説明する。

7章 「境界型防御との共存」では，境界型防御の利点とゼロトラストの利点から，各脅威に対して，どのように組み合わせが良いか，考察した内容を説明する。また，境界型防御も含めた技術要素について，NIST サイバーセキュリティフレームワーク（以下，CSF という。）との対応についても記載する。

8章 「ゼロトラスト導入における運用上の注意」では，ゼロトラスト導入時および導入後に発生するシステム運用における注意事項を説明する。

9章 「まとめ」では，本指南書の内容をまとめ，説明する。

1.3. 用語の定義

本書に記載する各用語は，以下のとおりとする。

- ゼロトラスト

  ネットワークが侵害されている場合であっても，情報システムやサービスにおいて，各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体のことをいう。すべてを信用しないということではなく，すべて確認するということを表す。

- ゼロトラスト・アーキテクチャ

  ゼロトラストの概念を利用し，コンポーネントの関係，ワークフロー計画，アクセスポリシー等を含むサイバーセキュリティ計画のことをいう。

- 指南書

  言葉の意味としては，武術・芸能などを教え示すことをいう。本書では，ゼロトラストを導入するための参考書の扱いとする。

- 認証

  対象の真正性を確認する行為のことをいう。IT システムでの認証においては，一般的に ID とパスワードによる本人確認が用いられることが多く，それに加え，ゼロトラストでは認証をより厳重にするため，多要素認証や端末情報などの追加要素を用いることが望ましいとされる。

- 認可

  対象が権限を持っているかを確認する行為のことをいう。ゼロトラストでは，システム等に対して事前にアクセス権を付与しておく静的な認可に加え，ユーザーの振る舞い等により動的にアクセス可能なリソースを変更する，動的な認可についての実装が望ましいとされる。

- 信用度レベル

  ユーザやデバイスなどの資産自体の脅威の度合いのことをいう。ゼロトラストの認証・認可はこのレベルを元に実施する。例えば，不審な挙動等を行った場合，レベルが下がり（脅威は上がる）認証が厳しくなる。

1.4. 免責事項

- このドキュメントは単に情報として提供され，内容は予告なしに変更される場合がある。
- 発行元の許可なく，本書の記載内容を複写，転載することを禁止する。
- このドキュメントに誤りが無いことの保証や，商品性又は特定目的への適合性の黙示的な保証や条件を含め明示的又は黙示的な保証や条件は一切無いものとする。
- 本書に記載の内容は，独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく，作成者の見解に基づいている。
- 本書の利用によるトラブルに対し，本書作成者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は，発行日から2年間とする。

1.5. 商標登録

- Microsoft，Windows，Azure，Azure AD，Active Directory は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標である。
- AWS，AWS DS は，米国 Amazon.com,Inc.の米国およびその他の国における登録商標または商標である。

2. ゼロトラストの概要

2.1. ゼロトラストの歴史

ゼロトラストという概念は，「ゼロトラスト」という言葉が生まれる前から，サイバーセキュリティの考え方としてあった。以下に，ゼロトラスト提唱までの歴史を記載する。直近では，NIST SP800-207 が発行され，基本的な考えが整理された。

表 2-1 ゼロトラストの歴史

年代	内容
2004 年以前	アメリカの国防情報システム庁（DISA）と国防総省は「ブラックコア」と呼ばれる安全な組織戦略に関する研究を発表した
2004 年	国際標準化グループとして Jericho Forum（ジェリコ・フォーラム）を正式に設立し「非境界化」問題の解決に注力する
2010 年	Forrester Research（フォレスター・リサーチ）社の John Kindervag（ジョン・キンダーバーグ）氏よりインフラから信用を取り除くことを行うことを前提とした考え方である「ゼロトラスト」を提唱した。 提唱内容：「誰も（ユーザー），どこも（ネットワーク），何も（デバイス）信用せず，アクセスごとに必ず安全性を確認する」
2017 年	Gartner（ガートナー）社，CARTA フレームワークを提唱。「継続的かつ動的なリスクや信用の評価」（信用性の高・低によって，情報システムへの接続に必要な手順を変える）
2018 年	Forrester Research（フォレスター・リサーチ）社，ZTX（Zero Trust eXtended）フレームワークを提唱。「相互に関係する7領域のセキュリティ製品やソリューションを組合せる」
2020 年	NIST SP800-207 発行，ゼロトラストアーキテクチャ 「ゼロトラストの基本的な考え方を整理（2020 年 8 月発行）」

2.2. ゼロトラストに関する文献

ゼロトラストに関する文献は数多く，様々な内容の記載がある。本指南書では，実際に文献を読み，参考となる代表的な文献とその概要を表 2-2 に記す。

No.①については，グローバルスタンダードとなる資料である。また，No.②については，公式見解ではないものの，国の考え方が組み込まれている資料である。

加えて，No.⑤のゼロトラスト大全には，実際にゼロトラストを導入している企業の情報が記載されている資料である。

表 2-2 ゼロトラストに関する文献例

No.	調査対象	文献の概要
①	NIST SP800-207 （Zero Trust Architecture：英語）	• ゼロトラストの基礎知識 • ゼロトラストの導入検討手順の概要
②	政府 CIO 補佐官等ディスカッションペーパー （政府情報システムにおけるゼロトラスト適用に向けた考え方）	• ゼロトラストに対する政府の考え • 問題意識・方向性の記載 （政府の公式見解ではない）
③	ゼロトラストネットワーク （O’REILLY・ジャパン）	• 技術的（専門的）な信用・信用の考え方 • 認証・認可ポリシー設定の考え方
④	IIJ 刊行雑誌 ZT 特集	• ゼロトラストを図や絵を用いて説明 • 各情報の抜粋版
⑤	ゼロトラスト大全 （日経 BP ムック）	• ゼロトラスト構成の概要説明（図・表） • 各社導入事例

2.3. ゼロトラストの基本的な考え方

ゼロトラストの基本的な考え方として，NIST SP800-207 に以下の 7 つの考え方の記載がある。考え方の解説を，表 2-3 に記す。

ゼロトラストでは，すべてを信用しないという表現がよくされるが，実際は，全てのデバイス，ユーザ，通信，ネットワークを監視し，認証・認可を行うこととしている。そして，これらの監視に加えて，No.4 の記載にあるとおり，動的ポリシーという信用度レベルで評価する仕組みを導入し，信用度レベルの低い（怪しい行動をしている）通信に対しては，認可させないこととしている。これは，人の作業でいうと，常に確認作業を行うということである。動的ポリシーについては，普段から素行が悪く，信用できない相手に対して，チェックを厳しくするのと同じ考えである（イメージは図 2-1 参照）。

表 2-3 NIST SP800-207 ゼロトラスト・アーキテクチャーの基本的な考え方

No.	基本的な7つの考え方
1	すべてのデータソースとコンピューティングサービスをリソースとみなす
2	ネットワークの場所に関係なく，すべての通信を保護する
3	企業リソースへのアクセスをセッション単位で付与する
4	リソースへのアクセスは，クライアントアイデンティティ，アプリケーション/サービス，リクエストする資産の状態，その他の行動属性や環境属性を含めた動的ポリシーにより決定する
5	すべての資産の整合性とセキュリティ動作を監視し，測定する
6	すべてのリソースの認証と認可を行い，アクセスが許可される前に厳格に実施する
7	資産，ネットワークのインフラストラクチャ，通信の現状について可能な限り多くの情報を収集し，セキュリティ体制の改善に利用する

＜認証イメージ＞

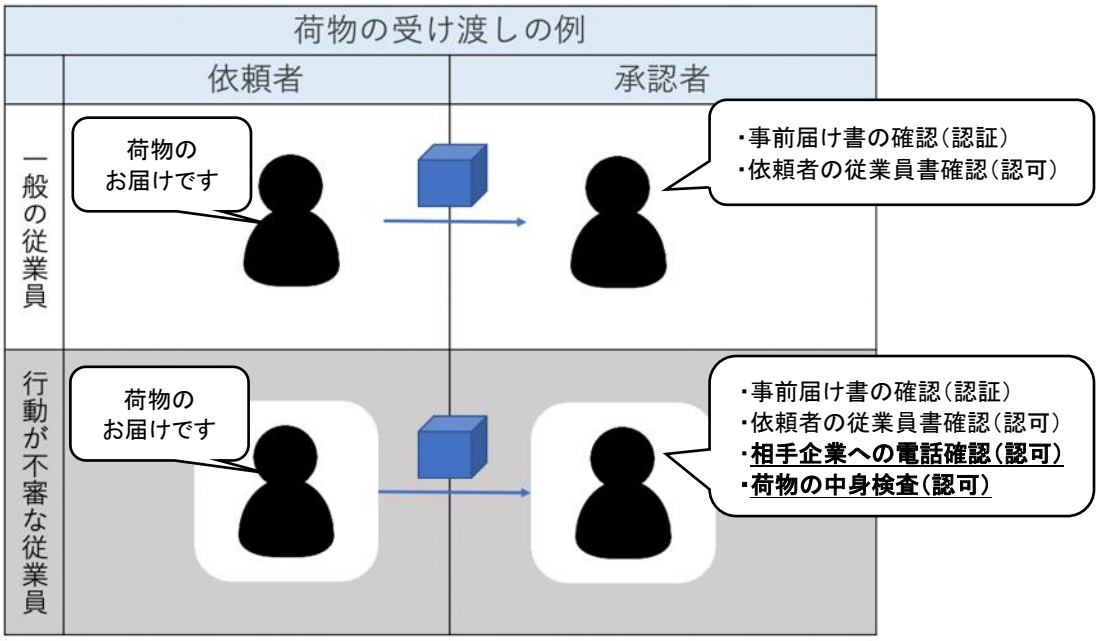


図 2-1 ゼロトラスト認証イメージ（複数チェック/不審人物にはチェックを強化）

（参考：NIST SP800-207 翻訳版）

1. **すべてのデータソースとコンピューテイングサービスをリソースとみなす**

　ネットワークは，複数のクラスのデバイスで構成されている場合がある。ネットワークに，アグリゲータ/ストレージにデータを送信する小さいデバイス，SaaS，アクチュエータに命令を送信するシステム，およびその他の機能がある場合もある。また，企業が所有するリソースにアクセスできる場合，個人所有のデバイスをリソースとして分類することも考えられる。

2. **ネットワークの場所に関係なく，すべての通信を保護する**

　ネットワークの場所だけでは信用を意味するものではない。企業所有のネットワークインフラストラクチャ上にある資産（例:レガシーネットワーク境界内）からのアクセスリクエストは，企業所有でない他のネットワークからのアクセスリクエストや通信と同じセキュリティ要件を満たす必要がある。言い換えれば，デバイスが企業所有のネットワークインフラストラクチャ上にあるからといって，自動的に信用が付与されるべきではない。すべての通信は，機密性と完全性を保護し，アクセス元に対する認証を提供し利用可能な最も安全な方法で行われる必要がある。

3. **企業リソースへのアクセスをセッション単位で付与する**

　アクセスが許可される前に，アクセス元の信用性が評価される。また，アクセスは，タスクを完了するために必要な最小限の権限で付与されるべきである。これは，この特定のトランザクションについては「最新のいつか」という意味でしかなく，セッションを開始する前，またはリソースとのトランザクションを実行する前に直接発生しない場合もある。しかし，あるリソースへの認証と認可が自動的に別のリソースへのアクセスを許可するわけではない。

4. **リソースへのアクセスは，クライアントアイデンティティ，アプリケーション/サービス，リクエストする資産の状態，その他の行動属性や環境属性を含めた動的ポリシーにより決定する**

　組織は，どのようなリソースを持っているか，そのメンバーが誰であるか（またはコミュニティにおけるユーザに関する認証），およびそれらのメンバーが必要とするリソースへのアクセスを定義することで，リソースを保護する。ゼロトラストの場合，クライアントアイデンティティには， ユーザアカウント（またはサービスアイデンティティ）と，企業がそのアカウントに割り当てた関連属性，または自動化されたタスクを認証するための機能を含めることができる。リクエストする資産の状態には，インストールされているソフトウェアのバージョン，ネットワークの場所，リクエストの日時，以前に観察された動作，インストールされているクレデンシャル等のデバイスの特性を含めることができる。行動属性には，自動化された主体の分析，デバイスの分析，および観察された使用パターンからの測定された逸脱が含まれるが，これらに限定されない。ポリシーとは，組織が主体，データ資産，またはアプリケーションに割り当てる属性に基づくアクセスルールのセットである。環境属性には，アクセス元のネットワークの場所，時間，報告されたアクティブな攻撃等が含まれる。これらのルールと属性は，ビジネスプロセスのニーズと許容可能なリスクレベルに基づいている。リソースのアクセスとアクションの許可ポリシーは，リソース/データの機密性に基づいて変化する。最小特権の原則により，可視性とアクセス性の観点から制限する。

