Zero Trust Architecture

４年たってどう進んだ？
（2021年3月3日　第63回NCWG会合）
（2024年6月28日　第73回NCWG会合）

2025年6月11日　第78回NCWG会合

- 株式会社コンピュート　取締役
- 三井物産セキュアディレクション株式会社
  プリンシパル・コンサルタント

福原　英之

アジェンダ

1. ゼロトラストとは？
2. 米国政府の動向
3. 国防総省ゼロトラストの概要
4. まとめ
5. Notebook LM による国防省ゼロトラストのサマリー

＜参考１＞ゼロトラストの背景

1. 境界防御の崩壊
   - マルウェアによる内部攻撃
   - 内部犯による攻撃
   - 標的型攻撃の高度化
2. SOAの成熟
   - Web-API、マイクロサービス化
3. 認証（AAA）技術の普及
   - 個人IDの普及
   - 多要素認証の普及
4. クラウドサービスの普及

⇒すべてのシステムがインターネットに
さらされているくらい危険

1．ゼロトラストとは？

Zero Trust

2010年　米国の調査会社フォレスター・リサーチ（Forrester Research）のジョン・キンダーバーグ氏（John Kindervag）が提唱した概念/造語

~~TRUST BUT VERIFIED~~

“never trust, always verify”

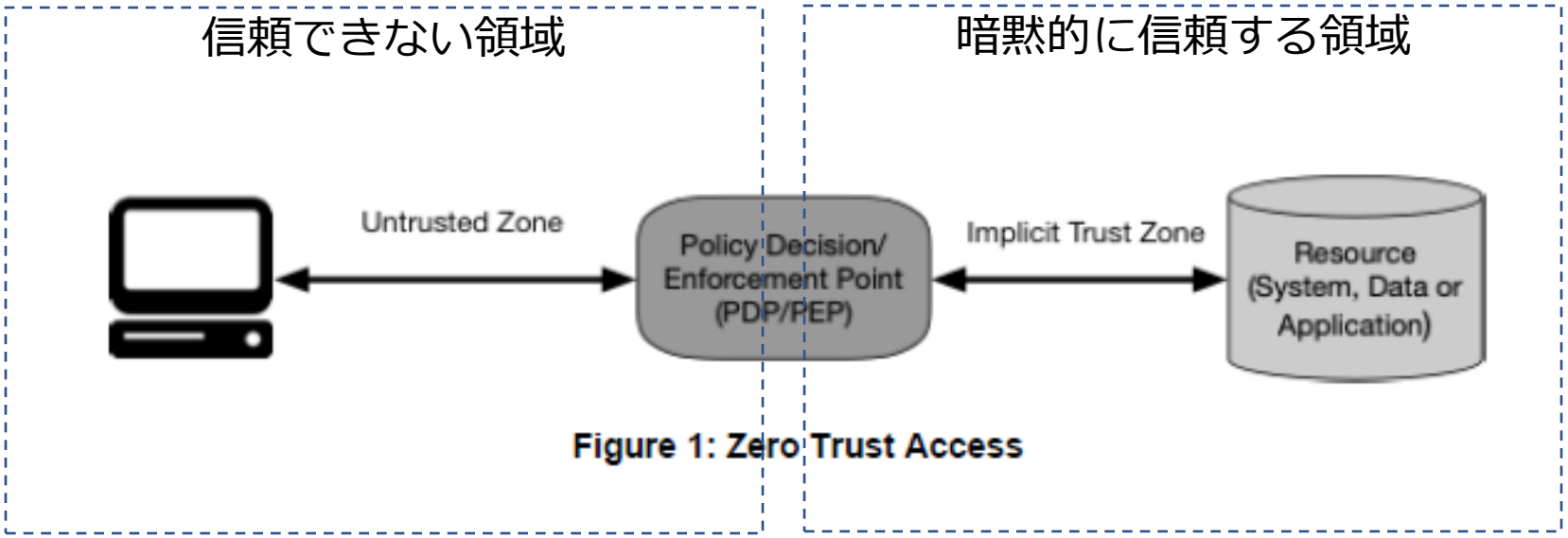
全てのデバイス、サーバ、ネットワークからのアクセスを信頼できない前提でセキュリティ対策を講じる

NIST (National Institute of Standards and Technology, , アメリカ国立標準技術研究所)

