FUJITSU

今までのシステムを ゼロトラストへ 移行するための手法とは

～ゼロトラスト導入で 実現すべき 5 つの領域～

目次

1. なぜ、ゼロトラストを実施していかなければならないのか

それは、セキュリティの向上もありますが、昨今においては企業にとっての様々なメリットが考えられます。その根本的な理由は、セキュアで利便性を高める環境を実現することにより、事業変革へと繋げていくことにあると考えます。

さらに、「ゼロトラストを実現するためにはどこから始めれば良いのか分からない」というお客様も多く、先ずは対策領域を 5 つに分けて整理していくことをお薦めします。

1.1 この混沌とした時代において企業に必要なこと

時代が大きく変わっている今、多様な考え方を持った人が繋がる環境を創り、そこからお客様にどのような価値を提供することができるのかを考えていく必要があり、そうしたことが業務の変革に繋がる、と考えます。

このような業務変革によって業務のやり方をデジタルベースに変革し、そうした環境から生み出されるイノベーティブな考え方から自らの商品価値を再定義することが必要であり、そして、こうした考え方を基にした取り組みが、圧倒的な事業変革のスピード向上に繋がるものと考えています。(図 1)

しかしながら、これまでのセキュリティは安全地帯を作り、外部の脅威から守るという考え方が主流であるため、こうしたことを従来のシステムのまま実現することはなかなか難しいところです。このような従来の概念から解放され、必要な時に、必要な人が、必要なリソースへ、アクセスする際に都度の認証を行うことによってそれぞれ問題がないか安全性を確保すること、それが「ゼロトラスト」の概念になります。(図 2)

