ご案内

本日は、ご参加いただき誠にありがとうございます。

セミナーの開始は**15:25**からです。

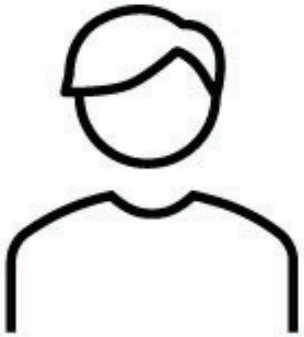
※セミナーの録音・録画・キャプチャ等はご遠慮ください。
※セミナー資料の二次配布はご遠慮ください。
※規格や法令についての説明は一例や概要となっています。
詳しくは原文をご確認ください。
※セミナー25分＋QA5分　の予定です。
ご質問によっては本日の回答を控えさせていただく場合もございます。
予めご了承くださいませ。

サイバーセキュリティの概要と適合性評価標準

一般財団法人日本品質保証機構
安全電磁センター　試験部
サイバーセキュリティ課

藤田　悠平

JQA 一般財団法人 日本品質保証機構



藤田　悠平

JQA　安全電磁センター

試験部

サイバーセキュリティ課

OT

Cyber security

DX

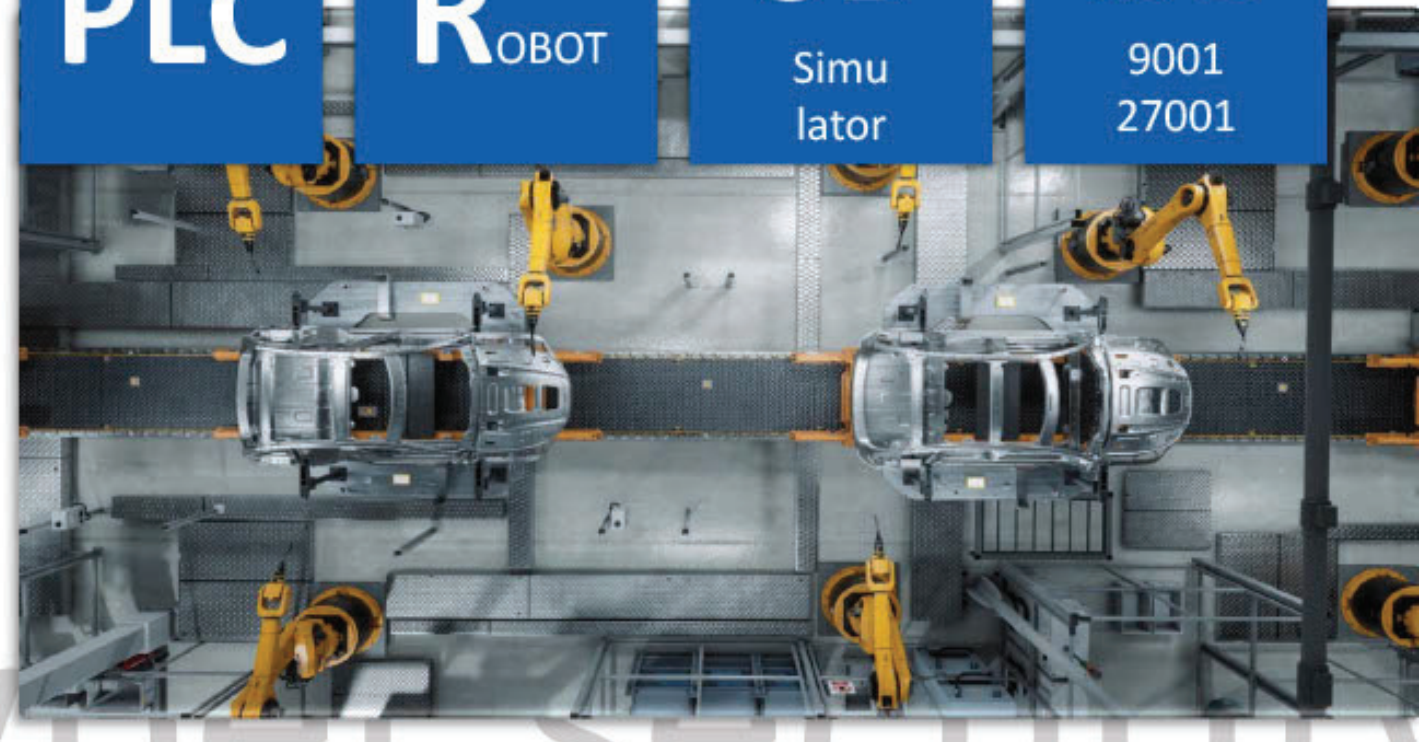
IoT

PLC