5. **すべての資産の整合性とセキュリティ動作を監視し，測定する**

資産は本質的に信用されない。企業は，リソースへのリクエストを評価する際に，資産に対し実施されているセキュリティ態勢を考慮する。Zero Trust Architecture（ZTA）を実装する企業は，デバイスやアプリケーションの状態を監視するために，継続的診断および対策（CDM）または同様のシステムを確立し，必要に応じてパッチを当て，修正する必要がある。侵害されていることが判明した既知の脆弱性を有する資産，および企業が管理していない資産は，最も安全な状態にあると考えられる企業が所有している，または企業に関連するデバイスとは異なる扱い（企業リソースへのすべての接続を拒否することを含む）を受ける可能性がある。これは，一部のリソースへのアクセスが許可されていても，他のリソースへのアクセスが許可されていない関連デバイス（例:個人所有のデバイス）にも適用される可能性がある。この場合も，企業リソースの現在の状態に関する実用的なデータを提供するために，堅牢な監視および報告システムが必要となる。

6. **すべてのリソースの認証と認可を行い，アクセスが許可される前に厳格に実施する**

これは，アクセスを取得し，脅威をスキャンして評価/適応し，継続的なコミュニケーションの中で信用を継続的に再評価するという一定のサイクルである。ZTA を導入する企業は，Identity Credential and Access Management（ICAM）と資産管理システムを導入することが推奨される。これには，一部またはすべての企業リソースへのアクセスに多要素認証（MFA）を使用することも含まれる。セキュリティ，可用性，ユーザビリティ，およびコスト効率のバランスを達成するポリシー（例:時間ベース，新規リソースのリクエスト，リソースの変更，主体の異常な活動の検出）によって定義し，再認証および再認証の可能性を伴う継続的な監視をユーザトランザクション全体にわたって実施する。

7. **資産，ネットワークのインフラストラクチャ，通信の現状について可能な限り多くの情報を収集し，セキュリティ体制の改善に利用する**

企業は，資産に対するセキュリティ態勢，ネットワークトラフィック，アクセスリクエストに関するデータを収集し，そのデータを処理し，得られた洞察をポリシーの作成と実施を改善するために使用するべきである。このデータは，主体からのアクセスリクエストのコンテキストを提供するためにも使用できる。

2.4. ゼロトラスト・アーキテクチャ構築時の前提条件

ゼロトラスト・アーキテクチャを構築するにあたり，ネットワーク接続に関する基本的な前提条件がある。これらの前提条件の一部は，企業が所有するネットワークインフラストラクチャに適用され，一部は非企業所有のネットワークインフラストラクチャ（例:公衆 Wi-Fi または公衆クラウドプロバイダ）に適用される。ゼロトラストを実装する企業のネットワークは，2.3 節で概説した原則と，以下の前提条件に基づいて構築する必要がある。

表 2-4 NIST SP800-207 ゼロトラスト・アーキテクチャのネットワーク構成における前提条件

No.	ネットワーク構築時の6つの条件
1	企業のプライベートネットワークは，暗黙のトラストゾーンとみなさない
2	ネットワーク上のデバイスは，企業が所有していないか，構成可能なものではない場合がある
3	どんなリソースも本質的に信用されるものではない
4	すべての企業リソースが企業のインフラストラクチャ上にあるわけではない
5	リモートの企業主体と資産は，ローカルネットワークの接続を完全に信用できない
6	企業のインフラストラクチャと非企業のインフラストラクチャとの間で移動する資産とワークフローには，一貫したセキュリティポリシーが必要

（参考：NIST SP800-207 翻訳版）

1. **企業のプライベートネットワークは，暗黙のトラストゾーンとみなさない**

   資産は常に攻撃者が企業ネットワーク上に存在すると考えるべきであり，通信は利用可能な最も安全な方法で行われるべきである。これには，すべての接続を認証したり，すべてのトラフィックを暗号化したりすることが含まれる。

2. **ネットワーク上のデバイスは，企業が所有していないか，構成可能なものではない場合がある**

   社外の訪問者や契約サービスには，その役割を果たすためにネットワークアクセスを必要とする非企業所有の資産が含まれている場合がある。これには，企業主体が所有していないデバイスを使用して企業リソースにアクセスできるようにする BYOD（Bring Your Own Device）ポリシーが含まれる。

3. **どんなリソースも本質的に信用されるものではない**

   すべての資産は，企業が所有するリソースへのリクエストが許可される前に，PEP を通じてそのセキュリティ態勢を評価されなければならない（情報資産と主体については第 2.1 項 6 と同様）。この評価は，セッションが続く限り，継続的に行われるべきである。企業所有のデバイスは，認証を可能にし，非企業所有のデバイスから送られてくる同じリクエストよりも高い信用度を提供する成果物を持つかもしれない。企業リソースへの認証には，主体のクレデンシャルだけでは不十分である。

4. **すべての企業リソースが企業のインフラストラクチャ上にあるわけではない**

リソースには，クラウドサービスだけでなく，企業の外に存在する主体も含まれる。企業が所有または管理する資産は，基本的な接続性とネットワークサービス（例:DNS 解決）のためにローカル（すなわち，非企業）ネットワークを利用する必要がある場合がある。

5. **リモートの企業主体と資産は，ローカルネットワークの接続を完全に信用できない**

リモートの主体は，ローカル（すなわち，企業が所有しない）ネットワークが敵対的であると仮定し，資産は，すべてのトラフィックが監視され，変更される可能性があると仮定する必要がある。すべての接続リクエストは認証/承認されるべきであり，すべての通信は可能な限り最も安全な方法で行われるべきである（すなわち，機密性，完全性の保護，およびソース認証を提供する)。上記のZTA の原則を参照すること。

6. **企業のインフラストラクチャと非企業のインフラストラクチャとの間で移動する資産とワークフローには，一貫したセキュリティポリシーが必要**

資産およびワークロードが企業のインフラストラクチャを移動するときには，セキュリティ対策を維持する必要がある。これには，企業ネットワークから外部組織のネットワークに移動するデバイス（リモートユーザ等）も含まれる。また，オンプレミスのデータセンターから外部組織のクラウドインスタンスに移行するワークロードも含まれる。

2.5. 本指南書におけるゼロトラストの考え

ゼロトラストとそのネットワークについての基本的な考え方は，2.3 節および 2.4 節に記載したとおりであり，ゼロトラストとは，「すべて信用しない」ではなく，「すべてにおいて確認し認証・認可を行う」ということである。また，ゼロトラストは境界型防御で守ることが困難な脅威に対して適用する対策ではあるものの，「境界型防御を排除する考え」ではない。既存に用いられている境界型防御も活かすことで，より強固なセキュリティを構築できると考える。

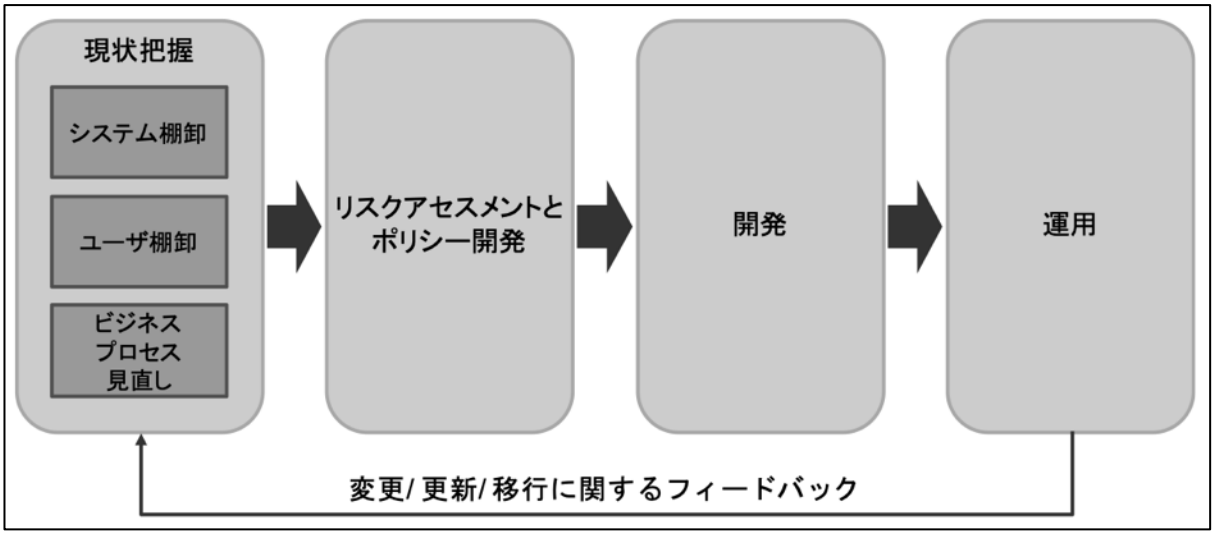
また，制御系システムにおいて，IoT 機器の普及やクラウドの利活用に伴い，情報系システムとの接続要望が増加してきている。ゼロトラストはクラウドの使用を基本とした考えであることから，制御系システムでのゼロトラストの活用は難しいとされてきたが，境界型防御での考え方が変わりつつあるという点では，制御系も同じであり，ゼロトラストは有効ではないかと考えられる。

これらを踏まえ，本指南書におけるゼロトラストの考えとして，境界型防御を活かし，すべてにおいて確認し，認証・認可を行う仕組みを用いた「ハイブリッド環境」を基準に考える。また，情報系と制御系の枠組みに囚われず，制御系システムに対してのゼロトラスト導入も視野に入れる。

2.6. ゼロトラスト導入に向けた進め方

ゼロトラストの導入プロセスについて，NIST SP800-207 を参考に，進め方を説明する。

まず，ゼロトラスト・アーキテクチャの移行には，資産（デバイスやネットワークなど），主体（ユーザ・権限など），ビジネスプロセスについて詳細に理解する必要がある。この知識が不十分だと，流れる通信をすべて確認できたとしても，承認する際に誤った判断をしてしまう。よって，導入する準備として，資産，主体，データフロー，ワークフローの調査を行う（図 2-2 現状把握）。現在の運用状況を把握していなければ，どのような新しいプロセスやシステムを導入する必要があるのかを判断することはできない。



出典：https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

図 2-2 ゼロトラスト・アーキテクチャ展開サイクル

準備の工程を実施した以降の進め方は，図 2-3 のプロセスで進めていく。

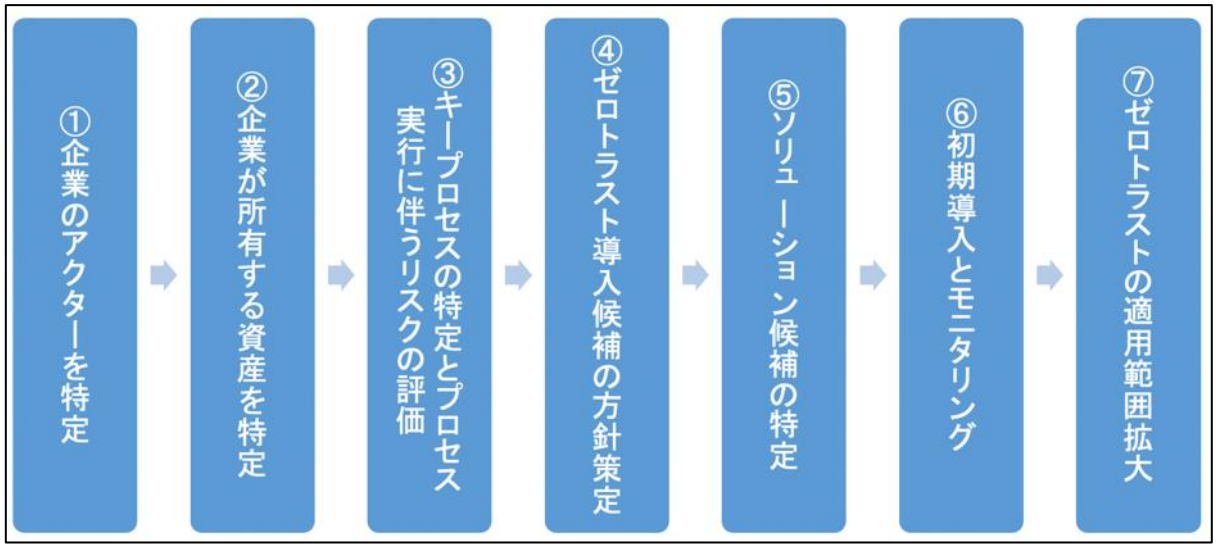


図 2-3 ゼロトラスト導入プロセス

各プロセスで実施すべき内容は，以下のとおり。

① 企業のアクターを特定

企業の主体には，単純なリソースと相互作用するサービスアカウントのような，ユーザに紐づいたアカウントとサービスに紐づいたアカウントの両方が含まれることがある。どのユーザにどのレベルの権限を与えるのかは精査が必要。基本的には，必要な対象に必要な権限だけ与えるという，最小権限の考え方で整理する。

