資料２

技術検討会議

2022年2月24日（木）

デジタル庁

ゼロトラストアーキテクチャ適用方針のガイドライン

1. ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯
2. ゼロトラストアーキテクチャについて
3. ゼロトラストアーキテクチャ適用のメリット
4. ゼロトラストの適用原則（素案）について
5. ご意見いただきたい論点

1. ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯
2. ゼロトラストアーキテクチャについて
3. ゼロトラストアーキテクチャ適用のメリット
4. ゼロトラスト適用原則（素案）について
5. ご意見いただきたい論点

１．ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯

- 「デジタル社会の実現に向けた改革の基本方針」（令和２年12月25日閣議決定）に基づき、デジタル庁が整備・運用等を実施する安心安全なシステム提供が求められている。
- 安心安全なシステム提供に不可欠なセキュリティアーキテクチャを実現するためのコア技術となる、セキュリティ検証、クラウドやゼロトラスト等について、「政府機関等のサイバーセキュリティ対策のための統一基準群」を踏まえた技術ガイダンス策定に向けた調査に加え、デジタル庁および民間有識者等による検討会を開催し、当該検討会で検討された内容も踏まえた技術ガイダンス（素案）を作成する。
- 諸外国政府がゼロトラストアーキテクチャの戦略を発表し、国家機関のシステムのゼロトラスト対応の動きが活発な中、日本政府・府省においてもゼロトラストの適用が求められる。
- 本技術検討会ではコア技術の1つであるゼロトラストをテーマとする。

ゼロトラストを適用するための概念と考え方をまとめたガイドラインの策定が必要

１．ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯

課題

- 境界型アーキテクチャを中心としたセキュリティ

  侵入を前提としないアーキテクチャを採用しており、プロアクティブな対策がなされていない
- 政府・府省向けゼロトラスト適用に関するガイドラインの未整備

  ゼロトラストの概念を日本政府・府省向け示したガイドラインが存在しない

対応の方向性

- ゼロトラストアーキテクチャ適用の検討

  境界型モデルからゼロトラストモデルへの移行を推進して、サイバーリスクに対してリアルタイムかつプロアクティブな対応が取れるようにする
- 政府・府省向けゼロトラストアーキテクチャ適用方針のガイドライン

  米国NISTなどの諸外国のフレームワークを用い、ゼロトラストアーキテクチャの原則をまとめ、政府・府省への今後のセキュリティの試金石とする

諸外国のフレームワークに基づいたゼロトラスト適用の原則を策定予定

1. ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯
2. ゼロトラストアーキテクチャについて
3. ゼロトラストアーキテクチャ適用のメリット
4. ゼロトラスト適用原則（素案）について
5. ご意見いただきたい論点

2．ゼロトラストアーキテクチャについて

ネットワーク上には、外部/内部を問わず脅威が存在するといった前提に立ち、ユーザー、デバイスなど個々のID（Digital Identity）に焦点を当て、**「都度必要なアクションに対して必要なレベルの認証を行い、問題なければ適切なアクセス権を認可する」**といった検証を厳密に行うことで、セキュリティを担保し、且つ柔軟なUser Experienceを実現するといった概念

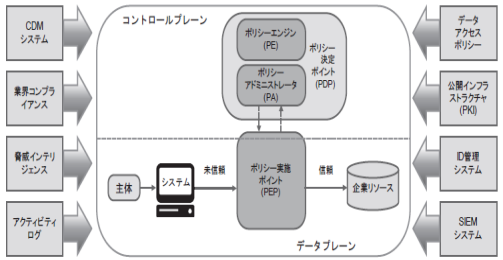


図 2:ゼロトラストの中核となる論理コンポーネント

出所;
米国National Institute of Standards and Technology
Zero Trust Architecture （nist.gov）

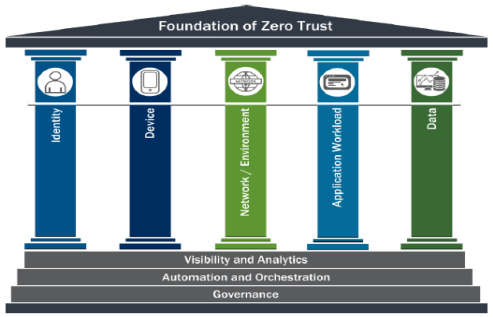
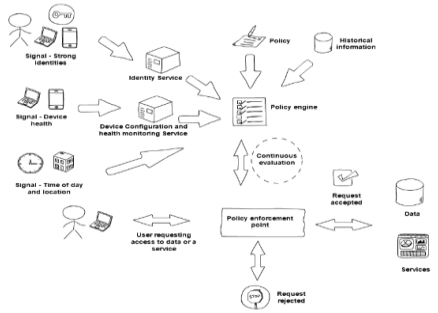


