（参考）アメリカ政府によるゼロトラストの推進（1/2）

参考資料３

2022年1月に米国ホワイトハウスより「米国政府ゼロトラスト移行戦略」が発表された。日々高度化するサイバー攻撃の脅威に対応するために、2025年9月末までに本戦略で定められた目標を達成することが求められる。

アメリカ政府の目指すビジョン
エンタプライズによって管理されるアカウントを所有し、必要なすべてにアクセス可能かつ、巧妙なフィッシング攻撃に対しても信頼性のある保護を提供する
利用するデバイスについて、一貫して追跡・監視を行い、内部リソースにアクセスする際のこれらデバイスの状態も考慮する
各機関のシステムは互いに分離され、システムの内外問わず、全ての通信を暗号化する
アプリケーションについて、厳格に試験を実施し、利用者に対してインターネットを介して安全に提供する
セキュリティチームとデータチームが協力して、データカテゴリ及びセキュリティルールを開発し、機密情報等への未承認アクセスを検知し、通信を遮断する

これらのビジョンはCISA※の発行するゼロトラストの5つの柱に沿って設計され、各柱について、以下のような方針が示されている。
各柱の対応事項の内容に応じて実施時期を早急に対応すべき事項は1年以内、それ以外を2025年9月末迄に設定している。

ゼロトラストの柱	具体的な実施事項	一年以内の早急の実施事項
アイデンティティ	・統合ID認証基盤の利用、MFA（PIV,FIDO2）の利用、属性ベースの動的なアクセス制御の実施等を求める。	・特殊文字の使用や定期的なパ スワードのローテーションを要求するパスワードポリシーの削除 ・MFAについてフィッシング耐性の認証を使用する
デバイス	利用している資産の管理や、EDRの導入を行い、政府全体として脅威の検知等を行う。	
ネットワーク	DNSリクエストとHTTP通信の暗号化、メールの暗号化、マイクロセグメンテーション及びネットワークのセグメント化を行う。	
アプリケーションとワークロード	定期的なセキュリティテストや、外部からの脆弱性方向、デプロイの自動化を行う。	・アプリケーションのセキュリティテストの基盤を政府にて構築する ・FISMA※で承認された認証システムを新たに1つ以上採用し、利用可能にする。
データ	セキュリティ対応の自動化(SOAR)、機密データへのアクセス監査（暗号キー管理）、インシデント等に対する調査及び回復能力向上（ログ管理・分析能力向上）を行う。	・90日以内にデータセキュリティに関するワーキンググループを設立し、効果的なデータ分類等を検討する。 ・120日以内に機密性に応じて文書を分類し、監視、閲覧制限の自動化を実現する。

※CISA：Cybersecurity and Infrastructure Security Agency（アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁
※FISMA：Federal Information Security Management Act（連邦情報セキュリティマネジメント法）

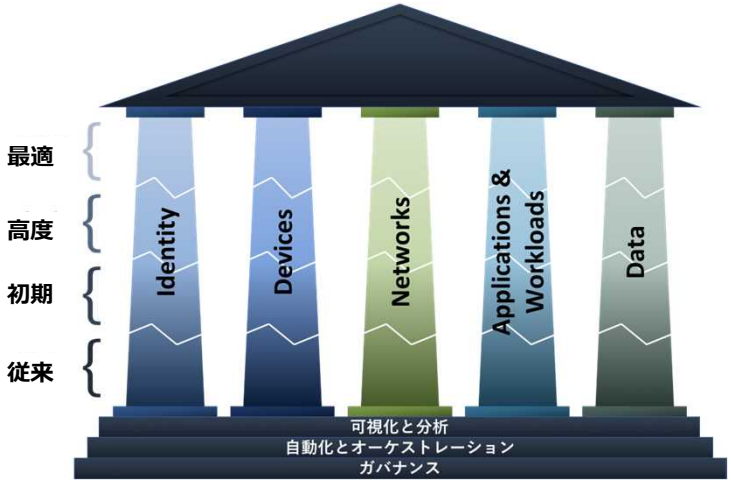
参考：Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