② 企業が所有する資産を特定

ゼロトラスト・アーキテクチャは，デバイスを識別して管理する能力が必要であり，企業内のデバイスはもちろん，企業所有ではないデバイスについても識別し監視する能力が必要。よって，企業の情報にアクセスするデバイスについては，「シャドーIT」も含めて可能な限り資産化する必要がある。なお，企業によって可視化されているもの（例:MAC アドレス，IP アドレス）と，管理者のデータ入力による追加分も含まれる。

③ キープロセスの特定とプロセス実行に伴うリスクの評価

業務プロセス，データフロー，および組織のミッションにおけるそれらの関係（プロセス）を特定する。次に信用度レベルをつけ，ゼロトラストへ移行するプロセスを決める。認証・認可の判断を導入することによる失敗のリスクを考慮し，初めはビジネスインパクトの低いビジネスプロセスから開始するのが望ましい。ある程度，認証・認可の挙動を掴んでから，対象を広げていくことで，リスクマネジメントにつながる。

④　ゼロトラスト導入候補の方針策定

資産またはワークフローを特定したら，影響を受ける対象をすべて特定する（上流リソース（例:ID管理システム），下流リソース（例:セキュリティ監視），エンティティ（例:主体ユーザ））。次に，企業管理者は，候補となるビジネスプロセスで使用されるリソースの信用度レベルの重み（重要度)を決定する。それらを踏まえて，何を対象に，どこへゼロトラストの機能を導入するのかを決める。

⑤　ソリューション候補を特定

④で策定した内容をもとに，導入箇所に適するソリューションを検討する。ソリューションの内容については，3章に記載している。また，4，5章には，いくつかの展開モデルケース（ユースケース）を想定し検証した結果を記載している。これらを参考にし，必要なソリューションを選定する。

⑥　初期導入とモニタリング

初期導入時には，適用したポリシーや初期動作の確認を含め，監視モードで運用する（遮断はしない）ことが望ましい。

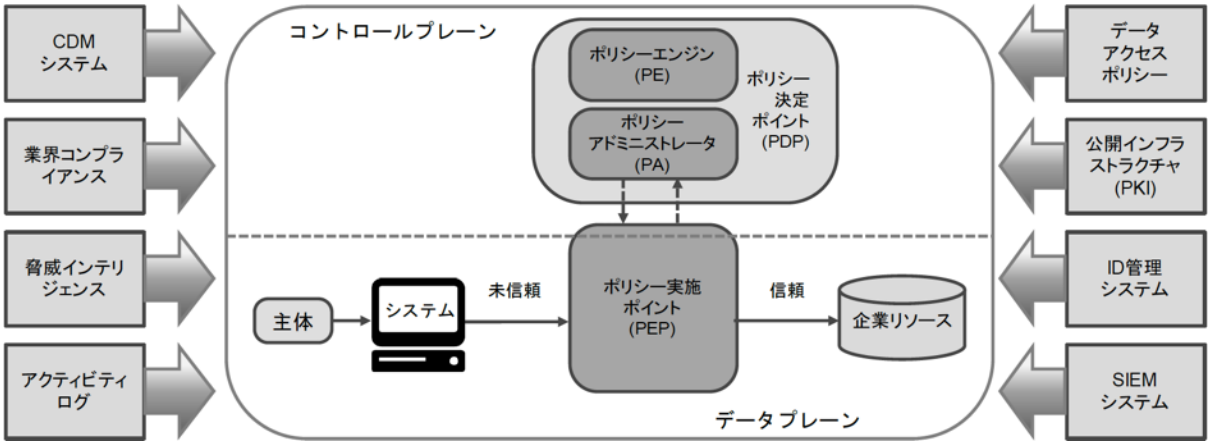
⑦　ゼロトラストの適用箇所拡大

運用フェーズに入ったら，ネットワークや資産の監視は継続し，トラフィックの記録を行う。これらを実施してく中で，ポリシーの変更や適用箇所の拡大を適宜実施していく。なお，ポリシー変更等を実施する場合は，深刻な問題にならないよう行う。

3. ゼロトラストの構成要素

3.1. ゼロトラストの基本概念

NIST(National Institute of Standards and Technology：米国国立標準技術研究所)は，ゼロトラストのアクセス制御システムを構成するための論理構成を提唱している【図 3-1 参照】。図 3-1 に示すように，ポリシーエンジン（PE：Policy Engine）とポリシーアドミニストレータ（PA：Policy Administrator）の要素で成り立っているポリシー決定ポイント（PDP：Policy Decision Point）とポリシー実施ポイント（Policy Enforcement Point）から構成されている。



出典：https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

図 3-1 論理コンポーネント（理想的なモデル）

- PDP(Policy Decision Point)：利用者（主体）からの企業リソースに対するアクセス要求を検証し，検証結果をポリシーに適用させることでアクセス許可の評価・判断を行う
- PE(Policy Engine)：アクセス要求の検証とポリシーの適用する
- PA(Policy Administrator)：PE の検証結果に基づいてアクセス許可否を PEP に連携する
- PEP(Policy Enforcement Point)：利用者からのアクセス要求を受け，PDP へ情報を流し，企業リソースへのアクセス制御を行う

3.2. 基本概念に基づくポイント

前項の基本概念に基づき企業にゼロトラスト製品を導入する際は，以下の 4 点を念頭に置く必要がある。

① 認証・認可
利用者を特定し，必要な企業リソース（データ）にアクセスするために必要最小限の権限を付与する。

② クラウド利用
オンプレミス・閉域網中心のネットワークを前提とした境界型防御設計を見直し，クラウド利用環境を想定したセキュリティ対策をする。

③ デバイスセキュリティ
近年，社外から利用するケースが増加しており，脅威にさらされやすくなった。デバイスがサイバー攻撃の踏み台となることを避けるため，デバイス毎に適切なセキュリティ対策をする。

④ ログ管理（ログの可視化）
サイバー攻撃が高度化しており，大量のログなどから脅威・脆弱性データを収集し，証跡を分析し，ログ監視による攻撃経路の特定・影響範囲の調査に必要となる。

3.3. ゼロトラスト構成要素（分類）

前項のポイントを踏まえた主なゼロトラスト構成要素（分類）を紹介する。

① CASB (Cloud Access Security Broker)
② CSPM (Cloud Security Posture Management)
③ EDR (Endpoint Detection and Response)
④ EMM (Enterprise Mobility Management)
⑤ IDaaS (Identity as a Service)
⑥ IRM（Information Rights Management）
⑦ SASE (Secure Access Service Edge)
⑧ SDP (Software Defined Perimeter)
⑨ SWG (Secure Web Gateway)
⑩ SOAR (Security Orchestration, Automation and Response)
⑪ UEBA (User and Entity Behavior Analytics)

① CASB（Cloud Access Security Broker：キャスビー）

CASB はガートナー社が 2012 年に提唱したコンセプトであり，その基本的な考え方は「利用者と複数のクラウドプロバイダーの間に単一のコントロールポイントを設け，そのポイントでクラウド利用の可視化や制御を行うことで，全体として一貫性のあるポリシーを適用できるようにする」という概念であり，CASB には大きく 4 つの機能がある。

【CASB の主な要素】

- 可視化：社内利用者がどのような SaaS を使っているのかを IT 管理者が監視できるようにする。
- データセキュリティ：アクセス権限の逸脱や機密情報の持ち出しをチェック／ブロックする。
- コンプライアンス：セキュリティに関する基準やポリシーを満たしていることを監査する。
- 脅威防御：セキュリティ脅威の検出／分析や防御を行う。

② CSPM（Cloud Security Posture Management：シーエスピーエム）

パブリッククラウド（IaaS，PaaS）に対して，セキュアな設定がなされていることを継続的に評価し，適切な設定への修正を支援するソリューションである。

クラウド側の設定を自動的に確認し，設定ミスや各種ガイドライン等への違反が無いかを継続してチェックすることができるものもある（アラート通知等有）。また，パブリッククラウドを利用する際のベストプラクティスをチェックルールとしてあらかじめ用意しているソリューションもあり，利用者へより安全な利用方法を提示してくれる。

③ EDR（Endpoint Detection and Response：イーディーアール）

エンドポイント（パソコン・サーバ・スマートデバイス等）の操作や動作の監視を行い，サイバー攻撃を受けたことを発見し次第対処するソリューションである。

【EDR の主な要素】

- サイバー攻撃，高度標的型攻撃（APT 攻撃）の兆候を検知する
- エンドポイントのログデータを解析し，相互の関連付けを行う
- リアルタイム監視（エンドポイントに影響を与えない，または最小限にする）
- アンチウイルスと連携する
- インシデントレスポンス（IR）とフォレンジック調査に利用できるよう可視化

【EPP との違い】

EPP（Endpoint Protection Platform）は，アンチウイルスソフトとも呼ばれている。エンドポイントにマルウェアなどが感染しないよう保護することを目的としたセキュリティ対策ツールの総称であり，従来から個人・企業等で広く利用されている。EDR に含まれているソリューションもある。

マルウェアに感染しないようにする EPP に対し，EDR はマルウェア侵入を許してしまった後の被害を抑えることを主目的としたセキュリティ対策である。

④ EMM（Enterprise Mobility Management：イーエムエム）

スマートフォンやタブレット等のモバイル端末を総合的に管理するツールのことである。ネットワークやセキュリティのポリシーに従った設定を行い，機能の有効化や，不要な機能の制限等を行える。また，端末紛失時の遠隔操作による端末ロックや端末内情報の削除，端末にインストールされているアプリケーションのリストの作成，利用者の勤怠情報等の把握等を行える製品もある。製品によっては，Windows10・macOS・iOS・Android 等様々な OS に対応している。

【EMM の主な要素】

- MDM（Mobile Device Management）
  スマートフォンやタブレット等を管理する端末管理に特化したソフトウェアのこと。
  - 端末を紛失時や盗難にあった場合，遠隔操作でロック，データ削除を行う
  - 使用するアプリの一括管理や OS のアップデートを行う
  - 端末を使用している利用者の管理を行う
- MAM（Mobile Application Management）
  アプリケーションを管理するソフトウェアのこと。
  - アプリケーションとデータを切り離して管理できる
  - 業務データと個人データ部分の分離できる
  - 業務データを個人データ領域へ移動する等のポリシー違反をブロックできる
- MCM（Mobile Contents Management）
  コンテンツを管理するソフトウェアのこと。
  - 安全な通信環境を構築し，端末から業務コンテンツにアクセス
  - 端末からのデータ閲覧は可能にするが，端末内への保存ができないように制御
  - 特定のコンテンツに対して，アクセス権限を管理

⑤　IDaaS（Identity as a Service：アイダース，アイディーアース）

クラウド上の様々なサービスの ID 管理を一元的に行うクラウドサービスのこと。SaaS（Software as a Service）等への認証（多要素認証，シングルサインオン）・認可（アクセスコントロール）・ID 管理・ID 連携を行う機能を有している。

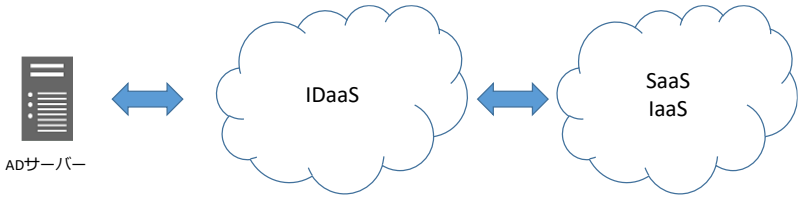


図 3-2 IDaaS イメージ

【IDaaS の主な要素】

- シングルサインオン（認証）

  一度メインの ID 管理システムへサインインすれば，他の複数のサービスやシステムへのサインインを自動で行ってくれる機能のこと。利用者は，サービス毎に ID・パスワードを入力する必要がなくなる。
- アクセスコントロール（認可）

  サービス・フォルダ等にアクセスが可能な利用者や端末，場所等に制限をかけ，管理者の許可を得た利用者のみがサービスを利用できるようにする。
- ID 管理

  アカウント作成や削除及び配属変更時の情報変更を一元管理が行えるサービス。アカウント情報をもつマスターシステムの情報を変更することによりシステム毎に情報を変更する必要がなくなる。

⑥　IRM（Information Rights Management：アイアールエム）

ファイルを暗号化した上で，利用者毎にアクセス権限を付与し管理する技術のこと。電子メールや文書，画像データ等のコンテンツを管理することで情報漏えいを防止することができる。

【IRM の主な要素】

- アクセス権限の制限

  ファイルが社内外のどこにあっても，権限を持つ利用者のみがファイルを開けるようにする。
- 操作権限の制限

  ファイルを開いた人の権限に応じて印刷，編集，コピー，保存等の操作を制限する。
- 参照期間の制限

  指定した時間が経過した後，または運用者が権限を削除した場合には即座にファイルを開けないようにする。

⑦ SASE (Secure Access Service Edge：サシー，サッシー)

ガートナー社は，セキュリティとネットワーク技術を単一のクラウドプラットフォームに集約し，安全かつ迅速なクラウドトランスフォーメーションを可能にするフレームワークと定義している。

つまり，通信が SaaS や IaaS 等に入る前にセキュリティ対策（CASB，SDP，SWG 等）を行ったり，WAN やインターネット等のネットワーク機能（CDN，SD-WAN 等）をクラウドから提供したりし，利用者は社内外の場所を問わず，SASE を経由してシステムをセキュアに利用できるセキュリティとネットワークのオールインワンサービスと言える。

⑧ SDP (Software Defined Perimeter：エスディーピー)

アクセスの境界線（Perimeter）をソフトウェア上で構築，集中的に制御し，アクセス制御に関わる設定を柔軟に動的に変更することにより安全にデータを転送する技術のこと。従来のファイアウォールの概念をソフトウェア上に持ち，利用者がどこにいても動的にアクセスを制御する。

通信の一例として，通信の接続元の端末に SDP のエージェント（兼ゲートウェイ）を導入し，SDP のコントローラがセキュアな VPN 接続を確立・通信許可等をソフトウェアが管理する。通信を開始したら，コントローラがアクセス可否を判断し，問題なければ接続先のネットワーク情報をエージェントへ伝える。コントローラとゲートウェイは別々で管理されているため，片方が侵害されても接続先への不正アクセスが許可されることはないのが特徴。

⑨ SWG (Secure Web Gateway：エスダブルジー)

外部への WEB アクセス等を安全に行うためのクラウド型プロキシのこと。アクセス先の URL や IP アドレスから安全性を確認・評価し，安全でないと評価された場合はアクセスを遮断する。（URL フィルタ，アプリケーションフィルタ，アンチウイルス，サンドボックス等をクラウド型で提供）

【SWG の主な要素】

- Web フィルタリング
  悪意のある Web ページをブロック
- DNS フィルタリング
  悪意のあるドメインをブロック
- データ漏洩防止（DLP）
  内側から外側に流れるデータを検査し機密データのパターンにマッチするとブロックしたり記録を残したりする機能
- マルウエア検出
  定義ファイルを使ってマルウェアを検出する
- 不正侵入防止
  自社開発のエンジン・シグネチャを使用
- 高度な脅威保護
  実行ファイルやドキュメントファイルをサンドボックスで不審な振る舞いがないか検査する
- SSL 復号
  SSL の暗号通信を復号して，通信パケットを詳細に分析する

⑩ SOAR（Security Orchestration, Automation and Response：ソアー）

セキュリティ運用の連携及び自動化・効率化を行うための技術のこと。

【SOAR の主な要素】

- 脅威と脆弱性の管理（Orchestration：連携）
  情報収集，証跡管理等のインシデント対応に必要な記録を残す。
- セキュリティ運用の自動化（Automation：自動化）
  事前にルールや手順を定義し，一般的なタスクを自動化する。
- セキュリティ・インシデント対応（Response：対応）
  脅威に対する対応を計画，管理，調整，監視する方法のこと。

⑪ UEBA（User and Entity Behavior Analytics：ユーイービーエー）

ネットワーク内のユーザーやデバイスによる通常/異常な振る舞いをモデル化・分析，検知するサービスのこと。振る舞いを監視・学習・処理することで特定の行動や振る舞いがサイバー攻撃に至る可能性を評価する。

UEBA の分析イメージ例は以下のようになる。

図 3-3 は利用者の行動の積み重ねにより，リスクスコアが高くなるリスク値の算出方法の一例である。UEBA は日々のエージングにより，運用者の設定や設定のメンテナンス負担を軽減して，不審な活動を可視化する。

図 3-3 UEBA 分析イメージ

【UEBA と SIEM の違い】

近年，SIEM（Security Information and Event Management）は，SOC（Security Operation Center）に必要不可欠なセキュリティ製品となってきた。SIEM は多くのエンタープライズシステムやその他のセキュリティツールと連動して企業全体のセキュリティログとイベントをすべて収集し，これらのイベントを分析して，セキュリティチーム向けのアラートを生成する。

不審な活動の分析という点では，SIEM も不審な行動を可視化する機能を備えているが，UEBA は複雑な分析ロジックを用いて大量のデータを分析することを前提に設計されているため，ユーザーやデバイスの不審な行動の可視化に特化した分析に優位性がある。ただし，SIEM との連携は必要不可欠と考える（図 3-4）。

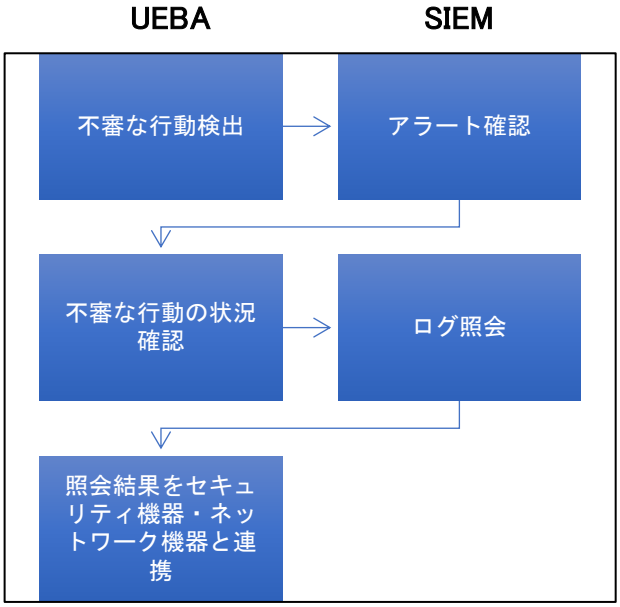


図 3-4 UEBA と SIEM の連携

4. ゼロトラストのモデルケース

4.1. モデルケースを用いた検証について

本プロジェクトでは境界型防御とクラウドの共存（ハイブリッド）を考慮したゼロトラストの検証を行った。ハイブリッド環境での検証を行うため，オンプレミス環境とクラウド環境をそれぞれ構築した(図 4-1)。

ゼロトラストの最終形は，境界型防御を無くした1対1の通信ではあるが，企業に導入していく場合，境界型防御の中に構築していくこととなる。ついては，境界型防御を活用しつつゼロトラストの要素を導入していくため，スモールスタートを考慮した検証を行うこととした。また，今回の検証では，複数社のソリューションを用いた。

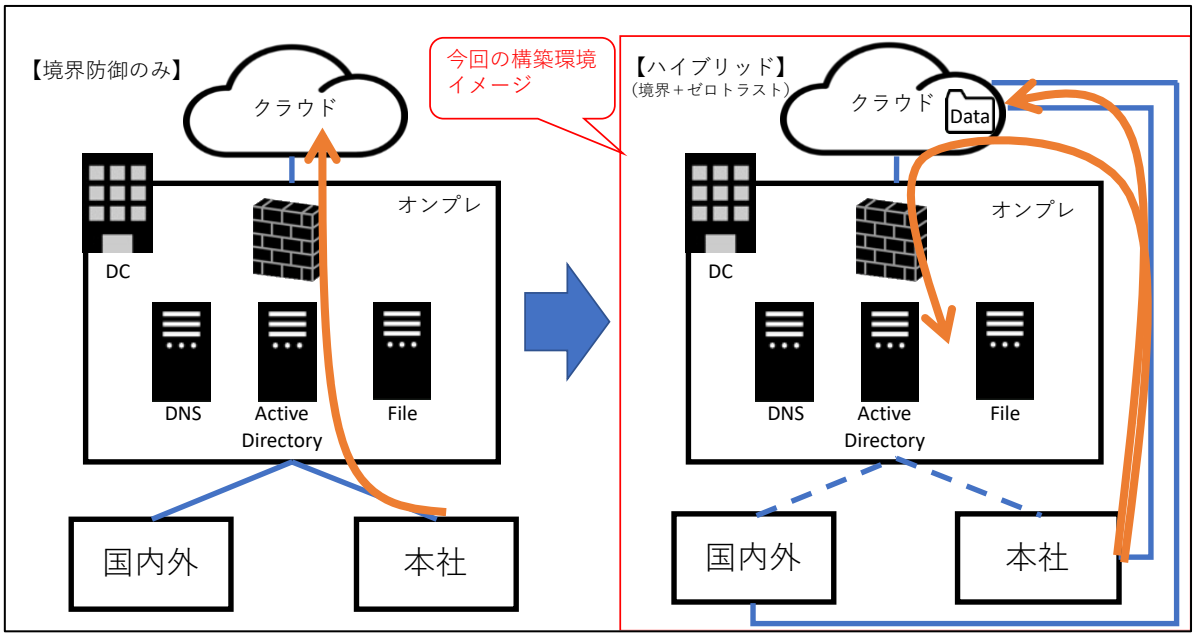


図 4-1 境界型防御モデルとハイブリッドモデル

4.2. モデルケースを用いた検証概要

前述で紹介した技術要素を用いてユースケース（基礎検証含む）を8つ抽出した(表 4-1)。

表 4-1 検証ユースケース

No	ユースケース	検証概要
0	基礎検証	ゼロトラストで考える基本的な挙動を確認した
A	社給端末による，社外からオンプレミス環境へのアクセス	クラウドやオンプレミス環境に社外から社給端末でアクセスした場合の検証
B	社内から機密情報の不正持ち出し（アップロード/ダウンロード）	機密情報を SaaS へアップロード/ダウンロードした場合の検証
C	BYOD（個人端末）による， 社外からクラウド環境へのアクセス	クラウド環境に社外から個人端末（モバイル含む）でアクセスした場合の検証
D	管理外端末（請負会社等）からの SaaS へのアクセス	SaaS に外部ユーザーが管理外端末でアクセスした場合の検証
E	クラウドの設定誤り防止	クラウドの設定誤り検知を CSPM で機能検証
F	SASE の機能検証	SASE 単体での検知・確認ができるのかの機能検証
G	制御系システムにおける，不正操作防止	認証機能がないシステムにどう認証させるか 制御信号を送る際の条件に応じた検知可否を検証

4.3. 各ユースケース検証結果について

4.3.1. ユースケース0（基礎検証）結果

以下のモデルケース環境にてゼロトラストの基本的な動きを確認するための簡易的な検証を実施した。

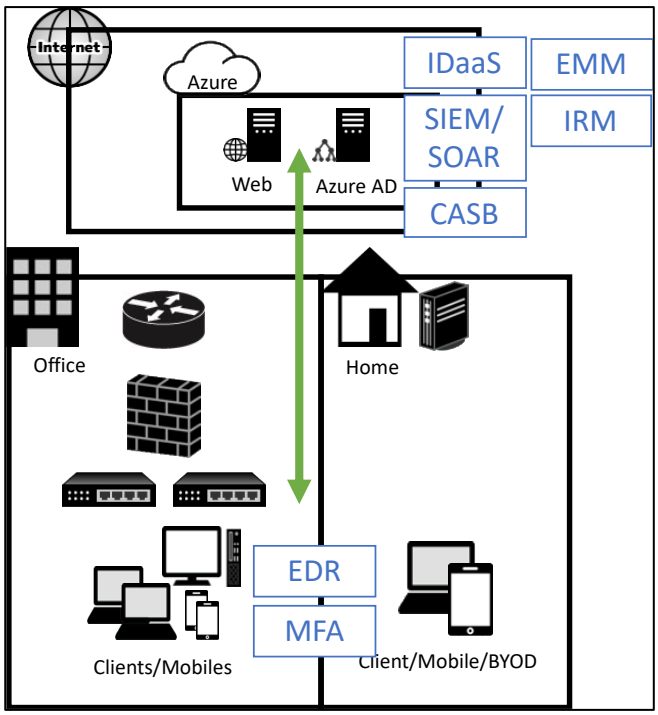


図 4-2 ユースケース0 モデルケース

表 4-2 ユースケースO検証内容

No	要素	検知	検証内容
1	CASB	異常系	突然のアクセス場所移動（海外回線からアクセス）を行い，振る舞い検知するか
2	IDaaS	正常系	モバイル端末が社外回線で企業クラウド環境へアクセスできるか
3	EDR	異常系	攻撃ツール（mimikaz）をダウンロード等で検知するか
4	EDR	異常系	攻撃ツール（Metasploit）をダウンロード等で検知するか
5	EDR	異常系	Zerologon（脆弱性）を検知するか
6	EDR	異常系	nmap（ネットワーク探知）を検知するか
7	EDR	異常系	telnet，リモートデスクトップ接続，PsExec を使用しサーバへアクセスする際，ログイン連続失敗を検知するか
8	EMM	異常系	攻撃者が遠隔操作で攻撃ツールをダウンロードできないようにする
9	IRM	異常系	社外秘ファイルをクラウドへアップロードできないようにする
10	IRM	異常系	社外秘ファイル（パスワード付き zip）をクラウドへアップロードできないようにする
11	MFA	異常系	EDR で検知したユーザーの危険度を上げ，多要素認証必須に変更できるか
12	SIEM	正常系	EDR で検知したアラートを SIEM に連携・記録できるか
13	SIEM/SOAR	異常系	（SIEM と SOAR の連携を検証） ログをトリガーに ID 管理システムのユーザー情報を自動で変更し，IDaaS を動的に変更できるか