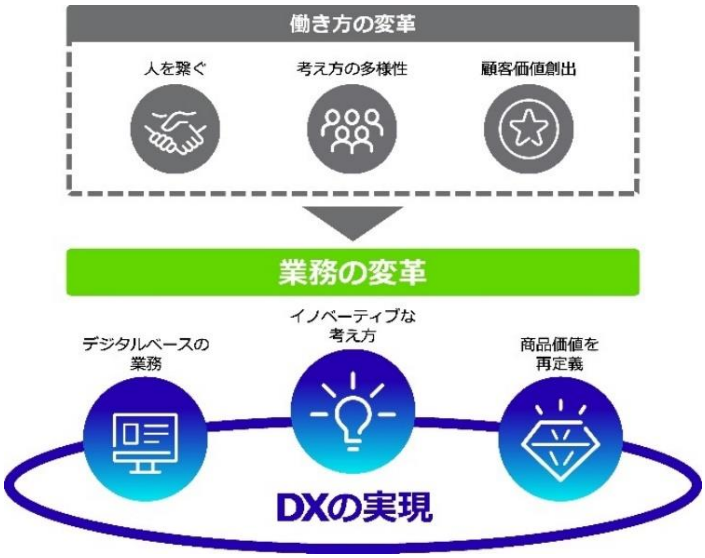


図 1：業務変革が導く DX の実現

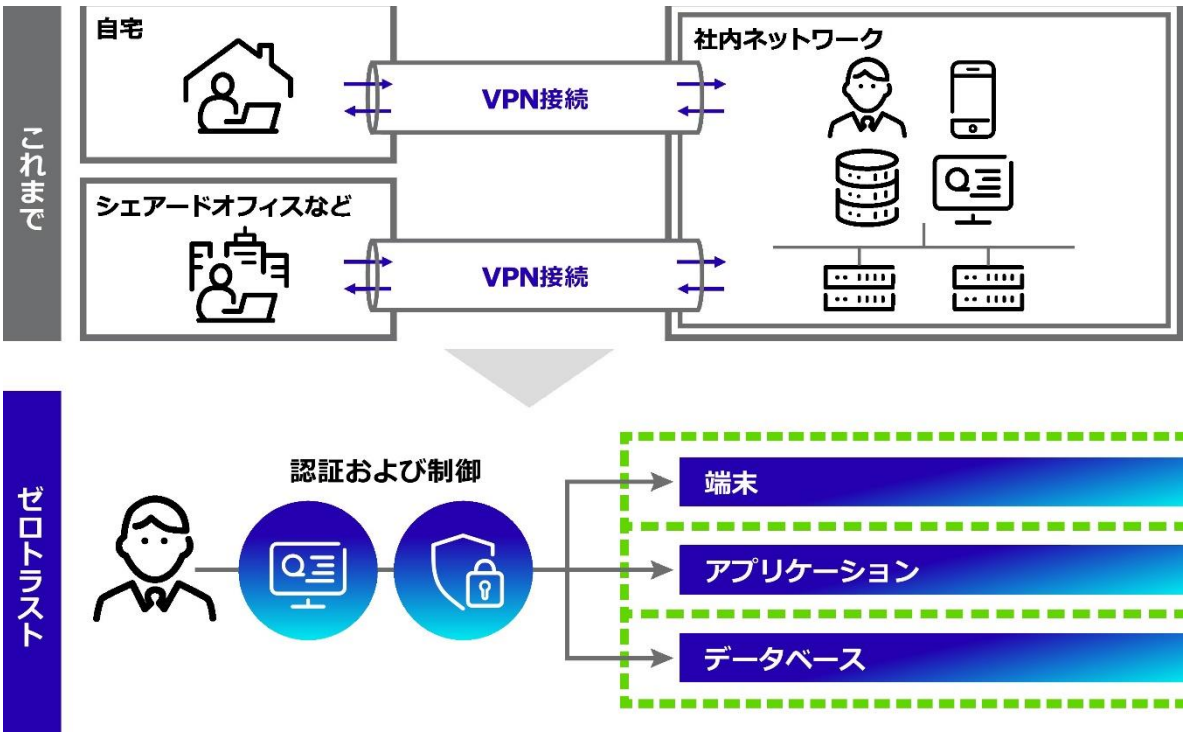


図 2：これまでのシステムからゼロトラストへの変化

1.2 これまでのシステムの問題※1

これを昨今のシステムの変化に落として考えてみましょう。まず、十数年前のシステムは、社内のみで守るということが常識でした。それが、クラウドを企業も積極的に利用する時代となって、様々なデータがクラウド上、つまり社内の境界の外に移行しました。さらに、コロナ禍もありテレワークの台頭によって、従業員も外に出ることになったため、データと従業員の両方が境界の外に出ることになりました。結果、一度社内を通って社外に出るといった VPN 通信において、帯域ひっ迫という通信経路上の遅延が発生することになりました。こうしたことによって新たな通信経路が必要になり、それが SASE(Secure Access Service Edge)などの概念によって実現してきていると言っていいでしょう。

ゼロトラストなどの技術を使った目指すべき姿としては、どこからでも同様に繋がる環境によって、場所に因らない働き方を作ること、しかも今までよりもセキュアに作り上げることです。このような意味で、ゼロトラストはオープンかつセキュアなシステムの構築を目指した概念でもあります。

こうした環境を整えることによって、働き方を変え、DX を実現し、事業を変革していけるのではないでしょうか。

※1 参考：NIST Special Publication 800-207 Zero Trust Architecture, NIST, https://csrc.nist.gov/publications/detail/sp/800-207/final, 2020 年 12 月

2. ゼロトラストを実現するための 5 つの領域

米国国立標準技術研究所が公開しているセキュリティに関するガイドライン NIST SP800 の定義から、ゼロトラストとは何であるのかを考えてみましょう。例えば、動的なアクセス制御、全ての通信の可視化、継続したセキュリティの改善などがあります。かなり多くの検討事項があるため、富士通ではエンドポイント、ネットワーク、クラウド・ワークロード、統合認証、オペレーションの 5 つの領域として整理し、ロケーション毎に分けて考えています。(図 3)

2.1 ネットワーク

この中で、まずは領域 2 のネットワークについて考えてみましょう。ネットワークの領域は、いわゆる SASE と呼ばれる、ゼロトラストを実現する包括的なネットワークの領域です。なぜ SASE が必要なのでしょうか。上述したようにコロナ禍などの影響による働き方の変化により、昨今はリモートワークを含めた様々な場所から働くということが多くなってきています。従来の社内/社外というシステム環境を前提とした防御の仕方であると、一度社内に集約するようなアクセスが必要となり、既存環境の帯域やプロキシ、ファイアウォールなどがボトルネックになってしまいます。