Figure 1: Foundation of Zero Trust[7]

出所；
米国CyberSecurity & Infrastructure Security Agency
CISA Zero Trust Maturity Model

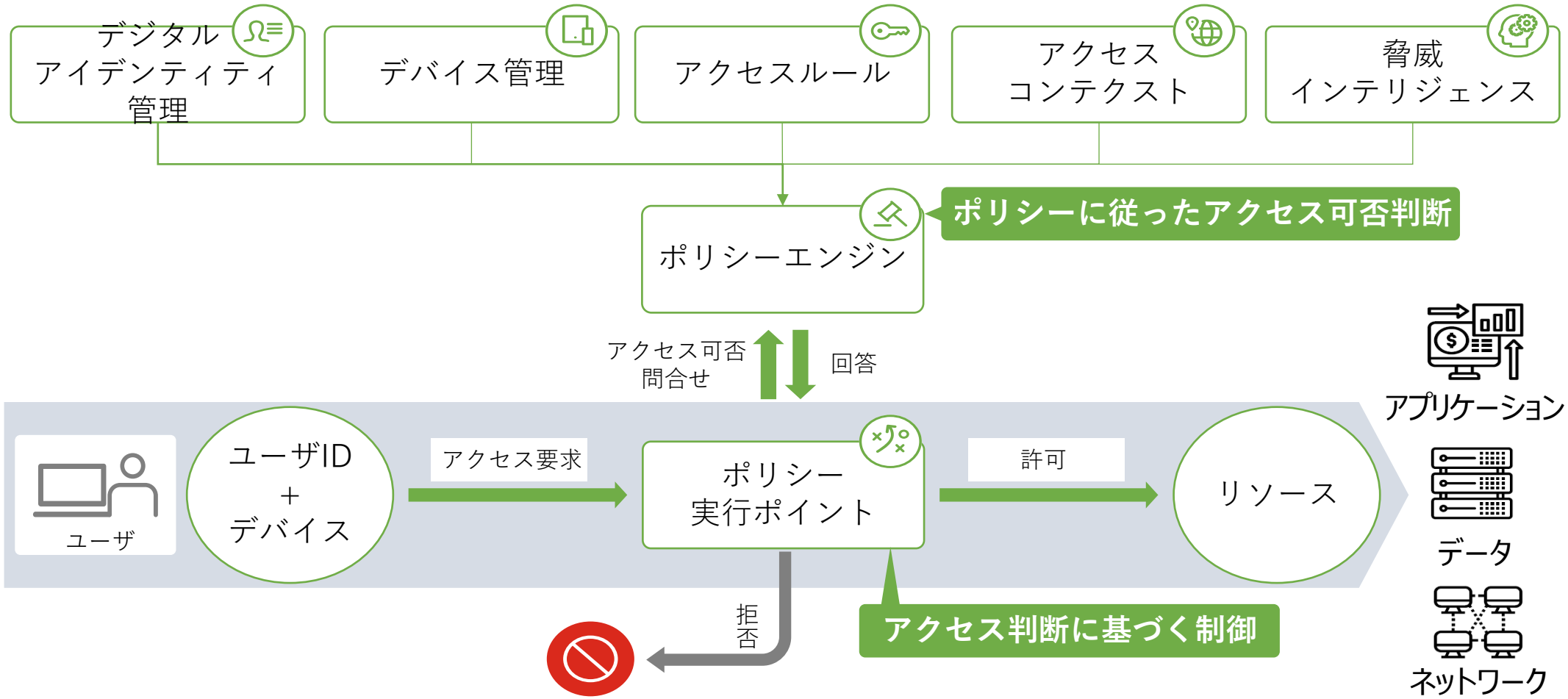


出所;
英国National Cyber Security Centre
Zero trust architecture design principles - NCSC.GOV.UK

- ゼロトラストアーキテクチャはセキュリティの概念モデルであり、ソリューションではない
- 上記概念モデルを実現するためには様々なコンポーネントを構成する必要がある
- これまでのネットワークセグメンテーションを単一の信頼源とせず、デジタルアイデンティティを基にした信頼付与へのシフト

