特集論文

OTネットワークセキュリティー機器“MELWALL”

OT Network Security Device "MELWALL"

高須賀史和*
Fumikazu Takasuka
木村有佑*
Yusuke Kimura

*インフォメーションシステム統括事業部

要　旨

近年，サイバー攻撃の対象として工場や発電所といったプラントやインフラの制御システムが狙われる事例が増えており，設備そのものや，サービスの提供や安全を維持するためのシステムを攻撃されることが懸念されている(1)。

三菱電機では，FA，電力，公共インフラなど幅広い分野での制御システムの知見や技術・経験を生かして，アセスメント・コンサル，セキュリティー対策導入，運用保守までをワンストップで提供するOT(Operational Technology)セキュリティーソリューションサービスを提供している。

OTネットワークセキュリティー対策製品の一つとして当社が提供するOTネットワークセキュリティー機器“MELWALL(メルウオール)”は，既存のネットワーク構成を変更せずにOTネットワークを論理的に分割してセキュリティー脅威の感染拡大防止を実現する。

1. ま え が き

従来，サイバー攻撃の対象は企業の業務システムやウェブサイトなどの情報システムが主体であり，これらのシステムが持つ機密情報を狙う攻撃が主流であった。しかし近年は，工場や発電所といったプラントやインフラの制御に用いられる制御システムが狙われ始めており，設備そのものや，サービスの提供や安全を維持するためのシステムを攻撃されることが懸念されている(1)。実際に大きな被害を受けた事例も存在する(**表1**)。

表1．制御系システムへのサイバー攻撃事例

年	業界／分野	概要
2015	電力	ウクライナ国内の電力施設でのマルウエア感染。首都キーウ北部とその周辺地域で停電が発生した。手動運用に切り替えて，30分以内に電力供給が再開され，約1時間15分後に完全に復電した。
2018	製造（半導体）	台湾の世界的半導体チップメーカーでのランサムウエア感染。重要なコンピュータがWannaCryの亜種に感染し，複数の工場で生産ラインが停止した。影響の大きかった工場では生産再開に約3日かかった。
2022	製造（自動車）	日本の自動車メーカーに自動車の内外装部品を生産する企業でマルウエア被害が発生。これがきっかけで，自動車メーカーの14工場28ラインが停止。約13,000台の生産が見送られることになった。

また，これまで独立したネットワーク内で運用されていることで一定の安全を確保してきた制御システムは，近年のIoT(Internet of Things)及びDX(Digital Transformation)の推進によってITシステムやクラウドへ接続されるようになることで，サイバー攻撃を受けるリスクが高まっている。そのため，制御システムの稼働維持を守りつつDXを推進するには，“つながる”ことによる新たな脅威への対応として，制御系(OT)へのセキュリティー対策導入が必要になる。

企業のセキュリティー対策は，情報系(IT)への対策は普及しつつある。一方で，ITネットワークにつながるOT環境への対策は，その規模や特性によって異なる技術課題があるため，セキュリティー対策が普及していない。

例えば，製造業の多くは工場内に設備を追加導入していく中でネットワーク構成が複雑になり，配線やIP(Internet Protocol)アドレスの変更が必要な境界分離等のセキュリティー対策が難しくなっている。また，保護対象のOT機器は，生産稼働を止められない，又は制御装置に対するサポートOSが更新されないためにOS更新やパッチ適用が行いにくく，サポート切れの古いOSのまま使用されているなど，機器本体への対策が施せない場合もある。

ほかにもOT環境ではIT環境と比べて資産，通信，セキュリティー対策状況などが把握されていない，またOT環境への対策製品導入後もインシデント発生後どのように対処すべきか現場では分からないなど運用面での課題もある。

こうした背景を受けて，当社ではアセスメント・コンサルティングから，ネットワーク・エンドポイントなどへの対策導入，運用保守までをワンストップで提供するOTセキュリティーソリューションサービスを提供している。

当社ではFA，電力，公共設備向けの制御システムの導入，運用・保守を行っている一方，自社の製品，工場，ITシステムへのセキュリティー対策として，製品・サービスのセキュリティー品質に対応する社内体制であるPSIRT(Product Security Incident Response Team)，情報セキュリティーインシデントに対する監視及び発生時に対応する組織であるCSIRT(Computer Security Incident Response Team)を構築するなど取組みを進めている。こうしたIT，OTそれぞれの技術，知見を活用し，このソリューションサービスを提供する。

本稿では，当社が提供するOTネットワークセキュリティー対策製品からMELWALL[2]についてその特長を述べる(**図1**)。MELWALLはOTネットワークの内部での論理的分割(セグメンテーション)をするネットワーク装置であり，OT環境ならではの課題を意識した機能を持っている。