（参考）アメリカ政府によるゼロトラストの推進（2/2）

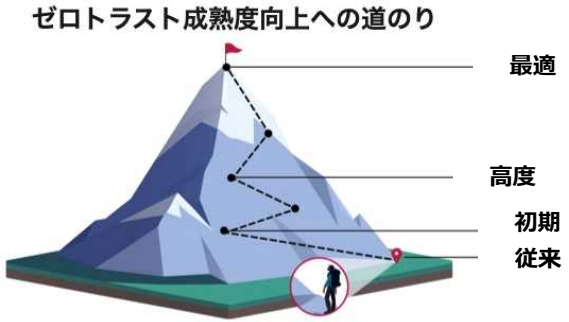
参考資料３

CISAは連邦政府機関がゼロトラストアーキテクチャを設計、実装、進化させる際に使用できるロードマップとして、ゼロトラスト成熟度モデルを発行している。CISAのゼロトラスト成熟度モデルでは、5つの柱に対して各成熟段階における対応を整理している。

■ ゼロトラスト成熟度の発展段階
ゼロトラスト成熟度モデルでは、各柱は時間の経過とともに以下の段階で成熟度が発展していくとされる。各柱は独自のペースで進展するため、柱間の調整が必要となる可能性がある。



■ ゼロトラスト成熟度向上に伴う、労力と利益の増加
全体・各柱内でゼロトラストの成熟度が進むにつれて、必要な労力と実現される利益が大幅に増加すると予想されている。



■ ゼロトラスト成熟度モデルの全体像
5つの柱について、「従来」「初期」「高度」「最適」の各段階に求められる対応を以下のように整理している。各段階の基準を用いて、各柱の成熟度を特定することで、必要な投資の評価、計画、維持を行うことが可能となる。

	Identity	Devices	Networks	Applications and Workloads	Data
最適	• 継続的な検証およびリスク分析 • 全社的なアイデンティティの統合 • 必要最小限のアクセスを自動的に提供	• 自動化されたサプライチェーンリスクマネジメントと統合された脅威防御を含む、物理的および仮想的な資産の継続的な分析 • リソースへのアクセスは、デバイスリスクのリアルタイムな分析によって決定	• ジャストインタイムと必要最小限のアクセスによるレジリエンスを備えた分散型マイクロペリメーター • アプリケーションプロファイルに応じた最適なコンフィギュレーションの管理 • 暗号技術の実用性を高めるベスト・プラクティスを統合	• 公共ネットワークで継続的に利用できるアプリケーション • すべてのワークフローで高度な攻撃を防御 • ライフサイクルに組み込まれたセキュリティテストによる不変的なワークロード	• データの継続的な棚卸し • データの分類とラベリングを全社的に自動化 • 最適化されたデータの可用性 • DLPによる情報流出遮断 • ダイナミックなアクセスコントロール • 使用中のデータを暗号化
	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	
高度	• フィッシングに強いMFA • アイデンティティ・ストアのセキュアな統合と一元管理 • アイデンティティのリスク評価の自動化 • 要求/セッションベースのアクセス	• ほとんどすべての物理的および仮想的な資産をトラッキング • 統合された脅威防御とコンプライアンスの実施 • 初回のリソースアクセスは、デバイスの状態に応じて決定	• 隔離とレジリエンスのメカニズムを拡充 • 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評価に基づいて柔軟性がある管理 • 対象のネットワークトラフィックを暗号化し、鍵の発行とローテーションを管理	• ミッションクリティカルなアプリケーションの大部分は、許可されたユーザーに対してパブリックネットワーク上で利用可能 • すべてのアプリケーションのワークフローで、コンテキストベースのプロテクションを導入 • 開発、セキュリティ、運用の各チームをコーディネート	• トラッキングによるデータインベントリーの自動化 • 一貫性のある、階層化され、対象を絞った分類とラベリング • 冗長化された可用性の高いデータストア • 静的DLP • コンテクストベースの自動化されたアクセス • 保存状態のデータを暗号化
	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	
初期	• パスワードによるMFA • 自己管理型およびホスト型アイデンティティ・ストア • マニュアルによるアイデンティティのリスクアセスメント • 自動レビューでアクセス権が失効する	• すべての物理的資産をトラッキング • 限られたデバイスベースのアクセスコントロールとコンプライアンス実施 • 自動化によって提供されるいくつかの保護機能	• クリティカルなワークロードの初歩的な分離 • ネットワーク ケイパビリティにより、アプリケーション増加に対応した可用性を管理 • 一部のネットワークで動的なコンフィギュレーションの管理 • より多くのトラフィックを暗号化し、鍵管理ポリシーを策定	• ミッションクリティカルなワークフローで、統合されたプロテクションを持ち、許可されたユーザがパブリックネットワーク上でアクセス可能 • CI/CDパイプラインによる定型的なコードデプロイの仕組み • デプロイメント前の静的・動的セキュリティテスト	• インベントリデータとアクセス制御のための限定的な自動化 • データ分類のための戦略に着手 • 一部に高可用性データストア • 通信中のデータを暗号化 • 初歩的な集中管理型鍵管理ポリシー
	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	
従来	• パスワードまたはMFA • オンプレミス・アイデンティティ・ストア • 限られたアイデンティティのリスクアセスメント • 定期的な見直しを行う永続的なアクセス	• デバイスのインベントリーを手動でトラッキング • 限定的なコンプライアンスの可視化 • デバイスからリソースにアクセスするための基準がない • 一部デバイスに脅威防御を手動で適用	• 大きなペリメーター/マクロセグメンテーション • 限られたレジリエンスの中で、ルールセットとコンフィギュレーションを手動で管理 • アドホックな鍵管理による最低限のトラフィックを暗号化	• プライベートネットワーク経由でアクセス可能なミッションクリティカルなアプリケーション • ワークフローに最低限のプロテクションを導入 • アドホックな開発テストと本番環境	• データを手動で棚卸し、分類 • オンプレミスのデータストア • 静的なアクセスコントロール • アドホックな鍵管理による、保存時および通信時に最低限のデータ暗号化

