特集論文

サイバー攻撃に備えた情報セキュリティーに対する取組み

Information Security Measures Preparing for Cyber Attacks

山本紳介* *Shinsuke Yamamoto*
大松史生* *Fumio Omatsu*
松石里加子* *Rikako Matsuishi*
古澤康一* *Koichi Furusawa*

*情報セキュリティ統括室

要　旨

企業にとってサイバー攻撃は，年々，大きな脅威になってきている。一方で，テレワークやクラウド活用事業の増加などに伴い，業務や事業環境が変化し，DX(デジタルトランスフォーメーション)を推進するためには，安心・安全にデータを活用できる環境が必要になってきている。

三菱電機グループの情報セキュリティー施策を統括する“情報セキュリティ統括室”では，技術的な側面だけではなく組織的及び人的な側面からもセキュリティーを確保できるように取り組んでいる。具体的には，高度な一元管理や多層防御などのサイバー攻撃対策，緊急時の即応体制の構築・整備，企業風土の醸成や従業員のリテラシー向上を重視した情報セキュリティー教育などを実施している。これによって，安心・安全にデータが活用できる環境を当社グループへ展開している。

1. ま え が き

当社グループでは，サイバーセキュリティーが重要な経営問題であることを認識し，2020年４月に当社グループの情報セキュリティー施策を統括する“情報セキュリティ統括室”を設置した。巧妙かつ多様化するサイバー攻撃に対して当社グループ全体で対抗するため，情報セキュリティ統括室が中心となって様々な取組みを実施している。

本稿では，サイバー攻撃に備えて情報セキュリティーに対して実施している取組みについて述べる。

2. サイバー攻撃対策の全体像

当社グループでは，クラウドサービスの利用，テレワークの普及に伴い，巧妙かつ多様化するサイバー攻撃への対策として，ネットワークや端末，サーバー(クラウド)の一元管理と，“多層防御”の導入に取り組んでいる。多層防御によって，サイバー攻撃の防御，不審な兆候及び侵入の検知を可能にして，さらに即時に対応する体制を整えることで，被害を防止するとともに最小化している。

またオフィスのほか，テレワーク，出張先からのアクセスによる業務に対応するため，認証を一元的に管理している。さらに，常に外部から多くの脅威にさらされているインターネット公開ウェブサイトについては，セキュリティーレベルを保つために当社が認定したウェブサイトだけを公開している。

セキュリティーの一元管理と即時に対応する体制に関する概要を**図１**に示す。

万が一拠点側で攻撃者に侵入された場合(①)でも，セキュリティーインフラ一元管理基盤で侵入を検知(②)し，検知結果についてはCSIRTへ通知する。CSIRTでは侵入による被害を特定し，必要な設定変更を拠点側へ指示(③)することによって，被害の拡大を防止する。

3. サイバー攻撃対策の具体的な取組み

3.1 多 層 防 御

当社グループでは，多層防御として“ネットワーク”“端末”“サーバー(クラウド)”の３階層の技術的なセキュリティー対策を実施している(**図２**)。

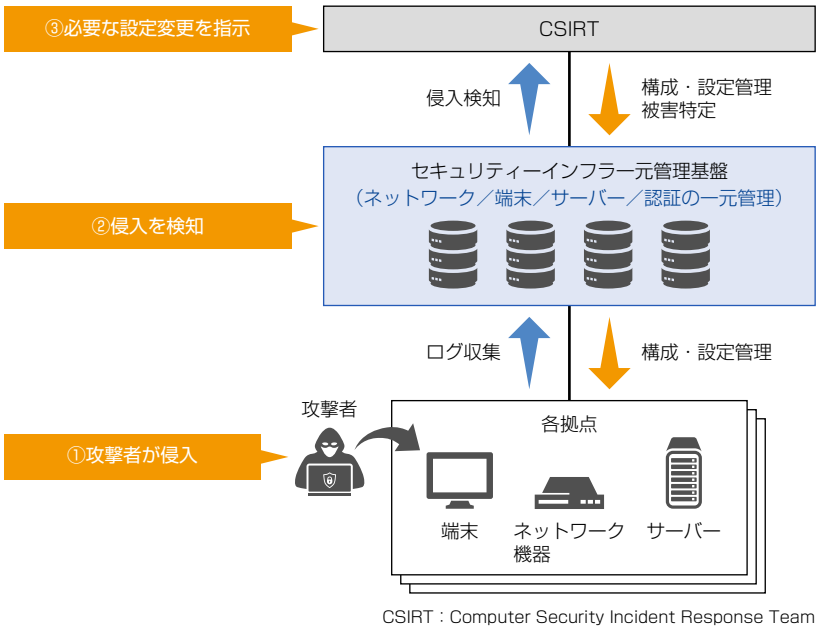

図１−セキュリティーの一元管理と即時に対応する体制

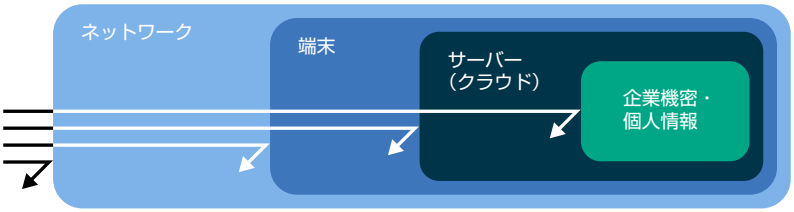

図２−多層防御

ネットワークでのセキュリティー対策では，インターネットと社内ネットワークの接続点に様々なセキュリティー対策機器を配置し，メールやウェブなどの通信を制御・監視することで，外部から社内への不正なアクセスやマルウエアの侵入を遮断している。社内から外部へ情報が漏えいすることを防ぐため，今後もこの通信遮断機能を強化していく。

端末のセキュリティー対策では，マルウエア対策ソフトウエアによるマルウエアの検知・駆除や，ソフトウエアの脆弱(ぜいじゃく)性を修正するセキュリティーパッチの適用を行う。この対策によって，端末へのマルウエア感染を防いで，攻撃を抑制するとともに，被害を局所化する。これを確実なものにするため端末を一元的に管理し，対策漏れを防止している。また，不審な振る舞いを検知するEDR(Endpoint Detection and Response)ソフトウエアを全端末に配備し，対策を強化している。さらに，二つ以上の要素の認証を組み合わせる多要素認証を導入し，セキュリティー対策を強固にしている。

クラウドの活用が進むサーバーに対しては，脆弱性の定期的な診断のほか，通信やクラウドの運用を監視している。これによって，重要な情報が格納されるサーバー(クラウド)で堅牢(けんろう)な環境を維持している。

サーバーやクラウドに格納される企業機密・個人情報に対しては，“最小権限の原則”(注1)(1)に基づいたアクセス制御と暗号化を適用する。これらの情報の管理については，規則の整備と徹底，従業員教育，点検活動も併せて実施している。

(注１)　間違いや無断使用の被害を防ぐために“大切な情報や機能にアクセスする権限は，必要最小限のものしか与えるべきではない”という原則。

3. 2　緊急即応体制

当社グループでは，MELCO(Mitsubishi Electric Corporation)−CSIRTを設置し，サイバー攻撃を常時監視するとともに，事案発生時に即時対応できる体制を構築している。また，従来は対応が不十分であった国内外の関係会社に対する監視体制も整備を進めている(**図３**)。

この体制の下，**3. 1節**に述べた通信監視による不審挙動の検知によってサイバー攻撃をいち早く見つけて遮断するとともに，端末側ではマルウエアの検知情報や端末のセキュリティー対策状況などを収集・把握し，分析・対策に生かせるよ

うにしている。万が一，事案が発生した場合は，この仕組みを駆使することで即座に被害状況を把握し，迅速で適切な対処・復旧によって被害を可能な限り抑えて，その後，事案を詳細に分析し恒久対策を実施する。

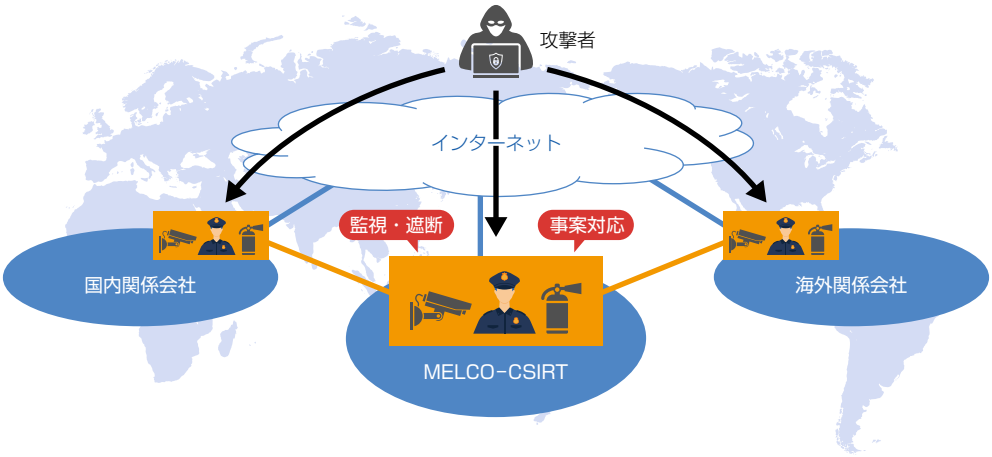

図3- MELCO-CSIRT

3.3　テレワーク時のセキュリティー対策

出張時のモバイル勤務以外にも，在宅勤務やサテライトオフィスの利用など，多様化するワークスタイルに対応してテレワークの活用が進んでいる。また近年では，新型コロナウイルス感染症(COVID-19)への対策として在宅勤務の機会が大幅に増加し，テレワークは一般的な働き方として浸透してきている。

一方で，ネットワークやクラウドの活用によって業務環境も多様化し，社内システムとインターネットとの境界を防御する従来のセキュリティー対策では不十分になっている。そのため，VPN(仮想専用通信網)接続によって通信を暗号化し安全性を確保するとともに，多要素認証も導入してより強固なセキュリティー対策を行っている。