SP 800-207: Zero Trust Architecture (ZTA)
2019/9/23: Draft1, 2020/2/13: Draft2, 2020/8/11: Final

https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207

＜参考２＞　ZTAの基本概念

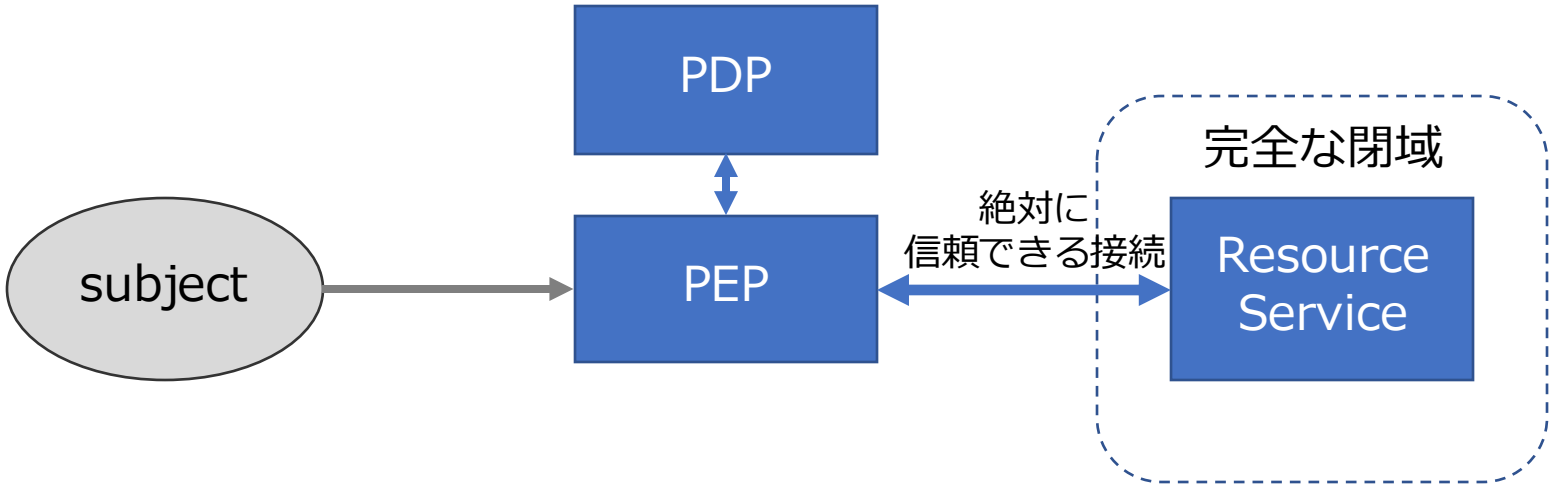


subject　　resource

図は、NIST SP800-207 より引用

＜参考３＞ZTAに絶対必要な要素

- リソースの閉域化
- PEPの配置
- PDPの配置
- アクセスポリシー
- アクセス可否を判断する情報



２．米国政府の動向①　(2020年～2022年)

- NIST
  - SP800-207 「Zero Trust Architecture」　（2020/8/11）
- White House
  - Executive Order 14028 「Executive Order on Improving the Nation’s Cybersecurity」（2021/5/12）
- OMB（Office of Management and Budget：行政予算管理局）
  - M-22-09「Moving the U.S. Government Toward Zero Trust Cybersecurity Principles」（2022/1/26）
    - ５つの要素に分けて、2024年までの実行を求めた
- DoD（Department of Defense：国防総省）
  - 「DoD Zero Trust Strategy」（2022/11/7）
    - 7つの柱に分けて実施する
    - 2027年度中にゼロトラストを実行する
    - 2028年以降のロードマップも含めてる

⇒具体的な技術に落とし込めていない

- 現在各ベンダーが絶賛ロビー活動

２．米国政府の動向②　(2023年～)

- NIST
  - SP800-207A 「A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments」（2023/9/13）
- CISA（サイバーセキュリティ・社会基盤安全保障庁）
  - Zero Trust Maturity Model v2.0（2023/4）
- DoD（Department of Defense：国防総省）
  - DoD Zero Trust Capability Execution Roadmap（2023/6/6）
    - 7つのピラーに対して、具体的な実装方法が記載されている
- NSA（国家安全保障局）
  - 「Advancing Zero Trust Maturity Throughout～」が7つのピラー毎に出されている（ほぼ2024年）
- CDO協議会／CISO協議会
  - Federal Zero Trust Data Security Guide（2024/10）

