第６１回一般論文

デジタルワークプレイスで実現する現場の生産性向上

～ゼロトラストへのシフトチェンジ～

会員名：鹿島建設株式会社（関東支部）

会社概要

名称　　：鹿島建設株式会社
所在地　　：東京都港区元赤坂１－３－１
設立年月日：１９３０年（昭和５年）
代表者　　：天野　裕正
資本金　　：814 億円余
従業員数　：8,129 名（2023 年 3 月末現在）
事業内容　：建設事業、開発事業、設計・エンジニアリング事業ほか

執筆者

ＩＴソリューション部
主任

藤本　奈央
（代表執筆者）

ＩＴソリューション部
課長代理

矢口　賢一

要旨

建設業においては、2024 年度から始まる時間外労働上限規制への対応として、現場の生産性向上や多様な働き方への対応が求められていた。しかしながら既存の IT 環境では、ネットワーク遅延、在宅勤務などで発生する情報セキュリティリスクの低減、様々な IT デバイスを安全かつ快適に利用できる環境整備、多様化するセキュリティインシデントへの対策の強化が課題となっていた。

これら課題を解決するために、多様な働き方と生産性向上を目指す IT 環境として「鹿島デジタルワークプレイス」を構築し、国内グループ会社を含めて展開した。「鹿島デジタルワークプレイス」ではゼロトラスト技術を採用し、インターネット環境をよりダイレクトに、かつ安全・効率的に活用するため、セキュリティ対策の強化とともにネットワーク・アーキテクチャーのシフトチェンジを行った。

インターネット上のサービスに直接通信する仕組みにしたことで、ネットワーク遅延の解消、通信品質の向上を実現するとともに、各種サービスへのアクセス制御や高度な脅威から組織を保護するためのセキュリティ機能をクラウド上に配置することで、場所やデバイスに依存しない柔軟な働き方が可能な環境を提供し、生産性を最大に高める働き方を選択することが可能となった。

目次

1　序論

建設業においては 2024 年度から始まる時間外労働の上限規制への対応が最重要課題であり、特に現場の長時間労働の是正にあたっては、現場事務所の週休二日の推進はもとより、柔軟な働き方を可能とする環境整備等、業界一丸となって取り組んでいる。鹿島においては、最先端の ICT/AI 技術やロボット技術を活用した施工の合理化をはじめ、様々な業務改善を進めているが、コロナ禍という想定外の危機が柔軟な働き方へのシフトを加速させ、時間外労働上限規制を含む働き方改革は、現場の中を含めて確実に進めなければならない状況となっている。

このような状況において、国内で常時稼働している約 600 の建設現場や鹿島グループ 16,000 人の働き方を支えるネットワーク基盤に関しては、これまで高速化や利用デバイスの多様化など、様々な要請に追従してきたが、これからの働き方変革を支える安全・安心な基盤としては、現在の延長線上の考え方では対応が難しい状況となってきている。

今後のネットワーク基盤を考慮するにあたり、避けることのできない変化の一つにクラウドシフトへの加速が挙げられる。新型コロナウィルスへの対応を契機として、ペーパーレス化や業務のデジタル化が進み業務システム等は従来のオンプレミスのシステムやファイルサーバからクラウドサービスへ急激に移行が進んでいる。当社においてはクラウドサービスを利用するにあたり、IT/セキュリティ部門による審査・許可制をとっているが、(図　1)の通り右肩上がりで申請は急増しており、特に昨年度は 2019 年と比較して 3 倍近い申請があったことからもクラウドシフトが進んでいることが分かる。そのような外部環境が変化している状況においても、鹿島のネットワーク基盤としては境界防御を前提とした構成であったため、新規のクラウドサービスを導入する度に、インターネット接続口の通信トラフィックの集中・急増による通信品質の低下が問題となり、後追いで改善してきた経緯がある。

また、情報セキュリティの考え方に関しても、セキュリティ調査会社である Mandiant 社のレポート（図 2）によると、従来のウイルス対策ソフトでは検知が困難なゼロデイ攻撃（ソフトウェアベンダーがパッチを公開する前に攻撃に悪用されるソフトウェアバグ）が増加傾向にあり、更に近年は突出して増えていることから、境界防御やアンチウィルス等の予防を前提とする考え方から、侵入・感染を前提とした対処対策に力点を置く方向に変換していく必要がある。このため、いつでも・どこでも適切なセキュリティ対策が執り行える仕組みが必要であった。

上記のような懸念を払拭するためには、時間や場所に依存しない多様な働き方への対応や将来に亘る通信の高速化への追従、さらには高度化するセキュリティ要件に対応した安心・安全・快適な IT 基盤に変革（トランスフォーメーション）していく必要がある。当社では、その実現手段として、従来の境界防御型の構成からゼロトラストへのシフトチェンジを進めることとした。

