製造現場に産業用IoTを導入する際のセキュリティ対策の手始め

産業用IoTを導入する企業が工場でセキュアにIoTを活用するために

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
河野 一之

アジェンダ

1. 産業用IoTの導入メリットならびにセキュリティリスク

2. 徐々に進むIoT活用とセキュリティ対策ガイドの要望

3. 実践すべき産業用IoT導入時のセキュリティ対策の手始め
   ～ セキュリティ対策ガイドの目的や活用イメージなどを解説 ～

4. ICSセキュリティを支援する各種無料サービスの紹介

アジェンダ

1. 産業用IoTの導入メリットならびにセキュリティリスク

2. 徐々に進むIoT活用とセキュリティ対策ガイドの要望

3. 実践すべき産業用IoT導入時のセキュリティ対策の手始め
   ～ セキュリティ対策ガイドの目的や活用イメージなどを解説 ～

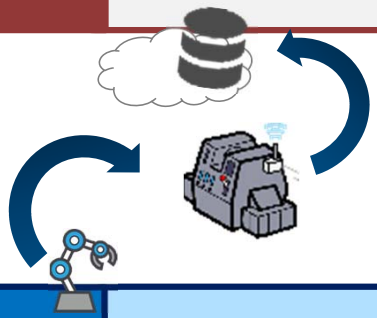
4. ICSセキュリティを支援する各種無料サービスの紹介

1-1.製造現場の課題と期待される産業用IoT導入メリット

■ 製造現場において次のような課題を抱え、産業用IoTの導入で改善が期待されている

課題

- 新規人材採用が困難な上、熟練者の退職で技術継承が困難
- 設備の老朽化等による機器故障や生産設備の停止
- 競争力維持に求められるさらなる生産性向上　など



産業用IoTの導入

メリット

- ✓ 製造自動化を支援し人員不足の解消や品質の安定化に貢献
- ✓ 機器等の稼働状況の見える化や故障予知で交換時期の把握
- ✓ クラウドなどでの生産データ分析による生産性改善

1-2.セキュリティ対策が不十分な産業用IoTのリスク

■ 一方、製造現場の産業用IoTのセキュリティ対策が不十分なままだと
潜在的にさまざまなセキュリティ被害が発生するリスクがある
例えば・・・

- ✓ 工場の機械が停止・遠隔操作される
- ✓ 検査データが改ざんされ、知らぬ間に不良品が出荷される
- ✓ 稼働データが改ざんされ、機器の異常発見が遅れる
- ✓ サイバー攻撃により自社の工場が停止することで、取引先に影響を与える 等

**このような事態にならないために、産業用IoTの活用においても
セキュリティ対策が求められている**

アジェンダ

1. 産業用IoTの導入メリットならびにセキュリティリスク

2. 徐々に進むIoT活用とセキュリティ対策ガイドの要望

3. 実践すべき産業用IoT導入時のセキュリティ対策の手始め
～ セキュリティ対策ガイドの目的や活用イメージなどを解説 ～

4. ICSセキュリティを支援する各種無料サービスの紹介

2-1.徐々に進むIoT活用とセキュリティ対策ガイドの要望

■ 制御システムユーザや制御機器ベンダ等からの相談や意見交換などで分かったこと

制御システムユーザや機器ベンダの声

- 産業用IoTで制御機器の稼働データを取りたい
- 産業用IoTを使って制御機器の遠隔監視や操作をしたい
- 制御機器も複数のNWに接続が可能なものがユーザに求められている　等

産業用IoT等で**制御システムの「つながる」化**が、徐々にではあるが進みつつある

制御システムユーザの声

一方で・・・
産業用IoTの活用時に**どんなセキュリティ対策をしてよいか分からない**
また**セキュリティに不慣れでも参考にできるものが欲しい**　等

2-2.産業用IoT導入のためのセキュリティ対策ガイドを作成

- 制御システムユーザ等の要望から本セキュリティ対策ガイドを作成。
- 経営者、現場管理者・技術担当者、受注ベンダ等との間で共通認識を得るために、セキュリティ知識に不慣れな製造業者にとって、分かりやすく、使いやすいセキュリティ対策ガイドを目指した。
- 2018年8月9日 Web公表
  全24ページ
  https://www.jpcert.or.jp/ics/information06.html