（参考）イギリス政府によるセキュリティ対策状況（1/3）

参考資料３

イギリス政府は「National Cyber Security Strategy 2016-2021」の達成状況と今後約10年間でインターネット、デジタル技術、そしてそれを支えるインフラが自国の利益にとって重要なものとなると考え、「National Cyber Strategy 2022」を掲げて、2030年におけるビジョンと、2025年までに優先的に実施すべき5つの達成目標を定めている。それに従って様々な対策を以下の通り実施している。

イギリス政府の目指すビジョン(National Cyber Strategy)

2030年において、サイバーセキュリティにおいて先進的であり続け、インターネットを通して、国家の利益を保護かつ増進を図る

2025年までに優先的に達成すべき5つの柱	概要
サイバーエコシステムの強化	• 適切な人材・知識・体制の構築 • 他国等との協力体制の強化 • 緊密な産学連携による競争力の強化
高いレジリエンスを持った豊かなデジタル国家作り	• サイバーリスクへの理解を深め、より適切な対策の実施 • サイバー攻撃を排除するため、より効果的な国家によるリスク管理や保護体制の強化
サイバーテクノロジーにおける積極的に中心的な役割を担える体制作り	• 重要な技術に対する高度な研究基盤の作成 • リーダーシップを発揮し、様々なコミュニティと連携してデジタル技術標準の策定
サイバー大国としてのリーダーシップ及び影響力	• サイバーセキュリティやレジリエンスを高めるために国際的なパートナーと協力 • 平和かつ安全なサイバー空間を促進するグローバルガバナンスについての議論を主導
サイバー脅威等の敵対者の検出・阻止・抑止	• 悪意のあるサイバー犯罪者や活動に関する情報を検出、調査、共有し保護

出典：https://www.gov.uk/government/publications/national-cyber-strategy-2022

- **ID管理、アクセス権限の管理等に関するガイドラインを整備**
  National Cyber Security Centre(NCSC)から、ID管理やアクセス権限、認証方法等について、具体的な実装をサポートするガイドラインを作成。

