ネットワークと環境のピラーを通じてゼロトラストの成熟度を進める

エグゼクティブサマリー

組織のネットワークにアクセスした後、悪意のあるサイバー・アクターが最もよく使う手法の１つは、ネットワークを横方向に移動し、より機密性の高いデータや重要なシステムにアクセスすることである。ゼロトラストのネットワークと環境のピラーは、きめ細かなポリシー制限を通じて、論理的・物理的にセグメント化、隔離、アクセス制御（オンプレミスおよびオフプレミス）を行う管理・機能を採用することで、敵対的な横の動きを抑制する。

ネットワークと環境のピラーは、他のゼロトラストのピラーと協調して、敵の侵害がネットワーク内部で発生することを想定し、ネットワーク全体の活動を制限、検証、監視する全体的なゼロトラスト・セキュリティ・モデルの一部として機能する。

このサイバーセキュリティ情報シートで紹介するコンセプトは、データフロー・マッピング、マクロ・マイクロ・セグメンテーション、ソフトウェア・デファインド・ネットワーキングを通じて、侵害の潜在的影響を制限するために既存のネットワーク・セキュリティ管理を強化するためのガイダンスを提供するものである。これらの機能により、ホストの分離、ネットワークのセグメンテーション、暗号化の実施、エンタープライズの可視化が可能になる。組織は、内部ネットワーク制御を成熟させることで、徹底的な防御態勢を大幅に改善し、その結果、ネットワーク侵入をより適切に封じ込め、検知し、隔離することができる。

序文

公的な報告によると、アメリカのある小売企業は 2013 年、ネットワーク・セグメンテーションの欠如が原因で重大なデータ漏洩に見舞われた。[1]情報漏洩に先立ち、サイバー犯罪者は、小売企業のいくつかの店舗が契約していた暖房、換気、空調（HVAC）会社のログイン認証情報を取得することに成功した。各店舗は、エネルギーと温度レベルを監視するために、HVAC 会社に企業ネットワークへのアクセスを許可していた。しかし、入手したログイン認証情報を使って、サイバー行為者は企業の POS システムにマルウェアを侵入させ、約 4000 万枚分のデビットカードやクレジットカードの情報を盗み出すことに成功した。この空調会社は、その責務を遂行するために小売企業のネットワークにアクセスする必要があったが、調査結果によると、この企業はネットワークのセグメンテーションとアクセス管理を実施することで、決済システムへのサードパーティからのアクセスを軽減できた可能性が高い。[2]

従来のネットワーク・セキュリティは、徹底的な防御アプローチを重視してきた。しかし、ほとんどのネットワークは、主に境界防御に投資している。ネットワーク境界の内側に入ると、エンドユーザー、アプリケーション、およびその他の事業体は、多くの場合、複数の企業リソースへの広範なアクセスを許可される。ネットワーク・ユーザーやコンポーネントが侵害されると、悪意のある行為者はネットワークの内外から重要なリソースにアクセスできるようになる。理想的には、組織は内部と外部の両方のトラフィックフローを管理、監視、制限する必要がある。

このサイバーセキュリティ・インフォメーション・シート（CSI）では、「ゼロトラスト（ZT）」セキュリティモデルに基づいて、境界防御に加えてリソースやデータの近くにセキュリティ制御を実装することに重点を置いたネットワークと環境のピラーについて説明する。このピラーの主な分野は、ネットワーク内のデータフローのマッピングと、横方向の動きを抑制するための強力なアクセス管理によるネットワーク・セグメンテーションの実装である。このシフトにより、ホストの分離、ネットワークのセグメンテーション、暗号化の実施、エンタープライズの可視化が可能になる。組織が内部ネットワーク制御を成熟させるにつれて、徹底的な防御態勢が大幅に改善され、その結果、ネットワーク侵入をネットワークのごく一部に隔離できるようになる。

