JSSA
情報セキュリティ研究プロジェクト

2022年度の活動状況と2023年度の活動計画

ZERO　TRUSTの実現に向けた情報の収集と発信

「サイバーインシデント対応」にかかる情報の収集と発信

Agenda

1. 情報セキュリティ研究プロジェクトの活動
2. 2022年度　ゼロトラストアーキテクチャとシステム監査
   ～ゼロトラストへの道～
3. 2023年度　研究テーマと活動計画

【付録】

Agenda

1. 情報セキュリティ研究プロジェクトの活動

2. 2022年度　ゼロトラストアーキテクチャとシステム監査
　　～ゼロトラストへの道～

3. 2023年度　研究テーマと活動計画

１．情報セキュリティ研究プロジェクトの活動

研究テーマと概要

- 情報セキュリティの確立と強化のための有効な考え方、具体的実施策の、幅広い研究と提案
- 時宜に応じたテーマの選定、関係する情報の収集と分析、多様な見解を尊重した意見交換により、参加者それぞれの研究を促進するとともに、研究プロジェクトとして研究成果にまとめ、公表・発表する。

- ＜テーマ＞
  - ■ ZERO TRUSTへの道～ZERO　TRUSTの実現に向けた情報の収集と発信
  - ■ 「サイバーインシデント対応」にかかる情報の収集と発信
  - ■ サイバーセキュリティ，事業継続と情報セキュリティ，デジタルフォレンジック，サプライチェーンセキュリティ，ソフトウェア開発の外部委託と情報セキュリティ 等

- ＜メンバー＞
  - ■ 成田 和弘（副主査）、木村 裕一、芳仲 宏、牧野 博文、山本 孟

1.1 「情報セキュリティ」研究プロジェクト（継続）

学会会員のホームページ＜研究活動＞に案内予定　－2023年度

「情報セキュリティ」研究プロジェクト（継続） （主査：－／副主査：成田和弘）	
研究テーマと概要	情報セキュリティの確立と強化のための有効な考え方、具体的実施策の、幅広い研究と提案 財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準（J-SOX）の改訂など、昨今のサイバーリスクに対する環境を踏まえたテーマの選定、関係する情報の収集と分析、多様な見解を尊重した意見交換により、参加者それぞれの研究を促進するとともに、研究プロジェクトとして研究成果にまとめ、公表・発表する。 ＜テーマ＞ • 「サイバーインシデント対応」にかかる情報の収集と発信 • サイバーセキュリティ，事業継続と情報セキュリティ，デジタルフォレンジック，サプライチェーンセキュリティ，ソフトウェア開発の外部委託と情報セキュリティ 等
計画日程	原則月1回の頻度でZoomオンライン会議にて開催する。 1. 情報セキュリティ、事業継続、リスクマネジメント等にかかる事例、国内外の基準・標準の動向調査等の情報共有 2. 各人の研究関連情報および事例に関する意見交換

1.2 2022年度 活動内容

⑴ 研究テーマ

「ゼロトラストアーキテクチャとシステム監査 ～ゼロトラストへの道～」

2021～2022年度において、NIST-SP800-207 におけるゼロトラストアーキテ クチャ（ZTA）を探求した。

⑵ 研究の動機

NIST-SP800-207 におけるゼロトラストアーキテクチャの考え方をわかりやすく伝えることを目指して活動する。

①ZTAが必要とされるようになった背景、②ZTAの考え方、③システム監査の際の考慮事項の三つを要点にして成果求めた。

⑶ 研究発表

① 2022年度第1回定例研究会(Webinar)発表　2023年2月25日（土）10:00～

② JSSAニュース №110（2023.4.3）研究会のページに報告

1.3 2022年度 研究の発端と目的

目的は「ゼロトラストアーキテクチャ（ZTA）」が「何の役に立つのか」を理解すること

- ゼロトラストアーキテクチャを必要とする背景・・・サイバーリスクの実態を理解する
  - ■ゼロトラストアーキテクチャは「手段」、その「目的」であるサイバーリスクを理解する
- 「NISTのゼロトラストアーキテクチャ」の考え方について整理する
  - ■原典ともいえるNIST-SP800-207に示された原則等をじっくり理解する
- 「NISTのゼロトラストアーキテクチャの実装」を概観する
  - ■実践のために公開されているNIST-SP1800-35（ドラフト）を参考に、ゼロトラストのアーキテクチャの参照モデルとリスク等を概観する
- サイバーセキュリティ/レジリエンスの向上に役立つようなシステム監査を検討する
  - ■ゼロトラストアーキテクチャの理解を通して得られた知見を活用し、サイバーリスクの軽減に役立つシステム監査を検討する

Agenda

1. 情報セキュリティ研究プロジェクトの活動

2. 2022年度　ゼロトラストアーキテクチャとシステム監査
　～ゼロトラストへの道～

　⇒ NISTの“ゼロトラストアーキテクチャ(ZTA)”についての研究報告です。

3. 2023年度　研究テーマと活動計画

2.1 ZTAの目的と背景 (1)

米国では、政府主導での“ゼロトラストアーキテクチャの実装プロジェクト”が進められている

- **NIST National Cybersecurity Center of Excellence**

  ■Implementing a Zero Trust Architecture

従来のネットワークセキュリティは境界防御に重点を置いていたが、**多くの組織には明確に定義された境界がなくなった**。現代のデジタルエンタープライズを保護するために、組織は、場所に関係なく、事業体リソース(アプリケーション、レガシーシステム、データ、デバイスなど)に「いつでもどこでも」安全にアクセスするための包括的な戦略を必要としている。

[Source] NIST, Implementing a Zero Trust Architecture , https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture （発表者による仮訳）（access 2023/1/23)

2.1 ZTAの目的と背景 (2)

複雑化するインフラと激化するサイバー攻撃

- 典型的な事業体のインフラストラクチャはますます複雑になっている。1つの事業体が、複数の内部ネットワーク、独自のローカルインフラストラクチャを備えたリモートオフィス、リモートまたはモバイルの個人、そしてクラウドサービスを運用している場合がある。事業体が境界を簡単には特定できないため、この複雑さには従来の境界ベースのネットワークセキュリティの方法では太刀打ちできない。**境界ベースのネットワークセキュリティは、攻撃者が境界を一度破ってしまうと、その後の横方向の動きを防げないことからも、不十分なものであることが明らかである。**
- この複雑な事業体が、「ゼロトラスト」（ZT）と呼ばれるサイバーセキュリティの新しいモデルの開発につながっている。

➢ **ゼロトラストアーキテクチャは、**以下の課題に対応するためにに作られたもの。
  - 事業体のインフラが複雑化し、境界の識別が難しく、**境界防御そのものが困難**になったこと。
  - サイバー攻撃の内部での横方向の動きに対応できないという**境界防御の弱点**があること。

[出典] NIST, SP800-207, Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, p.1（発表者による仮訳）（access 2023/1/23)

2.1 ZTAの目的と背景 (3)

アウトカム

- **テレワーカーのサポート；**オンプレミス、自宅、近所のコーヒー ショップの公衆 Wi-Fi など、その場所を問わず、事業体リソースにアクセスできるようになる。
- **リソースの保護；**オンプレミスかクラウドかその場所を問わない。
- **内側からの脅威への防御；**ネットワーク境界内ではどのユーザーも必然的に信頼するべきという無効な仮定からの脱却。
- **侵害からの防御；**攻撃者がネットワーク内を水平移動する能力を低下させ、侵害から防御する。アクセス制御は個々のリソースごとに適用できるので、攻撃者が1 つのリソースにアクセスできても、他のリソースへの踏み台にはできない。
- **インシデントの検出、対応、復旧の改善；**侵害が発生した場合の影響を最小限に抑える。侵害を制限することで、侵害の痕跡と回復までの時間を短縮できる。
- **事業体の機密データの保護；**データの転送中と保存中の両方で強力な暗号化を使用する。一貫した識別、認証、承認手順を実施し、デバイスの正常性を確認し、事業体ポリシーで指定されたその他すべてのチェックを実行した後でのみ、サブジェクトにリソースへのアクセスを許可する。
- **可視性の向上；**どのユーザーがいつ、どのように、どこからどのリソースにアクセスしているのか。すべてのアクセス セッション内のすべてのアクセス要求を監視し、記録する。
- **動的なリスクベースの評価の実施；**すべてのアクセス トランザクションとセッションの継続的な再評価をし、定期的な再認証と再承認からの情報の収集、動作中のデバイスの正常性検証、ふるまい分析、動作中のリソースの正常性検証、異常検出、およびその他のセキュリティ分析を行う。

[Source] The National Institute of Standards and Technology (NIST), SP 1800-35B Implementing a Zero Trust Architecture, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf, p.4, (access 2023/1/31)

2.2 ZTAの前提と原則（1）

NISTのゼロトラストアーキテクチャの運用上の定義

- ゼロトラスト（ZT）は、
  - ネットワークは侵害されていると見做し、
  - 情報システムおよびサービスにおいて要求のある都度、アクセスの真正さを強制的に要求することで不確実性を最小化するように設計された、概念とアイデアの集まりを提供する。
- ゼロトラストアーキテクチャ（ZTA）は、
  - ゼロトラストの概念を利用し、
  - コンポーネントの関係、ワークフローの計画、アクセスポリシーを網羅する事業体のサイバーセキュリティ計画である。
  したがって、
- ゼロトラストの事業体には、
  - ゼロトラストアーキテクチャ計画の成果として、
  - 事業体に配備された（物理および仮想の）ネットワークインフラストラクチャと運用ポリシーがある。

[出典] NIST, SP800-207, Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, p.4（発表者による仮訳）（access 2023/1/23）

2.2 ZTAの前提と原則 (2)

ゼロトラストアクセス

- ゼロトラストの定義は、**データとサービスを一対にしてアクセスコントロールを可能な限り細かく実施する**ことで、不正アクセスを防止することを目標とする
  - ■ 権限が付与されかつ承認されたサブジェクト（ユーザー、アプリケーション（またはサービス）、およびデバイスの組み合わせ）だけがデータにアクセスできる
  - ■ データアクセスとリソースアクセス（例えば、プリンター、コンピューティングリソース、モノのインターネット[IoT]アクチュエーター）の両方を対象とする
  - ■ 認証、認可、そして暗黙の信頼ゾーンを細分化し、認証メカニズムの可用性を維持して一時的な遅延を最小限に抑える
  - ■ アクセスルールもリクエストがアクションを実行するために必要な最小限の権限として可能な限り細かくする

■ アクセスは、ポリシー決定ポイント（PDP：policy decision point ）および対応するポリシー実施ポイント（PEP：policy enforcement point ）を通じて許可される

[Source] NIST, SP800-207 Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.4-5;Figure 1 Zero Trust Access,（発表者による仮訳）（access 2023/1/23)

2.2 ZTAの前提と原則 (3)

NIST SP800-207にはZTAの考え方を示す（Tenets of Zero Trust）

- **ZTAは、7つの基本原則を記述する。**
  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はリソースと見なす。
  2. ネットワークの場所に関係なく、すべての通信が保護される。
  3. 個々の事業体のリソースへのアクセスは、セッションごとに許される。
  4. リソースへのアクセスは、クライアントのアイデンティティ、アプリケーション／サービス、および要求している資産に観測された状況を含む動的ポリシーによって判定されるが、他の動作や環境の属性が含まれる場合もある。
  5. 事業体は、所有および関連するすべての資産の整合性とセキュリティポスチャーを監視および測定する
  6. すべてのリソースの認証と認可は動的であり、アクセスが許可される前に厳密に実施される。
  7. 事業体は、資産とネットワークインフラストラクチャと通信の現在の状態に関するできるだけ多くの情報を収集し、それを使用してセキュリティポスチャーを改善する。

  原則は、技術にとらわれない。たとえば、「ユーザーの識別（ID）」には、ユーザー名・パスワード、証明書、ワンタイムパスワードなどのいくつかの要素を含めることができる。

  これらの原則は、組織内で、または1つ以上のパートナー組織と共同で行われる作業に適用され、匿名のパブリックまたは消費者向けのビジネスプロセスには適用されない。

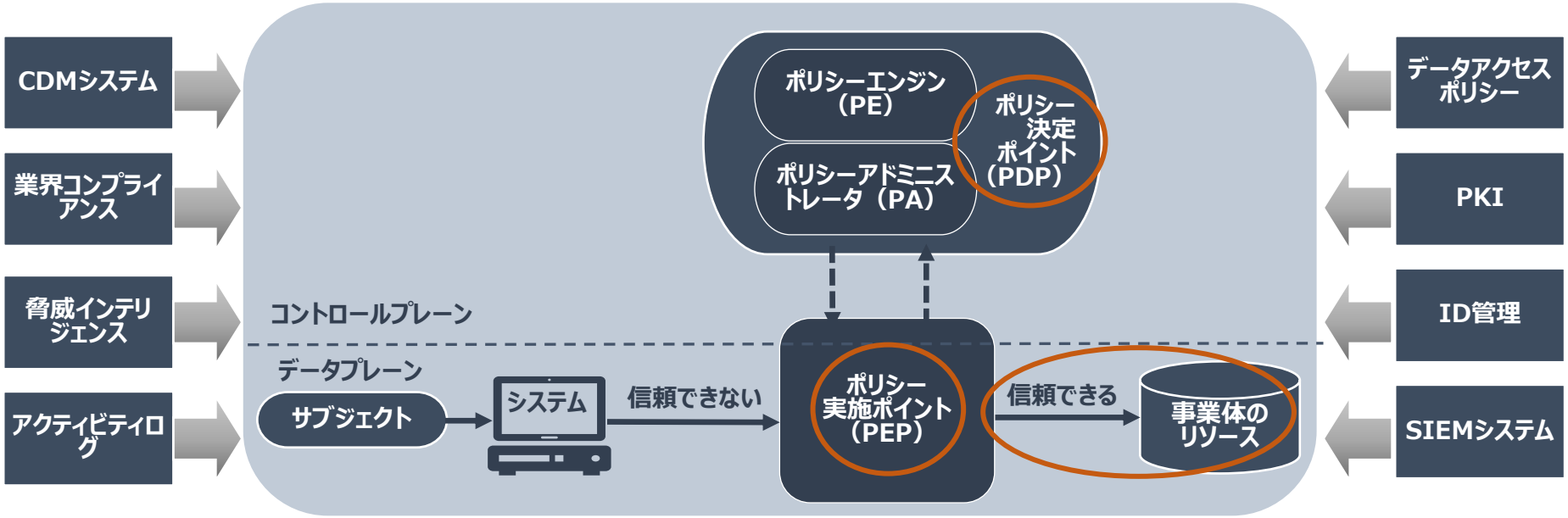
  組織は、外部のアクター（例えば、顧客や一般的なインターネットユーザー）に内部ポリシーを課すことはできないが、組織と特別な関係にある事業体以外のユーザ（例えば登録済みの顧客、従業員の扶養家族等）にゼロトラストベースのポリシーを実装できる場合がある。

[2] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020) Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.6-7（発表者による仮訳）（access 2023/1/23）

2.3 ZTAの論理コンポーネント (1)

概念フレームワークモデル

- 事業体のゼロトラストアーキテクチャ配備を構成する論理コンポーネントは数えきれないほどあり、オンプレミスサービスとして、またはクラウドベースのサービスとして運用される
- ポリシー決定ポイント（PDP）は、ポリシーエンジンとポリシーアドミニストレータの2つの論理コンポーネントに分類され、論理コンポーネントは、個別のコントロールプレーンを使用して通信するが、アプリケーションデータはデータプレーンで通信する



[出典] NIST, SP800-207, Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, p.9;Figure 2 Core Zero Trust Logical Componets,（発表者による仮訳）（access 2023/1/23)

2.3 ZTAの論理コンポーネント (2)

ポリシー決定ポイント（PDP)

- **ポリシーエンジン（PE）**：事業体のポリシーと外部ソース（CDMシステム、脅威インテリジェンスサービス）からの入力を使用して、信頼アルゴリズムに従ってリソースへのアクセスを許可、拒否、または取り消す決定を行ってログに記録し、これに基づいてポリシーアドミニストレータが決定を実行する。
- **ポリシーポリシーアドミニストレータ（PA）**：サブジェクトが事業体のリソースにアクセスするために使用するセッション固有の認証と認可トークンまたは認証情報を生成する。PEの決定に依存し、セッションが許可され、要求が認証されると、PAはPEPを構成してセッションの開始を許可する。セッションが拒否された場合、PAはPEPに信号を送り、接続をシャットダウンする。PEとPAを単一のサービスとして実装する場合があるが、論理的には２つのコンポーネントに分ける。PAが通信パスを作成するときのPEPとの通信は、コントロールプレーンを介して行われる。

ポリシー実施ポイント（PEP)

- **ポリシー実施ポイント（PEP）:**サブジェクトと事業体のリソース間の接続の有効化、監視、および最終的な終了を行う。PEPはPAと通信し、その要求を転送したり、PAからのポリシーの更新を受信したりする。これは、ゼロトラストアーキテクチャの一つの論理コンポーネントであるが、クライアント（例えば、ラップトップ上のエージェント）とリソース側（たとえば、アクセスをコントロールするリソースの前にあるゲートウェイコンポーネント）の2つの異なるコンポーネントに分割されることもあるし、通信パスのゲートキーパーとして動作する単一のポータルコンポーネントのこともある。PEPの先には、事業体のリソースをホストする信頼ゾーンがある。

[Source] NIST, SP800-207 Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, p.9;Figure 2 Core Zero Trust Logical Componets,（発表者による仮訳）（access 2023/1/23)