２．ゼロトラストアーキテクチャについて

各リソースへのアクセスはデジタルアイデンティティを元にそのアクセス可否を決定する



1. ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯
2. ゼロトラストアーキテクチャについて
3. **ゼロトラストアーキテクチャ適用のメリット**
4. ゼロトラスト適用原則（素案）について
5. ご意見いただきたい論点

3．ゼロトラストアーキテクチャ適用のメリット

これまでの境界型セキュリティの課題はゼロトラストアーキテクチャの適用で解決できる

境界型セキュリティの課題	ゼロトラストセキュリティの利点
固定的な防御設計 外部と内部を明確に分けている為、組織のインフラは悪意ある第三者から識別されやすく、また防御機能は静的なため、脅威に基づいた調整や適応が困難	**動的な防御設計** どこからのアクセス要求でも組織インフラを統合的に保護し、防御機能は脅威に合わせて動的かつ柔軟に設計できる
侵害発生時の延焼、被害の甚大化 多層的な防御策を講じていても、組織のインフラ境界に重大な侵害が発生すると、甚大な被害につながる可能性がある（ランサムウェア等）	**侵害発生時の被害の最小化** ユーザ、デバイス、アプリケーション、ネットワーク、データを分離して識別し、コンテキストベースでのリスク分析に基づく動的防御が可能となり、侵害発生時においても被害が最小化される
限定的な視認性 脅威として識別されるには、攻撃がインフラ境界に到達した場合に初めて特定されるため、境界防御に監視が集中し、インフラ内部の監視は限定的となる	**視認性の向上** 動的防御による異常検出、機械学習やAI等を用いた分析を行い、データインベントリをリアルタイムで監視することにより、ダッシュボード等で組織の脅威状況をより広範囲に把握できる
リアクティブな対応 攻撃が特定されたときに初めて対応が開始され、階層化された防御網の中で封じ込めを行うことで被害の最小化を期待する	**プロアクティブな対応** どのようなデータがどこに保存され、どのような処理をされているのか等の状況がデータインベントリによって可視化されるため、脅威状況に応じて率先した行動を取ることができる

1. ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯
2. ゼロトラストアーキテクチャについて
3. ゼロトラストアーキテクチャ適用のメリット
4. **ゼロトラスト適用原則（素案）について**
5. ご意見いただきたい論点

４．ゼロトラスト適用原則（素案）について

NIST、NCSCにCISAを加えた各ゼロトラストの原則を要約し、適用原則を策定

NIST	All data sources and computing services are considered resources（資産管理） ①	Access to individual enterprise resources is granted on a per-session basis（アクセス制御） ④	The enterprise monitors and measures the integrity and security posture of all owned and associated assetsる（監視、ログ、モニタリング） ⑥	The enterprise collects as much information as possible about the current state of assets, network infrastructure（資産管理、モニタリング） ⑥
	All communication is secured regardless of network location（ネットワーク保護） ⑤	Access to resources is determined by dynamic policy—（認証） ③	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.（ID管理） ②	
NCSC	Know your architecture including users, devices, services and data（資産管理） ①	Use policies to authorise requests（認証） ③	Don’t trust any network, including your own（ネットワーク保護） ⑤	
	Know your user, service and device identities（ID管理） ②	Authenticate and authorise everywhere（認証、ID管理） ④	Choose services which have been designed for zero trust（製品選定） ⑦	
	Assess user behaviour, service and device health（アクセス制御） ④	Focus your monitoring on users, devices and services（監視、ログ、モニタリング） ⑥		
CISA or US Gov（M-22-9）	Identity: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks. ① ② ③ ④	Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments. ⑤	Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information shari ① ② ③ ④	
	Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices. ① ② ③ ④	Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports. ① ② ③ ④		

要約	
資産の把握	①
デジタルアイデンティティの管理	②
準拠すべきポリシー	③
資産の状態確認	④
ネットワーク保護	⑤
監視強化と可視化	⑥
ゼロトラスト向けに作られたサービス選定	⑦