観客

本 CSI は、主に国家安全保障システム（NSS）、国防総省（DoD）、防衛産業基盤（DIB）を対象としたガイダンスを提供する。しかし、巧妙な悪意者に狙われる可能性のある他のシステムの所有者や運用者にとっても有用であろう。この CSI は、国防総省のゼロトラスト戦略、ゼロトラスト参照アーキテクチャー、サイバーセキュリティ参照アーキテクチャー（CSRA）からのガイダンスを組み込んでいる。[他のシステム所有者及び運用者向けの追加ガイダンスは、国立標準技術研究所（NIST）及びサイバーセキュリ ティ・インフラ保障局（CISA）からも入手可能である。[6], [7]

背景

国家のサイバーセキュリティ改善に関する大統領令（EO 14028）および国家安全保障覚書 8（NSM-8）は、連邦文民行政機関および NSS の所有者および運営者に対して、ZT サイバーセキュリティフレームワークを採用する計画を策定し、実施するよう指示している。[8], [9]

NSA CSI「Embracing a Zero Trust Security Model」は、ZT の概念を、サイバー脅威の偏在性を認識し、暗黙の信頼を排除し、代わりに運用環境のあらゆる側面の継続的検証を優先するという基本原則を持つセキュリティ戦略として定義している。ZT の実施努力は、時間の経過とともにサイバーセキュリティの防御、対応、運用を継続的に成熟させることを意図している。ZT の 7 つのピラー（ユーザー、デバイス、ネットワークと環境、データ、アプリケーションとワークロード、自動化とオーケストレーション、可視性と分析）のそれぞれにおける能力の向上は、脅威の評価と監視に基づく継続的な改善サイクルの要素であると考えるべきである。[10]