2.3 ZTAの論理コンポーネント (3)

データソース

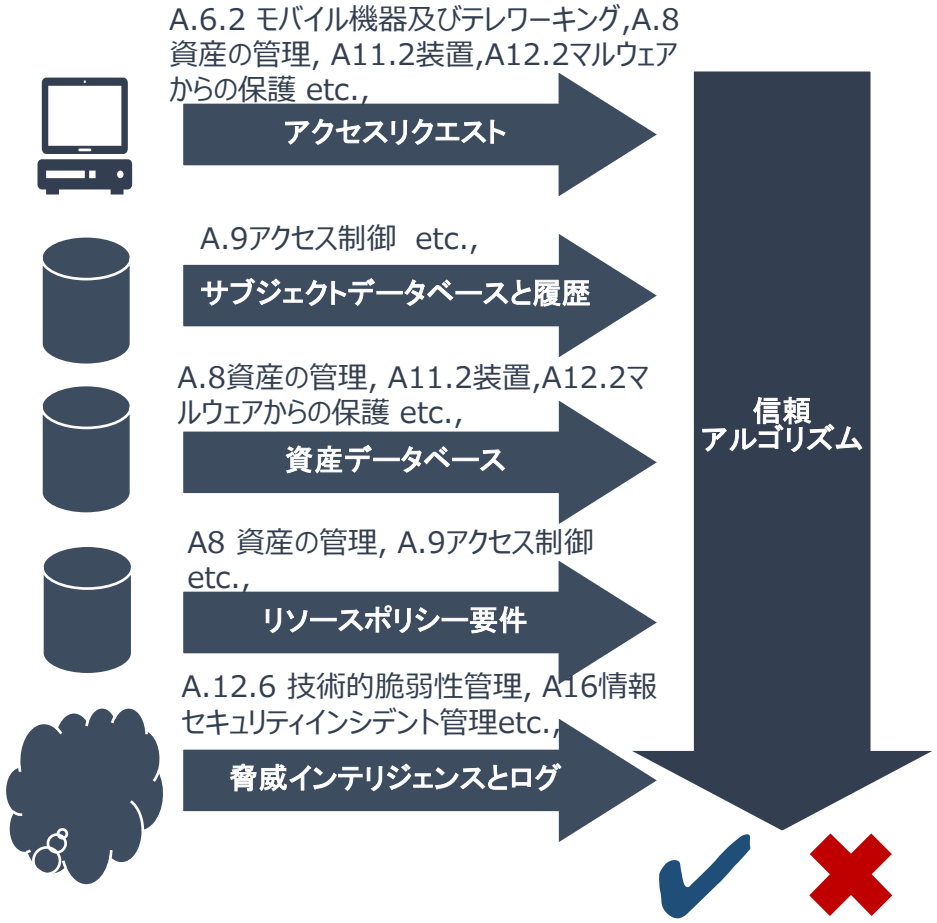
- **継続的診断対処（CDM）システム：**アクセス要求を行う資産に関する情報 - パッチが適用されたOS、・・・既知の脆弱性の有無、etc.
- **業界コンプライアンスシステム：**事業体に適用される規制制度・コンプライアンスを確保するためにのすべてのポリシールール、etc.
- **脅威インテリジェンス配信：**内部や外部からの攻撃・脆弱性情報 - ソフトウェアで発見された欠陥、マルウェア、他の資産への攻撃の報告、etc.
- **ネットワークおよびシステムアクティビティログ：**情報システムのセキュリティ体制に関するリアルタイムのフィードバック - 資産ログ、ネットワークトラフィック、etc.

- **データアクセスポリシー：**定義されたミッションの役割と組織のニーズに基づく、事業体のリソースへのアクセスに関する属性、ルール、ポリシー、etc.
- **公開鍵インフラストラクチャ（PKI）：**事業体の電子証明書を生成し、リソース、サブジェクト、サービス、アプリケーションの記録、etc.
- **ID管理システム：**ユーザーアカウントとアイデンティティレコードを作成、保存、管理 - サブジェクト情報、役割、アクセス属性、割当資産、etc.
- **セキュリティ情報およびイベント管理（SIEM）システム：**分析用セキュリティ情報の収集、事業体資産に対する攻撃の可能性の警告、etc.

[Source] NIST, SP800-207 Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, p.9;Figure 2 Core Zero Trust Logical Componets,（発表者による仮訳）（access 2023/1/23)

2.3　ZTAの論理コンポーネント (4)

信頼アルゴリズム



- **信頼アルゴリズム（TA）；**ポリシーエンジンのプロセス
  - アクセス要求：サブジェクトからの要求および要求者に関する情報（OSバージョン、使用ソフトウェア（承認アプリケーション）、パッチレベル等）
  - サブジェクトデータベース：「誰が」リソースへのアクセスを要求しているか（組織または共同作業者のサブジェクト（人とプロセスのセット）、サブジェクト属性や特権、ユーザーアイデンティティ（アカウントIDとPEPによって実行された認証チェックの結果の組み合わせ、時間と地理位置情報）、過去のサブジェクトの動作）
  - 資産データベース：資産の既知の状況（OSバージョン、存在するソフトウェア、その整合性、場所（ネットワークの場所と地理的場所）、パッチレベル）- リクエストを行っているアセット状況と比較する
  - リソースアクセス要件：リソースへのアクセスの最小要件を定義（MFA ネットワークの場所（海外のIPの拒否）、認証システムの保証レベル（データの機密性、資産構成の要求））
  - 脅威インテリジェンス：外部サービスまたは内部スキャンと検出からの、インターネット上の脅威とアクティブなマルウェアの情報（疑わしいデバイスの通信を特定する情報）

[Source] NIST, SP800-207 Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.17-19;Figure 7 Trust Algorithm Input,（発表者による仮訳）（access 2023/1/23)

2.3　ZTAの論理コンポーネント (5)

ZTAを境界ベースアーキテクチャのネットワークに導入するためのステップ　– ZTAへの移行シナリオ

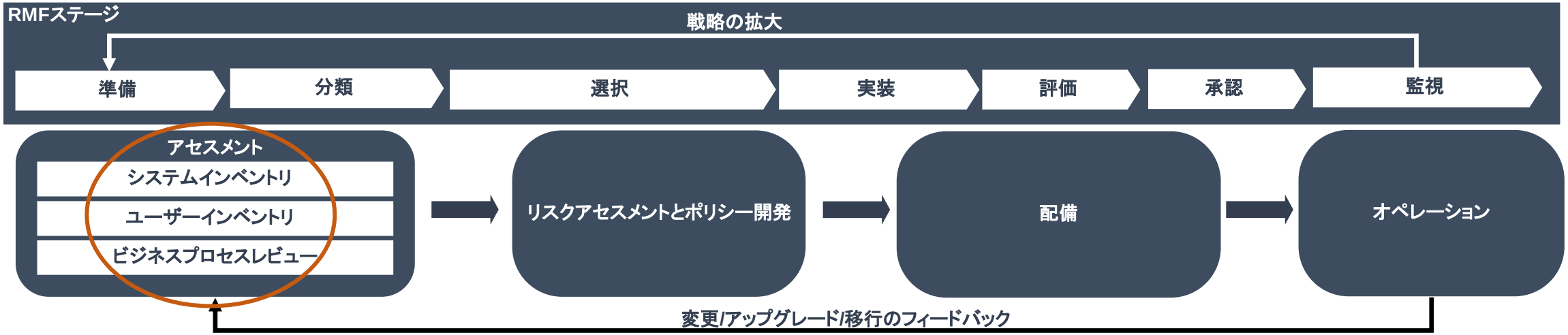
- ZTAの実装は、インフラストラクチャやプロセスの大規模な置き換えではなく旅。
- **ピュアゼロトラストアーキテクチャ**
  - ■グリーンフィールドアプローチ（訳注：新規開発）では、ゼロトラストアーキテクチャをゼロから構築することができるが、既存の組織の現実的な選択肢となることは少ない。
- **ハイブリッドゼロトラストアーキテクチャと境界ベースのアーキテクチャ**
  - ■大きなエンタープライズが単一のテクノロジー更新サイクルでゼロトラストに移行する可能性は低い。エンタープライズではゼロトラストアーキテクチャワークフローと、非ゼロトラストアーキテクチャワークフローは共存し、その期間は明確ではないだろう。
  - ■既存のワークフローをZTAに移行するには、（少なくとも）部分的な再設計が必要になるだろう。

[Source] NIST, SP800-207 Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.36-37;（発表者による仮訳）（access 2023/1/23)

2.3　ZTAの論理コンポーネント (6)

ZTAを境界ベースアーキテクチャのネットワークに導入するためのステップ　– ZTAへの移行シナリオ

- *ZTA*に移行するには、組織がその資産（物理および仮想）、サブジェクト（ユーザー特権を含む）、およびビジネスプロセスについて詳細な知識を持っている必要がある。この知識は、リソース要求を評価するときに*PE*によってアクセスされる。
- ZTAを事業体に導入する取り組みの前に、資産、サブジェクト、データフロー、ワークフローを調査する必要がある。この認識は、ゼロトラストアーキテクチャの展開が可能になる前に到達する必要のある基礎の状態である。
- 初期インベントリが作成された後には、定期的なメンテナンスと更新のサイクルがある。この更新には、ビジネスプロセスが変更される場合も、影響がない場合もあるが、ビジネスプロセスの評価を実施する必要がある。

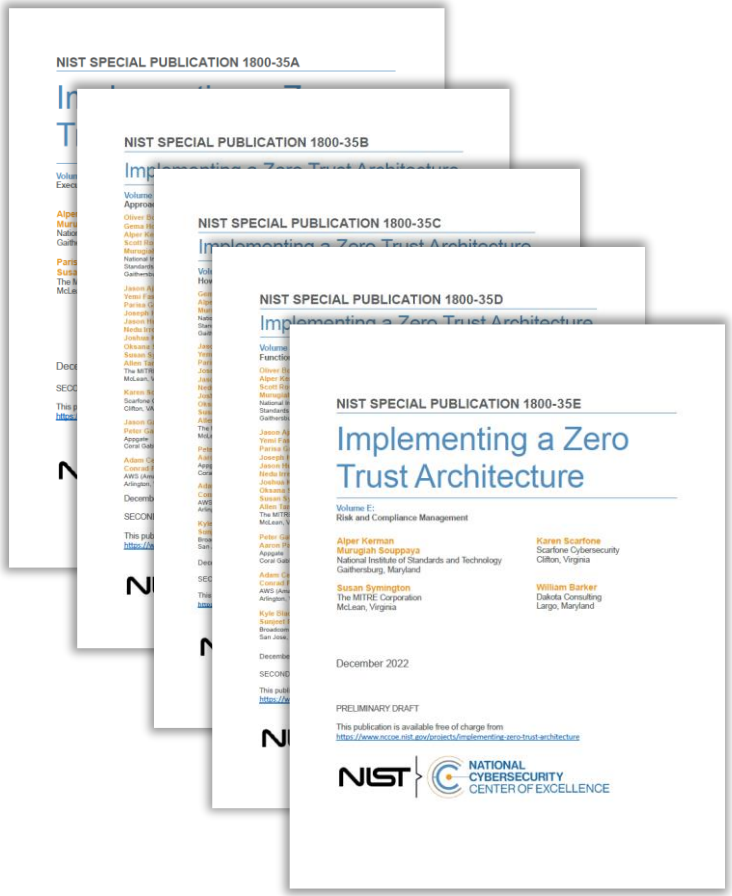


[Source] NIST, SP800-207, Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.37-38., Figure 12: ZTA Deployment Cycle（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (1)

リファレンス
NIST SPECIAL PUBLICATION 1800-35 Implementing a Zero Trust Architecture

- このガイドは、NCCoE (National Cybersecurity Center of Excellence) とその協力者達が**市販のテクノロジを使用して、NIST Special Publication (SP) 800-207、ゼロトラストアーキテクチャ Zero のコンセプトと原則に沿った相互運用可能なオープン スタンダード ベースの ZTA 実装を構築する方法をまとめたもの。**従来の汎用エンタープライズ情報技術 (IT) インフラストラクチャを保護するトラスト アーキテクチャ。プロジェクトが進行するにつれて、この 2 番目の予備ドラフトが更新され、コメントのために追加のボリュームもリリースされる。
  - **Volume A: エグゼクティブサマリー (Draft 第２版)**
  - **Volume B: アプローチ、アーキテクチャとセキュリティの特徴(Draft 第２版)**
  - Volume C: ハウツーガイド(Draft 第２版)
  - Volume D: 機能デモンストレーション(Draft 第２版)
  - **Volume E: リスクとコンプライアンスの管理(Draft)**



[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf , p.1,（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (2)

NIST SP1800-35の構成

- **最高情報セキュリティ責任者や技術責任者を含むビジネスの意思決定者**は、**NIST SP 1800-35A: エグゼクティブサマリー**を使用し、ソリューションが組織にどのように役立つか、このガイドのドライバー、私たちが対処するサイバーセキュリティの課題と、この課題を解決するためのアプローチを理解することができる。
- **テクノロジー、セキュリティ、およびプライバシープログラムマネージャー**（リスクを特定、理解、評価、および軽減する方法に関心のある）は、**NIST SP 1800-35B: アプローチ、アーキテクチャ、およびセキュリティの特徴**を使用できる。そしてまた、**NIST SP 1800-35E: リスクとコンプライアンスの管理**は、一般的な ZTA 参照設計の論理コンポーネントを、さまざまなサイバーセキュリティガイドラインと推奨実務ドキュメントに記載のセキュリティ特性にマッピングしている。
- **ITプロフェッショナル**（このようなアプローチを実装したい）は、**NIST SP 1800-35C: ハウツーガイド**を利用できる。このガイドには、製品のインストール、構成、およびこのプロジェクトの実装例を構築するための統合のステップに関する重要な手順が記載されており、それらの全体または一部をそのまま再現することができる。また、**NIST SP 1800-35D:機能デモンストレーション**を使用することもできる。これは、ZTA セキュリティ機能を紹介するために定義されたユース ケースと、各実装例でそれらを実証した結果を提供している。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf , p.4,（発表者による仮訳）（access 2023/1/23)

2.4　NISTのZTAの実装 (3)

エグゼクティブサマリー

NIST SP1800-35 Volume A は私たちが取り組むべきサイバーセキュリティの課題を示す。

⑴ 保護する必要があるビジネス アプリケーション、資産、およびプロセスを完全に理解するために必要な、適切な資産インベントリと管理の欠如。これらのリソースの重要性を明確に理解していないこと。

- A.8.1.1資産目録 他

⑵ 特定のアプリケーションやサービスに対して、きめ細かく、知る必要のあるアクセス ポリシーを実施するために必要な、組織全体のユーザー ロールの適切なデジタル定義、管理、および追跡の欠如。

- A.8.1.2資産の管理責任, A8.1.3資産利用の許容範囲 他

⑶ オンプレミスとクラウドの環境全体で通信フローと分散 IT コンポーネントがますます複雑になり、一貫した管理が困難なこと。

- A.9.1.2ネットワーク及びネットワークサービスへのアクセス, A.13通信のセキュリティ 他

⑷ 組織の通信および使用パターンの可視性の欠如 - 組織のサブジェクト、資産、アプリケーション、およびサービス間で発生するトランザクションの理解が限られていること、およびこれらの通信とその特定のフローを識別するために必要なデータがないこと。

- A.8.1.1資産目録, A8.1.3資産利用の許容範囲, A.9.1.2ネットワーク及びネットワークサービスへのアクセス 他

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf , pp.1-2,（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (3)

⑸ デバイスの正常性やサプライ チェーンのリスクへのエクスポージャを理解する際に、誤った仮定が行われることがよくあること。

- A.11.2.6 構外にある装置及び資産のセキュリティ, A.15 供給者関係 他

⑹ どのような相互運用性の問題が関係している可能性があるか、または管理者、セキュリティ担当者、オペレーター、エンドユーザー、およびポリシーの意思決定者が必要とする可能性のある追加のスキルとトレーニングに関する理解が欠如すること。必要なポリシーを開発するためのリソースと、移行計画を通知するために必要なパイロットまたは概念実証の実装が不足すること。

- A.11.2.6 構外にある装置及び資産のセキュリティ, A.15 供給者関係 他

⑺ 既存の投資を活用し、優先事項のバランスを取りながら、モダナイゼーション イニシアチブを通じて ZTA に向けて前進すること。

- A.5 情報セキュリティのための方針群 他

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf , pp.1-2,（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (3)

⑻ 完成されたZTAを構築するために、さまざまな成熟度のさまざまな種類の市販のテクノロジを統合し、機能を評価し、テクノロジのギャップを特定すること。

⑼ ZTA が環境の運用やエンドユーザー エクスペリエンスに悪影響を及ぼすのではないかという懸念。

⑽ セキュリティ ポリシーを配布、管理、実施するための標準化されたポリシーの欠如により、組織が断片的なポリシー環境または相互運用できないコンポーネントのいずれかに直面すること。

⑾ コミュニティ全体および組織内での ZTA に関する共通の理解と言語の欠如、組織の ZTA の成熟度の評価、ビジネスに最適な ZTA アプローチの決定、および実装計画の策定。

⑿ ZTA があらゆる規模の組織に適した一連の指針であるという認識ではなく、ZTA は大規模な組織にのみ適しており、多額の投資が必要であるという誤解。

⒀ すべてに適合する単一の ZTA はなく、ZTAがは、組織の要件とリスク許容度、および既存の投資されたテクノロジと環境に基づいて、組織ごとに設計および統合するべきものであること。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf , pp.1-2,（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (4)