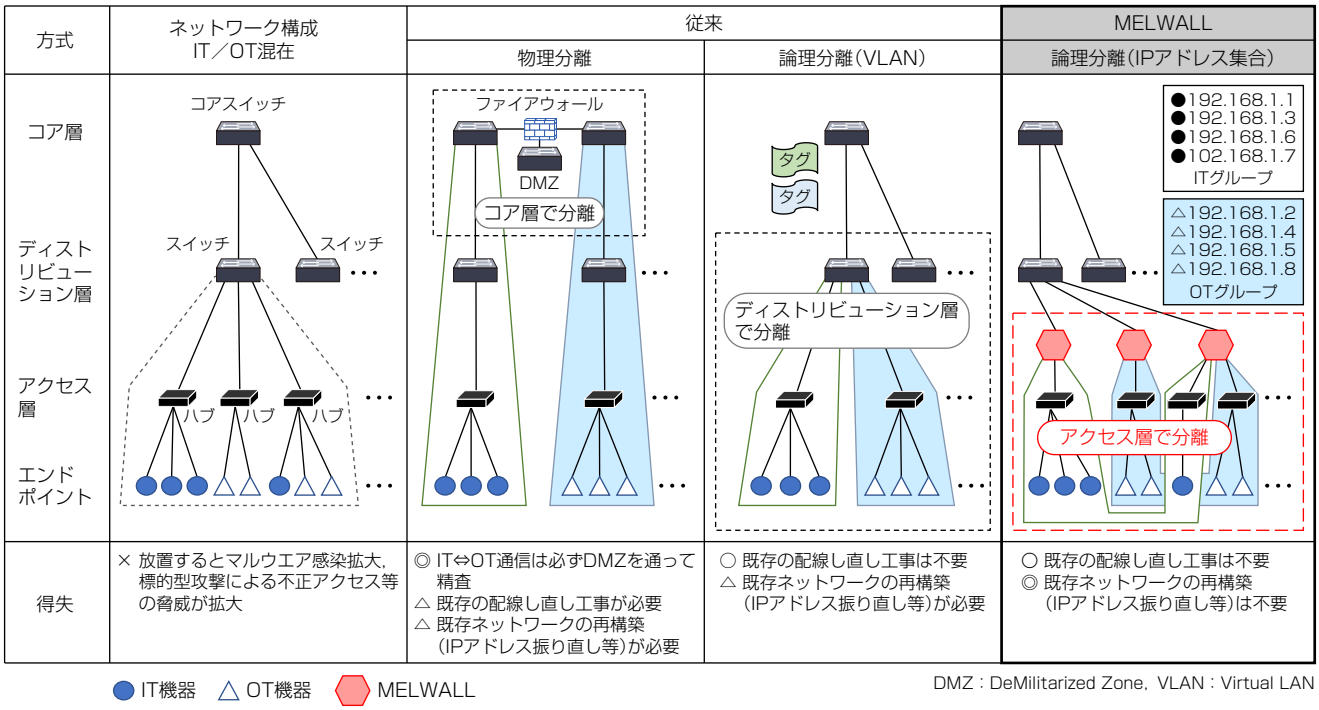

図1．MELWALLの特長

以降**2章**ではOTネットワークでの脅威対策の課題，**3章**では課題を解決するMELWALLの機能，**4章**では導入による効果を実装例とともに述べる。

2．OTネットワークでの脅威対策の課題

OTネットワークへの効果的なセキュリティー対策の一つとして，ネットワークのセグメンテーションが挙げられる。セグメンテーションとは，ネットワークをより小さな個別のネットワークに分割することであり，セグメントごとに固有の通信ポリシーなどを設定することによって，ネットワーク全体のセキュリティーレベルを上げることができる。

セグメンテーションの大きなメリットの一つは，サイバー攻撃を受けた際の被害を局所的に抑えられる可能性があることである。分割されていないフラットなネットワークでは，攻撃者に侵入された場合にネットワーク内のあらゆるIT／OT機器にアクセス可能になり，ネットワーク全体へのウイルス感染，重要な生産データの窃取や生産プログラムの改ざんなど，被害が拡大するおそれがある。また被害の拡大状況を把握することが困難であり，対応に遅れが生じてしまう。

セグメンテーションによって分割されたネットワーク間で不正な通信を遮断するような通信ポリシーが設定されていれば，攻撃者に侵入された場合でも他のセグメントへアクセスできず，一つのセグメントという小さな範囲で被害を抑えられる可能性がある。また被害拡大状況もセグメント単位で判断できる。

セグメンテーションの実施方法としては，ファイアウォールを境界点に設置し，適切な通信だけを通して，不適切な通信は通さないように通信ポリシーを設定する方法が一般的である。しかし，ファイアウォールをOTネットワークに導入する際には次の三つの課題がある。