出典：https://www.gov.uk/government/collections/identity-proofing-and-authentication

- **Network and Information Systems Regulation（NIS）を作成**
  英国で事業を行う公共インフラ及びデジタルサービスプロバイダーに対して、安全確保に焦点を当てた規制、報告義務、罰則を規定し、セキュリティ水準の向上を図る

出典：https://www.gov.uk/government/publications/second-post-implementation-review-of-the-network-and-information-systems-regulations-2018/second-post-implementation-review-of-the-network-and-information-systems-regulations-2018

- **ゼロトラストアーキテクチャの実現に向けた手引きを作成**
  ゼロトラスト実装に必要な8つの原則を示し、それぞれについて実装の手引きを作成している。しかし、すべての組織がゼロトラストアーキテクチャを採用できるわけではなく、システムの特性に応じた考慮が必要とも述べている。

出典：https://www.ncsc.gov.uk/collection/zero-trust-architecture/implementing-zta

- **NCSC vulnerability scanning**
  NCSCは、英国内にホストされインターネットアクセス可能なシステムについて脆弱性スキャンが可能なシステムを有し、現在稼働のテストを実施している。最終的な目的として、英国の脆弱性の概要を作成し、それらの公開することで復旧に役立てる狙いがある。

出典：https://www.ncsc.gov.uk/information/ncsc-scanning-information
https://www.ncsc.gov.uk/blog-post/scanning-the-internet-for-fun-and-profit

（参考）イギリス政府によるセキュリティ対策状況（2/3）

参考資料３

NCSCではゼロトラストアーキテクチャ設計に関する手引きを作成、実装に必要な8つの原則を記載し、大規模組織でのゼロトラスト導入を支援している。

No.	原則	概要
1	**ユーザ、デバイス、サービス、データを含むアーキテクチャの把握**	ゼロトラストへの移行において、既存のサービスも考慮しながら資産を把握し、リスクを評価することが重要。ゼロトラストのアプローチがすべてのリスクを軽減できない場合は、現行のセキュリティ対策を維持する必要がある。
2	**ユーザー、サービス、デバイスのIDの把握**	**・ユーザーID** 明確なユーザーディレクトリを使用し、各アカウントに最小限の権限を紐づける等、セキュリティガイドラインに従って適切にアクセス権を設定。 **・サービスID** サービスごとに一意なIDを作成し、最小の権限を与える。サービス間の通信は必要最小限になるように制限する。 **・デバイスID** デバイスを一意に識別し、デバイスに対してコンプライアンス準拠と健全性の確認を行い、実行可能な作業を制御する。
3	**ユーザの行動、サービス、デバイスの健全性を評価する**	**・ユーザ** ユーザの行動を注意深くモニタリングし、通常範囲の行動を定義し、監視を行うことが必要。 **・サービス** サービスの健全性はエンドユーザーがアクセスする際だけではなく、サービス同士が通信する際にも考慮する。 **・デバイス** デバイス管理サービス等を使用して、デバイスに適切なポリシーを適用し、ポリシーに準拠していることを確認する。
4	**ポリシーを利用したリクエストの認可**	**・継続評価** ユーザーやデバイスからの情報を監視し続け、セキュリティの信頼性が低下した場合には再認証を行う。ポリシーを適用するコンポーネントは定義した厳格なポリシーが満たされる場合のみ、接続を許可する。 **・ポリシーエンジンの保護** ポリシーエンジンを保護するため、信頼性の高い製品やサービスを使用し、信頼性の高いポイントにアクセスを制限する。信頼されるユーザーのみがポリシーをインポートできるよう制限し、ポリシーのレビューと監査も実施する。 **・複数のソースを用いたアクセス判断** アクセス判断を行う際は、ユーザID、デバイス、ユーザの振舞いなど複数のソースから判断し、これらの情報は過去情報とリアルタイム接続情報の両方から取得して信頼性を高める **・技術選択時の留意点** ゼロトラストアーキテクチャを実装するための技術を選択する際は、ポリシーエンジンが要求する情報が利用可能であることを確認する。

