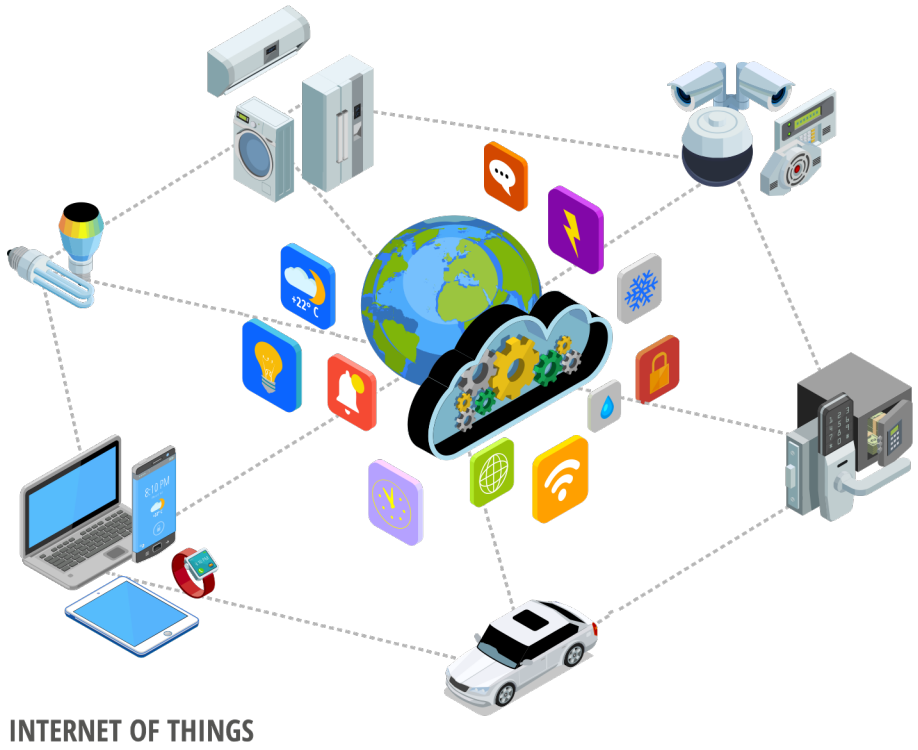
IoTセキュリティ教育資料

情報処理推進機構
産業サイバーセキュリティセンター5期
「初めてのセキュリティ塾」プロジェクト

本書の目的と対象読者

IoT機器のセキュリティリスクを理解する



IoT機器のセキュリティリスクを、企業でIoT機器の導入を検討中、または利用中の方に認識していただくことを目的としています。

第1章　IoTについて

1.1 IoTの定義

本書では”ネットワークに接続されているモノ”をIoTと定義します

IoT とは”Internet of Things”の略称であり
”モノ”がネットワークに繋がることを意味します。

参考｜IoT機器の一例

ハンディターミナル

スマートスピーカー

スマートグラス

プリンタ

ドローン

Webカメラ

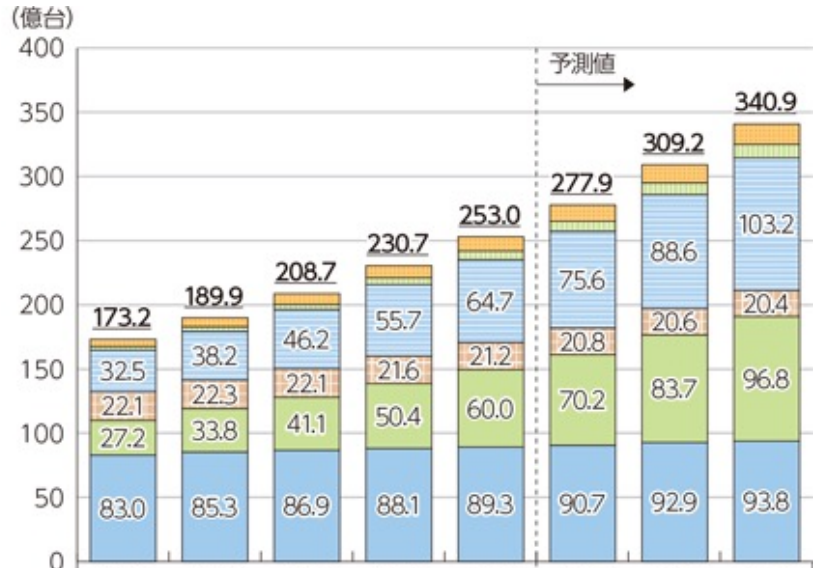
自動車

1.2 IoT機器の急速な普及

世界中の様々なモノがネットワークに繋がりその数は増加しています

パソコンやスマートフォンなど、
従来のインターネット接続端末に加え、
家電や医療機器、自動車など、
世界中の様々なモノがネットワークに
繋がるようになっています。

IoT機器は比較的安価で購入できるため、
急速に普及が進んでいます。



	2016	2017	2018	2019	2020	2021	2022	2023
合計	173.2	189.9	208.7	230.7	253.0	277.9	309.2	340.9
自動車・宇宙航空	5.7	7.1	8.5	9.8	11.3	12.7	14.2	15.7
医療	2.6	3.3	4.0	5.1	6.5	7.8	9.2	10.9
産業用途	32.5	38.2	46.2	55.7	64.7	75.6	88.6	103.2
コンピューター	22.1	22.3	22.1	21.6	21.2	20.8	20.6	20.4
コンシューマー	27.2	33.8	41.1	50.4	60.0	70.2	83.7	96.8
通信	83.0	85.3	86.9	88.1	89.3	90.7	92.9	93.8

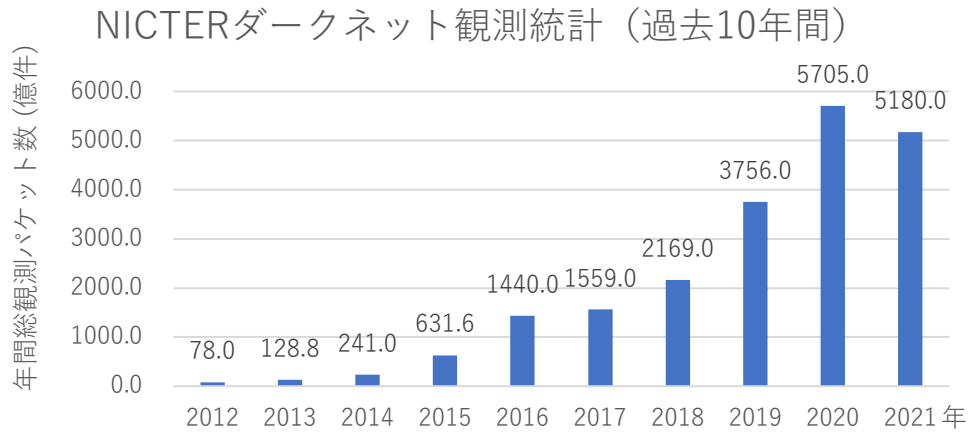
【参考URL】
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html

第2章　IoTセキュリティ

2.1 IoTのセキュリティ脅威

IoT機器を狙った攻撃は多い

NICT（国立研究開発法人情報通信研究機構）によるとサイバー攻撃は依然増加傾向にあり、2021年には5,180億回の攻撃がありました。
右のグラフに示されているとおり18.3%がIoT機器を狙った攻撃と言われています。
この状況を踏まえると、IoT機器のセキュリティは重要であると言えます。



