ゼロトラストの現状調査と事例分析に関する調査報告書

2021 年（令和 3 年）3 月 31 日

PwC あらた有限責任監査法人

pwc

目次

1.調査の概要

1.1. 調査の背景と目的

これまでの国内金融機関のセキュリティモデルは、ネットワーク内部を「信頼できるもの」とみなし、外部からの攻撃をファイアウォール等で防ぐ境界型セキュリティが主流であった。しかしながら、デジタライゼーションの進展に伴い、パブリック・クラウドの利用やリモートワークの普及、外部データ連携の促進等、守るべき情報資産や IT 資産が境界の外で活用されることが増え、ネットワーク境界での静的な防御が困難となってきている。そのため、内側と外側を区別せずに、すべてのアクセスを「信頼できないもの」として都度検証するゼロトラストと呼ばれるセキュリティモデルが注目されている。

このような背景から、本調査では、国内・海外金融機関および国内企業におけるゼロトラストに対する関心や、ゼロトラストセキュリティモデルの採用に向けた検討や取り組みの事例等を調査・考察することを通じて、今後、金融機関がセキュリティ・アーキテクチャーの見直しや高度化を行う上でのヒントとなるポイントや、ゼロトラストセキュリティモデルの適用を進める上での考え方等について取りまとめる。

1.2. 調査期間

2021 年（令和 3 年）1 月 27 日～3 月 31 日

1.3. 調査の対象

国内金融機関、海外金融機関、国内企業、ゼロトラスト関連ベンダー

1.4. 調査項目

本調査では、以下の項目について調査を行った。

- 国内金融分野におけるネットワークセキュリティの現状
- ゼロトラストの概念（NIST SP800-207 の定義等）
- 国内・海外金融機関、国内企業におけるゼロトラストに関する取り組み状況（事例、障壁等）
- ゼロトラスト関連サービスを提供しているベンダーの動向や提供されているソリューション

1.5. 調査手法

本調査では、公表されている文献・記事（インターネットサイトに掲載された情報を含む）の調査のほか、調査対象へのヒアリングやアンケートを実施し、これらの結果を PwC あらた有限責任監査法人（以下、PwC あらた）が取りまとめ、報告書を作成した。

なお、主なヒアリングおよびアンケートの対象先は以下のとおりである。

- 国内の金融機関
- 海外に本部を置く金融機関
- 国内企業（非金融）
- 国内外のゼロトラスト関連ベンダー

1.6. 調査の前提条件と免責事項

本調査および本報告書は、金融庁と PwC あらたとの間で締結した 2021 年（令和 3 年）1 月 27 日付のアドバイザリー・サービス契約書に基づき実施、作成されたものであり、また、委託元である金融庁担当職員の指示のもとで実施、作成されている。本報告書は、委託元である金融庁に対してのみ提出したものであり、本報告書を閲覧あるいは本報告書のコピーを入手閲覧した第三者の本報告書の利用に対して、PwC あらたは何らの契約上またはその他の責任を負うものではない。

本報告書は、調査を通じて得られた情報をもとに作成されている。本調査は上記「1.5. 調査手法」に記載したとおり、公表されている文献、記事等の閲覧、および本調査テーマに関連のある機関や関係者へのヒアリングおよびアンケートを通じて実施した。そのため、報告書には、調査対象とした文献の作成者や、ヒアリングやアンケートの対象先である個人および組織による私見や経験に基づく内容が含まれている。また、報告書には、本調査を通じて得られた情報をもとに、報告書の作成を担当した PwC あらたの執筆者による見解および考察が含まれている。

PwC あらたは、本報告書内に記載されたそれらの内容について如何なる意見表明や証明を行うものではなく、保証を行うものでもない。また、本報告書は上述した調査期間に収集した情報をもとに作成されており、報告書の内容に将来の事象が含まれている場合には、その将来の事象の実現可能性や信頼性を保証するものではない。

2. ゼロトラストとは

2.1. ゼロトラストの誕生と定義

2.1.1. ゼロトラストの誕生

ゼロトラストとは、特定の技術や製品、ソリューションを指す言葉ではなく、「企業のネットワークやデバイスからのアクセスを暗黙に信頼せず、常にアクセスの信頼性を検証することで企業の情報資産や IT 資産を保護すること」に焦点をあてたセキュリティの考え方である。

2004 年頃から、ネットワークの境界での静的な防御には限界があるとの考えが示され、ネットワークの位置に基づく暗黙の信頼、すなわち境界線を除去するという非境界化の議論が開始された。その後、2010 年頃に非境界型の考え方を進化させたゼロトラストというコンセプトが提唱された。

以降、クラウドサービスの利用拡大やリモートワークの普及により、ゼロトラストという考え方を取り入れたセキュリティモデルへの関心が高まり、ゼロトラストという言葉が広く使用されるようになったが、ゼロトラスト・アーキテクチャは製品やベンダーによって多様な実現方法があるため、用語や概念が統一されていない状況であった。そのような中、2020 年 8 月に米国国立標準技術研究所（NIST）が、用語と概念の共通基盤を形成することを試み、『Zero Trust Architecture（NIST SP800-207）』[1]を発行した。

2.1.2. NIST SP800-207 におけるゼロトラストに関する定義

NIST SP800-207 の「2 ゼロトラストの基本」に記載されているゼロトラストおよびゼロトラスト・アーキテクチャの定義は以下のとおりである。

【ゼロトラストの定義】 ※NIST SP800-207（原文および日本語訳）より抜粋

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

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。

[1] Zero Trust Architecture（NIST SP800-207）：
https://csrc.nist.gov/publications/detail/sp/800-207/final
ゼロトラスト・アーキテクチャ（参考日本語訳、2020 年 12 月 10 日公開、PwC コンサルティング合同会社）：
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html

【ゼロトラスト・アーキテクチャの定義】 ※NIST SP800-207（原文および日本語訳）より抜粋

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

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。

本報告書は、原則として NIST SP800-207 に示されたゼロトラストおよびゼロトラスト・アーキテクチャの考え方を踏まえて記載されている。

2.2. ゼロトラストが注目を集める背景

ここ数年で新たなセキュリティの考え方であるゼロトラストへの注目度が高まってきている。その背景は大きく 2 点ある。1 点目は、様々な企業がデジタル技術の利活用を進め、IT システムとその繋がりが複雑化・多様化していること、2 点目はサイバー攻撃自体も、そうしたデジタル技術の恩恵を受け、高度化・巧妙化していることである。こうした環境変化がある中、企業は、従来からのセキュリティの考え方だけでサイバー攻撃を防ぐことが困難となっている。

2.2.1. デジタル技術の進展による IT 環境の多様化とサイバーリスクの高まり

スマートデバイスや IoT の普及、データ通信の高速化・大容量化等により、様々なデータを活用して新たな価値を創造するデジタル社会へと変化している。また、少子高齢化による労働人口の減少などの課題を解決するため、場所や時間を問わない多様な働き方が広まっている。

それらの社会の変化に対応するため、多くの企業で、クラウドサービスの利用拡大、リモートワークの普及、IT システムやデータの外部連携が進んでおり、企業の IT システムやネットワークが多様化している。

(1) クラウドサービスの利用拡大

企業では、ビジネス環境の変化に対応するために、より迅速に IT システムを構築でき、スケーラビリティーやアジリティ等の特徴を有するクラウドサービスを利用する動きが急速に広がっている。

以前は、インターネットに接続されたクラウドサービスに機密性や可用性の懸念を抱く企業も多く、一部の限られた IT システムでのみ利用されているような状況であった。

しかしながら、近年は、大手クラウド事業者もセキュリティを最重要事項に掲げてセキュリティに関する機能の充実を進めるほか、さまざまな可用性ニーズを踏まえた機能や価格帯のサービスの提供を進めており、ユーザー企業の選択肢も大幅に広がっている。オンプレミスでは安易に手を出しづらい AI や機械学習などの高度な技術もクラウドであれば実証実験的に期間限定で利用してみる、といったことも容易となりつつある。

クラウド利用については、政府レベルでも同様の傾向である。日本の政府情報システムにおいても、「クラウド・バイ・デフォルト原則」に従い、オンプレミスではなくクラウドサービスの利用を第

一候補として検討すること[2]としている。こうした動きが、民間企業のさらなるクラウドサービスの活用を加速させていくことは間違いない。

(2) リモートワークの普及

自宅や外出先から業務を行うリモートワークは、十数年前から導入されており、インターネット等の外部ネットワークから社内ネットワークに VPN（Virtual Private Network）で接続する方法が一般的である。リモートワークを行うことは技術的には従来から可能であったが、自宅や外出先で情報を扱うことのセキュリティの問題や通信速度の問題から利用は限定的であった。

しかしながら近年では、労働人口の減少の影響で、子育てや介護との両立やジョブ型雇用など多様な働き方を実現するためにリモートワークが普及してきた。また、スマートフォンやタブレット端末などの多様なモバイルデバイスが普及し、外出先でのモバイルデバイスの活用による付加価値を付けたサービスを提供する企業も増えている。加えて、2020 年には新型コロナウイルス感染症（COVID-19）の影響により、出社抑制によるリモートワークのニーズが急増した。

(3) IT システムやデータの外部連携の増加

企業がデータを活用した付加価値を創出するために、自社だけでなく外部のデータを活用する機会や、自社のデータをパートナー企業と共有する機会が増えている。いわゆるシェアリングエコノミーと呼ばれる考え方の 1 つである。

データ利用企業は、データ提供企業が用意した API（Application Programming Interface）を通じて外部のデータを取得し、自社のデータと組み合せることで、ユーザーエクスペリエンスの向上や、より高機能なサービスの提供に役立てている。連携されるデータには地図や天候等の公益性の高いデータだけでなく、行動履歴やキャッシュレス決済データなどの、よりパーソナライズしたサービスの提供に役立つデータもあり、利活用が広がっている。

こうした API の開放を通じたデータの連携・利活用はインターネットやクラウドサービスとの相性も良いことから、近年のデジタル化の中で、多くの企業が多対多で繋がるきっかけとなっている。

このように、企業の IT システムやネットワークが多様化することで、従来からの境界型セキュリティにおける内部と外部の境界も複雑化し、外部からサイバー攻撃を仕掛ける対象となるアタックサーフェスが増えている。

外部の攻撃から守るべき内部と外部の接点（ファイアウォールや VPN 装置等）が増えることで、企業のネットワーク管理負荷が高まり、サイバー攻撃を防ぐことが困難になりつつある。実際に、海外拠点やグループ会社を踏み台とした内部ネットワークへの不正侵入、リモートワークを狙った VPN 装置の脆弱性に対する攻撃、クラウドサービスの設定ミスを突いた不正アクセスなどによる情報漏えいや業務停止等の被害が多く発生しており、サイバー攻撃の高度化・巧妙化により、サイバーセキュリティリスクが高まっている。

---

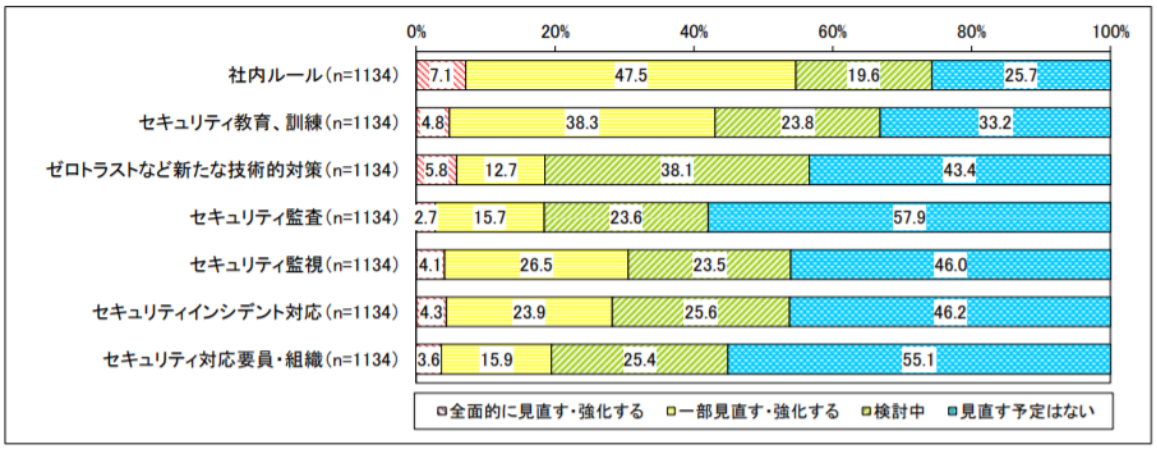
[2] 政府情報システムにおけるクラウドサービスの利用に係る基本方針：
https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf

2.2.2. ゼロトラストへの注目度の高まり

このような状況から、多様化した IT 環境をサイバー攻撃から守るための新たなセキュリティの考え方としてゼロトラストが注目を集めている。

企業の IT 投資・IT 戦略などの動向を調査した『企業 IT 動向調査報告書 2021』[3]によると、新型コロナウイルス感染症（COVID-19）を受けて、情報セキュリティ対策を「ゼロトラストなど新たな技術的な対策」に全面的または一部見直した割合は 18.5%であるが、検討中の企業まで合わせると 56.6%と過半数を超えており、ゼロトラストに関するセキュリティ対策に高い関心が寄せられていることが分かる。（図表 2-1 参照）

図表 2-1 情報セキュリティの各種施策の新型コロナでの見直しや強化



※日本情報システム・ユーザー協会「企業 IT 動向調査報告書 2021」より抜粋

[3] 企業 IT 動向調査 2021（一般社団法人日本情報システム・ユーザー協会（JUAS））：
https://juas.or.jp/library/research_rpt/it_trend/

2.3. ゼロトラストの概要

NIST SP800-207 の「2.1 ゼロトラストの考え方」には、NIST SP800-207 が理念的な目標として定めている 7 つの原則が記載されている。そのゼロトラストの 7 つの原則は以下のとおりである。（詳細は「3.1.1. ゼロトラストの原則」参照）

【ゼロトラストの原則】 ※NIST SP800-207（日本語訳）より抜粋

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*
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*
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*
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*
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*
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*
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*

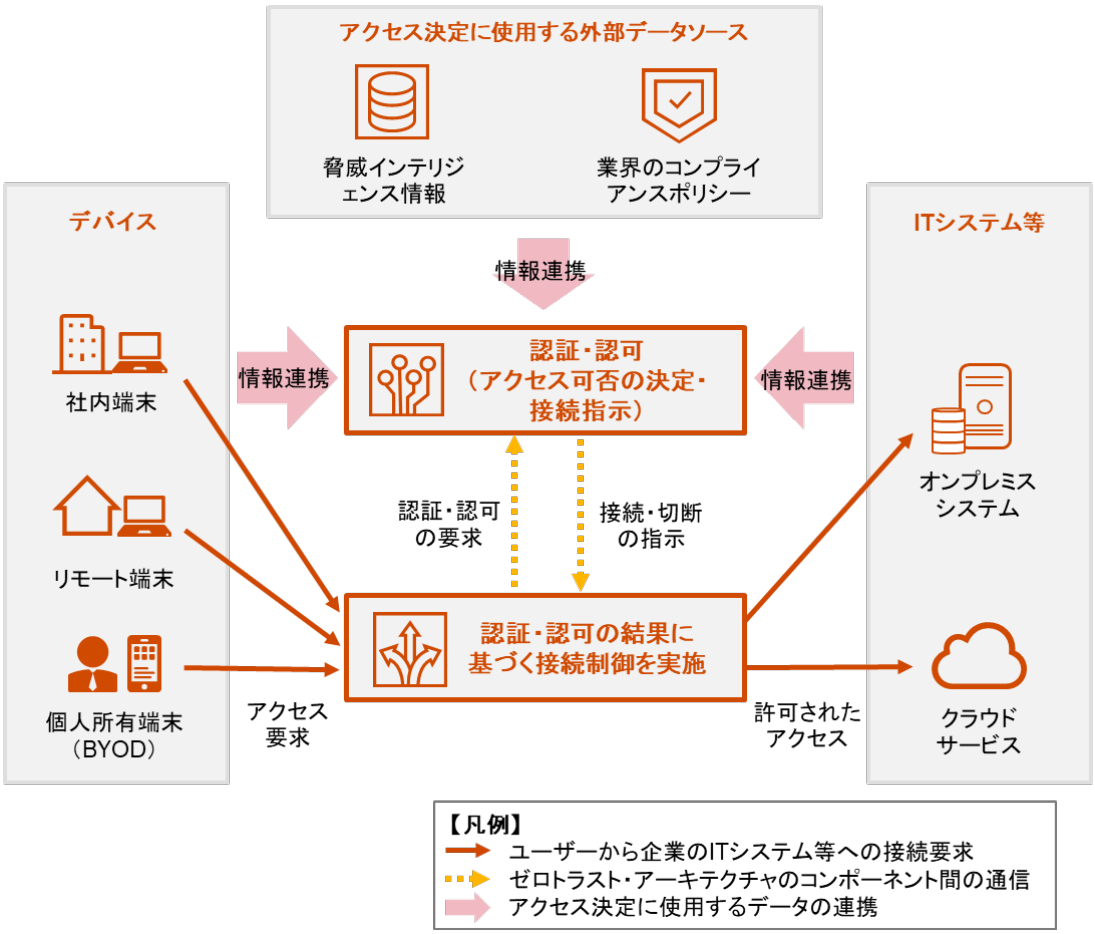
また、これらの原則を取り入れた全社的なサイバーセキュリティの設計思想がゼロトラスト・アーキテクチャと呼ばれる。

ゼロトラスト・アーキテクチャの論理モデルの概要を図表 2-2 に示す。ポイントは以下のとおりである。

- ユーザーから企業の IT システムへのアクセスは、デバイス（社内端末、リモート端末等）が接続されたネットワークの場所を問わず、すべてのデバイスからのアクセスに対してセッション単位で認証・認可を行う。
- デバイスや IT システムの状態（IP アドレス、ソフトウェアのバージョン等）、ユーザーの挙動（接続日時、過去の動作等）、通信ログといった内部の情報に加え、脅威インテリジェンス等の外部の情報を収集し、それらの情報をもとにユーザーからのアクセス要求の信頼性を動的に判断し、アクセス可否を決定する。

ゼロトラスト・アーキテクチャでは、企業が利用するデバイス（社内端末、リモート端末等）、IT システム、アプリケーション、データ等をすべてリソースとみなし、それらのリソースのセキュリティ状況やリソース間の通信の監視を行う。それらの情報を認証・認可の判断にリアルタイムで使用することにより、不正な通信を迅速に遮断することが可能となる。

図表 2-2 ゼロトラスト・アーキテクチャの論理的概要図



※知見をもとに PwC あらた作成

2.4. 境界型セキュリティとゼロトラストの違い

2.4.1. 境界型セキュリティの概要

現在は、内部と外部のネットワークに境界（ペリメーター）を設け、外部からの攻撃や内部からの情報流出をできる限りその境界で防止する境界型セキュリティの考え方が主流である。

一般的な境界型セキュリティでは、企業の内部ネットワークとインターネット等の外部ネットワークとの境界にファイアウォール等が設置され、必要な通信のみが許可される。また、内部と外部の間で通信の橋渡しが必要なメールサーバやインターネットプロキシサーバ等は、ファイアウォールで区切られた DMZ に設置される。こうした構成をとることで、内部のネットワークは、許可されたデバイスやユーザーのみがアクセス可能で、必要な通信のみ流れる信頼できるネットワークとみなされる。

つまり、境界型セキュリティは、企業として守るべき情報資産や IT 資産を信頼できる内部ネットワークに設置することによって保護するという考え方である。

2.4.2. 境界型セキュリティの課題

境界型セキュリティでは、攻撃者の侵入を境界で防ぐ入口対策に加えて、侵入後の被害拡大を防御・検知する内部対策、外部へのデータ流出を防ぐ出口対策等を組み合わせた多層防御の考え方が主流である。しかしながら、内部ネットワークのデバイスや通信は信頼するという考え方が根強いため、実際には境界が突破され不正侵入されてしまうと、内部対策の甘さから、他のデバイスや重要な IT システムへのラテラルムーブメント（水平移動）を攻撃者に許し、被害が拡大することも課題となっている。

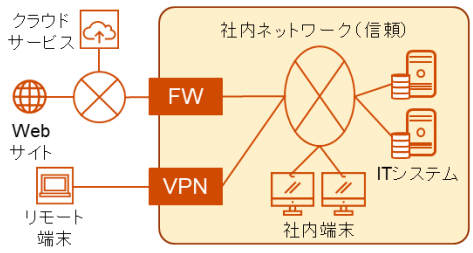
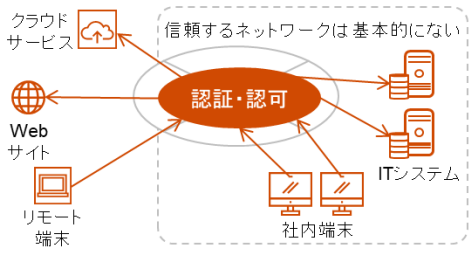
また、「2.2. ゼロトラストが注目を集める背景」にも記載したように、リモートワークの普及やクラウドサービスの利用拡大により、内外通信ニーズが増加し、境界が曖昧・複雑化しつつある点も、境界型セキュリティの課題となっている。具体的には、VPN 経由での外部からのアクセスは許可、特定のクラウドサービスに対する通信なら許可、というような増加するビジネスニーズへの対応がその一因となっている。更には、VPN 装置の脆弱性をついたサイバー攻撃の増加やシャドーIT の利用に起因したクラウドサービスからの情報漏えい等も増えており、境界型セキュリティは益々難しくなっている。

2.4.3. 境界型セキュリティとゼロトラストの違い

境界型セキュリティとゼロトラストの違いを図表 2-3 に示す。

境界型セキュリティに対してゼロトラストは、社内やクラウドサービス上の IT システム等へのアクセスの信頼性を常に検証することで守るという考え方であり、アクセスの都度、アクセス元の信頼性を評価することや、評価に必要な情報を常に収集して動的に更新することが重視される。信頼する内部ネットワークという概念がないゼロトラストという考え方では、デバイスがマルウェアに感染した場合でも、無条件に他のデバイスや IT システムへの通信を許可することはなく、常に動的ポリシーで認証・認可を行うため、マルウェアの拡散のリスクは低い。

図表 2-3 境界型セキュリティとゼロトラストの比較

	境界型セキュリティ	ゼロトラスト
ネットワーク構成イメージ		
信頼するネットワーク	社内ネットワーク（FW内部のWAN、LAN）	基本的にはない ➢ ITシステムや端末を限りなく小さい単位で信頼できるか評価
情報資産・IT資産の場所	信頼できるネットワーク（社内ネットワーク、特にデータセンター）の内部	場所には依存しない ➢ アクセス元の信頼性を都度評価
端末の種類・場所	基本的には社内に設置した自社の端末を利用 ➢ 外部からはVPN等で接続	場所や端末には依存しない ➢ 信頼性を都度評価 ➢ 個人所有端末や他社の端末も利用可能
セキュリティ対策の考え方	特に重視する境界での入口対策・出口対策に、内部対策を加えた多層防御が基本 ➢ 実際には内部対策が十分でない企業が多い	社内リソースへのアクセスの信頼性を常に評価 ➢ アクセス時に信頼性を動的に評価 ➢ ITシステムや端末単位でセキュリティを確保
侵害時の拡散	ラテラルムーブメント（水平移動）により、内部の他の端末やITシステムへの拡散が懸念される	機器間の通信では常に認証・認可を行うため、拡散のリスクは低い

※知見をもとに PwC あらた作成

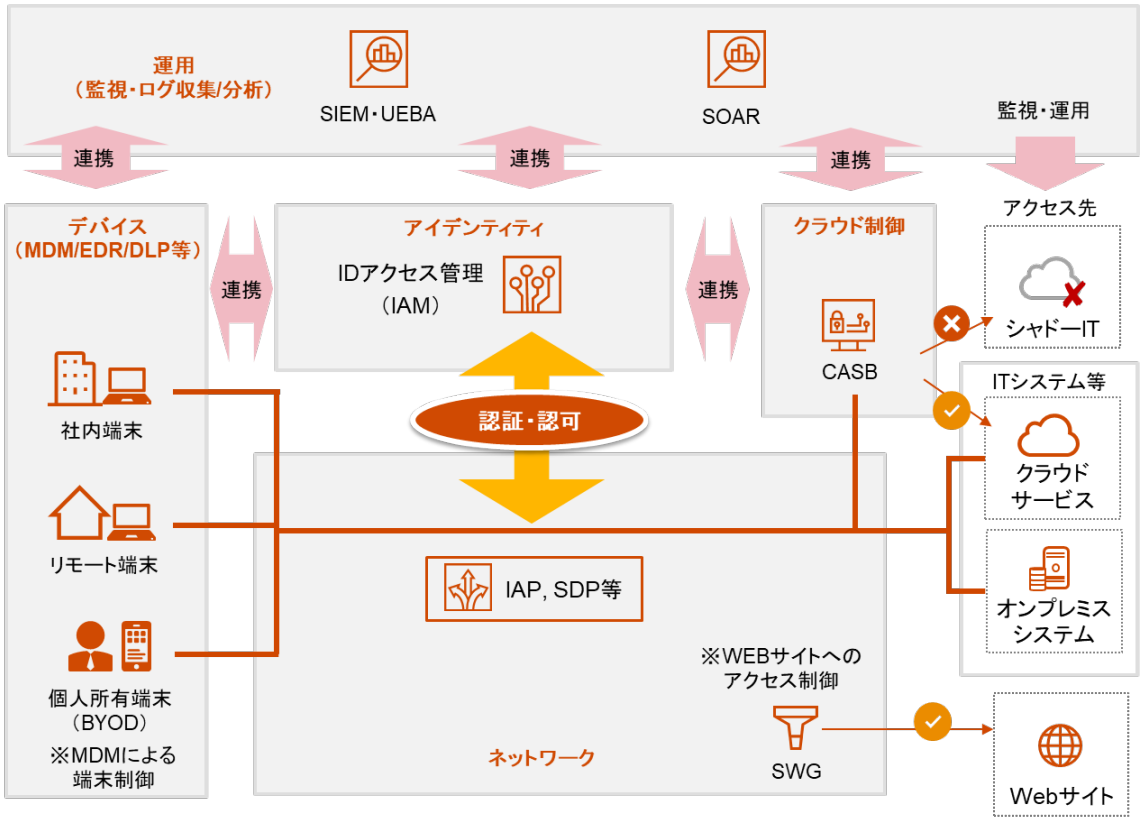
2.5. ゼロトラスト・アーキテクチャの実装イメージ

2.5.1. ゼロトラスト・アーキテクチャを構成するソリューションの分類

ゼロトラスト・アーキテクチャを実装するためのソリューションは大きく「デバイス」、「ネットワーク」、「アイデンティティ」、「クラウド制御」、「運用」に分類できる。

代表的なソリューションを用いてゼロトラスト・アーキテクチャを実装すると図表 2-4 のようなイメージの構成となる。

図表 2-4 ゼロトラスト・アーキテクチャの実装イメージ



※知見をもとに PwC あらた作成

ゼロトラスト・アーキテクチャでは、企業が利用する IT システム等へのアクセスは、必ず認証・認可され、一般的な構成では、認証・認可は IAM（ID アクセス管理）で行われる。また IAM では、デバイスのセキュリティ状況や運用ログ等の情報も活用しアクセス可否の判断するため、MDM（モバイルデバイス管理）等のデバイス管理ソリューションや SIEM（Security Information and Event Management）等の運用ソリューションと連携する。

ゼロトラスト・アーキテクチャを構成するためのソリューションを特定のベンダーのみが提供する製品のみで構成することは、現時点では難しい。そのため、複数ベンダーの製品を利用し、連携させて構成する必要があり、既存の IT 環境で利用しているセキュリティ製品も含めて、製品間の機能連携や互換性の状況なども加味して構成を検討していくことが必要となる。

2.5.2. ゼロトラスト・アーキテクチャを実装するためのソリューション

ゼロトラスト・アーキテクチャを構成する際に利用される代表的なソリューションを図表 2-5 に示す。

ここ数年でゼロトラスト・アーキテクチャの関連製品やサービスは充実してきており、導入実績も増えている。ゼロトラスト・アーキテクチャではインターネット上での通信がメインとなり、また認証・認可を判断するための動的ポリシーでは多くのデータを収集・分析することが想定される。

そのため、これらのソリューションを実現する製品の中には、クラウドサービス、とりわけ SaaS（Software as a Service）として提供されるものも多い。

図表 2-5 ゼロトラスト・アーキテクチャ関連の代表的なソリューション

分類	ソリューション名	概要
デバイス	MDM （Mobile Device Management） モバイルデバイス管理	ノートパソコン、タブレット端末、スマートフォン等のモバイル端末の監視や制御（位置情報を踏まえた制御、遠隔でのロック・データ消去、ポリシーや設定の集中管理、ログ監視等）を行うソリューション。
	MAM （Mobile Application Management） モバイルアプリケーション管理	スマートフォンやタブレット端末等のモバイル端末にインストールされているアプリケーションの管理（アプリケーションのインストール制御、他のアプリケーションとの連携制限、端末へのデータ複製の制限等）を行うソリューション。MDM がデバイスレベルでの管理を行うのに対し、MAM はアプリケーションとデータの管理を行うため、個人所有端末（BYOD）の管理にも利用される。
	EDR （Endpoint Detection and Response） エンドポイント検知・対応	デバイスやサーバにおけるサイバー攻撃を検知する。エンドポイント上の挙動に関わる情報を収集・分析し、不審な挙動を検知した場合は、迅速に対応（隔離や機能停止）を行うことで、ラテラルムーブメント等による被害や影響の拡大を防ぐことを支援するソリューション。
	DLP （Data Loss Prevention） データ漏えい防止	デバイスやサーバに保管されている機密情報が含まれたデータを検出し、そのデータに対して送信やコピー等の制限や監視を行うソリューション。
ネットワーク	IAP （Identity-Aware Proxy） ID 認識型プロキシー	オンプレミスやクラウド上のアプリケーションに対し行われるユーザーからのアクセスリクエストを IAM 等と連携し集中的に認証・認可するソリューション。プロキシーという名のとおり、ユーザーからアプリケーションアクセスは常に IAP を経由し認可されたアプリケーション、権限でのみにアクセスが可能となる。

分類	ソリューション名	概要
	SDP （Software Defined Perimeter） ソフトウェア定義ペリメーター	オンプレミスやクラウド上の IT システム等に対するユーザーからネットワーク接続要求を、コントローラーが中心となり、IAM と連携して認証・認可するソリューション。アクセスが許可されると、ユーザー側とアクセス先の IT システム等の間で、直接仮想通信網が構築されるが、一連の通信が終了すると仮想通信網は消滅するなど、境界がソフトウェアにより動的に構成・制御される。
	SWG （Secure Web Gateway） セキュア Web ゲートウェイ	業務上不要な Web サイトへのアクセス制限やダウンロードしたファイルのチェック等の Web サイトへのアクセス制御機能をクラウド型で提供するソリューション。
	次世代ファイアウォール （NGFW：Next Generation Firewall）	接続元/先や通信ポートにて制御する従来のファイアウォール機能に加え、サイバー脅威に対し、よりきめ細やかな制御ができるソリューション。有害な Web サイトやアプリケーション等を識別してアクセスを制御する機能や IPS の機能等を有したファイアウォールのこと。マイクロセグメンテーションのためなどにも利用される。
アイデンティティ	IAM （Identity and Access Management） ID アクセス管理	ユーザーの ID とアクセス情報を管理し、本人確認（認証）、適切なアクセス権限の付与（認可）、SSO（シングルサインオン）等を行うソリューション。
クラウド制御	CASB （Cloud Access Security Broker、キャスビー）	業務部門で契約しているものや個人で利用しているものも含め、自社で利用されているすべてのクラウドサービス（SaaS）の利用の可視化、安全性評価、通信遮断等の管理・制御を行うためのソリューション。
運用	SIEM （Security Information and Event Management、シーム） セキュリティ情報イベント管理	様々な機器やソフトウェアのログを一元的に管理・蓄積し、セキュリティ上の脅威となる事象を検知・分析するためのソリューション。
	SOAR （Security Orchestration, Automation and Response、ソアー）	脅威情報の管理・分析・優先度付け、インシデント管理の可視化・効率化、既知インシデントに対する定型対応の自動化等により、セキュリティ運用の自動化・効率化を実現するためのソリューション。
	UEBA （User and Entity Behavior Analytics）	機械学習等を利用してユーザーや機器の行動を分析し、通常と異なるユーザーの振る舞いを異常行動として検知するソリューション。

※知見をもとに PwC あらた作成

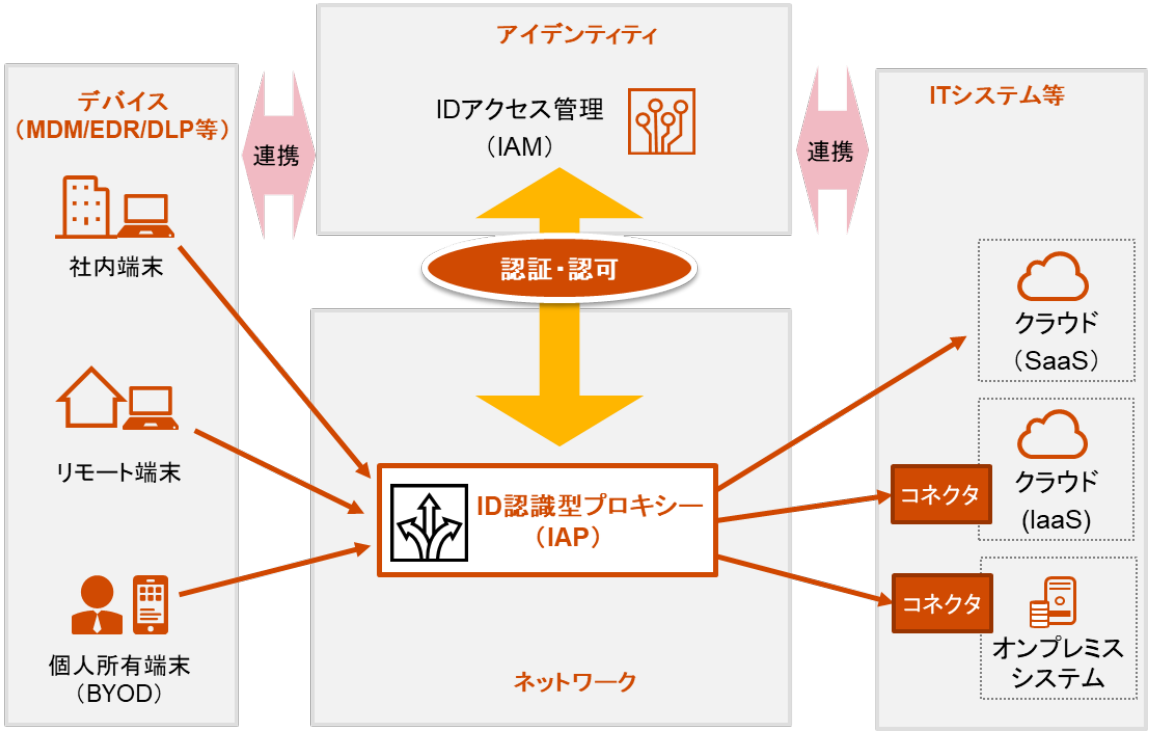
2.5.3. ゼロトラスト・アーキテクチャの主な実装イメージ

ゼロトラスト・アーキテクチャを実装するためのアプローチは多様であるが、大きく分けるとアイデンティティを中心としたものと、ネットワークを中心としたものが主流である。

(1) アイデンティティ中心のアプローチによる実装イメージ

アイデンティティ中心のアプローチによる実装イメージを図表 2-6 に示す。ユーザーから IT システム等へのアクセスをユーザーID にて制御し、IAP（ID 認識型プロキシー）と IAM（ID アクセス管理）が連携して認証・認可を行う。具体的には、IAM がアクセス元のユーザーID 情報に加えて、使用デバイスの状態やユーザーの行動に関する情報等を使用して、IT システム等へのアクセスの認証・認可を行い、IAP は IAM が決定したアクセス可否等をユーザーからのアクセス要求に対し適用する。

図表 2-6 アイデンティティ中心のゼロトラスト・アーキテクチャの実装イメージ



※知見をもとに PwC あらた作成

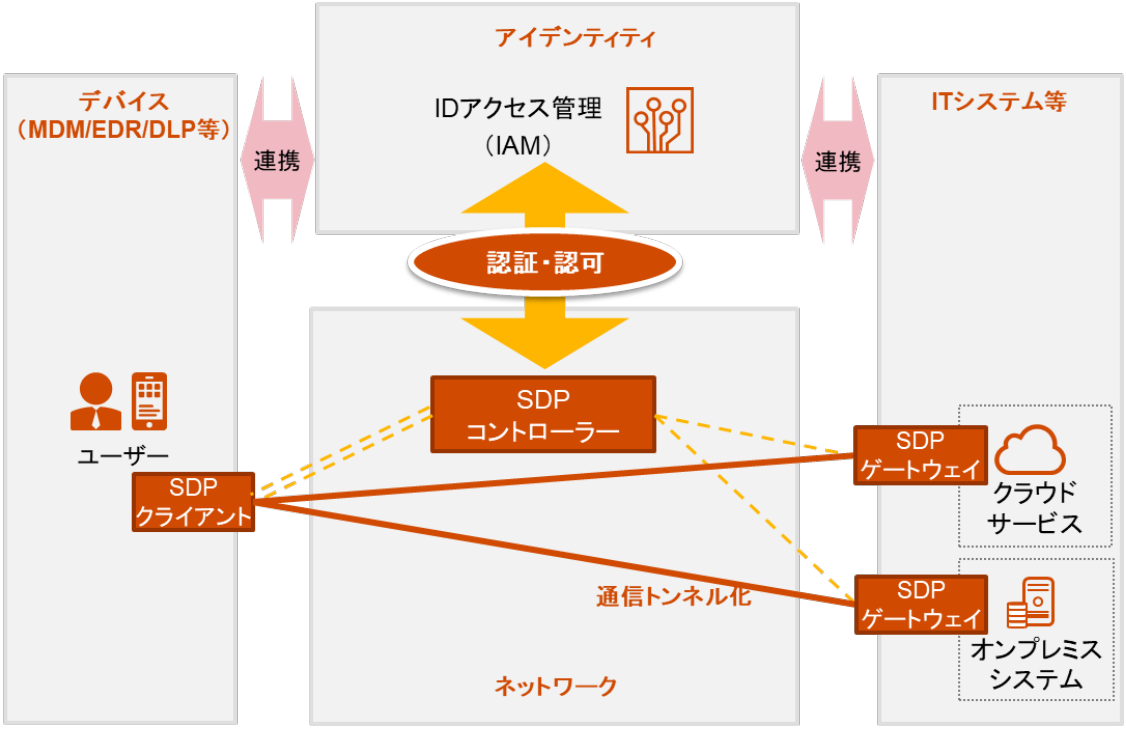
(2) ネットワーク中心のアプローチによる実装イメージ

ネットワーク中心のアプローチを実装する代表的なソリューションとして、SDP（Software Defined Perimeter）が挙げられる。SDP は、仮想的に境界を作ることでセキュアな通信を実現するソリューションである。IT システム等へのアクセスは、SDP コントローラーによって制御される。SDP コントローラーによってアクセスが許可された場合にのみ、SDP クライアント（接続元デバイス側）と SDP ゲートウェイ（IT システム側）の間でセキュアな通信用のトンネルが構成され、アクセスが可能となる。そのため、例えば、IT システムにアクセスしてから認証を行う接続方式と異なり、SDP では IT システムへの接続の前に、SDP コントローラーによる認証が先に実施される。したがって、SDP コントローラーによる認証が行われていないアクセスや拒否されたアクセスは、IT システム等への接続自体が行われないため、信頼性が確認できないアクセス元から IT システム等へ不正に通信されるリスクを低減できる。

図表 2-7 は、ユーザーからのクラウドサービスおよびオンプレミス環境への接続を SDP によって制御しているイメージである。ネットワーク中心のゼロトラスト・アーキテクチャは、SDP コントローラーが IAM（ID アクセス管理）と連携し、IAM がアクセスの認証・認可を実施する機能を担う

構成となる。IAM でアクセスが許可された場合、SDP コントローラーがデバイス側の SDP クライアントと IT システム側の SDP ゲートウェイ間で通信可能なセキュアなトンネルを構成する。このトンネルは VPN のような継続的に有効なものではなく、セッション毎に再度 IAM による認証・認可を受けて再構成される。

図表 2-7 ネットワーク中心のゼロトラスト・アーキテクチャの実装イメージ



※知見をもとに PwC あらた作成

なお、ネットワーク中心のアプローチとして、ネットワークやセキュリティの機能をクラウドサービスで実現する SASE（Secure Access Service Edge、サッシー）と呼ばれる考え方がある。

SASE は、米国ガートナー社が提唱したものであり、以下のように定義されている。

"*The secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of digital enterprises.*"[4]

（参考日本語訳）

SASE（Secure Access Service Edge）は、デジタル企業の動的でセキュアなアクセスへのニーズをサポートするために、包括的な WAN 機能と包括的なネットワークセキュリティ機能（SWG、CASB、FWaaS[5]、ZTNA[6]など）を組み合わせて提供するものである。

[4] Gartner, China Summary Translation: 'The Future of Network Security Is in the Cloud', Peter Liu, Neil MacDonald, 28 Feb 2020
https://www.gartner.com/document/3981540?ref=solrAll&refval=288164225（要 Gartner 購読権）

[5] FWaaS：Firewall as a Service の略

[6] ZTNA：Zero Trust Network Access の略

SASE は、これまでのデータセンターをアクセスの中心として位置づけるネットワークアーキテクチャではなく、ネットワーク機能とセキュリティ機能をクラウドサービスとして包括的に提供するという考え方である。ユーザーやデバイスのアイデンティティ、企業のセキュリティポリシーやコンプライアンスポリシーなどをもとに、ゼロトラスト・アーキテクチャと同じような認証・認可に関するセキュリティ機能に加え、トラフィックやキャッシュの状況を加味して最適な接続経路や接続方法を選択するネットワーク機能を提供する。

3. NIST SP800-207 の概要と解説

本章では、NIST SP800-207（原文および日本語訳）に記載されているゼロトラスト・アーキテクチャの概要について紹介する。なお、本章の NIST SP800-207 に関する解説は、文献調査やヒアリングを通じて得られた情報を参考にした解釈を含むものである。

また NIST SP800-207 の日本語訳は参考訳であり、完全性・正確性を保証するものではない点に留意が必要である。

3.1. ゼロトラスト・アーキテクチャの概要

3.1.1. ゼロトラストの原則

NIST SP800-207 の「2 ゼロトラストの基本」では、ゼロトラスト・アーキテクチャの設計・展開にあたって、以下の 7 つの原則を理想的な指針として挙げている。これらの原則は、NIST SP800-207 が理念的な目標として定めているものであり、採用するゼロトラストの戦略によっては、これらのすべての原則を、完全に満たさないゼロトラスト・アーキテクチャもあり得るとされている。

各原則の概要は、以下のとおりである。

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**
   企業が所有するすべてのリソースを対象とする。対象には SaaS（Software as a Service）などのクラウドサービスも含まれる。また個人所有端末（BYOD[7]）を利用して、企業リソースへアクセスする場合には、BYOD も対象に含む。

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**
   企業内ネットワークかどうかに関係なく、リソースへのアクセス要求を行うすべての通信の機密性・完全性を確保する。

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**
   リソースへのアクセスが許可される前に、アクセス元の信頼性を評価する。またアクセスの許可は、タスクを実行するための最小限の権限で許可されるべきである。セッション単位でのアクセス付与について、セッション開始やトランザクション実施前に、認証・認可が直接発生しない場合もあるとしているが、アクセス対象のリソースが変わる場合は、常に認証・認可を実施するべきとしている。

[7] BYOD：Bring Your Own Device の略。従業員が個人で所有する端末の業務利用を許可し、活用すること。

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**

　アクセス元のユーザーアカウントに関する情報（ID・パスワード、所属部門、役職等）や、ユーザーの行動履歴、アクセス元のリソースの状態（証明書、OS のバージョン、ネットワークの場所等）等をもとに、対象ユーザーからリソースへのアクセス可否を動的に決定する。

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**

　個人所有端末（BYOD）等も含めたデバイスやアプリケーションは、本質的に信頼されないものとして、すべて監視する必要がある。監視の結果、脆弱性があると判断されたデバイスがある場合は、パッチ等を適用させる、接続を拒否する、権限を制限する等の対応を行うこととなる。

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密に実施する**

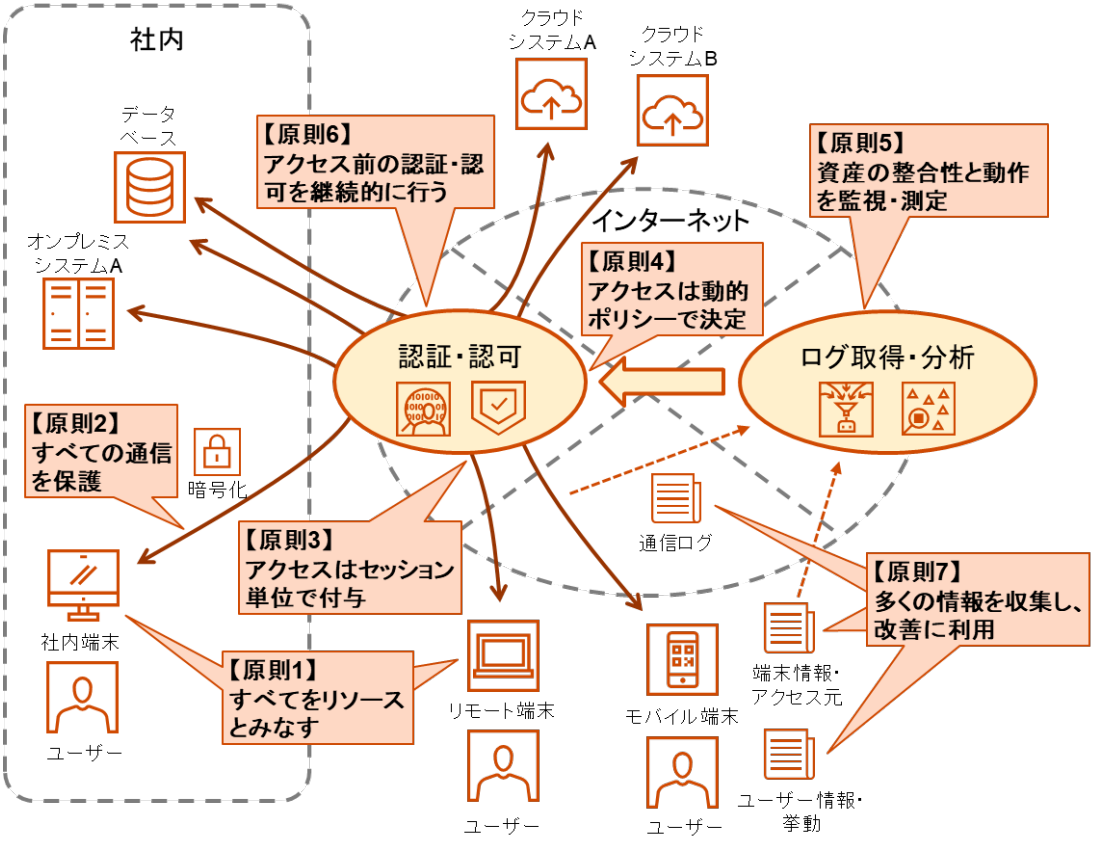
　すべての企業リソースに対するアクセスに対して、継続的にアクセスの信頼性を動的ポリシーにて再評価する必要がある。トランザクション全体に渡って継続的な監視を行い、セキュリティ、可用性、ユーザビリティ等のバランスを考慮した上で、必要に応じて再認証を行う。

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**

　リソースのセキュリティ状況や、ネットワークトラフィック、アクセス要求に関するデータを収集し、動的ポリシーの作成に使用する。（使用するデータの例は「3.1.4. ポリシーエンジンのトラストアルゴリズム」参照）

　IT 環境にこれらの原則を取り入れると図表 3-1 のようになる。これらの原則を実装するための具体的な技術要素は NIST SP800-207 では指定されておらず、様々な技術による実現方法が考えられる。また、これらの原則は、基本的には社内のビジネスプロセスを対象とし、インターネットユーザー等の不特定多数のユーザーとのビジネスプロセスには適用されないことを前提としたものである。ただし、登録顧客等の内部ポリシーを適用可能な外部ユーザーについては、対象となる場合がある。

図表 3-1 ゼロトラスト・アーキテクチャと 7 原則の関連図



※知見をもとに、PwC あらた作成

3.1.2. ゼロトラスト・アーキテクチャの論理コンポーネント

本項では、NIST SP800-207 の「2 ゼロトラストの基本」および「3 ゼロトラスト・アーキテクチャの論理的構成要素」の内容を参考に、ゼロトラスト・アーキテクチャの論理コンポーネントについて解説する。

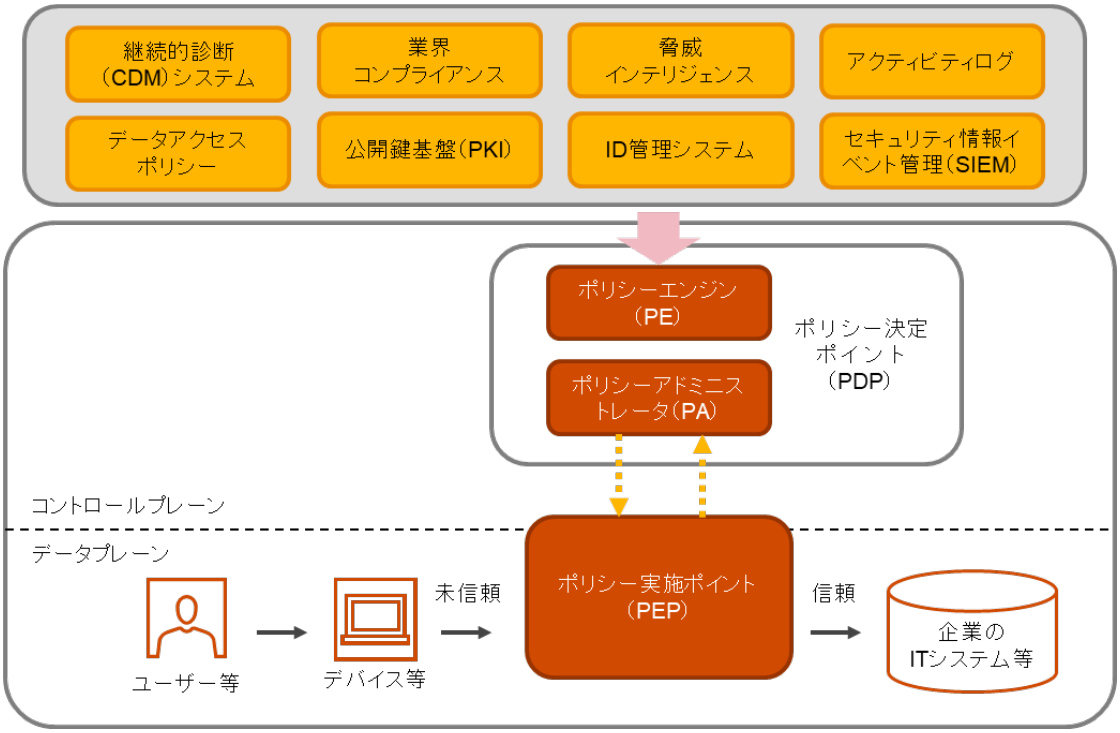
ゼロトラスト・アーキテクチャは、可能な限り粒度の細かいアクセス制御を実施することにより、データやサービスへの不正アクセスを防止することを目的とし、動的ポリシーによる認証・認可および認証・認可後の信頼されているアクセスとみなされる領域（暗黙のトラストゾーン）の縮小に焦点を当てている。

NIST SP800-207 に記載されているゼロトラストの中核となる論理コンポーネントとその関係性の概念図を図表 3-2 に示す。デバイスまたはユーザーが、企業の IT システム等へアクセスするためには、認証・認可を実施するポリシー決定ポイント（PDP）とポリシー実施ポイント（PEP）を必ず通過する必要がある。それらのポイントではアクセス要求を評価し、アクセスを許可するかどうかの決定を行っている。

暗黙のトラストゾーンとは、PDP・PEP 通過後のアクセスが信頼されている状態の領域であり、NIST SP800-207 では空港のセキュリティゲートを通過した後の搭乗エリアに例えて解説している。セキュリティチェックを終了した搭乗エリアにいる乗員や職員は信頼できる人として考えられているのと同様に、PDP・PEP を通過したトラフィックは信頼されたものと見なされる。PDP・PEP にてより精度の高いアクセス制御を実施するためには、PDP・PEP をより IT システム等に近づけ、この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。

これらのすべてのリソースへのアクセスに対する明示的な認証・認可の実施、および暗黙のトランストゾーンの縮小が、NIST SP800-207 のゼロトラスト・アーキテクチャの基本である。

図表 3-2 ゼロトラスト・アーキテクチャの中核となる論理コンポーネント



※NIST SP800-207 をもとに PwC あらた作成

ゼロトラスト・アーキテクチャの各論理コンポーネントの定義は図表 3-3 のとおりである。

図表 3-3 各論理コンポーネントの定義

論理コンポーネント		説明
ポリシー決定ポイント（PDP）	ポリシーエンジン（PE）	リソースへのアクセスの許可または拒否の最終的な決定を行う
	ポリシーアドミニストレータ（PA）	ポリシーエンジン（PE）の決定をもとに、主体（ユーザー等）とリソース間の通信経路の確立や遮断をポリシー実施ポイント（PEP）にて実行させる
ポリシー実施ポイント（PEP）		ポリシーアドミニストレータ（PA）と連携して、主体（ユーザー等）とリソース間の接続の有効化、監視、切断を行う

※NIST SP800-207 をもとに PwC あらた作成

ゼロトラスト・アーキテクチャの論理コンポーネントの中で、中心となるのがリソースへのアクセス許可を評価し、最終的に決定するポリシーエンジン（PE）である。より精度の高い評価を実施するためには、ポリシーエンジン（PE）がアクセス許可をどのような情報をもとに決定するかが重要になる。アクセス元であるユーザーがどの程度信頼できるか、使用しているデバイスがどのような状況か、またはアクセス元の位置情報に不審な変化がないかどうか等の様々な情報をもとに、アクセス要求を評価できるようにするためには、アクセス許可を判断するポリシーエンジン（PE）が、それぞれのデータソースと連携し、情報を取り入れる必要がある。図表 3-2 に示したように、ポリシーエンジン（PE）が連携するデータソースとし

ては、企業のデータアクセスポリシーや、ID 管理システム、セキュリティ情報イベント管理（SIEM）システムの情報だけではなく、外部からの脅威インテリジェンス等も挙げられる。

また、図表 3-2 に示したように、ネットワーク制御のための通信を行うコントロールプレーンとアプリケーションやサービスのデータ通信を行うデータプレーンを物理的または論理的に分離する必要がある。アクセス制御や認証情報のやり取りで使用する通信と、ユーザーのデータ通信が分離している点がゼロトラスト・アーキテクチャのネットワークの特徴である。

なお、ゼロトラスト・アーキテクチャの論理コンポーネントの実装では、各コンポーネントが複数のハードウェアまたはソフトウェアで構成される場合や、複数のコンポーネントが単一サービスで組み合わされている場合もある。一般的には、ポリシーエンジン（PE）は、単体の製品としてではなく、IAM（ID アクセス管理）等の他の機能の製品に組み込まれている提供されていることが多い。

3.1.3. ゼロトラスト・アーキテクチャの 3 つのアプローチ

ゼロトラスト・アーキテクチャの実装に関するアプローチとして、NIST SP800-207 の「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」では以下の 3 つを提示している。各アプローチは、ゼロトラストの原則（「3.1.1. ゼロトラストの原則」参照）を実装しているが、完全なゼロトラストソリューションには、3 つのアプローチのすべての要素が含まれるとしている。

(1) 拡張されたアイデンティティガバナンスを利用したゼロトラスト・アーキテクチャ

このアプローチは、認証・認可の重要な要素として、ユーザー等のアイデンティティを使用する。このアプローチでは、企業の IT システム等へのアクセス可否は、アイデンティティとアイデンティティの属性に基づいて決定される。IT システム等へのアクセスは、ユーザーに付与されたアクセス権限に基づくが、使用しているデバイスや IT システム等の状態、および環境要因等の他の要素を、アクセスの信頼度の計算において考慮する。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アクセスのみを許可する等、ユーザーのアイデンティティだけではなく、デバイスのアイデンティティやステータスの情報も二次的なデータとして使用し、アクセス権限が判断される。

このアプローチは、企業がゼロトラストのセキュリティコンポーネントを自由に構成できない SaaS などの IT システムに対しても利用可能であるという特徴がある。

(2) マイクロセグメンテーションを利用したゼロトラスト・アーキテクチャ

このアプローチは、ネットワークのマイクロセグメンテーションにより実現する方法である。一般的には、ネットワークのセグメント毎に複数のサーバが配置され、ファイアウォールは同一セグメント内の通信を制御しないが、マイクロセグメンテーションのアプローチは、そのセグメントをより細分化することにより、各サーバやアプリケーション単位へのアクセスを制御する方法になる。つまり、次世代ファイアウォール等のデバイスによって、ネットワークをより小さな論理セグメントに分割し、許可されたアクセスのみが、それらのセグメントにある企業の IT システム等にアクセスできるようにするというアプローチである。

このアプローチでは、次世代ファイアウォール等のデバイスを、ポリシー実施ポイント（PEP）として配置する。あまり高度では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採用して、マイクロセグメンテーションの機能の一部を実装することも可能ではあるが、管理コストと迅速な変化への対応が困難であるとされている。

このアプローチでは、ポリシー実施ポイント（PEP）として機能するデバイスが正しく管理され、脅威やワークフローの変化に対応するために、必要に応じて再構成可能であることが重要となる。

(3) ネットワークインフラと Software Defined Perimeter を利用したゼロトラスト・アーキテクチャ

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ゼロトラスト・アーキテクチャを実装する方法である。アプリケーション層またはそれより下位のレイヤーにて、仮想的なネットワーク（オーバーレイネットワーク）を構成する方法である。NIST SP800-207 では「2.5.3. ゼロトラスト・アーキテクチャの主な実装イメージ」に記載した SDP（Software Defined Perimeter）を使用したアプローチを挙げている。このアプローチでは、アクセス元とアクセス先のリソース間の通信をトンネル化し、ネットワーク上で動的に境界をつくりだす方法である。

上記の 3 つのアプローチの中では、(1)と(3)が、ソリューションとして提供・導入されるケースが多い傾向にある。(1)と(3)のアプローチによるソリューションの実装イメージは、「2.5.3. ゼロトラスト・アーキテクチャの主な実装イメージ」に記載している。

3.1.4. ポリシーエンジンのトラストアルゴリズム

本項では、NIST SP800-207 の「3.3 トラストアルゴリズム」の内容を参考に、ゼロトラスト・アーキテクチャのトラストアルゴリズムについて解説する。

「3.1.2. ゼロトラスト・アーキテクチャの論理コンポーネント」に記載したとおり、ポリシーエンジン（PE）は、アクセスを動的に評価し、アクセス許可の判断を行うゼロトラスト・アーキテクチャの頭脳であり、その思考プロセスをトラストアルゴリズムと呼ぶ。ポリシーエンジン（PE）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トラストアルゴリズムおよびトラストアルゴリズムが使用する情報はゼロトラスト・アーキテクチャにおいて重要なものとなる。以下にトラストアルゴリズムに入力データとして使用される主な情報および入力された情報の評価方法（トラストアルゴリズム）を解説する。

(1) トラストアルゴリズムにて使用される主な情報

ゼロトラスト・アーキテクチャにおいて、ポリシーエンジン（PE）は、連携している複数のデータソースをインプットにし、アクセス可否の決定を行う。以下は、NIST SP800-207 で紹介されているトラストアルゴリズムの入力データとして使用される情報の例である。

a) アクセス要求に関する情報

アクセス先のリソースの情報や、リクエスト元のデバイス等の情報（OS のバージョンや使用されているソフトウェア）等の情報である。

b) 主体データベースと履歴の情報

リソースへのアクセスを、「誰が」リクエストしているかという情報であり、リクエストを実施しているユーザーの属性や権限の情報である。ユーザーID の信頼度の計算においては、時間と地理的位置を属性として含めることや、過去の行動データを計算に使用することが考えられる。これらの情報は、通常 ID 管理システムやポリシー情報のデータベースに格納される。なお、ユー

ザーへの特権付与については、ユーザーの組織内での役割に応じてグループで付与するのではなく、個々のユーザー毎に個別に割り当てるべきとされている。

c) デバイスとその状態に関する情報

企業が所有するデバイスのステータス情報である。場合によっては、企業外のものや個人所有端末（BYOD）も対象となる。このデータベースには、デバイスの OS のバージョン、ソフトウェアの情報、ネットワークおよび地理的位置情報、パッチレベル等のステータスの情報が含まれる。

d) リソースに対するアクセス要件の情報

リソースへのアクセスに関する要件の情報であり、リソースの特性や関連する業務上での要求等に応じて定められる。例として、海外 IP アドレスからのアクセスを拒否する等の接続元の地理的制限や、リソースに格納されたデータの機密性に応じた接続元への制限、接続元のデバイスの構成に対する要件等などが挙げられる。リソースへのアクセスに求められる要件は、リソースのデータ管理者や、データを利用するビジネスプロセスの責任者の両方によって検討されるべきであるとしている。

e) 脅威インテリジェンス

インターネットでの一般的な脅威情報や、マルウェア等の情報であり、一般的には外部サービスを利用して入手することが多い。

(2) トラストアルゴリズムにおける評価方法

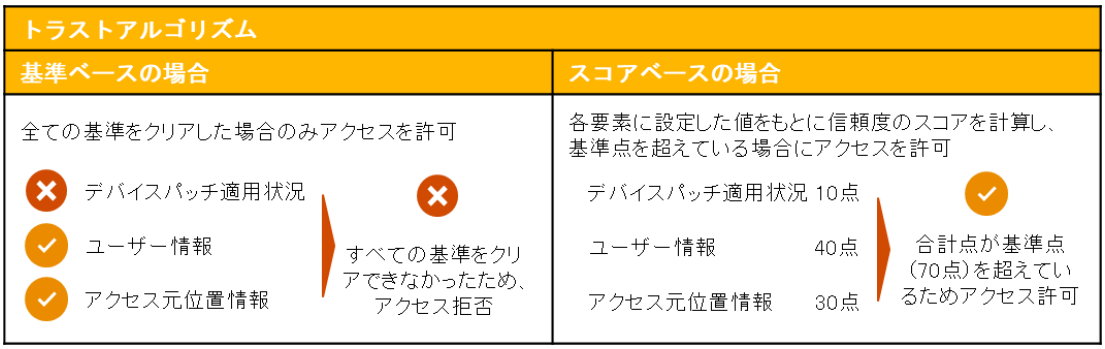
上記の各データソースの情報をもとにしてトラストアルゴリズムを使用してポリシーエンジン（PE）はアクセス可否の判断を行うが、トラストアルゴリズムでのデータの評価には様々な方法がある。NIST SP800-207 で紹介されているトラストアルゴリズムでの評価方法として、2 つの観点があり、1 つ目はデータ要素がどのように評価されるか（基準ベース vs スコアベース）、2 つ目はリクエストがどの時点のデータをもとに評価されるか（単一的 vs 文脈的）である。

a) 基準ベース vs スコアベース

データ要素の評価方法には、基準ベースとスコアベースがある。基準ベースは、設定した基準をベースとし、それをすべて満たした場合にアクセス許可を実施する方法である。スコアベースは、各データソースの値と、それに設定した重みづけに従って信頼度のスコアを計算し、最終的にスコアが閾値よりも高い場合にアクセス許可を実施する方法である。基準ベースは、設定が簡潔になるという長所がある。一方でスコアベースは、企業の基準に合わせて各要素の重みづけを設定するなどより詳細な設定をすることができる。

それぞれの評価イメージを図表 3-4 に示す。この例では、デバイスのパッチが 2 カ月前のものであったとして、基準ベースではその基準（例えば最新のパッチを適用している）を満たしていないためアクセスは拒否される。一方で、スコアベースの場合は、パッチ適用の評価は低くなるものの、他の情報から信頼度が高いと判断された場合、総合的に基準点を上回ればアクセスは許可される。

図表 3-4 トラストアルゴリズム（基準ベース・スコアベース）のイメージ



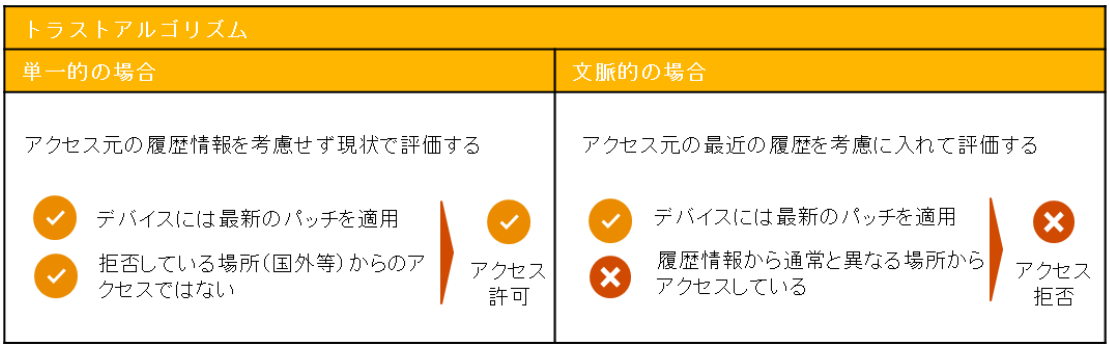
※知見をもとに、PwC あらた作成

b) 単一的 vs 文脈的

どの時点のデータをもとに評価を行うかは、単一的なものと文脈的なものがある。単一的なトラストアルゴリズムは、各リクエストを個別に扱い、評価の際にアクセス元のユーザーの履歴情報を考慮しない方法である。文脈的なトラストアルゴリズムは、アクセス元のユーザーやデバイスの履歴情報を考慮して判断する方法であり、これまでの行動パターンと異なる場合には、追加の認証チェックやアクセスリクエストの拒否を行う方法である。

図表 3-5 は、単一的および文脈的な評価のイメージであり、ユーザーが通常と異なる場所からアクセスしてきた場合に、単一的な評価方法では許可され、文脈的な評価方法では、ユーザーのアクセス元の位置の履歴情報から、通常と異なる場所からのアクセスのため信頼性が低いと判断されて拒否または追加認証が要求される。

図表 3-5 トラストアルゴリズム（単一的・文脈的）のイメージ



※知見をもとに PwC あらた作成

企業のインフラストラクチャの構成によって常に可能とは限らないが、上記のトラストアルゴリズムの評価方法のうち、単一的よりも文脈的であるものが望ましいとされている。文脈に基づいたトラストアルゴリズムを適用することにより、攻撃者に乗っ取られたアカウントや、内部攻撃のアクセス等による、正常なアカウントからの通常と異なるアクセスのリスクを軽減できるためである。単一的なトラストアルゴリズムは、迅速な評価ができる一方、アクセス元の履歴情報等の文脈的な情報を考慮しないため、正常な権限を持つユーザーからの攻撃を検出できない可能性がある。

どのようなトラストアルゴリズムを適用するかは、ユーザーから企業の IT システム等へのアクセスに影響を与えるため、トラストアルゴリズムを定義して実装する際には、セキュリティとユーザーの利便性等のバランスをとることが重要となる。

3.1.5. ゼロトラスト・アーキテクチャに関する脅威

ゼロトラスト・アーキテクチャを適切に実装し、運用することで、全体的なサイバーセキュリティのリスクを低減し、一般的な脅威から保護することができる。ただし、サイバーセキュリティのリスクはどのような企業であっても排除することは難しく、またゼロトラスト・アーキテクチャ特有の脅威も存在する。本項では、NIST SP800-207 の「5 ゼロトラスト・アーキテクチャに関連する脅威」の内容を参考に、ゼロトラスト・アーキテクチャに関する脅威を解説する。

a) ゼロトラスト・アーキテクチャの決定プロセスの転覆

これは、ポリシー決定ポイント（PDP）に関する脅威である。ゼロトラスト・アーキテクチャでは、ポリシーの決定を行うポリシーエンジン（PE）および通信経路の確立を行うポリシーアドミニストレータ（PA）が重要な役割を担う。ユーザーからリソースへのアクセスは、必ずこれらのコンポーネントによる承認が必要とされるため、適切に設定され、維持されなければならない。ポリシーエンジン（PE）の構成に関するアクセス権を持つ管理者ユーザーは、承認のない変更やミスを行わないようにする必要がある。そのため、ポリシーエンジン（PE）とポリシーアドミニストレータ（PA）は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、監査の対象とする必要がある。

b) サービス拒否またはネットワーク障害

企業リソースへの接続は、ポリシーアドミニストレータ（PA）が通信経路を制御しているため、ポリシーアドミニストレータ（PA）におけるネットワーク障害や DoS 攻撃（Denial-of Service attack）等は、リソースへのアクセスに影響を与える。また、ポリシーエンジン（PE）やポリシーアドミニストレータ（PA）にクラウドサービスを利用している場合は、サービスプロバイダ側の原因によりサービスが利用できなくなるケースも考えられる。

c) 盗まれたクレデンシャル/内部の脅威

ゼロトラスト・アーキテクチャは、適切に実装することで、搾取された認証情報による攻撃や内部からの不正アクセスのリスクを軽減し、ラテラルムーブメント（水平移動）を防ぐことができる。しかし、フィッシングやソーシャルエンジニアリング等によるアカウントへの攻撃や、有効な認証情報を持つ内部攻撃により、リソースが不正にアクセスされるリスクは依然としてある。

文脈的なトラストアルゴリズムを採用することで、通常の行動から外れたアクセスパターンを検出し、機密リソースへのアクセスを拒否するなど、従来からの境界型セキュリティでのアプローチよりも迅速に対応できる可能性が高い。

d) ネットワーク上の可視性

「3.1.1. ゼロトラストの原則」の原則 7 にあるように、ゼロトラスト・アーキテクチャでは、すべてのネットワークトラフィックを監視し、分析のために使用する必要がある。しかし、通信が暗号化されている場合や、企業が所有していない資産からの通信など、通常のネットワークの解析ツールでは十分に解析できない場合がある。

暗号化されたトラフィックの送信元や宛先アドレスなどのメタデータを収集し、それらを使用してネットワーク上で通信している攻撃者や潜在的なマルウェアを検出することができる。また機械学習の技術で、復号化および検査できないトラフィックの分析に使用する方法も考えられる。

e) 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、分析および動的ポリシーへの連携のために保存されているデータは、攻撃者の標的となり得る。ネットワークトラフィックの情報だけではなく、ネットワーク構成図、設定ファイル等の文書等も、攻撃者がこれら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リソースを特定することができる可能性があるため、保護する必要がある。

上記の情報を含む、すべての重要な企業データについては、不正アクセスを防ぐために、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構成すべきである。

f) 独自のデータフォーマットやソリューションへの依存

ゼロトラスト・アーキテクチャは、ID 管理ツールやデバイス管理ツール、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をもとにアクセス可否の決定を行うものであるため、システムまたは製品間の連携が重要となる。これらの情報連携の標準化が進んでいないため、企業が一部のベンダーにロックインされる状況となる可能性がある。あるベンダーにセキュリティ上の問題や障害が発生した場合のコストや、別のソリューションへの移行が必要となった場合にも、切り替えのための時間やコストがかかる可能性がある。DoS 攻撃と同様に、このリスクはゼロトラスト・アーキテクチャに特有のものではないが、企業のビジネスへ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べきである。

g) ゼロトラスト・アーキテクチャにおけるノンパーソンエンティティの利用

これは、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（ノンパーソンエンティティ）を、企業ネットワークのセキュリティ管理で使用する場合の考慮点である。人間の管理者の代わりに、人工知能等のエージェントがゼロトラスト・アーキテクチャの論理コンポーネント（ポリシーエンジン（PE）やポリシーアドミニストレータ（PA）等）と対話する必要がある場合には、認証方法や構成について検討する必要がある。ソフトウェアエージェントは、一般的に人間のユーザーと比較して、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の基準が低くなる可能性があり、理論的には攻撃者がソフトウェアエージェントを攻撃し、なりすまし等に利用される危険性がある。

3.2. ゼロトラスト・アーキテクチャの導入

本項では、NIST SP800-207 の「7 ゼロトラスト・アーキテクチャへの移行」の内容を参考に、ゼロトラスト・アーキテクチャの導入ステップを解説する。

NIST SP800-207 では、ゼロトラスト・アーキテクチャの実装は、一度の更新で全面的に移行できる可能性は低く、ひとつの道のりとして考えて、段階的に導入することを目指すべきであるとされている。さらに多くの企業で、ゼロトラスト・アーキテクチャと境界型セキュリティのアーキテクチャが永遠に共存し運用されていく可能性があるとしている。

境界型セキュリティと共存する場合は、企業は、共通のコンポーネント（ID 管理、デバイス管理、イベントロギング等）が、ゼロトラスト・アーキテクチャと境界型セキュリティのハイブリッド環境にて動作するのに、十分な柔軟性があることを確認する必要がある。またソリューションの選定にあたって、既存の IT システムのインタフェースと連携可能なものを選択することも考えられる。

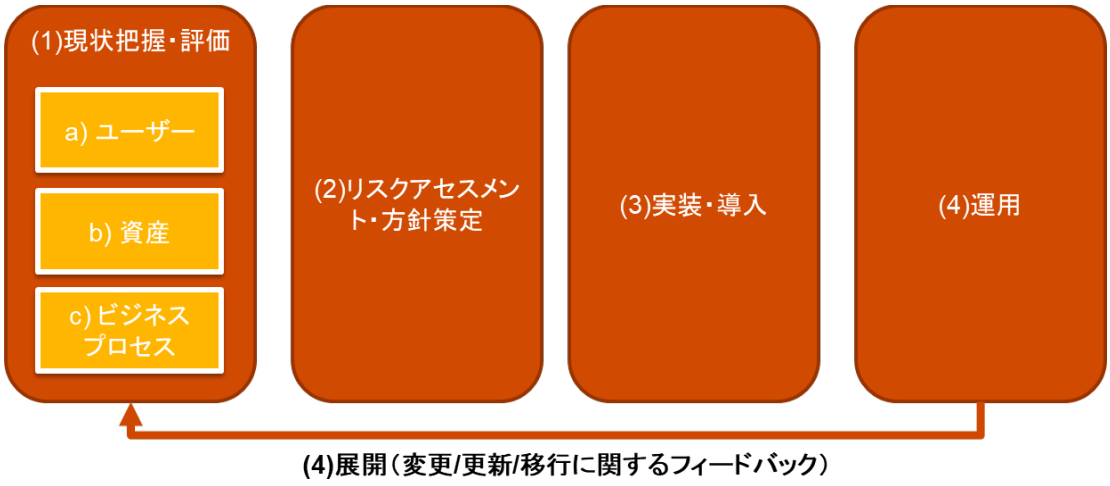
3.2.1. ゼロトラスト・アーキテクチャ導入前の準備

企業がゼロトラスト・アーキテクチャをどのように導入するかは、現在のサイバーセキュリティ管理態勢に依存する。そのため、ゼロトラスト・アーキテクチャを検討し、導入する前に、現在の情報資産・IT 資産、ユーザー、ビジネスプロセス、トラフィックフロー、および企業がそれらを識別し分類した依存関係のマッピングを整理しておく必要がある。これらの情報を使用して展開サイクルの最初のステップである「(1) 現状把握・評価」を行うことになる。

3.2.2. ゼロトラスト・アーキテクチャの導入ステップ

ゼロトラスト・アーキテクチャの展開サイクルとして、NIST SP800-207 が提示しているものを図表 3-6 に示す。ステップとして、「(1) 現状把握・評価」、「(2) リスクアセスメントと方針策定」、「(3)実装・導入」、「(4) 運用・展開」があり、これらの一連のステップを繰り返して、ゼロトラスト・アーキテクチャを段階的に導入していく。

図表 3-6 ゼロトラスト・アーキテクチャの展開サイクル



※NIST SP800-207 をもとに、PwC あらた作成

各ステップの概要は以下のとおりである。

(1) 現状把握・評価

ゼロトラスト・アーキテクチャを導入する取り組みを行う前に、情報資産・IT 資産（物理および仮想）、主体（ユーザーおよびユーザー権限）、データフロー、ワークフローの調査を行う必要がある。現在の運用状況を把握しなければ、どのような新しいプロセスや IT システムを導入する必要があるかの判断することができないためである。

NIST SP800-207 では、特定すべきものとして以下の 3 つを挙げている。ユーザーや IT システムのインベントリを作成した後は、定期的にメンテナンスと更新のサイクルを実施し、更新時にはビジネスプロセス変更有無に関わらず、ビジネスプロセスの評価を実施すべきであるとしている。

a) ユーザーの特定

ゼロトラスト・アーキテクチャではポリシーエンジン（PE）がアクセス元の主体に関する知識を持っている必要がある。主体には、サービスアカウントのようなユーザーに紐づくものや、ソフトウェアエージェント（ノンパーソンエンティティ）の両方が含まれる。特に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ーは、属性や役割を割り当てる際に、さらに精査が必要となる。ログや監査機能等を利用して、アクセス行動パターンを特定しながら、ビジネス要件を検討していく必要がある。

b) 所有する資産の特定

企業の資産を管理する能力は、ゼロトラスト・アーキテクチャの導入を成功させるための鍵となる。また、企業の IT システム等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となる。資産には、ノートパソコンやタブレットなどの物理機器に加えて、ユーザーアカウント、アプリケーション、デジタル証明書といったものも含まれる。所有するすべての資産の調査を完全に行うことが不可能な場合には、新たに発見された資産を迅速に特定、分類、評価する仕組みの構築を検討する必要がある。

資産の管理は、資産のデータベースを目録化して管理するだけではなく、構成管理と監視も含まれる。資産の監視によって得られた情報は、ポリシーエンジン（PE）がアクセスの判断を行う際に使用される。

また、企業が所有していない資産や「シャドーIT」も、可能な限り目録化する必要がある。シャドーIT は、他の資産のように企業側で管理されていないという点で留意が必要である。

c) ビジネスプロセス（キープロセス）の特定

ビジネスプロセス、データフロー、およびそれらの関係性を特定し、重要度に応じてランク付けすることでキープロセスを特定する。ビジネスプロセスの情報によって、IT システム等へのアクセス要求の許可や拒否の条件について判断することができる。

また、クラウドベースの IT システムを利用するプロセスや、リモートワークに関連するようなプロセスは、ゼロトラスト・アーキテクチャ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。候補となるビジネスプロセスを選定する際には、パフォーマンス、ユーザーエクスペリエンス、およびワークフローの変更点等を考慮すべきである。

(2) リスクアセスメント・方針策定

a) ゼロトラスト・アーキテクチャ候補のリスクアセスメント

ビジネス目標における関係性を考慮して、ビジネスプロセスの重要性の把握と、リスクアセスメントを実施する。場合によっては、ゼロトラスト・アーキテクチャへの最初の移行は、リスクの低いビジネスプロセスから開始することも考えられる。

候補となるサービスや業務ワークフローを特定する際には、企業にとってのプロセスの重要性、影響を受けるユーザー、関連する IT システム等の現状等、いくつかの要因を考慮する。

資産またはワークフローに対するリスクについては、NIST リスクマネジメントフレームワーク（NIST SP800-37）[8]を用いて評価することができる。

b) ゼロトラスト・アーキテクチャ候補の方針策定

ゼロトラスト・アーキテクチャの移行対象となるビジネスプロセスや資産を決定した後、影響範囲およびその対象をすべて特定する必要がある。影響を受けるものとして、ID 管理システムやデータベース等の IT システム、ログ管理やセキュリティ監視等の運用機能、ユーザーやサービスアカウント等が挙げられる。ゼロトラスト・アーキテクチャを段階的に導入する場合、最初は影響範囲が少ないものを先に対象とすることも考えられる。

次に、候補となるビジネスプロセスに適用するトラストアルゴリズムの方針を決定する。リソースの基準（基準ベースのトラストアルゴリズムを使用している場合）や信頼度レベルの重み（スコアベースのトラストアルゴリズムを使用している場合）を決定する必要がある（「3.1.4. ポリシーエンジンのトラストアルゴリズム」参照）。これらは、その後のフェーズにおいて適宜チューニングをしていく必要がある。

c) ゼロトラスト・アーキテクチャのソリューション選定

候補となるビジネスプロセスが決定した場合、ソリューションの候補を特定し、選定する。ビジネスプロセスの移行に関する動作を検証・評価するために、パイロットプログラムとしてテストを実施することも有用である。

以下は、ソリューション選定に際し、考慮すべき要因として挙げられているものである。

i) そのソリューションは、デバイスにソフトウェア等をインストールする必要があるか？

個人所有端末（BYOD）や企業外のユーザーが存在するなど企業が所有していない資産が使用されている、または使用する予定がある場合には影響が出る可能性がある。

ii) 対象のビジネスプロセスの IT システム等がオンプレミス環境にある場合も、そのソリューションが機能するか？

一部のソリューションでは、クラウド環境を前提とする場合もあるため、対象のビジネスプロセスに関連する IT システム等の場所は、ソリューション選定に影響を与える。

iii) そのソリューションは、分析のためにログに記録する手段を提供しているか？

ポリシーエンジン（PE）がアクセス可否の決定のために使用するデータの収集や、ポリシーエンジンとの連携機能を、該当ソリューションが提供しているかどうかである。

iv) 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、幅広いプロトコルやトランスポート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。

[8] Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy（NIST SP 800-37 Rev.2）:
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクルによるアプローチ（NIST SP 800-37 Rev.1）:
https://www.ipa.go.jp/files/000025329.pdf

v) そのソリューションは、ユーザー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、ユーザーのワークフローの変更を考慮する必要がある。

(3) 実装・導入

候補となるワークフローとゼロトラスト・アーキテクチャを構成するソリューションを決定した後は、導入を実施する。動的ポリシーの実装にあたっては、最初はアクセスが問題ないかどうか観察しながら運用することを推奨している。重要なユーザーアカウントが必要な IT システム等へのアクセスを拒否されたりするなど、業務上必要なアクセスが拒否されることがないようにするためである。

新しいビジネスプロセスに対してゼロトラスト・アーキテクチャを導入する場合は、初期導入後に適用予定の動的ポリシーを最初から適用せずに、ほとんどのリクエストに対してアクセスを許可し、取得したアクセスのログをもとに、適用予定の動的ポリシーと比較し、問題がないか検証を行う方法も考えられる。アクセス制限を緩めるような方法が選択できない場合には、ログを重点的に監視し、動的ポリシーを適宜調整することができる運用にしておくべきである。

(4) 運用・展開

定常的な運用フェーズに入ると、ネットワークや資産の監視を継続し、通信ログを取得する。動的ポリシーに関する設定等の変更作業は、初期導入時のように頻繁に調整するのではなく、業務影響を考慮して実施する。関連する IT システムやビジネスプロセスのユーザーまたはステークホルダーからのフィードバックをもとに、運用を改善していくことが重要である。この段階で、ゼロトラスト・アーキテクチャの段階的導入のために、次のフェーズの計画を始めることを検討する。次のゼロトラスト・アーキテクチャ展開にあたっては、同様の一連のステップを繰り返す。（図表 3-6 参照）

4. 金融機関のゼロトラストに関する取り組み状況

4.1. 国内金融機関の取り組み状況

本調査では、金融機関におけるゼロトラストに関する検討状況や導入状況を、文献調査やヒアリング調査の手法を用いて行ったものの、結果として、ゼロトラスト・アーキテクチャの導入あるいは積極採用に向けた取り組みを進めている金融機関はまだ少数であった。

しかしながら、一部の金融機関では、リモートワーク拡大のためや IT システムのクラウド化を進めるためにゼロトラストという考え方を踏まえた検討や導入を進めていることが確認された。

また、ゼロトラスト・アーキテクチャについて調査や検討は行ったものの、様々な理由から現時点ではゼロトラスト・アーキテクチャは導入しないとしている金融機関も確認された。

本項では、上記のような確認された事例をもとに、金融業界におけるゼロトラストに関する検討状況や導入状況の実態について記載する。

4.1.1. 金融業界におけるビジネス環境の変化

「2.2.1. デジタル技術の進展による IT 環境の多様化とサイバーリスクの高まり」に記載したようなデジタル社会への変革とそれを取り入れた働き方は、金融業界でも同様に広がっている。

たとえば、金融機関の顧客サービス面では、インターネットとスマートフォンの普及などにより、顧客はオンデマンドで自身のライフスタイルに適した金融サービスや金融機関を求めるように変化してきている。同時に、金融機関側も顧客志向を強めている。顧客の取引情報や行動履歴等のデジタル化された大規模データを収集、分析、活用し、顧客ニーズに適した金融サービスを開発することが命題になる中で、自社の所有するデータのみならず業界内外の企業とのデータ連携、あるいは IoT データの活用などにも積極的に取り組んでいる。

また、金融機関の労働環境面でも変革が進んでいる。金融機関の社員の働き方といえば、数年前までは支店や事務所で執務するのが当たり前であったが、足下では、少子高齢化を迎える中での柔軟な働き方の実現のためや、新型コロナウイルス感染症（COVID-19）への対策のため、多くの金融機関にもリモートワークが普及している。

4.1.2. IT 環境の変化とサイバーセキュリティリスクの高まり

上述したビジネス環境の変化に対応するため、多くの金融機関では、いくつかの共通的な取り組みが見られる。その 1 つが、クラウドサービスの利用の拡大である。クラウドサービスを利用することで開発スピードや拡張性あるいは最新技術の活用容易性を手に入れ、ビジネスの成長を加速させている。セキュリティ対策もクラウドに対するセキュリティリスクを踏まえた対応を進めている。もう 1 つの取り組みとして多く見られるのが、リモートワークの活用である。金融機関では、リモートワーク下でもセキュリティを保ち

ながら業務を行うための取り組みとして、セキュリティ設定を強化した専用のリモート端末や VPN、仮想デスクトップ（VDI：Virtual Desktop Infrastructure）等の導入や拡張を進めている。

以前より金融機関は、他業界の企業と比べて積極的にセキュリティ対策に取り組んでいる。具体的には、入口対策、内部対策、出口対策を組み合わせた多層防御の考え方を取り入れ、重要な IT システムやデータは堅牢なデータセンター内に設置し、社内のネットワークから分離して保護してきた。しかしながら、上述したクラウドサービスを利用する IT システムの増加やリモートワーク環境の拡大により、外部からのサイバー攻撃を受ける対象となるアタックサーフェスが増え、サイバーセキュリティの固有リスクが高まっている。また、そのリスクに対応するためのセキュリティ管理負荷も高まっている。

4.1.3. 金融機関におけるゼロトラストに関する検討状況

一部の金融機関では、ゼロトラスト・アーキテクチャに関する具体的な検討や導入を進めているが、金融機関全体としては少ない状況である。その背景として、金融分野はサービスの安定供給や顧客情報保護を重視しながら、早くから IT の利活用が進んだ業界でもあることから、既存の IT システムや境界型セキュリティの考え方が既に浸透・定着しており、比較的新しいセキュリティの考え方であるゼロトラスト・アーキテクチャの検討や導入が現段階では少数であることが挙げられる。

ゼロトラスト・アーキテクチャの検討や導入を進めている金融機関は、主にリモートワークの推進やクラウドサービスの活用を目的としている。

本調査では、ゼロトラスト・アーキテクチャの導入に向けた具体的な検討を進めている金融機関の事例が確認できた。その事例では、コミュニケーションツールや情報系システムのクラウド化が進む中で、将来的なデータ利活用を考えると、基本的にデータをクラウド上に集めてシステム間で連携させていく方針としており、勘定系システムや CRM システムのクラウド化も進めている。また、顧客向けサービス向上のため、外出先からも社内の IT システムに接続できるリモート端末の環境を構築してきたが、社内と社外で異なる端末であることの不便さ、端末管理負荷やコストの高まり、VPN の接続帯域の限界等の課題があった。クラウド化やリモートワークを進めていくために必要な IT 基盤を再検討した結果、まずはクラウドサービスで提供されている認証の仕組みを導入し、将来的にゼロトラスト・アーキテクチャへの移行を視野に入れながら検討を進めている。

一方で、メリット、デメリットを検討した結果、ゼロトラスト・アーキテクチャは当面導入しないと判断している金融機関もある。その理由は、現状実現したいことは既存 IT 環境で対応可能であること、ゼロトラストに関するソリューションが発展途上であること、導入コストが高いことなどである。その場合でも、ゼロトラストの原則を参考にして、認証の強化、内部通信の暗号化、通信のモニタリング強化など、内部対策の強化に取り組んでいる。

また、まだ調査や検討に着手できていない金融機関もある。検討が進んでいない理由として、ゼロトラストの検討以前に、自社の脆弱性対策やアクセス管理等の対策が十分にできていないのではないかと感じ、まずは基本的な対策について考え直していることを挙げている金融機関もあった。

4.1.4. 金融機関におけるゼロトラスト・アーキテクチャ導入状況

本調査では、リモート端末とクラウドサービスを対象にゼロトラスト・アーキテクチャを導入している国内金融機関が確認できた。その事例では、接続元ネットワークの位置情報やデバイスのパッチ適用状況やマルウェア検知情報を取り入れた認証・認可をクラウド上で実現している。ただし、NIST SP800-207 の原則にあるような多様な情報を含めた動的ポリシーを用いての認証・認可や、ログの監視・分析と通信の遮断・制限までは実現できておらず、今後段階的に取り組んでいく状況である。

NIST SP800-207 で示されているゼロトラスト・アーキテクチャを完全に実装できている事例は金融以外の国内の一般企業でも少なく、既存の IT システムやデータを多く保有する企業が完全なゼロトラスト・アーキテクチャに移行することは容易ではないと言える。

4.1.5. 国内金融機関のゼロトラスト・アーキテクチャの導入例

本項では、本調査で確認できた国内金融機関におけるゼロトラスト・アーキテクチャの導入事例を参考に、クラウド型コミュニケーションツールの活用やリモートワーク拡大の目的でのゼロトラスト・アーキテクチャの導入例を記載する。

a) ゼロトラスト・アーキテクチャ実装の背景・目的

数年前にメール、カレンダー、ファイルストレージ、Web 会議、チャット等の社内コミュニケーションツールをクラウド型の統合サービスに移管し、社内コミュニケーションの活性化を図ってきた。しかしながら、リモート端末からはインターネット VPN 経由で一度社内ネットワークに入ってから、再度インターネット上のクラウドサービスにアクセスするルートとなり、特に大容量のファイル送受信や Web 会議などの通信トラフィックの大きい処理が遅延する、不安定になるといった課題があった。それは、2020 年の新型コロナウイルス感染症（COVID-19）によるリモートワークの急速な拡大により、より顕著になった。

その課題を解決するため、リモート端末からクラウドサービスや Web サイトへの通信について、社内ネットワーク経由ではなく、直接インターネット経由にするローカルブレイクアウト（インターネットブレイクアウトとも呼ばれる）の実現を目指すこととなった。その際に、セキュリティを確保することと、ユーザーの利便性を損なわないことを重視し、使用しているクラウド型コミュニケーションツールとの連携実績が豊富な IAM（ID アクセス管理）と IAP（ID 認識型プロキシー）を導入することとした。

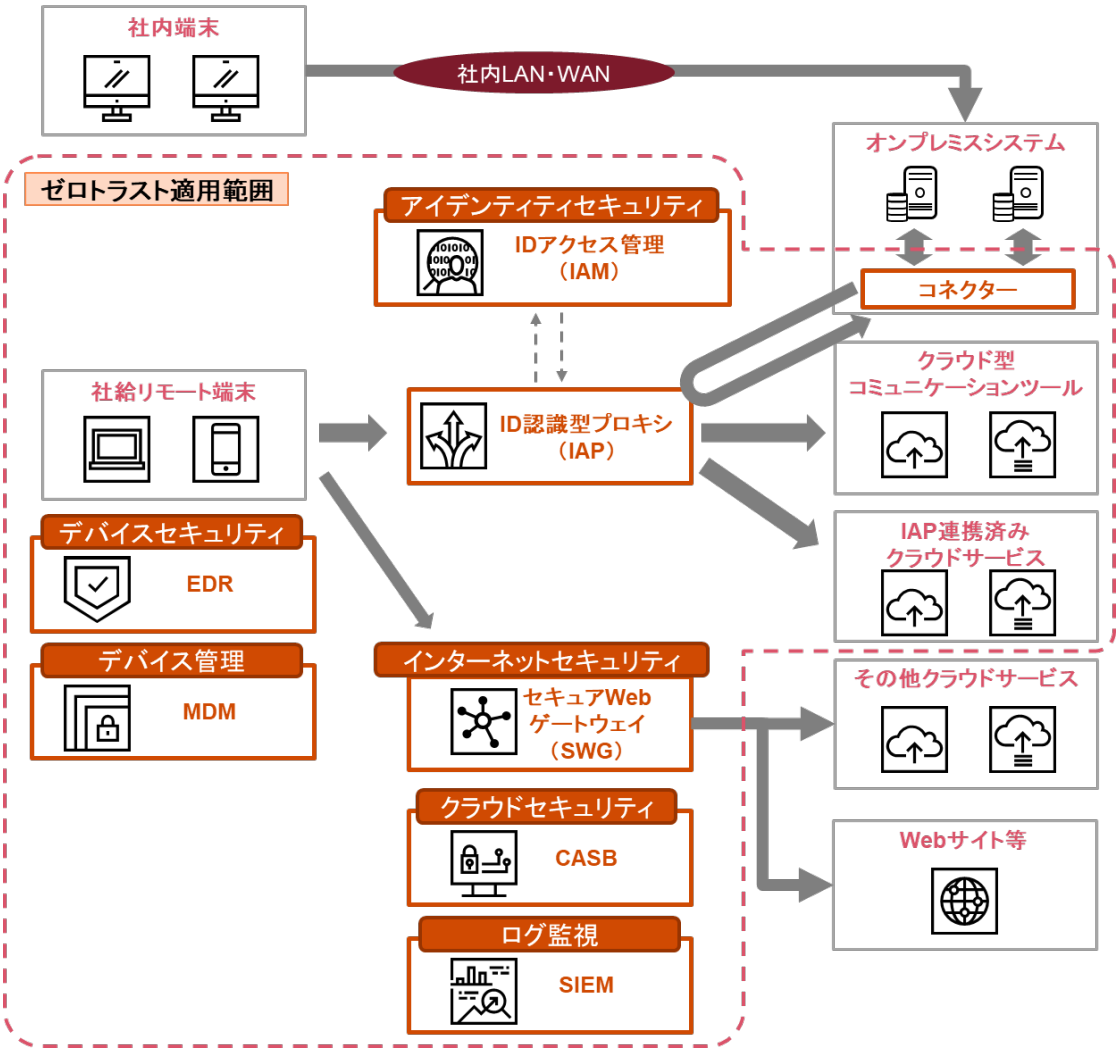
b) アプローチ・実装方法

リモート端末からのローカルブレイクアウトをゼロトラスト・アーキテクチャで実現したイメージを図表 4-1 に示す。

- リモート端末として配布している社給のノートパソコンおよびスマートフォンのエンドポイントセキュリティを強化した。具体的には、EDR と MDM（モバイルデバイス管理）の製品を導入し、一元管理している。
- リモート端末からクラウド型コミュニケーションツール、IAP と連携可能な SaaS、オンプレミス型システムへの通信は IAM と IAP で認証・認可を行っている。
- パスワード、生体情報による静的な多要素認証に加えて、IAM のデフォルト設定をベースに、接続元ネットワークの位置情報や OS のパッチ適用状況、EDR での脅威検出状況等の情報を用いた動的ポリシーにて認証・認可を行っている。
- 動的ポリシーのトラストアルゴリズムを随時見直しており、ユーザーの利便性を損なわないように注意している。
- リモート端末からオンプレミス型システムへの通信は、IAP とオンプレミス側に配置するコネクター間の通信を経由させている。この方法では、内側のコネクターから外側の IAP へセッションを確立して通信を行うため、外側からの内側への通信を許可するためにファイアウォールでポートを開放するようなことが無く、攻撃対象となりうる外側との接点を特定させないことでセキュアなアクセスを実現している。

- その他のクラウドサービス利用および Web サイト等へのアクセスは、IAM と IAP での認証・認可は行っていないが、SWG（セキュア Web ゲートウェイ）を利用することでセキュアに接続し、各種ログは SIEM や CASB によって収集している。

図表 4-1 国内金融機関のゼロトラスト・アーキテクチャ導入事例のイメージ



※知見をもとに PwC あらた作成

c) 得られた効果

- リモート端末からもセキュアなアクセスを実現することができたことで、リモートワークに柔軟に対応できた。
- リモート端末から社内コミュニケーションツールをインターネット経由で直接利用できるようになり、ネットワーク遅延や不安定になることが減少したため、コミュニケーションツールの利用が活性化した。

d) 今後の対応

- 事務所内で利用している社内端末は、まだ従来からの境界型セキュリティの考え方で守られた内部ネットワークに設置している。将来的には、社内ネットワークからしか利用できないオンプレミス型システムの利用はクラウドサービス型の仮想デスクトップ経由とし、社内端末もリモート端末と同等の接続形式に変更していくことも視野にいれている。

- IAP と連携できていないその他のクラウドサービスも IAM と IAP での認証・認可に移行することで、SSO（シングルサインオン）を実現し、ユーザーが認証を意識せず様々なサービスを利用できるようにしたい。
- 収集したログは不正アクセス等を検知した際の調査目的での利用は可能だが、それ以外に有効活用できていない。今後は、これらのログを積極的に分析し活用していきたい。

4.2. 海外金融機関の取り組み状況

本調査では、NIST SP800-207 の原則で示されているような、多様な情報で構成された動的ポリシーに基づいたアクセスの認証・認可を実現している事例は、海外金融機関でも確認できなかった。また、グローバルで事業を展開している海外金融機関からは、IT システムやネットワークが複数の国に跨っているため、現状では移行への障壁が大きいとの意見があった。

したがって、海外金融機関も国内金融機関と同様にゼロトラストという考え方には強い興味をもっているものの、短期的にゼロトラスト・アーキテクチャへの移行は難しいと考えており、今後も情報収集や関連製品動向の分析などを進めながら、段階的に取り組みを検討していくというのが総体的な動向である。

一方で、一部の海外金融機関では、ゼロトラスト・アーキテクチャの導入事例も見られた。導入の背景は、日本と同様、新型コロナウイルス感染症（COVID-19）への対応として、リモートワーク環境の整備ためにゼロトラストという考え方を採用したという事例である。具体的には、短期間で安全なリモートアクセスを実現するための手段として、クラウドサービス型の SDP（Software Defined Perimeter）をネットワークソリューションとして導入し、ゼロトラスト・アーキテクチャの取り組みの第一歩としている事例があった。（SDP を利用したゼロトラスト・アーキテクチャの実装イメージは「2.5.3.(2) ネットワーク中心のアプローチによる実装イメージ」参照）

また逆の事例として、ゼロトラスト・アーキテクチャは当面導入しないと判断している海外金融機関も確認できた。ただし、当該海外金融機関は、以前から内部不正を重要なリスクと認識し、IT システム面・運用面での内部不正対策に長年取り組んでいる。境界型セキュリティを採用しつつも、内部ネットワークとそれを利用するユーザーを暗黙に信頼するという考えではなく、以下のような対策の継続的な高度化を推進している事例であった。

- ユーザーによるデータへのアクセス状況やデータの移動状況、ネットワークトラフィック状況等について、UEBA（User and Entity Behaviour Analytics）などの収集・解析ツールを駆使しながら監視し、不審な動きを 24 時間 365 日の体制で調査・対応する態勢を整備・運用している。
- マルウェアのラテラルムーブメント（水平移動）を防ぐために内部ネットワークのセグメントの細分化を設計レベルで検討し実装する。
- 最小権限の原則、Need to Know の原則に従って個々のアプリケーションやデータへのアクセスを制限するとともに、必要に応じて多要素認証を採用している。
- 内部ネットワークに利用されているひとつひとつのネットワークデバイスを堅牢な状態に維持する。

このような多層かつ高度な内部対策へも取り組んでいるといった背景もあり、当該金融機関は、現段階ではゼロトラスト・アーキテクチャへの移行は考えていなかった。

5. ゼロトラスト・アーキテクチャ検討・導入時の主なポイント

本章では、文献調査やヒアリングを通じて得られた情報をもとに、ゼロトラスト・アーキテクチャの検討および導入時において考慮すべきポイントについて、図表 5-1 のとおり、「検討」、「計画」、「導入・運用」の各段階に分けて記載する。本調査にて確認した範囲では、ゼロトラスト・アーキテクチャを導入し、具体的な取り組みを行っている企業は比較的少ないことや、ゼロトラストに関する検討や取り組みを今後開始する金融機関が多いことから、検討段階と計画段階でのポイントを多く記載している。

なお、「3.2.2. ゼロトラスト・アーキテクチャの導入ステップ」にて NIST SP800-207 が示すゼロトラスト・アーキテクチャの展開サイクル（「現状把握・評価」、「リスクアセスメントと方針策定」、「実装・導入」、「運用・展開」）と異なる段階としている。

図表 5-1 検討、計画、導入・運用の各段階の概要

段階	概要
検討段階	ゼロトラストの考え方を理解し、企業全体の共通認識を作る段階である。自社におけるゼロトラストの位置づけを明確にし、経営陣はその方向性を示す。また、自社のビジネス環境を正しく理解し、今後目指すべき IT システムの姿やそのために必要なセキュリティのあり方のゴールを描く。
計画段階	ゼロトラスト・アーキテクチャを導入していくことを前提に、具体的な計画を立てる段階である。既存の IT システムを踏まえた移行計画を作成し、製品・ベンダー選定やゼロトラスト・アーキテクチャの運用設計を行う。この段階では、ありたい姿やあるべき姿だけではなく、実現可能な姿を描く。
導入・運用段階	ゼロトラスト・アーキテクチャを初めて導入する段階および動的ポリシーの変更を含めた導入後の運用を行う段階である。 運用段階では、ユーザーの協力も得ながらアーキテクチャの最適化と効果測定を継続的に行い、環境の変化も踏まえて必要に応じて計画を見直した上で、対象範囲の拡大などの次の段階の導入を行う。計画を見直した結果、「検討段階」や「計画段階」を繰り返すこともある。

※知見をもとに PwC あらた作成

5.1. 検討段階

検討段階では、「どのようにゼロトラスト関連の製品を導入するか」ではなく、自社のビジネスや IT システムにおける内部・外部環境の変化を考慮し、「今後どのような IT システムを目指すのか、そのためにどのようなセキュリティの考え方が必要か」という将来像について十分な検討を行う。そのためには、ゼロトラストという考え方をしっかりと理解し、社内で共通認識持つことが重要である。そこでポイントとなるのが、経営陣の理解、組織横断での検討、情報資産・IT 資産の特定と評価、実現可能なロードマップの作成である。なお、検討の結果、ゼロトラスト・アーキテクチャの導入に向けた具体的な取り組みに当面は着手しないという結論になることもある。

5.1.1. ゼロトラストに対する経営陣の理解と方向付けが不可欠

ゼロトラストに関する検討や取り組みは、「2.2. ゼロトラストが注目を集める背景」に記載したとおり、働き方や自社のビジネスを支える IT システムに大きな影響を与える。また、社外とのコラボレーション機会の創出や DX の推進など、新しいビジネスを検討するきっかけにもなり得る。つまり、ゼロトラストは単にセキュリティを高めるためだけのものではなく、新しいテクノロジーを活用しながら企業が進むべき方向性を定めるためのものでもある。

そのため、情報システム部門・セキュリティ部門の担当者や CIO・CISO だけではなく、経営陣がゼロトラストという考え方を十分に理解すること、理解した上でゼロトラストの考え方を取り入れていくかの自社の方向付けを行うことが求められる。

経営陣が理解すべきこととして、例えば以下のような内容が挙げられる。

- ゼロトラストが注目されている背景（「2.2. ゼロトラストが注目を集める背景」参照）
- ゼロトラスト・アーキテクチャの概要（「2.3. ゼロトラストの概要」参照）
- ビジネスや働き方等において自社が目指す将来像（「5.1.4. 「ありたい姿」から実現可能なロードマップを描く」参照）

また、検討の結果、自社にとってゼロトラストの考え方が有益であり、今後のセキュリティの方向性として位置づけるのであれば、その方針を全社に対して明確に示すことが重要である。

ゼロトラストに関する検討や取り組みに経営陣の協力を得られている企業は、検討の段階から経営陣を含む必要なステークホルダーを積極的に巻き込み、継続的な議論を行っている。その際、経営陣の理解度や認識を考慮して議論を行うよう工夫している。

例えば、経営陣のゼロトラストへの理解度があまり高くない状況であったため、経営陣に何度もワークショップを開催し、次のような内容を段階的に議論し、一緒に考えることでゼロトラスト・アーキテクチャの導入効果や必要性を理解してもらうよう働きかけた事例があった。

- 既存の境界型セキュリティの限界
- 自社のビジネスモデルや働き方における IT システムのあり方
- これらを踏まえた今後の自社のセキュリティのあり方

5.1.2. 情報システム部門だけでなく組織横断での全社的な検討が必要

ゼロトラストに向けた検討では、採用するソリューションや製品の具体的な内容について議論する前に、自社がどのようなビジネスや働き方を実現したいかを考えることが重要である。具体的には、IT を効率的に利活用しどのようなビジネスを創出・展開していきたいか、役職員がストレスなく本来の職務に集中できる IT 環境とはどうあるべきかなどを考えることがスタートラインとなる。そのため、情報システム部門だけで考えることのできるようなテーマではないことは明らかである。

また、ゼロトラスト・アーキテクチャの肝となる認証・認可の検討は、各業務システムに対してどの程度の条件・厳密さで認証・認可を設計するか、セキュリティとユーザー利便性のバランスを取りながら検討することが重要であり、IT システムのオーナーやユーザーの意見・判断が必要となる。

加えて、ゼロトラスト・アーキテクチャの検討には、セキュリティの担当者のみならず、ネットワーク管理やデバイス管理の担当者、あるいは共通基盤や各業務システムの管理者等の関与も不可欠となるため、部門全体で今後の IT システムやセキュリティのあり方について積極的に議論することが重要である。

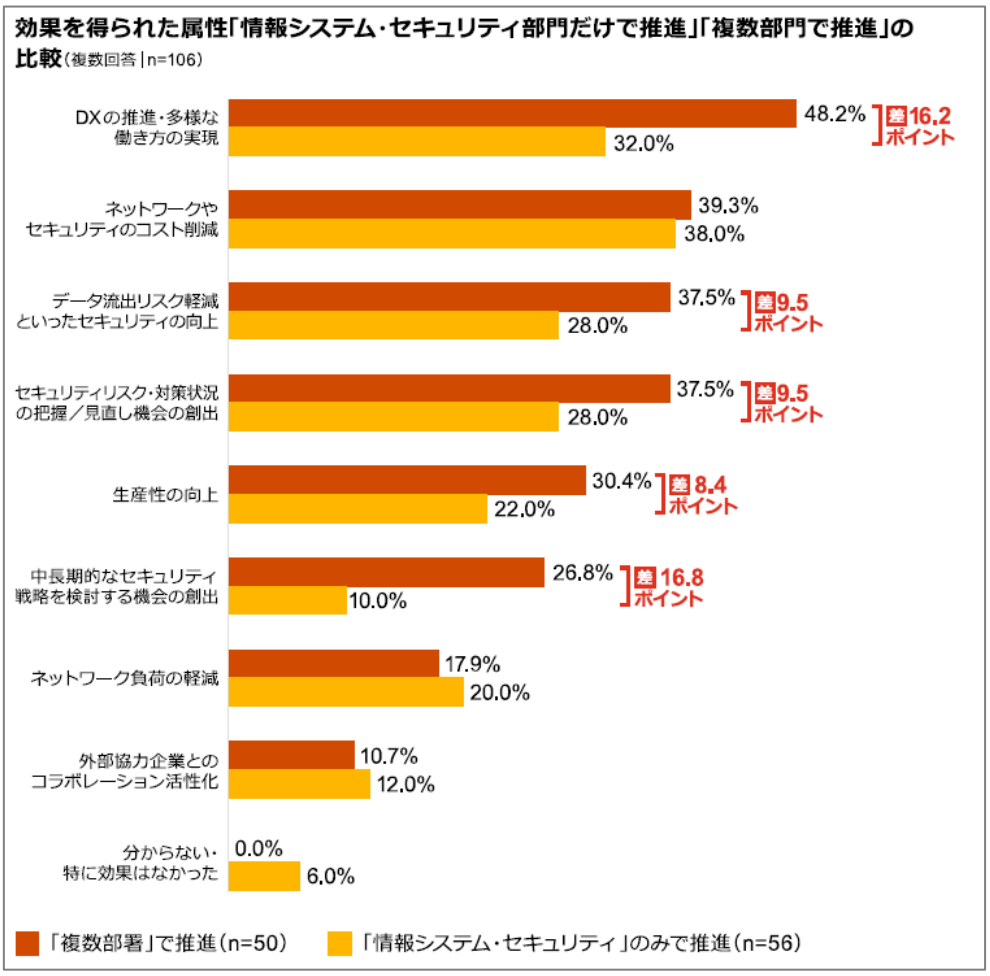
これらの理由から、ゼロトラストに関する検討や取り組みでは、検討段階から必要なステークホルダーを積極的に巻き込み、既存の組織の役割や責任範囲を超えた議論を行うことが重要である。その議論において外部専門家を活用することは、自社に足りない知識や経験を補完するだけでなく、組織間の利害関係や慣例を取り払った調整を行うためにも有効である。また、クラウド推進やデジタル推進でも見られる、CoE（Center of Excellence）と呼ばれる組織横断で新たな取り組みや議論を中核的に行う組織を作り、具体的な検討を進める方法も考えられる。

ゼロトラストに先進的に取り組む国内企業へアンケート調査を実施した『国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021』[9]によると、情報システム・セキュリティ部門のみでゼロトラストを推進している企業よりも複数部門で推進している企業の方がより多くの効果を得ていることが分かる（図表 5-2 参照）。

特に、「中長期的なセキュリティ戦略を検討する機会の創出」と「DX の推進・多様な働き方の実現」の効果を得られたという回答は、16 ポイント以上も上回る結果となっており、ゼロトラスト・アーキテクチャの導入によって、自社のビジネスや働き方に対する効果を得るためには、組織横断での取り組みが重要と言える。

[9] 国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021（PwC Japan グループ）：
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html

図表 5-2「情報システム・セキュリティ部門でのみ推進する企業」と
「複数部門で推進する企業」の得られた効果の比較



※PwC Japan グループ,『国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021』より抜粋

実際に必要なステークホルダーを巻き込んだ上で、ゼロトラストに関する検討や取り組みを進めることができている企業では、各担当者が所属組織の役割や責任にとらわれず、担当範囲を超えた検討と社内関係者への積極的な働きかけを行うことで、以下のような取り組みにつながり、ゼロトラスト・アーキテクチャへの移行の活動全体が活性化している。

- 社内向けにゼロトラストに関する取り組み状況を定期的に発信している
- 経営陣からゼロトラスト・アーキテクチャへ取り組むことの方針を全社に発信することで、関連部門の協力や支援が得られやすくし、協力者を増やしている
- 認証の手間や通信が遅いなどのユーザー意見を収集して利便性向上のために解決すべき課題を明確にしている
- 課題が発生した際に関係部門との協議・調整を迅速に行い解決している
- 情報システム部門内でゼロトラストの考え方や関連するソリューション等の勉強会を開催している

5.1.3. 前提として情報資産・IT 資産の特定と評価が必要

ゼロトラスト・アーキテクチャでは、情報資産や IT 資産の重要度、アクセス元のユーザーの役割や責任、デバイスの状態等の情報をもとに、動的ポリシーによって IT システムへのアクセスの認証・認可を行う。NIST SP800-207 の「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」で

以下のように記載されているとおり、情報資産・IT 資産の特定と評価は、ゼロトラストに関するあらゆる検討や取り組みの基礎となるものであり、これらが無ければ具体的な計画を立てることは難しい。

【ゼロトラストの定義】 ※NIST SP800-207（日本語訳）より抜粋

「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。」

情報資産・IT 資産を正確に特定することでデータフローを網羅的に識別することが可能となり、各 IT システムに対し、どのようなアクセスを許可するかの動的ポリシーを検討できる。

また、重要なビジネスプロセスにおいて、特定した情報資産や IT 資産がどのように利用されているかの関係性を明確にすることで、IT システムやデータの重要度を評価して決定する。この重要度は、「5.1.4. 「ありたい姿」から実現可能なロードマップを描く」に記載しているようなロードマップを検討する際のゼロトラスト・アーキテクチャの導入優先度を決める際の要素や、動的ポリシーの検討における IT システムへのアクセス要件の基礎的な情報として利用される。

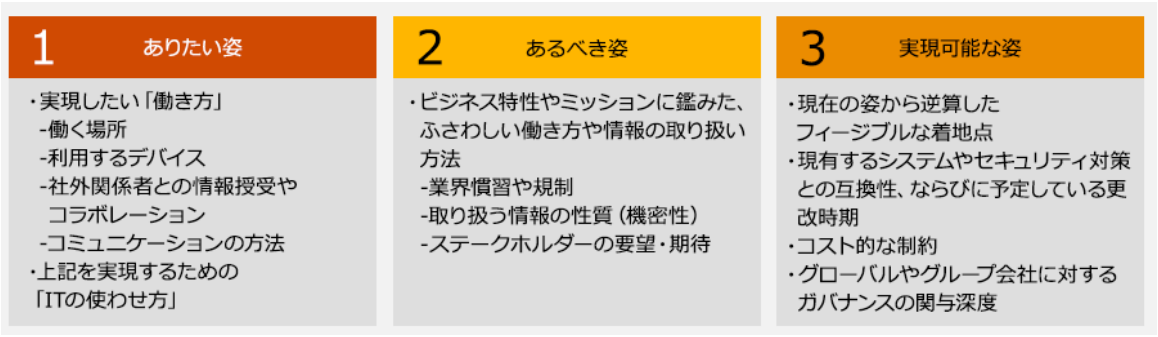
しかしながら、多くの企業ではクラウドサービスの利用拡大やリモートワークの普及等により IT システムやデータの所在が多様化しており、自社の IT 環境の把握は容易ではなくなってきている。そのため、ゼロトラスト・アーキテクチャの導入を進める前に、現状の情報資産・IT 資産について十分に調査・把握する必要がある。その際、ゼロトラストに関する検討や取り組みの最初から網羅的に自社の IT システムやデータを把握しようとするのではなく、検討や導入を進めながら自社の IT 環境の理解を深め、計画を柔軟に修正していく方法もある。

5.1.4. 「ありたい姿」から実現可能なロードマップを描く

ゼロトラストに関する検討や取り組みは、IT システムやセキュリティの改善自体が目的ではなく、それによりビジネスや働き方を目指すべき方向に変革するための一手段である。そのため、まずはビジネス目線で自社が「ありたい姿」を描いた上で、業界の商習慣や法規制等も踏まえた「あるべき姿」を検討することが重要である。なお「あるべき姿」を実現できればそれに越したことはないが、現実的には費用やスケジュール、技術的制約等のクリアすべき課題も存在するため、こうした点を企業として総合的に判断し、「実現可能な姿」を導き出した上で移行計画を立てることが一般的である。

「ありたい姿」、「あるべき姿」、「実現可能な姿」において検討すべきことの例を図表 5-3 に示す。「ありたい姿」の検討では、DX の推進や社内外のコラボレーション機会の創出も踏まえて、自社のビジネスや働き方を目指していくのか、そのためにどのような IT 環境が必要となるかを考える。「あるべき姿」の検討では、目指していくビジネスや働き方に対して、守るべき法規制やセキュリティの維持、外部の利害関係者からの要望・期待等を考慮する。「実現可能な姿」の検討では、現状の IT 環境等も踏まえて、「ありたい姿」や「あるべき姿」に向けて、既存 IT システムとの互換性、技術的制約、費用対効果、スケジュール等を考慮して、実現可能な移行計画を作成する。

図表 5-3 アーキテクチャの変更に際して検討していくべきこと



※PwC Japan グループ，「次世代の IT インフラ - ゼロトラスト・アーキテクチャ ゼロトラストへの移行に際する検討・留意事項」より抜粋

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture02.html

通常は、全ての IT システムを一斉にゼロトラスト・アーキテクチャに移行することは非現実的であるため、移行計画は段階的に実現していくロードマップとなる。段階的な移行計画を作成する際は、NIST SP800-207 の「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」に記載されているとおり、最初はリスクの低いビジネスプロセスから始め、動的ポリシーの精度を高め、十分な運用体制を整備した後に、より重要なビジネスプロセスへゼロトラスト・アーキテクチャを段階的に拡大していくことが有効である。その理由は、動的ポリシーの精度が低いと、ユーザーから IT システムへの正常なアクセスも遮断してしまい、業務に影響を与えることとなるためである。最初の段階で対象とするビジネスプロセスを検討する際の考え方として、例えば以下のようなものがある。

- ビジネスリスクが低い業務から始める。例えばリモートでできる間接的な業務からゼロトラスト・アーキテクチャを導入し、基幹業務は自社のナレッジが十分に蓄積された段階で導入していく。
- IT 環境として移行しやすい領域から始める。一般的に、クラウドサービスを利用している IT システムはゼロトラスト・アーキテクチャを適用しやすく、オンプレミス環境にある IT システムでは難しい。そのため、クラウドサービスを中心にゼロトラスト・アーキテクチャを導入し、オンプレミス環境の IT システムはシステム更改のタイミングでクラウド環境への移行も含め、ゼロトラスト・アーキテクチャへの移行を検討する。

なお、目先の VPN のキャパシティ問題の解決のような短期的な効果にのみ目を向けてゼロトラスト・アーキテクチャの導入を検討すると、ゼロトラストの恩恵を十分に得ることができず、結果的に費用対効果が得られない。また、将来的な「ありたい姿」を十分に検討せず、ゼロトラスト・アーキテクチャを導入してしまうと、自社の IT 基盤がビジネスや働き方と整合せず、目標とするような付加価値の創出やユーザー利便の達成が困難となる可能性がある。

5.2. 計画段階

計画段階では、自社の既存の IT 環境も考慮しながら、ゼロトラスト・アーキテクチャの段階的な導入計画を立てる。境界型セキュリティからゼロトラスト・アーキテクチャへの転換は、単にセキュリティに関するソリューションや製品が変わるものではない点や自社のセキュリティ管理ルールとの整合性の確認も必要な点に留意する必要がある。また、ゼロトラスト・アーキテクチャの推進体制や運用体制を検討し、

外部専門家の活用や人材育成計画も含め、ゼロトラスト・アーキテクチャを継続的に維持・管理できる体制を準備する。

5.2.1. リスクや既存 IT 環境との連携を考慮したソリューション・製品の選定

ゼロトラスト・アーキテクチャを導入する場合、「2.5.2. ゼロトラスト・アーキテクチャを実装するためのソリューション」に記載したようなソリューションや製品を新たに導入することとなる。ソリューションや製品を選定する際には、認証・認可に関わる製品のリスクを適切に評価して選定すること、および既存の IT 環境との連携可能なものを選定することが重要となる。

1 つ目の認証・認可に関わる製品のリスクについて、「3.1.5. b) サービス拒否またはネットワーク障害」に記載したとおり、ゼロトラスト・アーキテクチャでは、通信経路を制御しているポリシーアドミニストレータ（PA）やポリシーエンジン（PE）が利用できなくなるリスクを考慮する必要がある。これらの製品は、主にインターネット上での通信を制御するため、クラウドサービス（SaaS）として提供されているものが多く、サービスプロバイダ側の原因によりサービスが利用できなくなるケースも考えられる。クラウドサービスを利用する際の一般的な考慮事項は、『クラウドコンピューティングとサイバーセキュリティ等に関する調査報告書』[10]等に示されている。ただし、ゼロトラスト・アーキテクチャの認証・認可等のサービスは、サービス停止による影響が IT 環境全体に及ぶことや、導入後に認証・認可の精度を上げるためにナレッジを蓄積していくために他のサービスへの移行が容易ではないことから、それらの製品を選定する場合、以下のような観点で信頼できるサービスであるか検討し、選定・評価することがより重要となる。

- ゼロトラストに関するサービスの提供領域（今後の予定や継続性も含む）
- サービス要件（サービス稼働率、応答時間、処理性能、カスタマイズ性等）
- セキュリティ要件（脆弱性への対応、暗号鍵管理、WAF 機能、DDoS 対策機能、ログ取得有無等）
- コスト（イニシャルコスト、ランニングコスト、運用負荷等）
- サポート体制
- 公的認証・第三者評価・監査の有無（SOC2 レポート、ISO/IEC27001、ISO/IEC27017、ISO/IEC27018 等）
- 他サービス、製品との互換性
- 移行の容易性

2 つ目の既存の IT 環境との連携可能なものの選定について、境界型セキュリティとゼロトラストはセキュリティに対する考え方が異なるため、それらを実現するアーキテクチャも異なる。そのため、これら 2 つの考え方に基づく環境が同時に存在する場合、必要なソリューションが増えることでコストや管理負荷が高くなる。一度にすべての IT 環境をゼロトラスト・アーキテクチャに移行することができれば理想的だが、勘定系システム等の重要システムを保有する金融機関のような企業では現実的ではなく、企業内で従来からの境界型セキュリティの環境とゼロトラスト・アーキテクチャの環境を共存させることが多い。その際に考慮すべきポイントとして、ゼロトラストと境界型セキュリティにおいて共通する ID 管理やデバイス管理、ログ分析等のソリューションが双方の環境で問題なく動作することの確認が挙げられる。例えば、クラウドの認証基盤によって ID 管理を行う場合、境界型セキュリティでも同じサービスを使用し、アプリケーションにおける SSO（シングルサインオン）を実現することが可能である。また、ログの分析においても、境界型セキュリティの環境で従来から利用している SIEM 等を活用しつつ、ゼロトラスト・アーキ

[10] クラウドコンピューティングとサイバーセキュリティ等に関する調査報告書（PwC あらた有限責任監査法人）：https://www.fsa.go.jp/common/about/research/20190611-2.html

テクチャの導入において、不足している情報や機能を新しいソリューションや製品で補完しながら高度化していく方法がある。

5.2.2. ビジネス目標の達成を目指せる推進体制の整備

ゼロトラスト・アーキテクチャの導入を推進する際は、「自社の既存のビジネスや IT 環境の理解」、「ゼロトラスト・アーキテクチャに関する理解」、「自社が目指そうとしているビジネス目標の理解」の 3 つが必要となり、それらを持った人材を集めてゼロトラスト・アーキテクチャの推進体制を整備することが重要である。

1 点目の自社の既存のビジネスや IT 環境の理解は、ビジネスプロセスや情報資産・IT 資産を特定し、ゼロトラスト・アーキテクチャへの移行計画を作成するために必要となる。また、ゼロトラスト・アーキテクチャのソリューション・製品を選定する際にも既存 IT 環境からの移行容易性や境界型セキュリティとの連携可否を検討する際にも必要となる。

2 点目のゼロトラスト・アーキテクチャに関する理解は、自社に最適なゼロトラスト関連ソリューションや製品を選定、検討する上で必要となる。ゼロトラストはまだまだ新しい分野であり、ソリューションや製品市場も発展途上にある。またゼロトラスト・アーキテクチャは、単一の製品やソリューションで実現できるものでもない。複数のソリューションや製品を連携して実現することになるため、それらのメリットや、互換性、制約等の知識が必要となり、実際に導入や検証を行った経験等も重要となる。

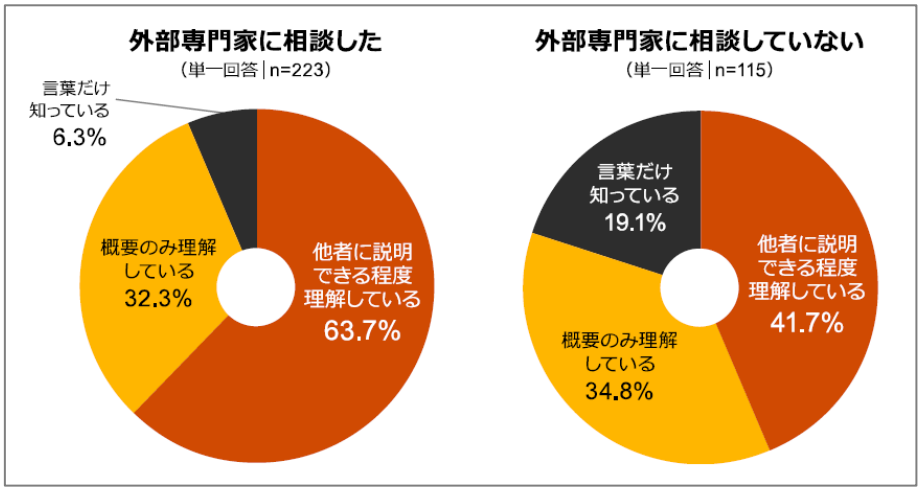
3 点目の自社が目指そうとしているビジネス目標の理解は、ゼロトラスト・アーキテクチャの導入が IT システムやセキュリティの改善だけでなく、自社のビジネスや働き方の変革が目的であることを意識しながら計画を作成し、効果を検証しながら必要に応じて計画を見直していくために必要となる。

こうした 3 つの理解を併せ持った人材を社内のみで確保することは通常困難である。そのため、ゼロトラスト・アーキテクチャの導入・検討には、自社のビジネス目標を理解し、一緒に検討してくれる外部専門家（IT ベンダーや外部コンサルタント等）の支援を受けることが多い。

『国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021』[11]によると、ゼロトラスト・アーキテクチャの導入において、外部専門家に相談をしている企業は、相談していない企業よりも、ゼロトラストの理解度についての回答において、「他者に説明できる程度理解している」が 20 ポイント以上高くなっている（図表 5-4 参照）。外部専門家には、システムインテグレータやセキュリティベンダー、コンサルティングファームが含まれており、その知見を活用し、自身もゼロトラストを正しく理解することで、適用範囲の最適化や可能性の最大化を図ることが可能になると考察されている。

[11] 国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021（PwC Japan グループ）：
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html

図表 5-4 外部の専門家への相談の有無別に見る理解度の傾向



※PwC Japan グループ,『国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021』より抜粋

5.2.3. 自社の既存セキュリティ関連ルールの見直しも合わせて行う

セキュリティ管理ルールを整備している多くの企業では、セキュリティの懸念から、社給端末で SaaS 等の社外のクラウドサービスを自由に利用することや個人所有端末(BYOD)を業務で利用することなどをルールで禁止している場合がある。ゼロトラストの考え方を取り入れることで、セキュリティを確保しながらこれらを利用できるようになる可能性がある。ただし、そのようなメリットを活かして多様な働き方やユーザーの利便性向上を実現するためには、自社のセキュリティに対する考え方を見直し、それに合わせて既存の社内ルールも見直す必要がある。

実際に、ゼロトラストに関する取り組みを積極的に行っている企業の中には、ゼロトラストに取り組むことで、早いスピード感で新しいテクノロジーを利用可能な IT 環境に変化しているものの、自社のセキュリティルールがその利用に整合しておらず、リスク評価や内部監査等で説明しても納得してもらえないという問題をかかえている企業があった。

そのため、ゼロトラスト・アーキテクチャの検討や導入に合わせて、内部監査部門やリスク管理部門、セキュリティ部門と積極的な議論を行い、セキュリティに関するリスク認識を変えることや、自社のセキュリティ関連ルールを見直すことの検討も進めることが重要である。

5.3. 導入・運用段階

導入・運用段階では、ゼロトラスト・アーキテクチャを導入し、導入後は運用しながら次の段階への展開を計画していく。その展開のサイクルを回すことで、自社のゼロトラスト・アーキテクチャやその運用体制を高度化していく。特にゼロトラスト・アーキテクチャでは、動的ポリシーによる認証・認可が IT システム利用、つまり業務に直接的に影響するため、トラストアルゴリズムの精度を高める取り組みや、理解を得ながらユーザーのデバイス管理を徹底していく取り組みが重要となる。また、こうした運用を継続的に行っていくためにも、可視化による効率化や定型処理の自動化を積極的に行うことで運用負荷を低減し、自社の人材を有効に活用していくことが求められる。

5.3.1. トラストアルゴリズムの設計と継続的な改善

ゼロトラスト・アーキテクチャでは、「3.1.4. ポリシーエンジンのトラストアルゴリズム」で記載したように、トラストアルゴリズムが認証・認可において重要な役割を担う。最小権限の原則に基づき、必要なユーザーが必要な情報資産・IT 資産に必要な時にのみアクセスできるように設計する必要があり、アクセス可否の決定に使用するトラストアルゴリズムが重要となるためである。認証・認可の精度を高めるためには、評価により多くの情報を用いること、および認証・認可の実績等からトラストアルゴリズムを継続的に改善していくことが重要となる。

図表 5-5 のようにトラストアルゴリズムで使用する情報（ユーザーの属性、インストールされているソフトウェアの情報、デバイスの OS のバージョン、ネットワークおよび地理的位置情報等）が多いほど、不正なアクセスを防ぐことが期待できる。一方で、多くの情報を用いた厳密な評価を行いすぎると、本来は業務で必要なユーザーからの IT システムへのアクセスを拒否してしまい、ユーザーの利便性低下につながる。実際に、ゼロトラスト・アーキテクチャを導入した企業では、トラストアルゴリズムに使用するアクセス元の地理的条件を限定しすぎてしまったため、出張等により通常とは異なる場所から業務を行う際にアクセスを拒否してしまった。そのため、地理的条件が変更となった場合はアクセスを拒否するのではなく、追加で生体認証を求めるトラストアルゴリズムに見直した。

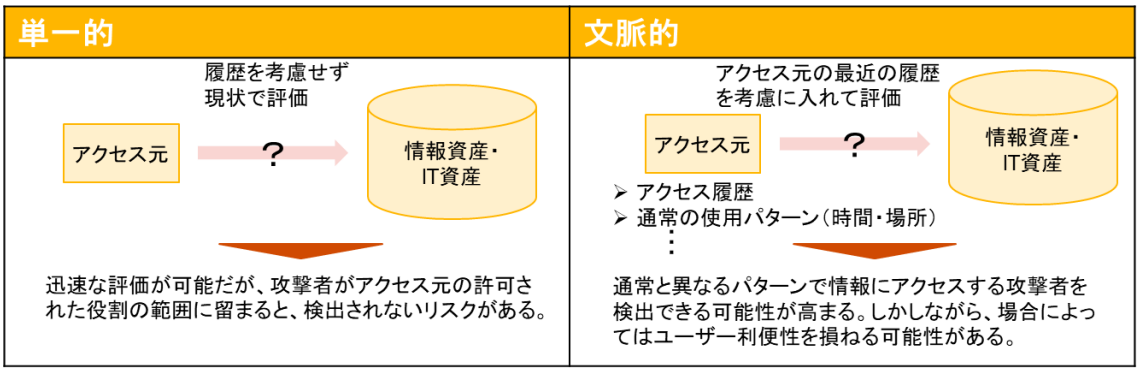
図表 5-5 使用する情報によるトラストアルゴリズムの精度の違い

トラストアルゴリズムの精度	トラストアルゴリズムで使用する情報(例)					認証・認可の結果（アクセスの許可/拒否）
	ユーザー	ソフトウェア	デバイス	所在地	ネットワーク	
精度が低いトラストアルゴリズム	チェックOK	チェックOK	チェック不可（対象外）	チェック不可（対象外）	チェックOK	アクセス許可
精度が高いトラストアルゴリズム	チェックOK	チェックOK	チェックNG	チェックOK	チェックOK	アクセス拒否

※知見をもとに PwC あらた作成

また、より精度の高いトラストアルゴリズムでは、トラストアルゴリズムで使用する情報を文脈的に判断する。文脈的というのは、図表 5-6 に示すようにそれぞれの情報について、最近の履歴も含めて評価することである。履歴を加味することで、ユーザーが通常とは異なるパターンで情報にアクセスする場合、そのアクセスが不正に認証情報を取得して使用している攻撃者によるものであることを検出できる可能性が高まる。このように文脈的なトラストアルゴリズムでは、より厳密なアクセス管理を実現できるが、それらを判断するための履歴情報の保存期間や保存方法、関連するデータの連携等、実現する上で考慮すべきこともある。トラストアルゴリズムを文脈的に判断することはゼロトラスト・アーキテクチャにおいて理想的ではあるものの、本調査では現時点でそれを実現している企業は確認できておらず、将来的に目指して検討を進めている段階である。

図表 5-6 トラストアルゴリズム（単一的・文脈的）による評価



※知見をもとに PwC あらた作成

上記のように、トラストアルゴリズムを定義して設計する際には、セキュリティとユーザーの利便性等のバランスをとることが重要である。また、自社のトラストアルゴリズムを定期的に見直し、継続的に改善していく必要があり、これらの見直しを柔軟に行っていくための体制と仕組みを構築することが重要である。

ゼロトラストに関する取り組みが進んでいる企業では、以下のような声が聞かれた。

- 導入初期に大まかなトラストアルゴリズムを定義した上で、ユーザーの声や自社の運用ナレッジを蓄積し、それらを考慮して継続的にトラストアルゴリズムの改善と最適化を図っている。
- ゼロトラスト・アーキテクチャ導入時に少人数のトライアルのグループを作成し、ユーザーの一部に新しいアーキテクチャを使ってもらいながら、意見を出してもらった。それらを参考にトラストアルゴリズムを最適化していき、現在では全社的にそのトラストアルゴリズムを採用している。

5.3.2. ユーザーの理解と協力が不可欠

ゼロトラスト・アーキテクチャでは、多様な情報を用いて動的ポリシーにより認証・認可が行われる。ユーザーが使用するデバイスにおいても、例えば、以下のような情報がアクセス可否の判断に利用されることがあり、適切にデバイスの管理を行うことが IT システムへアクセスするための前提として必要になる。

- OS のバージョン
- パッチの適用状況
- 地理的位置情報とネットワークの位置情報
- 危険なサイトの閲覧履歴

つまり、IT システムにアクセスするためには、ユーザーが使用するデバイスが自社の動的ポリシーが求めるセキュリティ水準に維持・管理されている必要があり、その必要性をユーザーに理解してもらい、協力を得ることが必要である。

また、デバイスの適切な管理の必要性を理解させることだけでなく、新しいアーキテクチャによって実現されるメリットをユーザーに実感してもらうこともデバイス管理を徹底するために効果的である。ゼロトラスト・アーキテクチャでは社内の IT システムに限らず、社外も含めた様々な IT サービスを利用できる可能性があり、IT システムへアクセスできるデバイスも多種多様になることも考えられる。また、アプリケーションを連携させることで都度 ID・パスワードを求められることがなくなり、ストレスなく様々なアプリ

ケーションを使うことも期待できる。こうしたメリットをユーザーに実感させることで、ユーザー側で必要となるデバイス管理に対する理解を得やすくなる。

それらに加えて、ゼロトラスト・アーキテクチャの導入初期段階では、自社の動的ポリシーが成熟しておらず、必要なアクセスを拒否してしまうことも考えられる。そうした場合に備え、事前の十分な検証とユーザーサポートの充実も必要になる。

5.3.3. 運用体制の整備と効率化と自動化による運用負荷の低減

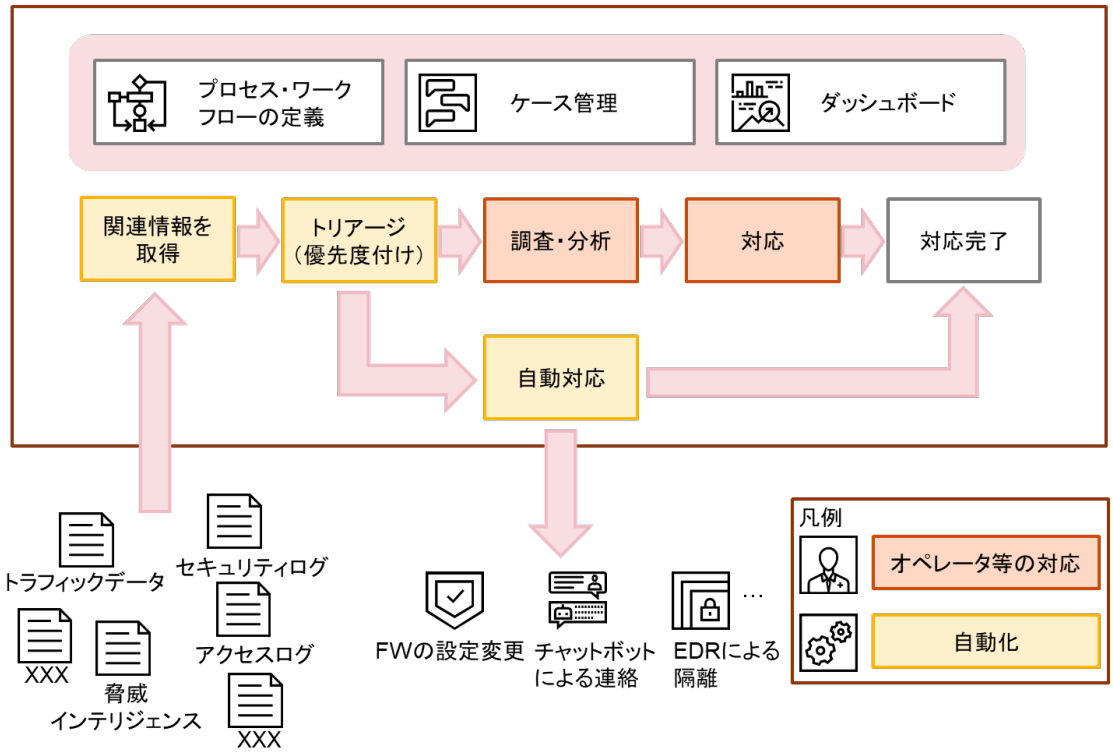
ゼロトラスト・アーキテクチャでは、ネットワークの場所に関係なくすべての通信を保護・検証・監視するため、IT システム運用において大量のログやアラートを確認し、それらの情報を使用して、不正アクセスの検知・対応、アクセスの許可・遮断、トラストアルゴリズムの見直し等の様々な判断を継続的に行っていく必要がある。そのため、境界型セキュリティよりも運用の負荷が高くなることが一般的である。また、境界型セキュリティと併存する場合は、共通のものもあるが、それぞれに対する運用が必要となる。

限られた自社の人材を有効に活用しながら十分な運用体制を整備するためには、社外リソースを活用した運用体制の整備や効率化と自動化による運用負荷の低減が重要となる。

運用への社外リソースを活用については、セキュリティログやアラートを監視する SOC（Security Operation Center）に外部のサービスを活用することが考えられる。SOC は境界型セキュリティでも活用されていたが、ゼロトラスト・アーキテクチャでは、監視の対象が IT インフラよりも業務システムに関するものとなるため、SOC にはより業務の理解が求められることとなる。そのため、SOC の業務の中でも、どこまで自社で対応し、どこから外部の SOC サービスに委託するのか、役割を明確にした上で運用体制を構築することが重要である。

効率化と自動化による運用負荷の低減については、従来からの境界型セキュリティにおいてもログの相関分析のため SIEM を導入したものの、ログの量や種類が増え、相関分析のロジックのメンテナンスが追い付かず、有効に活用できていない企業もある。ゼロトラスト・アーキテクチャの運用では、より多くの情報を活用して不正アクセスの検知・対応、アクセスの許可・遮断、トラストアルゴリズムの見直し等を行うことが求められるため、可視化による運用の効率化と運用・監視の自動化による運用負荷の低減を当初より計画しておくことが重要となる。中には、図表 5-7 に示すような SOAR（Security Orchestration, Automation and Response）を活用して、ログの分析結果を可視化し、定型的な作業やリスクの低い運用については自動化し、人は優先度の高いものや判断が難しいもののみを対応することで、運用負荷の低減を実現している企業もある。

図表 5-7 SOAR（Security Orchestration, Automation and Response）のイメージ



※知見をもとに PwC あらた作成

5.3.4. ゼロトラスト・アーキテクチャに対応したセキュリティ評価・監査指標の検討

ゼロトラストは、従来からの境界型セキュリティとセキュリティに対する考え方が異なるため、これまで企業が行ってきたセキュリティ評価や監査の指標だけでは十分なリスク評価ができない可能性がある。

境界型セキュリティでは、入口対策としてファイアウォールの設定や、IPS・IDS 等の侵入検知システムの導入、内部対策としてデバイスへのパッチ適用やマルウェア対策ソフトの導入、出口対策として外部へのトラフィックの監視等の項目をセキュリティ評価・監査にて確認してきた。内部と外部の境界という概念がなく、セッション毎に動的ポリシーによる認証・認可を行うゼロトラスト・アーキテクチャでは、これらの指標だけでは十分なリスク評価が行えない可能性がある。

ゼロトラスト・アーキテクチャでは、「3.1.1. ゼロトラストの原則」に記載したゼロトラストの各原則に対する成熟度や「3.1.5. ゼロトラスト・アーキテクチャに関する脅威」に記載したゼロトラスト固有のリスクに対する対応状況等の観点での評価指標を検討し、セキュリティを評価・監査する必要がある。

5.3.5. 次の段階へ移行するための基準の設定とモニタリング

「5.1.4. 「ありたい姿」から実現可能なロードマップを描く」に記載したように、ゼロトラスト・アーキテクチャの導入は段階的に行うことが一般的である。そのため、初期の導入が完了して運用が開始した後に、どのタイミングで次の段階に進むかの判断基準を設けることが重要となる。

ゼロトラスト・アーキテクチャの運用開始後は、認証・認可におけるトラストアルゴリズムの調整や IT システム運用の変更、ユーザーサポート等の対応を行い自社のナレッジを蓄積し、対応力を高めながらゼロトラスト・アーキテクチャを最適化していく。こうした取り組みによって、自社がゼロトラスト・アーキテクチャに順応した時期に、当初計画していた次の段階に移行することが望ましい。ただし、限られた人で運

用や継続的な改善を行っている中では、なかなか次の段階へ移行できない場合がある。そのため、次の段階に移るための基準を設けて、それをモニタリングして判断することが有効である。基準として、定量的・定性的のどちらも考えられるが、例えば以下のようなものが挙げられる。

- ゼロトラスト・アーキテクチャに関連する問い合わせ件数
- 業務上必要な認証・認可の拒否件数
- 開発・運用部門の負荷（フィードバック）
- 運用コスト
- ユーザーの声（フィードバック）

上記のような観点でモニタリングを行うことで、よりリスクの高いビジネスプロセスやそれに関連するITシステムのゼロトラスト・アーキテクチャへの移行の判断が可能となる。モニタリングの結果は、次の段階における有益なインプット情報となり、また、重大な改善点が発見された場合は、全体の移行計画の見直しや自社の現状把握を繰り返すことも考えられる。このように、状況に応じて適切なタイミングで計画と移行を進めることがゼロトラスト・アーキテクチャの導入において重要であり、これらを展開サイクルとして繰り返していくことが望ましい。

6. 金融業界における今後のセキュリティの考え方

本章では、今回の調査を通して得られた内容と PwC あらたの知見をもとに、デジタル変革の進む社会の中で、金融機関がゼロトラストと呼ばれる新たなセキュリティモデルとどのように向き合っていくことが望ましいのか、あるいはゼロトラストという考え方を踏まえてどのようにサイバーセキュリティを高度化していくことが考えられるかについて考察する。

6.1. 基本的なセキュリティ対策を徹底する

ゼロトラスト・アーキテクチャでは、デバイスの状態や場所等の情報から動的ポリシーを決定することや、セッション毎に認証・認可を行うことが注目されがちであるが、「すべての情報資産や IT 資産を特定して管理すること」、「エンドポイントのセキュリティを維持すること」、「ログを取得して監視すること」といった、従来からの境界型セキュリティでも重要とされてきた対策も必要不可欠である。

すべての情報資産・IT 資産の特定と管理では、利用している IT システムやデバイスが漏れなく把握・管理されると同時に、シャドーIT の防止や検知の実現が重要である。具体的には、CASB を導入してクラウドサービスの利用を制限・監視することや、MDM で管理されたデバイスのみを利用可能とすることなどが挙げられる。

エンドポイントのセキュリティの維持では、IT システムやデバイスを常に健全な状態に保ち、セキュリティの基本を徹底する「サイバーハイジーン（衛生管理）」と呼ばれる対策が重要である。サイバーハイジーンには、複雑なパスワードや多要素認証などアクセス時の本人確認を徹底する、不要なソフトウェアは導入せず、不要なサービスやプロトコルは無効化する、常に最新のセキュリティパッチを適用する、EDR などのマルウェア対策ソフトを導入するなどが含まれる。

ログの取得と監視では、セキュリティの観点で、外部・内部からの不審なアクセスや不正な操作を特定するために必要なログを、ネットワーク機器やサーバで取得し、必要な期間保存すること、そして取得したログを分析して不正アクセス・操作の特定に活用することが重要である。ログの活用としては、不正アクセス等が疑われる事案が発生した際の事後の分析に使用することだけではなく、リアルタイムで分析して不正通信の検知と遮断を適宜に行うことなども挙げられる。また、SIEM では、外部に接続している IT システムやネットワーク機器に関するログの収集・分析にとどまらず、内部不正や攻撃者の侵入に備えて内部の様々なネットワーク機器や IT システムからもログを取得し、一元的に集約して高度な分析を行うことなども重要となる。

これらの対策の中には、多くの金融機関が従来から取り組んできているものを多く含むが、実際には、シャドーIT までは特定できていない、ソフトウェアやサービス・プロトコルの要・不要を詳細に定義した設定まではできていない、タイムリーな脆弱性情報の収集とパッチ適用が行えていない、ログは取得しているが事後の調査目的での活用に留まっているなど、改善の余地のある金融機関も多い。ゼロトラストに関する検討と合わせて、これらの基本的なセキュリティ対策が十分にできているかを評価し、十分でない場合は改善に向けた取り組みを行うことが必要である。

6.2. 潮流を見極めながら自社に適したゼロトラストの検討を続ける

ゼロトラスト・アーキテクチャの導入に取り組んでいる金融機関はあるもが、既存の IT 環境を維持しつつ移行を進めることの難しさ、ソリューションやその導入・運用に必要な人的リソースやコストの問題、参考となる他社事例がまだまだ限定的であるなどの点から検討が進んでいない金融機関が多い。

「2.2.1. デジタル技術の進展による IT 環境の多様化とサイバーリスクの高まり」に記載したとおり、クラウドサービスの利用拡大、リモートワークの普及、IT システムやデータの外部連携の増加といった世の中の流れが進むにつれて、セキュリティを維持していくためにはゼロトラストの考え方が重要になってくる。それは、金融業界も例外ではない。

ゼロトラスト・アーキテクチャに関する技術やソリューションは年々進化しており、導入実績も増えている状況である。現時点では「ゼロトラストという考え方の必要性を感じていない」、「ゼロトラストを検討するための人や知識が不足している」、「具体的な取り組みを進めたいが技術やコストで適切なソリューションがない」などの理由から、ゼロトラスト・アーキテクチャの導入に向けた取り組みを行っていない金融機関も少なくない。しかし、そうした金融機関であっても、ゼロトラストの考え方を理解した上で、ゼロトラスト・アーキテクチャに関するソリューションの情報やゼロトラストという考え方を取り入れた良好事例等を継続的に収集していくこと、そして自社のビジネスの状況や IT 環境に適したソリューションや導入方法がないかを見極めながら、自社にとってのゼロトラストやセキュリティのあり方を検討し実現に向けて取り組み続けていくことが重要である。

6.3. 新たなビジネスを支えるセキュリティの考え方として捉える

これまで、セキュリティは企業の情報資産や IT 資産を保護するためのものであり、企業にとって「守り」のためのものとして位置づけられてきた。ゼロトラストの考え方は、リモートワークをはじめとした多様な働き方を実現したい企業やデータやクラウドサービスを活用した新たなビジネスを創出したい企業に有効なセキュリティの考え方である。言い換えれば、従来からの境界型セキュリティのみに固執し、IT 利活用の範囲を制限してしまう場合は、新たなビジネスの可能性を広げることへの制約になりかねない。

そのため、金融機関がゼロトラスト・アーキテクチャの導入を検討する際には、IT システムやセキュリティ面でのメリットやデメリットを比較するのみではなく、自社のビジネスや働き方にどのような効果や便益をもたらすかを第一に考えることが重要となる。ゼロトラスト・アーキテクチャは、本調査で事例として取り上げたリモートワークやクラウドサービス領域での活用のみならず、以下のようなケースでの利用も期待される。

- 外部委託先や代理店が金融機関の IT システムやデータへアクセスし、業務連携する際の認証・認可
- オープンネットワークに接続された IoT デバイス等から金融機関がデータを収集する場合の接続時の認証・認可

上記は一例に過ぎないが、FinTech をはじめとする様々なビジネスの広がりの可能性がある金融分野においては、ゼロトラストを単なるセキュリティ対策としてとらえるのではなく、新たな金融サービス実現に貢献できるセキュリティの考え方として柔軟に捉えていくことも重要である。

ご注意

本報告書内に記載されたインターネット上の URL は 2021 年（令和 3 年）3 月現在のものであり、URL およびその内容は、その後、変更、移動、削除される場合がある。

2020 年（令和 2 年）度 金融庁委託調査

ゼロトラストの現状調査と事例分析に関する調査報告書

PwC あらた有限責任監査法人

2021 年（令和 3 年）3 月 31 日 発行