# サイバーリスクに対して
# 我が国の産業基盤をどのように護るべきか

情報セキュリティ＆危機管理セミナー
2019年2月8日
独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
副センター長　田辺雄史

# アジェンダ

１．情報セキュリティ10大脅威

２．サイバーセキュリティを取り巻く現状

３．制御セキュリティのリスク対策

４．産業サイバーセキュリティセンターの事業紹介

1．情報セキュリティ10大脅威

2．サイバーセキュリティを取り巻く現状

3．制御セキュリティのリスク対策

4．産業サイバーセキュリティセンターの事業紹介

# 1．情報セキュリティ10大脅威

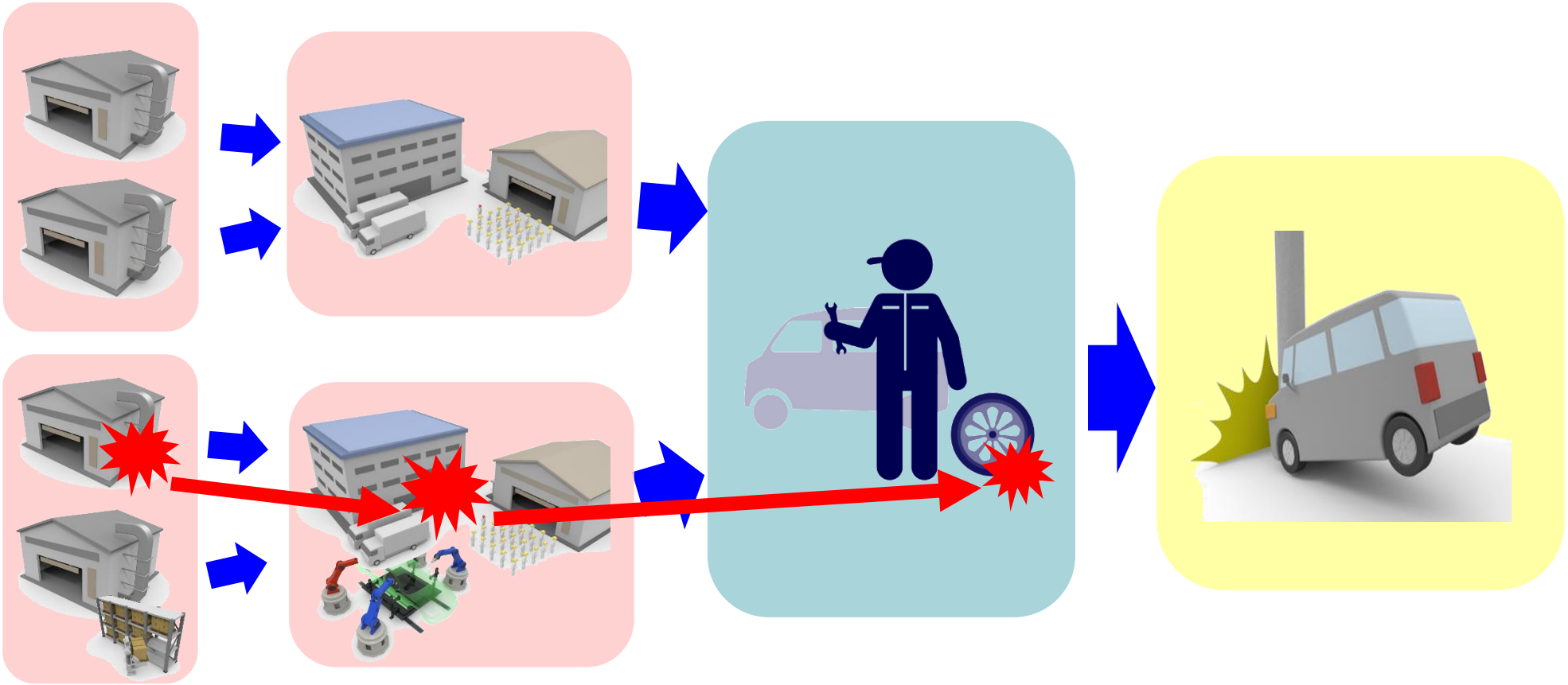
## 情報セキュリティ10大脅威　2019

| 昨年順位 | 個人 | 順位 | 組織 | 昨年順位 |
|---|---|---|---|---|
| 1位 (*1) | クレジットカード情報の不正利用 | 1位 | 標的型攻撃による被害 | 1位 |
| 1位 | フィッシングによる個人情報等の詐取 | 2位 | ビジネスメール詐欺による被害 | 3位 |
| 4位 | 不正アプリによるスマートフォン利用者の被害 | 3位 | ランサムウェアによる被害 | 2位 |
| NEW | メールやSNSを使った脅迫・詐欺の手口による金銭要求 | 4位 | サプライチェーンの弱点を悪用した攻撃の高まり | NEW |
| 3位 | ネット上の誹謗・中傷・デマ | 5位 | 内部不正による情報漏えい | 8位 |
| 10位 | 偽警告によるインターネット詐欺 | 6位 | サービス妨害攻撃によるサービスの停止 | 9位 |
| 1位 | インターネットバンキングの不正利用 | 7位 | インターネットサービスからの個人情報の窃取 | 6位 |
| 5位 | インターネットサービスへの不正ログイン | 8位 | IoT機器の脆弱性の顕在化 | 7位 |
| 2位 | ランサムウェアによる被害 | 9位 | 脆弱性対策情報の公開に伴う悪用増加 | 4位 |
| 9位 | IoT 機器の不適切な管理 | 10位 | 不注意による情報漏えい | 12位 |

