

# 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～



一般社団法人 JPCERT コーディネーションセンター

2018年8月

## 目次

はじめに .....	2
経営者の皆さまへ.....	3
本書における産業用 IoT のセキュリティ対策の考え方.....	4
産業用 IoT の導入プロセス：外部事業者との役割・業務分担.....	5
産業用 IoT の構成要素：対策ナビゲーションマップ .....	9
IoT デバイスでのセキュリティ対策ポイント.....	10
工場内 IoT ネットワーク(LAN)でのセキュリティ対策ポイント.....	12
サーバでのセキュリティ対策ポイント .....	15
外部ネットワーク(WAN)でのセキュリティ対策ポイント.....	18
クラウドでのセキュリティ対策ポイント.....	19
おわりに.....	20
用語集 .....	21
参考文献.....	22

## はじめに

ものづくり産業ではIoT(Internet of Things : 本書では産業用を対象として、「産業用IoT」と記載します)が活用されつつあります。例えば、生産性向上のために工場の設備にセンサを取り付けて稼働状況を見える化すること、突然の機械の故障を防ぐために稼働データを分析して故障を予知すること、データの解析結果を使って機械の自動制御を行うこと等、様々な用途で産業用IoTが導入され始めています。

一方で、産業用IoTの導入により工場内の様々な機器がネットワークに“つながる”ことで、サイバー攻撃等の新たな脅威に対応する必要があります。

### <産業用IoTへのサイバー攻撃により発生しうるリスク例>

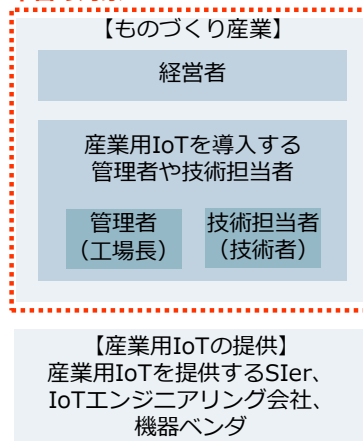
- ・ 工場の機械が停止・遠隔操作される
- ・ 検査データが改ざんされ、知らぬ間に不良品が出荷される
- ・ 稼働データが改ざんされ、機器の異常発見が遅れる
- ・ サイバー攻撃により自社の工場が停止することで、取引先に影響を与える

このように、産業用IoTがサイバー攻撃を受けることで、自社の生産活動への影響のみならず、取引先などのサプライチェーン全体にまで影響を及ぼす恐れがあります。

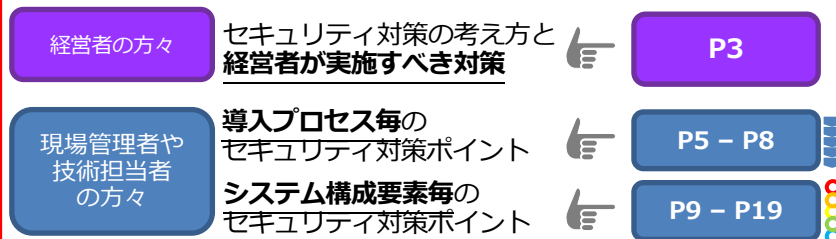
本書は、**産業用IoTの導入において一定レベルのセキュリティを確保**するために必要となる**基本的な対策のポイントを示した**ものです。主に、産業用IoTを導入する企業の**経営者**、**システム管理者**、**技術担当者**の皆さまに読んでいただくことを想定しています。

本書は産業用IoTの導入時のセキュリティ対策に焦点を絞っていますが、運用時点で必要なセキュリティ対策については、本書に加え、本書の参考文献をご参照ください。また、産業用IoTの構築等において、外部委託先に要求する発注仕様書のセキュリティ要件に利用することも可能です。

### 本書の対象



立場やニーズに応じて、必要な箇所をご覧ください。



## 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あります。

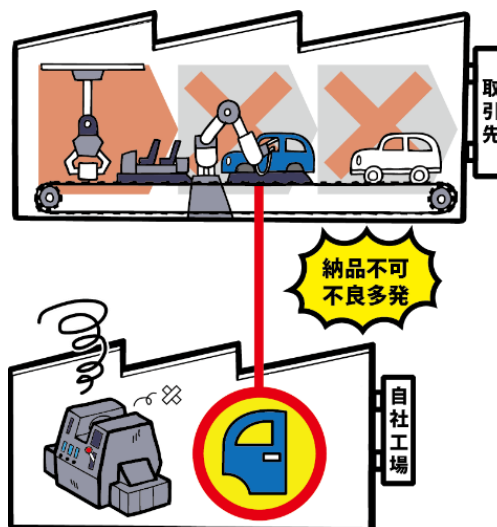
サイバー攻撃などにより、工場の生産計画や品質に影響が発生すると、売上が減少したり、ブランド価値を毀損したりする等、企業経営に影響を与える恐れがあります。