（参考）イギリス政府によるセキュリティ対策状況（3/3）

参考資料３

NCSCではゼロトラストアーキテクチャ設計に関する手引きを作成、実装に必要な8つの原則を記載し、大規模組織でのゼロトラスト導入を支援している。

No.	原則	概要
5	**すべての接続に対して認証・認可**	**・MFA** 良好なユーザーエクスペリエンスを維持しながらMFAを導入する。 **・ユーザビリティ** 強力な認証がサービスを阻害しないことが重要。重要な操作時のみ追加認証を求め、パスワードレス認証も検討する。 **・サービス間連携** サービス間のリクエストにも相互認証を行い、通信する両サービスが本物であることを確認する。この際通常はAPIトークン、OAuthなどのフレームワーク、または公開鍵基盤（PKI）を使用する。
6	**ユーザ、デバイス、サービスに焦点を当てて監視**	**・監視対象** ゼロトラストにおける監視対象は、VPN等の通信経路上のモニタリングではなく、各デバイスに対して行う必要がある。 **・BYODとゲストデバイス** BYODやゲストデバイスがある場合、モニタリング可能なデバイスとは異なる程度の信頼度を設定する。 **・ネットワークモニタリング** ネットワークモニタリングは、パフォーマンスの測定、ネットワークに接続されているデバイスの特定、不正なデバイスや悪意のある活動の検出を行うために実施する。オンプレミスのサービスをホスティングしている場合には特に重要。
7	**自身を含むすべてのネットワークを信頼しない**	**・デバイス利用ポリシーの強制** 悪意のあるURLやフィッシング検出を行うセーフウェブブラウジング機能等、デバイスのセキュリティ機能をポリシーとして適用することを検討する。 **・サイバーハイジーン** 未承認のホストの監視やネットワークコンポーネントのパッチ適用などネットワークのサイバーハイジーンを維持する。
8	**ゼロトラストに対応したサービスの選択**	**・レガシーサービス** レガシーサービスにゼロトラストを導入する場合、管理の手間や使い勝手の問題が増える可能性があるため、この課題に取り組むリソースを確保することが重要 **・再開発をしない** 独自のサポートインフラを作成することは、コストや複雑さ、エラーの可能性のため避けるべきである。 **・標準を利用** デバイスとサービスの間で相互運用性を実現するため、可能な限り標準的な技術を使用する。 **・クラウド上のサービスの活用** クラウドでの管理されたサービスも相互運用性やセキュリティ向上に役立つ。

（参考）シンガポール政府によるセキュリティ対策状況（1/2）

参考資料３

シンガポール政府は「The Singapore Cybersecurity Strategy 2016」の達成状況と５年間のサイバーセキュリティを取り巻く環境の変化を考慮して、「 The Singapore Cybersecurity Strategy 2021」を策定し、以下の「戦略的な柱」、「基本的な取組」を基に様々な対策を実施している。

戦略的な柱	ゴール	概要
弾力性のあるインフラの構築	• デジタルインフラのセキュリティ及び弾力性を強化する	• マルウェア等の巧妙な脅威・セキュリティリスクに対応するためのアプローチやフレームワークを検討する • 政府のシステムに対して、セキュリティポリシーの見直しや、アーキテクチャの最新化等を促し、安全性と耐障害性を向上させる • 政府内に留まらず、他の重要なシステムや事業体の保護に努め、新たな脅威・リスクに対処する
より安全やサイバー環境の構築	• 安心、安全なデジタル環境の創出	• 政府のネットワークインフラインフラの保護やユーザのデバイスに係るエンドポイントセキュリティの強化を図る。 • 脅威に対する対策として、データ保護基準等の設定の支援を行う • セキュリティに対するキャンペーン等を実施、ユーザ自身の意識や態度を高める
サイバーセキュリティ対策における国際的な協力の強化	• オープン、安全、安定、平和的、相互作用ができる環境の醸成	• 国際的なサイバーセキュリティに対する規範や法律の適用に関する理解や議論の促進を図る • 起こりうる未知のサイバー攻撃に対応するために多国間での協力を推進する。