４．ゼロトラスト適用原則（素案）について

ゼロトラストアーキテクチャ適用方針のガイドラインを策定するにあたり、
諸外国のフレームワークから導出された適用原則を主軸とした構成を予定している

ゼロトラスト目次案

本ガイドラインは概念と考え方を中心とした記載とし、適用に係る具体的な方針については別添、または留意事項として補記する程度を予定

ゼロトラストを適用するための基本的な原則を大項目として構成する
（詳細は次ページ以降に記載）

14

４．ゼロトラスト適用原則（素案）について

2-1：資産の把握

	概要
2-1-1 ゼロトラストジャーニーの第一歩	NIST、NCSC等ではゼロトラスト適用の第一歩は資産の把握からと説明がある。本ガイドラインにおいても同様の方針を想定している。
2-1-2 ツールの活用	ユーザ、サービス、デバイスなどのエンティティが境界の内外に複雑に配置されるため、手動での資産把握は困難となり、資産管理ツールなどの活用が求められる。

記載方針

- 資産（ユーザ、デバイス、サービス）の定義
- 政府・府省の環境に照らし合わせ、対象となる資産の種類（ハードウェア、ソフトウェア、ライセンス）識別（機密情報レベル）、範囲（オンプレミス、クラウド、BYOD）などの整備
- BYODなどのツールをインストールできない端末等の方針などの整備

2-2：デジタルアイデンティティの管理

	概要
2-2-1 デジタルアイデンティティの重要性	ゼロトラストアーキテクチャではデジタルアイデンティティ(以後、ID)をベースとしたアクセス制御が重要であり、IDがシステム接続との境界となり、最も重要なコンポーネントとなる。
2-2-2 デジタルアイデンティティに関する留意事項（ID一元管理）	組織全体でIDを一元管理することが望ましい(次ページ参照)

記載方針

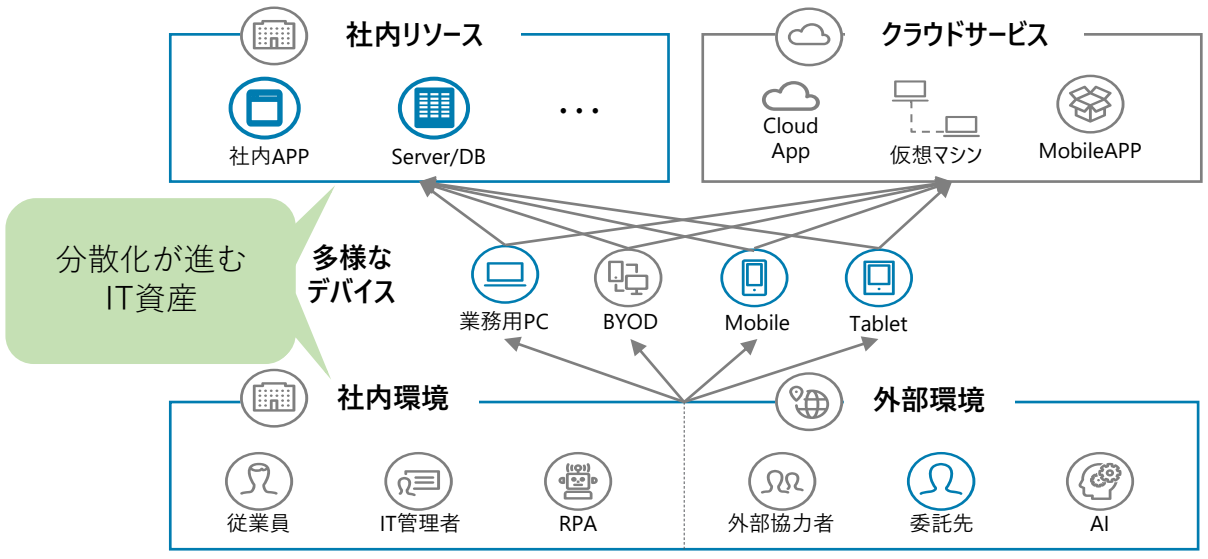
- 場所が関係なくなり、「誰が」が重要となる
- IDは資産や資産の状態把握、アクセスリクエスト承認だけでなく、監視やログにも大きく影響する
- エンティティを一意に識別するためには可能な限り一元管理、統合管理を推奨
- 一元管理、統合管理する場合の適用範囲の整備
- 政府・府省が各々で管理するIDを横断的かつ統合的に一元管理する事まで求めるのか、それぞれの府省が一意にIDを管理すればよいのか、段階的、部分的にでも統合管理を進めるほうがよいのか等の課題・問題の整理
(IDの一元管理については次ページ参照)

４．ゼロトラスト適用原則（素案）について

従来の境界型防御ではネットワーク内外への資産分散等複雑化したIT環境を保護する事が困難で、IDがリソースアクセスの境界となるゼロトラストアーキテクチャの適用が求められる

複雑化したIT環境

ITリソースへのアクセス境界が曖昧となっている



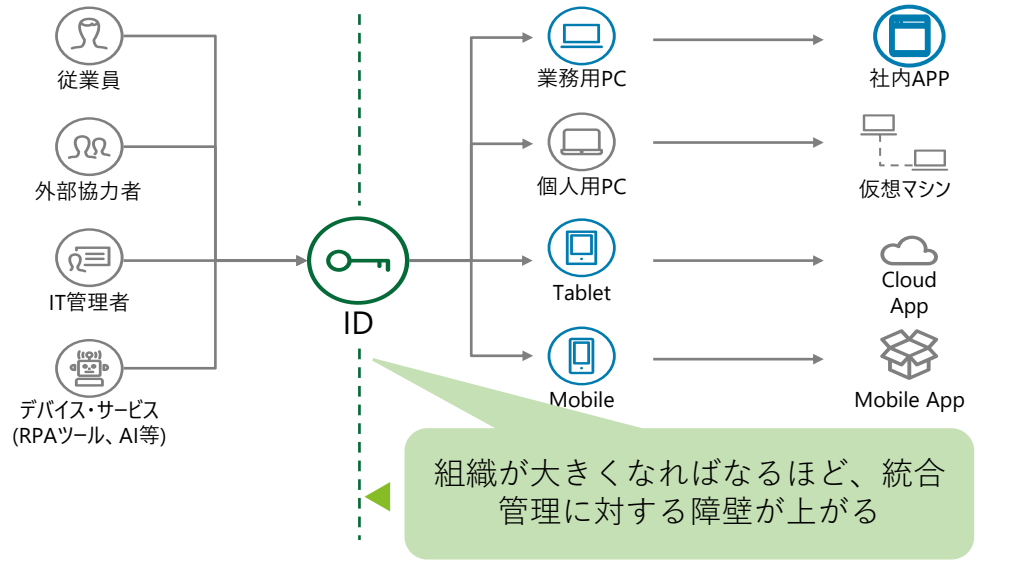
・複雑化したIT環境ではクラウド等、**社内ドメインの外側**にもITリソースが存在する

・そのため、**アクセス境界が曖昧となり**、使用者、場所、時間およびデバイスに関わらず**ネットワークセグメンテーションによるアクセス制御（境界型防御）に依存ができなくなった**

・**どこからでも、どのデバイスからでも**ITリソースへのアクセスが求められるため、セキュリティレベルの維持が困難

IDを境界としたIT環境

IDにアクセス権を付与し厳密な管理の元でITリソースを利用させる



・曖昧となったアクセス境界は実質的に**IDが各ITリソースへのアクセス境界**となる

・従業員、外部協力者等の人だけではなく、**デバイス、サービス（RPAツール、AI等）、データのIDも管理対象**となる

・IDの**アクセス要求の妥当性**を認可するために、アイデンティティやそのメタデータ（context?）に応じた**厳密**かつ**リアルタイム**な管理が求められる

