<ホワイトペーパ>

産業系ネットワークセキュリティの最前線

株式会社テリロジー

新美竹男

はじめに

産業系ネットワーク(“**OT ネットワーク**”とも呼ばれる)に繋がっている重要インフラ資産を守ることは、企業 IT のセキュリティ対策とも若干似ているが、産業系ネットワーク固有の課題がある。

産業系ネットワークに接続される産業制御システム（以下 **ICS** と略す）は色々な産業基盤に応じてカストマイズされているが、依然としてレガシーWindows OS のプラットフォーム上で稼働している。そして、これら ICS 環境は、信頼性と可用性を十分に考慮する必要がある。ICS は数年以上の間、無停止で稼働することが必須とされており、平均的な稼働寿命は数十年となっている。逆に、サイバー攻撃者は彼らの進化しつつある手口によってこうした脆弱性を突いたレガシー基盤に簡単に侵入でき、いつでも攻撃することが出来ると云える。

企業 IT ネットワークは、継続的に運用管理され、急速に巧妙化しているサイバー脅威に対しても防御対策をとっているが、制御系ネットワークは伝統的にセキュリティよりも信頼性と可用性が最優先される。

だからと云ってサイバー攻撃に対して何もしないという選択肢はない。産業系ネットワークの生産性とセキュリティ攻撃の潜在的なインパクトを考えると、新しいセキュリティ対策の方策を見出す必要がある。海外の重要な産業分野ではサイバー攻撃が起きている現実の実例からもわかるように、産業系ネットワークは益々、攻撃者のターゲットになってきている。

産業系ネットワークの安全・安心の重要性

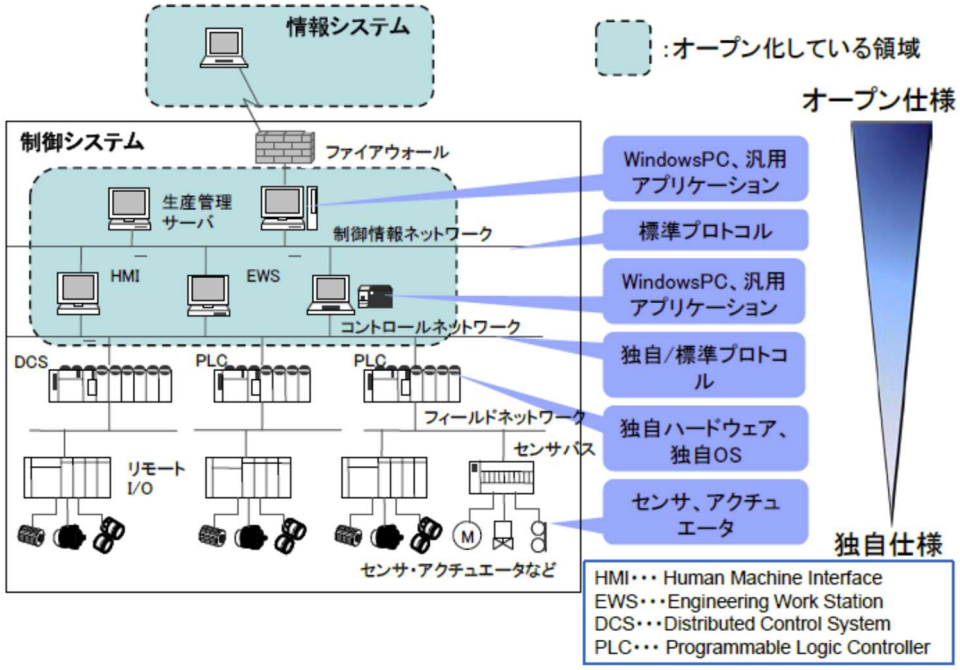
産業系ネットワークのセキュリティレベルを向上させる必要性は誰もが認めるところである。最も重要なインフラ基盤で中核をなすのが ICS であり、このインフラ基盤への不正アクセスの防止とか、物理面も含めサイバーセキュリティ対策が急務である。ICS が外部からのサイバー脅威にさらされるケースとして、産業系ネットワークと IT ネットワークの統合が挙げられる。