ROBOT

3D Simulator

ISO 9001 27001



Cyber security

サイバーセキュリティの概要と適合性評価標準

導入 5分

15分 サイバーセキュリティ

規格類 5分

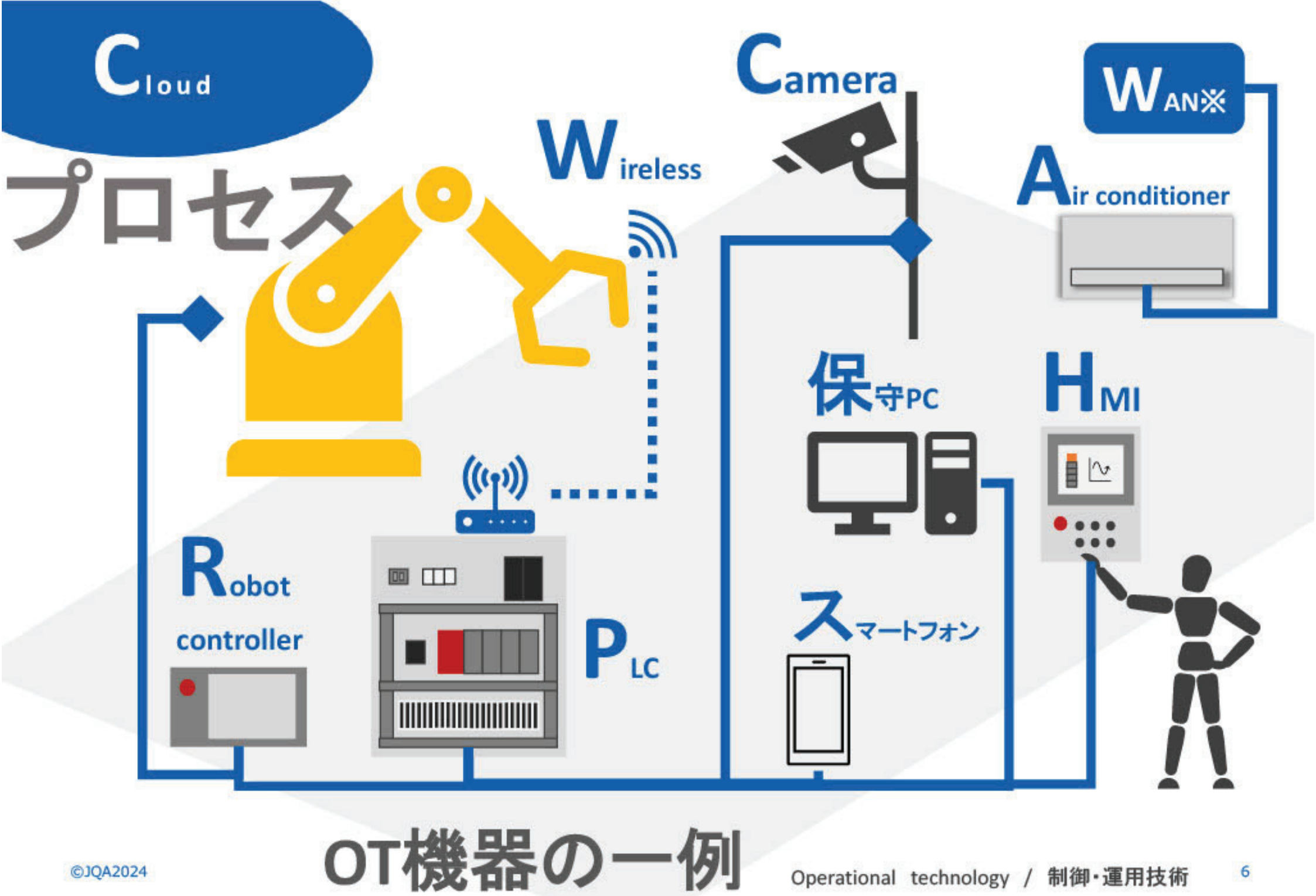
Cyber

OT

Operational technology / 制御・運用技術

Cybersecurity

サイバーセキュリティ



OT機器の一例

Cyber

OT システム

使用環境

開発

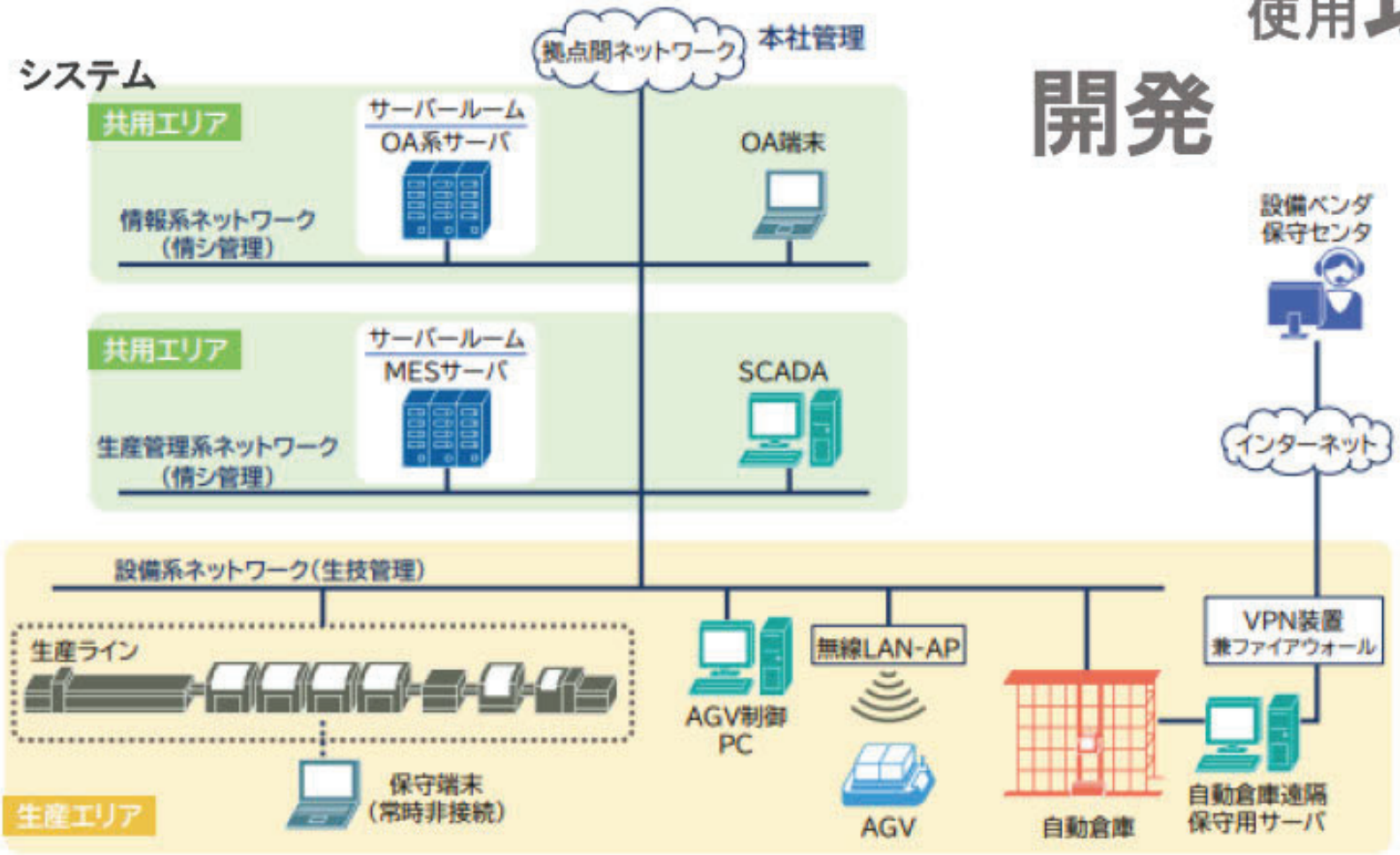


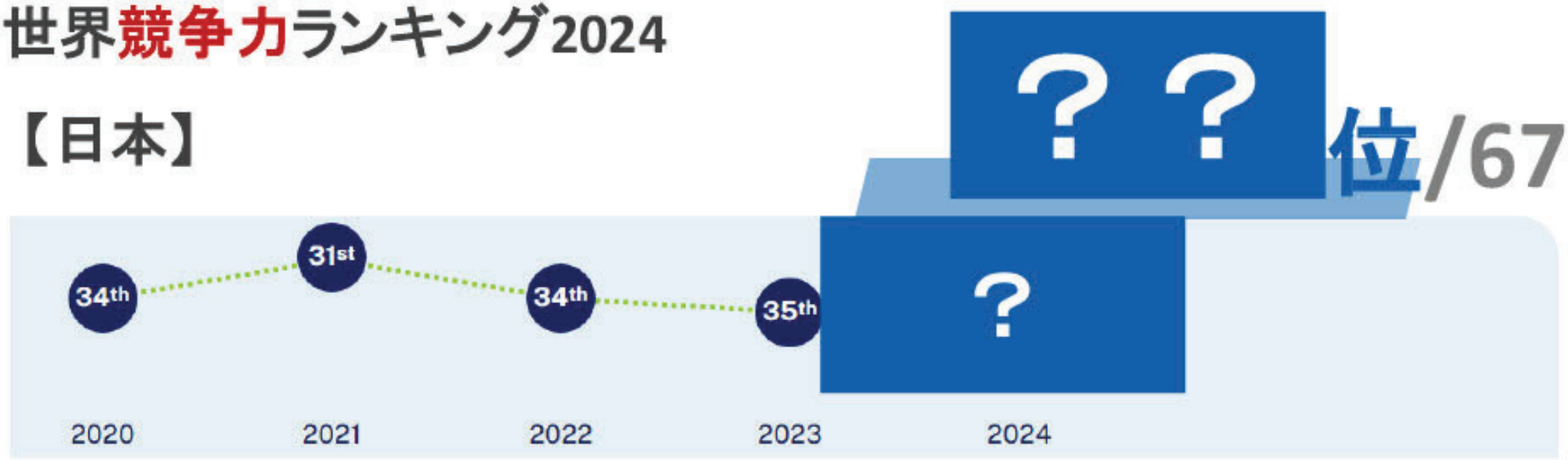
図 2-1 工場システムの例

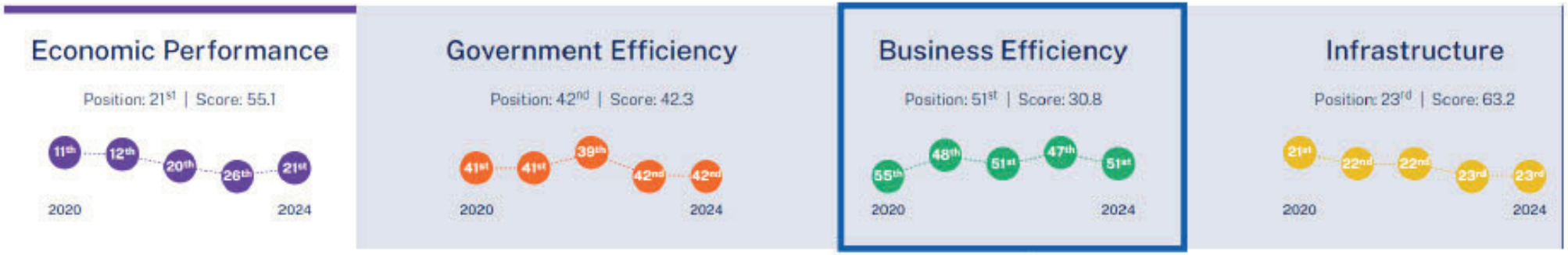
出典:工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(METI/経済産業省)