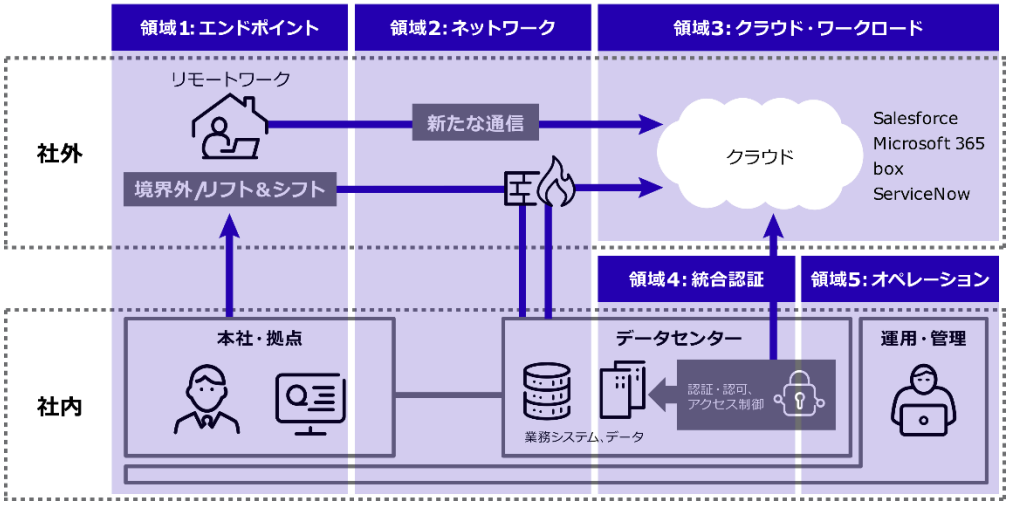


図 3：ゼロトラストに必要な 5 つの領域

SASE の導入

このような課題を解決するために、SASE を導入するメリットがあるのです。SASE を用いて直接システムを利用します。ネットワークの制御やセキュリティの機能を持ち、さらに、クラウド環境の利用状況を把握するなど、 SASE は仮想的な境界として働きます。(図 4)

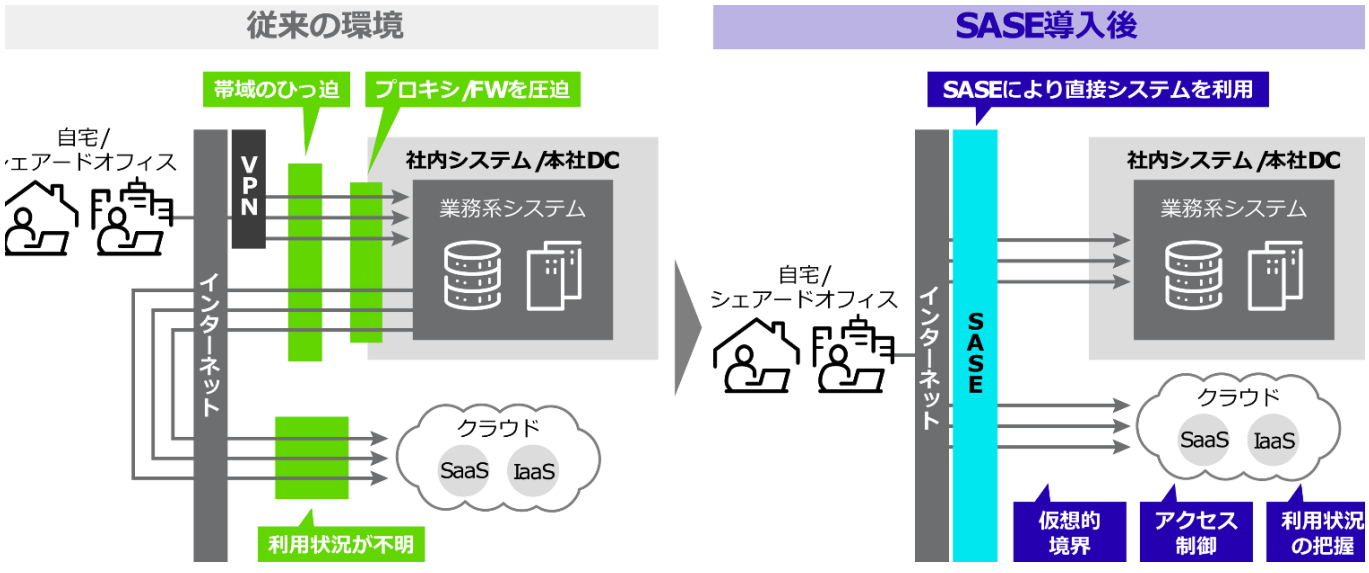


図 4：従来の境界型の環境で現れる課題を解決する SASE とは

富士通では、SASE 環境を CloudProtect シリーズにて提供しています。「**Prisma Access**」を利用した SASE の実現や、富士通独自の可視化ダッシュボードによりネットワークやセキュリティをシンプルかつ強固に一元管理します。

