特集論文

三菱電機グループの端末一元管理

増冨勇輔*
甲斐　道*
廣瀬論也**

Consolidated Terminal Management of MITSUBISHI ELECTRIC Group

Yusuke Masutomi, Toru Kai, Nobunari Hirose

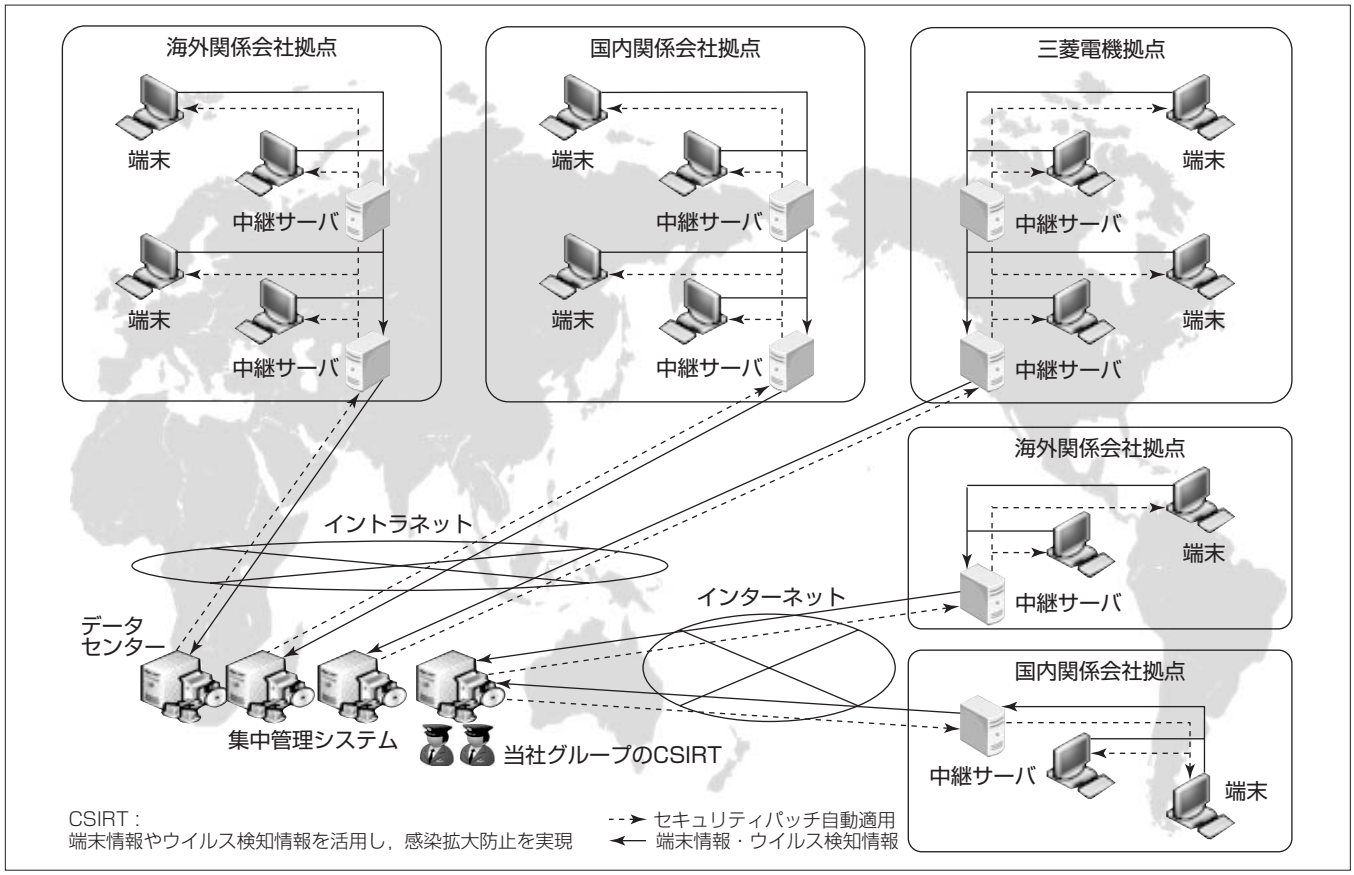
要　旨

三菱電機及び国内・海外関係会社（以下“当社グループ”という。）は，三菱電機グループネットワーク（以下“イントラネット”という。）環境で，セキュアな情報管理を目的に，当社グループ全体で統一的な認証IDの利用を可能とするグループ認証基盤を構築するなど，情報システムセキュリティの強化に取り組んでいる(1)。

標的型攻撃，Web改ざん，サービス不能攻撃などのサイバー攻撃のうち，特に標的型攻撃が日々高度化・巧妙化する中で，当社は責任あるグローバル企業として，グループ一体となった標的型攻撃対策が必要不可欠である。

当社グループは，端末セキュリティ強化，インターネット接続点の出入口対策，情報管理，従業員教育などを実施している。しかし，当社グループの更なるセキュリティレベル向上のためには，統一的な標的型攻撃対策が必要である。そのため，当社グループの端末を集中して管理し，セキュリティレベルの向上を実現する端末一元管理を展開している。

端末一元管理の端末情報収集やウイルス検知情報収集等の機能を他の標的型攻撃対策と連携させることで，当社グループ全体の標的型攻撃対策を強化する。また，当社グループのCSIRT（Computer Security Incident Response Team）が端末情報やウイルス検知情報を活用することで，当社グループ全体のセキュリティレベルを向上させる。



端末一元管理のシステム構成

当社グループ各社に配置する中継サーバと，データセンターに配置する集中管理システムをイントラネット又はインターネット経由で連携させる。集中管理システムは中継サーバ経由で端末にセキュリティパッチの自動適用を実行し，感染予防を実現する。また，集中管理システムが中継サーバ経由で収集した端末情報やウイルス検知情報を当社グループのCSIRTが活用することで，感染拡大を防止する。

*三菱電機㈱ IT戦略室　**三菱電機インフォメーションシステムズ㈱

1. まえがき

標的型攻撃は，日々高度化・巧妙化しながら特定企業や団体の機密情報などを窃取する。

当社グループは，端末セキュリティ強化，インターネット接続点の出入口対策，情報管理，従業員教育など，多角的に標的型攻撃対策を講じている。しかし，現状の標的型攻撃対策を維持・運用するだけではなく，これらを網羅的に見直し，日々進化する新たな脅威にも備えることが重要である。そのため，当社グループ全体のセキュリティレベル向上のための基盤となる端末一元管理を展開中である。

本稿ではこの端末一元管理について述べる。

2. サイバー攻撃

2.1 サイバー攻撃の種類[2]

サイバー攻撃は大きく次の3つに分類され，インターネット通信を介して実行されることが多い。そのためインターネット通信を利用する，あらゆる企業・団体・個人はサイバー攻撃を受ける可能性がある。

⑴ 標的型攻撃

特定の企業や団体などを攻撃の対象とする。なりすましメールに添付されたファイルなどからウイルスを送り込み，組織内の機密情報，知的財産，顧客データなどを狙う攻撃であり，日々高度化・巧妙化している。