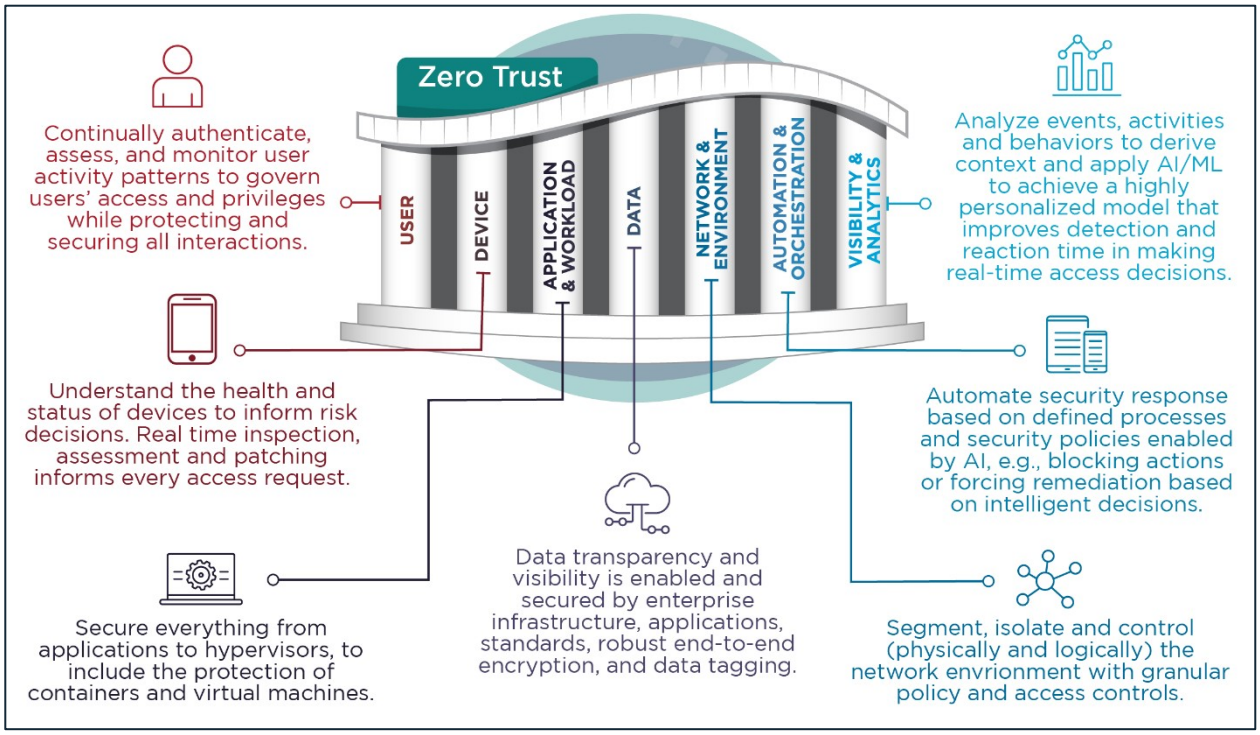

図 *1*：ゼロトラストの *7* つのピラーの説明

図 1 は、ネットワークと環境のピラーを含む ZT のピラーを示している。ZT 成熟度モデルのネットワークと環境のピラーの構成要素の能力とマイルストーンについては、本 CSI を通して詳述する。支ピラーは独立しているわけではなく、ネットワークと環境の支ピラーの能力の多くは、示されているように、他の支ピラーの能力に依存しているか、他の支ピラーの能力と整合している。

ネットワークと環境のピラー

ネットワークがハードウェアとソフトウェアの接続であるのに対し、DoD CSRA および NIST SP 800-207 で定義されているサイバーセキュリティ環境は、ネットワークコンポーネント、非人間事業体、相互コミュニケーションのためのプロトコルのすべてを包含するデジタルエコシステムである。[5], [6] ZT 成熟度モデルは、4 つのネットワーキングと環境のピラーとなる各機能のいくつかの重要な機能を通じて、ネットワークの安全性を徹底的に高める：

- データフロー・マッピング
- マクロ・セグメンテーション
- マイクロ・セグメンテーション
- ソフトウェア・デファインド・ネットワーキング

ネットワークと環境は、最初に意図的に開発され、環境のライフサイクルを通じて維持・改善されなければならない、セグメント化された堅牢なアーキテクチャを通じて、このモデルに貢献する。

セキュアなネットワーク・セグメンテーション・フレームワークに加えて、ZT アーキテクチャは、すべてのユーザー、デバイス、データの強力な暗号化と永続的検証によるセキュアなネットワーク・トラフィック管理を採用している。自動化とオーケストレーションは、定義されたプロセスとセキュリティ・ポリシーに依存し、必要に応じてネットワーク・セグメンテーションを動的に分離または変更するアダプティブ・ネットワーク機能を備えている。直感的なアナリティクスは、ネットワークやその他のイベントやアクティビティに不審な行動がないか監視する。適切に適用されれば、これらの機能はすべて ZT アーキテクチャをサポートし、ネットワークのセキュリティを大幅に改善する可能性を秘めている。

ネットワークと環境のピラーは、ネットワークアクセスを定義し、ネットワークとデータフローを管理し、アプリケーションとワークロードをセグメント化し、エンドツーエンドの暗号化を使用することで、重要なリソースを不正アクセスから隔離する。これは、マクロ・ミクロレベルでの適切なネットワーク・セグメンテーションと、集中制御と自動化を可能にするソフトウェア・デファインド・ネットワーキング（SDN）の組み合わせによって達成される。このピラーは、組織のデータに対する認識と理解の深さによって決まる。データがどのようにスタンドアロンネットワーク内を流れるのか、そして物理インフラ、クラウドコンピューティング、分散作業環境を相互接続するネットワーク間を流れるのか。

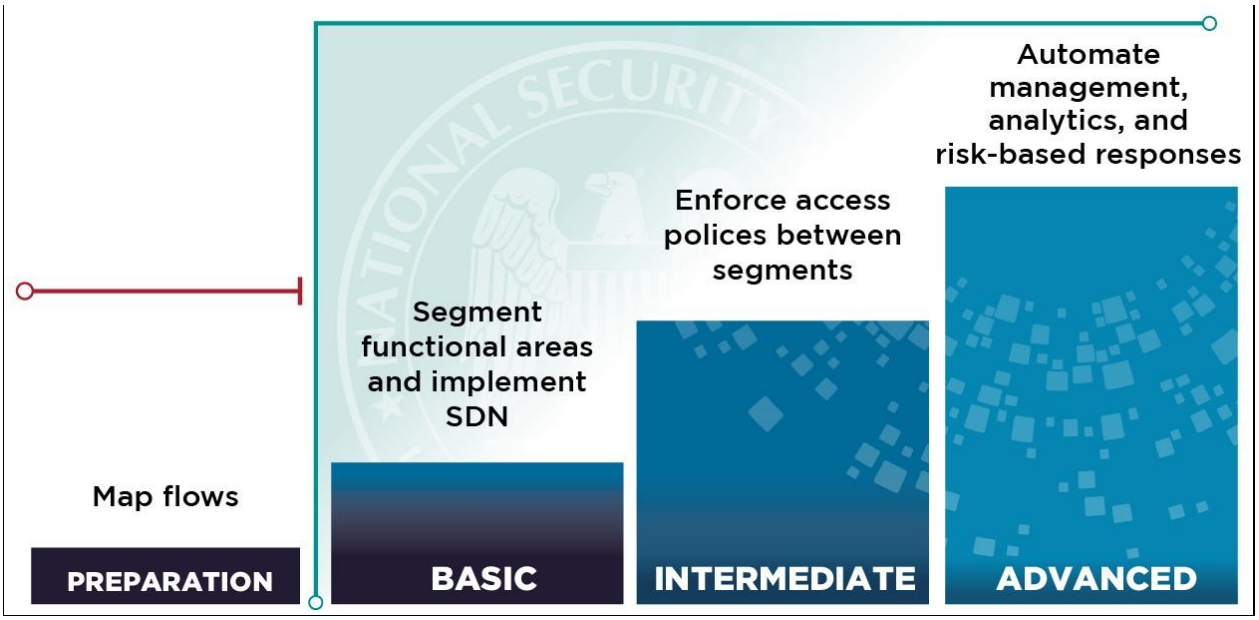

図 2：ゼロトラストのネットワークと環境のピラーの成熟度

データフロー・マッピング

データフロー・マッピングは、データが組織内を移動する経路を特定し、データがある場所やアプリケーションから別の場所へどのように変換されるかを記述する。この作業により、データが保存または処理される内部および外部のノードが明らかになり、データの誤用を発見することができる。組織は、データ所有者とネットワーク・チームの知識を活用して、包括的なデータフロー・マップを作成すべきである。

このマップは、データが適切に暗号化されていないデータフローを特定することもできる。転送中のデータが暗号化されていない場合、データ送信者は可能な限りエンド・ツー・エンドの暗号化を有効にするか、仮想プライベート・ネットワーク（VPN）、または同等の暗号化トンネルやプロトコルを活用して転送中のデータを保護すべきである。

データの防御が不十分なフローを発見するだけでなく、このデータフロー・マッピング・プロセスは、マクロ・セグメンテーションやミクロ・セグメンテーションなど、他のネットワーク活動の基礎となる。さらに、データがネットワークをどのように流れるかを理解することは、アナリティクスによって異常なトラフィックの挙動を効率的に識別するのに役立つ。

表 *1*：データフロー・マッピングの成熟度

準備	基礎	中級	上級
データが保存され処理される場所と、データ構成要素がどの状態に保存されているかを識別する。	組織は、物理的および論理的データフローのマッピングを開始する。このレベルでは、マッピングは主に手作業で行われる。 暗号化されていないデータフローは、暗号化されたデータフローに、あるいは暗号化されたネットワークトンネルやプロトコル内に移行する。	組織はアプリケーションの完全なリストを持ち、重要なデータフローを特定している。 マッピングの正確性を維持するために、いくつかの自動化が実施されている。識別された異常なデータフローは、このレベルで分離または除去されるべきである。	組織はデータフローの完全な目録を持っている。 自動化は管理者を監視し、すべての現在、新規、または異常なデータフローを低減する。

マクロ・セグメンテーション

ネットワークのセグメンテーションは、ZT アーキテクチャーの設計と実装において極めて重要である。それは以下のように分解できる：

- マクロ・セグメンテーション
- マイクロ・セグメンテーション

マクロ・セグメンテーションは、ネットワークを複数の個別のコンポーネントに分割し、それぞれが異なるセキュリティ要件をサポートすることで、組織のネットワークのさまざまなエリア間を移動するトラフィックを高レベルで制御する。言い換えれば、マクロ・セグメンテーションは、企業内の下部組織の分離と考えることができる。例えば、IT 部門の従業員は、経理部門のネットワーク・セクションや、そこに存在するすべてのデータやリソースにアクセスすべきではない。このようなネットワークの境界は、アクセス管理と相まって、攻撃対象領域を縮小し、横の動きを防ぐことでセキュリティを提供する。さらに、マクロ・セグメンテーションは、セキュリティ対応を自動化する道を開く。その結果、データ侵害、サービス拒否、マルウェアの拡散による損失のリスクをさらに最小限に抑えることができる。

