制御システムにおける営業秘密保護について

2017年5月29日

技術研究組合制御システムセキュリティセンター
村瀬 一郎

制御システムネットワーク

CSSCではコントローラを中心としたシステムを制御システムと呼ぶ

・制御情報ネットワークは、IP（Internet Protcol）化が進んでいる
・制御ネットワークは、必ずしもIP化されておらず、制御ネットワークは非IPであることも多い
・リモートメンテナンス回線・リモート監視回線はIP化が進んでいる
・通信機器と端末・サーバは、汎用化が進んでいる

PLCとDCS

DCS

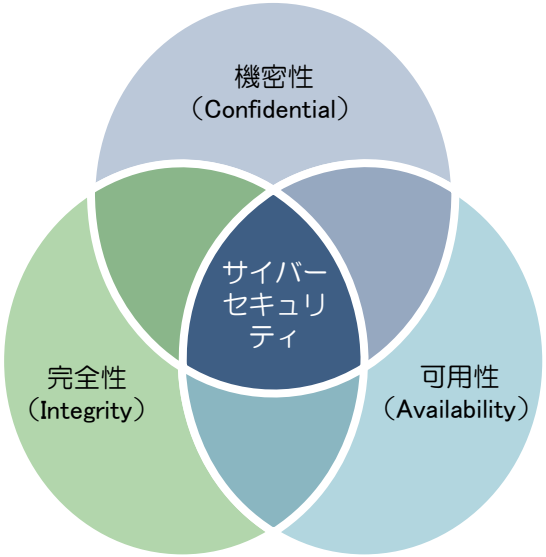
一般に、DCSは、オペレータ（運転員）が制御・監視を行うためのHMI（Human Machine Interface）と、フィールドネットワークに接続して、HMI とコントローラを接続する制御ネットワークの3つの構成要素からなる。化学やガスプラントで利用。

PLC

PLC は、パソコンと監視・制御ソフトウェアの組み合わせ行するものである。組

情報システムセキュリティと制御システムセキュリティ

- サイバーセキュリティとは、資産(情報や装置etc)の機密性・完全性・可用性を維持することである。これらはサイバーセキュリティの３要件とされ、英語の頭文字を取ってCIAと呼ばれる。いずれの要素についてもバランスよく維持することが重要である。
  - 機密性（Confidential）
    - 許可された者が許可された方法でのみ資産にアクセスできることを確実にすること。つまり、権限のないユーザーがアクセスできないようにすること。
  - 完全性（Integrity）
    - 資産の正確さ及び完全さを保護する特性
  - 可用性（Availability）
    - 許可された利用者が必要な時に適時にアクセス可能であり、確実に利用できる状態

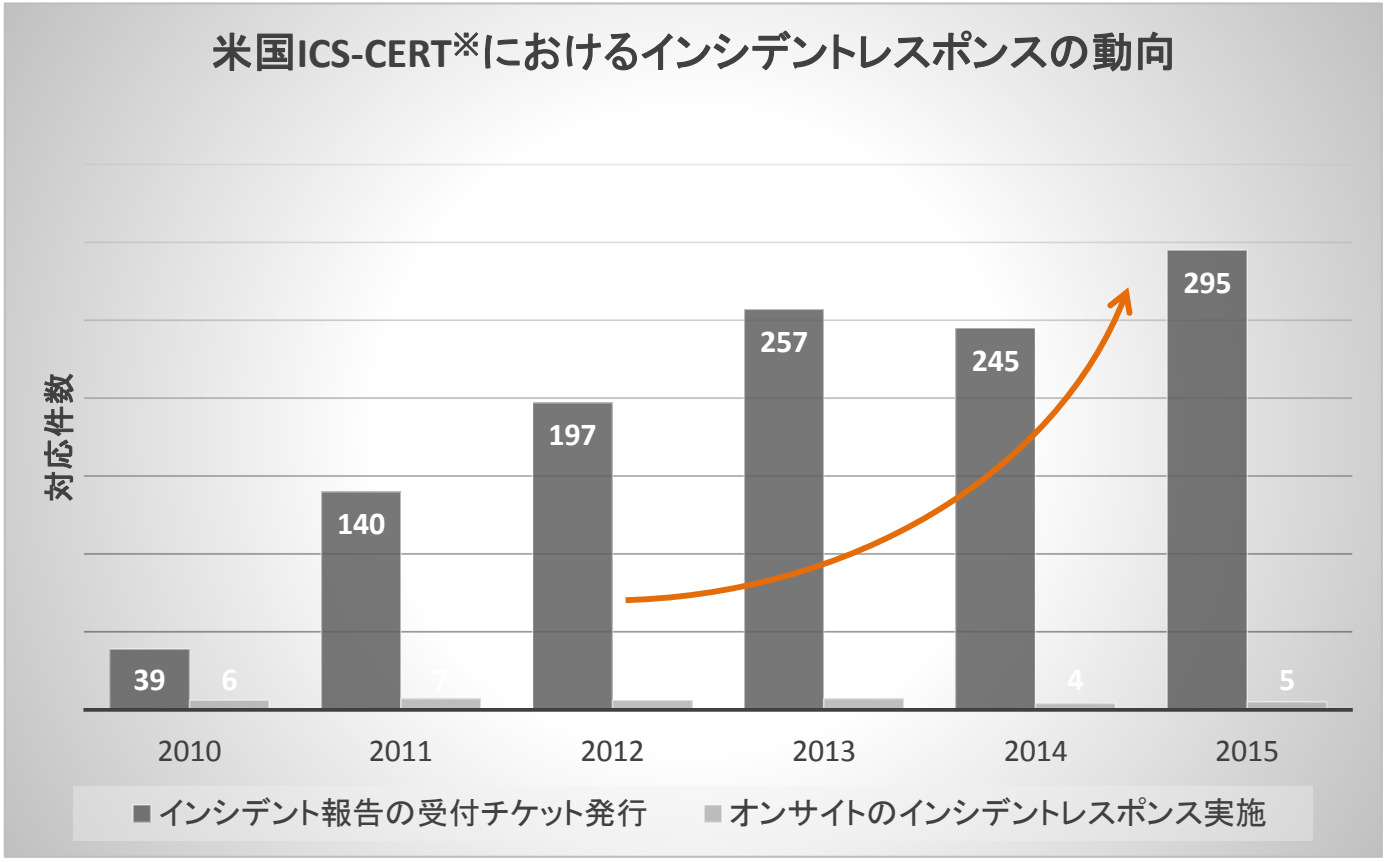


・制御システムにおいても、情報システムにおいても、可用性・機密性・完全性のバランスを確保することが重要。

・可用性を阻害する技術、機密性を阻害する技術、完全性を阻害する技術はそれぞれ特徴がある

制御システムのセキュリティインシデントの動向

- 制御システムにおけるインシデントは世界的に増加傾向
- 2010年度にStuxnetによって制御システムへの攻撃が顕在化
- 2015年度は1位工場(97)、2位電力(46)、3位水道(25)、化学(4)



※ICS-CERTとは

米国国土安全保障省（DHS）が運営する制御システムに特化したインシデント対応機関。制御システムに関する国内のインシデント報告を受け、専門家による分析・対応サービスを提供する。
(http://www.us-cert.gov/control_systems/ics-cert/)

出典：ICS-CERT, “ICS-CERT Year in Review FY2015_Final“ に基づき作成

ウクライナの大規模停電

- 2015年12月23日にウクライナでサイバー攻撃による大規模停電（電力会社2-3社、影響人数 約22万人、停電時間3時間程度）が発生した。
- 当初はBlackEnergy3と呼ばれるマルウェアにより、監視制御システムのサーバのハードディスクが破壊されたことにより停電が発生したと報道されていたが、ハードディスクの破壊が停電に直結することは考えにくい。
- その後、リモート制御により（30カ所、110万ボルト級変電所7か所、35万ボルト級変電所23か所）のブレーカー遮断がなされたことが判明した。（BlackEnergy3の関与は不明）
- ウクライナ政府は、ICS-CERTに調査を要請し、ICS-CERTは以下の調査結果を発表した。

1.約22万5千人の顧客に影響が及んだ。
2.VPN接続を介して電力会社の監視制御システムへアクセスが行われていた。
3.一連の攻撃にBlackEnegryが初期のアクセス手段として用いられたかどうかは定かではない。

http://styknews.info/novyny/ns/2015/12/23/frankivsk-na-pivgodyny-zalyshyvsia-bez-svitla-foto

Havex (Dragon Fly)のインシデント事例

- Stuxnet以来と言われる制御システムを狙ったマルウェアが2014年に発見。
- 制御システムの異機種間（あるいは内部）データ交換に多く使われるOPCクラシック（DA）を狙うトロイの木馬型マルウェア。
- 外部に接続した保守用PC経由で制御システム上のOPCサーバの情報を外部（攻撃者）へ送信する。

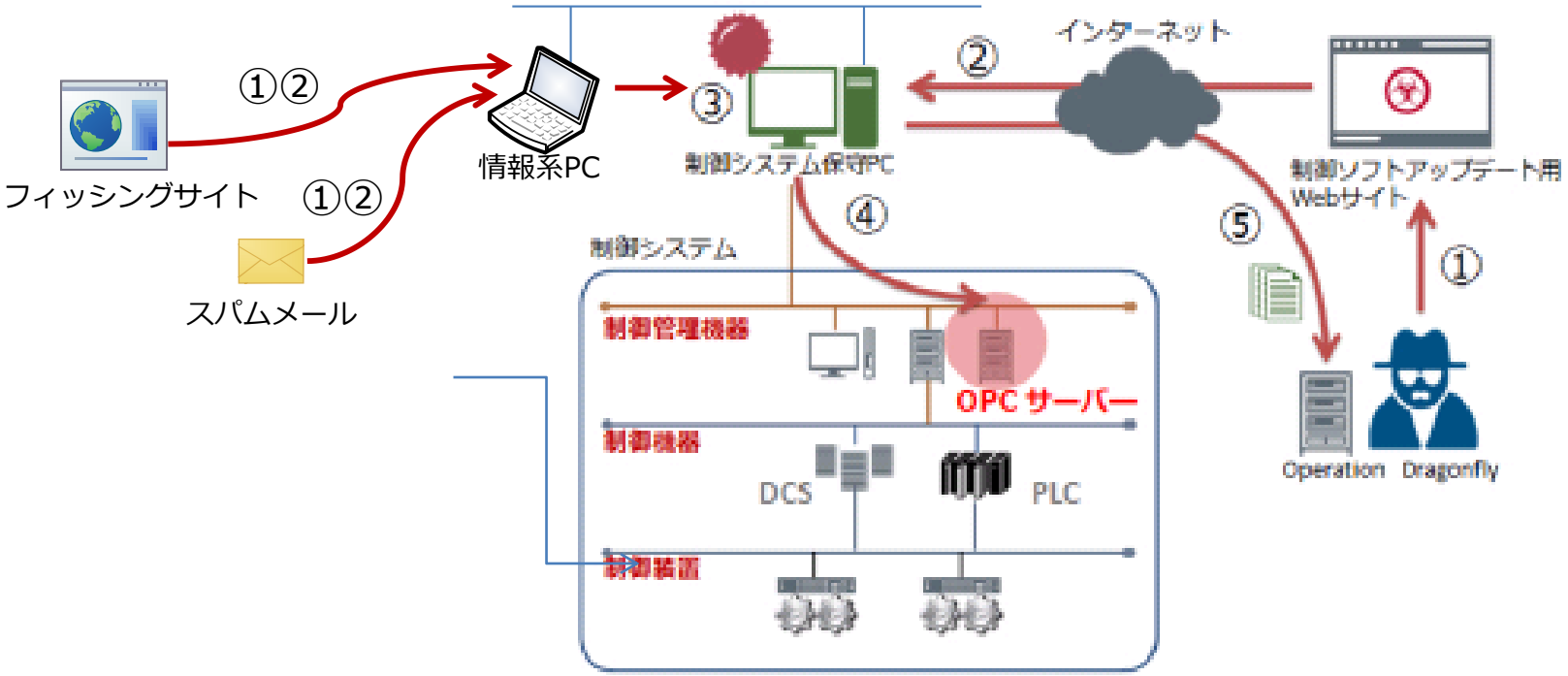
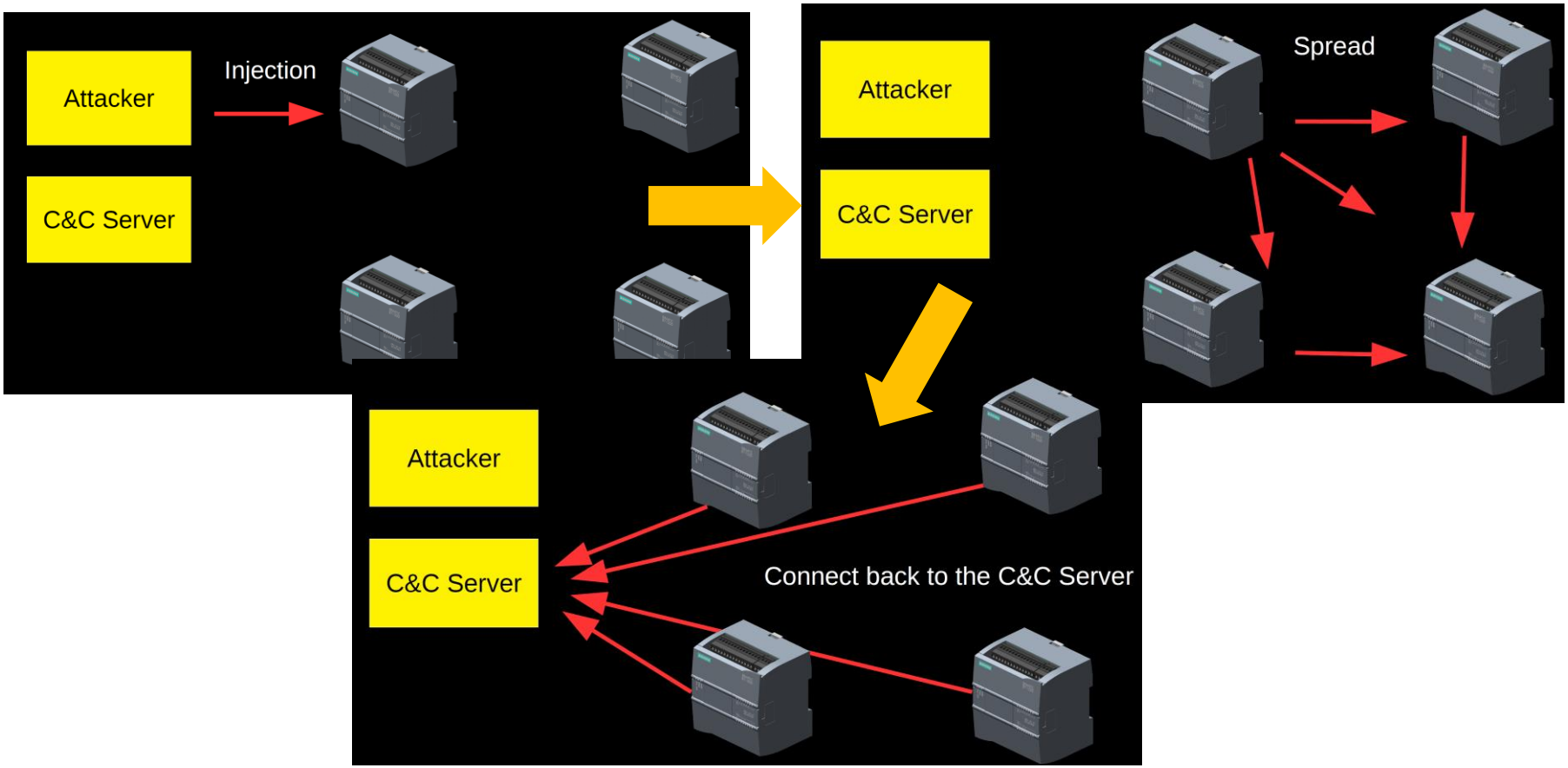