アウトカム　– サンプルソリューションとそのシナリオのサポート

- ZTAの実装プロジェクトの成果は、サンプル ソリューションを開発し、それらがさまざまなシナリオをサポートすることを実証し、さまざまな対象者を対象とした複数のボリュームで構成される NIST SP 1800 であるこのプラクティス ガイドで調査結果を公開することである。

○ ユーザーの場所やユーザーデバイス (管理対象または非管理対象) に関係なく、リソースへのユーザーアクセスをサポート
○ 場所 (オンプレミスまたはクラウドベース) に関係なく、ビジネス資産とプロセスを保護
○ 内部関係者の脅威を制限 (内部関係者 (ユーザーと個人以外のエンティティの両方) は、自動的には信頼されない)
○ 侵害を制限 (攻撃者が環境内を横方向に移動する能力を低下させる)
○ 事業体の機密情報をデータ セキュリティ ソリューションで保護
○ リソースのインベントリ、実装されている構成と制御、すべての通信とその特定のフロー、およびリソースへのアクセスと保護の方法に対する可視性を向上させ、この理解を使用した、有用で完全なセキュリティ ポリシーの策定および適用
○ リアルタイムかつ継続的な監視とログ記録、およびリソース アクセスのポリシー主導型、リスクベースの評価と適用の実行

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf , pp.2-3,（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (5)

NIST SP1800-35 Volume B アプローチ、アーキテクチャとセキュリティの特徴として ①ユースケース ②ZTAの一般的な参照アーキテクチャ ③アクセスの制限 を解説

①ユースケース

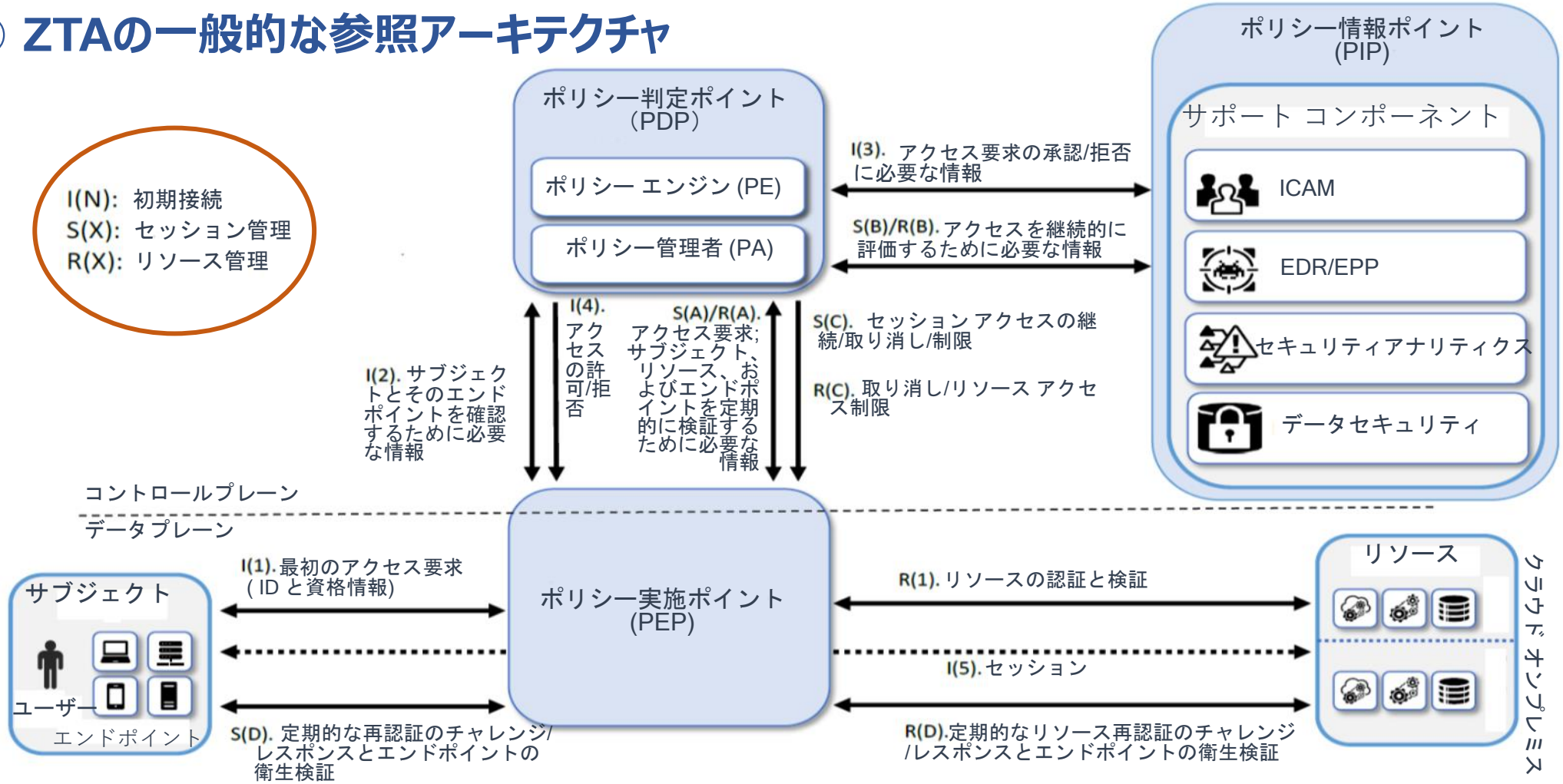
たとえば、現在導入されているVPN によるリモートアクセスのテクノロジーをゼロトラストアーキテクチャに置き換える必要があるかどうかを考える場合、社内の環境で社内パソコンからシステムにアクセスを許されていた人が、そのシステムを社外で使用するためにVPN に接続してきたときのセキュリティを確保できているかどうかをチェックする。

- 従業員、特権のある第三者、およびゲストによるアクセス
- 公衆 Wi-Fi 、インターネットを介して、本社、支社、またはテレワークにいるユーザーから要求されたアクセス
- サーバー間アクセス
- オンプレミスとクラウドの両方にあるリソースの保護
- 事業体が管理するデバイス、契約者が管理するデバイス、および個人用デバイスの使用
- 事業体リソースと公的に利用可能なインターネット サービスの両方へのアクセス
- リソース アクセス リクエストのきめ細かな信頼レベルを自動的かつ動的に計算する機能

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf , pp.7-8,（発表者による仮訳）（access 2023/1/23)

2.4 NISTのZTAの実装 (5)

② ZTAの一般的な参照アーキテクチャ



事業体が高度に分散されたシステムを持っている場合、さまざまな場所にあるリソースを保護するために多くの PEP が存在する。また、負荷分散をサポートするために複数の PEP を持つこともあるが、簡単にするために、単一の PEP、単一のサブジェクト、および単一のリソースを含む相互作用に焦点を限定している。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf , p.50 Figure 4-1 , （発表者による仮訳） （access 2023/1/23)

2.4 NISTのZTAの実装 (5)

③ ZTAの一般的な参照アーキテクチャとアクセス制限

ZTAの論理コンポーネントについて、Volume Bでは「ZTAの一般的な参照アーキテクチャ」を示し、アプローチ、アーキテクチャとアクセスの制限を解説している。。

⑴ 論理コンポーネントに示されたPEPやPDPがどのような流れでアクセスを許可し、セッションを管理するか

⑵ 「サブジェクト」と「リソース」、I(X)：初期接続、R(X)：リソース管理、S(X)：セッション管理の流れ

⑶ ポリシー実施ポイントの認証、その管理状況に問題が無いことの確認（衛生検証）

2.4 NISTのZTAの実装 (6)

NIST SP1800-35 Volume E リスクとコンプライアンスの管理

従来のアーキテクチャとの比較

従来	ＺＴＡ
①ネットワークセキュリティ	
・境界防御に重点を置く ・いったん侵入されるとネットワーク境界内を容易に横方向に展開されてしまうなど、ネットワーク内のサブジェクトが侵害された場合に弱い	・各リソースを個別に保護 ・職務を遂行するために必要があるリソースのみにアクセスすることができるので、侵入者や悪意のある内部者の脅威を制限することができる
②リソースへのアクセス要求	
・リソースへのアクセスを許可した後、アクセスセッションを監視していないと不正アクセスに成功した攻撃者に十分な時間を与えてしまう	・アクセス許可を継続的に検証することで、リソースへのアクセスを許可した後の脅威も制限する
③クラウドコンピューティング	
・クラウドは従来のネットワーク境界の外にあり、従来のネットワーク境界戦略では保護できない	・ネットワークの場所にかかわらず各リソースを個別に保護する

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.3-5（発表者による仮訳）（access 2023/1/23）

2.4 NISTのZTAの実装 (6)

従来のアーキテクチャとの比較

従来	ＺＴＡ
④ リモートワーカー	
・事業体リソースへの承認済みアクセスを要求するサブジェクトの再アクセスは、経由経路、アクセス者者本人、リソースへのアクセス範囲の判別、制限が曖昧な可能性がある	・事業体内での役割または事業体との関係に関して、どのリソースへのアクセスを許可されているかを正確に判断するための認証および許可サービスで、アクセスする必要があるリソースのみに制限できる
⑤外部コンポーネントの利用	
・必要な機能を実行するために一部の事業体リソースにアクセスする必要がある場合があるが、ネットワーク境界内のすべてのリソースへの包括的なアクセスを許可してしまう	・すべてのサブジェクトが、目的を達成するためにアクセスする必要があるリソースのみに限定できる ・攻撃者にとっての有用性は限定的であり、一般的な攻撃ベクトルとして機能することはない

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.3-5（発表者による仮訳）（access 2023/1/23）

2.4 NISTのZTAの実装 (6)

従来のアーキテクチャとの比較

従来	ＺＴＡ
⑥ リスクマネージメント	
境界防御の脆弱性 ・ネットワーク境界防御パラダイムが有効な環境での無許可アクセスに対するリソースの脆弱性は、境界内のすべてのサブジェクトに配置される暗黙の信頼の結果である ・境界内のすべてのリソースが互いに到達可能であるにもかかわらず、セキュリティ境界が外部の脅威に対する包括的な保護のみ ・1 つのサブジェクトが侵害されると、境界内で到達可能な多くのリソースが侵害される可能性がある。 ・リソース アクセス セッションは継続的に評価されないため、リソースは、最初のアクセス要求の許可を得てサブジェクトまたはリソースを侵害することに成功した悪意のあるアクターによる攻撃に対して脆弱である。	ZTAのリスクと制約 ・ゼロトラストアーキテクチャ自体のコアコンポーネント(ポリシーエンジン、ポリシー管理者 、またはポリシー実施ポイントなど)や、コアコンポーネントに重要な情報を提供する機能が侵害された悪用に対して脆弱である ・ゼロトラストアーキテクチャは、侵害されたシステムまたはリソースを修正するのには役立たない

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.3-5（発表者による仮訳）（access 2023/1/23）

2.5 リスクと情報セキュリティ管理 (1)

ZTA リファレンス アーキテクチャ セキュリティ マッピング

- ZTA 参照設計の論理コンポーネント によって実行されるサイバーセキュリティ機能と、さまざまな関連するサイバーセキュリティ ドキュメントに列挙されているセキュリティ特性との間のマッピング
  - 重要インフラのサイバーセキュリティを改善するためのフレームワーク (NIST サイバーセキュリティ フレームワーク CSF) 1.1 サブカテゴリ、
  - NIST SP 800-53r5 (情報システムおよび組織のためのセキュリティおよびプライバシー管理) セキュリティ管理
  - 大統領令 (EO) 14028 大統領令 (EO) 14028の下で使用される「EO-Critical Software」のセキュリティ対策で定義されたセキュリティ対策
- マッピングのすべての要素 (ZTA サイバーセキュリティ機能、CSF サブカテゴリ、SP 800-53 コントロール、および EO 14028 セキュリティ対策) は、サイバーセキュリティ リスクを軽減し、セクター固有の推奨プラクティスを含むコンプライアンス要件を満たす方法を含む概念である。

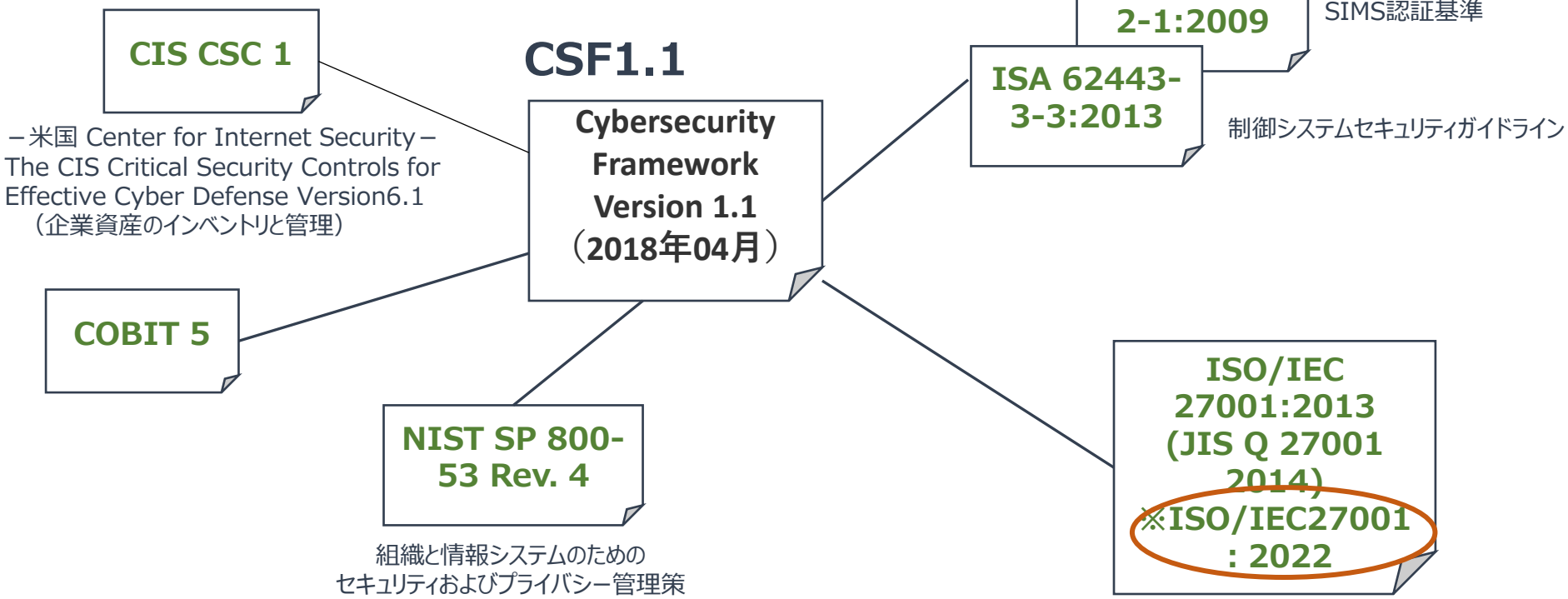
注）上記のうち、「ZTA サイバーセキュリティ機能とCSF サブカテゴリ」の研究に使用した仮訳を「付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング」として掲載しました。
出典がドラフトであること、研究目的の仮訳であることに留意して、参考としてご覧ください。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.5-8（発表者による仮訳） （access 2023/1/23）

【参考】 CSF / ISMS(ISO/IEC 27001) マトリックスとZTAの視点

NCCoEがサイバーセキュリティの課題に適用する製品などの特性を、NIST “CSF”及び適用可能な標準・推奨プラクティスにマップしている。

- **“CSF ”の機能とカテゴリの項目に対応させている参考情報**



[Source] IPA セキュリティ関連NIST文書 https://www.ipa.go.jp/security/publications/nist/index.html を参照して作成

【参考】 ISO/IEC27001：2022

⑴ ISO/IEC 27001：2022
情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項

・タイトルの変更；Information security, cybersecurity and privacy protection - Information security management systems – Requirements
・現状のITサービスに対応；クラウドサービスやICTについてのIT用語、管理策を追加

⑵ ISO/IEC 27002：2022　情報セキュリティ，サイバーセキュリティ及びプライバ シー保護－情報セキュリティ管理策

・8.27 安全なシステム アーキテクチャとエンジニアリングの原則
a. 組織の情報システムはすでに侵害されており、ネットワーク境界セキュリティだけに依存してい ないと仮定する。
b. 情報システムへのアクセスに「決して信頼せず、常に検証する」アプローチを採用する。
c. 情報システムへのリクエストがエンドツーエンドで暗号化されるようにする。
d. 情報システムへの各要求を、組織の内部から発信されたものであっても、オープンな外部ネットワークから発信されたかのように検証する (つまり、境界の内外を自動的に信頼しない)。
e. 「最小特権」および動的アクセス制御技術を使用する (5.15、5.18、および 8.2 を参照)。
これには、認証情報 (5.17 を参照)、ユーザー ID (5.16 を参照)、ユーザー エンドポイント デバイスに関するデータ、およびデータ分類 (5.12 を参照) などのコンテキスト情報に基づ く、情報またはシステムへの要求の認証および承認が含まれる。
f. 認証情報 (5.17 を参照)、ユーザー ID (5.16)、ユーザー エンドポイント デバイスに関する データ、およびデータ分類 (5.12 を参照) を含む情報に基づいて、要求者を常に認証し、 情報システムへの承認要求を常に検証する。
たとえば、強力な認証 (例: 8.5 参照）。

2.5 リスクと情報セキュリティ管理 (2)