Cyber

世界競争力ランキング2024

【日本】





出典 Japan - IMD business school for management and leadership courses

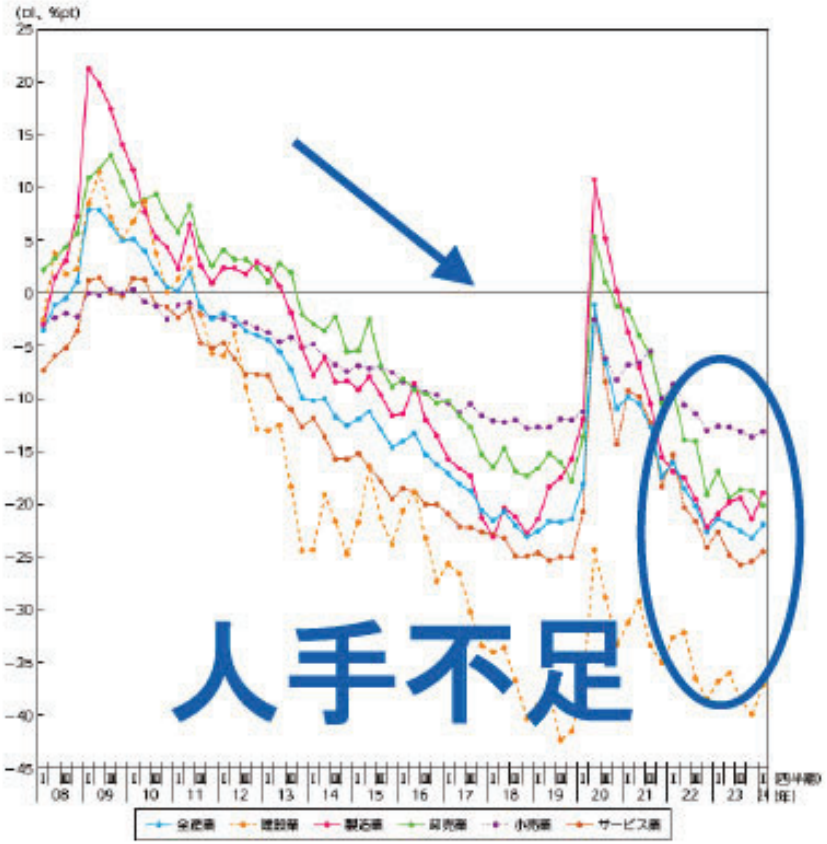
51位

＞ライトハウス工場 「日本 ●%」

※デジタル技術や環境配慮などの先進工場

Cyber

図211-4　中小企業における産業別従業員数過不足DI（今期の水準）の推移



備考：従業員数過不足DIは、今期の従業員数が「過剰」と答えた企業の割合（%）から、「不足」と答えた企業の割合（%）を引いたもの。
資料：中小企業庁「中小企業景況調査」（2024年3月）

出典　2024年版ものづくり白書（ものづくり基盤技術振興基本法第8条に基づく年次報告）（METI/経済産業省）

労働人口　減

若者人口　減

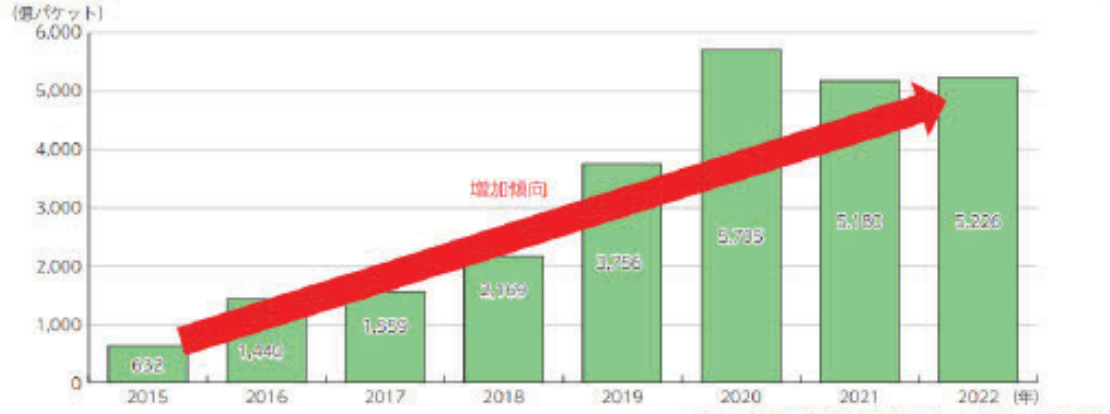
労働時間　減

デジタル化

Risk

Cyber

図表4-10-2-1 NICTERにおけるサイバー攻撃関連の通信数の推移



(出典) NICT「NICTER観測レポート2022」を基に作成

8倍

図表4-10-2-3 サイバーセキュリティに関する問題が引き起こす経済的損失

調査・分析の実施主体	対象地域	対象期間	経済的損失の概要	損失額
トレンドマイクロ	日本	2021年	セキュリティインシデントに起因した1組織あたり年間平均被害額	3億2,850万円
警察庁	日本	2022年上半期	ランサムウェア被害に関連して要した調査・復旧費用の総額	20%が100万円未満 14%が100万～500万円未満 10%が500万～1,000万円未満 37%が1,000万～5,000万円未満 18%が5,000万以上
FBI	米国	2021年	サイバー犯罪事件による被害報告総額	69億ドル
NFIB	英国	2022年	サイバー犯罪による被害報告総額	630万ポンド
Sophos	世界31か国	2021年	直近のランサムウェア攻撃の修復に要した1組織あたりの年間平均コスト	140万ドル
IBM	世界	2022年	組織における1回のデータ侵害にかかる世界平均コスト	435万ドル
Cybersecurity Ventures	世界	2023年【予測】	サイバー犯罪によるコスト	8兆ドル
McAfee、CSIS	世界	2020年	サイバー犯罪によるコスト	9,450億ドル

(出典) 各種公開資料を基に作成

3億円

8兆ドル

出典 総務省｜令和5年版 情報通信白書｜サイバーセキュリティに関する問題が引き起こす経済的損失 (soumu.go.jp)第10節 サイバーセキュリティの動向

Cybersecurity

サイバー攻撃

標的型攻撃

•企業など特定の組織やユーザーグループを狙ったサイバー攻撃。
攻撃者がターゲットの知人や取引先になりすまし、悪意のあるファイルを添付したメールや悪意のあるサイトへ誘導するURLリンクを送り、PCやスマートフォンなどの端末をマルウェアに感染させようとする攻撃

ランサムウェア

•身代金を要求するために使用されるマルウェア。デバイスへの攻撃が成功すると、マルウェアは画面をロックしたり、ディスクに保存されているデータを暗号化したりして、デバイス所有者の画面に身代金の要求と支払情報を表示。

Emotet（エモテット）

•電子メールを介して感染する遠隔操作型のボットマルウェア。Emotetは、悪意のあるサイトにアクセスしたり、悪意のあるマクロを含むファイルを開いたりすることで感染。感染後は、情報漏えいやマルウェア・スパム送信などのさらなる攻撃に利用されたり、ランサムウェアなど他のマルウェアに感染することなどが確認されている。

サプライチェーン攻撃

•企業や政府機関など正面からの侵入が困難な組織をターゲットとする場合に、セキュリティ対策が比較的脆弱な取引先や子会社を経由して攻撃を仕掛ける手法。 攻撃者は、取引先からの電子メールを偽造してターゲット企業に送信したり、ターゲット企業が使用するソフトウェア製品に不正なアップデートを仕込んだりする。

Cybersecurity

ランサムウェア攻撃事例

2021年10月、公立病院がランサムウェアに感染し、電子カルテの利用ができなくなり、医療、事務で利用していたサーバーもダウン。こうした状況により、外来会計ができない状態に陥った。病院が復旧を依頼した企業に7,000万円を支払い、65日後に電子カルテシステムを再稼働することに成功した。

サプライチェーン攻撃事例

2022年２月ごろ、大手自動車メーカーのサプライチェーンに連なる部品メーカーがサイバー攻撃を受け、マルウェアに感染。これがきっかけとなり、自動車メーカーの14工場28ラインが停止した。典型的なサプライチェーン攻撃であり、日本の基幹産業を支える自動車メーカーが約1万台以上の自動車の生産を見送るという未曾有の事態になった。

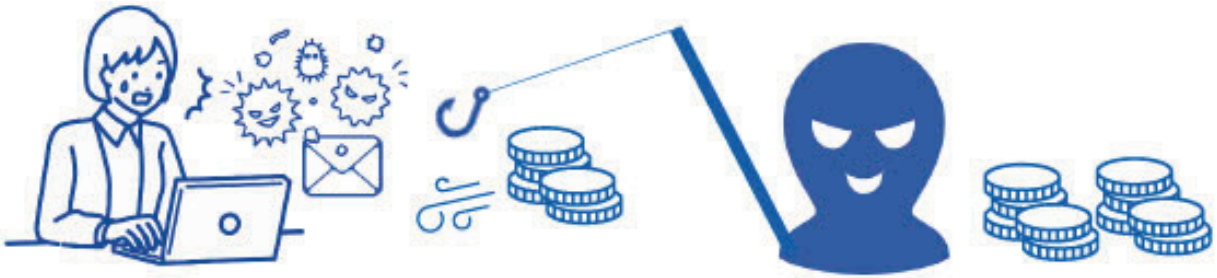
◆不特定多数を対象としたサイバー攻撃

フィッシング詐欺

信頼できる企業や組織を装った攻撃者が、ターゲットの個人情報を要求する。
一般的なフィッシングの手法は、銀行や金融機関を装って電子メールを送信し、電子メール内の偽のフォームに入力させたり、
口座情報やログイン情報の入力を要求するWebページにアクセスさせたりすることで不正に個人情報を取得するものが挙げられる。

