NIST Special Publication 800-207

ゼロトラスト・アーキテクチャ

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

本書は、以下より無料で利用可能である:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

邦訳:PwCコンサルティング合同会社

NIST Special Publication 800-207

ゼロトラスト・アーキテクチャ

Scott Rose
Oliver Borchert
Advanced Network Technologies Division
Information Technology Laboratory

Stu Mitchell
Stu2Labs
Stafford, VA

Sean Connelly
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

本書は、以下より無料で利用可能である:
https://doi.org/10.6028/NIST.SP.800-207

August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

発行機関

本文書は、連邦情報セキュリティ近代化法 (FISMA：Federal Information Security Modernization Act) 2014 年、合衆国法典 (U.S. Code) 第44編 第3541条等、および公法 (P.L.) 113条-28 条に基づく法的責任により、米国国立標準技術研究所 (NIST：National Institute of Standards and Technology、以下、NISTと称す) によって作成された。NISTは、連邦政府情報システムの最低限の要求事項を含む情報セキュリティ標準及びガイドラインを策定する責務があるが、このような標準及びガイドラインを国家安全保障システムに適用するには、このようなシステムについての政策的権限を有する適切な連邦政府機関の明確な承認が必要となる。このガイドラインは、行政管理予算庁 (OMB：Office of Management and Budget) による通達 (Circular) A-130 号の要求事項と一致している。

本文書のいかなる内容も、商務長官が法的権限に基づき連邦政府に対して義務及び拘束力を与えた標準及びガイドラインを否定するものではない、また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わるものと解釈したりしてはならない。本文書は、非政府組織が自由に使用することもでき、米国における著作権の対象ではないが、NISTに帰属する。

National Institute of Standards and Technology Special Publication 800-207
Natl. Inst. Stand. Technol. Spec. Publ. 800-207, 59 pages (August 2020)
CODEN: NSPUE2

本書は、以下より無料で利用可能である：
https://doi.org/10.6028/NIST.SP.800-207

本文書中で特定される商業的組織、機器、または資料は、実験的な手順や概念を適切に説明するためのものである。このような特定は、NISTによる推奨または承認を意味するものではなく、これらの組織、機器、または資料が、必ずしもその目的のために利用可能な最善のものであることを意味しているわけではない。

本文書には、NISTに与えられた法的責任に従って現在策定中の他の文書への参照がある場合がある。本書に記載されている情報は、概念及び方法論を含め、そのような関連文書が完成する前であっても、連邦政府機関によって使用される可能性がある。したがって、それぞれの文書が完成するまで、現在の要求事項、ガイドライン、及び手順は、存在する限り効力を有する。連邦政府機関は、計画及び移行の目的のために、NISTによるこれらの新しい文書の策定を綿密に従うことを希望するかもしれない。

パブリックコメント募集期間中に、組織がすべてのドラフト文書をレビューし、NISTへフィードバックを提供することを奨励する。上記以外の多くの NISTサイバーセキュリティ関連文書は、https://csrc.nist.gov/publications において入手可能である。

本文書に対するコメントは以下に提出できる：

National Institute of Standards and Technology
Attn: Advanced Network Technologies Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8920) Gaithersburg, MD 20899-8920
Email: zerotrust-arch@nist.gov

すべてのコメントは、連邦情報公開法 (FOIA ：Freedom of Information Act) の下で開示の対象となる。

コンピュータシステムの技術に関する報告書

NISTの情報技術ラボラトリ (ITL：Information Technology Laboratory) は、米国の度量衡と標準規格に関する基盤において技術的リーダーシップを提供することにより、米国の経済及び社会福祉に貢献している。ITLは、テストの開発、テスト技法の開発、参照データの作成、概念実証の実施及び技術的分析を通じて、情報技術 (IT) の開発と生産的利用の発展に努めている。ITLの責務には、連邦政府の情報システムにおいて、国家安全保障に関連する情報以外の情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、技術面、物理面、管理面及び運用面での標準規格及びガイドラインを策定することが含まれる。Special Publication 800シリーズでは、ITLの学術研究、ガイドラインについて、情報システムセキュリティ及び産業界、政府機関及び学術機関とのその共同活動における支援活動の取り組みとともに報告する。

要旨

ゼロトラスト (ZT) とは、スタティックなネットワークベースの境界線防御から、ユーザ、資産、およびリソースに焦点を当てた防御へと移行する、進化するサイバーセキュリティの一連のパラダイムを指す用語である。ゼロトラスト・アーキテクチャ (ZTA) は、ゼロトラストの概念を利用し、産業や企業のインフラストラクチャとワークフローを計画するものである。ゼロトラストでは、資産やユーザアカウントには、物理的な場所やネットワーク上の位置 (すなわち、ローカルエリアネットワークやインターネット) や資産の所有権 (企業や個人が所有するもの) だけに基づく暗黙の信頼がないことを前提としている。認証と認可 (主体とデバイスの両方) は、企業リソースへのセッションが確立される前に実行される個別の機能である。ゼロトラストは、リモートユーザ、BYOD (Bring Your Own Device) 、企業所有のネットワーク境界内には存在しないクラウドベースの資産等、企業ネットワークの流行に対応したものである。ゼロトラストでは、ネットワークの場所がリソースのセキュリティ態勢の主要な要素とみなされなくなったため、ネットワークセグメントではなく、リソース (資産、サービス、ワークフロー、ネットワークアカウント等) を保護することに焦点を当てている。本文書では、ゼロトラスト・アーキテクチャ (ZTA) の概念的な定義を含み、ゼロトラストが企業の全体的な情報技術セキュリティ態勢を改善する可能性のある一般的な展開モデルとユースケースを示している。

キーワード

アーキテクチャ; サイバーセキュリティ; エンタープライズ; ネットワークセキュリティ; ゼロトラスト

謝辞

本文書は、複数の連邦政府機関間の共同作業の成果物であり、連邦CIO議会によって監督されている。本文書の作成は、アーキテクチャサブグループが担当しているが、称賛に値する特定の人物がいる。Federal CIO Council ZTA プロジェクトのプロジェクトマネージャーである Greg Holden氏、NIST/National Cybersecurity Center of Excellence ZTA のプロジェクトマネージャーである Alper Kerman氏、そして Douglas Montgomery氏である。

対象読者

本文書は、企業のセキュリティアーキテクト向けにゼロトラストを説明することを目的としている。民間の分類されていないシステムに対するゼロトラストの理解を助け、ゼロトラストセキュリティの概念をエンタープライズ環境に移行して展開するためのロードマップを提供することを意図している。組織のサイバーセキュリティ管理者、ネットワーク管理者、責任者は、本文書からゼロトラストとZTAについての洞察を得ることができる。企業には、独自のビジネスユースケースやデータ資産を保護するための措置が必要であるため、ZTAの単一の展開計画を推奨することを意図したものではない。組織のビジネスとデータを十分に理解することから始めることで、ゼロトラストへの強力なアプローチが可能になる。

商標

特許開示通知

注意：情報技術研究所 (ITL) は、本書のガイダンスまたは要件を遵守するために使用許可が必要となる可能性のある特許権者に対して、ITLにそのような特許請求を開示するよう要請してきた。しかし、特許権者はITLの特許募集に応じる義務はなく、ITLは、どの特許がこの出版物に適用されるかを特定するための特許調査を行っていない。

本書のガイダンスまたは要求事項に準拠するために使用許可が必要となる可能性のある特許請求項を特定するためのITLの呼びかけに続いて、そのような特許請求項の1つまたは複数の通知を受領した。

このことを公表することにより、ITLは、特許請求項の有効性や範囲、またはそれに関連する権利の有効性や範囲に関して、いかなる立場もとらない。しかし、既知の特許権者は、次のいずれもないことを記載した保証書をNISTに提出している。(1) 本質的な特許請求項を保有しておらず、現在保有するつもりもない旨の一般的な免責事項、(2) 合理的な条件で、明らかに無差別に他の当事者とロイヤリティーフリーまたはロイヤリティーを支払うライセンスを交渉すること。

詳細は zerotrust-arch@nist.gov から入手できる。

本出版物の使用における特許侵害を回避するために必要とされる唯一のライセンスであることを表明するものではなく、暗示するものでもない。

目次

付録

図

表

1 序章

一般的な企業のインフラストラクチャは、ますます複雑になっている。各企業では、複数の内部ネットワークや独自のローカルインフラストラクチャを持つリモートオフィス、リモートおよび/またはモバイル環境の端末、そしてクラウドサービスを運用するようになった。このような複雑さは簡単に社内外を区別できる単一の境界線を定義することが困難となり、境界防御によるネットワークセキュリティが危殆化している。また、境界防御によるネットワークセキュリティは、一度攻撃者が境界線を突破すると、それ以上の企業内ネットワークの横断移動を妨げることができないため、不十分であることが示されている。

このような複雑なインフラストラクチャを有する組織が、「ゼロトラスト」(ZT) として知られるサイバーセキュリティの新しいモデルの開発を先導している。ZTのアプローチは、主にデータとサービスの保護に焦点を当てているが、すべての企業の資産 (デバイス、インフラストラクチャコンポーネント、アプリケーション、仮想およびクラウドコンポーネント) と主体 (エンドユーザ、アプリケーション、およびリソースから情報をリクエストするその他の端末等) を含むように拡張することが可能/推奨されている。本文書では、各章の内容が直接エンドユーザに関連する場合を除き、「主体 (subject) 」という用語を使用する。ZTセキュリティモデルでは、環境に攻撃者が存在し、組織が所有する環境は、組織が所有しない環境と同様に信頼できるものではないと仮定している。この新しいパラダイムでは、組織は暗黙の信頼を前提とせず、資産やビジネス機能に対するリスクを継続的に分析・評価し、これらのリスクを緩和するための保護策を講じなければならない。ZTでは、これらの保護策は通常、アクセスを必要とするものとして特定された主体や資産へのリソース (データや計算リソース、アプリケーション/サービス等) へのアクセスを最小限に抑え、各アクセスの身元とセキュリティ態勢を継続的に認証し、認可することを含んでいる。

ゼロトラスト・アーキテクチャ (ZTA) は、ZTの原則に基づいた組織向けのサイバーセキュリティアーキテクチャであり、データ侵害を防止し、内部ネットワーク上の水平移動 (ラテラルムーブメント) 移動を制限するように設計されている。本書では、ZTAやその論理的なコンポーネント、想定される展開シナリオおよび脅威について説明している。また、ゼロトラストを構築しようとしている組織のための一般的なロードマップを示し、ゼロトラスト・アーキテクチャに影響を与える可能性のある関連する連邦政府のポリシーについても説明している。

ZTは、単一のアーキテクチャではなく、ワークフロー、システム設計、および運用のための一連の基本原則であり、あらゆる分類や機密レベルのセキュリティ態勢を向上に活用できる[FIPS199] 。ZTAへの移行は、組織がそのミッションにおけるリスクをどのように評価するかに関する道筋であり、技術の全面的な置き換えで単純に達成することはできない。とはいえ、多くの組織は、今日の組織におけるインフラストラクチャで既にZTAの要素を保有している。組織は、ゼロトラストの原則、プロセスの変更、およびデータ資産とビジネス機能を保護する技術的な施策を、ユースケースごとに段階的に導入することを目指すべきである。ほとんどの企業におけるインフラストラクチャは、IT近代化イニシアチブへの投資を継続し、組織のビジネスプロセスを改善しながら、ゼロトラストと既存の境界ベースの防御策を平行して運用されるであろう。

組織は、ゼロトラストを効果的に実現するためには、包括的な情報セキュリティ施策を実施し、レジリエンスを考慮した設計を実現する必要がある。既存のサイバーセキュリティポリシーとガイダンス、アイデンティティとアクセス管理、継続的な監視、ベストプラクティスとのバランスが取れていれば、ZTAは脅

威から守ることができ、リスクマネジメントのアプローチにより組織のセキュリティ態勢を向上させることができる。

1.1 連邦政府機関に関連したゼロトラストの取り組みの歴史

ゼロトラストという概念は、「ゼロトラスト」という言葉が生まれる以前からサイバーセキュリティに存在している。国防情報システム庁 (DISA) と国防総省は、「ブラックコア」[BCORE] と呼ばれる、より安全な組織戦略に関する研究を発表した。ブラックコアでは、境界線ベースのセキュリティモデルから、個々のトランザクションのセキュリティに焦点を当てたモデルへの移行が行われた。2004年に開催されたジェリコフォーラムでは、ネットワークの位置情報に基づく暗黙の信頼を制限し、大規模なネットワークセグメント上の単一の静的な防御に頼ることの限界を考慮して、境界線を除去するという考え方が公表された [JERICHO] 。非境界化の概念は進化し、後に当時Forrester社所属のJohn Kindervag氏[1]によって、より大きなゼロトラストの概念へと改良された[2]。ゼロトラストはその後、ネットワークの位置に基づく暗黙の信頼からセキュリティを離れ、代わりにトランザクション単位での信頼の評価に焦点を当てたさまざまなサイバーセキュリティソリューションを説明するために使用される用語となった。民間企業も高等教育機関も、境界線ベースのセキュリティからゼロトラストの原則に基づくセキュリティ戦略へと進化を遂げてきた。

連邦政府機関は、10年以上前からゼロトラスト原則に基づくセキュリティへの移行を促しており、連邦情報セキュリティマネジメント法 (FISMA) 、リスクマネジメントフレームワーク (RMF) 、Federal Identity Credential Access Management (FICAM) 、Trusted Internet Connections (TIC) 、継続的診断および対策 (CDM) プログラム等の機能とポリシーを構築してきた。これらのプログラムはすべて、データとリソースへのアクセスを許可された当事者に制限することを目的としている。これらのプログラムが開始された当初は、情報システムの技術的限界による制約があった。セキュリティポリシーは大部分が静的で、企業が最大の効果を得るために制御できる大規模な「チョークポイント」で実施されていた。技術が成熟するにつれ、アクセスリクエストを継続的に分析し、動的かつ粒度の高い方法で評価することが可能になってきており、「アクセスの必要性」に基づいて、侵害されたアカウント、ネットワークを監視する攻撃者、およびその他の脅威によるデータの漏洩を緩和することができる。

1.2 本文書の構成

本文書は以下のように整理されている。

- 第2章では、ZTとZTAを定義し、企業向けにZTを設計する際のいくつかの前提条件をリストアップしている。また、この章では、ZT設計の理念リストも掲載している。
- 第3章では、ZTの論理コンポーネント (ビルディングブロック) について説明する。ユニークな実装では、同じ論理機能を提供しながらも、ZTAコンポーネントの構成が異なる可能性がある。

[1] https://go.forrester.com/blogs/next-generation-access-and-zero-trust/

[2] NISTの文書内で市販の製品やサービスについて言及しているものは、情報提供のみを目的としたものであり、NISTによる推奨や推奨を意味するものではない。

- 第4章では、ZTAによって企業環境がより安全になり、悪用されにくくなる可能性のあるユースケースをいくつか挙げている。これらには、遠隔にいる従業員、クラウドサービス、ゲストネットワークを持つ企業が含まれる。

- 第5章では、ZTAを使用している企業に対する脅威について説明する。どのようなアーキテクト化されたネットワークにおいても、これらの脅威の多くは似ているが、異なる緩和技術が必要になる場合がある。

- 第6章では、連邦政府機関のための既存のガイダンスにZTAの考え方がどのように適合するか、あるいは補完するかを論じている。

- 第7章は、企業 (連邦政府機関等) をZTAに移行するための出発点を示している。これには、ZTの理念に導かれたアプリケーションと企業インフラストラクチャの計画と展開に必要な一般的なステップの説明が含まれている。

2 ゼロトラストの基本

ゼロトラストは、リソースの保護に焦点を当てたサイバーセキュリティのパラダイムであり、信頼は決して暗黙のうちに与えられるものではなく、継続的に評価されなければならないという前提に基づいている。ゼロトラスト・アーキテクチャは、企業リソースとデータセキュリティに対するエンドツーエンドのアプローチであり、アイデンティティ (個人またはノンパーソンエンティティ) 、クレデンシャル、アクセス管理、運用、エンドポイント、ホスティング環境、および相互に接続されたインフラストラクチャを網羅している。最初の焦点は、アクセスを必要とする者にリソースを制限し、業務遂行に必要な最低限の権限 (例：読み取り、書き込み、削除) のみを付与することにある。これまで、政府機関 (および一般的な企業ネットワーク) では、ネットワークの境界防御に重点を置いており、認証された主体には、内部ネットワークに入った後、広範なリソースの集まりにアクセスする権限が与えられている。その結果、環境内での不正な水平移動 (ラテラルムーブメント) は、連邦政府機関にとって最大の課題の一つとなっている。

Trusted Internet Connections (TIC) や境界線上のファイアウォールは、強力なインターネットゲートウェイを提供する。これにより、インターネットからの攻撃者をブロックするのに役立つが、TICや境界線上のファイアウォールは、ネットワーク内部からの攻撃を検出してブロックするのにはあまり役に立たず、組織の境界外の主体 (例：リモートワーカー、クラウドベースのサービス、エッジデバイス) を保護することはできない。

ゼロトラストとゼロトラスト・アーキテクチャの定義は以下の通り。

> *ゼロトラスト* (ZT) は、ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断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集合体のことである。*ゼロトラスト・アーキテクチャ* (ZTA) は、ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシー等を含むサイバーセキュリティ計画のことである。従って、ゼロトラスト企業とは、ゼロトラスト・アーキテクチャ計画の産物として、組織のネットワークインフラストラクチャ (物理的および仮想的) と運用ポリシーを指す。

企業は、ゼロトラストをコア戦略として採用することを決定すると、ゼロトラストの原則 (下記第2.1項を参照) を念頭に置いて開発された計画として、ゼロトラスト・アーキテクチャを生成する。この計画は、企業内で使用するためのゼロトラスト環境を構築するために展開される。

この定義は、*データおよびサービスへの不正アクセスを防止し、アクセス制御の実施を可能な限り詳細化すること*を目的としている。つまり、許可される承認された主体 (ユーザ、アプリケーション/サービス、デバイスの組み合わせ) は、他のすべての主体 (すなわち、攻撃者) を排除してデータにアクセスすることができる。これをさらに一歩進めて、「データ」という言葉を「リソース」に置き換えることで、ZTとZTAは単なるデータアクセスではなく、リソースアクセス (例：プリンタ、計算リソース、Internet of Things [IoT] アクチュエータ) という意味にもなる。

完全に排除することが困難な不確実性を減少させるために、認証、認可、暗黙のトラストゾーンの縮小に焦点を当て、可用性を維持し、認証メカニズムの時間的な遅延を最小化する。アクセスルールは、リクエストのアクションを実行するのに必要な最小限の権限を強制するために、可能な限り細かく設定されている。

図1に示すアクセスの概念図では、主体は企業リソースへのアクセスを必要とする。アクセスは、ポリシー決定ポイント (PDP) と対応するポリシー実施ポイント (PEP) を介して付与される[3]。

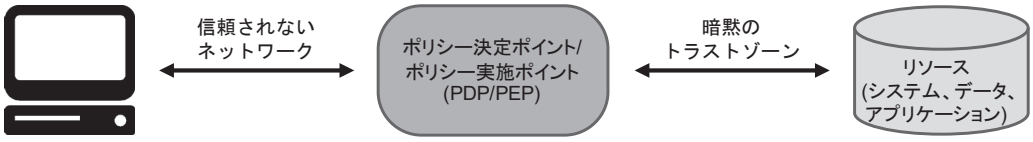

図 1：ゼロトラストアクセス

このシステムでは、主体が真正であり、リクエストが有効であることを確認しなければならない。PDP/PEPは、主体がリソースにアクセスすることを許可するために適切な判断を下す。これは、ゼロトラストが認証と認可という二つの基本的な領域に適用されることを意味している。このユニークなリクエストに対する主体の身元に関する信頼度はどの程度か？主体の身元に対する信頼度を考慮した場合、リソースへのアクセスは許可されるか？リクエストに使用されるデバイスは適切なセキュリティ対策がなされているか？考慮すべき他の要因があり、信頼度を変化させる要因 (例：時間、主体の場所、主体のセキュリティ態勢) はあるか？全体として、企業は、リソースアクセスのための動的なリスクベースのポリシーを開発・維持し、これらのポリシーが個々のリソースアクセスリクエストに対して正しく一貫して実施されることを保証するためのシステムを構築する必要がある。つまり、企業は、主体が基本的な認証レベル (例：資産へのログイン) を満たしていれば、それ以降のすべてのリソースリクエストが同様に有効であると仮定される暗黙の信頼性に頼るべきではない。

「暗黙のトラストゾーン」は、すべてのエンティティが、少なくとも最後のPDP/PEPゲートウェイのレベルまで信頼されている領域を表している。例えば、空港における乗客の検閲モデルを考えてみる。すべての乗客は、空港のセキュリティチェックポイント (PDP/PEP) を通過して搭乗ゲートにアクセスする。乗客、空港職員、航空機乗務員等がターミナルエリア内をうろうろしており、すべての個人が信頼されていると考えられる。このモデルでは、暗黙のトラストゾーンは搭乗エリアである。

PDP/PEPは、PEPを超えたすべてのトラフィックが共通の信頼レベルを持つように、一連の制御を適用する。PDP/PEPは、トラフィックの流れの中でその位置を超えて追加のポリシーを適用することはできない。PDP/PEPが可能な限り特定のポリシーを適用できるようにするためには、暗黙のトラストゾーンを可能な限り小さくする必要がある。

ゼロトラストは、PDP/PEPをリソースに近づけるための一連の原則と概念を提供する。この考え方は、企業を構成するすべての主体、資産、ワークフローを明示的に認証し、承認することである。

[3] OASIS XACML 2.0で定義された概念の一部 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

2.1 ゼロトラストの考え方

ZTの多くの定義や議論では、広域の境界防御 (例：企業におけるファイアウォール) を除去するという概念が要因として強調されている。しかし、これらの定義のほとんどは、ZTAの機能能力の一部として、何らかの形で (マイクロセグメンテーションやマイクロペリメータ等；第3.1節を参照) ペリメータに関連するものと定義し続けている。以下では、何が除外されるかではなく、むしろ関与すべき基本的な理念の観点から、ZTおよびZTAを定義しようとする試みである。これらの理念は理想的な目標であるものの、与えられた戦略に対してすべての理念がその純粋な形で完全に実装されるとは限らないことを認識しなければならない。

ゼロトラスト・アーキテクチャは、以下のゼロトラストの基本的な考え方を遵守して設計され、展開される。

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をリソースとみなす**
   ネットワークは、複数のクラスのデバイスで構成されている場合がある。ネットワークに、アグリゲータ/ストレージにデータを送信する小さいデバイス、SaaS、アクチュエータに命令を送信するシステム、およびその他の機能がある場合もある。また、企業が所有するリソースにアクセスできる場合、個人所有のデバイスをリソースとして分類することも考えられる。
2. **ネットワークの場所に関係なく、すべての通信を保護する**
   ネットワークの場所だけでは信頼を意味するものではない。企業所有のネットワークインフラストラクチャ上にある資産 (例：レガシーネットワーク境界内) からのアクセスリクエストは、企業所有でない他のネットワークからのアクセスリクエストや通信と同じセキュリティ要件を満たす必要がある。言い換えれば、デバイスが企業所有のネットワークインフラストラクチャ上にあるからといって、自動的に信頼が付与されるべきではない。すべての通信は、機密性と完全性を保護し、アクセス元に対する認証を提供し利用可能な最も安全な方法で行われる必要がある。
3. **企業リソースへのアクセスは、セッション単位で付与する**
   アクセスが許可される前に、アクセス元の信頼性が評価される。また、アクセスは、タスクを完了するために必要な最小限の権限で付与されるべきである。これは、この特定のトランザクションについては「最新のいつか」という意味でしかなく、セッションを開始する前、またはリソースとのトランザクションを実行する前に直接発生しない場合もある。しかし、あるリソースへの認証と認可が自動的に別のリソースへのアクセスを許可するわけではない。
4. **リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する**
   組織は、どのようなリソースを持っているか、そのメンバーが誰であるか (またはコミュニティにおけるユーザに関する認証) 、およびそれらのメンバーが必要とするリソースへのアクセスを定義することで、リソースを保護する。ゼロトラストの場合、クライアントアイデンティティには、ユーザアカウント (またはサービスアイデンティティ) と、企業がそのアカウントに割り当てた関連属性、または自動化されたタスクを認証するための機能を含めることができる。リクエストする資産の状態には、インストールされているソフトウェアのバージョン、ネットワークの場所、リクエストの日時、以前に観察された動作、インストールされているクレデンシャル等のデバイスの特性を含めることができる。行動属性には、自動化された主体の分析、デバイスの分析、および観察された使用パターンからの測定された逸脱が含まれるが、これらに限定されない。ポリシーとは、組織が主体、データ資産、またはアプリケーションに割り当てる属性に基づくアクセスルールのセットである。環境属性には、アクセス元のネットワークの場所、時間、報告されたアクティブな攻撃等が含まれる。これらのルールと属性は、ビジネスプロセスのニーズと許容

可能なリスクレベルに基づいている。リソースのアクセスとアクションの許可ポリシーは、リソース/データの機密性に基づいて変化する。最小特権の原則により、可視性とアクセス性の観点から制限する。

5. **すべての資産の整合性とセキュリティ動作を監視し、測定する**
   資産は本質的に信頼されない。企業は、リソースへのリクエストを評価する際に、資産に対し実施されているセキュリティ態勢を考慮する。ZTAを実装する企業は、デバイスやアプリケーションの状態を監視するために、継続的診断および対策 (CDM) または同様のシステムを確立し、必要に応じてパッチを当て、修正する必要がある。侵害されていることが判明した既知の脆弱性を有する資産、および企業が管理していない資産は、最も安全な状態にあると考えられる企業が所有している、または企業に関連するデバイスとは異なる扱い (企業リソースへのすべての接続を拒否することを含む) を受ける可能性がある。これは、一部のリソースへのアクセスが許可されていても、他のリソースへのアクセスが許可されていない関連デバイス (例：個人所有のデバイス) にも適用される可能性がある。この場合も、企業リソースの現在の状態に関する実用的なデータを提供するために、堅牢な監視および報告システムが必要となる。
6. **すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する**
   これは、アクセスを取得し、脅威をスキャンして評価/適応し、継続的なコミュニケーションの中で信頼を継続的に再評価するという一定のサイクルである。ZTAを導入する企業は、Identity Credential and Access Management (ICAM) と資産管理システムを導入することが推奨される。これには、一部またはすべての企業リソースへのアクセスに多要素認証 (MFA) を使用することも含まれる。セキュリティ、可用性、ユーザビリティ、およびコスト効率のバランスを達成するポリシー (例：時間ベース、新規リソースのリクエスト、リソースの変更、主体の異常な活動の検出) によって定義し、再認証および再認証の可能性を伴う継続的な監視をユーザトランザクション全体にわたって実施する。
7. **資産、ネットワークインフラストラクチャ、通信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利用する**
   企業は、資産に対するセキュリティ態勢、ネットワークトラフィック、アクセスリクエストに関するデータを収集し、そのデータを処理し、得られた洞察をポリシーの作成と実施を改善するために使用するべきである。このデータは、主体からのアクセスリクエストのコンテキストを提供するためにも使用できる。(第3.3.3.1節を参照)。

上記ZTの原則は、各技術にとらわれない設計となっている。例えば、「ユーザ識別 (ID) 」には、ユーザ名/パスワード、証明書、ワンタイムパスワード等のいくつかの要素が含まれる。これらの原則は、組織内で行われる作業、または一つ以上のパートナー組織との連携で行われる作業に適用され、匿名の公開または利用者に面したビジネスプロセスには適用されない。組織は、外部アクター (例：顧客や一般的なインターネットユーザ等) に内部ポリシーを課すことはできないが、組織と特別な関係を持つ非企業ユーザ (例：登録顧客、従業員の扶養家族) にZTベースのポリシーを実装することはできるかもしれない。

2.2 ネットワークのゼロトラスト観点

ネットワークの計画と展開にZTAを利用する組織では、ネットワーク接続に関する基本的な前提条件がいくつかある。これらの前提条件の一部は、企業が所有するネットワークインフラストラクチャに適用され、一部は非企業所有のネットワークインフラストラクチャ (例：公衆Wi-Fiまたは公衆クラウドプロバイダ) に適用される。これらの前提条件は、ZTAの形成を指示するために使用される。ZTAを実装する企業ネットワークは、上記で概説したZTAの原則と、以下の前提条件に基づいて構築する必要がある。

1. **企業のプライベートネットワークは、暗黙のトラストゾーンとみなさない**
   資産は常に攻撃者が企業ネットワーク上に存在すると考えるべきであり、通信は利用可能な最も安全な方法で行われるべきである (第2.1項2を参照)。これには、すべての接続を認証したり、すべてのトラフィックを暗号化したりすることが含まれる。
2. **ネットワーク上のデバイスは、企業が所有していないか、構成可能なものではない場合がある**
   社外の訪問者や契約サービスには、その役割を果たすためにネットワークアクセスを必要とする非企業所有の資産が含まれている場合がある。これには、企業主体が所有していないデバイスを使用して企業リソースにアクセスできるようにするBYOD (Bring-your-own-device) ポリシーが含まれる。
3. **どんなリソースも本質的に信頼されるものではない**
   すべての資産は、企業が所有するリソースへのリクエストが許可される前に、PEPを通じてそのセキュリティ態勢を評価されなければならない (情報資産と主体については第2.1項6と同様)。この評価は、セッションが続く限り、継続的に行われるべきである。企業所有のデバイスは、認証を可能にし、非企業所有のデバイスから送られてくる同じリクエストよりも高い信頼度を提供する成果物を持つかもしれない。企業リソースへの認証には、主体のクレデンシャルだけでは不十分である。
4. **すべての企業リソースが企業のインフラストラクチャ上にあるわけではない**
   リソースには、クラウドサービスだけでなく、企業の外に存在する主体も含まれる。企業が所有または管理する資産は、基本的な接続性とネットワークサービス (例：DNS解決) のためにローカル (すなわち、非企業) ネットワークを利用する必要がある場合がある。
5. **リモートの企業主体と資産は、ローカルネットワークの接続を完全に信頼できない**
   リモートの主体は、ローカル (すなわち、企業が所有しない) ネットワークが敵対的であると仮定し、資産は、すべてのトラフィックが監視され、変更される可能性があると仮定する必要がある。すべての接続リクエストは認証/承認されるべきであり、すべての通信は可能な限り最も安全な方法で行われるべきである (すなわち、機密性、完全性の保護、およびソース認証を提供する)。上記のZTAの原則を参照すること。
6. **企業のインフラストラクチャと非企業のインフラストラクチャとの間で移動する資産とワークフローには、一貫したセキュリティポリシーが必要**
   資産およびワークロードが企業のインフラストラクチャを移動するときには、セキュリティ対策を維持する必要がある。これには、企業ネットワークから外部組織のネットワークに移動するデバイス (リモートユーザ等) も含まれる。また、オンプレミスのデータセンターから外部組織のクラウドインスタンスに移行するワークロードも含まれる。

3 ゼロトラスト・アーキテクチャの論理的構成要素

企業におけるZTA導入を構成する論理コンポーネントは数多くある。これらのコンポーネントは、オンプレミスまたはクラウドベースのサービスを介して運用される。図2の概念フレームワークモデルは、コンポーネントとその相互作用の基本的な関係を示している。これは、論理的なコンポーネントとその相互作用を示す理想的なモデルであることに注意すること。図1から、ポリシー決定ポイント (PDP) は、ポリシーエンジンとポリシーアドミニストレータ (以下に定義) の二つの論理コンポーネントに分解される。アプリケーションデータがデータプレーン上で通信されるのに対し、ZTAの論理コンポーネントでは別個のコントロールプレーンを使用して通信する (第3.4節を参照)。

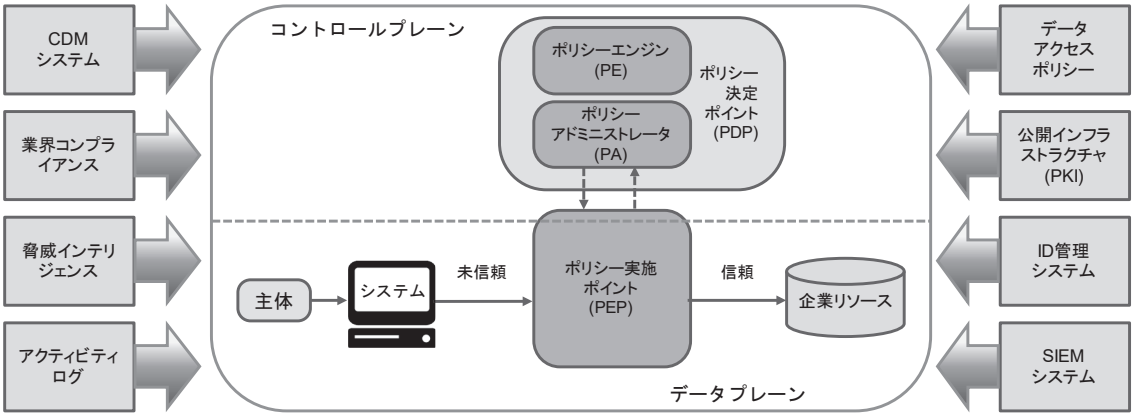

図 2：ゼロトラストの中核となる論理コンポーネント

以下は、コンポーネントの説明である。

- **ポリシーエンジン (PE)** ：このコンポーネントは、指定された主体のリソースへのアクセスを許可するための最終的な決定を行う。PEは、外部ソース (例：CDMシステムや後述の脅威インテリジェンスサービス) からの入力と同様に、企業のポリシーを使用して、リソースへのアクセスを許可したり、拒否したり、取り消したりするために、トラストアルゴリズム (第3.3節を参照) への入力として使用する。PEはポリシーアドミニストレータと対になっている。ポリシーエンジンは決定 (承認または拒否) を行い、ログに記録し、ポリシーアドミニストレータはその決定を実行する。
- **ポリシーアドミニストレータ (PA)** ：このコンポーネントは、(関連するPEPへのコマンドを介して) 主体とリソース間の通信経路の確立や遮断を行う役割がある。PAは、クライアントが企業リソースにアクセスするために使用するセッション固有の認証、認証トークンまたはクレデンシャルを生成する。PAは、PEと密接に結びついており、最終的にセッションを許可または拒否するかはPEの判断に依存する。セッションが許可され、リクエストが認証されると、PAはPEPを設定してセッションの開始を許可する。セッションが拒否された場合 (または以前の承認がキャンセルされた場合) 、PAはPEPに接続を遮断するように命令する。実装によっては、PEとPAを単一のサービスとして扱う場合もある；ここでは、それは二つの論理コンポーネントに分割されている。

PAは、通信パスを作成する際にPEPと通信する。この通信は、コントロールプレーンを介して行われる。

- **ポリシー実施ポイント (PEP)** :このシステムは、主体と企業リソース間の接続を有効にし、監視し、最終的に接続を終了する役割を担う。PEPはPAと通信して、リクエストを転送したり、PAからポリシーの更新を受信したりする。これはZTAにおける単一の論理コンポーネントであるが、クライアント側 (例:ノートパソコン上のエージェント) とリソース側 (例:リソースの前にあるアクセスを制御するゲートウェイコンポーネント) 、または通信経路のゲートキーパーとして機能する単一のポータルコンポーネントの二つの異なるコンポーネントに分割することができる。PEPの先には、企業リソースをホストするトラストゾーン (第2章を参照) がある。

ZTAを実装している企業のコアコンポーネントに加えて、いくつかのデータソースが、アクセスの決定を行う際にポリシーエンジンが使用する入力とポリシールールを提供する。これらのデータソースには、ローカルのデータソースだけでなく、外部 (すなわち、企業が制御していない、または企業が作成したものではない) のデータソースも含まれる。これらには、以下のようなものがある。

- **継続的診断および対策 (CDM) システム**:企業の資産の現在の状態に関する情報を収集し、構成およびソフトウェアコンポーネントに更新を適用する。企業のCDMシステムは、適切なパッチ適用済みオペレーティングシステム (OS) を実行しているかどうか、企業が承認したソフトウェアコンポーネントの完全性や承認されていないコンポーネントの存在、資産に既知の脆弱性があるかどうか等、アクセスリクエストを行っている資産に関する情報をポリシーエンジンに提供する。CDMシステムはまた、企業のインフラストラクチャ上でアクティブな非企業のデバイスのポリシーのサブセットを特定し、潜在的に実施する役割も担っている。
- **業界のコンプライアンスシステム**:これは、企業が該当する可能性のある規制体制 (例:FISMA、医療、金融業界の情報セキュリティ要件) に準拠していることを保証する。これには、企業がコンプライアンスを確保するために策定するすべてのポリシールールが含まれる。
- **脅威インテリジェンスフィード**:ポリシーエンジンがアクセスの判断を下すのに役立つ内部または外部ソースからの情報を提供する。これらは、内部および/または複数の外部ソースからデータを取得し、新たに発見された攻撃や脆弱性に関する情報を提供する複数のサービスである可能性がある。これには、新たに発見されたソフトウェアの欠陥、新たに特定されたマルウェア、およびポリシーエンジンが企業資産からのアクセスを拒否したい他の資産への攻撃の報告も含まれる。
- **ネットワークおよびシステムのアクティビティログ**:企業のシステムは、資産ログ、ネットワークトラフィック、リソース・アクセス・アクション、およびその他のイベントを集約し、企業情報システムのセキュリティ対策に関するリアルタイム (または、ほぼリアルタイム) のフィードバックを提供する。
- **データアクセスポリシー**:これらは、企業リソースへのアクセスに関する属性、ルール、およびポリシーのことである。この一連のルールは、 管理インターフェースを介して エンコードされている場合と、ポリシーエンジンによって動的に生成されている場合がある。これらのポリシーは、企業内のアカウントやアプリケーション/サービスの基本的なアクセス権限を提供するため、リソースへのアクセスを許可するための出発点となる。これらのポリシーは、組織の定義されたミッションロールとニーズに基づいている必要がある。

- **企業の公開鍵基盤 (PKI)** :このシステムは、企業がリソース、主体、サービス、およびアプリケーションに対して発行した証明書を生成し、ログを取得する役割を担う。これには、グローバルな証明書機関のエコシステムや連邦PKI[4]も含まれ、企業のPKIと統合されている場合もあれば、統合されていない場合もある。これは、X.509証明書に基づいて構築されていないPKIである可能性もある。
- **ID管理システム**:これは、企業のユーザアカウントおよびアイデンティティレコード (例: Lightweight Directory Access Protocol (LDAP) サーバ) の作成、保存、管理の役割を担うこのシステムには、必要な主体者情報 (例:名前、電子メールアドレス、証明書) や、役割、アクセス属性、割り当てられた資産等の他の企業特性が含まれている。このシステムは、ユーザアカウントに関連付けられた成果物のために他のシステム (PKI等) を利用することが多い。このシステムは、より大きな連合コミュニティの一部である可能性があり、企業以外の従業員や、共同作業のための企業以外の資産へのリンクを含む可能性がある。
- **セキュリティ情報およびイベント管理 (SIEM) システム**:これは、後に分析するために、セキュリティ中心の情報を収集する。このデータは、ポリシーを改善し、企業の資産に対する攻撃の可能性を警告するために使用できる。

3.1 ゼロトラスト・アーキテクチャのアプローチのバリエーション

企業がZTAのワークフローを実施するには、いくつかの方法がある。これらのアプローチは、使用するコンポーネントと組織のポリシールールにより異なる。各アプローチは、ZTの理念を実装しているが (第2.1節を参照) 、一つまたは二つ (または単一コンポーネント) をポリシーの主要な要素として使用することができる。完全な ZTソリューションには、三つのアプローチすべての要素が含まれる。アプローチには、拡張されたアイデンティティガバナンス、論理的マイクロセグメンテーション、およびネットワークベースセグメンテーションが含まれる。

特定のアプローチは、他のユースケースよりもいくつかのユースケースに適している場合がある。企業向けにZTAを開発しようとしている組織は、選択したユースケースと既存のポリシーが、他のアプローチよりも一つのアプローチを指すことに気づくかもしれない。それは他のアプローチが機能しないことを意味するのではなく、むしろ他のアプローチを実装することがより困難であり、企業が現在のビジネスフローを実施する方法に対してより根本的な変更を必要とする可能性があることを意味する。

3.1.1 拡張されたアイデンティティガバナンスを利用したZTA

ZTAを開発するための拡張されたアイデンティティガバナンスによるアプローチでは、ポリシー作成の重要な要素としてアクターのアイデンティティを使用する。企業リソースへのアクセスをリクエストする主体がいなければ、アクセスポリシーを作成する必要はない。このアプローチでは、企業リソースのアクセスポリシーは、アイデンティティと割り当てられた属性に基づいている。リソースアクセスの主な要件は、指定された主体に付与されたアクセス権限に基づいている。使用されているデバイス、資産の状態、および環境要因等の他の要因は、最終的な信頼度計算 (および最終的なアクセス権限) を変更したり、ネットワークの場所に基づいて特定のデータソースへの部分的なアクセスのみを許可する等、何らかの方法で結果を調整したりする可能性がある。個々のリソースまたはPEPリソースを保護するコンポーネントは、アクセスを許可する前に、ポリシーエンジンにリクエストを転送するか、主体を認証してリクエストを承認する方法を持っていなければならない。

[4] https://www.idmanagement.gov/topics/fpki/

企業向けに拡張されたアイデンティティガバナンスのアプローチは、オープンネットワークモデルや、社外の訪問者によるアクセスやネットワーク上の企業以外のデバイスが頻繁に使用される企業ネットワークを使用して採用されることが多い (第4.3節 ユースケースを参照)。ネットワークアクセスは、はじめにすべての資産に付与されるが、企業リソースへのアクセスは、適切なアクセス権限を持つアイデンティティに制限される。基本的なネットワーク接続を許可することには、悪意のある行為者がネットワークの偵察を試みたり、ネットワークを使用して内部またはサードパーティに対するサービス拒否攻撃を実行したりする可能性があるという欠点がある。企業は、ワークフローに影響を与える前に、そのような行動を監視して対応する必要がある。

デバイスのアイデンティティとステータスがアクセス決定のための二次的なサポートデータを提供するため、アイデンティティ駆動型アプローチは、リソースポータルモデル (第3.2.3節を参照) とうまく機能する。配置されているポリシーに応じて、他のモデルも同様に機能する。アイデンティティ駆動型のアプローチは、企業が所有または運営するZTセキュリティコンポーネントを使用できない可能性のあるクラウドベースのアプリケーション/サービスを使用する企業 (多くのSaaSオファリング等) にも有効である。企業は、リクエストしている主体のアイデンティティを使用して、これらのプラットフォーム上でポリシーを策定し、実施することができる。

3.1.2 マイクロセグメンテーションを利用したZTA

企業は、ゲートウェイのセキュリティコンポーネントによって保護された固有のネットワークセグメント上に、個々またはグループのリソースの配置に基づき、ZTAを実装することを選択するかもしれない。このアプローチでは、企業は、インテリジェントスイッチ (またはルータ) 、次世代ファイアウォール (NGFW) 、または特殊用途のゲートウェイデバイス等のインフラストラクチャデバイスを配置して、各リソースまたは関連するリソースの小グループを保護するPEPとして機能させる。あるいは（また追加で）、企業は、ソフトウェアエージェント (第3.2.1節を参照) やエンドポイントの資産上のファイアウォールを使用して、ホストベースのマイクロセグメンテーションを実装することを選択することもできる。これらのゲートウェイデバイスは、クライアント、資産、またはサービスからの個々のリクエストへのアクセスを動的に許可する。モデルによっては、ゲートウェイは単独のPEPコンポーネントであるか、またはゲートウェイとクライアント側エージェントで構成されるマルチパートPEPの一部である場合がある (第3.2.1節を参照)。

このアプローチは、保護するデバイスがPEPとして機能し、デバイスの管理がPE/PAコンポーネントとして機能するため、さまざまなユースケースと展開モデルに適用される。このアプローチは、アイデンティティガバナンスプログラム (IGP) が完全に機能する必要であるが、ゲートウェイコンポーネントに依存して、不正アクセスや探索からリソースを保護するPEPとして機能する。

このアプローチに必要なのは、PEPコンポーネントが管理されており、脅威やワークフローの変化に対応するために、必要に応じて反応したり再構成したりできることである。あまり高度でないゲートウェイデバイスやステートレスファイアウォールを使用することで、マイクロセグメント化された企業のいくつかの機能を実装することは可能であるが、管理コストと変化に迅速に適応することの難しさから、この方法は非常に悪い選択となる。

3.1.3 ネットワークインフラとSoftware Defined Perimeterを利用したZTA

最後のアプローチは、ネットワークインフラストラクチャを使用してZTAを実装する。ZTAの実装は、オーバーレイネットワーク (すなわち、OSI参照モデルのレイヤ7を指すが、より下位に設定することも可能)。これらのアプローチはSoftware Defined Perimeter (SDP) アプローチと呼ばれることもあり、

ソフトウェア定義ネットワーク (SDN) [SDNBOOK] やインテントベースネットワーキング (IBN) [IBNVN] の概念を頻繁に含んでいる。このアプローチでは、PAはネットワークコントローラとして機能し、PEによる決定に基づいてネットワークをセットアップし、再構成する。クライアントは、PAコンポーネントによって管理されるPEPを介してアクセスをリクエストし続ける。

このアプローチがアプリケーション層 (すなわち、レイヤ7) で実装される場合、最も一般的な展開モデルはエージェント/ゲートウェイである (第3.2.1節を参照)。この実装では、エージェントとリソースゲートウェイ (単一のPEPとして動作し、PAによって構成される) は、クライアントとリソース間の通信に使用される安全なチャネルを確立する。このモデルには、クラウド仮想ネットワーク、非IPベースのネットワーク等、他のバリエーションがあるかもしれない。

3.2 抽象的なアーキテクチャの展開されたバリエーション

上記の構成要素はすべて論理構成要素である。それらは必ずしも固有のシステムである必要はない。単一の資産が複数の論理コンポーネントの職務を実行してもよく、同様に、論理コンポーネントは、タスクを実行するための複数のハードウェアまたはソフトウェア要素から構成されてもよい。例えば、企業の管理されたPKIは、デバイスの証明書発行を担当する一つのコンポーネントと、エンドユーザへの証明書発行に使用されるもう一つのコンポーネントで構成されていてもよいが、両方とも同じ企業のルート証明書局から発行された中間証明書を使用する。現在市販されているいくつかのZT製品では、PEとPAのコンポーネントが単一のサービスに組み合わされている。

アーキテクチャの選択されたコンポーネントの展開にはいくつかのバリエーションがあり、以下のセクションで概説する。企業ネットワークの設定方法によっては、一つの企業内で異なるビジネスプロセスに複数のZTA展開モデルが使用されている場合がある。

3.2.1 デバイスエージェント/ゲートウェイベースの展開

この展開モデルでは、PEPは、リソース上に存在するコンポーネントと、リソースの前に直接配置されたコンポーネントの二つに分けられる。例えば、各企業発行の資産には、接続を調整するデバイスエージェントがインストールされており、各リソースには、リソースがゲートウェイとのみ通信するように直接リソースの前に配置されたコンポーネント (すなわち、ゲートウェイ) があり、基本的にはリソースのプロキシとして機能する。エージェントは、リクエストが評価されるように、いくつか (またはすべて) のトラフィックを適切なPEPに向けるソフトウェアコンポーネントである。ゲートウェイはポリシーアドミニストレータと通信し、ポリシーアドミニストレータによって設定された承認済み通信パスのみを許可する役割を担う (図3を参照)。

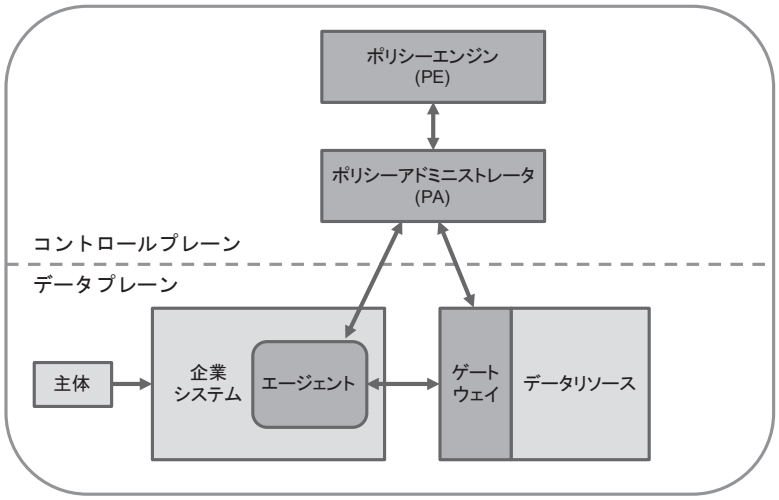

図 3：デバイスエージェント/ゲートウェイモデル

典型的なシナリオでは、企業支給のノートパソコンを持つ主体が、企業リソース (例：人事アプリケーション/データベース) へ接続する場合、リクエストはローカルエージェントによってポリシーアドミニストレータに転送される。ポリシーアドミニストレータとポリシーエンジンは、企業のローカルの資産であっても、クラウド上のサービスであっても構わない。ポリシーアドミニストレータは、評価のためにリクエストをポリシーエンジンに転送する。リクエストが許可された場合、ポリシーアドミニストレータは、コントロールプレーンを介してデバイスエージェントと関連するリソースゲートウェイとの間の通信チャネルを構成する。これには、インターネットプロトコル (IP) アドレス、ポート情報、セッションキー、または同様のセキュリティアーティファクト等の情報が含まれる。デバイスのエージェントとゲートウェイが接続し、暗号化されたアプリケーション/サービスのデータフローが開始される。デバイスエージェントとリソースゲートウェイ間の接続は、ワークフローが完了したとき、またはセキュリティイベント (例：セッションのタイムアウト、再認証の失敗) のためにポリシーアドミニストレータによってトリガーされたときに終了する。

このモデルは、ゲートウェイと通信できる個別のリソースだけでなく、堅牢なデバイス管理プログラムを導入している企業に最適である。クラウドサービスを多用する企業の場合、これはクラウドセキュリティアライアンス (CSA) のSoftware Defined Perimeter (SDP) [CSA-SDP] のクライアントサーバ実装である。このモデルは、BYODポリシーを導入したくない企業にも適している。アクセスは、企業保有の資産上に設置可能なデバイスエージェントを介してのみ可能である。

3.2.2 エンクレーブベースの展開

この展開モデルは、上記のデバイスエージェント/ゲートウェイモデルのバリエーションである。このモデルでは、ゲートウェイコンポーネントは資産や個々のリソースの前にあるのではなく、図4に示すように、リソースエンクレーブ (例：オンロケーションデータセンター) の境界にある。通常、これらのリソースは単一のビジネス機能を提供したり、ゲートウェイと直接通信できたりしない場合がある (例：ゲートウェイと通信するために使用でき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] を持たないレガシーデータベースシステム)。この展開モデルは、単一のビジネスプロセス (例：ユーザ通知、データベース検索、給与支払い) にクラウドベースのマイクロサービスを使用する企業にとっても有用である。このモデルでは、プライベートクラウド全体がゲートウェイの後ろに配置されている。

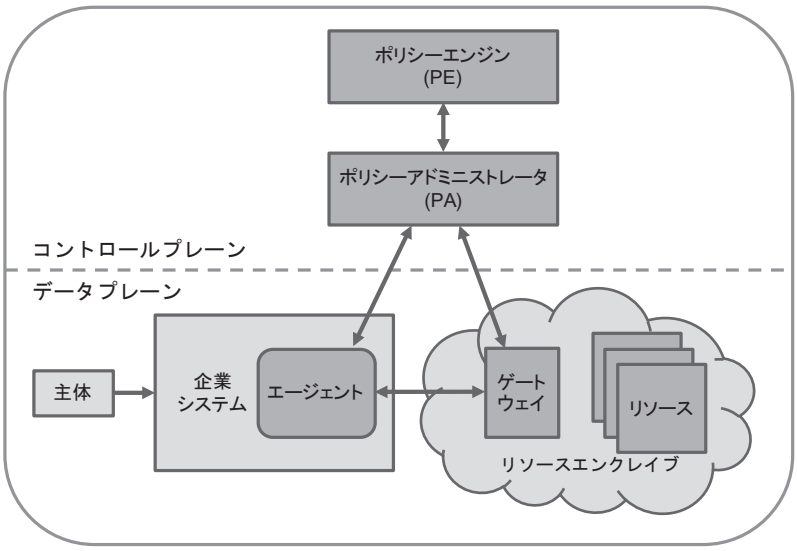

図4：エンクレイブゲートウェイモデル

このモデルは、デバイスエージェント/ゲートウェイモデルとのハイブリッドである可能性がある。このモデルでは、企業の資産には、エンクレイブゲートウェイに接続するために使用されるデバイスエージェントがあるが、これらの接続は、基本的なデバイスエージェント/ゲートウェイモデルと同じプロセスを使用して作成される。

このモデルは、個別のゲートウェイを設置できないレガシーアプリケーションやオンプレミスのデータセンターを持つ企業にとって有用である。企業は、デバイスエージェントをインストール/構成するために、堅牢な資産および構成管理プログラムを必要とする。デメリットは、ゲートウェイがリソースの集合体を保護するため、個々のリソースを個別に保護できない可能性があることである。また、これにより、主体がアクセス権限のないリソースを見るかもしれない。

3.2.3 リソースポータルベースの展開

この展開モデルでは、PEPは、主体からのリクエストのゲートウェイとして機能する単一のコンポーネントである。ゲートウェイポータルは、個々のリソースのためのものであっても、単一のビジネス機能に使用されるリソースの集合体のためのセキュアエンクレーブであってもよい。一例として、図5に示すように、レガシーアプリケーションを含むプライベートクラウドまたはデータセンターへのゲートウェイポータルがある。

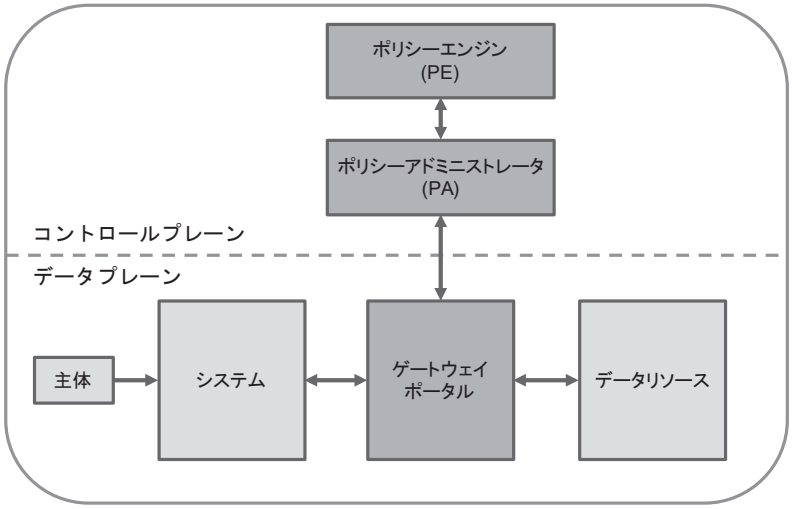

図 5:リソースポータルモデル

このモデルの主な利点は、ソフトウェアコンポーネントをすべてのクライアントデバイスにインストールする必要がないことである。また、このモデルは、BYODポリシーや組織間のコラボレーションプロジェクトに対しても柔軟性がある。企業の管理者は、使用前に各デバイスが適切なデバイスエージェントを持っていることを確認する必要はない。しかし、アクセスをリクエストするデバイスからは、限られた情報を推測することができる。このモデルは、資産とデバイスがPEPポータルに接続した後にのみスキャンと分析が可能となるため、マルウェア、パッチされていない脆弱性、および適切な構成について継続的に監視することができない場合がある。

このモデルの主な違いは、リクエストを処理するローカルエージェントが存在しないことで、企業は、ポータルに接続したときにしか資産を見たりスキャンしたりできないため、それらの完全な可視性や任意の制御ができないかもしれない。企業は、軽減または補償するために、ブラウザの分離等の手段を採用できるかもしれない。これらの資産は、これらのセッションの間、企業からは見えなくなるかもしれない。このモデルはまた、攻撃者がポータルを発見してアクセスを試みたり、ポータルに対するサービス拒否 (DoS) 攻撃を試みたりすることを可能にする。ポータルシステムは、DoS攻撃やネットワークの混乱に対して可用性を提供するために、十分なプロビジョニングを行う必要がある。

3.2.4 デバイスアプリケーションのサンドボックス化

エージェント/ゲートウェイ展開モデルのもう一つのバリエーションは、資産上でコンパートメント化されて実行される審査済みのアプリケーションやプロセスである。これらのコンパートメントは仮想マシン、コンテナ、または他の実装を使用することができるが、目的は同じである。侵害された可能性のあるホストや資産上で実行されている他のアプリケーションからのアプリケーションインスタンスを保護することである。

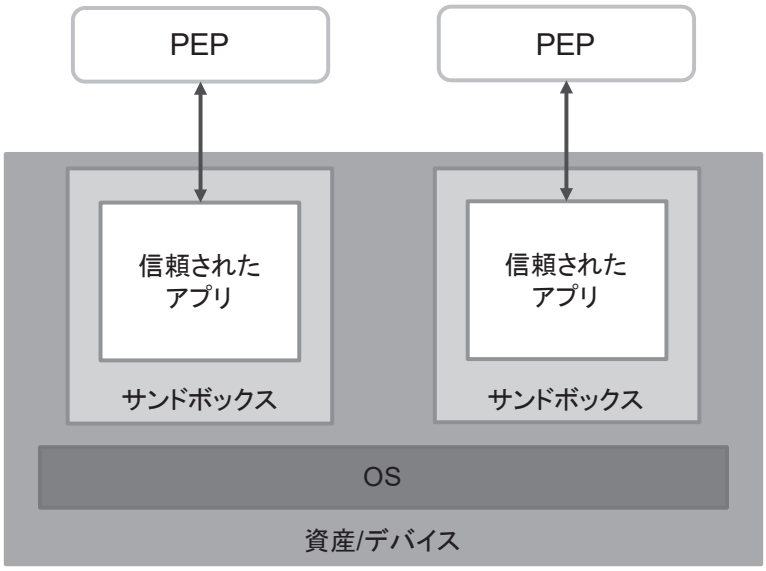

図 6：アプリケーションのサンドボックス

図6では、主体となるデバイスは、サンドボックス内で承認済みかつ検証済みアプリケーションを実行している。アプリケーションはPEPと通信してリソースへのアクセスをリクエストできるが、PEPは資産上の他のアプリケーションからのリクエストを拒否する。PEPは企業のローカルサービスまたはクラウドサービスになる可能性がある。

このモデルの主な利点は、個々のアプリケーションが資産の残りの部分からセグメント化されていることである。資産の脆弱性がスキャンできない場合、これらの個別のサンドボックス化されたアプリケーションは、ホスト資産上の潜在的なマルウェア感染から保護される可能性がある。このモデルのデメリットの一つは、企業はすべての資産に対してこれらのサンドボックス化されたアプリケーションを維持しなければならず、クライアント資産に対する完全な可視性が得られない可能性があることである。また、企業は各サンドボックス化されたアプリケーションが安全であることを確認する必要があり、単にデバイスを監視するよりも多くの努力が必要になる可能性がある。

3.3 トラストアルゴリズム

ZTAを導入している企業にとって、ポリシーエンジンは頭脳であり、PEのトラストアルゴリズムはその主要な思考プロセスであると考えることができる。トラストアルゴリズム (TA) は、ポリシーエンジンがリソースへのアクセスを最終的に許可するか否かを決定するために使用するプロセスである。ポリシーエンジンは、複数のソース (第3章を参照) からの入力を受ける：主体と主体の属性と役割、主体の過去の行動パターン、脅威インテリジェンスソース、およびその他のメタデータソースである。このプロセスは、図7に示す通り、大まかなカテゴリにグループ化できる。

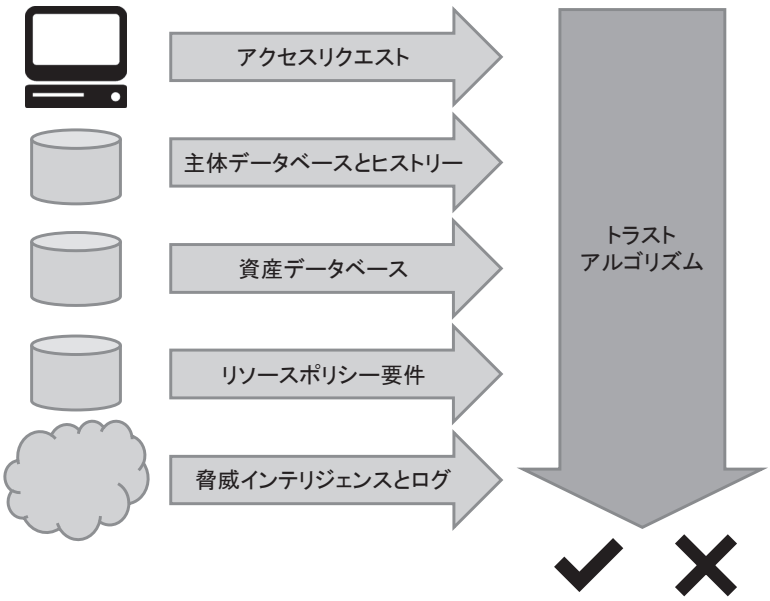

図 7:トラストアルゴリズムの入力

図7では、入力はトラストアルゴリズムに何を提供するかに基づいてカテゴリ分けしている。

- **アクセスリクエスト**:これは主体からの実際のリクエストのことである。リクエストされたリソースが主に使用される情報であるが、リクエスト元に関する情報も使用される。これには、OSのバージョン、使用されているソフトウェア (例:リクエストするアプリケーションが承認済みアプリケーションリストに存在しているか？) 、およびパッチレベル等が含まれる。これらの要因や資産のセキュリティ態勢によっては、資産へのアクセスが制限されたり、拒否されたりする場合がある。
- **主体データベース**:これは、リソースへのアクセスをリクエストしている「誰か」のことである [SP800-63]。これは、企業またはコラボレーターの主体 (人間とプロセス) のセットであり、主体の属性/権限が割り当てられている。これらの主体と属性は、リソースアクセスのためのポリシーの基準を形成する [SP800-162] [NISTIR 7987]。ユーザアイデンティティは、論理的なアイデンティティ (例:アカウントID) とPEPによって実行される認証チェックの結果の組み合わせを含むことができる。信頼度を導出する際に考慮することができるアイデンティティの属性には、時間と地理的位置が含まれる。複数の主体に与えられる特権の集合は、役割と考えることができるが、特権は、組織内の特定の役割に適合する可能性があるという理由だけではなく、個々の主体に個別に割り当てられるべきである。この集合、エンコードされ、ID管理システムおよびポリシーデータベースに格納されるべきである。これには、いくつかの (TA) 変種における過去に観測された主体の行動に関するデータも含まれる (第3.3.1節を参照)。
- **資産データベース (および観測可能なステータス)** :これは、各企業が所有する (場合によっては非企業/BYOD) 資産 (物理的および仮想的、ある程度の範囲) の既知のステータスを格納したデータベースである。これは、リクエストを行った資産の観測可能な状態と比較され、OSのバージョン、ソフトウェアの存在、その完全性、位置 (ネットワークの位置とジオロケーション) 、およびパッチレベルの情報が含まれている。

このデータベースと比較した資産の状態によっては、資産へのアクセスが制限または拒否されることがある。

- **リソース要件**:この一連のポリシーは、ユーザIDと属性データベースを補完 [SP800-63] し、リソースへのアクセスのための最低限の要件を定義する。要件には、MFAネットワークロケーション (例:海外IPアドレスからのアクセスを拒否する) 、データの機密性、および資産構成のための要求等の認証保証レベルが含まれている場合がある。これらの要件は、データ保管者 (すなわち、データの責任者) と、データを利用するビジネスプロセスの責任者 (すなわち、ミッションの責任者) の両方によって開発されるべきである。
- **脅威インテリジェンス**:これは、インターネット上で動作している一般的な脅威やアクティブなマルウェアに関する情報フィードである。これには、疑わしいと思われるデバイスからの通信に関する特定の情報も含まれる (マルウェアのコマンドおよび制御ノードの可能性のあるクエリ等)。これらのフィードには、外部サービスや内部のスキャンや発見が含まれており、攻撃シグネチャや軽減策が含まれている場合もある。これは、企業ではなくサービスの管理下にある可能性が高い唯一のコンポーネントである。

各データソースの重要度の重みづけは、独自のアルゴリズムでも、個々企業により設定されても良い。これらの重み値は、企業にとってのデータソースの重要性を反映するために使用することができる。

最終的な決定は、実行のためにPAに渡される。PAの仕事は、認可された通信を可能にするために必要なPEPを構成することである。ZTAがどのように配置されているかによっては、認証結果と接続設定情報をゲートウェイやエージェント、またはリソースポータルに送信する必要がある。また、PAは、ポリシー要件に従って接続を再認証して再認可するために、通信セッションを保留または一時停止することもできる。また、PAは、ポリシーに基づいて接続を終了するためのコマンドを発行する責任がある (例:タイムアウト後、ワークフローが完了したとき、セキュリティアラートによるもの)。

3.3.1 トラストアルゴリズムのバリエーション

TAを実施するためには、さまざまな方法がある。さまざまな実施者は、上記の要因の重要性の認識に応じて、上記の要因を別々の方法で評価したいと考えるかもしれない。TAを差別化するために使用できる主な特徴が他に二つある。一つ目は、要因がどのように評価されるかである。それは、二値判定としてか、全体の「スコア」や信頼度の重み付けされたとしてかである。二つ目は、同じ主体、アプリケーション/サービス、デバイスによる他のリクエストとの関連で、リクエストがどのように評価されるかである。

- **基準ベース vs. スコアベース**:基準ベースのTAは、リソースへのアクセスが許可されたり、アクション (例:読み取り/書き込み) が許可されたりする前に、満たされなければならない属性のセットを想定している。これらの基準は企業によって設定され、各リソースに独立して設定されるべきである。すべての基準が満たされた場合にのみ、アクセスが許可されたり、アクションがリソースに適用されたりする。スコアベースのTAは、各データソースの値と企業が設定した重みに基づいて信頼度を計算する。スコアがリソースに対して構成されたしきい値よりも大きい場合、アクセスが許可されるか、アクションが実行される。

そうでない場合は、リクエストが拒否されるか、アクセス権限が減少する (例：ファイルの読み取りアクセスは許可されているが、書き込みアクセスは許可されていない)。

- **単一的 vs. 文脈的**：単一的なTAは、各リクエストを個別に扱い、評価の際に主体の履歴を考慮しない。これにより、より迅速な評価が可能になるが、攻撃が主体の許可された役割の範囲内に留まると、検出されないリスクがある。文脈的なTAは、アクセスリクエストを評価する際に、主体またはネットワークエージェントの最近の履歴を考慮に入れる。これは、PEがすべての主体とアプリケーションの状態情報を保持していなければならないことを意味するが、PEが特定の主体に対して見ているパターンとは異なるパターンで情報にアクセスするために、不正なクレデンシャルを使用している攻撃者を検出する可能性が高めるかもしれないことを意味する。これはまた、PEは、主体が通信する際に対話するPA (および PEP) によって、ユーザの行動を知らされなければならないことを意味する。主体の行動の分析は、許容される利用のモデルを提供するために使用することができ、この行動から逸脱した場合には、追加の認証チェックやリソースリクエストの拒否を引き起こす可能性がある。

二つの要素は常に互いに依存しているわけではない。すべての主体および/またはデバイスに信頼度を割り当て、すべてのアクセスリクエストを独立して (すなわち、単数で) 考慮するTAを持つことは可能である。しかし、文脈的なTAでは、スコアがリクエストしたアカウントの現在の信頼度を提供し、人間の管理者によって修正される静的なポリシーよりも、変化する要因に迅速に適応するため、より動的で粒度の高いアクセス制御を提供する能力を提供することができる。

理想的には、ZTAのトラストアルゴリズムは文脈に沿ったものであることが望ましいが、企業が利用できるインフラストラクチャコンポーネントでは常に可能とは限らない。コンテキストに基づいたTAは、攻撃者が侵害された対象アカウントや内部攻撃のための「通常の」アクセスリクエストのセットに近い位置に留まる脅威を軽減することができる。トラストアルゴリズムを定義して実装する際には、セキュリティ、ユーザビリティ、および費用対効果のバランスをとることが重要である。組織内のミッション機能や役割に対する過去の傾向や規範と一致する行動に対して、主体に再認証を継続的に促すと、ユーザビリティの問題が発生する可能性がある。例えば、ある組織の人事部の従業員が通常の業務で20～30件の従業員記録にアクセスする場合、文脈的なTAは、アクセスリクエストが突然1日で100件を超えた場合にアラートを送信することがある。また、通常の営業時間後に誰かがアクセスリクエストを行った場合、攻撃者が侵害された人事アカウントを使用して記録を流出させた可能性があるため、文脈的なTAはアラートを送信することもある。これらの例は、単一のTAでは新しい行動を検出できないかもしれないのに対し、文脈的なTAでは攻撃を検出することができる。別の例では、通常は営業時間中に財務システムにアクセスする会計士が、真夜中に認識できない場所からシステムにアクセスしようとしているとする。文脈的なTAは、アラートをトリガーし、NIST Special Publication 800-63A [SP800-63A] に概説されているように、より厳格な信頼度またはその他の基準を満たすことを主体に要求する場合がある。

各リソースの基準または重み/閾値のセットを開発するには、計画とテストが必要である。企業の管理者は、ZTAの初期導入時に、承認されるべきアクセスリクエストが誤った設定のために拒否されるという問題に遭遇する可能性がある。これは、導入の初期の「調整」段階で発生することになる。企業のビジネスプロセスが機能するようにしながら、ポリシーが確実に適用されるように、基準またはスコアリングの重みを調整する必要があるかもしれない。このチューニングフェーズがどのくらいの期間必要かは、

進捗状況に関する企業によって定義するメトリックスと、ワークフローで使用されるリソースの誤ったアクセス拒否/許可の許容範囲によって異なる。

3.4 ネットワーク/環境構成要素

ZT環境では、ネットワークの制御と構成に使用される通信フローと、企業の実業務を行うのに使われるアプリケーション/サービス通信フローの分離 (論理的または物理的) が必要である。これはしばしば、ネットワーク制御通信のためのコントロールプレーンと、アプリケーション/サービス通信フローのためのデータプレーンに分解される [Gilman] 。

コントロールプレーンは、さまざまなインフラストラクチャコンポーネント (企業所有のものとサービスプロバイダからのものの両方) が、資産の維持と構成、リソースへのアクセスの判断、許可、または拒否、およびリソース間の通信パスを設定するために必要な操作を実行するために使用される。データプレーンは、ソフトウェアコンポーネント間の実際の通信に使用される。この通信チャネルは、コントロールプレーンを介してパスが確立される前にはできない場合がある。例えば、コントロールプレーンは、PAおよびPEPによって、主体と企業リソース間の通信パスを設定するために使用される。その後、アプリケーション/サービスのワークロードは、確立されたデータプレーンパスを使用することになる。

3.4.1 ZTAをサポートするためのネットワーク要件

1. **企業の資産は、基本的なネットワーク接続を備えること**
   企業が管理しているかどうかにかかわらず、ローカルエリアネットワーク (LAN) は基本的なルーティングとインフラストラクチャ (例：DNS) を提供する。リモートの企業の資産は、必ずしもすべてのインフラストラクチャサービスを使用するとは限らない。

2. **企業が所有または管理している資産と、デバイスの現在のセキュリティ態勢を区別すること**
   これは、企業が発行したクレデンシャルと、認証できない情報 (例：なりすましが可能なネットワークMACアドレス) を使用しないことによって決定される。

3. **企業はすべてのネットワークトラフィックを監視すること**
   企業はすべてのパケットに対してアプリケーション層 (すなわちOSI参照モデルのレイヤ7) の検査を行うことができない場合でも、データプレーン上で検出されたパケットを記録する。企業は、接続に関するメタデータ (例：アクセス先、時刻、デバイスアイデンティティ) をフィルタリングして、ポリシーを動的に更新し、アクセスリクエストを評価する際にPEに通知する。

4. **企業リソースは、PEPにアクセスしないと到達できないこと**
   企業リソースは、インターネットからの任意の着信接続を受け入れない。リソースは、クライアントが認証され認可された後にのみ、カスタム設定された接続を受け入れる。これらの通信パスは、PEPによって設定される。リソースは、PEPにアクセスしなければ発見できない場合もある。これにより、攻撃者がPEPの背後にあるリソースをスキャンしてターゲットを特定したり、DoS攻撃を仕掛けたりすることを防ぐ。すべてのリソースをこの方法で隠すべきではないことに注意すること。一部のネットワークインフラストラクチャコンポーネント (例：DNSサーバ) はアクセス可能でなければならない。

5. **データプレーンとコントロールプレーンは論理的に分離すること**
   ポリシーエンジン、ポリシーアドミニストレータ、およびPEPは、論理的に分離されており、企業の資産やリソースから直接アクセスできないネットワーク上で通信する。データプレーンは、アプリケーション/サービスのデータトラフィックのために使用される。

ポリシーエンジン、ポリシーアドミニストレータ、およびPEPは、資産間の通信パスを通信し、管理するためにコントロールプレーンを使用する。PEPは、データプレーンとコントロールプレーンの両方からメッセージを送受信できなければならない。

6. **企業資産は、PEPコンポーネントに到達できること**
   企業の主体は、リソースへのアクセスを得るために、PEPコンポーネントにアクセスできなければならない。これは、接続を可能にする企業資産上のウェブポータル、ネットワークデバイス、またはソフトウェアエージェントの形をとることができる。

7. **PEPは、ビジネスフローの一部としてポリシーアドミニストレータにアクセスする唯一のコンポーネントであること**
   企業ネットワーク上で動作する各PEPは、クライアントからリソースへの通信パスを確立するために、ポリシーアドミニストレータへの接続を持っている。すべての企業のビジネスプロセストラフィックは、一つ以上のPEPを通過する。

8. **リモートの企業資産は、企業のネットワークインフラストラクチャを最初にトラバースすることなく、企業リソースにアクセスできるようにすべきである**
   例えば、リモートの主体は、企業によって利用され、パブリッククラウドプロバイダによってホストされているサービス (例：電子メール) にアクセスするために、企業ネットワーク (すなわち、仮想プライベートネットワーク [VPN]) へのリンクバックを使用する必要はない。

9. **ZTAアクセス決定プロセスをサポートするために使用されるインフラストラクチャは、プロセス負荷の変化を考慮して拡張可能なものにすべきである**
   ZTAで使用されるPE、PA、およびPEPは、あらゆるビジネスプロセスの重要な構成要素となる。PEPに到達するまでの遅延や到達不能 (またはPEPがPA/PEに到達不能) は、ワークフローの実行能力に悪影響を及ぼす。ZTAを実装する企業は、予想されるワークロードに合わせてコンポーネントを提供するか、必要に応じて使用量の増加に対応できるようにインフラストラクチャを迅速に拡張できる必要がある。

10. **企業の資産は、ポリシーまたは観測可能な要因により、特定のPEPに到達できない場合がある**
    例えば、リクエストする資産が企業の本国以外に位置している場合、モバイル資産が特定のリソースに到達できない可能性があるというポリシーがあるかもしれない。これらの要因は、場所 (地理的またはネットワークの位置) 、デバイスの種類、またはその他の基準に基づく可能性がある。

4 導入シナリオ/ユースケース

どのような企業環境でも、ゼロトラストを念頭に置いて設計することができる。ほとんどの組織では、既に企業のインフラストラクチャにゼロトラストの要素を導入しているか、情報セキュリティとレジリエンスについてのポリシーとベストプラクティスを導入しているところである。
いくつかの展開シナリオとユースケースは、ゼロトラスト・アーキテクチャに容易に適合できる。例えば、ZTAは、地理的に分散している組織や移動性の高い従業員を抱える組織にルーツを持っている。一方で、どのような組織でもゼロトラスト・アーキテクチャの恩恵を受けることができる。

以下のユースケースでは、企業は境界ベースのインフラストラクチャとZTAインフラストラクチャの両方を持っている可能性が高いため、ZTAは明示的に示されていない。第7.2節で説明したように、企業内でZTAコンポーネントと境界ベースのネットワークインフラストラクチャが同時に運用されている期間が存在する可能性が高い。

4.1 遠隔地に設備を所有する企業

最も一般的なシナリオは、本社と一つ以上の地理的に分散した拠点が、企業所有の物理ネットワーク接続によって接続されていない場合である (図8を参照)。遠隔にいる従業員は、企業所有のローカルネットワークを完全に使用できなくても、タスクを実行するために企業リソースにアクセスする必要がある場合がある。企業は、企業の本社ネットワークに繋がるMPLS (Multiprotocol Label Switch) リンクを持っているかもしれないが、すべてのトラフィックに対して十分な帯域幅を持っていない場合や、クラウドベースのアプリケーション/サービス向けのトラフィックが企業の本社ネットワークを通過することを望まない場合がある。同様に、従業員が在宅勤務をしたり、遠隔にいて、企業所有のデバイスや個人所有のデバイスを使用したりする場合もある。このような場合、企業は一部のリソース (例：従業員のカレンダー、電子メール) へのアクセスを許可しながら、より機密性の高いリソース (例：人事データベース) へのアクセスを拒否したり、を制限したりしたい場合がある。

このユースケースでは、PE/PAをクラウドサービス (通常、優れた可用性を提供し、リモートワーカーが企業のインフラストラクチャに依存してクラウドリソースにアクセスする必要がない) としてホストすることがしばしばあり、終端の資産にエージェントをインストールしたり (第3.2.1 節を参照) または終端の資産からリソースポータルにアクセスしたりする (第3.2.3 節を参照) 。リモートオフィスやリモートワーカーは、クラウドサービスによってホストされているアプリケーションやサービスにアクセスするために、すべてのトラフィックを企業ネットワークに送り返さなければならないため、PE/PAを企業のローカルネットワーク上でホストするのは、最も応答性を犠牲にする可能性がある。

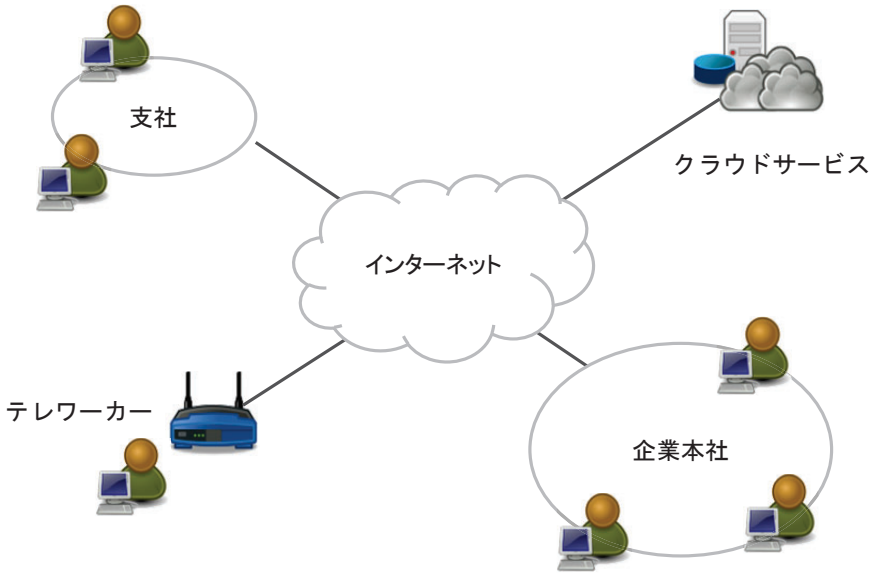

図8：遠隔地にいる従業員がいる企業

4.2 企業のマルチクラウド/Cloud to Cloud環境

ZTAを導入するための一般的なユースケースとして、複数のクラウドプロバイダを利用する企業が増えている (図9を参照)。このユースケースでは、企業はローカルネットワークを持っているが、アプリケーション/サービスやデータをホストするために二つ以上のクラウドサービスプロバイダを使用している。アプリケーション/サービスは、データソースとは別のクラウドサービス上でホストされることもある。パフォーマンスと管理の容易さのために、クラウドプロバイダAでホストされているアプリケーションは、企業ネットワークを介してアプリケーションをトンネルバックさせるのではなく、クラウドプロバイダBでホストされているデータソースに直接接続できるようにする必要がある。

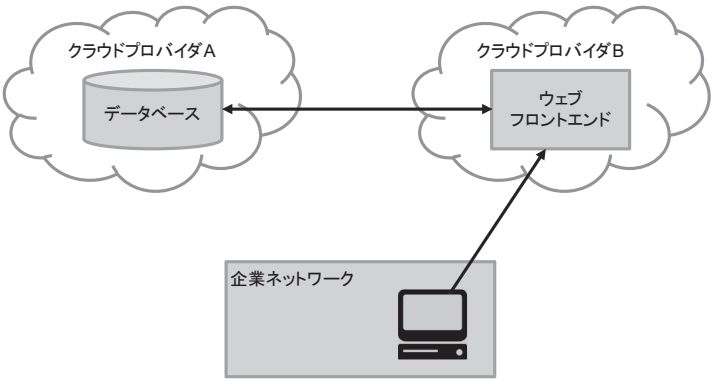

図9：マルチクラウドのユースケース

このユースケースは、CSAのSoftware Defined Perimeter (SDP) 仕様 [CSA-SDP] の「サーバ - サーバ」実装である。企業がクラウドでホストされたアプリケーションやサービスにより多く移行するにつれ、境界線ベースのセキュリティに依存することは、企業の負債になることが明らかになってきている。第2.2節で説明したように、ZTの原則では、企業が所有・運用するネットワークインフラストラクチャと、他のサービスプロバイダが所有・運用するインフラストラクチャとの間に違いはないと考えている。

マルチクラウド利用に対するゼロトラストアプローチは、PEPを各アプリケーション/サービスやデータソースのアクセスポイントを設置する。PEとPAは、どちらのクラウド上に存在してもよく、また外部のクラウドプロバイダ上に存在してもよい。クライアントは (ポータルまたはローカルにインストールされたエージェントを介して) PEPに直接アクセスする。このようにして、企業は、企業外でホストされている場合でも、リソースへのアクセスを管理することができる。課題の一つは、さまざまなクラウドプロバイダが同様の機能を実装する独自の方法を持っていることである。企業のアーキテクトは、利用する各クラウドプロバイダで企業のZTAをどのように実装するかを意識する必要がある。

4.3 契約サービスおよび/または非従業員アクセスのある企業

もう一つの一般的なシナリオは、オンサイトにおいて社外の訪問者および/または契約サービスプロバイダを含む企業で、業務を行うために企業リソースへの限定的なアクセスを必要とする場合である (図10を参照)。例えば、企業は独自の内部アプリケーション/サービス、データベース、および資産を持っている。これらには、時折オンサイトでメンテナンスを提供するプロバイダと契約しているサービスも含まれる (例:外部プロバイダが所有し管理しているスマート暖房や照明システム)。これらの社外訪問者やサービスプロバイダは、タスクを実行するためにネットワーク接続を必要とする。ゼロトラスト企業では、これらのデバイスや訪問サービスの技術者がインターネットにアクセスできるようにすると同時に、企業リソースを隠蔽することができる。

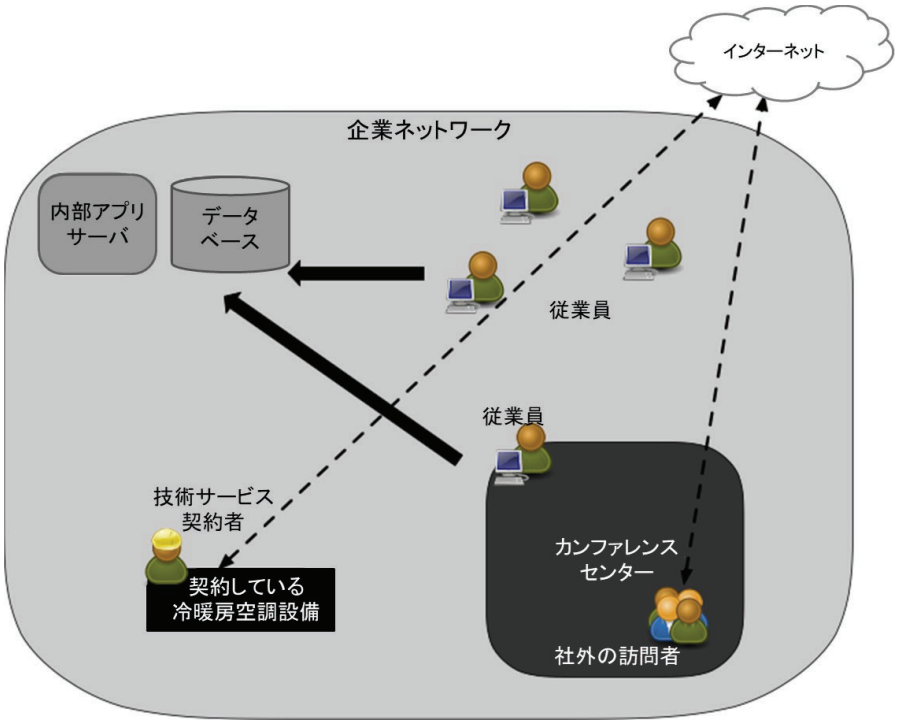

図 10:非従業員アクセスのある企業

このユースケースでは、この組織は、社外の訪問者が従業員と交流するカンファレンスセンターも持っている。ここでも、SDPのZTAアプローチでは、従業員のデバイスと主体が区別され、適切な企業リソースにアクセスできる可能性がある。キャンパスを訪れる社外の訪問者は、インターネットにはアクセスできるが、企業リソースにはアクセスできない。また、ネットワークスキャンで企業サービスを発見することができないかもしれない (すなわち、アクティブなネットワーク偵察やeast-westムーブメントの防御)。

このユースケースでは、PEとPAは、クラウドサービスとして、またはLAN (クラウドサービスをほとんど使用しない、または使用しない場合を想定) 上でホストされている可能性がある。企業の資産は、インストールされたエージェント (第3.2.1項を参照) を持つか、ポータル (第3.2.3項を参照) を介してリソースにアクセスすることができる。PAは、すべての非企業の資産 (エージェントがインストールされていない、またはポータルに接続できないもの) が、ローカルリソースにはアクセスできないが、インターネットにはアクセスできることを保証する。

4.4 企業の垣根を越えた連携

四つ目のユースケースは、企業間の連携である。例えば、企業Aと企業Bの従業員が関与するプロジェクトがあるとする (図11を参照)。この二つの企業は別の連邦政府機関 (G2G) である場合もあれば、連邦政府機関と民間企業 (G2B) である場合もある。企業Aは、プロジェクトに使用されているデータベースを運営しているが、企業Bの特定のメンバーにデータへのアクセスを許可しなければならない。企業Aは、企業Bの従業員が必要なデータにアクセスするために特別なアカウントを設定し、他のすべてのリソースへのアクセスを拒否することができるが、これはすぐに管理が困難になる可能性がある。フェデレーションID管理システムに両組織が登録されていれば、両組織のPEPがフェデレーションIDコミュニティの主体を認証できるようになり、これらの関係をより迅速に確立することができる。

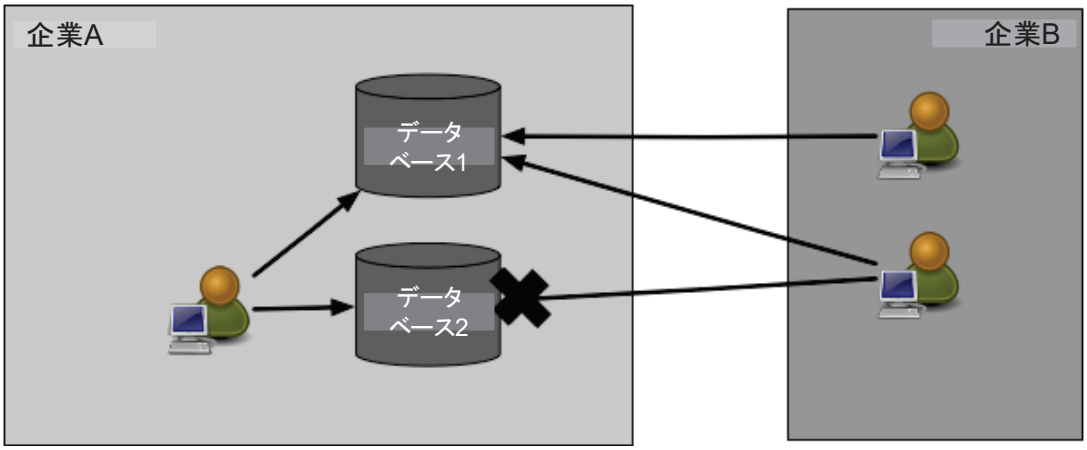

図11：企業間のコラボレーション

このシナリオは、両企業の従業員が組織のネットワークインフラ上にいない場合があり、アクセスする必要のあるリソースは、1つの企業環境内にあるか、クラウドでホストされている場合があるため、ユースケース1 (第4.1節) と似たようなものになる可能性がある。つまり、企業Aのアクセスポリシーに基づいて、企業Bに属する特定のIPアドレスが企業Aのリソースにアクセスすることを許可する複雑なファイアウォールルールや企業全体のアクセス制御リスト (ACL) は必要ない。このアクセスをどのように実現するかは、使用する技術によって異なる。ユースケース1と同様に、クラウドサービスとしてホストされているPEとPAは、VPN等を確立することなく、すべての関係者に可用性を提供することができる。企業Bの従業員は、自社の資産にソフトウェアエージェントをインストールするか、ウェブゲートウェイを介して必要なデータリソースにアクセスするように要求されることがある (第3.2.3項を参照)。

4.5 公開サービスまたは顧客サービスを提供する企業

多くの企業に共通する機能は、公開サービスであり、ユーザ登録を含む場合 (すなわち、ユーザは一連のログインクレデンシャルを作成するか、または発行されなければならない) と含まない場合がある。このようなサービスは、一般の人々、既存のビジネス関係を持つ顧客、または従業員の扶養家族のような特別な外部ユーザのためのものである可能性がある。いずれの場合も、リクエスト元の資産は企業が所有しているものではない可能性が高く、企業は社内サイバーセキュリティポリシーを適用できるかどうかに制約を受けている。

アクセスするためにログインクレデンシャルを必要としない一般的な公開リソース (例：公開ウェブページ) については、ZTAの原則は直接適用されない。企業は、リクエスト元の資産の状態を厳密に制御することはできず、匿名の公開リソース (例：公開ウェブページ) は、アクセスするためにクレデンシャルを要求しない。

企業は、顧客 (すなわち、ビジネス関係のある者) や特別なユーザ (例：従業員の扶養家族) 等の登録された一般ユーザのためのポリシーを確立することができる。ユーザがクレデンシャルを生成、または発行される必要がある場合、企業は、パスワードの長さ、ライフサイクル、およびその他の詳細に関するポリシーを策定し、オプションまたは要件としてMFAを提供することができる。しかし、企業は、このクラスのユーザに対して実装できるポリシーが限られている。受信リクエストに関する情報は、公開サービスの状態を判断し、正当なユーザを装った攻撃の可能性を検出するのに役立つかもしれない。例えば、登録ユーザ用のポータルが、登録された顧客から一般的なウェブブラウザのセットの一つを使用してアクセスされることが分かっていたとする。不明なブラウザタイプや既知の古いバージョンからのアクセスリクエストが突然増加した場合、何らかの自動化された攻撃を示す可能性があり、企業は、特定されたこれらのクライアントからのリクエストを制限するための措置を取ることができる。企業はまた、リクエスト元のユーザや資産についてどのような情報を収集し、記録することができるかについての法令や規制にも注意する必要がある。

5 ゼロトラスト・アーキテクチャに関連する脅威

どんな企業でも、サイバーセキュリティのリスクを排除することはできない。既存のサイバーセキュリティポリシーとガイダンス、アイデンティティとアクセス管理、継続的な監視、および一般的なサイバー衛生に補完される場合、適切に実装、および維持されたZTAは、全体的なリスクを低減し、一般的な脅威から保護することができる。一方で、脅威の中には、ZTAを実施する際に特有の特徴を持つものもある。

5.1 ZTAの決定プロセスの転覆

ZTAでは、ポリシーエンジンとポリシーアドミニストレータが企業全体の重要なコンポーネントとなる。企業リソース間の通信は、PEとPAによって承認され、場合によってはPEとPAが設定されない限り発生しない。つまり、これらのコンポーネントは適切に設定され、維持されなければならない。PEのルールへの構成アクセス権を持つ企業の管理者は、承認されていない変更を行ったり、企業の運用を混乱させるようなミスを犯したりする可能性がある。同様に、侵害されたPAは、通常であれば承認されないリソースへのアクセスを許してしまう可能性がある (例：不正な個人所有デバイスへのアクセス)。関連するリスクを軽減するには、PEとPAのコンポーネントを適切に構成して監視し、構成の変更はすべてログに記録して監査の対象とする必要がある。

5.2 サービス拒否またはネットワーク障害

ZTAでは、PAはリソースアクセスのための重要なコンポーネントである。企業リソースは、PAの許可と、場合によっては設定操作がない限り、相互に接続することはできない。攻撃者がPEPやPE/PAへのアクセスを妨害したり拒否したりすると (すなわち、DoS攻撃やルートハイジャック) 、企業の運用に悪影響を及ぼす可能性がある。企業は、適切に保護されたクラウド環境にポリシー適用を設置するか、サイバーレジリエンスに関するガイダンス [SP 800-160v2] に従い、複数の場所に複製することで、この脅威を軽減することができる。

これはリスクを軽減するものであるが、リスクを排除するものではない。Miraiのようなボットネットは、主要なインターネットサービスプロバイダに対して大規模なDoS攻撃を行い、何百万人ものインターネットユーザへのサービスを妨害する[5] 。また、攻撃者が企業内の一部またはすべてのユーザアカウント (例：支社、もしくはたった1人のリモート従業員) からPEPやPAへのトラフィックを傍受してブロックする可能性もある。このような場合、影響を受けるのは企業内の一部の主体のみである。これは、従来のリモートアクセスVPNでも可能であり、ZTAに特有のものではない。

また、ホスティングプロバイダが誤ってクラウド型のPEやPAをオフラインにしてしまうこともある。クラウドサービスは、インフラストラクチャ・アズ・ア・サービス (IaaS) [6] とSaaSの両方で、過去に障害が発生した事例がある[7] 。ポリシーエンジンやポリシーアドミニストレータコンポーネントがネットワークからアクセスできなくなると、運用上のエラーにより、企業全体が機能しなくなる可能性がある。

[5] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[6] https://aws.amazon.com/message/41926/

[7] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12286870

また、PAから企業リソースにアクセスできないリスクもあり、主体にアクセスが許可されていても、PAはネットワークからの通信経路を設定できない。これは、DDoS攻撃や単に予期せぬ大量の使用が原因で発生する可能性がある。これは、何らかの理由でリソースが利用できないために、一部またはすべての企業の主体が特定のリソースにアクセスできないという点で、他のネットワーク障害と似ている。

5.3 盗まれたクレデンシャル/内部の脅威

ZTや情報セキュリティとレジリエンスのポリシー、およびベストプラクティスを適切に実装することで、攻撃者が搾取したクレデンシャルや内部攻撃を介して広範なアクセスを得るリスクを低減することができる。ネットワークの場所に基づく暗黙の信頼を持たないというZTの原則は、攻撃者が企業内で足がかりを得るためには、既存のアカウントやデバイスを侵害する必要があることを意味する。適切に開発・実装されたZTAは、侵害されたアカウントや資産が、通常の権限やアクセスパターンを超えてリソースにアクセスすることを防ぐ必要がある。これは、攻撃者が興味を持っているリソースに関連するアクセスポリシーを持つアカウントが、攻撃者の主要なターゲットになることを意味する。

攻撃者は、フィッシング、ソーシャルエンジニアリング、またはそれらを組み合わせた攻撃を使用して、価値のあるアカウントのクレデンシャルを取得することがある。「価値のある」とは、攻撃者の動機に応じて異なる意味を持つ場合がある。例えば、企業の管理者アカウントは価値があるかもしれないが、金銭的な利益に関心のある攻撃者は、金銭的なリソースや支払いリソースにアクセスできるアカウントを同等の価値があると考えるかもしれない。アクセスリクエストに対するMFAの実装は、侵害されたアカウントからの情報損失のリスクを減らすことができる。しかし、有効なクレデンシャルを持つ攻撃者 (または悪意のある内部攻撃者) は、アカウントにアクセスが許可されているリソースにアクセスできる可能性がある。例えば、有効な人事担当者のクレデンシャルと企業所有の資産を持つ攻撃者や侵害された従業員が、従業員データベースにアクセスできる可能性がある。

ZTAはリスクを軽減し、侵害されたアカウントや資産がネットワーク全体で水平移動 (ラテラルムーブメント) を行うことを防ぐ。侵害されたクレデンシャルが特定のリソースへのアクセスを許可されていない場合、そのリソースへのアクセスを拒否され続けることになる。さらに、コンテキストトラストアルゴリズム (第3.3.3.1節を参照) は、レガシーな境界ベースのネットワークで発生した場合よりも、この攻撃を検出して迅速に対応する可能性が高い。文脈的なTAは、通常の行動から外れたアクセスパターンを検出し、侵害されたアカウントや内部攻撃の脅威による機密リソースへのアクセスを拒否することができる。

5.4 ネットワーク上の可視性

第3.4.1節で述べたように、すべてのトラフィックはネットワーク上で検査され、ログに記録され、企業に対する潜在的な攻撃を特定し、それに対処するために分析される。しかし、前述したように、企業ネットワーク上のトラフィックの一部 (大部分) は、レイヤ3ネットワーク解析ツールでは可視性が不足する場合がある。このようなトラフィックは、企業が所有していない資産 (例：企業のインフラストラクチャを使用してインターネットにアクセスする契約サービス) や、パッシブモニタリングに耐性のあるアプリケーション/サービスから発生している可能性がある。ディープパケットインスペクション (パケットの深層検査) や暗号化されたトラフィックを調査できない企業は、ネットワーク上の攻撃者の可能性を評価するために他の方法を使用する必要がある。

だからといって、企業がネットワーク上で見た暗号化されたトラフィックを分析できないわけではない。

暗号化されたトラフィックのメタデータ (例：送信元や宛先アドレス等) を収集し、それらを使用してネットワーク上で通信しているアクティブな攻撃者や潜在的なマルウェアを検出することができる。機械学習の技術 [Anderson] は、復号化および検査できないトラフィックの分析に使用できる。このタイプの機械学習を採用することで、企業はトラフィックを正規なものか悪意の可能性があり対応が必要なものかに分類することができるようになる。

5.5 システムとネットワーク情報の保存

企業ネットワークトラフィックの監視と分析に関連する脅威は、分析コンポーネントそのものである。モニタースキャン、ネットワークトラフィック、およびメタデータが、コンテキストポリシーの構築、フォレンジック、またはその後の分析のために保存されている場合、そのデータは攻撃者の標的となる。ネットワーク図、設定ファイル、その他のネットワークアーキテクチャ文書と同様に、これらのリソースは保護されている必要がある。攻撃者がこの情報へのアクセスに成功すれば、企業アーキテクチャへの洞察を得て、さらなる偵察や攻撃のための資産を特定することができるかもしれない。

ZT企業における攻撃者のもう一つの偵察情報源は、アクセスポリシーをエンコードするために使用される管理ツールである。蓄積されたトラフィックと同様に、このコンポーネントにはリソースへのアクセスポリシーが含まれており、攻撃者に、どのアカウントが侵害に最も価値があるか (例：目的のデータリソースへのアクセス権を持つアカウント) に関する情報を与えることができる。

すべての貴重な企業データについては、不正アクセスやアクセスの試みを防ぐために、適切な保護が施されていなければならない。これらのリソースはセキュリティ上重要なものであるため、最も制限の厳しいアクセスポリシーを設定し、指定された管理者アカウントまたは専任の管理者アカウントからのみアクセスできるようにしなければならない。

5.6 独自のデータフォーマットやソリューションへの依存

ZTAは、アクセスの決定を行うために、リクエスト元の主体や使用されている資産、企業や外部のインテリジェンス、脅威分析に関する情報を含む複数の異なるデータソースに依存している。多くの場合、この情報の保存と処理に使用される資産は、情報の相互作用と交換方法について共通のオープンな標準を持っていない。このため、企業が相互運用性の問題により、一部のプロバイダにロックインされてしまうことがある。あるプロバイダにセキュリティ上の問題や障害が発生した場合、企業は、多大なコスト (例：複数の資産を交換する) や長期にわたる移行作業 (例：ポリシールールをある独自の形式から別の形式に置き換える) を経ずに、新しいプロバイダに移行できない可能性がある。DoS攻撃と同様に、このリスクはZTAに特有のものではないが、ZTAは (企業とサービスプロバイダの両方にある) 情報への動的なアクセスに大きく依存しているため、混乱は企業の中核的なビジネス機能に影響を与える可能性がある。関連するリスクを軽減するために、企業は、パフォーマンスや安定性等の典型的な要因に加えて、ベンダーのセキュリティ管理、企業のスイッチングコスト、サプライチェーンのリスク管理等の要因を考慮して、サービスプロバイダを総合的に評価する必要がある。

5.7 ZTA管理におけるノンパーソンエンティティ (NPE) の利用

人工知能やその他のソフトウェアベースのエージェントは、企業ネットワークのセキュリティ問題を管理するために配備され始めている。これらのコンポーネントは、人間の管理者の代わりにZTAの管理コンポーネント (例：ポリシーエンジン、ポリシーアドミニストレータ) と対話する必要がある。ZTAを実装している企業で、これらのコンポーネントがどのように自分自身を認証するかは、未解決の問題である。

ほとんどの自動化された技術システムは、リソースコンポーネントへのAPIを使用する際に、何らかの認証手段を使用することが想定されている。

設定やポリシーの実施に自動化技術を使用する場合の最大のリスクは、フォールスポジティブ (無害な行為を攻撃と間違える) やフォールスネガティブ (攻撃を通常の活動と間違える) が企業のセキュリティ態勢に影響を与える可能性である。これは、誤った判断を修正し、判断プロセスを改善するために、定期的に再チューニング分析を行うことで低減することができる。

関連するリスクは、攻撃者が権限を持たないタスクを実行するように、攻撃者がNPEを誘導したり、強制したりすることができることである。これらのソフトウェアエージェントは、人間のユーザと比較して、管理またはセキュリティ関連のタスクを実行するための認証 (例：APIキー vs. MFA) の基準が低くなる可能性がある。攻撃者がエージェントと対話することができれば、理論的には、攻撃者がエージェントを騙して、攻撃者に大きなアクセスを許可したり、攻撃者に代わって何らかのタスクを実行させたりすることができる。また、攻撃者がソフトウェアエージェントのクレデンシャルにアクセスし、エージェントになりすましてタスクを実行してしまう危険性もある。

6 ゼロトラスト・アーキテクチャと既存の連邦ガイダンスとの連携の可能性

いくつかの既存の連邦政府の方針と指針は、ZTAの計画、展開、および運用に関係している。これらのポリシーは、企業がよりゼロトラスト指向のアーキテクチャに移行することを禁じるものではなく、組織のゼロトラスト戦略の策定に影響を与える可能性がある。既存のサイバーセキュリティポリシーやガイダンス、ICAM、継続的な監視、一般的なサイバー衛生を補完すると、ZTAは、組織のセキュリティ態勢を強化し、一般的な脅威から保護することができる。

6.1 ZTAとNISTリスクマネジメントフレームワーク

ZTAの展開では、指定されたミッションやビジネスプロセスに対する許容可能なリスクを中心としたアクセスポリシーを策定する必要がある (第7.3.3項を参照)。リソースへのネットワークアクセスをすべて拒否し、接続された端末を介してのみアクセスを許可することも可能であるが、これは多くの場合、過度な制限であり、作業の達成を阻害する可能性がある。連邦政府機関がその任務を遂行するためには、許容できるレベルのリスクがある。与えられたミッションの遂行に関連したリスクは、特定および評価され、受け入れられるか、または緩和されなければならない。これを支援するために、NISTリスク管理フレームワーク (RMF) が開発された [SP800-37] 。

ZTAの計画と実装により、企業によって定義された認可の境界が変更される可能性がある。これは、新しいコンポーネント (例：ポリシーエンジン、ポリシーアドミニストレータ、PEP) が追加され、ネットワーク境界防御への依存度が低下することによるものである。RMFに記載されている全体的なプロセスは、ZTAでは変更されない。

6.2 ゼロトラストとNISTプライバシーフレームワーク

ユーザのプライバシーと個人情報 (例：個人特定情報) を保護することは、組織にとって最も重要な関心事である。プライバシーとデータの保護は、FISMAやHeath Insurance Portability and Accountability Act (HIPAA) 等のコンプライアンスプログラムに含まれている。これを受けて、NISTは、組織が使用するためのプライバシーフレームワーク [NISTPRIV] を作成した。本文書は、プライバシーリスクと緩和戦略を記述するためのフレームワークを提供するとともに、企業がユーザのプライバシーや組織が保存・処理する個人情報に対するリスクを特定し、測定し、緩和するためのプロセスを提供している。これには、企業がZTAの運用をサポートするために使用する個人情報や、アクセスリクエストの評価に使用されるバイオメトリクス属性が含まれる。

ZTのコアとなる要件の一部は、企業が環境内のトラフィックを検査してログに記録すること (監視システムで復号できないトラフィックを扱う場合は、少なくともメタデータを記録して検査すること) である。このトラフィックの中には、個人情報が含まれていたり、プライバシーリスクを伴ったりするものもある。組織は、ネットワークトラフィックの傍受、スキャン、ロギングに関連して起こりうるリスクを特定する必要がある [NISTIR 8062]。これには、ユーザへの通知、同意の取得 (ログインページやバナー等を介して) 、企業ユーザへの教育等のアクションを含む可能性がある。NISTプライバシーフレームワーク [NISTPRIV] は、ゼロトラスト・アーキテクチャを開発している企業のプライバシー関連のリスクを特定し、緩和するための正式なプロセスを開発するのに役立つ可能性がある。

6.3 ZTAと連邦政府のアイデンティティ、クレデンシャル、およびアクセス管理アーキテクチャ

主体のプロビジョニングは、ZTAの重要なコンポーネントである。PEが関連する主体とリソースを識別するための情報が不十分な場合、ポリシーエンジンは、接続の試みがリソースへの接続を許可されているかどうかを判断することができない。ゼロトラストの展開に移行する前に、強力な主体のプロビジョニングと認証ポリシーが必要である。企業は、PEがアクセスリクエストを評価するために使用できる主体の一連の明確な属性とポリシーを必要としている。

連邦行政管理予算局 (OMB) は、連邦政府のアイデンティティ管理の改善に関するM-19-17を発行した。この方針の目標は、「...国家の任務遂行、信頼、および安全を可能にするものとしてのアイデンティティのための共通のビジョン」を策定することである [M-19-17] 。このメモでは、すべての連邦機関に対し、アイデンティティ発行および管理に関連する取り組みを管理するためにICAM事務所を組織するよう求めている。これらの管理ポリシーの多くは、NIST SP 800-63-3, *Digital Identity Guidelines* [SP800-63] の勧告を使用すべきである。ZTA は正確なアイデンティティ管理に大きく依存しているため、ZTAの取り組みはすべて、組織のICAMポリシーを統合する必要がある。

6.4 ZTAとTrusted Internet Connections 3.0

TICは、OMB、DHS、および連邦政府一般調達局 (GSA) が共同で管理する連邦政府のサイバーセキュリティイニシアチブであり、連邦政府全体のネットワークセキュリティベースラインを確立することを目的としている。歴史的に、TICは境界ベースのサイバーセキュリティ戦略であり、各組織は外部ネットワーク接続を統合して監視する必要があった。TIC1.0とTIC2.0に内在するものは、境界線の内部が「信頼されている」という前提であるのに対し、ZTAは、ネットワークの位置が「信頼」できるものと判断しないこと (すなわち、組織の内部ネットワークには「信頼」がない) と仮定している。TIC2.0は、組織の境界にあるTICアクセスポイントに配備される一連のネットワークベースのセキュリティ機能 (例：コンテンツフィルタリング、監視、認証) を提供しており、これらの多くはZTの原則と整合性を持つ。

TIC3.0は、クラウドサービスおよびモバイルデバイスに対応するために更新された [M-19-26] 。TIC3.0では、「信頼」の定義が特定のコンピューティングコンテキストによって異なる可能性があり、また、トラストゾーンを定義するためのリスク許容度が組織によって異なることが認識されている。さらに、TIC3.0には、更新されたTIC Security Capability Handbookがあり、これは以下の2種類のセキュリティ機能を定義している。(1) 企業レベルで適用される普遍的なセキュリティ機能、(2) TICのユースケースで定義されているように、複数のポリシー実施ポイント (PEP) に適用されるネットワークレベルの機能であるPEPセキュリティ機能。PEPセキュリティ機能は、組織の境界にある単一のPEPではなく、所定のデータフローに沿って配置された任意の適切なPEPに適用することができる。これらのTIC3.0セキュリティ機能の多くは、ZTAを直接サポートしている (例：暗号化トラフィック、強力な認証、マイクロセグメンテーション、ネットワークとシステムのインベントリ、その他)。TIC3.0は、特定のアプリケーション、サービス、および環境におけるトラストゾーンとセキュリティ機能の実装を説明する具体的なユースケースを定義している。

TIC3.0がネットワークベースのセキュリティ保護に焦点を当てているのに対し、ZTAはアプリケーション、ユーザ、データの保護に対応したより包括的なアーキテクチャである。TIC3.0のユースケースが進化するにつれ、ZTA TICのユースケースはZTA実施ポイントに展開されるネットワーク保護を定義するために開発される可能性が高い。

6.5 ZTAとEINSTEIN (NCPS - National Cybersecurity Protection System)

NCPS (運用上はEINSTEINとして知られている) は、サイバー脅威から連邦政府を守るために、侵入検知、高度な分析、情報共有、および侵入防止機能を提供する統合システムである。NCPSの目標は、サイバーリスクを管理し、サイバー保護を向上させ、パートナーにサイバー空間の安全を確保する権限を与えることであり、ゼロトラストの全体的な目標と一致している。EINSTEINのセンサーは、CISAのNational Cybersecurity and Communications Integration Center (NCCIC) が連邦政府のネットワークを守り、連邦政府機関の重大なインシデントに対応することを可能にする。

DHSの状況認識のためのNCPSセンサーの配置は、連邦政府の境界ネットワーク防御に基づいているが、ZTAは資産、データ、その他のすべてのリソースを保護する。NCPSプログラムは、クラウドベースのトラフィックに関するセキュリティ情報を利用することで状況認識が維持されるように進化しており、ZTAシステムからの拡大された状況認識テレメトリーの基礎を築くのに役立っている。NCPSの侵入防止機能も、現在のNCPSの拠点とZTAシステムの両方でポリシーの実施を知らせることができるように進化する必要がある。連邦政府全体でZTAが採用されるようになると、NCPSの実装は継続的に進化するか、NCPSの目的を達成するために新しい機能を導入する必要がある。インシデント対応者は、ゼロトラスト・アーキテクチャを導入している連邦政府機関が利用可能な政府機関のトラフィックの認証、トラフィック検査、およびロギングから得られる情報を潜在的に活用できる可能性がある。ZTAで生成された情報は、イベントの影響度を定量化するためのより良い情報となる可能性があり、機械学習ツールはZTAデータを利用して検出を改善することができる。ZTAからの追加ログは、インシデント対応者による事後分析のために保存される可能性がある。

6.6 ZTAとDHS Continuous Diagnostics and Mitigations (CDM) プログラム

DHS CDMプログラムは、連邦政府機関の情報技術 (IT) を改善するための取り組みである。その態勢に欠かせないのは、組織自身の中にある資産、構成、および主体に対する組織の洞察力である。システムを保護するためには、組織は、インフラストラクチャの基本的なコンポーネントとアクターを発見し、理解するためのプロセスを設定する必要がある。

- **何がつながっているのか？**
  組織ではどのようなデバイス、アプリケーション、およびサービスが使用されているのか？これには、脆弱性や脅威が発見された際に、これらの人工物のセキュリティ対策を観察し、改善することが含まれる。
- **誰がネットワークを使用しているか？**
  どのユーザが組織に所属しているか、またはどのユーザが企業リソースへのアクセスを許可されている外部ユーザなのか？これらには、自律的なアクションを実行している可能性のあるNPEが含まれる。
- **ネットワーク上で何が起こっているのか？**
  企業は、システム間のトラフィックパターンやメッセージについての洞察力を必要としている。
- **データはどのように保護されているか？**
  企業は、情報が保存時、転送時、および使用時にどのように保護されるかについて、ポリシーを設定する必要がある。

強力なCDMプログラムを導入することは、ZTAの成功の鍵となる。例えば、ZTAに移行するためには、企業は使用可能なインベントリを作成するために、物理的および仮想的資産を発見して記録するシステムを持っていなければならない。DHS CDMプログラムは、連邦政府機関内でZTAへの移行に必要な機能を構築するために、いくつかの取り組みを開始した。

例えば、DHS Hardware Asset Management (HWAM) [HWAM] プログラムは、安全な構成を展開するために、組織がネットワークインフラ上のデバイスを特定するのを支援する取り組みである。これは、ZTAへのロードマップを開発する際の最初のステップに似ている。組織は、ネットワーク上に存在する資産 (またはリモートでリソースにアクセスする資産) を可視化して、ネットワークの活動を分類、構成、監視する必要がある。

6.7 ZTA、Cloud SmartとFederal Data Strategy

Cloud Smart[8] 戦略、更新された Data Center Optimization Initiative [M-19-19] ポリシー、および Federal Data Strategy[9] は、すべて、ZTAを計画する組織のいくつかの要件に影響を与えている。これらのポリシーでは、オンプレミスとクラウドの両方で、データの収集、保存、アクセスの方法を棚卸し、評価することを求められている。

この棚卸は、どのようなビジネスプロセスとリソースがZTAの導入によって利益を得るかを判断する上で重要である。主体とリソースが企業ネットワーク境界の外側にあり、用途、スケーラビリティ、およびセキュリティにおいて最大の恩恵を受けられる可能性が高いため、主にクラウドベースであるか、またはリモートワーカーが主に使用するデータリソースやアプリケーション、サービスは、ZTAアプローチの良い候補となる (第7.3.3節を参照)。

Federal Data Strategyでの追加的な検討事項の一つは、組織のデータ資産を他の組織や一般の人々がどのようにしてアクセス可能にするかということである。これは、企業間連携のZTAのユースケースに対応する (第4.4節を参照)。これらの資産にZTAを使用する組織は、戦略を策定する際に、共同作業や公開の要件を考慮に入れる必要があるかもしれない。

[8] 連邦政府のクラウドコンピューティング戦略：https://cloud.cio.gov/strategy/
[9] 連邦データ戦略： https://strategy.data.gov/

7 ゼロトラスト・アーキテクチャへの移行

ZTAの実装は、インフラストラクチャやプロセスを全面的に置き換えるのではなく、一つの道のりである。組織は、もっとも価値のあるデータ資産を保護するために、ゼロトラストの原則、プロセスの変更、およびテクノロジーソリューションを段階的に導入することを目指すべきである。ほとんどの企業は、ITの近代化を先導するための投資を継続しながら、終わりのないゼロトラスト/境界ベースのハイブリッドモードでの運用を継続するであろう。ZTの原則に基づくアーキテクチャへの移行を含むIT近代化計画を持つことは、企業が小規模なワークフローを移行するロードマップを策定するのに役立つかもしれない。

企業がどのようにある一つの戦略に移行するかは、現在のサイバーセキュリティの態勢と運用に依存する。企業は、重要なZTに焦点を当てた環境 [ACT-IAC] を展開することが可能になる前に、一定レベルのベースラインを持つべきである。このベースラインには、資産、主体、ビジネスプロセス、トラフィックフロー、および、企業として識別しカテゴライズした依存関係のマッピングを持つことが含まれる。企業は、候補となるビジネスプロセスのリストと、このプロセスに属する主体/資産のリストを作成する前に、この情報を必要とする。

7.1 純粋なゼロトラスト・アーキテクチャ

グリーンフィールドアプローチでは、ゼロトラスト・アーキテクチャを一から構築することが可能である。企業が業務に使用したいアプリケーション/サービスとワークフローを把握していると仮定すると、それらのワークフローのためにゼロトラストの原則に基づいたアーキテクチャを作成することができる。ワークフローが特定されると、企業は必要なコンポーネントを絞り込み、個々のコンポーネントがどのように相互作用するかのマッピングを開始できる。この時点から、インフラストラクチャを構築し、コンポーネントを構成するためのエンジニアリングと組織による作業となる。これには、企業が現在どのように設定し、どのように運用しているかに応じて、追加の組織的な変更が含まれる場合がある。

実際には、連邦政府機関や既存のネットワークを持つ組織にとって、これが実行可能なオプションとなることはほとんどない。しかし、組織が独自のインフラストラクチャを構築する必要があるような新しい責任を果たすことを求められる場合もあるかもしれない。このような場合には、ZTの概念をある程度導入することが可能かもしれない。例えば、ある組織は、新しいアプリケーション、サービス、またはデータベースを構築することを伴う新しい責任を与えられるかもしれない。その組織は、アクセスを許可する前に主体が信頼できるかどうかを評価したり、新しいリソースの周りにマイクロペリミターを確立したりする等、ZTの原則と安全なシステムエンジニアリング [SP8900-160v1] に、新たに必要とされるインフラストラクチャを設計することができる。成功の度合は、この新しいインフラストラクチャが既存のリソース (例：ID管理システム) にどの程度依存しているかに依存する。

7.2 ハイブリッドZTAと境界ベースのアーキテクチャ

主要な企業が、一度の技術更新でゼロトラストに移行できる可能性は低い。企業内でZTAワークフローがZTA以外のワークフローと永遠に共存する可能性がある。企業に対するZTAアプローチへの移行は、一度に一つのビジネスプロセスで行われる可能性がある。企業は、共通の要素 (例：ID管理、デバイス管理、イベントロギング) が、ZTAと境界ベースのハイブリッドセキュリティアーキテクチャで動作するのに十分な柔軟性を持っていることを確認する必要がある。また、企業のアーキテクトは、ZTAの候補となるソリューションを、既存のコンポーネントとインターフェースが取れるものに限定したいと考えるかもしれない。

既存のワークフローをZTAに移行するには、(少なくとも) 部分的な再設計が必要になる。企業は、ワークフローのためにまだそうしていない場合は、安全なシステムエンジニアリング [SP800-160v1] を採用する機会ととらえることができる。

7.3 境界ベースのネットワーク構成にZTAを導入するためのステップ

ZTAへの移行には、組織がその資産 (物理的および仮想的) 、主体 (ユーザ権限を含む) 、ビジネスプロセスに関する詳細な知識を持っている必要がある。この知識は、リソースリクエストを評価する際にPEがアクセスする。知識が不十分であれば、ほとんどの場合、情報が不十分なためにPEがリクエストを拒否してしまうというビジネスプロセスの失敗につながる。これは、組織内に未知の「シャドーIT」が存在する場合に特に問題となる。

企業にZTAを導入するための取り組みを行う前に、資産、主体、データフロー、ワークフローの調査を行う必要がある。この認識が、ZTAの導入を可能にする前に到達しなければならない基礎的な状態を形成する。企業は、現在の運用状況を把握していなければ、どのような新しいプロセスやシステムを導入する必要があるのかを判断することはできない。これらの調査は並行して実施することができるが、どちらも組織のビジネスプロセスの調査に結び付けられている。ZTAの採用は、組織のビジネス機能に対するリスクを低減するためのプロセスであるため、これらのステップは、RMF [SP800-37] のステップにマッピングすることができる。ZTAを実施するための道筋は、図12のように表現できる。

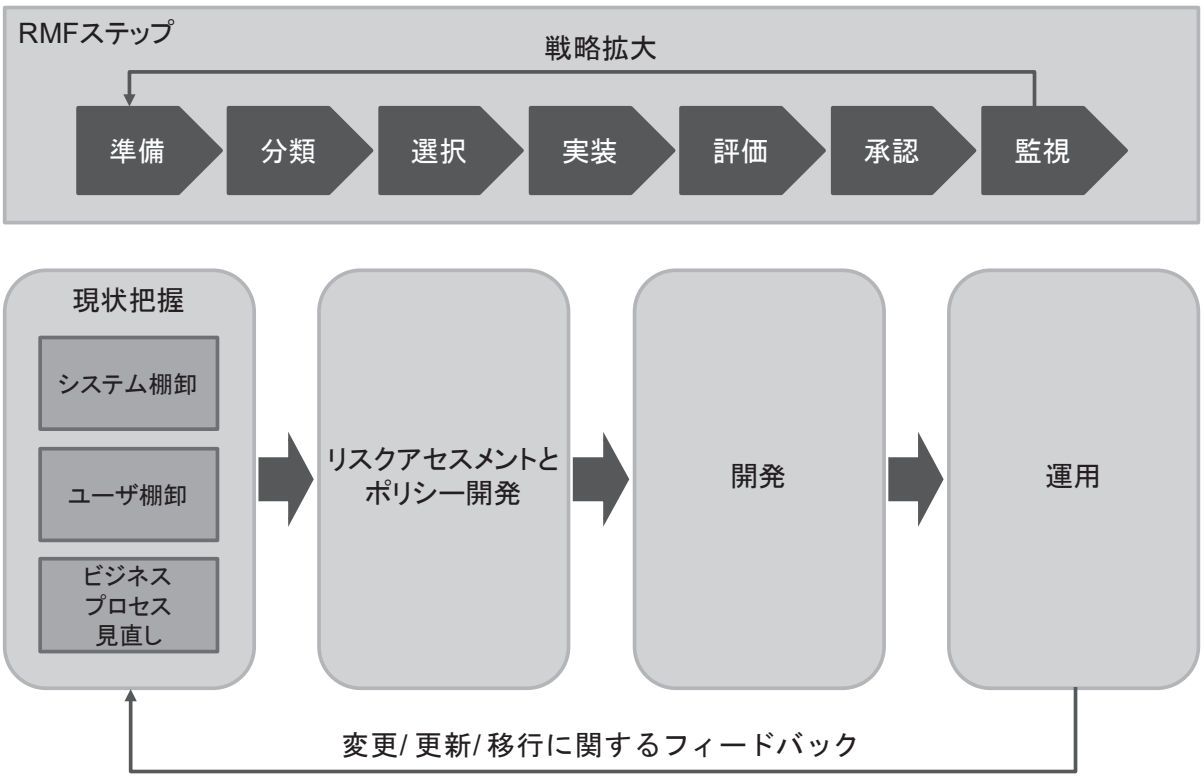

図 12:ZTA展開サイクル

初期のインベントリが作成された後、定期的にメンテナンスと更新のサイクルがある。この更新は、ビジネスプロセスを変更する場合もあれば、影響がない場合もあるが、ビジネスプロセスの評価を実施すべきである。例えば、デジタル証明書プロバイダの変更は、大きな影響がないように見えるかもしれないが、証明書ルートストアの管理、証明書透明性のログ監視等、最初は明らかではない要因が関与している可能性がある。

7.3.1 企業のアクターを特定する

ゼロトラスト企業を運営するためには、PEは企業の主体に関する知識を持っていなければならない。主体には、リソースと相互作用するサービスアカウントのような、人間的なものとNPEの両方が含まれる可能性がある。

開発者やシステム管理者のような特別な権限を持つユーザは、属性や役割を割り当てる際に、さらに精査が必要になる。多くのレガシーなセキュリティアーキテクチャでは、これらのアカウントは、すべての企業リソースにアクセスするための包括的な権限を持っている可能性がある。ZTAは、ログや監査アクションを使用してアクセス行動パターンを特定しながら、開発者や管理者がビジネス要件を満たすために十分な柔軟性を持つことを可能にしなければならない。ZTAの導入では、NIST SP 800-63Aのセクション5 [SP800-63A] で概説されているように、管理者がより厳しい信頼レベルまたは基準を満たすことを要求する場合がある。

7.3.2 企業が所有する資産を特定する

第2.1節で述べたように、ZTAの主な要件の一つは、デバイスを識別して管理する能力である。また、ZTAには、企業所有のネットワークインフラストラクチャ上にある、または企業リソースにアクセスする企業所有ではないデバイスを識別して監視する能力も必要である。企業資産を管理する能力は、ZTAの導入を成功させるための鍵となる。これには、ハードウェアコンポーネント (例：ノートパソコン、電話、IoTデバイス) とデジタル成果物 (例：ユーザアカウント、アプリケーション、デジタル証明書) が含まれる。企業が所有するすべての資産の調査を完全に行うことは不可能な場合があるため、企業は、企業が所有するインフラストラクチャ上にある新たに発見された資産を迅速に特定し、分類し、評価する能力の構築を検討する必要がある。

これは、単に企業資産のデータベースを目録化して管理するだけではない。これには、構成管理と監視も含まれる。資産の現在の状態を監視する能力は、アクセスリクエストを評価するプロセスの一部である (第2.1節を参照)。これは、仮想の資産やコンテナ等の企業の資産を構成し、調査し、更新することができなければならないことを意味する。これには、その物理的な (最も予測できるものとしての) 位置とネットワーク上の位置の両方も含まれる。この情報は、リソースアクセスの決定を行う際に、PEに情報を提供されなければならない。

企業が所有していない資産や企業が所有する「シャドーIT」も、可能な限り目録化する必要がある。これには、企業によって可視化されているもの (例：MACアドレス、ネットワークの位置) と、管理者のデータ入力により追加されたものが含まれる。この情報は、アクセスの決定に使用されるだけでなく (コラボレーターやBYOD資産がPEPに連絡する必要がある場合があるため) 、企業による監視やフォレンジックロギングにも使用される。シャドーITは、これらのリソースが企業所有でありながら、他のリソースのように管理されていないという点で、特別な問題を示している。特定のZTAアプローチ (主にネットワークベース) は、シャドーITコンポーネントが知られておらず、ネットワークアクセスポリシーに含まれていない可能性があるため、シャドーITコンポーネントが使用不能になる可能性さえある。

多くの連邦政府機関は、既に企業の資産の特定を開始している。HWAM [HWAM] やソフトウェア管理 (SWAM) [SWAM] 等のCDMプログラム能力を確立している省庁は、ZTAを実施する際に、そこから得られる豊富なデータを持っている。組織はまた、組織のミッションにとって重要なものとして特定された高価値資産 (HVA) を含むZTA候補プロセスのリスト (M-19-03) を持っているかもしれない。この作業は、どのようなビジネスプロセスもZTAで (再) 設計できるようになる前に、企業または省庁全体で存在する必要がある。これらのプログラムは、ZTAへの移行時だけでなく、企業の一部となる新しい資産、サービス、ビジネスプロセスを会計処理する際にも、企業の変化に対して拡張性と適応性があるように設計されていなければならない。

7.3.3 キープロセスの特定とプロセス実行に伴うリスクの評価

組織が実施すべき第三のインベントリは、業務プロセス、データフロー、および組織のミッションにおけるそれらの関係を特定し、ランク付けすることである。ビジネスプロセスは、リソースへのアクセスリクエストが許可されたり拒否されたりする状況を知らせるべきである。企業は、ディスラプションが組織全体に悪影響を及ぼす可能性を低くするため、最初のZTAへの移行では、リスクの低いビジネスプロセスから開始することを望むかもしれない。十分な経験を積めば、より重要なビジネスプロセスが候補になる可能性がある。

クラウドベースのリソースを利用したり、リモートワーカーが使用したりするビジネスプロセスは、ZTAの対象となることが多く、可用性とセキュリティが改善される可能性がある。企業の境界をクラウドに移行したり、VPNを介したりしてクライアントを企業ネットワークに取り込むのではなく、企業のクライアントが直接クラウドサービスを要求することができる。企業のPEPは、クライアントにリソースへのアクセスを許可する前に、企業ポリシーに従っていることを確認する。また、設計者は、特定のビジネスプロセスにZTAを導入する際に、パフォーマンス、ユーザエクスペリエンス、およびワークフローの脆弱性の増加等のトレードオフの可能性も考慮する必要がある。

7.3.4 ZTA候補の方針策定

候補となるサービスや業務ワークフローを特定するプロセスは、組織にとってのプロセスの重要性、影響を受ける主体のグループ、ワークフローに使用されるリソースの現状等、いくつかの要因に依存する。資産またはワークフローに対するリスクに基づく資産またはワークフローの価値は、NISTリスクマネジメントフレームワーク [SP800-37] を用いて評価することができる。

資産またはワークフローを特定したら、ワークフローで使用または影響を受ける上流のリソース (例：ID管理システム、データベース、マイクロサービス) 、下流のリソース (例：ロギング、セキュリティ監視) 、およびエンティティ (例：主体、サービスアカウント) をすべて特定する。これは、ZTAへの最初の移行としての候補の選択に影響を与える可能性がある。企業主体の特定のサブセット (例：購買システム) で使用されるアプリケーション/サービスは、企業の主体ベース全体に不可欠なもの (例：電子メール) よりも優先される場合がある。

次に、企業管理者は、候補となるビジネスプロセスで使用されるリソースの基準 (基準ベースのTAを使用している場合) または信頼度レベルの重み (スコアベースのTAを使用している場合) を決定する必要がある (第3.3.1節を参照)。管理者は、チューニングフェーズでこれらの基準または値を調整する必要があるかもしれない。これらの調整は、ポリシーが効果的でありながら、リソースへのアクセスを妨げないようにするために必要である。

7.3.5 ソリューション候補の特定

候補となるビジネスプロセスのリストが開発されると、企業のアーキテクトは、候補となるソリューションのリストを作成することができる。いくつかの展開モデル (第3.1節を参照) は、特定のワークフローや現在の企業のエコシステムに適している。同様に、ベンダーのソリューションの中には、他のものよりも一部のユースケースに適しているものもある。以下は考慮すべきいくつかの要因である。

- **そのソリューションは、コンポーネントをクライアントの資産にインストールする必要があるか？**
  これは、BYODや省庁を超えたコラボレーション等、企業所有ではない資産が使用されている、または使用したい場合のビジネスプロセスを制限する可能性がある。
- **ビジネスプロセスのリソースが完全に企業の構内に存在する場合、そのソリューションは動作するか？**
  一部のソリューションでは、リクエストされたリソースはクラウド内に存在し (いわゆるnorth-south トラフィック) 、企業の境界内には存在しない (east-west トラフィック) と想定している。候補となるビジネスプロセスリソースの場所は、プロセスのZTAと同様に、候補となるソリューションに影響を与える。
- **そのソリューションは、分析のために相互作用をログに記録する手段を提供しているか？**
  ZTの重要なコンポーネントは、アクセス決定時にPEにフィードバックされるプロセスフローに関連するデータの収集と使用である。
- **そのソリューションは、さまざまなアプリケーション、サービス、プロトコルを幅広くサポートしているか？**
  ソリューションによっては、幅広いプロトコル (Web、セキュアシェル [SSH] 等) やトランスポート (IPv4やIPv6) をサポートしている場合もあれば、Webや電子メールのような狭い範囲でしか動作しない場合もある。
- **そのソリューションは、主体の行動に変更を必要とするか？**
  ソリューションによっては、所定のワークフローを実行するために追加のステップを必要とする場合がある。これにより、企業の主体がワークフローを実行する方法が変更される場合がある。

解決策の一つは、既存のビジネスプロセスを単なる置き換えではなく、パイロットプログラムとしてモデル化することである。このパイロットプログラムは、複数のビジネスプロセスに適用できるように一般化したり、1つのユースケースに特化したものにしたりすることができる。パイロットは、主体をZTA導入に移行し、レガシープロセスのインフラストラクチャから離れる前に、ZTAの「試験場」として使用することができる。

7.3.6 初期導入とモニタリング

候補となるワークフローとZTAコンポーネントが選択されると、初期導入を開始することができる。企業管理者は、選択したコンポーネントを使用して開発されたポリシーを実装する必要があるが、最初は監視モードで運用することをお勧めする。重要なユーザアカウント (例：管理者アカウント) は、必要なリソースへのアクセスを拒否されたり、割り当てられたりしたすべてのアクセス権を必要としない場合がある。

新しいZTビジネスワークフローは、ポリシーが効果的で実行可能であることを確認するために、しばらくの間はレポート専用モードで運用することができる。これにより、企業はベースラインの資産やリソースのアクセスリクエスト、動作、通信パターンを理解することができる。レポート専用とは、ほとんどのリ

クエストに対してアクセスを許可し、接続のログやトレースを初期に開発したポリシーと比較することを意味する。MFAに失敗したリクエストや、既知の攻撃者が制御するIPアドレスや不正なIPアドレスからのリクエストを拒否するようなアクセスポリシーを実施し、ログに記録するが、初期導入後は、ZTワークフローの実際のインタラクションからデータを収集するために、アクセスポリシーをより甘くする必要がある。ワークフローのベースラインのアクティビティパターンが確立されれば、異常な動作をより容易に特定することができる。もし、より甘い運用ができない場合は、企業ネットワークの運用者はログを注意深く監視し、運用経験に基づいてアクセスポリシーを修正する準備をしておく必要がある。

7.3.7 ZTAの拡大

十分な信頼が得られ、ワークフローポリシーセットが洗練されると、企業は定常的な運用フェーズに入る。ネットワークや資産の監視は継続し、トラフィックの記録 (第2.1節を参照) を行うが、レスポンスやポリシーの変更は、深刻にならないようにテンポを落として行う。また、関係するリソースやプロセスの主体や利害関係者は、運用を改善するためのフィードバックを提供しなければならない。この段階で、企業の管理者はZT展開の次のフェーズの計画を始めることができる。前のロールアウトと同様に、候補となるワークフローとソリューションセットを特定し、初期ポリシーを策定する必要がある。

一方で、ワークフローに変更が発生した場合は、動作中のZTアーキテクチャを再評価する必要がある。新しいデバイス、ソフトウェア (特にZT論理コンポーネント) の大幅なアップデート、組織構造の変更等、システムへの重大な変更は、ワークフローやポリシーの変更につながる可能性がある。実際、一部の作業は既に行われていると仮定して、プロセス全体を再考する必要がある。例えば、新しいデバイスを購入したが、新しいユーザアカウントが作成されていない場合、デバイスの目録だけを更新する必要がある。

参考文献

[ACT-IAC] American Council for Technology and Industry Advisory Council (2019) *Zero Trust Cybersecurity Current Trends*. Available at https://www.actiac.org/zero-trust-cybersecurity-current-trends

[Anderson] Anderson B, McGrew D (2017) Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM, Halifax, Nova Scotia, Canada), pp 1723-1732. https://doi.org/10.1145/3097983.3098163

[BCORE] Department of Defense CIO (2007). Department of Defense Global Information Grid Architecture Vision Version 1.0 June 2007. Available at http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

[CSA-SDP] Cloud Security Alliance (2015) SDP Specification 1.0. Available at https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[FIPS199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[Gilman] Gilman E, Barth D (2017) *Zero Trust Networks: Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., Sebastopol, CA), 1st Ed.

[HWAM] Department of Homeland Security (2015) *Hardware Asset Management (HWAM) Capability Description*. Available at https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf

[IBNVN] Cohen R, Barabash K, Rochwerger B, Schour L, Crisan D, Birke R, Minkenberg C, Gusat M, Recio R, Jain V (2013) An Intent-based Approach for Network Virtualization. *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*. (IEEE, Ghent, Belgium), pp 42-50. Available at https://ieeexplore.ieee.org/document/6572968

[JERICHO] The Jericho Forum (2007) *Jericho Forum Commandments*, version 1.2. Available at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

[M-19-03] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[M-19-17] Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[M-19-19] Office of Management and Budget (2019) Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019. Available at https://datacenters.cio.gov/assets/files/m_19_19.pdf

[M-19-26] Office of Management and Budget (2019) Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB Memorandum M-19-26, September 12, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

[NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W (2015) Policy Machine: Features, Architecture, and Specification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. https://doi.org/10.6028/NIST.IR.7987r1

[NISTIR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[NISTPRIV] National Institute of Standards and Technology (2020) Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[SDNBOOK] Nadeau T, Gray K (2013) *SDN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies*. (O'Reilly) 1st Ed.

[SP800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63A

[SP800-160v1] Ross R, McEvilley M, Oren JC (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP800-160v2] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[SWAM] Department of Homeland Security (2015) *Software Asset Management (SWAM) Capability Description*. Available at https://www.us-cert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

付録A-略語

API	Application Programming Interface
BYOD	Bring Your Own Device
CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
DoS	Denial of Service
G2B	Government to Business (private industry)
G2G	Government to Government
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
PA	Policy Administrator
PDP	Policy Decision Point
PE	Policy Engine
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RMF	NIST Risk Management Framework
SDN	Software Defined Network
SDP	Software Defined Perimeter
SIEM	Security Information and Event Monitoring
TIC	Trusted Internet Connections
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Architecture

付録B-ZTAにおける現状とのギャップの特定

ゼロトラストコンポーネントとソリューションの現在の成熟度は、本文書の開発のために実施されたリサーチの中で調査を行っている。この調査の結果、ZTAエコシステムの現状は、広く採用するには十分に成熟していないと結論づけられた。ZTA 戦略を使用して企業環境を計画し、展開することは可能であるが、必要なすべてのコンポーネントを提供する単一のソリューションは存在しない。また、現在利用可能なZTAコンポーネントの中には、企業内に存在するさまざまなワークフローのすべてに使用できるものはほとんどない。

以下は、ZTAエコシステムにおいて特定されたギャップと、さらなる調査が必要な領域をまとめたものである。これらの分野の中には、ある程度の作業の基盤があるものもあるが、多様なZTAに特化した企業の環境での経験が十分ではないため、ZTAの理念がこれらの分野をどのように変化させるのかはよく知られていない。

B.1 技術調査

複数のベンダーが招待され、ゼロトラストに関する製品や見解を発表した。この調査の目的は、ゼロトラスト・ベースの企業のインフラへの移行や既存のZTA実装の維持を妨げる、欠落した部分を特定することであった。これらのギャップは、即時の展開 (即時または短期) 、メンテナンスや運用に影響を与えるシステム上のギャップ (短期または中期) 、欠落した知識 (将来の研究領域) に分類することができる。これらを表 B-1 にまとめた。

表B-1：特定された展開ギャップの概要

カテゴリー	質問例	特定したギャップ
即時展開	• 調達要件はどのように書けばよいのか？ • ZTAプランは、TIC、FISMA、その他の要件とどのように連携しているのか？	• ZTAの共通フレームワークと語彙の欠如 • ZTAが既存の政策に抵触するとの認識
システム	• ベンダーロックインを防ぐにはどうしたらよいか？ • 異なるZTA環境はどのように相互作用するのか？	• ベンダーAPIへの依存度が高すぎる
より多くの調査が必要な分野	• ZTAに直面して脅威はどのように進化していくのか？ • ZTAに直面して、業務プロセスはどのように変化していくのか？	• ZTAを持つ企業での攻撃成功例 • ZTAを使用した企業でのエンドユーザの経験を文書化

B.2 ZTAへの即時移行を阻むギャップ

これらは、現時点でZTAの採用を遅らせている課題である。これらは当面の問題として分類され、将来のメンテナンスやマイグレーションはこのカテゴリでは考慮されていなかった。先進性のある企業は、メンテナンスのカテゴリをZTAコンポーネントの初期展開を妨げる当面の懸念事項と考えるかもしれないが、これらの問題は、この分析では別のカテゴリと考えられる。

B.2.1 ZTAの設計・計画・調達における共通用語の欠如

企業インフラストラクチャの設計と展開のための戦略としてのゼロトラストは、まだ形成中の概念である。業界では、まだZTAのコンポーネントと運用を説明するための用語や概念を統一していない。このため、組織 (例：連邦政府機関) がゼロトラストの企業インフラストラクチャを設計し、コンポーネントを調達するための一貫した要件とポリシーを開発することが困難になっている。

第2.1節と第3.1節の推進要因は、ZTAを説明するための用語と概念の中立的な基盤を形成するための最初の試みである。概念的なZTAコンポーネントと展開モデルは、ZTAについての基本的な用語や考え方としての役割を果たすために開発された。その目的は、企業の要件開発や市場調査を行う際に、ZTAソリューションの見方、モデル化、議論を行うための共通の方法を提供することにある。上記のセクションは、連邦政府機関でのZTAの経験が増えるにつれ、不完全なものになるかもしれないが、現在のところ、共通の概念的枠組みのベースとしての役割を果たしている。

B.2.2 ZTAが既存の連邦政府のサイバーセキュリティポリシーに抵触するという認識

ZTAは、既存のサイバーセキュリティの見解とは相容れない一連のソリューションを持つ単一のフレームワークであるという誤解がある。ゼロトラストは、コンセプトやアイデアの多くが長い間流通してきたため、現在のサイバーセキュリティ戦略の進化と見るべきである。連邦政府機関は、既存のガイダンス (第6章を参照) を通じて、サイバーセキュリティに対して、よりゼロトラストなアプローチをとるよう奨励してきた。組織が成熟したID管理システムと堅牢なCDM機能を備えていれば、ZTAへの道を歩んでいることになる (第7.3節を参照)。このギャップは、ZTAとそれが以前のサイバーセキュリティのパラダイムからどのように発展してきたのかという 誤解に基づいている。

B.3 ZTAに影響を与えるシステムギャップ

これらは、ZTAの初期導入と展開、および継続的な運用・成熟度に影響を与えるギャップである。これらのギャップは、組織におけるZTAの採用を遅らせたり、ZTAコンポーネント業界の分断を招いたりする可能性がある。システム上のギャップは、オープンスタンダード (規格開発機関 (SDO) または業界コンソーシアムによって作成されたもの) が参考となる分野である。

B.3.3 コンポーネント間のインターフェースの標準化

技術調査の中で、ゼロトラストの単一ソリューションを提供しているベンダーはないことが明らかになった。さらに、単一ベンダーのソリューションを使用することは、ゼロトラストを達成し、ベンダーのロックインのリスクを回避する上では、望ましくないかもしれない。

これは、購入時だけでなく、長期間にわたってコンポーネント内での相互運用性を実現することにつながる。

多くの製品はゼロトラストの中の単一の特定分野に焦点を当てており、データやサービスを別のコンポーネントに提供するために他の製品に依存している (例:リソースアクセスのためのMFAの統合)。ベンダーは、この統合を実現するために、標準化されたベンダー独自のAPIではなく、パートナー企業が提供する独自のAPIに依存していることが多い。このアプローチの問題点は、これらのAPIが独自仕様であり、単一ベンダーの管理下にあることである。制御しているベンダーはAPIの動作を変更することができ、インテグレータはそれに応じて製品を更新する必要がある。このため、製品間の互換性に影響を与える可能性のあるAPI内の変更を早期に通知するために、ベンダーのコミュニティ間で緊密な連携が必要となる。これは、ベンダーと利用者にさらなる負担を強いることになる。ベンダーは製品を変更するためにリソースをかける必要があり、利用者は、あるベンダーが独自のAPIに変更を加えた場合、複数の製品にアップデートを適用する必要がある。さらに、ベンダーは、最大の互換性と相互運用性を実現するために、各パートナーコンポーネントのラッパーを実装し、維持する必要がある。例えば、多くのMFA製品ベンダーは、異なる種類のクライアントの組み合わせで使用できるように、クラウドプロバイダやアイデンティティ管理システムごとに異なるラッパーを作成する必要がある。

利用者側では、これは製品を購入するための要件を開発する際に追加の問題を発生させる。購入者が製品間の互換性を識別するために信頼できる基準がない。したがって、コンポーネントの互換性要件の最小セットを特定することができないため、ZTAに移行するための複数年のロードマップを作成することは非常に困難である。

B.3.4 独自仕様のAPIへの過度の依存に対処するための新たな標準化

ZTAを開発するための単一のソリューションは存在しないため、ゼロトラスト企業のための単一のツールやサービスは存在しない。したがって、企業がZTAに移行することを可能にする単一のプロトコルやフレームワークを持つことは不可能である。現在、ZTAのリーディングオーソリティになろうとするさまざまなモデルやソリューションが存在している。

このことは、ZTAへの移行を支援するために、オープンで標準化されたプロトコルやフレームワークのセットを開発する機会があることを示している。Internet Engineering Task Force (IETF) のようなSDOは、脅威情報の交換に有用と思われるプロトコルを規定している (XMPP-Grid [1] と呼ばれている)。クラウドセキュリティアライアンス (CSA) は、Software Defined Perimeter(SDP) [2] のフレームワークを作成しているが、これもZTAに役立つ可能性がある。有用なZTAに必要なZTA関連のフレームワークやプロトコルの現状を調査し、仕様の作成や改良が必要な箇所を特定するための取り組みを行うべきである。

B.4 ZTAにおける知識格差と今後の研究分野

ここに記載されているギャップは、組織が企業にZTAを採用することを妨げるものではない。これらは、運用中のZTA環境に関する知識のグレーゾーンであり、ほとんどが成熟したゼロトラストの導入に時間と経験がないことに起因している。これらは、研究者が今後取り組むべき分野である。

B.4.5 ZTAに対する攻撃者の対応

企業に適切に実装されたZTAは、従来のネットワーク境界ベースのセキュリティよりも、企業のサイバーセキュリティ態勢を向上させる。ZTAの目的は、攻撃者へのリソースの露出を減らし、ホストの資産が侵害された場合に企業内での横移動を最小限に抑えたり、防止したりすることである。

しかし、しっかりとした攻撃者たちは、ZTAに直面した場合には、その場しのぎではなく、行動を変えることになるであろう。未解決の問題は、攻撃がどのように変化するかということである。一つの可能性としては、クレデンシャルを盗むことを目的とした攻撃が、MFA (例：フィッシング、ソーシャルエンジニアリング) を標的とした攻撃にまで拡大されることが考えられる。もう一つの可能性としては、ハイブリッドZTA/境界ベースの企業においては、攻撃者はZTAの理念が適用されていない (すなわち、従来のネットワーク境界ベースのセキュリティに従う) ビジネスプロセスに焦点を当て、実際には、ZTAのビジネスプロセスへの足掛かりを得るための試みとして、低い (手に届く) 場所に、ぶら下がる果実を標的とする。

ZTAが成熟し、より多くの配備が見られ、経験を積むにつれて、リソースの攻撃面を縮小するというZTAの有効性が明らかになるかもしれない。また、古いサイバーセキュリティ戦略と比較した場合のZTAの成功の指標も開発する必要があるだろう。

B.4.6 ZTA環境でのユーザエクスペリエンス

ZTAを使用している企業でエンドユーザがどのように行動するかについては、これまで厳密な調査が行われていなかった。これは主に、分析に利用できる大規模なZTAのユースケースがないためである。しかし、ZTA企業の一部であるMFAやその他のセキュリティ操作に対してユーザがどのように反応するかについての研究は行われており、この研究は、企業でZTAワークフローを使用する際のエンドユーザの経験と行動を予測するための基礎を形成する可能性がある。

ZTAがエンドユーザ体験にどのように影響するかを予測できる研究の一つは、企業におけるMFAの使用とセキュリティ疲れに関する研究である。セキュリティ疲れ [3] とは、エンドユーザが非常に多くのセキュリティポリシーや課題に直面し、それが生産性に負の影響を与え始める現象である。他の研究では、MFAがユーザの行動を変化させる可能性があることが示されているが、全体的な変化はまちまちである [4] [5] 。一部のユーザは、プロセスが合理化され、使い慣れたデバイス (例：スマートフォンのアプリケーション) を使用したり、持ち歩いたりしている場合には、MFAを快く受け入れる。しかし、一部のユーザは、ビジネスプロセスに個人所有のデバイスを使用しなければならないことに憤慨したり、ITポリシーに違反する可能性があるかどうかを常に監視されていると感じたりしている。

B.4.7 企業やネットワークの破壊に対するZTAのレジリエンス

ZTAベンダーエコシステムの調査では、ZTAを導入する企業が検討しなければならない幅広いインフラが示された。前述したように、現時点では完全なゼロトラストソリューションを提供する単一のプロバイダは存在しない。その結果、企業は複数の異なるサービスや製品を購入することになり、コンポーネントの依存関係が網の目状になってしまう可能性がある。一つの重要なコンポーネントに障害が発生したり、アクセスできなくなったりすると、一つまたは複数のビジネスプロセスに影響を与える障害が連鎖的に発生する可能性がある。

調査対象となったほとんどの製品やサービスは、堅牢性を提供するためにクラウドの存在に依存しているが、クラウドサービスでさえも、攻撃や単純なエラーによってアクセス不能になることが知られている。このような場合、アクセスの判断に使用される主要なコンポーネントにアクセスできなくなったり、他のコンポーネントと通信できなくなったりする可能性がある。例えば、クラウドに配置されたPEおよびPAコンポーネントは、分散型サービス拒否 (DDoS) 攻撃においても到達可能かもしれないが、リソースを持って配置されたすべてのPEPには到達できない可能性がある。ZTA展開モデルのチョークポイントの可能性を発見し、ZTAコンポーネントが到達できない、または到達可能性が限られている場合のネットワーク運用への影響を調べる研究が必要である。

ZTAを採用する際には、企業のCOOP (Continuity of Operations) 計画の見直しが必要になる可能性が高い。ZTAを導入すると、リモートワーカーがオンプレミスと同じリソースにアクセスできるようになるため、多くのCOOP要因が容易になる。しかし、ユーザが適切なトレーニングを受けていなかったり、経験が不足していたりすると、MFAのようなポリシーもマイナスの影響を与える可能性がある。緊急時にユーザがトークンや企業デバイスへのアクセスを忘れてしまったり、アクセスできなくなったりする可能性があり、これは企業ビジネスプロセスのスピードと有効性に影響を与える。

B.5 参考文献

[1] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Software Defined Perimeter Working Group “SDP Specification 1.0” Cloud Security Alliance. April 2014.

[3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. *IT Professional* 18(5):26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D, Shechtman GM, Alsop AS (2009) Productivity and Usability Effects of Using a Two-Factor Security System. *SAIS 2009 Proceedings* (AIS, Charleston, SC), p 37. Available at http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)* (ACM, Orlando, FL), pp 212-224. https://doi.org/10.1145/3134600.3134629