富士通の FENICS 回線やユニバーサルコネクトというリモートアクセスサービスを利用されているお客様には、今の回線に付け足していくことにより、ゼロトラストを実現する基本的な要素を提供します。さらに、既に店舗や一部の事務所がインターネットへ直接出られているお客様の場合は、手軽にセキュリティを強化できる「**CloudProtect DNS セキュリティ**」をご用意しています。

2.2 クラウド・ワークロード

次に、クラウド・ワークロードの領域について考えてみましょう。昨今、クラウドリフト＆シフトによりインフラ構築作業が楽になってきた一方で、セキュリティの懸念も出てきています。社内環境であれば独立した環境でセットアップして、インフラ SE がセキュリティ監査をし、環境に繋げるという段取りであったものが、クラウドを利用することによって直ぐにインターネットから接続してセットアップできるようになりました。

しかしながら、この様な利便性の改善の一方で、構築中の不備などにより誰もが社外から内部ネットワークに接続できてしまった、というような事案も増えてきています。加えてクラウド環境の設定に問題がないかを、一元的かつ網羅的に常に確認しておくことは非常に大変なことです。

そこで富士通では、各種クラウドの設定に問題がないかを確認したり、疑わしい権限の追加などがないかを確認したりするためのソリューションである「**Prisma Cloud**」を提供しています。これにより、様々なクラウド環境を一元的に管理し、各種コンプライアンスを基に診断することを実現します。

2.3 統合認証

次に、統合認証の領域について見ていきましょう。様々なクラウドを利用する際には、シングルサインオンするためのプロビジョニングが必要となります。マルチクラウドを利用すると、各 SaaS やクラウドごとに連係データを生成する必要があるため管理が煩雑となり、運用上苦労することになります。

こうしたことを解決するために、認証認可、ID 管理の仕組みを整えるお客様は多くいます。図 5 左側の IDM（Identity Management の略称）で人事情報から吸い上げたユーザー情報や権限情報を、各 SaaS へ連携し、右側の IDP（Identify Provider の略称）において ID 管理と認証管理の仕組みを提供する、という動きが必要です。

そこで富士通では、IDM と IDP の認証基盤を簡単に用意できる「**CloudProtect ID マネージャー・ID プロバイダー**」というソリューションを提供しています。これにより利便性を向上し、管理の負担軽減を行います。

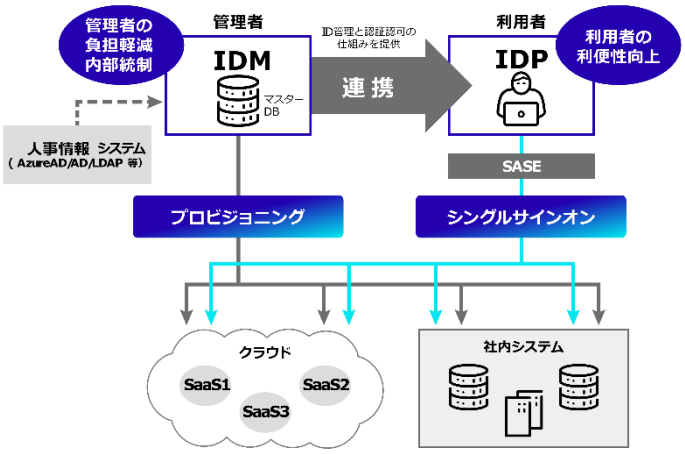


図 5：ゼロトラストに必要な認証・認可 ID 管理

2.4 エンドポイント

次に見ていくのは、エンドポイントの領域です。クラウドの利用や働き方の多様化により、様々な場所から様々な場所へアクセスするようになったため、サイバー攻撃の把握とその追跡が難しくなってきています。そこで、あらゆるログを集め分析し、追跡することが重要となります。各環境からログを集め、環境全体で何が起こっているのかを常に把握することが必要となり、その追跡・対処のためにエンドポイントでのセキュリティが重要になってきました。

