IoT Sec for Users

5分でIoTのセキュリティリスクがわかる本

はじめに

本書は情報処理推進機構(*1 IPA)が主催する第5期中核人材育成プログラム(*2　ICSCoE)の受講生が学んだ知見を活かして、IoTセキュリティに関してまとめたハンドブックです。

ハンドブックを作成した目的は、企業でDX（Digital Transformation）推進に伴い、今後利用が進んでいくIoT機器に潜むセキュリティリスクを認識していただくことです。
IoTの導入を検討する方や既に利用されている方々が、セキュリティインシデントの被害者や加害者にならないために＊3 IoTセキュリティガイドライン及び＊4 CCDSのガイドラインを参照していただくことで、IoTセキュリティ向上の一助になれば幸いです。

＊1 **I**nformation-technology **P**romotion **A**gency, Japan
＊2 **I**ndustrial **C**yber **S**ecurity **C**enter **o**f **E**xcellence
＊3 [IoTセキュリティガイドライン]
URL: https://www.soumu.go.jp/main_content/000428393.pdf
＊4 [CCDSのガイドライン]
URL: https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021-extra_v2.0_jpn.pdf

IoT
Internet of Things

Chapter 1 IoTについて

Point 01

IoT機器は何か、対象読者は誰かを紹介します

Point 02

世の中でどのようなIoT機器が使用されていて
どのくらい攻撃の標的となっているのかを紹介します

Point 03

IoT機器の特性に基づくリスクとIoTセキュリティ
ガイドラインの確認箇所を紹介します

01

IoT機器とは

”Internet of Things”の略称のこと。
ネットワークに繋がる”モノ”であり、本書では
「固有にIPアドレスを持ち、単体またはWiFi経由でインターネットに繋げられる機器」をIoT機器と定義しています。

IoT機器の一例

・プリンタ　　・ハンディターミナル
・WEBカメラ　　・スマートスピーカー

IT企業だけでなく、産業系、医療系など、多くの業界でIoT機器が利用されています。

02

対象読者

IoTセキュリティガイドラインは、機器メーカー、サービス提供会社も関係していますが、このハンドブックは企業利用者に注目しています。

●ハンドブック対象読者

企業にてIoT機器を導入または利用している人を対象としています。

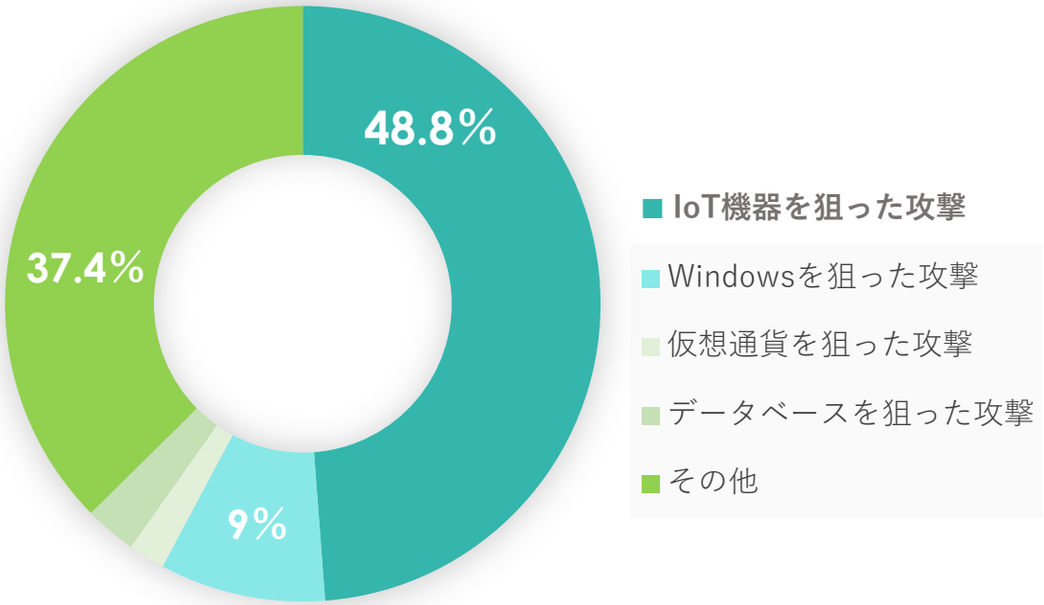
●IoTセキュリティガイドライン対象読者

企業にてIoT機器を導入または利用している人を対象としています。

03

世の中のIoT機器の利用台数

2022年には300億台を超える見込みです。
利用数に伴ってリスクも増えてしまいます。



観測されたサイバー攻撃のうち、
約半数の48.8%がIoT機器を狙った攻撃であった！

【引用元】サイバー攻撃の最近の動向等について
[総務省]https://www.soumu.go.jp/main_content/000722477.pdf

04

IoT機器のリスク

IoT 特有の性質はリスクとなるためきちんと抑えましょう！

IoT 特有の性質

- 脅威の影響範囲・度合いが大きい
- ライフサイクルが長い
- 監視が行き届きにくい
- ネットワーク環境の理解が不十分
- 機能・性能が限られている
- 開発者が想定していなかった利用

製造・医療現場ではIoT機器の制御が生命の危機にさらされる可能性があります。
Chapter 2 で実際に発生したインシデント事例を確認しましょう。

ガイドラインの確認箇所

IoT機器のリスクの詳細についてはIoTセキュリティガイドラインの要点3～7(P18～P25)を確認しましょう！

Incident Report

Chapter 2 インシデント事例

Point

IoT機器に関するインシデント事例を5つ紹介します
それぞれの事例にて攻撃手順や、チェックすべきポイント
さらにCCDSガイドラインおよびIoTセキュリティガイドライン
の確認箇所を紹介します

Case 01

無線LANの通信傍受による情報漏洩

【引用元】企業等が安心して無線LANを導入・運用するために
[総務省]https://www.soumu.go.jp/main_content/000199320.pdf

発生日	不明
発生地	日本
攻撃手法	通信傍受
攻撃手順	1. 攻撃者が脆弱な暗号化を使用している通信を傍受し暗号キーを解読 2. 傍受したデータを解読したキーで復元
影響	情報漏洩 復元したデータから画像ファイルを抽出し公開したとされている

無線LAN使用時のポイント

カフェの無料Wi-Fiなど通信の暗号化規格が古い無線LANは、ビジネスで利用しないようにしましょう。
無線LANを設置する際は設定する通信の暗号化規格に注意しましょう。

ガイドラインの確認箇所

注意すべき点は無線LAN機器に適切な認証機能の導入や適切なネットワーク接続をすることです。詳細はIoTセキュリティガイドラインの要点14(P40)、要点16(P44)、CCDSのガイドラインNo,2-1(P14)を確認しましょう！

Case 02

IoT機器のマルウェア感染-Mirai

【引用元】https://project.nikkeibp.co.jp/idg/atcl/idg/14/481542/102800290/

発　生　日　2016年10月21日

発　生　地　アメリカ　DNSサービス会社

攻撃手法　不正アクセス、一斉攻撃

攻撃手順
1. 初期のIDとパスワードが推測され不正アクセス
2. 攻撃者は攻撃者サーバを操作
3. 攻撃者サーバから感染した機器へ攻撃命令
4. 機器からサーバへ一斉通信で攻撃

影　　響　サービス提供先のWEB停止
感染した機器から新たに機器へ感染拡大した

IoT機器使用時のポイント

インターネットにつながるIoT機器は攻撃対象となりマルウェアに感染する可能性があります。初期パスワードを使用していると簡単に攻撃されてしまいます。

ガイドラインの確認箇所

注意すべき点は機器の初期設定です。詳細はIoTセキュリティガイドラインの要点4(P20)、要点15(P42)対策例の項目を確認しましょう！

Case 03

フィンランドの暖房停止

【引用元】https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

発　生　日　2016年11月

発　生　地　フィンランド、ビル業界

攻撃手法　サービス拒否(DDoS)攻撃

攻撃手順
1. 攻撃者が脆弱な機器を発見し不正アクセス
2. 攻撃者は攻撃者サーバを操作
3. 攻撃者サーバから感染した機器へ攻撃命令
4. 複数の機器から一斉に攻撃し制御システムを停止

影　　響　全館集中暖房と温水循環制御システムが停止されて暖房機能が停止したとされている

IoT機器使用時のポイント

システムの接続先が増え、外部から攻撃を受けるリスクが増えます。
インターネットから接続できる機器がある場合大量の攻撃を受ける可能性があります。

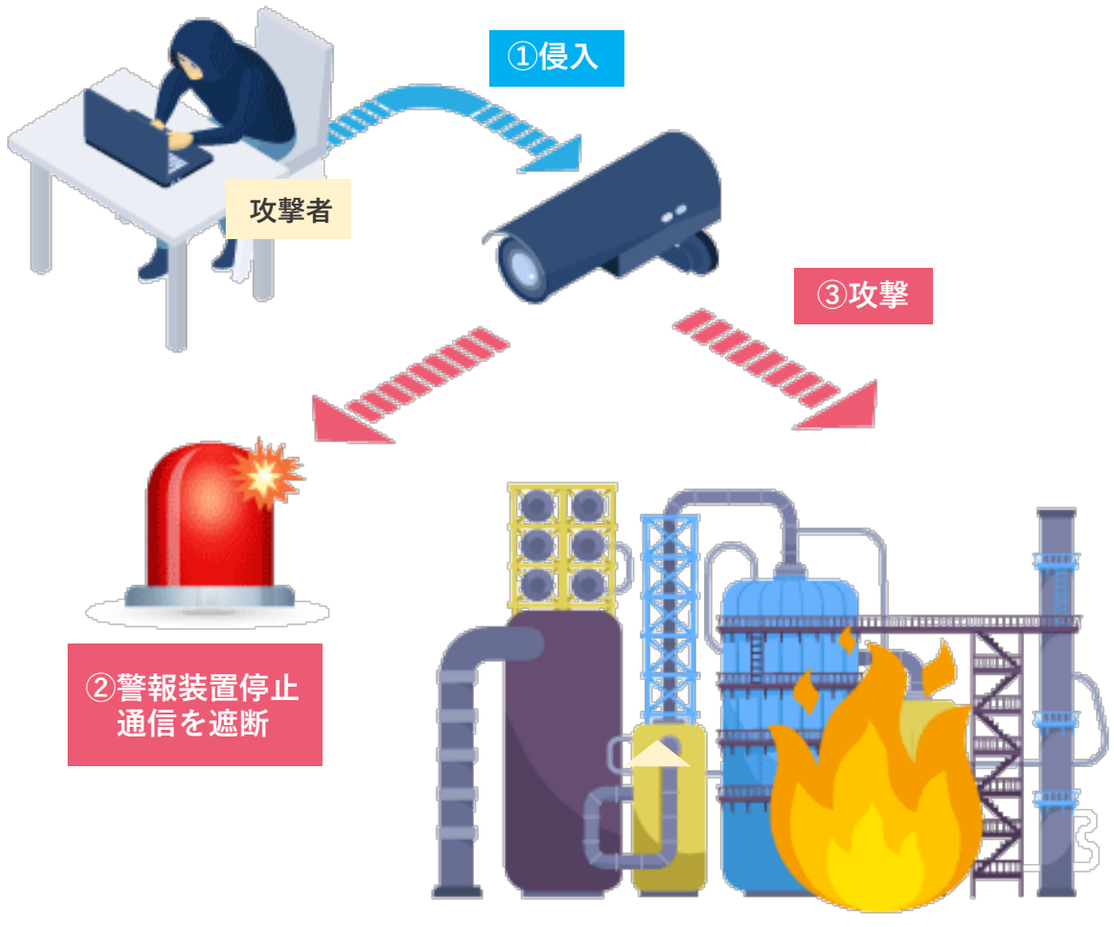
ガイドラインの確認箇所

注意すべき点は安全安心な運用状態を維持することです。詳細はIoTセキュリティガイドラインの要点9(P31)異常検知の項目、要点19(P51)対策例の項目を確認しましょう！

Case 04

トルコのパイプライン爆発

【引用元】重要インフラにおけるサイバー攻撃の脅威と課題　CSSCの取組紹介
技術研究組合制御システムセキュリティセンター（CSSC）
https://www.ipa.go.jp/files/000057714.pdf



発　生　日　2008年8月5日

発　生　地　トルコ

攻撃手法　監視カメラの脆弱性から侵入

攻撃手順
1. 監視カメラのソフトウェアの脆弱性を利用して内部ネットワークに侵入
2. 警報装置を停止させ、通信を遮断
3. 攻撃によりパイプライン内の原油の圧力が上昇

影　　響　原油の圧力が上昇し爆発を引き起こしたとされており、巨額損失が発生した

IoT機器使用時のポイント

IoT機器に脆弱性がある場合、その脆弱性を突かれ内部ネットワークに侵入される可能性があります。
