IPA

制御システム利用者のための脆弱性対応ガイド

重大な経営課題となる制御システムのセキュリティリスク

～ 制御システムを運用する企業が実施すべきポイント ～

第3版

＊この資料は複製・配布自由です

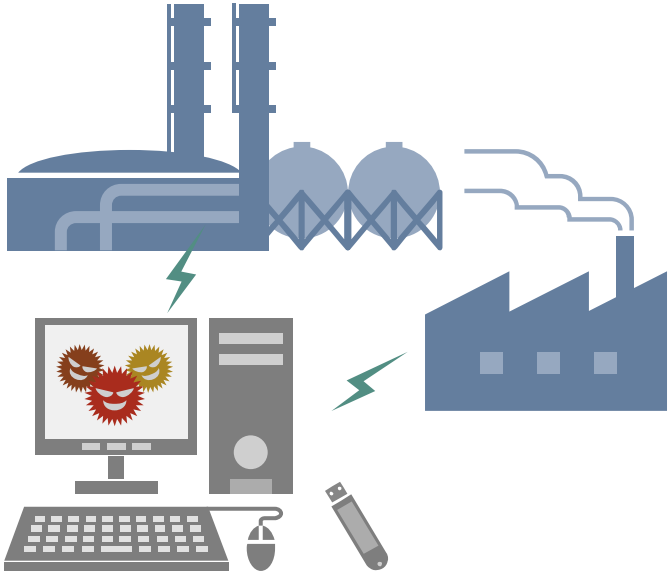
制御システムのセキュリティリスクをご存知ですか？

- 本資料は、制御システムを利用されている企業の皆様が、制御システムを使い続けていくうえで、今後検討が必須となるセキュリティリスクについて、ご紹介する目的で作成しました。

- 工場やプラントで利用されている制御システムは、適切なセキュリティ対策がなされていない場合、工場の生産ラインの停止や設備損壊、環境汚染等を引き起こし、企業に甚大な損失を与える可能性があります。実際に国内外で大きな被害が発生しています。

- 本資料は、次の内容で構成されています。
  - 制御システムのリスク
  - 制御システムに関して経営者がすべきこと
  - 制御システムのセキュリティ対策のポイント

- 本資料は、次の方にお読みいただくことを想定しています。
  - 制御システムを運用されている企業の経営者の皆様 / 経営企画、リスク管理部門等のリスク管理担当の皆様
  - 制御システムの導入及び調達を担当する皆様
  - 制御システムの運用・管理に携わる管理者の皆様



目次

経営者・役員 / 経営企画、リスク管理部門等のリスク管理担当者向け

導入及び調達の担当者 / 運用・管理に携わる管理者向け

1. 制御システムのリスク

経営者・役員 / 経営企画、リスク管理部門等のリスク管理担当者向け

1.1. 制御システムとは

- 制御システムとは、エネルギー分野（電力、ガス等）や石油・化学、鉄鋼業等のプラントにおける監視・制御、機械・食品等の工場の生産・加工ラインなどで、多くの企業に利用されているシステムです。

石油化学プラント

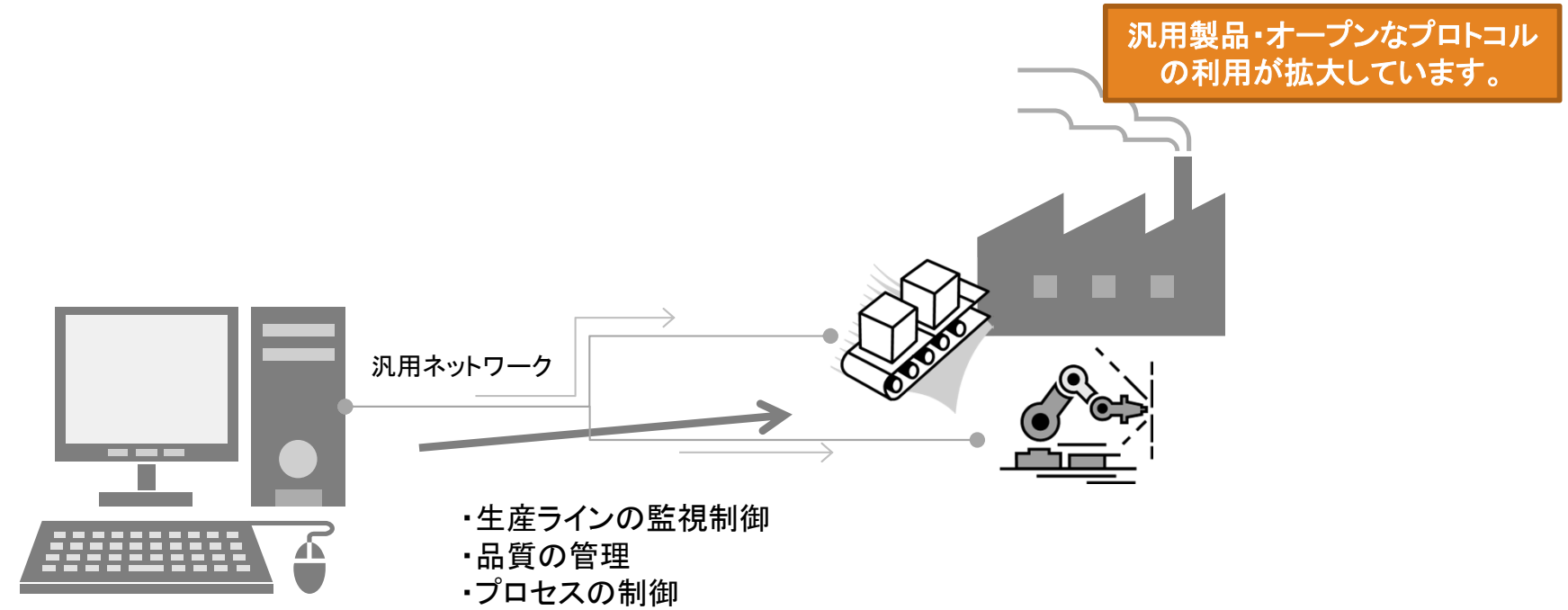
工場の生産ライン

以下のような業種の工場・プラントや社会インフラでは、制御システムが利用されています。

工場・プラント　石油、化学、鉄鋼、自動車・輸送機器、精密機械、食品、製薬、ビル管理、等
社会インフラ　電力、ガス、水道、鉄道、等

1.2. 制御システムで今、起こっていること (1)

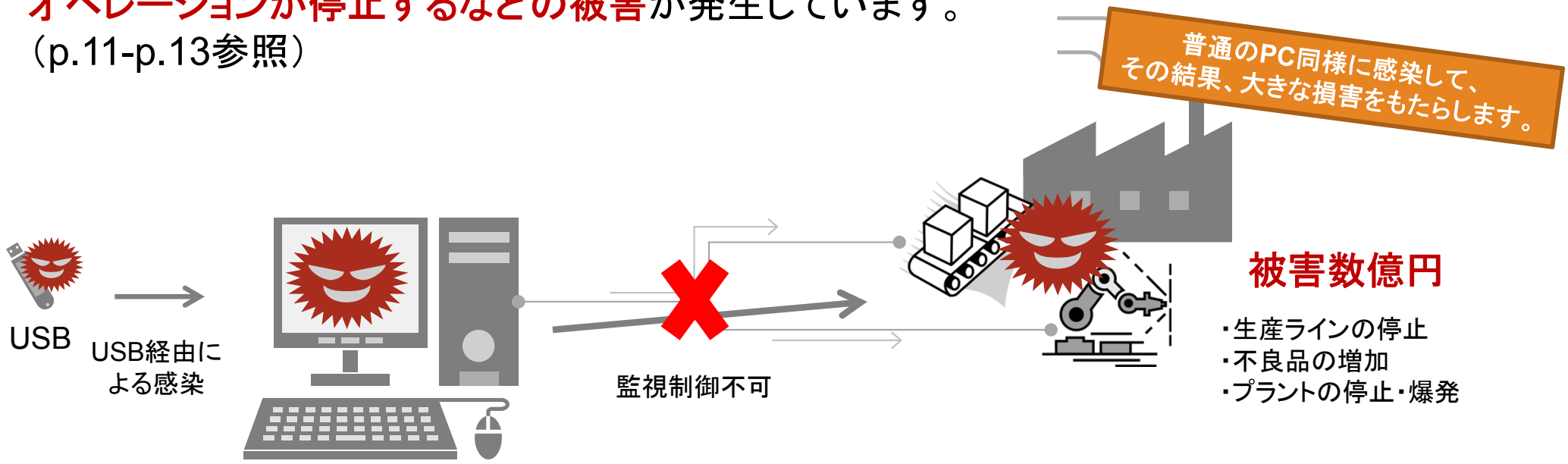
- 制御システムでは、オフィスや個人宅で利用されているPCが同じように多く使われています。
- 制御システムで使われているPCが、オフィスのPCと同じようにウイルスに感染したら、どうなるでしょうか。



