



ゼロ・トラスト成熟度モデル

2023年4月

バージョン 2.0

サイバーセキュリティ・インフラセキュリティ庁

サイバーセキュリティ・ディビジョン

免責事項：本文書は TLP:CLEAR と表示されている。情報公開は制限されない。情報源は、情報が悪用されるリスクが最小限または全く予見されない場合、公開に適用される規則および手続きに従って TLP:CLEAR を使用することができる。標準著作権規則に従い、TLP:CLEAR の情報は制限なく配布することができる。トラフィック・ライト・プロトコルの詳細については、<http://www.cisa.gov/ttp/>。

改訂履歴

バージョン番号は、この文書が修正されるたびに更新される。この文書は、最新のセキュリティ対策と技術を反映するために、必要に応じて更新される。表 1 に、文書の改訂履歴を示す。

表 1 : 改訂履歴

バージョン	日付	改訂内容	影響を受けるセクション/ページ
1.0	2021 年 8 月	初回リリース	すべて
2.0	2022 年 3 月	RFC フィードバックへの対応	すべて

ゼロ・トラスト成熟度モデル

目次

1. 序文	4
2. 現在の環境.....	4
3. ゼロ・トラストとは何か？	5
4. ゼロ・トラスト導入の課題.....	6
5. ゼロ・トラスト成熟度モデル.....	7
5.1 アイデンティティ	14
5.2 デバイス	16
5.3 ネットワーク.....	21
5.4 アプリケーションとワークロード	25
5.5 データ	29
5.6 横断的な能力.....	33
6. 参考文献.....	35
7. CISA リソース	36

図表一覧

図 1:ゼロトラスト成熟度モデルの柱

図 2:ゼロトラスト成熟度ジャーニー

図 3:ゼロトラスト成熟度進化

図 4:ゼロトラスト成熟度モデルの概要表のリスト

表 1 : 改訂履歴

表 2:アイデンティティの柱

表 3:デバイスの柱

表 4:ネットワークの柱

表 5:アプリケーションとワークロード

表 6:データ

表 7:横断的な機能

1. 序文

サイバーセキュリティ・インフラセキュリティ保障局（CISA）は、連邦文民行政機関のサイバーセキュリティ・プログラムと能力の進化と運用化を支援するなど、サイバーセキュリティ・リスクを理解、マネジメント、削減するための国家の取り組みを主導している。CISA のゼロ・トラスト成熟度モデル（ZTMM）は、急速に進化する環境と技術状況の中で、ゼロ・トラストに関連する継続的な近代化努力を達成するためのアプローチを提供する。この ZTMM は、大統領令（EO）14028「国家のサイバーセキュリティ改善」§(3)(b)(ii)（¹）に従い、組織がゼロ・トラスト・アーキテクチャへの移行計画を策定・実施する際に取り得る数多くの経路の 1 つである。この計画は、各省庁がゼロ・トラスト・アーキテクチャ（ZTA）を実施する計画を策定することを求めている。ZTMM は、EO 14028 が要求する連邦政府機関向けに特別に調整されているが、すべての組織は、この文書に概説されているアプローチを検討し、採用を検討すべきである。

2. 現在の環境

最近のサイバー事件（^{2,3}）は、多くの大企業と同様、連邦政府全体で効果的なサイバーセキュリティを確保するための広範な課題を浮き彫りにし、サイバー脅威から国家を守るためには「従来通り」のアプローチではもはや不十分であることを示している。CISA は、サイバー・リスクを理解し、マネジメントし、低減するための国家的な取り組みを主導する中で、明確で実行可能な、リスク情報に基づいたアプローチを用いて連邦文民行政機関を保護するための新たな課題に対応しなければならない。新たな脅威に対する十分なサイバー防衛には、脅威行為者のコストを大幅に増加させ、完全な運用能力まで迅速に回復するための耐久性とレジリエンスを改善することによって、敵に打ち勝つスピードと敏捷性を高めることが必要である。

CISA のサイバーセキュリティの使命は、効果的な国家サイバー防衛を推進・可能にし、国家の重要機能のレジリエンスを強化し、強固な技術エコシステムを促進するための国家的取り組みを主導することにより、サイバー空間を防衛し、安全を確保することである。CISA は、FCEB 機関全体のサイバー状況認識を維持し、.gov ドメインの安全を確保し、連邦政府民間機関、重要インフラ所有者および運用者、ならびに業界パートナーを支援し、重大なサイバーインシデントを管理する上で重要な役割を果たしてい

¹ 執行 Exec. Order No.26633 (May 17, 2021). <https://www.govinfo.gov/content/pkg/FR-2021-0517/pdf/2021-10460.pdf>.

² DHS CISA. 緊急指令 21-01- SolarWinds Orion コードの危殆化の低減 <https://www.cisa.gov/emergency-directive-21-01>.

³ DHS CISA. 緊急指令 21-02 - Microsoft Exchange オンプレミス製品の脆弱性の低減 <https://www.cisa.gov/emergency-directive-21-02>.

る。CISA は既知または疑いのあるサイバー脅威を防御し、軽減する能力を維持しているが、脅威の状況は進化しており、新しい新興技術の採用が課題となっている。

EO 14028 は、連邦政府のサイバーセキュリティ近代化に対する新たなコミットメントと優先順位付けを示すものであった。EO14028 は、連邦政府に求められるセキュリティ・モデルとしてゼロトラストを掲げ、FCEB 各機関に ZTA の実施計画を策定するよう求めた。典型的な計画は、各省庁のサイバーセキュリティの現状をアセスメントし、ZTA を完全に導入するための計画を立てるものである。CISA の ZTMM は、連邦政府のサイバーセキュリティとリスク削減の主導機関として、各省庁のゼロトラスト戦略の策定と実施計画の継続的な進化を支援し、CISA の各種サービスが各省庁全体のゼロトラスト・ソリューションを支援する方法を提示している。

OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles",⁴、ZTMM に概説されている柱に沿って、連邦政府機関が採用すべき具体的な行動を詳述している。この覚書は連邦 ZTA 戦略を定め、2024 会計年度末までにサイバーセキュリティ目標を達成し、FCEB 防御を強化することを各機関に求めている。CISA は ZTMM を改訂し、M-22-09 の各省庁に対する方向性にさらに沿うようにした。FCEB 機関は、ゼロ・トラスト戦略の策定と実施と並行して、このメモを見直すべきである。

3. ゼロ・トラストとは何か？

国立標準技術研究所(NIST)特別刊行物(SP)800-207 は、ゼロトラストと ZTA の運用定義を以下のように定めている：

ゼロトラストは、ネットワークが危険にさらされているとみなされる中で、情報システムとサービスにおいて、正確で最小特権のリクエストごとのアクセス決定を実施する際の不確実性を最小化するために設計された概念とアイデアのコレクションをプロバイダに提供する。

ZTA とは、ゼロトラストの概念を用いたエンタープライズのサイバーセキュリティ計画であり、コンポーネント関係、ワークフロー計画、アクセスポリシーを包含する。

したがって、ゼロ・トラストエンタープライズとは、ZTA 計画の成果としてエンタープライズが導入するネットワークインフラ（物理および仮想）と運用ポリシーのことである。⁵

⁴OMB Memo M-22-09. ゼロトラスト・サイバーセキュリティ原則に向けて米国政府を動かす。2022 年 1 月 26 日。
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>。

⁵NIST SP 800-207: ゼロ・トラスト・アーキテクチャ。2020. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>。

SP 800-207 は、ZT の目標が「データとサービスへの不正アクセスを防止することと、アクセス管理の実施を可能な限り細かくすること」であることを強調している。同様に、国家安全保障電気通信諮問委員会（NSTAC）は、ゼロトラストについて、「いかなるユーザーや資産も暗黙のうちに信頼されることはないという考えを前提としたサイバーセキュリティ戦略」と説明している。この戦略では、情報漏洩がすでに発生しているか、今後発生することを前提としているため、エンタープライズ境界で行われる 1 回の検証によって、ユーザーに機密情報へのアクセスを許可すべきではない。その代わりに、各ユーザー、デバイス、アプリケーション、トランザクションを継続的に検証しなければならない。⁶ゼロ・トラストは、ロケーション中心モデルから、ユーザー、システム、アプリケーション、データ、資産間のきめ細かなセキュリティ制御を備えた、時間とともに変化するアイデンティティ、コンテキスト、データ中心のアプローチへの移行を意味する。このシフトは、セキュリティポリシーの開発、実装、実施、および進化をサポートするために必要な可視性を提供する。基本的に、ゼロトラストは、組織のサイバーセキュリティの哲学と文化を変える必要があるかもしれない。

ゼロ・トラストへの道は漸進的なプロセスであり、実施には何年もかかるかもしれない。

しかし、長期的には、ゼロトラストによって、エンタープライズ全体に対して「一律」のセキュリティ投資を行うのではなく、最も重要なデータやサービスに対してより慎重にセキュリティ投資を行うことができるようになる。

4. ゼロ・トラスト導入の課題

連邦政府は、多くの大企業と同様、ZTA の導入においていくつかの課題に直面している。レガシー・システムは「暗黙の信頼」に依存していることが多く、アクセスや認可が固定的な属性に基づいて評価されることはまれである。暗黙の信頼に基づいて構築された既存のインフラは、ゼロトラストの原則により合致するようにシステムを変更するための投資が必要となる。さらに、技術的な状況が進化し続ける中、新たなソリューションと、ゼロトラストの目標を達成する最善の方法に関する継続的な議論が最も重要である。

ゼロトラストの採用には、設計目標を効果的に達成し、サイバーセキュリティ態勢を改善するために、連邦政府全体のシニア・リーダーシップ、IT スタッフ、データおよびシステム所有者、ユーザーの関与と協力が必要である。連邦政府のサイバーセキュリティの近代化には、各省庁が縦割りでサイロ化された IT サービスとスタッフを、共通のアーキテクチャとガバナンス・ポリシーに全庁的な賛同を得なが