先に述べた小売企業のデータ漏洩のケースでは、ある空調会社がサービス関連業務のためにネットワークへの有効なアクセス権を与えられていた。しかし、ネットワークは適切にセグメンテーションされていなかったため、サイバー行為者は HVAC 会社の従業員の一部から盗んだ認証情報を使ってネットワークにアクセスし、販売時点情報管理システム（POS）へピボットすることができた。[1] 公的な報告によると、マクロ・セグメンテーションによってこれを防ぐことができ、顧客と企業の損失を数百万ドル削減できたという。[2]

表 2：マクロ・セグメンテーションの成熟度

準備	基礎	中級	上級
ネットワーク上のさまざまなセキュリティ・レベルを定義する。 ネットワーク構造の論理的区別をマッピングする。	組織は、ビジネス機能、場所、資産の重要性に基づいてネットワークをセグメント化し始める。 既存のセグメント（例：VLANS）内で、内部セキュ リティ管理を強化する。	セグメント間の横方向の移動を制限するアクセスポリシーは、セキュリティポリシーに基づいて定義され、ファイアウォールルールに書き込まれる。	ネットワークはさらに細かく分割され、自動化された中央管理システムが統合され、ネットワークの成長を管理するように構成されている。

マイクロ・セグメンテーション

マイクロ・セグメンテーションは、ネットワークの一部をより小さなコンポーネントに分割し、厳密なアクセス・ポリシーによってデータが横方向に流れるのを制限することで、粒度の細かいレベルでのセキュリティを提供する。マイクロ・セグメンテーションは、サブ組織内のネットワーク分離と考えることができる。同じ部署の従業員は、明示的に必要とされない限り、互いのリソースにアクセスすべきではない。これにより、ネットワーク境界ですでに確立されているポリシーを補強し、アプリケーションやリソースにより近い場所で追加のセキュリティ施行を行うプロバイダが提供される。したがって、マイクロ・セグメンテーションでは、ユーザー、アプリケーション、またはワークフローを個々のネットワーク・セグメントに分離することで、攻撃対象領域をさらに縮小し、侵害が発生した場合の影響を制限する。

この小売企業のネットワークへの侵入が発生したのは 10 年前のことだが、学んだ教訓はサイバーセキュリティ業界全体に響き続けている。例えば、POS システムを互いに、そして他のシステムからマイクロ・セグメンテーションすることで影響を限定できたかもしれないので、マイクロ・セグ

メンテーションは今や多くの組織の防御態勢の主要な構成要素となっている。今日の SDN テクノロジーは中央制御と自動化されたポリシー実施によってこれをより管理しやすくしている。

表 3：マイクロ・セグメンテーションの成熟度

準備	基礎	中級	上級
アイデンティティとアプリケーション・アクセスに基づいて、ネットワーク上のさまざまなセキュリティ・レベルを定義する。	組織は、サービスごとの相互接続と、重要なデータフローの分離に移行し始める。	組織はエンドポイントとアプリケーションの分離メカニズムを、マイクロ・セグメント間のイングレス／エグレス・コントロールとともに、ネットワーク・アーキテクチャのより多くの部分に導入する。コントロールは必要に応じてテストされ、改善される。	組織は、アプリケーション・プロファイルとデータフローに基づく広範なマイクロ・セグメンテーションを採用し、サービス固有の相互接続のための接続認証を継続的に行っている。 中央管理プラットフォームは、自動化された最適な可視性と、異常な動作に対するアラートを含むセキュリティ監視を提供するように改良されている。

ソフトウェア・デファインド・ネットワーキング

SDN はマイクロ・セグメンテーションによる粒度の細かさ、適応性、ポリシーの集中管理という点でユニークな利点を提供する。SDN コンポーネントを既存のインフラに統合することで、カスタマイズ可能なセキュリティモニタリングとアラートも可能になる。