【検証で得た気づき】

- クラウドに対して社内認証と同じレベルで社外認証を導入するには IDaaS が有効であることがわかった。
- 不審な行動（攻撃ツールのダウンロードなど）の検知を行うためには，デバイス管理ツールである EDR，EMM が有効であることがわかった。
- ユーザーの行動から，危険度をレベル分けすることで認証・認可の方法を変えるなどの振る舞い検知ツールの CASB，および MFA（多要素認証）による認証の追加が有効であることがわかった。
- EDR で端末の挙動を検知し，そのログを SIEM/SOAR と連携し，CASB の振る舞い検知を利用するなど，各機能を組み合わせることで，検知だけではなく，防御や対応等の複合的な対策ができる可能性があることがわかった。

4.3.2. ユースケース A について

No	ユースケース	検証概要
A	社給端末による，社外からオンプレミス環境へのアクセス	クラウドやオンプレミス環境に社外から社給端末でアクセスした場合の検証

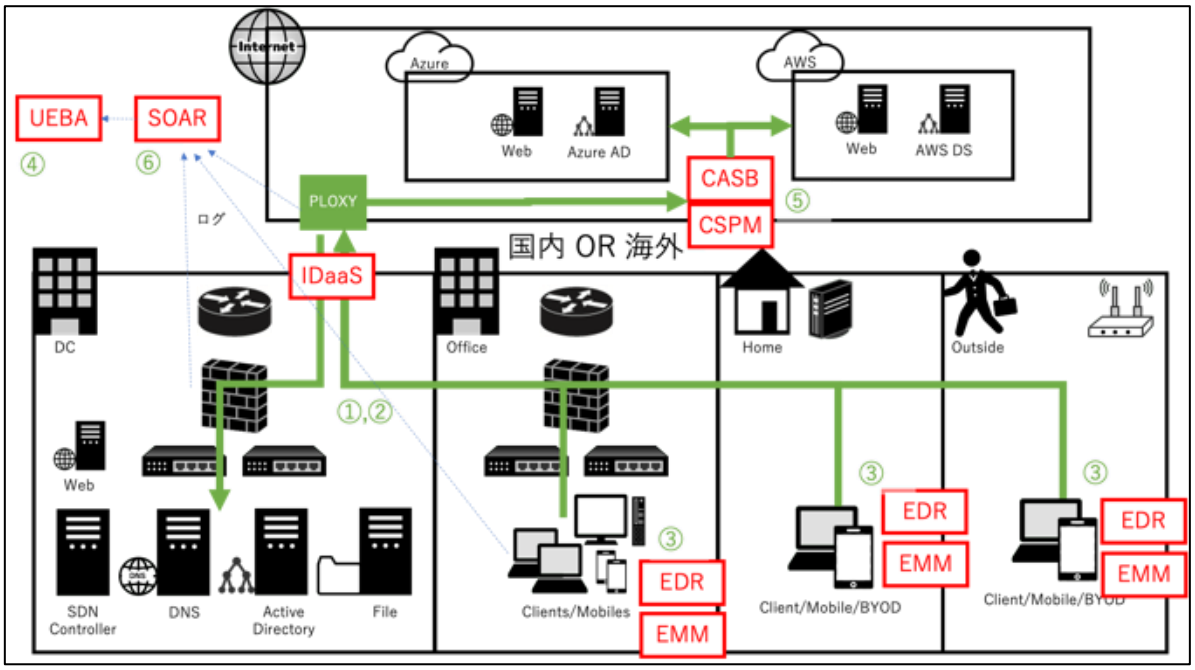


図 4-3 ユースケース A モデルケース

表 4-3 ユースケース A 検証内容

No	要素	検知	検証内容
1	IDaaS	異常系	22 時～5 時での不審なログインを検知する
2	IDaaS	異常系	22 時～5 時での不審なログインをブロックする
3	IDaaS	異常系	想定外の国からの不審なログインを検知する
4	IDaaS	異常系	想定外の国からの不審なログインをブロックする
5	IDaaS	異常系	想定外の IP からの不審なログインを検知する
6	IDaaS	異常系	想定外の IP からの不審なログインをブロックする
7	IDaaS	異常系	管理外端末からの不審なログインを検知する
8	SIEM	異常系	管理外端末からの不審なログインを検知する
9	IDaaS	異常系	管理外端末からの不審なログインをブロックする
103	EDR	異常系	不審なドメインに対しての接続を検知する
11	EDR	異常系	ファイルレスマルウェアの実行を検知する
12	SIEM	異常系	ファイルレスマルウェアの実行を検知する
13	SWG	正常系	社外からオンプレミス FS にアクセスする
14	EDR	異常系	端末のセキュリティ対策製品を無効化したことを検知する
15	EDR	正常系	遠隔で端末のデータ消去を行う
16	CASB	異常系	クラウド FS のデータが大量に連続印刷されることを検知，ブロックする
17	SIEM	異常系	クラウド FS のデータが大量に連続印刷されることを検知する
18	CASB	異常系	クラウド FS のデータが大量にダウンロードされることを検知，ブロックする
19	SIEM	異常系	クラウド FS のデータが大量にダウンロードされることを検知する

【検証で得た気づき】

- クラウドに対して社内外から同じレベルで認証するにあたり，IDaaS が有効であることがわかった。
- SIEM に関しては連携するログ数を選択しておくことでディスクの肥大化を防ぐことができる。
- クラウド製品の SIEM はオンプレミス製品よりログ連携が比較的簡単であることがわかった。

4.3.3. ユースケース B について

No	ユースケース	検証概要
B	社内から機密情報の不正持ち出し(アップロード/ダウンロード)	機密情報を SaaS へアップロード/ダウンロードした場合の検証

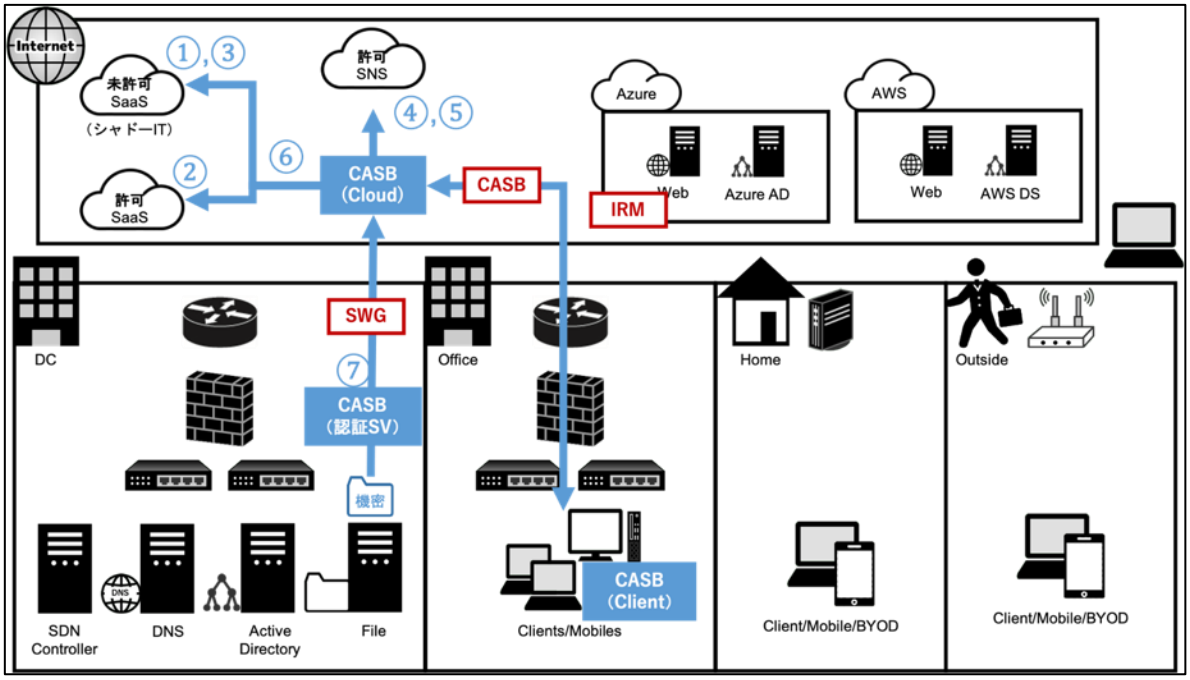


図 4-4 ユースケース B モデルケース

表 4-4 ユースケース B 検証内容

No	要素	検知	検証内容
1	CASB	異常系	ブラックリスト型制御ポリシー（未許可 SaaS へのアクセスを遮断）を適用，未許可 SaaS へのアクセスを遮断する
2	CASB	正常系	ホワイトリスト型制御ポリシー（全ての SaaS へのアクセスを遮断，許可 SaaS へのアクセスのみ許可）を適用，許可 SaaS へのアクセスを許可する
3	CASB	異常系	ホワイトリスト型制御ポリシー（全ての SaaS へのアクセスを遮断，許可 SaaS へのアクセスのみ許可）を適用，未許可 SaaS へのアクセスを遮断する
4	CASB	正常系	【許可 SNS へのアクセス許可】 SNS への操作制限ポリシー（全ての SNS に対して，投稿・アップロード等の操作を禁止，アクセスは許可）を適用，許可 SNS へのアクセスを許可する
5	CASB	異常系	【許可 SNS への投稿等操作遮断】 SNS への操作制限ポリシー（全ての SNS に対して，投稿・アップロード等の操作を禁止，アクセスは許可）を適用，許可 SNS への投稿操作を遮断する
6	CASB	異常系	DLP（Data Loss Prevention／情報漏洩対策）ポリシーを適用，以下の各形式の機密情報ファイル（フォルダ）のアップロードを遮断する ⅰ．機密情報ファイル ⅱ．機密情報，非機密情報を含むフォルダ ⅲ．機密情報，非機密情報を含む ZIP フォルダ ⅳ．機密情報，非機密情報を含むパスワード付き ZIP フォルダ
7	SWG CASB	異常系	オンプレミス環境内に CASB ベンダーから提供されている認証用サーバを構築 社内ネットワークからオンプレミスファイルサーバへのアクセス時に認証用サーバを経由するように設定を行い，社内ネットワークからオンプレミスファイルサーバへのアクセスを制御する

【検証で得た気づき】

- 機密情報の持ち出し対策には，CASB と DLP の組合せが有効であることがわかった。
- 境界型防御との共存（ハイブリッド）を実行するために，SWG と CASB を組み合わせることで，オンプレミス環境のデータ移動（アップロード／ダウンロード）制限に有効であることがわかった。

4.3.4. ユースケース C について

No	ユースケース	検証概要
C	BYOD（個人端末）による，社外からクラウド環境へのアクセス	クラウド環境に社外から個人端末（モバイル含む）でアクセスした場合の検証