⑴　ネットワーク構成変更(IPアドレス変更など)が必要

ファイアウォールでのセグメンテーションの場合，VLANを構築する場合が多く，ネットワークに接続するOT機器に対して設定変更作業(IPアドレスの振り直しなど)が必要になり，コストがかかるほか，機器の稼働停止を伴うリスクがある。

⑵　通信制御の設定・運用に膨大な負荷がかかる

従来のファイアウォールでは，IPアドレスベースでポリシー設定をするものが多く，導入時や設定変更時に作業負荷が大きくなる。また，設定者に十分な知識やスキルがないと設定ミスが生じてしまう可能性が高い。

⑶　OT環境内に存在する機器を把握しきれていない

これはIoT機器などの導入を進めている企業に多く見受けられるが，OT環境にある機器を把握しきれておらず，セグメンテーション実施のための十分な情報がないため導入が難しいといった課題がある。

当社では，これらOT環境特有の課題を解決するOTネットワークセキュリティー機器MELWALLを開発している。

3．MELWALLの特長

MELWALLはOTセキュリティーソリューションで提供される製品の一つであり，OTネットワークのセグメンテーションを実現する。MELWALLは**２章**に示す課題を解決する特長的な機能を備えており，特許権も取得(特許第7086257号，特許第7209791号，特許第7209792号)している。また直感的に操作できるGUI(Graphical User Interface)を充実させ，通信ポリシーの設定や運用でのユーザーの作業負荷を軽減する設計になっている。

この章ではMELWALLの特長的な機能について述べる。

3.1　グループ単位での通信制御機能

この機能は**２章**の課題⑴を解決するものである。MELWALLでは，任意のIPアドレスを任意のグループに所属させ，そのグループ間での通信制御を可能にする。そのため機器のIPアドレスを変更することなくMELWALLを導入でき，通信制御を実現できる。またグループ単位で通信の許可／拒否を設定するため，IPアドレス単位でポリシー設定をするよりもポリシー数が膨大になりにくく，設定や管理の作業負荷を軽減する。

3.2　グループ単位でのポリシー設定方式

この機能は**２章**の課題⑵を解決するものである。MELWALLはグループ単位の通信制御を設定するためのGUIに大きな特長を持つ。**図２**に示すポリシー設定画面では，送信元／送信先グループやプロトコル，ポート番号，通信の許可／拒否，ログ取得の有無などが簡単なボタン操作で指定できる。また，グループ単位でのポリシー作成であることからポリシー数が膨大になることなく，導入・運用時にユーザーの作業負荷を軽減できる設計になっている。

図２．MELWALLのポリシー設定画面

3.3　未登録のエンドポイントの検知・グループ分け

この機能は**２章**の課題⑶を解決するものである。MELWALLは自身と同一のネットワーク内に存在する機器を検知す

る機能を持っている。検知した機器がMELWALLに登録されていないIPアドレスを持つ場合，一度UNKNOWN(未分類)グループとして未分類エンドポイント画面に一覧表示される(**図3**)。

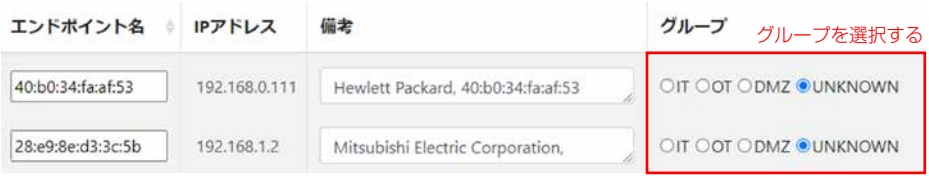

図3．MELWALLの未分類エンドポイント一覧画面

未分類エンドポイント一覧画面ではIPアドレス，MAC(Media Access Control)アドレス，メーカー名などが表示されており，ユーザーがエンドポイントの特定をしやすいようになっている。ユーザーはこれらの情報から，エンドポイントを適切なグループに分類する。またこれらの情報の横にはエンドポイントのグループが表示されており，簡単なボタン操作でエンドポイントのグループ分けを実施できる。

4．MELWALLの導入効果

この章では，**3章**で述べたMELWALLの機能を踏まえて，MELWALLをOT環境に導入した際の効果について述べる。

図4にOT環境へのMELWALL導入例を示す。**図4**左側の対策前ではOTネットワーク内はフラットな構成になっており，OTネットワーク内の機器は全て疎通可能な状態である。また，ネットワーク内には存在を把握できていないOT機器も存在する。このような状況で攻撃者にOTネットワーク内に侵入されると，被害がOTネットワーク全体に広がってしまう。

