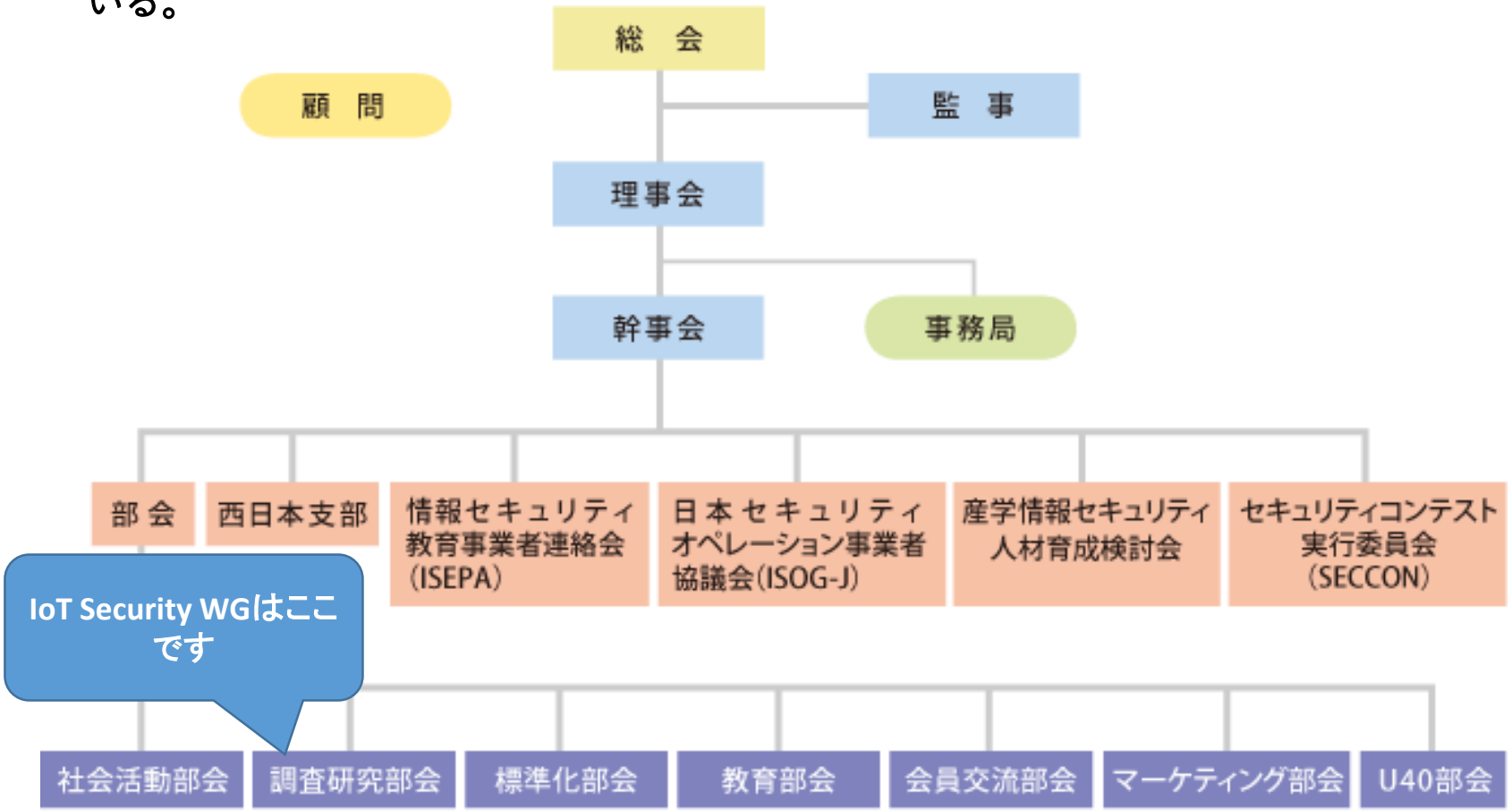
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