当社グループは，在宅勤務，サテライトオフィス勤務，モバイル勤務(出張)の全てに対して，サイバー攻撃から防御するためのセキュリティー対策を引き続き強化していく。

3.4　インターネット公開ウェブサイトの管理

当社グループでは，過去に発生した不正アクセスによる事案を契機に，インターネット公開ウェブサイトのセキュリティーレベルを保つために当社が認定したものだけを公開することをルール化している。

事前にセキュリティー検査を実施してセキュリティーホールを解消したウェブサイトでなければ，公開を許可しない。またインターネット上の公開ウェブサイトを定期的に点検することで管理状況を把握し，不要なウェブサイトの廃止のほか，攻撃の進化とともにセキュリティー対策が不十分になったウェブサイトについてはセキュリティー対策を強化している。

4. 情報セキュリティーの教育

当社では，企業機密・個人情報の適切な取扱いを徹底する企業風土の醸成や，従業員のリテラシー向上に努めている。機密等級に応じたファイルのサーバー保管や暗号化などの具体的な安全管理措置や，不審メールへの適切な対処を従業員が確実に実施できるよう，次の教育プログラムを実施している。

(1)　全従業員への教育

約5万人の全従業員などを対象に情報セキュリティーの教育をeラーニングで実施(年1回)し，当社の方針，情報漏えい事案の概況，個人情報保護関連法令，不正競争防止法，一人一人が認識すべき安全管理措置(組織的・人的・技術的・物理的)を周知徹底している。また，テレワークの急増やクラウド活用による業務形態・環境の変化に伴い，適宜，従業員向けの教育資料を展開している。

(2)　キャリアパスに沿った教育

新入社員，新任課長，個人情報資産管理者，運営に関わる事務局向けの研修などを通して，各階層や担当業務で求められる役割を果たすために必要な企業機密管理・個人情報保護の教育を実施している。

⑶　不審メール対処予行演習

サイバー攻撃対策として，当社では役員を含む全従業員を対象に“不審メール対処予行演習”を実施し，定期的に不審メールへの対処方法を確認しており，国内関係会社の従業員も同演習に参加できるようにしている。海外関係会社については，地域担当部門の下，米州，欧州，アジアでそれぞれの地域の実情に合わせて予行演習を実施している。

⑷　その他の個別教育

海外赴任者に対しては赴任前研修の中で，企業機密管理・個人情報保護に関する海外でのリスク，海外での情報漏えい事案の事例について教育している。

5. 継続的な改善活動

これまで述べた情報セキュリティーに対する各種の取組みについて，年度初めに年度方針に基づく計画を策定(Plan)し，各種情報セキュリティー施策の展開や従業員への教育を行った(Do)上で，情報セキュリティーの運用状況を点検(Check)し，その結果を基に施策などを見直す(Act)ことで，情報セキュリティーレベルのスパイラルアップを図っている。

6. OTセキュリティーに対する取組み

インターネットなど外部との接点を持たないクローズな環境で稼働していた工場の現場にも，IoT(Internet of Things)やDX，テレワークといった様々な新技術，環境変化の流れが押し寄せてきており，工場もオープンな環境で稼働するようになってきた。その結果，今まで無縁であったサイバー攻撃の脅威が工場にまで及び，近年，様々なところで工場停止など重大な被害が多発するようになってきた。

当社では，工場をサイバー攻撃から守る社内体制として，情報セキュリティ統括室にOT(Operational Technology)セキュリティーの専門グループを設置し，当社工場に対するサイバーセキュリティー対策の強化に取り組んでいる。

具体的には，Purdue(パーデュー)参照モデル(注2)をベースに，工場内のシステムや機器の設置位置を論理的に層別し，各層(Layer)に対するセキュリティー要件を明確化・文書化したものを基に，各工場でセキュリティー対策を推進している。セキュリティー要件は，IEC 62443-2-1(注3)などの規格を参考にしている。

(注２)　産業用制御システムを機能階層ごとに論理的に区分し，セキュリティーを確保すべきIT／OTネットワークゾーンのマップを提示できるようにする。

(注３)　国際標準化団体IEC(International Electrotechnical Commission)から発行されており，制御システムでのセキュリティーガイドラインとして幅広く活用されている。その中でもIEC62443-2のシリーズは工場向けの要件がまとめられている。

7. む　す　び

情報セキュリティ統括室で実施している情報セキュリティーに対する取組みは，サイバー攻撃の防御，不審な兆候及び侵入の検知を可能にする。また，そうした取組みを継続的に改善することで，当社グループ全体のセキュリティー向上に寄与している。

今後も巧妙かつ多様化するサイバー攻撃に対して，多面的にサイバーセキュリティー対策を強化し，安心・安全な社会の実現に貢献していく。

参 考 文 献

⑴　独立行政法人 情報処理推進機構：安心相談窓口だより 2021年度(アプリのアクセス権限を確認しましょう)(2021)
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210914.html