IoT領域におけるセキュリティ対策で高度化するサイバー攻撃の脅威に対応

当社はセキュリティ製品やソリューションを提供してきましたが、昨今のサイバー攻撃における脅威はこれまでのIT(情報技術)領域だけに留まらず社会インフラや製造設備にも及んでいます。こうしたOT(制御技術)領域でのセキュリティ意識やニーズの高まりを受け、当社でもIoTセキュリティ市場の新たな製品を提供できるよう取り組んでいます。

IoT機器・インフラシステムを取り巻く脅威

標的型攻撃やランサムウェアの急増により、社会インフラや製造設備などのIoT領域に対するセキュリティ対策のニーズがこれまで以上に高まってきています。従来はPCをはじめとするIT機器がネットワークに接続していましたが、今ではIT機器に限らず、車載や家電のほか、製造設備や社会インフラといった多種多様な機器がネットワークに接続する時代を迎えています。

調査会社のIDC Japanによると、2016年の国内IoTセキュリティ製品市場規模は、前年比27.5%増の518億円で、2021年には1,250億円まで成長すると見込まれています**(図-1)**。これは、ネットワークへの接続によりIoT領域へのサイバー攻撃が現実的な脅威として迫っており、IoTセキュリティ市場への需要が高まっていることを示しています。

既に海外では電力の発送電設備や空港・地下鉄の制御システムに対してサイバーテロがあり、停電やシステム停止の事故が発生しています。こうした海外のサイバーテロは、重要なデータを暗号化し使用できなくさせて、復旧に対しては身代金を請求するランサムウェアが主体です。攻撃の手口が巧妙かつ悪質であり極めて深刻な状況です。このようなことから、国内においても電気やガスなどを含めた重要な社会インフラシステム、製造工場やプラントなどへのセキュリティの重要性は急速に高まっていると言えるでしょう。

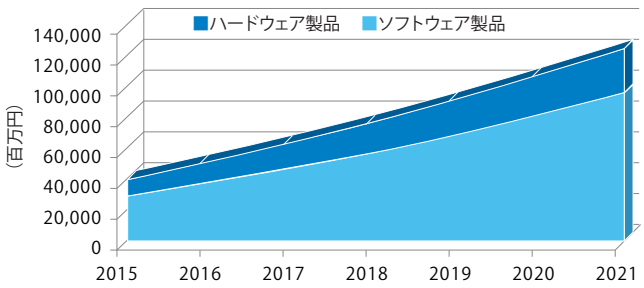

図-1 国内IoTセキュリティ市場 製品セグメント別 売上額予測、2015年～2021年(出典: IDC Japan, 2017年11月)

当社のお客様の間でも、セキュリティに対する経営者の意識はますます高まっています。ただ、サイバー攻撃の手口が多様化しており、意識はあってもどうすればいいのか、どういう製品でどのような対策ができるのか分からないというケースをよく耳にします。またセキュリティ製品は導入していても従来の製品では対応できないランサムウェアなどの新たな脅威も増加しています。

当社は、IT領域に対する標的型攻撃対策、改ざん検知、資産管理、クライアントセキュリティなどさまざまなセキュリティ対策製品やソリューションを提供していますが、海外のサイバーテロを例としたOT領域のセキュリティに関して話を聞く機会が増えており、早急にお客様のニーズに応えられる製品を提供していかねばならないと考えています**(図-2)**。

OT機器・システムを守る3つの製品

当社は、米国シリコンバレーで最新技術、最新製品を発掘するなど、セキュリティ製品や市場の調査を継続的に行っており、今後、次の3つの製品を当社のお客様に提供していけるよう準備を進めています。

(1) IoT機器への不正アクセスの自動検知

例えば、店舗などは監視カメラを設置して、店内の映像をサーバー側に蓄積し、何かあった場合に当時の映像を確認しています。このようなシステムにおいて、最近では外部からの不正アクセスによって監視カメラの設定情報が書き換えられ、ネットワークの経路を変えられて悪意のある不正サイトに映像が漏えいしたケースも見られます。

こうした脅威を検知するため、当社では、ネットワークのパケットを監視して不正なルートにアクセスしていないかをチェックする製品を準備しています**(図-3)**。機械学習を利用して通常の通信ルートを学習し、通常とは異なる経路で通信が発生した場合にアラート通知を行い、ネットワーク機器と連携して不正な経路

への通信を遮断する仕組みを提供します。

(2) 全体のアクセス経路を可視化

企業にはさまざまなネットワーク機器が存在しますが、すべてのネットワーク機器にアクセスして設定情報の取得を行い、アクセス経路のマップを作成、ネットワーク経路を可視化することができます。

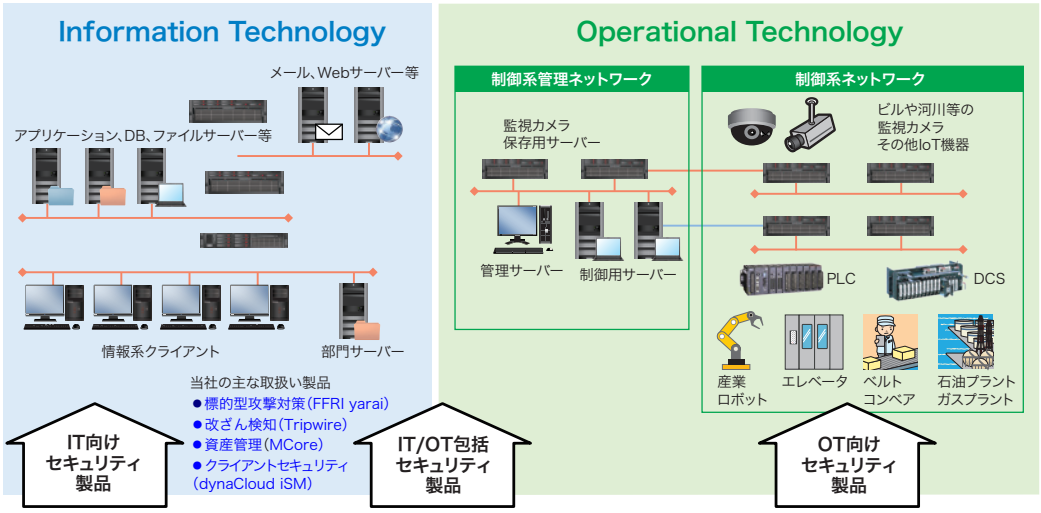

図-2　ITおよびOT領域

ネットワークの規模が大きくなると、機器の構成情報を1台ずつ管理するには大変な労力を要します。この製品を使えば、企業内のネットワーク全体が構成図として可視化され、設定した経路の正常性が一目で確認でき、PCI DSSなどのコンプライアンス・ポリシー準拠や監査対応が行えます。また、ネットワークの脆弱性リスクの検出と改善に向けた対応の優先度が把握できるようになります。

(3) ユーザーの行動分析を機械学習で監視

資産管理ソフトウェアの導入によってユーザーの操作ログなどさまざまなデータを収集できますが、これまでの操作ログは、情報漏えいの発覚後に誰がどのような操作をしたのか確認するために利用する場合が多く、通常は膨大なデータを保管しているだけでビッグデータとしての活用はしていない場合がほとんどです。本製品は、AD AUDITログ、アクセスログ、DBログ、メールログといったログを読み取り、機械学習を活用して、ユーザーの操作について行動分析を行うものです。日頃はUSBを利用しない人が突然ある日から大量のデータをUSBメモリに書き出している、普段アクセスしないサーバーに頻繁にアクセスし大量のファイルをダウンロードしている、といった予期せぬ行動をその場で検知することができます。

痒いところに手が届くセキュリティ製品を

当社のお客様にヒアリングをすると、「ソフトウェアのインストールが行えない製造ラインの機器に対してもエージェントレスのセキュリティ対策を行いたい」、「未知の脅威に対しても検知できる仕組みが欲しい」、「重要な個人情報を扱うシステムを外部攻撃から守りたい」といった声が聞かれます。前述した製品やソリューションを提供してニーズに応えることは急務となっており、研究開発に注力しているところです。

製造系のラインを持っているお客様においては、IT領域ではセキュリティ対策ができていても、それと切り離されている製造ラインでは手つかずの状態、というケースが少なくありません。当社では、IT領域向けのセキュリティに関しては多くのお客様に製品やソリューションを提供してきました。今後は、OT領域向けの商材も取り揃え、IoTセキュリティ市場に対して積極的に当社の技術力をアピールしながら、従来製品・ソリューションと合わせて拡販をしていきます。

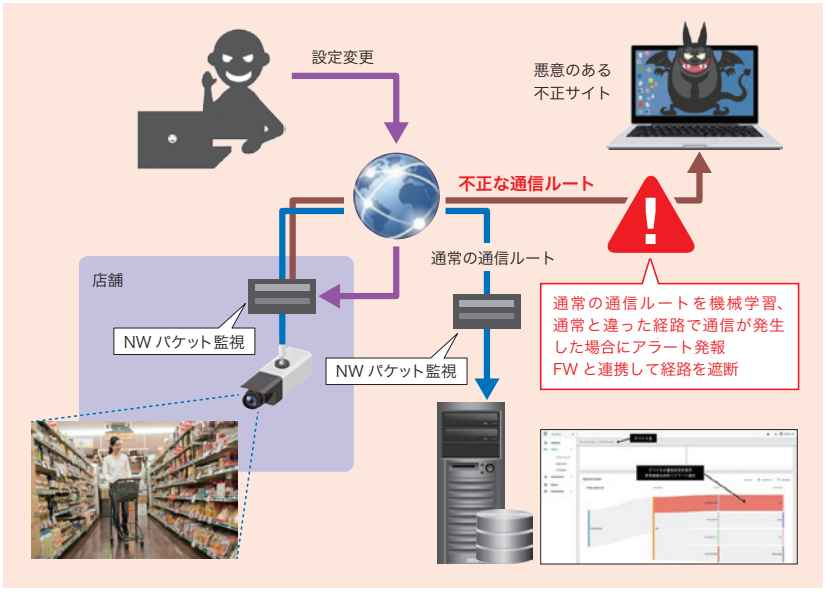

図-3　監視カメラへの不正アクセスの自動検知

(デジタルエンジニアリング第３事業部

三ヶ月 一弘、渡邊 健一)