IoTセキュリティ早引きガイド解説

IoT Security WG リーダー
松岡正人@株式会社

JNSAとは？　組織と活動

- ネットワークのセキュリティに関する技術の向上、標準化の推進、一般社会への啓発などについて、社会活動、調査研究、標準化、教育などの各部会が活動を行っている。



部会・支部等はさらに各WGに分かれて活動しています。

IoT Security Working Groupの活動

- 2014/4 発足
- 目的は、IoTの市場調査・アーキテクチャとセキュリティ範囲検討・脅威の洗い出しと調査・調査報告書の取りまとめ
- 市場調査：あまりにも広大なため、終りのない旅に…
- アーキテクチャとセキュリティ範囲：先達の成果物を参照（IoT-A Project, IPA, ISACA, OWASP・・・）
- 脅威の洗い出しと調査
- Raspberry Pi の実装実験
- ガイド作成、2016/6 公開

http://www.jnsa.org/result/iot/

「コンシューマ向け IoT セキュリティガイド」解説

みたいなことを昨年お話ししました

世の中にたくさんガイドが登場しました！

No	組織	名称
1	DHS	STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS
2.1	ENISA	Security and Resilience of Smart Home Environments
2.2	ENISA	Security and Resilience of Intelligent Public Transport. Good practices and recommendations
2.3	ENISA	Cyber security for Smart Cities
2.4	ENISA	Cyber security and resilience for Smart Hospitals
2.5	ENISA	Securing Smart Airports
2.6	ENISA	Cyber Security and Resilience of smart cars
2.7	ENISA	Baseline Security Recommendations for IoT
3	FTC	Internet of things Privacy & Security in a Connected World FTC Staff Report JAN 2015
4	IETF	Best Current Practices for Securing Internet of Things (IoT) Devices
5	IIC	Industrial Internet Security Framework
6	IoT推進コンソーシアム	IoTセキュリティガイドライン
7.1	IPA	ＩｏＴ開発におけるセキュリティ設計の手引き
7.2	IPA	つながる世界の開発指針
7.3	IPA	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
8	ISACA	INTERNET OF THINGS：RISK AND VALUE CONSIDERATIONS
9	OWASP	OWASP IoT Security Guidance

ボリュームもいっぱいです…

JNSA

ページ数	組織	名称
17ページ	DHS	STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS
77ページ	ENISA	Security and Resilience of Smart Home Environments
68ページ	ENISA	Security and Resilience of Intelligent Public Transport. Good practices and recommendations
54ページ	ENISA	Cyber security for Smart Cities
56ページ	ENISA	Cyber security and resilience for Smart Hospitals
84ページ	ENISA	
84ページ	ENISA	
103ページ	ENISA	
71ページ	FTC	Report JAN 2015
13ページ	IETF	Best Current Practices for Securing Internet of Things (IoT) Devices
173ページ	IIC	Industrial Internet Security Framework
61ページ	IoT推進コンソーシアム	IoTセキュリティガイドライン
100ページ	IPA	ＩｏＴ開発におけるセキュリティ設計の手引き
109ページ	IPA	つながる世界の開発指針
40ページ	IPA	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
13ページ	ISACA	INTERNET OF THINGS：RISK AND VALUE CONSIDERATIONS
ウェブ1ページ	OWASP	OWASP IoT Security Guidaance

合計 1124ページ

どうしてガイドを作ろうと考えたか？

- このWGでガイド作るとかいうのはもう無理
- もういろいろ世の中進んできた
- NISTもENISAもがっつり作り始めた
- 国内も出てきた（IPAとか）

読み解くのが追いついていない！

手分けして、読み込んで共有

- たくさんある英文や日本語の文書を手分けして読むことに
- 読み解く中で、いろいろ違いがあるのが見えてきた
- これをどうまとめるのがみんなの役に立つのか

それぞれの紹介文を作ろう！

手分けして、読み込んで共有

- たくさんある英文や日本語の文書を手分けして読むことに
- 読み解く中で、いろいろ違いがあるのが見えてきた
- これをどうまとめるのがみんなの役に立つのか

それぞれの紹介文を作ろう！

現在作業中！

- 読み解いたものを共通のフォーマットでとりあえずまとめてみる
- 文書の特徴をハイライトできれば、必要な文書を選択できる
- 世界のIoTセキュリティがどうなっていくのか