アジェンダ

1. 産業用IoTの導入メリットならびにセキュリティリスク

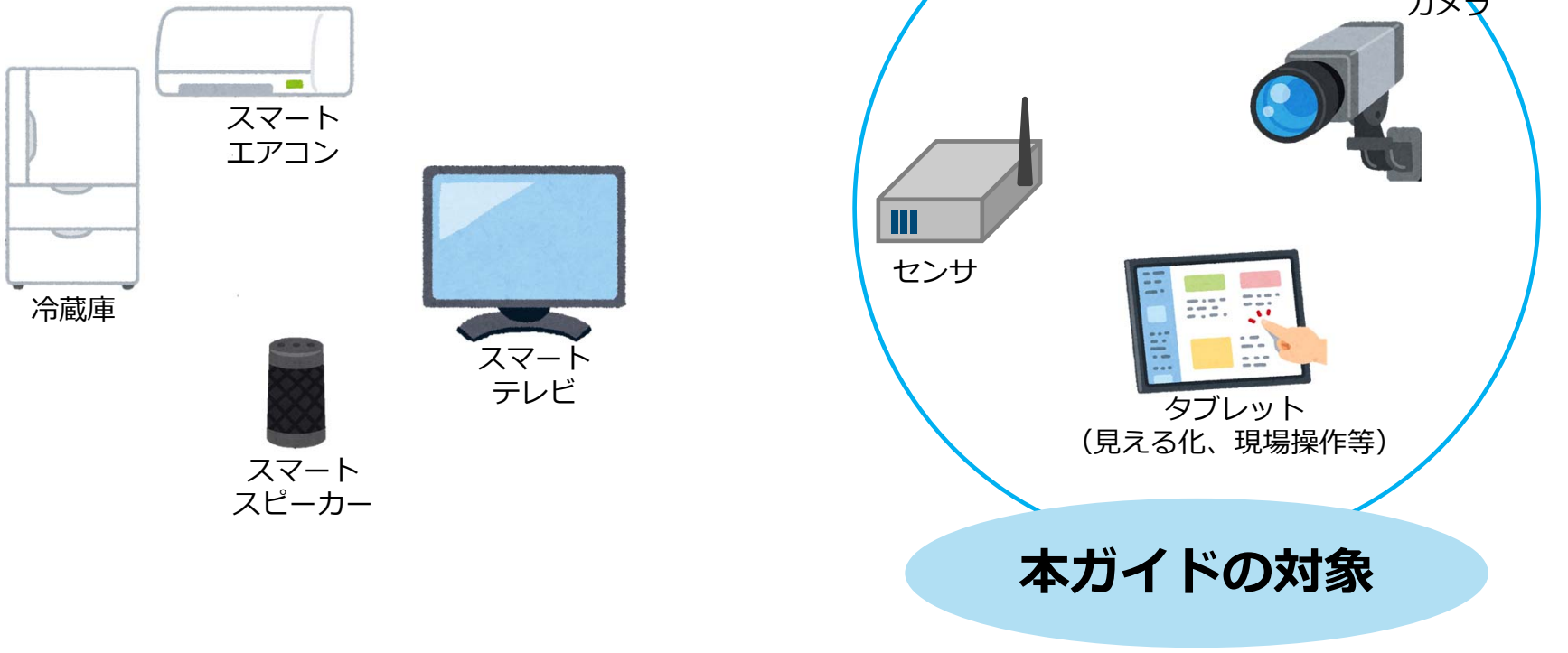
2. 徐々に進むIoT活用とセキュリティ対策ガイドの要望

3. 実践すべき産業用IoT導入時のセキュリティ対策の手始め
～ セキュリティ対策ガイドの目的や活用イメージなどを解説 ～

4. ICSセキュリティを支援する各種無料サービスの紹介

3-1.本ガイドで取り上げる産業用IoT（例）

■ 本セキュリティ対策ガイドで取り上げる産業用IoTは主に次のような製品を指す



3-2.ガイドの目的

■ 『工場における産業用IoT導入のためのセキュリティ ファーストステップ』は記載のセキュリティ対策を行うことで次の点の実現を目的としている。

目的

産業用IoT導入による制御システムへのセキュリティリスクを低減

- セキュアな環境におけるIoTの活用で、**生産停止などの自社の事業継続リスクを低減**
- 生産停止等による取引先等への影響といった**サプライチェーンのセキュリティリスクを低減**

これらのセキュリティリスクを低減して、結果的に生産改善などの本来業務に注力できる

3-3.ガイドの特徴

■本ガイドは、セキュリティに不慣れなICSの担当者でもセキュリティリスクを理解し、**現場で活用しやすいように**次の特徴がある。

特徴① **基本的なセキュリティ対策に絞り、これから取り組む方のためのセキュリティ対策の入門的なガイドとした**

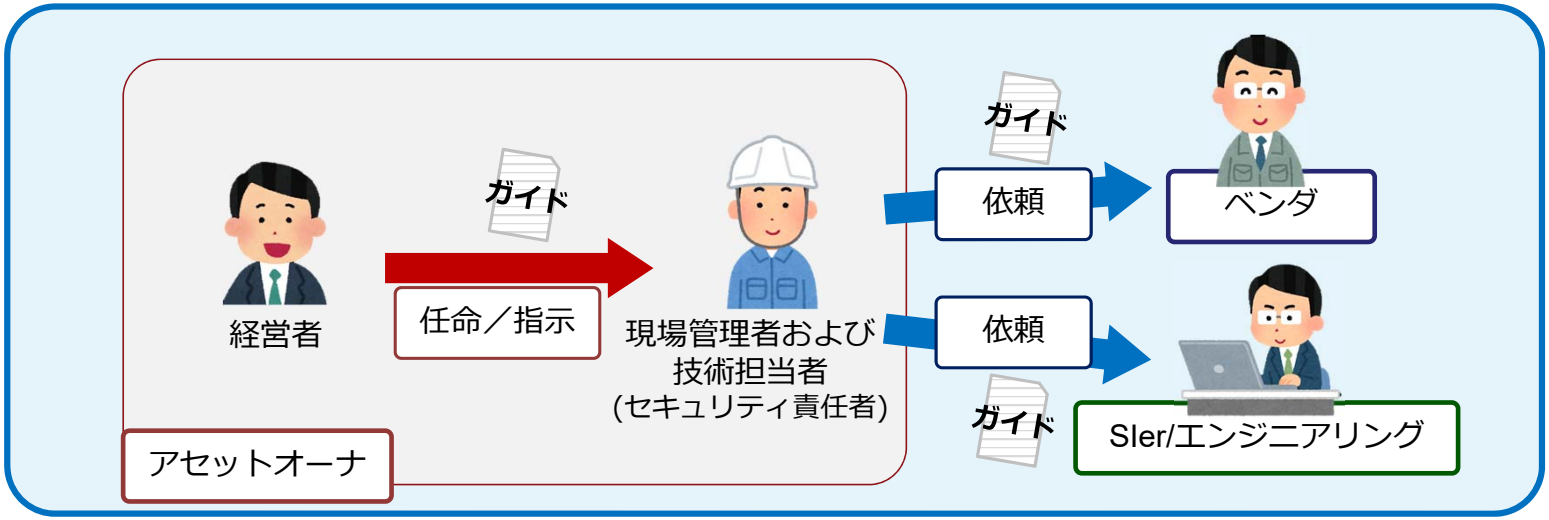
特徴② **実質20ページ程度とし、セキュリティに不慣れな方でもわかりやすい表現に努めて読みやすくした**

特徴③ **視覚的に対策箇所を把握し、対象の対策ページを迅速に参照できるようなモデル図を採用した**

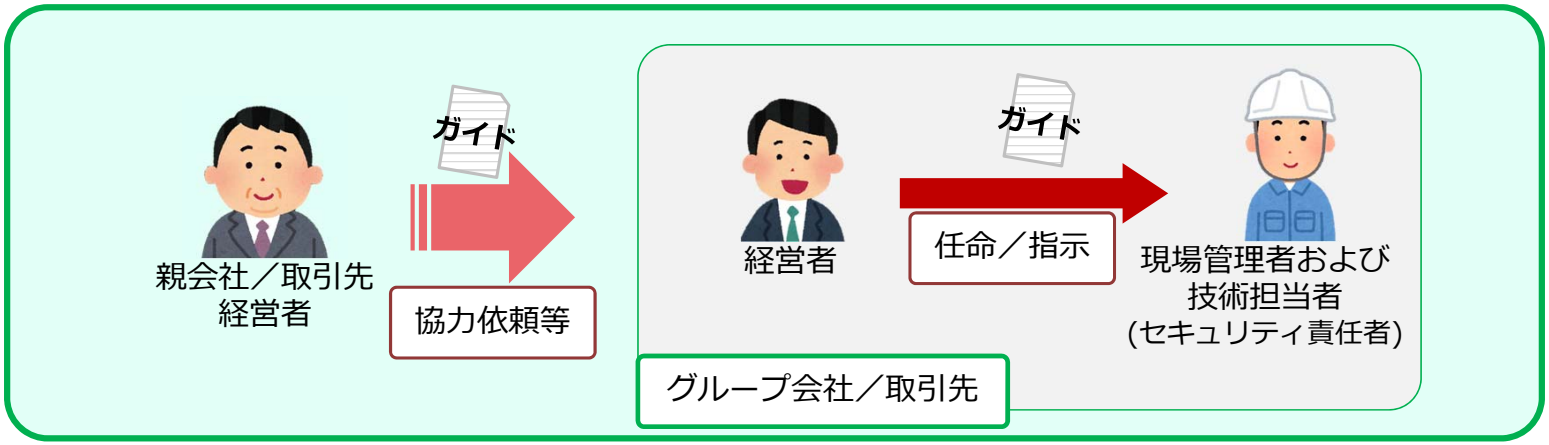
製造現場のIoT活用における**「セキュリティ対策の手始め」**として、本ガイドを活用いただきたい