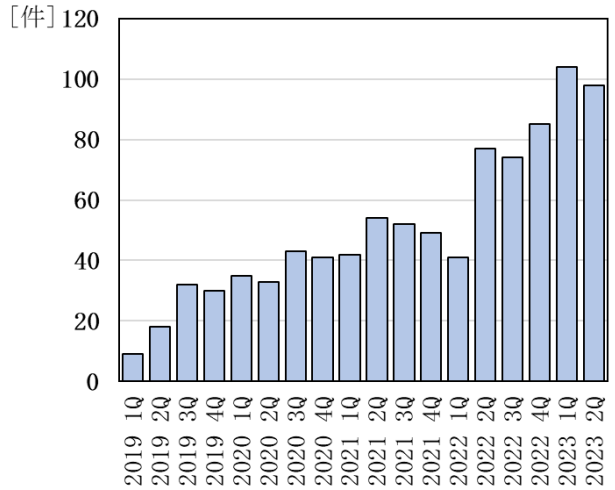

図　1　鹿島におけるクラウドサービス利用申請件数

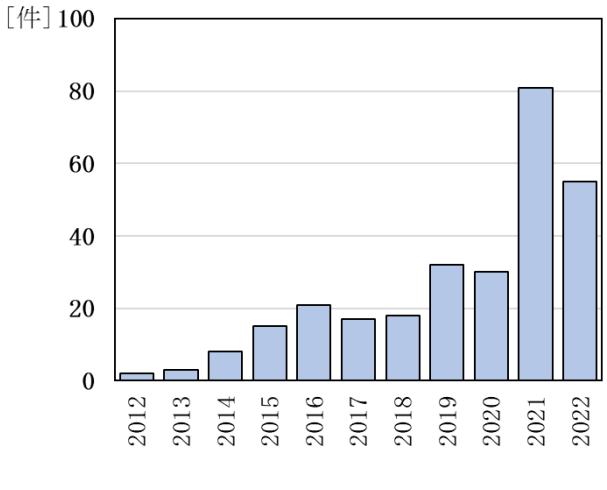

図　2　ゼロデイ攻撃の調査件数

２　現場の生産性向上を推進する鹿島デジタルワークプレイス

本章では、現場の生産性の向上や多様な働き方に対応する新たな IT 基盤の整備にあたり策定した「鹿島デジタルワークプレイス」の全体像について述べる。

鹿島デジタルワークプレイスとは、社員自らがリアルとサイバーを使い分け、各自が直面している状況下で最大限に高められる働き方を選択することを可能とする安心・安全・快適な IT 環境である。働き方の変化や加速するクラウド活用、高度化するサイバー攻撃等に対して、安全で利便性の高い環境を実現・提供することにより、社員の生産性を向上させるという目標へ向け、2021 年度から 2023 年度にかけての鹿島中期経営計画における重点実施項目として進めてきたものである（図　3）。

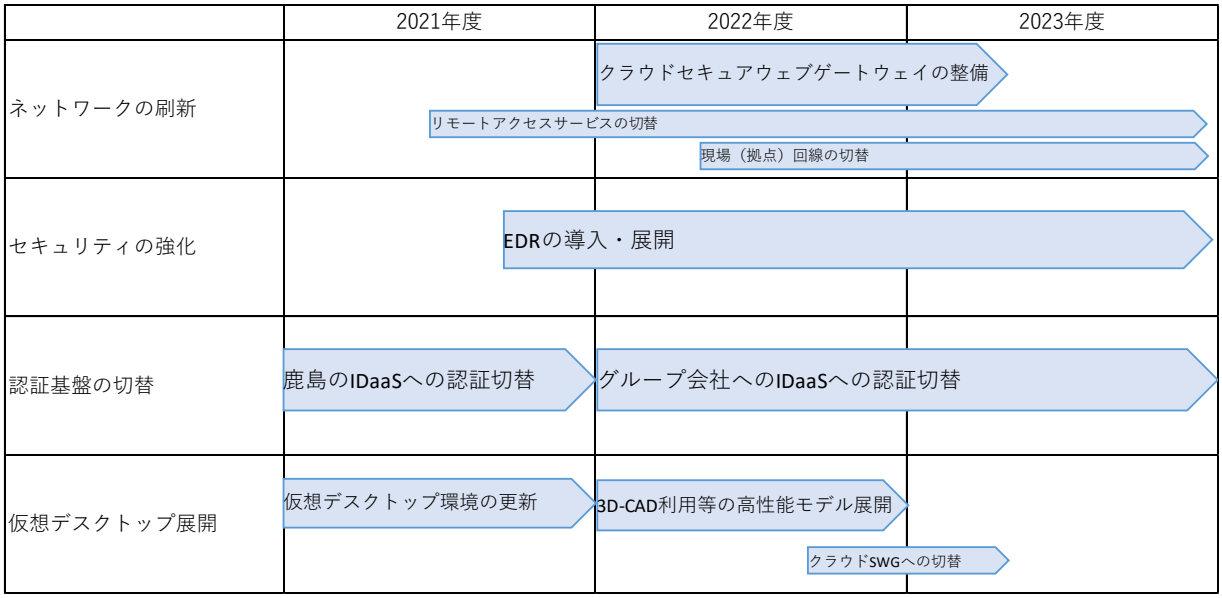

図　3　鹿島デジタルワークプレイス展開スケジュール

鹿島デジタルワークプレイスを実現するための技術的な方針は以下の 4 点である（図　4）。

- クラウドセキュアウェブゲートウェイ(Secure Web Gateway)（以下、クラウド SWG）を導入し、従来の閉域網経由の通信に加え、閉域網以外からの接続についても統一的な制御ポリシを適応できるネットワーク環境を構築する。
- Endpoint Detection and Response（以下、EDR）によるふるまい検知や Security Operation Center(以下、SOC)による常時監視を行うことで、管理者によるインシデント発生時の対処を可能とする環境を構築し、セキュリティ強化を図る。
- テレワークに関して、従来の社給機器を用いた VPN 接続のほかに、仮想デスクトップ環境を構築・提供し、私用端末から安全に業務を可能とする環境を構築する。
- これらの仕組みを支える認証基盤については、クラウド上の様々なサービスの ID 管理を一元的に行う Identity as a Service（以下、IDaaS）を利用し、各種クラウドサービスに対するユーザプロビジョニングやシングルサインオン等を実現し、ユーザ認証やデバイス認証に加えて、必要に応じて多要素認証等も実施する。