EDR/XDR の導入

これを実現するのが、EDR や XDR と呼ばれるエンドポイントでのセキュリティです。EDR や XDR では、様々な場所にあるエンドポイントからの情報を吸い上げ、監視や追跡を行います。お客様の環境に合わせてご提供できるように様々なソリューションをご用意しています。

2.5 オペレーション

最後に、オペレーションの領域について見ていきましょう。この領域はいわゆる NOC/SOC と言われるような運用の部分を指しています。オペレーションでは、それぞれの領域からログを収集し、相関分析を実施してインシデントの対応に当たっていく必要があります。

富士通では、高度エキスパートがインシデントの対応に当たる、「**インテリジェンスマネージドセキュリティサービス**」を提供しています。各製品の検知ログのスクリーニングや検知シナリオをサービス内で保有していますので、お客様が新たな環境で最初からセキュリティ運用を立ち上げるよりも早く実施することができます。また、お客様の CSIRT の立場でセキュリティ専門家が業務を支援するサービスも提供しています。

ゼロトラストはこの 5 つの領域に分けると理解がしやすいということで、それぞれの領域についてお伝えしてきました。

富士通ではこれら全ての領域に対応しており、お客様環境に適したソリューションを組み合わせることで、お客様のゼロトラストを実現します。

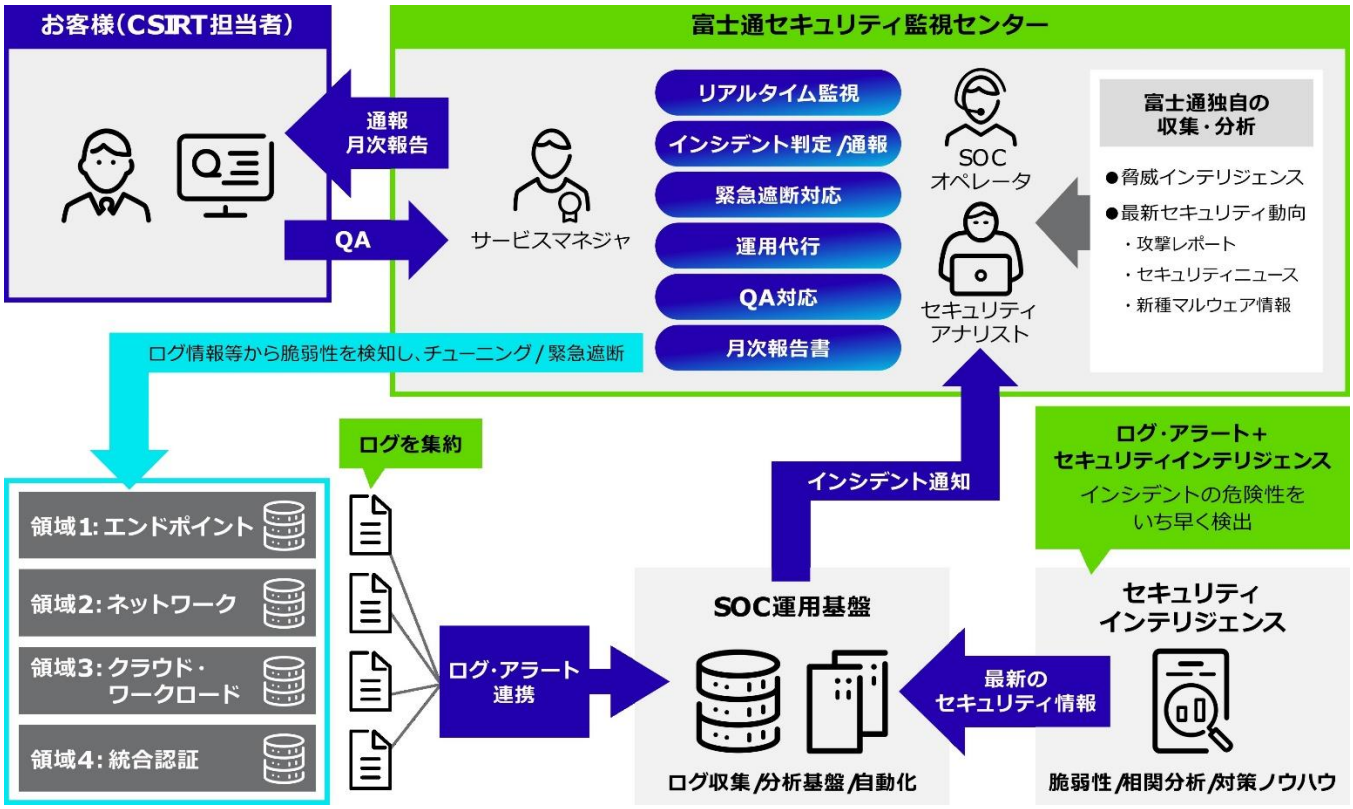


図6：実践ソリューション：インテリジェンスマネージドセキュリティサービス

