ゼロトラスト
指針となる原則

Release Candidate

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance®

This is a Release Candidate version and is subject to change.

日本語版提供に際しての告知及び注意事項

本書「ゼロトラスト指針となる原則」は、Cloud Security Alliance (CSA)が公開している「Zero Trust Guiding Principles」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2023年12月22日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSAジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定
CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3)　CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３.　本書の適切な管理

(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。

(3)　本書をダウンロードした者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4)　本書を印刷した者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４.　原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５.　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「ゼロトラスト指針となる原則」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

伊藤　吉也
納本　健太
加藤　孝史
諸角　昌宏

謝辞

CSA ゼロトラスト・ワーキンググループ

ゼロトラストの研究とガイダンスの範囲は、必然的にクラウドとオンプレミス環境、モバイル・エンドポイントを含み、モノのインターネット（IoT）とオペレーショナルテクノロジー（OT）に適用されます。CSA ゼロトラスト（ZT）ワーキンググループの目標は以下のとおりです。

- 情報セキュリティ(InfoSec)の現代的で必要かつクラウドに適したアプローチとして、ゼロトラストのベストプラクティスを共同で開発し、認知度を高める。
- 組織がそれぞれのニーズと優先事項に基づいて十分な情報に基づいた意思決定を行えるよう、さまざまなゼロトラスト手法の長所と短所について、ソートリーダーシップを提供し、業界を教育する。
- アーキテクチャに対して、意図的に製品およびベンダーに中立的なアプローチをとり、ゼロトラストの実装を成熟させる。
- テクノロジー、セキュリティ、ビジネス、オペレーション間の連携を可能にする。

筆頭著者

Alex Sharpe

執筆者

Madhav Chablani
Frank DePaola
Jonathan Flack
Sai Honig
Shamik Kacker
Andrea Knoblauch
Rajesh Murthy
Denis Nwanshi
Lars Ruddigkeit
Paul Simmonds
Nelson Spessard
Bernd Wegmann
Heverin Joy Williams
Lauren Wise

査読者

Sam Aiello
Jason Garbis
Brett James
Yves Le Gelard
Jennifer Minella
Chandrasekaran Rajagopalan
Aaron Robel
Michael Roza

CSAスタッフ

Erik Johnson
Stephen Lumpe

目次

要旨

ゼロトラスト（ZT）は、デジタルトランスフォーメーションや組織のセキュリティとレジリエンスを高めるその他の取り組みの一環として、組織が採用することが非常に有用な戦略的考え方です。ゼロトラストは、セキュリティ業界内での様々な対立するメッセージや、確立されたゼロトラスト基準の欠如から、誤解されやすく、複雑になりすぎています。実際は、ゼロトラストは、私たちの働き方や生活の変化、例としてはリモートワーカー、サードパーティへの依存の増加、およびクラウドの採用などにより、より重要になりつつある長年の原則に基づいています。この文書は、「最小特権の概念」、「職務の分離」、「セグメンテーション」などの確立された情報セキュリティ（InfoSec）の原則を含む基本原則を示すことによって、ギャップを埋め、明確にすることを目的としています。これらの指針となる原則は、すべてのゼロトラストの柱、さまざまなユースケース、異なる環境、製品の間で一貫性を保ちます。このガイダンスは、業界の発展とともに進化していきます。

エグゼクティブサマリ

ゼロトラストは、情報セキュリティ（InfoSec）に対するシンプルなアプローチですが、しばしば誤解され、複雑になりすぎています。ZTの哲学と戦略は正しく理解すれば、組織がセキュリティを強化し、レジリエンスを高め、デジタルトランスフォーメーションを導くために利用できる貴重なツールとなります。本書は、ゼロトラストとは何かを明確に理解し、ZTを計画、実装、運用する際に覚えておくべき指針を提供することを目的としています。

歴史的に、情報セキュリティは資産を収集し、管理された物理的な境界内に囲い込む能力に基づいたセキュリティモデルでの技術的コントロールに大きく依存していました。これはもはや時代遅れです。ゼロトラストは、人、プロセス、組織、テクノロジー間の全体的な関係を認識し、歴史的な技術的コントロールだけではもはや十分ではないとしています。ユーザーはこれまで、企業の境界内に位置することに基づいて「信頼されている」と思っていました。ゼロトラストは、資産へのアクセスを許可する前に、場所に関係なく検証を要求することで、この概念を覆します。