２．米国政府の動向③　結果・現状

- U-22-09の達成状況
  - 2024年9月4日　連邦政府CIO（Clare Martorana）
    - 主要24機関は90%台後半の達成率

    https://www.nextgov.com/cybersecurity/2024/09/major-agencies-are-close-meeting-september-zero-trust-deadline-federal-cio-says/399270/
- U-22-09の効果
  - GSA（一般調達局）
    - 政府機関向けZTAの実装部品カタログを提供
      - Achieve Zero Trust Capabilities Using These Cloud Identity Adoption Best Practices | GSA
  - NSA
    - 7つのピラー毎のガイドを公開
  - DoD
    - 具体的な実装計画を公開

3．DoD Zero Trust Strategyの概要

“never trust, always verify”

3-1. DoD Zero Trust Strategy の概要

<全体像> （notebooklmで下書き作成）

- 2027年末までに、DoDは「Target Level ZT」を達成する（戦略目標）
- 現在既知の脅威からのリスクを管理するために必要な、最低限のゼロトラスト能力のアウトカムと活動のセットが含まれます。
- これはあくまで最低限のレベルであり、その後も継続的に成熟が進められることになります。
- 7つのピラーに分ける

7つのピラー（柱）	
1．ユーザ	5．ネットワークと環境
2．デバイス	6．自動化とオーケストレーション
3．アプリケーションとワークロード	7．可視性と分析
4．データ	

3-2.　7つのピラーの超要約①

Pillar(7つの柱)	2027年までにやること
1．User	ID管理システムのデータソースを明確にする
	特権アカウントと非特権アカウントを把握する
	ローカルで管理している特権アカウントを把握する
	権限を最小化し自動化する
2．Device	デバイス管理システムを導入し、資産・脆弱性・パッチ管理する
	UEDM等の管理ツールで、デバイスのコンプライアンスポリシーチェックを実施する（Unified Endpoint ＆ Device Management）
3．Application & Workload	アプリケーションの構成要素の詳細を把握する
	SBOMを管理しリスクを管理する
	脆弱性管理ツールで脆弱性に対応する
	継続的検証ツールによって更新時も（自動）検証する
4．Data	データのタグ付けと分類のためにデータを分析する
	データのタグ付けとラベル付けを実装する
	SDSの調査と実装(Software Defined Storage)

＊ワークロード：複数のプログラムやアプリケーション、または緊密に連携するコンポーネントの集まり

3-2.　7つのピラーの超要約②

Pillar(7つの柱)	2027年までにやること
5．Network & Environment	アクセスポリシーを標準化して細かく設定する
	APIのフィルタを定義し、実装する
	プロキシ等で属性やフロー、デバイスのコンプライアンスに従ったアクセス制限を実装する
6．Automation & Orchestration	データのタグ付けと機密分類を自動化する
	APIを標準化し標準に合わせる
7．Visibility & Analytics	ログフォーマットを標準化する
	分析対象を明確にし、リスクレベルを分析する
	分析ツールを導入する
	MLやUEBA (User and Entity Behavior Analytics) を活用して正常・異常を判定する
	脅威インテリジェンスを収集し集約する

4. まとめ① Zero Trustのための前提（システム化以前にやるめきこと）

- 組織で管理されたID
  - 全社で統一したIDを発行し、認証に使う
- データの分類
  - 全社統一の基準で、データを機密性や種類で分類する
- インベントリ管理
  - ハードウェア、ソフトウェアのインベントリを全社で一元管理する
- API疎結合
  - 全社（クラウド含む）のシステム連携は、API（RESTfull）疎結合にする
- ポリシーやルールの整備
  - セキュリティや、システムアーキテクチャのポリシーを明文化し、定着させる
- 継続的な運用体制の整備
  - 上記内容を継続できる（見直しを含む）ように、強制権限を持つ組織体制を整備する。