CSF1.1とZTAの対応状況

(1) NCCoEはプロジェクトとして、ZTAの標準ベースの実装を示す。
　NIST CSFに沿った一連のサイバーセキュリティの課題に対処する市販のテクノロジを使用したZTAの構築例を推奨する。
(2)「ゼロトラスト アーキテクチャの実装」において、セキュリティ管理マップを示し、CSF機能とZTAに適用可能なカテゴリーをマップしている。(右表朱の記部)

「セキュリティ管理マップ」はCybersecurity Framework Version 1.1（2018年04月）に示される。

　右表は、NCCoE がこのサイバーセキュリティの課題に適用する商用製品の特性を、「重要インフラストラクチャのサイバーセキュリティを改善するためのフレームワーク」およびその他の NIST ガイダンスに記載されている適用可能な標準および推奨プラクティスにマップしている。
　この情報は、ソリューションのセキュリティ特性に対する標準、ガイドライン、および推奨プラクティスの適用可能性を文書化するためのアプローチを表しているが、製品やサービスが規制当局の承認または認定に関する業界の要件を満たすことを意味するものではない。

機能	識別子	カテゴリー	
特定	ID.AM	資産管理	ID.AM−1，2，5
	ID.BE	ビジネス環境	
	ID.GV	ガバナンス	
	ID.RA	リスクアセスメント	ID.RA−1，3
	ID.RM	リスクアセスメント管理戦略	
	ID.SC	サプライチェーンリスクマネジメント	
防御	PR.AC	アクセス制御	PR.AC−1，3，4，5，6，7
	PR.AT	意識向上およびトレーニング	
	PR.DS	データセキュリティ	PR.DS−2，5，6，8
	PR.IP	情報を保護するためのプロセスおよび手順	PR.IP−1，3
	PR.MA	保守	
	PR.PT	保護技術	PR.PT−3，4
検知	DE.AE	異常とイベント	DE.AE−2，3，5
	DE.CM	セキュリティの継続的なモニタリング	DE.CM-1,2,4,5,6,7,8
	DE.DP	検知プロセス	DE.DP−5
対応	RS.RP	対応計画の作成	
	RS.CO	コミュニケーション	
	RS.AN	分析	
	RS.MI	低減	RS.MI−1，2
	RS.IM	改善	
復旧	RC.RP	復旧計画の作成	
	RC.IM	改善	
	RC.CO	コミュニケーション	

[Source] NISTゼロトラスト アーキテクチャの実装 ｐｐ.11～14

【参考】情報セキュリティ管理マップ

NIST「ゼロトラスト アーキテクチャの実装」に、添記のCSF機能マップを参照する。

⇒ CSFに対応したZTAの機能を確認するため

サイバーセキュリティ フレームワーク v1.1		
機能	カテゴリ	サブカテゴリ
識別 (ID)	アセットマネジメント（ID.AM）	ID.AM-1: 組織内の物理デバイスとシステムがインベントリされます。
		ID.AM-2: 組織内のソフトウェア プラットフォームとアプリケーションがインベントリされます。
		ID.AM-5: リソース (ハードウェア、デバイス、データ、時間、人員、ソフトウェアなど) は、分類、重要度、およびビジネス価値に基づいて優先順位付けされます。
	リスク評価 (ID.RA)	ID.RA-1: 資産の脆弱性が特定され、文書化されています。
		ID.RA-3: 内部と外部の両方の脅威が特定され、文書化されています。
プロテクト (PR)	ID 管理、認証、およびアクセス制御 (PR.AC)	PR.AC-1: ID と資格情報は、承認されたデバイス、ユーザー、およびプロセスに対して発行、管理、検証、取り消し、および監査されます。
		PR.AC-3: リモート アクセスが管理されている。
		PR.AC-4: 最小限の特権と職務の分離の原則を取り入れて、アクセス許可と承認を管理します。
		PR.AC-5: ネットワークの完全性が保護されている (ネットワークの分離、ネットワークのセグメンテーションなど)。
		PR.AC-6: ID は証明され、クレデンシャルにバインドされ、相互作用でアサートされます。

サイバーセキュリティ フレームワーク v1.1		
機能	カテゴリ	サブカテゴリ
		PR.AC-7: ユーザー、デバイス、およびその他の資産は、トランザクションのリスク (個人のセキュリティとプライバシーのリスク、およびその他の組織のリスクなど) に見合った認証 (単一要素、多要素など) が行われます。
	データセキュリティ (PR.DS)	PR.DS-2: 転送中のデータは保護されています。
		PR.DS-5: データ漏洩に対する保護が実装されています。
		PR.DS-6: ソフトウェア、ファームウェア、および情報の完全性を検証するために、完全性チェック メカニズムが使用されます。
		PR.DS-8: ハードウェアの完全性を検証するために、完全性チェック メカニズムが使用されます。
	情報保護のプロセスと手順 (PR.IP)	PR.IP-1: IT/産業用制御システムのベースライン構成が作成および維持され、セキュリティ原則 (最小機能の概念など) が組み込まれています。
		PR.IP-3: 構成変更管理プロセスが整備されています。
	保護技術 (PR.PT)	PR.PT-3: 必須機能のみを提供するようにシステムを構成することにより、最小機能の原則が組み込まれます。
		PR.PT-4: 通信および制御ネットワークは保護されています。

サイバーセキュリティ フレームワーク v1.1		
機能	カテゴリ	サブカテゴリ
探知	異常とイベント (DE.AE)	DE.AE-2: 検出されたイベントを分析して、攻撃の対象と方法を理解します。
		DE.AE-3: イベント データは、複数のソースとセンサーから収集され、関連付けられます。
		DE.AE-5: インシデント アラートのしきい値が設定されています。
	セキュリティ継続的監視 (DE.CM)	DE.CM-1: ネットワークは、潜在的なサイバーセキュリティ イベントを検出するために監視されています。
		DE.CM-2: 潜在的なサイバーセキュリティ イベントを検出するために、物理環境が監視されます。
		DE.CM-4: 悪意のあるコードが検出されました。
		DE.CM-5: 不正なモバイル コードが検出されました。
		DE.CM-6: 潜在的なサイバーセキュリティ イベントを検出するために、外部サービス プロバイダーのアクティビティが監視されます。
		DE.CM-7: 許可されていない人員、接続、デバイス、およびソフトウェアの監視が実行されます。
		DE.CM-8: 脆弱性スキャンが実行されます。
	検出プロセス (DE.DP)	DE.DP-5: 検出プロセスは継続的に改善されています。
応答	緩和 (RS.MI)	RS.MI-1: インシデントは封じ込められています。
		RS.MI-2: インシデントは軽減されます。

[Source] NIST ゼロトラスト アーキテクチャの実装 pp.11～14 October 2020

2.5 リスクと情報セキュリティ管理（3） －CSF、ISO/IEC27001とZTAの視点

ISMS 該当項目		ID 識別						PR 防御						DE 検知			RS 対応					RC 復旧			備考
付属書A.以外の該当項目		AM	BE	GV	RA	RM	SC	AC	AT	DS	IP	MA	PT	AE	CM	DP	RP	CO	AN	MI	IM	RP	IM	CO	凡例：
4.1項：組織の状況、6項：計画、7.4項：コミュニケーション、8.3項：リスク対応、9項：パフォーマンス評価、9.3項：レビュー、10項：改善			4.1	6		8.3 9.3					9 10							7.4			10		10	7.4	(1) 表内のCSFカテゴリとISMS項目の ○：両者に適合、 ◎：適合するZTAの特性 (2) 下記ISMS項目はCFSカテゴリに該当無し
A.5	情報セキュリティ方針			○																					A.5.1.2無
A.6	組織	○		○	◎	○		◎	○	◎	○					○		○						○	A.6.1.4/5無
A.7	人的資源のセキュリティ			○				◎	○	◎						○		○							
A.8	資産の管理	◎				○				◎			○												A.8.1.3無
A.9	アクセス制御							◎		◎	○		◎												A.9.2.5無
A.10	暗号									◎															A.10.1.2無
A.11	物理的及び環境的	○	○			○		◎		◎	○	○	○		◎										
A.12	運用のセキュリティ	◎	○		◎				○	◎	◎		○	◎	◎				○	◎					
A.13	通信のセキュリティ	○	○					◎		◎			◎	○											
A.14	システム導入開発・保守							◎		◎	◎		◎		◎	○									A.142.6/9、A.14.3.1無
A.15	供給者関係		○	○			○					○			◎										
A.16	インシデント管理				○						○			◎		◎	○	○	○	◎	○	○	○		
A.17	継続		○	○			○			○	○		○												
A.18	順守				○			◎			○					○									A.18.1.2/2、A18.2.1無
		1,2 ,5	3無		1,3			1,3 ～ 7		2,5 ,6, 8	1, 3		3,4	2,3 ,5	1無 1,2, 4～ 8	5			5無	1,2					凡例：黒字(例 3無＝BE-3)はISMSに該当無し 赤字は ZTA 該当のCSF項目

[Source] “Cybersecurity Framework Version 1.1 ” と NIST “ゼロトラストアーキテクチャの実装”より作成

2.5 リスクと情報セキュリティ管理 (4)

CSFとISMSを俯瞰し、導き出せることは次のとおり。

⑴ CSFとISMSは、情報セキュリティの機能・管理策として、互いに網羅されており、差異はない。

⇒ システム監査において、例えばチェックリストの形で両者を適用できる。

⑵ CSFの表2 “フレームワークコア”に示されるとおり、CSFはISMSの付属書A以外の項目を参照・リンクさせている。 （4.1項：組織の状況、6項：計画、7.4項：コミュニケーションなどの7項目）

なお、CSFの ID識別 BE-3、DE検知 CM-3、RS対応 AN-5の３つは参考情報のISMSがない。

また、ISMSの A.5.1.2、A.6.1.4と6.1.5、A.8.1.3などの12項目がCSFに該当するカテゴリはない。

⇒ CSF、ISMSをシステム監査に適用する場合、上述のリンクされていない項目の吟味が必要といえる。

⑶ ZTAについては、NIST “ゼロトラストアーキテクチャの実装”の「セキュリティ管理マップ」に、対応するCSF機能をピックアップしている。（シート78、79参照、シート80のマトリックス表に適合するZTA項目を◎で示す）

⇒ ZTAにおいて、ISMSからは、A.8 資産管理、及びA.12 運用のセキュリティの着眼がポイントとなる。

A.12では、マルウェアからの保護、ログの取得・監視、技術的脆弱性の管理が求められている。

CSFからは、PR 防御の AC アクセス制御、DS データセキュリティ、PT 保護技術に、DE 検知の CM セキュリティの継続的なモニタリングの着眼が求められる。

[Source] https://csrc.nist.gov/publications/detail/sp/1800-35/draft

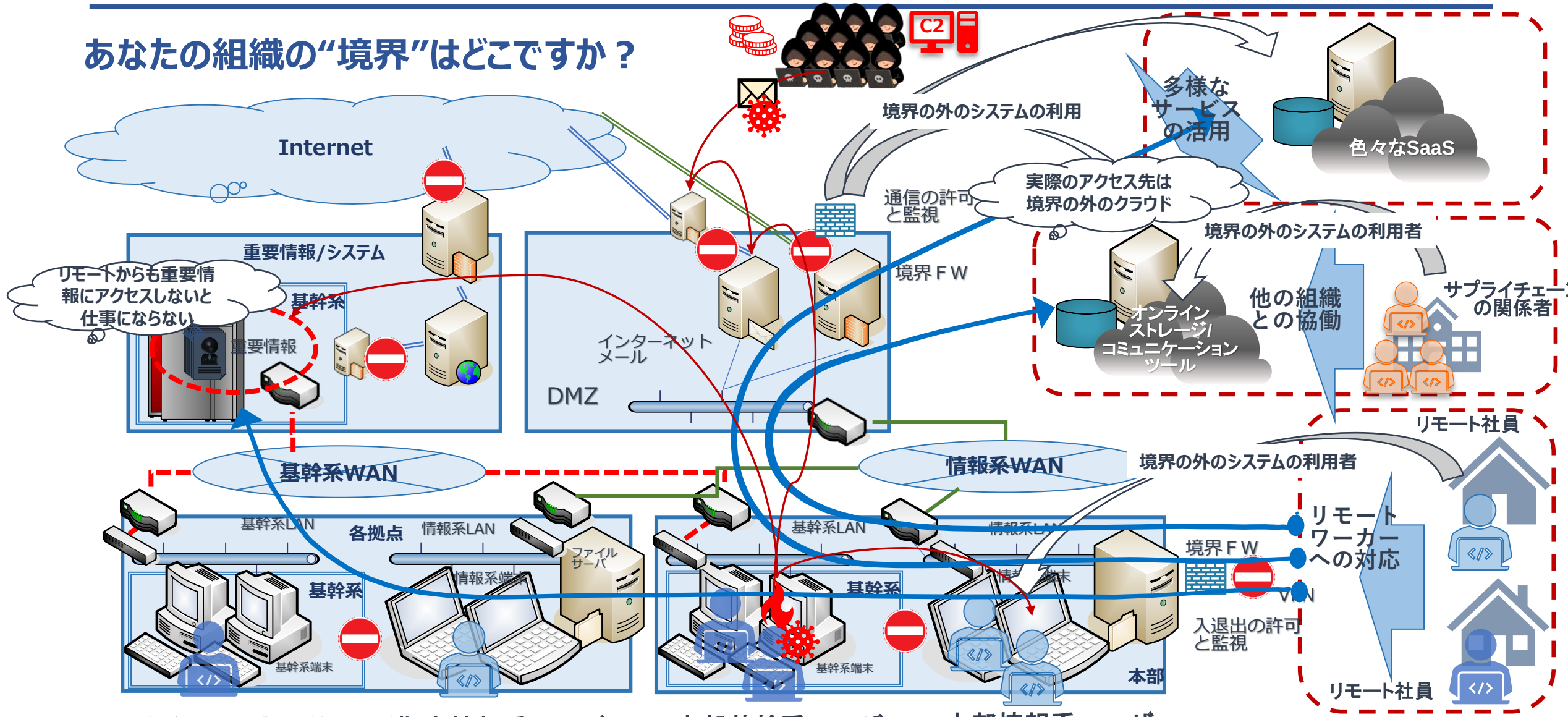
2.6 ZTAとシステム監査 (1)

システム監査の際の考慮事項

- ZTAは、「目的」ではなく、複数の内部ネットワーク、独自のローカルインフラストラクチャを備えたリモートオフィス、リモートまたはモバイルの個人、そしてクラウドサービス等、“複雑化するインフラと激化するサイバー攻撃への対応”を目的とした「手段」である。ZTAの知見を活かした監査の視点としては以下が考えられる
  - ■監査対象組織が、境界ベースのネットワークセキュリティの方法で運用している場合
    - 複雑なネットワークでの境界認識をどのように行っているか、境界それぞれの脆弱性管理状況、サイバー攻撃で攻撃者が内部に侵入した場合のその後の横方向の動きの防御策等
  - ■監査対象組織が、ZTAを「手段」として選択している場合
    - アーキテクチャ導入のライフサイクルに応じた監査の視点での、“複雑化するインフラと激化するサイバー攻撃への対応”についての評価・検証

[出典] NIST, SP800-207, Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.37-38., Figure 12: ZTA Deployment Cycle（発表者による仮訳）（access 2023/1/23)

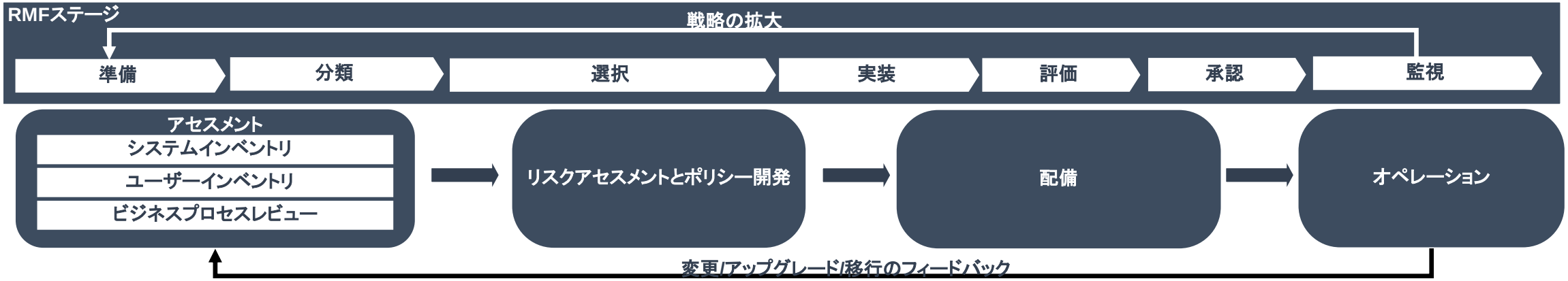
【参考】 境界ベースのネットワークセキュリティの着眼点



2.6 ZTAとシステム監査 (2)

アーキテクチャ導入のライフサイクルに応じた監査の視点

- ゼロトラストアーキテクチャに移行するには、組織がその資産（物理および仮想）、サブジェクト（ユーザー特権を含む）、およびビジネスプロセスについて詳細な知識を持っている必要がある。この知識は、リソース要求を評価するときに*PE*によってアクセスされる。
  - ■ **ゼロトラストアーキテクチャの理解と境界防御からの移行の留意点**
- ゼロトラストアーキテクチャを事業体に導入する取り組みの前に、資産、サブジェクト、データフロー、ワークフローを調査する必要がある。この認識は、ゼロトラストアーキテクチャの展開が可能になる前に到達する必要のある基礎の状態である。
  - ■ **資産、サブジェクト、データフロー、ワークフローの把握・管理状況（CSF1.1）**
- 初期インベントリが作成された後には、定期的なメンテナンスと更新のサイクルがある。この更新には、ビジネスプロセスが変更される場合も、影響がない場合もあるが、ビジネスプロセスの評価を実施する必要がある。
  - ■ **継続的なリスクアセスメントに基づくフィードバックと改善**