### 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。

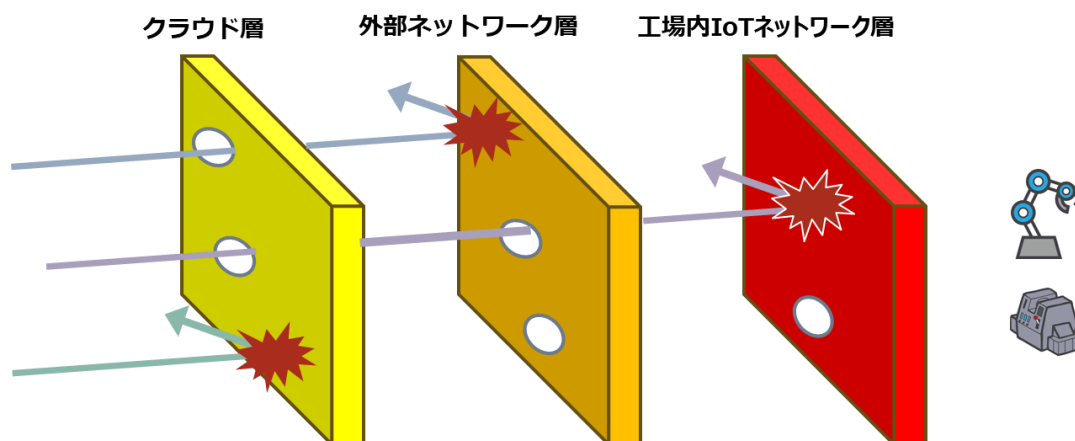
経営者は、産業用 IoT を導入すると決めた際には「セキュリティ対策は投資の重要な要素」と考え、対策に必要なリソース（予算、人員等）を確保し、現場の管理者に本書等を参考にして適切なセキュリティ対策を講じるように指示してください。

## 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。

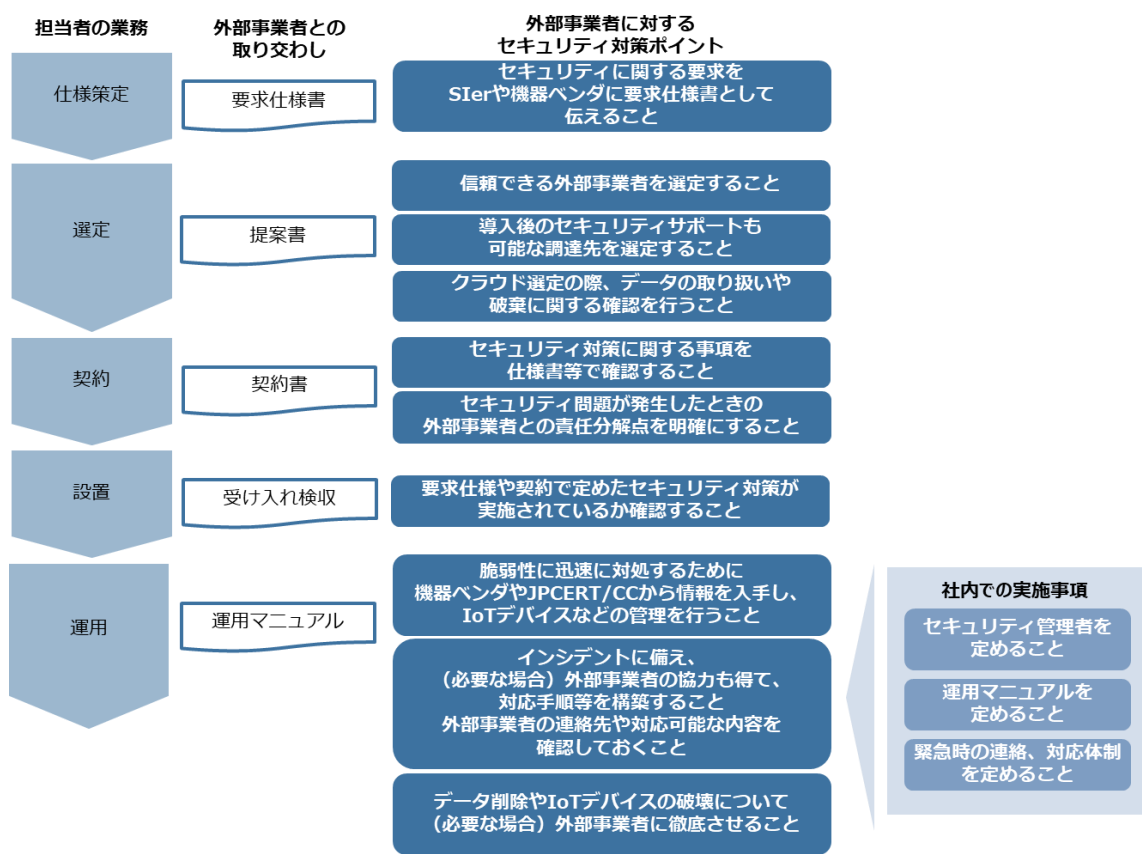


自社の工場の稼働データや情報システムにおける生産管理等のデータを分析し、生産の効率化といった付加価値を創造して工場にフィードバックする「**自社内でつながる IoT**」の場合、データの保護や解析結果の妥当性の確保が重要となります。

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。

## 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。



## 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

要求仕様書の作成では、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<sup>1</sup>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可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。

<sup>1</sup> 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>

**P - 4 設置時**

**1. セキュリティ対策の実施・確認**

システムの導入時は、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで十分に確認します。不明な点があれば、外部事業者を確認するようにします。

**P - 5 運用時**

**1. セキュリティ管理者を配置**

事業の変化や新たな脅威へ対応するために、セキュリティ対策は絶えず見直しと改善が必要です。セキュリティ対策に関する責任を持ち、対策のレベルを維持改善するために、経営層はセキュリティ管理者を定め、適切な権限とリソースを与えます。

**2. 運用マニュアルの作成**

運用時に留意すべきセキュリティ事項を、運用マニュアル<sup>2</sup>としてまとめます。

**3. 従業員に対するセキュリティ教育の実施**

工場の現場担当者は、ITに関する知識が乏しい場合があります。そのため、産業用IoTの導入に伴い、現場担当者に対して、ITの基礎知識や産業用IoTの利用方法、セキュリティに関する教育を行います。

**4. IoTデバイスの管理**

セキュリティのリスクから守るべきものを特定し、不要なデバイスの接続や発見された脆弱性に迅速に対処するために、機器ベンダや JPCERT/CC から情報を定期的に入手します。

また、IoT デバイスの型番やソフトウェアのバージョン、サポート期限等を管理する台帳<sup>3</sup>を作成し、定期的に棚卸しします。台帳に加え、運用時に実施すべき対策（IoT デバイスの不正利用や盗難、パッチの適用、ログのチェック等）、IoT デバイスの状況を見直すタイミングを定めます。



JPCERT/CC 提供の制御システム関連情報は以下となります。

**制御システムセキュリティ情報**

<https://www.jpccert.or.jp/ics/ics-community.html>



<sup>2</sup> 運用マニュアルの策定では、以下のドキュメントが参考になります。  
 日本電気制御機器工業会「制御システムセキュリティ運用ガイドライン」  
[https://www.neca.or.jp/wp-content/uploads/control\\_system\\_security\\_guideline2017.pdf](https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline2017.pdf)  
 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第 2.1 版」  
<https://www.ipa.go.jp/files/000055520.pdf> (第 2 部 4 セキュリティポリシーの策定、付録 3)  
<sup>3</sup> 台帳作成時は、以下のドキュメントが参考になります。  
 JPCERT/CC「J-CLICS Step2」(1.システムとビジネスリスクの理解)  
[https://www.jpccert.or.jp/ics/J-CLICS\\_STEP2\\_guide.pdf](https://www.jpccert.or.jp/ics/J-CLICS_STEP2_guide.pdf)



## 5. インシデントに備えた体制検討

インシデントを早期に検知するために、通信や IoT デバイスに関するログを定期的に確認する仕組みや体制を構築します。インシデントの検知時は、迅速に対応することが被害を最小にするため、インシデントへの対応手順や対応体制を事前に検討・整備しておきます。自社で対応が難しい内容は、外部事業者に依頼します。工場の管理者は、インシデントに関わる原因究明や復旧作業を迅速に行うために、情報系システムやセキュリティの担当者など、社内関係者との連絡・連携体制の構築と言った社内の協力体制を確立します。システムインテグレータやクラウド事業者等、外部事業者の緊急連絡先や、外部事業者が対応可能な支援内容も予め確認します。

JPCERT/CC へのインシデント報告窓口は以下となります。

### 制御システムインシデント対応依頼

<https://www.jpccert.or.jp/ics/ics-form.html>



## 6. データ破棄に関する確認

IoT デバイスを廃棄する際に、デバイスに残された認証情報が悪用されて攻撃に利用されたり、残されたデータを不正に利用されたりすることを防ぐために、利用終了時の IoT デバイスやクラウド等からのデータ削除や物理的な破壊（委託先における廃棄証明書等の提出）を行うことを、運用マニュアルに記載しておきます。