⁶大統領国家安全保障電気通信諮問委員会。Zero Trust and Identity Management に関する大統領への報告書。

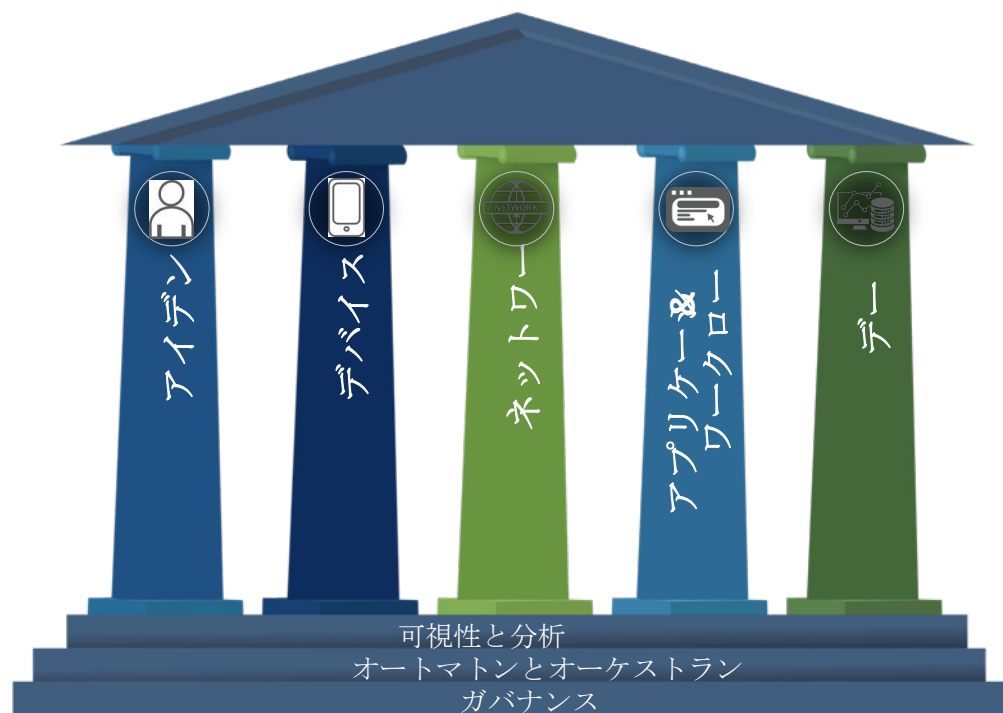
[https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero %20Trust %20and%20Trusted%20Identity%20Management.pdf](https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf)

ら、ゼロ・トラスト戦略の協調的かつ協調的なコンポーネントへと移行させることが必要である。これには、現在および将来のクラウド技術採用計画も含まれる。⁷

連邦政府機関は、さまざまな出発点からゼロトラストへの旅を始めている。しかし、出発点に関係なく、ゼロ・トラスト導入の成功は、生産性の改善、エンドユーザー・エクスペリエンスの向上、ITコストの削減、柔軟なアクセス、セキュリティの強化など、多くのメリットを生み出すことができる。

5. ゼロ・トラスト成熟度モデル

ZTMM は、5つの異なる柱にまたがる実装の勾配を表しており、最適化に向けて時間の経過とともに些細な進歩を遂げることができる。図1に示す柱には、**アイデンティティ、デバイス、ネットワーク、アプリケーションとワークロード、データ**が含まれる。各柱には、以下の横断的な機能に関する一般的な詳細が含まれている：「可視性と分析」、「自動化とオーケストレーション」、「ガバナンス」である。



⁷ 各省庁は、クラウド移行とデータ保護の推奨アプローチに関する追加ガイダンスとして、CISA、米国デジタルサービス、FedRAMP が共同で作成したクラウド・セキュリティ・テクニカル・リファレンス・アーキテクチャーを検討すべきである。[クラウド・セキュリティ・テクニカル・リファレンス・アーキテクチャ v.2 \(cisa.gov\)](https://www.cisa.gov/cloud-security-technical-reference-architecture-v2)。

図 1：ゼロ・トラスト成熟度モデルの柱⁸

CISA の ZTMM は、ゼロ・トラストへの移行をサポートする数多くの道のりのひとつである。

ZTA の様々な出版物が、この成熟度モデルの開発に影響を与えた（詳細はセクション 6 を参照）。このモデルは、NIST SP 800-207 に概説されているゼロトラストの 7 つの信条を反映している：

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みなされる。
2. すべてのコミュニケーションは、ネットワークの場所に関係なく保護されている。
3. 個々のエンタープライズ・リソースへのアクセスは、セッションごとに許可される。
4. リソースへのアクセスは動的なポリシーによって決定される。
5. エンタープライズは、所有するすべての資産と関連資産の完全性とセキュリティ状況を監視し、測定する。
6. すべてのリソースの認証と認可は動的に行われ、アクセスが許可される前に厳格に実施される。
7. エンタープライズは、資産、ネットワークインフラ、コミュニケーションの現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に活用する。

各機関が最適なゼロ・トラストの実施に向けて移行するにつれ、関連するソリューションは、柱をより完全に統合し、政策決定をより動的に実施する自動化されたプロセスやシステムにますます依存するようになる。各支柱はそれぞれのペースで前進することができ、柱を越えた調整が必要になるまで、他よりも早く前進することもある。しかし、この協調は、互いに、そしてエンタープライズ全体の環境と互換性のある能力と依存関係があって初めて達成できる。これにより、ゼロトラストへの漸進的な進化が可能になり、またそれが定義される。

NIST のゼロトラストへの移行のステップに沿って、各省庁は、ゼロトラスト機能（本モデルに概説されている柱と機能を含む）に投資する前に、現在のエンタープライズシステム、リソース、インフラ、要員、およびプロセスをアセスメントする必要がある。⁹このアセスメントは、ゼロトラストの成熟度をさらに高めるための既存の能力と、優先順位をつけるべきギャップを特定する上で、各省庁を支援するこ

⁸ この図は、米国技術評議会（ACT）および業界諮問委員会（IAC）の「Zero Trust Cybersecurity Current Trends」（2019 年）の図 1 からヒントを得たものである。

<https://www.actiac.org/system/files/ACTIAC%20Zero%20Trust%20Project%20Report%2004182019.pdf>

⁹ NIST ホワイトペーパーゼロ・トラスト・アーキテクチャの計画：A Planning Guide for Federal Administrators.

<https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final>

とができる。また、各機関は、きめ細かな最小権限アクセス管理を可能にし、さらなるリスクを軽減するために、各柱にまたがる能力を調整する機会を計画することができる。¹⁰

な出発点から、イニシャル、アドバンス、オプティマルへと進む ZTM の旅の 3 段階は、連邦政府の ZTA 実施を促進する。段階が進むごとに、より高い保護レベル、詳細さ、複雑さが要求される。

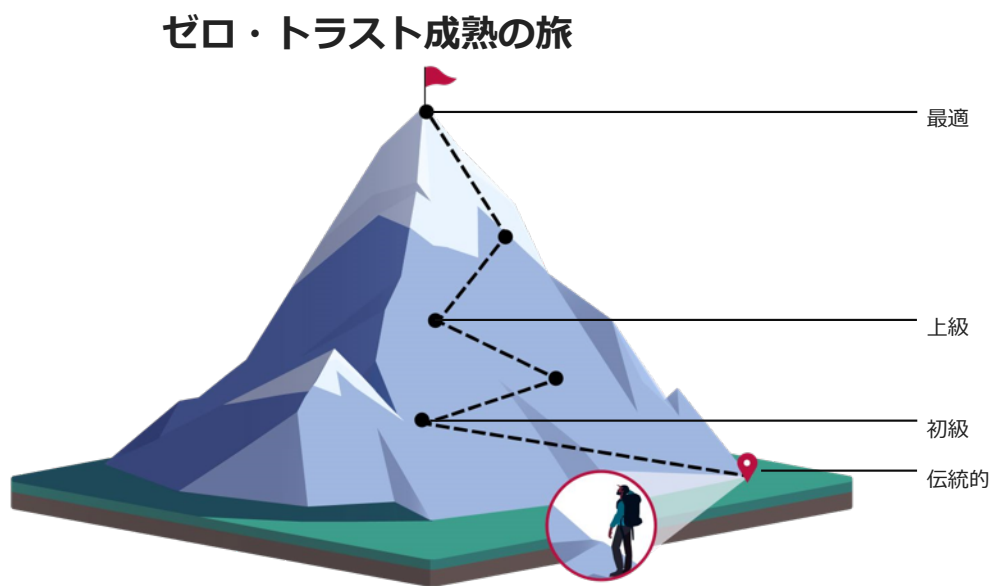


図 2 : ゼロ・トラスト・ジャーニー

図 2 に見られるように、ゼロトラストの成熟度が各柱の間で、また各柱の中で進むにつれて、必要な労力レベルと実現される利益は大幅に増加すると、各省庁は予想すべきである。各機関は、ZTA の旅程を描く中で、特定のミッションのニーズに合わせて柱の成熟度を進め、他の柱にまたがるさらなる成長を支援する機会を探るべきである。図 3 は、従来のエンタープライズから、より動的な更新、自動化されたプロセス、統合された機能、および（成熟度モデルで説明されている）最適段階のその他の特徴を特徴とする将来の状態へと、時間の経過とともに意図される省庁の進化を強調している。これらの段階は動的で指数関数的に成長する。ある成熟段階から別の成熟段階への計画的な進展は、時間の経過とともに範囲と影響が変化する可能性がある。

¹⁰ NIST SP 800-53 Revision 5 の AC-6 を参照のこと。 <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>。

