ICSCoE TLP:WHITE

ゼロトラスト移行のすゝめ

2022 年 6 月

独立行政法人情報処理推進機構

産業サイバーセキュリティセンター

中核人材育成プログラム　５期生

ゼロトラストプロジェクト

まえがき

ゼロトラストは、これまでの「境界内部は信頼できる領域で、境界外部は信用できない領域である」という考え方ではなく、「たとえ境界内部であっても無条件に信用せず全てにおいて確認し認証・認可を行う」という考え方に基づいて社内の情報資産を守る概念である。この概念は 2010 年ごろから提唱されていたが、近年の新型コロナウィルス感染症(COVID-19)の蔓延によるテレワークの普及や、DX 推進に伴うクラウドサービス利用の急増などにより、社内の情報資産が境界の内側に留まらず、境界の外側の資産も守らなければならない現状から更に注目が高まっている。

ゼロトラストの概念について説明している書籍や WEB ページは多数あり、どのような概念なのか理解している方は多いと考える。一方でゼロトラストは具体的なソリューションを指しているわけではないため、ベンダーに導入を依頼することで実現できるものではない。そのため「どのようにゼロトラスト構成へ移行するプロジェクトを進めればよいのかわからない」という声は多いと考えた。

今回、上記の課題を解決するためにプロジェクトを立ち上げ、さまざまな組織のゼロトラスト移行を支援してきたコンサル企業やベンダー企業、また実際に移行したユーザー企業に対し、ゼロトラスト環境へ移行するために必要な流れについてヒアリングを行った。

本書ではゼロトラスト構成への移行を検討している組織の担当者に対し、ヒアリングの内容を参考にした上で、プロジェクトメンバーで検討したゼロトラスト構成へ移行する際の流れを示す。

最後に、ゼロトラストはこれといった正解がある概念ではないため、本書で記載した流れについても唯一無二の正解ではなく、一つの参考として捉えていただきたい。

目次

本書の構成

第 1 章：「はじめに」では、ゼロトラストの概念についての説明、国内におけるゼロトラスト導入に関する実態調査の紹介を行い、本書の目的を説明する。

第 2 章：「ゼロトラスト構成への移行」では、ゼロトラスト構成への移行を検討している組織に対し、必要なマインドや具体的な進め方の解説を行う。

第 3 章：「まとめ」では、本書の内容をまとめ、説明する。

免責事項

- このドキュメントは単に情報として提供され、内容は予告なしに変更される場合がある。
- 発行元の許可なく、本書の記載内容を複写、転載することを禁止する。
- このドキュメントに誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証や条件を含め明示的又は黙示的な保証や条件は一切無いものとする。
- 本書に記載の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、作成者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書作成者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は，発行日から 2 年間とする。

なお、本書を利用するにあたって前提知識として、”情報処理技術者試験(IT パスポート試験)の合格程度の水準”の知識が必要となる。

第1章：はじめに

1.1.ゼロトラストとは

ゼロトラストとは、2010 年にアメリカの調査会社フォレスターリサーチが提唱した概念で、「境界型防御内のネットワークは安全で、境界外部のネットワークは危険だ」という従来の考え方に対して、「たとえ境界内部であっても無条件に信用せず、全てにおいて確認し認証・認可を行う」という概念である。ゼロトラストの基本的な考え方は NIST SP800-207 で解説されており、以下の表 1-1 に記す基本的な 7 つの考え方がある。

表 1-1　NIST SP800-207 ゼロトラスト・アーキテクチャの基本的な考え方

No.	基本的な 7 つの考え方
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を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、ネットワークの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、セキュリティ体制の改善に利用する

この概念は新型コロナウィルス感染症の蔓延によるテレワークの普及や、DX 推進に伴うクラウドサービス利用の急増などにより、社内の情報資産が境界の内側に留まらず、境界の外側の資産も守らなければならない現状から更に注目が高まっている。

本書では、ゼロトラストを構成する重要な要素を「ID 統制」「デバイス統制・保護」「ネットワークセキュリティ」「データ漏洩防止」「ログの収集・分析」に分類し、ゼロトラストとの関連性とそれぞれに関連するソリューションを紹介する。ここでは、セキュリティ面だけでなくユーザー利便性、運用効率化の観点でもメリットがあることを理解いただきたい。

◆ ID 統制

ゼロトラストの概念を実装するにあたり、最も重要と言えるのが ID 管理である。なぜなら「信頼できるネットワークが存在しない」というゼロトラストの概念において「誰が」リソースにアクセスしようとしているのか都度的確に識別し認証・認可を行うことが重要だからである。この管理が不適切な場合、例えば退職者のアカウントを悪用されて、機密ファイルが閲覧、持ち出しされるなど、重大なインシデントに繋がりかねない。一方で、昨今 SaaS サービスの利用拡大によりサービス個別で ID 管理を行うと、管理者の負担が非常に大きい。その結果、適切な管理を実施する困難になることが新たなリスクとなっている。そのため ID 管理は可能な限り一元的に統制された状態で適切に行われるべきである。

関連するソリューション

- IDaaS (ID as a Service)

【主な機能】

➢ ID 管理

組織が利用するあらゆるシステム・サービスの ID を一元的に管理する。
IDaaS への ID 登録は、オンプレミスの ID 管理基盤と連携することができる。また IDaaS の持つ ID 情報を SaaS サービスに反映させる(プロビジョニングを行う)ことで、オンプレミスだけでなく、SaaS サービスなども含めて一元的に ID 管理が可能な環境を提供する。これにより組織全体の ID 管理業務負荷が軽減し、ID 削除の対応漏れなどが発生するリスクが低減する。

➢ SSO (Single Sign On)

ユーザーが一度 IDaaS から認証・認可を受ければ、さまざまなサービスへのサインインをパスワード入力なしで行うことができる。つまり、ユーザーはサービスごとにパスワードを覚える必要がなくなる。またシステム管理者はパスワード管理の負荷が軽減される。ユーザーは IDaaS から認証・認可を受けるための ID、パスワードのみ管理すれば良いため、簡単なパスワードの減少、複数サービスで同パスワードを使い回すといったリスクを軽減出来る。

➢ アクセスコントロール

サービス・フォルダ等にアクセスが可能な利用者や端末、場所等に制限をかけ、許可を得た利用者のみがサービスを利用できるようコントロールする。
また、ユーザーが普段と異なるネットワークやデバイスからのアクセスを試みた場合に追加の認証を求める動的な認証・認可も実現できる。

◆ デバイス統制・保護

テレワークなど多様な働き方が求められる現代において、デバイスが攻撃を受けるリスクは以前に比べて高くなっている。そのためデバイスのセキュリティはこれまで以上に気を使わなくてはならなくなった。また、境界型防御の中でデバイスを利用する場合と比較して、テレワーク環境下ではデバイスに対して適切なセキュリティ設定を施すことやその確認が難しくなっている。そのため組織で管理すべきデバイスの洗い出しや、より強固なデバイスの保護、ユーザーがどこにいてもデバイスの統制が取れる環境を作る必要がある。またゼロトラストの概念においては、組織の資産にアクセスするデバイスが組織の管理下にあること、適切な設定が行われていることを認証・認可の際にチェックすることが重要である。

関連するソリューション

- MDM (Mobile Device Management)

  【主な機能】

  - デバイスの機能制限

    デバイスの機能のうち、業務に必要な機能以外は利用させない制御が可能である。例えば Bluetooth への接続や外部記憶媒体の接続などを制限出来る。

  - デバイス紛失時の対応

    遠隔から端末をロックするリモートロックや、端末のデータを消去するリモートワイプといった機能がある。端末の紛失時にはこのような機能を用いて情報漏洩の発生を未然に防ぐことが可能である。

  - ポリシーやアプリケーションの一斉配布

    管理下のすべての端末に対して「適用すべきセキュリティ設定」や「必要なアプリケーションの配布」などを一斉に行うことができる。また、適用状況も確認できる。

  - IDaaS との連携

    IDaaS と連携することで、組織の管理下にあり、適切な設定が施されている端末からのみアクセスを可能にするといった制御が可能となる。

- EPP (Endpoint Protect Platform)

  【主な機能】

  - マルウェア検知・遮断

    アンチウィルス製品の役割はマルウェアを検知して遮断することである。従来はパターンマッチングによる検知が一般的であったが、最近は機械学習や振る舞い解析などの技術を用いて未知の攻撃を防ぐことができる製品もある。

- EDR (Endpoint Detection and Response)

  【主な機能】

  - 監視機能

    ファイル操作、プロセス、イベントなどあらゆる挙動を監視する。不審な挙動を発見するとユーザーや管理者にアラートで知らせる。
    また、既知の攻撃だけでなく、未知の攻撃に対しても振る舞い検知で対応可能である。

  - 攻撃を受けた後の対応

    デバイスが攻撃を受けた場合に、ネットワーク隔離や不審な挙動をしているプロセスの中断といった対応を自動で行う。

  - IDaaS との連携

    IDaaS へリスク情報を連携することで、EDR により計算されたリスク値をもとに、リスクの高い状態にある端末から各種サービスへのアクセスを禁止する制御が可能である。

◆ ネットワークセキュリティ

現在、社外から社内環境にアクセスする際に VPN を使用している組織は多いと思われる。昨今の標的型攻撃はテレワークの影響もあり VPN 装置を狙って社内ネットワークに侵入するケースが多発している。VPN はネットワークに対するアクセス認証を行う。これは一度攻撃を受けると、社内ネットワークのさまざまな機器にアクセス可能になることを意味し、表 1-1 中の「すべてのリソースに対し、アクセスが許可される前に、認証と認可を厳格に実施する」というゼロトラストの概念に適していない。