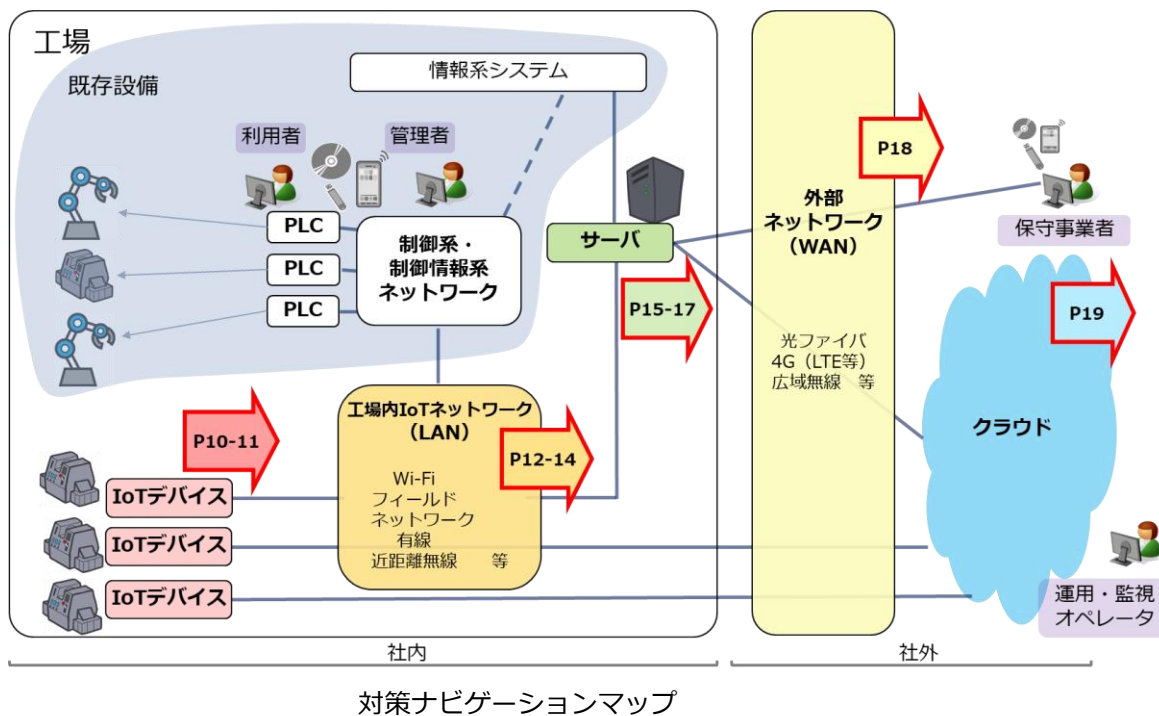


万一、サイバー攻撃を受けた場合、顧客や取引先、あるいは社会から管理責任を問われることとなります。

説明責任を果たすために、実施したセキュリティ対策やログ等の記録は保存を行い、証拠として提示できることも必要です。

## 産業用 IoT の構成要素：対策ナビゲーションマップ

以下の対策ナビゲーションマップに産業用 IoT の一般的なシステムを構成する要素を示しています。導入を検討しているシステム構成と照らし合わせて、構成要素毎のセキュリティ対策ポイントを示したページをご覧ください。



- IoTデバイスでのセキュリティ対策ポイント p.10-11
- 工場内IoTネットワーク(LAN)でのセキュリティ対策ポイント p.12-14  
※制御系、制御情報系ネットワークとの接続はこのパートにて記載しています。
- サーバでのセキュリティ対策ポイント p.15-17
- 外部ネットワーク(WAN)でのセキュリティ対策ポイント p.18
- クラウドでのセキュリティ対策ポイント p.19

## 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。

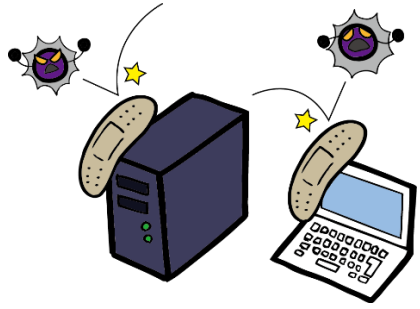


パスワードは、推測されにくく強度の高いもの<sup>4</sup>を設定します。

<sup>4</sup> 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運用ガイドライン」[https://www.neca.or.jp/wp-content/uploads/control\\_system\\_security\\_guideline2017.pdf](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>）

### D-3 IoTデバイスの脆弱性対策をしましょう

脆弱性を悪用して、不正アクセスやウイルス感染が引き起こされることから、脆弱性対策は重要です。特に IoT デバイスをインターネットに直接接続する構成を取る場合は注意する必要があります。

重点的な対策例	<ul style="list-style-type: none"> <li>● 導入時にソフトウェアを最新の状態にします。</li> <li>● 脆弱性は随時発見されることから、運用時も常にソフトウェアを最新の状態にするために、メンテナンス計画を立てます。</li> <li>● 定常的な脆弱性対策が困難な場合は、回避策の検討をしつつ、攻撃を受けた場合のリスクを明確にし、事後対応（インシデント対応）について事前に計画しておきます。</li> </ul>	
---------	--	--

### D-4 盗難対策を行いましょう

IoT デバイスは小型で容易に持ち出しが可能である場合が多いため、物理的な盗難対策をする必要があります。

重点的な対策例	<ul style="list-style-type: none"> <li>● IoT デバイスにワイヤーロックをかけたり、施錠されているキャビネットに IoT デバイスを収容したりといった盗難対策を行います。</li> </ul>
---------	---

### D-5 IoTデバイスへの周辺機器の接続を適切に管理しましょう

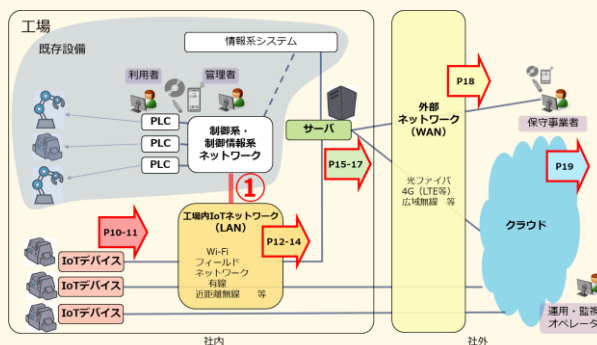
工場では USB メモリ等外部記憶媒体を通じたウイルス感染事例があり、IoT デバイスにも外部記憶媒体を接続するケースがあることから、外部記憶媒体を中心とした周辺機器のセキュリティ対策をする必要があります。

重点的な対策例	<ul style="list-style-type: none"> <li>● 工場で使用する USB メモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理します。</li> <li>● IoT デバイスに接続する USB メモリ等の外部記憶媒体は、ウイルス対策ソフトでチェックする、ウイルスチェックが可能な USB メモリを用いる等の対策を行います。</li> <li>● 使用しない USB ポート、シリアルポートは栓をするなど物理的に閉塞します。</li> </ul>
---------	---

## 工場内 IoT ネットワーク(LAN)でのセキュリティ対策ポイント

### Point 制御システムネットワークとの接続に注意

工場内 IoT ネットワークと既存の制御システムネットワークの接続（図中①）には細心の注意が必要です。多くの場合、制御システムネットワーク内の機器は脆弱で、セキュリティを確保するために完全に独立させるか、外部との通信を厳格に制限しています。しかし、産業用 IoT では、外部のクラウドサービス利用時などインターネットを使用するケースが想定されることから、潜在的に外部からの侵入のリスクを有し、結果として工場の生産活動が阻害されるような事態も想定されます。



### 工場内 IoT ネットワーク(LAN)のセキュリティ対策が不十分な場合のリスク例

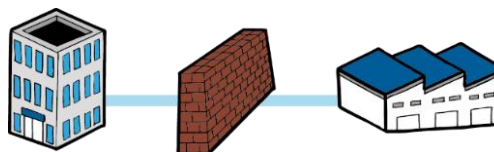
- 工場内 IoT ネットワークにウイルスなどの侵入を許し、通信データを窃取されることで、技術や生産に関するデータが漏えいするリスクがあります。
- 工場内 IoT ネットワークにウイルスなどの侵入を許し、通信データが改ざんされることで誤った分析・解析が行われ、運用者が操作判断を誤ったり、誤った制御が行われたりするリスクがあります。
- 工場内 IoT ネットワークの一部の IoT デバイスに感染したウイルスが、ネットワーク経由で感染を拡大し、被害が大きくなるリスクがあります。

#### L-1 工場内 IoT ネットワークの境界で必要な通信だけに制限しましょう

オフィス内の PC はインターネットなどの外部ネットワークと接続してメールの受信、Web サイトの閲覧などを行っていることから、ウイルス感染の可能性があります。このため、オフィス等の情報系ネットワークと工場内 IoT ネットワークを接続しないことが外部からの脅威の流入を防ぐ点で肝要です。接続する必要がある場合は、ネットワーク境界でセキュリティ対策を十分に行う必要があります。

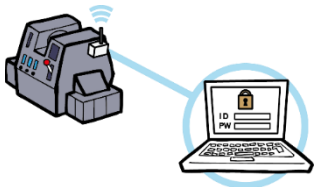
#### 重点的な対策例

- 工場内 IoT ネットワークと情報系ネットワークをつなぐ場合は、ネットワークの境界にルータやファイアウォールを設置し、必要な通信だけを許可するように設定します。また、システムの仕様が変更になった場合は、忘れずにこれら設定の見直しをします。



## L-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ます。第三者がすぐに調べることができることから、導入時に変更しなければなりません。

<p>重点的な 対策例</p>	<ul style="list-style-type: none"> <li>● ネットワーク機器に初期設定されていたパスワードは導入時に変更します。</li> <li>● 設定変更画面などの認証を有効・無効に設定できる場合は、必ず有効にします。また、認証画面は WAN 側からはアクセスできないように設定しましょう。</li> </ul> <p>パスワードは、推測されにくく強度の高いもの<sup>5</sup>を設定します。</p>	
---------------------	--	---

## L-3 ネットワーク機器への接続を限定しましょう

不正な端末をネットワークに接続されると、通信を窃取・改ざんされるリスクが高まることから、不正な端末がネットワーク機器に接続できないようにする必要があります。

<p>重点的な 対策例</p>	<ul style="list-style-type: none"> <li>● ネットワーク機器に不必要な機器が接続されないよう、不要なポートは物理的に閉塞すると同時に、設定で無効化します。</li> <li>● ネットワーク機器に不要な機器が接続されていないか、シリアルポート、コンソールポートなどを定期的を確認します。</li> <li>● ネットワーク機器は、管理・保守などの目的で各種サービス（ssh,sftp など）を稼働させることができます。必要なサービスだけを稼働させるように設定します。</li> <li>● 無線 LAN 機器は、電波の伝搬範囲を適切に設定します。（窓付近にアクセスポイントを設置しない、電波の出力を調整する等）</li> </ul>
---------------------	---

<sup>5</sup> 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運用ガイドライン」[https://www.neca.or.jp/wp-content/uploads/control\\_system\\_security\\_guideline2017.pdf](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>）

**L - 4 無線 LAN 通信では暗号化を有効にしましょう**

無線 LAN は電波の傍受が容易であるため、盗聴されても重要情報が漏れないように、データ暗号化などセキュリティ対策がなされた通信方式を選ぶ必要があります。

重点的な 対策例	<ul style="list-style-type: none"> <li>● 無線 LAN の通信を暗号化します。暗号化の設定は、その時点で無線機器に実装されるプロトコル・暗号の中で、最も安全性が高いものを選びます<sup>6</sup>。</li> </ul>
-------------	---