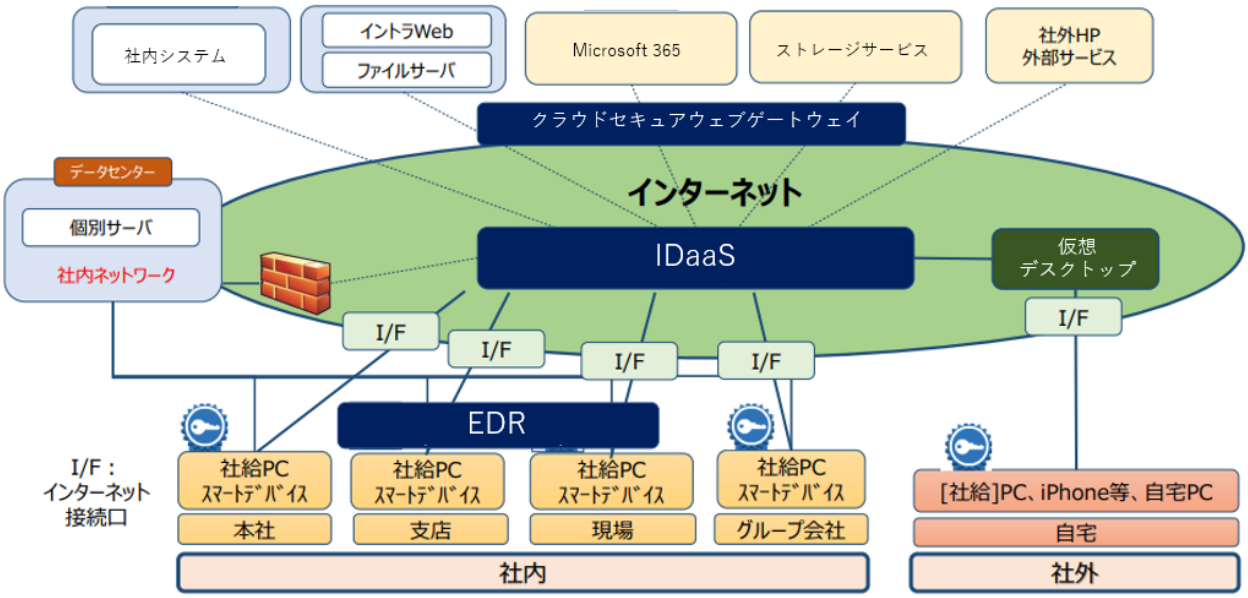

図　4　鹿島デジタルワークプレイスの構成図

本稿では鹿島デジタルワークプレイスを支え、鹿島の将来にわたるネットワーク基盤となるゼロトラストネットワークの構成要素のうち、ネットワーク構成およびセキュリティ強化を中心に、その導入手順や導入効果について述べる。

3　ネットワーク基盤の刷新

本章では、鹿島デジタルワークプレイスの実現へ向けたネットワーク基盤の取り組みについて述べる。デジタル時代の進展と働き方の多様化に伴い、トラフィックルートの複雑化、そしてトラフィックの大容量化への対応を考慮した。

3．1　従来のネットワーク基盤における課題

従来の鹿島のネットワーク基盤（図５）は、インターネットへの接続に対して一般的な境界防御を前提とした構成であった。そのため各端末からインターネットへの通信については、必ず閉域網及び Proxy サーバを経由して一つのインターネットゲートウェイから接続していた。なお、Microsoft 365 宛の通信は別経路として分離し、その他の一部の通信はデフォルトルートを経由して接続していた。

（1）　トラフィックの集中によるサービス品質の低下

この従来のネットワーク基盤における課題としては、クラウドサービスの利用増に伴うインターネット接続数及び通信量の増加が発生し、その結果として業務時間内にインターネットゲートウェイの回線逼迫が頻発し、業務効率の低下を招いていた。また、拠点（現場）からの接続においては、インターネットゲートウェイの回線逼迫のみならず、フレッツ網等から閉域網を経由しており、接続遅延が発生するなど通信品質としては決して良好な環境ではなかった。さらに、コロナ禍で急増したテレワークで利用するインターネット VPN もすべての通信を閉域網へ経由させるため、全社の回線逼迫に加え、折り返しの通信による遅延等も発生していた。

（2）　インターネットゲートウェイの運用上の課題

不適切な URL へのアクセスを阻止する仕組みである URL フィルタリングにおいて、通信経路を制御するファイル(以下、Pac ファイル)を複数用意し、利用用途に応じて利用者の Pac ファイルを変更させる運用となっており、利便性が高い状態ではなかった。また、突発的な通信量の増加に関しても、その原因となっているユーザを特定する場合には IP アドレスから特定する必要があったため、調査に時間を要していた。

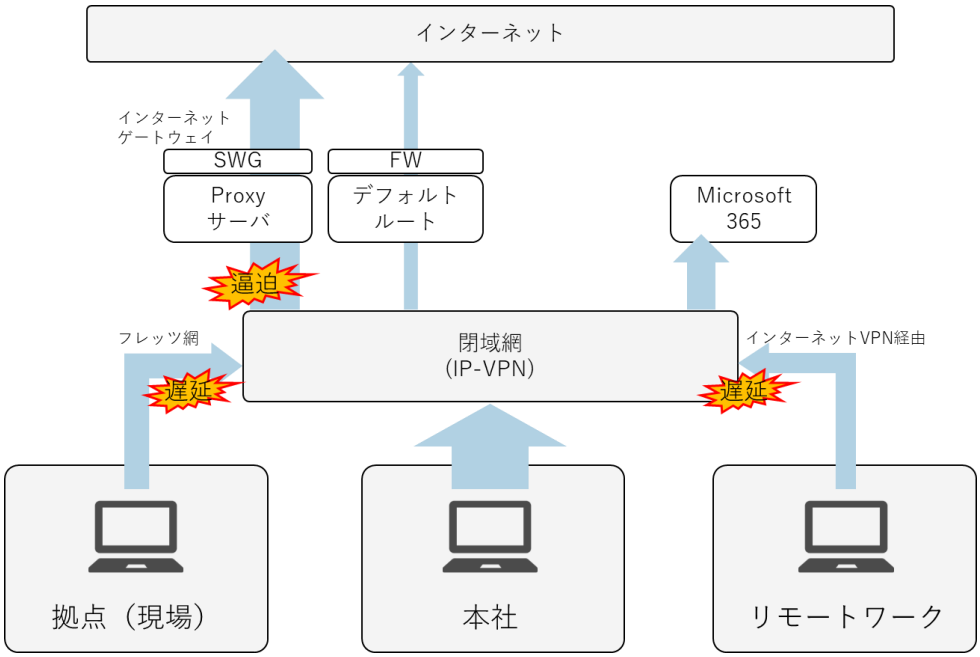

図　5　ネットワーク構成略図

３．２　ネットワーク基盤の課題に対する解決策

従来の課題に対する解決策として、クラウド SWG を導入することとした。本導入により、閉域網以外からの接続についても統一的な制御ポリシを適応できるネットワーク基盤を構築し、以下のような対策を実施した（図　6）。