4. まとめ②　Zero Trustのためのシステムの実装

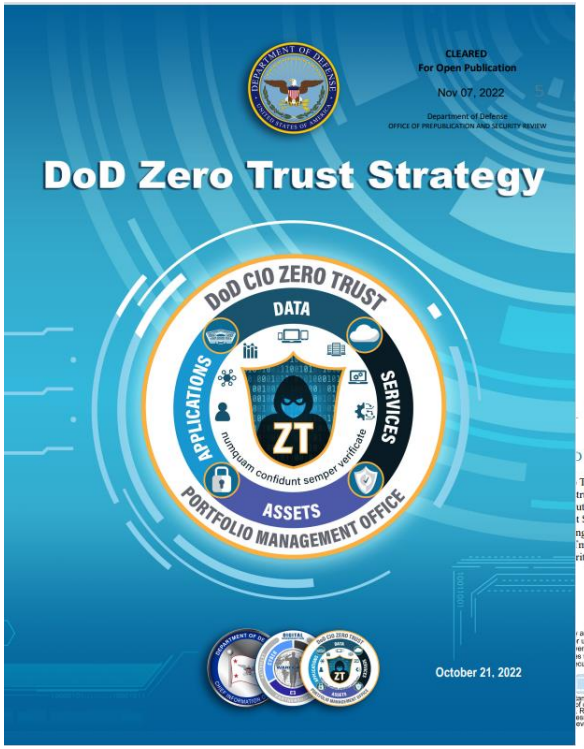
- IDMによるID管理
  - IDMを導入し、すべてのシステムのID情報を自動連携する
- デバイス管理とEDR導入
  - MDMやEDRをすべての端末と必要なサーバに導入し一元管理する
- マイクロセグメンテーションと徹底した通信アクセス管理
  - マイクロセグメンテーションを徹底する
  - セグメント間、ゾーン間の通信アクセス制限を徹底する
- データ分類とタグ付けの自動化
  - ポリシーに基づきデータ分類とタグ付けを自動化する
- 属性に基づいたデータアクセス制御
  - 【肝】SubjectとResourceの両方の属性でデータアクセスを制限する
- インベントリー情報に基づく脆弱性管理
  - 脆弱性情報を自動入手し、インベントリの脆弱性を自動管理する
- ログ集約（SIEM）と常時監視
  - 常時監視し、対応できるシステムと共に、体制を強化する

５．Notebook LM による
国防省ゼロトラストのサマリー

国防総省ゼロトラスト戦略：2027年の目標と活動

- DoD-ZTStrategy.pdf
- ZT-CapabilitiesActivities.pdf

DoD Zero Trust Strategy （37ページ）



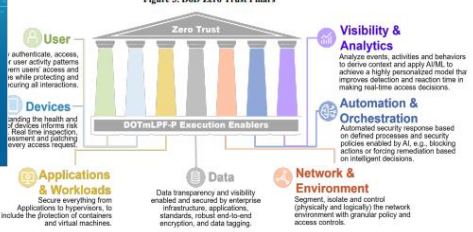
Systems Policy 21 (CNSSP 21), and account for the National Institute of Standards and Technology's (NIST) ZT tenets.[33]

Reduce Complexity. Align technical and security programs with ZT goals and mission objectives to streamline regulations and standards for managing security and risk.

Zero Trust Pillars

Trust capabilities across the IE must be developed, deployed, and operated within an organizing truct defined by seven DoD Zero Trust Pillars and their enablers to ensure standardization of ution. These pillars, as depicted in **Figure 3**, provide the foundational areas for the DoD Zero t Security Model and the DoD Zero Trust Architecture.[34] The execution enablers are cross- ng, non-technical capabilities and activities that address culture, governance, and elements of mLPF-P (e.g., ZT Training, etc.).[35] This ZT security model re-thinks the implementation of rity access to resources and is determined by dynamic policy, including observable state of user

Figure 3. DoD Zero Trust Pillars



[33]The seven tenets of zero trust are outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture, p. 6. These include: 1) All data sources and computing services are considered resources; 2) All communication is secured regardless of network location; 3) Access to individual enterprise resources is granted on a per-session basis; 4) Access to resources is determined by dynamic policy; 5) The enterprise monitors and measures the integrity and security posture of all owned and associated assets; 6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed; 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.

[34] See the DoD ZT RA, v2.0, Sections 2.2 – 2.3, pp. 20 - 23 for a more detailed explanation of the DoD ZT Security Model, the strategic benefit for each pillar and the intended result of all seven pillars working together.

[35] Details regarding supporting enablers will be further refined and integrated into next versions of the *DoD ZT Capability Roadmap* and addressed in implementation plans. Enablers identified to-date include: ZT Awareness & Culture, Adaptive Implementation Governance, ZT Policy Framework, ZT Training, and others.

Executive Summary

"Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

— Executive Order on Improving the Nation's Cybersecurity 12 May 2021

Five Years into the Future

The Department of Defense's (DoD) risk-based Zero Trust Framework employed across the Joint Force and the defense ecosystem protects our information systems[1] from increasingly sophisticated attacks as our adversaries seek to affect our warfighters and DoD mission success. Zero Trust principles are now integrated into each of the five cybersecurity functions that represent key elements of a successful and holistic cybersecurity program – Identify, Protect, Detect, Respond, and Recover.[2] As a result, DoD will successfully mitigate attempts to deny, degrade, disrupt, deceive, or destroy our information systems. Operators at all levels are confident that the data accessed, the assets deployed, the applications used, and the services provided are secured and resilient.

Today

The Department's Information Enterprise is under wide scale and persistent attack from known and unknown malicious actors. The Department's most consequential strategic competitor and the pacing challenge for the Department, the People's Republic of China,[3] as well as other state-sponsored adversaries and individual malicious actors often breach the Department's defensive perimeter and roam freely within our information systems. The Department must act now.

Vulnerabilities exposed by data breaches inside and outside the Department of Defense demonstrate the need for a new, more robust cybersecurity framework that facilitates well-informed risk-based decisions.[4] Zero Trust security eliminates the traditional idea of perimeters, trusted networks, devices, personas, or processes and shifts to multi-attribute-based levels of confidence that enable authentication and authorization policies founded on the concept of least privileged access. Implementing the Zero Trust Framework requires designing a more efficient architecture that enhances security, the user experience, and overall mission performance.

Zero Trust uses continuous multi-factor authentication, micro-segmentation, advanced encryption, endpoint security, analytics, and robust auditing, among other capabilities, to fortify data,

[1] Information system includes "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information". See DoD Instruction (DoDI) 5000.82, *Acquisition of Information Technology (IT)*, 21 Apr 2020, p. 17.

[2] See US National Institute of Standards and Technology (NIST), Special Publication 1271, *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*, 6 August 2021, for descriptions of cybersecurity core functions and a set of guidelines for mitigating organizational cybersecurity risks.

[3] *Fact Sheet: 2022 National Defense Strategy*, 28 March 2022.

[4]Risk" refers to probability of an undesired event or condition and 2) the consequences, impact, or severity of the undesired event, were it to occur. See *DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, January 2017, p. 3

DoD Zero Trust Capabilities Activities（13ページ）

CLEARED
For Open Publication
Dec 17, 2024
25-T-0638
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
1.1.1	Inventory User	User	Component	Target Level ZT	25.9	DoD Components utilize enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity lifecycle management processes (i.e. joiner/mover/leaver/returner). IT Privileged users are clearly identified.	1. Identified Managed Non-Privileged Users. 2. Identified Managed Privileged Users. 3. Identified applications using their own user account management for non-administrative and administrative accounts. 4. Identify the Authoritative Source of Identities.	Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the true and up-to-date user data.		Rule Based Dynamic Access Pt1
1.2.1	Implement App Based Permissions per Enterprise	User	Enterprise and Component	Target Level ZT	17.7	The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for -adding/updating attributes within the solution to betters support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by the roles.	1. Enterprise roles/attributes needed for user authorization to application functions and/or data have been-vetted and approved through the ICAM governance processes. 2. Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e. attributes and entitlements) while maximizing the usage of self-service attributes and entitlements. 3. Components identify attributes associated with PAM activities within their network/system boundary. 4. Component ICAM implementation obtain authoritative information about personnel (i.e. attributes, and entitlements) from a central attribute source once. available, or from other DoD Components using standard profiles otherwise.	Authoritative attributes requiired to implement conditional user access into applications are available to support privileged access management.		
1.2.2	Rule Based Dynamic Access Pt1	User	Component	Target Level ZT	22.1	DoD Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time access and Just-Enough-Administration methods.	1. Access to applications'/services' functions and/or data are limited to users with appropriate Attribute Based Access Control (users, devices, environment etc.) allowing for granular and flexible control. 2. All possible applications use JIT/JEA permissions for administrative users.	Periodic challenges occur where access is affected if challenge is failed within accepted response parameters. Access is always predicated on authentication and authorization with activity happening (decisions made) in real time.	Single Authentication Inventory User	Rule Based Dynamic Access Pt2; AI-enabled Network Access

5-1. ユーザ

- 2027年までに、すべての個人および非個人エンティティ（NPE）に対して、**強力な認証**が適用され、アクセスは**最小特権の原則**に基づいて制限・強制されるようになります
  - エンタープライズレベルの信頼できるIDソースの利用と、ローカルなIDソースとの連携。
  - 属性ベースのアクセス制御（ABAC）ルールに基づいた、アプリケーションごとの権限管理。
  - 特権ユーザーアカウントに対する**特権アクセス管理（PAM）**ソリューションの導入と、Just-in-Time（JIT）/ Just-Enough-Administration（JEA）の原則の適用。
  - 標準化されたアカウントライフサイクル管理プロセスの確立。
  - ユーザーおよびエンティティの行動分析（UEBA）とユーザーアクティビティモニタリング（UAM）ツールの導入と、エンタープライズIDプロバイダー（IdP）との連携。
  - デフォルト拒否（Deny by Default）ポリシーの適用と、過剰な権限の削除。
  - セッションごとの認証の実施と、セキュリティ属性やデータ重要度に基づいた定期的認証の適用。
  - エンタープライズ公開鍵基盤（PKI）ソリューションの導入と、コンポーネントPKIとの連携による、検証されたエンタープライズIDプロバイダープラットフォームの確立

5-2.　デバイス①

- すべてのデバイスが識別、インベントリ化、承認、認証され、**継続的にリアルタイムでパッチ適用**される状態を目指します
  - 環境内のデバイスのインベントリ作成と属性の追跡。
  - DoDエンタープライズPKIソリューションを利用した、サポート対象および管理対象デバイスへのx509証明書の展開。
  - デバイスやサービスアカウントなどのNPEの、エンタープライズIdPへの統合。
  - **Comply to Connect（C2C）**ポリシーの実施と強制による、ネットワーク接続前のデバイスのコンプライアンスチェック。
  - ファイル整合性監視（FIM）およびアプリケーション制御ツールの導入。
  - 次世代アンチウイルス（NGAV）ツールの導入と、C2Cソリューションとの連携。
  - 管理されていないリモートおよびローカルデバイスアクセスのデフォルトでのブロック。

5-2.　デバイス②

- すべてのデバイスが識別、インベントリ化、承認、認証され、**継続的にリアルタイムでパッチ適用**される状態を目指します
  - 管理されたBring Your Own Device（BYOD）およびInternet of Things（IoT）デバイスの、エンタープライズデバイス管理ソリューションとエンタープライズIdPへの統合と、動的なアクセスポリシーおよび最小特権の原則の適用。
  - アセット、脆弱性、パッチ管理ツールの導入による、デバイスのコンプライアンス確認と、自動化および統合に向けたAPIの活用。
  - 統合エンドポイントデバイス管理（UEDM）ツールの導入による、最小コンプライアンス、アセット管理、APIサポートの実現。
  - エンドポイント検出・対応（EDR）ツールの導入と、C2Cソリューションとの連携による、高度な脅威の検出と対応の自動化。
  - 拡張検出・対応（XDR）ソリューションの導入と、C2CおよびSIEMとの連携による、脅威状況の包括的な把握と協調的な対応

5-3.　アプリケーションとワークロード①

- すべてのアプリケーションとワークロードが保護され、コンテナや仮想マシンの保護も含まれます。
  - 利用されている承認済みアプリケーションとコード（オープンソース、商用、内製開発を含む）のインベントリ作成。
  - 最新のDevSecOpsプロセスとCI/CDパイプラインのベストプラクティスの適用と、脆弱性管理の統合。
  - アプリケーションセキュリティとコード修正の標準化されたアプローチの導入と、APIゲートウェイの保護。
  - 承認済みバイナリとコードの体系的な管理（サプライヤーリスク管理、承認済みリポジトリの利用、部品表（BOM）の活用、業界標準の脆弱性管理）。
  - 脆弱性管理プログラムの確立と、公開および非公開の脆弱性リポジトリの追跡と管理。

5-3.　アプリケーションとワークロード②

- すべてのアプリケーションとワークロードが保護され、コンテナや仮想マシンの保護も含まれます。
  - CI/CDパイプラインへのセキュリティテスト、インシデントレスポンス、SIEMアラート/ロギングの統合による、継続的な検証の実施。
  - 認証後のIDとデバイスとの統合による、承認済みリソース承認ゲートウェイの展開と、外部向けアプリケーションへの適用。
  - すべての可能なアプリケーションへのポリシー強制の適用と、CI/CDパイプラインへの承認の統合による、自動化された意思決定。
  - ソフトウェア定義コンピューティング（SDC）ポリシーの確立と、承認済みコードライブラリとパッケージを使用したベースラインの作成と適用

＊ワークロード

複数のプログラムやアプリケーション、または緊密に連携するコンポーネントの集まり

5-4. データ①

- エンタープライズインフラストラクチャ、アプリケーション、標準、堅牢なエンドツーエンド暗号化、データタグ付けによる、**データの透過性と可視性**の実現
  - データタグ付けとラベル付けのためのアルゴリズムの開発と、管理体制の確立。
  - 業界のベストプラクティスに基づいたデータ分類標準の確立と実装、手動および自動のタグの識別。
  - 必須のデータ権限管理（DRM）オーバーレイと保護メカニズムを含む、相互運用性標準の開発。
  - ソフトウェア定義ストレージ（SDS）ポリシーの策定と、SDS実装に向けた既存データストレージ戦略とテクノロジーの評価。
  - データタグ付けツールと分類ツールの実装による、ルールの作成、変更、テストの実施。
  - データ損失防止（DLP）の実施ポイントのビジネスルールの特定と、標準化されたロギングの確保。