3-4.本ガイドの活用シーンとプレーヤー

事業者内での活用



サプライチェーンでの活用



3-5.ガイドの構成（各読者層向けに３つのパートに大別）

■ 各読者ごとに大きく分けて次の３つでパートに分かれている

［パート１］経営者向け

◆ 本ガイド「経営者の皆さまへ」（P3）
- 国内外で実際に発生した被害とその対応コスト等を交え、産業用IoT 導入時のセキュリティ対策の必要性を解説

［パート２］経営者や現場管理者、技術担当者向け

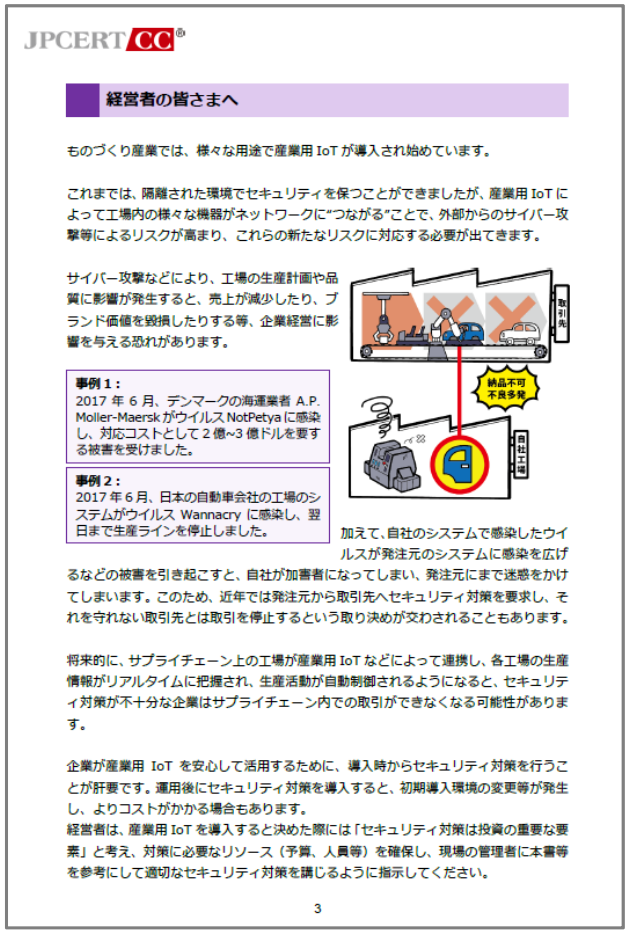
◆ 本ガイド「本書における産業用IoTのセキュリティ対策の考え方」（P4）
- 「クラウド層」、「外部ネットワーク層」、「工場内IoTネットワーク層」とIoT ネットワークを構成する各層ごとにセキュリティ対策を行うことで防御の効果を高めることができる多層防御の必要性を解説

［パート３］現場管理者や技術担当者、エンジニアリング会社・SIer向け

◆ 本ガイド「産業用IoT の導入プロセス：外部事業者との役割・業務分担」（P5 ～ 8）
「産業用IoT の構成要素：対策ナビゲーションマップ」（P9 ～ 19）
- 仕様策定から運用までのプロセスで実施すべきセキュリティ対策を解説
- 産業用IoTシステムの5つの構成要素ごとに実施すべきセキュリティ対策を解説

3-6.［パート１］経営者向け

◆ **「経営者の皆さまへ」**（P3）



JPCERT CC®

経営者の皆さまへ

ものづくり産業では、様々な用途で産業用 IoT が導入され始めています。

これまでは、隔離された環境でセキュリティを保つことができましたが、産業用 IoT によって工場内の様々な機器がネットワークに“つながる”ことで、外部からのサイバー攻撃等によるリスクが高まり、これらの新たなリスクに対応する必要が出てきます。

サイバー攻撃などにより、工場の生産計画や品質に影響が発生すると、売上が減少したり、ブランド価値を毀損したりする等、企業経営に影響を与える恐れがあります。

事例 1：
2017 年 6 月、デンマークの海運業者 A.P. Moller-Maersk がウイルス NotPetya に感染し、対応コストとして 2 億~3 億ドルを要する被害を受けました。

事例 2：
2017 年 6 月、日本の自動車会社の工場のシステムがウイルス Wannacry に感染し、翌日まで生産ラインを停止しました。

加えて、自社のシステムで感染したウイルスが発注元のシステムに感染を広げるなどの被害を引き起こすと、自社が加害者になってしまい、発注元にまで迷惑をかけてしまいます。このため、近年では発注元から取引先へセキュリティ対策を要求し、それを守れない取引先とは取引を停止するという取り決めが交わされることもあります。

将来的に、サプライチェーン上の工場が産業用 IoT などによって連携し、各工場の生産情報がリアルタイムに把握され、生産活動が自動制御されるようになると、セキュリティ対策が不十分な企業はサプライチェーン内での取引ができなくなる可能性があります。

企業が産業用 IoT を安心して活用するために、導入時からセキュリティ対策を行うことが肝要です。運用後にセキュリティ対策を導入すると、初期導入環境の変更等が発生し、よりコストがかかる場合もあります。
経営者は、産業用 IoT を導入すると決めた際には「セキュリティ対策は投資の重要な要素」と考え、対策に必要なリソース（予算、人員等）を確保し、現場の管理者に本書等を参考にして適切なセキュリティ対策を講じるように指示してください。

3

- 工場内の様々な機器が「つながる」と利便性の向上とともに**セキュリティリスクも増大**
- 被害にあうと生産計画や品質に影響し、売上減少などで**事業の経営に影響を与える**
- 事実、海運業や製造業でネットワーク経由で被害が発生
- 将来的には取引先等サプライチェーンへの影響が懸念される