生産ラインや化学プラントの監視制御には、WindowsやLinuxなどの汎用的なOSを搭載したPCがよく使われています。接続するネットワークには、イーサネットなどの世界中のオフィスや家庭で一般的に利用されているものが利用されています。

1.2. 制御システムで今、起こっていること (2)

- 工場の生産ラインやプラントで使われているPCがウイルス感染*すると、ラインやプラントの停止などの事態に陥る可能性があります。
- 悪意のある攻撃者により感染させられた場合には、爆発などにより人的損傷や設備損壊、環境破壊を引き起こす可能性もあります。
- 実際に**国内の工場の生産ラインが停止し数億円の損害**をもたらしたり、海外では**製鉄所のオペレーションが停止するなどの被害**が発生しています。
（p.11-p.13参照）



工場の生産ラインやプラントで使われているPCが、USB経由等でウイルスに感染し、ラインの停止やプラントの爆発、環境破壊といった事態に陥った事例があります。

*ウイルス、ワーム、トロイの木馬を含む悪質なコードの総称をマルウェアといい、ウイルス感染だけでなくワームやトロイの木馬に感染する可能性もあります。

1.3. 制御システムのリスク (1)

- 制御システムでは、近年、情報システム同様に、ウイルス感染や不正アクセス等のサイバー攻撃のリスクが増大しています。

- しかしながら、**セキュリティ対策はほとんど意識されていないケースが多く***、場合によっては非常に脆弱なシステムとなっています。
そのため、工場の生産ラインの停止や設備損壊、環境破壊等を引き起こし、**企業に甚大な損失を与える可能性が高まっています**。

- **特定のプラントを標的としたサイバー攻撃も起こっています。**
2020年に東京で開催されるオリンピック・パラリンピックのような大きなイベントは、サイバー攻撃のターゲットとなりやすく、その脅威がさらに高まることが予想されます。

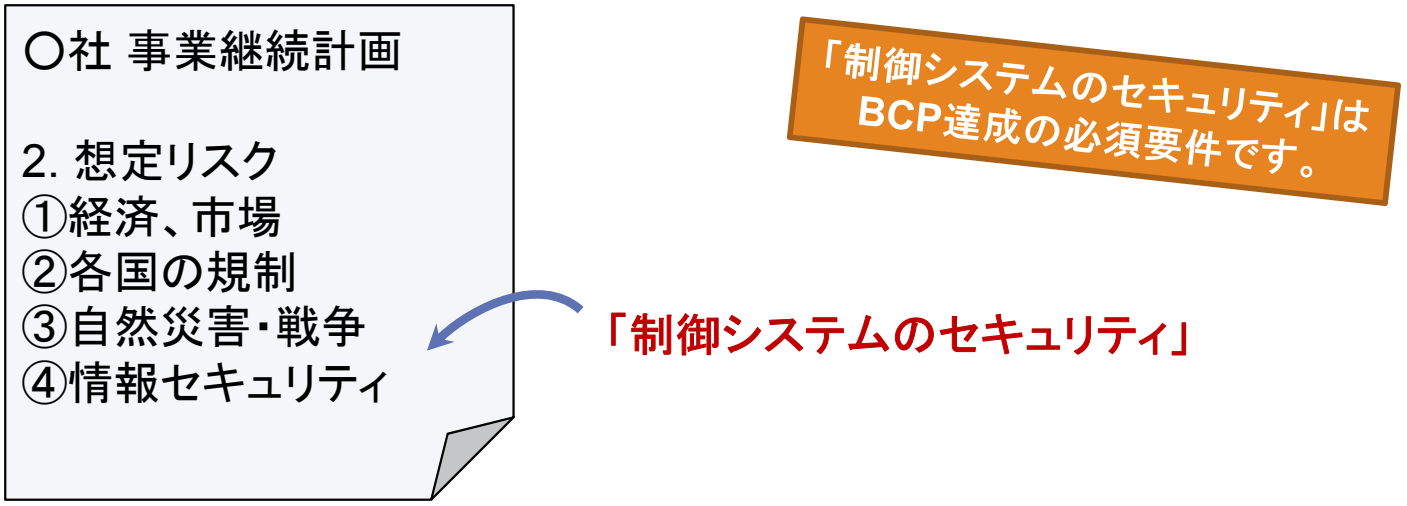
2014年11月に成立したサイバーセキュリティ基本法に基づき、電力・ガス等の重要インフラ分野ではセキュリティ対策が強化される方向にあります。

*ファイアウォールやウイルス対策ソフトを導入するだけでは不十分です。

1.3. 制御システムのリスク (2)

- このような脅威の高まりは、一般の工場やプラント等の制御システムにも波及することが予想され、これらの制御システムに対して、情報システム同様にセキュリティ対策を行うことが不可欠となっています。

- 今や制御システムのセキュリティの問題は、**経済的な損害だけでなく、社会的信用の失墜に繋がりうる**ものです（p.11-p.13参照）。「制御システムのセキュリティ」は、**事業継続計画（BCP）において想定する主要なリスクの一つ**であり、**経営責任が問われる課題**として捉える必要があります。



2. 制御システムに関して経営者がすべきこと

経営者・役員 / 経営企画、リスク管理部門等のリスク管理担当者向け

2.1. 制御システムセキュリティの実態

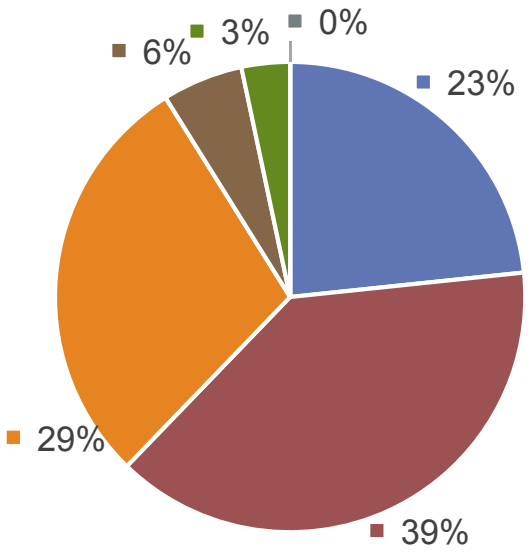
アンケート調査から次の実態が明らかになりました。

- 制御システムのセキュリティリスクは9割の回答企業が認識
- セキュリティインシデントはヒヤリハットまで含めると2割弱の回答企業が経験*

* たまたま発見されただけで、実際には起きていることに気づいていない状況も考えられます。

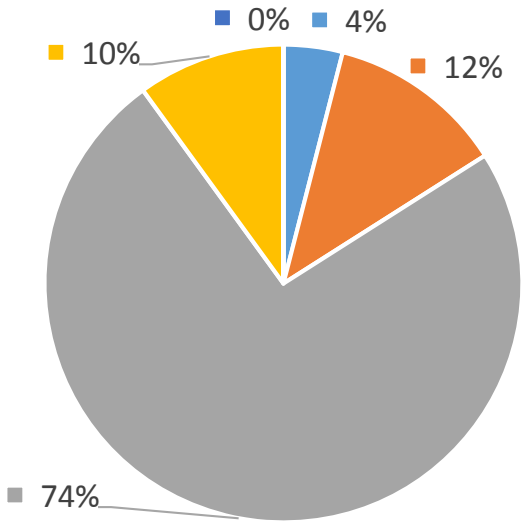
IPA「平成27年度 制御システムユーザ企業におけるセキュリティリスクへの対応に関する態調査」より国内のPA（Process Automation）及びFA（Factory Automation）ユーザ企業のうち、上場企業より抽出した1140社中100社から回答を得た。