政府・府省に関しては組織規模も大きく、また組織内で様々なID管理主体が存在しており、IDの統合管理に関しては大きな障壁があると想定される

４．ゼロトラスト適用原則（素案）について

2-3：準拠すべきポリシー

2-3-1
動的なポリシー

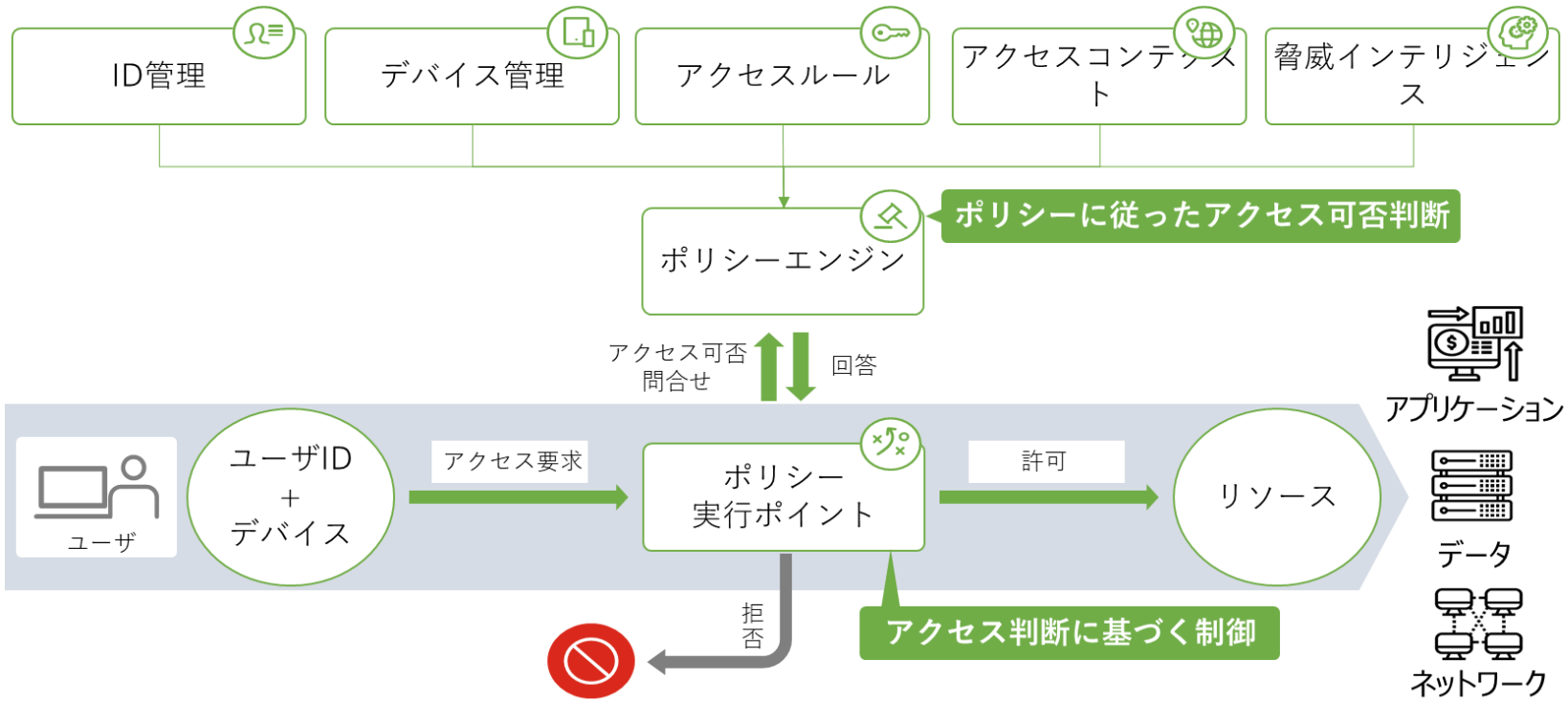
概要

アクセス時の様々なコンテキストを元に動的にアクセス制御する。

記載方針

- Policy EngineなどのNISTの構成と同等の記載
- アイデンティティやデバイスだけではなく、脅威インテリジェンス等も踏まえる

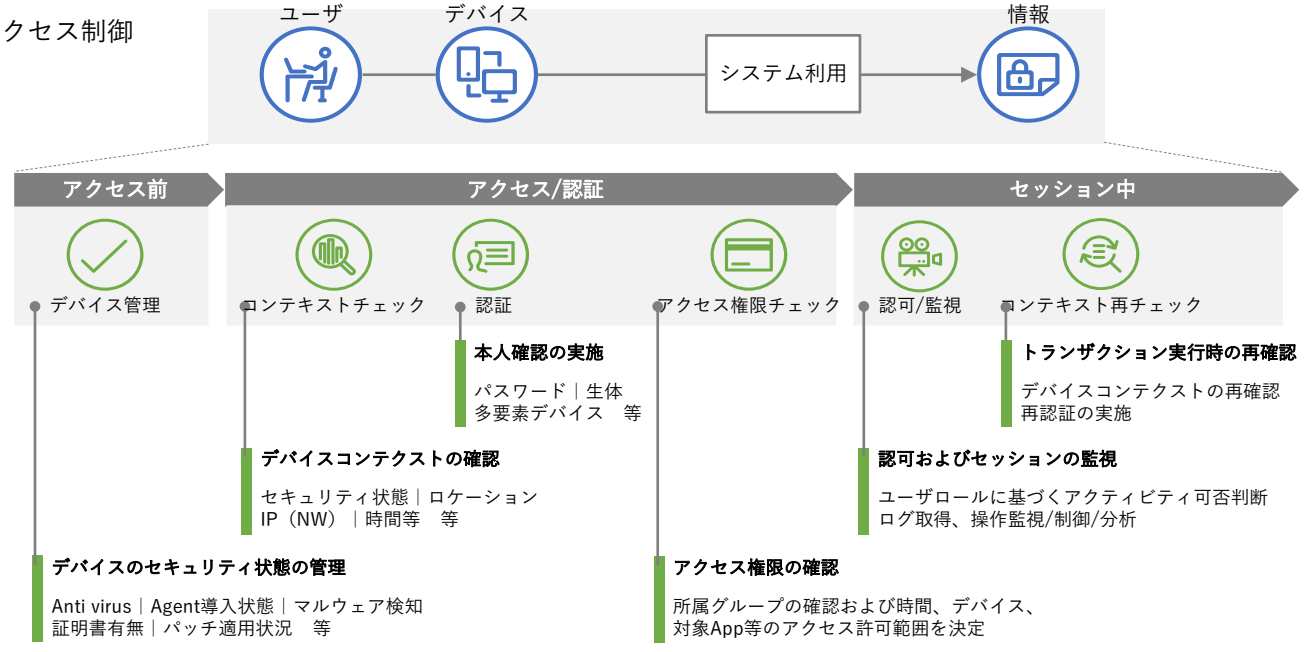
ポリシー実行イメージ



4．ゼロトラスト適用原則（素案）について

	概要	記載方針
2-4：資産の状態確認 2-4-1 属性に基づく認証・認可	これまでの役割ベースから属性ベースで認証・認可を行う必要がある。	➢ 役割ベースの認証・認可と属性ベースの認証・認可の違いの整理 ➢ 属性ベースの認証・認可がデジタルアイデンティティとアクセス承認の要であること
2-4-2 認証に関する留意点	ゼロトラストアーキテクチャにおいては「多要素認証」が求められる。	➢ 多要素認証に加え、リスクベース認証、パスワードレス認証など、様々な認証があるが、基本的には「本人確認ガイドライン」に準ずる形式とする

例)属性ベースのアクセス制御



４．ゼロトラスト適用原則（素案）について

	概要	記載方針
2-5：監視強化と可視化 2-5-1 アクティビティ監視	一意のアイデンティティが紐づけられたユーザ、サービス、デバイスのアクティビティの監視を行う。	➢ アクティビティ監視レベルの整理 （どのレベルまで監視することが求められるのか）
