パーソル ワークスデザイン

PERSOL

IT 環境の見直しをご検討されているご担当者さま向け

お客さまにマッチしたソリューションをご提案!

セキュリティ施策を成功に導く
「マネージド ゼロトラスト」

KDDI × PERSOL パーソル ワークスデザイン

「マネージド ゼロトラスト」とは

テレワークが普及し、働き方が多様化する中で注目を集める「ゼロトラスト」。では、自社の IT 環境をゼロトラストに対応させるためには、どのようなアプローチが必要なのでしょうか。このホワイトペーパーでは、KDDI がワンストップで支援する「マネージド ゼロトラスト」のモデルを参考に、ゼロトラスト化を推進する際に重要な考え方について解説します。

With コロナ・After コロナに向けて新しい働き方が普及した結果、オンラインを活用した非対面コミュニケーションが増加しています。このような変化の中、企業が構築しているネットワーク環境も新たな働き方に対応したものへの変革が求められています。従来のオフィスワークでは、オフィスへ出社し社内のみで仕事を行うことが大前提としてありました。そのため、業務で使用する情報は社外へ持ち出さないのが鉄則であり、同様にネットワーク環境も社内と社外を明確に区別していました。このような従来型のセキュリティ対策を「境界型」と呼びます。

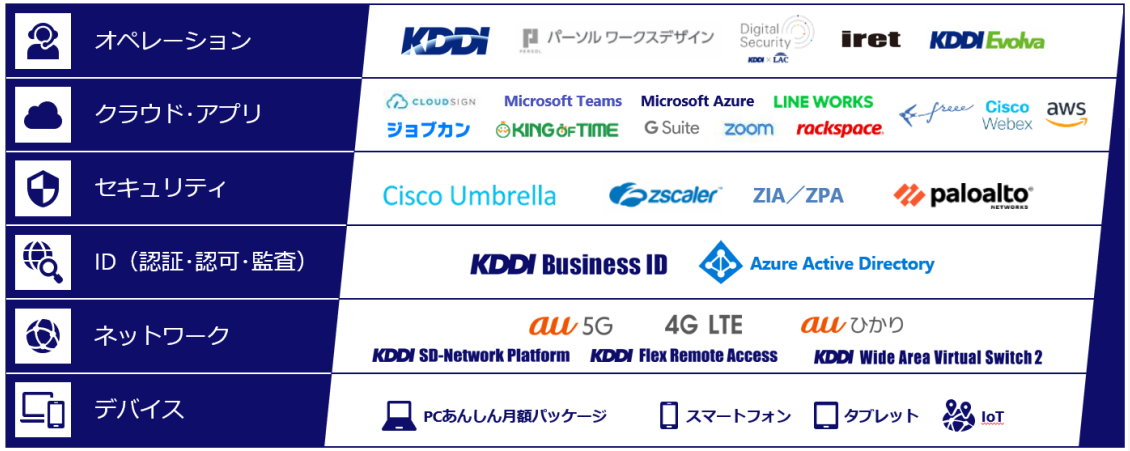
これに対し、リモートワークなどで働き方が多様化した現在は、自宅のインターネット環境を使用するケースが増えています。その結果、従来の境界型のセキュリティ対策では対応しきれなくなっているのが現状です。そのため、社内はもちろん社外でも安全に業務を遂行できるよう、時間や場所にとらわれないセキュリティを確保することが、多くの企業における共通の課題となっています。
このような課題を解決するのが、**「マネージド ゼロトラスト」**です。

「マネージド ゼロトラスト」は、**「場所にとらわれず、安心・安全・簡単につなぐ」を実現するセキュリティモデル**です。お客さまのニーズに合わせ、ネットワークやセキュリティ、デバイスなどを組み合わせながら、最適なソリューションをワンストップで支援しています。