(*1)クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018年個人1位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取、に分割。

# 1．情報セキュリティ10大脅威

## サプライチェーンの弱点を悪用した攻撃



部品メーカ　組　立　製　品

１．情報セキュリティ10大脅威

**２．サイバーセキュリティを取り巻く現状**

３．制御セキュリティのリスク対策

４．産業サイバーセキュリティセンターの事業紹介

# 2．サイバーセキュリティを取り巻く現状

## 社会インフラ・産業基盤を狙ったサイバー攻撃の世界的な増加

近年は社会インフラ・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。海外においては、既に他国家などからなされるサイバー攻撃により、**社会インフラ・産業基盤の安全が脅かされる事案が発生**。

### 原発の制御システム停止（米国、2003年）

発電所の制御システムがウィルスに感染。制御システムが**約５時間**にわたって**停止**。

### ロンドン五輪への攻撃（英国、2012年）

**毎秒約１万件の不正通信**。開会式会場の電力システムへの攻撃情報。手動に切り替え。

### 製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに**侵入**し、不正操作をしたため、**生産設備が損傷**。

### 変電所へのサイバー攻撃（ウクライナ、2015年、2016年）

マルウェア感染により、変電所が**遠隔制御**された結果、数万世帯で3～6時間にわたる**大停電**が発生。

# 2．サイバーセキュリティを取り巻く現状

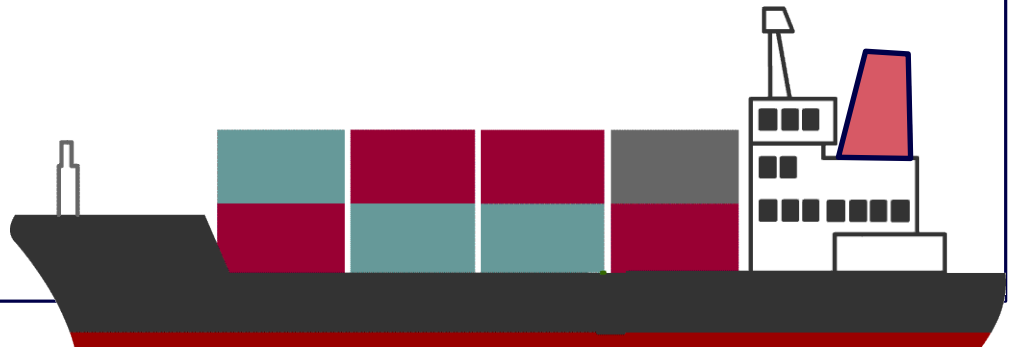
## 2017年度のインシデント事例

大手海運グループ（270～330億円の損害）

**荷役（コンテナの積込み・積下ろし）を管理する**
**システムが、マルウェア「NotPetya」に感染**

被害内容

- 数週間にわたりコンピュータがオフライン
- 顧客とコミュニケーションを取る手段を失い、予約取り消し
- 攻撃を受けた後に**サービスと信頼性を回復**するための**コストが増加**