ゼロトラストは、「信頼せず、常に検証する」、最小特権の概念、セグメンテーションの実践といった長年の原則を活用し、サイバーハイジーンを高め、TCOとインシデントによる損害を削減し、復旧時間の短縮を促進します。既存のセキュリティ対策をZTの原則で補強することで、企業は複雑で分散した環境で資産を保護するためのより強固な基盤を確立することができます。このプロアクティブなアプローチは、セキュリティポスチャを強化し、脅威の進化に伴う潜在的なリスクを最小限に抑えます。

ゼロトラストは、侵害が起こることも認識しています。レジリエンスを育むために、ZT は影響範囲（訳注：原文では"blast radius"（爆発半径））を抑制し、侵害の影響を軽減すると同時に、迅速な回復を促進する手段を提供します。これらの同じ技術は、悪意ある者が必要とする作業と投資を増加させ、インシデントの可能性をさらに低下させます。

ゼロトラストに対する最近の関心は、新しいビジネスモデル、クラウドの採用、および政府の新しい要件に後押しされています。ゼロトラストは、米国では大統領令[1]によってすべての連邦政府機関に義務付けられており、欧州連合（EU）でのデジタルオペレーショナルレジリエンス法（DORA）[2]やネットワークおよび情報セキュリティ（NIS2）指令[3]などのイニシアチブを通じて世界的に採用されています。ゼロトラストは、すべてのゼロトラストイニシアチブに共通する基本原則の組み合わせを通じて、必要な保証を提供します。本文書では、あらゆるZTイニシアチブの指針となるこれらの基本原則の概要を示します。

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.digital-operational-resilience-act.com/
[3] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

はじめに

組織はゼロトラストを活用して、データとネットワークのサイバーセキュリティ管理手法を幅広く変革します。原則、信条、柱、アーキテクチャ計画、フレームワークなど、多くのゼロトラスト管理のコンセプトが登場しています。この進化は旅のようなものですが、ZTによる変革は、単一のプロジェクト（ビジネス、運用、技術）や特定の製品と同一視されるものではありません。ゼロトラストは、高度に分散したアーキテクチャにおける重要資産の保護を強化することを目的とした成熟した方法論です。それぞれのZTの旅は異なるものであることを理解し、前もってすべての主要な利害関係者との計画を立てる必要があります。ビジネスとの整合性が高ければ高いほど、ゼロトラストの旅が成功する可能性は高くなります。

多くの組織が、クラウドの導入やリモートワークの促進のために運営モデルを変更しています。従来のセキュリティ対策では、これによってもたらされた新たなリスク環境には十分に対応できません。サイバーレジリエンスの向上を目指す組織は、サイバーリスクを軽減するために、もはや硬い外殻や技術的コントロールだけに頼ることはできません。サイバー脅威の状況は進化し続けており、従来の要塞モデルの防御能力を超えて拡大しています。

守るべきものの範囲も広がっています。もはやIT資産やデータだけを扱う時代ではありません。IT以外のデバイス、ワークロード、アプリケーション、ビジネスプロセスにも範囲が広がっています。これは一般に、データ、アプリケーション、資産、サービス、略してDAASと呼ばれています。

セキュリティアーキテクチャをビジネス・オペレーティング・モデルと整合させることで、組織は、ビジネスプロセスを阻害することなく適切なセキュリティを提供しながら、ビジネスを変革することができます。ゼロトラストが基本的なコンセプトとして受け入れられると、プライバシー、コンプライアンス、リスク管理など、他の多くの企業の取り組みが支援されます。

この文書は、どのような組織でもゼロトラストへの移行を計画または開始する際に活用できる指針となる原則を提供します。

対象読者

この文書の主な対象者は、情報保護の実務者とその経営幹部です。指針となる原則として、本文書の内容はすべてのゼロトラスト構想にまたがります。この指針となる原則は、業界団体や標準化団体がゼロトラストの知識体系（BOK）を構築する際に使用されるものと認識しています。

指針となる原則

ゼロトラストは、単独の概念や技術ではありません。むしろ、さまざまな原則、戦略、テクノロジーを包含する包括的なセキュリティ戦略とアプローチです。進化する脅威の状況や、従来の境界ベースのセキュリティモデルの限界に対処するために設計されています。

以下の指針となる原則は、実務者がゼロトラストの旅を順調に進め管理していくのに役立つように設計されています。

目的を念頭に置いて始める（ビジネス／ミッションの目的）

ゼロトラストは、善意の者は内部に、悪意ある者は外部にという従来の要塞モデルからのパラダイムシフトです。従来の要塞モデルは、特定の固定された場所に構築された組織で使用される場合にうまく機能しました。今日、組織は分散し、多くの場合、グローバルなエコシステムの中で生きています。ゼロトラストは、組織の分散した従業員と内部と外部を持たない技術モデルにセキュリティアーキテクチャを合わせるように設計されています。