「マネージド ゼロトラスト」6 つのコンポーネント

マネージド ゼロトラストでは、お客さまの IT インフラや働き方に応じて、6 つのコンポーネントを組み合わせることで高い価値を発揮でき、安全で利便性の高い環境を実現します。

ネットワークを導入することで課題が解決した従来とは異なり、現在は業務アプリケーションのクラウド化や働き方の多様化、標的型攻撃の高度化などに合わせてセキュリティ面を見直す必要があります。



2021 年 8 月時点

資料提供元：KDDI 株式会社

お客さまのネットワーク構成に合わせた最適なソリューションをご支援

ゼロトラスト化において重要な考え方のひとつに「段階的に導入する」ことが挙げられます。初期段階から完全なゼロトラストモデルを導入するのではなく、お客様の現状に合わせて段階的に導入していくことが重要です。そこで、以下では導入ステップを 3 つの段階に分け、完全なゼロトラストモデルを導入するまでの流れを解説します。

段階的に導入することが重要

社内システムや業務アプリケーションは業務内容や部署ごとに異なります。しかし、これら複数のシステムを一気にクラウド化することは難しく、技術的にも運用的にもさまざまな問題が生じるリスクがあります。そのため、既存の社内システムや業務アプリケーションのクラウドシフトの段階に応じて、最適なゼロトラストのコンポーネントを導入していくことが重要です。

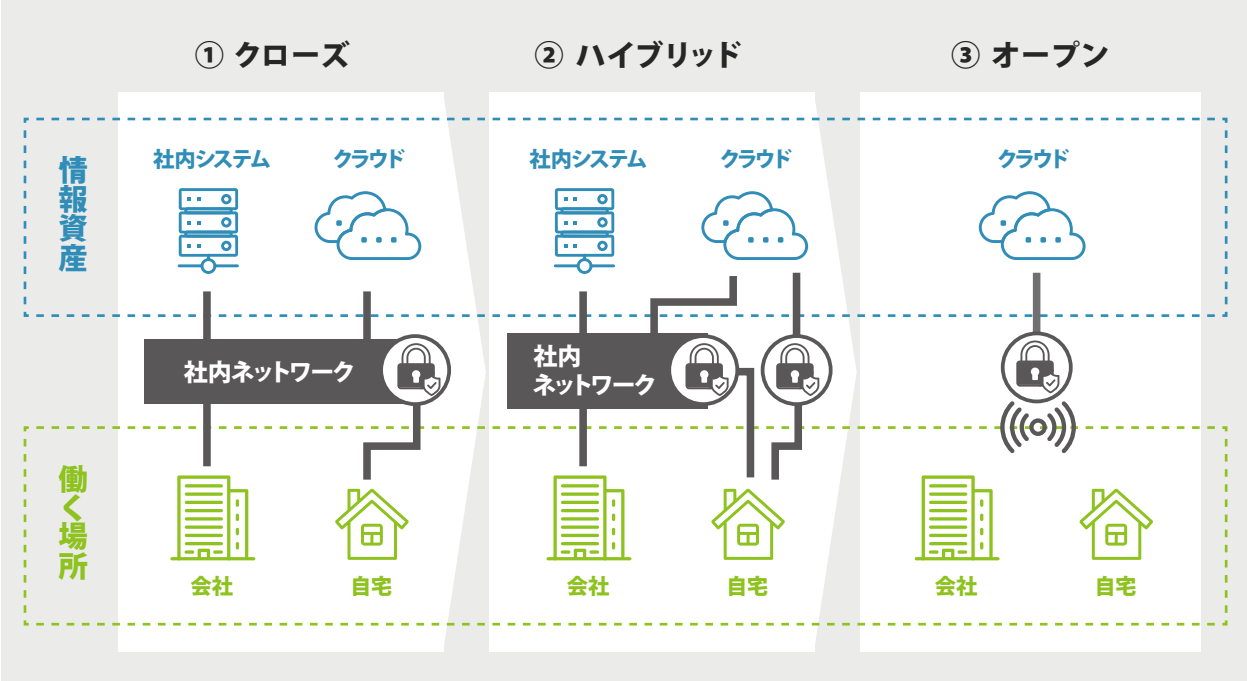
以下の図は、社内システムや業務アプリケーションのクラウドシフトを 3 つのフェーズに分類したものです。