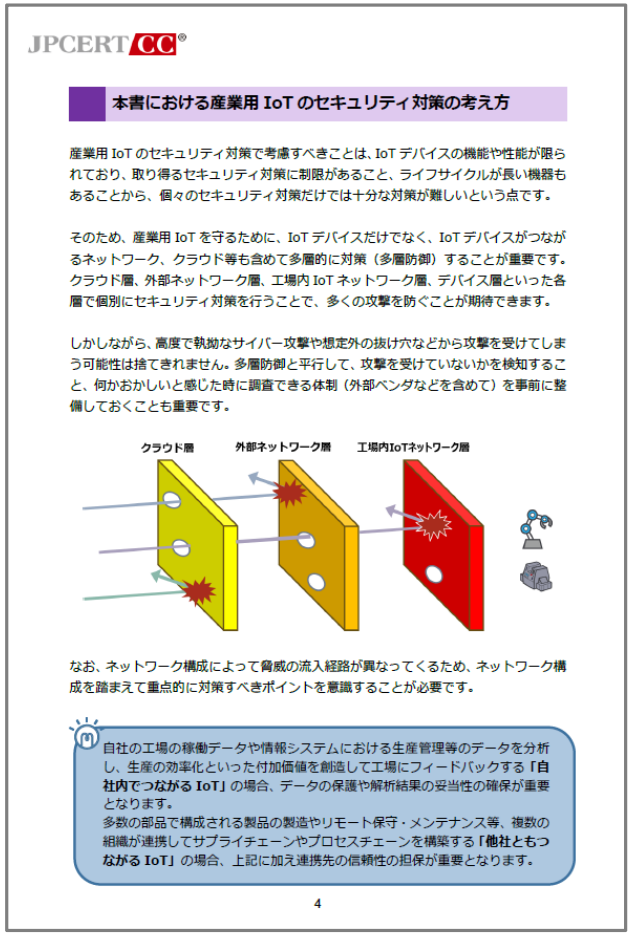
セキュリティ対策は IoT投資の一環

経営者が行うべき役割を理解いただく

- ✓ リソース（予算、人員）確保
- ✓ 本ガイドを参考にセキュリティ対策実施の指示

3-6.［パート2］経営者や現場管理者、技術担当者向け

◆「本書における産業用IoTのセキュリティ対策の考え方」（P4）



JPCERT CC®

本書における産業用 IoT のセキュリティ対策の考え方

産業用 IoT のセキュリティ対策で考慮すべきことは、IoT デバイスの機能や性能が限られており、取り得るセキュリティ対策に制限があること、ライフサイクルが長い機器もあることから、個々のセキュリティ対策だけでは十分な対策が難しいという点です。

そのため、産業用 IoT を守るために、IoT デバイスだけでなく、IoT デバイスがつながるネットワーク、クラウド等も含めて多層的に対策（多層防御）することが重要です。クラウド層、外部ネットワーク層、工場内 IoT ネットワーク層、デバイス層といった各層で個別にセキュリティ対策を行うことで、多くの攻撃を防ぐことが期待できます。

しかしながら、高度で執拗なサイバー攻撃や想定外の抜け穴などから攻撃を受けてしまう可能性は捨てきれません。多層防御と平行して、攻撃を受けていないかを検知すること、何かおかしいと感じた時に調査できる体制（外部ベンダなどを含めて）を事前に整備しておくことも重要です。

なお、ネットワーク構成によって脅威の流入経路が異なってくるため、ネットワーク構成を踏まえて重点的に対策すべきポイントを意識することが必要です。

自社の工場の稼働データや情報システムにおける生産管理等のデータを分析し、生産の効率化といった付加価値を創造して工場にフィードバックする「**自社内でつながる IoT**」の場合、データの保護や解析結果の妥当性の確保が重要となります。
多数の部品で構成される製品の製造やリモート保守・メンテナンス等、複数の組織が連携してサプライチェーンやプロセスチェーンを構築する「**他社ともつながる IoT**」の場合、上記に加え連携先の信頼性の担保が重要となります。

4

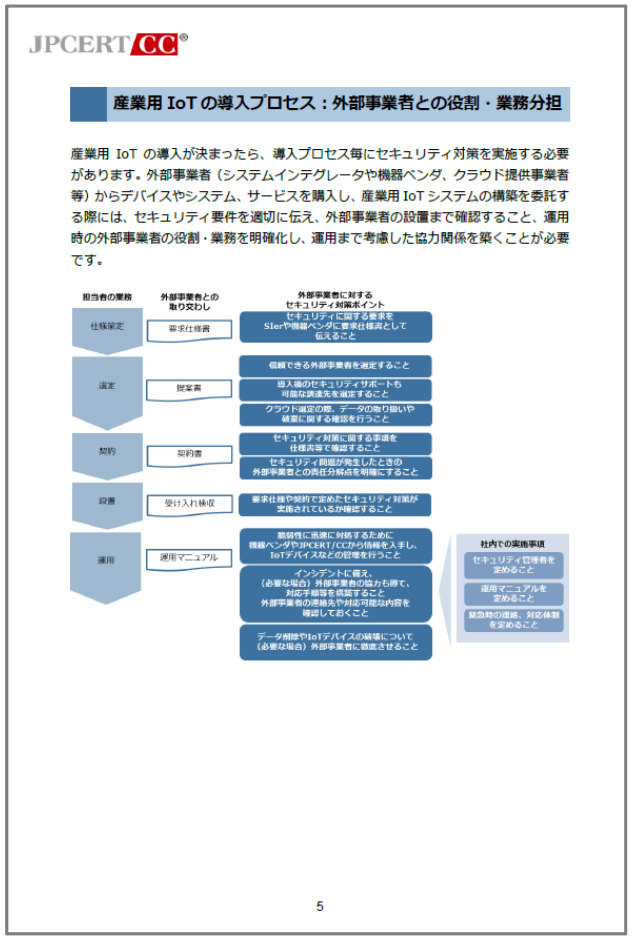
- IoTデバイスは機能制約等のため、それ自体では十分にセキュリティ対策ができない
- クラウド、外部NW、工場内IoTNW、デバイスなど個別に対策を行うことが重要

さまざまな対策を重層的に行う
多層防御が効果的

経営者や現場管理者等に多層防御による
セキュリティ対策の重要性を理解いただく

3-6.［パート3］現場管理者や技術担当者、SIer等向け ①

◆「産業用IoT の導入プロセス：外部事業者との役割・業務分担」（P5～8）


JPCERT CC®

産業用 IoT の導入プロセス：外部事業者との役割・業務分担

産業用 IoT の導入が決まったら、導入プロセス毎にセキュリティ対策を実施する必要があります。外部事業者（システムインテグレータや機器ベンダ、クラウド提供事業者等）からデバイスやシステム、サービスを購入し、産業用 IoT システムの構築を委託する際には、セキュリティ要件を適切に伝え、外部事業者の設置まで確認すること、運用時の外部事業者の役割・業務を明確化し、運用まで考慮した協力関係を築くことが必要です。