・通信量の増加によって逼迫していたインターネットへの接続を、各拠点やリモートワークから直接クラウド SWG へ通信させる（ローカルブレイクアウト：LBO）ことで、URL フィルタリングや FireWall 等のセキュリティを担保するとともに、通信の分散化を図る。

・クラウド SWG は IDaaS と連携しユーザ認証を行うことで、URL フィルタリングポリシについてもユーザ・グループ単位での制御が可能となり、ログについてもユーザが紐づく形で取得を可能とする。

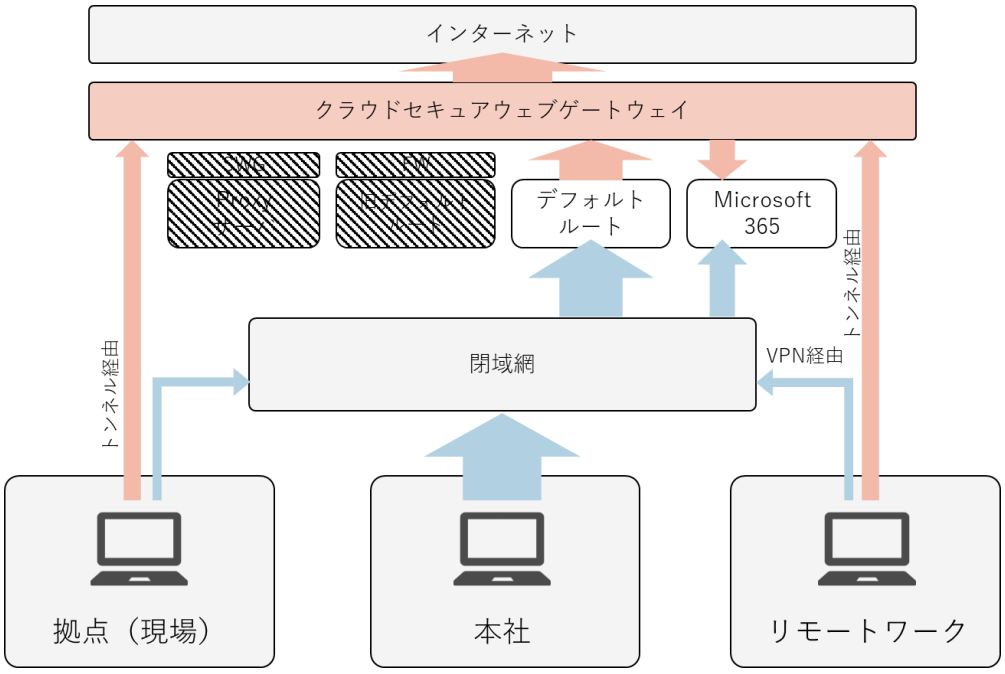

図　6　クラウド SWG 導入後のネットワーク構成略図

クラウドSWGを導入し、既存のインターネットゲートウェイからの移行・切替は以下の6ステップで実施した。なお、本実施の影響範囲は鹿島グループ全体に至るものであり、数十年に一度の大規模なネットワーク刷新となっている。

・クラウドSWGと閉域網の接続
・クラウドSWGへのURLフィルタリング、FireWallルールの移行
・接続する端末へのクライアントソフト・中間証明書の配布
・SaaSへのIPアドレスの登録変更
・通信経路の切替
・既存インターネットゲートウェイの廃止

（1）クラウドSWGと閉域網の接続

クラウドSWGへの移行を安全かつ確実に行うため、クラウドSWGを既存のインターネットゲートウェイとは別に新たなデータセンター内に構築し、クラウドSWGへは既存のインターネットゲートウェイとは異なる通信経路で接続する構成とした。

（2）クラウドSWGへのURLフィルタリング、FireWallルールの移行

続いて、クラウドSWGの設定として、既存インターネットゲートウェイに設定されているURLフィルタリングおよびFireWallルールの移行を実施した。

URLフィルタリングについて、既存インターネットゲートウェイとクラウドSWGではカテゴリフィルタの分類が大きく異なるため、ほぼ新規構築に近い形となった。個別に設定していたホワイトリストやブラックリスト等は移行できたが、カテゴリフィルタの分類が変わることで、今までアクセスできていたサイトにアクセスできなくなることを懸念したが、その全量を確認することは不可能であるため、通信経路切替え後にチューニング期間を設け対処する方針とした。

また、既存のインターネットゲートウェイでは一部のカテゴリに対して実施していたSSLインスペクション(クライアントとサーバ間の SSL 暗号化されたインターネット通信を捕捉し検査する機能)を、クラウドSWGでは一部を除きすべてのカテゴリに対して有効とすることとした。中間証明書の影響で利用できなくなるサービス等も考えられたため、一部の部署で先行切替による影響確認を行い、主要なシステムに関しては事前に検証を行った。

（3）接続する端末へのクライアントソフト・中間証明書の配布

クラウドSWGへ接続するには通信のトンネリングや通信経路の制御を実施するために、専用のクライアントソフトを各端末にインストールする必要があった。また、SSLインスペクションを実施するにあたり中間証明書も配布する必要があった。

社給パソコンに関しては、デバイス管理ツールを利用してクライアントソフトのインストーラを配信し、中間証明書を含む全台への配布・組込みを行った。

iPhoneやiPadについては、モバイルデバイス用の管理ツール(MDM[Mobile Device Management]ツール)にて中間証明書のみ配信を行った。

クラウドSWGは通常ユーザ認証を実施する必要があるため、利用者に紐づかないサーバの扱いである。しかし、サーバは閉域網での接続を前提としているため、クライアントソフトは導入せず、クラウドSWG側サーバが設置されるIPアドレスのセグメントを一括してユーザ認証やSSLインスペクションの除外設定を行う構成とした。