また、SaaS サービスの利用拡大により、全ての通信が社内のゲートウェイを抜けると通信量の増大により遅延が発生し、業務に支障が出るという課題もある。その際にローカルブレイクアウトと呼ばれる、社内環境のゲートウェイを経由せずに直接インターネットに抜けてサービスにアクセスする手法がとられることが多い。ゼロトラストは、全ての通信は保護されるべきという考え方であり、そういった通信に対しても必要なセキュリティ対策を施す必要がある。また、組織は守るべきステムを把握する必要があるが、組織が認知していない SaaS サービスの利用(以降、シャドーIT と呼ぶ)も課題となっており、対策を打つ必要がある。

関連するソリューション

- IAP (Identity Aware Proxy)

  【主な機能】

  - アプリケーション単位の接続制御

    VPN がネットワーク単位での認証であるのに対し、IAP はオンプレミス上の WEB アプリケーションに対し、アプリケーション単位での認証が可能となる。環境を実装する際には、社内環境に接続対象のシステムと通信できる位置にコネクタを配置する必要がある。通信はこのコネクタ→IAP の方向で開始されるため、社内オンプレミス環境の FW にインバウンド通信の穴を開ける必要がない点もメリットである。WEB アプリケーション以外のレガシーアプリケーションなどに IAP を経由したアクセスを導入したい場合は、クライアントにエージェントをインストールすることでアクセス可能となる製品もある。

  - IDaaS との連携

    IDaaS と連携することで、ユーザー属性や使用デバイスといった情報から、オンプレミス環境のアプリケーションにアクセス制御を実装できる。

- SWG (Secure Web Gateway)/CASB (Cloud Access Security Broker)
  【主な機能】
  - 悪性な WEB コンテンツへのアクセス制限
    社内オンプレミスのプロキシサーバで行っている WEB フィルタリングと同様に組織のポリシーに基づいた WEB フィルタリングを実装することが出来る。不審な IP アドレスや URL はベンダーがリスト化しているものに組織独自でルールを追加することも可能である。

  - SSL 復号機能
    SSL で WEB サービスの通信を暗号化しているものに対し、SSL 通信の復号をリアルタイムで行い、通信内容の詳細をチェックする。

  - マルウェアの検出
    WEB 経由で送信されるデータの中にマルウェアが仕込まれていないかシグネチャと比較して検知する機能や、実行ファイルはサンドボックス上で不審な振る舞いを行わないかチェックする機能がある。

  - シャドーIT の可視化、制限
    管理されたデバイスからの通信を監視することで、組織の中で利用されている SaaS サービスを可視化できる。この時、セキュリティ上懸念がある SaaS サービスなど、利用することが好ましくないものが見つかった場合は、アクセスを遮断するなどの制御が可能である。

  - テナント識別
    同じ SaaS サービスであっても、組織で契約しているテナントと個人で契約しているテナントを識別し、アクセスを制御することが出来る。社内情報が個人利用のサービスにアップロードされることを防止できる。

◆ データ漏洩防止

ゼロトラストの概念ではすべてデータをリソースと見做し、保護対象としている。つまり、内部犯行者や攻撃者による機密情報の不正なデータの持ち出しを防ぐ、もしくは持ち出されたとしてもデータを閲覧させないといった観点での対策が必要である。またこのような対策は、悪意のある行為だけでなく、人為的なミスによる情報漏洩への対策としても有効に働く。

関連するソリューション

- DLP (Data Loss Prevention)
  主な機能
  - 機密情報の不正な取り扱い防止
    あらかじめ組織として機密情報の定義を行った上で、機密情報が含まれるファイルの取り扱いを制限することが出来る。例えば、社内機密ファイルのダウンロード禁止やアップロード禁止、外部記憶媒体へのコピー禁止、メール転送禁止といった制御を行うことが出来る。

- IRM (Information Right Management)
  主な機能
  - 機密ファイルやメールの暗号化とアクセス制御
    機密ファイルやメールを暗号化した上でアクセス権限を設けることで、アクセス権を持たない第三者にファイルが漏洩したとしても、情報が閲覧されることを防ぐ。また、アクセス権をもつユーザーに対しては編集可能、印刷可能といった権限を細かに設定することが出来る。

◆ ログの収集・分析

ゼロトラストの概念に「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、ネットワークの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、セキュリティ体制の改善に利用する」とある。このように、社内 IT 環境を構成する機器からログを集約・分析することでサイバー攻撃の早期検知や対応を行うことはもちろん、恒久的な対策の検討も行うことで、より良い IT 環境を目指す必要がある。

関連するソリューション

- SIEM (Security Information and Event Management)

主な機能

- あらゆる機器からのログ集約と可視化
  組織内の各種サーバやネットワーク機器など、あらゆる資産からログを収集し、一元管理することが出来る。また、ダッシュボードにおいてログの可視化を行うことで、直近の組織に対する攻撃の動向などを把握することが出来る。

- 収集したログの分析
  収集したログを分析することで、不審な通信や挙動の検知を行う。さまざまな機器のログを集約しているため、複数の機器のログを合わせて関係性を探る相関分析という手法も可能である。脅威インテリジェンスを用いた脅威検知や、機械学習により異常な振る舞いを検知するアノマリ検知といった手法があり、検知ルールについては組織でカスタマイズ可能である。

1.2.ゼロトラスト構成への移行に関する実態調査から見えること

ゼロトラスト構成への移行に関する実態について、Fortinet 社、Microsoft 社、PwC 社の報告書を元に、移行の状況や、障壁となっている課題について以下にまとめる。

◆　ゼロトラストの重要性と移行状況

Microsoft 社が 2021 年に組織のセキュリティ意思決定者を対象に行った調査(対象国：米国、日本、ドイツ、オーストラリア/ニュージーランド)では、ほぼ全員(96%)がゼロトラスト構成への移行が必要であると回答している。また、移行状況については約 76%の組織が移行を始めている(うち 35%は完全に移行済)と回答した。

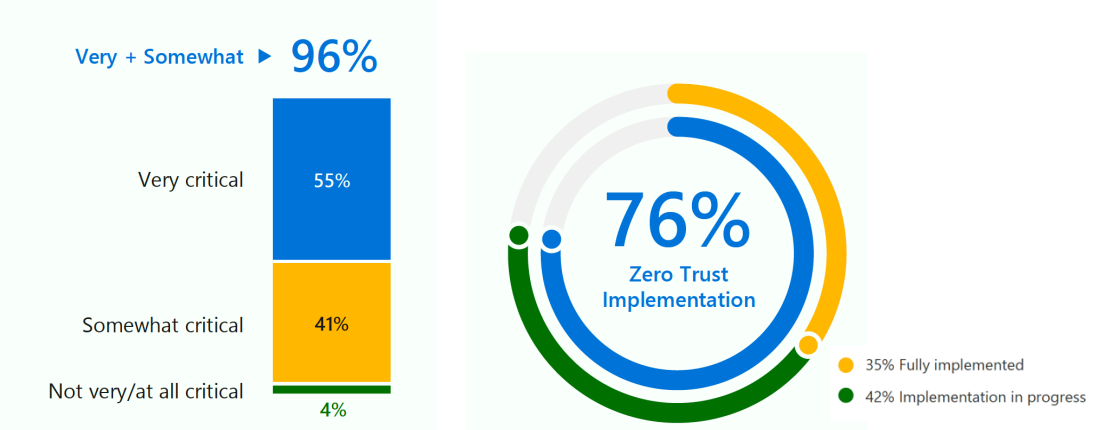


図 1-1 Microsoft 社によるゼロトラストの重要性(左)と移行状況(右)についての調査結果
(出典：Microsoft Security, Zero Trust Adoption Report(July 2021), p8, exhibit1, p11, exhibit 5)

この数字から多くの組織でゼロトラスト構成への移行が進んでいるように感じる。しかし Microsoft 社によると、この結果はあくまで自己評価によるもので、ゼロトラストの成熟度について誤認している組織もあり、移行済と回答した組織のうち約半数は完璧にゼロトラストの概念を採用できている訳ではないと主張している。そのため実際の移行状況は**図 1-1**(右)ほど高くはなく、未だ課題を残している組織も多い。

◆　ゼロトラスト構成へ移行する難しさ、具体的な課題

Fortinet 社が 2022 年に公表した世界中のセキュリティ専門家やビジネスリーダーを対象に行った調査では、ゼロトラスト構成への移行にあたり、約 8 割の組織が難しさを感じているという結果が出ている。その内約 50%は「とても難しい」「極度に難しい」と感じている。

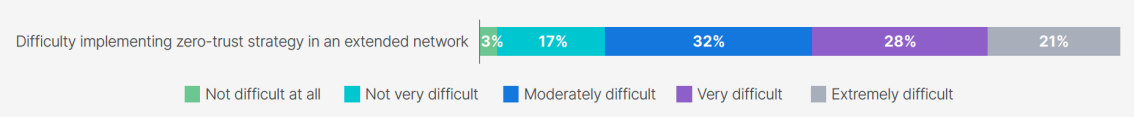


図 1-2　Fortinet 社によるゼロトラスト構成への移行の難しさに関する調査結果
（出典：Fortinet, The State of Zero Trust Report(January 10 2020), p7, figure 7）

また、具体的に直面した課題に関する調査では、完全なソリューションを持つベンダーの欠如、予算の不足、ゼロトラスト移行に関する知識不足が上位に挙がった。
ゼロトラストの概念を全て詰め込んだ製品を提供するベンダーの欠如により、セキュリティコンポーネントごとに導入した結果、部分的で、非統合的なソリューションとなってしまうことがあると Fortinet 社は主張している。さまざまなソリューションを統合して構築するゼロトラスト構成では、各ソリューションの連携のしやすさといった点にも注意を払わなければならない。