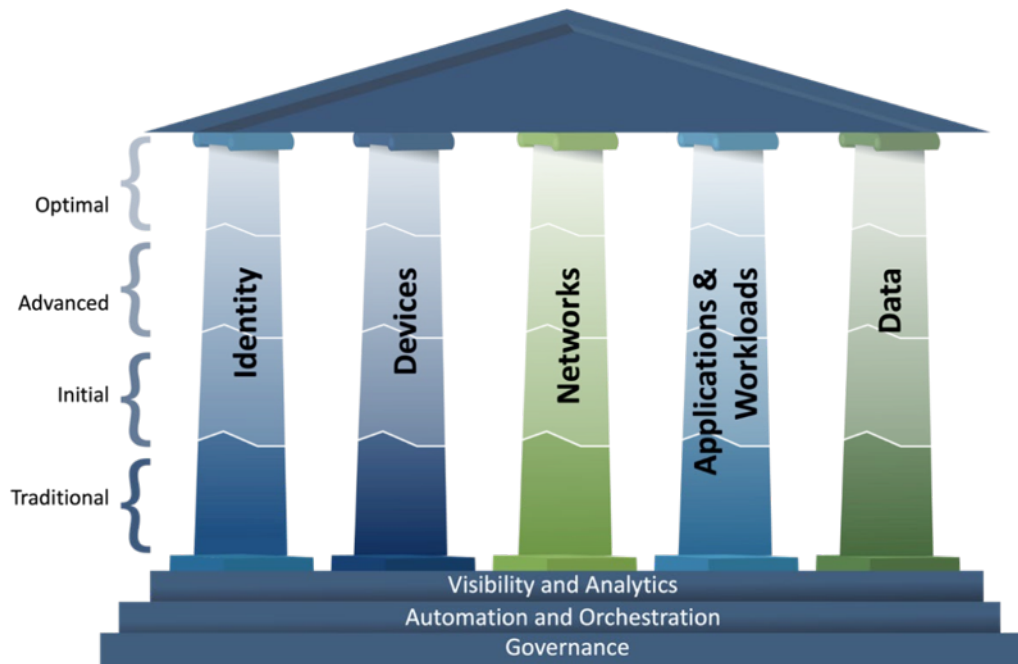


図 3 : ゼロ・トラスト成熟度の進化

各省庁は、以下の各段階の指針規準を使用して、ゼロ・トラスト・テクノロジーの各柱の成熟度を特定し、成熟度モデル全体に一貫性を持たせるべきである：

- **従来の手作業**で構成されたライフサイクル（すなわち、確立から廃止まで）と属性（セキュリティとロギング）の割り当て、外部システムに個別に依存し、一度に 1 つの柱に対処する静的なセキュリティポリシーとソリューション、プロビジョニング時にのみ確立される最小特権、ポリシー実施のサイロ化された柱、手作業による対応と低減の展開、依存関係、ログ、テレメトリの限定された相関関係。
- 属性割り当ての自動化、ライフサイクルの設定、ポリシーの決定と実施、外部システムとの統合を伴う初期的な柱をまたぐソリューション、プロビジョニング後の最小権限への若干の対応変更、内部システムの集約された可視性。
- **高度-該当する場合は**、構成とポリシーのライフサイクルと割り当ての自動制御を、支柱をまたいで連携させながら行う。
- 自動化された/観察されたトリガーに基づく動的なポリシーで自己報告する資産とリソースへの属性の**最適な、完全に自動化された**、ジャスト・イン・タイムのライフサイクルと割り当て、資産とそれぞれの依存関係に対する動的な最小権限アクセス（必要十分かつ閾値内）、継続的なモニタリングによる柱を越えた相互運用性、包括的な状況認識による一元的な可視性。

図 4 は、ZTMM のハイレベルな概要を示したもので、各柱と各成熟段階における柱固有の機能の主要な側面が含まれている。

	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	<ul style="list-style-type: none"> Continuous validation and risk analysis Enterprise-wide identity integration Tailored, as-needed automated access 	<ul style="list-style-type: none"> Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections Resource access depends on real-time device risk analytics 	<ul style="list-style-type: none"> Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience Configurations evolve to meet application profile needs Integrates best practices for cryptographic agility 	<ul style="list-style-type: none"> Applications available over public networks with continuously authorized access Protections against sophisticated attacks in all workflows Immutable workloads with security testing integrated throughout lifecycle 	<ul style="list-style-type: none"> Continuous data inventorying Automated data categorization and labeling enterprise-wide Optimized data availability DLP exfil blocking Dynamic access controls Encrypts data in use
	Visibility and Analytics		Automation and Orchestration		Governance
Advanced	<ul style="list-style-type: none"> Phishing-resistant MFA Consolidation and secure integration of identity stores Automated identity risk assessments Need/session-based access 	<ul style="list-style-type: none"> Most physical and virtual assets are tracked Enforced compliance implemented with integrated threat protections Initial resource access depends on device posture 	<ul style="list-style-type: none"> Expanded isolation and resilience mechanisms Configurations adapt based on automated risk-aware application profile assessments Encrypts applicable network traffic and manages issuance and rotation of keys 	<ul style="list-style-type: none"> Most mission critical applications available over public networks to authorized users Protections integrated in all application workflows with context-based access controls Coordinated teams for development, security, and operations 	<ul style="list-style-type: none"> Automated data inventory with tracking Consistent, tiered, targeted categorization and labeling Redundant, highly available data stores Static DLP Automated context-based access Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration		Governance
Initial	<ul style="list-style-type: none"> MFA with passwords Self-managed and hosted identity stores Manual identity risk assessments Access expires with automated review 	<ul style="list-style-type: none"> All physical assets tracked Limited device-based access control and compliance enforcement Some protections delivered via automation 	<ul style="list-style-type: none"> Initial isolation of critical workloads Network capabilities manage availability demands for more applications Dynamic configurations for some portions of the network Encrypt more traffic and formalize key management policies 	<ul style="list-style-type: none"> Some mission critical workflows have integrated protections and are accessible over public networks to authorized users Formal code deployment mechanisms through CI/CD pipelines Static and dynamic security testing prior to deployment 	<ul style="list-style-type: none"> Limited automation to inventory data and control access Begin to implement a strategy for data categorization Some highly available data stores Encrypts data in transit Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration		Governance
Traditional	<ul style="list-style-type: none"> Passwords or MFA On-premises identity stores Limited identity risk assessments Permanent access with periodic review 	<ul style="list-style-type: none"> Manually tracking device inventory Limited compliance visibility No device criteria for resource access Manual deployment of threat protections to some devices 	<ul style="list-style-type: none"> Large perimeter/macro-segmentation Limited resilience and manually managed rulesets and configurations Minimal traffic encryption with ad hoc key management 	<ul style="list-style-type: none"> Mission critical applications accessible via private networks Protections have minimal workflow integration Ad hoc development, testing, and production environments 	<ul style="list-style-type: none"> Manually inventory and categorize data On-prem data stores Static access controls Minimal encryption of data at rest and in transit with ad hoc key management
	Visibility and Analytics		Automation and Orchestration		Governance

図 4 : ハイレベル・ゼロ・トラスト成熟度モデルの概要

これらの成熟段階と各柱に関連する詳細により、機関は ZTA に向けて前進するために必要な投資をアセスメントし、計画し、維持することができる。サブセクション 0~5.5 は、5 つの異なる柱にまたがるゼロトラストへの移行を支援するためのハイレベル情報を提供する：**アイデンティティ**、**デバイス**、**ネットワーク**、**アプリケーションとワークロード**、**データ**である。各柱には、その柱とモデル全体との統合をサポートするための、可視性と分析、自動化とオーケストレーション、ガバナンス機能に関する一般的な詳細も含まれている。

これら3つの横断的能力は、以下の記述に基づき、柱を越えた機能の相互運用性をサポートする活動を強調するものである：

- **可視性と分析**：可視性とは、エンタープライズワイドな環境の特性やイベントから生じる観察可能な成果物を指す。¹¹サイバー関連のデータ分析に重点を置くことで、インシデントが発生する前に、政策決定に情報を提供し、対応活動を促進し、事前予防的なセキュリティ対策を策定するためのリスクプロファイルを構築することができる。¹²
- **自動化とオーケストレーション**：ゼロトラストは、製品やサービス全体のセキュリティ対応機能をサポートする自動化ツールとワークフローをフル活用する一方で、そのような機能、製品、サービスの開発プロセスの監視、セキュリティ、相互作用を維持する。
- **ガバナンス**：ガバナンスとは、省庁のエンタープライズをマネジメントし、ゼロトラスト原則と連邦政府要件の履行を支援するセキュリティリスクを軽減するために、省庁のサイバーセキュリティポリシー、手順、プロセスを、各柱の内部で、また各柱にまたがって定義し、実施することである。

13

ZTMM は連邦エンタープライズにとって重要なサイバーセキュリティの多くの側面をカバーしているが、インシデント対応に関連する活動、ロギング、監視、アラート、フォレンジック分析、リスク受容、リカバリなどのサイバーセキュリティの他の側面については言及していない。¹⁴エンタープライズのサイバーセキュリティ態勢管理のその他の側面やベストプラクティスは、成熟度モデルの機能には明確に含まれていない。成熟度モデルは排他的であることを意図していないが、運用技術に特有の課題、¹⁵特定のクラスのモノのインターネット（IoT）デバイス、¹⁶またはデセプション・プラットフォーム、認証されたウェブ・アプリケーション・ファイアウォール、行動分析などの新興技術を広く取り入れることには対応していない。ゼロ・トラスト・ソリューションに機械学習や人工知能の機能を最適に組み込

¹¹CISA の eVRF（extensible Visibility Reference Framework）ガイドブック (<https://www.cisa.gov/blog/2022/04/19/scuba-it-means-better-visibility-standards-and-security-practicesgovernment-cloud>) を参照のこと。

¹²各省庁は、可視化ニーズの決定と投資を行う際に、ロギング要件に関するさらなるガイダンスとして、OMB Memo M-21-31, *Improving Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (2021年8月27日) を検討すべきである。 <https://www.whitehouse.gov/wpcontent/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-RemediationCapabilities-Related-to-Cybersecurity-Incidents.pdf>.

¹³ NIST サイバーセキュリティフレームワーク Version 1.1 の識別カテゴリのガバナンス機能 (<https://www.nist.gov/cyberframework/framework>) に基づいている。

¹⁴ バックアップはデータの柱に含まれるが、データの完全性と復旧に関する詳細なガイダンスについては、省庁は NIST SP 1800-11: <https://csrc.nist.gov/News/2020/sp-1800-11-data-integrity-ransomware-recovery> を参照すべきである。

¹⁵ NIST.運用技術セキュリティの手引き：NIST は SP 800-82r3 ドラフトに対する意見を要求する。
<https://csrc.nist.gov/News/2022/guide-to-operational-technology-ot-security>.

¹⁶ NIST.IoT プログラムのサイバーセキュリティ <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iotprogram>.

むための推奨事項などの方法論は、このモデルには含まれない。成熟したアセスメント機関は、各柱の成熟に伴い、不正アクセスや変更を検知するために、セキュリティ機能、基盤インフラ、ポリシーのパフォーマンスと完全性を監視・評価するための措置を講じるべきである。機関は、悪用の新たな機会を作り出したり、セキュリティ・プロトコルを弱めたりしないよう注意すべきである。連邦エンタープライズ全体のスケールでソフトウェアとハードウェア・システムの完全性を効果的に保証するためには、研究開発が必要である。^{17,18,19}

ZTA の導入を計画する際、機関はリスク、ミッション、連邦政府の要件、および運営上の制約を含む要因に基づいて決定を下すべきである。このモデルは、一般に連邦エンタープライズの単一管理領域または認定境界と整合しているが、省庁は、外部パートナー、利害関係者、サービスプロバイダーとの相互作用や依存が、ZTA にどのように影響するかもアセスメントすべきである。²⁰この成熟度モデルは、厳格な要件セットとしてではなく、各省庁が ZTA を成功裏に実施し、全体的に改善されたサイバーセキュリティ態勢を採用するための一般的なガイドとして捉えるべきである。

¹⁷ NIST NCCOE: Supply Chain Assurance. <https://www.nccoe.nist.gov/supply-chain-assurance>.

¹⁸ <https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices>. NIST NCCOE: Software Supply Chain and DevOps Security Practices.

¹⁹ 各機関は、ソフトウェア部品表 (SBOM) および脆弱性悪用可能性交換 (VEX) に関して利用可能な情報およびリソースを、コミュニティの進歩に伴い、<https://www.cisa.gov/sbom>。

²⁰ これらの考慮事項は、信用証明書の信頼、サプライチェーンのアセスメント、データ分類の違い、ポリシーの例外、リスク閾値のパリエーションなど、柱や機能にまたがる。

5.1 アイデンティティ

ID とは、非個人事業体を含め、機関の利用者または事業体を一意に記述する属性または属性 セットを指す。

機関は、過剰なアクセスを許可することなく、適切な目的のために適切なときに適切なリソースへのユーザおよび事業体のアクセスを確保し、実施する必要がある。省庁は、エンタープライズ全体で可能な限り ID、クレデンシャル、およびアクセス管理ソリューションを統合して、強力な認証を実施し、状況に応じた認可を与え、省庁のユーザおよび事業体の ID リスクを評価する。省庁は、必要に応じて ID ストアおよび管理システムを統合して、エンタープライズ ID と、それらに関連する責任および権限の認識を強化する。

表 2 に、信頼ゼロに関連する ID 機能と、ID のコンテキストにおける「可視性と分析」、「自動化とオーケストレーション」、および「ガバナンス」の考慮事項を示す。

表 2: アイデンティティの柱

機能	伝統的	初級	上級	最適
認証	事業体は、事業体 ID 用の静的アクセスで、パスワードまたは多要素認証 ²¹ (MFA) の	事業体は、MFA を使用して ID を認証する。MFA は、1 つの要素としてパスワード	代理店が動き始める FIDO2 ²² または PIV ²³ を介したパスワードレス MFA の	省庁は、アクセスが最初に許可されたときだけでなく、フィッシング耐性のある MFA

²¹ MFA 向けの CISA リソースは <https://www.cisa.gov/mfa>。

²²FIDO2 は、FIDO (Fast IDentity Online) アライアンスと W3C (World Wide Web Consortium) が共同で開発したプロトコルのセットである。FIDO2 は、簡単で安全なパスワードレス認証を可能にするように設計されている。このアプローチは、W3C の WebAuthn プロトコルと FIDO アライアンスの CTAP (Client to Authenticator Protocol) プロトコルを活用している。

FIDO アライアンス。FIDO アライアンス - パスワードよりも安全なオープン認証標準 <https://fidoalliance.org/>。

ワールド・ワイド・ウェブ・コンソーシアム Web 認証：公開鍵認証情報にアクセスするための API。 <https://www.w3.org/TR/2021/REC-webauthn-2-20210408/>。

FIDO アライアンス。Client to Authenticator Protocol. 標準提案、2021 年 6 月。 <https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-toauthenticator-protocol-v2.1-ps-errata-20220621.html>。

²³個人 ID 検証。PIV クレデンシャルは、連邦政府が管理する施設および情報システムに適切なセキュリティ・レベルでアクセスするために使用される、米国連邦政府全体のクレデンシャルである。 <https://playbooks.idmanagement.gov/piv/>。

機能	伝統的	初級	上級	最適
	いずれかを使用して ID を認証する。	ドを含む場合があり、複数の事業体属性（ロケールやアクティビティなど）の検証を必要とする。	初期実装を含め、フィッシング耐性のある MFA および属性を使用してすべての ID を認証する。	を使用して継続的に ID を検証する。
アイデンティティ・ストア	省庁は、自己管理されたオンプレミス（すなわち、省庁によって計画、導入、保守された）ID ストアのみを使用する。	省庁は、自己管理 ID ストアとホストされた ID ストア（クラウドまたは他の省庁など）の組み合わせを持っており、ストア間の統合は最小限である（シングルサインオンなど）。	省庁は、自己管理およびホストされた ID ストアの安全な統合と統合を開始する。	省庁は、必要に応じて、すべてのパートナーおよび環境に ID ストアを安全に統合する。
リスクアセスメント	当機関は、ID リスク（すなわち、ID が侵害される可能性）について限定的な判断を行う。	省庁は、可視性をサポートするために、手作業の方法と静的ルールを使用して ID リスクを決定する。	省庁は、アクセス決定および対応活動に情報を提供するために、いくつかの自動分析および動的ルールを使用して ID リスクを決定する。	Agency は、継続的な分析と動的なルールに基づいてアイデンティティ・リスクをリアルタイムで判断し、継続的な保護を提供する。
アクセス管理（新機能）	省庁は、特権アカウントと非特権アカウントの両方について、定期的なレビューを伴う永続的なアクセスを認可する。	省庁は、特権付きアクセス要求も含め、自動レビューで失効するアクセスを認可する。	弊庁は、特権アクセス要求を含め、アクションおよびリソースに合わせた、必要性に応じたセッション・ベースのアクセスを認可する。	省庁は自動化を利用して、個々の行動や個々のリソースのニーズに合わせた、ジャスト・イン・タイムで必要十分なアクセスを認可する。
可視性と分析能力	省庁は、ユーザーと事業体の活動ログ、特に特権クレデン	機関は、ユーザーと事業体の活動ログを収集し、日常	事業体は、一部のユーザーと事業体のアクティビティログ	省庁は、行動ベースの分析を含む、ユーザー・アクティビ

機能	伝統的	初級	上級	最適
	シャルを収集し、いくつかの定型的な手動分析を行う。	的な手動分析と一部の自動分析を行っているが、ログの種類間の相関は限定的である。	のタイプにわたって自動分析を実行し、可視性のギャップに対処するために収集を強化する。	ティ・ログ・タイプの自動分析を実行することにより、エンタープライズ全体の包括的な可視性と状況認識を維持する。
自動化とオーケストレーション能力	省庁は、ほとんど統合されることなく、自己管理アイデンティティ（ユーザと事業体）を手動でオーケストレーション（オンボード、オフボード、および無効化）し、定期的なレビューを行う。	省庁は、特権ユーザおよび外部 ID のオーケストレーションを手動で行い、非特権ユーザおよび自己管理事業体のオーケストレーションを自動化する。	省庁は、特権ユーザー・アイデンティティのオーケストレーションを手動で行い、すべての環境にわたって統合されたすべてのアイデンティティのオーケストレーションを自動化する。	省庁が自動化行動、登録、配備の必要性に基づいて、すべての環境を完全に統合し、すべてのアイデンティティをオーケストレーションする。
ガバナンス能力	ID ポリシー（認証、クレデンシャル、アクセス、ライフサイクルなど）は、静的な技術メカニズムおよび手動レビューによって実施される。	最小限の自動化と手作業による更新で、エンタープライズ全体に適用される ID ポリシーを定義し、実装を開始する。	エンタープライズは、自動化されたアイデンティティポリシーを導入し、エンタープライズ全体で実施する。そして定期的に方針を更新する。	継続的な実施と動的な更新により、すべてのシステムにわたるすべてのユーザと事業体に対して、全社的な ID ポリシーを導入し、完全に自動化する。

5.2 デバイス

デバイスとは、サーバー、デスクトップ機、ラップトップ機、プリンター、携帯電話、IoT デバイス、ネットワーク機器など、ネットワークに接続できるあらゆる資産（ハードウェア、ソフトウェア、ファームウェアなどを含む）を指す。

デバイスは、機関が所有する場合もあれば、職員、パートナー、または訪問者の所有物である BYOD (Bring-your-Own-Device) の場合もある。省庁は、すべての省庁・デバイスを保護し、省庁が制御していない認可デバイスのリスクを管理し、認可されていないデバイスによるリソースへのアクセスを防止する必要がある。デバイス管理には、ハードウェア、ソフトウェア、ファームウェアなど、すべての資産の動的インベントリを、構成や関連する脆弱性が判明した場合とともに維持することが含まれる。

多くの機器は、ZTA に特有の課題があり、リスク・ベース・プロセスの一環として、ケース・バイ・ケースで評価しなければならない。例えば、ネットワーク機器、プリンタなどは、認証、可視性、およびセキュリティのためのオプションが限られている場合がある。BYOD ポリシーを採用する機関は、そのようなデバイスの可視性と管理を維持するためのオプションが少なくなる可能性が高い。デバイスの技術的状況は変化し続けており、エンタープライズに新たなデバイスが組み込まれるにつれて、これらのデバイスに関連する進化するリスクを管理し続ける必要がある。²⁴場合によっては、機関は、デバイスの特定のサブセットについて、ガイダンスを採用することができないかもしれない。また、レガシーデバイスには、未修正の脆弱性、利用可能な設定ミス、未知のリスクが多く存在することが多いため、信頼できるデバイスとそのサービスが耐用年数に達しておらず、ライフタイムサポートの対象であることを確認する上で、機関は課題に直面するだろう。しかし、このような課題にもかかわらず、各機関は ZTA に向けてかなりの前進を遂げることができるはずである。