全部読まなくてもいいように！

はじめに

JNSA IoT Security WG は、2014年の発足当時から IoTセキュリティの指針、標準や規格などについて調査をおこなっており、調査から得た知見を元に、もっともセキュリティの課題が大きいと思われたコンシューマIoT向けの提言をまとめたレポートを2016年に発行しました。

その後コンシューマのみならず多くの業種や産業向けのIoTセキュリティについて関係者によって整理され、様々な組織から指針や標準が発行されました。

しかし、発行された指針や標準があまりにも多すぎるため、それらの文書を読み解くのに多くの時間を割かなければならないというジレンマが生まれるに至りました。

そこで、本ハンドブックを発行することで、主要な発行済み文書の目的や主たる読者、特徴などをまとめることで情報を整理するための時間を節約することができると考えました。

作成者一同、このハンドブックがみなさんのビジネスのお役に立てることを願っています。

JNSA IoT Security WG メンバー一同

1

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS

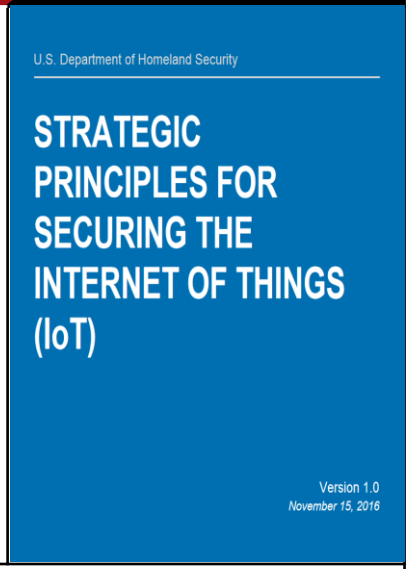
IoTの安全性確保のための戦略的原則

STRATEIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS
IoTの安全性確保のための戦略的原則

発行	2016年01月13日

Internet of Things（IoT）を構成するネットワーク接続されたデバイス、システム、およびサービスの成長は、私たちの社会に大きなチャンスと利益をもたらします。しかし、IoTのセキュリティは、急速な技術革新と展開に追いついておらず、実質的な安全性と経済的リスクをもたらしています。

このドキュメントでは、これらのリスクについて説明し、設計、製造、所有、運用するデバイスおよびシステムビジネスの責任あるレベルに向けて構築するための、拘束力のない原則と推奨されるベストプラクティスを提供します。



参考別紙	なし
Topic	U.S. Department of Homeland Security (DHS)
URL	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

「IoTの安全性確保のための戦略的原則」レポートの項目

IoT開発、展開、利用に関わるプレイヤーにデザインから販売後の製品の破棄にわたるまで、セキュリティを担保するために守るべき原則を挙げて、守るように呼びかけている

No	項目	概要	Page
1	**INTRODUCTION AND OVERVIEW**	IoTの概要・状況について説明し、セキュリティ確保のための原則の概要、本文書の**適用対象**の説明をしています。	02~04 (3P)
2	**STRATEGIC PRINCIPLES FOR SECURING IOT**	IoTの設計、製造、展開の全範囲にわたってセキュリティを向上させるための**6つの戦略原則**と関連するプラクティスの説明をしています。	05~17 (13P)
3	**CONCLUSION**	6つの原則を基にセキュリティを推進することを推奨するとともにIoTセキュリティの強化のためのさらなるステップとして政府と産業間で取り組まなければならない**4つの努力**を挙げている	13~14 (2P)
	APPENDIX: GUIDANCE AND ADDITIONAL RESOURCES	原則を作成するにあたって参考とした文書(特にNTIAとNIST)を挙げている。	14~17(4P)

2.1

Security and Resilience of Smart Home Environments

スマートホーム環境のセキュリティとレジリエンス

Security and Resilience of Smart Home Environments
スマートホーム環境のセキュリティとレジリエンス

発行	**2015年12月01日**

製品ライフサイクルのあらゆる段階に適用されるグッドプラクティス、すなわちスマートホーム環境の実装から廃棄までにおいて、サイバー脅威からスマートホーム環境を保護することを目的とした内容を記載したもの。

本レポートでは、さまざまな種類のデバイスに対するセキュリティ対策の適用の必要性が強調されている。

グッドプラクティスは、製造元、ベンダー、ハードウェアとソフトウェアのソリューションプロバイダ、および開発者に適用される。欧州市民、標準化団体、研究者、政策立案者にも役立つとされている。
このグッドプラクティスは、現在のセキュリティレベルを評価し、新しいセキュリティ対策の実装を評価するためにも使用できるとされている。

参考別紙	なし
Topic	IoT and Smart Infrastructures：Smart Homes
URL	https://www.enisa.europa.eu/publications/security-resilience-good-practices

2.2

Security and Resilience of Intelligent Public Transport. Good practices and recommendations

インテリジェントな公共交通機関のサイバーセキュリティとレジリエンス：優れた実践と推奨事項

Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations
インテリジェントな公共交通機関のサイバーセキュリティとレジリエンス：優れた実践と推奨事項

発行	**2016年01月12日**
本レポートは、セクター、地方自治体、事業者、製造業者、政策立案者からの専門家へのアンケート調査およびインタビューに基づきまとめられている。 レポートでは、公共交通機関における重要な資産を保護し、IPT(インテリジェント・パブリック・トランスポート：インテリジェントな公共交通機関)システムのセキュリティを確保するために配備できる既存のセキュリティ対策（優良事例） を基にした、**IPTシステムの重要な資産を防御する実際的なアプローチを提案している。**	
参考別紙	なし
Topic	IoT and Smart Infrastructures：Smart Cities
URL	https://www.enisa.europa.eu/publications/good-practices-recommendations

2.3

Cyber security for Smart Cities

スマートシティのサイバーセキュリティ

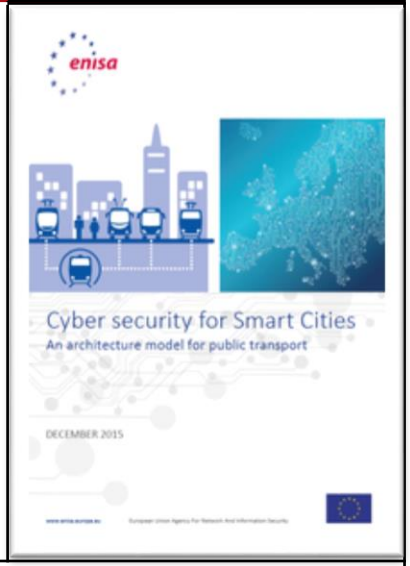
Cyber security for Smart Cities
スマートシティのサイバーセキュリティ

発行	2016年01月12日

本研究の主な目的は、SC(スマートシティ)における運輸部門のアーキテクチャをモデル化し、IPT(Intelligent public transport)オペレータのサイバーセキュリティのグッドプラクティスを明確にすることとされている。

グッドプラクティスは、異なる都市と成熟度で比較出来ようにされており、事業者と地方自治体の代表者は、サイバーセキュリティに関して同じ成熟度を持つ他の都市に遅れをとっているかどうかを迅速に評価し、そうであれば適切な措置を講じることが出来るとされている。

この調査は主に実践的なガイダンスの提供に重点を置いている。



参考別紙	なし
Topic	IoT and Smart Infrastructures：Smart Cities
URL	https://www.enisa.europa.eu/publications/smart-cities-architecture-model

2.4

Cyber security and Resilience for Smart Hospitals

スマート病院のサイバーセキュリティとレジリエンス

Cyber security and resilience for Smart Hospitals
スマート病院のサイバーセキュリティとレジリエンス

発行	2016年11月24日

この調査報告書は、病院の情報セキュリティの役員および業界が、スマート病院における情報セキュリティのレベルを高めるための重要な推奨事項を提案している。

スマート病院の環境とその具体的な利用目的を特定し、IoTコンポーネントが医療機関を支援する場合の、資産と関連する脅威を特定している。

文書および経験的データの分析、およびスマート病院に特に関連する攻撃シナリオの調査を行い、サイバー攻撃に有効な緩和手法やグッドプラクティスを示している。

参考別紙	なし
Topic	Critical Infrastructures and Services：Health IoT and Smart Infrastructures：Smart Cities
URL	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