3. ゼロトラストへどのように移行すればいいのか

ここまでゼロトラストを実現するための 5 つの領域についてお伝えしてきましたが、これら広範囲にわたる変更についてどこから手を付ければいいのか、ということをお伝えします。まず、ゼロトラスト環境へ 1 日で切り替えることは現実的には困難です。通常、新システムの稼働にあたっては、稼働しているシステムとは別に新しいシステムを作ってテストし、旧システムから切り替える、というやり方が多いものですが、ゼロトラストに関しては一斉切り替えは困難です。よって、順次稼働させていく並行環境が必要となります。では、それをどのように切り替えていけば良いのでしょうか。

移行の考え方として、ポイントを 3 つ挙げます。一つ目として、段階的な移行があります。これは、境界型防御の環境下に構築していくことが前提となります。どのように既存業務を止めずに並行環境を作り稼働させるかがポイント、ということです。

二つ目として、ビジネスインパクトの低いビジネスプロセスから実施するということです。これは、スモールスタートで初めて、順次拡大できる部分から移行していく、ということです。

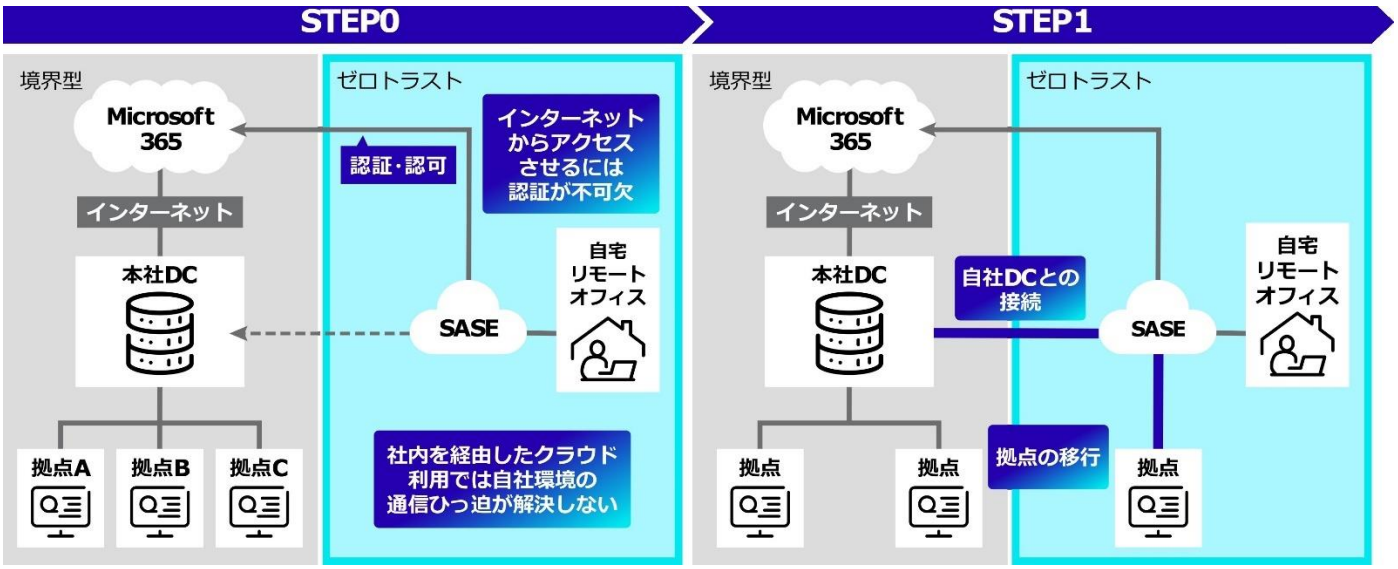
そして三つ目としては、企業や団体の課題や導入状況を踏まえて実施していくということです。これは、それぞれの企業や団体が置かれている課題の優先順位は様々であるためです。ゼロトラスト導入に唯一の解というものはなく、このようなことを考慮に入れていく必要があるということです。