【参考URL】
https://www.nict.go.jp/press/2022/02/10-1.html

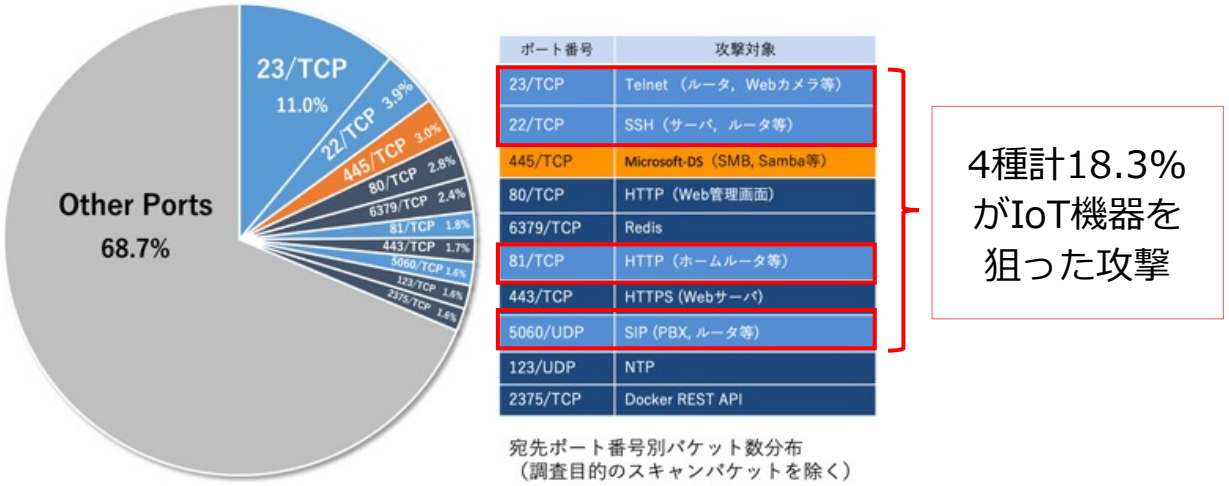
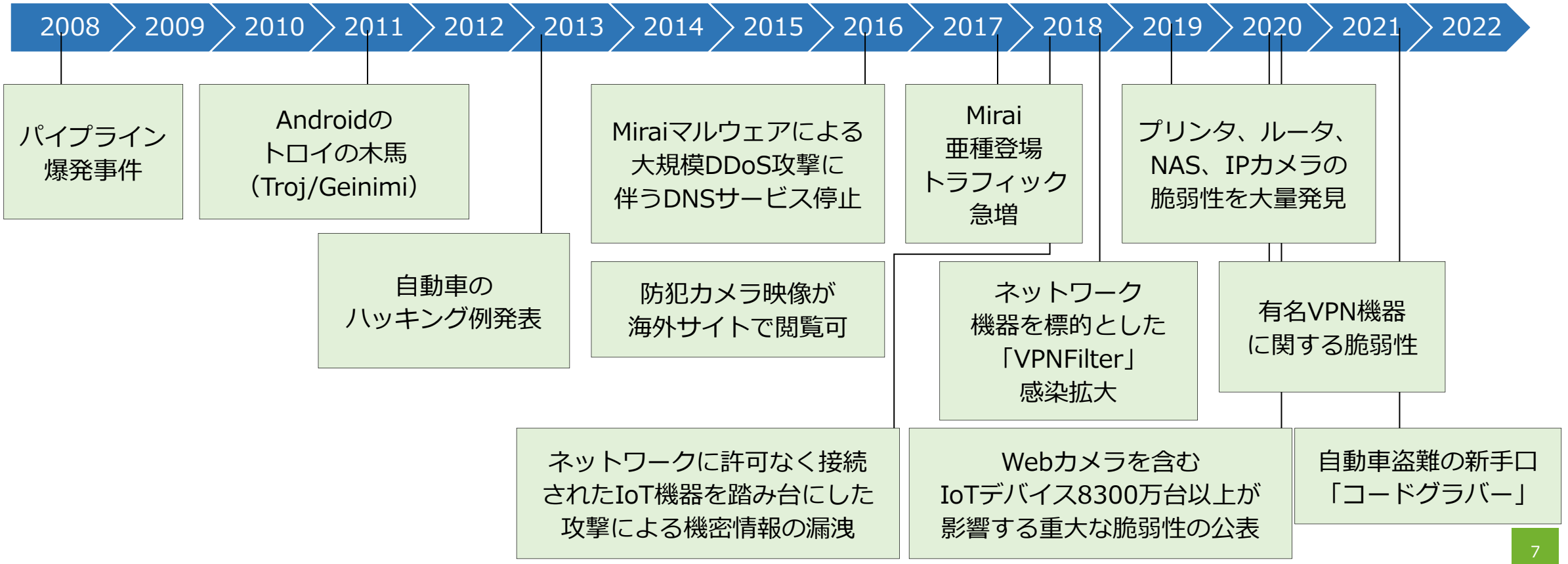


図. 宛先ポート番号別パケット数分布（調査目的のスキャンパケットを除く）
注: 2位の22/TCPには、一般的なサーバ（認証サーバなど）へのスキャンパケットも含まれます。
また、その他のポート番号（Other Ports）の中にはIoT機器を狙ったパケットが多数含まれます。

2.2 事例紹介

IoT機器を悪用したセキュリティインシデントは多数ある

IoT機器に関連したセキュリティインシデントやニュース



2.2 事例紹介①

2008年 トルコのパイプライン爆発事故

2008年8月5日 午後11時頃にパイプラインが爆発。
攻撃者は監視カメラの通信ソフトの脆弱性を利用して
内部ネットワークに侵入したと報道されています。
さらに、警報装置を停止させ、パイプライン内の原油の圧力
を異常に高めて爆発を引き起こしました。
鎮火と復旧には３週間もかかり、巨額の損失を被りました。