⑵ Web改ざん

Webサイトに侵入して内容を書き換え，クレジットカード情報などの個人情報窃取や，不正サイトへ誘導する攻撃である。

⑶ サービス不能攻撃

大量のアクセスや不正パケットを送り付け，サーバやネットワークで提供するサービスを機能不全にする攻撃である。

2.2 標的型攻撃の手法

標的型攻撃は，次の攻撃手法を用いて標的者に攻撃をする(**図1**)。

①攻撃者がなりすましメールを標的者に送付

②標的者が添付ファイルを開き，ウイルスに感染

③ウイルスが攻撃者のサーバへのアクセス経路を確保

④ウイルスが内部を調査し，新たなウイルスを送り込む

⑤新たなウイルスが情報を窃取

当社グループはこれらの攻撃手法を用いる標的型攻撃に対して多角的に対策しつつ，高度化する攻撃に対して網羅的に見直しを実施している。

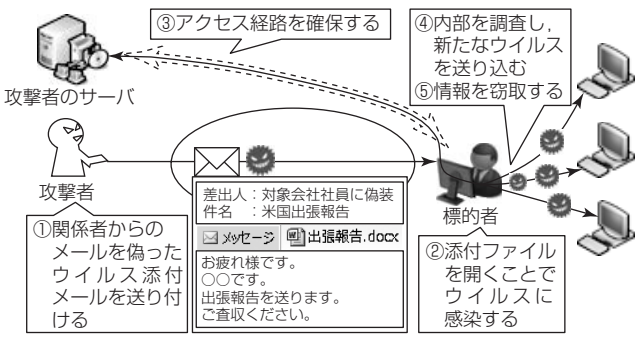


図1．標的型攻撃の攻撃手法

3. 三菱電機グループの標的型攻撃対策

標的型攻撃は，なりすましメール等を使ってウイルスを潜入させた後，ウイルスを遠隔操作して機密情報窃取等の被害を拡散させる。

グループ会社間をイントラネットで接続している場合，いずれかの1社が攻撃を受けると，イントラネットを介して連鎖的に他社へ被害が波及する。これは当社グループでも起こり得ることであり，適切な対応を講じる必要がある。しかし，攻撃が非常に高度・巧妙であるため単一の対策で対応するのは不可能であり，攻撃段階に合わせた複数の対策が必要になる。

3.1 標的型攻撃対策の全体像

当社グループでは，標的型攻撃対策として次の5つの施策に取り組んでいる(**図2**)。

⑴ 端末一元管理

当社グループのCSIRTが，当社グループ全端末のセキュリティ対策状況を一元的に管理する。

⑵ 端末セキュリティ強化

当社グループのCSIRTが，世の中の情報セキュリティインシデントの発生状況などを確認し，当社グループの全端末に対してセキュリティ強化設定を一斉に適用する。

⑶ インターネット接続点の出入口対策

当社グループのCSIRTが，インターネットを出入する通信を監視して不正な通信を遮断する。

⑷ 情報管理

情報の自動暗号化とともに，セキュリティの強固な情報保管庫を活用して情報の流出を防ぐ。

⑸ 従業員教育

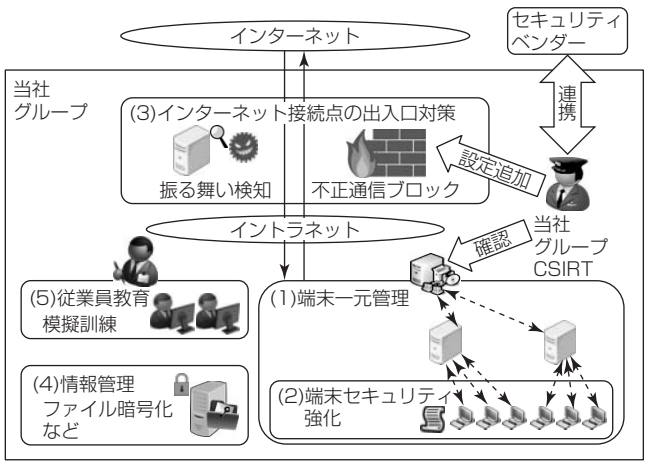


図2．標的型攻撃対策の全体像

e-learningや，標的型攻撃を模倣したなりすましメール送付などの模擬訓練を当社グループの従業員に対して実施する。

日々進化する新たな脅威に備えるため，この５つの対策を網羅的に見直し，強化を推進している。このうち，端末のセキュリティ対策状況を管理する端末一元管理は，当社グループ全体のセキュリティレベル向上のための基盤となる施策である。

3.2　端末一元管理の目的

端末一元管理は，当社グループが講じている標的型攻撃対策を強化するために，これまで以上の感染予防と感染拡大防止の実現を目的としている。

⑴　感染予防

標的型攻撃対策は，始めに，ウイルスへの感染を防止する対策が必要になる。そのためには，日々発見されるソフトウェアの脆弱(ぜいじゃく)性に対してすみやかに対処する必要がある。

現在，多くの企業でWindows(注1)の脆弱性に対しては，Microsoft社のWSUS(Windows Server Update Services)を活用してセキュリティパッチを適用している。

一方，Java(注2)やAdobe Acrobat Reader(注3)，Adobe Flash Player(注3)等の非Microsoft系のソフトウェアへの対処は，個々の端末ユーザーの手動更新に依存せざるを得ない環境であることが多く，統一的な対処や対処状況の一元管理が困難な場合が多い。

これを解決するため，当社グループ全体に端末一元管理を展開し，これまでに実施しているWindowsのセキュリティパッチ自動適用に加え，非Microsoft系のソフトウェア脆弱性に対しても統一的な対処を可能にし，セキュリティパッチの適用遅れや適用漏れを防止する。

⑵　感染拡大防止

標的型攻撃の高度化・巧妙化に伴い，感染予防対策を施した場合でもウイルス感染を完全に防止することは困難である。

したがって，ウイルス感染後の対策も重要となるため，当社グループのCSIRTは，メールやインターネットの通信を監視し，ウイルス感染端末が発信する通常とは異なる通信の挙動を日々確認している。

現在も，通常とは異なる通信を確認した場合，ウイルス感染端末を特定することで感染拡大を防止しているが，当社グループ全体の端末情報を一元的に管理する端末一元管理を展開することでウイルス感染端末の特定にかかる時間の短縮を可能とし，これまで以上の感染拡大防止を実現する。

(注１)　Windowsは，Microsoft Corp. の登録商標である。
(注２)　Javaは，Oracle Corp. の登録商標である。
(注３)　Adobe Acrobat Reader，Adobe Flash Playerは，Adobe Systems Inc. の登録商標である。

4.　端末一元管理のシステム

端末一元管理のシステム設計上の考慮点，感染予防，感染拡大防止の実現方法について述べる。

4.1　システム設計上の考慮点

当社グループの全端末に対してセキュリティパッチを効率的に配信することと，当社グループのどの端末が攻撃されても，すみやかに検知し，迅速かつ継続的な対応が可能となるよう，IPアドレスやホスト名等の端末情報を集中管理するシステムを構築した。

データセンターに集中管理システムを配置し，拠点側に設置する中継サーバと連携する構成とした。この構成をとる上での考慮点を次に述べる(**図３**)。

⑴　インターネット経由での接続

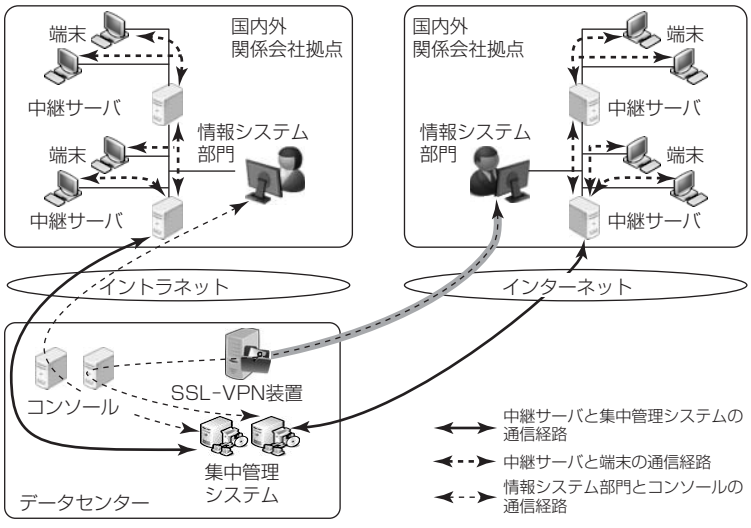
業務の特性上，イントラネットに接続していない当社グループ会社が存在する。これらの会社に対しても端末一元管理システムが利用できるよう，イントラネット経由だけでなく，インターネット経由でも中継サーバと集中管理システムを安全に通信させることを可能にした。

⑵　耐障害性

中継サーバは集中管理システムからセキュリティパッチを受信し，かつ端末から端末情報を受信する。当社グループ各社に中継サーバを設置することで，集中管理システムとの通信が途絶えた場合でも，中継サーバが端末にセキュリティパッチを継続的に配信することや，端末から最新の端末情報を収集することを可能にした。

⑶　端末情報の保護

このシステムは，当社グループ各社の情報システム部門から集中管理システムに直接アクセスできない仕組みにしている。具体的には，当社グループ各社の情報システム部門は，データセンターに設置しているコンソールと呼ばれ



SSL-VPN：Secure Socket Layer Virtual Private Network

図３．システム構成概要と考慮点

るサブシステム経由で集中管理システムにアクセスする。これによって，情報システム部門の端末に情報を残さず，仮に情報システム部門の端末がウイルスに感染した場合でも情報が窃取されない仕組みとしており，収集した端末情報に対する安全性を高めている。

4.2　感染予防対策

4.2.1　端末設定情報確認

当社グループ各社の端末にインストールされているソフトウェアやレジストリ値などの設定情報を収集し，当社グループのCSIRTがセキュリティベンダーなどから収集したセキュリティ情報と照らし合わせることで，新たなセキュリティリスクに対して迅速に対処することを可能とした。