こうしたことを考慮した結果、テレワーク環境から始められるお客様は多いです。なぜなら、テレワーク環境は万が一何かあったとしても出社すればいいというところから始めると、ビジネスインパクトも少ないということから、段階的な移行のファーストステップとしては実施しやすい環境であると言え、この様なお客様が多いものと考えられます。

3.1 段階的移行

では次に段階的移行の一例を挙げます。

テレワークから始める場合でも、認証の仕組みから整備することがよくあります。そして、社外環境から SASE ネットワークへの利用を開始します。自宅などから使えるようになれば、順次、支店などの拠点に展開していくという段取りを行います。とはいえ、一律な答えはありませんので、企業や団体の状況に合わせて新規に展開知る拠点から、などの場合もあります(図 7)。



今までのシステムをゼロトラストに移行するための手法とは

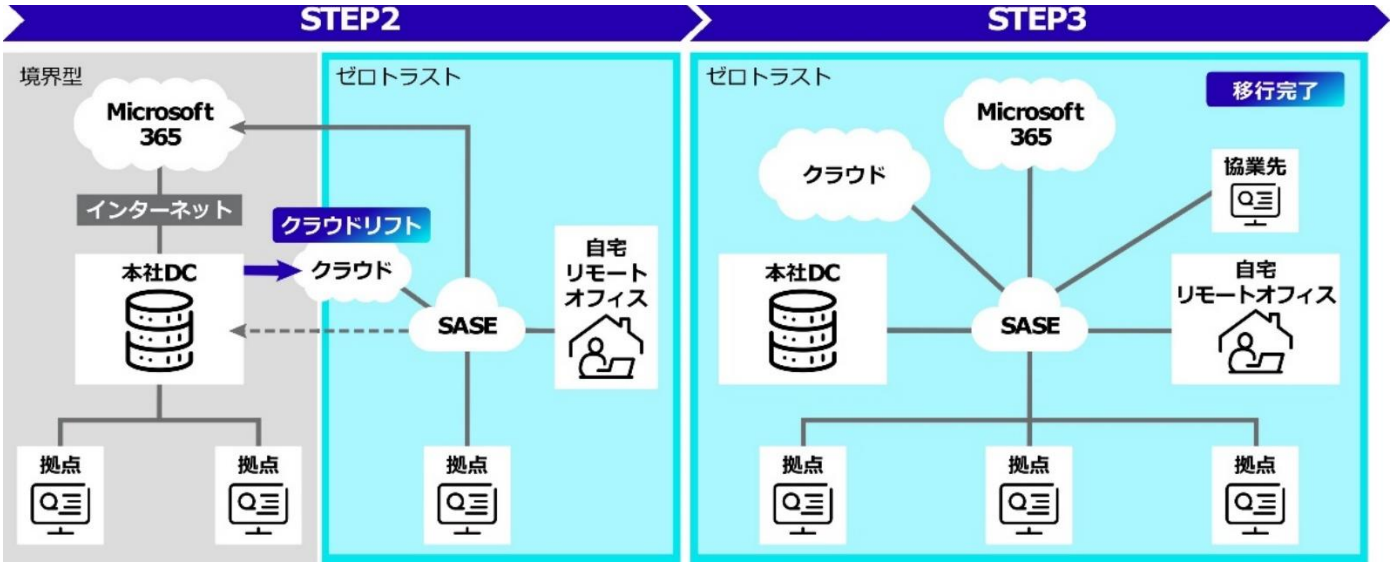


図７：段階的移行のステップ（一例）

認証から始めるお客様が多い理由は、先ずインターネットから直接アクセスできるようにしなければ、よくある課題である帯域のひっ迫が解消しないからです。インターネット経由でアクセスさせるためにはインターネット上において認証認可する仕組みが必要であり、そのために、まず認証を整備するということが多いということです。自宅やリモートオフィスからの業務の確認が正常にできたら、次に拠点の移行ということで、新規に出来る拠点や店舗から、と始められるお客様が多いです。そうした中で全拠点を一斉に切り替えるよりも、順次移行というやり方を行います。