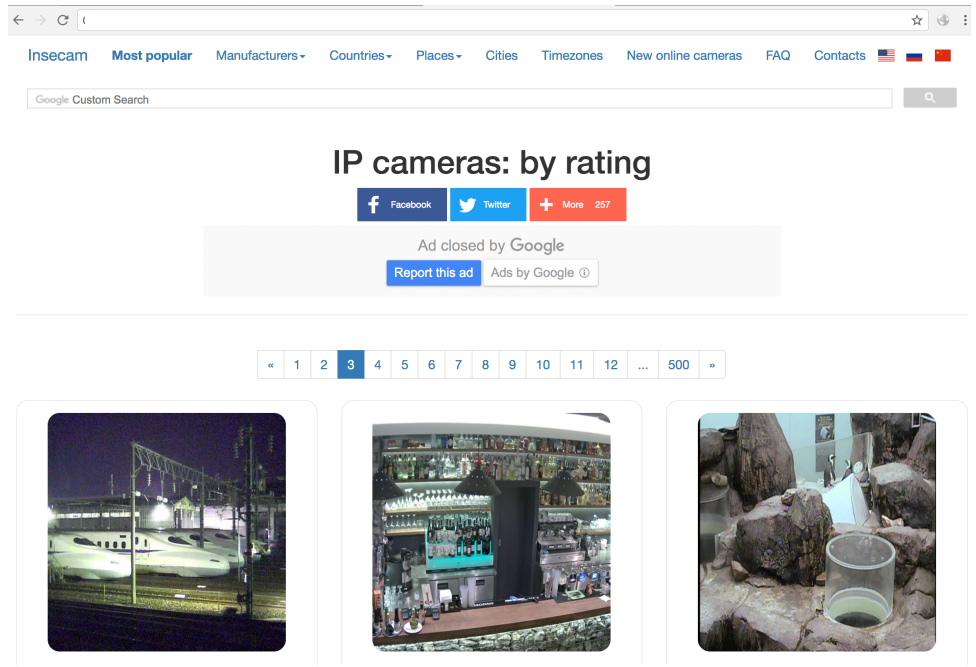
【参考URL】
https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html
https://time-space.kddi.com/digicul-column/world/20160715/
https://www.ipa.go.jp/files/000057714.pdf

2.2 事例紹介②

Webカメラの映像漏洩

Webカメラの認証設定を行わず
安易に設置すると意図せずインターネット上で
その映像が公開されてしまうケースがあります。

また、Webカメラの管理画面にログインするための
デフォルトのユーザ・パスワード情報は
インターネット上のマニュアルで公開されている
ことがあります。
攻撃者は公開情報を悪用し、様々な攻撃を試みます。



2.2 事例紹介③

2016年 DNSサービスに大規模DDoS攻撃

IoT機器を踏み台にした攻撃もあり、組織が被害者だけでなく加害者になる可能性もあります。
2016年にDNSサービスを提供する企業が大規模なDDoS（分散型サービス拒否）攻撃を受けました。
攻撃者はデフォルトのユーザ・パスワードのIoT機器約10万台をマルウェアに感染させて、DNSサーバに大量のデータを送信させました。
その結果サーバはダウンし、DNSサービスは停止。
サービスを利用していた世界各国の様々な大手企業がアクセス障害に陥りました。

Home > Cybercrime > Major DDoS Attacks Signal Need for Strengthened Cyber Defenses

Major DDoS Attacks Signal Need for Strengthened Cyber Defenses

By Daniel Leslie (CA) on November 3, 2016
Posted in Compliance and risk management, Cybercrime

On Friday, October 21, a series of Distributed Denial of Service (DDoS) attacks were launched against the servers of Dyn, a major DNS host. DNS hosts operate in a manner akin to a switchboard for the Internet, helping to route domain names (e.g., dataprotection-report.com) to underlying IP addresses (e.g., 104.28.6.115). By attacking Dyn, hackers were able to prevent end-users from reaching the websites and online services that relied on Dyn, including Netflix, Twitter, Spotify, SoundCloud, Amazon, AirBnB, Reddit, PayPal, Pinterest, CNN, Fox News, the Guardian, the New York Times, and the Wall Street Journal. In a statement, Dyn described the attack as “a sophisticated, highly distributed attack involving 10s of millions of IP addresses.”