初期パスワードや簡単なパスワードは変更しないと簡単に攻撃されてしまいます。

ガイドラインの確認箇所

注意すべき点は安全安心に運用することと初期設定です。
詳細はIoTセキュリティガイドラインの要点15(P42)、要点17(P46)、CCDSのガイドラインNo1-5(P12)の対策例の項目を確認しましょう！

Case 05

IoT機器を踏み台に利用した情報窃盗

【引用元】Cybersecurity Management and Oversight at the Jet Propulsion Laboratory
[NASA] https://oig.nasa.gov/docs/IG-19-022.pdf

発　生　日　2018年4月頃

発　生　地　アメリカ

攻撃手法　適切に管理されていない機器を踏み台にして侵入し情報窃取

攻撃手順
1. 攻撃者が何らかの形で内部ネットワークに侵入
2. 内部ネットワーク内を調査し、IoT機器が接続されていることを確認後、IoT機器にアクセス
3. 侵入した機器から内部ネットワーク情報を調査
4. 調査した情報をもとに機密情報を窃取

影　響　10ヶ月間もの間、内部情報が収集されており
その期間収集されたデータが漏洩した

IoT機器使用時のポイント

初期パスワードを使用していると簡単に攻撃されてしまいます。
適切に運用するために接続する機器の管理をしましょう。

ガイドラインの確認箇所

注意すべき点は安全安心に運用管理を実施することです。
詳細はIoTセキュリティガイドラインの要点13(P39)、
要点15(P42)対策例の項目を確認しましょう。また、要点7(P25)を確認して他の過去事例からも学びましょう！

Security Validation

Chapter 3 セキュリティホール検証

Point

セキュリティホール検証はIoT機器に対して検証した内容を事例ベースで紹介します

検証に必要な前提条件や所要時間、攻撃手順やチェックすべきポイントについてもChapter 2 と同様に紹介しています

WEB カメラ01

不正な通信による カメラ映像窃取

前提条件 初期のID、パスワード、
RTSPポートを使用、カメラと通信できる状態

所要時間 2時間程度（カメラの仕様を把握する必要あり）

攻撃手順

1. カメラの型番等から初期のID、パスワード、IPアドレス情報をWEB上のマニュアルから入手
2. RTSPポートに対して、収集した情報をもとに映像取得リクエストを送信
3. 受信したリクエストに従ってカメラから映像の一部を送信

IoT機器使用時のポイント

初期のID、パスワードを利用しているとID、パスワードが入手され不正な操作や不正に映像を窃取される可能性があります
デフォルトポートから不正に映像を窃取される可能性があるため、デフォルトポートの変更、または不要なポートは閉じましょう。

ガイドラインの確認箇所

注意すべき点は適切な初期設定とアクセス制限をすることです。詳細は、 IoTセキュリティガイドラインの要点15(P42)、CCDSのガイドラインNo1-1(P4)の対策例の項目を確認しましょう！

WEB カメラ02

脆弱性を持つWEBカメラのパスワード窃取

前提条件 WEBカメラのIPアドレスを把握、通信できる状態
カメラに脆弱性が存在している状態

所要時間 10分

攻撃手順

1. ポートスキャンでカメラの管理用ポートを特定
2. 脆弱性を利用し、不正なリクエストを送信
3. カメラのID、パスワードを入手
4. カメラの管理画面にログイン
5. 映像や録画データの情報を取得

IoT機器使用時のポイント

IoT機器に脆弱性がある場合、その脆弱性を突かれて内部に侵入され機密情報が窃取される可能性があります。

ガイドラインの確認箇所

注意すべき点は、安全安心に運用することです。詳細は、 IoTセキュリティガイドラインの要点17(P46)、CCDSのガイドラインNo1-5(P12)の対策例の項目を確認しましょう！

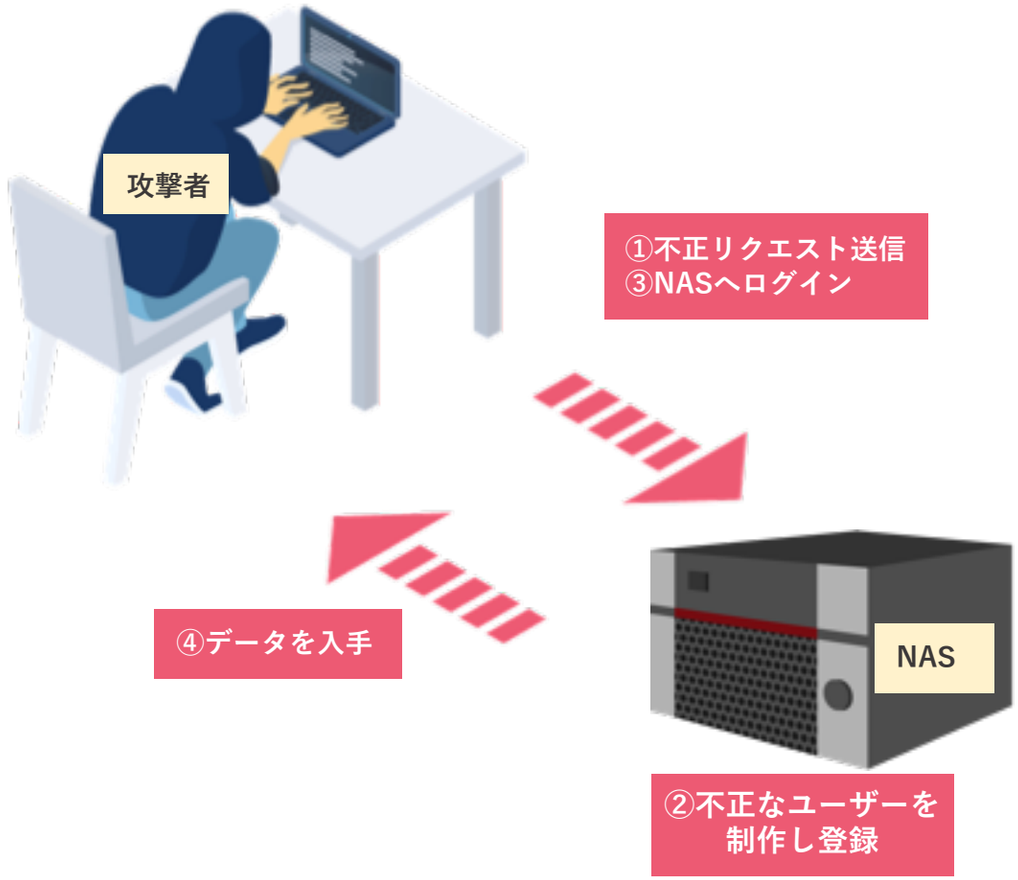
NAS

リモートコマンドの不正実行

前提条件 NASのIPアドレスを把握、通信できる状態
NASに脆弱性が存在している状態

所要時間 1時間程度

攻撃手順
1. 任意のユーザを作成する不正リクエストを送信
2. 脆弱性のあるNASがリクエストを受信し
   不正なユーザを作成し登録
3. 作成したユーザにてNASへログイン
4. NASに保存しているデータを入手



IoT機器使用時のポイント

IoT機器に脆弱性がある場合、その脆弱性を突かれ、マルウェアが配置されるリスクや機密情報が窃取される可能性があります。

ガイドラインの確認箇所

注意すべき点は、安全安心に運用することです。詳細は、 IoTセキュリティガイドラインの要点17(P46)、CCDSのガイドラインNo1-5(P12)の対策例の項目を確認しましょう！

Conclusion

Chapter 4 終わりに

Point

IoT機器を実際に購入してから廃棄するまでに注意すべきことや実施すべきことについて記載しています

終わりに

ここまでで学べたこと

色々なIoT機器がありインターネットに接続することで便利
になる反面、適切に運用していないとセキュリティリスク
の増加につながります！

購入する際に確認すべきこと

初期パスワードの変更ができるIoT機器を確認しましょう！
また、セキュリティアップデートの内容や脆弱性の情報を
提供してくれるベンダを選定するようにしましょう！

導入する際にやるべきこと

ガイドラインや社内のセキュリティルールを参照した上で、
機器の管理をしているセキュリティ担当部門と相談して
安全な環境に導入できるようにしましょう！

運用する際に確認すべきこと

社内のセキュリティルールによって運用方法が
決まっていることが多いためルールを確認しましょう！
ルールと併せてガイドラインなど公開されてる資料を
参照し適切に機器の管理をしましょう！

廃棄する際にやるべきこと

IoT機器に保存されている機密情報やプライバシー情報は
消去して廃棄しましょう！
廃棄時やリユース時に情報漏洩が起こる可能性があります！

用語集

脆　弱　性

プログラムの不具合や設計上のミスが原因となって
発生した情報セキュリティ上の欠陥のこと
セキュリティホールとも呼ばれる

ＤＸ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｆｏｒｍａｔｉｏｎ）

デジタル技術で企業の業務を改革し優位性を確立すること

マルウェア

悪意のあるソフトウェアという意味であり、コンピューター
ウイルスのこと

暗号化規格

データが第三者に漏れないようにするための技術であり
WEP、WPA、WPA2、WPA3などが存在する
※WEP、WPAは脆弱なため、現在ほぼ利用されていない

踏　み　台

攻撃者が特定機器を乗っ取りその機器を起点に攻撃を
仕掛ける手法

ＤＤｏＳ攻撃

ウイルス感染させた端末同士でネットワークを形成し
ネットワークやシステムに過剰な負荷をかける手法

ＣＣＤＳ

一般社団法人重要生活機器連携セキュリティ協議会

ＮＡＳ（Ｎｅｔｗｏｒｋ　Ａｔｔａｃｈｅｄ　Ｓｔｏｒａｇｅ）

ネットワーク上に接続できるハードディスクのこと

ＲＴＳＰポート

Real Time Streaming Protocol
WEBカメラなどにあるポートでクライアントとサーバの間
で再生したい動画や音声の所在情報の伝達や、再生の開始・
停止などを制御する通信ポートのこと