# 2．サイバーセキュリティを取り巻く現状

## 2017年度のインシデント事例

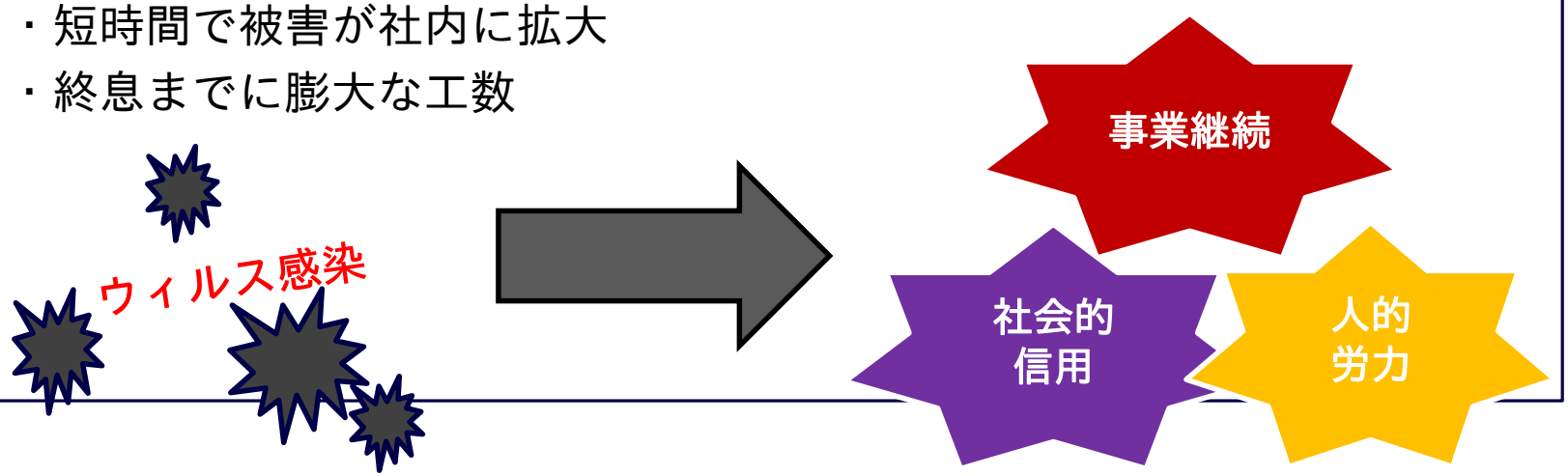
国内大手製造業

**自己増殖型ランサムウェアである**

**「WannaCry」ウイルスに感染**

被害内容

- グループ社内ネットワークのWindowsサーバーが感染して、システム障害を起こす
- 短時間で被害が社内に拡大
- 終息までに膨大な工数



# 2．サイバーセキュリティを取り巻く現状

## 脅威の動向

2017年は大規模なインシデントこそ発生しなかったものの、今後、制御システムのサイバー脅威が高まる予兆となる事件や傾向を認知。

- 制御システムのマルウェア感染
  - ✓ 2017年1～6月に制御システムのランサムウェア感染を435件確認（Kaspersky Lab.Inc）
  - ✓ 制御システムに特化したマルウェア（TRITON、Stuxnet等）の出現
  - ✓ 内部関係者の過失によるウィルス感染

- 情報報機関からの高度なハッキングツールの流出
  - ✓ 米中央情報局、米国国家安全保障局保有の脆弱性や高度なハッキングツールが流出。今後出現するウィルスやサイバー攻撃の高度化の懸念。

- 国家の関与
  - ✓ 国家紛争やテロのドメインがサイバー空間に拡大。制御システムへのサイバー攻撃により重要インフラを損壊・機能停止に。相手国に簡単かつ効果的にダメージを与える攻撃手段へ。