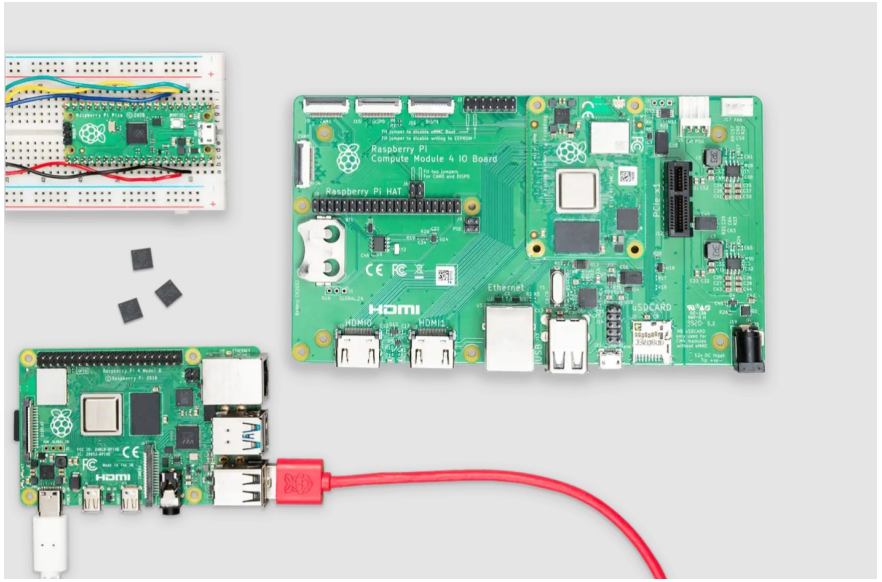
【参考URL】
https://www.dataprotectionreport.com/2016/11/major-ddos-attacks-signal-need-for-strengthened-cyber-defenses/
https://xtech.nikkei.com/it/atcl/news/16/102203079/
https://www.jpcert.or.jp/magazine/chronology/

2.2 事例紹介④

IoT機器を踏み台に利用した情報窃取

2018年にアメリカの研究所で、組織ネットワークに許可なく接続された小型コンピュータRaspberry Pi（右図）を踏み台にした攻撃が起きました。

攻撃者はネットワークに侵入後、様々な機密情報を窃取しました。さらに、この攻撃は気づかれることなく10ヵ月も続きました。



【参考画像】
https://www.raspberrypi.com/

【参考URL】
https://www.trendmicro.com/jp/iot-security/news/3723
https://www.nedo.go.jp/content/100904087.pdf
https://oig.nasa.gov/docs/IG-19-022.pdf

2.2 IoTが狙われる理由

IoT機器は管理が不十分

なぜIoTは狙われる？
PCやサーバに比べて管理や監視が行き届きにくく、
セキュリティ意識も低くなりやすい（デフォルトパスワードによる運用等）ためです。

このようにIoT機器はPCやサーバに比べて脆弱で、サイバー攻撃の被害を受けていても気付きにくいので、攻撃者にとって格好の標的となっています。

2.3 IoTセキュリティ対策

最低限のセキュリティ対策は初期パスワード変更と資産管理

初期パスワードを変更する

製品の初期パスワードがメーカのサイト上に公開されていることもあります。
変更せずに利用すると容易に第三者が不正にアクセス出来るため危険です。
初期パスワードを悪用して感染を広げるマルウエアもあるため変更は必須と言えるでしょう。

IoT資産も資産管理対象とする

IoT機器が資産管理対象に含まれていないケースがあります。
そのため、管理が不十分で攻撃をされてもすぐに気づけない危険性があります。

※今回は事例と関連する重要な上記2点にフォーカスしましたが、上記以外のセキュリティ対策は、
4.2 IoTセキュリティガイドラインを参照してください。

第3章　終わりに

3.1 終わりに

IoTを導入する際は、セキュリティを意識しよう

IoT機器は手軽に購入・設置が出来て便利な反面、多くの脆弱性など
セキュリティリスクが潜んでいます。そのため、攻撃者にとっては格好の攻撃
対象であることを理解しておくことが大切です。

IoT機器を利用する際は、予め社内規定を確認し、セキュリティ部署に相談
するなど、セキュリティに配慮することが重要です。

3.2 主なIoTセキュリティガイドライン

IoT推進コンソーシアム　総務省　経済産業省／IoT セキュリティガイドライン ver 1.0
https://www.soumu.go.jp/main_content/000428393.pdf

JPCERT/CC IoT　セキュリティチェックリスト
https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

一般社団法人　重要生活機器連携セキュリティ協議会
IoT機器セキュリティ要件ガイドライン2021年版_ver2.0
https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021_v2.0_jpn.pdf

IPA IoTのセキュリティ
https://www.ipa.go.jp/security/iot/index.html

米標準技術研究所（NIST）：NISTIR 8200 （Draft） Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things （IoT）
https://csrc.nist.gov/publications/detail/nistir/8200/archive/2018-02-14

欧州サイバーセキュリティ機関（ENISA）：Baseline Security Recommendations for IoT
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot