安全なリモートワーク環境の提供

～ 大学のソフトウェア資産の安全な有効活用 ～

丹羽 量久[1)], 舘野 康彦[2)], 馬場 祐介[3)], 保坂 大輔[4)], 西 豪宏[5)]

1) 長崎大学 ICT 基盤センター
2) 株式会社内田洋行 システムズエンジニアリング事業部
3) トレンドマイクロ株式会社 公共ビジネス本部
4) Dropbox Japan 株式会社 ソリューションアーキテクト
5) シスコシステムズ合同会社 セキュリティ事業担当

k-niwa@nagasaki-u.ac.jp

Providing secure remote work environment

～ Safe and effective use of university software assets ～

NIWA Kazuhisa[1)], TATENO Yasuhiko[2)], BABA Yusuke[3)], HOSAKA Daisuke[4)], NISHI Takehiro[5)]

1) Center for Information and Communication Technology, Nagasaki Univ.
2) Systems Engineering Division, UCHIDA YOKO Co., Ltd.
3) Public Sector Business, Trend Micro Incorporated
4) Solution Architect, Dropbox Japan K.K.
5) Global Security Sales Organization, Cisco Systems G.K.

概要

新型コロナウイルス禍は、常時想定していなかった「リモートワーク」という仕事のスタイルを我々に注目させた。今春、準備期間がほとんどない状態でスタイルの変更を強いられ、大変な状況におかれた機関が数多く見受けられた一方で「リモートワーク」のスタイルを合理的に取り入れていく動きも確認された。このような状況から、今後はハイブリッド型の業務体系を採用する機関も現れると考えられる。本セッションでは、安心して「リモートワーク」に取り組むための課題について情報交換する。そして、セキュリティ対策に万全を期すための設備、環境、サービス等さまざまな面から「リモートワーク」を支援するソリューションについて紹介する。

1 はじめに

新型コロナウイルス感染症の罹患拡大の影響は我々の仕事のスタイルに大きな変化をもたらした。いつもどおりに出勤できず、自宅等での「リモートワーク」を強いられたため、キャンパス内での利用を想定している情報システムに外部から安全に接続できるように設備を緊急に整備した機関も多かったのではなかろうか。中には、こうした「リモートワーク」のスタイルを合理的に取り入れる動きも見られ、業務改善に繋がる可能性が示唆されたことになる。

一方、アメリカ合衆国の事例を基にした、日本の大学における職員の在宅勤務（テレワーク）の可能性についての報告[1]もなされており、大いに参考になる。

この企画セッションでは、安心して「リモートワーク」に取り組むための課題について情報交換する。そして、セキュリティ対策に万全を期すための設備、環境、サービス等さまざまな面から安全な「リモートワーク」を支援するソリューションについて取り上げる。

2 リモート端末管理のセキュリティアップデート（株式会社内田洋行）

リモートワーク導入の動きは、これまでにも「働き方改革」[2]の側面から多くの組織で検討され、一部で導入されてきたが、新型コロナウイルス禍は一気にその動きを加速させた。今後の社会情勢を見据えたとき、コロナ禍だけでなく、地震や水害等の災害を見据えた BCP 対策の一環として、ま

た東京五輪の際の働き方として、リモートワークは一過性のものではなく、広く深く浸透していくものと見込まれる。

従来から、当社は端末やソフトウェア管理、セキュリティ対策等を支援する管理ソリューションを提供してきたが、昨今のリモートワークの急速な導入を受け、大学や学校等の教育機関、自治体、企業等から、特にセキュリティ対策面でのリモートワーク端末の管理手法についての相談を受けることが増えてきた。ここでは、端末のセキュリティ対策の基本となる、OS やソフトウェアのアップデート管理について、組織における実践例を踏まえて解説する。

2.1 セキュリティ・アップデートの重要性と課題

さまざまなセキュリティ対策が施された組織内のネットワークに PC を接続して利用する場合に比べ、自宅等のホームネットワーク、携帯端末等を利用したテザリング、場合によっては公共の無線環境からの利用は、PC がむき出しの状態でネットワーク上の脅威にさらされることになる。標的型攻撃等、OS やソフトウェアの脆弱性をついた攻撃に対する最も重要で基本的な対策は、セキュリティパッチやアップデートを適切に適用していくことである。ところが、多くの組織では、組織ネットワーク接続時ならパッチ適用できるが、自宅等のインターネット越しでは不可ということが多い。また、Windows OS と Office 製品等のマイクロソフト社製品は自動適用が可能だが、その他のソフトウェア類は不可ということも深刻な課題である。総務省から公表されている「テレワークセキュリティガイドライン」[3]においても、『貸与用のテレワーク端末の OS 及びソフトウェアについて、アップデートを行い最新の状態に保つ』ことが、実施すべき対策として掲げられている。

2.2 セキュリティ・アップデート対策支援ソリューション

適切なパッチ適用管理は、脆弱性をつかれる前にその穴を直しておくという意味で、いわば「予防措置」的なセキュリティ対策である。リモートワーク端末は、攻撃を受けて利用不可となってしまった場合、組織ネットワーク外にあり且つ物理的に離れた場所にあることで、復旧にも時間を要し、業務継続に重大な支障をきたすだけでなく、情報漏えい等の事故可能性も一層高まる。

セキュリティ・アップデート対策支援ソリューション「ASSETBASE」は、これらの課題を解決し、リモートワーカーの安全で快適な PC 利用環境を維持することを強力に支援する。ASSETBASE が有する優れたセキュリティ・アップデート対策機能の主な特長は以下の通りである。

- Microsoft、Adobe、Java、Zoom など多くの製品のパッチに対応（図 1 参照）
- インターネット経由での配信に対応
- PC の診断用定義ファイルとともにパッチコンテンツを配信し、管理者負担を軽減
- パッチ間の相互関係も自動判断し、「必要となる前提パッチ」等も自動適用
- 各パッチの重要度や CVE 情報、各メーカーの公表 URL 等の情報も提供
- PC の未適用パッチの状況を自動識別、必要となるパッチのみを配信し適用
- PC への強制適用だけでなく、利用者に適用開始を委ねるプル型配信にも対応

図 1 サポート対象ソフトウェアの例

これらの特長ある機能を活用し、多くの組織で導入されているが、このところ特に重要性を増しているのが、Windows 10 のアップデート管理である。通常のセキュリティパッチに加え、半年に 1 回程度の機能更新があり、巨大なサイズのアップデートをいかに実施していくかが大きな課題となっている。ASSETBASE は、ネットワーク負荷の低減技術も独自の優れた機能を有しており、組織における適切な管理を支援する。

たとえば、ある教育委員会および配下の小中学校では、児童生徒が利用する 10,000 台を超えるタブレット PC に対し、パッチ適用管理を迅速に実施しており、パッチだけでなく、授業で利用するアプリ類の配信インストール等にも活用されている。またある大学では、教職員が使用する業務用 PC に対してのパッチ適用に活用されている。ある企業では、3,000 台超の PC に対し、リモートワーク等の組織外への接続を行う PC を含めた全台へのパッチ適用を実施しており、ネットワーク負荷低減技術により勤務時間中の適用実施が可能となっている。

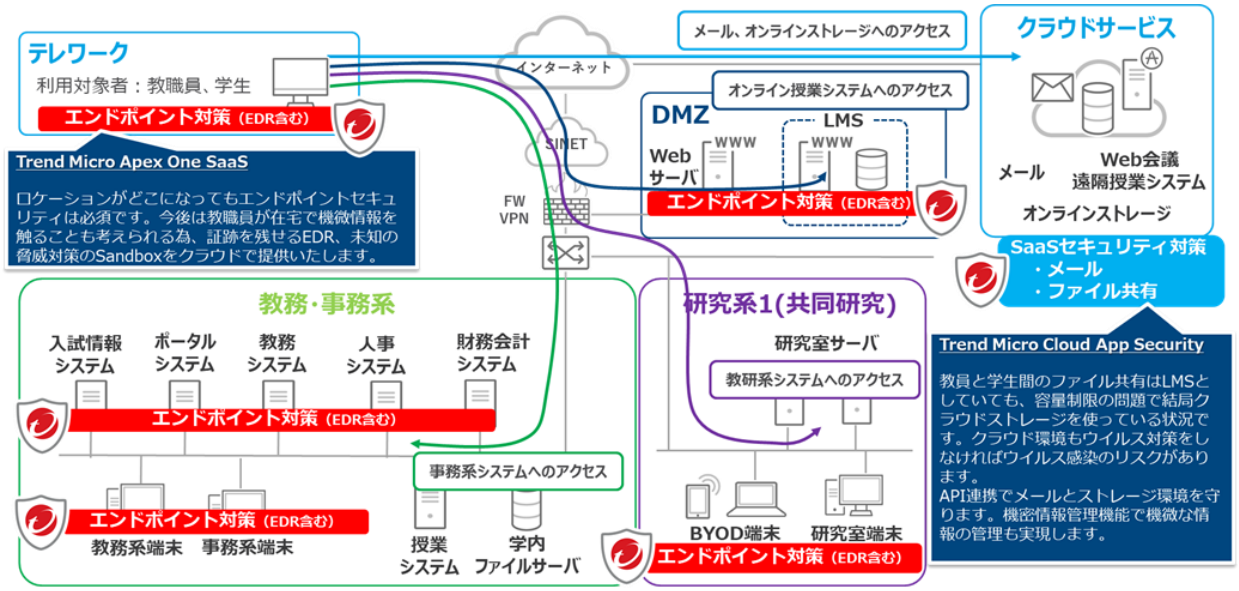

図 2 テレワーク環境の例

2.3 クラウド型マネージドサービス

ASSETBASE のパッチ適用管理機能では、インターネット経由での提供が可能という特性を活かし、パッチ配信の業務そのものを当社が請け負う形態、つまりマネージドサービスという形でこれら管理業務をサービスとして提供することも可能である。たとえば、ある教育委員会では、教職員が使用する校務用 PC を対象として、当社が有する ASSETBASE システムをクラウド型で提供し、パッチ適用管理業務を当社が運用している。

リモートワークは今後の日本社会においても広く浸透していくと考えられる。利用環境の整備の際には、上述したセキュリティ対策をご検討いただければ幸いである。

3 サイバーセキュリティの視点から（トレンドマイクロ株式会社）

新型コロナウイルスの影響で大学が求められる 2 点を取り上げて，サイバーセキュリティの視点から解説する。

3.1 授業環境の変化に伴うセキュリティ課題と対策

授業環境の変化がもたらした課題は、オンライン授業実施のサイジングが出来ていなかったことと、双方向コミュニケーションへの対応が必要となったことが考えられる。インターネット回線、VPN（Virtual Private Network）、サーバー等の増強と Web 会議サービスの契約によって、遠隔授業に必要なツールは揃えることができたが、サイバーセキュリティ上の課題への対応は今後の課題となると考える。教員と学生間でファイル共有を行う際等、LMS の容量制限の問題でセキュリティ対策が十分になされていないオンラインストレージ等を利用している事例が散見される。最近はそれらを経由したマルウェアの感染被害が出ており、利用するサービスの特定やセキュリティ対策を検討する必要がある。また、機微な情報を保護する観点で、これまでのオンプレミス環境ではデータの特定と管理が困難であったが、最近、オンラインストレージ上の機密情報管理が実現できるようになった。次に当社がこの機能を提供するクラウド環境（ストレージ、メール）のセキュリティと機密情報管理の Cloud App Security を紹介する。

3.2 業務継続のためのリモート接続環境整備に伴うセキュリティ課題と対策

業務継続のためのリモート接続環境整備についての課題としては、学外でできる仕事が極めて限定されていることである。緊急事態宣言解除と共に出勤させた大学もある一方で、これを機にテレワーク環境の整備を進める大学もある。たとえば、VPN 接続環境を構築したり、VPN 接続数を増やしたりすることにより、全教職員が利用可能な環境を用意した大学がある。

さらに、サイバーセキュリティ上の課題への対応も必要である。エンドポイントセキュリティは場所に関係なく必須だが、学外での機微情報の取り扱いを許可する場合は高度サイバー攻撃に備えて証跡を残せる環境や未知の脅威対策を整備することが重要だ。これまではゲートウェイで各種対

策を行ってきたが、通信の SSL 化が進み、働く場所が多様になると、ゲートウェイのセキュリティ対策だけでは対応できないケースが出てきている。たとえば、エンドポイントにクラウド技術を活用して EDR（Endpoint Detection and Response）や Sandbox 等の技術を実装していくことにより、最適なテレワーク対策を講じることができると考えられる。

本セッションでは、エンドポイントへの EPP・EDR・Sandbox 技術をクラウドで提供する Apex One SaaS を紹介する。また、オンラインで受講できる教育ツールとして、オンライン版インシデント対応ボードゲーム（大学版）、PC やサーバーのフォレンジック調査演習についても取り上げる。

4 オンライン環境下におけるコラボレーションを支援するスマートワークスペース（Dropbox Japan 株式会社）

4.1 テレワークに関する実態調査の概要

2020 年 4 月から 5 月にかけて、全国のオフィスワーカー有識者約 1,000 名を対象としたインターネット調査を実施した。本調査の目的は、新型コロナウイルス感染症の拡大防止に向けたテレワークの急速な導入を受けて、2019 年 10 月頃に行った調査から、デジタルツール活用に関する企業の意識・実態がどのように変化したのかを明らかにすることにあった。

4.2 調査結果から見る課題とニーズ

今春の調査結果から、テレワーク実施企業の多くでは、「長時間労働の是正」「健康増進（ワークライフバランス）」「生産性の向上」等のメリットを享受していることが確認できた。一方で、完全なテレワーク体制に移行できていない企業では、「社内の必要なファイルにアクセスするのが不便だった」「印鑑を押す書類があった」等の様々な課題が浮き彫りとなった。

また、テレワーク環境に求められる IT システムとしては、クラウドストレージ、ビデオ会議システム、チャットシステムに加えて、コラボレーションを円滑に行うための「共同オンライン作業場システム」が多くの企業で求められていることも判明した。

4.3 教育機関との共通点：オンライン環境下におけるコラボレーション

本調査の主な対象は民間企業のオフィスワーカーであったが、昨今のコロナ禍において、多くの教育機関が「学生向けのオンライン授業の運営」や「教職員のリモートワーク環境の整備」等様々な施策に取り組んでおり、従事する活動は異なるものの、オンライン環境下におけるコラボレーションの必要性という観点においては、多数の共通点を見出すことができる。

4.4 スマートワークスペース

本調査結果において必要性が明らかったとなった「共同オンライン作業場システム」の一つの解として「スマートワークスペース」を提唱する。具体的には、ファイルの安全な保管と既存ワークフローを最適化する Dropbox Business やドキュメントの管理・共有により作業効率を向上させる Dropbox Paper がこのようなオンライン環境下においてこそ威力を発揮し、教員と学生のセキュアなファイル共有や、学生同士の活発なコラボレーションを実現する。本セッションでは、コロナ禍以前より Dropbox Business を用いて新キャンパス開設を機に BYOD（Bring Your Own Device；私的デバイス活用）の基盤となるファイル共有環境を構築した教育機関の事例や、ファイルサーバーと VPN では対応が難しかった学外からの情報アクセスニーズへのソリューションとして Dropbox Business を導入した事例を紹介する。

4.5 利便性を高める電子署名ソリューション

2020 年より国内での提供を正式に開始した電子署名ソリューション、HelloSign（ハローサイン）と組み合わせることにより、さらにワークフローの効率化を実現できる。例えば、例年 3 月から 4 月にかけて、膨大な人数の新入生から入学誓約書、規則遵守同意書等の各種署名を回収する業務に対して、セキュアに電子化できる HelloSign を適用することにより、大幅な業務効率化が実現できる。セッションでは、これらに加えて、従来では FAX で行っていた資材発注業務の電子化等、ワークフローに的確に合わせた具体的な活用方法を交えて紹介する。

5 安全なハイブリッド授業・テレワーク環境を提供するクラウドセキュリティ（シスコシステムズ合同会社）

急加速するハイブリッド授業の展開においてサイバー攻撃は拡大しており、当社はこの問題に対処するための全方位的なセキュリティ・ポートフ

ォリオを提供している。

5.1 クラウドサービスの推進によって「ID」の保護が重要な要素になる

従来は物理的な「場」をある種の認証の要素として利用できていた。クラウド利用が進むことで、教職員学生の物理的なアクセス場所は自由になっており、クラウド上では正規のユーザかどうかの識別は多くの場合ユーザ名・パスワード等のクレデンシャルに依存する。このクレデンシャルが漏洩等侵害を受けた場合に容易に不当なサービスを許すことになってしまう。

これを防ぐために、クラウド型多要素認証の仕組みとして Cisco Duo を提供している。アメリカ合衆国の Internet2 でも多くの大学が利用をしており、日本でも提供開始とともに利用者数を伸ばしている。

5.2 在宅にいるユーザであっても VPN なしで高速な学習環境を提供

在宅ユーザは Cisco Duo により、VPN を経由せずにゼロトラストベースでのアクセスが可能となり、安全かつ高速に学内のサイトにアクセスし、リモートデスクトップ環境（Remote Desktop Protocol と Virtual Desktop Infrastructure）等も利用できる。従来型のセキュリティでは HTTPS 通信を一度解読し、中身を検査する等を行っていたことが、高コスト化や遅延増を産む原因になっていた。この問題を回避するため Cisco Umbrella ではクラウドにて DNS レイヤーにおけるセキュリティ対策を基本提供し、加えてセキュア Web、ファイアウォール、クラウドアプリの利用制限やシャドー IT の可視化・制御に有効な CASB（Cloud Access Security Broker）等を提供している。なお、リリース直後より AXIES 年次大会の会場インフラに Cisco Umbrella を提供し、マルウェア通信の阻害等を成功させてきた。この Cisco Umbrella は国内大学での導入実績も増えている。

5.3 マルウェアの防御に加えて、マルウェアの挙動も可視化

マルウェアの侵入防御の根本的対策としては、侵入時の形跡を特定し、追跡する。またマルウェアの侵入後の挙動も把握することが重要となる。

当社が提供するエンドポイントの対策（EDR：Endpoint Detection and Response）の Cisco Advanced Malware Protection（AMP）for Endpoints はこれらの機能に加え、侵入時にはマルウェアと認識されなかったものが、後にマルウェアと判定された場合にも即座にローカルマシン上から排除する機構を有しており、高い防御率と低い誤検知率を同時に兼ね備え、常時診断・常時対処が実現している。

5.4 包括的なセキュリティ監視の可視化・自動化が必要

攻撃手法が高度・多様化した結果、防御方法も様々な手段が存在し、当社が提供するものを含め多様なポートフォリオでの対応が求められている。一方、マルチベンダーでのセキュリティ対策は、監視が複雑となるため、アラートの見過ごし等により甚大なセキュリティリスクがもたらされることがある。この課題に対応するため、当社では統合モニタリングソリューション Secure-X により、セキュリティ調査・修復の可視化、自動化、簡素化を実現した。Secure-X は、当社セキュリティ製品のお客様に無償で提供している。

6 おわりに

インターネット経由で安全にアクセスするために必要となるセキュリティ対策について、さまざまな観点から情報を提供した。安心して「リモートワーク」に取り組むための環境構築の参考になれば幸いである。

参考文献

[1] 石村 史、大学における職員の在宅勤務（テレワーク）の可能性、海外学術動向レポート集、日本学術振興会、2020. https://www-overseas-news.jsps.go.jp/wp/wp-content/uploads/2020/04/04.19.ishimura.fumi_.sfo_.pdf（2020 年 10 月 15 日閲覧）

[2] 厚生労働省、「働き方改革」の実現に向けて、2020. https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000148322.html（2020 年 10 月 15 日閲覧）

[3] 総務省、テレワークセキュリティガイドライン（第 4 版）、2018. https://www.soumu.go.jp/main_content/000545372.pdf（2020 年 10 月 15 日閲覧）