①クローズ：情報資産が全て社内ネットワークの中にあるケースです。この場合、自宅から社内ネットワークへアクセスできるようにリモートアクセスのソリューションを追加します。

②ハイブリッド：情報資産が社内ネットワークとクラウド環境の両方に存在するケースです。この場合、①のパターンに加えて、クラウド環境にも自宅から直接アクセスできるようにします。

③オープン：情報資産が全てクラウド環境に移行したケースです。

上記のうち、「③オープン」は完全ゼロトラスト化が実現できたフェーズといえます。しかし、全ての企業にとって必ずしも完全ゼロトラスト化が理想とは断言できません。お客さまが求める環境に応じて「クローズ」や「ハイブリッド」も含めた選択肢を検討し、運用していくことが重要です。



情報資産の場所を見極めることが重要

ゼロトラストを実現する上で重要なポイントには何があるのでしょうか。弊社では、情報資産のクラウドシフトに応じて、ご提供できるゼロトラストモデルを 2 つに分類しています。ここでは、お客様の IT 環境に応じて、どのモデルを導入すれば良いのかを一例として紹介します。

ゼロトラスト化を推進する上では、現時点において「自社の情報資産がどの程度クラウドへ移行できているか」を見極めることが非常に重要です。

これは同時に、「自社の情報資産がどの程度社内ネットワークに残っているか」を理解することでもあります。自社の情報資産の所在を知ることで、自社に適したゼロトラストモデルが把握でき、同時に「クローズ」「ハイブリッド」「クラウド」のうち、どのモデルを目指すべきなのかが見えてきます。

クラウドシフトに応じた 2 つのゼロトラストモデル

弊社では、クラウドシフトに応じたゼロトラストモデルを「リモートアクセスをベースとした強化モデル」と、「ゼロトラストモデル（セキュア PC モデル）」の 2 つに分類しています。

情報資産がオンプレミス型の社内システムにある場合、「リモートアクセスをベースとした強化モデル」を選択します。一方、情報資産のクラウド化が進んでいる場合には、クラウドベースの「ゼロトラストモデル（セキュア PC モデル）」の導入が望ましいといえます。

	リモートアクセスをベースとした強化モデル	ゼロトラストモデル（セキュア PC モデル）※
目指すモデル	クローズ / ハイブリッド	オープン
業務・情報資産	社内システム・オンプレミスがベース	クラウドがベース
ポイント	①トラフィック分散（ダイレクトインターネットアクセス） ②インターネットセキュリティ強化（社内外で同一のセキュリティ） ③認証強化と利便性向上（多要素認証と SSO）	①NW に依存しないクラウドセキュリティ（社内外を意識しない安全なアクセス） ②ゼロトラストを実現する統合認証基盤（Azure AD 連携） ③どこにでも持ち出せるセキュアな PC（PC＋SIM＋エンドポイントセキュリティ）
コンポーネント	KDDI Flex Remote Access Cisco Umbrella/KDDI Business ID	Zscaler/M365 コンポーネント Azure AD/LTE 対応 PC

※KDDI が導入したゼロトラストセキュリティのノウハウをソリューション化したモデル

導入ステップの例

ゼロトラスト化に向け、自社にとって最適なモデルが把握できたら、導入のために必要なステップを理解しておきましょう。弊社では、本格展開の前にトライアルを含む 4 つのステップの実施を推奨しています。具体的にどのような導入ステップを経るのか、以下に一例を紹介します。

ゼロトラストモデルの導入にあたっては、いきなり本格展開を行うことは難しいため、その前の段階でトライアルを実施し課題点などを把握する必要があります。弊社で推奨している全体の流れとしては、トライアルと本格導入の 2 段階に分け、合計 4 つのステップを経ることです。