# 2．サイバーセキュリティを取り巻く現状

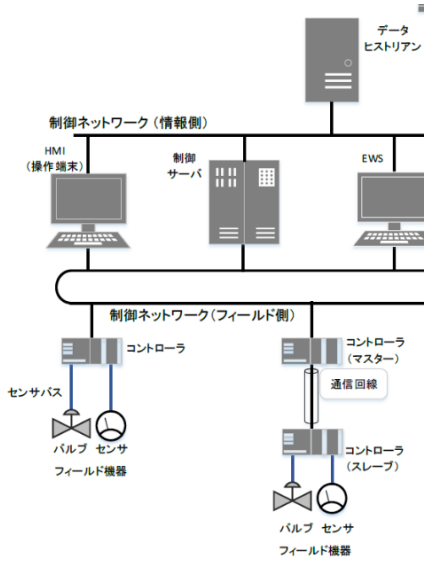
**制御システムとは**

社会インフラや工場・プラントの監視・制御や生産・加工ラインにおいて、他の機器やシステムを管理・制御するために用いられている機器群

社会インフラや工場・プラントは時代の進展とともに大規模かつ複雑化

➡ 制御システムの重要性増大

また、従来制御システムは、固有システムで構成され、外部ネットワークや共有システムとは未接続。
近年管理のため、情報システムとの接続経路を有しているケースが増加。




制御システム構成例

# 2．サイバーセキュリティを取り巻く現状

## 近年のセキュリティ対策のトレンド

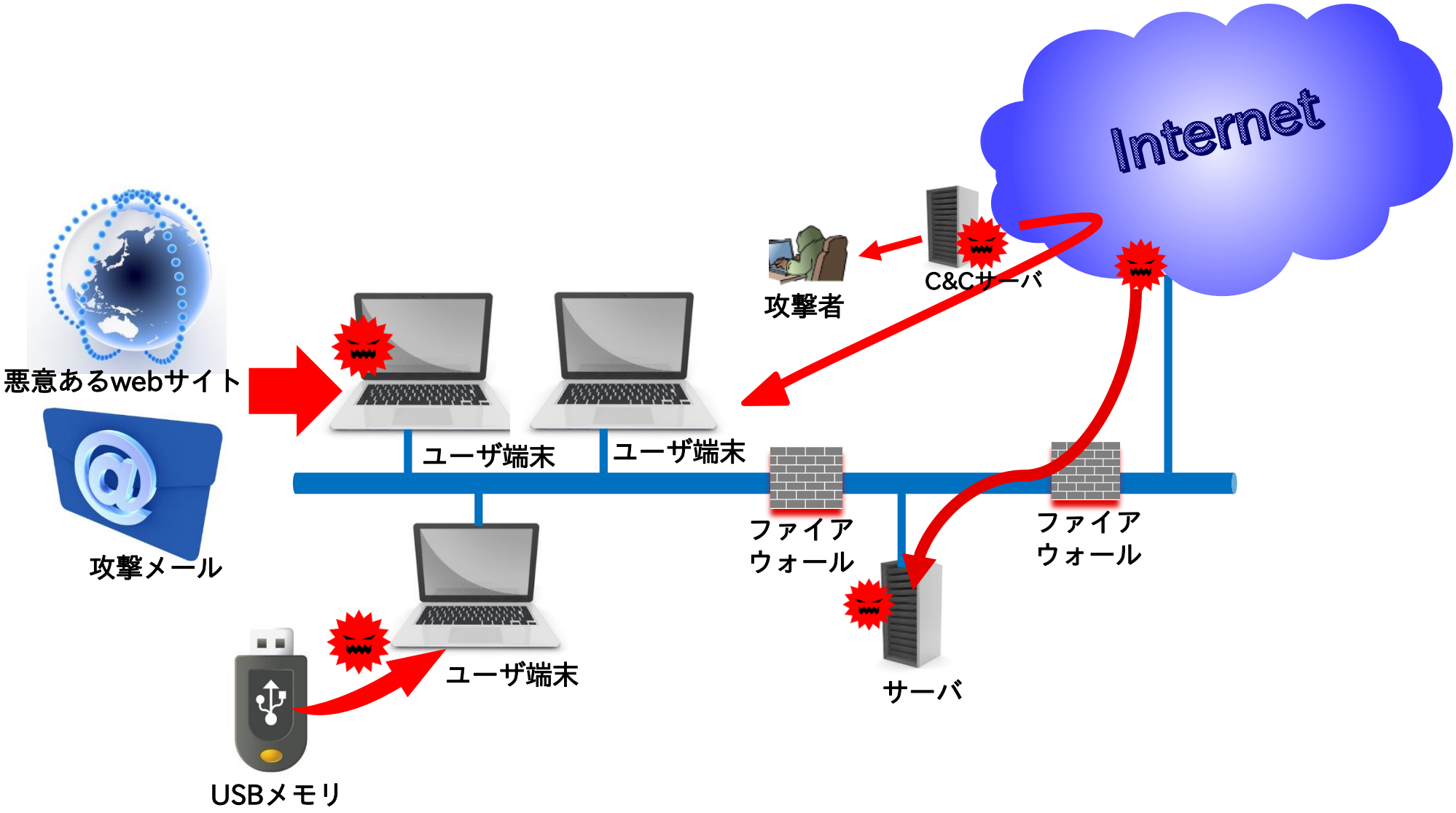
1. IT（Infomation Tecnology）からOT（Operasional Tecnology）へ
   →設備等の機能停止等で、社会の機能不全、経済的なダメージが現実に
2. 研修から演習へ
   →座学では、体得しきれず演習スタイルが主流に（攻守、実機の利用、etc）
3. 現場から経営へ
   →以前からの課題であるが、情報システム部門にとどまらない段階に

### 制御システムと情報システムにおける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 |
| セキュリティの対策 | モノ（設備、製品）<br>サービス（連続稼働） | 情報 |
| 技術のサポート期間 | 10年～20年 | 3年～5年 |
| 求められる可用性 | 24時間365日の安定稼働<br>（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 |