指針となる原則は安定したものであることを認識することが重要です。各組織にとってどのような意味を持ち、どのような価値を提供するかは、国やセクター、個々の組織に特有のものです。

目的を念頭に置いて始めるということは、望む方向と目的地について明確なビジョンを持つということであり、燃え尽き症候群を避けながら、より早く成果を実現することを可能にします。

多くの場合、望まれる成果には以下が含まれます。

- 新たな提案、これまで到達できなかった市場への参入、未知の競争優位性など、合理的なリスクで価値を創造することを可能にします。
- コンプライアンス、サイバーレジリエンス、プライバシーのすべての要件に対応する基盤を確立することで、コンプライアンスにかかるコストを削減します。
- インシデントの影響（コストなど）を軽減します。
- ITの複雑さを軽減し、プロセスの負債を減らします。
- TCOの削減
- サードパーティリスク管理（TPRM）の基盤構築
- 現在および将来の脅威をより防げるであろう、よりレジリエントなガバナンス、リスク管理、コンプライアンス（GRC）プログラム。

複雑にしすぎない

ゼロトラストの核心は、セキュリティアーキテクチャを私たちの働き方や生活様式に合わせる形で長年にわたって適用される原則の集合体である、ということを忘れがちです。ゼロトラスト・ソリューションへの進化は、特に、最も重要な資産を優先して、時間をかけて意図的な段階を踏んでいく場合には、見た目ほど複雑ではありません。最も重要な資産に対処したら、重要度に基づいて残りの資産に移行していきます。

予防的、検知的、是正的（または、リアクティブ）な、実施されテストされたセキュリティコントロールは、ゼロトラストの基礎を形成します。これらの基本は、ゼロトラストの取り組みの成功に不可欠です。

- 最小特権の概念によるアクセス制御（例：予防的）
- 職務の分離（例：予防的）
- セグメンテーション／マイクロセグメンテーション（例：予防的）
- ロギングとモニタリング（例：検知的）
- コンフィギュレーション・ドリフトの修正（例：是正的／リアクティブ）

ゼロトラストは、組織を従来の要塞モデルから現代の組織に共通する分散モデルへと移行させるために、これらの基本原則に基づいています。また、継続的な認証と認可（例：予防的）、ユーザーとエンティティの行動分析（UEBA）（例：検知的）、および動的なポリシー実施ポイント（例：是正的／リアクティブ）を追加することで、コントロールをよりきめ細かく、より繊細にする機会でもあります。

コントロールタイプをゼロトラストのために再作成したり、過度に複雑にしたりする必要はありません。むしろ、既存のコントロールのスピード、パフォーマンス、敏捷性を最適化することができます。

セキュリティの基本が土台となります。「最小特権の原則」と「職務の分離」がその有力な例です。すべてのユーザー（従業員、請負業者、ベンダー）が一意に識別され、その権限が定期的に見直され、必要に応じて更新されるようにすることはもう1つの例です。アイデンティティのライフサイクル管理が鍵となります。

セグメンテーションとマイクロセグメンテーションを組み込むことで、上記のような管理を実施し、インシデントの影響を軽減することができます。自動化により、ルーチンタスクに必要な手作業プロセスを簡素化できます。

製品は優先事項ではない

歴史的に、サイバー関連はすべて技術者の領域でした。技術的な問題を技術で解決するのは当然のことであり、それは通常、製品の購入や、かなりの頻度でコンサルティングサービスにつながります。多くの点で、ゼロトラストは、テクノロジーそのものよりも、人、プロセス、組織の次元に関わるものです。

人、プロセス、組織の側面を考慮せずに製品に大きく依存した戦略は成功しません。ZTの旅を実現するために製品購入だけに依存することは、ZTの旅とは言えません。他の次元に最初に取り組めば、要件をよりよく理解することができ、より強力な長期的ZT戦略をサポートし、必要であれば適切な製品を選択できる可能性が高まります。

アクセスは意図的な行為である

ゼロトラストの主な差別化要因の1つは、物理的またはネットワーク境界に依存しないことです。要塞モデルのような従来のモデルでは、ネットワークへのアクセスを許可されたユーザーは、他の資産へのアクセスを許可するのに十分であるとみなされていました。このような哲学が生まれたのは、創設時に存在したテクノロジーの限界と、境界内に資産を集めることができる世界で活動していたからです。

今日、組織は、リモートワーカー、クラウドなどのサードパーティへの依存度の増加、複雑化するサプライチェーンなど、グローバルな環境の中に存在しています。多くの点で、組織は壁の外に存在するものにより依存しています。

テクノロジーは、物理的な境界やネットワーク境界に依存することよりも良いものができるところまで進歩しています。ゼロトラストは、このようなテクノロジーの進歩を利用して、ユーザーをよりよく識別し、よりきめ細かいアクセス制御の決定をより頻繁に行えるようにします。

今日の世界では、アイデンティティは明示的に検証され、その検証プロセスを経た認可後にのみアクセスが許可されなければなりません。

歴史的には、誰がどの資産にアクセスできるかを決定するのは、主にIT組織に依存してきました。近年では、誰がいつまで何にアクセスできるかを決定するビジネスオーナー（データオーナーなど）やプロセスオーナーへの依存が高まっています。IT組織はますますカストディアン（例：データ・カストディアン）として見られています。

インサイドアウトであり、アウトサイドインではない

インサイドアウト戦略を用いれば、企業方針の書き方は、″何から守ろうとしているのか？″から ″何を守ろうとしているのか？″に変わります。

レガシーセキュリティ・モデルは、強固な外部との境界に依存しています。このようなモデルは、内側にいる者は善人であり、外側にいる者は悪人であると想定しています。過去20年以上にわたって脱境界化[4]が進み、より多くの人や資産が内部よりも外部に存在しています。このことは、アウトサイドインというセキュリティ哲学が、もはや私たちの働き方や生き方にそぐわなくなっていることを意味します。どんな組織にも無限の資源（例：時間、お金、エネルギー）があるわけではないので、私たちは、最も費用対効果の高いところにエネルギーを注ぐ必要があります。

資産の価値は、私たちの努力に優先順位をつけるための指針です。ビジネス・インパクト・アセスメント（BIA）があれば、そこから始めます。そうでない場合は、資産目録を作成し、資産を価値に基づいて分類します。価値の高いものから低いものへと、資産のランクを積み重ね、作業の指針とします。

保護すべき資産とその関係がわかれば、保護サーフェスと攻撃サーフェスの両方を特定することができます。

現代の組織において、私たちが保護しようとしているのは、通常、データ、アプリケーション、資産、サービスです。これらは一般的にDAASと呼ばれています。

- **データ**：流出したり、悪用されたりすると、組織がトラブルに巻き込まれる可能性がある機密データです。一般的に、データが機微と見なされるのは、規制当局などの第三者が機微であると言っているか、知的財産か組織の運営に必要な業務データであるためです。

- **アプリケーション**：ソフトウェア、ハードウェア、および多くの場合インフラストラクチャの集合体であり、それらが協調して一連の要件を満たします。

- **資産**：組織が所有または管理する、価値を提供する資源。資産には、情報技術（IT）、制御・運用技術（OT）、モノのインターネット（IoT）機器（POS端末、SCADA制御、製造システム、医療機器など）が含まれます。

- **サービス**：特定のコストやリスクを所有することなく、組織が望む成果を促進することで、顧客に価値を提供するためのビジネスおよび技術的専門性のアプリケーション。現代の企業では、SaaS（Software-as-a-Service）のようにクラウドベースであったり、API（Application Program Interface）のようにアプリケーション間であったり、DNS（Domain Name System）のよ

[4] https://en.wikipedia.org/wiki/Jericho_Forum

うに一般的な用途であったりします。

キプリング・メソッド（5W1H）は、ポリシーを作成するための標準的なツールです。それはビジネスモデルの中でセキュリティ戦略の整合性を確保するために不可欠です。

以下の質問は、資産のオーナー（ビジネス）と資産のカストディアン（通常はIT）の協力によってのみ答えられます。

- **誰が**その資産にアクセスできるのか？彼らは何をすることができるのか？彼らが本人であることを確認できますか？
- **どの**資産にアクセスしようとしているのか？**どの**ようなアクションが許可されているのか？
- **いつ**許可されたアクセスは始まるのか？**いつ**許可は終了しますか？アクセスが許可される時間は決まっていますか？
- **どこ**にその資産はありますか？特定の場所からしかアクセスできないのか？資産へのアクセスが許可されていない場所がありますか？
- **なぜ**このユーザーはこの資産にアクセスする必要があるのか？資産を保護する理由は、その機微性です。その機微性は、コンプライアンス上の義務によって定義されているのでしょうか？
- **どのように**。資産にアクセスできる方法は限られていますか？

侵害は起こる

サイバーリスクから100%守られていると考えるのは非現実的です。防御者がすべての穴をふさぐことは現実的ではないですが、攻撃者は1つの穴だけ見つければよいのです。ゼロトラスト実装の中核は、資産へのアクセスを許可する前に、主張された身元と許可されたアクセスを直接検証することです。

従来のモデルは、物理的・技術的なコントロールに大きく依存していました。組織はまた、悪意ある者を排除する能力に依存していました。世界がよりデジタル化され、壁がより多くの穴を持つにつれて、世界は侵害が起こるものであると認識するようになりました。侵入は多くの場合、実在する内部関係者を装った外部者によって、時には実際の内部関係者によって行われます。ゼロトラストの役割は、侵害の可能性を減らし、その影響を軽減し、迅速な回復を促進することです。そのためには、より強固なアクセス制御を導入し、潜在的なインシデントの検知に注意を払い、インシデント対応と復旧の計画を立てます。

ほとんどのインシデントが、根本的には人間の問題であることを理解すれば、侵害は必ず起こるものであることが理解できます。セキュアであることに集中する代わりに、実務者の考え方はレジリエンスに切り替わります。インシデントの影響範囲を小さくする鍵は、セグメンテーションとマイクロセグメンテーションです。

セグメンテーションとマイクロセグメンテーションは、企業内を横移動する能力を制限し、悪質な行為の伝播を制限することで、可能性と影響を低減します。例えば、悪質な行為者が有効なユーザーのアカウントを乗っ取ったとしても、セグメンテーションによって、有効なユーザーの領域外にはアクセスできません。マルウェア（例：ランサムウェア）の場合、1台のマシンへの感染が企業全体に無闇に広がることはありません。

より伝統的なセキュリティモデルでは、いったん境界の内側に入れば、信頼され、その境界内であればどこにでも自由に移動できます。旧来のセキュリティアーキテクチャは、キャドバリー・エッグのようなもので、外側は堅く、内側はネバネバしています。スパイがコミュニティに入ってしまえば、堂々と自由に移動できることを想像してみてください。

ゼロトラスト・モデルでは、ユーザーとデバイスはどこにいても信頼されません。あらゆる資産にアクセスする前に、それらを尋問しなければなりません。多くの曲がりくねった道があり、家と家がつながっているヨーロッパの古い都市を想像してください。隣人はお互いを知っています。このような通りに行けば、誰もが不審に思い、尋問を受けます。なぜここにいるのか？何の用だ？泥棒か？観光か？仕事で来たのか？それは一度ではなく、行く先々で起こります。ゼロトラストも同じです。資産へのアクセスが要求されればいつでも、身元が確認され、許可されたアクセスが確認され、やりとりが記録されます。尋問のレベルは、資産の価値とリスク環境に見合ったものです。

考え方の転換により、ZTの旅からの重要な成果を得られます。第一に、発生した場合に（そして、発生するであろう）侵害の影響範囲を限定することができます。第二に、ハッカーが企業内を横方向に移動する能力を低下させます。第三に、一度の出来事で被害を受ける資産を限定することで、影響を軽減します。

取締役会や経営幹部の観点からは、予測可能性こそが重要な成果かもしれません。ユーザーが侵害された場合、潜在的な影響は限定的であることがわかります。影響は、もはや企業全体ではありません。何がリスクなのかを正確に把握することができます。侵害が発生する可能性が100%になることはもはやなく、影響を計算することができないこともはやありません。

アイデンティティ、行動、資産をより効果的に関連付けることができれば、データ損失防止（DLP）の取り組みも大幅に強化されます。定義された境界がないため、DLPはもはや、何が入ってきて何が出ていくかを監視するだけの単純なものではありません。革新的なデータ発見メカニズムを備えたZTの原則を活用することで、潜在的な侵害を事前に検知し、侵害が発生した場合に迅速に対処し、データ損失タスクの管理および運用の複雑さを軽減することができます。

重要なのは、頻繁に、資産の価値に見合った方法で検証することです。ユーザーの行動に異常がないかを探し、悪意のある行為者があなたの資産を狙っていると推定することは、このための不可欠な要素です。

リスク選好を理解する

リスク選好（Risk Appetite）は、リスクマネジメントの概念としてよく知られています。リスク選好とは、組織がその目的を追求する間、受け入れてもよいリスクのレベルです。固有リスクとは、行動（すなわち、対応）をとる前に存在するリスクのレベルです。目的は、リスクをリスク選好以下のレベルまで低減するために、リスク対応を行うことです。これを「受容可能リスク（Acceptable Risk）」といいます。

