

IoT セキュリティ 標準/ガイドライン ハンドブック 2017年度版

バージョン：1.0

発行：2018/05/01

作成：JNSA IoT Security WG

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

本ハンドブックに掲載している ガイドライン等の一覧



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	ITU-T	Y.4806
10	NIST	SP800-160 Systems Security Engineering
11	OTA	IoT Trust Framework(V2)
12	OWASP	OWASP IoT Security Guidance

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS

IoTの安全性確保のための戦略的原則

STRATEGIC 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。

U.S. Department of Homeland Security

**STRATEGIC
PRINCIPLES FOR
SECURING THE
INTERNET OF THINGS
(IoT)**

Version 1.0
November 15, 2016

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](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	<ul style="list-style-type: none">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、本文書の適用対象を説明	02~04 (3P)
2	STRATEGIC PRINCIPLES FOR SECURING IoT	<ul style="list-style-type: none">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つの戦略的原則と関連するプラクティスを説明	05~17 (13P)
3	CONCLUSION	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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)

「IoTの安全性確保のための戦略的原則」

- 対象として4名のプレイヤーを挙げている



開発から利用までのそれぞれの段階でIoTのセキュリティについて考慮をすべきプレイヤーを4名挙げている

No	対象	役割
1	IoT developers	デバイス、センサ、サービス、またはIoTのコンポーネントの設計・開発時のセキュリティを考慮する
2	IoT manufacturers	コンシューマデバイスとベンダー管理デバイスの両方のセキュリティを向上させる
3	Service providers	IoTデバイスを利用したサービスを実装する際に、IoTデバイスによるセキュリティとサービスがうまく動くようなインフラストラクチャのセキュリティを考慮する
4	Industrial and business-level consumers	IoTデバイスのセキュリティに関する製造業者およびサービスプロバイダーのリーダー（連邦政府および重要インフラの所有者および運営者を含む工業およびビジネスレベルの消費者を示す）

「IoTの安全性確保のための戦略的原則」

- 以下の6項目を戦略的原則として挙げている



No	項目	適用対象
1	Incorporate Security at the Design Phase	IoT developers、IoT manufacturers、Service providers
2	Promote Security Updates and Vulnerability Management	IoT developers、IoT manufacturers、Service providers
3	Build on Recognized Security Practices	IoT developers、IoT manufacturers
4	Prioritize Security Measures According to Potential Impact	IoT developers、IoT manufacturers、Industrial and business-level consumers
5	Promote Transparency across IoT	IoT developers、IoT manufacturers、Industrial and business-level consumers
6	Connect Carefully and Deliberately	IoT manufacturers、Service providers、Industrial and business-level consumers

「IoTの安全性確保のための戦略的原則」

- 以下の6項目を戦略的原則として挙げている



No	項目	適用対象
1	Incorporate Security at the Design Phase	<ul style="list-style-type: none">IoTデバイスのデザイン段階でのセキュリティの考慮をするべきであり、例としてデフォルトパスワードを難しいものに、利用するOSを最新のものに、セキュアチップ組み込んだハードウェアを利用することを推奨また、製造されたものについてIoTに関する判例法はないが、適切なセキュリティ設計に対する製造物責任の適用が期待されると明記
2	Promote Security Updates and Vulnerability Management	<ul style="list-style-type: none">デザイン時にセキュリティを考慮しても、製品展開後に脆弱性が見つかる場合もありうるのでセキュリティ更新の仕組みを設けるべきプラクティクスとして自動更新を推奨し、対応期間(寿命)も考慮する必要があり、見つかった脆弱性はコーディネートされる必要がある
3	Build on Recognized Security Practices	<ul style="list-style-type: none">従来ITシステムに対するセキュリティの機構やテストの仕組みなどのノウハウをIoT開発にも活用すべき例えば、NISTサイバーセキュリティリスク管理フレームワークをリスクとベストプラクティクスの発見の出発点として提案しており、他にも情報共有プラットフォームへの参加も検討することを挙げている

「IoTの安全性確保のための戦略的原則」

- 以下の6項目を戦略的原則として挙げている



No	項目	適用対象
4	Prioritize Security Measures According to Potential Impact	<ul style="list-style-type: none"> IoTシステムは一つ一つ異なるため、それぞれの脅威に対する影響、優先度等を考える必要がある それには「Redチーム」演習や既存のシステムのIoT化することの影響の考慮をしっかりとっていく必要がある IoTセキュリティはIoTデバイスのみならず、デバイスとサービスとプロセスの固有のリスクやそれぞれの相対的なリスクも考慮すべき
5	Promote Transparency across IoT	<ul style="list-style-type: none"> 利用している他ベンダーの製品やOSSについての脆弱性等セキュリティ情報を収集し、把握しておかなければ簡単で低コストな製品を利用する場合、正確なセキュリティ評価を行えない また、製造者から利用者までのどこでセキュリティを担保すべきかを確認すべき 開発するIoT製品のソフトウェア部品表の作成やベンダー間の情報共有の必要性、Bug Bountyの利用を提案
6	Connect Carefully and Deliberately	<ul style="list-style-type: none"> IoT製品のネットワークへの接続について、接続する必要があるものなのか、継続的な接続が必要かどうか検討を行い、意図的に慎重にネットワークと接続すべき 特に産業のIoT利用者は考慮すべき 接続後も常にIoT製品をコントロールできるようにしておき、いつでも切断可能な状態であるべき

「IoTの安全性確保のための戦略的原則」

- これから4つの努力を行うと結論している



本文書でDHSは6つの原則をそれぞれのプレイヤーが守っていくとともに、IoTセキュリティの次の段階に進むために、政府と産業間で4つの努力に取り組まなければならないと述べている

No	対象	役割
1	Coordinate across federal departments and agencies to engage with IoT stakeholders and jointly explore ways to mitigate the risks posed by IoT.	<ul style="list-style-type: none">DHSと連邦パートナーは、IoTセキュリティ強化のために業界パートナーと引き続き努力
2	Build awareness of risks associated with IoT across stakeholders	<ul style="list-style-type: none">DHSは他の機関、民間セクター、国際パートナーと協力して、国民の意識啓発、教育、訓練の取組みを加速

「IoTの安全性確保のための戦略的原則」

- これから4つの努力を行うと結論している



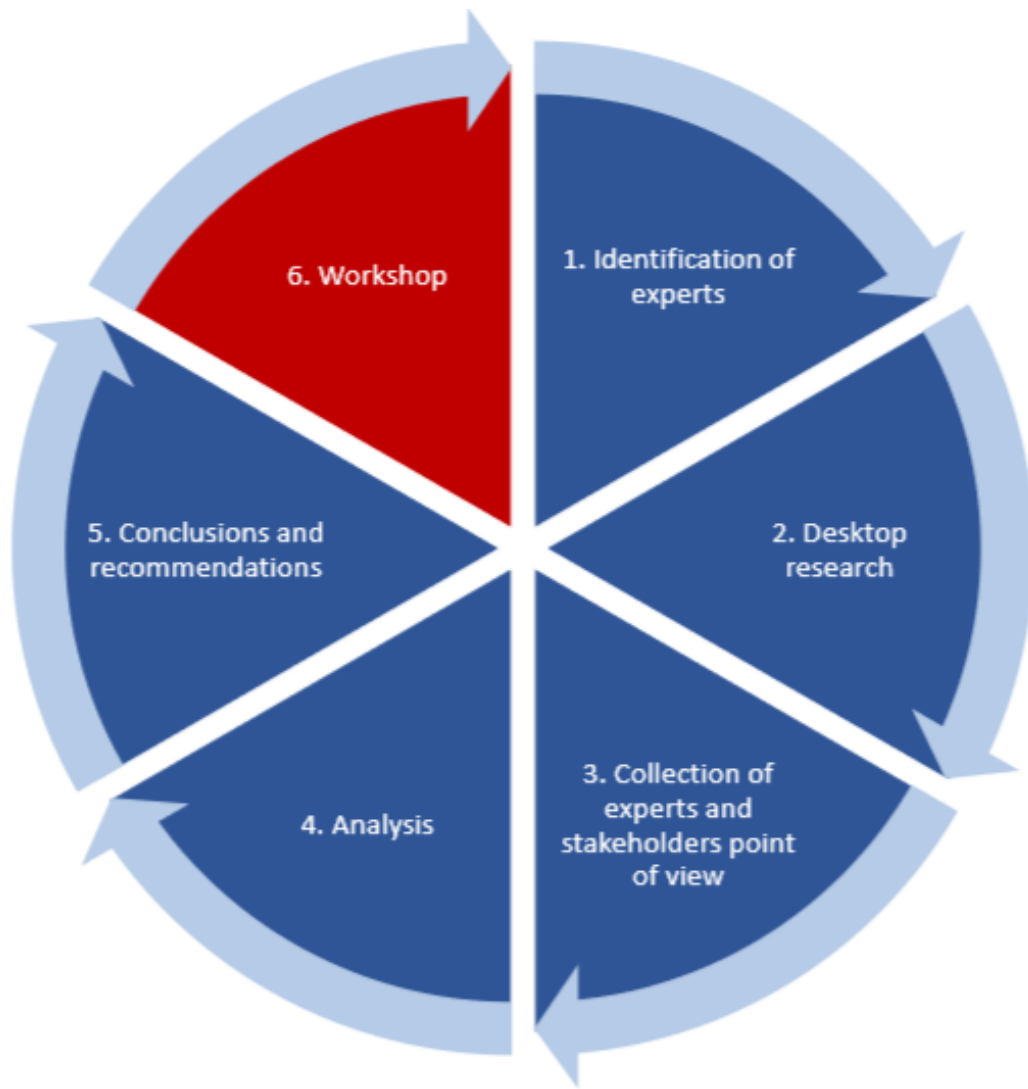
No	対象	役割
3	Identify and advance incentives for incorporating IoT security	<ul style="list-style-type: none"> 政策立案者、立法者、利害関係者は、IoTのセキュリティを強化するための取り組みをより効果的に促進する方法を検討する必要がある 現在の環境では、特定の製品またはシステムのセキュリティに対する責任を誰が負っているのかがしばしば不明なため、DHSおよびその他のステークホルダーは、不法行為責任、サイバー保険、法律、規制、自主的な認証管理、標準設定イニシアチブ、自主的な業界レベルのイニシアチブ、およびその他の仕組みが経済活動と革新的なイノベーションを依然として促進しながらセキュリティを向上させる方法を検討する必要がある
4	Contribute to international standards development processes for IoT	<ul style="list-style-type: none"> IoTは全世界で同じようなセキュリティの検討事項の多くを評価し始めています。IoT関連の活動は、一貫性のない標準や規則のセットに分かれていないことが重要 DHSは、国際基準の開発を支援し、イノベーションを促進し、安全保障を促進するという我々のコミットメントと一致するように、国際パートナーと民間部門と協力