**L - 5 工場内 IoT ネットワーク内の監視・異常検知をしましょう**

異常が発生した場合、迅速に対応するために工場内 IoT ネットワーク内の通信を監視し、異常を検知し、迅速に対応することが重要です。

重点的な 対策例	<ul style="list-style-type: none"> <li>● 工場内 IoT ネットワーク内の通信を監視し、異常を検知した場合にアラートを通知します。必要に応じて、侵入検知・防御システム (IDS/IPS) 等の機器を導入します。</li> </ul>
-------------	--

<sup>6</sup> 総務省「企業等が安心して無線 LAN を導入・運用するために」  
[http://www.soumu.go.jp/main\\_content/000199323.pdf](http://www.soumu.go.jp/main_content/000199323.pdf)

## ○ サーバでのセキュリティ対策ポイント

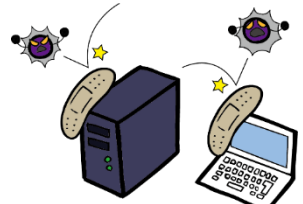
産業用 IoT を構成する工場内のサーバは、クラウドなどの外部との通信遅延を回避したり、IoT デバイスが行う処理を代わりに実施させたりすることで高速・高度なアプリケーション処理を実現させるといった目的で設置される場合があります。

### サーバのセキュリティ対策が不十分な場合のリスク例

- ・ サーバに不正にアクセスされ、内部のデータを窃取されて重要な技術や生産に関するデータが漏えいしたり、内部のデータが消去されたりするリスクがあります。
- ・ サーバにウイルスを仕込まれることで、内部のデータが不正に改ざんされたり、プログラムが書き換えられたりすることで分析・解析結果が誤ったものとなり、工場の稼働に悪影響を与えるリスクがあります。

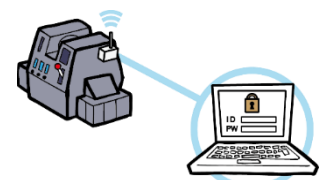
#### S - 1 サーバの脆弱性対策をしましょう

脆弱性を使用して、不正アクセスやウイルス感染が引き起こされることから、脆弱性対策は重要です。脆弱性対策を定期的実施できるように、サーバの導入前から定期メンテナンス計画、パッチの適用方法について検討します。

<p>重点的な対策例</p>	<ul style="list-style-type: none"> <li>● 導入時に OS 及びアプリケーション等が最新の状態になるようパッチを適用します。</li> <li>● 脆弱性は随時発見されることから、パッチ適用の影響について事前に検証した後、可能な限り、運用時も定期的にソフトウェアを最新の状態にするために、パッチに関する情報収集方法やパッチの適用方法を定めておきます。</li> </ul>	
----------------	---	---

#### S - 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、導入時に変更しなければなりません。

<p>重点的な対策例</p>	<ul style="list-style-type: none"> <li>● サーバ及びサーバアプリケーション等に初期設定されていた ID・パスワードは導入時に変更してください。その際、パスワードは、強度の高いもの<sup>7</sup>を設定します。</li> </ul>	
----------------	---	---

<sup>7</sup> 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運用ガイドライン」[https://www.neca.or.jp/wp-content/uploads/control\\_system\\_security\\_guideline2017.pdf](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>)



### S - 3 アカウントを適切に設定しましょう

アカウントを奪われて不正に使われないためにも、アカウント毎に必要な最小限の権限とすることが重要です。権限とは、利用者 ID 発行、フォルダ作成、データの参照・書き込み・削除等の利用可能な機能です。

重点的な 対策例	<ul style="list-style-type: none"> <li>● アカウント毎にアクセス権限を付与します。特に、全権限を持つアカウント (Administrator, root など) は利用できるユーザを限定します。</li> <li>● 運用時、アカウントを定期的に見直すタイミングを定め、アカウントやアクセス権限が適切かどうかを確認し、使わなくなったアカウントや権限を削除します。</li> <li>● 一定時間内のログインエラー回数が基準値を超えた場合には、そのアカウントを一定時間使用禁止にする等、アカウントロックの仕組みを設定します。</li> </ul>
-------------	--

### S - 4 サーバへの周辺機器の接続を適切に管理しましょう

工場では USB メモリ等外部記憶媒体を通じたウイルス感染事例があり、IoT でも外部記憶媒体を利用するケースがあることから、外部記憶媒体を主とした周辺機器のセキュリティ対策をする必要があります。

重点的な 対策例	<ul style="list-style-type: none"> <li>● 工場で使用する USB メモリ等の周辺機器は、管理台帳を作成し、保管場所で施錠管理します。</li> <li>● サーバに接続する USB メモリ等の外部記憶媒体は、ウイルス対策ソフトでチェックする、ウイルスチェックが可能な USB メモリを用いる等の対策を行います。</li> <li>● 必要に応じて、許可された USB メモリ以外の読み込みを禁止するツールの利用も検討します。</li> <li>● 使用しない USB ポートは栓をするなど物理的に閉塞します。</li> </ul>
-------------	---

