制御システム向けサイバー攻撃センサの開発

Development of cyber attack detection system for ICS

有元　伯治　Michiharu Arimoto
佐々木　太一　Taichi Sasaki
佐内　大司　Daiji Sanai

キーワード
セキュリティ，サイバー攻撃，攻撃検知，制御システム，重要インフラ

近年，社会インフラや産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大している。東京オリンピック・パラリンピックを狙ったサイバー攻撃も懸念され，重要インフラにおけるサイバー攻撃への対策が急務となっている。このニーズをうけて，制御システム（ICS：Industrial Control Systems）向けのサイバー攻撃検知センサを開発した。これにより，もし制御システムにサイバー攻撃が侵入しても，システム内部での攻撃を早期に検出することを期待できる。本稿では，その検知技術について報告する。

In recent years, the risk of cyber-attacks that damage public and industrial infrastructure has increased. There are also concerns about cyber-attacks aimed at the Tokyo Olympics and Paralympics. Measures against cyber-attacks on critical infrastructure are therefore urgently needed. To meet this need, we have developed a cyber-attack sensor for industrial control systems. With this sensor, even if an attacker manages to enter the control system, detection of the attack at an early stage can be expected. In this paper, we report on the detection technology.

1. 背景

2019年4月1日，サイバーセキュリティ基本法改正が施行され，重要インフラ事業者等におけるサイバーセキュリティの確保が義務化された。2019年8月の時点で重要インフラ事業者として指定されているのは，情報通信，金融，航空，空港，鉄道，電力，ガス，政府・行政サービス，医療，水道，物流，化学，クレジットおよび石油の14分野であるが，それ以外の産業分野を含めて，2020東京オリンピック・パラリンピックの開催までの早急なセキュリティ対策が求められている。

このような中で，「人を中心としたオートメーション」で事業展開をするazbilグループは，重要インフラ事業者に制御システム（図1参照）を提供している。制御システムのサイバーセキュリティの確保の要となる，ローカルネットワークにおけるセキュリティ技術を2000年から研究開発してきた。

本稿では，制御システムのセキュリティ上の特徴と，制御システム向けのサイバー攻撃検知センサの検知技術について説明する。

2. 制御ネットワークの特徴とセキュリティ課題

制御システムの構成は，分野や業種によって差異はあるが，センサやアクチュエータが繋がるフィールドネットワーク，PLC（Programmable Logic Controller），DCS（Distributed Control System）などのコントローラ，EWS（Engineering WorkStation：エンジニアリング・ワークステーション）やOPC（OLE for Process Control）サーバなどが繋がる制御系ネットワーク，生産管理サーバなどが繋がる制御系情報ネットワークから構成される（図1）。

制御情報ネットワークや制御システムネットワークに接続されているHMI（Human-Machine Interface），EWS，OPCサーバなどにはWindows®が多く使われているため，これらのネットワーク・セグメントはWindowsネットワークで成されていることが多い。そのため，サイバー攻撃の最初のターゲットとされるのが，これらのネットワーク上のWindowsである。

Windowsを中心に構成される制御ネットワークをセキュリティの視点で見たとき，同じようにWindows中心のオフィスの情報系ネットワークとは違った次のような特徴がある。

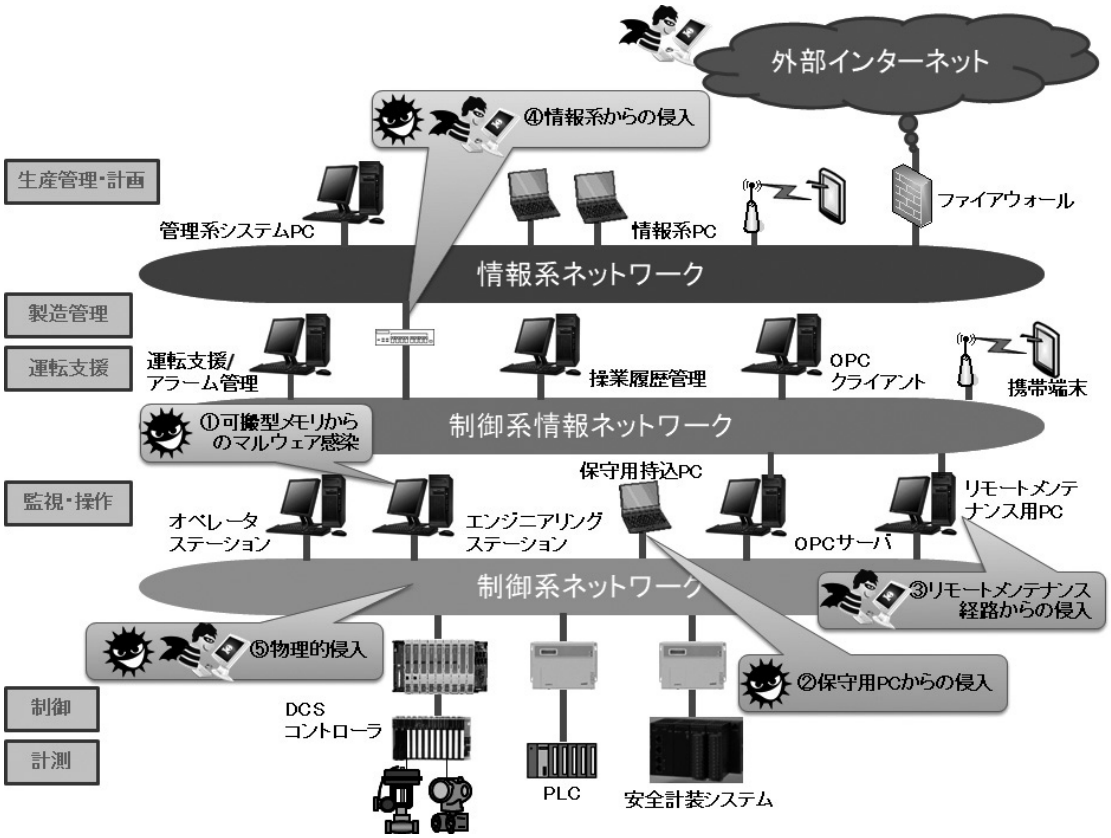

図1　制御システムの構成 [1]

(1)24時間連続運転

制御システムの多くは，24時間365日連続稼働することを基本として設計されていて，これらを停止するのは，計画的な定期メンテナンスの時だけである。そのときでも，安定して動作することを優先するためにOSのパッチの適用はほとんど行われない。

(2)長い使用年数

制御システムは，ひとたび稼働すると10年～20年と長い期間使用される。

(3)古いOSが使われている

使用年数が長いため，既にサポート切れになっているOSがそのまま稼働していることがある。可用性が優先であり，リスクを伴うOSの更新は先送りにされてきた。

(4)古い設計思想

10年以上前の古い設計思想で設計されている。当時の設計では，利便性の高いファイル共有手段として，Administratorアカウントや管理共有(C$やAdmin$など)が多用されていた。この問題は，システムを丸ごと乗っ取られてしまう危険性があり，サポート切れのOSの問題よりも根が深いが，あまり認知されていない。

(5)共通アカウント

すべてのWindowsにおいて共通のユーザーアカウントとパスワードが使用されている。

(6)メンテナンスPCの接続

メンテナンス用のWindowsを必要に応じて，システムに接続することがある。

(7)決められたアクセスだけのネットワーク

オフィスのような人によるアクセスではなく，設計されたとおりに決められたアクセスだけが発生する。制御システムでは，決められたアクセス以外が発生する場合は，何らかの異常が発生していることが疑われる。

3. Windows ネットワークの基礎知識

3.1 Windowsへの侵入/操作とは

Windowsは他のWindowsを自由に管理できるネットワーク関連機能を標準搭載している。Windowsの共有機能が有効になっているとき，Administratorグループのユーザーアカウントとそのパスワードが分かりさえすれば，他のWindowsを自由にコントロールすることができる。管理共有に接続できる状態は，このWindowsを自由にコントロールできる状態である。

そして，ローカルネットワークに侵入した後のサイバー攻撃の多くは，この標準機能を悪用しているが，このような管理機能があることは一般ユーザーにはあまり認識されていない。

3.2 Windowsのセキュリティ機能とその推移

Windowsはバージョンアップを繰り返し，セキュリティを強化してきた(図2)。Windows® XPでは，DCOM (Distributed Component Object Model)をはじめとしたネットワーク機能に対して，ポリシーによるアクセス制御が加えられた。

Windows XP SP2（Service Pack 2）とWindows Server® 2003では，ファイアウォールが標準搭載され，必要最低限のサービス以外へのアクセスが制限された。さらに，Windows Vista®とWindows Server® 2008から導入されたユーザーアカウント制御（UAC:User Account Control）により，管理者権限を必要とするプログラムの実行が制限された。そして，Windows 10では，アンチマルウェア機能としてWindows Defenderが標準搭載された。

3.3 DCOMのセキュリティ

DCOMは，米マイクロソフトが開発したCOM（Component Object Model）を拡張した分散コンピューティング環境である。共通のアカウントとパスワードをもつコンピュータ間で自動的に接続できてしまう。

米マイクロソフトは，これへのセキュリティ対策として，デフォルトではDCOMを利用できないように制限した。この機能を利用するためには，Windowsのファイアウォールの設定を変更し，さらにUACを無効にする必要がある。

制御システムで使われることがあるOPC Classicは，クライアントとサーバの接続にDCOM通信を使用している。そのため，OPCが動作しているPCは，DCOMを悪用されるリスクがある。

4. 制御システムにおけるサイバー攻撃検知へのアプローチ

4.1 基本アプローチ

我々は制御システム上を流れるWindowsネットワークをレイヤー7で分析し，Windowsの危険な操作やサイバー攻撃を検知することに取り組んだ。WindowsネットワークのSMB（Server Message Block）やMSRPC（Microsoft Remote Procedure Call）などを分析することにより，詳細なネットワーク活動を監視できる。制御システムに悪影響がないようにパケットキャプチャ方式を採用した。パケットキャプチャ方式は，システムの構成ノード上で稼働する必要がなく，また，システムのネットワークにパケットを送出しないため制御システムに負荷をかけない。

ITシステムと同様に制御システムにおいても，Windowsのファイル共有やデータ交換などが行われており，Windowsのネットワークコマンドが流れている。サイバー攻撃により発生したネットワークコマンドも消去や改変することはできず，正常な操作によるものに紛れてネットワークを流れる。その中から，サイバー攻撃や危険な操作が行われた場合の特徴を捉えた攻撃検知を試みた。

4.2 研究開発

まず，サイバー攻撃に利用される可能性のあるWindows API（Application Programming Interface）を洗い出した。そのAPIが実行された際に飛ぶネットワークパケットを多面的に分析した。攻撃者の手法は，マルウェアやハッキングツール，シェルなど様々で特定できないが，攻撃者がどのようなツールやコマンドを用いるかにはかかわらず，その内部ではWindows APIが実行されている。

Windowsには数千種類のWindows APIがある。ハッカーがサイバー攻撃を行うとき，これらのWindows APIが利用されている。そして，ハッカーが多用するAPIには管理者権限が必要であることが多い。我々はここに注目した。そこで，管理者権限を必要とすることが多いシステム管理のAPIを調査した。例えば，それは，イベントログ，レジストリ，サービス，アカウントなどを管理するAPIである。さらに，リモート

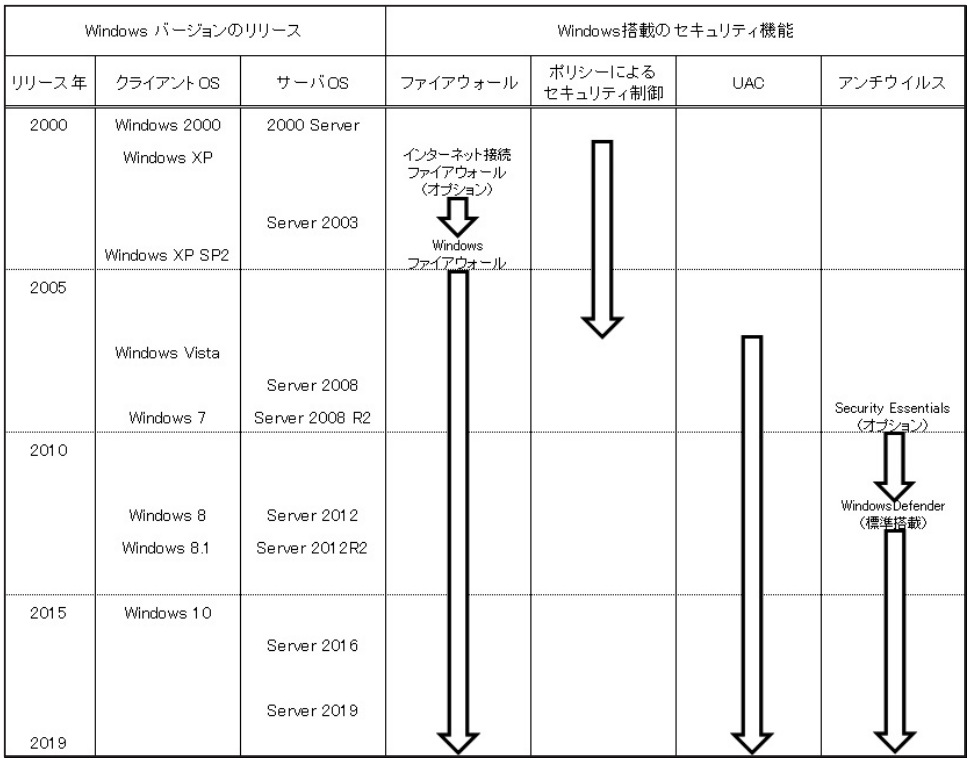

図2　Windowsのセキュリティ機能とその推移

コンピュータに対して実行可能なAPIとネットワークコマンドとの関連性を調査し，マッピングした。

その結果，ネットワークコマンドから管理者操作をある程度特定できることが分かった。そして，このネットワークコマンドは，ハッカーの隠ぺい工作の影響を受けにくいことから，ネットワークコマンド監視によるサイバー攻撃検知手法は実用性の高い手法だといえる。

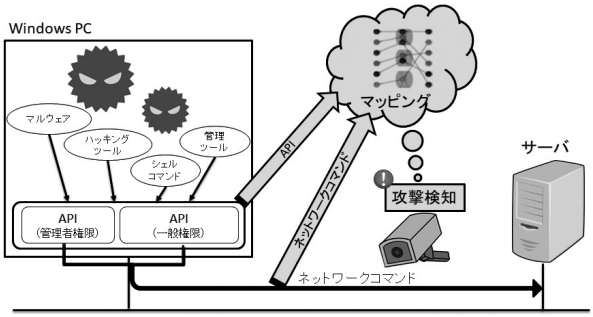

図3　Windows APIとネットワークコマンドのマッピング

Windows APIとネットワークコマンドの関連性の調査とマッピングに加えて，制御システムの特徴やハッカーの行動特性を考慮し，以下の調査も行った。

(1) Windows XPなど古いWindowsのAPIとネットワークコマンドの関連性の調査，マッピング
(2) 制御システムで特徴的なDCOM利用時の管理操作とネットワークコマンドのマッピング
(3) アクセス制限のかかる管理者コマンドの洗い出しと，ネットワークコマンドへのマッピング
(4) 古い設計思想のシステムの特徴をネットワークコマンドとマッピング
(5) ハッカーの活動の微かな痕跡とそのネットワークコマンドに現れる特徴を調査
(6) ハッカーの行動パターンから，関連するネットワークコマンドを調査
(7) Windowsのシステムが利用する非公開APIの調査

4.3　サイバー攻撃を検知するネットワークセンサの実装

我々は，これまでWindowsネットワーク解析技術（VISUACTテクノロジー）を開発[2]してきた。この技術によりWindowsネットワークのパケットをリアルタイムで解析し，ネットワークコマンドを抽出することができる。それに，本稿で述べたWindows APIとネットワークコマンドのマッピング技術を組み合わせて，サイバー攻撃を検知するネットワークセンサを開発した。このセンサによって，正規なアクセスに紛れた攻撃や不審なアクセスを検知することが可能になった。これにより，制御システムへの現実的なセキュリティ対策の導入を目指している。

5. 稼働中の制御システムへの現実的なセキュリティ対策

5.1　現場で稼働システムの現状を調査

稼働中の制御システムに対して，システムに影響を及ぼすセキュリティ対策の導入はリスクがある。サイバー攻撃検知センサは，パケットキャプチャ方式を採用し，稼働中のシステムに影響なく，既存ネットワークに設置できる。現場でシステムの現状を調査し，マルウェアによる攻撃を検知したり，システムの使われ方やセキュリティ上の弱点を洗い出せる。

これまで，重要インフラを中心とした制御システムで，サイバー攻撃検知センサを使ったセキュリティ検査を行ってきた。その結果，予想以上に多くのシステムで，危険なコマンドや操作が検知された。制御システムで特徴的にみられる旧OSや共通アカウント，管理共有の利用など，古い設計思想による設定，運用が行われていることに起因するものが多くみられた。

5.2　システムの弱点監視を強化

連続稼働している制御システムでは，問題や弱点が発見された場合でも，設計変更やシステム更新を，短期的に実施することは難しい。しかし，短期的な対策が難しいにしても，システムが侵害されやすい状態にあることを認識し，運用上利用せざるを得ない弱点部分を中心にセキュリティ監視の強化を実施する必要がある。ここでは，システムの弱点に対して，攻撃や不審なアクセスがないか重点的に監視することが重要である。

5.3　設計仕様外の通信を監視

制御システムでは設計仕様どおりの通信が行われるのが原則である。通信するノードの組合わせがあらかじめ決められているので，設計上想定外の通信を監視することが有効である。設計外の通信が見つかれば，攻撃の可能性があり，調査や監視強化の対象になる。

設計外のIPアドレスやポートの組合わせが発生していないかを監視し，気づきを提供する。さらに，Windowsネットワークの監視によって，攻撃に使われるコマンドを検知することができる。

6. 新しいセキュリティ課題への挑戦

我々は，想定できないサイバー攻撃の手口に追従するために，その根底にある普遍的な課題に取り組んできた。新しいネットワークの機能はハッカーの行動の見えない化にも利用されるが，それらの検知が今後の課題となる。現在，次の2つの技術課題に取り組んでいる。

(1) ネットワークの暗号化とその弊害

データの機密性がますます求められるため，これからのネットワークが暗号化されていくことは間違いない。その半面で，ネットワークが暗号化されると通信内容が見えなくなるというリスクがある。つまり，暗号化は，サイバー攻撃の隠蔽に利用され，サイバー攻撃を検知できなくなる可能性がある。そこで，暗号化によって通信内容がわからなくても，サイバー攻撃を検知できる新しいアルゴリズムが必要となる。

(2) IPv6（Internet Protocol Version 6）への対応

IoTの加速にともなって，IPv6の普及も加速している。一方で，ハッカーは，以前よりIPv6を悪用してきた。このこ

とは，あまり認識されていない。そのため，IPv6に未対応のツールが多いという現実がある。IPv6をベースとした攻撃の監視や検知のための技術開発が急務である。

＜参考文献＞
(1) 木内誠，田中良則，関英信，黒木亮，小森谷良明:「ICSのサイバーセキュリティへの取組み。今，生産制御システム（ICS）が狙われている！」，azbil Technical Review，2015年4月発行号，pp.25-32
(2)「いつ，誰が，どこのファイルに，何をしたのか？」，azbil Technical Review特別別冊 azbil 技術レポート 2006，pp.47-48

＜著者所属＞
有元　伯治　アズビル株式会社
IT開発本部開発1部
佐々木　太一　アズビル株式会社
IT開発本部開発1部
佐内　大司　アズビル株式会社
人事部付