担当者の業務	外部事業者との取り交わし	外部事業者に対するセキュリティ対策ポイント
仕様策定	要求仕様書	セキュリティに関する事項をSIerや機器ベンダに要求仕様書として伝えること
選定	提案書	信頼できる外部事業者を選定すること 導入後のセキュリティサポートも可能な調達先を選定すること クラウド選定の際、データの取り扱いや破棄に関する確認を行うこと
契約	契約書	セキュリティ対策に関する事項を仕様書等で確認すること セキュリティ問題が発生したときの外部事業者との責任分解点を明確にすること
設置	受け入れ検収	要求仕様や契約で定めたセキュリティ対策が実施されているか確認すること
運用	運用マニュアル	脆弱性に迅速に対処するために機器ベンダやJPCERT/CCから情報を入手し、IoTデバイスなどの管理を行うこと インシデントに備え、（必要な場合）外部事業者の協力も得て、対応手順等を策定すること 外部事業者の連絡先や対応可能な内容を確認しておくこと データ削除やIoTデバイスの破壊について（必要な場合）外部事業者に確認させること

社内での実施事項
- セキュリティ管理者を定めること
- 運用マニュアルを定めること
- 緊急時の連絡、対応体制を定めること

5

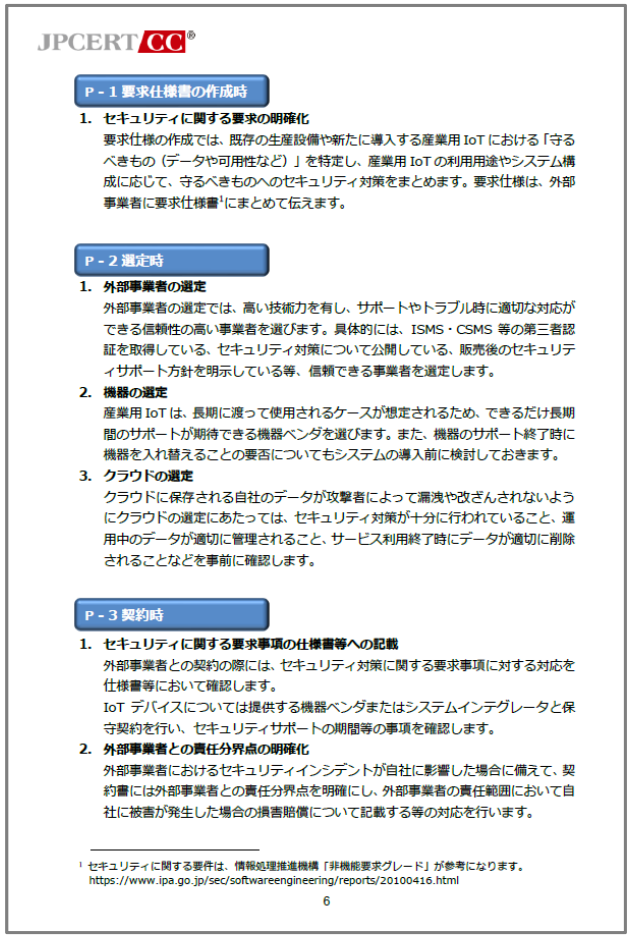
- 導入プロセスを意識した**マネジメント視点のセキュリティ対策**が重要
- 5つの導入プロセスごとの対策で**包括的にセキュリティを確保**
- ベンダ等外部事業者との役割や責任を明確化し、運用まで考慮した協力関係を築く

各プロセスのセキュリティ対策は社内外の関係者とのセキュリティ対策の確認や周知となる重要な手続き

現場管理者やSIer等関係者間で実施するセキュリティ対策のマネジメント体制を構築

3-6.［パート３］現場管理者や技術担当者、SIer等向け ②

◆「産業用IoT の導入プロセス：外部事業者との役割・業務分担」（P5～8）



JPCERT CC®

P - 1 要求仕様書の作成時

1. **セキュリティに関する要求の明確化**
   要求仕様の作成では、既存の生産設備や新たに導入する産業用 IoT における「守るべきもの（データや可用性など）」を特定し、産業用 IoT の利用用途やシステム構成に応じて、守るべきものへのセキュリティ対策をまとめます。要求仕様は、外部事業者に要求仕様書[1]にまとめて伝えます。

P - 2 選定時

1. **外部事業者の選定**
   外部事業者の選定では、高い技術力を有し、サポートやトラブル時に適切な対応ができる信頼性の高い事業者を選びます。具体的には、ISMS・CSMS 等の第三者認証を取得している、セキュリティ対策について公開している、販売後のセキュリティサポート方針を明示している等、信頼できる事業者を選定します。
2. **機器の選定**
   産業用 IoT は、長期に渡って使用されるケースが想定されるため、できるだけ長期間のサポートが期待できる機器ベンダを選びます。また、機器のサポート終了時に機器を入れ替えることの要否についてもシステムの導入前に検討しておきます。
3. **クラウドの選定**
   クラウドに保存される自社のデータが攻撃者によって漏洩や改ざんされないようにクラウドの選定にあたっては、セキュリティ対策が十分に行われていること、運用中のデータが適切に管理されること、サービス利用終了時にデータが適切に削除されることなどを事前に確認します。

P - 3 契約時

1. **セキュリティに関する要求事項の仕様書等への記載**
   外部事業者との契約の際には、セキュリティ対策に関する要求事項に対する対応を仕様書等において確認します。
   IoT デバイスについては提供する機器ベンダまたはシステムインテグレータと保守契約を行い、セキュリティサポートの期間等の事項を確認します。
2. **外部事業者との責任分界点の明確化**
   外部事業者におけるセキュリティインシデントが自社に影響した場合に備えて、契約書には外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自社に被害が発生した場合の損害賠償について記載する等の対応を行います。

[1] セキュリティに関する要件は、情報処理推進機構「非機能要求グレード」が参考になります。
https://www.ipa.go.jp/sec/softwareengineering/reports/20100416.html