（4）SaaSへのIPアドレスの登録変更

既存インターネットゲートウェイからインターネットへ接続する際はすべての通信が固定のグローバル

IP アドレスから通信されていたが、クラウド SWG ではクラウド SWG が持つ動的なグローバル IP アドレスから通信する仕様となっている。そのため、送信元の IP アドレスで接続が制限を行っているサイトについては、クラウド SWG 側で接続先を登録し、その接続元として鹿島固有の IP アドレスとなるような転送設定を実施し、従来と同様に IP アドレス制限による接続を可能とした。シングルサインオン認証の仕組みの 1 つである SAML 認証に対応している一部の SaaS についてはこのタイミングで IP アドレス制限から IDaaS との連携に切り替えたものもあった。

なお、接続元 IP アドレス制限を行う際にはこれまで事前申請制としていたが、実際には未申請のままで利用されているケースもあり、経路の切替え後に想定していなかった未登録サイトへのアクセスエラー等の問合せが発生した。

（5）通信経路の切替え

まず、デフォルトルートの切替えを先行実施した。インターネットへの接続に関して、通常はプロキシ(Proxy サーバ)を経由して通信するため、デフォルトルートについては事前に夜間の切替え検証を実施したうえで全社一斉に切替えを行った。

一方、プロキシ経由の通信の切替えについては、IT 担当者や一部の部署などに対して影響範囲を区切りながらのスモールスタートとし、徐々に対象範囲を広げながら参照する Pac ファイルを変更することで経路の切替えを行った。FTP や SSH の通信もプロキシ経由であったが、クラウド SWG への切替えにあたっては各ソフトウェア上で設定変更を実施する必要があるため、利用者向けに変更内容を周知し対応した。

経路切替えは利用者への影響が大きいため、上記のように最新の注意を払いながら実施したが、切替え後には想定以上に様々な要因のアクセス不具合の問合せが発生した。URL フィルタリングや IP アドレス制限、中間証明書による影響等の様々な要因が考えられたものの、切り分けが難解なものも多く、切替え後 1～2 カ月はクラウド SWG のチューニングに追われる形となった。事前の検証等では確認しきれない用途も多々あるため、業務への影響を最小化するためには切替え後のフォローを十分な体制で臨む必要があった。

（6）既存インターネットゲートウェイの廃止

Pac ファイルによる通信経路の切替え後も直接プロキシを経由した通信が残っていたため、通信ログから通信元を特定し設定変更を促した。最終的には概ね全ての通信がクラウド SWG 経由に変更されたのを確認したうえで、Proxy サーバの DNS レコードを変更し、既存インターネットゲートウェイを廃止した。

４　セキュリティの強化

本章では、鹿島デジタルワークプレイスを支えるセキュリティの取り組みについて述べる。新たな働き方は場所や時間に依存しないことから、セキュリティインシデントも同様に時間や場所に依存せず発生することが見込まれるため、これまでのセキュリティ運用体制も見直していく必要がある。また、昨今のサイバー攻撃の動向を踏まえると、内への侵入を前提としたゼロデイ攻撃などの未知の脅威への対応といったセキュリティ対策の強化が必要であった。

４．１　従来のセキュリティ体制や対策における課題

新たな働き方の実現や昨今の脅威動向を鑑みると、セキュリティ体制や対策に関して以下のような問題が存在していた。

（1）　サイバー攻撃の進化に追従できていない

エンドポイントの主たるセキュリティ対策として、マルウェア対策やファイアウォールなどの機能を持ち、事前防御を目的とした EPP（Endpoint Protection Platform）を導入していた。しかしながら、以下の課題が存在していた。

- EPP は既知のマルウェアや脅威に対する防御を強みとしており、昨今増加してきているゼロデイ攻撃などの未知の脅威を防ぐことが難しい。
- EPP では、ファイルレス攻撃（攻撃プログラムがメモリ上で実行され、OS に標準搭載されている Power Shell 等の正規プログラムを用いる攻撃）を検知することが難しい。
- サイバーキルチェーン（※）で表されるサーバ攻撃過程を検知・把握することが難しく、特に「④エクスプロイト」「⑤インストール」時の不正な挙動を検知する新たな仕組みが必要である。

※サイバーキルチェーンとは、サイバー攻撃の一連の行動を「偵察」、「武器化」、「デリバリー」、「エクスプロイト」、「インストール」、「C&C」、「目的の実行」といった 7 つの段階に分けてモデル化したもので、その構造を理解することで、各フェーズの攻撃に有効な対策をとることができることになる。（図 7）。

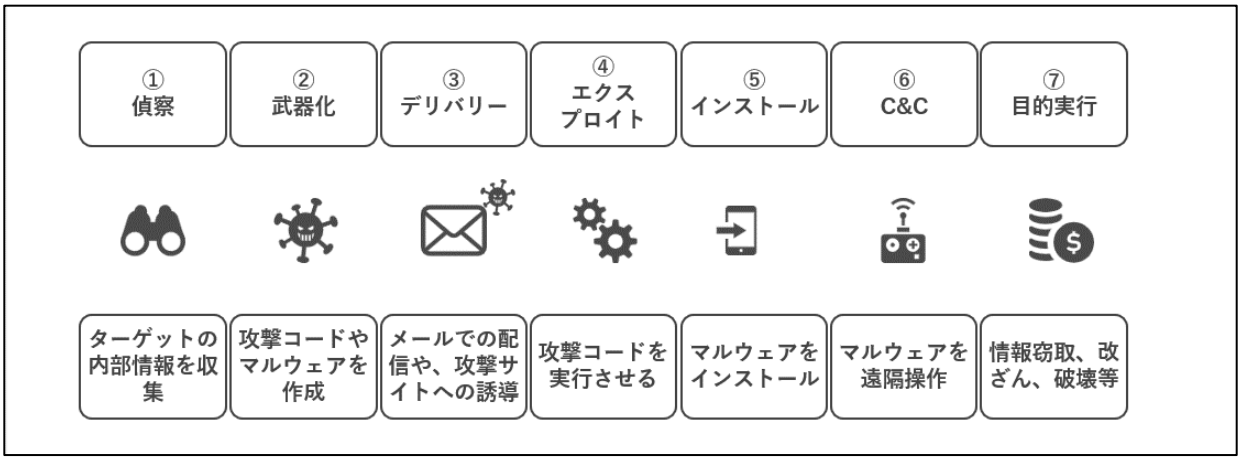

図 7　サイバーキルチェーン

（2）　再発防止策が講じきれない

EPP では、マルウェアなどの危険性のあるファイルの検知・ブロックは対処できるが、そのファイルがいつ作成され、どういった経路で侵入していたかを確認することが困難であった。そのため、適切な再発防止策を講じることができず、事象が再発する懸念が残ることになっている。