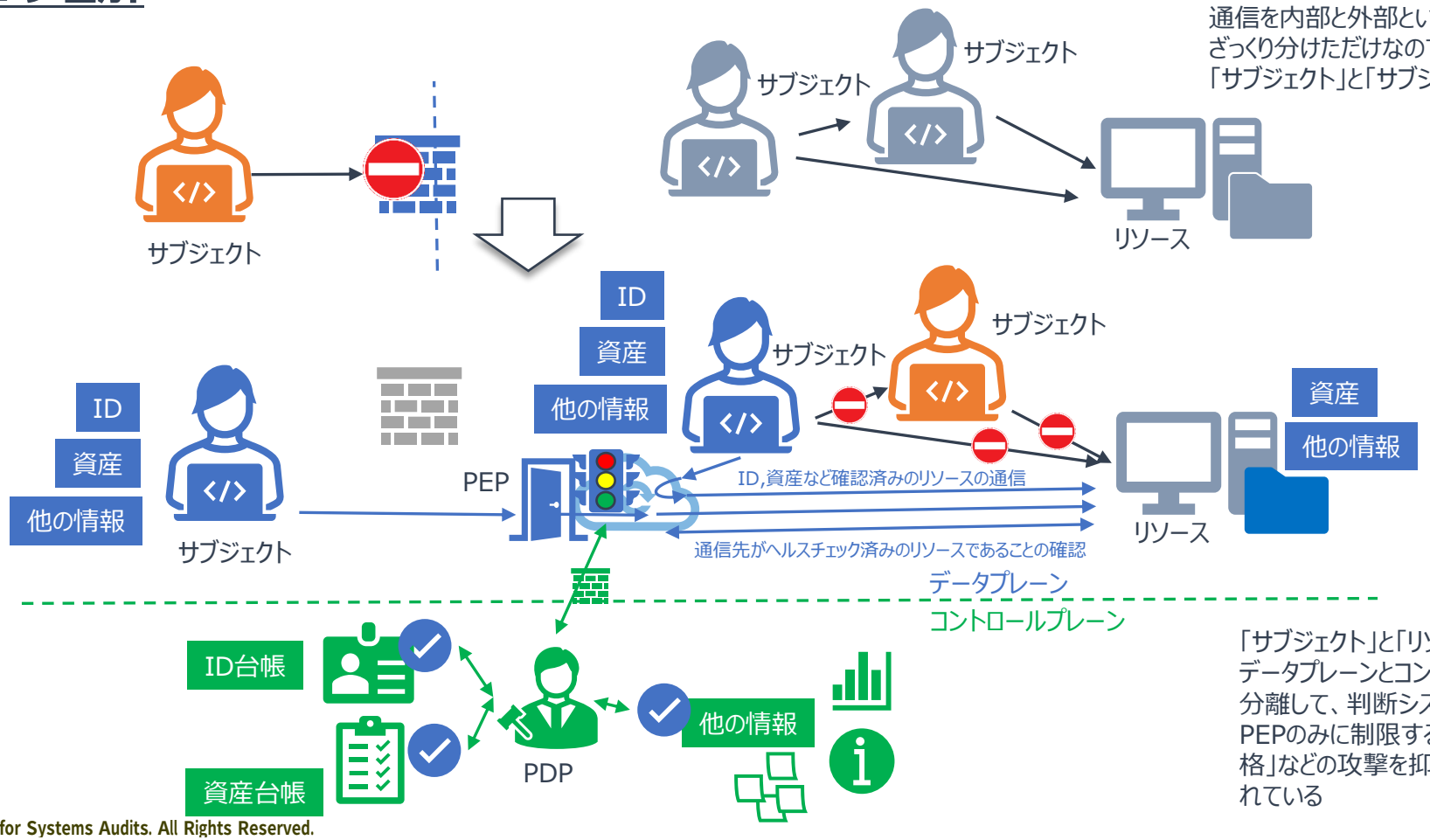


[Source] NIST, SP800-207, Zero Trust Architecture, NIST, https://doi.org/10.6028/NIST.SP.800-207, pp.37-38., Figure 12: ZTA Deployment Cycle（発表者による仮訳）（access 2023/1/23)

【参考】 ゼロトラストアーキテクチャとシステム監査

ZTAの理解と境界防御からの移行の留意点

- **ZTAの理解**



境界防御アーキテクチャのシステムは、
通信を内部と外部という「場所（アドレス）」で
ざっくり分けただけなので、内部の「サブジェクト」と「リソース」、
「サブジェクト」と「サブジェクト」が自由に「通信」できた。

（境界防御のアーキテクチャ）

（ゼロトラストアーキテクチャ）

ゼロトラストアーキテクチャでは、
まず、「ID台帳」や「資産台帳」を
もとに、「リソース」と「サブジェクト」が
信頼できるものかどうかを確認
さらに、時間や接続場所などの
セキュリティポリシーに合った通信かを
「丁寧に確認」してから通信を許可

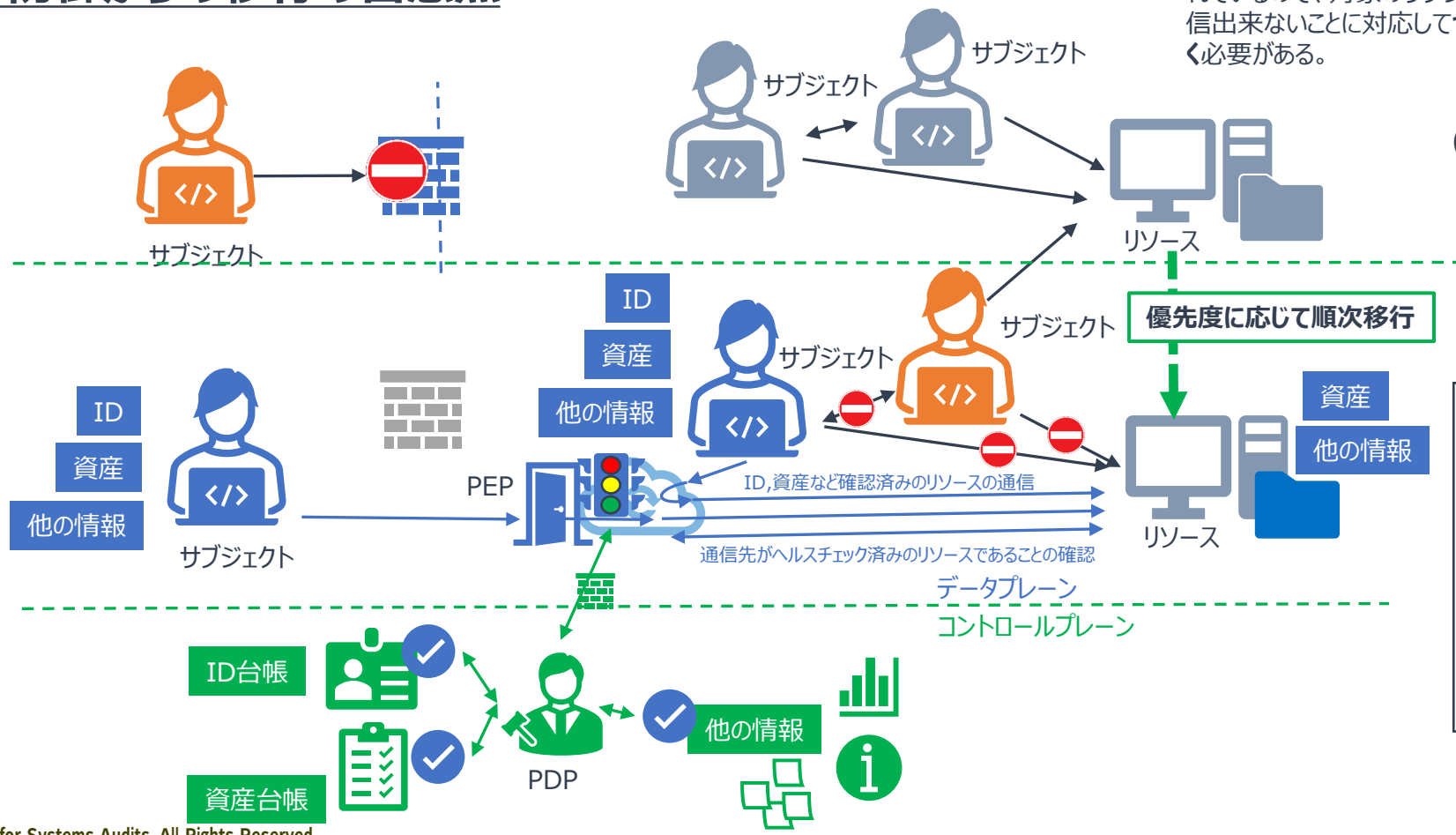
「サブジェクト」と「リソース」が通信する
データプレーンとコントロールプレーンを
分離して、判断システムとの通信を
PEPのみに制限することで、「権限昇
格」などの攻撃を抑止するように設計さ
れている

【参考】 ZTAとシステム監査

ZTAの理解と境界防御からの移行の留意点

- **境界防御からの移行の留意点**

境界防御アーキテクチャのシステムは、内部の「サブジェクト」と「リソース」、「サブジェクト」と「サブジェクト」が自由に「通信」できることを前提に構築されているので、対象のサブジェクトとリソースを洗い出し、順次自由には通信出来ないことに対応して**ゼロトラストアーキテクチャの領域を広げていく**必要がある。

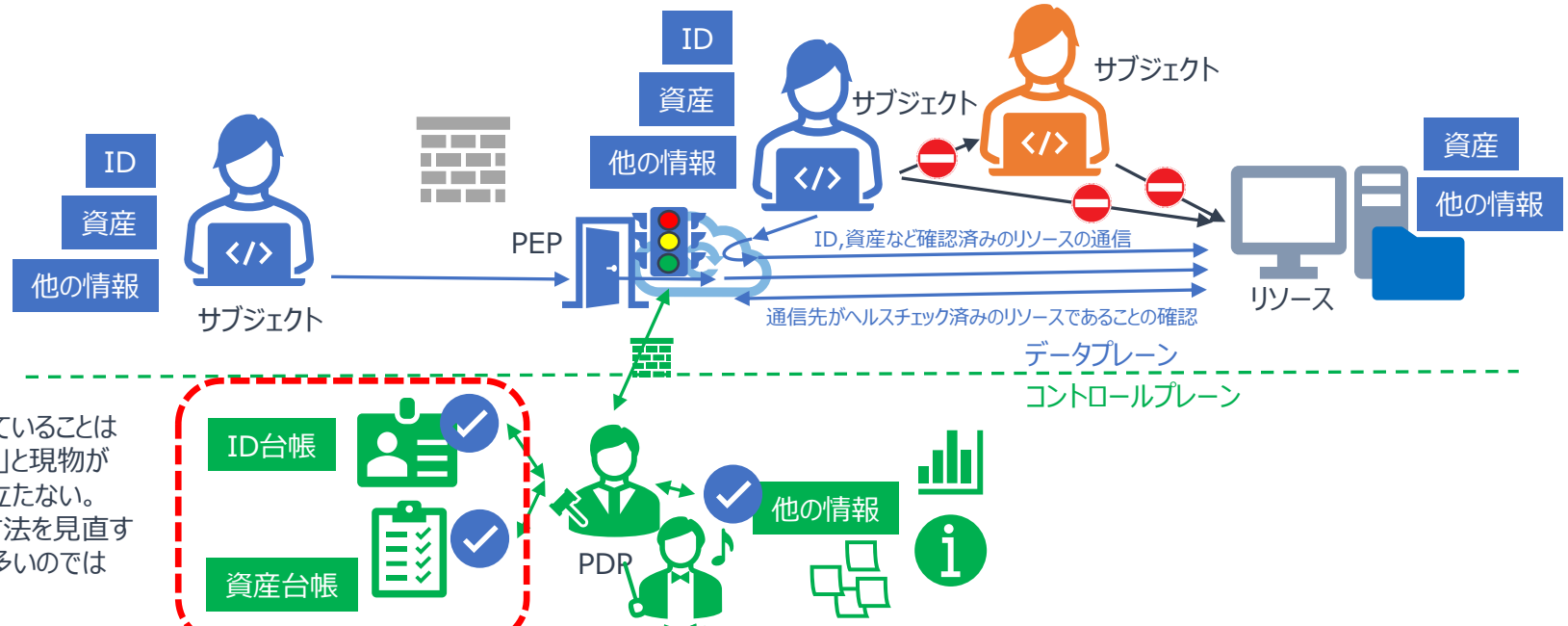


システム監査の目的：
①ZTAの適用が目標、対象、時期などが明確にされ、適切に実施されるか。
②リソースの洗い出し、リスクアセスメント実施などの基本が確実に実施されているか。
③ZTAの適用方法、手順にぬけ、誤りがなく進められているか。 など

【参考】 ZTAとシステム監査

資産、サブジェクト、データフロー、ワークフローの把握・管理状況（CSF1.1）

- **システム化されたID管理と資産管理が「起点」**



【参考】 ZTAとシステム監査

資産、サブジェクト、データフロー、ワークフローの把握・管理（CSF1.1）

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
統合エンドポイント管理 (UEM)/モバイル デバイス管理 (MDM)	アプリケーションとデータを保護するための事業体ポリシーに従って、事業体のデスクトップ コンピューター、ラップトップ、および/またはモバイル デバイスを管理および保護する。デバイスのコンプライアンスを確保する。脆弱性と脅威を軽減および修正する。不審なアクティビティを監視して、侵入を防止および検出する。マルウェア、ウイルス、およびその他の悪意のあるトラフィックまたは不正なトラフィックを防止、検出、および無効にする。可能であれば感染ファイルを修復する。アラートを提供し、修復アクションを推奨する。データを暗号化する。エンタープライズ アプリケーションと更新プログラムをデバイスにプッシュし、ユーザーがアクセスを許可されているエンタープライズ アプリケーションをダウンロードできるようにし、必要に応じてデバイスからすべてのアプリケーションとデータをリモートで削除し、デバイスでのユーザー アクティビティを追跡し、デバイスのセキュリティ問題を検出して対処する。	ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。 サポートされている (先行)	デバイスを UEM/MDM システムに登録するには、デバイスが組織のインベントリの一部であることがわかっている必要がある。
		ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。サポートする (不可欠)	UEM/MDM は、UEM/MDM で管理されているデバイスでアプリケーションをインストール、管理、構成、および更新するため、これらのアプリケーションに関するインベントリ情報を提供する。
		ID.RA-1: 資産の脆弱性が、識別され、文書化されている。サポートする (不可欠)	UEM/MDM は、たとえば、管理対象デバイスのソフトウェアを更新することで、デバイスの脆弱性を特定して修復できる場合がある。
		ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。サポートする (不可欠)	UEM/MDM は疑わしいアクティビティを監視する場合がある。マルウェア、ウイルス、およびその他の悪意のあるトラフィックを検出して無効にする。管理対象デバイス上の感染ファイルを修復する。
		PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	UEM/MDM は、デバイスが準拠するまで、管理しているリモート デバイスがリソースにアクセスできないようにする場合がある。
		PR.DS-1: 保存されているデータが、保護されている。サポートする (例示)	UEM/MDM は、デバイスに保存されているデータを暗号化する場合がありますが、デバイスに保存されているデータは、別のメカニズムを介して暗号化することもできる。
		PR.DS-2: 伝送中のデータが、保護されている。サポートする (例示)	UEM/MDM は、デバイスから送信されたデータを暗号化する場合がありますが、このデータは別のメカニズムを介して暗号化することもできる。
		PR.DS-5: データ漏えいに対する防御対策が、実装されている。サポートする (例示)	UEM/MDM は、デバイス上でのユーザー アクティビティを追跡し、不正なトラフィックを監視して、データ漏洩の防止、検出、軽減に役立てることができる。
		PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されていサポートする (例示)	UEM/MDM は、更新をインストールする前に、整合性チェックを使用して更新を検証する場合がある。また、整合性チェックを使用して、デバイスのソフトウェアとファームウェアのコンプライアンスを検証する場合もある。
		PR.DS-8: 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。サポートする (例示)	UEM/MDM は、デバイスを信頼する前に、デバイスのハードウェアの整合性を検証するために整合性チェックを使用するデバイス構成証明または同様のメカニズムに依存する場合がある。
			:他12項目（詳細は巻末「付録； ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング」参照