2.5

Securing Smart Airports

スマート空港の確保

Securing Smart Airports
スマート空港の確保

発行	2016年12月16日

スマートな空港が直面する新たな脅威に対応するため、このレポートは空港の意思決定者（CISO、CIO、ITディレクターおよび操縦士）および空港情報セキュリティ専門家のためのガイドを提供している。

このレポートでは、サイバーセキュリティの既存の知識や実態の調査と、専門家との検証インタビューに基づいて、スマートな空港の重要な資産が特定されている。

これらの調査や分析に基づいて、**スマートコンポーネントの脆弱性を中心に詳細な分析と脅威のマッピングが行われている。**

参考別紙	Good practices mind map Smart Airports asset groups and assets Threat Taxonomy Simple Threat Taxonomy
Topic	IoT and Smart Infrastructures : Smart Cities Critical Infrastructures and Services IoT and Smart Infrastructures : Smart Airports
URL	https://www.enisa.europa.eu/publications/securing-smart-airports

2.6

Cyber Security and Resilience of smart cars

スマートカーのサイバーセキュリティとレジリエンス

Cyber Security and Resilience of smart cars
スマートカーのサイバーセキュリティとレジリエンス

発行	2017年01月13日

この報告書は、スマートカーの安全性が社会の安全性を保証するという特殊性を意識し、サイバー脅威に対するスマートカーの安全性を保証するためのグッドプラクティスを特定することを目的に調査・作成されたもの。

この調査報告には、スマートカーに存在する機密性の高い資産、対応する脅威、リスク、緩和要因、実装可能なセキュリティ対策を記載している。

本報告書では、スマートカーに関連する分野の専門家に連絡を取り、ノウハウと専門知識を収集している。 これらの情報交換により、ポリシーと標準、組織的対策、セキュリティ機能の三つの優良事例につながったと記載されている。

参考別紙	なし
Topic	IoT and Smart Infrastructures : Smart Cars
URL	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

2.7

Baseline Security Recommendations for IoT

IoTのベースラインセキュリティの推奨事項

Baseline Security Recommendations for IoT
IoTのベースラインセキュリティの推奨事項

発行	**2017年11月20日**

ヨーロッパにおけるIoTセキュリティのためのベースラインを設定することを目指した文書。

この分野におけるベースラインとなり、今後のイニシアチブおよび開発のための基盤となることが示されている。

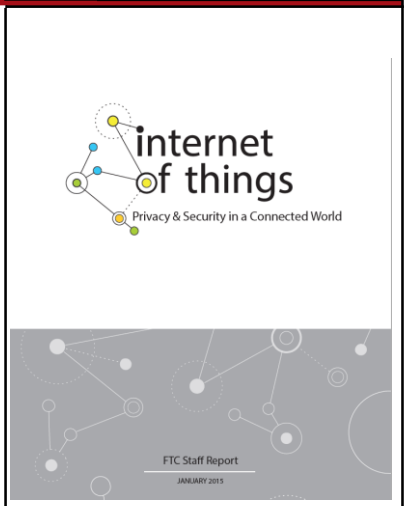
これまでの調査資料の集大成ともいえる資料であり、現時点では、ENISAのIoTに関するガイド文書として、最初に読むべき文献と言える。

参考別紙	なし
Topic	IoT and Smart Infrastructures
URL	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

3

Internet of things Privacy & Security in a Connected World
FTC Staff Report
JANUARY 2015

米国FTC(連邦取引委員会)のIoTに関する報告

発行	2015年
ここでは「IoTでのプライバシー問題」を中心とした法制化への議論（パネリストによる議論）がなされている （IoTの機器が増え、個人はプライバシーを求めている） ・ 個々の議論にはIoT化へのヒントになる話が含まれる ・「家、車、ウエアラブル」はまだチャレンジ段階 ・IoTは仮想と物理の融合が進むが、現状での把握は難しい ・委員会はセキュリティとプライバシーの法制化を進めるが、自主規制の努力も同時に進める	
参考別紙	なし
Topic	IoT Privacy & Security
URL	https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