フィッシング攻撃事例

2018年1月、国内の暗号資産取引所が外部からメールを利用したフィッシング攻撃を受け、580億円相当の暗号資産が流出・盗難される事態に至った。



Cybersecurity

DoS攻撃/DDoS攻撃

1台または複数のPCやサーバーを利用して、標的のサーバーに大量のアクセスやデータを送りつけるサイバー攻撃。データを送りつけることで標的のサーバーに負荷がかかり、Webサイトのアクセス障害やサービス停止などの被害が発生。
DoS攻撃とDDoS攻撃の違いは、攻撃に使用するPCが1台か複数台かによる。
DDoS攻撃の場合、攻撃に使用される複数の端末は、第三者のPCを悪用している可能性がある。そのためDoS攻撃よりも攻撃性が高く、匿名性が高いため、より悪質な攻撃となる。

DoS/DDoS攻撃事例

2015年11月、東京開催の国際スポーツ競技大会の組織委員会のWebサイトにDDoS攻撃が行われ、サイトが約12時間にわたって閲覧不能となった。

ゼロデイ攻撃

- メーカーが修正プログラムの配布などの対応をする前に、OSやソフトウェアに発見された脆弱性を利用する攻撃。

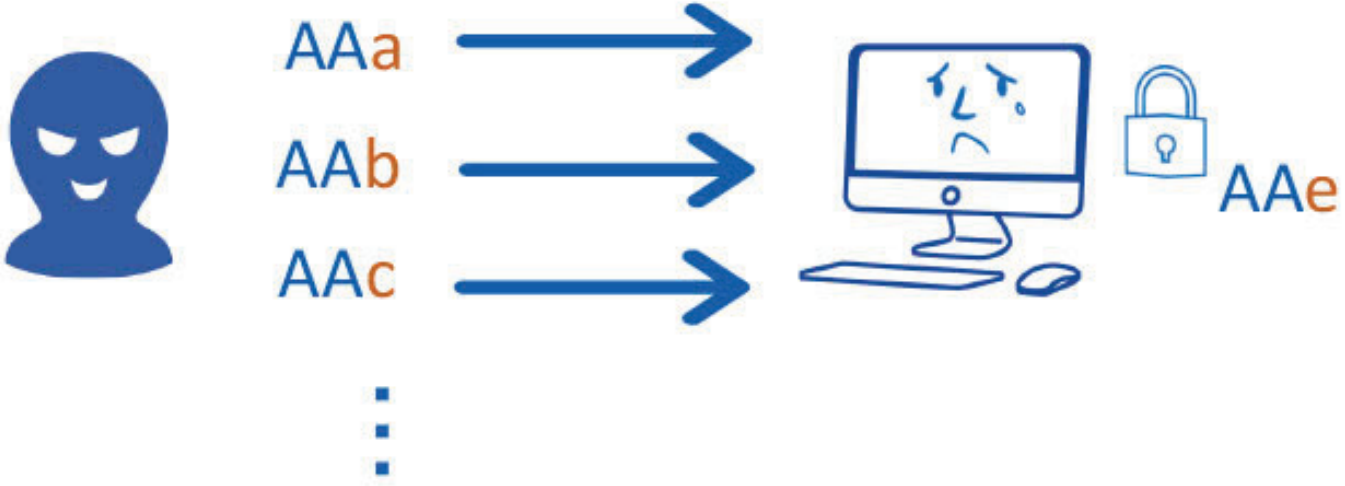
脆弱性とは、コンピュータのOSやソフトウェアにおいて、プログラムの欠陥や設計ミスにより発生するセキュリティ上の欠陥。
脆弱性が発見されると、企業やベンダーは更新プログラムを作成し、アップデートを実施することで対応するが、新たな脆弱性は次々と発見されるため、アップデートまでの間は脆弱性が放置されることになる。
攻撃者はこの脆弱性を狙っており、このようなアップデートまでの隙を突いた攻撃を「ゼロデイ攻撃」と呼ぶ。

Cybersecurity

総当たり攻撃（ブルートフォースアタック）

パスワードなどを不正に解読する際に、可能な限りすべての組み合わせを試す攻撃方法。

この方法は、人力では手間と時間がかかりすぎてしまうが、現在は簡単に実行できるツールが広く出回っており、時間の制約がない限り、パスワードを解読して侵入することができる方法。

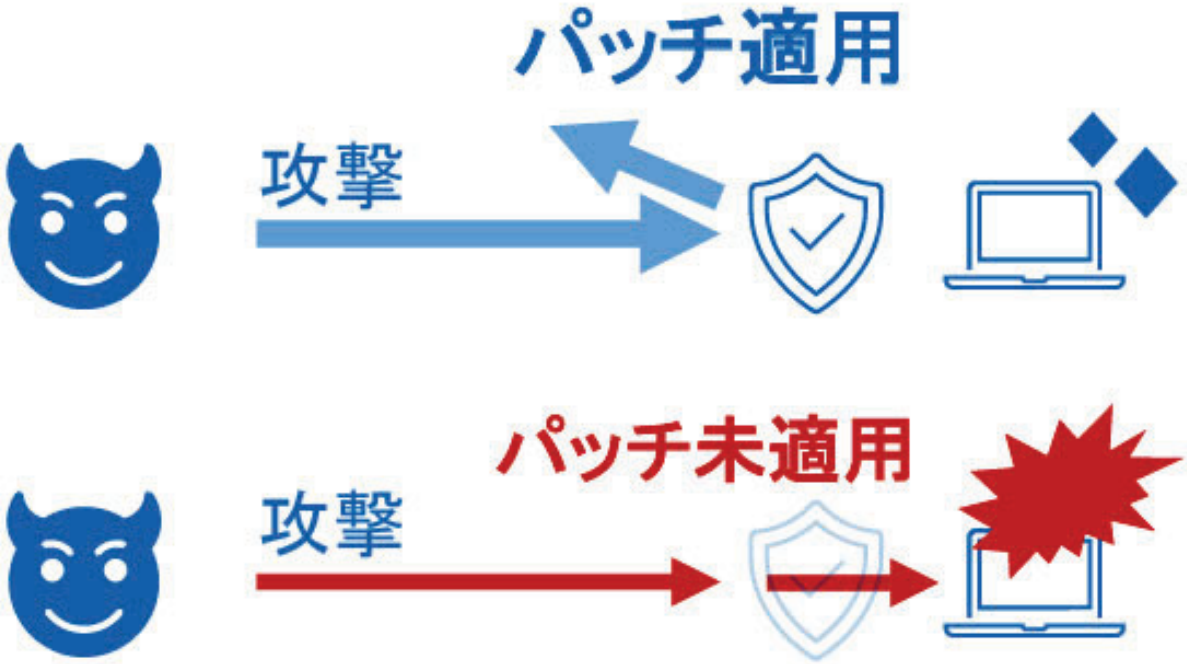


効果的なセキュリティ対策；
パスワード設定の厳格化、
・数字と英字の組合せ。
・同じパスワードの使いまわしをしない。
など
多要素認証などの導入で総当たり攻撃（ブルートフォースアタック）の被害を防ぐ。

Cybersecurity

脆弱性対策情報の公開に伴う悪用

ソフトウェアやハードウェアの脆弱性対策情報の公開は、製品の利用者に脆弱性の脅威や対策の情報を広く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行うおそれがある。



Cybersecurity

情報セキュリティ10大脅威 2024（IPA）

順位	「組織」向け脅威	初選出年	過去
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典：情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

Cybersecurity

制御システムへの攻撃

POINT　外部との情報ネットワーク接続がない場合でもインシデントリスクは有る

マルウェア攻撃事例1

Stuxnet と呼ばれるマルウェアが核燃料施設に持ち込まれ、マルウェアに感染させられたコンピュータによって、遠心分離機を制御する PLC の設定ロジックが改ざんされ、周波数変換器※1が攻撃されたことにより、約 8,400 台の遠心分離機のうち約 1,000 台2が稼働不能に陥り、操業が一時停止する事態となった。
制御ネットワークへのマルウェア持ち込み方法は USBメモリと考えられている。

※1出力周波数を変換することで、モーターの速度を制御できる装置

出典：IPA.【事例4】Stuxnet：制御システムを標的とする初めてのマルウェア（参照2024年1月19日）

POINT　計装システムも攻撃対象になることがある

マルウェア攻撃事例2

「2017 年 12 月に公表されたマルウェア「HATMAN（別名:TRITON / TRISIS）」は、安全計装システム※2（以下、SIS：Safety Instrumented System）を標的とした初のマルウェアである。当該マルウェアは中東の企業で使用されていた Schneider Electric 社製の SIS コントローラー(Triconex)や関連製品に対して、サイバー攻撃※3を行うために開発・使用されたという。結果的にSIS のフェールセーフ※4機能が作動し、操業が一時停止する事態となった」

※2 安全計装システム：一つ以上の安全関連システムを導入するために用いられるシステム
※3 サイバー攻撃：ネットワークを介してパソコンやスマホなどの情報端末に対し不正アクセス、情報窃取、システム停止などを目的とした操作を行うこと。
※4 フェールセーフ：異常発生時に安全な方向に動作させる考え方、手法。