5-4. データ②

- エンタープライズインフラストラクチャ、アプリケーション、標準、堅牢なエンドツーエンド暗号化、データタグ付けによる、**データの透過性と可視性**の実現
  - デジタルアセット管理におけるデータ権限管理（DRM）の実施ポイントのビジネスルールの特定と、標準化されたロギングの確保。
  - 高リスクデータリポジトリに対するDRMと保護ツールの有効化。
  - データプロデューサーによって定義されたデータタグを使用した、データ権限管理（DRM）および保護ソリューションの確立と、高リスクデータの暗号化と保護。
  - データプライバシーと保護（DPP）に沿ったデータ損失防止（DLP）の強化と、属性注入による保護措置の発動。
  - SDSポリシーによって確立されたゼロトラストのアウトカムに対する、コンポーネントDAASポリシーの適合性を保証するガバナンスメカニズムの確立。
  - エンタープライズIdPとのソリューションとポリシーの統合

5-5.　ネットワークと環境①

- ネットワーク/環境（オンプレミスおよびオフプレミス）の**論理的および物理的なセグメンテーション、分離、制御**と、きめ細かいアクセスおよびポリシー制限の適用
  - きめ細かいネットワークアクセスルールとポリシーの作成と、既存ネットワーク技術への実装。
  - ソフトウェア定義ネットワーキング（SDN）または代替ネットワーキングアプローチインフラストラクチャの実装と、セグメンテーションゲートウェイと認証決定ポイントの統合、標準化されたログリポジトリへの出力。
  - ネットワークインフラストラクチャとフローの、物理的または論理的な制御プレーン、管理プレーン、データプレーンへのセグメンテーション（IPv6/VLANアプローチの利用）。
  - デバイス属性と動作に基づいたプロキシと強制チェックのSDNまたは代替ネットワーキングアプローチソリューションへの組み込み。

5-5.　ネットワークと環境②

- ネットワーク/環境（オンプレミスおよびオフプレミス）の**論理的および物理的なセグメンテーション、分離、制御**と、きめ細かいアクセスおよびポリシー制限の適用
  - ミッション/組織ベースのマクロセグメンテーションの実施による、ラテラルムーブメントの制限。
  - サービスコンポーネント（Web、アプリケーション、データベースなど）、ポート、プロトコルの基本的なセグメンテーションを可能にする、マイクロセグメンテーションインフラストラクチャのSDNまたは代替ネットワーキングアプローチ環境への実装。
  - ユーザーとデバイスに対する、論理ネットワークゾーン、役割、属性、条件に基づいたアクセスコントロール、ネットワークリソースに対する特権アクセス管理サービス、APIアクセスに対するポリシーベースの制御の確立。
  - データフローマッピングと監視標準に基づいた、伝送中のデータの保護ポリシーの有効化（連合情報共有、システム境界を越える共有、アーキテクチャコンポーネント間の保護を含む）

5-6.　自動化とオーケストレーション①

- 手動のセキュリティおよびその他の該当するプロセスを自動化し、**エンタープライズ全体でポリシーベースのアクションを迅速かつ大規模に実行**
  - 既存のサイバーセキュリティポリシーと標準のカタログ化とインベントリ作成、ZTターゲット機能を満たすためのポリシーの更新と作成。
  - ユーザー、データ、ネットワーク、デバイスピラーからのデータを使用した、ミッション/タスクおよび非ミッション/タスクDAASアクセス用のアクセスプロファイルルールの開発と、エンタープライズセキュリティプロファイルルールの作成。
  - エンタープライズセキュリティプロファイルルールと、コンポーネントセキュリティプロファイルルールの統合。
  - 手動および自動で実行可能なすべてのタスクアクティビティの識別と分類、手動アクティビティの廃止検討。
  - ターゲットレベルのZTA機能を実現するために必要な、セキュリティオーケストレーション、自動化、応答（SOAR）ソリューション内のベースライン統合と相互運用性の確立と実装。
  - 既存のデータタグ付けと分類標準と要件を使用した、必要に応じた機械学習ソリューション/機能の統合と実装。