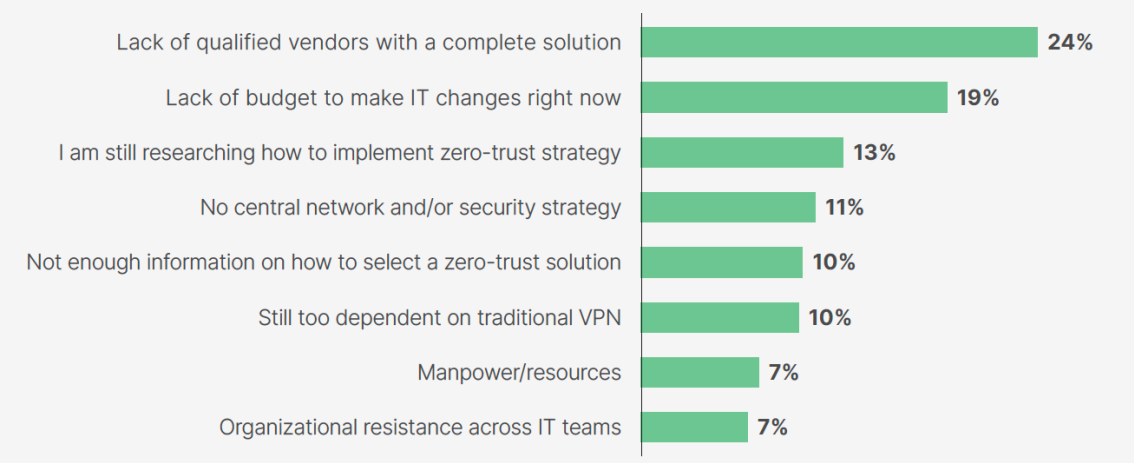


図 1-3　Fortinet 社によるゼロトラスト移行の際に直面した課題に関する調査
（出典：Fortinet, The State of Zero Trust Report(January 10 2020), p7, figure 11）

PwC が日本国内の企業を対象に行ったゼロトラストアーキテクチャに関する実態調査（図 1-4）でも、ゼロトラスト構成への移行に関する課題や障壁についてアンケートが行われた。その結果、約 85%の組織が何かしらの課題に直面しており、具体的な課題として「予算」や「ゼロトラスト移行に関する知識不足」に起因する項目が挙げられた。この結果は Fortinet の調査と類似している。一方で、経営層が協力的でないといった意見は、ボトムアップで施策を推進する組織が多い国内特有のものであるように感じた。後に第 2 章でも説明するが、ゼロトラストのように多くのリソースを要する施策を実施するには、経営層自らが理解し推進する姿勢が重要である。

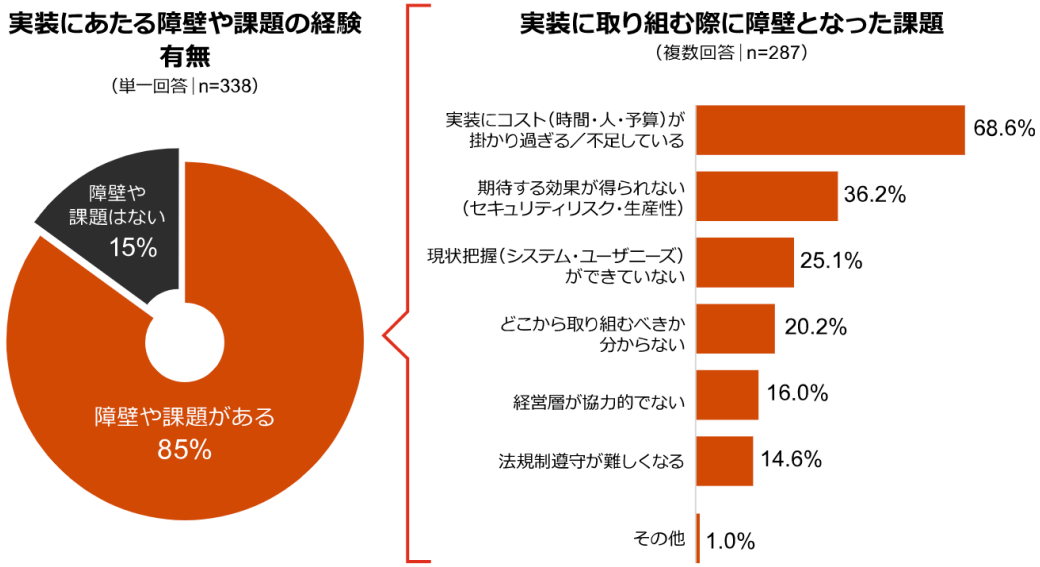


図 1-4　PwC 社によるゼロトラスト移行の際に直面した課題に関する調査

（出典元：https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html に記載された図表 4）

◆　担当者のゼロトラスト理解度の重要性

PwC 社が実施した担当者のゼロトラストに関する理解度別に得られた効果を調査したアンケートでは、ほぼ全ての項目で担当者の理解度が高いほど大きな効果が得られることが示されている。またその差はセキュリティ観点に比べ、DX 推進やコスト削減といった項目で顕著である。組織の担当者がゼロトラストの概念とは何か、具体的にどのようなメリットが得られ、それを実現するためにどのような営みが必要になるのかを適切に把握し、推進する必要がある。

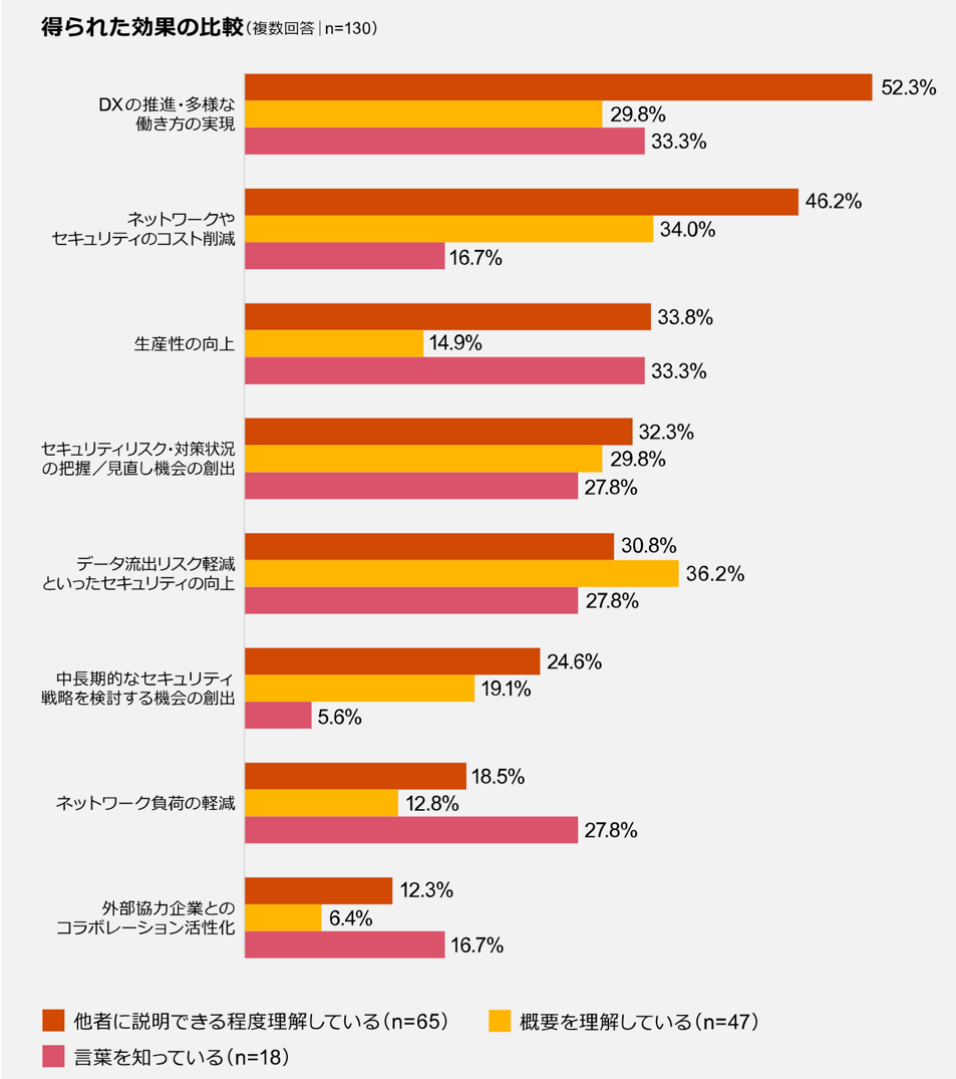


図 1-5　PwC 社による担当者のゼロトラスト理解度の重要性に関する調査

（出典元：https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html）

1.3.本書の目的

ゼロトラストの概念は近年のテレワークやクラウド利用の普及により注目を集めているが、1.2 節で紹介した調査結果からも分かるように、いざ自組織に実装しようとしたときにはさまざまな課題に直面することが予想される。また、ゼロトラスト移行の効果を最大限発揮するためには、ゼロトラストに対する担当者の理解が不可欠である。

そこで本書ではゼロトラストの概念を自組織に実装する際に必要となる検討の流れや、得られるメリット、ソリューションの導入順序とその際のポイントについてまとめる。これからゼロトラスト移行を検討している組織の担当者に参考にしていただけると幸いである。

第2章：ゼロトラスト構成への移行

2.1.ゼロトラスト構成へ移行検討中の組織に必要なマインド

ゼロトラスト構成への移行で最も重要な点は、何を解決するためにゼロトラストという戦術を使うのかを明確化することである。この部分がはっきりしないままプロジェクトを推進すると「ゼロトラスト構成に移行すること」が目的化してしまい、組織の課題にあった構成にならない可能性がある。ゼロトラストとは概念であり、唯一無二の正解という構成はない。なぜなら組織が抱える課題はそれぞれ異なるからである。その点を組織の担当者が理解した上でプロジェクトを推進する必要がある。

また、ゼロトラストはセキュリティ観点の概念ではあるものの、実装の際にはユーザーの利便性やシステム運用の効率化の面でも大きな効果を発揮する。そのため、セキュリティ対策というよりも、組織全体の IT 戦略として考え、推進すべきである。組織全体の IT 戦略としてプロジェクトを推進するためには、セキュリティ・IT 部署だけでなく、経営者をはじめ関係部署の協力が不可欠である。どのように協調すべきかは第 2.3 章で解説するが、ここではセキュリティ・IT 部門だけで進める内容ではないということを理解していただきたい。特に他部署と「現 IT 環境についてのレビュー・今後どのような働き方をしたいか」といった内容をすり合わせる事は非常に重要である。

また、経営者の理解も大きな成功要因の一つである。経営者自身が組織のリスクや目指すべき姿を見極め、トップダウンでプロジェクトを推進している組織ほど円滑にプロジェクトが進みやすい。これはゼロトラスト構成への移行に限った話ではないが、重要な観点の一つである。

2.2.ゼロトラスト移行の進め方

ゼロトラスト実装において「どこから取り組むべきかわからない」という課題がPwC のアンケートでも上がっていたが、同様の悩みを抱えている組織は多いと考えられる。

本章では、ゼロトラスト構成への移行支援を行っているコンサル企業・ベンダー企業、また実際にゼロトラスト構成へ移行したユーザー企業にヒアリングを行った結果を参考に、我々のプロジェクトで検討したゼロトラスト構成への移行の流れとその際のポイントを解説する。

全体的な流れは図 2-1 の通りである。

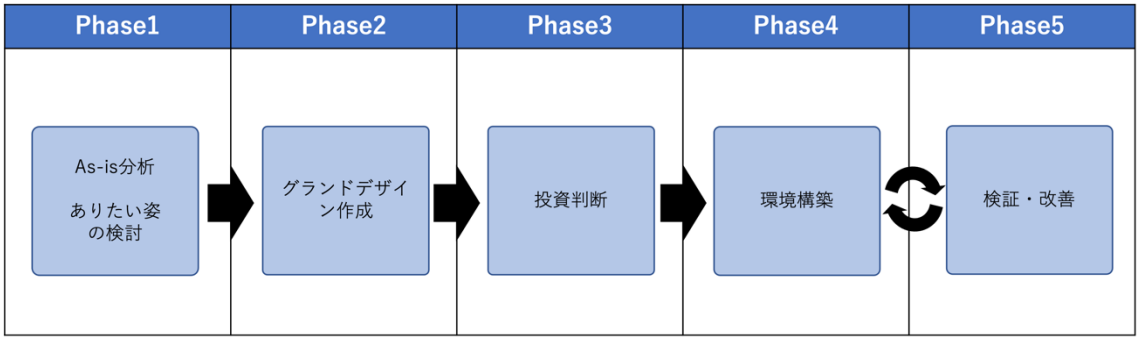


図 2-1　ゼロトラスト構成へ移行するための全体的な流れ

Phase1:　ゼロトラスト構成を目指すにあたって最も重要な観点はその目的を明確化することである。そのため、最終的に組織がどのようにありたいか明確にすることや、As-is 分析により現在抱えている課題を可視化することが重要である。ここではセキュリティに関するリスク分析だけでなく、既存 IT 環境のユーザビリティや運用負荷などにも目を向けて改善すべき点を洗い出し、ありたい姿を検討する。

Phase2:　次に、グランドデザインの作成を行う。ここでは Phase1 の結果を元に将来的にどのようになりたいか、その環境を実現するためにどのようなソリューションが必要かを検討する。

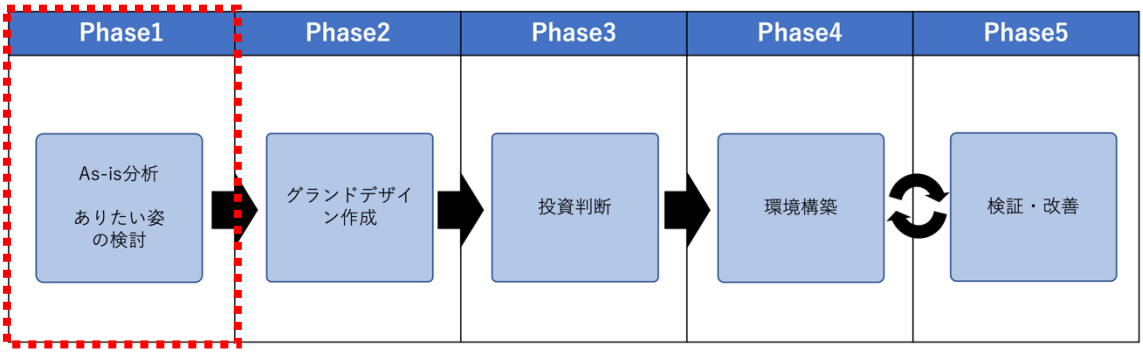
Phase3:　グランドデザインの作成ができたら投資判断が必要となる。ここでは経営者を初め、ステークホルダーに納得してもらうための説明が必要となる。

Phase4:　Phase2 で作成したグランドデザインを元に環境を構築する。

Phase5:　ユーザーからのフィードバックを得つつ、より良い構成に改善する。

それぞれのフェーズで必要な検討事項など、詳細を以降で説明する。

2.2.1.As-is 分析、ありたい姿の検討　(Phase1)



As-is 分析やありたい姿の検討は組織のゼロトラスト移行の目的を見定めるための重要なフェーズである。この部分を疎かにすると何のためにやるのか曖昧になってしまい、結果として期待していた効果を最大限発揮できないおそれがある。

また、検討を行う際、セキュリティの観点はもちろん、既存 IT 環境のユーザー利便性や運用負荷の観点も含めた課題を洗い出し、ありたい姿を描くべきである。

◆　As-is 分析

- **セキュリティ観点**

  セキュリティ観点の課題を洗い出す手法として、まずは既存のフレームワーク(NIST CSF など)を用いたリスク分析を行う。その際、正しくリスク分析を行うために以下のような観点で確認が必要である。

  - 既存 IT 環境の NW 構成
  - 組織の持つ情報資産の洗い出し
  - 物理的な執務箇所の把握
  - 使用している ID 基盤とその運用
  - 重要データの保護

    ※重要データはどこに置かれていて、誰がどのデバイスからアクセス可能か

- **ユーザー利便性観点**

  既存 IT 環境のユーザー利便性に関しては、事業部門(ユーザー部門)の社員にアンケートやヒアリングを行い、満足しているところや改善してほしいところを調査する。この際、業務内容によって意見が異なる可能性があるため一つの部署だけではなく、さまざまな部署から意見を吸い上げることが重要となる。

- **IT 環境の運用効率化観点**

  運用効率化の観点は、関係する部署と共に、負荷が大きい業務や対応が難しい業務を洗い出し、どのような運用が理想的か検討を行う。運用を効率化させることで、DX のような組織を発展させるための施策に人材を活用できるため、重要な観点である。

As-is 分析を行った結果、出てきた課題の例を表 2-1 に示す。可視化された課題をもとに、ありたい姿を検討する。

表 2-1　As-is 分析から抽出された課題例

観点	課題
セキュリティ	• さまざまなシステム・サービスで個別に ID 管理を行なっており、不要なユーザーの削除など、適切な管理を実施できていないものが存在する。 • システム・サービスにアクセスする際の認証強度が弱い。 • 組織内のデバイスを統制できておらず、必要なセキュリティ設定が管理すべき全ての端末に行き届いていない。 • 無断で SaaS サービスの利用を行う社員がいる(シャドーIT)。組織で管理すべきシステムを全て把握できていないため、セキュリティ対策を打てていないものがある。 • 正規のユーザーであれば、機密ファイルの持ち出しが簡単にできてしまう。 • 境界防御の中のセキュリティ対策が十分でなく、一度境界内部に侵入されると簡単にラテラルムーブメントされてしまう。
ユーザー利便性	• あらゆるサービスを利用する際にパスワードの入力を求められる。入力の手間がかかるのはもちろん、複数のパスワードを覚え、管理するのが面倒である。 • セキュアなテレワーク環境が整っていないため、働く場所が制限されてしまう。
運用効率化	• SaaS 利用も少しずつ増えてきているが、それぞれのサービスで ID 管理を行なっており、運用の負荷が大きい。 • ユーザーがパスワードを忘れた際のパスワードリセットの作業などで多くの工数を割いている。 • デバイスのキッティング作業やセキュリティ設定の配布に多くの工数を割いている。

また、ゼロトラストと親和性が高いありたい姿の項目を表 2-2 にまとめた。

表 2-2　ゼロトラストと親和性が高いありたい姿の例

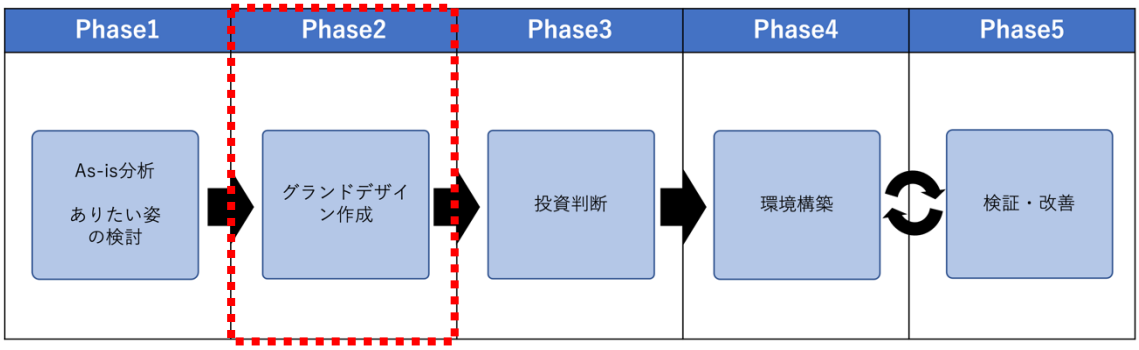
観点	ゼロトラストと親和性が高い内容
セキュリティ	・システムにアクセスする際の認証・認可の強度を上げたい ・業務に利用するデバイスを統制できる環境を整えたい ・各システム・サービスの ID 管理を一元的に行いたい ・シャドーIT (無断 SaaS 利用など)をなくしたい ・セキュアにリモートアクセスできる環境を整備したい ・ローカルブレイクアウト時のセキュリティ対策を行いたい ・内部犯行による情報漏洩対策を行いたい
ユーザー利便性	・いつでもどこでも安全、快適に働ける環境の整備を行いたい ・パスワードレス化によりユーザー負担の軽減を図りたい ・クラウドサービスを積極的に活用したい
運用効率化	・デバイスのキッティング作業やパッチ適応作業を効率化したい ・システムのパスワード管理の負担を軽減したい ・システムごとの ID 管理による負担を軽減したい

組織の課題を洗い出した上でありたい姿を検討した結果、表 2-2 に記載のある内容のような IT 環境を目指す組織(表 2-1 のような課題を抱えている組織)は、ゼロトラストの概念を適用することが有効である。

★ポイント

As-is 分析を行わず、目先の課題からありたい姿を検討してグランドデザインを作成した場合、潜在的な課題に気づけない可能性がある。そのため As-is 分析と併せてありたい姿を検討することが重要である。

2.2.2.グランドデザイン作成　(Phase2)



この章では、Phase1 で描いたありたい姿を実現するために必要なソリューションは何か検討し、将来的に目指すべき構成(To-be 構成)を明らかにするために必要なグランドデザインの作成について説明する。

これを行うことで具体的にどのような対応が必要になるのか明確化するとともに、投資判断に必要な観点についても整理ができる。

◆ **グランドデザインの作成**

グランドデザインの作成に必要な取り組みは、以下の通り。

① As-is 構成に対し、To-be 構成、Can-be 構成を描く
② To-be 構成の各ソリューションと As-is 分析で見えた課題の対応関係をマッピングする
③ ロードマップを作成する

この取り組みを行うことで、組織の目指す姿の可視化や必要なコストなどが具体化できる。それぞれの観点について以下で説明する。

① As-is 構成に対し、To-be 構成、Can-be 構成を描く
それぞれの構成に関する説明は以下の通りである。

As-is 構成	：現状の構成
To-be 構成	：ありたい姿を実現するために必要な構成
Can-be 構成	：一足飛びに To-be 構成に行くのは難しい場合の中間地点

To-be 構成を検討するにあたり、ありたい姿から具体的なソリューションに落とし込みを行う必要がある。
例えば表 2-2 に示した、「システムにアクセスする際の認証・認可の強度を上げたい」に対しては、IDaaS 製品を導入し、すべてのシステムへアクセスする際に必ず通信を経由させることで、多要素認証を強制出来る。また、MDM や EDR と連携することで管理下にあるデバイスか、危険な状態にないかをチェックして認証・認可を行うことも有効である。
このように、他のありたい姿の項目についても具体的なソリューションの落とし込みをイメージする。そうすることで To-be 構成に必要なソリューションを洗い出すことが出来る。
その後は、各ソリューションを製品レベルに落とし込む必要がある。各ソリューションはさまざまなベンダーから提供されているため、自社の環境に適合するか、他のソリューションと連携しやすいかなども考慮した上で製品を選定する。また複数のソリューションを一つにまとめた製品もあるので、機能についてはよく確認することも重要である。

上記のような考え方で作成した To-be 構成のイメージを図 2-2 に示す。

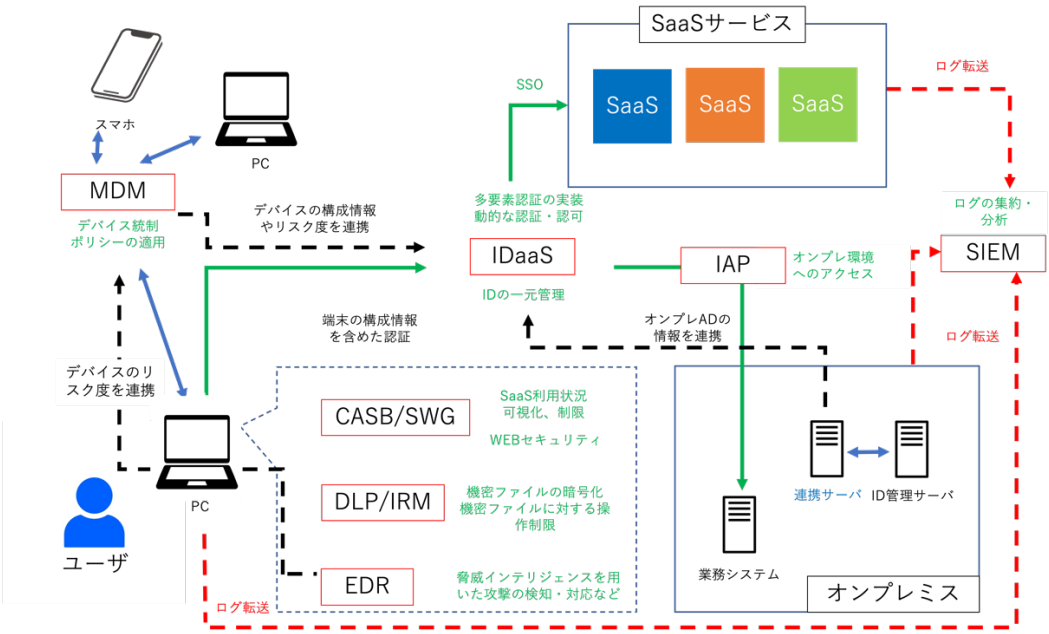


図 2-2　To-be 構成のイメージ(例)

また、As-is 構成から一足飛びに To-be 構成にいけない場合は、中間地点として Can-be 構成を考える。まずはその環境を目標として進め、最終的に To-be 構成を実現するのが良い。

② To-be 構成の各ソリューションと As-is 分析で見えた課題の対応関係をマッピングする

図 2-2 の To-be 構成で示した図の中に緑文字で記載したものがそれにあたる。各ソリューションで解決できる課題を整理することで、組織が思い描いたありたい姿をもれなく実現できているか、各ソリューションがゼロトラスト構成の中でどのような役割を果たしているか確認することができる。

③ ロードマップを作成する

To-be 構成に向けて環境を移行していくにあたり、ロードマップを作成し、計画的に実装を進めていくことは非常に重要である。
ロードマップを作成するにあたり、ゼロトラスト構成の実装順序について説明する。

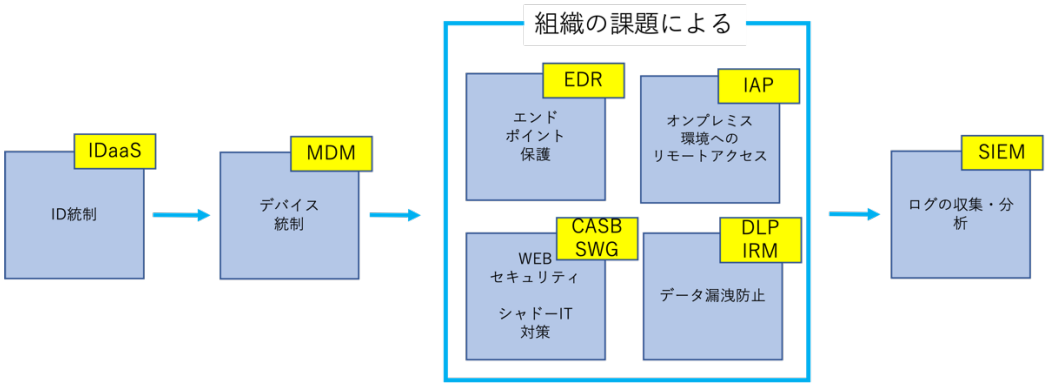


図 2-3　ゼロトラストソリューションの実装順序

ゼロトラスト構成を支えるソリューションは多くあるが、図 2-3 のような順序で実装していくことを提案する。ゼロトラスト構成への以降は、まずは ID 統制から始めるべきである。ID 統制はゼロトラストの概念の中でも中核を担う要素であり、認証・認可を行う上でユーザーの識別は非常に重要なポイントである。また後にユーザーとデバイスの紐付けやユーザーとコンテンツの紐付けを行うための基盤作りとして必要なことから、ゼロトラスト構築の初めに取り掛かるべき内容である。ここで ID 基盤をきれいな状態にしておかなければ、その後のソリューション展開を行った際に不適切な通信を認証・認可してしまう可能性がある。

次に取り掛かるべき課題は、デバイス統制である。デバイス統制は組織が守るべきデバイスを洗い出し、組織の管理下に置くことである。その結果セ

キュリティパッチの適用や、アプリケーションの配布などを一括で実施することが出来る。この課題対応を早めに済ませておく必要があるのは、ゼロトラスト構成に移行するためのデバイスに必要なソリューション(例えば EDR など)の展開や、その確認が一元的に行えるためである。仮にこの部分が不十分な状態でソリューションを展開すると、デバイス対策に漏れが生じる事がある。その結果、漏れたデバイスがセキュリティホールとなり、攻撃者に悪用されるおそれがある。また、デバイス統制を行うことで、IDaaS と連携して組織の管理下にあるデバイスからのみアクセスを可能にするといった制御も実現できる。

ここまで、ID 統制・デバイス統制の優先度が高いという説明を行ったが、残りのエンドポイント保護やシャドーIT 対策などの課題の優先順位は組織の中で重要度や影響範囲などの観点で優先順位をつけて進めるべきである。一方で、ログ分析基盤の構築や対応の部分の優先度を下げているのは、まずは防御の観点で必要なセキュリティ対策の基盤を構築してから、環境の監視を行うべきと考えたためである。

図 2-3 ではウォーターフォール的な流れで図示したが、実際には ID 統制を行いつつ、デバイス統制を行うなど、並行して作業することも可能である。

このような考え方をもとに作成した仮想のロードマップを図 2-4 に示す。

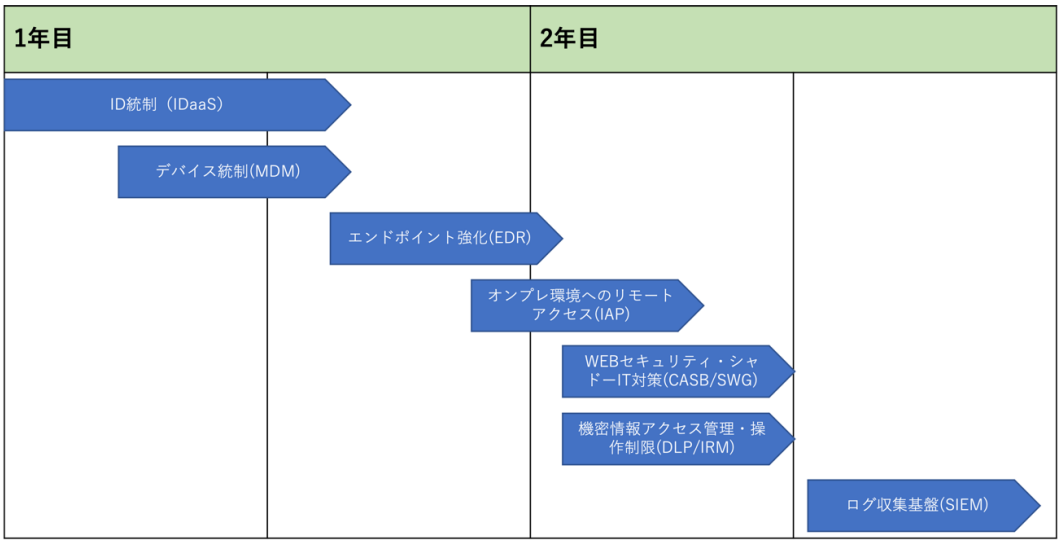


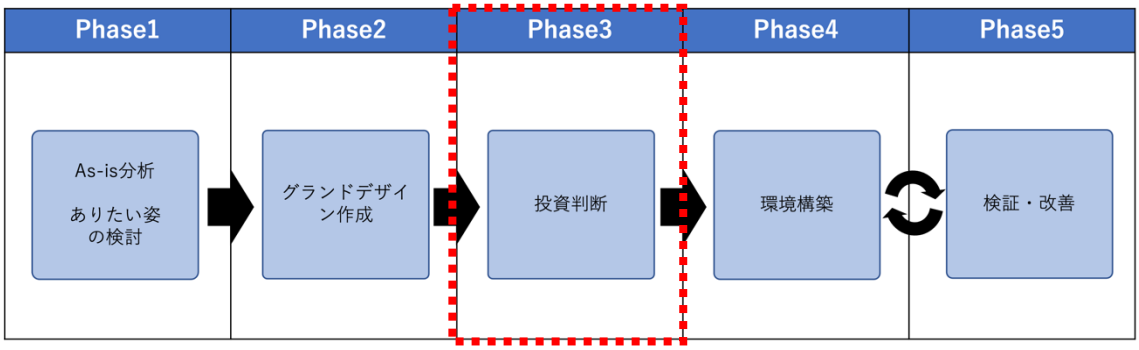
図 2-4　ゼロトラスト移行のロードマップの例

このとき、「新たに発生するコスト」「不要になるコスト」「得られる効果」の発現時期についても整理しておく。図 2-4 の IDaaS を例にとって考えると、1

年目から IDaaS のライセンス利用料が発生し、その約半年後には効果として ID の一元管理によるセキュリティレベルの向上と運用効率向上、SSO によるユーザー利便性向上といった効果が見込まれる。このような情報を整理し、可視化することがステークホルダへの説明の際に重要である。また、図 2-4 では 2 年でゼロトラスト構成へ移行するロードマップを描いた。ゼロトラストはセキュリティの最新技術を動員して守りを固めるため、導入と改善のスピード感（アジリティ）が重要である。

※不要になるコストとは、ゼロトラスト環境構築のために購入した製品に、既存で使用している製品の機能が含まれている場合に発生する削減可能なライセンス料などを想定している。例えば、「IAP を用いて社外から社内アプリケーションへアクセス可能になるため、既存の VPN 関連の費用が不要になる」といったものである。

2.2.3.投資判断　(Phase3)



この章では、ゼロトラスト構成へ移行するために必要な投資判断の重要なポイントについて解説を行う。

◆ 投資効果に関するポイント

ゼロトラスト構成に移行することで、既存の環境よりもセキュリティレベルは向上する。しかしゼロトラスト投資の承認を得るため、経営者に向けて「この対策を行わなかった場合、このような被害が出る可能性がある」といったホラーストーリーで説明することはおすすめしない。なぜなら、どの程度の確率でどの程度の被害が発生するのかも不確実でわかりにくく、理解されない場合があるからである。ゼロトラストの概念は前述した通りセキュリティ戦略も含めた IT 戦略として捉えるべきものと考える。そのため、投資の承認を得る際には「どのようなリスクに対応可能になるか」といったセキュリティ観点の効果と合わせて、「ユーザーの利便性向上」や「運用の効率化」などを総合的に盛り込んで説明を行うことが重要である。

以下にそれぞれの観点での投資効果の例を示す。

➢ セキュリティレベル向上観点

- ランサムウェアなどに代表される標的型攻撃への対策
- 動的な認証・認可を実装することによる、不正アクセスリスクの低減
- シャドーIT 撲滅による適切な資産管理とセキュリティ対策
- セキュアなリモートアクセス手法の確立
- 内部不正による情報漏洩対策

など

- ユーザー利便性向上観点
    - テレワークセキュリティのレベルが向上することで、社員がいつでもどこからでも安全に働くことのできる環境を提供
    - SSO の仕組みを導入することでユーザーが各システムに対して ID・パスワードの入力や管理の負担軽減

    など

- 運用効率化観点
    - MDM の導入によるデバイスのキッティング作業の効率化
    - IDaaS で一元的に ID 管理を行うことによる、個別 SaaS 単位での ID 管理の負担軽減
    - SSO の仕組みを導入することによる、個別システムでのパスワード管理業務の負担軽減

    など

- その他の観点

    昨今、サプライチェーンのセキュリティが課題である。ゼロトラスト構成でセキュリティレベルを引き上げることで協業先として認められ、新しいビジネスチャンスが得られる可能性もある。

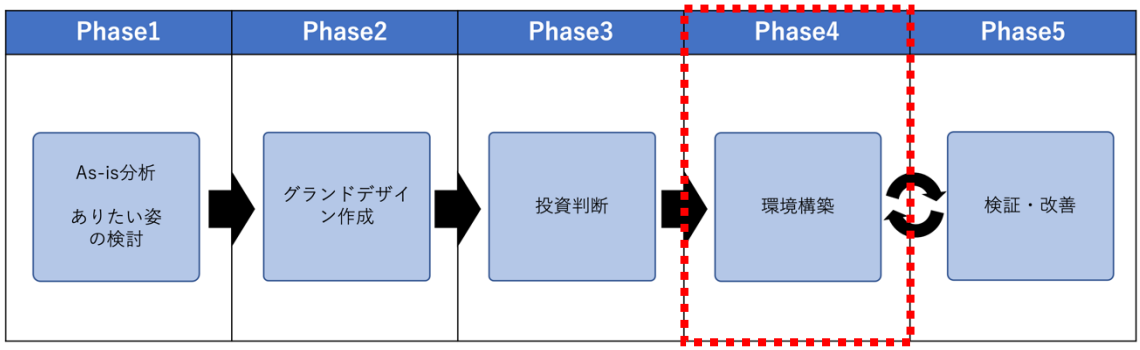
また、経営者には、いつ、どの程度の出費が発生するのか、いつ、どのような効果が得られるのかという情報を示すべきである。Phase2 のグランドデザインで作成したロードマップに従いその部分を丁寧に説明する。

参考：IT コストの抑制観点について

コスト観点については、基本的に既存環境で行えていなかったセキュリティ対策を行うことになるのでコストは増になる。一方でゼロトラスト構成を目指すにあたり購入したライセンスが、既存環境で使用している機能を包含している場合は、その部分を置き換えることにより不要となるライセンスが発生する可能性もある。このようなライセンスの置き換えや集約が発生することにより、コストメリットが生じる組織もある。この部分は既存の IT 環境に依存するため、「ゼロトラスト構成に移行すれば絶対にコストメリットが生じる」とは考えない方が良い。

2.2.4.環境構築　（Phase4）

この章では、ゼロトラスト構成の代表的なソリューションの環境構築を行う際の流れやポイントを解説する。



◆ ID 統制（IDaaS）

実装時のポイント

- 信頼できる ID ソースの確認
  信頼できる ID ソースとは社員に一意の ID が割り振られ、退職者の ID 削除など運用が適切に行われている ID ソースである。もし信頼できる ID ソースが存在しない場合は、まずその基盤を作るところから始める必要がある。

- 共有 ID の緩和措置検討
  共有 ID の利用は責任の所在が曖昧になること、管理が困難になることという問題が生じる。その結果、離任者や退職者からアクセスを許すリスクが生じる。このリスクを低減するために、可能な限り共有 ID の使用は廃止する。どうしても廃止できない部分については、パスワード管理ツールを導入し、パスワードを隠蔽しつつツールを介してシステムにアクセスさせるなど、緩和策を検討する。

- IDaaS と信頼できる ID ソース連携
  IDaaS へ ID 情報を連携する。主な IDaaS 製品では Active Directory などの ID 管理システムから繋ぎ込みを行うための機構を準備していることが多いが、製品依存の部分があるので、事前に確認が必要である。

- SaaS サービスへの SSO の設定
  IDaaS の主な機能に SSO がある。SSO の機能を有効に活用することで、ユーザーの利便性向上、システム運用者のパスワード管理の負荷軽減が見込まれる。 一方、SaaS サービスが必ずしも SSO に対応しているとは限らない点に注意が必要である。そのため、SaaS サービスを選定する際は、SSO に対応しているかを意識して選定することをおすすめする。

- SaaS サービスへの ID プロビジョニング
  ID プロビジョニングとは、IDaaS が持っている ID 情報を、各 SaaS サービスに連携する機能である。従来は個別に ID 管理を実施していたが、ID プロビジョニングにより各 SaaS サービスの ID も一元管理できるようになった。結果として、ID の管理工数削減が期待できる。
  一方、認可設計は各 SaaS サービス側で行う必要があるため注意が必要である。

- アクセスポリシーの検討
  IDaaS は柔軟な認証・認可の設計ができる。具体的には、ユーザーが普段とは違う NW からアクセスしてきた場合に追加認証を行うことや、アクセス元の端末に必要なセキュリティパッチが適用されていない場合にアクセスを遮断するなどが挙げられる。細かなルールでアクセス管理を行うことによりセキュリティレベルの向上が図れる一方、フォールスポジティブによる業務影響も考えられるため、PoC の段階や運用していく中で組織にあったポリシーを見つける必要がある。

◆ デバイス統制 （MDM）

実装時のポイント

- 管理すべき端末の洗い出し
  この作業が MDM 導入において最も重要な部分である。適切にデバイスの洗い出しができなかった場合、MDM 製品を導入したとしても管理外のデバイスのセキュリティレベルは低い状態を維持してしまう。洗い出しができたら MDM 製品を導入し、普段デバイスのキッティング作業で行なっている設定や、セキュリティパッチの適用、アプリケーションの配布などを MDM を通して適用する。

- 機能の利用制限
  アプリケーションのインストール/アンインストールの制限や、Bluetooth 機器への接続、外部記憶媒体の接続など、業務上不必要な機能から攻撃される可能性を低減する。業務を行うにあたり必要な機能を見極めて設定することと、組織にあった設定を運用の中でチューニングする必要がある。

- コンプライアンスポリシーの設定
  デバイスの状態を自動で収集し、組織が定めたコンプライアンスに準拠しているか確認することができる。ディスクの暗号化が有効になっているか、ウィルス対策ソフトが有効になっているか、指定したバージョン以上の OS を利用しているかなど、様々な観点でデバイスのチェックを行うことができる。まずは組織としてデバイスがどのような状態であることが望ましいか検討する必要がある。

- IDaaS との連携
  MDM で統制されているデバイス、組織が定めたコンプライアンスポリシーを満たしているデバイスのみアクセスを許可するという制御を IDaaS と連携することで実施できる。

◆ WEB セキュリティ・シャドーIT 対策(CASB・SWG)

実装時のポイント

- 悪性コンテンツへのアクセス制限
  オンプレミスの境界型防御内でセキュリティ機構が行なっている制御を確認し、SWG 製品へそのポリシーの落とし込みを行う。アダルトコンテンツといったカテゴリによるフィルタリングや不審なドメインへの接続制限などの設定を行う。

- SaaS サービスの利用状況可視化
  CASB の機能により、組織が利用している SaaS サービスの可視化を行うことができる。これにより、これまでシャドーIT として利用されていたサービスについて統制を行うことが可能となる。また CASB には SaaS サービスのセキュリティレベルを評価する機能も含まれているものもあり、組織で利用している SaaS サービスにセキュリティリスクの高いものはないか確認することができる。様々な部署で同じような機能を有する SaaS サービスを利用していないか確認したのちに一つのサービスに統合するなど、コスト最適化の観点でも有益な情報を得ることができる。

- 利用を許可している SaaS サービス以外へのアクセス制限
  前段で SaaS サービスの可視化を行った上で、組織として利用を許可する SaaS サービスの検討を行い、利用を認めないものについては制限を行う。この際、突然機能を制限すると業務影響が出る可能性が高いため、代替となる SaaS サービスの提案を行い、代替 SaaS サービスへの業務切り替えを確認した上でアクセスを制限する必要がある。利用部門とのコミュニケーションが必須となる作業である。

- テナント識別設定
  同じ SaaS サービスであっても、組織で契約しているテナントと、個人で契約しているテナントが存在する場合がある。このような場合に、業務で使用する場合には組織で契約しているテナントにのみアクセス可能とすることができる。この設定により業務データを個人で契約している SaaS サービスへの不正なアップロードを制御することが出来る。

◆ データ漏洩防止(DLP/IRM)

実装時のポイント

- 組織における機密情報の定義
  まずは、組織において制御すべき機密情報を定義することが重要である。機密情報を明確にすることで、検知ルールの作成や必要となる制御を検討することが出来る。また、その機密データの格納場所や管理方法を把握することも重要である。

- 検知ルールの策定
  DLP や IRM で機密ファイルを検知する手法として、手動でファイルにラベリングを行う手法やファイル中のキーワードを元に検知する手法がある。手動によるラベリング設定は簡単であることがメリットである。一方、人間が機密度を判断するため、セキュリティに関するリテラシが求められることや、ファイルごとにラベリングを行うため運用負荷が大きいといったデメリットがある。そのため、例えばファイル中の「機密」のようなキーワードや、マイナンバーだと考えられる数字列が見つかった場合に機密情報と自動で判断して制御する手法が推奨されている。この際、組織における機密情報の定義を元に関連するキーワードを検知ルールに組み込む作業が必要となる。

- 制御内容の検討
  機密ファイルに対し、機密情報が管理されるべき場所や、機密情報のレベルに応じたアクセス可能なユーザーなどを定義した上で必要な制限の設定を行う。DLP では機密情報が管理されるべき場所からのダウンロード、管理されるべきでない場所へのアップロード、メール転送、外部記憶媒体へのコピーなどを禁止することができる。IRM では機密情報にアクセス可能なユーザーとその権限(編集や印刷など)を制御することができる。

- モニターと改善
  運用していく中で、機密情報の制御に関してフォールスポジティブやフォールスネガティブが発生した場合、検知ルールのチューニングを行う必要がある。また、禁止操作の発生ログを確認することで情報漏洩が起こりやすい場所の把握もすることが出来る。その情報を元に、ユーザーに教育を徹底することも重要である。

◆ エンドポイント保護(EDR)

導入のポイント

- 脅威インテリジェンスを活用した検知が有効
  日々高度化・複雑化するサイバー攻撃に対応するためには最新の脅威インテリジェンスに基づいて検知・対応を行う機能が有効である。脅威インテリジェンスを活用可能な製品を選定することをおすすめする。

- チューニング
  どのような挙動を検知しアラートを上げるのか、組織で必要なポリシーを定め、運用の中で改善する。これを行わなければフォールスポジティブよるユーザーへの業務影響や、運用部門の負担増が発生する可能性がある。過検知が発生した際には、業務に必要なシステムのホワイトリスト登録といったポリシーチューニングが求められる。

- アラート対応
  EDR は導入したのちに、検知されたアラートに適切に対応することで真価を発揮する。アラート対応について、内製・外注といった選択肢がある。どちらを選択するかは組織の判断に委ねられるが、「自組織にアラート検知にあたる人的リソースの確保ができるか」「(人的リソースが確保される前提で)アラート対応できる技術力を持った人材が自組織にいるか」が主な判断基準となる。技術力に不安のある組織は、試験運用中にアラート対応を自組織で行い、対応の難しい部分のみ SOC 事業者へ外注する選択肢もある。その際、外注先と協調してアラート対応を行い、人材を育てることで最終的にはアラート対応を内製で行う方針を立てる事もできる。

- IDaaS 連携
  EDR の監視機能により、リスクレベルが高いと判断されたデバイスからのアクセスを禁止することができる。これを実現するために、IDaaS と EDR を連携させる。

◆ オンプレミス環境へのリモートアクセス(IAP)

導入のポイント

- 接続対象システムの確認
  IAP の導入は、接続対象のシステムを洗い出すところから始める。 IAP は WEB アプリケーションへの通信を前提としたサービスである。WEB アプリケーション以外のレガシーアプリケーションなどに IAP を経由したアクセスを導入したい場合は、クライアントにエージェントをインストールすることでアクセス可能となる製品もある。組織のニーズに応じた製品選定を行う。

- コネクターの配置
  IAP を利用したリモートアクセスを実行するには、接続したいシステムと疎通可能な場所にコネクタを配置する必要がある。コネクタは複数システムで併用出来るが、コネクタの負担が増えるとスループットや可用性に影響を与える可能性がある。そのため、高スループット、高可用性が求められるサービスに関しては専用のコネクタを用いることで対応することも出来る。

◆ ログの収集・分析(SIEM)

導入時のポイント

- ログ分析を行う目的の明確化
  SIEM 導入にあたり、目的を明確化することが重要である。目的が定まっていないと、どの機器からどのログを SIEM に転送するか検討することが出来ない。「とりあえず全てのログを取り込む」という考え方ではストレージの容量圧迫やネットワーク帯域の逼迫を引き起こしてしまうため注意が必要である。

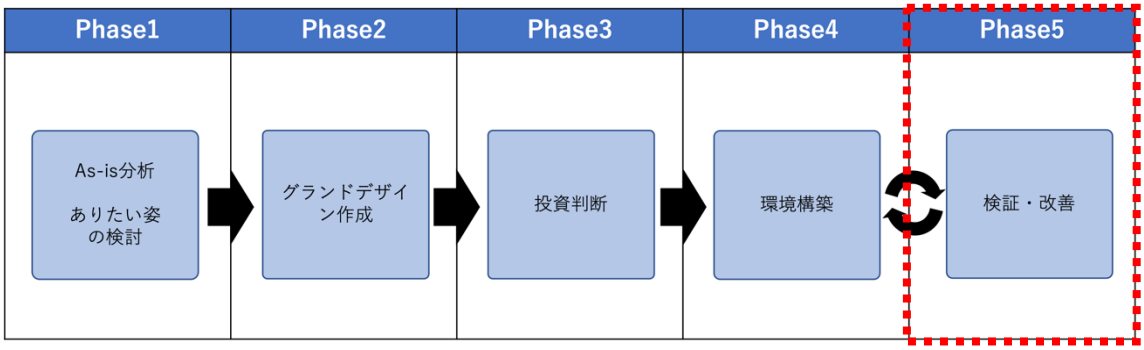
- ログの保存期間
  法令遵守やストレージの有効活用のために、ログの保存期間を決める必要がある。規制や法令によって保存期間が定められているものもあるため、組織の所有するデータに該当するものがないか確認を行うべきである。また取得するログの種類と、保存期間から必要なストレージの容量を見積もるといった観点でも重要である。

- 検知ルールの検討、作成
  SIEM を導入する目的にあった検知ルールを検討する。この時、あまりにも多くのアラートが上がるような設定にしてしまうと運用部門のアラート対応が追いつかなくなり、重要なアラートを見落としてしまう恐れがある。必要なアラートを見極めた上で、組織にあったチューニングを行うことが重要である。

- 運用体制の検討
  SIEM は導入後のアラート対応や、検知ルールのチューニングを日々行う必要があるため、事前に必要な体制を整えておく必要がある。アラート対応を内製化するか外注するかの判断は EDR と同様である。

★環境構築の際のポイント
ゼロトラストのソリューションに限った話ではないが、試験運用を行わずに全社展開すると、業務影響があった際に組織運営に大きな影響を与える可能性がある。そのため、まずは IT 部門で最低限の機能確認や動作確認を行った後に、各部門からパイロットユーザーを募って試験運用を行うことが望ましい。幅広い部門からパイロットユーザーを募ることで、さまざまな業務に対する影響を確認出来る。

2.2.5.検証・改善（Phase5）



ゼロトラスト環境は、構築して終わりではない。IDaaS のアクセスポリシーや、EDR、SIEM の脅威検知ルールなど、あらゆるソリューションで運用の中でのチューニングが必要である。その際、セキュリティ強度を求めすぎた結果、ユーザー利便性の低下に繋がってはいけない。セキュリティ強度とユーザー利便性のバランスの取れたゼロトラスト環境を維持するためには、日々ユーザーの声に耳を傾ける必要がある。

また、サイバー攻撃の手法は日々巧妙化するため、組織のセキュリティ対策も日々改善が必要である。ゼロトラストは概念でありこれといった正解の構成は存在しない。そのため一度構築したゼロトラスト環境を「正解」と捉えることなく、外部環境の変化に伴う新たなリスクに対応するために、最新の防御手法をキャッチアップし、構成を柔軟に改善していくマインドが組織に必要である。改善の手法は、MITRE ATT&CK Evaluations 等を活用した机上でのリスク分析や、ペネトレーションテストによる脆弱性の把握など様々存在する。このような取り組みによって顕在化したリスクを評価し、優先順位をつけて着実に対応することが組織に求められる。「これでセキュリティ対策は完璧」という構成はこれからも存在しない。

加えて、システムユーザーへのセキュリティ教育も引き続き実施する必要がある。組織の IT 環境をゼロトラスト構成にすることにより、不審な通信やマルウェアの検知率が上がると考えられる。一方で、ゼロトラスト構成にしたからといって全ての攻撃を防ぐことは出来ない。そのため、従来通りの「不審なメールは開かない」「不審な WEB サイトにアクセスしない」といった基本的なセキュリティ教育を徹底することはもちろん、リモートワークなど、新たなリスクについてもユーザーに教育を行い、組織全体でセキュリティ意識を向上させる取り組みが引き続き重要である。

2.3.プロジェクトの推進体制

ここまで、組織の IT 環境をゼロトラスト構成に移行する際に必要な検討や重要なポイントについて解説してきた。本節では、プロジェクトを推進するための体制や、必要な協力関係について解説する。

ゼロトラスト構成への移行は、セキュリティ・IT 部署のみで検討する内容ではない

第 2.1 章で説明した通り、ゼロトラスト構成への移行検討は経営者をはじめ、さまざまな部署と協調して推進することで、高い効果を得ることができる。以下に具体的な内容を示す。

- 経営者
  経営者は、プロジェクトを推進する上で最も重要なステークホルダーである。経営者がゼロトラスト構成への移行の必要性を理解することで、ヒト・モノ・カネのリソースが割り当てられる。また、経営者がトップダウンで施策を推進している企業ほど円滑にプロジェクトが進みやすい。

- 法務部門
  ゼロトラストを推進する上で、従業員のデバイス上でどのような行動をしているか、(例えばどのような WEB サイトを閲覧しているかなど)リアルタイムで監視する必要がある。これは、個人情報保護法で守られるべき内容であるため、監視を行う場合は目的と取り扱う個人情報を明記して社内規定に定め、従業員に明示する必要性がある。このような施策に伴う法的観点のフォロー目的で参画してもらう。

- 人事部門
  組織の ID 管理を適切に行う上で、人事情報との連携は必要不可欠である。人事異動や退職のようなイベントが発生した際に、ID を適切に保つための手法を人事部とすり合わせておく必要がある。

- 経理部門
  ゼロトラスト構成に移行するにあたり、組織の資産を適切に把握する必要がある。シャドーIT の利用など、IT 部門で管理できていないシステム・デバイスは経理部門が管轄する支払い履歴から確認できる。これにより守るべき資産の特定ができる。もし組織内の違う部署で同じようなサービスを別々に利用している場合、それらを統一することで守るべき資産のシンプル化やコストの効率化を実現出来る。

- 事業部門(ユーザー部門)
  ユーザーとなる事業部門は、既存の IT 環境だけでなく、ゼロトラスト構成へ移行した後の環境のフィードバックも得られる重要なステークホルダーである。ユーザー部門と密にコミュニケーションを図りながら、組織全体が快適に業務できる環境を実装し、改善を重ねていく。

上記のような部署と協調し、社員が安全・快適に働くことができる環境を作り上げていく。ゼロトラストに限らず、セキュリティ対策はビジネスを促進するために必要な取り組みであることを理解し一体となって取り組むことが重要である。

第3章：まとめ

本書では、ゼロトラストの概念を自組織に採用する際に必要な取り組みについて、検討から実装、運用に至るまでの流れと重要なポイントについて解説を行った。

ゼロトラストは概念であり、これといった具体的な正解が存在するものではない。そのため自組織の課題を洗い出し、その結果を元に将来的にどうありたいかを明確化することが重要である。「ゼロトラスト構成に移行すること」は目的ではなく手段であることを担当者は理解しなければならない。

また、ゼロトラスト構成への移行は、ユーザーの利便性や運用の効率化といった観点も考慮した上で、組織の IT 戦略として検討されるべきである。そのため、セキュリティ部署・IT 部門だけではなく、経営者を初め関係する様々な部署と協力してプロジェクトを推進することが求められる。特に経営者はプロジェクトをトップダウンで推進するための重要なステークホルダーである。

ゼロトラストは「全てを信用しない」概念というよりは「全てを確認した上で認証・認可を行う」概念である。そのため、認証・認可を適切に行うための基盤となる ID 統制、デバイス統制が優先的に取り組むべき課題である。

本書で示したゼロトラスト構成への移行の流れは、様々な企業・個人へのヒアリングをもとに作成したが、あくまでプロジェクトメンバーで考察した結果であり、ヒアリングに協力いただいた企業・個人の主張とは異なる点がある。そのため本書の内容が唯一無二の正解だとは考えていない。しかし、ゼロトラスト構成への移行を検討しているが何から始めて良いか分からない組織の担当者が参考にできる内容は本書に詰め込むことが出来たと考えている。

なお、本書は 2022 年 6 月時点での考えをもとに執筆したものであり、二年後にも本書の内容がそのまま通用するとは考え難い。ゼロトラストは現有技術を総動員した概念であるという点をふまえ、最新の情報や技術を常にアップデートし続ける必要がある。

本書が、自組織の IT 環境改善の助けになれば幸いである。

謝辞

本書の作成にあたりまして、SCSK 株式会社様、NRI セキュアテクノロジーズ株式会社様、NTT コミュニケーションズ株式会社様、株式会社アイシン様、株式会社竹中工務店様、株式会社ラック様、三菱ケミカル株式会社様、三菱ケミカルシステム株式会社様、また個人として吉田浩和様（５０音順）、他にもご協力いただいた組織の皆様にゼロトラスト移行の進め方についてヒアリングさせていただくなど、多大なるご支援・ご尽力を賜りました。お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる、満永拓邦先生、門林雄基先生には、本書の元となるゼロトラストプロジェクトのメンター・講師として、ご指導・ご助言とともに、各検証機材のご支援を賜り続けてきました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトをともに実施した、下記メンバーの皆様にも感謝を伝えたいと思います。

<ゼロトラストプロジェクトメンバー>

【リーダー】
鳥羽瀬　世宇

【メンバー】

内野　隆志　　駒居　智之　　田所　直樹　　前川　和輝