（3）　ユーザに依存したセキュリティ運用となっている

セキュリティインシデントが発生した際には、「検知・分析」、「初動対応・封じ込め」、「根絶・復旧」、「事

後対応」という４つのステップで対応している。その中の「封じ込め」においては、セキュリティ担当者がユーザに連絡して、ユーザ自身で当該端末をネットワークから切り離す運用となっていた。そのため、ユーザと連絡が取れない場合には封じ込めが実施できず、被害が拡大してしまう可能性があった。

なお、当社の働き方の特徴として、現場での業務時などではパソコンから離れて業務を行うタイミングも多く存在しているため、サイバー攻撃の検知から切り離しを実施するまでに時間を要する場合もあり、マルウェアの横感染が行われてしまうリスクがあった。

（４）　深夜や休日のアラートに気づきにくい

既存のセキュリティ運用は社内のセキュリティ担当者が業務時間内で対応していたため、２４時間３６５日の対応は取れていなかった。そのため、深夜帯や休日などセキュリティ担当者が不在の際には、セキュリティ製品のアラートに気付くのが遅れ、被害が拡大してしまう可能性があった。

４．２　セキュリティの課題に対する解決策

新たな働き方におけるセキュリティの確保及び昨今の脅威動向を踏まえ、セキュリティ対策や体制を以下のように刷新した。

（１）　サイバー攻撃の進化に追従したソリューションの導入

・既存の EPP に加え、NGAV（Next Generation Anti-Virus）を含む EDR（Endpoint Detection and Response）を新たに導入した。これにより各端末の振る舞いを常に監視し、未知の脅威やファイルレス攻撃を早期に検知することが可能となった（図　８）。

・当社が導入した EDR は MITRE ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）に準拠しているため、様々な攻撃者グループが使用する一般的な手法やテクニックを検知することが可能となっている。そのため、サイバーキルチェーンにおける各フェーズの振る舞いを検知・ブロックすることが可能となった。

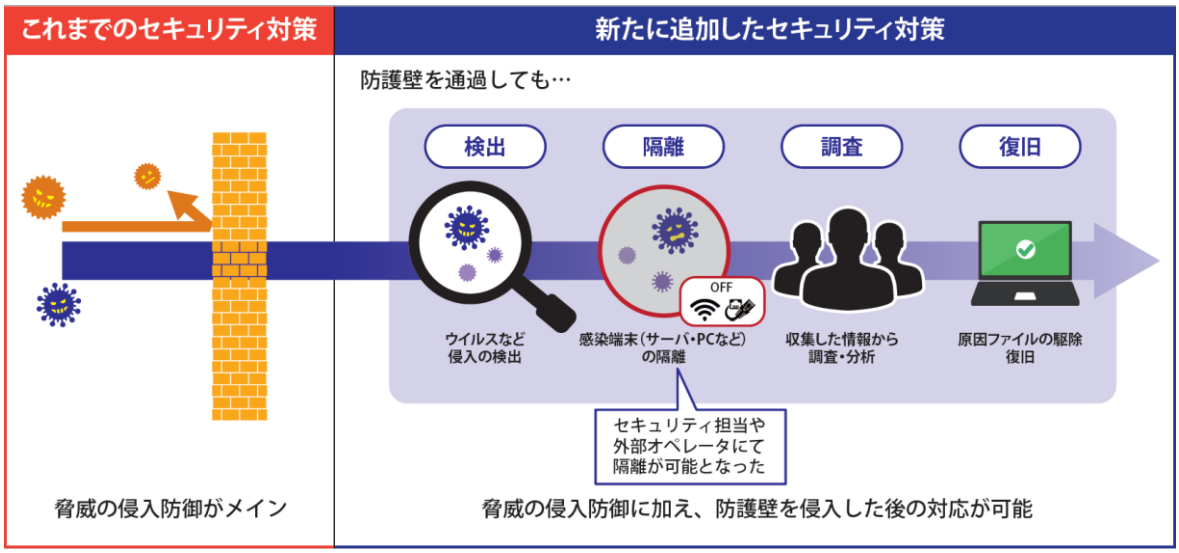

図　８　EDR 導入後のセキュリティ対策

（２）　侵入経路の可視化

・パソコンの操作ログを取得する製品を導入することで、ファイルの作成・削除といったファイル操作や USB メモリなどの外部デバイスの接続・切断などが可視化できるようになった。これにより侵入経路が特定でき、適切な再発防止策を講じることが出来るようになった。

・また、パソコンの操作ログを取得していることをユーザに公開することで、自身のパソコン操作に対する意識が芽生え、誤操作等による情報漏洩の抑止効果にも期待できた。

（３）　対応の迅速化（ユーザに依存しない切り離し）

・EDR ではセキュリティ管理者側で脅威のある端末をネットワークから切り離すことができる。そのため、検知後の迅速な対応が可能となり、被害拡大のリスクを極小化することができた。

（４）　監視体制の強化

・セキュリティオペレーションを専門とする外部サービス（外部 SOC）に監視及び EDR によるセキュリティ運用業務を委託した。これにより 24 時間 365 日監視を実現させるだけでなく、有事の際には EDR による早急な切り離しを対応することで感染拡大を防ぐことが出来ている。