出典：IPA.【事例3】2017年 安全計装システムを標的とするマルウェアP.4（参照2024年1月17日）

Cybersecurity

港湾システムへの攻撃

2023 年 7 月 NUTS（名古屋港統一ターミナルシステム）全ターミナルの作業が停止

- ✓ 日本初の港湾施設における大規模なサイバー攻撃
- ✓ 復旧まで ー 約3日
- ✓ 侵入口 ー VPN機器や外部USBなどが考えられる（特定はされていない）
- ✓ 国土交通省が「コンテナターミナルにおける情報セキュリティ対策等検討委員会」を設置。

出典：『Port OF Nagoya 2023-2024』｜名古屋港管理組合公式ウェブサイト (port-of-nagoya.jp)

出典：国土交通省名古屋港コンテナターミナルのサイバー攻撃におけるインシデント対応についてshiryo2.pdf (nisc.go.jp)

Cybersecurity

セキュリティインシデント

外的要因

- サイバー攻撃など外部からの攻撃
- 自然災害をはじめとする不測の事態

内的要因

- セキュリティ体制の不備
- 企業や組織内人員の故意による情報漏洩
- 個人情報が保存されているPC・USBメモリの紛失や盗難

をはじめとするヒューマンエラー

インシデントが発生してしまうと・・・

対策のための時間や**コスト大**

社会的**信用の低下**

訴訟

株価

などの恐れが・・・

Cybersecurity

サイバーセキュリティ

Cybersecurity

セキュリティ３要素

機密性
Confidentiality

アクセスを認可された者だけが、情報にアクセスできることを確実にすること

実装技術：アクセス制御、 **パスワード**認証、 PGPによる暗号化、
セキュリティ区画の立ち入り制限、etc.

完全性
Integrity

情報が正確であり、完全であることを保護すること

実装技術：デジタル署名、アクセスログ、etc.

可用性
Availability

情報へのアクセス許可のある人が必要な時点で情報にアクセスできること

実装技術：システムの2重化(多重化）、サーバのUPS、
ハードディスクのRAID構成、etc.

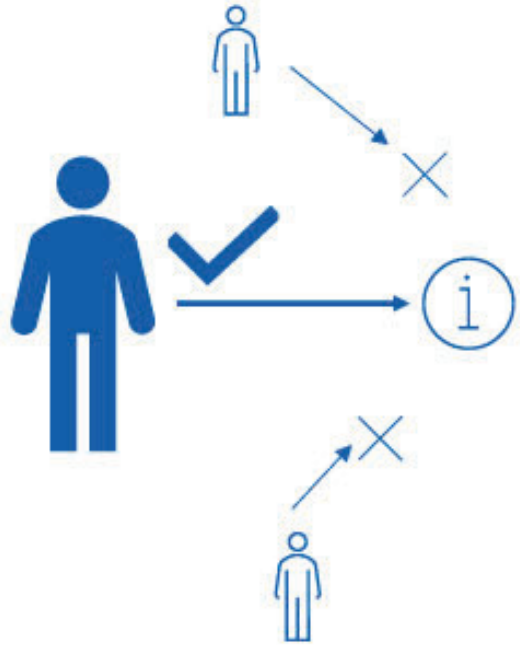
Cybersecurity

機密性 : Confidentiality

(IEC 62443-4-2: 3.1.12)

認可されてない個人、プロセス、又はデバイスに情報が開示されないことの保証

“情報へのアクセス許可のある人だけが情報を利用することができ、許可の無い者は情報の使用、閲覧が出来なくすること”



実装技術例

- アクセス制御
- パスワード認証
- PGP（暗号化プログラム）による暗号化*
- セキュリティ区画の立ち入り制限

*暗号化：データの内容を他人には分からなくするための方法

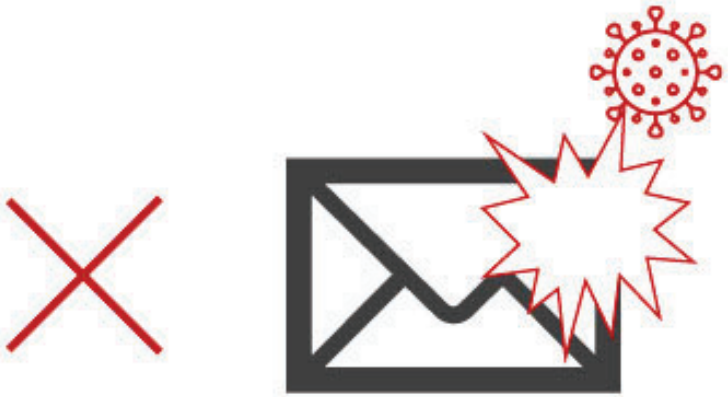
Cyber

完全性 : Integrity

(IEC 62443-4-2: 3.1.27)

資産の正確性及び網羅性を保護する特性

“情報が正確であり、完全であることを保護すること。情報資産に正確性があり改竄されていないこと“



実装技術例

- デジタル署名*
- アクセスログ*

*デジタル署名：暗号化された電子的署名。本人証明に使用される。

*アクセスログ：アクセスを記録したもの。

Cybersecurity

可用性 : Availability

(IEC 62443-4-2: 3.1.7)

制御システムの情報及び機能へのタイムリーで信頼できるアクセスおよび使用を保証する特性

“情報へのアクセス許可のある人が必要な時点で情報にアクセスできること”

実装技術例

- システムの2重化*（多重化）
- サーバのUPS*
- ハードデスクのRAID* (Redundant Arrays of Inexpensive Disks)

*システムの2重化：障害などに備え予備のシステムを用意すること。
*UPS（無停電電源装置：Uninterruptible Power Supply）：停電時などに一定時間電力を供給できる電源装置。
*RAID（レイド、Redundant Arrays of Inexpensive Disks）：複数の外部記憶装置（ハードディスクなど）を一台の記憶装置として運用する技術

Cybersecurity

真正性 : Authenticity

(IEC 62443-4-2: 3.1.6)

オリジンの認証及び完全性の検証を通じて、エンティティが主張しているものであるという特性。

“ なりすましではないということ”