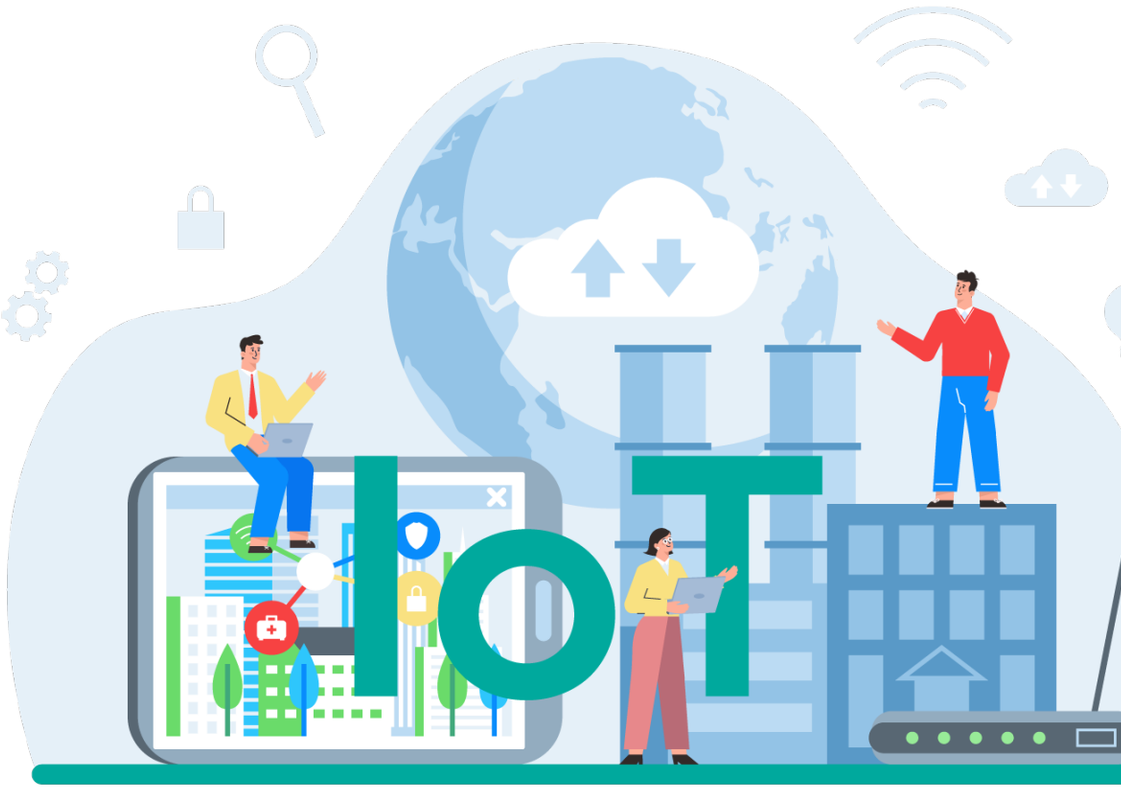
謝辞

本書をまとめるにあたっては、多くの方々にお世話になりました。
以下に感謝の意を示します。
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中核人材育成プログラム第5期受講者の皆様に感謝いたします。
皆様から多数のご意見や多彩なアイディア、参考文献などをご教授いただいたことにより、本冊子を作成することができました。心より感謝申し上げます。

【監修】
IPA産業サイバーセキュリティセンター
中核人材育成プログラム講師
満永　拓邦　　門林　雄基

【制作】
IPA産業サイバーセキュリティセンター
中核人材育成プログラム第5期受講者
IoT Sec for Users
川口　翔太郎　　牧野　祐基
赤木　駿一　　木村　太祐
佐藤　幸太　　杉浦　良祐
林　拓雅　　宮澤　文隆

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（ICSCoE）



5分でIoTのセキュリティリスクがわかる本
初版発行 2022年6月

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（ICSCoE）
IoT Sec for Users