図1：Operation Dragonfly の制御システムベンダーのWebサイトを使った攻撃の仕組み（マカフィー社資料より）

注：マカフィー社＋他資料より

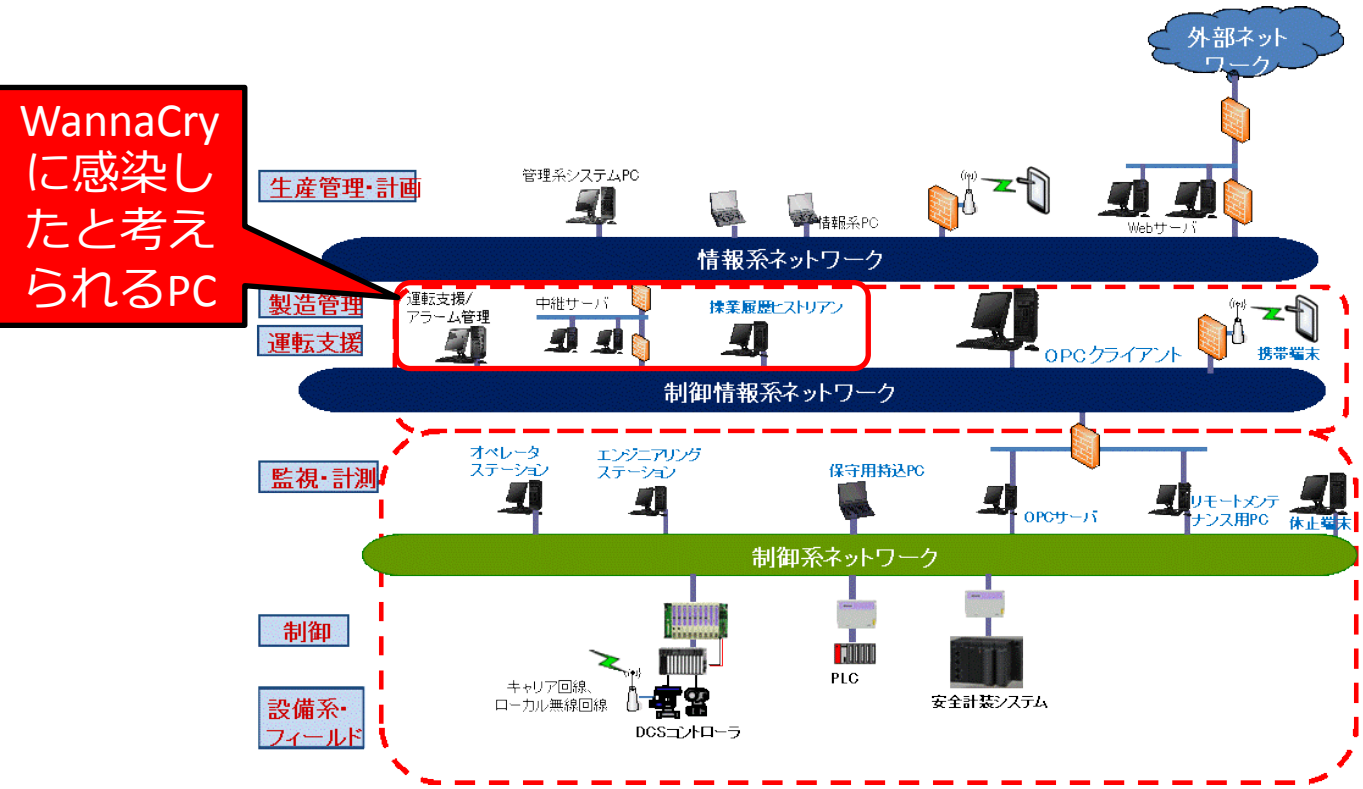
新たなる脅威PLC Blaster(Black Hat 2015,2016)

- PLCへ拡散・攻撃するマルウェアが登場した。
- 攻撃はPLCのオリジナルコードの後に悪意あるプログラムを挿入する。
- ベンダー独自の通信プロトコルを攻撃者に解析され、開発されている。



Source: https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf

WannaCryと制御システム



英国の日産サンダーランド自動車工場5月13日頃より工場内で障害が発生し、自動車生産が一時的に止まるなどして影響が生じた。

我が国の制御システムでの脅威

USBポート

- USBメモリからのウィルス感染事例は頻繁に発生している

リモートメンテナンス回線

- 某社は米国の中央監視室からリモートメンテナンス回線によりタービンをリアルタイム監視
- リモートメンテナンス回線の先の端末からの不正アクセス・マルウェア混入

操作端末の入れ替え

- 日本の自動車会社では、ベンダが入れ替えた端末にウィルスが混入していた事例あり

物理的侵入

- 監視端末のパスワードが無い
- IDやパスワードは共通化、壁に張出し

その他

- 制御システムに関わるシステム構成図等が学会・ベンダ技術雑誌・広報誌・ウェブサイト等に公開されている

まとめ

1. 機密性・可用性・完全性

制御システム（情報システムでも）においては、機密性確保だけではなく、可用性確保が重要な場面が存在し、機密性・可用性・完全性のバランスが重要

2. 制御システムにおける機密性

- 可用性を阻害するための攻撃を受ける可能性を排除するために、システム構成や仕様等の機密性確保は重要
- 一部分野（化学分野・医療品分野等）においては、製品製造のためのシステム構成や制御パラメータが製造ノウハウであるため機密性レベルが高い

3. 橋渡し人材

経営層に、対策の必要性・コストを話すことができる人材

以下の素養が必要

-制御システムとセキュリティに関わる技術的素養

-経営的視点（ビジネスリスク分析と管理、人事、法制度、経理等）