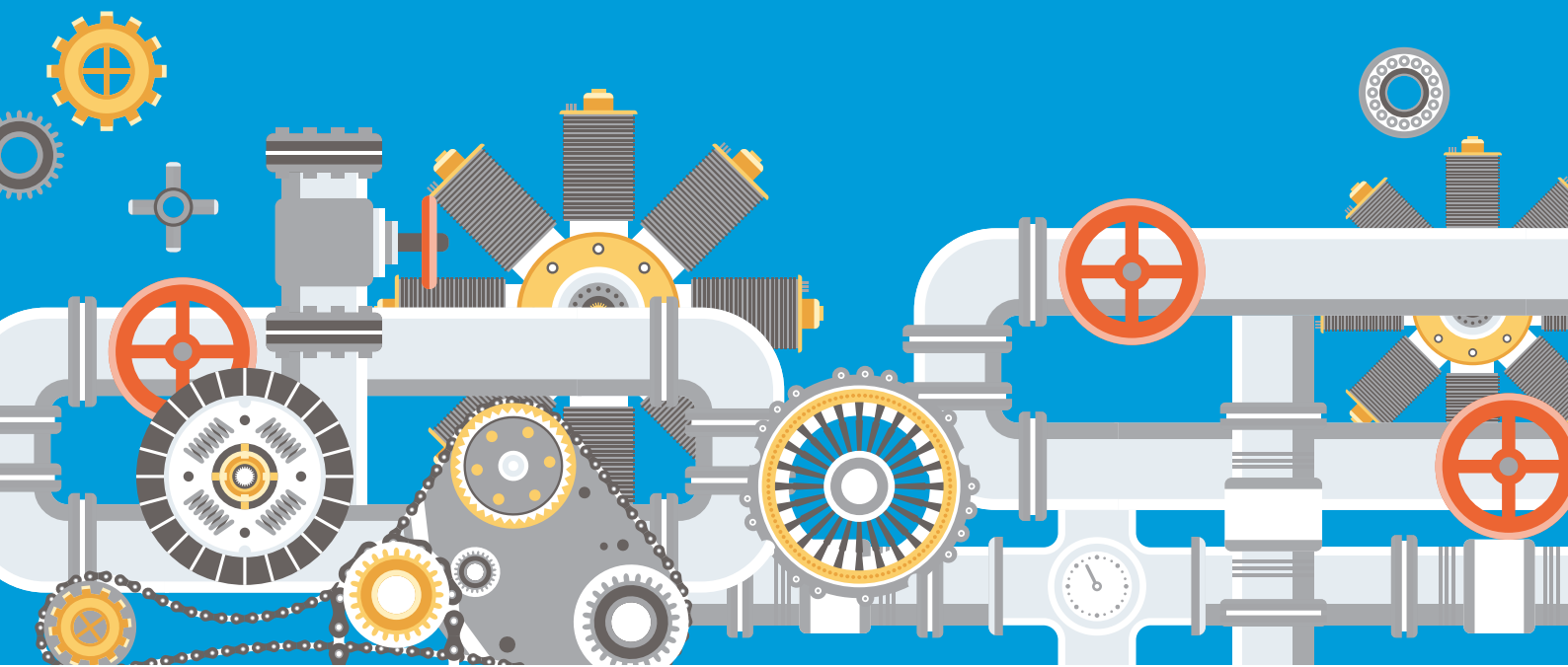
「OTセキュリティ」

SEMINAR REPORT

2019年4月19日、SCSKがパロアルトネットワークス、CyberXと共催で「OTセキュリティ」をテーマにしたアフタヌーンセミナーを開催した。OTとはOperational Technologyの略で、主に産業系システムの制御技術のことを指す。サイバー攻撃の増加を背景にIT（Information Technology：情報技術）のセキュリティ対策は認知されてきたが、OTにおけるセキュリティ対策はまだまだ認知されていない。

IIoT（Industrial Internet of Things：産業用IoT）の普及や第四次産業革命への対応から、OT環境へのセキュリティリスクが高まっている。本セミナーでは、OTセキュリティの基礎知識から現状、最適なセキュリティ対策製品までを把握できる内容となっている。



AGENDA

REPORT 1

第1部

『OTセキュリティ総論』
～OTセキュリティの変遷と今後求められる対策とは～

ジェイティ エンジニアリング株式会社
システムインテグレーション部 企画開発担当 シニアコンサルタント
福田敏博 氏

REPORT 2

第2部

『工場サイバーセキュリティ』
～これからの“つながる”工場に求められるセキュリティとは～

パロアルトネットワークス株式会社
技術本部 システムエンジニア
八木下利勝 氏

REPORT 3

第3部

グローバルで圧倒的な実績を誇る
No.1 OTセキュリティベンダー『CyberX』

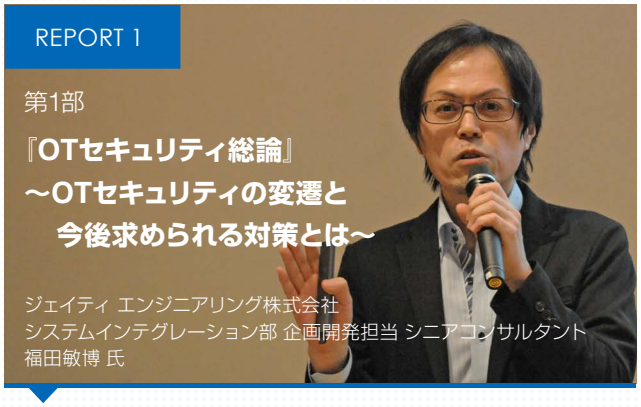
SCSK株式会社
ITプロダクト&サービス事業本部
ネットワークセキュリティ部
吉田圭佑 氏

REPORT 4

第4部

Palo Alto Networks × CyberX
連携ソリューション

SCSK株式会社
ITプロダクト&サービス事業本部
ネットワークセキュリティ部
玉川昇 氏



OTセキュリティの変遷と、リスクアセスメント手法

福田氏はまず、ジェイティ エンジニアリング(JTE)について紹介した。JTEは、専売公社が日本たばこ(JT)へ民営化した際に、技術者集団として設立された会社。たばこの生産技術で培ったノウハウを生かし、工場の建築や電気・機械設備のエンジニアリング、そしてそれらに関わるシステムインテグレーション(SI)の3つの事業を柱にしている。福田氏が所属するSI部は、システムの受託開発のほかパッケージソフトの自社開発・販売など多岐にわたるビジネスを展開。その中で福田氏はOTセキュリティのコンサルティングに携わっている。

福田氏は山口県宇部市の出身で、30年以上にわたり産業オートメーション系の仕事に従事。約40の資格を持ち、『工場・プラントのサイバー攻撃への対策と課題がよ～くわかる本』の著者でもある。一般的な情報システムを「IT」と呼ぶのに対して、ここ近年産業オートメーション系のシステムなどを「OT」と呼ぶことが多い。多くの企業がITのセキュリティ強化を進める一方、OTのセキュリティは、大手の製造業であってもまったく進んでいない現状がある。企業のガバナンスを考える上でも、この現状に疑問を持ったことが、この分野の仕事を始めたきっかけだったという。お客様のセキュリティ管理にITだけでなくOTを加えて欲しいという強い思いが、コンサルティングのポリシーでありミッションであるとした。

そして福田氏は、OTセキュリティの変遷を振り返った。そもそもの始まりは、2010年に確認された「Stuxnet」。Stuxnetは、SCADAやPLCといった制御システムやコントローラーを攻撃するマルウェアで、これによりイランの原子力発電所が制御不能となった(約8,400台の遠心分離機が停止)。OTがサイバー攻撃の標的になったことは非常に衝撃的であり、日本ではこれを受けて2011年に経済産業省が「制御システムセキュリティ検討タスクフォース」を立ち上げている。以降、2012年には技術研究組合 制御システムセキュリティセンター(CSSC)の設立、2014年には日本情報経済社会推進協会(JIPDEC)がISMSのOTバージョンといわれるCSMS認証制度を始めた。2017年には独立行政法人 情報処理推進機構(IPA)が産業サイバーセキュリティセンターを設立。ITのセキュリティだけでなくOTにも対応できる人材育成プログラムを始めており、福田氏はこのセンターの発足当初から有識者委員として関わっている。現在では、これ以外にも多くの業界団体などがOTセキュリティに関するカンファレンスやセミナーを開催し、OTセキュリティ対策の普及啓発を進めている。

代表的なインシデントに関しては、最初に2011年の「SHODAN」を挙げた。これはインターネット上につながっている機器を検索できるサービスで、インターネットに直結する制御システムが数多く見つかったということで話題となった。そして、2014年には「Havex」という、OPCプロトコルの脆弱性を突いて制御機器の情報搾取を行うマルウェアが出現。また、同年にはドイツの製鉄所がサイバー攻撃によって溶鉱炉が破壊された。

2015年には電力会社へのサイバー攻撃によりウクライナで大規模な停電があり、2017年はランサムウェア「WannaCry」が猛威を振るった。WannaCryの影響で日本の自動車工場が1日操業を止めた報道はまだ記憶に新しい。同じく2017年には、安全計装システムを狙う「Hatman」が登場している。また福田氏は「キラーUSB」と呼ばれる攻撃の動画を紹介した。キラーUSBは、PCに接続すると高電圧を流して基板を物理的に破壊するもので、身近なところで開発キットが出回っている脅威にも触れた。

OT環境のセキュリティ対策の進め方について、福田氏はリスクアセスメントが非常に重要であり、リスクアセスメント無しでの対策はあり得ないという原則を論じた。一般的にリスクアセスメントは、「リスクの特定」「リスクの分析」「リスクの評価」という手順で進めていく。ここで福田氏は、ある制御システムのネットワーク図を示した。一見、よく整備されたネットワークに見えるが、実はネットワークセグメントが非常に大きいため、ひとたび1台のPCがWannaCryに感染すると、ネットワーク全体に影響が広がる可能性がある。その背景には、度重なるシステム拡張があると福田氏は指摘する。システムを拡張する際に、セキュリティリスクへの考慮がなくネットワークが単純に拡張される。その結果、重要なシステムとそうでないシステムが同じセグメントに混在してしまう。また、USBメモリをデータ交換などで使用したり、リモート接続でメンテナンスするシステムが同居していたりすると、そこが脅威の入口になる可能性もある。

リスクの分析には、特定したリスクから脅威と脆弱性の大きさを数値化し、資産価値を考慮してリスク値を求める。たとえば「リスク値=(脅威レベル+脆弱性レベル)×資産価値」といった計算式を使用する。この結果からリスク対応を行うことになるが、対応には「低減」「回避」「保有」「移転」の選択肢がある。ほとんどの場合、セキュリティ対策によりリスクを下げる「低減」を選ぶことになる。では、具体的にどのような対策を行うのか。これは、CSMSの認証基準(国際規格IEC 62443-2-1準拠)を参考にするなら、第5章に詳細管理策として対策の要件が数多く規定されている。ここからリスクに適した管理策を選び、それを自社の対策として具現化するのだ。福田氏は例として、実際のセキュリティポリシーを紹介した。多くの対策が規定されていることがわかる。

福田氏は最後に、JTEのサービスを紹介した。同社では2014年からOTセキュリティのコンサルティングサービスを開始しており、CSMS認証の取得支援やリスク分析、ポリシー策定のサービスを行っている。さらに、それ以外のコンサルティングサービスとして、2019年から工場・プラントなどの製造部門を対象にRPA活用のコンサルティングも始めている。また今後、新たなOTセキュリティのコンサルティングとして、OT環境に対するレッドチームサービスを提供したいとして、セッションを締めくくった。

工場セキュリティのポイントと解決策

続いて、八木下氏は工場のサイバーセキュリティの変化について説明した。従来の工場は、社内のネットワークと隔離することで安全性を確保していた。しかし、2011年以降のIndustry 4.0、スマートファクトリーと呼ばれるデジタル変革の動きにより、日本も工場をネットワークにつなぐという考え方が進み、さまざまな活用が生み出されている。これにより、工場の稼働状況やスケジュールの進捗、各オーダーの完成レベルの確認など、迅速な経営判断が可能になる。また、製造ラインのログを収集してクラウドに上げ、活用することで稼働状況やメンテナンス状況、リモートメンテナンスなどに活用できる。ITとOTのつながりがより重要視されているのが現状であるとした。

工場がネットワークにつながることにより、さまざまなメリットがある。しかし、同時に多くのセキュリティリスクにさらされる懸念があると八木下氏は指摘する。リスクには外的要因と内的要因があり、外的要因にはランサム

ウェアや、マルウェアを活用した標的型攻撃、IoT危機を狙うMiraiボットといった脅威がここ数年活発になっている。日本では2017年5月にランサムウェアWannaCryによって、日本の大きな製造業さまでも工場ラインが停止してしたことを例に挙げた。内的要因では、内部関係者によるサイバー攻撃やデータの漏えい、ミスによるインシデントなどの脅威がある。ネットワークにつながることで、OTは安全という前提は崩れてきているとした。

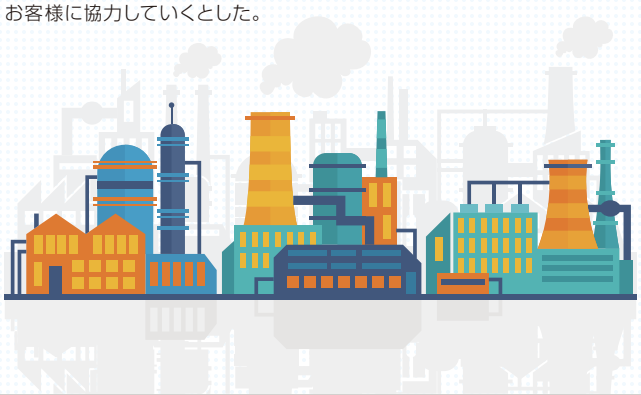
これらの要因により、たとえば工場ラインを遠隔操作で停止され製造が停まってしまったり、稼働データを改ざんされ機器の異常の発見が遅れてしまったり、検査結果を改ざんされ不良製品が出荷されてしまうといった影響を受ける可能性がある。結果として、取引に大きな影響を及ぼし、売上の減少や企業のブランド価値の低下など、企業経営に大きな影響を与えるおそれがある。そこで八木下氏は、理想的なICSのセキュリティを選択するための3つのポイントを挙げた。

1つ目は、役割ベースのアクセス制御を含む詳細なネットワークセグメンテーションを行うこと。2つ目は、ネットワークとエンドポイント、IoTのセキュリティを統合し、かつインテリジェンスを共有し、情報活動を行っていくこと。3つ目は、これらをゼロトラストで実現すること。ゼロトラストを実現するためには、「完全な可視化」「L7ベースの制御」「ノイズログの大幅削減」「AIによる危険アラートの絞り込み」、そして最後に「インシデントに対しての確実なレスポンス」が必要になる。

完全な可視化のためには、それぞれの環境、環境間のトラフィックを見える状態に再構築する必要がある。これがネットワークセグメンテーションである。これにより、誰が何を利用しているか、リスクが含まれていないかを見ていく。L7ベースの制御は、ネットワークトラフィックからSCADAやICSのシステムで使われる重要なプロトコルを識別できるようにすること。これらは、次世代ファイアウォールを使うことで、コスト削減と合わせて実現できる。また、ポイントセキュリティをつぎはぎで導入するのではなく、予防的なメカニズムを駆使して連携動作させ、相互間で脅威インテリジェンスを共有することが重要なポイントのひとつとなる。

また、HMIやIoTサーバーのワークステーション、サーバーなどのエンドポイントでは、古いOSを使っていたり、長期間にわたり使い続けたり、常時稼働が求められる。これらの保護も重要で困難な課題である。たとえば、パロアルトネットワークスの「Traps」では、シグネチャレスでマルウェアが起動した時点で防御するといった特徴がある。未知の脅威に対しては、脅威インテリジェンスである「WildFire」と連携することで対応できるとした。セグメント化された環境に導入された複数の次世代ファイアウォールについては、「Panorama」で一元管理でき、ポリシーの展開も容易に行えTOC削減の効果もある。

さらに、パロアルトネットワークスが提供する無料ツール「MineMeld」を活用することで、今まで管理者が手動で実施していた脅威情報の収集、収集した脅威情報の各セキュリティデバイスへの適用を自動化し、運用効率を高めることもできる。「GlobalProtect」もしくはPrisma Accessを活用すれば、社内外の環境を問わず、さまざまな端末に対してセキュリティポリシーを一貫して適用できる。このように、パロアルトネットワークスのソリューションを活用することで、包括的なセキュリティオペレーションプラットフォームを展開できるとした。一方で、攻撃者は工夫を凝らしてこれらの対策をすり抜ける攻撃を仕掛けることもある。そこで現在は、EDRやSIEMなどを検討するケースも多い。こうしたニーズに対応するため、「Cortex XDR」を4月にリリースしている。八木下氏は、パロアルトネットワークスはICSゼロトラスト戦略実現をサポートするためのプラットフォーム、ソリューションを提供し、お客様に協力していくとした。



REPORT 3

第3部

グローバルで圧倒的な実績を誇るトップクラスのOTセキュリティベンダー『CyberX』

SCSK株式会社
ITプロダクト&サービス事業本部
ネットワークセキュリティ部
吉田圭佑 氏

OTシステムの特徴とセキュリティを考えるポイント

SCSKの吉田氏は、SCSKを紹介するとともに、OTシステムの定義から現状、そしてCyberXの概要について説明を行った。これまで隔離されていたOTシステムが、IoTやデジタルトランスフォーメーションといった時代の流れを背景に、情報システムやインターネットとつながっていく状況にある。特に日本では、国際的なイベントを複数控えており、ハクティビストなどによるサイバー攻撃が懸念されているとした。

OTシステムは、そもそも隔離されていることを前提に設計されているので、セキュリティが考慮されておらず、情報システムと比較して非常に脆弱であるという特性がある。また、安全性（セーフティ）が非常に重要視される。人命に関わる重大な事故につながることもあるためだ。また、OTシステムにはIEC62443という国際規格があり、「パデューリファレンスモデル」がベースとなっている。

パデューリファレンスモデルは多段階層となっており、一番上が情報システムや基幹システムのレイヤーで、二番目からがOTのレイヤーとなる。最初にデータの収集、監視、蓄積のレイヤー、その下が集中制御のレイヤー、その下がPLCを含む個別制御のレイヤー、そして一番下が工場のラインなどで稼働するフィールドマシンのレイヤーとなる。このレイヤー間、あるいはレイヤー内で通信が行われる。

続いて吉田氏は、OTシステムの特徴について説明した。まず、プロトコルが全く統一されていないという特徴がある。ベンダーの数だけプロトコルがあるといっても過言ではない。そして、人命に関わるリスクもあるので、高い安全水準が求められる。IPAによる「セキュリティリスク分析ガイド」では、使用期間が非常に長いことが挙げられている。10年、20年という圧倒的な長さで、しかも24時間365日の可用性が求められている。そして、インシデントが起きたときの周りに与える影響が非常に大きいことも特徴に挙げた。

OTシステムの状況として、2010年に発覚したStuxnetを起点として、OTセキュリティが注目を集めている。また、OTシステムに存在するさまざまな機器の脆弱性の報告が増加しており、脆弱性に対する攻撃や感染も増えている。一方で、OTシステム自体も変化している。これまでは、それぞれがユニークなプラットフォームであったのが、WindowsやLinuxなどの汎用的なものが使われ始めている。これは通信プロトコルでも同様だ。そして何より、外部との接続や、USBなどの記憶媒体の持ち込みも、現場では起きている。

IPAではこれらの状況から、これまで隔離された固有のプラットフォーム、システムが外部につながっていくことで、セキュリティの脅威が高まっていると指摘している。IPAでは、ユーザーの現状についても調査しており、これによると、セキュリティリスクに関して多くの企業が認識はしているが、対策に取り組んでいる企業の割合は高くなかった。その理由は、「インターネットに接続していないから」が最も多く、いまだに認識が低い。そもそもIoTやスマートファクトリー化はつながることが前提であるし、そうでないと欧米の先進的な企業と競争できない。

具体的なセキュリティ対策について、吉田氏はNICTの製造業向けのセキュリティガイドを引用した。ガイドでは、ゾーニングと多層防御を提唱している。ゾーニングは、フラットなネットワークをファイアウォールによってセグメント化すること。多層防御は、ファイアウォールに加えIDSを導入することとしている。つまり、パロアルトネットワークスのファイアウォールでセグメント分

けを行い、IDSとしてCyberXを導入するという、まさしくSCSKが推進しているソリューションが適しているわけだ。

CyberXは2013年に設立された会社で、OTネットワーク向けセキュリティ事業を展開している。本社は米国だが、エンジニアはイスラエルにいる。中心メンバーは、イスラエルの国防軍でインフラ系サイバーセキュリティのブルーチームを担っていた。CyberXのIDSは、ヨーロッパ、北米を中心に500社以上、1200拠点で導入されている。OTシステムのプロトコルや脆弱性に豊富な知見があり、パロアルトネットワークスのファイアウォールのほかSIEMとの連携を実現している。これにより、OTシステムのセキュリティをIT側のSOCで対応できるようにしていることが特徴だ。

機能としては、OTのシステムにある端末、アセットのインベントリをリスト化できる。あるいは、そのネットワークのトポロジーを生成する。また、特許を持つ5つのセキュリティエンジンを搭載しており、これらを複合的に使うことで脅威を検知する。さらに、連携や自動対応が可能なアラートの通知機能も持つ。ペンテストのような攻撃シミュレーション機能も搭載している。パデューリファレンスモデルでのOTの上位層からSCADA、PLCといったレイヤーまでカバーし、イーサネットの通信をサポートする。構成としては、ネットワークスイッチのミラーポートに接続して、パッシブにパケットを収集して解析する。OTのオペレーションにまったく影響を与えないことも特徴であるとした。

そして吉田氏は、CyberXの欧州、北米でのユースケースを6件紹介した。いずれもCyberXならではの機能で課題を解決している。最後に吉田氏は、SCSKではCyberXのPOCのご支援をはじめ、オンサイトでの導入支援や立ち会い、クライテリアの作製やシナリオの作成、使い方のレクチャーなどをしているので、ぜひお声がけくださいとした。

パロアルトネットワークスのファイアウォールとCyberXが連携するメリット

SCSKでCyberXを担当している玉川氏は、パロアルトネットワークスのファイアウォールとCyberXを連携させるメリットについて、デモを交えて紹介した。CyberXは、単体で非常に強力な運用監視と脆弱性診断の機能を持っている。CVEのみならず学習された運用基準から逸脱した動作を検知するとアラートを発して管理者に通知する。また、脆弱性診断により個々のアセットに、どのような脆弱性が存在するのかをレポートとして出力してくれる。しかし、CyberXはアラート通知を行うのみで、これだけではOTネットワークはセキュアにはならない。通知への対処が必要になる。

対処とは、OTネットワーク内に怪しい動きがあれば、マルウェアが侵入していないか該当するデバイスをチェックしたり、脆弱性のあるソフトウェアをバージョンアップしたりすることになる。しかし、多くのデバイスやソフトウェアは工場のラインで使われているため、有効な対策を迅速に講じることが難しい。最近はOTネットワークをITネットワークに接続するケースも増えているが、脆弱で丸裸な状態のOTネットワークをつなげるのはリスクが高い。そこでファイアウォールを設置することになるが、設置すれば何でも防げるかというと、そうでもない。OTならではの膨大なベンダー固有のプロトコルに対応していることや、内部に存在する脅威がITネットワークから外部に出ていくことを阻止することが求められる。

そこで玉川氏は、CyberXとパロアルトネットワークスのファイアウォールが連携するコンセプトを紹介した。一つ目は、CyberXが検出したマルウェア、あるいはマルウェアとおぼしき動きを検出したときに、CyberXからパロアルトネットワークスへ自動的に「当該デバイスの通信をブロックしてください」というセキュリティポリシーを定義することができる。二つ目は、ファイアウォールを導入する際の効率化である。ファイアウォールには、あらかじめセキュリティポリシーを設定する必要がある。これは、通信などの許可をデバイスごと、IPアドレスごとに定義することとなる。

しかし、セキュリティポリシーを設定するためには、その前段階としてネットワーク内にどのようなデバイス（アセット）があり、どのようなMACアドレスやIPアドレスなのかを漏れなく把握する必要がある。一般的にファイアウォールの設定では、個々に異なる性質のデバイスごとに一つずつ手入力により登録しなければならない。これらは非常に大変な作業となる。CyberXでは、ネットワークのパケットをキャプチャすることで、ネットワーク内に存在するデバイス、MACアドレス、IPアドレス、装置ベンダーやタイプを把握し、これらの詳細情報をタグ情報として管理している。これをパロアルトネットワークスのファイアウォールに読み込ませる際に、タグ情報ともども読み込ませることが可能である。パロアルトネットワークス側では、タグ情報をもとにデバイスのグループ化を行い、グループポリシーを設定することで、装置種別ごとの特殊なフィルタを一括登録可能となる。

玉川氏は、CyberXのダッシュボードを示し、一つ目のコンセプトのデモを行った。そのデモでは、すでに異常を検出した状態（トータルで12件の異常が検出されていて、そのうちクリティカルが3件、メジャー、マイナー、ワーニング、それぞれのカテゴリ別に表示）にしてある。ただし、この全てをパロアルトネットワークスのファイアウォールに連携させる必要はなく、OTネットワークからITネットワークに出て行くようなマルウェアアクティビティのみを連携させれば良い。その判断は、CyberXが自動で行う。一例として、玉川氏がマルウェア検出をクリックすると、WannaCryの検出であり「Unblock」と表示されている。すでにパロアルトネットワークスのファイアウォールに転送されており、ポリシーが自動生成されている。これをパロアルトネットワークスのファイアウォールではどう見えるかを説明するために、玉川氏は表示画面を切り替えた。ポリシー画面を表示すると、先ほどのポリシーがCyberXからすでに自動設定されている。

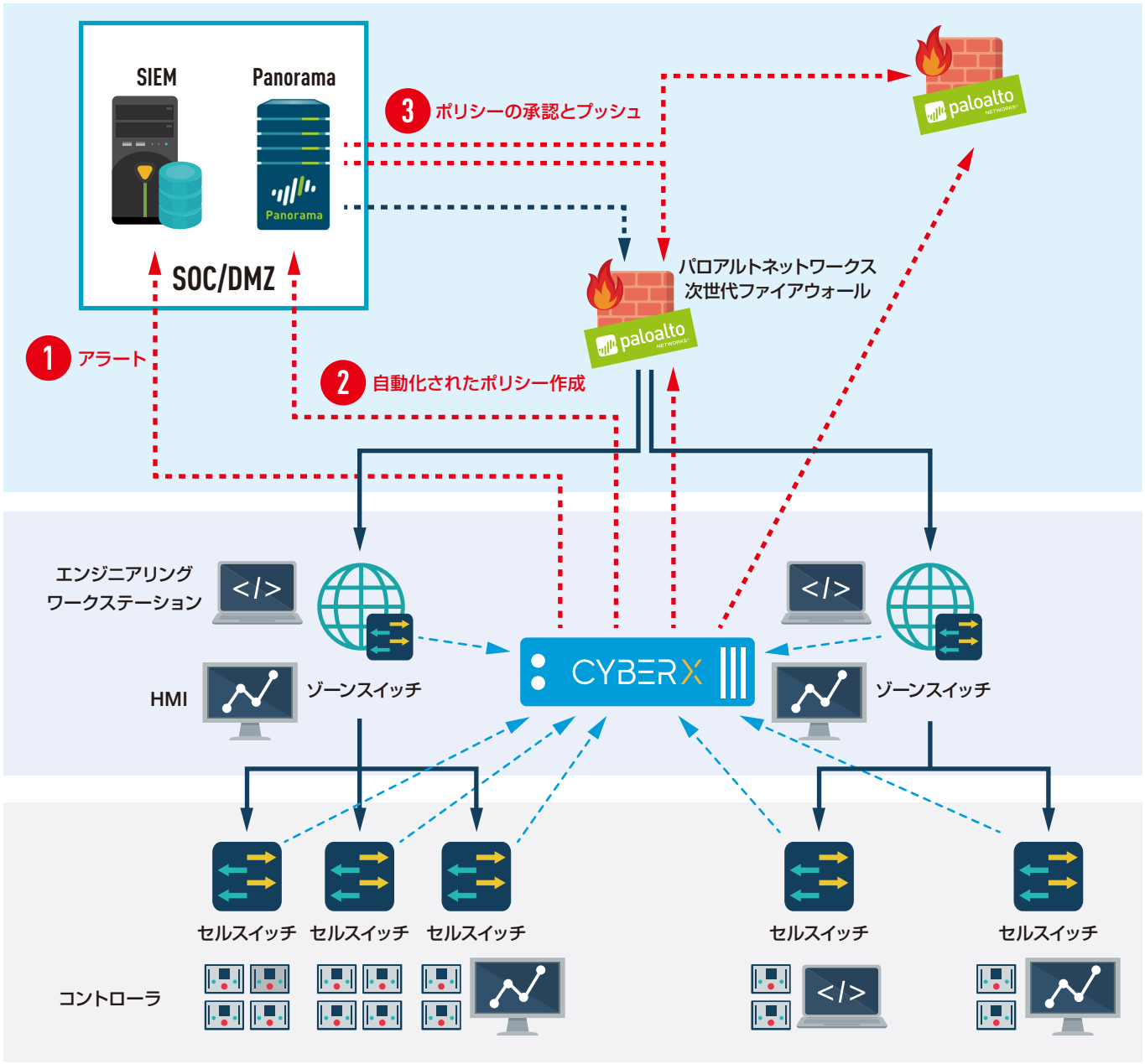
また、手動によるBlock、Unblockも可能であると述べた。

続いて、二つ目のコンセプトのデモを行った。CyberXは、ネットワークのトラフィックをキャプチャしてパケットの進路解析を行うことで、ネットワーク内にあるデバイスやその詳細を把握できる。この際、CyberXは全体像としてアセットマップを作成する。これを拡大すると、アセットのインベントリ、IPアドレスとタイプ、サーバーやPLCといった種別まで自動検出していることがわかる。玉川氏は、パロアルトネットワークスのファイアウォールに転送されたアセット情報から、フィルタリングによりセキュリティポリシーを一括適用するデモを行った。アセット情報が詳細なので、さまざまな切り口でグループ化し、ポリシーを適用できる。これをIPアドレスごとにひとつひとつ手動で設定するのは大変な作業であると強調した。

デモを行ったのは2つのコンセプトであったが、もうひとつ重要なコンセプトがあると玉川氏は言う。それは、Cortexに収集されたパロアルトネットワークスのパケット情報を、逆にCyberXへ取り込み、そこに潜む脆弱性を分析する機能である。また、アタックベクターという機能も紹介した。これは、CyberXにより検出された脆弱性に対して、攻撃のシミュレーションを行うというもの。たとえば、パスワードを平文で使っていると、それを悪用してデバイスまでアクセスされる可能性がある。こういった攻撃の可能性を点数で表示してくれる機能だ。パスワードを暗号化するようにして再度、アタックベクターを実施すると、点数が向上する。

また玉川氏は、2つのデモの後で、パロアルトネットワークスのファイアウォールのポリシーを全て削除し、再びCyberXから自動設定するというデモも行った。その作業はセッションの間に非常に短時間で終了し、アラートメールが届いた。なお、アラートの通知方法には、SIEMへの転送も用意されている。これは、IT系のSOCと連携して、アラート情報を一元管理できるようにしたものだ。以上で、玉川氏はセッションを終えた。

Palo Alto Networks + CyberX



本書記載内容に関するお問い合わせ

SCSK株式会社
ITプロダクト＆サービス事業本部　ネットワークセキュリティ部
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント　TEL : 03-5859-3037
E-mail : paloalto-info@ml.scsk.jp　http://www.scsk.jp/product/common/paloalto/
E-mail : cyberx-info@ml.scsk.jp　http://www.scsk.jp/product/common/cyberx/