

IPA テクニカルウォッチ

『新しいタイプの攻撃』に関するレポート

～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～

# IPA テクニカルウォッチ：『新しいタイプの攻撃』に関するレポート

～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～

## 目次

---

1. 昨今のサイバー攻撃の実態と傾向.....	2
1.1. 新しいサイバー攻撃手法の出現.....	2
1.2. 社会インフラへの攻撃の広がり.....	2
2. 『新しいタイプの攻撃』の実態.....	2
2.1. 脅威・問題点分析について.....	2
2.2. 『新しいタイプの攻撃』の流れ.....	3
3. 『新しいタイプの攻撃』に関する対策と課題.....	4
4. IPAの今後の取組み.....	6
4.1. 脅威と対策研究会.....	6
付録1：『新しいタイプの攻撃』の解析.....	7
付録2：システム環境の変化.....	9
付録3：サイバー攻撃に関する各国の反応.....	10

# IPA テクニカルウォッチ：『新しいタイプの攻撃』に関するレポート

～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～

2010年12月17日

IPA（独立行政法人 情報処理推進機構）

セキュリティセンター

## 1. 昨今のサイバー攻撃の実態と傾向

### 1.1. 新しいサイバー攻撃手法の出現

脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃が出現してきている。この新しいサイバー攻撃は2010年の春頃から海外ではAPT(Advanced Persistent Threats)と呼ばれている。

IPAでは、システムへの潜入等の「共通攻撃手法」と情報窃取等の目標に応じた「個別攻撃手法」から構成される攻撃であると分析した。このように「共通攻撃手法」と「個別攻撃手法」を持った攻撃をIPAでは、『新しいタイプの攻撃』と呼ぶ。

この攻撃を使った最近の事例としては世界的に話題となった Stuxnet と呼ばれるコンピュータウイルスが挙げられる。Stuxnet は、原子力発電所の制御システムに影響を及ぼしたのではと報道されている。なお、日本国内でも数件の検出事例が報告されているが、被害事例は報告されていない。

### 1.2. 社会インフラへの攻撃の広がり

従来の攻撃対象は、情報システムであり、そのシステム上にある資産や情報等を狙ったものであった。電力や鉄道等のような社会インフラは、制御システムを組み込んで、実現されている。そのため制御システムを攻撃されると社会インフラが影響を受け、社会全体が影響を受ける可能性がある。

このように、社会インフラが攻撃者のターゲットになったことに合わせて、防御側が守るべきシステム範囲も広がり、制御システムの関係者を巻き込んだ体制も必要となってきている。

## 2. 『新しいタイプの攻撃』の実態

IPAでは、システムへの潜入等の「共通攻撃手法」と情報窃取等の目標に応じた「個別攻撃手法」から構成される攻撃であると分析した。

### 2.1. 脅威・問題点分析について

脅威は、システム構成や業務などで異なる。「個別攻撃手法」の対象を、情報システムや制御システムにすることにより、幅広い各種システムが攻撃対象となり、個別の防御対策は困難である。

例えば日本において、前述の制御システムは、一般に米国等と比較して、制御ネットワークが独立・分離されている事に加え、制御システムも今回悪用された制御システムの製品ベンダーとは異なる事から、直ちに、海外と同様の脅威が発生するとは限らない。日本における適切な対策を進めるためには、単に技術的な情報を海外から得るだけでは無く、日本の実情に応じた分析と対策を行う必要がある。

そのためには、「共通攻撃手法」に対する対策を、日本の実情に応じた影響(ビジネスインパクト)をシステム設計の中で検討し、対策を実施することが重要である。

また、攻撃者は Windows や Linux に熟知しているだけでなく、制御システムについての知識も十分持っていると推測される。このような攻撃者に対応するためには、防御側でも制御システムを含む幅広い技術者の連携で対応する必要があるということも言える。