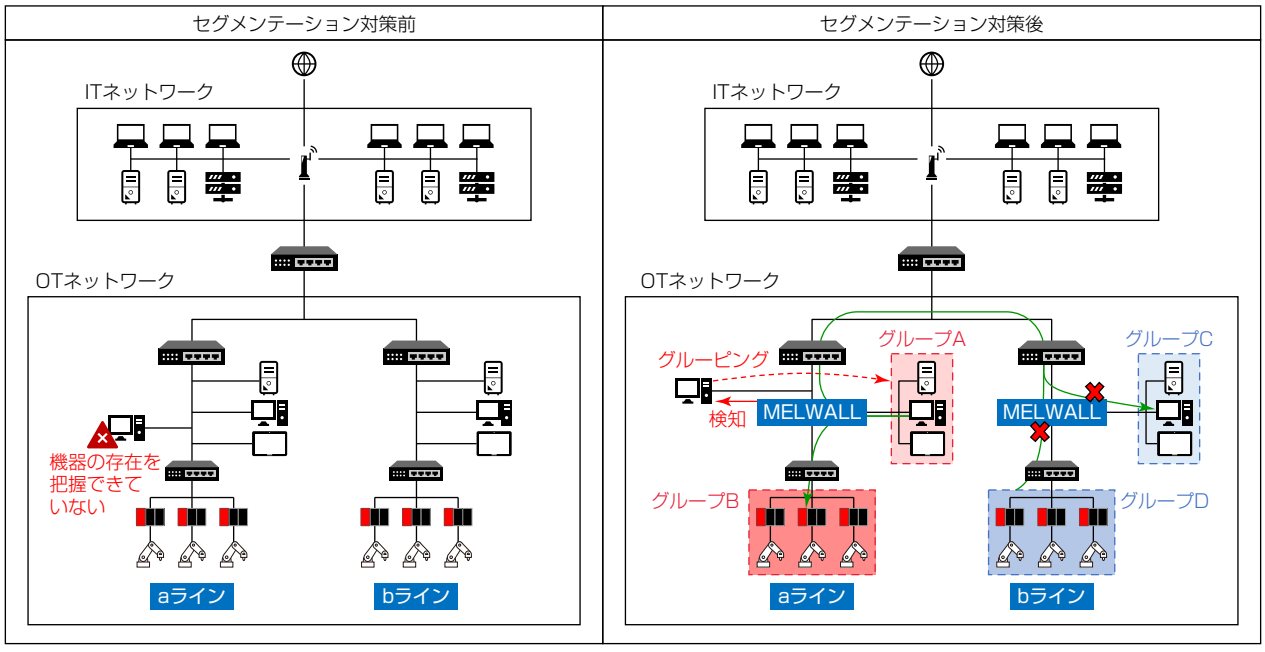

図4．OTネットワークへのMELWALL導入例

図4右側はMELWALL導入後の状態を示す。MELWALLのグループ単位でのポリシー設定機能によって，OTネットワーク内の機器をグループA～Dのようにグループ分けする。グループ単位での通信制御であるため，IPアドレスの変更や大きなネットワーク構成の変更は不要である。またMELWALLの機器検知機能によって，把握できていなかったOT機器の情報を検知し，適切なグループに所属させる作業に活用できる。これらのグルーピングは**3．3節**で述べたGUIで，直感的に設定できる。

図4右側の例では，グループを四つに分割している。これらのグループ間に適切なポリシーを設定することによってOTネットワークのセグメンテーションが実現される。例えばグループAは，グループBとは通信が許可されているが，グループC，Dとは通信が許可されていないとする。このとき，aラインのネットワークに攻撃者が侵入し，グループAに属する機器がマルウエアに感染したとしても，グループAの機器からグループC，Dへの通信が許可されていないことから，bラインへの被害拡大は抑えることができる。また，グループA，B間でも正常な通信だけを許可するような強固なポリシー設定になっていれば，被害の拡大を抑えられる可能性が高くなる。

5. むすび

OTネットワークのセグメンテーションをエンドポイントのグルーピングによって実現するOTネットワークセキュリティー機器MELWALLの特長について述べた。

今後もOT環境の対策導入・運用の課題を踏まえて，MELWALLの機能拡張を進めていくとともに，制御システムの安全性を高める製品・サービスを提供し続けられるよう進化し，社会に貢献していく。

参考文献

(1) 独立行政法人 情報処理推進機構：制御システムのセキュリティ
https://www.ipa.go.jp/security/controlsystem/index.html
(2) 木村敏之：サイバー攻撃から生産ラインを守る新たなネットワーク脅威対策技術，三菱電機技報，**94**，No.8，480～483（2020）