6

- 5つのプロセスごとに次のような点を実施

① **仕様策定**: SIer等への要求仕様にセキュリティ要件を盛り込む

② **選定**: 第三者認証取得の外部事業者のサービスや長期的なセキュリティサポートが期待できるベンダの機器を選定

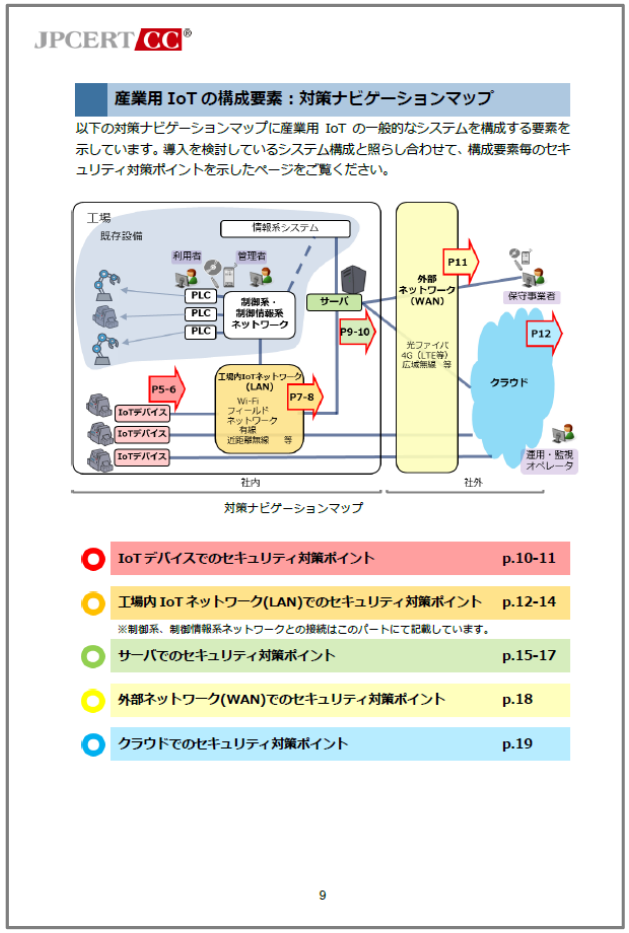
③ **契約**: ①を元にセキュリティ対策事項の確認や責任分界点の明確化をして外部事業者と契約

④ **設置**: ①,③を元に受入検査を実施

⑤ **運用**: 脆弱性の情報収集や適用手順の作成、セキュリティ被害発生時の対応手順や体制構築、産業用IoT製品廃棄時の対応手順等を作成

3-6.［パート3］現場管理者や技術担当者、SIer等向け ③

◆「産業用IoT の構成要素：対策ナビゲーションマップ」（P9～19）

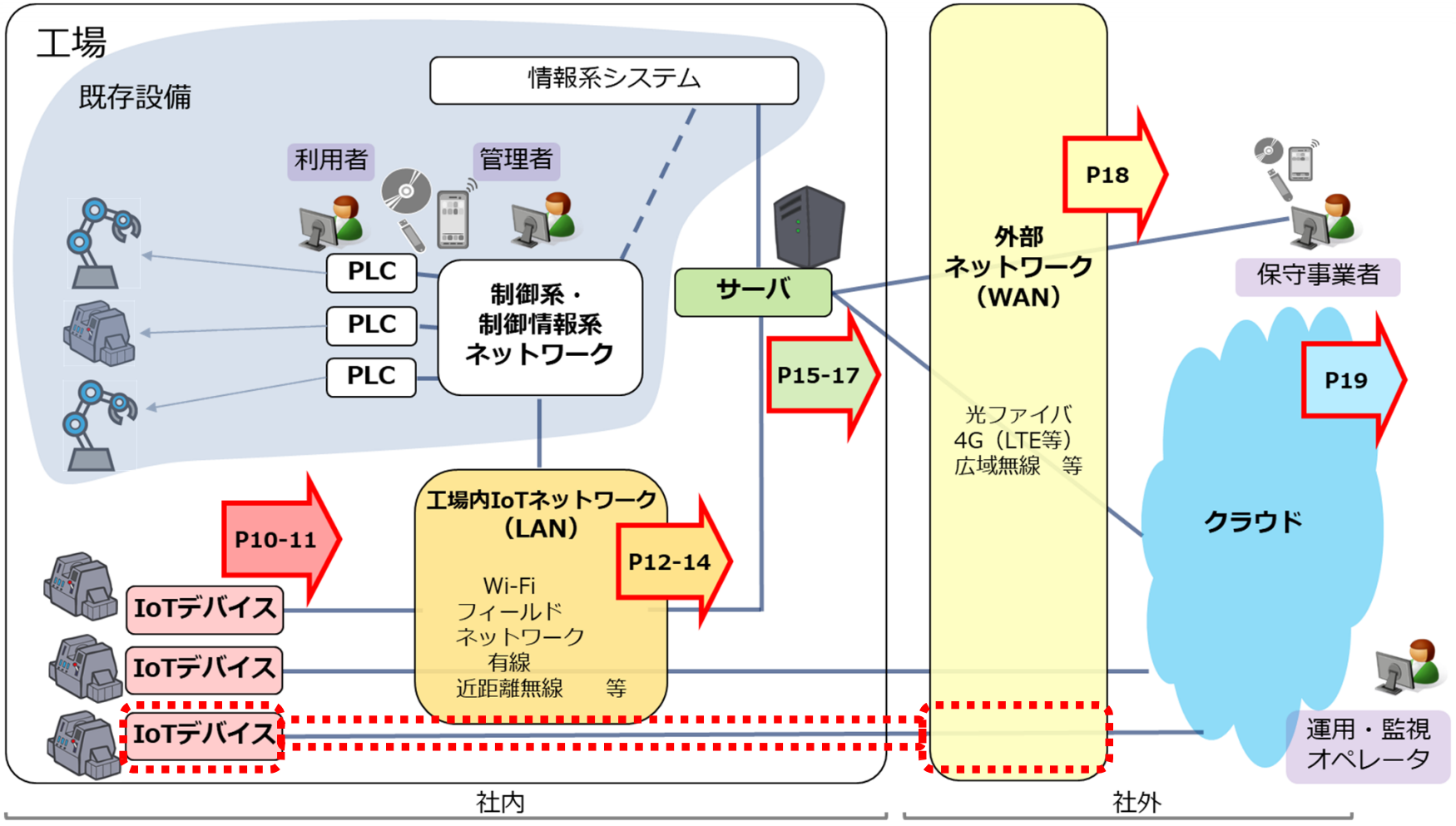


- 産業用IoTネットワークモデルと5つの構成要素から導入箇所等を視覚的に把握
  ①IoTデバイス、②工場内IoTNW（LAN）、
  ③サーバ、④外部NW（WAN）、⑤クラウド
- 各要素のページ番号を参照して、対象箇所の技術的な対策ページへ移動し、具体的なセキュリティ対策とその必要性を把握してセキュリティ対策を実施