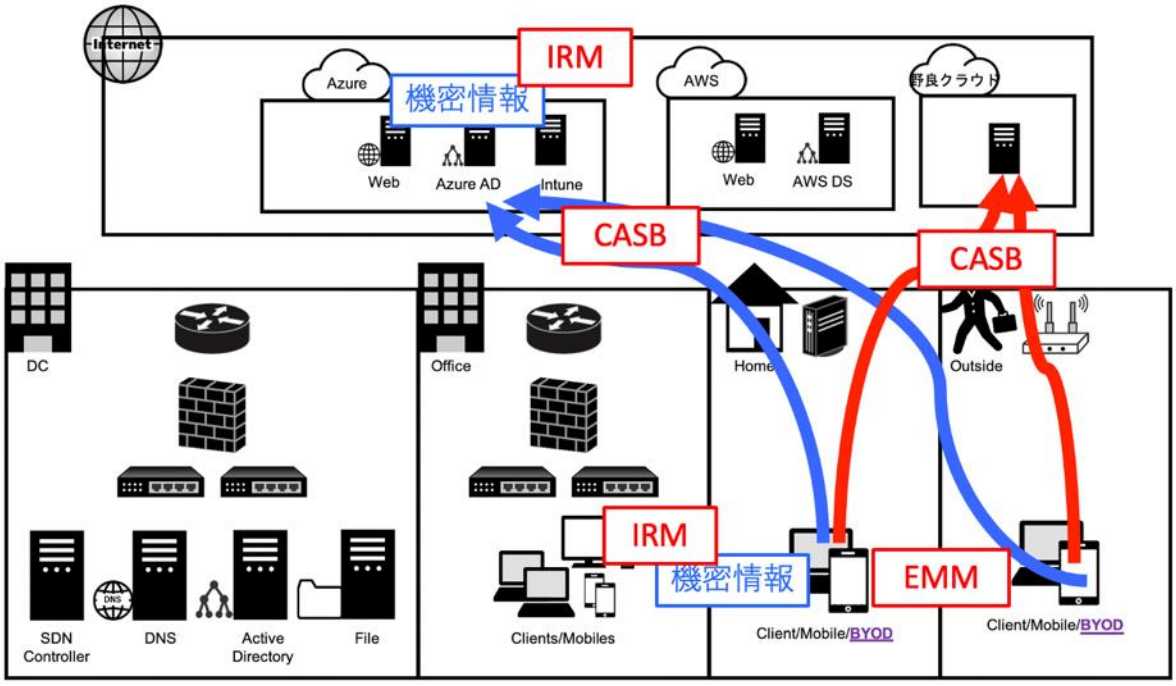


図 4-5 ユースケース C モデルケース

表 4-5 ユースケース C 検証内容

No	要素	検知	検証内容
1	EMM	正常系	BYOD 端末の管理
2	CASB	正常系	許可されたファイルに対する制御
3	CASB	異常系	未許可ファイルに対する制御
4	CASB	異常系	不正な端末からのログイン
5	CASB	異常系	端末乗っ取りの検知（振る舞い）
6	EDR	異常系	マルウェア感染の検知
7	CASB	異常系	マルウェアアップロードの検知
8	CASB	異常系	管理クラウドへの大量データダウンロード/アップロードの検知
9	CASB	異常系	野良クラウドへの社内データアップロードの禁止
10	IRM	異常系	アクセス権管理によるデータ保護

【検証で得た気づき】

- BYOD 端末で使用している OS によっては，EDR 等による制御が働かないケースもありうる。他に，CASB はユーザーの想定しない操作により適切に制御が働かないこともある。これらの理由から情報漏えいを前提として考えておき，その対策として IRM を組合せることが有効であるとわかった。
- 利便性と安全性を秤にかけ，許容できないリスクに備えて大胆な機能制限を設けてしまうことも選択肢である。

4.3.5. ユースケース D について

No	ユースケース	検証概要
D	管理外端末（請負会社等）からの SaaS へのアクセス	SaaS に外部ユーザーが管理外端末でアクセスした場合の検証

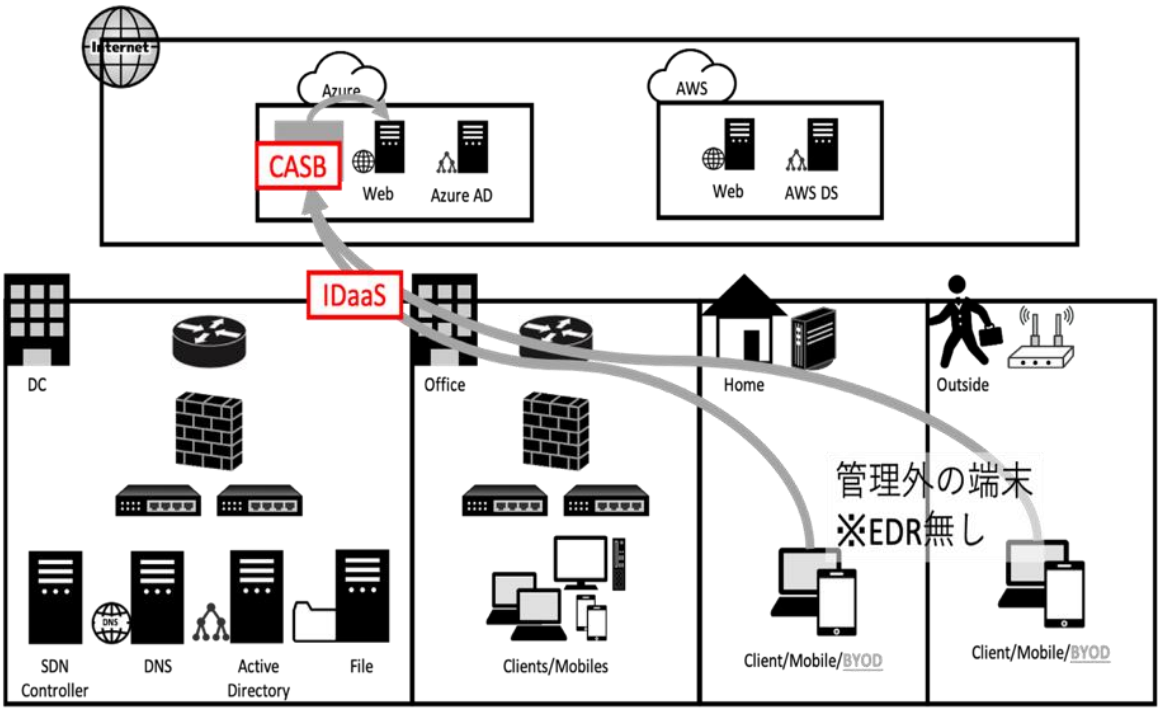


図 4-6 ユースケース D モデルケース

表 4-6 ユースケース D 検証内容

No	要素	検知	検証内容
1	IDaaS	正常系	IDaaS に自社ユーザーと請負業者のユーザーを混在させ，請負業者のアカウントでの不正アクセスを検知，遮断する
2	IDaaS	–	IDaaS を多段(前段 IDaaS_A，後段 IDaaS_B)にし，社員は IDaaS_A を経由し，IDaaS_B で認証，請負業者は，IDaaS_A で認証させる。
3	IDaaS	–	IDaaS を並列に並べ，社員は IDaaS_A で認証，請負業者は IDaaS_B で認証させる。
4	CASB	異常系	CASB の SaaS API 接続にて，請負業者のユーザーアカウント(IDaaS 連携なし)で，SaaS から任意のファイルがダウンロードされた際に検知できるか。
5	IdaaS CASB(リバプロ)	–	CASB の SaaS リバースプロキシモードで請負業者のユーザーアカウント(IDaaS 連携あり)のファイルのアップロードを禁止
6	IdaaS CASB(リバプロ)	–	CASB の SaaS リバースプロキシモードで請負業者のユーザーアカウント(IDaaS 連携あり)のファイルのダウンロードを禁止
7	IdaaS CASB(リバプロ)	–	CASB の SaaS リバースプロキシモードで請負業者のユーザーアカウント(IDaaS 連携あり)が，ポリシー違反をした際に再認証を求める。

【検証で得た気づき】

- 外部ユーザーの SaaS へのアクセス制御について，IDaaS が有効であることがわかった。
- 社内で使用している認証系システムと IDaaS を組み合わせて使うことで，人の出入りの管理を別でできると言った利点があることがわかった
- 外部ユーザーからのアクセスに対してのセキュリティにおいて，IDaaS や CASB などでシステムで強化するだけでなく，機密情報の取り扱いや，契約上の制約等の運用と合わせることで更なる効果が期待できる。

4.3.6. ユースケース E について

No	ユースケース	検証概要
E	クラウドの設定誤り防止	クラウドの設定誤り検知を CSPM で機能検証

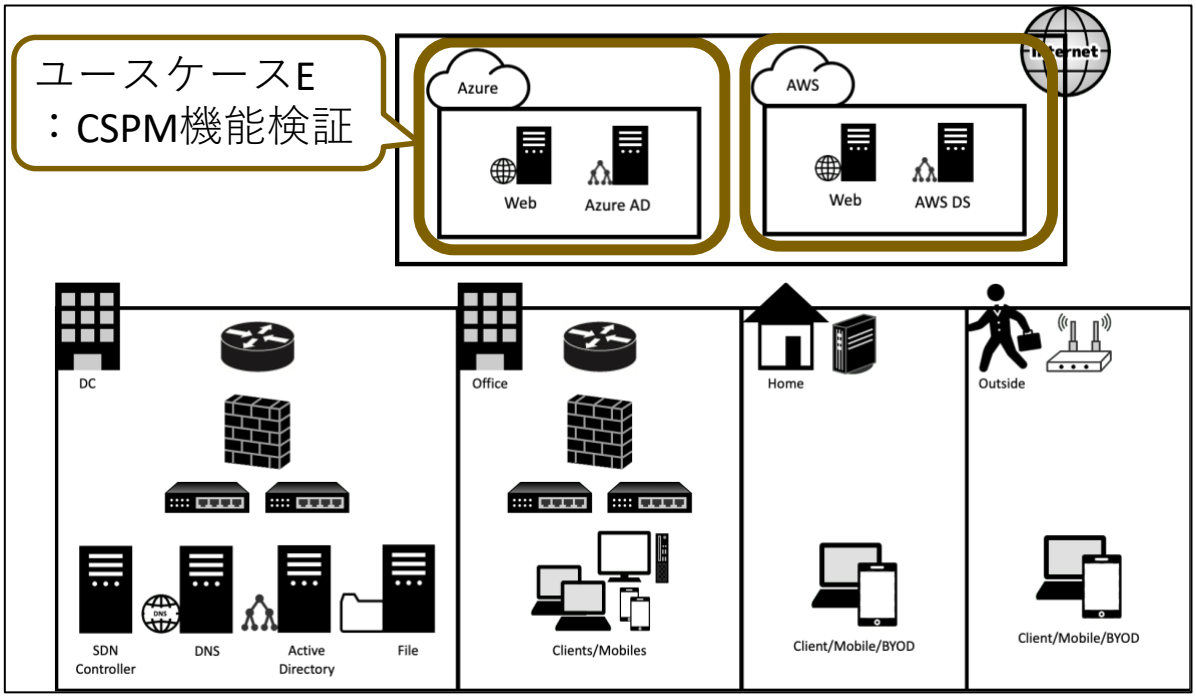


図 4-7 ユースケース E モデルケース

表 4-7 ユースケース E 検証内容

No	要素	検知	検証内容
1	CSPM	正常系	SSH(port22)が開いている場合にアラート検知するか
2	CSPM	正常系	ポリシー違反(SSH(port22)オープン)を発見後，自動修正ルールを適用できるか
3	CSPM	異常系	検証 No2 で自動修正されたポートを再度オープンにした場合，再度自動修正されるか
4	CSPM	正常系	NIST CSF や GDPR，MITERATT&CK など，定義のテンプレートを用いたアラートルールを設定できるか

【検証で得た気づき】

- クラウドの設定誤り，設定漏れ，改ざんの検知や自動修復に CSPM が有効であることがわかった
- 監査等でのポリシー遵守のエビデンスを出すのにも有効であることがわかった
- CSPM だけでは，検知はできるものの，攻撃を止めることはできないため，攻撃から守るためには，クラウド側のセキュリティ対策を導入すると更なる効果が期待できる
- ポリシーを決め自動修復ができる場合，本番環境への影響が考えられるため，CSPM 自体のセキュリティも考慮する必要がある

4.3.7. ユースケース F について

No	ユースケース	検証概要
F	SASE の機能検証	SASE 単体での検知・確認ができるのかの機能検証

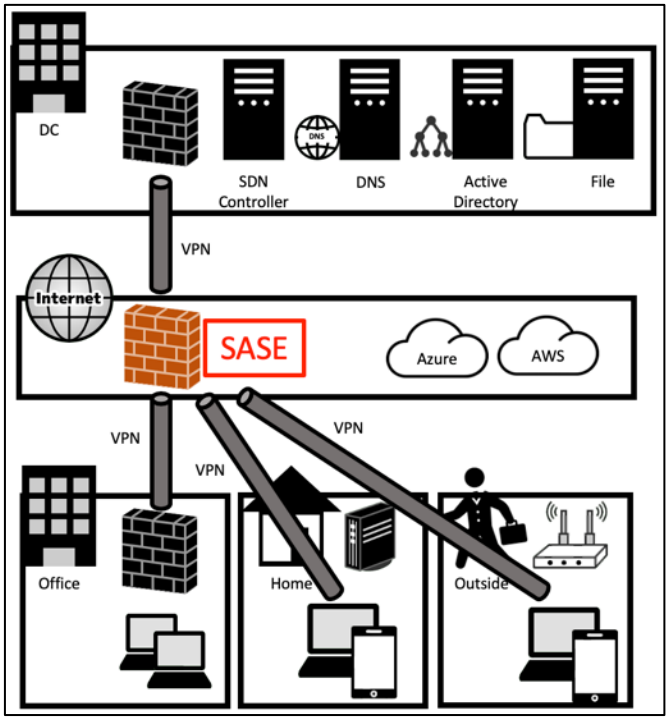


図 4-8 ユースケース F モデルケース

表 4-8 ユースケース F 検証内容

No	要素	検知	検証内容
1	SASE	正常系	ユーザー，デバイスによるアクセス制御できるか
2	SASE	正常系	URL フィルタリングできるか
3	SASE	異常系	マルウェアによる攻撃や情報窃取を防御できるか