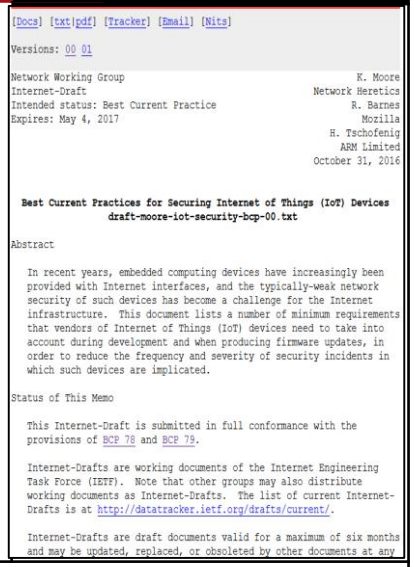
4

Best Current Practices for Securing Internet of Things (IoT) Devices

IoTの安全性確保のためのベストプラクティクス Best Current Practices for Securing Internet of Things (IoT) Devices

発行	2016年10月31日

近年、組み込みコンピューティングデバイスはますますインターネットインターフェースを提供されており、そのようなデバイスの典型的に弱いネットワークセキュリティは、インターネットインフラストラクチャの課題となっている。 この文書は、IoT（Internet of Things）デバイスのベンダーが、開発中およびファームウェアアップデートを作成する際に、そのようなデバイスが関与するセキュリティインシデントの頻度と重大度を減らすために考慮する必要のある**最小限の要件**を列挙しています。



[Docs] [txt|pdf] [Tracker] [Email] [Nits]

Versions: 00 01

Network Working Group — K. Moore
Internet-Draft — Network Heretics
Intended status: Best Current Practice — R. Barnes
Expires: May 4, 2017 — Mozilla
H. Tschofenig
ARM Limited
October 31, 2016

Best Current Practices for Securing Internet of Things (IoT) Devices
draft-moore-iot-security-bcp-00.txt

Abstract

In recent years, embedded computing devices have increasingly been provided with Internet interfaces, and the typically-weak network security of such devices has become a challenge for the Internet infrastructure. This document lists a number of minimum requirements that vendors of Internet of Things (IoT) devices need to take into account during development and when producing firmware updates, in order to reduce the frequency and severity of security incidents in which such devices are implicated.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any

参考別紙	なし
Topic	Network Working Group
URL	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

5

Industrial Internet Security Framework

インダストリー インターネット セキュリティ フレームワーク

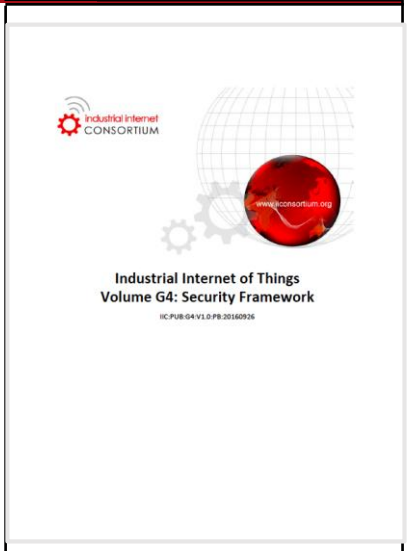
Industrial Internet Security Framework（IISF）

Industry（産業）の種別を問わず、IoTセキュリティの考え方をまとめた文書がIISFであ

Industrial Internet Security Framework
インダストリアルインターネット セキュリティフレームワーク

発行	**2016年9月26日**

産業界毎に異なるセキュリティ要件を包括的にとらえた文書。
クラウドから通信経路、プロトコル、組み込み機器から管理・運用、プライバシーや安全のための規格まで、IoTを構成する様々な要素のみならず、サプライチェーンまでも網羅している。
想定すべきリスクと対策の概論が記載されているが、実用的なものではなく、IISFに基づいた現実的なセキュリティシステムの構築と検証はテストベッドと呼ばれる実証試験の中で個別具体的に行われている。テストベッドの結果についての概要は公開されているが、すぐにつかえる情報はメンバーのみの公開となっている。