全体構成や各対策の理解を促しセキュリティ対策の参考にしていただく

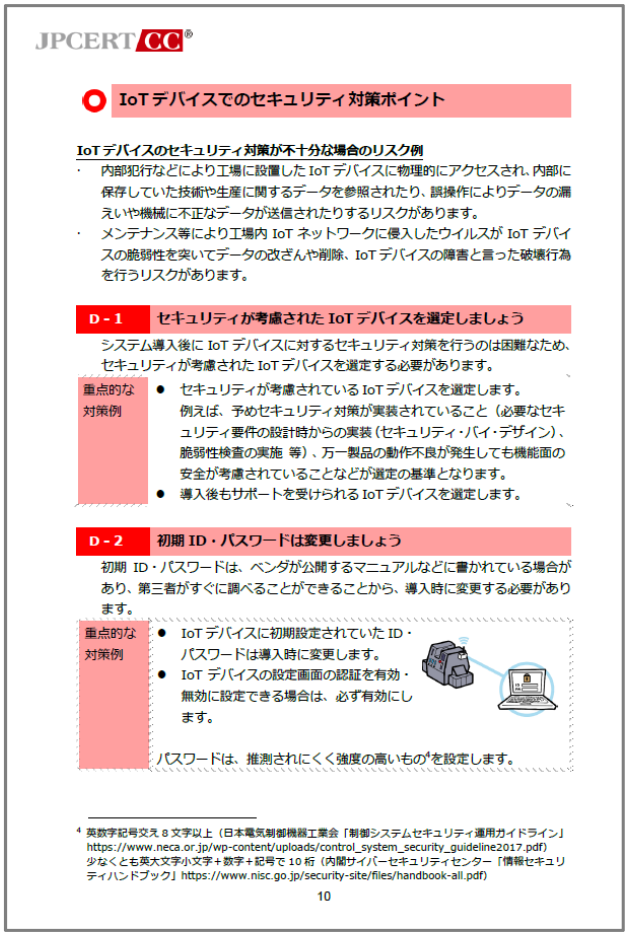
部分導入の場合を含めて産業用IoT導入において、まず何から実施するかの参考として活用。

産業用IoT の (5つの) 構成要素：対策ナビゲーションマップ



3-6.［パート3］現場管理者や技術担当者、SIer等向け ④

◆「産業用IoT の構成要素：対策ナビゲーションマップ」（P9～19）



JPCERT CC®

IoT デバイスでのセキュリティ対策ポイント

IoT デバイスのセキュリティ対策が不十分な場合のリスク例

- 内部犯行などにより工場に設置した IoT デバイスに物理的にアクセスされ、内部に保存していた技術や生産に関するデータを参照されたり、誤操作によりデータの漏えいや機械に不正なデータが送信されたりするリスクがあります。
- メンテナンス等により工場内 IoT ネットワークに侵入したウイルスが IoT デバイスの脆弱性を突いてデータの改ざんや削除、IoT デバイスの障害と言った破壊行為を行うリスクがあります。

D-1 セキュリティが考慮された IoT デバイスを選定しましょう

システム導入後に IoT デバイスに対するセキュリティ対策を行うのは困難なため、セキュリティが考慮された IoT デバイスを選定する必要があります。

重点的な対策例

- セキュリティが考慮されている IoT デバイスを選定します。
  例えば、予めセキュリティ対策が実装されていること（必要なセキュリティ要件の設計時からの実装（セキュリティ・バイ・デザイン）、脆弱性検査の実施 等）、万一製品の動作不良が発生しても機能面の安全が考慮されていることなどが選定の基準となります。
- 導入後もサポートを受けられる IoT デバイスを選定します。

D-2 初期 ID・パスワードは変更しましょう

初期 ID・パスワードは、ベンダが公開するマニュアルなどに書かれている場合があり、第三者がすぐに調べることができることから、導入時に変更する必要があります。

重点的な対策例

- IoT デバイスに初期設定されていた ID・パスワードは導入時に変更します。
- IoT デバイスの設定画面の認証を有効・無効に設定できる場合は、必ず有効にします。

パスワードは、推測されにくく強度の高いもの[4]を設定します。

[4] 英数字記号交え 8 文字以上（日本電気制御機器工業会「制御システムセキュリティ適用ガイドライン」https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline2017.pdf）
少なくとも英大文字小文字＋数字＋記号で 10 桁（内閣サイバーセキュリティセンター「情報セキュリティハンドブック」https://www.nisc.go.jp/security-site/files/handbook-all.pdf）

10

<u>各対策ページは次の3つで構成</u>
①セキュリティ対策が不十分な場合のリスク例
②個々のセキュリティ対策の重要性の解説
③重点的なセキュリティ対策例の紹介

■ 例: IoTデバイスでの対策ポイント

- IoTデバイスのセキュリティ対策が不十分な場合、**設計時の脆弱性の作り込み**、不正アクセスによる**内部データの漏えい**や**データの改ざん・削除**、**物理的な盗難**等のセキュリティリスクが想定される
- 次のようなセキュリティ対策が必要になる
  - ✓ セキュリティ実装のIoTデバイスの選定
  - ✓ 盗難防止のワイヤーロック
  - ✓ 不正アクセス低減のための初期ID／PW変更
  - ✓ ソフトウエアの最新アップデート など

※本ガイド掲載のセキュリティ対策で一定のセキュリティ確保は可能だが、十分ではない点に留意。

3-7.制御システム関係者からのお声や引用など（一部）

■ 制御システム関係者からのお声や引用していただいた記事を紹介。

セキュリティに不慣れな制御システムユーザでも使えるガイドが欲しかった。
（制御システムユーザ）

こんな制御システムユーザ向けのガイドが出て欲しいと思っていた
（制御機器設計者）

制御システムユーザに紹介させていただきたい
（セキュリティベンダ）

こういうガイドがもっとたくさん出た方がいいと思う
（制御システムコンサルタント）

■ TechFactoryサイトでの引用記事

経営者がトップダウンで動けば、日本の企業は素早く変われる

2018年8月、JPCERT コーディネーションセンターが「**工場における産業用IoT導入のためのセキュリティ ファーストステップ**」を公開しました。この資料も大変よくまとまっているので、ぜひご一読をオススメします。

その冒頭は「経営者の皆さまへ」という文言から始まっています。これを少々引用しましょう。

> 企業が産業用IoT（Internet of Things）を安心して活用するために、導入時からセキュリティ対策を行うことが肝要です。運用後にセキュリティ対策を導入すると、初期導入環境の変更などが発生し、よりコストがかかる場合もあります。
>
> 経営者は、産業用IoTを導入すると決めた際には「セキュリティ対策は投資の重要な要素」と考え、対策に必要なリソース（予算、人員など）を確保し、現場の管理者に本書などを参考にして適切なセキュリティ対策を講じるように指示してください。

重要なポイントは、「**導入時からセキュリティ対策を行うことが肝要**」という点です。開発から運用の全てのポイントでセキュリティを入れ込む「DevSecOps」や「シフトレフト」という考え方は、経営層の一声があればとてもたやすく導入できます。