組織は一枚岩ではありません。組織のさまざまな部分で、許容できるリスクのレベルが異なることはよくあることです。これらは一般にリスク許容度と呼ばれます。例えば、金融サービス会社のベンチャーキャピタル部門は、同じ金融機関の債券部門よりも高いレベルのリスクを許容します。この区別は重要ですが、ゼロトラストの指針となる原則は、リスク選好とリスク許容度に等しく適用されます。読みやすくするため、ここでは区別しません。

ゼロトラストは、発生可能性と[5]影響[6][7]、またはその両方を提言するためのコントロールを実施することにより、固有リスクを許容可能なレベルまで低減します。

CIAの三要素とは、組織が資産に対する潜在的な被害（例えば、影響）を検討するのに役立つように設計された、広く受け入れられている情報セキュリティ（InfoSec）モデルです。完全性を期すため、NISTとISOの定義が含まれています。

1. **機密性**：個人的なプライバシーや専有情報を保護する手段を含め、情報へのアクセスや開示に関する定められた制限を維持すること[8]。

   許可されていない個人、組織、またはプロセスに対して、情報が利用可能になったり、開示されたりしないという性質[9]。

   データの流出は、資産の機密性が失われる例です。

2. **完全性**[10] ：不適切な情報の改ざんや破壊から保護することであり、情報の否認防止と真正性の確保を含みます[11]。
   データが不正な方法で改ざんされたり破壊されたりしていないという性質[12]。

[5] https://csrc.nist.gov/glossary/term/likelihood
[6] https://csrc.nist.gov/glossary/term/impact
[7] ISO31000のリスクマネジメントでは、"結果"という用語を使用しています。
[8] https://csrc.nist.gov/glossary/term/confidentiality
[9] https://www.iso.org/standard/14256.html
[10] ISOには、データ完全性の定義しかありません。
[11] https://csrc.nist.gov/glossary/term/integrity
[12] https://www.iso.org/standard/14256.html

完全性の喪失は、3つの中で最も把握しにくいものです。一般的なルールとして、信頼を失うようなことがあれば、それは完全性への攻撃です。例えば、ファイルがコンピューターウイルスに感染した場合などです。ディープフェイク、ハルシネーション、人工知能（AI）、そしてあらゆる形態の詐欺は、完全性の喪失を伴います。

3. **可用性**：情報への適時で信頼できるアクセスと利用の確保[13]。

   権限を与えられたエンティティが、要求に応じてアクセスでき使用可能であるという性質[14]。

   ランサムウェアは、おそらく資産の可用性を失った結果として最も認識されています。データを暗号化することで、ビジネスはアクセスを拒否されます。水道のようなユーティリティへのアクセスが拒否される場合も、可用性に対する攻撃です。

すべての組織はリスク選好を決定する必要があります。その決定は、単にZTの旅にとどまりません。その旅の一部として、合意されたこと、ゼロトラストの役割、組織が定期的に使用しているツールを理解することをお勧めします。最も一般的なツールはリスク登録簿です。

サイバーリスクは、ビジネスが管理しなければならないリスクのうち、他の多くのリスクに影響を与える可能性がある数少ないリスクの一つであるため、完全に定量化することは困難です。多くの組織では、代わりに定性的な尺度（例：非常に高い、高い、中程度、低い）を選択しています。

また、EUのデジタルオペレーショナルレジリエンス法（DORA[15] ）、ネットワーク及び情報セキュリティ（NIS）指令（NIS2）[16]、NIST SP 800-53[17]、あるいは連邦金融機関検査協議会（FFIEC）が開発したサイバーセキュリティ評価ツール（FFIEC's CAT）[18]のような標準に準拠することを求められている、あるいは選択しているところもあります。

組織によっては、バリュー・アット・リスク（VaR）[19]を計算するために、様々な定量化技術を採用することを選択しています。最も有名なものの一つは、FAIR（Factor Analysis of Information Risk）[20]です。

いずれの戦略を採用するのであっても原則は変わらず、ゼロトラストの核心は、リスクを許容可能なレベルまで低減することです。

[13] https://csrc.nist.gov/glossary/term/availability
[14] https://www.iso.org/standard/14256.html
[15] https://www.digital-operational-resilience-act.com/
[16] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[17] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[18] https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_may_2017.pdf
[19] https://www.investopedia.com/terms/v/var.asp
[20] https://www.fairinstitute.org/

組織は常に進化し続けなければ消滅します。脅威の状況も絶えず進化しているため、組織はリスク選好を絶えず再評価する必要に迫られています。いずれにしても、新たな脆弱性や新たな悪用を発見する可能性があります。

さらに問題を複雑にしているのは、組織が適切に予測したり準備したりできない未知のものが常に存在することです。ランサムウェアはその典型例です。この概念はコミュニティではよく知られていたが、暗号通貨が普及するまでは実用的ではなかったため、主流ではありませんでした。このようなリスクを総称して「未知の未知(unknown-unknowns)」と呼びます。

ゼロトラストの基本的な攻撃と防御の側面は、このような進化や未知の未知に対して組織を将来的に保護するために大いに役立ちます。新たな脅威が現れたり、新たな脆弱性が生まれたり、これまで未知の未知であったものが現れたりした場合、ゼロトラストの中核となる原則は、発生確率または影響（潜在的にはその両方）を低減します。

COVID-19 パンデミック、地政学的動向、サプライチェーン・ショック、インパクトの大きい気候変動事象、重要インフラに対するサイバー脅威の増大は、政府や組織のオペレーショナルレジリエンスに対する見方にパラダイムシフトをもたらしており、自社のリスク許容度を理解し、定量化することの重要性は、今後もますます高まっていくでしょう。すでに、EUのDORAのような新しい法律が世界の他の管轄区域で定義されつつあります。これは、新たなサイバー脅威に絶えず革新し、適応していかなければならない企業のリスク管理実務に長期的な影響を与えるでしょう。

そこでゼロトラストが重要な役割を果たします。少なくとも、組織をよりレジリエントにし、敏捷性を高めることができます。

トップからの方向づけを確保する

ゼロトラストは企業全体での取り組みであり、テクノロジー以上のものであるため、成功させるためには組織のあらゆるレベルの協力が必要です。これは、適切なエグゼクティブ・スポンサーとトップからの明確なメッセージがあって初めて達成できます。適切な人物を任命し、常に情報を提供し続けなければなりません。完璧な世界であれば、シニアリーダーシップは、事業戦略、適切な資本配分、企業方針などとの整合性を含む、ゼロトラストの重大性を積極的に伝えるでしょう。

あらゆる状況において最善なのは、ゼロトラストを取締役会が支援することです。少なくとも、シニアリーダーシップがスポンサーになる必要があります。ゼロトラストの取り組みが事業部または地域に限定されている場合は、ゼロトラストの取り組みは、事業部の代表者または地域内の組織図上のトップ（例：国別代表者）がスポンサーになるのが最も効果的です。

ゼロトラスト活動を成功させるためには、コミュニケーションが重要です。一貫性のある追跡可能な情報の流れを通じて、参加者と利害関係者間の整合性を確保するように構成されたコミュニケーション計画は、ZTの旅の方向付けに役立ちます。

ステークホルダーをマッピングした図は、役割と責任を明確にします。一般にRACI（Responsible, Accountable, Consulted, Informed）図と呼ばれるこの図は、プロジェクトやビジネスプロセスのタスクや成果物を完成させるために、さまざまな役割がどのように関与するかを記述したものです。

リーダーは、ゼロトラスト・モデルを全面的に支持し、組織にとってのその重要性を強調することによって、方向づけるべきです。その重要性を定期的に伝えるべきです。サイバーリスクは全員の責任であることを認識する企業文化を浸透させることも重要です。一部の者の責任ではありません。

ゼロトラスト文化を浸透させる

ゼロトラストは、IT部門や最高情報セキュリティ責任者（CISO）だけの責任ではなく、全員の責任です。ZTの基本原則は、トレーニングと意識向上プログラムに織り込まれるべきです。問題が発生したときにそれを発見し、提起できるように従業員に権限を与えることで、頭痛の種を防ぎ、サイバーレジリエンスを高めることができます。

ゼロトラスト文化とは何か？それは、従業員が何をどの程度まで保護しなければならないかを強く意識する文化です。最も重要なことは、全スタッフがアクセスの認可は決して暗黙の了解ではないことを理解することです。それは意図的な行為です。組織が取引するすべての従業員と個人は、疑わしい活動を特定し、サイバー関連の懸念を適切なチャネルに報告する方法を知っている必要があり、また、特定のセキュリティコントロールが存在している理由を理解している必要があります。ゼロトラスト文化は適応性があり、特定のテクノロジーやアーキテクチャに縛られることはありません。従業員は、現在および将来にわたって最も理にかなった方法で資産を保護する権限を与えられます。

セキュリティは、かつては個別の部門（つまりIT部門）の管轄でしたが、今では広く浸透しています。開発者はそれを受け入れることができます。ビジネスリーダーはそれを受け入れることができます。エンドユーザーは、デバイスとの摩擦のないインタラクションを通じて、その利点を体験することができます。そして何よりも、組織はゼロトラストによってテクノロジーをより賢く活用できるようになることを理解すべきです。この種の文化を採用する際のリスクは、分散した文化的認識が定着する前に、中央集権的なセキュリティ部門の役割を減らしてしまうことにあるかもしれません。

組織内にゼロトラスト文化を浸透させることは、ゼロトラスト・セキュリティ・モデルの理解と受け入れを組織の全レベルで促進することを意味します。

小さく始めて、クイックウィンに集中する

ゼロトラストは戦略であり、特定の製品群ではないため、その基礎となるコンセプト（インサイドアウトからの設計など）に取り組むことで、チームは多額の先行投資をすることなく、段階的に成功を収めることができます。DAASの要素で構成される保護サーフェスを特定し、規模と影響に基づいて優先順位をつけるべきです。

小規模で低コストの保護サーフェスをパイロットとして選択し、その測定基準を活用してセキュリティパラダイムへの変化を強調し、ビジネス価値を実証できるようにすれば、リーダーシップからの賛同を得たり維持したりすることが容易になります[21] 。完全なゼロトラストへの移行は、多くのプラスのビジネス成果をもたらします。より大きな組織にとってのメリットと、すべてのサイバー関連の変更によって削減されたリスクを強調し続けることが重要です。

多くのことを引き受けすぎたり、時間がかかるより大きな勝利を目指したりすると、プロジェクトは泥沼にはまり、組織のゼロトラストへの取り組みは成功ではなく失敗に結びつきます。

継続監視

ゼロトラストは、どの参加者（例：ユーザー、デバイス、サービス、アプリケーション）も暗黙的に信頼されないことを前提としています。その代わり、要求されたIDを受け入れるか、または要求されたアクセスを許可するかの決定は、意図的な行為です。企業リソースへのアクセス要求はすべて、アクセスが許可される前に、未知のソースからのものであるかのように認証され、認可が検証されなければなりません。その場合でも、許可は（永続的ではなく）期間限定です。

悪意ある者は、しばしば正当なユーザーのアカウントを侵害し、悪意ある内部関係者は、しばしば自分たちのニーズに合わせて権限を超えようとすることが知られているため、イベントを監視しログに記録することが重要です。監視は、潜在的な悪意ある行動を早期に発見するために不可欠です。ログ取得は、侵害の指標（IOC）を特定し、影響を判断し、証拠を収集するために不可欠です。監視とログ取得の両方が、継続的な改善を促進します。最終的には組織全体の活動を監督するような監視を行うことが重要です。

ゼロトラスト・インフラの監視と維持には、アクセス権限の定期的な監査、ネットワークの振る舞いの継続的な監視、最新のセキュリティパッチの維持、リスク評価の実施、ユーザーのセキュリティ意識の強化が含まれます。

[21] 攻撃サーフェスと保護サーフェスの詳細な説明は、クラウドセキュリティアライアンス（https://cloudsecurityalliance.org/zt/resources/）が主催するZero Trust Advancement Center Resource Hubに掲載されています。

ゼロトラスト＝境界がない、というのはよくある誤解です。今日の相互接続された世界では、境界はかつてほど明確でも強固でもありません。しかし、悪意ある者を排除し、善意の者だけを入れることを保証する戦略に頼ることができないからといって、私たちは勤勉に努める義務から解放されるわけではありません。その逆で、資産を守るために内部と外部の境目を定義し、監視し、管理することは組織の義務です。

Useful References

- Zero Trust Advancement Center Resource Hub hosted by Cloud Security Alliance, https://cloudsecurityalliance.org/zt/resources/
- US Federal Zero Trust Resource Hub. https://zerotrust.cyber.gov/

Suggested Reading

- National Security Telecommunications Advisory Committee (NSTAC), Report to President on Zero Trust and Trusted Identity Management, 2022 https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf
- Zero Trust Maturity Model Version 2, Cybersecurity and Infrastructure Security Agency (CISA)、2023年4月 https://www.cisa.gov/zero-trust-maturity-model
- Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Press Release for NSA Guidance on Advancing Zero Trust Maturity Throughout the User Pillar, US National Security Agency (NSA), 2023 https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3328152/nsa-releases-recommendations-for-maturing-identity-credential-and-access-manage/
- Advancing Zero Trust Maturity Throughout the User Pillar, National Security Agency (NSA), March 2023 https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF
- Zero Trust Architecture, National Institute of Standards and Technology (NIST), Special Publication 800-207, 2020 https://csrc.nist.gov/publications/detail/sp/800-207/final