マイクロ・セグメンテーションは伝統的なシステムコンポーネントと手動コンフィギュレーションで実現できるが、SDN の集中化された性質はネットワーク全体のダイナミックな実装と管理を可能にする。SDN は分散フォワーディングプレーンを介して集中制御サーバによるパケットルーティングの制御を可能にし、ネットワークに更なる可視性を提供し、統一されたポリシーの実施を可能にする。

SDN は既に現在使われている多くの最新のネットワーク機器の機能であり、新しい機器の柔軟な統合と制御を可能にする。加えて、SDN ネットワーク管理プラットフォームはすぐに利用でき、手動タスクを自動化できる。これは共通の一元管理されたポリシーの下でのネットワークセグメントの統合を容易にし、ネットワークがスケールするにつれて設定ミスのようなヒューマンエラーのリスクを減らす。

ネットワーク全体のセキュリティが SDN によるマイクロ・セグメンテーションの恩恵を受ける一方で、SDN コントローラ (SDNC) 自体は適切なコンフィグレーションと継続的なモニタリングを必要とする優先的なターゲットになり得る。必要なタスクの自動化を促進するためにアプリケーション・プログラミング・インタフェース (API) を呼び出すスクリプトが書かれるように、SDNC のコンフィギュレーションはそれらの API を公開することができる。SDN は更新とセキュリティポリシーの自動化によってネットワークセキュリティを改善する。しかしながら、API の公開を防ぐためには、セキュリティ制御の不正な無効化と SDN 機能の他の危殆化を防ぐためのサイバーセキュリティの優れた実践（と規律）が必要である。これらのリスクと推奨されるプラクティスの詳細については、Software Defined Networking コントローラのリスクマネジメントを参照。[11]

専用の API 管理者ロールは、SDN 管理者と同じレベルのアクセスを許さない制限された権限で作成されるべきである。SDNC は認可された API 管理者からのみ API 呼び出しを受け付けるべきである。API 呼び出しは、転送中のデータを保護するために、可能な限り適切な暗号化プロトコル（例えば TLS v1.2 またはそれ以降、SSH v2 またはそれ以降）と相互認証（クライアントとサーバの証明書など）を使ってセキュリティ保護されるべきである。

表 4：ソフトウェア・デファインド・ネットワーキングの成熟度

準備	基礎	中級	上級
組織は彼らの管理範囲内のネットワークセグメントをマップし、SDN コンポーネントの統合のためのロードマップを特定する。	SDN コンポーネントを統合し、管理ポリシー、ネットワーク設定ルール、タスクスケジュール（更新など）と共にセントラルコントロールプレーンを開発する。 SDN API をマップし、ロールを確立し、暗号化と認証を使用して API 呼び出しを行うように SDNC を設定する。	相互接続性をテストし、最適な粒度でセグメンテーションルールを採用するための設定を行う。 異常な動作や不審な動作を管理者に通知するアラートシステムを構築する。	高度なアナリティクスとコントロールを採用する。 ネットワークをテストし、侵入者がセグメント間を横方向などに移動できるネットワーク経路を特定する。 厳密なアクセス管理により、適宜パスを制限する。

概要

ここで開発した成熟度モデルに従ってネットワークと環境のピラーのロードマップを拡張し、洗練させることで、エンタープライズアーキテクチャの弱点やギャップを突く脅威に抵抗し、検知し、対応するためのプロセスを組織に提供する。これらのプロセスは、脅威がシステムの名目上の境界内にすでに存在すると想定する運用上の考え方をサポートする。リスクが継続的にアセスメントされ、適切な対応が適時に実施され、必要に応じて追跡調査や損害管理が行われるようにするためには、警戒が必要である。

NSA は、ネットワークの所有者と運用者が、この CSI に記述されている成熟度モデルの高度なレベルに見合った能力を開発することによって、ネットワークと環境を強化することを強く推奨する。ネットワークと環境のセキュリティは、現在のすべてのデータフローの正確なインベントリを確立することから始まる。これにより、これらのフローへのアクセスが適切に保護され、吟味され、適切であることが保証される。