引用元：宮田健の「セキュリティの道も一歩から」（32）：
「ウチには関係ないよ」と考えている中小企業経営層の皆さまへ
（TechFactory）
http://techfactory.itmedia.co.jp/tf/articles/1811/08/news002.html

3-8.セキュリティ対策ガイド（日本語版）の入手方法

■ 紹介したセキュリティ対策ガイドは次のURLからダウンロードできる。

【ダウンロード手順】

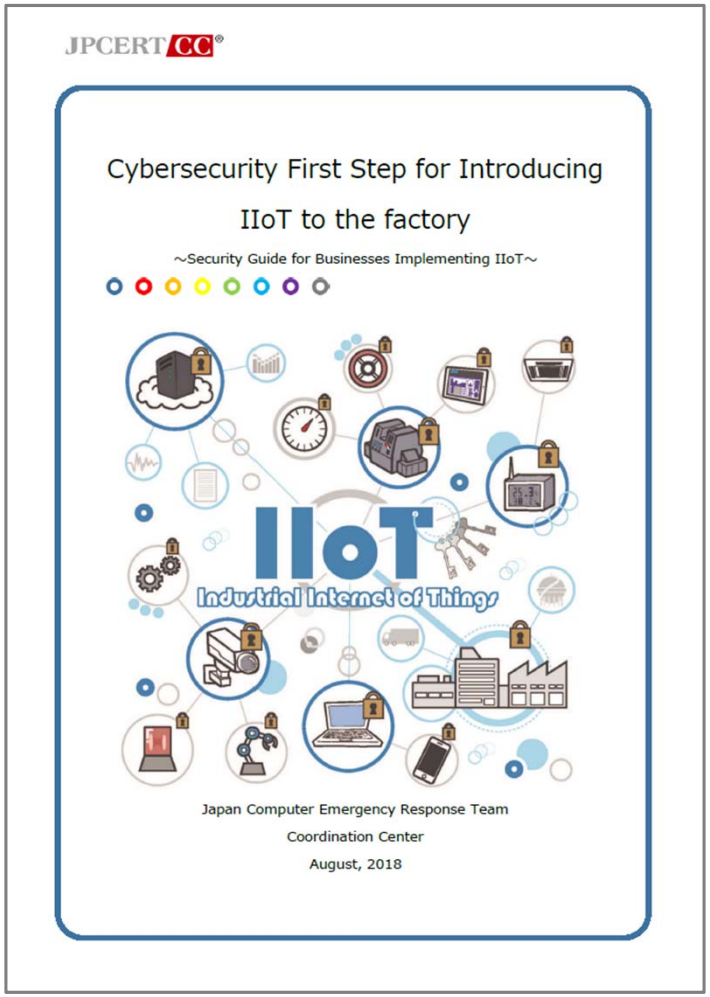
下記URLにアクセス し、Webページ内の以下のPDF欄**（赤枠部分）**をクリック。

工場における産業用IoT導入のためのセキュリティ ファーストステップ
https://www.jpcert.or.jp/ics/information06.html

Webページ内にこの表を見つけたら、ここをクリック

公開日	タイトル	PDF
2018-08-09	工場における産業用IoT導入のためのセキュリティ ファーストステップ ～産業用IoTを導入する企業のためのセキュリティガイド～	2.09MB デジタル 署名付

3-9.セキュリティ対策ガイド（英語版）のご案内



■ 概要と活用メリット

➢ **概要：**

・構成等、内容は日本語版と同じ

➢ **活用メリット：**

・国内・海外拠点で同一内容のセキュリティ対策を実施可能

・海外拠点の担当者のセキュリティスキルがあまり高くなくても活用可能

■ 英語版公表時期

➢ 2019年春の予定

アジェンダ

1. 産業用IoTの導入メリットならびにセキュリティリスク

2. 徐々に進むIoT活用とセキュリティ対策ガイドの要望

3. 実践すべき産業用IoT導入時のセキュリティ対策の手始め
～ セキュリティ対策ガイドの目的や活用イメージなどを解説 ～

4. ICSセキュリティを支援する各種無料サービスの紹介

4-1.変化の激しいサイバー脅威のトレンド把握

おすすめ　効率的な制御システムセキュリティ情報の収集

■ 変化の激しいサイバー脅威のトレンドや脆弱性情報などを把握

制御システムセキュリティ情報提供用メーリングリスト

- **国内外で確認された制御システムに深刻な影響の可能性がある情報の適宜配信**
- **国内外の制御セキュリティ、脅威情報の月刊配信**

制御システムセキュリティ情報ポータルサイトConPaS

- **制御機器、制御製品の脆弱性情報の適宜配信**
- **制御システムセキュリティガイドやツール提供**

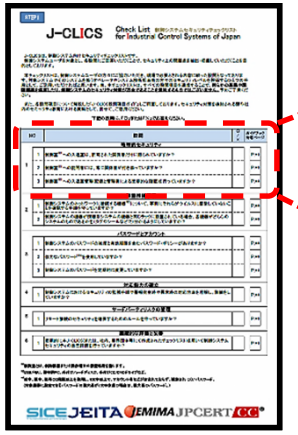
JPCERT/CC はこれらの情報を無料提供しています。ぜひお申込みください。

4-2.簡易に行える制御システムのセキュリティ評価

おすすめ　制御システムのセキュリティ評価を簡易に実施できる

制御システムセキュリティ自己評価簡易ツール（J-CLICS）

- 制御システム関係者全員とシステム管理者向けの2つのSTEPで構成
- 各STEPはガイドとチェックリストで構成。各々10問程度のチェック式
- 日本語版と英語版があり、国内拠点と海外拠点を同一条件で評価可能



NO	設問	○／×	ガイドブック対応ページ
	物理的セキュリティ		
1	1 制御室※1への入退室は、許可された関係者だけに限られていますか？		P.**
	2 制御室※1への訪問者には、常に関係者が付き添っていますか？		P.**
	3 制御室※1への入退室管理(記録と管理者による定期的な確認)を行っていますか？		P.**

「J-CLICS」は SICE/JEITA/JEMIMA と共同開発したICSセキュリティ評価ツールである。JPCERT/CC の Web にて本評価ツールを無料提供している。ぜひご利用ください。

制御システムセキュリティで困ったら・・・

情報収集やセキュリティ評価など、制御システムセキュリティで困ったら、
下記へお気軽にお問い合わせください。

■ **制御システムセキュリティに関する各種ご相談**

- **Email：icsr@jpcert.or.jp**
- **https://www.jpcert.or.jp/ics/**

■ **制御システムインシデントの報告や初動対応の支援依頼等**

- **Email：icsr-ir@jpcert.or.jp**
- **https://www.jpcert.or.jp/ics/ics-form.html**

JPCERT/CC 制御システムセキュリティ対策グループ

Progressing ICS Security >>

ご清聴ありがとうございました