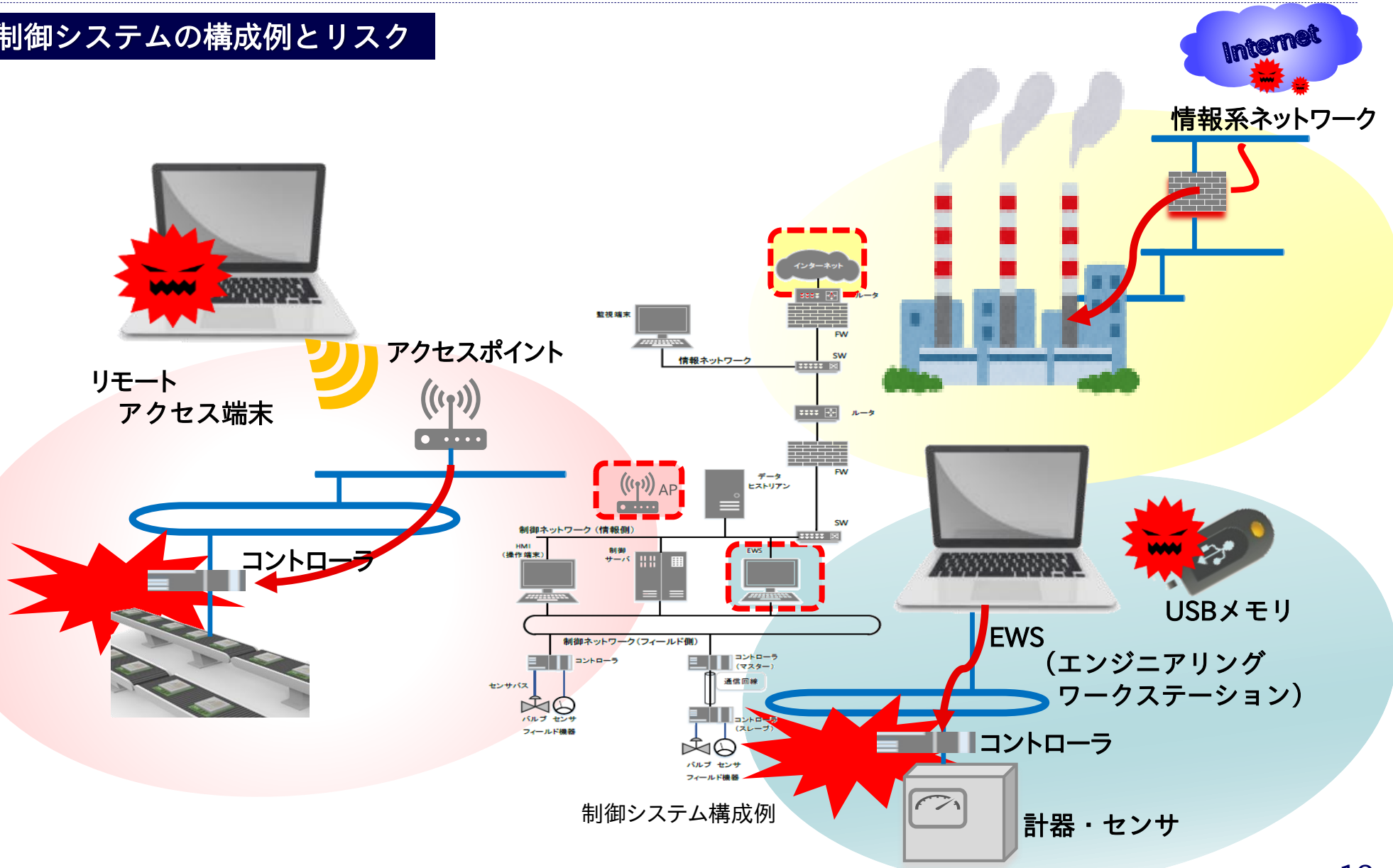
# 2．サイバーセキュリティを取り巻く現状

## 情報システムの構成例とリスク



# 2．サイバーセキュリティを取り巻く現状

## 制御システムの構成例とリスク




制御システム構成例

# 2．サイバーセキュリティを取り巻く現状

- 制御システムは、ウィ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
- セキュリティ被害の主原因は下記の4ケースに分類され、制御システムの運用状態において大きな脅威

被害事例の原因の多くは、こういった基本的な部分にある

### USBメモリ

- USBメモリからのウィルス感染事例は頻繁に発生。
- 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。

### 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、ウィルス混入が発生。

### 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、入れ替え時にウィルス感染していた端末から被害が発生。
- システムに接続する保守用端末が原因となるケースも有。

### 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を通過。
- 工業用無線LANからの侵入事例も有。
- パソコンのID、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。

