2021 年 8 月 26 日
ドコモ・システムズ株式会社
株式会社日立製作所
シスコシステムズ合同会社

ドコモ・システムズのゼロトラスト対応「次世代テレワーク基盤」を ドコモ・システムズ、日立、シスコが構築

テレワーク環境の安全性と利便性を両立し、コミュニケーションの活性化や生産性の向上を支援

ドコモ・システムズ株式会社(以下、ドコモ・システムズ)、株式会社日立製作所(以下、日立)、シスコシステムズ合同会社(以下、シスコ)は、ドコモ・システムズの DX プロジェクトの一環として、セキュアで快適なテレワーク環境を整備するため、ゼロトラストネットワーク技術を活用した「次世代テレワーク基盤[*1]」を構築しました。ゼロトラストネットワークは、アクセス情報をすべて信頼せず(ゼロトラスト)、あらゆる端末や通信のログを取得し、都度認証を行うもので、クラウドシフトが進む DX(デジタルトランスフォーメーション)時代に即したセキュリティモデルです。

本取り組みでは、日立グループのゼロトラストネットワークの導入ノウハウとシスコとの強固なパートナーシップを生かし、先行導入を進めていた Microsoft 365 とシスコのゼロトラスト関連サービスを適材適所に組み合わせ、テレワーク環境の安全性と利便性の両立を実現しました。

2021 年 7 月より、ドコモ・システムズにて、管理部門からシステム開発部門まで 700 名規模で利用を開始しており、各自の業務端末からインターネットに直接接続し、社内システム・アプリケーションとクラウド上の SaaS[*2] の双方へセキュアかつ快適にアクセスすることが可能になりました。これにより、今後さらなるコミュニケーションの活性化や生産性の向上が期待されています。

現在、新型コロナウイルスの感染拡大を契機に、多くの企業がニューノーマルな働き方を検討・導入し始めており、テレワークが急速に拡大する中で、コミュニケーション面・セキュリティ面の課題が顕在化し、安全性と利便性を両立する新たなネットワーク環境が求められています。

これまでのテレワーク環境は、社内と社外のネットワークを分離する「境界型セキュリティ」に基づいて構築されており、社内システムをオンプレミス環境で稼働させ、VDI[*3] を用いて外部からのアクセスを許可する形で実現していました。この方式では、全ての通信が社内システムを経由するため、テレワークが増加するほどにネットワーク帯域が逼迫し、通信の遅延や切断といった利便性の低下の要因となります。そこで、社内と社外のネットワークの境界を設けず、クラウド側とエンドポイントとなる端末側で、常にすべてのアクセスを監視し、認証・認可を行うゼロトラストネットワークが DX 時代に即したセキュリティモデルとして注目されています。

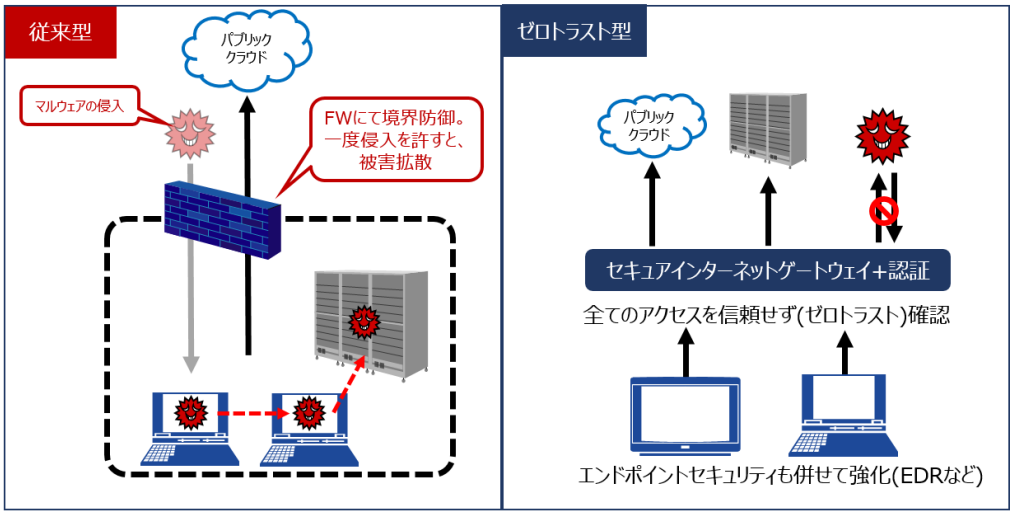

図 1: ゼロトラストネットワークの概要

ゼロトラストネットワークには、大きく「認証」「アクセス制御」「デバイス保護・管理」のプロセスがあり、数多くの関連商材を適切に組み合わせて、設計・構築することが必要です。今回は、その中でも、ユーザーの利便性を損なうことなく、強固なアカウント管理や高度なセキュリティサービスを容易に実現することをポイントに、ゼロトラストの概念に基づく「次世代テレワーク基盤」を構築しました。