制御システムのセキュリティリスクに関する認識



	n	%
1 認識して対策済み	23	23.0
2 認識して対応中	39	39.0
3 認識しているが未対応	27	27.0
4 認識していない	7	7.0
5 わからない	4	4.0
5 無回答	0	0.0
全体	100	100.0

セキュリティインシデントの発生状況



	n	%
1 事件・事故の経験あり	4	4.0
2 事件・事故はないがヒヤリハットの経験あり	12	12.0
3 経験がない	74	74.0
4 わからない	10	10.0
5 無回答	0	0.0
全体	100	100.0

2.2. 実在する制御システムの被害事例 (1)

実際に制御システムでウイルス感染や不正アクセス等のサイバー攻撃により多くの被害が発生しています。

生産ラインが停止する被害が発生しています。

事例1　自動車工場

被害:　**自動車生産50 分間停止等、約1,400万ドル（約17億円）の損害**

被害企業:ダイムラー・クライスラー（現ダイムラー）

原因:　ウイルス感染。外部から持ち込まれて接続されたノートPCの可能性が指摘されている

概要:　2005年8月18日、13の自動車工場がウイルス感染により操業停止となった。ウイルス感染により、各工場のシステムはオフラインになり、組み立てラインで働く50,000 人の労働者は作業を中断し、生産が50 分間停止した。部品サプライヤへの感染も疑われ、部品供給の懸念も生じた。結果として、およそ1,400 万ドル（約17億円）の損害をもたらした。

出所: 情報処理推進機構「重要インフラの制御システムセキュリティとIT サービス継続に関する調査」, 2009.3
http://www.ipa.go.jp/files/000013981.pdf

2.2. 実在する制御システムの被害事例 (2)

事例2　石油パイプライン

石油パイプラインの爆発や製鉄所の操業停止といった事態が発生しています。

被害:　トルコの石油パイプラインの爆発

被害企業:BP（British Petroleum、運営主体）

原因:　2008年、サイバー攻撃により石油パイプラインが爆発した可能性が指摘されている。攻撃者は、パイプラインに設置されている監視カメラの通信ソフトの脆弱性を利用して内部ネットワークに侵入。不正に動作制御系にアクセスし、警報装置の動作を停止させたうえで、管内の圧力を異常に高めて爆発を引き起こしたとされる。

出所:Bloomberg, “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar Era,” 2014.12.10
http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

事例3　製鉄所

被害:　ドイツの製鉄所の操業停止

被害企業:ドイツの製鉄所

原因:　攻撃者は、電子メールに添付したマルウェアにより情報を入手し、製鉄所のオフィスネットワークに不正侵入。その後、生産設備の制御システムに不正侵入を拡大させた。不正操作より、溶鉱炉を正常に停止できず、生産設備が損傷する大きな被害を受けた。

出所:[1]BSI（ドイツ連邦情報セキュリティ庁）, “Die Lage der IT-Sicherheit in Deutschland 2014（2014年版サイバー犯罪白書）”
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile
[2]BBC, “Hack attack causes 'massive damage' at steel works,” 2014.12.22, http://www.bbc.com/news/technology-30575104
[3]経済産業省製造産業局鉄鋼課・非鉄金属課, 金属競争力強化検討会デジタルデータ活用小委員会資料, 2015

2.2. 実在する制御システムの被害事例 (3)

報道こそほとんどされていないものの、国内でも多数の被害が発生しています。

事例4　国内　自動車工場

被害:　　自動車の生産ラインの処理能力低下

被害企業:国内自動車メーカー

原因:　　業者による端末入れ替え時にウイルスが混入し、システム内のパソコン約50台がウイルス感染し、処理能力が低下。

出所:毎日新聞「サイバー攻撃:車工場ウイルス感染　制御システム、処理能力低下――08年、西日本で」, 2011.11.27

事例5　国内　半導体工場

被害:　　半導体工場の生産ライン停止

被害企業:国内大手半導体メーカー

原因:　　品質検査を行う検査装置へのウイルス感染により生産ラインが停止。

USBメモリ経由での感染であった。

出所:MONOist「産業制御システムのセキュリティ(5):事例から見る、製造現場でのセキュリティ導入のツボ」 http://monoist.atmarkit.co.jp/mn/articles/1402/12/news082.html

- 品質検査を行う検査装置などへのウイルス感染や不正アクセスは、製品の品質問題を引き起こす可能性もあります。
- こういったリスクに対して、経営層が対策に取り組む必要があります。

2.3. 経営層が実施すべきポイント

経営層には、制御システムセキュリティに取り組む環境を整えることが望まれます。

ポイント：対策マネジメント組織を構築する

現場の管理者はわかっていてもマネジメントする組織がなければ、また同じことが起こります。

■ 現状を把握しセキュリティ対策を浸透させていくための取り組みを推進する担当組織（または担当者）を設置することが重要です。

- セキュリティポリシーの策定、対策の計画と実行
- 実行状況の監査と改善サイクル
- 要員への教育

公に認められる第三者認証として、制御システムに関するセキュリティマネジメントシステム（CSMS）認証があります。（参考5（p.30）参照）

ポイント：サプライチェーン全体で考える

子会社や取引先も含めて検討する必要があります。

■ 制御システムのセキュリティを事業継続計画（BCP）で想定する主要なリスクとして捉え、自社だけでなく、子会社や取引先を含むサプライチェーン全体のセキュリティを検討することが重要です。