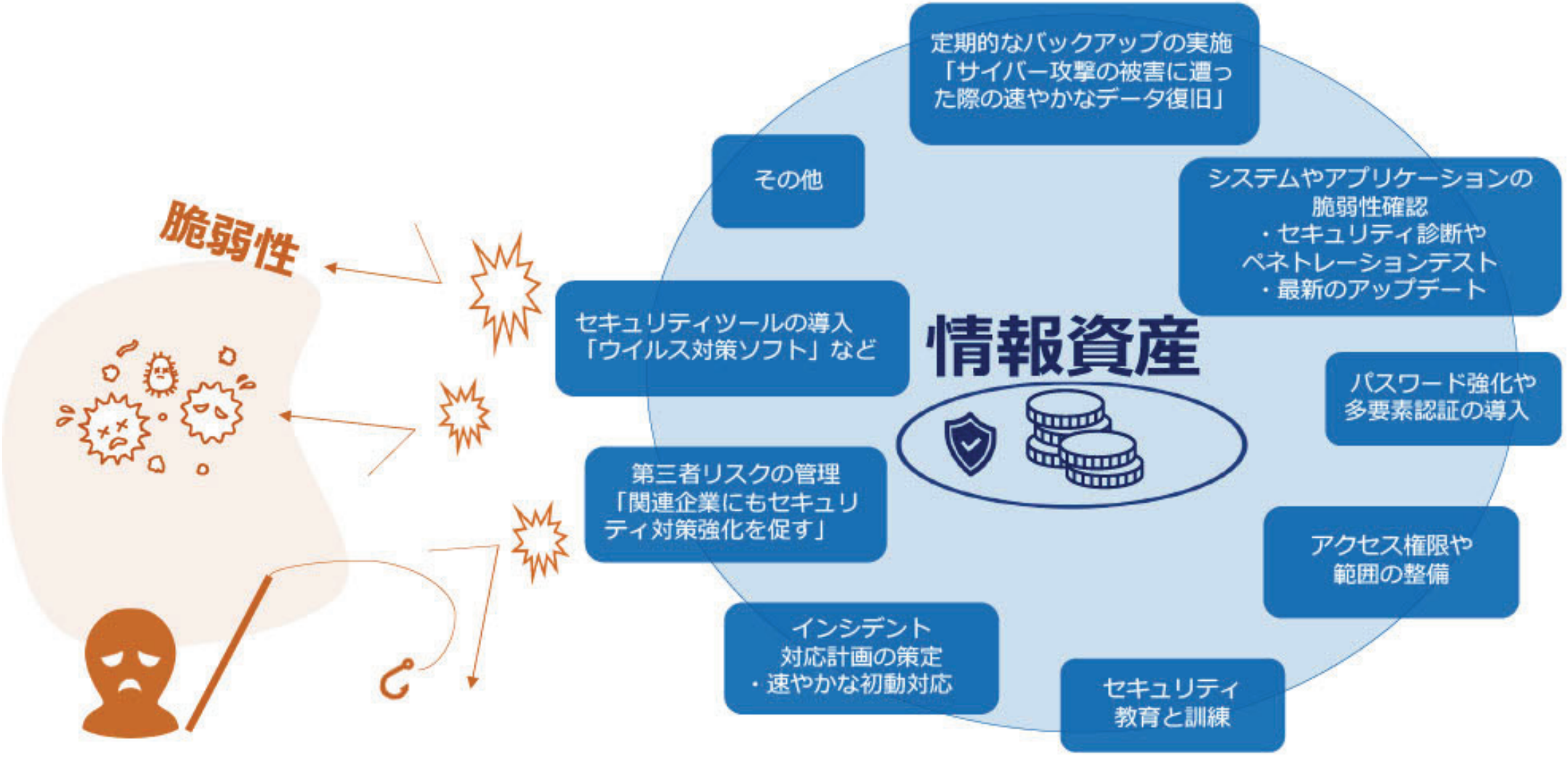
侵害例

他人のIDやPASSで侵入

対策

多要素認証

Cybersecurity



Cybersecurity

OTセキュリティ

Cybersecurity

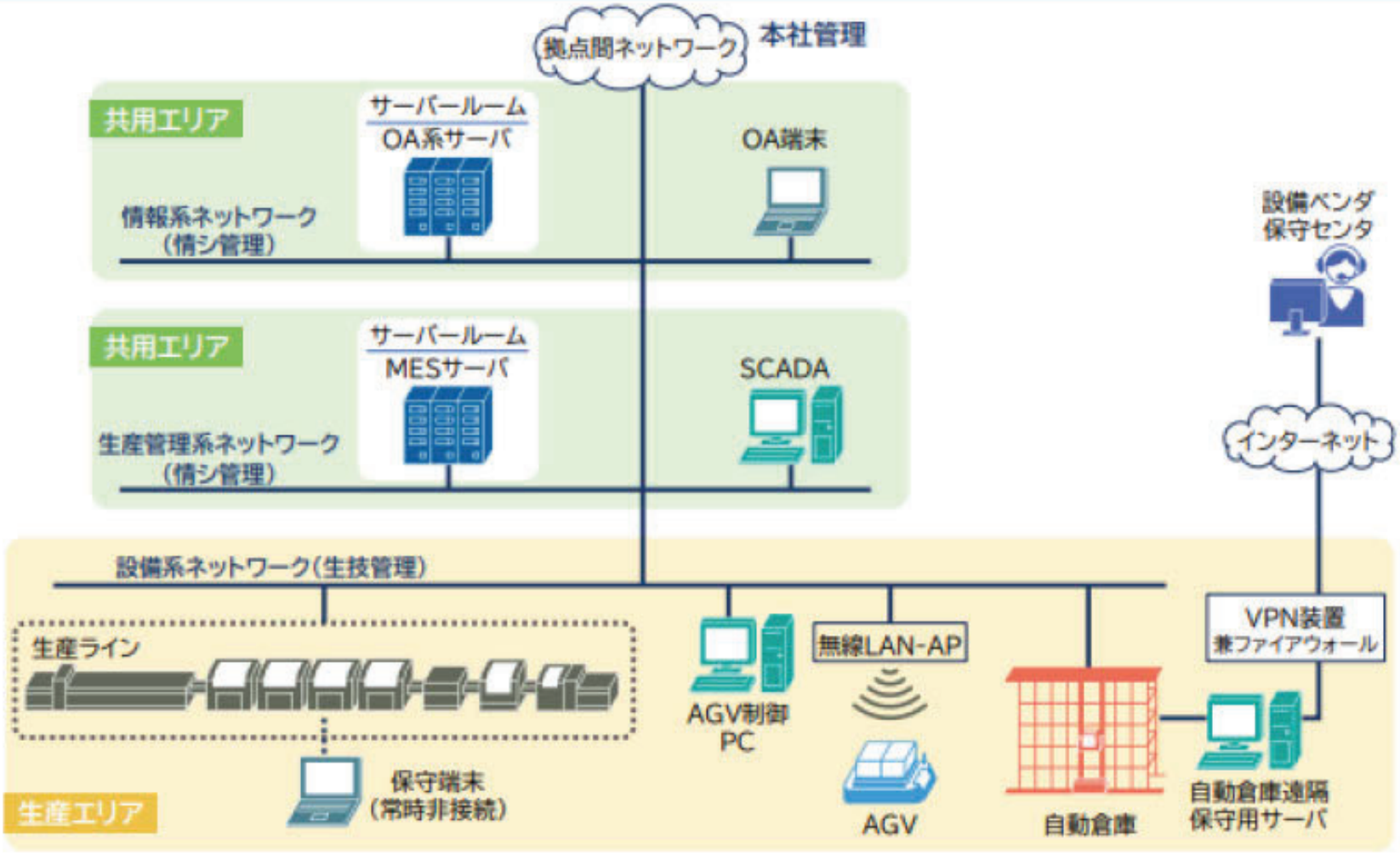
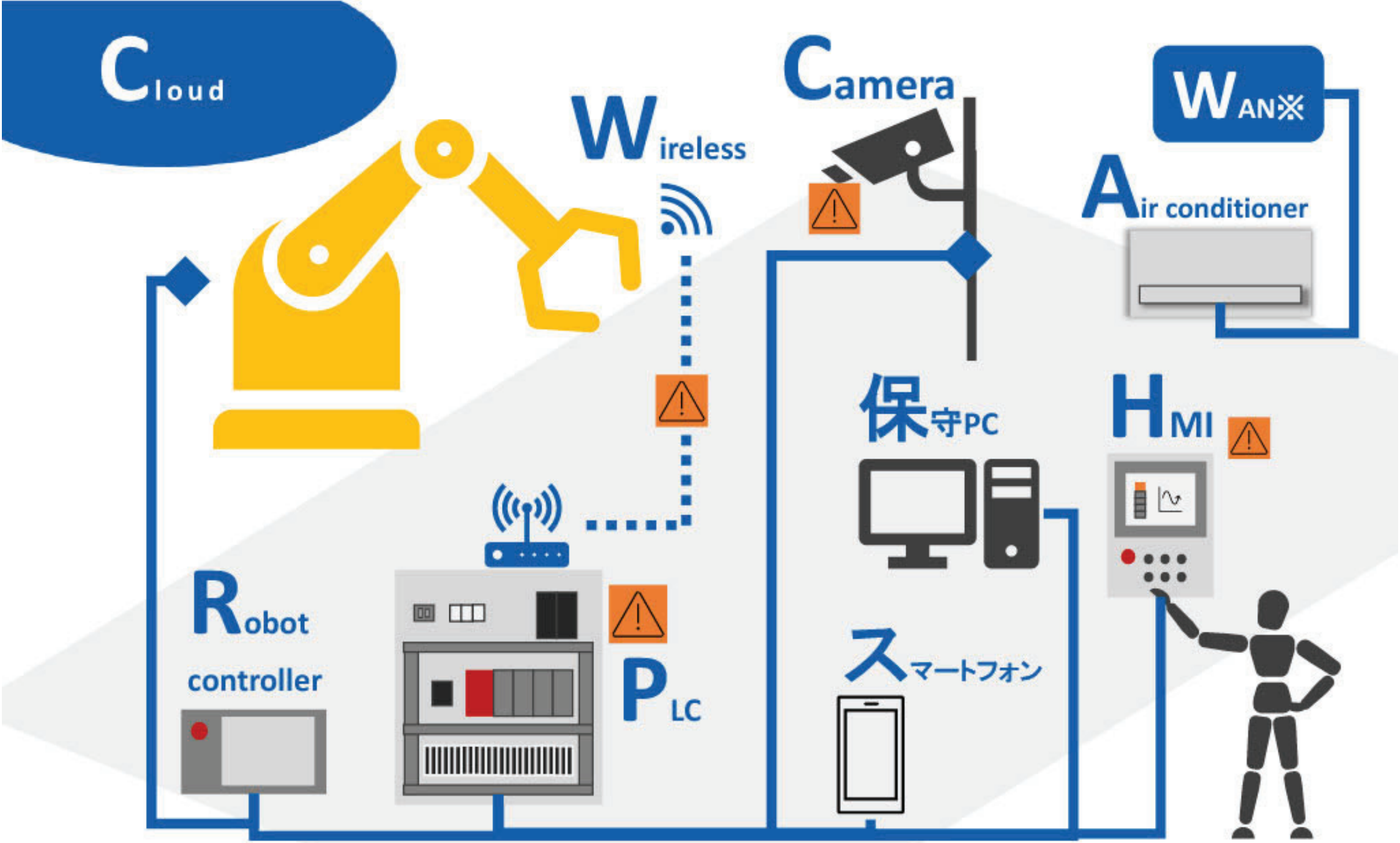


図 2-1 工場システムの例

出典:工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(METI/経済産業省)


Cloud
Wireless
Camera
WAN※
Air conditioner
保守PC
HMI
Robot
controller
PLC
スマートフォン

Cybersecurity

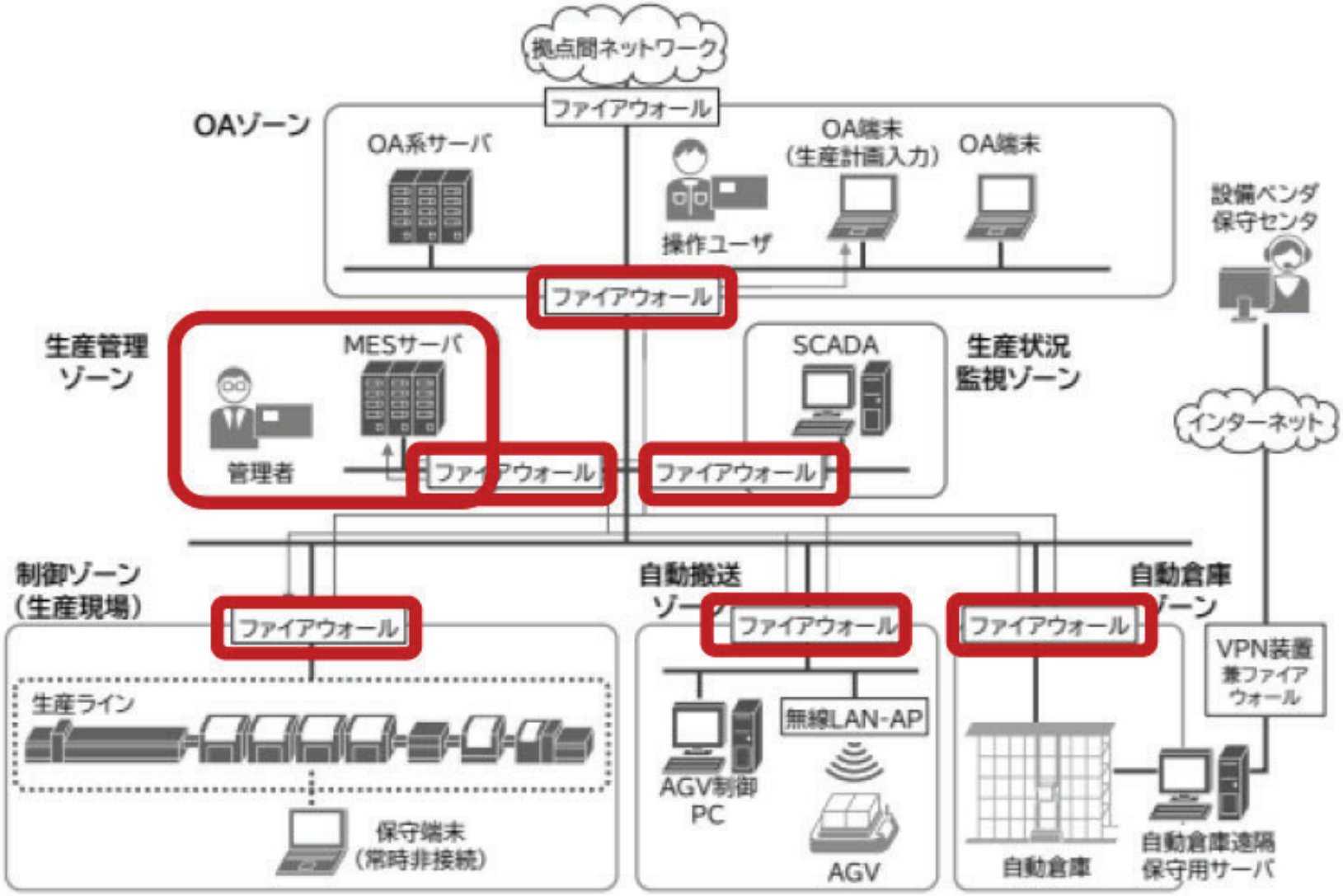


図 3-3 要件に対する各ゾーンでの対策(例)

出典:工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(METI/経済産業省)

キーボード

マテハンI/O

AGV/AMR

PLC

リスク

データ盗聴

遠隔攻撃

不正操作

可用性の喪失

犯罪の踏み台

人的被害

対策

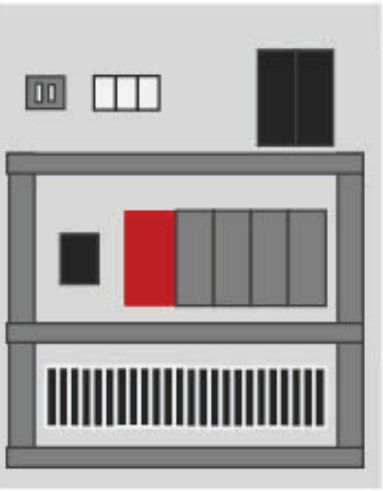
最新Ver.

認証

暗号化

アクセス管理

デフォルト設定からの変更



PLC

リスク

ネットワーク侵入

集中管理

SCADA

全社システム

PG書換、異常を停止

IT攻撃

スクリプト

イーサネット

人的ミス

古いPG

隣のライン

対策

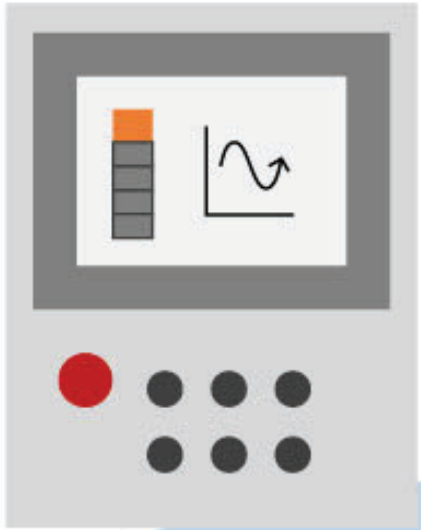
パスワード

リードオンリー

盤の施錠

通信監視、制限

FW最新



HMI

リスク

不正操作

設備破壊

品質変化

情報漏洩

ネットワーク侵入

見た目の偽装

（正常に見せる）

対策

ハードウェア

認証

アクセス管理

Camera

リスク

- 情報漏洩
- ネットワーク侵入
- 攻撃者からの監視
- DoS予備軍
- 可用性の喪失

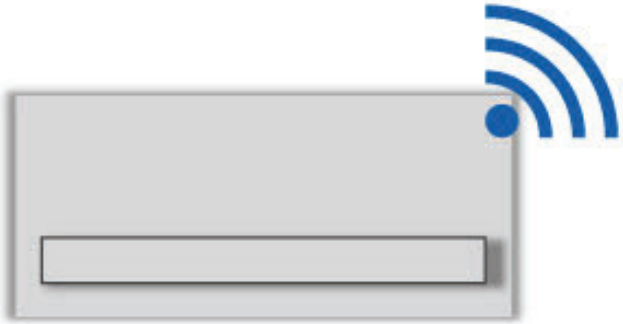
対策

- アクセス制限
- パスワード設定
- デフォルトの設定を変更

法令と適合性評価標準

法令と適合性評価標準

参考例



法令

CRA RED PSTI

規格

EN 303 645
（整合規格の候補とされています）

法令と適合性評価標準

無線機器指令のサイバーセキュリティ要件について、委任規則で適用範囲が明確化され、規制が開始される見込み。

無線機器指令（RED）2014/53/EU

■ 必須要件（第３条）

【特定要件 3(3)】

d. 通信網やその機能に害を与えず、また通信網の資源を濫用せず、サービスの受容できない低下を引き起こさないこと;

e. ユーザーや加入者の個人情報やプライバシーの保護を確かとする防護手段を持つこと;

f. 詐欺行為の防止のための機能を備えること。

サイバーセキュリティーの委任規則（DELEGATED REGULATION）EU 2022/30

【 Article 1 】

1. 特定要件 3(3)dは、直接通信するか他の機器を介して通信するかにかかわらず、**インターネットを介して通信できるすべての無線機器に適用される。**('internet-connected radio equipment')