併せて、自社のデータセンターなどと SASE を繋げて、ゼロトラスト環境からデータセンターへのアクセスを実施します。次に、ゼロトラストと境界型のハイブリッドの環境の中で、自社データセンターからクラウドリフト＆シフトを進めていきます。最終的に全拠点の環境を移行すると、SASE を中心としたネットワーク構成となり、構成がシンプルになります。フルインターネットで一元的にセキュリティやログを管理します。

こうした移行は一例です。実際はお客様の環境や課題によってやり方を変えていく必要があり、ベストプラクティスは今のところ確立していません。

そこで、富士通はお客様のゼロトラストを確実に実現するために２つご用意しました。

１つ目は、「ゼロトラストロードマップ策定支援」です。こちらは、ゼロトラストの実現に向けてどのように進めていけば良いのか分からないお客様向けです。現在の状況に合わせて課題を抽出し、最適なロードマップの策定を行います。

２つ目のサービスは、「**ゼロトラストセキュリティ構築・運用サービス**」です。このサービスでは、ゼロトラストで導入すべきソリューションを一気通貫にて対応し、稼働後のセキュリティやシステムの運用を含めて実施します。

3.2 ゼロトラストソリューション

富士通では、ゼロトラストを実現する全ての領域のソリューションを取り揃えており、お客様環境に適したゼロトラストを実現します。(図８)

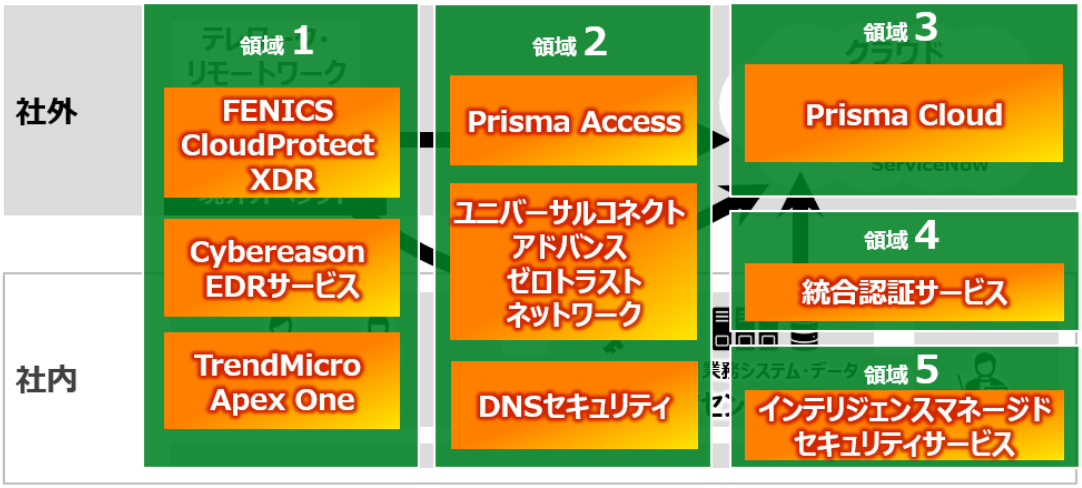


図８：ゼロトラストソリューション

さいごに

本書ではゼロトラストはなぜ必要であるのか、その構成要素についてお伝えしました。

ゼロトラストは全体を考えて実施していく必要があります。このようなノウハウを持っている富士通に、お任せください。

【ご参考】

Zero Trust Network 未来を見据えた社会を実現するサイバーセキュリティ 詳しくはこちら

富士通 セキュリティ 詳しくはこちら

富士通 ネットワークサービス 詳しくはこちら

お問い合わせ先

富士通コンタクトライン（総合窓口）

0120-933-200

受付時間 ：平日 9:00～12:00、13:00～17:30 (土曜・日曜・祝日・当社指定の休業日を除く)

富士通株式会社　https://www.fujitsu.com/jp/services/infrastructure/network/security/zero-trust/

【発行元】富士通株式会社
〒105-7123 東京都港区東新橋 1-5-2 汐留シティセンター