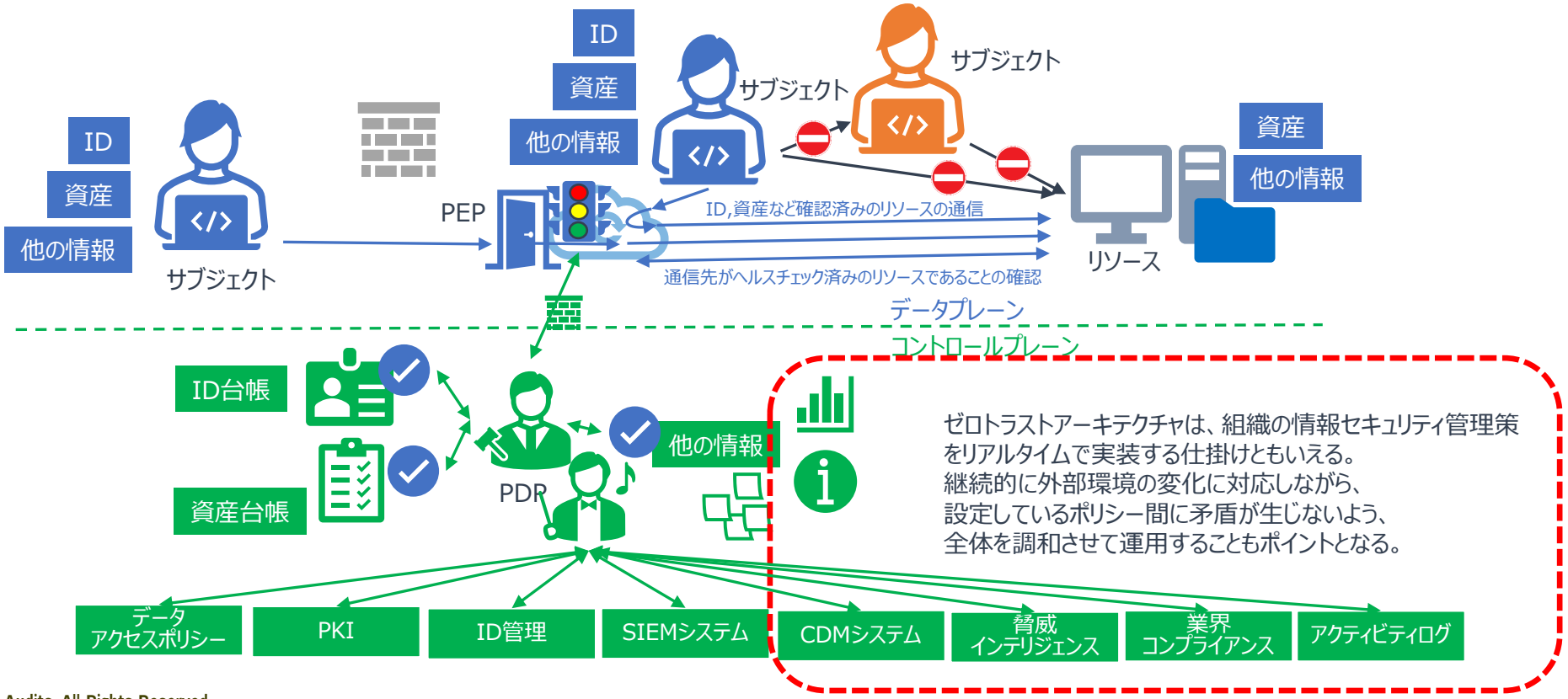
高度な資産管理が求められており、計画的な取り組みが必要。
サブジェクト、データフロー、ワークフローについてのコントロールは巻末「付録； ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング」参照

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

【参考】 ZTAとシステム監査

継続的なリスクアセスメントに基づくフィードバックと改善

- **継続して全体が調和して動き続けられることがポイント**



2.6 ZTAとシステム監査 (3)

システム監査の実施のシナリオ

ZTAの導入、移行に伴い、その確実な達成のために、確認し、問題の解決をするべき事項が発生する。それをシステム監査により対応する。

1. システム監査の目的：
   ①ZTAの導入、移行を通じた**組織のサイバーセキュリティ対策の現状の正しい把握（そもそも完璧はない）**
   （例：**侵入検知がどの程度できるか、漏洩痕跡発見時にどの情報が対象となる可能性があるかどの程度特定できるか、フォレンジック対象情報がどの程度保全される設定になっているか、最悪の事態発生時のバックアップは安全な環境に確保されているか**）
   ②ZTAの適用が目標、対象、時期などが明確にされ、適切に実施されるか。
   ③リソースの洗い出し、リスクアセスメント実施などの基本が確実に実施されているか。
   ④ZTAの適用方法、手順にぬけ、誤りがなく進められているか。 など

2. システム監査実施の切口

- 上記の切口のシステム監査は、次のような段階で実施する事が考えられる。(既存組織からの移行として考えている)
  - 初期準備段階
  - 基本事項確認段階
  - 実行、移行段階
  - 運用段階

【参考】 システム監査の実施

初期準備段階・基本事項確認（実装準備）の着眼例

段階	監査での確認	監査対象	基準等
構築導入の前提事項の確認 （この段階で監査は可能か、適切か？）	トップの決断、ZTへの移行計画、 ZT推進体制等	トップの決定事項、 計画書（自社、ベンダ活用）、 適用範囲と影響	社内規程 情報セキュリティポリシー
初期準備事項 前提事項の確認つづき	ZTA適用（移行）対象確認 ZTA実装のための展開確認 対象の確認 リスクアセスメント	リソース洗い出し、セッション洗い出し、分離 ポリシー（自社、業界）、規制、制度 対象の調査実施 リスク構成図 外部委託範囲、内容	（管理策） CSF1.1 ISMS SP1800-35 Vol.E(DRAFT) SP800-207 社内規程
基本事項確認 （実装準備）	実装に提供されるコンポーネントの構成と機能	・リスクアセスメント実施状況 ・アクセスポリシー ・ID管理、 ・ユーザアカウント管理 ・イベント管理	（管理策） CSF1.1 ISMS SP1800-35 Vol.E(DRAFT) SP800-207

【参考】 システム監査の実施

実行、移行段階および運用の着眼例

段階	監査での確認範囲	監査対象	基準等
実行、移行段階 （実装）	移行シナリオ 推進体制、実装状況、 ZT原則の確認 利用ツールの妥当性	要件を満たしているか 実施内容が、ZT原則に沿う内容か	（管理策） CSF1.1 ISMS SP1800-35 Vol.E(DRAFT) SP800-207 (原則の実施事項)
運用 ＊１	運用状況（＊１の状況） コンプライアンスの遵守 動的対応の実施状況	トラフィック、ログの取得、監視状況 遵守事項の確認（各種基準、ポリシー) 運用ポリシー	ZTA設計内容 （基準、管理策） 運用ポリシー

＊１
PEPが正常に機能していること
PDPが正常に機能していること
PIPが正常に機能していること

【参考】 システム監査の実施

実行、移行段階および運用の着眼例（CSF1.1）

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
ポリシー エンジン (PE)	エンタープライズ ポリシー、機能コンポーネントからの情報、および信頼アルゴリズムに基づいて、リソースへのアクセスを許可、拒否、または取り消すかどうかを決定する	PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	PE は、ポリシーに基づいてリモート アクセスを決定する。ZTA では、リモート アクセスの管理を支援するために PE を適用する必要がある。ZTA では、リモートかローカルかに関係なく、すべてのアクセス要求に同じポリシーが適用されることに注意すること。
			ZTA はローカル アクセス ポリシーとリモート アクセス ポリシーを区別しないが、コンプライアンス フレームワークでは区別する必要がある。
ポリシー管理者 (PA)	サブジェクトとリソース間の通信パスを確立およびシャットダウンする PEP にコマンドを送信することにより、PE のポリシー決定を実行する。	PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	PA は、アクセス決定情報を PE から PEP に伝達することにより、リモート アクセス決定の実施をサポートする。PEP では、決定を実施できる。ZTA では、リモート アクセスの管理を支援するために PA を適用する必要がある。
ポリシー施行ポイント (PEP)	エンタープライズ リソースをホストするトラストゾーンを保護する。サブジェクトとリソース間の接続を有効化、監視、および終了する。要求を PA に転送し、PA からコマンドを受信する。	PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	PEP は、リモート アクセスの決定を強制する。ZTA では、リモート アクセスの管理を支援するために PEP を適用する必要がある。
		PR.AC-5: ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。サポートする (例示)	PEP は、保護する事業体の部分への不正アクセスを防ぐことができる。単一のリソースを保護するために使用される場合、必ずしもネットワーク分離またはネットワーク セグメンテーションが提供されるわけではない。ただし、個別のネットワーク セグメントを保護および分離するために導入することはできる。ネットワークのセグメンテーションは、PEP 以外のメカニズムによっても提供される場合がある。
		PR.DS-5:データ漏えいに対する防御対策が、実装されている。サポートする(不可欠)	PEP は、保護する事業体の一部からの情報の無許可の転送を防ぐ。ZTA では、データ漏洩を防ぐために PEP を適用する必要がある。
		PR.PT-4:通信ネットワークと制御ネットワークが、保護されている。サポートする(不可欠)	ZTA をサポートするには、データ プレーンとコントロール プレーン (ネットワーク) を論理的に分離する必要がある。PEP は、両方のプレーンからメッセージを送受信できる唯一のコンポーネントである。プレーンを相互に保護し、事業体の資産やリソースがコントロール プレーンに直接アクセスできないようにする。
		DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	PEP は、サブジェクトとエンタープライズ リソース間の接続を監視して、禁止されているアクティビティまたは疑わしいアクティビティを検出するために使用できる。ただし、必ずしもそうするように構成する必要はない。ネットワーク監視は、PEP 以外のメカニズムによっても提供される場合がある。
		RS.MI-1: インシデントは、封じ込められている。サポートする(不可欠)	ZTA では、PEP がインシデントの封じ込めの中心となる。リソースが侵害された場合、他のリソースを保護する PEP は、攻撃者が侵害されたリソースからそれらの他の PEP によって保護されたリソースに横方向に移動するのを防ぐ。

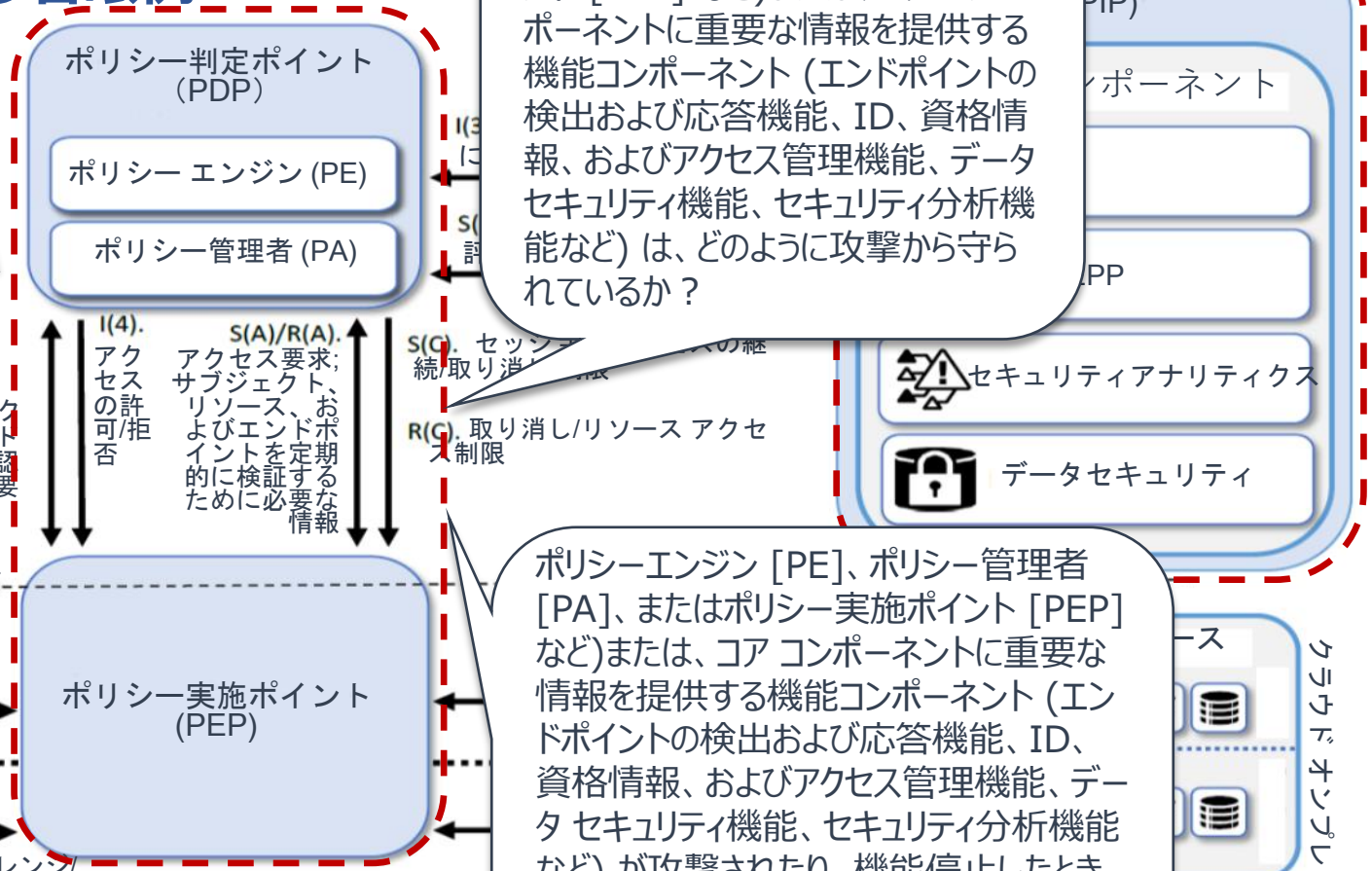
[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

【参考】 システム監査の実施

実行、移行段階および運用の着眼例

制約）ZTA によって保護されたネットワークは、ZTA 自体の 1 つまたは複数のコアコンポーネント (ポリシー エンジン [PE]、ポリシー管理者 [PA]、またはポリシー実施ポイント [PEP] など)または、コア コンポーネントに重要な情報を提供する機能コンポーネント (エンドポイントの検出および応答機能、ID、資格情報、およびアクセス管理機能、データ セキュリティ機能、セキュリティ分析機能など) が侵害された悪用に対して脆弱である。

ポリシー エンジン [PE]、ポリシー管理者 [PA]、またはポリシー実施ポイント [PEP] など)または、コア コンポーネントに重要な情報を提供する機能コンポーネント (エンドポイントの検出および応答機能、ID、資格情報、およびアクセス管理機能、データ セキュリティ機能、セキュリティ分析機能など) は、どのように攻撃から守られているか？



ポリシー エンジン [PE]、ポリシー管理者 [PA]、またはポリシー実施ポイント [PEP] など)または、コア コンポーネントに重要な情報を提供する機能コンポーネント (エンドポイントの検出および応答機能、ID、資格情報、およびアクセス管理機能、データ セキュリティ機能、セキュリティ分析機能など) は、正しく機能しているか？
監視により異常に速やかに気づき、対応する体制があるか？

ポリシーエンジン [PE]、ポリシー管理者 [PA]、またはポリシー実施ポイント [PEP] など)または、コア コンポーネントに重要な情報を提供する機能コンポーネント (エンドポイントの検出および応答機能、ID、資格情報、およびアクセス管理機能、データ セキュリティ機能、セキュリティ分析機能など) が攻撃されたり、機能停止したときに、どのような対応が準備されているか？
・システム・ネットワークの冗長性
・迅速な復旧のための対策

さまざまな場所にあるリソースを保護するために多くの
のリソースを含む相互作用に焦点を限定している。

の PEP を持つこともあるが、簡単にす

a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf , p.50 Figure 4-1 ,（発表者による仮訳）（access 2023/1/23)

2.6 ZTAとシステム監査 (4)

課題

以下のような課題が想定される

①システム監査を誰が実施するか　　前提確認段階は、重要であるが、実際には難しい(のでないか)
ZTへの移行方法が試行錯誤の状況でのシステム監査を実施するシステム監査人は現実には存在しないなど難しい
(外部委託によってコンサルテーションを受けるなどが考えられる)
→ システム監査人にとってはネットワーク技術など、新たな技術の習得が課題

②運用は旅の途中だから、常にチェック、確認していることが必要
ZT移行中の適切なポイントの把握
→ 対象組織のエンタープライズアーキテクチャの理解など必ずしも文書化が十分でない可能性のある領域への対応が課題

ZT移行後は、コンプライアンスや動的な対応に関して監査が必要であり、体制も必要

- → ZTAは高度な自動化が前提であり、自動化されたシステム処理の検証技術の確立などは大きな課題

システム監査の実施に関しては、ZTは組織により実装が多様でそれぞれ異なるため、実施内容、実施方法など、未検討事項も多く、今後さらなる研究が必要

まとめ

- 複数の内部ネットワーク、独自のローカルインフラストラクチャを備えたリモートオフィス、リモートまたはモバイルの個人、そしてクラウドサービス等、“複雑化するインフラと激化するサイバー攻撃への対応”を目的とした「手段」であるが、その実装は現在の組織の状況に依存するため、個別で多様なものになります。
- ZTAは激化するサイバー攻撃への強力な防御手段ですが、万能な「銀の玉」ではなく、難しさや構造上の弱点もあり、その特性をよく理解して活用していくことが重要です。
- 現在、サイバーリスクはすべての組織にとって、重要なリスクであり、重要な課題です。わたしたちシステム監査人も、ZTAを含めた新しい技術の理解に継続的に取り組むとともに、監査対象組織における「インフラの複雑度」と「サイバー攻撃のリスクの大きさ」をよく理解し、対象組織にとってさらに「価値のある」監査業務を提供することに注力すべきであると再認識いたしました。
- 本研究が少しでも皆様のお役に立つことを希望するとともに、研究を継続し、さらなる成果を皆様と共有したいと思います。

Agenda

1. 情報セキュリティ研究プロジェクトの活動
2. 2022年度　ゼロトラストアーキテクチャとシステム監査
   ～ゼロトラストへの道～
3. 2023年度　研究テーマと活動計画