多くの ICS は、インターネット接続、Web ベースのアプリケーションといった IT システムが普及する１０数年前に構築されたインフラ基盤が普通で、こうしたレガシーな環境で依然と稼働している場合が殆どだ。制御系システムは**エアーギャップ**化されていたために、セキュリティ対策については後回しにされた。つまり、エアーギャップで産業系ネットワークは外部ネットワークと完全に隔離され、これによって安心・安全の神話が続いていた。

IT/OT 統合の必要性は、徐々に深まりつつある。この統合は当初の段階ではセキュリティ対策は優先事項ではなく、殆ど検討されなかった。最近、企業は IT ネットワークと産業系 OT ネットワークとの統合でインフラ基盤をセキュアに担保するため、その IT/OT のボーダエッジ（境界線）にファイアウォールを導入し始めた。そして必要以外の不明なトラフィックはすべて遮断した。

下図に示すように、エアーギャップはもはや存在しないということになったが、クリティカルな産業システム基盤への潜在的な不正経路が存在し、悪用される可能性が出てきた。

制御システムのオープン化：汎用製品＋標準プロトコル



出典：IPA 作成資料

産業システムで使用される最も一般的な初期攻撃の手口には、スピアフィッシング、水飲み場、DB インジェクションなどがある。ターゲットを絞ったスピアフィッシング（以下注参照）は、オープンソースインテリジェンス（OSINT）を使用してソーシャルエンジニアリングを促進する場合に非常に効果的である。フィッシングメールには、悪意のある添付ファイ

ルが含まれている場合や、悪意のある Web サイトにターゲットを誘導する場合がある。フィッシングされたユーザはそれによって感染し、より広範に拡散してしまう。

（注）フィッシングとは、ユーザを誘い込んで URL をクリックさせる初期のハッキングテクニックで、スピアフィッシングは、それとは対照的に、非常に標的型の攻撃であり、ユーザ個人をだましてリンクをクリックさせたり、添付ファイルを開かせたりする手口。

ペイロードに埋め込むマルウエアの無料キットは、Web attackerやtorrent、Zeus（ZBOT）、Ghostnet（Ghostrat）、Mumba（Zeus v3）、Mariposa などインターネットから容易に入手出来る。サイバー攻撃者は、マルウェアを難読化(Obfuscation)することによって、ウイルス対策やその他の検出メカニズムによる検出を回避させる。

一旦、ネットワークに侵入し、システムが感染すると、マルウェアは他のシステムに拡散しようとする。産業系ネットワークに侵入すると、低いレベルにアクセス出来る脆弱性の弱点を見つけて、この感染の拡散を狙う。つまり、上記で図示するレベル 4 からレベル 3 へのアクティブな脆弱な接続を検出し、そしてそこを踏み台にしてレベル 3 からレベル 2 に深堀りする。このため、強力なサイバーセキュリティ防御対策が重要となる。

APT とマルウェアの武装化

産業システムへの巧妙化されたサイバー攻撃の手口は、その攻撃ターゲットに到達するまでに十分な感染拡散が必要となるので、誰にも分らないようにする可能性が高い。

マルウェアは誰にも分らないように忍び込ませて、マルウェア対策ソフトウェアの無効化や回避、永続的な Rootkit のインストール、トレースファイルを削除したり、リモートアクセス用のバックドアを確立する前に攻撃手口が検出されないようにしたり、ファイアウォールに穴を開けたり、ターゲットネットワークに拡散したりする。

例えば、Stuxnet は産業分野では有名なマルウエアで今年で 10 周年を迎えるが、ホスト侵入検知ツールをバイパスして（従来の IDS/IPS では検出出来ないゼロデイエクスプロイトを使用）検出を回避し、正規なソフトウエアとして偽装 （盗まれたデジタル証明書を使用）し、システムからトレースファイルを削除して追跡できないようにした代表的なものである。特別な予防策として、マルウェアの存在を検出する機能を更に回避するため、Stuxnet は、他のホストに特定の回数感染した後、ホストから自動的に退去する。

Stuxnet やその他最新のマルウェアは、“高度な永続的脅威”（APT）と見なされている。APT の 1 つの側面としては、こうしたマルウェアはしばしば検出が困難であり、持続性を確立する手段を有するため、検出されて除去された場合でもシステムが再起動されても引き続

き攻撃動作し続けることが出来る。サイバー攻撃者は、システムの再感染や、複数の並列浸透ベクトルと方法の使用など、永続的なマルウェアや他の永続性の方法を使用して、広範な一貫性のある成功を確実にする。

他のAPTやエネルギー業界（石油・天然ガスパイプラインを狙う）組織的攻撃例としてNight Dragonなどがある。

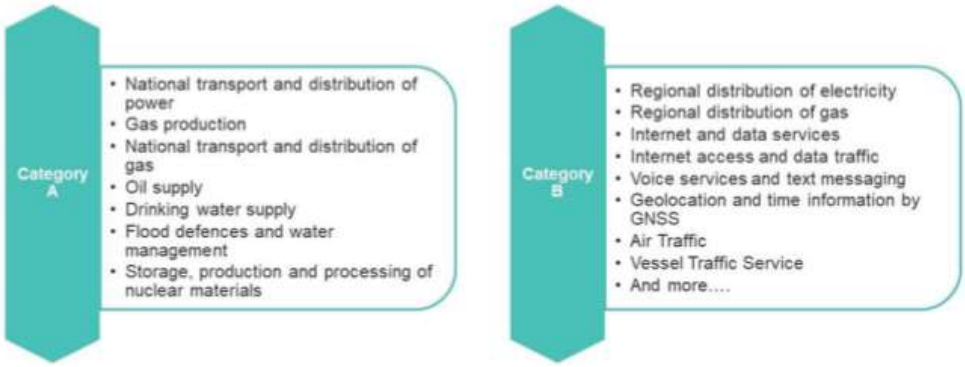
ランサムウェアの猛威

感染した欧州企業から、サプライチェーン経由で国内企業に感染拡散！

2020年6月にホンダとEnelグループで発生したEKANS/SNAKEランサムウエアのインシデントのニュースが世界に報道。日経ビジネスの吉野記者は、書面で「６月のホンダへのEKANS/SNAKEランサムウエアについて、日経ビジネスの吉野記者の記事を引用して、「ホンダに大打撃をもたらした攻撃の実行者はまだ判明していない。それでも状況証拠から民間のサイバー犯罪者だった可能性が浮上している。工場などの産業機器を標的にするのは国家が運用するサイバー部隊であり、民間のサイバー犯 罪者は手を出さないというこれまでの常識を覆す騒動となるかもしれない。」と説明している。

出典：経済産業省商務情報政策局「産業分野におけるサイバーセキュリティ政策」資料

そして、欧州の社会重要インフラ企業では、最近ランサムウエア攻撃が多発しており、以下のカテゴリーが狙われているようだ。



おわりに

産業系ネットワークといっても多岐にわたっており、IPAは重要インフラ分野を特定してICSセキュリティに向けたガイドラインを作成している。国内製造業の場合、国内だけでなく海外を含め、サプライチェーンによる分業構造が基盤となっている。このことは、すなわち脆弱性を含めたセキュリティ対策レベルの低い拠点を踏み台にしたサイバー攻撃が今後も起こりうるということだ。そして、COVID-19を契機に、CIセクター(CI:Critical Infrastructure)のサイバーセキュリティリスクが加速すると予測されている。