・さらに運用業務の委託会社とは別に EDR ベンダ（セキュリティベンダ）も常時ログを監視しており、EDR の監視レベルの向上が図れている。

セキュリティ監視体制の改善前後を図示し比較すると以下のようになる（図　９）。

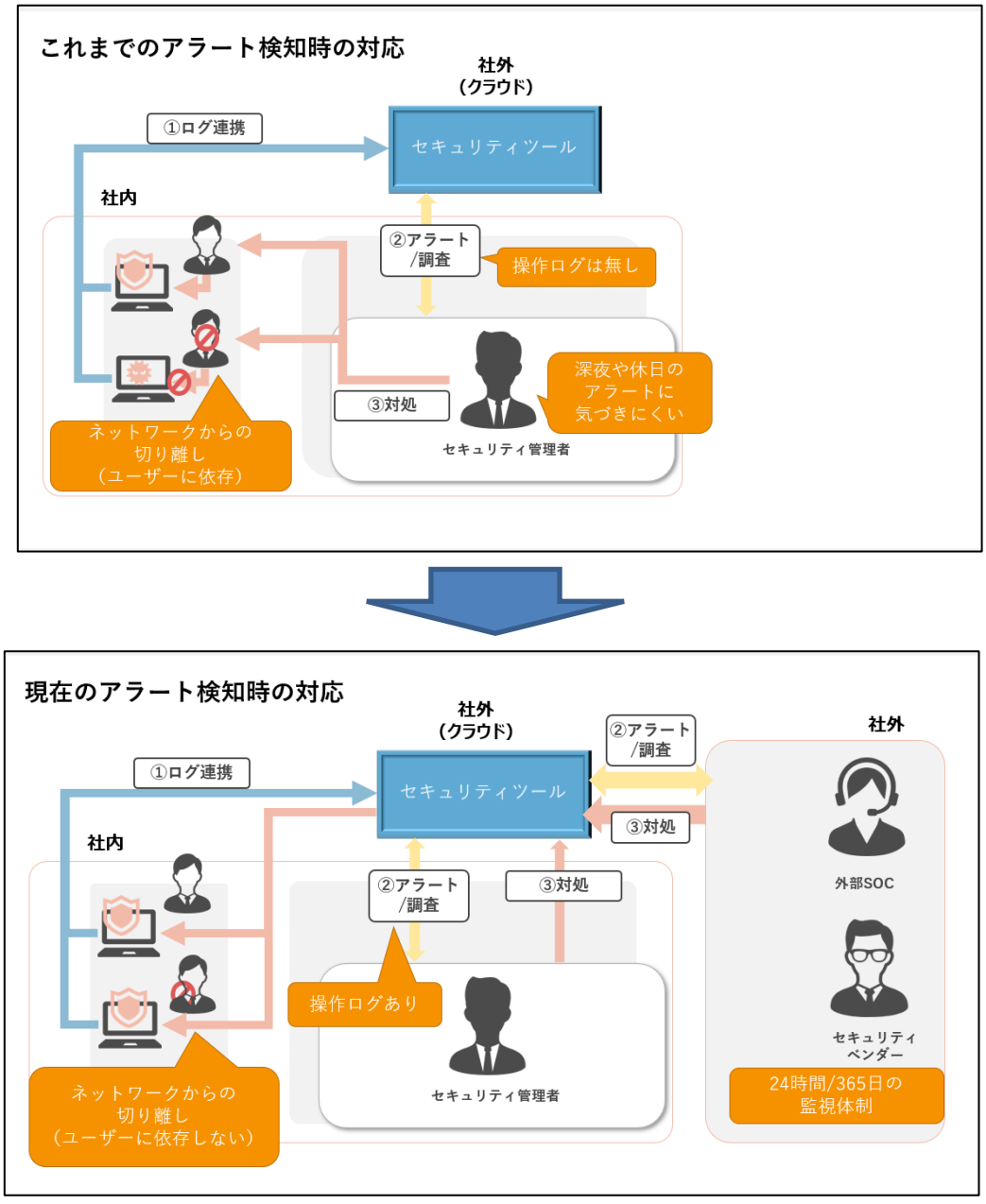

図　９　セキュリティ監視体制

５　有効性・評価

（１）　ネットワーク基盤の刷新

クラウド SWG を導入しネットワーク基盤に刷新したことで、従来の構成では実現できなかった拠点（現場）通信からのインターネット接続をローカルブレイクアウトできるようになった。従来の閉域網経由でインターネットへ接続した場合と比較した結果を示す。従来回線では特に業務時間である 8 時半から 12 時、13 時から 17 時半の時間帯において混雑していたが、ローカルブレイクアウトを実施した回線ではいずれの時間においても大幅に通信速度が向上していることがわかる（図　１０）。ローカルブレイクアウト回線に切り替えた拠点の社員からも、従来回線では Web サイトを開くのに時間を要したものが、Web サイトへのアクセスが早くなり、ストレスがかなり緩和されたという声も多く上がっている。LBO は 1 分 1 秒の改善効果が 2024 年問題に直接寄与する有効な手段であるとともに、今後もクラウド利用の急増や、3 次元モデルに設計・施工等で活用される情報を付加した BIM・CIM データ等のデータ量の増大は避けられない中で、トラフィック集中を継続的に回避できるネットワーク構成は、持続的な働き方の変化に追従できるソリューションであると評価している。

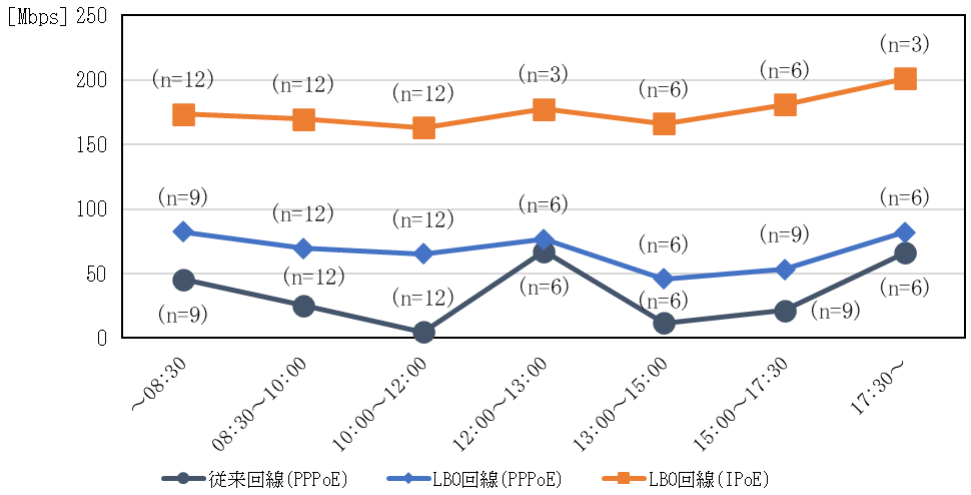

図　１０　拠点（現場）からのインターネット通信速度

（計測サイト　https://speedtest.gate02.ne.jp/を利用）

テレワーク時に利用する VPN サービスや仮想デスクトップ環境についてもインターネット接続をローカルブレイクアウトとし、セキュリティを保った状態での性能向上を実施した。また、クラウド SWG を利用する際には原則 IDaaS での認証を必須としているため、通信ログについてもユーザに紐づいた状態で確認ができるようになり、トラブルやインシデント発生時の調査が容易となった。さらに、管理画面の分析機能を用いることでトラフィックの状況等を即時に分析できるため、突発的な通信量増加に対する原因究明等に非常に有用であった。