3.1　2023年度　PJ研究テーマ

「サイバーインシデント対応」にかかる情報の収集と発信

● 2023年度 研究テーマ

「サイバーインシデント対応」を研究テーマに予定します。

研究の過程で、情報セキュリティを取り巻く環境変化、インシデントやリファレンスの動向により、また、究明する重点を判断しテーマのステップアップを図ります。

● 取組み

情報セキュリティの確立と強化のための有効な考え方、具体的実施策の、幅広い研究と提案に取り組みます。

財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準（J-SOX）の改訂、ISO/IEC 27001の改訂など、昨今のサイバーリスクに対する環境を踏まえたテーマの選定、関係する情報の収集と分析、多様な見解を尊重した意見交換により、参加者それぞれの研究を促進するとともに、研究プロジェクトとして研究成果にまとめ、公表・発表します。

情報セキュリティ、事業継続、リスクマネジメント等にかかる事例、国内外の基準・標準の動向調査等の情報共有、及び各人の研究関連情報および事例に関する意見交換を行います。

3.2 PJの計画日程と参加メンバーの募集

PJ実施のシナリオ

- 計画日程

原則　月1回の頻度でZoomオンライン会議を開催します。

学会の研究会、研究大会において、研究結果・成果を報告します。

- 研究のアプローチ

⑴ 目標の設定・設定そのものの議論、周辺知識の取得、論題・疑問点の設定

⑵ 参考文献、根拠資料の収集と明示、引用の区別

⑶ 学会員としてパーソナリティ、オリジナリティを活かし、かつ、協調を醸すコミュニケーション・論議

⑷ 業務に役立たせる情報、シンキングツールの発信

参加メンバーの募集

- 参加方法

システム監査学会HP　◆研究活動◆　研究プロジェクトの登録（随時受け付けています。）

【付録】

ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA研究報告の一つとして
本内容を付録の形で開示

ZTAコンポーネント、その機能、
CSFとのマッピングは、ZTAを
具体的に把握する伝手となる

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
ポリシー エンジン (PE)	エンタープライズ ポリシー、機能コンポーネントからの情報、および信頼アルゴリズムに基づいて、リソースへのアクセスを許可、拒否、または取り消すかどうかを決定する	PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	PE は、ポリシーに基づいてリモート アクセスを決定する。ZTA では、リモート アクセスの管理を支援するために PE を適用する必要がある。ZTA では、リモートかローカルかに関係なく、すべてのアクセス要求に同じポリシーが適用されることに注意すること。
			ZTA はローカル アクセス ポリシーとリモート アクセス ポリシーを区別しないが、コンプライアンス フレームワークでは区別する必要がある。
ポリシー管理者 (PA)	サブジェクトとリソース間の通信パスを確立およびシャットダウンする PEP にコマンドを送信することにより、PE のポリシー決定を実行する。	PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	PA は、アクセス決定情報を PE から PEP に伝達することにより、リモート アクセス決定の実施をサポートする。PEP では、決定を実施できる。ZTA では、リモート アクセスの管理を支援するために PA を適用する必要がある。
ポリシー施行ポイント (PEP)	エンタープライズ リソースをホストするトラストゾーンを保護する。サブジェクトとリソース間の接続を有効化、監視、および終了する。要求を PA に転送し、PA からコマンドを受信する。	PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	PEP は、リモート アクセスの決定を強制する。ZTA では、リモート アクセスの管理を支援するために PEP を適用する必要がある。
		PR.AC-5: ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。サポートする (例示)	PEP は、保護する事業体の部分への不正アクセスを防ぐことができる。単一のリソースを保護するために使用される場合、必ずしもネットワーク分離またはネットワーク セグメンテーションが提供されるわけではない。ただし、個別のネットワーク セグメントを保護および分離するために導入することはできる。ネットワークのセグメンテーションは、PEP 以外のメカニズムによっても提供される場合がある。
		PR.DS-5:データ漏えいに対する防御対策が、実装されている。サポートする(不可欠)	PEP は、保護する事業体の一部からの情報の無許可の転送を防ぐ。ZTA では、データ漏洩を防ぐために PEP を適用する必要がある。
		PR.PT-4:通信ネットワークと制御ネットワークが、保護されている。サポートする(不可欠)	ZTA をサポートするには、データ プレーンとコントロール プレーン (ネットワーク) を論理的に分離する必要がある。PEP は、両方のプレーンからメッセージを送受信できる唯一のコンポーネントである。プレーンを相互に保護し、事業体の資産やリソースがコントロール プレーンに直接アクセスできないようにする。
		DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	PEP は、サブジェクトとエンタープライズ リソース間の接続を監視して、禁止されているアクティビティまたは疑わしいアクティビティを検出するために使用できる。ただし、必ずしもそうするように構成する必要はない。ネットワーク監視は、PEP 以外のメカニズムによっても提供される場合がある。
		RS.MI-1: インシデントは、封じ込められている。サポートする(不可欠)	ZTA では、PEP がインシデントの封じ込めの中心となる。リソースが侵害された場合、他のリソースを保護する PEP は、攻撃者が侵害されたリソースからそれらの他の PEP によって保護されたリソースに横方向に移動するのを防ぐ。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳）（access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
アクセス ポリシー	各サブジェクトに各リソースへのアクセスを許可するために満たす必要がある条件を定義する	ID.AM-3: 組織内の通信とデータフロー図が、作成されている。 サポートされている (先行)	各サブジェクトのリソースへのアクセスに関するポリシーを適切に策定するには、サブジェクトとリソース間の予想される許容可能なデータ フローを十分に理解する必要がある。
		ID.AM-4: 外部情報システムが、カタログ作成されている。 サポートされている (先行)	各サブジェクトの外部情報システムへのアクセスに関するポリシーを適切に策定するために、アクセスを許可するシステムをカタログ化する必要がある。
		ID.AM-5: リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。 サポートされている (先行)	組織のために策定されるアクセス ポリシーは、アクセスが要求されているリソースの分類、重要度、およびビジネス価値に部分的に基づいている必要がある。
		ID.RA-5: 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。サポートする (例示)	組織は、検出された脅威や脆弱性などのさまざまな要因に基づいてリスクを計算する「信頼レベル」または同様のアクセス ポリシーを定義し、この計算されたリスクに基づいて、特定のアクセス要求に対する ZTA の応答を決定できる。
		ID.RA-6: リスク対応が、識別され、優先順位付けされている。サポートする (例示)	組織は、検出された脅威や脆弱性、ユーザーの行動、ユーザーの場所などのさまざまな要因に基づいてリスクを計算する「信頼レベル」または同様のアクセス ポリシーを定義し、この計算されたリスクに基づいて、特定のアクセス要求に対する ZTA の応答を基にすることができる。たとえば、リスクが特定のしきい値以下であると判断された場合、要求は許可される。リスクが特定のしきい値を超えている場合、リクエストは拒否される。
		PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。サポートする(不可欠)	アクセス ポリシーは、特定のリソースにアクセスするためのアクセス許可と承認が、最小限の特権と職務の分離の原則に準拠していることを確認するためのメカニズムである。
		PR.AC-7: ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている。サポートする(不可欠)	アクセス ポリシーは、トランザクションのリスクに見合ったサブジェクトの認証を保証するメカニズムである。

[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳）（access 2023/1/23）

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
(つづき) アクセス ポリシー		PR.IP-12: 脆弱性管理計画が、作成され、実装されている。サポートされている (先行)	組織は、脆弱性管理計画を作成し、この計画に一部基づいてアクセス ポリシーを定義および実施することが期待されている。
		DE.AE-1: ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。サポートされている (先行)	アクセス ポリシーを定義する前に、承認されたデータ フローを十分に理解し、それらを実施するポリシーを定義できるように、ネットワーク操作のベースラインと、ユーザーおよびシステムの予想されるデータフローを確立する必要がある。
		DE.AE-1: ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。サポートする (例示)	確立されたアクセス ポリシーは、目的のデータ フローを管理および適用する。
		DE.AE-5: インシデント警告の閾値が、定められている。サポートする (例示)	インシデント アラートのしきい値を設定するポリシーを定義して、しきい値に達したときに指定したアクション (アラートの生成など) が実行されるようにすることができる。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャコンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係（および関係プロパティ）	関係の説明
アイデンティティマネジメント	事業体のユーザー アカウントとデバイス アカウント、ID レコード、役割情報、および組織内のアクセス決定の基礎となるアクセス属性を作成および管理して、適切なサブジェクトが適切なリソースに適切なタイミングで適切にアクセスできるようにする。	ID.AM-6: 全従業員とサードパーティの利害関係者 (サプライヤー、顧客、パートナーなど) に対してのサイバーセキュリティ上の役割 と責任が、定められている。 サポートされている (先行)	アイデンティティマネジメント は、サイバーセキュリティの役割とそれに関連する権限と責任のデジタル表現の作成、保存、および管理をサポートする。また、ユーザー ID へのロールの割り当てもサポートしている。ユーザーの役割と責任のこれらの表現を作成、保存、および管理できるようにするには、役割と責任自体がすでに確立されている必要がある。
		PR.AC-1: 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。サポートする (不可欠)	アイデンティティマネジメント は、ID とそれに関連付けられた役割および資格情報の発行、保管、管理、および取り消しをサポートする。また、ユーザーとデバイスの認証を実行する際の資格情報の検証もサポートしている。
		PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。サポートする(不可欠)	アイデンティティマネジメント は、役割のデジタル表現と関連するアクセス許可を定義および管理するために使用される。これは、最小特権と職務分離の原則に基づいている。最小限の特権と職務の分離、および事業体内での責任の変更や離職に応じて各ユーザーの役割を管理する。
		PR.AC-6: ID は、ID 利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで行使されている。サポートする (不可欠)	アイデンティティマネジメント は、ID と資格情報の関連付けを格納および管理する。

[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23）

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
アクセスと認証情報管理	ユーザーとデバイスの認証 (SSO や MFA など) を実行し、アイデンティティ、ロール、およびアクセス属性を使用して、どのアクセス要求が承認されるかを判断することにより、リソースへのアクセスを管理する。	PR.AC-6: ID は、ID 利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで行使されている。サポートされている (先行)	アクセス要求が承認されているかどうかを判断するために、アクセスおよび資格情報管理コンポーネントは、ユーザーまたはデバイスにバインドされ、アクセス要求の一部として行使される資格情報を検証することにより、アクセスを要求しているユーザーまたはデバイスを認証する。このコンポーネントが認証できるようにするには、ユーザー ID とデバイス ID が行使される必要がある。
		PR-AC-7: ユーザー、デバイス、およびその他の資産は、トランザクション(例えば、個人のセキュリティとプライバシーのリスク、およびその他の組織のリスク)のリスクに見合った認証 (単一要素、多要素など) が行われている。サポートする (不可欠)	アクセスと認証情報のマネジメント コンポーネントの主な機能は、ユーザーとデバイスの認証を実行することである。
		RS.MI-1: インシデントは、封じ込められている。サポートする (例示)	正当なユーザーの資格情報が盗まれ、攻撃者がそれを使用してリソースへの不正アクセスを取得した場合、アクセスと資格情報の管理コンポーネントは、攻撃者が正当なユーザーの役割または属性で許可されているリソースにのみアクセスできるように制限する。これは、インシデントを封じ込める方法の一例である。
		RS.MI-2: インシデントは、緩和されている。サポートする (例示)	正当なユーザーの資格情報が盗まれ、攻撃者がそれらを使用してリソースへの不正アクセスを取得した場合、攻撃者は、正当なユーザーの役割が許可する方法でのみそのリソースへのアクセスを許可されます (たとえば、読み取り専用と読み取り/書き込み)。) 。これは、インシデントを軽減する方法の一例である。
		DE.CM-7: 権限のない人員、接続、デバイス、およびソフトウェアの監視が実施されている。をサポート（不可欠）	アクセスと認証情報のマネジメント コンポーネントは、継続的かつ断続的なユーザー認証と承認を実行できるため、未承認のユーザーとデバイスを監視できる。

[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
フェデレーション ID	ZTA によって承認されている ID またはオブジェクトに関連するすべての属性を集約し、関連付けます。これにより、あるドメインのユーザーが別のドメインのデータまたはシステムにシームレスに安全にアクセスできるようになり、完全に冗長なユーザー管理を行う必要がなくなる。 フェデレーション ID は、従来の ICAM データを包含し、より大きなフェデレーション ICAM コミュニティの一部である可能性のある ID をサポートし、事業体以外の従業員を含む可能性がある。	ID.AM-6: 全従業員とサードパーティの利害関係者 (サプライヤー、顧客、パートナーなど) に対してのサイバーセキュリティ上の役割 と責任が、定められている。 サポートされている (先行)	フェデレーテッドアイデンティティ コンポーネントを使用すると、さまざまなグループ (事業体の従業員とサードパーティの利害関係者 (サプライヤー、顧客、パートナーなど) など) に対して確立および保存されているサイバーセキュリティの役割と責任を管理および適用できる。これらの役割と責任は、実施する前にすでに確立されている必要がある。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
アイデンティティ ガバナンス	要件と規制へのコンプライアンスを確保するために、ユーザー ID とアクセス制御機能 (職務分掌、役割管理、ログ記録、監査、アクセス レビュー、分析、レポートの確保など) を管理するためのポリシー ベースの集中化された自動化されたプロセスを提供する。	PR.AC-1: 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。サポートする (不可欠)	アイデンティティガバナンスコンポーネントの重要な機能は、ID と資格情報の監査をサポートすることである。
		PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。サポートする(不可欠)	アイデンティティガバナンスコンポーネントは、最小限の特権と職務の分離の原則を組み込んだ方法で、アクセス許可と承認を管理する。
		ID.GV-1: 組織のサイバーセキュリティポリシーが、定められ、周知されている。 サポートされている (先行)	アイデンティティガバナンスコンポーネントは、組織のサイバーセキュリティ ポリシーが、規制、法律、およびその他のガバナンス関連の要件に準拠するような方法で実施されることを保証する。このポリシーは、アイデンティティガバナンスコンポーネントによって施行される前に確立されている必要がある。
		ID.GV-2: サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。サポートする (不可欠)	アイデンティティガバナンスコンポーネントは、組織が規制、法律、およびその他のガバナンス関連の要件に従って運営されるようにするために、サイバーセキュリティの役割と責任を内部の役割および外部パートナーと調整および調整することをサポートする。
		ID.GV-3: プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。サポートされている (先行)	アイデンティティガバナンスコンポーネントが従うプロセスは、組織がすべての法的要件および規制要件に準拠して運用されるように定義されている。アイデンティティガバナンスプロセスを定義するには、これらの要件を十分に理解する必要がある。これらの要件は変化するため、継続的に管理する必要があり、ID ガバナンス プロセスの変更が必要になる場合がある。
		ID.GV-4: ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。サポートする (不可欠)	アイデンティティガバナンスコンポーネントが従うプロセスは、サイバーセキュリティ リスクに対処する目的で定義および管理される。
		PR.PT-1: 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。サポートする (不可欠)	アイデンティティガバナンスコンポーネントは、ポリシーと規制に従って、すべての ID 管理アクティビティをログに記録し、監査する。

[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャコンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係（および関係プロパティ）	関係の説明
多要素認証 (MFA)	ユーザーが知っているもの (パスワードなど) だけでなく、持っているもの (トークンなど) も提供するようユーザーに要求することで、ユーザー ID を認証する。	PR.AC-7: ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている。サポートする(不可欠)	MFA コンポーネントを使用すると、リスクの高いアクセス要求に必要な第 2 要素を使用してユーザーを認証できる。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳）（access 2023/1/23）