ポイント：現状の対策状況を確認するように指示を出しましょう。

自分の状態を把握することが重要です。

■ 制御システムの導入及び調達の担当者向け ⇒ p.21
■ 制御システムの運用・管理に携わる管理者向け ⇒ p.22 - p.24

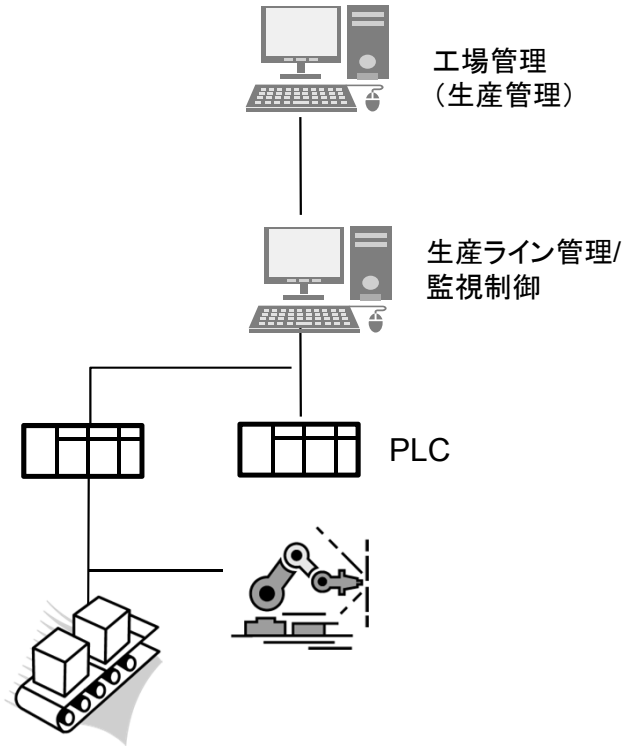
3. 制御システムのセキュリティ対策のポイント

導入及び調達の担当者 / 運用・管理に携わる管理者向け

3.1. 制御システムの構成

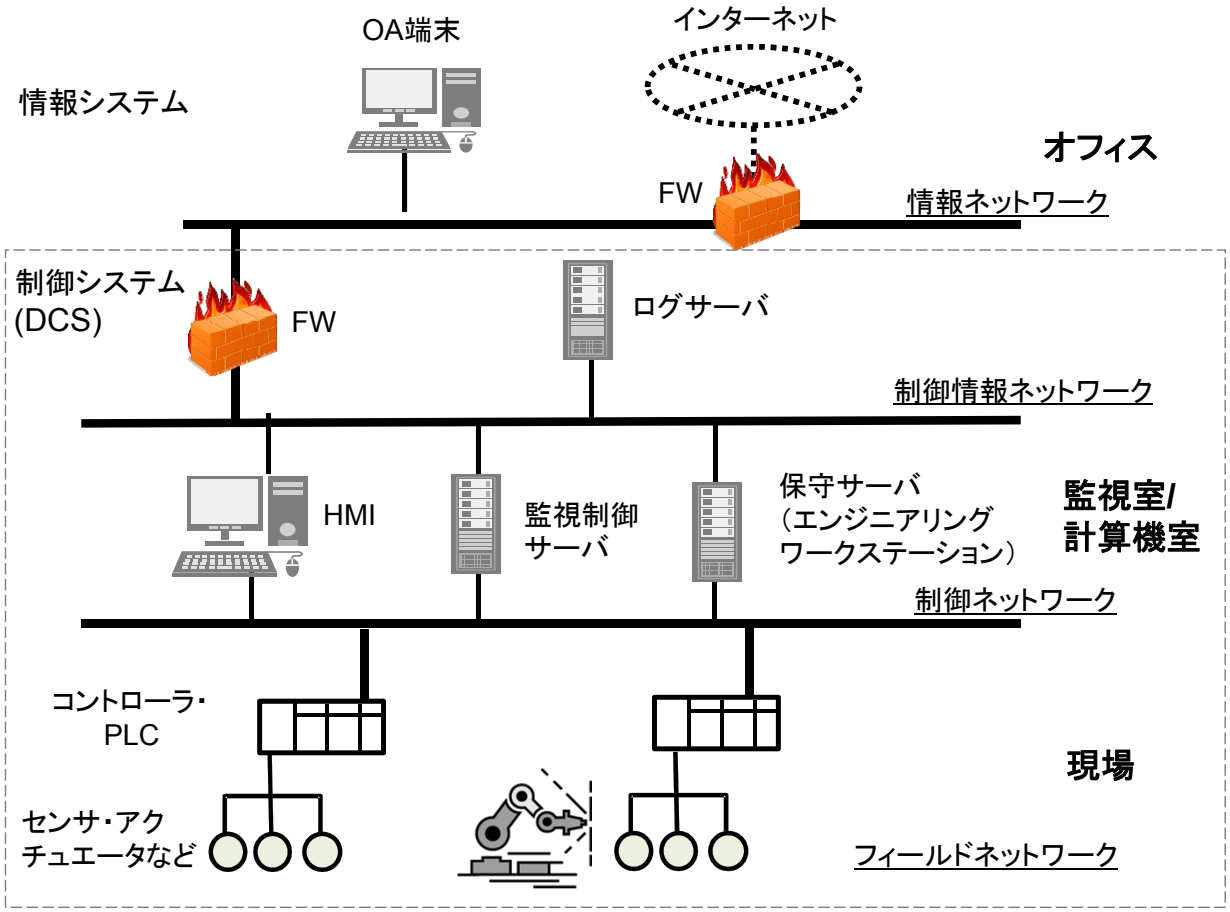
主に大規模化学プラントで使われるような大規模な制御システムから、工場の生産ラインの制御に使われるような小規模な制御システムまで想定しています。

小規模な制御システム
（主に工場の生産ラインの制御など）



*PLC：Programmable Logic Controller
HMI：Human Machine Interface
DCS：Distributed Control System

大規模な制御システム
（主に電力、ガス、化学のプロセス制御など）



3.2. 制御システムの特徴

- 制御システムには情報システムとは異なる特徴もあり、その特徴にあった対策が必要です。
  - 制御システムは社会基盤・産業基盤を支えており、稼働が停止すると社会的な影響・事業継続上の影響が大きいため、継続して稼働できることが重視されています。
  - 情報システムは大量のデータ処理を目的として導入されることが多いため、可用性よりも処理能力が求められ、顧客情報等の機密情報の漏えいは影響が大きく機密性が重視される傾向があります。

制御システムと情報システムにおける情報セキュリティの考え方の違い

	制御システム	情報システム
セキュリティの優先順位	システムが**継続して安全に**稼働できることを重視	情報が適切に管理され、情報漏えいを防ぐことを重視
セキュリティの対象	モノ（設備、製品） サービス（連続稼働）	情報
技術のサポート期間	10年～20年	3～5年
求められる可用性	24時間365日の安定稼働 （再起動は許容されないケースが多い）	再起動は許容範囲のケースが多い
運用管理	現場技術部門	情報システム部門

3.3. 制御システムへの脅威と脆弱性

セキュリティ被害を引き起こした原因は主に4ケースに分類され、現状の国内の制御システムの運用状態において大きな脅威となっています。

被害事例の原因の多くは、こういった基本的な部分にあります。

USBメモリ

- USBメモリからのウイルス感染事例は頻繁に発生しています
- しかしながら、USBポートは運用上なくすことは不可能なことが多く、メンテナンス上も不可欠です

リモートメンテナンス回線

- 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・ウイルス混入が発生しています

操作端末の入れ替え/保守用端末の管理

- 操作端末は、汎用パソコンであることが一般的であり、入れ替え時にウイルス感染していた端末から被害が発生しています
- システムに接続する保守用端末が原因となるケースもあります

内部犯行・工業用無線LAN等

- 内部犯行者は物理セキュリティはすり抜けます
- 工業用無線LANからの侵入事例もあります
- PCのIDやパスワードの共通化、メモ書きの貼り付けなどは、悪用されやすい、危険な運用です

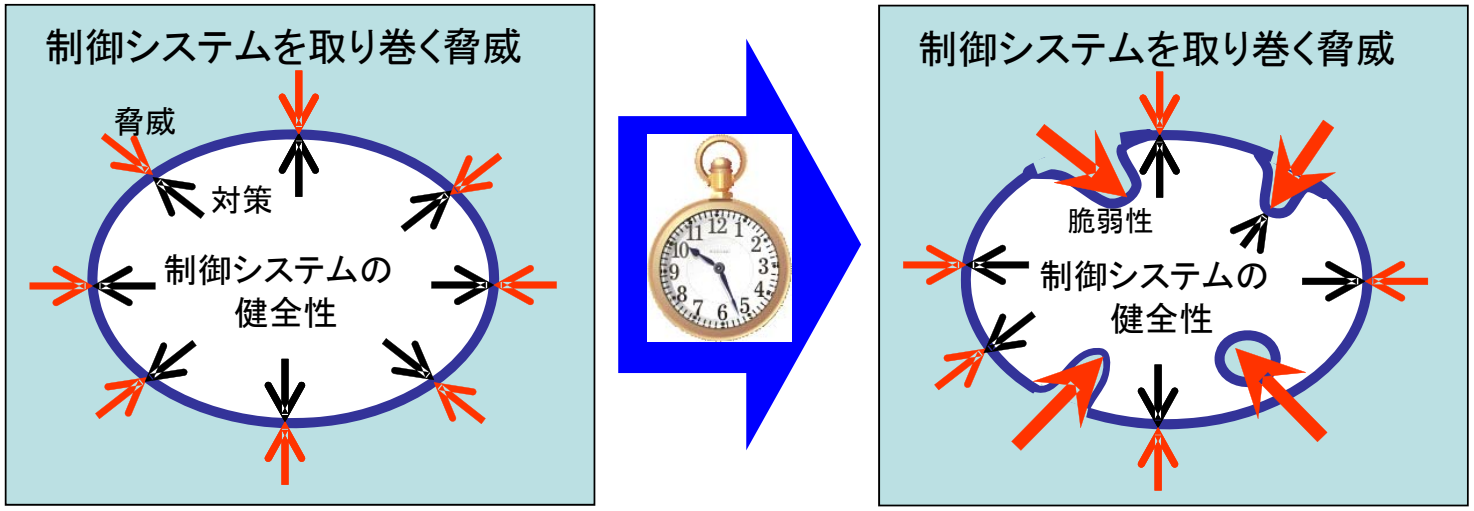
多くのケースで、**端末や制御機器の脆弱性が修正されていない場合に、**これらの脅威は被害を引き起こします。*

*一部では、修正プログラムが未公開の脆弱性を悪用し、特定の制御システムをターゲットとするような高度なサイバー攻撃も発生しています。（参考6（p.31）、参考7（p.32）参照）

3.4. 脆弱性対応とは (1)

脆弱性とは、情報セキュリティ上の「弱点」「ほころび」 です。

- ウイルスやサイバー攻撃などは、端末や制御機器の脆弱性を突いて、不正な働きをします。
- 逆にいうと、脆弱性がない、もしくはあったとしても修正されていれば、多くの攻撃を防ぐことができます。
- セキュリティ対策は、前ページに挙げたような**脅威への対策**に加えて、情報セキュリティ上の「弱点」「ほころび」である**脆弱性の面**からも対策を行う必要があります。



開発当初は、脅威に対して適切な対処がなされ、健全性が高い

時間が経つと脅威が変化するため、そのままでは健全性を維持できない

3.4. 脆弱性対応とは (2)

ウイルスの駆除だけでは脆弱性には対応できません。

- ウイルスを駆除しても脆弱性を修正しなければ、再感染の可能性があります。
- 脆弱性の修正のためには、ソフトウェア製品の場合、製品ベンダのセキュリティ更新プログラム（パッチ）を適用する必要があります。（p.23参照）
- 脆弱性は日々発見され、一部の脆弱性は対策がない状況のまま公開されています。
- 実際に、制御システム製品の脆弱性についても発見されています。（参考4（p.29）参照）

トピックス　Windows XPのサポート終了

- Windows XPのサポートとセキュリティ更新プログラム等の提供が2014年4月に終了し、セキュリティ対策という面で大きな問題になりました。
- サポート終了後も Windows XPは使い続けること自体は可能ですが、セキュリティ更新プログラムが提供されないため、脆弱性がもし見つかっても、脆弱性を解決しないままで使用し続けることになり、ウイルス感染やサイバー攻撃のリスクが高くなります。
- 多くの制御システムではWindows XPがいまだに使われており、非常に危険な状態となっています。

3.5 設計・開発・導入段階における対策と脆弱性対応

以下に示す項目は、今後実施することが必須となってくる項目です。

制御システムの導入及び調達の担当者向け

ベンダもただではセキュリティ対策をやってくれません。

ポイント1：調達時の要求仕様にセキュリティ要件を含める

- セキュリティ対策にはコストがかかるため、調達側が仕様作成の時点で意識をすることが大変重要です。
- 調達で競争入札とする場合、必要なセキュリティ対策を具体的に要件に含めて提案させるようにしましょう。
- リスク評価を実施した上で、セキュリティを考慮した設計・開発を依頼しましょう。以下のような項目の検討が必要です。
  - ネットワークの分離（制御ネットワーク/制御情報ネットワーク/情報ネットワーク等）
  - USBメモリ等の外部記憶媒体からの感染対策
  - 開発時・運用時の脆弱性対策
  - セキュリティ強度の高い機器・ツールの採用

EDSA認証*などの制御システムセキュリティについての認証を取得している製品もあります。

ポイント2：運用・保守契約において、セキュリティに関する項目を含める

- 運用・保守契約においてセキュリティに関する項目を含めることが必要です。
- 具体的には、以下のような項目が必要です。
  - ウイルス感染及び不正侵入時の対応
  - 脆弱性対応（脆弱性対策情報の提供、パッチ適用等）

ベンダの協力なしでは対応が難しい項目です。

* ISASecure EDSA（Embedded Device Security Assurance）認証：制御機器のセキュリティ保証に関する認証制度です

3.6. 運用段階における対策と脆弱性対応 (1)

制御システムの運用・管理に携わる管理者向け

クローズドなネットワーク構成であることは原則です。クローズドなネットワークでも、ウイルス感染や不正アクセスのリスクがあり、その原則を抑えた上で、多重・多層に防御することが必要です。

⇒「インターネットにつながっていなければ安全」というのは過去の話です。人為的なミスに加え、悪意を持った関係者により深刻な事態に陥ることも予想されるため、対策を進める必要があります。

- 制御システムを守るためには、脅威（セキュリティ被害の原因）の抑制と脆弱性対応の両方に取り組む必要があります。
- また、日常の安全衛生活動に加えるなど、継続的にシステムの状態を把握する必要があります。
- 以下、脅威の抑制に効果的なポイントを紹介します。ただし、これだけ実施すれば十分というわけではない点にはご注意ください。

ポイント1：被害の原因となっているUSBや入れ替え端末に対しての対策

■ 以下のポイントはクローズドな制御システムの主な感染源となっています。

☑ USBメモリ
- USBポートを取り外す/ロックする
- USBメモリ挿入時に、専用PCでウイルスチェックを行う
- USBメモリ利用規則の策定
- 利用できるUSBメモリの管理

☑ 操作端末の入れ替え/保守用端末の管理
- 入れ替え時のスタンドアロンでのウイルスチェック
- 保守用端末等の機器の管理（持ち込み禁止等）

☑ リモートメンテナンス回線
- 接続されている端末の認証
- 利用時のみの接続

3.6. 運用段階における対策と脆弱性対応 (2)

制御システムの運用・管理に携わる管理者向け

セキュリティ更新プログラムの適用など、脆弱性対応は自社だけでは実施が難しいものであり、ベンダと協力して実施する必要があります。

ポイント2：セキュリティ更新プログラム（パッチ）を適用する

- 脆弱性は日々発見されているため、脆弱性対策情報については常に自らもしくはベンダを通して収集を行うことが望まれます。
- 脆弱性が悪用され、システムへの影響が深刻な場合には、パッチをすみやかに適用すべきです。
  - ただし、制御システムの中には、常時稼働が必須でパッチを適用できないケースがあります。そのような場合には、メンテナンス時や操業停止時などに計画的にパッチを適用する必要があります。
  - パッチを適用すると、アプリケーションの動作に影響する可能性があります。ベンダと相談して、事前に動作検証を行う必要があります。
- パッチの適用が難しい場合は、脅威への対策（p.22, p.24参照）を徹底して、セキュリティ被害の発生を回避することが望まれます。

3.6. 運用段階における対策と脆弱性対応 (3)

制御システムの運用・管理に携わる管理者向け

セキュリティ対策の一環として、ネットワークを流れるデータやログデータの監視等の取組みを推奨します。

ポイント3：制御システムのネットワークを流れるデータ、ログデータを監視する

セキュリティ事件・事故の検知や分析を行うため、

- 制御システムのネットワークを流れるデータを監視する
- 専用のログ管理ツールを導入する
- 制御システムにもともと組み込まれているログ管理機能を使う

- 国内でもアンケート回答事業者の約5割が、ポイント3に挙げたような対策を実施しています。
- 他にもパスワード管理など、リスクに応じて実施すべき対策があります。ガイドラインや対策の評価ツールを参考に対策を実施しましょう。（参考8（p.33）参照）

IPA「平成27年度 制御システムユーザ企業におけるセキュリティリスクへの対応に関する態調査」より国内のPA（Process Automation）及びFA（Factory Automation）ユーザ企業のうち、上場企業より抽出した1140社中100社から回答を得た。

参考資料

参考1. 制御システムのセキュリティに対する取り組み
参考2. 情報セキュリティ早期警戒パートナーシップ
参考3. 脆弱性対策情報データベース：JVN iPedia
参考4. 制御システム製品の脆弱性
参考5. CSMS（サイバーセキュリティマネジメントシステム）
参考6. 制御システムを標的としたサイバー攻撃（Stuxnet、Havex）
参考7. 制御システムを標的としたサイバー攻撃（ウクライナの大規模停電）
参考8. 参考URL

参考1. 制御システムのセキュリティに対する取り組み

制御システムのセキュリティに対して多くの取り組みが行われています

- 経済産業省では、2011年12月に制御システムセキュリティ検討タスクフォースを設置するなど、制御システムのセキュリティについて取り組みを進めています。
- 2012年3月に発足した技術研究組合制御システムセキュリティセンター（CSSC）や情報処理推進機構（IPA）、JPCERT/CCにより、普及啓発や人材育成、研究開発が進められています。

制御システムセキュリティに対する主な取り組み

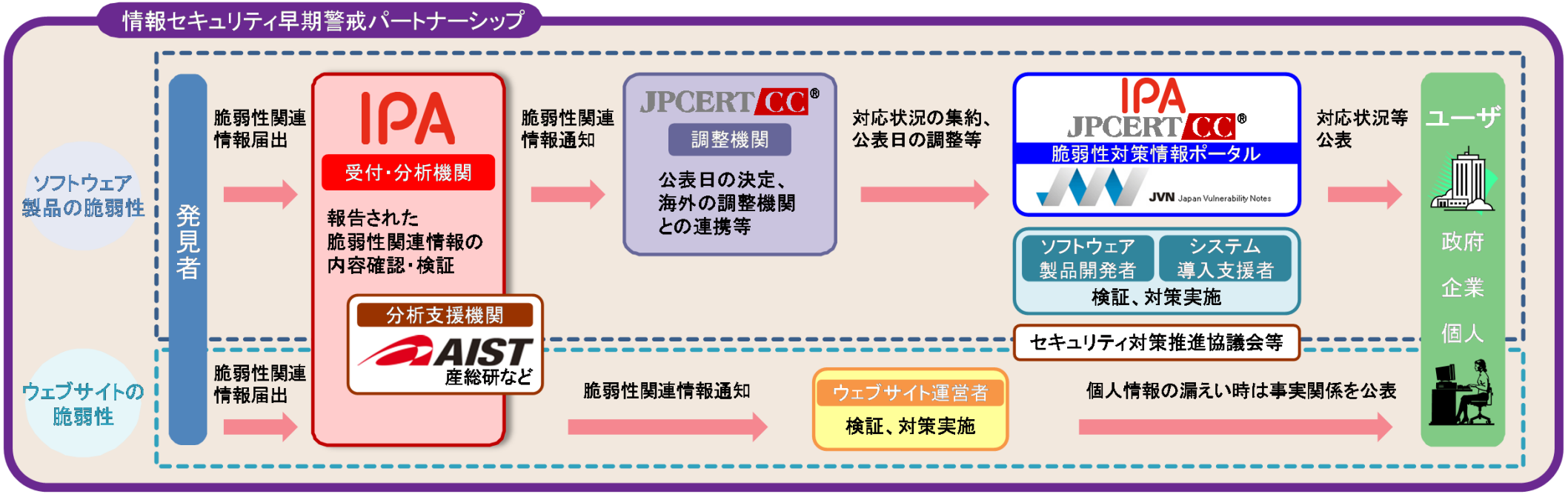
CSSC	・アズビル、横河電機、日立製作所等の制御ベンダやトレンドマイクロ、マカフィー等のセキュリティベンダ等、32社が参加。 ・制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証等を実施。 ・制御機器のセキュリティ保証に関する認証制度「EDSA認証」を運用。 ・電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、ベンダ等を集めて、セキュリティインシデント発生の検知手順や障害対応手順の妥当性を検証するサイバーセキュリティ演習を実施。
JIPDEC	・マネジメントシステムの第三者評価制度であるプライバシーマーク制度やISMS/ITSMS/BCMS適合性評価制度などの制度運用と普及拡大を行っており、制御システムのセキュリティマネジメントシステム（CSMS）認証制度を運用。
IPA	・経済産業省所管の独立行政法人であり、コンピュータウイルスやセキュリティに関係する調査・情報提供を実施。 ・脆弱性関連情報の取扱い業務をJPCERT/CCとともに実施し、情報流通のための仕組みである「情報セキュリティ早期警戒パートナーシップ」を運用。 ・制御システムセキュリティの普及啓発のためのビデオなどを展開。
JPCERT/CC	・コンピュータセキュリティの情報を収集し、インシデント対応の支援やコンピュータセキュリティ関連情報の発信を実施。 ・制御システムに関するインシデントの受付を実施。

CSSCの検証施設
（宮城県多賀城市）

参考2. 情報セキュリティ早期警戒パートナーシップ

制御システム製品の脆弱性含め、発見された脆弱性に関する届出を受け付け、対策の実施を促しています

- IPAでは、「ソフトウエア等脆弱性関連情報取扱基準」（平成29年経済産業省告示第19号）の告示を踏まえ、ソフトウェア製品（制御システム製品を含む）及びウェブアプリケーションの脆弱性に関する届出を受け付けています。
- IPAでは、脆弱性に関する届出を受け付けた場合、JPCERT/CCに連絡し、JPCERT/CCから当該製品の開発者にその旨を連絡し、脆弱性対策の実施を促します。
- 同制度では制御システム製品の脆弱性についても扱っており、制御システムを運用している事業者は制御システムベンダを通して脆弱性対策情報を受け取る可能性があります。



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

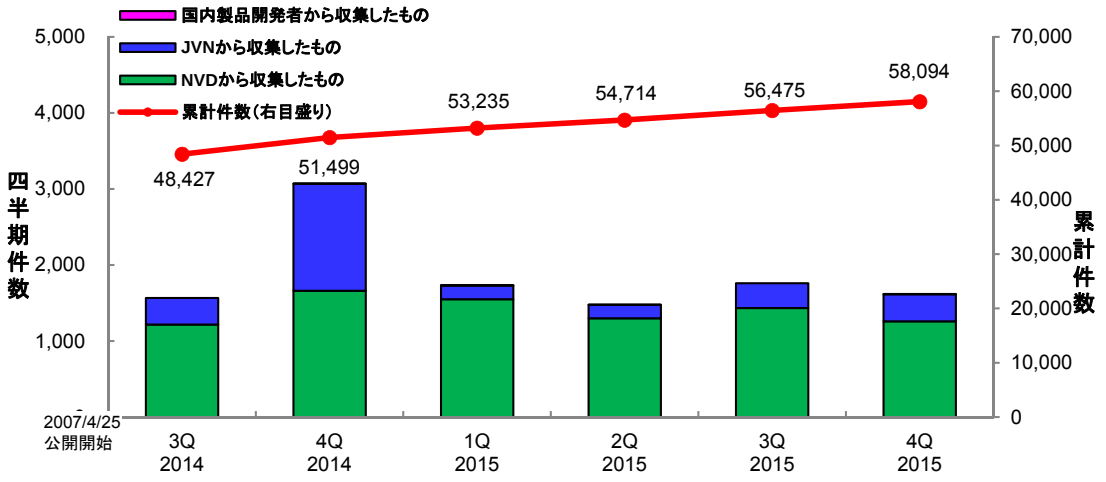
参考3. 脆弱性対策情報データベース：JVN iPedia

JVN iPediaでは制御システム製品の脆弱性が登録・公開されています

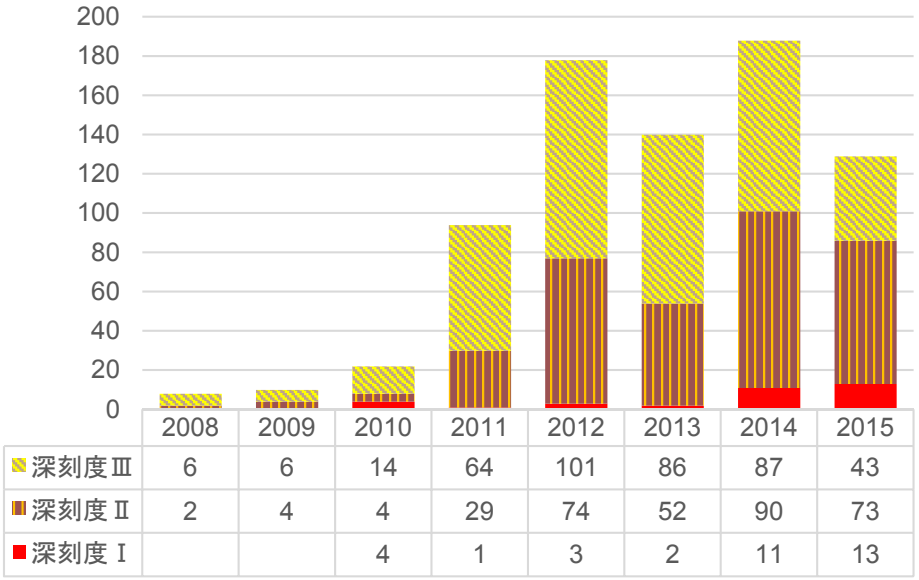
- 脆弱性対策情報データベース
  「JVN iPedia（ http://jvndb.jvn.jp/）」
  国内外で使用されているソフトウェアの脆弱性対策情報を収集・公開することにより、それらを容易に利用可能とすることを目指しています。
- 制御システムソフトウェアの脆弱性も、約600件、登録されています。

脆弱性対策情報の登録件数(2015年第4四半期)

	情報の収集元	登録件数	累計件数
日本語版	国内製品開発者	4件	172件
	JVN	355件	6,077件
	NVD	1,260件	51,845件
	計	1,619件	58,094件
英語版	国内製品開発者	4件	172件
	JVN	52件	1,165件
	計	56件	1,337件



JVN iPediaの登録件数の四半期別推移



	2008	2009	2010	2011	2012	2013	2014	2015
深刻度Ⅲ	6	6	14	64	101	86	87	43
深刻度Ⅱ	2	4	4	29	74	52	90	73
深刻度Ⅰ			4	1	3	2	11	13

脆弱性対策情報を公表した「制御システム」の年別公表件数

JVN: Japan Vulnerability Notes、JPCERT/CC及びIPAの脆弱性対策情報ポータルサイト。
NVD: National Vulnerability Database、米国国立標準技術研究所NISTの脆弱性データベース。

参考4. 制御システム製品の脆弱性

PLCなどの制御システム製品にも多くの脆弱性が発見されています

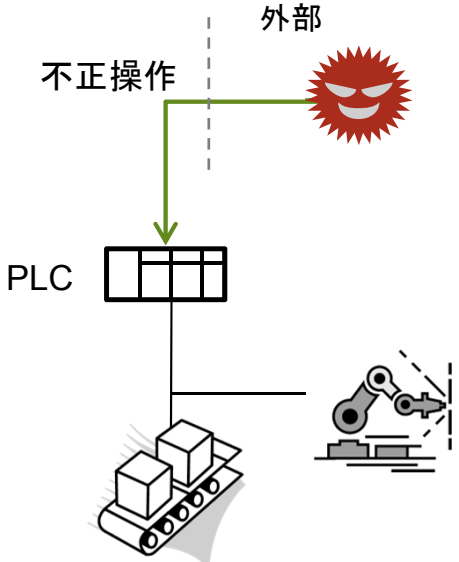
- 2012年1月、工場の生産ラインや化学プラントなどで使用される複数社の制御機器PLC（Programmable Logic Controller）において、複数の脆弱性（バックドア、暗号や認証不足、弱いパスワード等）が公開されています。*

- これらの脆弱性においては、実際の攻撃に悪用可能な実証コードも公開されています。（日本および欧米のメーカーの5社、6製品について悪用可能な実証コードが公開。）

- これらの脆弱性を狙われて攻撃されてしまうと、制御機器を外部から不正操作されてしまう可能性があります。

- 上記の脆弱性以外にも、前ページに示したように、PLCを含む制御システム製品の脆弱性が多く発見されており、一部は悪用可能な実証コードとともに公開されています。

- 2015年5月、警察庁から、産業制御システムで使用される特定のPLCのソフトウェアの脆弱性を探索するインターネット上での行為の観測が報じられました。**



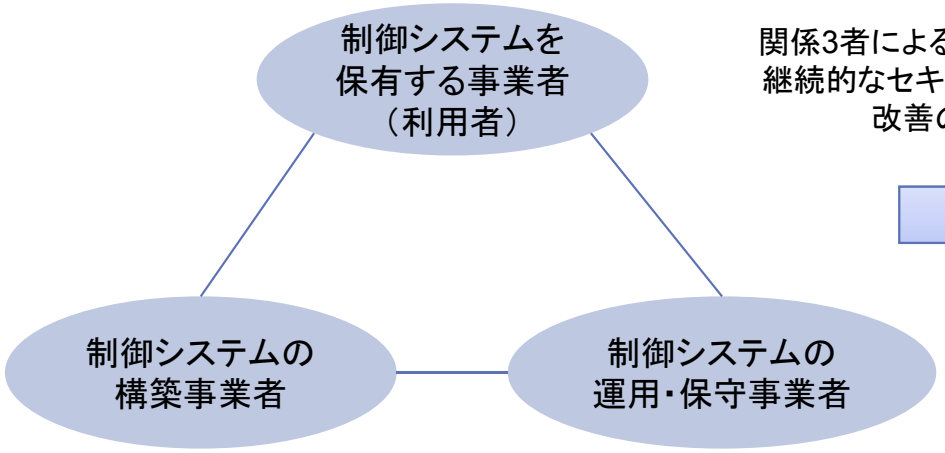
*参考URL：http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-020-01.pdf
**参考URL：https://www.npa.go.jp/cyberpolice/detect/pdf/20150526.pdf

参考5. CSMS（制御システムに関するサイバーセキュリティマネジメントシステム）

制御システムのセキュリティに関する組織の管理体制の認証制度です

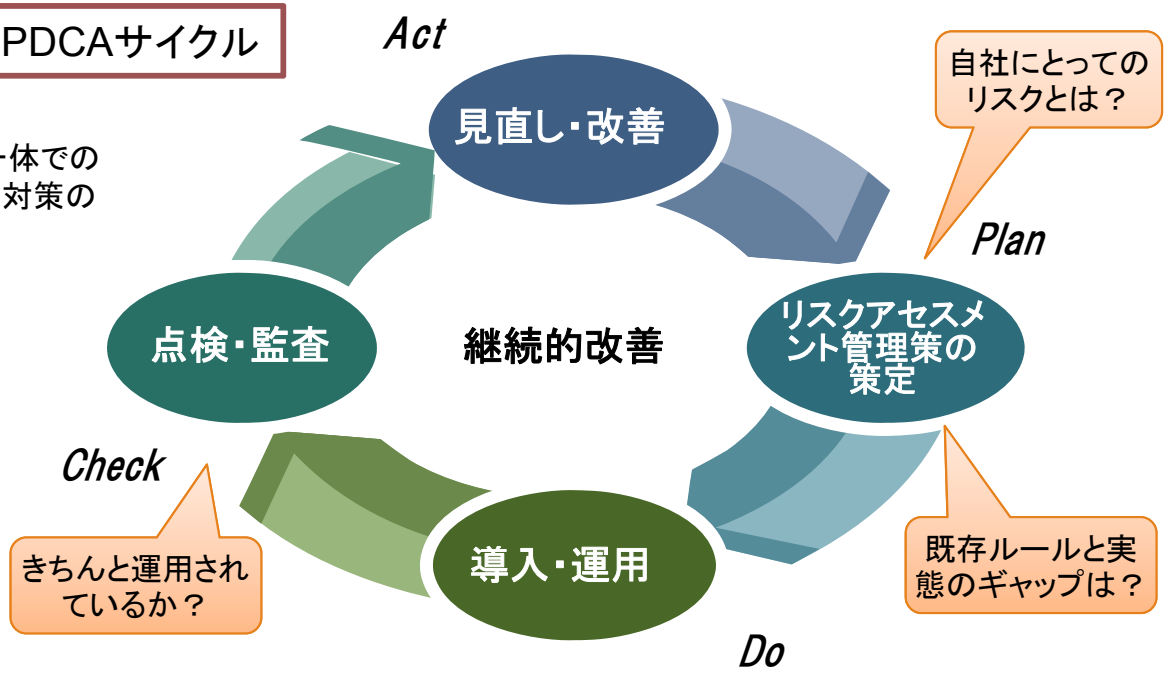
- 国際標準化機関である国際電気標準会議（IEC）は、制御システムのセキュリティに関して、取り組むべき組織の管理体制（マネジメントシステム）について規定した国際標準IEC 62443-2-1（CSMS基準）を2010年に定めています。
- わが国では、IEC 62443-2-1に基づき、自社の制御システムのセキュリティに関する組織の管理体制がCSMS基準に適合していることを客観的に示すための適合性評価制度が始まっています。