具体的な特長は以下の通りです。

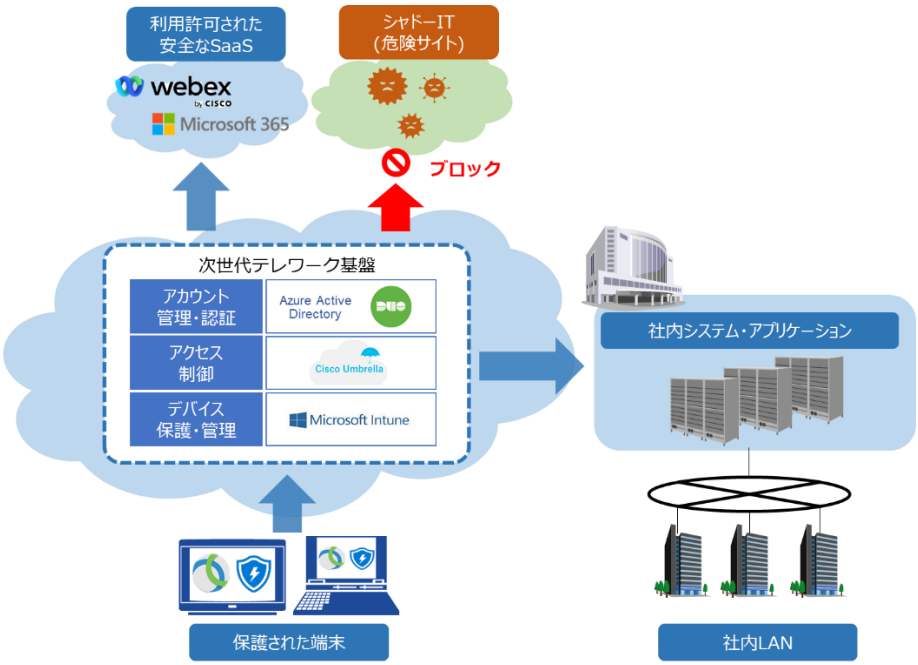

図 2: 次世代テレワーク基盤の構成

1. アカウント管理・認証

アカウント管理・認証を行う Azure Active Directory と、多要素認証が可能な Cisco Secure Access by Duo を組み合わせ、ID 管理と多要素認証の管理を分けた上で連携して取り入れること

で、強固な認証環境を提供します。アカウントの振る舞いからリスクを検知した場合、早急にアカウントを凍結し、不正なアクセスを防ぎます。また、異なるベンダー間のシングルサインオン連携により、ユーザーは 1 回認証を行えば、自社システムや Microsoft 365 など必要な業務アプリケーションにシームレスにアクセスすることが可能です。

2. インターネットアクセス制御と社内システム・アプリケーションへのアクセス制御

危険サイトや利用禁止サイトへのアクセスを防ぐセキュアインターネットゲートウェイ(SIG)である Cisco Umbrella を導入することで、全通信を対象に高度なセキュリティを確保しています。例えば、クラウド上に配置したドメインネームシステム(DNS)でドメインや IP アドレスを確認し、危険と判断されるアクセスをブロックします。また、Cisco Umbrella はセキュアウェブゲートウェイ(SWG)としても機能し、クラウドアプリケーション制御機能(CASB)により、利用状況を可視化し、社員が勝手に使用するリスクの高いアプリケーション(シャドーIT)を個別にブロックするなどの高度なセキュリティサービスを容易に導入することができます。これらにより、柔軟性の高いインターネットアクセスを実現しています。さらに、Cisco Secure Access by Duo により、アカウント認証後も、OS のサポート切れなどデバイスの状態や、アクセス場所およびデバイスとネットワークとの整合性などのセキュリティポリシーをチェックし、問題があった場合は、社内システム・アプリケーションへのアクセスをブロックすることが可能です。

3. デバイス保護・管理

エンドポイントとなる端末の監視の強化として、Microsoft Intune と Microsoft Defender for Endpoint を導入することで、ログ情報を常時取得・分析処理し、サイバー攻撃のマルウェアやウイルスをリアルタイムに検知、管理者に迅速な通知を行います。また、Azure Information Protection により、端末に保存されている機密データを保護することができ、万一の端末紛失やウイルス感染にも対応することが可能です。

今後、今回のドコモ・システムズでのゼロトラスト対応のノウハウを、ドコモ・システムズ、日立、シスコのそれぞれの立場で生かし、ゼロトラストネットワークの普及に努めることで、企業の DX の実現やニューノーマルな働き方を支援していきます。

* 1「次世代テレワーク基盤」:従来からドコモ・システムズが提供してきたサービスアセット群と先進クラウドサービスをセキュアかつシームレスに連携させることで従来よりも生産性を高めることを目的としたリモートワーク基盤。
* 2 SaaS : Software as a Service
* 3 VDI : Virtual Desktop Infrastructure

■商標

・その他、記載されている会社名、製品名は、各社の登録商標または商標です。

■本件に関するお問い合わせ先

ドコモ・システムズ株式会社 クラウド事業部
お問い合わせフォーム：https://ddreams.docomo-sys.co.jp/inquiry/contact_protector.php

株式会社日立製作所 サービスプラットフォーム事業本部 IoT・クラウドサービス事業部
お問い合わせフォーム：http://www.hitachi.co.jp/it-pf/inq/NR/

シスコシステムズ合同会社 プレスルーム 鈴木、石丸
TEL: 03-6738-5028（鈴木）03-6434-6809（石丸）
E-Mail: press-jp@cisco.com
URL：https://news-blogs.cisco.com/apjc/ja/

以上