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
統合エンドポイント管理 (UEM)/モバイル デバイス管理 (MDM)	アプリケーションとデータを保護するための事業体ポリシーに従って、事業体のデスクトップ コンピューター、ラップトップ、および/またはモバイル デバイスを管理および保護する。デバイスのコンプライアンスを確保する。脆弱性と脅威を軽減および修正する。不審なアクティビティを監視して、侵入を防止および検出する。マルウェア、ウイルス、およびその他の悪意のあるトラフィックまたは不正なトラフィックを防止、検出、および無効にする。可能であれば感染ファイルを修復する。アラートを提供し、修復アクションを推奨する。データを暗号化する。 エンタープライズ アプリケーションと更新プログラムをデバイスにプッシュし、ユーザーがアクセスを許可されているエンタープライズ アプリケーションをダウンロードできるようにし、必要に応じてデバイスからすべてのアプリケーションとデータをリモートで削除し、デバイスでのユーザー アクティビティを追跡し、デバイスのセキュリティ問題を検出して対処する。	ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。 サポートされている (先行)	デバイスを UEM/MDM システムに登録するには、デバイスが組織のインベントリの一部であることがわかっている必要がある。
		ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。サポートする (不可欠)	UEM/MDM は、UEM/MDM で管理されているデバイスでアプリケーションをインストール、管理、構成、および更新するため、これらのアプリケーションに関するインベントリ情報を提供する。
		ID.RA-1: 資産の脆弱性が、識別され、文書化されている。サポートする (不可欠)	UEM/MDM は、たとえば、管理対象デバイスのソフトウェアを更新することで、デバイスの脆弱性を特定して修復できる場合がある。
		ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。サポートする (不可欠)	UEM/MDM は疑わしいアクティビティを監視する場合がある。マルウェア、ウイルス、およびその他の悪意のあるトラフィックを検出して無効にする。管理対象デバイス上の感染ファイルを修復する。
		PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	UEM/MDM は、デバイスが準拠するまで、管理しているリモート デバイスがリソースにアクセスできないようにする場合がある。
		PR.DS-1: 保存されているデータが、保護されている。サポートする (例示)	UEM/MDM は、デバイスに保存されているデータを暗号化する場合がありますが、デバイスに保存されているデータは、別のメカニズムを介して暗号化することもできる。
		PR.DS-2: 伝送中のデータが、保護されている。サポートする (例示)	UEM/MDM は、デバイスから送信されたデータを暗号化する場合がありますが、このデータは別のメカニズムを介して暗号化することもできる。
		PR.DS-5: データ漏えいに対する防御対策が、実装されている。サポートする (例示)	UEM/MDM は、デバイス上でのユーザー アクティビティを追跡し、不正なトラフィックを監視して、データ漏洩の防止、検出、軽減に役立てることができる。
		PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されていサポートする (例示)	UEM/MDM は、更新をインストールする前に、整合性チェックを使用して更新を検証する場合がある。また、整合性チェックを使用して、デバイスのソフトウェアとファームウェアのコンプライアンスを検証する場合もある。
		PR.DS-8: 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。サポートする (例示)	UEM/MDM は、デバイスを信頼する前に、デバイスのハードウェアの整合性を検証するために整合性チェックを使用するデバイス構成証明または同様のメカニズムに依存する場合がある。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
（つづき） **統合エンドポイント管理 (UEM)/モバイル デバイス管理 (MDM)**		PR.IP-1: 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。サポートする (不可欠)	UEM/MDM は、ソフトウェアとファームウェアの予想されるベースラインのインストールと構成に関して、デバイスが組織のポリシーに準拠していることを保証する。UEM/MDM は、エンドポイントでこれらのベースラインを適用および維持する。
		PR.IP-1: 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。サポートされている (先行)	UEM/MDM が実施するエンドポイントのベースライン構成は、組織のポリシーに従って、最小機能の概念などのセキュリティ原則に基づいて開発されている必要がある。UEM/MDM の動作は、このようなベースラインの存在に依存する。
		PR.IP-6: データは、ポリシーに従って破壊されている。サポートする (例示)	UEM/MDM は、ポリシーに従って、必要に応じてデバイスからアプリケーションとデータをリモートで削除できる。他のメカニズムも、必要に応じてデータを破棄できる。
		PR.IP-12: 脆弱性管理計画が、作成され、実装されている。サポートされている (先行)	UEM/MDM は、組織の脆弱性管理ポリシーを適用することにより、デバイス ソフトウェア、ファームウェア、および構成で検出された脆弱性と脅威を軽減および修復できる。これらのポリシーは、UEM/MDM が適用する前に存在している必要があり、組織の脆弱性管理計画の少なくとも一部を構成する。
		PR.PT-2: リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。サポートする (例示)	UEM/MDM は、ポリシーの必要に応じて、リムーバブル メディアの使用を制限できる。
		PR.PT-3: 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。サポートする (例示)	UEM/MDM を使用して、必須機能のみを提供するようにデバイスを構成できる。
		DE.CM-3: 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	UEM/MDM は、疑わしい動作についてユーザー アクティビティを監視できる。
		DE.CM-4: 悪質なコードは、検知されている。サポート（例）	UEM/MDM は、さまざまな種類の悪意のあるコードを防止、検出、無効化する。

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
（つづき） **統合エンドポイント管理 (UEM)/モバイル デバイス管理 (MDM)**		DE.CM-5: 不正なモバイルコードは、検知されている。対応（例）	UEM/MDM は、不正なモバイル コードを検出できる場合がある。
		DE.CM-7: 権限のない人員、接続、デバイス、およびソフトウェアの監視が実施されている。をサポート（不可欠）	UEM/MDM は、許可されていないソフトウェアと接続についてデバイスを監視する。
		RS.MI-1: インシデントは、封じ込められている。サポートする(不可欠)	UEM/MDM は、マルウェアやその他の悪意のあるアクティビティまたは不正なアクティビティを検出して無効にするなど、インシデントを封じ込めるのに役立つ多くのアクティビティを実行する。可能であれば感染ファイルを修復する。デバイスで疑わしいアクティビティまたは悪意のあるアクティビティが検出された場合、アラートを提供し、修復アクションを推奨する。また、デバイスに保存されているデータを暗号化するため、ロックされたデバイスを盗んだ人に対するデータの有用性が制限される。
		RS.MI-2: インシデントは、緩和されている。サポートする (不可欠)	UEM/MDM は、マルウェアやその他の悪意のあるアクティビティまたは不正なアクティビティの検出と無効化など、インシデントの軽減に役立つ多くのアクティビティを実行する。可能であれば感染ファイルを修復する。デバイスで疑わしいアクティビティまたは悪意のあるアクティビティが検出された場合、アラートを提供し、修復アクションを推奨する。また、デバイスに保存されているデータを暗号化するため、ロックされたデバイスを盗んだ人に対するデータの有用性が制限される。

[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳）（access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャコンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係（および関係プロパティ）	関係の説明
エンドポイントの検出と対応 (EDR)/	ウイルス対策、データ暗号化、侵入防止、EDR、データ損失防止 (DLP) などのエンドポイント保護テクノロジの統合スイートを通じて、エンドポイントへの脅威を検出して阻止する。	ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。 サポートされている (先行)	デバイスに EDR/EPP ソフトウェアをインストールするには、デバイスが組織のインベントリの一部であることがわかっている必要がある。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャコンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係（および関係プロパティ）	関係の説明
エンドポイント保護プラットフォーム (EPP)	アプリケーションとデータを保護するように設計されたメカニズムが含まれる場合がある。ハードウェア、ファームウェア、ソフトウェア、および構成に関するポリシーにデバイスが準拠していることを確認する。エンドポイントの脆弱性、疑わしいアクティビティ、侵入、感染、およびマルウェアを監視する。許可されていないトラフィックをブロックする。マルウェアを無効にして感染を修復する。ソフトウェアとアップデートの管理と管理。行動と重要なデータを監視する。また、必要に応じて、エンドポイントを追跡、トラブルシューティング、ワイプできるようにする。	ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。サポートする (不可欠)	EDR/EPP は、デバイス上のソフトウェアのインベントリを作成できる。
		ID.RA-1: 資産の脆弱性が、識別され、文書化されている。サポートする (不可欠)	EDR/EPP はデバイスをスキャンして、不足しているパッチや古いソフトウェアを検出し、報告する。後で指示された場合は、パッチをインストールすることもできる。
		ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。サポートする (不可欠)	EDR/EPP は、マルウェア、ウイルス、およびその他の署名ベースの脅威を検出して無効にする。
		PR.AC-3: リモートアクセスが、管理されている。サポートする (不可欠)	EDR/EPP には、デバイスとの間の不正な接続をブロックするファイアウォールが含まれている場合がある。
		PR.DS-1: 保存されているデータが、保護されている。サポートする (例示)	EDR/EPP はデバイスに保存されたデータを暗号化する場合がありますが、デバイスに保存されたデータは別のメカニズムを介して暗号化することもできる。
		PR.DS-2: 伝送中のデータが、保護されている。サポートする (例示)	EDR/EPP はデバイスから送信されたデータを暗号化する場合がありますが、このデータは別のメカニズムを介して暗号化することもできる。
		PR.DS-5: データ漏えいに対する防御対策が、実装されている。サポートする (例示)	EDR/EPP には、デバイスとの間の不正なトラフィックをブロックするファイアウォールが含まれている場合がある。
		PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されていサポートする (例示)	EDR/EPP は、整合性チェックを使用して、更新をインストールする前に検証する場合がある。また、整合性チェックを使用して、デバイスのソフトウェアとファームウェアのコンプライアンスを検証する場合もある。
		PR.IP-1: 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。サポートする (不可欠) およびサポートされている (先行)	EDR/EPP は、ソフトウェアとファームウェアの予想されるベースラインのインストールと構成に関して、デバイスが組織のポリシーに準拠していることを保証する。EDR/EPP が実施するこのベースラインは、組織のポリシーに従って、最小機能の概念などのセキュリティ原則に基づいて開発されている必要がある。そのため、EDR/EPP の操作はそのようなベースラインの存在に依存するが、これらのベースラインを強制および維持することもできる。
		PR.IP-6: データは、ポリシーに従って破壊されている。サポートする (例示)	EDR/EPP は、ポリシーに従って、必要に応じてデバイスからアプリケーションとデータをリモートで削除できる。他のメカニズムも、必要に応じてデータを破棄できる。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳）（access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
（つづき） エンドポイント保護プラットフォーム (EPP)		PR.IP-12: 脆弱性管理計画が、作成され、実装されている。サポートされている (先行)	EDR/EPP は、組織の脆弱性管理ポリシーを実施することにより、デバイス ソフトウェア、ファームウェア、および構成で検出された脆弱性と脅威を軽減および修復できる。これらのポリシーは、EDR/EPP が施行する前に存在している必要があり、組織の脆弱性管理計画の少なくとも一部を構成する。
		PR.PT-2: リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。サポートする (例示)	EDR/EPP は、ポリシーの要求に応じてリムーバブル メディアの使用を制限できる。
		PR.PT-3: 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。サポートする (例示)	EDR/EPP を使用して、必須機能のみを提供するようにデバイスを構成できる。
		DE.CM-4: 悪質なコードは、検知されている。サポート（例）	EDR/EPP は、マルウェア、ウイルス、およびその他の署名ベースの脅威を検出して無効にする。
		DE.CM-5: 不正なモバイルコードは、検知されている。対応（例）	EDR/EPP は、不正なモバイル コードを検出できる場合がある。
		DE.CM-7: 権限のない人員、接続、デバイス、およびソフトウェアの監視が実施されている。をサポート（不可欠）	EDR/EPP は、許可されていないソフトウェアと接続についてデバイスを監視する。
		DE.CM-3: 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	EDR/EPP は、疑わしい動作についてユーザー アクティビティを監視できる。
		RS.MI-1: インシデントは、封じ込められている。サポートする(不可欠)	EDR/EPP は、マルウェア、ウイルス、およびその他の悪意のあるトラフィックや不正なトラフィックの検出と無効化など、インシデントの封じ込めに役立つ多くのアクティビティを実行する。可能であれば感染ファイルを修復する。また、デバイスで疑わしいアクティビティや悪意のあるアクティビティが検出されたときにアラートを提供し、修復アクションを推奨する。また、デバイスに保存されているデータを暗号化するため、流出した場合のデータの有用性が制限される。
		RS.MI-2: インシデントは、緩和されている。サポートする (不可欠)	EDR/EPP は、マルウェア、ウイルス、およびその他の悪意のあるトラフィックや不正なトラフィックを検出して無効にするなど、インシデントの軽減に役立つ多くのアクティビティを実行する。可能であれば感染ファイルを修復する。また、デバイスで疑わしいアクティビティや悪意のあるアクティビティが検出されたときにアラートを提供し、修復アクションを推奨する。また、デバイスに保存されているデータを暗号化するため、流出した場合のデータの有用性が制限される。

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
セキュリティ情報およびイベント管理 (SIEM)	多くのソースからセキュリティ情報とセキュリティ イベント データを収集して統合する。データを関連付けて分析し、異常を検出し、潜在的な脅威と脆弱性を認識するのに役立ちます。データコンプライアンス要件に準拠するためにデータをログに記録する。	DE.AE-2: 検知したイベントは、攻撃の標的と手法を理解するために分析されている。サポート（例）	SIEM は、多くのコンポーネントからセキュリティおよびイベント情報を収集する。この集約されたデータは、攻撃の対象と方法を理解するために分析される場合がある。
		DE.AE-3: イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。サポートする (不可欠)	SIEM の重要な機能は、複数のソースからセキュリティ イベント データを収集して関連付けることである。
		DE.AE-4: イベントがもたらす影響が、判断されている。サポートする (例示)	セキュリティ アナリストは、SIEM データを使用して、イベントの影響を判断するのに役立てることができる。
		PR.PT-1: 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。サポートする (例示)	SIEM は、ポリシーの要求に従って、セキュリティ情報とイベント アクティビティのログを集約できる。
		DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	SIEM ログは、異常な動作や潜在的なサイバーセキュリティ イベントのその他の指標を検出するために、ネットワーク アクティビティを監視する間接的かつ非リアルタイムの方法として調べることができる。
		RS.AN-2: インシデントがもたらす影響は、把握されている。サポートする (例示)	SIEM ログは、セキュリティ アナリストがサイバーセキュリティ インシデントの影響を理解するのに役立つデータを提供できる。
		RS.AN-3: フォレンジックが、実施されている。サポートする (例示)	SIEM ログは、セキュリティ アナリストがサイバーセキュリティ インシデントのフォレンジック分析を実行するのに役立つデータを提供できる。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23）

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャ コンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係 (および関係プロパティ)	関係の説明
脆弱性のスキャンと評価	事業体のインフラストラクチャとリソースをスキャンしてセキュリティ リスクを評価する。脆弱性と設定ミスを特定する。また、インシデントへの対応の調査と優先順位付けに関する修復ガイダンスを提供する。	DE.CM-8: 脆弱性スキャンが、実施されている。サポートする (不可欠)	脆弱性スキャンおよび評価コンポーネントの重要な機能は、脆弱性スキャンを実行することである。
セキュリティ統合プラットフォーム	SIEM とその他のセキュリティ ツールを 1 つの画面に統合して、脅威に関する洞察の生成をサポートし、サイバーセキュリティ インシデントの追跡、管理、および解決を支援する。事前定義されたインシデント対応ワークフローを実行して、情報を自動的に分析し、対応に必要な操作を調整する。	RS.RP-1: 対応計画が、インシデントの発生中または発生後に実行されている。サポートする (例示)	セキュリティ統合プラットフォーム は、定義済みのインシデント対応ワークフローを実行できる。
		RS.AN-2: インシデントがもたらす影響は、把握されている。サポートする (例示)	セキュリティ アナリストは、セキュリティ統合プラットフォーム を使用してセキュリティ イベントとその影響を視覚化し、インシデントをよりよく理解できるようにする。
		RS.AN-3: フォレンジックが、実施されている。サポートする (例示)	セキュリティ アナリストは、セキュリティ統合プラットフォームを使用して、サイバーセキュリティ インシデントのフォレンジック分析を実行できる。
セキュリティ検証	ZTA のサイバーセキュリティ制御の有効性を継続的に監視、測定、検証する	DE.DP-3: 検知プロセスが、テストされている。サポートする (不可欠)	セキュリティ検証は、検出プロセスおよびその他の ZTA サイバーセキュリティ コントロールの有効性をテストおよび検証するために使用される。
		DE.DP-5: 検知プロセスが、継続的に改善されている。サポートする (例示)	組織は セキュリティ検証 を使用して、サイバーセキュリティ制御の有効性を継続的に監視、測定、および検証できるため、組織は検出プロセスを継続的に改善できる。
ネットワーク探索	ネットワーク上のデバイスとユーザーがもたらすリスクを発見、分類、評価する。	ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。サポートする (不可欠)	ネットワーク探索の重要な機能は、ネットワークを監視して、組織に脅威を与える可能性のある未知または予期しないデバイスやアクティビティを検出、特定、および文書化することである。
		DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	ネットワーク探索は、不審なイベントを示している可能性のある未知または予期しないデバイスやアクティビティを特定するのに役立ちます。これは、潜在的なサイバーセキュリティ イベントを検出するためにネットワークを監視する方法の一例である。
		DE.CM-7: 権限のない人員、接続、デバイス、およびソフトウェアの監視が実施されている。をサポート（不可欠）	ネットワーク探索コンポーネントの重要な機能は、ネットワーク上の無許可のデバイスと接続を検出することである。

[Source] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳）（access 2023/1/23)

付録）ZTA 参照設計の論理コンポーネントと CSF サブカテゴリ間のマッピング

ZTA 論理アーキテクチャコンポーネント	ZTA コンポーネントの機能	機能と CSF サブカテゴリとの関係（および関係プロパティ）	関係の説明
仮想プライベートネットワーク	許可されたリモート ユーザーが事業体内に安全にアクセスできるようにする。(内部に入ると、ZTA はユーザーのリソースへのアクセスを管理する。)	PR.AC-3: リモートアクセスが、管理されている。サポートする (例示)	リモート ユーザーが VPN 経由で事業体にアクセスすることを要求することは、リモート アクセスの管理に使用できるメカニズムの 1 つである。
		PR.DS-2: 伝送中のデータが、保護されている。サポートする (例示)	VPN は、転送中のデータを暗号化する方法の 1 つである。
		DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。サポートする (例示)	VPN で送信されるトラフィックを監視して、禁止されているアクティビティや疑わしいアクティビティを検出できる。
証明書管理	TLS 証明書の発行、インストール、検査、失効、更新、その他の管理を自動化する機能を提供する。	ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションのインベントリが作成されている。 サポートされている (先行)	サーバーとソフトウェアは、証明書を発行するために、識別され、組織のインベントリ内にあることがわかっている必要がある。
		PR.AC-1: 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。サポートする (不可欠)	サーバーの身元の検証 (つまり、認証) は、TLS 証明書の発行、使用、および管理に依存する。
		PR.AC-6: ID は、ID 利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで行使されている。サポートする (不可欠)	サーバー ID の証明 (認証) には TLS 証明書が必要である。
		PR.DS-2: 伝送中のデータが、保護されている。サポートする (不可欠)	暗号化された TLS トランスポート接続のセットアップは、TLS 証明書に依存する。
		PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。サポートする (不可欠)	TLS トランスポート接続はトラフィックの整合性チェックを提供し、TLS 接続のセットアップは TLS 証明書に依存する。公開鍵暗号化に依存する整合性メカニズムはすべて、TLS 証明書によってサポートされている。

[出典] NIST, SP1800-35 Implementing a Zero Trust Architecture Volume E: Risk and Compliance Management, NIST, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf , pp.9-26（発表者による仮訳） （access 2023/1/23)

参照ください。