2. 特定要件 3(3)eは、**個人データ、またはトラフィックデータと位置データを処理する機能を持つ**、以下の機器に適用される。

(a) 下記(b),(c),(d)以外の、**インターネットに接続された無線機器。**

(b) 育児専用に設計または意図された無線機器。

(c) 玩具安全指令の対象となる無線機器。

(d) 以下のいずれかに着用、ストラップ、または吊り下げられるように設計または意図された無線機器。

(i) 頭、首、胴体、腕、手、脚、足など、人体のあらゆる部分。

(ii) 帽子、手着、履物を含む、人間が着用する衣服。

3. 特定要件 3(3) fは、インターネットに接続された無線機器が所有者またはユーザーが**金銭、金銭的価値、または仮想通貨を送金できる場合に適用される。**

規制開始

【施行予定日】 2025年8月1日（現地時間）

【整合規格の有力候補】 EN 303 645

法令と適合性評価標準

ETSI EN 303 645

法令と適合性評価標準

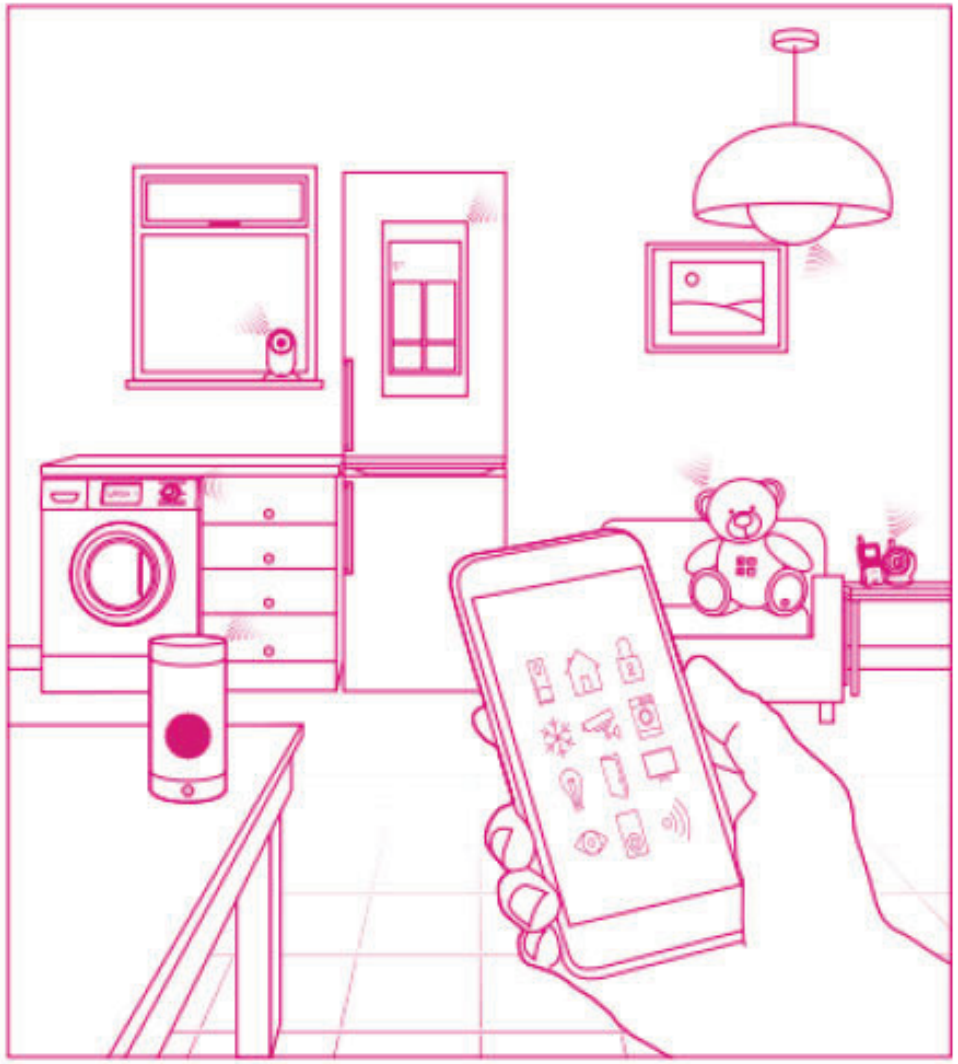
ETSI EN 303 645は、一般消費者向けIoTデバイスのための初の国際的なサイバーセキュリティ規格です。この規格は、設計から運用に至るまで、サイバーセキュリティのリスクを軽減するための包括的なフレームワークを提供しており、**無線機器指令のサイバーセキュリティ要件の基準として機能すると考えられています。**

また、ETSI EN 303 645に基づく認証制度が導入されている国があります。

シンガポール: ETSI EN 303 645が、IoTデバイスのセキュリティ基準として利用されています。

ドイツ、フィンランド: ETSI EN 303 645に基づくセキュリティラベリング制度が導入されています。

日本: ETSI EN 303 645を参照しているセキュリティ要件適合評価及びラベリング制度（JC-STAR）が2024年度導入予定。



⚠ 2024年10月現在、無線機器指令のサイバーセキュリティ要件に対する整合規格は定されていません。

お知らせ

JQAのサービス

サービス概要（EN 303 645）モジュールAの場合

ETSI EN 303 645の事前準備からレポート発行まで

全体の流れ

ステップ0 サイバーセキュリティ導入セミナー、技術相談等

ステップ1 DUTの識別

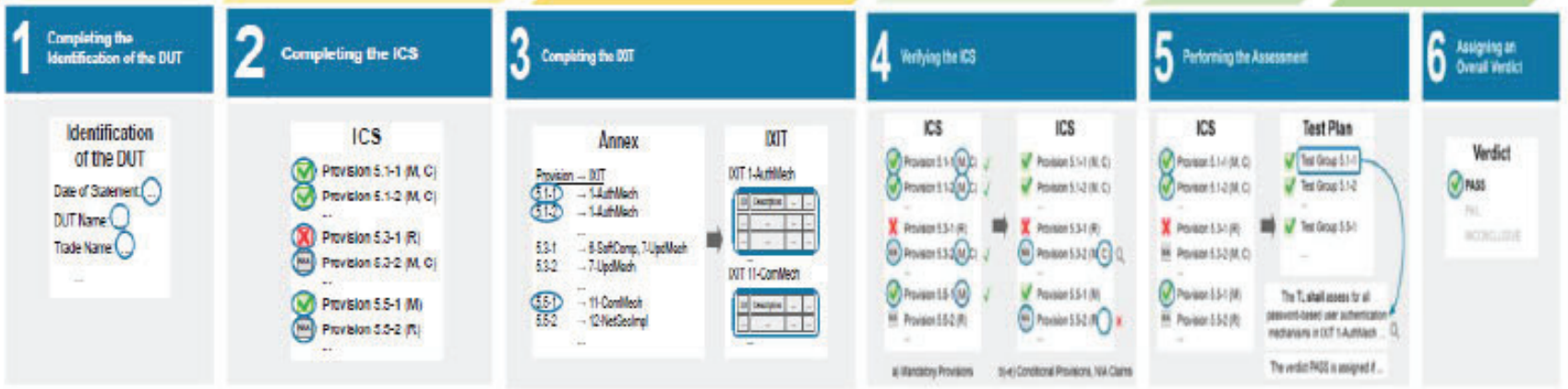
ステップ2 ICS（実装適合宣言）作成

ステップ3 IXIT（テスト用の実装追加情報）作成

ステップ4 ICS（実装適合宣言）の検証

ステップ5 適合性評価

ステップ6 判定



<ステップ0>

- 技術相談、社内共有、社内教育、申請資料作成のための社内文書類の洗い出し、プリチェック等

<ステップ1～3>

- ICSやIXIT等のプロフォーマの作成
  Annex A及びBに従ったプロパフォーマの作成、方向性や記載内容の確認・検討、その他、文書化

<ステップ4～6>

- ICSやIXIT等のプロパフォーマを基にした、適合性評価と判定
  テスト条件やテスト手順の検討、テストの実行と結果判定

サービス概要（EN 303 645）モジュールAの場合

事前準備からレポート発行までの**フルサポート**
ステップ単位でのサポートも可能

ステップ0

・サイバーセキュリティ要件の解説
(ETSI EN 303 645 およびETSI TS 103 701)
・技術相談
・提出書類の洗い出し
・セミナー実施
・ご要望に応じたサポート業務

技術相談やセミナー

ステップ1～3

・ETSI EN 303 645 及びETSI TS 103 701の技術文書作成サポート
・Annex A及びBに従ったPro forma作成アドバイス、記載内容の確認・検討
などその他、文書化サポート　など

要求文書の作成サポート

ステップ4～6

・ICSの検証サポート
・各種Pro formaを基にした、テスト計画立案サポート
・テスト条件や手順の検討サポート
・テストの実行とテスト結果の判定
・レポート発行　など

テストの計画、実施、評価、判定

⚠ 期間と費用は目安です。評価対象、事前準備、要件の理解度、ステップ１からステップ３の完成度、コメントに対する是正処置などにより、大きく変わります。

■サイバーセキュリティ関連のサービスについて、お気軽にお問い合わせください

一般財団法人　日本品質保証機構　（JQA）

◆ 安全電磁センター 営業課
TEL：042-679-0246 / FAX： 042-679-0170
E-mail：jtp-safety-cstm@jqa.jp

◆ 北関西試験センター 営業課
TEL：072-729-2244 / FAX：072-728-6848
E-mail：kita-customers@jqa.jp

ご清聴
ありがとうございました