オンプレミス・コンピューティングの資産管理では、物理資産（デバイス）の文書化と管理が行われる。機関がクラウド環境に移行するにつれて、機関のクラウド資産と仮想資産を管理・追跡するための新たな検討事項と機会が生まれる。クラウド資産には、コンピュート・リソース（仮想マシン、サーバー、コンテナなど）、ストレージ・リソース（ブロック・ストレージ、ファイル・ストレージなど）、プラットフォーム資産（データベース、ウェブ・サーバー、メッセージ・バス/キューなど）、ネットワーク・リソース（仮想ネットワーク、VPN、ゲートウェイ、DNS サービスなど）、および他の管理クラウド・サービス（人工知能モデルなど）に関連する仮想リソースが含まれる。

表 3 は、ゼロトラストに関連するデバイスの機能、およびデバイスのコンテキストにおける可視化と分析、自動化とオーケストレーション、ガバナンスに関する考慮事項を示している。

²⁴ 各省庁は OMB Memo M-22-01 *Improving Detection of Cybersecurity Vulnerabilities and Incident on Federal Government Systems through Endpoint Detection and Response* を参照すべきである。 <https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf>。

表3：デバイスの柱

機能	伝統的	初級	上級	最適
ポリシーの実施とコンプライアンスの監視（新機能）	デバイスのコンプライアンスに関する可視性（デバイスの動作を検査する能力）は、あったとしても限られており、ポリシーを実施したり、ソフトウェア、構成、脆弱性を管理する方法はほとんどない。	省庁は、自己報告されたデバイスの特性（デバイス上の鍵、トークン、ユーザなど）を受け取るが、実施メカニズムは限られている。省庁は、ソフトウェアの使用を承認し、更新および構成変更をデバイスにプッシュするための予備的な基本プロセスを備えている。	省庁は、デバイスへの初級アクセス時に検証されたインサイト（つまり、管理者がデバイス上のデータを検査し検証できる）を持っており、ほとんどのデバイスと仮想資産に対してコンプライアンスを実施している。資産管理機関は、自動化された方法を使用して、デバイスと仮想資産の管理、ソフトウェアの承認、脆弱性の識別とパッチのインストールを行っている。	デバイスと仮想資産のライフタイムを通じて、インサイトを継続的に検証し、コンプライアンスを実施する。省庁は、仮想資産を含むすべての省庁環境にわたって、デバイス、ソフトウェア、構成、および脆弱性管理を統合する。
アセット&サプライチェーンリスクマネジメント（新機能）	資産管理機関は、エンタープライズ全体またはベンダー横断的な方法で物理的または仮想的な資産を追跡しておらず、エンタープライズリスクを限定的な視野で、デバイスやサービスの独自のサプライ	省庁は、すべての物理資産と一部の仮想資産を追跡し、強固なフレームワーク（例：NIST SCRM）を使用して、連邦政府の勧告に従ったポリシーとコントロール・ベースラインを確立することにより、サプライチェーンリスクを管理している。 ²⁵	アセスメント機能は、複数のベンダーにまたがって機能する自動化されたプロセスを通じて、物理的および仮想的な資産の包括的なエンタープライズビューの開発を開始し、取得の検証、開発サイクルの	資産管理機関は、ベンダーやプロバイダを問わず、すべての資産を包括的かつリアルタイムに近い形で把握し、サプライチェーン・リスクマネジメントを必要に応じて自動化し、サプライチェーンの障害を許容するオペレーションを

²⁵ NIST NIST はサプライチェーンリスクマネジメントのためのサイバーセキュリティガイダンスを更新した。 <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>.

機能	伝統的	初級	上級	最適
	チェーンマネジメントを場当たり的に行っている。		追跡、サードパーティ評価の提供を行う。	構築し、ベストプラクティスを取り入れている。
リソース・アクセス（旧データ・アクセス）	省庁は、リソースへのアクセスに使用されるデバイスや仮想資産に対する可視性を必要としない。	省庁は、一部のデバイスまたは仮想資産に特性の報告を求め、この情報を使用してリソースへのアクセスを承認する。	省庁の最初のリソース・アクセスは、検証されたデバイスまたは仮想アセットのインサイトを考慮する。	省庁のリソース・アクセスは、デバイスや仮想資産内のリアルタイムのリスク分析を考慮する。
デバイス脅威防御（新機能）	省庁は、一部のデバイスに脅威防御機能を手動で配備している。	省庁は、デバイスや仮想資産への脅威防御機能の配備と更新のための自動化されたプロセスをいくつか有しているが、ポリシーの実施とコンプライアンス監視の統合は限定的である。	省庁は、脅威防御機能をデバイスと仮想資産用の集中型ソリューションに統合し始め、これらの機能のほとんどをポリシー実施とコンプライアンス監視に統合している。	すべてのデバイスと仮想資産に対応する高度な機能を備え、デバイスの脅威保護、ポリシー実施、コンプライアンス監視のための統一的なアプローチを導入した、一元化された脅威保護セキュリティソリューションがある。
可視性と分析能力	分析機関では、物理的にラベルの制限されたインベントリおよびソフトウェア監視を使用して、定期的にデバイスを確認し、若干の手作業による分析を行っている。	省庁は、利用可能な場合、デバイスの手動インベントリおよびエンドポイントの監視と併せて、デジタル識別子（インタフェース・アドレス、デジタル・タグなど）を使用する。一部の省庁のデバイスおよび仮想資産は、リスクに基づく異常検知のための自動分析（ソフトウェア	Agency は、インベントリ収集（デスクトップ、ラップトップ、携帯電話、タブレット、およびそれらの仮想資産など、すべての標準ユーザー・デバイスのエンドポイント監視を含む）と、不正なデバイスを検出するための異常検知の両方を自動化する。	ネットワークに接続されたすべてのデバイスと仮想資産のステータス収集を自動化し、アイデンティティとの関連付け、エンドポイント監視の実施、リソース・アクセスを通知する異常検知を行う。仮想資産のプロビジョニングおよび/またはデプロビジョニ

機能	伝統的	初級	上級	最適
		ア・ベースのスキャンなど) の対象となっている。		ングのパターンを追跡し、異常を検出する。
自動化とオーケストレーション能力	エンタープライズ内のデバイスを手動でプロビジョニング、構成、および/または登録する。	省庁は、デバイスおよび仮想資産のプロビジョニング、構成、登録、および/またはデプロビジョニングのプロセスを自動化するためのツールおよびスクリプトの使用を開始する。	弊庁は、非準拠（脆弱性、検証されていない証明書、未登録の mac アドレス）のデバイスおよび仮想資産を特定し、手動で切断または隔離するための監視および実施メカニズムを実装している。	省庁は、デバイスと仮想資産のプロビジョニング、登録、監視、分離、修復、およびデプロビジョニングのためのプロセスを完全に自動化している。
ガバナンス能力	省庁は、従来型および周辺コンピューティングデバイスのライフサイクル ⁽²⁶⁾ について、いくつかのポリシーを設定し、これらのデバイスの保守（更新、パッチ、消毒など）を手動プロセスに依存している。	弊庁は、新しいデバイスの調達、非従来型コンピューティング・デバイスと仮想資産のライフサイクル、およびデバイスの監視とスキャンを定期的実施するためのポリシーを設定し、実施する。	エンタープライズ・省庁は、デバイスと仮想資産のライフサイクルについて、その列挙と説明責任を含むエンタープライズ全体のポリシーを設定し、自動化された実施メカニズムをいくつか備えている。	省庁は、エンタープライズ全体のすべてのネットワーク接続デバイスと仮想資産のライフサイクルのポリシーを自動化する。

²⁶ ライフサイクルには、デバイスの調達、設定、追跡、監視、更新、使用、サニタイジング、デプロビジョニング、リカバリーが含まれる。

5.3 ネットワーク

ネットワークとは、代理店内ネットワーク、ワイヤレスネットワーク、インターネットなどの典型的なチャンネルに加え、メッセージ伝送に使われるセルラーチャンネルやアプリケーションレベルチャンネルなど、その他の潜在的なチャンネルを含むオープンなコミュニケーション媒体を指す。

ZTA は、従来の境界重視のセキュリティ・アプローチからの移行を可能にし、内外部のトラフィック・フローの管理、ホストの分離、暗号化の実施、アクティビティのセグメント化、エンタープライズ全体のネットワーク可視性の強化を可能にする。ZTA は、アプリケーション、データ、その他のリソースにより近い場所でセキュリティ制御を実施することを可能にし、従来のネットワークベースの防御を強化し、防御の奥行きを改善する。各アプリケーションは、アクセス、優先度、到達可能性、依存サービスへの接続、接続経路に対する要求について、ネットワークによって独自に扱われる。これらのネットワーク・アプリケーションの要求はアプリケーション・プロファイルとして捕捉することができ、プロファイルを繰り返すことでトラフィック・クラスとして扱うことができる。

表 4 は、ゼロトラストに関連するネットワーク機能と、ネットワークのコンテキストにおける「可視化と分析」、「自動化とオーケストレーション」、「ガバナンス」の考慮事項を示している。

表 4：ネットワークの柱

機能	伝統的	初級	上級	最適
ネットワーク・セグメンテーション	省庁は、ネットワーク・セグメント内の到達可能性を最小限に制限する大規模な境界／マクロセグメンテーションを使用して、ネットワーク・アーキテクチャを定義する。また、マルチサービス相互接続（バルク・トラフィック VPN トンネルなど）に依存する場合もある。	省庁は、ネットワーク・アーキテクチャの導入を開始した。 クリティカルなワークロードの分離、最小機能原則に基づく接続の制約、サービス固有の相互接続への移行。	省庁は、インGRESS/エグレスのマイクロ・ペリメーターとサービス固有の相互接続により、エンドポイントおよびアプリケーション・プロファイルの分離メカニズムの展開を、ネットワーク・アーキテクチャのより多くの部分に拡大する。	省庁のネットワーク・アーキテクチャは、完全に分散されたインGRESS/エグレスのマイクロ・ペリメーターと、動的なジャスト・イン・タイムとジャスト・イン・ファウル接続性を備えたアプリケーション・プロファイルに基づく広範なマイクロ・セグメン