参考別紙	Industrial Internet Reference Architecture http://www.iiconsortium.org/IIRA.htm
Topic	IoT セキュリティ関連のアーキテクチャ、設計、技術、トラストワージーに適切な手順
URL	http://www.iiconsortium.org/IISF.htm

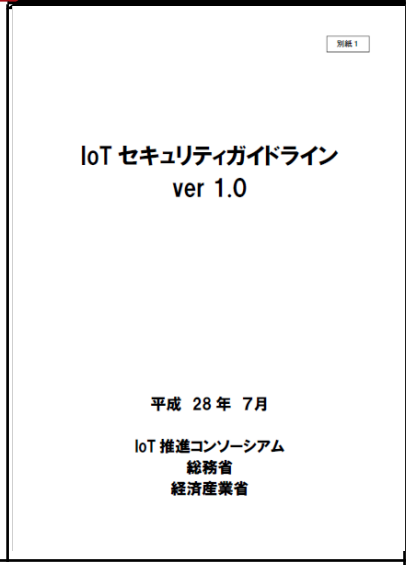
6

IoT セキュリティガイドライン

IoTセキュリティガイドライン

発行	IoT セキュリティガイドライン（2016年07月05日初版）

この文書は、ＩｏＴライフサイクルを「方針」、「分析」、「設計」、「構築・接続」、「運用・保守」の5段階に分け、合計21の要点でガイドラインにまとめています。内、14項目は「つながる世界の開発指針」を流用しています。
ＩｏＴ推進コンソーシアムは2015年10月に総務省、経産省主導で設立されました。全てのＩｏＴサービス関係者を対象読者とした文章となっています。
一律に具体的なセキュリティ対策の実施を求めるのではなく、対象者の役割・立場に応じて適切なセキュリティ対策の検討することが期待されています。
また、一般利用者のための4つのルールが提示されています。


別紙1

IoT セキュリティガイドライン
ver 1.0

平成 28 年 7月

IoT 推進コンソーシアム
総務省
経済産業省

発行者	ＩｏＴ推進コンソーシアム
参考別紙	なし
URL	http://www.iotac.jp/wg/security/

7.1

ＩｏＴ開発における
セキュリティ設計の手引き

IoT開発におけるセキュリティ設計の手引き

発行	2016年05月12日
この文書は、IoT開発においてセキュリティ設計を担当する開発者向けの手引きとなっています。 文書では、IoTのセキュリティ設計において行う、脅威分析・対策検討・脆弱性の対応方法の進め方について、デジタルテレビ、ヘルスケア機器、スマートハウス、コネクテッドカーを例に具体的に解説しています。 セキュリティ対策がOWASP・OTAなど海外の代表的なIoT関連のセキュリティガイドとの対応付けられており、客観性がある資料となっています。 付録Cの IoTにおける暗号技術利用リストでは、IoTシステムにおける最低限の利用・運用の方針を明示しています（IoTシステムでは実装が困難なことを考慮し、ITシステムより緩やかな目標となっています）。	
発行者	独立行政法人情報処理推進機構（IPA）　セキュリティセンター
参考別紙	なし
URL	https://www.ipa.go.jp/security/iot/iotguide.html

7.2

つながる世界の開発指針

つながる世界の開発指針

発行	2017年6月30日第2版（2016年03月24日初版）

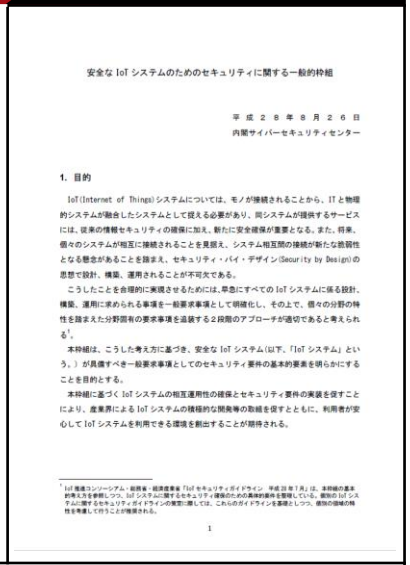
この文書は、安全安心なIoTの実現のために開発者に認識してほしい重要ポイントを17の指針でまとめている国内初のIoT製品に関する開発指針です。
安全安心の概念として、セーフティ、セキュリティのほか、リライアビリティ（ユーザが利用したいときに機能を利用でき、他システムと適切な連携を行ない、悪影響を与えないこと）が含まれています。
製品やシステム開発時のチェックリストとしての利用を想定（受発注の要件確認に活用することも想定）しています。
開発指針の前段として、リスク想定の進め方について詳しく言及されています。
第2版では利用時の品質の視点で、記載内容がアップデートされています。