2-6：ネットワーク保護 2-6-1 暗号化	APIのHTTPS化、TLS1.3の利用、DNS-over-HTTPSやDNS-over-TLSといった外部通信の暗号化を必須とする。	➢ 米国政府のゼロトラスト戦略ではかなり具体的なプロトコルまで指定さているが、本ガイドラインでは「APIを暗号化する」「DNSの暗号化が必須」といったレベルでの記載を予定 ➢ DNSの暗号化等、現実的にまだ困難な対応についての記載方針の整理
2-7：サービスの選定 2-7-1 ゼロトラストサービスと謳う機能の利活用	単一サービスでゼロトラストを完結するのではなく、また資産を保護するためにはゼロトラストに適用した様々なサービスを組み合わせる必要がある。	➢ ゼロトラストに適合したサービス例等の具体化（一つの製品、ソリューションだけでゼロトラストは完結しないため、ケース説明が必要と思慮）

1. ゼロトラストアーキテクチャ適用方針のガイドライン策定に至る経緯
2. ゼロトラストアーキテクチャについて
3. ゼロトラストアーキテクチャ適用のメリット
4. ゼロトラスト適用原則（素案）について
5. **ご意見いただきたい論点**

５．ご意見頂きたい論点

- **ゼロトラストアーキテクチャについて**
  適用の要否、適用にあたっての留意点、検討の方向性等
- **ゼロトラストアーキテクチャ適用のメリットについて**
  ゼロトラスト適用の具体的な事例、適用したことによる課題等
- **ゼロトラスト適用原則（素案）について**
  諸外国のフレームワークの活用、網羅性、政府・府省への適切性、盛り込むべき要素等