【検証で得た気づき】

- SASE は FW 機能に近く，通信の内容を検知する機能があることがわかった
- Web 閲覧制御，マルウェア対策などにも SASE に一定の効果があることがわかった
- SASE を通過しない通信（内部から内部への通信など）は検知できず，検知するためにはクラウド側に認証基盤を置いて，必ず通過する仕組みを作る必要があることがわかった。
- 認証基盤をクラウドにおけない場合は，振る舞い検知のできるソリューションを入れると更なる効果が期待できる。

5. 制御系システムへのゼロトラスト導入検証

5.1. 制御系システムへのゼロトラスト適用の背景

4章では主に情報系システムのケースでの導入方法を考えてきた。ゼロトラストはクラウドを使用する前提で考えることことから情報系システムへの導入として考えられており，制御系システムへの導入は難しい（メリットがない）と思われている。しかし，制御系システムについても，IoT 機器やクラウドなど，情報系システムとの接続要件が出てきていることから，状況としては情報系システムと同様に境界型防御だけでは防ぎきれない事態が近い将来訪れると想定できる。ゼロトラストの考えを導入することは有効と考えられるため，制御系システムへの導入についても検証した。

5.2. 対象スコープの設定について

制御系と情報系の簡易的な接続構成図の例を図 5-1 に記す。図 5-1 の情報系システムのエリアのセキュリティについては，前章までのゼロトラストの対策で対応できると考えるため，制御系システムのエリアの範囲で対象スコープを検討する。

制御系システムでは，大きく分けると，制御サーバ，HMI（Human Machine Interface：パソコン，キーボード・マウス・ボタン，操作盤など），制御機器があるが，今回の対象は HMI を例に記載する。その理由として，HMI が制御信号を流す起点となるというところと，USB の接続によるウイルス感染や制御端末の不正利用等が想定できるためである。

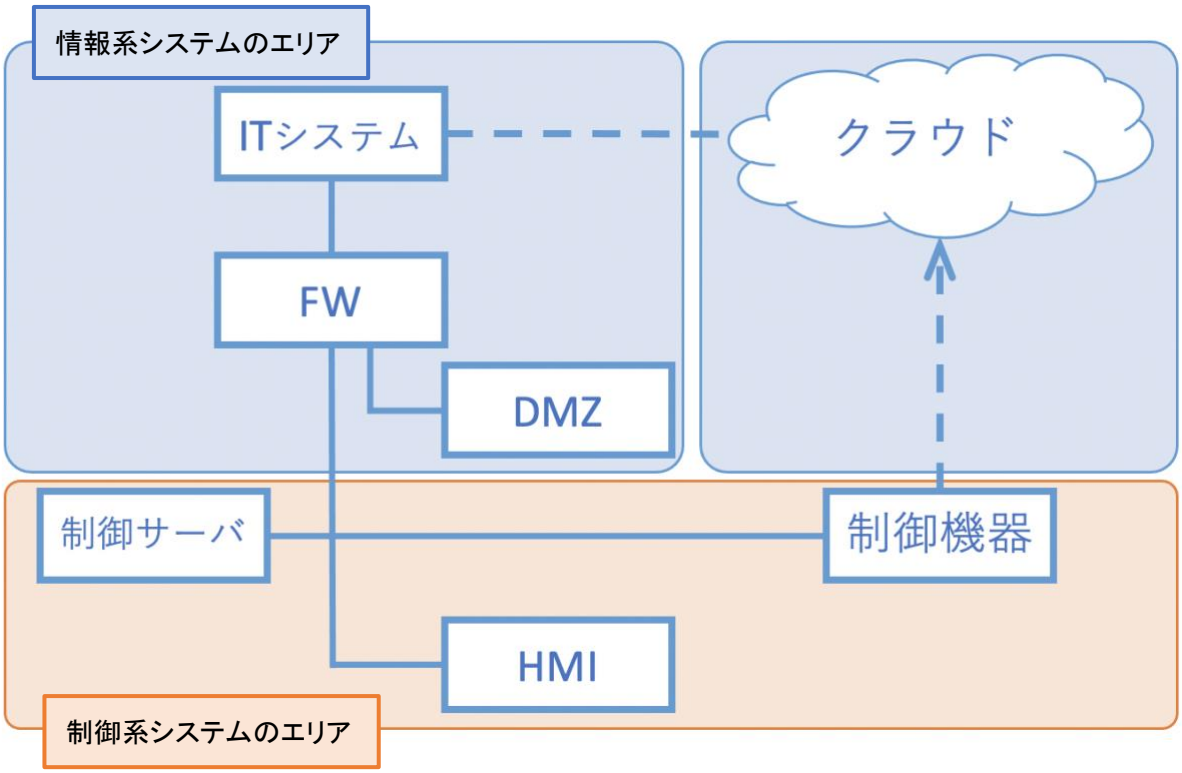


図 5-1 制御系システムと情報系システムの接続構成図例

5.3. 制御系システムにゼロトラストを導入するための課題

情報系システムとの違いとして，制御系システムには主に以下の課題が考えられる。

- 認証機能が備わっていないケースが多く，情報系のゼロトラストと同じ方法が使えない
- 制御系システムに検知ツールやログ収集ツール等を入れることで可用性への影響がある
- 独自プロトコルやレガシーシステムを使用しているため，一元的な導入が難しい
  （ライフサイクルが長いという懸念もある）

等

上記事項から，制御系システム内へゼロトラストの機能を導入するのではなく，制御に関わる部分において，ゼロトラストの機能を導入する方法を考える必要がある。また，制御系の境界型防御の考えとして，「制御系システムを使用できるものは信用する」という観点もあることから，「内部の人間が不正を働く」といった観点も含めて検討を行う。

5.4. 導入検証例・結果

5.3 の課題を踏まえ，一例として以下の内容で検証を実施した。

結果として，認証の機能のみを社内の情報系システムで使用している認証系システムと連携し実施することで，制御系システム側への影響を極力抑えるとともに，内部からの不正操作・不正利用という観点ではセキュリティを向上することができたと考えられられる。ただし，認証機能を導入するということは，少なからず現場作業に影響がでることになり，ユーザビリティの観点では改善していくことが必要。よって，導入する際には，DevOps（Development＋Operations）の考えも取り入れ，運用側とともに考えていくことが重要である。本検証における改善案も以下の内容に記載しておく。

制御系システムへのゼロトラストの導入検証として実施したが，単純に入れるということは難しい。しかし，情報系システムへの連携方法を工夫することで，ゼロトラストの要素を取り入れることは可能であると考える。

＜導入検証例＞

〇前提条件

- 従業員証（IC カード）は常に携行し，情報系システムに従業員データ（所属，役職，権限等）の登録があること
- 従業員データはクラウドソリューションの IDaaS 機能と連携していること
- 社給携帯端末を保有しており，社給携帯端末には指紋認証等の多要素認証機能が付与されていること
- 入退室管理の情報は情報系システムと連携していること

〇検証条件

図 5-2 に検証環境を記す。制御系システムの HMI の操作で使用するキーボード・マウスを電源付 USB ハブに接続する。また，HMI から制御機器へ流れる制御信号について，電源付 USB ハブを経由する構造とする。電源付 USB ハブの電源制御に対して，認証機能を用いる構造とする。

従業員証をカードリーダーに置き，その認証情報をクラウドにアプリの IDaaS の機能に連携することで，多要素認証または二段階認証を行うことにより，情報系システムに登録している従業員の権限や入退室管理の情報と照合し，認証結果を返すという仕組みとする。

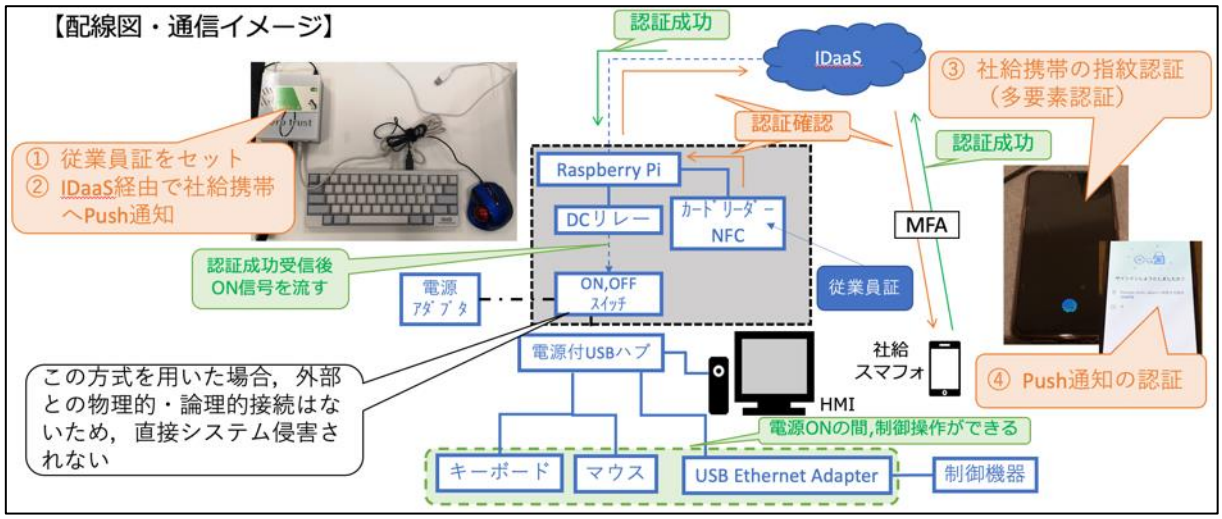


図 5-2　制御系システムへのゼロトラスト導入検証図

〇検証結果

図 5-2 の仕組みどおり，制御系システムに直接影響のなく，電源付 USB ハブの電源制御を用いて，多要素認証を導入することができた。検証では，細かい従業員情報を設定してはいなかったが，ここに使用権限等の条件を組み込むことで，より詳細な制御ができると考えられる。この結果から以下の効果が見込まれる。

・制御系システム自体に従業員データ等をいれる必要がない（従業員の入替による変更の不要）
・制御機能を使用する際の台帳への記載等の台帳管理は不要となる
・他人の従業員証の不正利用の防止ができる
・HMI がウイルス感染したとしても，認証されていなければ信号が制御機器に到達しない
・認証側からのサイバー攻撃は，ネットワークがつながっていないため制御側への影響はない

など

〇今後の改善案

上記検証の内容では，毎回従業員証を置く，多要素認証を行うなどのユーザビリティに問題があるため，その改善が必要（例えば，カードリーダーをパッシブスキャン型に変え，近づいただけで認証できるようにする，多要素認証も認証情報をキャッシュ保持し，1日1回にする　など）。

また，セキュリティ面においても，入退室管理のエラー回数等で，ユーザの信用レベルを変化させ，認証を厳しくする等，ゼロトラストの要素を情報系側で付与することで，さらなる効果の期待が考えられる。

6. 導入方法

6.1. 課題の確認

1 章でも紹介した「NIST SP800-207」には，ゼロトラストを導入・構築するための様々な構成要素が含まれているが，これらは一企業が導入するには専任チーム等，相応の労力を要する。

ゼロトラストを実現させるためには，既存のセキュリティを活用しつつ，ハイブリッド型としてスモールスタートで実施していくことが現実的である。ゼロトラストをいち早く導入した Google 社も「BeyondCorp」の実現に 8 年の歳月を要している。現在，ほとんどの企業が従来の境界型防御によるセキュリティを構築していると考えると，ゼロトラストへ一斉更新することは，コスト面・運用面・人的資源を考えると難易度が高いと言える。まずは自社の課題を整理し，何をしたいか等の要件定義をまとめた上で，課題にあったソリューションを見つけることがゼロトラストへの第一歩と考える。

6.2. ゼロトラスト導入のポイント

「これを導入すればゼロトラスト実現！」や「ゼロトラスト」と言う名の製品はこの世の中に存在しない。前述でも述べたように要件定義に合わないソリューションを購入すると管理・運用の負担増となる。ついてはソリューションを導入する際に押さえておきたいポイントを述べる。

① ID 管理の強化【IDaaS】

従来の ID（メールアドレス含む）・パスワードによる認証では適切な利用者がアクセスしているとは言えず，漏洩やなりすましのリスクが考えられる。ID 管理だけでなく，使用デバイスやアプリケーションのセキュリティ状態（最新のセキュリティパッチは適用されているか？）によるアクセス管理の機能を行うため，IDaaS を導入するという選択肢もある。

② デバイス管理の強化【EMM，EDR】

続いて信用できる利用者を限定したあとは，デバイス保護を強化すること。リモートワークの増加に伴い様々なデバイスを利用する機会が増えた。また，COVID-19 感染拡大に乗じたフィッシング詐欺メールやマルウェアを含んだ標的型攻撃メールも近年増加している。