発行者	独立行政法人情報処理推進機構（IPA）　ソフトウェア高信頼化センター
参考別紙	なし
URL	http://www.ipa.go.jp/sec/reports/20160324.html

7.3

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

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

発行	2016年08月26日
この文書は、安全なIoTシステムが具備すべき一般的要求事項としてのセキュリティ要件の基本要素を明らかにすることを目的としています。 文書では、IoTシステムをIoTシステムの集合体“System of Systems(SoS)”として捉え、IoTセキュリティとして、安全性、機密性、完全性、可用性の4要件を確保することを前提として定義しています。 その上で、IoTセキュリティを確保するためのIoTシステムの設計・構築・運用の基本原則として、以下の2つを挙げています。 ・セキュリティ・バイ・デザインによりセキュリティを事前に考慮 ・セキュリティの確保を稼動前に検証できる仕組みの構築	
発行者	内閣サイバーセキュリティセンター（NISC）
参考別紙	なし
URL	https://www.nisc.go.jp/active/kihon/res_iot_fw2016.html

8

INTERNET OF THINGS : RISK AND VALUE CONSIDERATIONS

モノのインターネット：リスクと価値の考察

INTERNET OF THINGS : RISK AND VALUE CONSIDERATIONS

ISACAでは、IoTを利用してビジネス価値を得るためにリスクをいかにコントロールするかという視点で整理したホワイトペーパーを発行しています。

INTERNET OF THINGS：RISK AND VALUE CONSIDERATIONS
モノのインターネット：リスクと価値の考察

発行	**2015年1月27日**
Internet of Things（IoT）革命は、驚異的な変革をもたらす可能性があり、同時にビジネスに大きな混乱を招く可能性があり、IoTを利用することによってビジネス価値と組織の競争力を導き出すことができる。**しかし、IoTは、ビジネスに付加価値を与えると同時に、新たなリスクをももたらすため、**(アシュアランス、セキュリティ、リスク)専門家は、組織のリスクを再定義する必要があることが記載されている。 このホワイトペーパーでは、**Internet of Things（IoT）に取り組む組織が考慮するべき9つの重要な事項を、「９つの質問」として提示している。**	
参考別紙	なし
Topic	IoT Risk and Value
URL	https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx

9

OWASP
IoT Security Guidance

OWASP IoT Security Guidance

発行	2017年02月14日

IoTのセキュリティに関連して、製造者（Manufacturer）、開発者(Developer)、消費者(Consumer)の対象者別に作成されたセキュリティガイダンスから構成される。これらはそれぞれの視点から考慮しなければならない基本的なガイドラインの集合を提供する。製造者に対してはより安全な製品を製造することを、開発者がより安全なアプリケーションを構築することを、消費者がより安全な商品を購入することを助けることが目的である。

これらは考慮しなければならないことの包括的なリストではなく、そのように取り扱ってはならない。

しかし、これらの基本的な点を確認しておくことで、IoTのセキュリティを強化できる。

参考別紙	なし
Topic	OWASP IoT Security Guidance
URL	https://www.owasp.org/index.php/IoT_Security_Guidance

今後の予定

- WG内でのレビューと訂正（3月いっぱい）
- JNSA総会までに公開（4月の予定）
- 2018年度は漏れている文書の追加や既存文書のパートを更新（するかも）
- パワフルなメンバー募集中です♪

IoTセキュリティのセミナーのお知らせ

CCDS、JPCERT、NCAと共同でIoTセキュリティの話をします！

日程：2018年2月26日（月）

会場： 浅草橋ヒューリックホール＆ カンファレンス

近日募集開始！

ご静聴ありがとうございました