Appendix

ゼロトラスト適用原則（素案）について

諸外国フレームワークを参照し、ゼロトラストアーキテクチャに必要となる原則を検討

NIST SP 800-207*1

最も一般的なNISTのゼロトラスト原則のガイドライン。

NCSC Zero trust architecture design principles *2

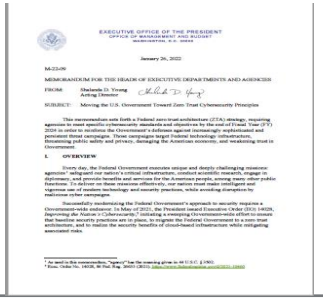
NCSCにおけるゼロトラスト7大原則

US CISA / Gov （M-22-9） *3

CISAが策定したゼロトラスト成熟度モデル

OFFICE OF MANAGEMENT AND BUDGET *4

■ CISAのゼロトラスト成熟度モデルを元に発行したゼロトラスト戦略



*1:出所:米国National Institute of Standards and Technology 、Zero Trust Architecture （nist.gov）
*2:出所:英国National Cyber Security Centre、Zero trust architecture design principles - NCSC.GOV.UK
*3:出所:米国CyberSecurity & Infrastructure Security Agency 、CISA Zero Trust Maturity Model
*4:出所:米国政府、M-22-09 Federal Zero Trust Strategy （whitehouse.gov）

ゼロトラスト適用原則（素案）について

NCSCのZero trust architecture design principlesは8原則で成り立っている

No	原文	概要	取組み例
1	Know your architecture including users, devices, services and data	資産（人、モノ、サービス、情報）を把握	資産管理
2	Know your user, service and device identities	IDを（人、モノ、サービス）を管理	ID管理
3	Assess user behaviour, service and device health	正常性を評価	検証、検疫
4	Use policies to authorise requests	ルールに基づいた承認	認証
5	Authenticate and authorise everywhere	場所を問わない認証および承認	資産管理、ID管理
6	Focus your monitoring on users, devices and services	エンドポイント監視の強化	監視、ログ、モニタリング
7	Don't trust any network, including your own	境界内外全てのネットワークを検証	検証、検疫、暗号
8	Choose services which have been designed for zero trust	ゼロトラストを前提としたサービス選定	ルール整備

ゼロトラスト適用原則（素案）について

NIST SP800-207のゼロトラストは7原則で成り立っている

No	原文	概要	取組み例
1	All data sources and computing services are considered resources	全てのデータとサービスをリソースとみなす	資産管理
2	All communication is secured regardless of network location	全てのネットワーク通信を保護する	暗号
3	Access to individual enterprise resources is granted on a per-session basis	リソースへのアクセス時はセッションごとに許可判定を行う	検証、検疫
4	Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.	リソースへのアクセスの許可判定は動的ポリシーで制御	認証
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets	すべての資産のセキュリティ状態を監視、測定する	監視、ログ、モニタリング
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	すべての認証と許可は動的かつ厳密に行う	ID管理
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	資産、ネットワーク等の現況情報をできるだけ多く収集しセキュリティ向上に活用する	資産管理、モニタリング

常時診断・対応型セキュリティアーキテクチャ技術レポート

常時診断・対応型セキュリティアーキテクチャ技術レポート(仮)はCDMアーキテクチャの要約で構成する予定です

目次･構成案

目次（案）

- 1はじめに
  - 1背景と目的
  - 2適用対象
  - 3位置づけ
  - 4用語
- 2基本方針
  - 1ゼロトラストにおけるCDM
  - 2米国版CDMプログラム
- 3CDMの詳細項目
  - 1CDMの概要とアーキテクチャ
  - 2事例

その他の技術レポートと同様の構成と内容を想定

ゼロトラストアーキテクチャとの関連性

IPA「次世代政府セキュリティアーキテクチャの検討」より「2.アーキテクチャの概要」の要約

以下の内容のうちどこを対象とするか
- ✓ 概要図はIPAを流用
- ✓ 各レイヤごとの説明（ガバナンスレイヤ、業務レイヤ、アプリケーションレイヤ、技術レイヤ）をどこまで詳細に記載する必要があるか

関連性に関するイメージ図（From NIST）

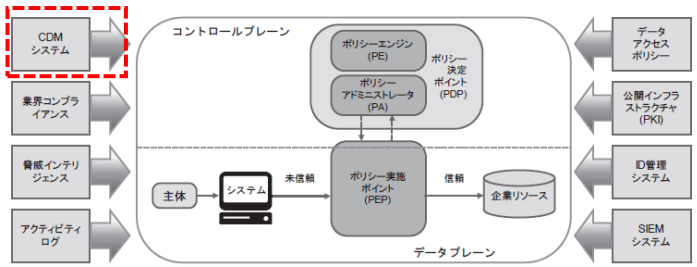


図 2: ゼロトラストの中核となる論理コンポーネント