ネットワークと環境の能力を成熟させるために、組織は以下を行うべきである：

- 使用パターンと業務上のビジネス要件に基づいてデータフローをマッピングする。

- ネットワークをマクロとミクロの両レベルで適切にセグメント化する。
- 集中制御と自動化されたタスクのために、それが利用可能で実用的であれば SDN を使う。
- セキュリティ・ポリシーを自動化し、運用の効率性と俊敏性を高める。
- リスクベースの手法を使用して、境界、マクロ、ミクロの境界において、悪意のあるトラフィックや未承認のトラフィックがネットワーク・リソースに到達する前に確実にドロップされる仕組みを含むアクセス・ルールを定義する。

さらなるガイダンス

NSA は、国防総省の顧客が ZT システムを試験的に導入するのを積極的に支援し、既存の NSS や国防総省のプログラムとの活動を調整し、NSS、国防総省、DIB 環境の中で ZT を統合するという課題を通してシステム開発者を支援するための追加の ZT ガイダンスを開発している。今後予定されているガイダンスは、エンタープライズ・ネットワークへの ZT の原則と設計の組み込みを整理し、ガイドし、簡素化するのに役立つだろう。

引用文献

[1] コンピュータワールド Target Breach Happened Because a Basic Network Segmentation Error.2014. https://www.computerworld.com/article/2487425/target-breach-happened-because-of-a basic-network-セグメンテーション-エラー.html

[2] 上院商務・科学・運輸委員会。2013 年 Target データ漏洩の「キルチェーン」分析。2014. https://www.commerce.senate.gov/services/files/24d3c229 xml-ph-0000@deepl.internal 4f2f-405d-b8db-a3a67f183883

[3] 国防総省。国防総省ゼロトラスト戦略。https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[4] 国防総省。DoD Zero Trust Reference Architecture.https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[5] 国防総省。国防総省サイバーセキュリティ参照アーキテクチャ。2023 年。https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[6] 国立標準技術研究所.NIST 特別刊行物 800-207: Zero Trust Architecture.2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[7] サイバーセキュリティ・インフラセキュリティ庁.ゼロトラスト成熟度モデル。2023. https://www.cisa.gov/zero-trust-maturity-model

[8] ホワイトハウス大統領令 14028: 国のサイバーセキュリティの改善。https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations サイバーセキュリティ

[9] ホワイトハウス White House National Security Memorandum 8: Improving Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.2022. https://www.govinfo.gov/content/pkg/DCPD-202200025/pdf/DCPD-202200025.pdf

[10] 国家安全保障局。ゼロトラスト・セキュリティ・モデルを採用する。2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[11] 国家安全保障局。Software Defined Networking Controllers のリスクマネジメント。2023. https://media.defense.gov/2023/Dec/12/2003357491/-1/-1/0/CSI_MANAGING_RISK_FROM_SDN_CONTROLLERS.PDF.

推薦の免責事項

本文書に含まれる情報および意見は、「現状のまま」提供されるものであり、いかなる保証も行わない。本書に記載されている、商号、商標、製造事業者、その他による特定の商用製品、プロセス、またはサービスへの言及は、米国政府による推奨、推薦、または支持を意味するものではなく、本ガイダンスを広告または製品推奨の目的で使用してはならない。

目的

本文書は、国家安全保障システム、国防省、防衛産業基盤の情報システムに対する脅威を識別し広 報する責任、サイバーセキュリティ仕様と低減策を策定し発行する責任など、NSA のサイバーセキュリティ 任務を推進するために作成された。この情報は、すべての適切な利害関係者に届くように広く共有されることがある。

連絡先

サイバーセキュリティレポート フィードバック CybersecurityReports@nsa.gov

サイバーセキュリティに関する一般的なお問い合わせまたはお客様のご要望：Cybersecurity_Requests@nsa.gov

防衛産業基盤に関するお問い合わせとサイバーセキュリティサービス：DIB_Defense@cyber.nsa.gov

メディアお問い合わせ / プレスデスク NSA メディアリレーション：443-634-0721, MediaRelations@nsa.gov