機能	伝統的	初級	上級	最適
				テーションで構成されている。 サービス固有の相互接続のためである。
ネットワーク・トラフィック・マネジメント (新機能)	アプリケーション・パフォーマンス監視や異常検知などの監視機能は限定的であり、ミッション・クリティカルなアプリケーションのプロファイル変更の監査とレビューは手動で行われる。	省庁は、明確なトラフィック管理機能を持つアプリケーション・プロファイルを確立し、すべてのアプリケーションをこれらのプロファイルにマッピングし始める。静的ルール適用をすべてのアプリケーションに拡大し、アプリケーションプロファイルアセスメントの定期的な手動監査を実施する。	アセスメント・省庁は、リソースを最適化するための動的なネットワーク・ルールと構成を実装している。このルールは、自動化されたリスク対応アプリケーション・プロファイルの評価と監視に基づいて定期的に適応される。	省庁は、アプリケーション・プロファイルのニーズを満たし、ミッションの重要性、リスクなどに基づいてアプリケーションを再優先するために、継続的に進化する動的なネットワーク・ルールと構成を実装する。
トラフィックの暗号化 (旧暗号化)	省庁は最小限のトラフィックを暗号化し、暗号化キーの管理と安全性を確保するために手動またはアドホックなプロセスに依存している。	内部アプリケーションへのトラフィックはすべて暗号化し、外部アプリケーションへのトラフィックは暗号化する。 ²⁷ 鍵管理ポリシーを正	省庁は、該当するすべての内部および外部トラフィックプロトコルの暗号化を確保し、 ²⁸ 鍵と証明書の発行とローテーションを管理し、暗号の俊敏性のためのベストプラク	省庁は、適切なトラフィックの暗号化を継続し、安全な鍵管理のための最小特権原則を全社的に実施し、暗号の俊敏性のためのベスト・プラクテ

²⁷ 例えば、HTTP と HTTPS の両方のオプションが利用可能な場合、ポリシーと設定は HTTPS を優先する。

²⁸ ゼロ・トラスト導入の一環として、検査や可視化の必要性からネットワーク・トラフィックを暗号化および復号化する（またはしない）ことに関して、各機関が検討すべきさまざまなリソースがある：OMB M-15-13、M-19-26、M-22-09、DHS 拘束的運用指令 18-01、NIST SP 800-207 などである。<https://www.cisa.gov/uscert/ncas/alerts/TA17-075A>。

機能	伝統的	初級	上級	最適
		式化し、サーバ/サービスの暗号鍵を保護する。	ディスクの組み込みを開始する。 ²⁹	ディスクを可能な限り広く取り入れる。
ネットワーク・レジリエンス (新機能)	CIA は、ミッションクリティカルとみなされないワークロードに対しては、限られたレジリエンスメカニズムで、個々のアプリケーションの可用性要求にのみ合致するように、ケースバイケースでネットワーク機能を構成している。	追加アプリケーションの可用性要求を管理し、ミッションクリティカルとみなされないワークロードのレジリエンスメカニズムを拡張するために、省庁はネットワーク機能の構成を開始する。	省庁は、大半のアプリケーションの可用性要求とレジリエンス・メカニズムを動的に管理するネットワーク機能を構成している。	省庁は、すべてのワークロードに対する可用性要求の変化に適応するために、総合的なデリバリーと認識を統合し、相応のレジリエンスを提供する。
可視性と分析能力	同局は、集中的な状況認識の開発を開始するために、最小限の分析で限定的な境界に焦点を当てたネットワーク監視機能を組み込んでいる。	ネットワーク・エナメレーションを含む) 侵害の既知の指標に基づくネットワーク監視機能を採用し、各環境における状況認識を向上させ、分析と脅威ハンティング活動のために、トラフィックの種類と環境を横断した遠隔測定に関連付けを開始する。	異常ベースのネットワーク検知機能を配備し、あらゆる環境における状況認識を高め、分析のために複数のソースからのテレメトリの関連付けを開始し、強固な脅威ハンティング活動のために自動化されたプロセスを組み込んでいる。	エンタープライズ・ワイドの状況認識と、すべての検知ソースにわたるテレメトリ相関を自動化する高度なモニタリング機能を実現しながら、省庁はすべての省庁のネットワークと環境にわたるコミュニケーションの可視性を維持する。
自動化とオーケストレーション能力	省庁は、ポリシー要件と状況認識を定期的に統合しながら	省庁は、一部の省庁のネットワークまたは環境の構成と	省庁は、自動化された変更管理手法 (CI/CD	省庁のネットワークと環境は、自動化された変更管理手

²⁹ DHS 暗号敏捷性インフォグラフィック。 <https://www.dhs.gov/publication/cryptographic-agility-infographic>.

機能	伝統的	初級	上級	最適
	ら、省庁のネットワークと環境の構成とリソースのライフサイクルを管理するために、手動プロセスを使用している。	ソースのライフサイクルを管理するために、自動化された方法の使用を開始し、すべてのリソースがポリシーと遠隔測定に基づいて定義された寿命を持つことを保証する。	など) を使用して、すべての省庁のネットワークおよび環境の構成およびリソースのライフサイクルを管理し、認識されたリスクに対応し、ポリシーおよび防御を実施する。	法によって管理される infrastructure-as-code を使用して定義される。
ガバナンス能力	省庁は、境界の防御に重点を置いたアプローチで、静的なネットワーク・ポリシー（アクセス、プロトコル、セグメンテーション、アラート、修復）を導入している。	省庁は、全社的なルールを適宜継承しながら、個々のネットワークセグメントやリソースに合わせたポリシーを定義し、実施し始める。	省庁は、カスタマイズされたポリシーの実施に自動化を取り入れ、境界線に重点を置いた防御から移行を促進する。	省庁は、アプリケーションとユーザーのワークフローに基づいて、カスタマイズされたローカル制御、動的な更新、安全な外部接続を可能にするエンタープライズ規模のネットワークポリシーを実施する。

5.4 アプリケーションとワークロード

アプリケーションとワークロードには、オンプレミス、モバイルデバイス、クラウド環境で実行される機能システム、コンピュータプログラム、サービスが含まれる。

各機能は、配備されたアプリケーションを管理し、安全なアプリケーション配信を確保すべきである。きめ細かいアクセス管理と統合された防御により、状況認識を強化し、アプリケーション固有の脅威を軽減することができる。OMB M-22-09 に従い、当局は、認可されたユーザがパブリック・ネットワーク上でアプリケーションを利用できるようにする機会を模索し始めるべきである。また、DevSecOps および CI/CD プロセスのベストプラクティス（不変のワークロードの使用を含む）を可能な限り採用すべきである。^{30,31}各機能は、認定境界と ATO の更新に重点を置いた運用から、あたかも外部に向けたアプリケーションをサポートし、それに見合ったセキュリティを提供する運用に移行するための選択肢を探るべきである。

表 5 は、ゼロトラストに関連するアプリケーションワークロード機能、およびアプリケーションとワークロードのコンテキストにおける「可視性と分析」、「自動化とオーケストレーション」、「ガバナンス」に関する考慮事項を示している。

表 5: アプリケーションとワークロード

機能	伝統的	初級	上級	最適
アプリケーション・アクセス (旧アクセス認可)	省庁は、主にローカル認可と静的属性に基づいてアプリケーションへのアクセスを認可する。	省庁は、有効期限付きの要求ごとに、コンテキスト情報（ID、デバイスのコンプライアンス、および/またはその他の属性など）を組み込んだアプリケーションへのアク	省庁は、拡張されたコンテキスト情報と、最小特権原則に従った強制的な有効期限条件により、アプリケーションのアクセス決定を自動化する。	省庁は、リアルタイムのリスク分析および行動や使用パターンなどの要因を組み込んで、アプリケーション・アクセスを継続的に認可する。

³⁰ NIST プロジェクト : <https://csrc.nist.gov/Projects/devsecops#plans>.

³¹ NIST SP 800-204C: Service Mesh によるマイクロサービスベースのアプリケーションのための DevSecOps の実装。2022 年 3 月 8 日。
<https://csrc.nist.gov/publications/detail/sp/800-204c/final>.

機能	伝統的	初級	上級	最適
		セス認可機能の実装を開始する。		
アプリケーション防御（旧スレット防御）	省庁の脅威防御は、アプリケーションのワークフローとの統合は最小限であり、既知の脅威に対して汎用的な防御を適用している。	省庁は、脅威防御をミッションクリティカルなアプリケーションのワークフローに統合し、既知の脅威と一部のアプリケーション固有の脅威に対する防御を適用する。	省庁は、脅威防御をすべてのアプリケーションのワークフローに統合し、一部のアプリケーション固有の脅威や標的型脅威から保護する。	Agency は、すべてのアプリケーション・ワークフローに高度な脅威防御を統合し、アプリケーションに合わせた高度な攻撃に対するリアルタイムの可視化とコンテンツ認識による防御を提供する。
アクセシブル・アプリケーション（旧アクセシビリティ）	省庁は、一部のミッションクリティカルなアプリケーションを ³² プライベートネットワークと保護されたパブリックネットワーク接続でのみ利用可能にする。 (VPN など) を監視する。	CIA は、必要な認可ユーザーに対し、ブローカー接続を介して、オープンなパブリック・ネットワーク上でミッション・クリティカルなアプリケーションの一部を利用できるようにしている。	認可されたユーザーが必要に応じて、オープンなパブリック・ネットワーク接続を介して、該当するミッション・クリティカル・アプリケーションのほとんどを利用できるようにしている。	弊庁は、必要に応じて、認可されたユーザーおよび機器に対して、オープンな公共ネットワーク上ですべての該当するアプリケーションを利用できるようにする。
セキュアなアプリケーション開発と展開のワークフロー（新機能）	諜報機関には、堅牢でないコード展開メカニズムを備えた、その場限りの開発、テスト、本番環境がある。	CI/CD パイプラインによる正式なコード・デプロイメント・メカニズムと、最小特権原則をサポートする必要なアクセス制御を備えた、開発、	開発、セキュリティ、運用の各分野で、それぞれ独立したチームを編成し、開発者が本番環境にアクセスできないようにする。	省庁は、可能な限り不変のワークロードを活用し、再デプロイメントによってのみ変更が有効になるようにし、デプロイメント環境への管理者ア