デバイスのセキュリティ保護に有効なソリューションは，EMM と EDR がある。

EMM は前項でも述べた MDM と MAM に分類され，MDM はデバイスからの情報漏えいを防ぐ機能を持っており，MAM は端末にインストールしたアプリケーションの管理を行える。EMM により「企業領域」と「個人領域」を分割し，企業データを個人領域へ持ち出せなくすることも可能である。

これまで境界型防御（ファイアウォールや IDS／IPS，サンドボックス型製品等）に守られていた端末は，ゼロトラスト環境では様々な脅威に対して直接触れることとなる。こうした脅威に対して，従来のアンチウイルスソフトでは防ぐことはできなくなりつつある。ここでデバイスのセキュリティ対策で重要なソリューションとして，EDR を導入する。EDR は振る舞い検知型（不審な挙動を検知するというもの）のため，未知の脅威であっても一定の精度で検知でき，万が一イ

ンシデントが発生したとしても発生後の対応を強化できる。

ただし，最近では BYOD を利用するケースも増えていることから，BYOD に企業が用意したソリューションを適用できるかを確認することが肝要である。（OS のバージョンによって未対応のものもあるため）

③ ネットワークセキュリティ対策【SWG／SDP】

境界型防御で VPN ゲートウェイを利用してクラウドへアクセスする場合，社外から VPN ゲートウェイ⇒社内 LAN を経由してからインターネット（クラウド）への接続が必要であった。テレワーク利用者の急増や，クラウドサービス利用増加に伴い，企業のネットワーク帯域が逼迫している。

SWG を利用することにより，今まで VPN ゲートウェイが担っていた機能をクラウドへ移管し，企業のネットワーク帯域を通過することなくトラフィックをセキュア管理できる。

また，SDP には SWG 機能のみならず CASB 機能も備わっているソリューションも存在するため，自社にあったソリューションを選定することが肝要である。

④ セキュリティ運用（監視・分析，インシデントレスポンス）の自動化【SIEM/SOAR】

ゼロトラストを実現するためには境界型防御とは違ったセキュリティリスクの管理が必要となる。従来の人員では対応しきれない場合も起こりうるため，SOAR によるインシデントの監視・分析から対応の自動化を行い，脱属人化のセキュリティ運用を行うことも検討する必要がある。

SOAR を利用しない場合，運用者はインシデント発生後に SIEM でログを確認し，EDR 等をチェック，IDaaS・SWG 等での権限操作や EDR でデバイス隔離などを対応する必要があり，SOAR を活用することで，上記のフローを自動化し，速やかにインシデント対応を完了させることができ，レジリエンス力向上に寄与する。ただし，完全自動化は危ういため，重要なポイントでの人の介在は必要により考えること。

6.3. ゼロトラスト導入の注意点

紹介したソリューションを導入するにはセキュリティ投資が必要になる。経営者によっては，セキュリティ対策の重要性は理解しているものの，これまで被害を受けていないため「費用」として判断することが考えられる。ゼロトラスト導入担当は，セキュリティ対策は「投資」であることを主張しつつ，企業イメージ・株価上昇につなげるための重要な「戦略」であることを提言することが肝要である。

なお，費用はライセンス体系（ユーザ単位・デバイス単位等）で変わるため，ベンダーから見積もりを取得すること。

7. 境界型防御との共存

7.1. 境界型防御とゼロトラストの違いについて

今回の検証では，境界型防御とゼロトラストを両方使用したケースをもとに実施した。表 7-1 に境界型防御の考え方と，ゼロトラストの考え方を記載する。境界型防御は外からの侵入を防ぎ，「外部の攻撃による社内へのウイルス感染や不正侵入から身を守る」ということであり，それに対しゼロトラストは，内部から攻撃された場合，「内部の攻撃による社外への情報流出や不正操作から身を守る」ということである。

つまり，境界型防御とゼロトラストは，見ている視点が違うだけで，どちらが優れているから大丈夫，劣っている方は不要（ファイアウォール（FW）や境界型防御は不要）ということではない。そのため，既存の境界型防御を排除するだけでなく，共存させることで，より良いセキュリティができるのではないかと考える。

表 7-1 境界型防御とゼロトラストの防御の考え方

セキュリティ対策	考え方	対象製品
境界型防御	外部からのサイバー攻撃による社内の資産（端末類，情報，システムなど）への侵入を防ぐ。 →サイバー攻撃にやられないための対策	FW，IDS，IPS など
ゼロトラスト	内部からのサイバー攻撃（内部犯行含む）による社内の資産（端末類，情報，システムなど）の改ざん，流出を防ぐ。 →サイバー攻撃にやられたとしても重要な情報を漏らさないための対策	4 章参照

7.2. 境界型防御とゼロトラストの組み合わせ

導入プロセスについては，「2 章 2.6 ゼロトラスト導入に向けた進め方」を参照にする。

検証結果も踏まえ，NIST サイバーセキュリティフレームワークを基準に，境界型防御の要素とゼロトラストの要素を反映した図を図 7-1 に記す。境界型防御は主に「防御」「検知」の対策であり，今回検証した機能は，他の「特定」「対応」「復旧」の対策もできている。このことから，ゼロトラストの製品を全て導入することで，全ての攻撃ステップでの対応も可能かと考えるが，境界型防御が使用できないというわけではない。考え方にはなるが，境界型防御を活かし，現在運用で実施している対策箇所にゼロトラストの機能を入れ，効率化させるという方法もある。

繰り返しにはなるが，導入プロセスで，何をどう守るべきかを考えるなかで，境界型防御の選択肢も入れて考えることで，運用面も含め総合的に良いセキュリティが構築できると考える。

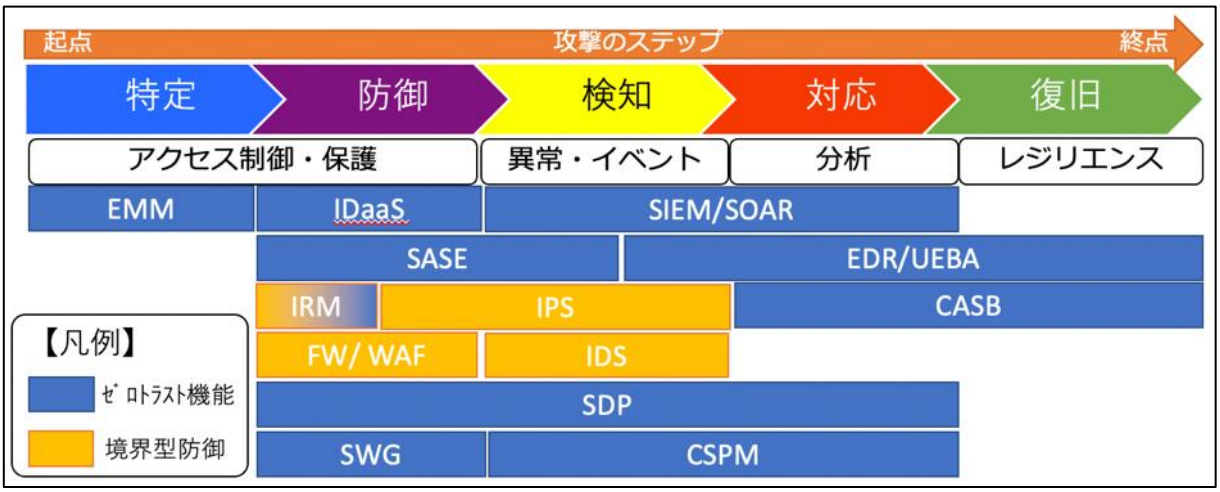


図 7-1 サイバーセキュリティフレームワークへの防御機能の落とし込み

8. ゼロトラスト導入における運用上の注意

8.1. ゼロトラスト導入後の運用について

ゼロトラスト運用に関わる内容として，2 章の「2.3 ゼロトラストの基本的な考え方」には「資産，ネットワークインフラストラクチャ，通信の現状について可能な限り多くの情報を収集し，セキュリティ体制の改善に利用する」とあり，「2.6 ゼロトラスト導入に向けた進め方」には，「変更/更新/移行に関するフィードバック」という記載がある。また，同箇所③に「初めはビジネスインパクトの低いビジネスプロセスから開始するのが望ましい」と記載をしている。

上記を踏まえると，ゼロトラストはビジネスインパクトの低いところから，徐々に拡大していくという展開方法になるため，運用をしていく中で，どれくらいの期間で見直すかというところを計画しておく必要がある。そして，導入当初は，ユーザに直接影響がでることから，問い合わせ等が増えることも想定した準備をしておくことが重要である。

また，対象を拡大していく際には，業務によってビジネスインパクトが変わるため，信用度レベルの考え方も合わせて見直す必要がある。それに，合わせて影響する運用部署へ丁寧な説明が必要となる。運用側にも受け入れられるよう，リスクコミュニケーションを意識して，調整をしていく。

8.2. 運用時の注意事項について

上記を踏まえ，以下のポイントを注意事項としてあげる。なお，以下ポイントについては，あくまで一例であるため，自社の検討の中で重要となったポイントは追加すること。

＜注意事項＞

- □ どのような計画でゼロトラストを進めていく（拡大していく）のかを策定し，定期的に見直しをかける
- □ 日々導入当初は機能が正しく動いているのかを監視し，異常だけでなく正常な状態も確認する
- □ 適用時には，必ず運用から問い合わせがくるため，その対応の要員を配置する
- □ 運用部門に受け入れてもらえるよう，運用部門へのメリットも含めて調整する
  （リスクコミュニケーション）
- □ 範囲を拡大する際は，事前に運用部門と調整し，業務に支障がでないようにする
- □ 範囲を拡大するときには，業務の重要度に合わせて，ポリシーの見直しも行う
  （一度策定したポリシーで永久的に良いとは限らない）
- □ 運用部署の業務ルールが変わった際にも，必要に応じてポリシーの見直しを行う
  （システム側だけでなく，運用側の情報をキャッチし，見直す）

9. まとめ

本指南書は，ゼロトラストの基本的な考え方やゼロトラストに用いられる技術要素の説明から始まり，情報系システム・制御系システムへのゼロトラスト導入における，実際の検証結果を踏まえた評価を記載した。また，既存の境界型防御を活かしつつ，ゼロトラストを使用するケースについても，検証結果から考察した。

ゼロトラストはこれを入れれば良いというものではなく，自社の守るべき資産に合わせリスクをどう考え，どういった技術を組み合わせて守るのかという大前提の元，今までの「外部から攻撃を受けないためにどうすれば良いか」という考えだけでなく，「外部からの攻撃を受けた後，内部からの攻撃をどう防ぐか」という考えを加えた言葉だと捉えるのが良い。

今回実施した検証は一例であるが，ゼロトラストに用いられる多種多様の技術を使用し，その検証結果をまとめているため，この指南書を読むことで，技術がどういうものかを知ることができるので，それらをどう使用するかを考える一助となる。

また，運用面の注意事項においても，今回の検証で得られたことを記載していることから，実運用を行う時でも，注意点を踏まえてどう運用するかを考える一助となる。

本指南書を作成するにあたって検証した内容が，そのまま使用できるとは思っていないが，ゼロトラストを導入するために，何から初め，どう考え，どう導入していくのかということを考えることのできる材料は，この指南書に詰め込めたと思っている。

なお，本書は 2021 年 6 月時点での製品・サービスの検証結果をもとに執筆したものであり，二年後にも本書の内容がそのまま通用するとは考えられない。ゼロトラストは現有技術を総動員した戦い方であるという点をふまえ，最新の情報や技術を常にアップデートし続ける必要がある。

本指南書が，自社へのゼロトラスト導入の助けになれば幸いである。

謝辞

本指南書の作成にあたりまして，各製品ベンダーの方々に製品・ライセンス貸出しをしていただくとともに，多大なるご支援・ご尽力を賜りました。諸般の事情により，全ての方のお名前をここに挙げることはできませんが，お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また，産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる，門林雄基先生，小林和真先生，満永拓邦先生，登大遊先生，小林裕士先生，目黒有輝先生，前田一平先生には，本指南書の元となるゼロトラストプロジェクトのメンター・講師として，ご指導・ご助言とともに，各検証機材のご支援を賜り続けてきました。改めて御礼申し上げます。

そして，本指南書の作成や本プロジェクトをともに実施した，下記メンバーの皆様にも感謝を伝えたいと思います。

＜ゼロトラストプロジェクトメンバー＞

（総勢23名）

【リーダー】

水田　創

【サブリーダー】

飯島　安恵	酒井　宏尚
木下　徳一	関谷　英樹

【メンバー】

秋間　和兵	小山　慎一郎	根本　剛
岩本　智裕	末田　敦史	波多野　拓貴
大内　皓陽	砂田　翔平	松山　幸輝
落合　英明	谷　祐輔	三池　勝
折下　伸也	谷内　俊輔	村上　幸司
影井　誠一郎	時﨑　涼輔	吉田　拓也