5-6.　自動化とオーケストレーション②

- 手動のセキュリティおよびその他の該当するプロセスを自動化し、**エンタープライズ全体でポリシーベースのアクションを迅速かつ大規模に実行**
  - 手動および自動で実行されるすべての応答アクティビティの識別と分類。
  - ターゲットレベルのZTA機能を可能にするための、セキュリティオーケストレーション、自動化、応答（SOAR）ツールの標準要件の開発と、SOARソリューションの調達と実装。
  - 自動化とオーケストレーションのツールとソリューションの、DoDエンタープライズAPIの機械可読なパターンとプロトコルに基づいたコンプライアンスと機能の分析。
  - 承認済みパターンとプロトコルを少なくとも概説する、アプリケーションプログラミングインターフェース（API）標準（または同等の自動交換メカニズム）の確立と、既存APIの標準への更新。
  - サイバーセキュリティインシデント対応ガイダンスの確立と、脅威イベントのワークフローの有効化（内部コンテキスト、過去の脅威イベント、その他の脅威インテリジェンスの利用）。
  - 高度な脅威イベントのワークフローの開発

5-7.　可視性　と分析

- イベント、アクティビティ、振る舞いを分析してコンテキストを導き出し、AI/MLを適用してリアルタイムのアクセス決定を改善するモデルを実現
  - 監視、検出、対応の現在および将来のスケーリングニーズの分析と、コンポーネントのビジネス/ミッション考慮事項とリスク調整に沿った優先順位付け計画の作成。
  - ログおよびフローソース（ファイアウォール、EDR、Active Directory、スイッチ、ルーターなど）の識別と優先順位付け、高優先度ログの収集計画の作成、DoDエンタープライズレベルでのオープン業界標準ログ形式の合意と実装。
  - 一般的なユーザーおよびデバイスアクティビティの開発と、コンポーネントによって導き出された脅威の相関関係およびアセットIDベースの応答のためのルールの開発。
  - セキュリティ情報イベント管理（SIEM）ソリューションにおける脅威アラートの、サイバー脅威インテリジェンス（CTI）データフィードを含む形での拡張、高度な脅威を検出するための逸脱および異常ルールの開発。
  - すべてのZTピラーにわたるデータを分析するための分析ツールの機能の最小要件の開発と、分析ツールの調達と実装。
  - サイバー脅威インテリジェンス（CTI）プログラムポリシー、標準、プロセスの開発と、組織のCTIチームの設立、ZTピラー全体からの共通データフィードからのインテリジェンスの収集と、中央リポジトリ（SIEMなど）への集約。
  - CTIチームの拡張と、既存および認証済みのプライベートおよび制御された脅威インテルの分析、ZTピラー全体での適切なアクションと制御の強制。

END

3-3. 米国政府の言い出したゼロトラストの要素

M-22-09「Moving the U.S. Government Toward Zero Trust Cybersecurity Principles」

- 認証
  - 組織が管理したIDでアプリケーションにアクセスする。
  - MFAを使う
- デバイス
  - 使用するデバイスのインベントリを完全に持つ
  - インシデントに対して防止、検出、対応することができる
- ネットワーク
  - 全てのDNSクエリとHTTP通信を暗号化する
  - “マイクロセグメンテーション”を始める
- アプリケーションと運用
  - 全てのアプリケーションをインターネットに接続されているものとして扱う
  - 定期的にテストを実施する
  - 外部からの脆弱性情報を取り入れる
- データ
  - データを分類して保護する方法を明確にして共有する
  - 機密データへのアクセスを監視し、組織全体でログと情報を集約する

The 24 CFO Act Agencies

•Agency for International Development	•国際開発庁
•Department of Agriculture	•農務省
•Department of Commerce	•商務省
•Department of Defense	•国防省
•Department of Education	•教育省
•Department of Energy	•エネルギー省
•Department of Health and Human Services	•保健福祉省
•Department of Homeland Security	•国土安全保障省
•Department of Housing and Urban Development	•住宅都市開発省
•Department of the Interior	•内務省
•Department of Justice	•司法省
•Department of Labor	•労働省
•Department of State	•国務省
•Department of Transportation	•運輸省
•Department of the Treasury	•財務省
•Department of Veterans Affairs	•退役軍人省
•Environmental Protection Agency	•環境保護庁
•General Services Administration	•一般調達局
•National Aeronautics and Space Administration	•アメリカ航空宇宙局
•National Science Foundation	•アメリカ国立科学財団
•Nuclear Regulatory Commission	•原子力規制委員会
•Office of Personnel Management	•人事管理局
•Small Business Administration	•中小企業庁
•Social Security Administration	•社会保障局