### S - 5 不要な物理ポートやサービスを停止しましょう

サーバの不要な物理ポートやサービスを停止することで、外部から不正アクセスを受ける可能性を低減することができます。

重点的な 対策例	<ul style="list-style-type: none"> <li>● 不要な物理ポート (LAN ポート、USB ポート、シリアルポート等) は栓をするなど物理的に閉塞します。</li> <li>● OS を設定する際に、業務に不要なサービス (FTP 等) は無効化の設定をします。</li> </ul>
-------------	---

## S - 6 サーバのログを定期的に確認しましょう

常時稼働しているサーバは攻撃者にとって恰好の攻撃の足場になります。特に運用優先で脆弱性対策を十分に行っていないサーバは、いつの間にか侵入を許してしまっている危険性もあります。サーバのログを定期的に確認することで、不正アクセスなどの早期発見が期待できます。

重点的な 対策例	<ul style="list-style-type: none"> <li>● サーバ導入時にログが取得されるように設定します。その際、ログの保存容量が大きくなりすぎないようにファイル圧縮などの対策も行います。</li> <li>● サーバのログを定期的に確認します。社内で確認できる者がいない場合は、外部に依頼することを検討します。</li> <li>● サーバのログは、過去半年から1年程度をDVD-ROMなどに別途保管します。</li> <li>● 異常が発生した場合、アラートを通知する設定を行います。</li> </ul>
-------------	---

## S - 7 サーバのウイルス対策を行いましょ

USBメモリや外部ネットワークを経由したウイルスの侵入を防止、あるいは侵入した際も早期検知・対処により被害の最小化を図るために、ウイルス対策を行うことが重要です。

重点的な 対策例	<ul style="list-style-type: none"> <li>● ウイルス感染を検知・駆除するために、ウイルス対策ソフトを導入します。ブラックリスト型のウイルス対策ソフトは常に最新の状態を維持します。更新ファイルの適用の際には、安全性を事前に確認したUSBメモリを使用するなど細心の注意を払います。</li> </ul>
-------------	--

## 外部ネットワーク(WAN)でのセキュリティ対策ポイント

### 外部ネットワーク(WAN)のセキュリティ対策が不十分な場合のリスク例

- ・ インターネットから工場のネットワークへ不正侵入され、技術や生産に関するデータが漏えいするリスクがあります。
- ・ ルータやFWなどのGW機器に対するDDoS攻撃によってクラウドとの通信が阻害されるリスクがあります。

#### W - 1 外部ネットワーク接続はセキュアな回線を選定しましょう

外部から攻撃されるリスクを低減するために、できるだけインターネットを利用しないことが重要です。

<p>重点的な対策例</p>	<ul style="list-style-type: none"> <li>● クラウド等外部との接続は、VPNや専用線（LTE回線等を含む）を選定します。</li> <li>● Internet VPNを利用する場合は、FWやルータのフィルタ設定などを厳格に行います。</li> </ul>	
----------------	---	--

#### W - 2 工場内IoTネットワークと外部ネットワークとの境界では、必要な通信だけに限定しましょう

一般的な情報システム同様、ネットワーク境界で通信を必要最小限に制限することで、工場内データの外部流出や外部からの不正アクセスを防御することが重要です。

<p>重点的な対策例</p>	<ul style="list-style-type: none"> <li>● 工場内IoTネットワークと外部ネットワーク（WAN）の境界に設置されるルータやファイアウォール等で、クラウドへの通信やリモート保守等の必要な通信だけを許可するように設定します。具体的には、外部から内部への通信は、リモート保守などに限定します。内部から外部への通信も同様に、クラウドなどの必要な通信先に限定します。</li> <li>● クラウドとの通信が工場の稼働時間中に限定される場合など、常時接続が必要でない場合は、未使用時に通信機器の電源を切る等、回線を切断します。</li> </ul>
----------------	--

## ○ クラウドでのセキュリティ対策ポイント

### セキュリティ対策が不十分なクラウドを利用した場合のリスク例

- ・ クラウドへのサイバー攻撃により、クラウドにアップロードした技術や生産に関するデータの漏えいや改ざんのリスクがあります。
- ・ クラウドが停止することで、工場の IoT デバイスからデータを分析できなくなるなどの影響を受けるリスクがあります。

### C - 1 クラウドサービスのセキュリティ対策を確認しましょう

クラウドにおけるサーバ脆弱性の放置や管理体制の不備等により、サイバー攻撃が発生し、工場の稼働に影響を及ぼすリスクがあることから、クラウドのセキュリティ対策について、ユーザが主体的に確認する必要があります。

#### 重点的な 対策例

- クラウドサービスのセキュリティ対策状況について、契約や規約、ホワイトペーパー等で確認し、十分なセキュリティ対策<sup>8</sup>がなされているかどうかを確認します。ISMS クラウドセキュリティ認証等、クラウド事業者における認証の取得状況も、クラウドサービスを選ぶ際の参考となります。
- クラウドサービスでは固定 IP アドレスサービスを使用します。工場側の通信機器では、クラウド側の固定 IP アドレスを指定して通信先を限定するように設定し、外部からの接続要求は必要に応じて破棄するように設定します。
- クラウドサービスの異常を検知するために、定期的にログを確認したり、必要に応じてアラート通知等のサービスを利用したりします。