① 環境構築 ネットワークや端末管理などをはじめとしたインフラを構築するとともに、要件や運用の建付けも同時に行います。

②トライアル トライアルに参加するメンバーをアサインした上で、トライアンドエラーを繰り返しながら、課題の洗い出しや今後の機能追加要件の把握、業務活用方法を模索します。

③ 本格展開準備 トライアルで浮かび上がった課題の改善に取り組みます。必要に応じて設備やインフラの増強・拡張を行い、同時に社内規程などの見直しも行います。

④ 本格展開 社内ユーザーからの問い合わせに対応できるようユーザーサポートの活用を促進します。

STEP1

環境構築

新しいインフラの構築

数ヶ月間のプロジェクト

- ネットワークインフラの構築
- 端末管理インフラの構築
- パソコン設計、GPO 以降
- 運用建付け

STEP2

トライアル

一部メンバーをアサイン

トライアンドエラーでの
トライアル

- 協力的なトライアルユーザー
- Teams を活用した不具合申告

STEP3

本格展開準備

新しいインフラの構築

トライアル課題の改善、
設備増強

- 社内規定の変更
- ネットワークインフラの拡張
- 内部不正対策環境の構築

STEP4

本格展開

ユーザーサポート活用促進

導入において懸念点される運用負荷

情報システム部門のご担当者さまの中には、「ゼロトラストを導入することによって担当業務が増え、今以上に業務負荷が増大するのではないか」と懸念を抱く方も少なくありません。以下では、情報システム部門のご担当者さまや IT 管理者さまがどのような運用負荷を懸念しているのか、一例を紹介します。

エンドユーザー向けの対応

PCやスマートフォンなどのデバイス管理や証明書管理などについて、社内ユーザー（システム利用者さま）からのメールや電話による問い合わせが多く発生する可能性があります。これにより、ヘルプデスクご担当者さまの負担が増大する懸念が生じることも考えられます。

デバイス管理
ID・アカウント管理
証明書管理
問い合わせ対応

IT インフラとしての対応

ゼロトラストの導入にあたっては、IT インフラとして複数コンポーネントを統合し、最適化を図りながら運用していくことになります。そのため、インフラやシステム管理者さまの運用負荷が増大することもあるでしょう。

複数コンポーネントの
統合運用

Remote Access
SWG
IAM
EDR
CASB

継続したセキュリティへの対応

セキュリティ対策の面においても、ログ収集や監視、リスク分析など継続した対応が必要です。これにより、セキュリティ対策のご担当者さまやシステム管理者さまの工数が増大する可能性があります。

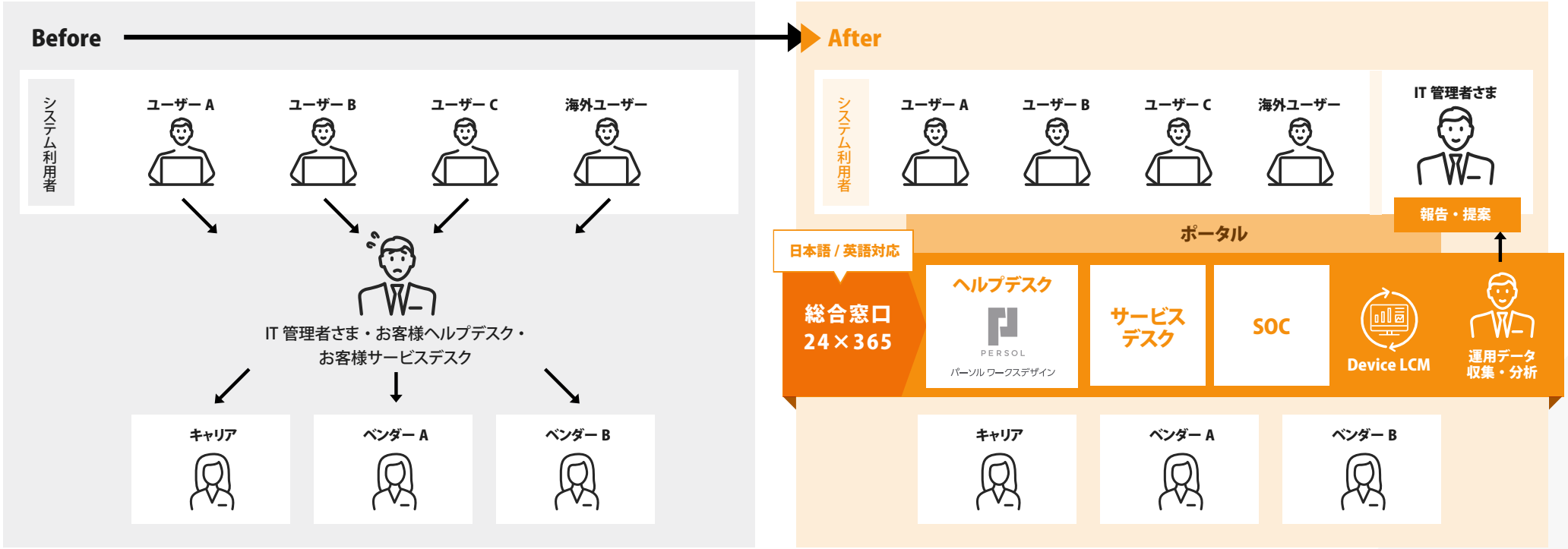
ログ収集と管理
リスク分散
脅威情報のアップデート
インデント対応

「マネージドゼロトラスト」のサポート体制

ゼロトラストの導入にあたっては、情報セキュリティ部門や IT 部門においてさまざまな運用負荷の増大が懸念されます。しかし、「マネージド ゼロトラスト」は、前項で紹介した運用負荷を軽減できるよう、充実したサポート体制を構築しています。

これまで、情報システム部門のヘルプデスクご担当者さまや IT 管理者さまは、社内ユーザー（システム利用者さま）から問い合わせを受けるたびに、システムを提供するキャリアや各ベンダーとのやり取りに追われていました。

「マネージド ゼロトラスト」では総合窓口を設置しており、「お客さま業務サポート」や「システム・サービス運用」、「セキュリティ運用」を代行する機能を備えています。そのため、情報システム部門のご担当者さまや IT 管理者さまは、総合窓口における各担当者からの報告を待つだけとなります。従来のように社内ユーザーの問い合わせ内容をキャリアや各ベンダーに取り次ぐ必要がなく、大幅な業務効率化が実現できるでしょう。



社内ユーザー（システム利用者さま）からの問い合わせ対応を受ける総合窓口の中でも、その入り口となる「ヘルプデスク」の部分をパーソルワークスデザインが担当し、サポートさせて頂きます。

特別なご案内

当ホワイトペーパーをダウンロードして頂いた方限定で、
「マネージド ゼロトラスト」に関する個別相談会を開催します。

パーソルワークスデザインでは、当ホワイトペーパーではお答えできなかった
「マネージド ゼロトラスト」についての疑問にお答えいたします。

参加方法

1. 資料ダウンロード時にご入力頂いたメールアドレス宛に、個別相談会のご案内をお送りしております。
2. ご参加のお日にちを複数候補ご記載の上、ご案内メールに返信してください。
3. 日程調整ができ次第、担当よりご連絡をいたします。

ご不明点・その他お問い合わせはこちら

パーソルワークスデザイン株式会社
お問い合わせ窓口
820454@persol.co.jp

PERSOL

パーソル ワークスデザイン

2021 年 9 月発行
パーソルワークスデザイン株式会社
東京都豊島区池袋 2-65-18 池袋 WEST ビル
https://www.persol-wd.co.jp/