（２）　セキュリティの強化

EDR の導入により、これまで検知することのできなかった脅威を捉え対応することが可能となったことは、当社のセキュリティレベル向上に大きく貢献したといえる（図　１１）。一方、業務で使用している正常な実行ファイルも脅威として検知（過検知）が多数発生していることが伺える。こうした過検知については都度詳細分析やユーザーヒアリングを行い、安全が確認できたものから検知除外設定を進めている。生産性を維持するためのセキュリティ対策が生産性を下げる要因とならないよう、過検知への対策は迅速確実に実施していく必要がある。

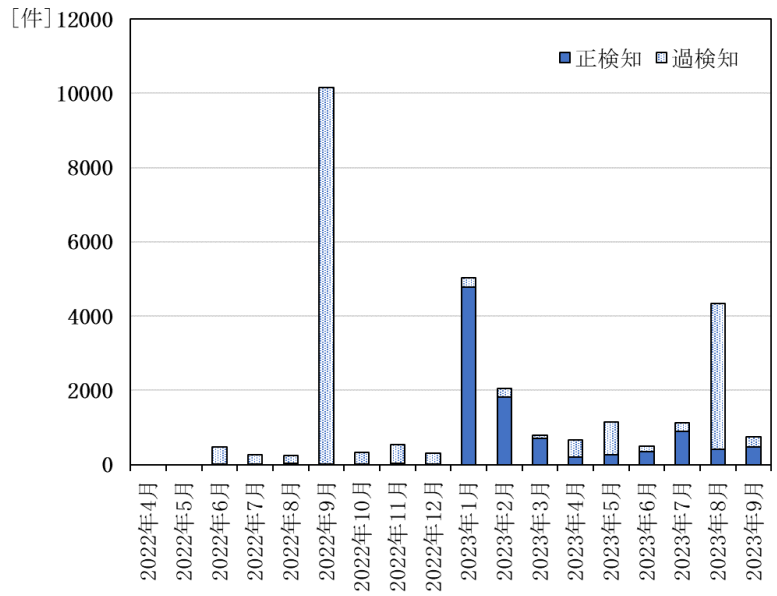

図　１１　鹿島建設における EDR 検知件数

（３）　在宅勤務などで発生するセキュリティリスクの低減

本稿では詳細は割愛したが、鹿島デジタルワークプレイスとしては仮想デスクトップ環境の構築・提供により、従来は認められなかった私用端末からの業務がセキュアに実現できる環境も整えている。この環境により、突発的な在宅勤務へ安全に対応することが可能となり、より柔軟な働き方への対応が可能となっている。セキュリティ面においても業務データを多量に含む社給端末の持ち運びによる紛失・盗難による情報漏洩リスクを低減させることができた。

また、IDaaS についてもクラウドサービスの ID 集約による利便性の向上だけでなく、ユーザ認証とデバイス認証の組み合わせによるアクセス制御等、ゼロトラストの中心となるための下準備を整えることができた。

６　まとめ・今後の課題

建設業においては担い手不足等の課題解決に対して更なる生産性の向上が求められており、その実現へ向けては今後も ICT の活用が期待されている。今回整備した鹿島デジタルワークプレイスの構築においてはネットワーク基盤とセキュリティ強化に関して大きな変革を遂げることとなった。現状では未だ一部閉域網に依存している構成ではあるが、今後はオンプレミスのシステムについてもクラウドシフトやクラウドリフトといった DX 化を進められ、それらを安全かつ効率的に利活用することを可能とするゼロトラストな環境へシフトチェンジすることで、現場の生産性が高まることを期待する。また、拠点の通信に関しては順次ローカルブレイクアウト構成に切替えを行い、今後のクラウドサービスの更なる増加に対しても柔軟に対応できる環境として展開を進めたい。

セキュリティに関して、今回は対処的対策として EDR に重きを置いた対応を進め、レジリエンス力を高められた。ただ、過検知を減らしつつ検知レベルを上げるといったチューニング（運用）も併せて行っていく必要があり、こうした「手段」としての EDR 運用を確実に遂行していかなければ、生産性の向上という「目的」の達成に影響が出てしまう。導入がゴールではなく更なる高みを目指していくには、導入意図を意識し続け運用を継続することが重要となる。そうして運用品質を維持した上で、従来のセキュリティ取り組みである予防的対策の強化や、セキュリティ要素の更なる可視化（IT 資産、権限、脆弱性など）を進めることで、企業セキュリティの底上げを行っていく所存である。

建設業という社会インフラ構築に携わる者として、今後も企業の生産性を高め、社会貢献に繋げていきたい。

参考文献

鳥羽瀬 世宇、内野 隆志、駒居 智之、田所 直樹、前川 和輝、ゼロトラスト移行のすゝめ、
https://www.IPa.go.jp/jinzai/ics/core_human_resource/final_project/2022/zero-trust-mgn.html、
2023 年 11 月 2 日閲覧
JAMES SADOWSKI、CASEY CHARRIER、2022 年、ゼロデイの悪用が加速度的に続く、
https://www.mandiant.jp/resources/blog/zero-days-exploited-2022、2023 年 11 月 2 日閲覧
井本 直樹、境界防御とゼロトラスト概説、情報の科学と技術、73 巻、3 号、2023 年 3 月 1 日、
一般社団法人情報科学技術協会

商標