## 2.2. 『新しいタイプの攻撃』の流れ

標的型メール攻撃や USB メモリを悪用したウイルス等による組織の情報搾取を目的とした情報システムへの攻撃においても同様な共通の攻撃手法が用いられる。セキュリティベンダー等の各機関が出しているレポートやIPAでの解析結果<sup>1</sup>を踏まえると、『新しいタイプの攻撃』は概ね下記のようなステップで攻撃が行われる。

### ＜「共通攻撃手法」と「個別攻撃手法」の流れ＞

(「共通攻撃手法」)

- ① インターネットや USB メモリを通じた情報システムへのウイルス感染
- ② システムの脆弱性を利用することによる情報システム環境内部でウイルスの拡散
- ③ バックドアを作成し、外部の指令サーバ(C&C サーバ)と通信することにより、ウイルスの増強や新たなウイルスのダウンロードの実行  
※ウイルスの増強やダウンロードは以降④⑤の手順でも実行される可能性あり。

(「個別攻撃手法」: Stuxnet の場合)

- ④ 原子カシステム等を制御する装置が配備してある、制御システムへの侵入
- ⑤ 制御システム上にある装置に対する攻撃の実行

### ＜『新しいタイプの攻撃』イメージ＞

『新しいタイプの攻撃』をロケットの例で考えてみると、下記の図のように特定のシステムへの攻撃に特化した(「個別攻撃手法」)ペイロード部と特定のシステムに侵入する為の共通仕様部分(「共通攻撃手法」)のランチャー部に分けることができる。一連の攻撃の流れで考えると、ペイロード部とランチャー部からなるロケットが、システムに侵入し、ペイロード部で特定のシステムに攻撃を加える。即ち、実際に目的を達成するためのペイロード部を積んだロケットが目的地に向けて、発射される形となる。

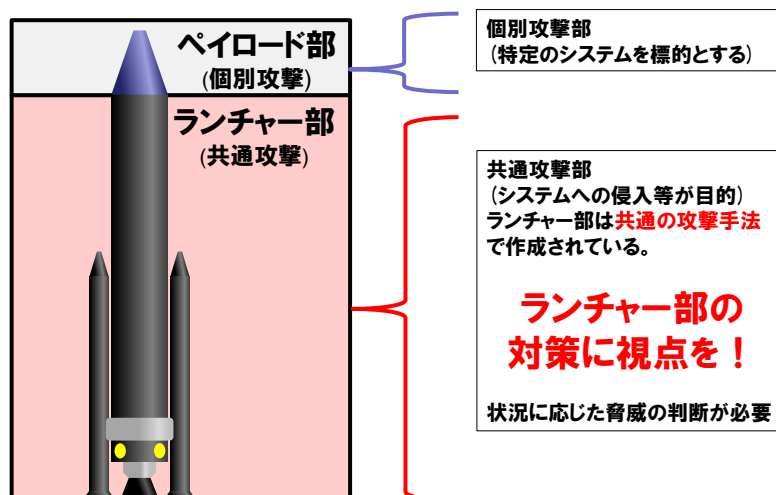


図 2.2-1 ロケットを例にした『新しいタイプの攻撃』のイメージ

<sup>1</sup> 付録 1: 『新しいタイプの攻撃』の解析を参照。

### 3. 『新しいタイプの攻撃』に関する対策と課題

本章では、先に挙げた「ペイロード部」と「ランチャー部」に分けて、対策と今後の課題について述べる。

#### <ペイロード部の対策と課題>

##### 1)対策

ペイロード部については、制御システム等はオープンでない環境であり、かつ設計や構成情報が開示されていない為、組織やシステムの特性に合わせて対策を行う必要がある。ただ、個別対策となると膨大なコストや対策が間に合わない可能性がある為、ペイロード部が制御システムに送り込まれる前段である、ランチャー部と合わせた形で対策を考えていく必要がある。

##### 2)課題

日本国内の実情として、制御システムと情報システムを管理する機関や部門は別々に存在し、双方で情報が共有できておらず、システム全体で対策の立案が難しい状況にある。その為、汎用的なサイバーセキュリティ対策技術と組織のシステム構成に特化した対策技術の両者が必要であることから、攻撃に応じた技術や対応体制の連携が必要である。

#### <ランチャー部の対策と課題>

##### 1)対策

ランチャー部の攻撃の特徴は、対策が行えない未知（ゼロデイ）の脆弱性が利用されており、ウイルスのパターンファイルの更新だけでは防げないケースがあり、従来の製品ベースの対策だけでは困難な状況にある。ランチャー部の対策において、着目すべき点は、攻撃が第1ステップの侵入、第2ステップの複製、第3ステップの外部からの指らの指令の受信といったように、多層ステップから構成されることである。その為、対策としては、攻撃者との通信を遮断する為にネットワークレベルでの多層的な防御を行い、攻撃の最終目標まで到達する前にネットワークを介した動きを封じる必要がある。表3.1に、内閣官房情報セキュリティセンター(NISC)で検討された成果<sup>2</sup>をもとに「脅威と対策研究会」<sup>3</sup>で纏めた6つの対策を提案する。

---

<sup>2</sup> <http://www.nisc.go.jp/inquiry/index.html>

<sup>3</sup> 4.1「脅威と対策研究会」を参照。

表 3.1 システム・ネットワーク設計対策要件

No	機能要件項目	機能要件内容	要件理由及び背景	設計事例
1	プロキシの認証情報のチェック	一般 PC の外部 Web アクセス時、認証プロキシによる認証アクセスを設計。	ウイルスが、独自の通信メソッドを用いて搾取した情報を悪性サイトに送信する場合、認証情報を使用しない場合が多いことが確認されている。 ※ウイルスが既認証状態を使用した攻撃仕様となった場合は、防止出来ない。	・認証プロキシ
2	HTTP,SSL 通信のヘッダーチェック	外部通信（GET,POST コマンドのヘッダー等通信内容）の検出・遮断。	ウイルスが窃取した情報を外部の悪性サイトに送付する場合、新たな攻撃コードをダウンロードする場合、C&C サーバからの指示を受信する場合に多くは 80/tcp,443/tcp が用いられる。	・NOC/SOC 監視
3	未知のウイルスを検出可能なソフトウェアの導入	ゼロデイ脆弱性含む、ウイルスが脆弱性を使用した時の挙動検知。	PC 上のウイルスの脆弱性利用等の挙動などから攻撃動作を検出することにより、未知ウイルスや、未知の脆弱性を突く「ゼロデイ攻撃」を検出し防御することが可能な製品が複数の企業から発表されてきている。 ・ただし、従来のウイルス対策ソフトを補完するものとして、防御機能、管理工数等十分な評価の上で設計利用検討の可能性がある。	・振り舞い検知タイプのウイルス対策ソフトの導入
4	スイッチ等での VLAN ネットワーク分離設計	ルータ、スイッチによる必要なアクセス範囲に限定した、VLAN 及びルーティング設定。 特に、管理系端末 LAN の分離設計。	システムへの影響を最小化するため、攻撃時の影響範囲をネットワーク設計上分離できるようにする。 ・Conficker、Stuxnet 事案等対処事例	・ネットワーク設計 ・ルータ、スイッチの VLAN 設定
5	最重要部のインターネット直接接続の分離設計	最重要部の通常サービス（http,ssl）に関するインターネット直接接続を分離設計し、外部からの制御シーケンスの影響を回避する。	外部からの制御シーケンスは、http,ssl 等の通常通信を多用する。 USB 等を介し、最重要部にウイルスが侵入した場合でも、インターネットを介した環境等攻撃分析情報の搾取、攻撃ウイルス更新、攻撃指示の影響を回避する。	・ネットワーク設計
6	システム内 P2P 通信の遮断と検知	VLAN 設定において、P2P 通信の到達範囲を限定する。	外部のダウンロードサーバからアップデートされるウイルスは、外部接続可能な P2P 用に仕立てた内部 PC を経由して、内部システムに存在するウイルスの一斉バージョンアップやリモートコントロールを行う。	・ネットワーク設計

## 2)課題

システム管理者においては、『新しいタイプの攻撃』に関するシステム・ネットワーク設計対策要件を具体的かつ、適用可能な形にしていく必要がある。

## 4. IPAの今後の取組み

### 4.1. 脅威と対策研究会

IPAでは『新しいタイプの攻撃』などの新しい脅威に対応するため、さまざまな分野の専門家の知見を共有する場として「脅威と対策研究会」を立ち上げた。この研究会では、脅威を分析し、対策を検討し、注意喚起、解説資料や脅威パターンと対策セットなどを成果として公表していく予定である。

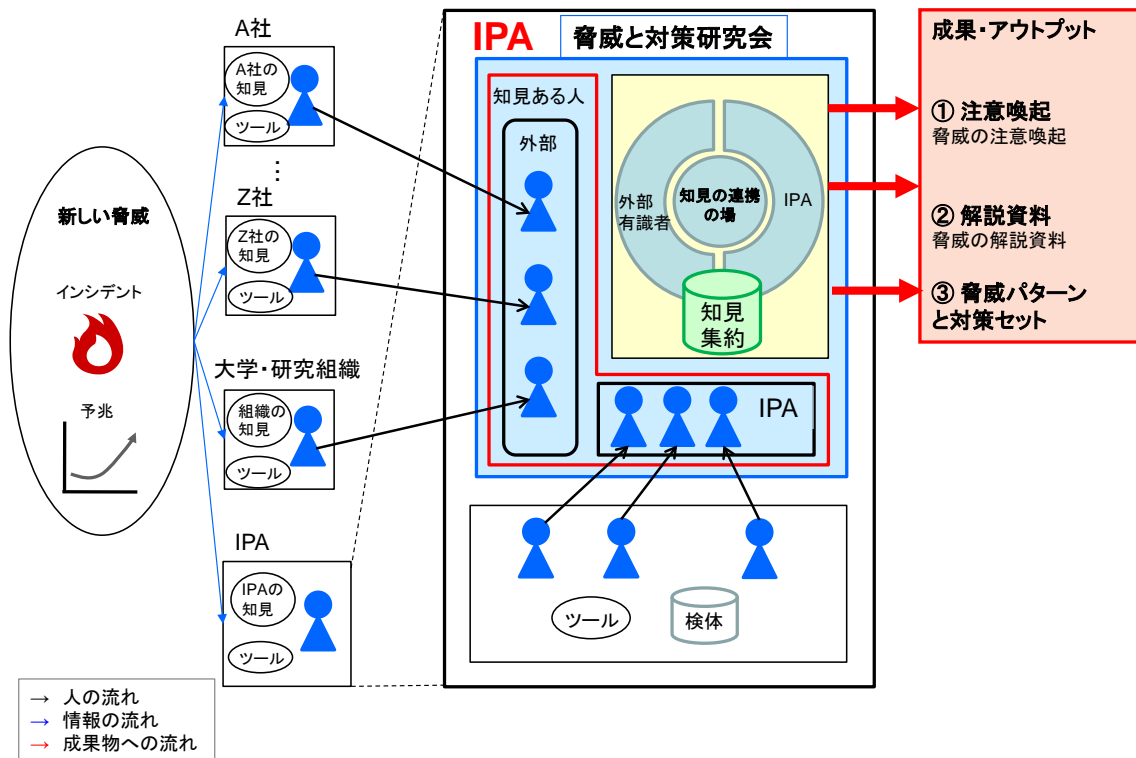


図 4.1-1 IPA「脅威と対策研究会」活動イメージ

## 付録 1：『新しいタイプの攻撃』の解析

IPA では、『新しいタイプの攻撃』の一例として、Stuxnet 検体の解析を行っている。各機関が出しているレポートと IPA の解析結果を総合的にまとめると次のようになる。

### <Stuxnet の総合的な特徴>

- ① 500K バイト以上のプログラムで、4000 弱の機能を持っている。
- ② 複雑であり、オブジェクト指向で開発されている。
- ③ 2つのルートキットを持ち、制御システムをターゲットとしている。
- ④ 複数の未知の脆弱性(ゼロデイ)を利用している。
- ⑤ 作成者は、Windows について造詣が深いことが分かる。また、制御システムである WinCC/Step7 についても詳細を知っている。

### <IPA で解析した結果>

#### ① 感染経路

現状判明している感染経路の1つは、USBメモリを介した感染である。Stuxnetに感染しているUSBメモリの内容をWindowsPCで表示するだけで感染活動が開始する。

#### ② USBメモリ経由の感染活動

USBメモリ内のファイルを表示すると、Stuxnetが動作を始める。感染活動の最初に、USBメモリ内のStuxnet本体のファイル群をユーザーから見えなくするように隠す(Windowsの動作を変更し表示されないようにするが、この時点ではファイルはUSBメモリ内に実在している)。

この様子を図.付録 1-1~図.付録 1-2 に示した。感染前の段階でコマンドラインからUSBメモリの中身を確認すると図.付録 1-3 のようにファイルは存在している。

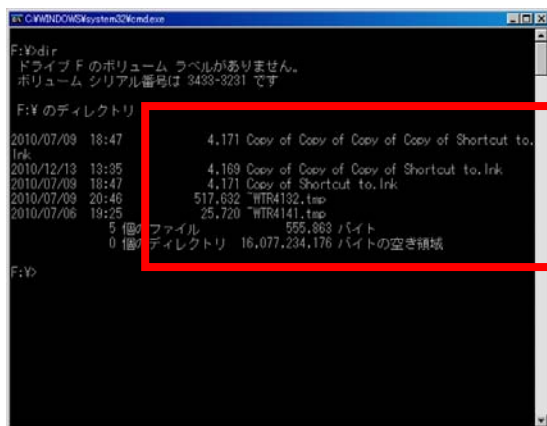


図.付録 1-1 コマンドラインからファイルの存在を確認

次に、エクスプローラでUSBメモリ内のファイルを表示させると一瞬、図.付録 1-2 の上の図のようにファイルが表示されるが、すぐにすべて見えなくなる。ファイル名などを確認する余裕はない。これはInkの脆弱性<sup>4</sup>を利用した攻撃によるものである。

<sup>4</sup> 2010年7月に発見されたWindowsのショートカットファイル「Ink」を悪用した脆弱性

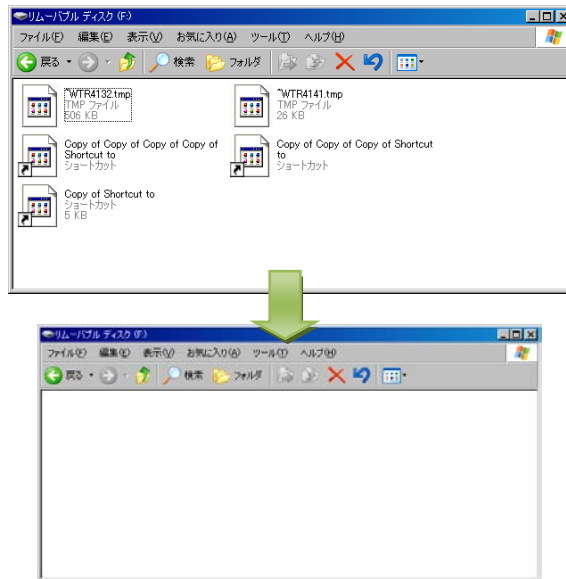


図.付録 1-2 USB メモリの中身をエクスプローラで表示

その後、いくつかのファイル（プログラム）を対象 PC に対してコピーし、動作させる。また、PC 再起動後も Stuxnet のプログラムが動作するように設定する。これらプログラムの詳細については現在解析中であるが、少なくとも1つのドライバが動作し、ファイルシステムを監視していることが分かっている。図.付録 1-3 のように感染後に作成されるドライバはファイルシステムを見張っている。またこのドライバの他の部分で、ファイルの隠ぺい等の処理を行っていることが分かっている。

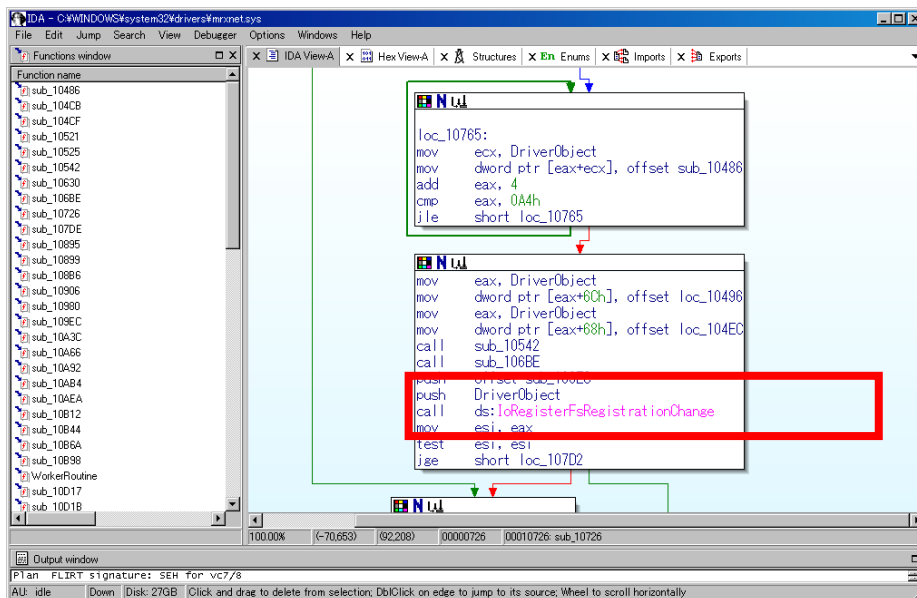


図.付録 1-3 ファイルシステムを監視するため API 呼び出し（mrxnet.sys 内）

感染時の最後の動作として、USB メモリ内にあったファイル群をすべて削除する。他の Stuxnet に関する報告によれば、感染後に PC に USB メモリを挿入すると、その USB メモリに新たに感染するという説明があるが、そのような活動は現在解析している検体においては、まだ確認できていない。

## 付録 2：システム環境の変化

Stuxnet が出現するまでは、汎用製品や標準プロトコルで構成されている情報システムだけが攻撃対象であった。

一方、IPAの調査報告<sup>5</sup>にもあるように欧米や日本の制御システムにおいても、図.付録2に示すように制御システムのオープン化（汎用製品や標準プロトコルの利用）が進展している。

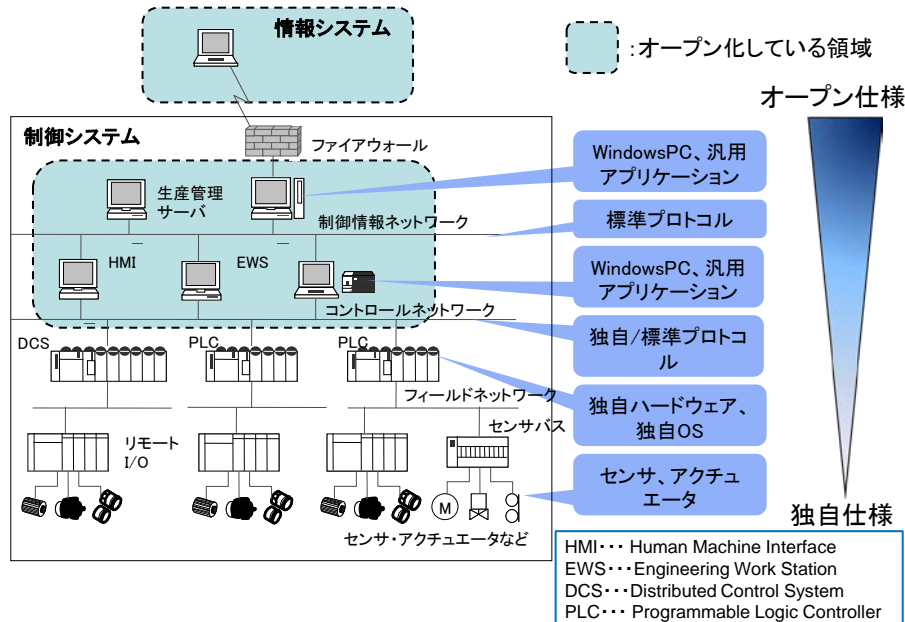


図.付録2 制御システムのオープン化:汎用製品+標準プロトコル

このように攻撃のターゲットが制御システムに移った要因として、独自仕様を利用していった制御システムの環境が、徐々にオープンな仕様に変化してきていることが挙げられる。

日本では、経済産業省がプラント設備に関して 234 社にアンケートを行った結果をまとめた資料<sup>6</sup>によると、制御システムにおけるサーバの 8 割以上、端末の 9 割近くが Windows系を利用している。外部記憶装置については、サーバ・端末とも、USBが 7 割、CD/DVDリーダを 5 割程度保有している。また、サーバにおけるネットワーク接続ポートとしては、6 割がイーサネットを保有している。さらに、外部ネットワークとは 4 割弱が接続しており、接続先は、リモートメンテナンス回線が 5 割超、インターネットが 4 割である。また、社内情報システムとは半数以上が接続している。このようにプラント設備での制御システムにおいては、汎用製品や標準プロトコルの利用が進みつつあることが示されている。

また、日本の制御システムに関しては、情報システムと制御システムを担当する部門が別である場合が多い。そのため、今回のように情報システムと制御システムに跨って攻撃される場合を想定した脅威分析、システム設計や対処が実施困難な現状である。なお、制御システムの脆弱性対策情報については、IPAとJPCERT/CCが共同で運営している JVN<sup>7</sup>において、23 件公開<sup>8</sup>(2010 年 12 月現在)している。

<sup>5</sup> 制御システムセキュリティの推進施策に関する調査報告書：

[http://www.ipa.go.jp/security/fy21/reports/ics\\_sec/documents/ics\\_sec2010.pdf](http://www.ipa.go.jp/security/fy21/reports/ics_sec/documents/ics_sec2010.pdf)

<sup>6</sup> 「工業用装置等における汎用 IT 技術応用に起因する脅威と対策に関する実態調査事業」報告書

<sup>7</sup> JVN は、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。

### 付録 3：サイバー攻撃に関する各国の反応

『新しいタイプの攻撃』である Stuxnet によるサイバー攻撃は、汎用製品（Windows や Linux）や標準プロトコル（TCP/IP 等）の利用が拡大している制御システム（制御システムのオープン化と呼ぶ）への初めての警告となる事例といわれている。

米国ではDHS(Department of Homeland Security)が推進しているICS（産業用制御システム）へのサイバーセキュリティ対策強化活動のカンファレンス<sup>9</sup>で、Stuxnetについての報告がなされている。

EUではENISA(European Network and Information Security Agency)において、解析した結果をレポートとして報告しており、制御システムに対しての注意喚起<sup>10</sup>を行っている。

このように米国や EU では、産業用制御システムへのサイバー攻撃を見据えた上記のような対応が進んでいる。

以上

---

<sup>8</sup> Stuxnet に関連する情報は、以下の URL で脆弱性対策情報を公開しています。

<http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001829.html>

<sup>9</sup> [http://www.us-cert.gov/control\\_systems/icsjwg/presentations.html](http://www.us-cert.gov/control_systems/icsjwg/presentations.html)

<sup>10</sup>

<http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1>