- 多くの企業で制御システムのセキュリティ対策はあまり意識されておらず、端末や制御システムの大多数は脆弱性が修正されていない。
- そのため、工場の生産ラインの停止や設備損壊などを引き起こし、企業に甚大な損失を与える可能性が高まっている。

1. 情報セキュリティ10大脅威

2. サイバーセキュリティを取り巻く現状

**3. 制御セキュリティのリスク対策**

4. 産業サイバーセキュリティセンターの事業紹介

# 3．制御セキュリティのリスク対策

**サイバーセキュリティ経営ガイドライン**
経営層には、制御システムセキュリティに取組む環境を整えることが望まれる

➢ **対策マネージメント組織を構築**

**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の設置**

✓セキュリティポリシィの策定、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ージメントシステム（ＣＳＭＳがあります。）

現場の管理者は分かっていてもマネージメントする組織がなければ、また同じことがおきます。

➢ **サプライチェーン全体で考える**

✓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、自社だけではなく、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

子会社や取引先も含めて検討する必要があります。

➢ **現状の対策状況を確認するように指示を出す**

✓制御システムの導入及び調達の担当者
✓制御システムの運用・管理に携わる管理者

自分の状態を把握することが重要です。

# 3．制御セキュリティのリスク対策

➢ セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドラインを公表　（https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html）