対象者



関係3者による三位一体での
継続的なセキュリティ対策の
改善の実施

PDCAサイクル



期待できる効果

- 社内のセキュリティガイドラインの改善
- 社員の意識や取り組みの向上
- 認証取得による、取引先からの信頼向上

リスクの低減だけでなく、
顧客からの信頼向上にも
つながります

*CSMS：Cyber Security Management System for IACS (Industrial Automation and Control System)

参考6. 制御システムを標的としたサイバー攻撃（Stuxnet、Havex）

■ 制御システムを標的とした高度なサイバー攻撃が発生しています

Stuxnet（スタックスネット）

被害概要： イランの核燃料施設のウラン濃縮用遠心分離機の PLC（Programmable Logic Controller）が不正に操作され、8,400台もの遠心分離機が稼働不能となり、核開発計画に3年程度の遅れが発生したといわれている。

事例概要： Stuxnetは、主にUSBメモリを介して制御システム内の PC に感染を広げ、最終的には操作端末を感染させた。
さらに、操作端末では、オペレータが気づかないように、密かにPLC を不正に操作することで、最終標的であるウラン濃縮用遠心分離器の回転速度を変化させ機能停止に追いこんだ。
以下のような脆弱性を利用したといわれている。

- Microsoft Windows の 5件の脆弱性（うち、4件は未公表の脆弱性）
- SCADAソフトウェア（監視制御のためのソフトウェア）のパスワードに関する脆弱性

Havex（ハーベックス）

被害概要： 欧州の電力会社を中心に、制御システムを管理するOPCサーバに関する情報の漏えいを引き起こした。

事例概要： 2014年、エネルギー業界の複数の特定企業を標的とした制御システムに対する攻撃が発覚。
攻撃者は、正規の制御ソフトアップデート用サイトを改ざんし、インストーラの中にマルウェアを含めることで、制御システムの保守PCを感染させ、OPCサーバの情報を取得して外部に送信する。
OPCサーバには制御システムの情報が蓄積されているため、さらなる攻撃の準備ともいわれている。

SCADA: Supervisory Control And Data Acquisition
OPC: OLE(Object Linking and Embedding) for Process Control

参考7. 制御システムを標的としたサイバー攻撃（ウクライナの大規模停電）

■ 特定の制御システムを標的とした高度なサイバー攻撃が停電を引き起こしたとされています

ウクライナの大規模停電(2015)

被害概要： 2015年12月23日に、ウクライナ西部の電力供給会社がマルウェアに感染し、供給地域の140万人に影響を与える停電が発生した。マルウェアの種類はBlack EnergyやKillDiskと言われており、マルウェア感染した端末からSCADAへの攻撃が行われたと推定される。

事例概要： 2015年の半ばから、BlackEnergyを使う攻撃グループは、ウクライナを標的としてきた。今回は、ウクライナの政党に関する文書を装ったWord文書を、メールの受信者に開かせ、コンテンツを有効にさせた際に、受信者のPCに寄生し、組織内のネットワークに侵入した。KillDisk等のモジュールを搭載したBlackEnergy 3の亜種が停電に関与していると推定されており、2016年2月現在も米国ICS-CERTとCERT-UAとが調査を継続している。初期のBlackEnergyは、トロイの木馬であり、DDoS攻撃の管理者ツールとして使われていたが、近年制御システム用のプラグインを追加し、注意が必要な存在となっている。

出所：米国ICS-CERTによる制御システムを狙ったサイバー攻撃への注意喚起、等に基づき作成
Ongoing Sophisticated Malware Campaign Compromising ICS (Update D) | ICS-CERT
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

出所：BlackEnergyに帯する注意喚起を行うCERT-UAのWebページ
До уваги системних адміністраторів щодо можливих атак BlackEnergy http://cert.gov.ua/?p=2464, 2016

参考8. 参考URL

情報提供コンテンツ

- 技術研究組合制御システムセキュリティセンター 「CSSC説明ビデオ」
  - http://youtu.be/wbEiDQZU5sI
- IPA 映像コンテンツ「今　制御システムも狙われている！ ー情報セキュリティの必要性ー」（独立行政法人 情報処理推進機構）
  - https://www.ipa.go.jp/security/keihatsu/videos/index.html
- IPA Webサイト「制御システムのセキュリティ」（独立行政法人 情報処理推進機構、制御システムのセキュリティ関連情報を掲載）
  - https://www.ipa.go.jp/security/controlsystem/index.html

ガイドライン・ツール等

- 「制御システムセキュリティ運用ガイドライン」（日本電気制御機器工業会（NECA））
  - http://www.neca.or.jp/wp-content/uploads/control_system_security_guideline.pdf
- 制御システム向けの簡便なセキュリティ自己評価ツール「日本版SSAT(Scada Self Assessment Tool)」（JPCERT/コーディネーションセンター）
  - https://www.jpcert.or.jp/ics/ssat.html
- 「制御システムセキュリティ自己評価ツール(J-CLICS)」（JPCERT/コーディネーションセンター）
  - https://www.jpcert.or.jp/ics/jclics.html

脆弱性対策情報の取扱い

- 「情報セキュリティ早期警戒パートナーシップガイドライン」（独立行政法人 情報処理推進機構, 一般社団法人JPCERTコーディネーションセンター 他）
  - https://www.ipa.go.jp/security/ciadr/partnership_guide.html
- 脆弱性対策情報ポータルサイト「JVN」
  - http://jvn.jp/
- 脆弱性対策情報データベース「JVN iPedia」
  - http://jvndb.jvn.jp/
- 「制御システム用製品の開発ベンダにおける脆弱性対応について」（JPCERTコーディネーションセンター ）
  - https://www.jpcert.or.jp/ics/information05.html

その他

- 技術研究組合制御システムセキュリティセンター　Webサイト
  - http://www.css-center.or.jp/
- 「サイバーセキュリティマネジメントシステム（CSMS）認証制度の確立について」（一般財団法人日本情報経済社会推進協会）
  - https://www.jipdec.or.jp/topics/news/20140425.html
- 「CSMSユーザーズガイド」（一般財団法人日本情報経済社会推進協会）
  - http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS111-08.pdf

【制御システム利用者のための脆弱性ガイド】

重大な経営課題となる制御システムのセキュリティリスク

～ 制御システムを運用する企業が実施すべきポイント ～

2015年3月 第1版発行
2016年3月 第2版発行
2017年3月 第3版発行

独立行政法人情報処理推進機構
〒113-6591
東京都文京区本駒込2丁目28番8号　文京グリーンコードセンターオフィス16階
URL　https://www.ipa.go.jp/security/
電話　03-5978-7527　　FAX　03-5978-7552