³² これには国家安全保障システムは含まれない。National Security Memorandum (NSM)-8 "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-onimproving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/> を参照のこと。

機能	伝統的	初級	上級	最適
		テスト、本番環境（自動化を含む）のためのインフラストラクチャをプロバイダとして提供する。		クセスを削除して、コードデプロイメントの自動化プロセスを採用する。
アプリケーション・セキュリティ・テスト（旧アプリケーション・セキュリティ）	省庁は、主に手動テスト手法により、配備前にアプリケーション・セキュリティ・テストを実施する。	アプリケーションの配備に先立ち、手作業による専門家の分析を含むセキュリティテストを実施するために、静的テスト手法と動的テスト手法（すなわち、アプリケーションが実行中であること）の使用を開始する。	当機関は、定期的な動的テスト手法の使用など、アプリケーションの開発・展開プロセスにアプリケーション・セキュリティ・テストを統合している。	省庁は、エンタープライズ全体のソフトウェア開発ライフサイクル全体を通じて、配備済みアプリケーションの定期的な自動テストによってアプリケーション・セキュリティ・テストを統合している。
可視性と分析能力	省庁は、限定的な集計と分析で、ミッションクリティカルなアプリケーションのパフォーマンスとセキュリティをある程度監視している。	アプリケーションのプロファイル（状態、健全性、パフォーマンスなど）とセキュリティ監視の自動化を開始し、ログ収集、集計、分析を改善する。	識別は、ほとんどのアプリケーションのプロファイルとセキュリティの監視を自動化し、ヒューリスティックによってアプリケーション固有およびエンタープライズ全体の傾向を識別し、可視性のギャップに対処するために時間をかけてプロセスを改善する。	省庁は、エンタープライズ全体の包括的な可視性を維持するために、すべてのアプリケーションにわたって継続的かつ動的な監視を実行する。
自動化とオーケストレーション能力	省庁は、保守とレビューの制限付きで、プロビジョニング時に静的なアプリケーション	弊庁は、関連するセキュリティおよびパフォーマンス目標を満たすために、アプリケーション構成（場所およびア	省庁は、運用や環境の変化に対応するために、アプリケーションの設定を自動化する。	省庁は、セキュリティとパフォーマンスを継続的に最適化するために、アプリケーション構成を自動化する。

機能	伝統的	初級	上級	最適
	ホスティングの場所とアクセスを手動で確立する。	クセスを含む) を定期的に変更する。		
ガバナンス能力	アプリケーションへのアクセス、開発、配備、ソフトウェア資産管理、技術導入時のセキュリティテストと評価 (ST&E)、パッチ適用、ソフトウェアの依存関係の追跡は、主に手動の実施方針に頼っている。	アプリケーション開発 (開発インフラへのアクセスを含む)、展開、ソフトウェア資産管理、技術導入時の ST&E、パッチ適用、および (例えばソフトウェア部品表による) ミッションのニーズに基づくソフトウェアの依存関係の追跡のためのポリシー施行の自動化を開始する。	省庁は、アプリケーションと、アプリケーション開発および配備のライフサイクルの全側面について、階層化され、調整されたポリシーを全社的に導入し、可能な場合は自動化を活用して施行を支援する。	政府は、CI/CD パイプラインを通じてアプリケーションの動的アップデートを組み込むなど、アプリケーション開発とデプロイメントを管理するポリシーを完全に自動化する。

5.5 データ

データには、連邦政府のシステム、デバイス、ネットワーク、アプリケーション、データベース、インフラ、バックアップ（オンプレミスおよび仮想環境を含む）に存在する、または存在したすべての構造化および非構造化ファイルおよびフラグメント、ならびに関連するメタデータが含まれる。

省庁のデータは、連邦政府の要件に従って、デバイス、アプリケーション、およびネットワーク上で保護されるべきである。機関は、データをインベントリ化し、分類し、ラベル付けし、³³、静止時および転送中のデータを防御し、データの流出を検知し、阻止するメカニズムを導入すべきである。政府は、データ・ライフサイクル・セキュリティのすべての側面がエンタープライズ全体で適切に実施されるよう、データ・ガバナンス・ポリシーを慎重に作成し、見直すべきである。

表 6 に、ゼロトラストに関連するデータ機能、およびデータコンテキストにおける可視化と分析、自動化とオーケストレーション、ガバナンスに関する考慮事項を示す。

表 6：データ

機能	伝統的	初級	上級	最適
データインベントリ管理	省庁は、一部の省庁データ（ミッション・クリティカルなデータなど）を手動で識別し、インベントリ化している。	オンプレミス環境とクラウド環境の両方について、データのインベントリ・プロセスの自動化を開始し、ほとんどの省庁のデータをカバーし、データ損失に対する防御の組み込みを開始する。	省庁は、静的属性やラベルに基づくデータ損失防止戦略により、該当するすべての省庁のデータを網羅し、エンタープライズ全体のデータインベントリとトラッキングを自動化する。	省庁は、該当するすべての庁データを継続的にインベントリ化し、データ流出の疑いを動的にブロックする堅牢なデータ損失防止戦略を採用している。

³³ NIST NCCOE: データ分類 <https://www.nccoe.nist.gov/data-classification>.

機能	伝統的	初級	上級	最適
データ分類（新機能）	省庁は、限定的かつ場当たり的なデータ分類機能を採用している。	省庁は、定義されたラベルと手動による実施メカニズムを備えたデータ分類戦略の実施を開始する。	省庁は、シンプルで構造化されたフォーマットと定期的なレビューにより、一貫性のある、階層化された、的を絞った方法で、一部のデータ分類とラベリングプロセスを自動化する。	エンタープライズ・省庁は、堅牢な技術、きめ細かく構造化されたフォーマット、あらゆるデータタイプに対応するメカニズムにより、エンタープライズ全体でデータの分類とラベリングを自動化する。
データの可用性（新機能）	省庁は、主にオンプレミスのデータ・ストアからデータを利用できるようにしているが、オフサイト・バックアップもある。	省庁は、一部のデータを冗長化された可用性の高いデータ・ストア（クラウドなど）から利用できるようにし、オンプレミスのデータについてはオフサイト・バックアップを維持する。	省庁は主に、冗長で可用性の高いデータストアからデータを利用できるようにし、過去のデータへのアクセスを保証する。	同局は、ユーザーや事業者のニーズに応じて、履歴データを含むデータの可用性を最適化するために、動的な方法を使用している。
データ・アクセス	政府は、静的なアクセス管理を通じて、データに対するユーザーおよび事業者のアクセス（読み取り、書き込み、コピー、他者へのアクセス許可など）をガバナンスする。	エンタープライズ全体で最小特権の要素を組み込んだ自動データアクセス管理の導入を開始する。	省庁は、ID、デバイス・リスク、アプリケーション、データ・カテゴリなどの様々な属性を考慮し、該当する場合は時間制限を行うデータ・アクセス管理を自動化する。	省庁は、継続的なアクセス許可のレビューにより、エンタープライズ全体の動的なジャスト・イン・タイムおよびジャスト・イン・ジャフのデータアクセス管理を自動化する。
データ暗号化	セキュリティ・省庁は、静止時および転送時に最小限の省庁・データを暗号化し、暗号化キーの管理と安全性を確保	データセキュリティ機関は、転送中のすべてのデータ、および実行可能な場合は静止中のデータ（ミッション・クリ	エンタープライズ全体にわたって、静止時および転送時のすべてのデータを可能な限り暗号化し、暗号の俊敏性を取	データセキュリティ機関は、適切な場合に使用中のデータを暗号化し、エンタープライズ全体で安全な鍵管理のため

機能	伝統的	初級	上級	最適
	するために手動またはその場しのぎのプロセスに依存している。	ティカルなデータや外部環境に保存されたデータなどを暗号化し、鍵管理ポリシーと安全な暗号鍵の正式化を開始する。 ³⁴	り入れ始め、暗号鍵を保護する（すなわち、秘密はハードコードされず、定期的にローテーションされる）。	の最小特権原則を実施し、可能な限り最新の標準と暗号の俊敏性を使用して暗号化を適用する。 ³⁵
可視性と分析能力	省庁は、場所、アクセス、使用状況を含むデータの可視性が限られており、分析は主に手動プロセスで構成されている。	データインベントリ管理、分類、暗号化、アクセス試行に基づいて可視化され、自動化された分析と相関が行われる。	省庁は、自動化された分析と相関関係により、より包括的で全社的な方法でデータの可視性を維持し、予測分析を採用し始める。	アセスメントは、データの包括的なビューと継続的なセキュリティ態勢評価をサポートする予測分析を含む堅牢な分析により、データのライフサイクル全体にわたって可視性を確保する。
自動化とオーケストレーション能力	データセキュリティ機関は、データのライフサイクルおよびセキュリティ・ポリシー（アクセス、使用、保存、暗号化、防御、構成、保護、バックアップ、分類、サニタイズなど）を、手作業による、場合によっては場当たりのプロセスで実施している。	省庁は、データライフサイクルおよびセキュリティポリシーを実施するために、いくつかの自動化されたプロセスを使用している。	エンタープライズ全体で一貫性のある、階層化された、的を絞った方法で、ほとんどのエンタープライズ・データについて、主に自動化された方法によってデータ・ライフサイクルおよびセキュリティ・ポリシーを実施する。	エンタープライズ全体の全エージェントのデータについて、データ・ライフサイクルとセキュリティ・ポリシーを可能な限り自動化する。