基本的な取組	ゴール	概要
活気あるサイバーセキュリティの開発環境の構築	• 研究・開発によって支えられるサイバーセキュリティエコシステムの創出	• サイバーセキュリティに関する研究を民間とも協力して行い、知識を共有しつつ、サイバーセキュリティに対する能力の向上を図る • 民間の研究開発の援助やスタートアップの支援を通して、サイバーセキュリティの製品・サービスの開発を推進する • サイバーセキュリティソリューションの採用の奨励や企業の国際展開を支援し、サイバーセキュリティに関する市場の成長を後押しする
優秀なサイバー人材の育成	• サイバーセキュリティに対する労働力の維持及び増強	• 若者や女性等に対してサイバーセキュリティに関するキャリアの広報活動を行い、多様な人材の確保を目指す • 人材育成を強化し、競争力のある人材を育成する

出典：https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

- **ガバメントゼロトラストアーキテクチャのフレームワークの提示**
  政府システムのゼロトラストアーキテクチャ導入を目指して、導入に係るフレームワークを提供

出典：https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture

- **SNDGG(Smart Nation and Digital Government Group)の設立**
  デジタルインフラのセキュリティや耐障害性等の確保のために、政府や民間企業へ技術的なガイダンスやサポートを提供

出典:https://www.tech.gov.sg/media/technews/digital-government-smart-nation-pursuing%20singapore-tech-imperative

- **GovTech Digital Academyの実施**
  政府職員に向けて、ICT関連知識の習得を目的とした、学習の機会を提供し、人材育成に努める

出典：https://www.thedigitalacademy.tech.gov.sg/

（参考）シンガポール政府によるセキュリティ対策状況（2/2）

参考資料３

シンガポール政府はサイバーセキュリティ態勢を強化することを目的として、ガバメントゼロトラストアーキテクチャー（GovZTA）というフレームワークを提供している。GovZTA は4つの主要原則と期待される効果によって管理される。

GovZTA の4つの主要原則

コントロールポイント	4つの原則	期待される効果
アーキテクチャのアクセス強化	**最小の権限適用とアクセス制御の実施**	ユーザー、デバイス、およびアプリケーションは、グループ化し、特定の権限を割り当て、ID ベースの最小限の権限が適用される。 リソースへのアクセスは、リクエスト毎に動的なアクセスポリシーを使用して検証される。
アプリケーションサービスの確保	**横方向の動きの制限**	ネットワークを細分化し、アプリケーションを分離し、データを論理的に分離することで、障害の影響範囲を最小限に抑える。
オペレーション準備態勢の強化	**セキュリティの自動化とオーケストレーションの統合**	継続的にオペレーションが行われるサービスに対しては、セキュリティに必要なプロセス・ワークフローを自動化する。
	検知と対応の強化	プラットフォーム、ホスト、ネットワーク、アプリケーション、データの各レイヤーにわたってログを集約し、セキュリティ情報とアプリケーションのパフォーマンスを分析する。

5つの柱と2つの必要要素

上記の4つの原則を基に、更に5つの技術的柱と、ゼロトラスト達成に必要な2つの要素で構成される実装フレームワークが開発された。

5つの技術的柱	IDENTITY 強力な認証ときめ細かな権限付与	DEVICES エンドポイントの優れた可視性とコントロール	NETWORKS 可能な限り小さなトラストゾーンと複数のセグメントに分解する	APPLICATIONS アプリへのサインオンをオンデマンドセッションで管理する	DATA ライフサイクルを通してデータアクセスを制御する

2つの必要要素	VISIBILITY & AUTOMATION	すべてのアクティビティを把握し、リアルタイムで意思決定を行い、ポリシーに基づいた対応を迅速に実行する。
	GOVERNANCE	様々なプラットフォームを通じて、ゼロトラストの実装に関する技術的なリーダーシップと指示を提供する。

出典：https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture