安全な重要インフラを実現するアーキテクチャ

近年のIoT（Internet of Things）などの発展に伴ってさまざまな機器がネットワークに接続されるようになってきています．このような状況の下，サイバーセキュリティに対するさらなる脅威の増大が懸念されています．NTTセキュアプラットフォーム研究所では，重要インフラを構成するネットワークを守るためのセキュリティインシデントの検知技術，インシデントの分析と対処を自動化する技術，および装置や機器に潜在するセキュリティリスクを減らすための技術の研究開発に取り組んでいます．

うえの　まさみ　　かしま　しんご
上野　正巳　/加島　伸悟
いがらし　ゆみのぶ　　ほり　　まさひろ
五十嵐　弓将　/堀　　正弘
NTTセキュアプラットフォーム研究所

サイバーセキュリティに対する脅威

IoT（Internet of Things）の発展に伴い，さまざまな機器がネットワークに接続されるようになってきており，2020年にはIoT機器は530億台に達すると予測されています(1)．ネットワークに接続される機器の増加は，サイバーセキュリティの脅威の増大を招きます．例えばオンラインの監視カメラのシステムや，ビデオレコーダー機器にマルウェアを仕掛けられて機器がボット化し，ほかのITサービスにDDoS（Distributed Denial of Service）攻撃を行うなど，サイバー攻撃の送信元となっていたという事例がすでに報告されています(2),(3)．

一方で，「情報通信」「金融」「航空」「鉄道」「電力」「ガス」などのさまざまな重要インフラにおいても，サービスの高品質化や省力化のためにIT化が急速に進んでおり，IT依存度が高まった結果，システム障害によるインフラサービスへの影響の事例がいくつも指摘されています(4)～(6)．

このような重要インフラにおいても，ネットワークに接続する機器の増加による脅威の増大に備え，早急に対策を講じていく必要があります．本稿では，重要インフラである「情報通信」分野の１つとして位置付けられる広域ネットワーク（WAN: Wide Area Network）*1に主眼を置き，さまざまな重要インフラをサイバー攻撃から守るためのセキュリティ対策技術について説明します．

広域ネットワークのセキュリティ

従来より，ネットワークのセキュリティを保持するには，セキュリティポリシーが運用されているセキュアゾーンと，セキュリティが守られていない可能性のある非セキュアゾーンを定めて，その境界でセキュアゾーンを守るという方法がとられています．広域ネットワークにおいても，ネットワーク事業者の観点からみると，ネットワークオペレータが運用管理する設備内は十分にセキュリティが確保された信頼の範囲内であるセキュアゾーンと想定でき，一方，ホームゲートウェイ（HGW）や企業用のルータなどのCPE（Customer Premises Equipment）*2装置よりもお客さま側の設備は，ネットワークオペレータが管理できず信頼性を担保できないために非セキュアゾーンであると想定されます．そのため，お客さま設備とネットワーク事業者設備の境界点に，ゲートウェイにあたるエッジルータなどの装置を設置して，回線の単位でネットワークに対するセキュリティを担保してきました．

しかし今後，IoTなどの発展に伴ってお客さま設備側に接続される機器がさらに増加すると考えられるため，よりそれらの機器に近いCPE装置において通信を制御することが求められるようになると想定されます．

広域ネットワークのセキュリティを守るための仕組み

広域ネットワーク内のセキュリティを守り，また感染や攻撃といった何らかのインシデントが発生した際にも素早く対処を行うためには，インシデントの検知の仕組み，検知したインシデントを分析し対処を決定する仕組み，決定した対処を実施する仕組みが必要になります．この大きなセキュリティ

＊1　広域ネットワーク：一施設内程度の規模で用いられるローカル・エリア・ネットワーク（LAN）と比較して，より広域なネットワークの総称．具体的な例としては，地理的に離れたLANを専用回線などで相互接続したネットワークや，インターネット上に構築された仮想的なプライベート網（VPN）などがあります．
＊2　CPE：インターネット接続サービスの利用者が，ネットワークに接続するために利用者自身の宅内に設置する機器．

対策の枠組みは従来と変わりませんが，冒頭で述べた環境変化の中，広域ネットワークのセキュリティを守るためには，CPE装置がセキュアゾーン内にある仕組みと連携しつつ，非セキュアゾーンに存在する機器のインシデントの検知や対処を正しく行うことが重要です．また，CPE装置はセキュアゾーンと非セキュアゾーンの境界に位置することから，CPE装置の内包リスク（潜在的な欠陥や誤設定，出荷前に不正に埋め込まれたマルウェアなど）や物理リスク（部品の不正な入れ替えなど）を減らすための仕組みもさらに必要になってきます．

以降では，これらの課題を解決するためにNTTセキュアプラットフォーム研究所で研究開発中のセキュリティ対策技術である，健全性確認技術，セキュリティオーケストレーション技術，真正性・完全性確認技術のそれぞれについて説明します（**図**）．

健全性確認技術

PCやサーバなど従来の情報処理機器を守るための侵入検知の仕組みとして，IDS（Intrusion Detection System）

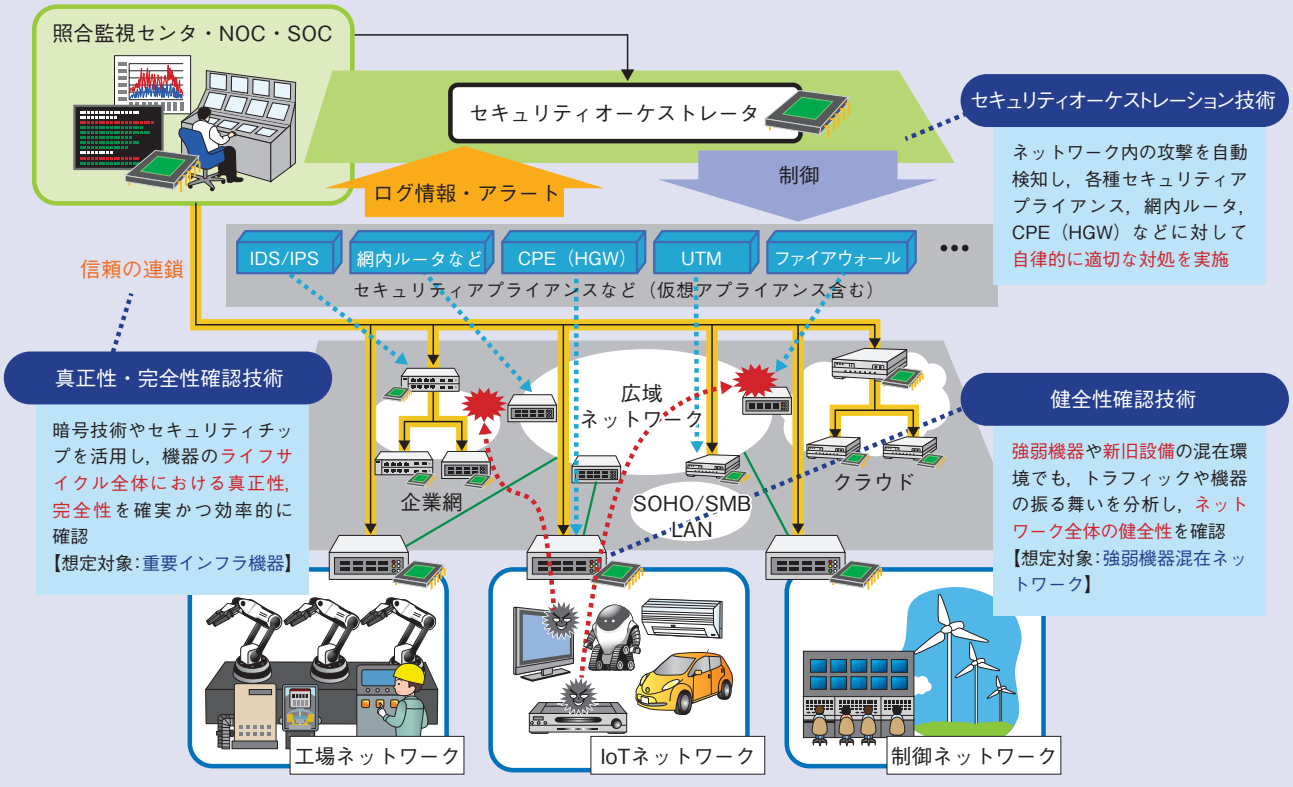


図　研究開発中のセキュリティ対策技術

やIPS（Intrusion Prevention System）[*3]があります．しかし，これらは主にPCやサーバを対象としており，重要インフラを構成する機器やIoT機器に対応した製品はまだ少ない状況です．特に，重要インフラや工場などで使われる制御・監視機器やIoT機器は，広域に配備された膨大な数の機器がネットワークに接続し，それらがさまざまな環境の下，無人で自律動作を行う点で従来の情報処理機器とは大きく異なります．さらに，これらの機器は特定の用途専用に設計・製造される場合が多いため，機能・性能が制限され（セキュリティ的に弱い機器）たり，また長期にわたって継続利用されて更新期間が長く（古い機器）なるなど，機器自体でセキュリティ対策を取ることが難しいという問題があります．

この問題に対応するため，NTTセキュアプラットフォーム研究所では，制御・監視機器やIoT機器自体に手を加えることなく，機器外部のネットワークにおいて機器の異常な振舞いを検知することにより，システム全体の健全性劣化の予兆をいち早くとらえることをめざした健全性確認技術を研究しています．より具体的には，個別にセキュリティ対策を施すことが難しい弱い機器や古い機器の通信トラフィックおよび動作ログから得られる統計情報を，機器の上位にあるHGWなどのCPE装置で取得し，その統計情報から機器種類や利用形態の特徴を含んだ健全状態を表現する解析モデルを構築することにより，解析モデルで表現される通常（健全な）挙動から逸脱した動作を発見することを可能とするアノマリ検知技術を研究しています．

セキュリティオーケストレーション技術

検知したインシデントを分析し対処する仕組みとしては，多くのセキュリティ製品のベンダが自社のセキュリティアプライアンスなどにより検知と制御を連動させる製品を提供していますが，ベンダ自社や提携する数社の製品のみとの連携に限られています．

NTTセキュアプラットフォーム研究所では，ベンダによらない検知や分析と制御の連携を実現しセキュリティオペレーションの自動化，半自動化を行う仕組みであるセキュリティオーケストレーション技術を開発し，事業会社各社に提供しています．これまではセキュリティの脅威が明確だったデータセンタやオフィスのセキュリティアプライアンスのオペレーションを連携する技術として開発を行ってきましたが，今後はIoTの発展に併せHGWなどのCPE装置も含めたオーケストレーションへと拡大させていくことをめざしています．例えば，通信先の少ないIoT機器に対してはあらかじめホワイトリストなどを用いて通信先や通信元を制限しておくことにより，問題が発生した際に通信量の制限や遮断といった通信の制御を機器単位で実施できるようにしています．

真正性・完全性確認技術

通常，検知装置，制御を行うセキュリティ装置，およびCPE装置は，非セキュアゾーンに置かれます．これらの装置の内包リスクや物理リスクを減らすことによって信頼の範囲を広げることができれば，万が一のインシデント発生時にも，より迅速な対処を行うことが可能になります．

NTTセキュアプラットフォーム研究所では，これらの装置およびそれらに接続する機器の信頼性を高めるため，制御対象機器を確実に識別する技術（真正性確認技術）と，その機器に搭載されているソフトウェアの正しさを確認する技術（完全性確認技術）を研究しています．

＊3　IDS/IPS：ITシステムやネットワークに対する外部からの不正行為を検出，またはそれらを防御するシステムのこと．

■真正性確認技術

真正性確認技術は，制御・通信機器自体がなりすまされていないこと，正しいものであることを確認するための技術です．具体的には，「信頼の起点（Root of Trust）」となる専用サーバを頂点として，各機器上に配置され「信頼の基点」となる耐タンパ部品による連鎖的な関係（信頼の連鎖）を構築し，この連鎖上で暗号技術を応用した機器認証を行うことによってシステム全体の真正性の確認を行います．ここで用いられる耐タンパ部品は，外部からの解析や非正規な手段によるデータ読み出しが非常に難しい機構を持っており，内部に安全にデータや暗号鍵を管理することができます．

■完全性確認技術

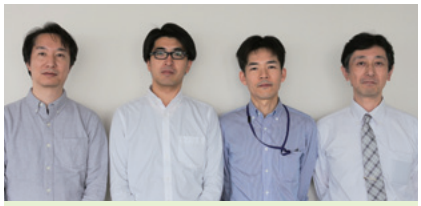
完全性確認技術は，制御・通信機器で動作しているソフトウェアや管理されているデータが，改ざんされていないことを確認するための技術です．完全性確認技術は，真正性確認技術により構築された「信頼の連鎖」を基盤としており，耐タンパ部品により安全に管理される正解値と，機器上のソフトウェアとを照合することにより，不正な改ざんが行われていないことを確認します．完全性確認技術は，システム全体を対象としたスケーラビリティを確保し，ソフトウェアのライフサイクル全体を考慮している，といった特長があります．

今後の展開

ネットワークに接続する機器の爆発的な増加が見込まれる状況に対して，重要インフラのセキュリティを守るための取り組みとして広域ネットワークを題材に対策技術を紹介しました．感染や攻撃といった何らかのインシデントが発生した際にも素早く対処を行うためには，インシデントの検知の仕組み，検知したインシデントを分析し対処を決定する仕組み，および決定した対処を実施する仕組み，さらに装置の内包リスク，物理リスクを減らすための仕組みが必要となり，NTTセキュアプラットフォーム研究所では，それぞれ健全性確認技術，セキュリティオーケストレーション技術，真正性・完全性確認技術として取り組みを行っています．これらの技術は，広域ネットワークに限らず通信を伴うIT化が行われている領域に適用可能な技術であり，今後重要インフラをはじめとしたさまざまな領域に適用域を拡大していく予定です．

■参考文献

(1) http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc254110.html
(2) https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/
(3) https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/
(4) http://www.nisc.go.jp/active/infra/pdf/infra_rt3_r1.pdf
(5) http://www.nisc.go.jp/inquiry/pdf/itizon_gaiyou.pdf
(6) http://www.nisc.go.jp/inquiry/pdf/it_izon_honbun.pdf



（左から）上野　正巳/ 加島　伸悟/ 五十嵐　弓将/ 堀　　正弘

NTTセキュアプラットフォーム研究所では普段の生活の基盤となっている重要インフラのネットワークをサイバー攻撃から守る研究に日々取り組んでいます．

◆問い合わせ先

NTTセキュアプラットフォーム研究所
企画担当
TEL　0422-59-3212
FAX　0422-59-2971
E-mail　scpflab@lab.ntt.co.jp