³⁴ これには、主要な店舗を統合し、単発の、あるいはサイロ化された主要な店舗への依存を減らす努力も含まれるはずである。

³⁵ 関連する標準や最新情報については NIST を参照のこと：(1) <https://www.nist.gov/itl/fips-general-information>、(2) <https://www.nist.gov/cryptography>、(3) <https://csrc.nist.gov/publications/detail/nistir/8413/final>。

機能	伝統的	初級	上級	最適
ガバナンス能力	政府は、データガバナンスポリシー（保護、分類、アクセス、インベントリ作成、保管、リカバリ、削除など）を、手作業で実施している。	政府は高レベルのデータガバナンスポリシーを定義し、主に手作業による細分化された実施に依存している。	政府は、エンタープライズ全体のデータ・ライフサイクル・ポリシー施行の統合を開始し、データ・ガバナンス・ポリシーのより統一された定義を可能にする。	省庁のデータ・ライフサイクル・ポリシーは、可能な限り統一され、エンタープライズ全体で動的に実施される。

5.6 横断的な能力

横断的な能力である「可視性と分析」、「自動化とオーケストレーション」、「ガバナンス」は、5つの柱のそれぞれを横断して進歩を統合する機会を提供する。各機関は、特定の柱に関してこれらの能力を成熟させると同時に、柱から独立して各能力を成熟させることもできる。可視性と分析機能は、包括的な可視性をサポートし、政策決定に情報を提供し、対応活動を促進する。自動化とオーケストレーションの機能は、これらの洞察を活用して、セキュリティインシデントを処理し、発生したイベントに対応するための堅牢で合理化された運用をサポートする。ガバナンスにより、政府機関は、リスクベースの意思決定を支援するために、規制、法律、環境、連邦、運用上の要件を管理・監視できる。ガバナンス機能はまた、ミッション、リスク、およびコンプライアンスの目標をサポートするために、適切な人材、プロセス、およびテクノロジーが配置されていることを保証する。

表7は、これらの分野横断的な能力のそれぞれについて、ハイレベルの成熟度の推移を示したものである。

表7：横断的な能力

機能	伝統的	初級	上級	最適
可視性と分析	分析機関は、エンタープライズ全体の限られたログを手作業で収集しているが、その忠実度は低く、分析も最小限である。	アセスメントは、ミッションクリティカルな機能のログとイベントの収集と分析の自動化を開始し、可視性のギャップがないか定期的にプロセスを評価する。	エンタープライズ全体（仮想環境を含む）のログとイベントの自動収集を拡大し、複数のソースを相関させる集中分析を行う。	省庁は、一元化された動的監視とログおよびイベントの高度な分析により、エンタープライズ全体の包括的な可視性を維持する。
自動化とオーケストレーション	霞ヶ関は、静的かつ手作業のプロセスに依存し、自動化が限定的なオペレーションと対応活動を編成している。	同機能は、重要なミッション機能をサポートするため、オーケストレーションとレスポンス活動の自動化を開始する。	省庁は、エンタープライズ全体のオーケストレーションと対応活動を自動化し、複数のソースからのコンテキスト情報を利用して意思決定を行う。	省庁のオーケストレーションと対応活動は、エンタープライズ全体の変化する要件と環境の変化に動的に対応する。

機能	伝統的	初級	上級	最適
ガバナンス	省庁は、エンタープライズ全体でアドホックな方法でポリシーを実施し、手動プロセスまたは静的な技術的メカニズムによってポリシーが実施される。	最小限の自動化と手作業による更新で、エンタープライズ全体に適用されるポリシーを定義し、実装を開始する。	段階的でカスタマイズされたポリシーを全社的に導入し、可能な限り自動化を活用して施行を支援する。アクセス・ポリシーの決定には、複数のソースからのコンテキスト情報を組み込んでいる。	継続的な実施と動的な更新により、カスタマイズされたローカル制御を可能にするエンタープライズ・ワイド・ポリシーを導入し、完全に自動化する。

参考文献

CISA は、本ガイダンスを作成・改訂するにあたり、以下の連邦政府 ZTA 出版物を参考にした。

行政管理予算局 M-22-09

この覚書は、連邦ゼロトラスト・アーキテクチャ戦略を定めたもので、高度化・持続化する脅威キャンペーンに対する政府の防御を強化するため、2024 会計年度末までに特定のサイバーセキュリティ標準と目標を達成することを各省庁に求めている。この戦略には、強力なエンタープライズ・アイデンティティとアクセス管理（MFA を含む）に重点を置くこと、可能な限り早急にすべてのネットワーク・トラフィックを暗号化すること、セキュリティ・アクセス・ルールを自動化する基盤の構築を支援すること、すべてのアプリケーションをインターネット・アクセス可能なものとして扱うこと、などが含まれている。

国立標準技術研究所特別資料 800-207

NIST の SP 800-207 は、エンタープライズ・セキュリティ・アーキテクトのためのゼロ・トラストについて記述しており、民間の未分類のシステムに対するゼロ・トラストの理解を助け、ゼロ・トラストのセキュリティ概念をエンタープライズ環境に移行し、展開するためのロードマップを提供している。SP 800-207 は、複数の連邦機関の協力の成果であり、連邦最高情報責任者（CIO）評議会が監督している。NIST は、さらなる ZTA 実装ガイダンスを開発・公開している。³⁶

国防総省ゼロトラスト・リファレンス・アーキテクチャ

国防総省（DoD）のゼロ・トラスト・リファレンス・アーキテクチャは、国防総省情報ネットワーク（DoDIN）を相互運用可能なゼロ・トラストの最終状態にうまく進めるために使用できる、データ中心のエンタープライズ標準と機能を説明している。³⁷

国家安全保障局、ゼロ・トラスト・セキュリティ・モデルを採用

NSA の Embracing Zero Trust Security Model は、ゼロ・トラスト・セキュリティ・モデルの利点と実装上の課題について説明している。³⁸ 詳細な戦略を構築し、必要なリソースを投入し、実装を成熟させ、ゼロトラスト・モデルに完全にコミットすることが、望ましい結果を達成するために重要であるこ

³⁶ NIST. "Implementing a Zero Trust Architecture Project". <https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture>.

³⁷ 国防総省「ゼロ・トラスト・リファレンス・アーキテクチャ」。バージョン 2.0。
[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf).

³⁸ NSA. 「ゼロ・トラスト・セキュリティ・モデルの採用」。バージョン 1.0。2021 年 2 月。
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_U00115131-21.PDF

とを論じている。この文書の提言は、この最新のサイバーセキュリティ・モデルの導入を検討しているサイバーセキュリティ・リーダー、エンタープライズ・ネットワークの所有者、管理者を支援するものである。

CISA リソース

CISA プログラムは、ZTA への柱の統合を含め、ゼロトラストの柱となる分野全体でサイバーセキュリティの支援とガイダンスを提供する。以下の文書は、ゼロトラストに移行する省庁にとって有用なリソースである。CISA は、各省庁が ZTA を策定するのに合わせて、これらのリソースの見直しと改良を継続し、時間の経過とともにリソースを追加していく予定である。

継続的な診断と低減

CDM ガイダンスは [CDM ホームページ](#) で見ることができる。

高額資産

HVA のガイダンスは、[HVA PMO | CISA のホームページ](#)で見ることができる。

- [高額資産管理オーバーレイ、バージョン 2.0、2021 年 1 月](#)
- [高額資産管理に関する FAQ、バージョン 1.0、2018 年 1 月](#)
- [高額資産の確保、2018 年 7 月](#)
- [CISA インサイト 2019 年 9 月 高額資産の確保](#)
- [拘束的運用指令 18-02-高額資産の安全確保（2018 年 5 月）](#)

国家サイバーセキュリティ防御システム

NCPS のガイダンスは、[NCPS ガイダンス・リポジトリのページ](#)で見ることができる。

- 国家サイバーセキュリティ保護システム（NCPS）クラウド・インターフェース・リファレンス・アーキテクチャー第 1 巻：一般ガイダンス、バージョン 1.4、2021 年 5 月
- 国家サイバーセキュリティ保護システム（NCPS）クラウド・インターフェース・リファレンス・アーキテクチャー 第 2 巻：報告パターン・カタログ ドラフト、バージョン 1.1、2021 年 5 月

サイバーセキュリティ・シェアード・サービス・オファリング（旧品質サービス管理室）

- [品質サービス・マネジメント・オフィス ファクトシート](#)
- [連邦政府向け集中型ミッション支援能力（M-19-16）](#)、2019 年 4 月

信頼できるインターネット接続

TIC ガイダンスは、[TIC ガイダンス・リポジトリのページ](#)で見ることができる。

- 信頼できるインターネット接続 3.0 プログラムガイドブック、バージョン 1.1、2021 年 7 月
- トラステッド・インターネット・コネクション 3.0 リファレンス・アーキテクチャ、バージョン 1.1、2021 年 7 月
- Trusted Internet Connections 3.0 セキュリティ機能カタログ、バージョン 2.0、2021 年 10 月
- トラステッド・インターネット・コネクション 3.0 伝統的 TIC ユースケース、バージョン 1.0、2021 年 4 月
- トラステッド・インターネット・コネクション 3.0 ブランチ・オフィスのユースケース、バージョン 1.0、2021 年 4 月
- トラステッド・インターネット・コネクション 3.0 リモート・ユーザー使用例、バージョン 1.0、2021 年 10 月
- 信頼されたインターネット接続 3.0 クラウドユースケース、ドラフト、2022 年 6 月

その他の CISA リソース

- [クラウド・セキュリティ・テクニカル・リファレンス・アーキテクチャ](#)
- [ゼロ・トラスト原則をエンタープライズモビリティに適用する](#)
- [セキュアクラウドビジネスアプリケーション \(SCuBA\) テクニカルリファレンスアーキテクチャ \(TRA\) \(ドラフト\)](#)
- [拡張可能なジビリティ・リファレンス・フレームワーク \(eVRF\) ガイドブック \(ドラフト\)](#)
- [多要素認証](#)
- [ゼロ・トラスト原則をエンタープライズモビリティに適用する](#)
- [サイバー・レジリエンス・レビュー・アセスメント](#)
- [govCAR ファクトシート](#)
- [Cybersummit 2021 セッション 2 日目 : ゼロ・トラスト](#)