1.経営者が認識すべき３原則

（1）経営者が、リーダーシップを取って対策を進めることが必要

（2）自社のみならず、ビジネスパートナーを含めた対策が必要

（3）平時及び緊急時のいずれにおいても、関係者との適切なコミュニケーションが必要

２．経営者がCISO等に指示すべき１０の重要事項

**リスク管理体制の構築**

（１）組織全体での対策方針の策定

（２）方針を実装するための体制の構築

（３）予算・人材等のリソース確保

**リスクの特定と対策の実装**

（４）リスクを洗い出し、計画の策定

（５）リスクへの対応

（６）PDCAの実施

**インシデントに備えた体制構築**

（７）緊急対応体制の構築

（８）復旧体制の構築

**サプライチェーンセキュリティ**

（９）サプライチェーンセキュリティの確保

**関係者とのコミュニケーション**

（10）情報共有活動への参加

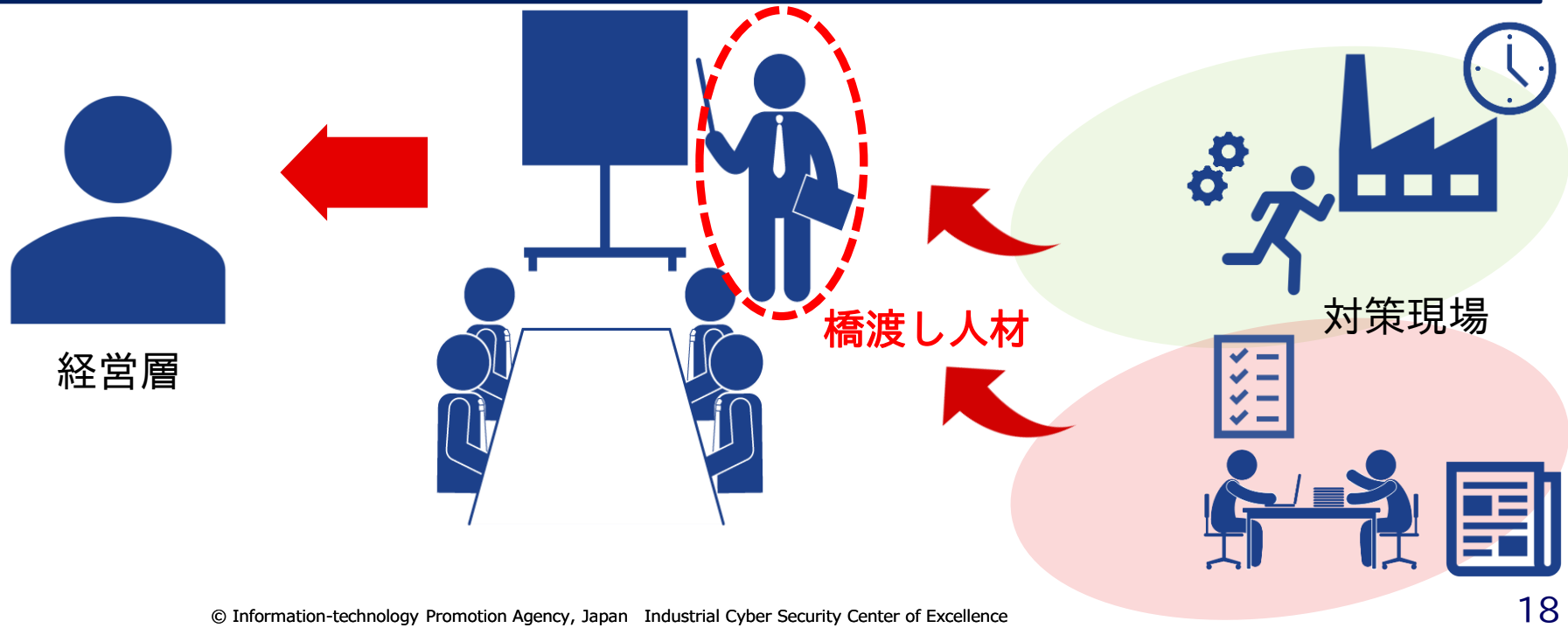
# 3．制御セキュリティのリスク対策

## 橋渡し人材の重要性

**経営層と現場をつなぐ「橋渡し人材」**

経営層が直接、サイバーセキュリティの専門的な知見をもつ実務者層とコミュニケーションをとることは難しい。専門技術を理解したうえで、一般的な業務や組織マネジメントにも通じた「橋渡し人材」が有事の際には重要な役割を果たす。

橋渡し人材は、部署横断的に情報を収集・分析して経営層とコミュニケーションを行うため、多面的なスキルを要求され、その育成は重要インフラ企業の課題。



1. 情報セキュリティ10大脅威

2. サイバーセキュリティを取り巻く現状

3. 制御セキュリティのリスク対策

**4. 産業サイバーセキュリティセンターの事業紹介**

# ４．産業サイバーセキュリティセンターの事業紹介

## 日本政府における産業サイバーセキュリティ施策方針

社会インフラ・産業基盤における、
**サイバー攻撃に対する防護力を強化**することは、
国家全体の喫緊の課題

OT(制御技術）とIT（情報技術）の知見を結集させた
世界レベルのサイバーセキュリティ対策の中核拠点
「産業サイバーセキュリティセンター」を2017年4月に発足

# 4．産業サイバーセキュリティセンターの事業紹介

**人材・組織強化、技術、ノウハウ**を結集し、社会インフラ、及び産業基盤のサイバーセキュリティ対策抜本的強化を図るために、**３つの事業**を柱に推進。

## 人材育成事業

- 自社システムのリスクを認識し、必要なセキュリティ対策を判断できる人材の育成
- 模擬プラントを用いた実践演習による、現場で活きるスキルの醸成
- 国内外の有識者、専門家との連携を促進
- 企業等の経営層へ、サイバーセキュリティ対策の必要性、人材活用についての啓発

## 制御システムの安全性・信頼性検証事業

- 実際の制御システムの安全性・信頼性に関するリスク評価・対策立案を行う

※IPAセキュリティセンターと連携して実施する事業

中核となる3事業


## 脅威情報の調査・分析事業（サイバー技術研究室）

- 脅威情報を収集、新たな攻撃手法など調査・分析
- 外部のホワイトハッカーの協力を得つつ、高度なサイバー技術の調査・研究

※IPAセキュリティセンターと連携して実施する事業

# 4．産業サイバーセキュリティセンターの事業紹介

## 人材育成事業（平成30年度事業）

### 中核人材育成プログラム

- 将来、企業などの経営層と現場担当者を繋ぐ、**“中核人材”**を担う方を対象としたプログラム。
- OTとITのスキルを核とした上で、サイバーセキュリティ対策の必要性を把握し、プロジェクトを強力に推進していく力を養う**1年間のトレーニング**。

**中核人材育成プログラム-年間スケジュール**

| 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| プライマリー（レベル合わせ） | | | ベーシック（基礎演習） | | | | アドバンス（上級演習） | | 卒業プロジェクト | | |
| 開講式 | | | ビジネス・マネジメント・倫理 | | | | | | | | 修了式 |
| | | | プロフェッショナルネットワーク（含む海外） | | | | | | | | |

### 責任者向けプログラム

- **業界別トレーニング（2日間）**：業界の固有事情を踏まえた熟議。対象業界のラインナップも拡充しつつ、最先端のセキュリティトピックスに対応。政策担当者も議論に参加。
- **国際トレーニング（2日間）**：米国企業の現役サイバーセキュリティ責任者、米国サイバー軍出身者らによる講義・机上演習（1日目は講義、 2日目は机上演習）。ウォーゲーム形式で「CISO」「工場長」「広報担当者」などの役割を体験しつつ、企業を守るスキルとメソッドを習得。
- NEW **戦略マネジメント系セミナー（11～12月週次夕方開催全7回）**：「企業におけるサイバーセキュリティ対策の機能」をメインテーマに講義・演習・ケースディスカッションを通じて熟議。技術的側面の議論ではないため、戦略企画、総務、広報など、リスク管理全般に関する責任者クラスの方も歓迎。産業横断サイバーセキュリティ人材育成検討会による協力。

**短期プログラム-年間スケジュール**

| | | | |
|---|---|---|---|
| 業界別トレーニング | 8月24,25日 業界別(1回目)（金属、石油、化学、製薬、製造） | 11月16,17日 業界別(2回目)（電力、ガス） | 2月15,16日 業界別(3回目)（鉄道、航空、船舶、交通） |
| 国際トレーニング | | 11月2,3日 国際トレーニング(1回目) | 2月1,2日 国際トレーニング(2回目) |
| NEW 戦略マネジメント系セミナー | | 11～12月、週次夕方開催全7回 | |

### ワン・デイ・エクステンション

- 産業サイバーセキュリティ対策への気づきの視点を端的に得ていただくとともに、各プログラムの有効活用についてご検討いただけるよう、各プログラムのエッセンスとなる特別演習等を提供。経団連・経営トップセミナー等と連携し、東京（10月31日）と大阪（2月5日）にて2度開催予定。

# 4．産業サイバーセキュリティセンターの事業紹介

## 制御システムの安全性・信頼性検証事業

➢制御システムのセキュリティに関する国際規格の活用の推進

- ✓ 制御システムのセキュリティについて、分野を限定しない汎用的な基準であり、セキュリティマネージメントからシステムや機器・デバイスまでをカバーする国際標準であるIEC62443シリーズの活用を推進。
- ✓ そのため、制御システムを保有する企業が、国際標準に準拠したセキュリティマネージメントシステムを構築するにあたっての基本となる、保護対象となるシステムのセキュリティの実態を把握するリスク分析を行うための「制御システムのセキュリティリスク分析ガイド」を公開（平成29年10月）。
- ✓ さらに、セーフティ要件を満たす制御システムによって稼働中の工場、プラント等の既存設備に対して、国際標準に準拠したセキュリティ対策を検討するための「制御システム セーフティ・セキュリティ要件検討ガイド」第２版を公開（平成30年10月）。





➢実際の制御システムの安全性・信頼性に関する情報収集・対策立案を実施

- ✓ 重要インフラのシステム障害発生のリスク低減および発生時の影響範囲縮小のため、障害事例を収集し、システム障害の原因分析・対策検討を行い、一般化・抽象化・普遍化した教訓を作成・共有。
- ✓ 重要産業や社会基盤を標的型サイバー攻撃の脅威から守るため、標的型サイバー攻撃情報の収集・分析、対策情報の共有をおこなう「J-CSIP（ジェイシップ）」や、 標的型サイバー攻撃を受けてしまった組織の被害状況の分析と対策の早期着手を支援する 「J-CRAT（ジェイクラート）」を推進。

# 4．産業サイバーセキュリティセンターの事業紹介

## 脅威情報の調査分析事業（サイバー技術研究室）

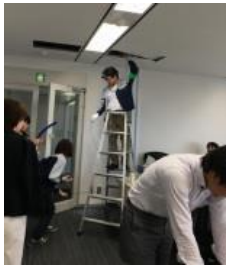
➢国内のホワイトハッカーのコミュニティの協力を得つつ、高度なサイバー技術の研究開発

- ✓ 国内のホワイトハッカーコミュニティの構築とその能力の活用により、公的機関や重要インフラなどにおけるセキュリティ課題への対応や、技術的な支援の実施。
- ✓ 国内及び国際的なセキュリティ機関同士の連携による、世界における最新のサイバー攻撃情報の調査分析と、その対策の立案。
- ✓ 産業サイバーセキュリティセンターをハブとして、国内の組織や研究者やホワイトハッカーコミュニティを横断したオールジャパンの体制で、サイバードメインの安全性を確立するのに寄与する、高度なサイバー技術研究プロジェクトを推進。

➢人材育成事業の受講生がサイバーセキュリティ分野の研究者との協働により研究活動を実施

- ✓ 中核人材育成プログラムの受講生のうちの有志が、サイバー技術研究室に入り、ホワイトハッカー等の研究者との協働により、ネットワークの構築、サイバー攻撃の観測、サイバー技術の調査・研究等に挑戦。
- ✓ 中核人材育成プログラム受講者への特別講義を開催。

サイバー技術研究室の風景



# ご清聴ありがとうございました