また，セキュリティパッチ未適用の端末情報をデータセンターで一元的に管理し，端末情報を当社グループのCSIRT及び各社の情報システム部門が確認することで，社内のセキュリティパッチ適用を促し，適用を徹底することを可能とした。

4.2.2　セキュリティパッチ適用までの時間短縮

当社グループの端末に対して最新のセキュリティパッチを短期間に自動適用することで脆弱性に対処するが，セキュリティパッチが公開されてから端末へ適用するまでの時間短縮を実現するため，プロセスを最適化した(**図4**)。

ベンダーから新たなセキュリティパッチが配布された際，端末一元管理運用部門(以下“運用部門”という。)がOSや広く利用されている基本的なソフトウェアの起動などの動作確認を実施する。

当社グループ各社の情報システム部門は，運用部門が実施する動作確認を省略して，各社が持つ業務アプリケーションなどに対してのみ影響の有無を検証する。

また，端末利用者が手動で適用していた非Microsoft系ソフトウェアのセキュリティパッチを端末一元管理を利用して適用することで，適用までの時間短縮を可能とした。

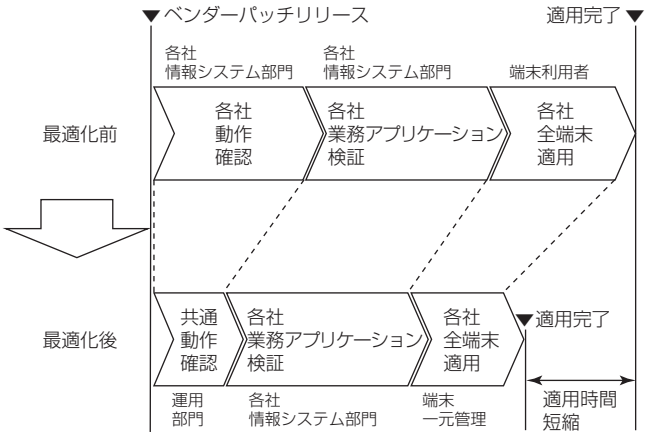


図4．セキュリティパッチ適用プロセスの最適化

4.2.3　管理対象外端末検知

管理対象外端末がネットワークに接続されたことを検知する仕組みを提供する。管理対象外端末を発見した場合，該当ネットワークを管理・管轄する部門と連携し，管理対象外端末をネットワークから切り離すとともに情報の漏えいや感染の有無を迅速に確認することを可能とした。

4.3　感染拡大防止対策

4.3.1　端末情報収集

標的型攻撃は，標的者の端末をウイルスに感染させる。これに対して，当社グループのCSIRTが感染端末を特定し，感染端末を管轄する当社グループ各社と連携することでネットワークから隔離する等の対応を実施している。

この対応には，端末の状態を正確かつ迅速に把握することが重要であるが，従来はグループ各社が個別に端末情報を収集していたため端末情報が統一されておらず，セキュリティ事案発生時の感染端末特定や対策完了確認までに多くの時間がかかっていた。

当社グループ各社の端末情報を一元的に管理する端末一元管理を展開することで，感染端末の正確かつ迅速な特定を実現し，感染拡大防止を可能とした。

4.3.2　ウイルス検知情報収集

当社グループのCSIRTなどが新たなウイルス感染を確認した場合，セキュリティ対策ベンダーからパターンファイルの提供を受ける。

このパターンファイルを当社グループ各社が利用しているウイルス対策ソフトに反映し最新化することで，新たなウイルス検知情報の収集と感染範囲の把握を可能とする。

これによって，適切なウイルス駆除方式の立案と効率的なウイルス駆除を実現し，感染拡大防止を可能とした。

5.　む　す　び

標的型攻撃が高度化・巧妙化する中，従来の標的型攻撃対策を維持・運用するだけではなく，新たな脅威を防止する継続的な取組みが必要である。

標的型攻撃対策の一環として，感染予防と感染拡大防止を目的とする端末一元管理を展開しているが，今後は従業員の故意や過失によって発生する情報セキュリティインシデントの防止策としても活用を広げる。

参　考　文　献

(1)　長尾　剛，ほか：グループ認証基盤の構築，三菱電機技報，**86**，No.12，679～682（2012）
(2)　JVN iPedia：脆弱性対策情報データベース
http://jvndb.jvn.jp/index.html