<sup>8</sup> 対策の判断基準として、国が提供しているガイドライン等が参考になります。  
 経済産業省「クラウドセキュリティガイドライン」と「活用ガイドブック」  
<http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html>  
 総務省「クラウドサービスを利用する際の情報セキュリティ対策」  
[http://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/business/admin/15.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/15.html)

## おわりに

今後、ものづくり産業における技術の進化により、IoT・産業用 IoT や Industry4.0 等と呼ばれるように、工場のシステムが様々なネットワークに接続される時代が来ると予想されています。そういった新しい時代に対応して行くにあたり、セキュリティの確保は重要な課題となります。セキュリティ対策の不備により、工場の生産活動が阻害されるといった事態は避けなければなりません。本書が、産業用 IoT を導入される企業において、セキュリティ対策向上の一助となることを願います。

用語集

用語	意味
CSMS	Cyber Security Management System サイバーセキュリティマネジメントシステム 制御システムを対象とした、サイバーセキュリティのマネジメントシステム。制御システムセキュリティに関する国際標準 IEC62443 のうち、組織の管理面の標準 IEC62443-2-1 をベースにした枠組み
DDoS 攻撃	Distributed Denial of Service 分散型サービス不能攻撃 大量または不正なパケットをネットワーク機器やサーバに送りつけてサービスが正常に行えない状態を引き起こすサイバー攻撃
FW (ファイアウォール)	Firewall 異なるネットワークの境界に設置し、通過すべき通信とそうでない通信を分ける機器
IDS/IPS	Intrusion Detection System 不正侵入検知システム Intrusion Prevention System 不正侵入防止システム
Internet VPN	インターネット上に、仮想的に専用線接続されている状況を実現すること
ISMS	Information Security Management System 情報セキュリティマネジメントシステム 組織においてセキュリティを管理するための枠組みであり、ISO27001 で標準化されている。
LAN	Local Area Network 拠点内で用いられるネットワーク
LPWA	Low Power Wide Area 低消費電力で遠距離通信を実現する通信方式 (LoRa、Sigfox 等)
VPN	Virtual Private Network インターネットや多人数が利用する閉域網上に、仮想的に専用線接続されている状況を実現すること
WAN	Wide Area Network 地理的に離れた拠点を接続するネットワーク
脆弱性	ソフトウェア等におけるセキュリティ上の弱点
セキュリティ・バイ・デザイン	企画・設計段階からセキュリティ面でのリスクを想定し、対策を確保すること

## 参考文献

### [IoT 全般]

- IoT 推進コンソーシアム IoT セキュリティワーキンググループ「IoT セキュリティガイドライン ver1.0」 (2016 年 7 月)  
<http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf>
- 内閣サイバーセキュリティセンター「安全な IoT システムのためのセキュリティに関する一般的枠組」 (2016 年 8 月)  
[https://www.nisc.go.jp/active/kihon/pdf/iot\\_framework2016.pdf](https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf)

### [IoT 開発者]

- 情報処理推進機構「つながる世界の開発指針第 2 版」 (2017 年 6 月)  
<https://www.ipa.go.jp/files/000060387.pdf>
- 情報処理推進機構「IoT 開発におけるセキュリティ設計の手引き」 (2017 年 12 月改訂)  
<https://www.ipa.go.jp/files/000052459.pdf>
- 情報処理推進機構「つながる世界のセーフティ & セキュリティ設計入門」 (2015 年 10 月)  
<https://www.ipa.go.jp/files/000055007.pdf>

### [IoT 利用者 (工場)]

- 経済産業省「CPS/IoT セキュリティ対応マニュアル」 (平成 28 年度 IoT 推進のための社会システム推進事業 (スマート工場実証事業) 報告書) (2017 年 3 月)  
[http://www.meti.go.jp/policy/mono\\_info\\_service/mono/smart\\_mono/H28SmartFactory\\_DataProfile\\_Security\\_Report.pdf](http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report.pdf)
- 経済産業省/NEDO「IoT セキュリティ対応マニュアル産業保安版」 (2018 年 4 月)  
[http://www.meti.go.jp/policy/safety\\_security/industrial\\_safety/sangyo/hipregas/files/security\\_manual.pdf](http://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/security_manual.pdf)

### [制御システム]

- SICE/JEITA/JEMIMA/JPCERT コーディネーションセンター「J-CLICS」 (2013 年 3 月)  
<https://www.jpCERT.or.jp/ics/jclics.html>
- 日本電気制御機器工業会「制御システムセキュリティ運用ガイドライン」 (2017 年 11 月改訂)  
[https://www.neca.or.jp/wp-content/uploads/control\\_system\\_security\\_guideline2017.pdf](https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline2017.pdf)

### [中小企業]

- 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第 2.1 版」 (2017 年 1 月)  
<https://www.ipa.go.jp/files/000055520.pdf>

## 著作権・引用や二次利用等について

本資料の著作権は一般社団法人 JPCERT コーディネーションセンターに帰属します。

引用・転載・再配布等につきましては、広報 (pr@jpcert.or.jp) にご連絡ください。

本文書内に記載されている情報により生じるいかなる損失または損害に対して、JPCERT/CC は責任を負うものではありません。