ENISA資料の読み方

ENISAの公開資料の特徴と読み方

- ENISAの公開資料は次の特徴がある。
 - 実務家と専門家のWGや会議体を作った上で調査・分析を行っている。
 - リスク分析のためのアセットの分析が詳細に行われている。
 - 脅威の定義やリスク分析が行われている。
(リスクシナリオの検討もされている)
 - グッドプラクティスの収集と分析がされた上で提言が策定されている。
 - 関係者への提言が目的とされている。

調査のためのメソロジーもある



No 五つのステップ

1 専門家の特定

2 机上調査

3 専門家とステークホルダーの視点の収集

4 分析

5 結論と提言

6 ワークショップ

公開文章の構成もおおむね共通している



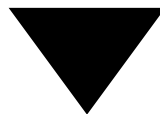
注目すべきは、「資産の特定」、「リスク分析」、「グッドプラクティス」

章立て	記載されている内容
エグゼクティブサマリ	概要と提言について要約
はじめに	目的や結果について概要を記載
定義	ターゲットとする内容の定義、関連法令、利害関係者、資産もここに含まれる場合がある
資産の特定	定義に含まれる場合もあるが、テーマにとって重要となる資産について整理
リスク分析	脅威の特定とリスクシナリオの想定。マインドマップで作成した文書でも公開
グッドプラクティスとのギャップの分析	リスクに対してグッドプラクティスが有効であることの検証とグッドプラクティスに対するギャップを分析した結果を説明
セキュリティのグッドプラクティス	グッドプラクティスの分類と概要の説明
推奨事項	ギャップ分析などの結果から、各利害関係者向けに推奨事項を提言

提言の対象者も概ね同じ

提言や勧告の対象者

- 対象とする企業のための推奨事項
- 対象とする企業と関連者への推奨事項
- 業界団体および団体のための提言・勧告
- 業界団体、協会、セキュリティ会社のための提言・勧告
- 政府機関のための提言・勧告

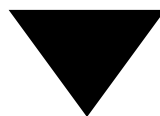


提言や勧告されている内容は一般的な内容であり
対象とするカテゴリなどにおいて特殊な提言や勧告などはあまりない

付属書や付録がある場合

以下のような付属書や付録がある

- 詳細事項
- グッドプラクティスのチェックリスト
- 脅威とグッドプラクティスやセキュリティ対策とのマッピング
- レビューされたセキュリティ基準と参考文献
- IoTセキュリティインシデントの例
- トピックの例



付属書(Annex)と付録(Appendix)がある場合
本文に記載できなかった詳細、脅威とグッドプラクティス、
セキュリティ対策とマッピングをした結果が示されているため参考になる

ENISA IoT and Smart Infrastructures Publications

ENISAでは、IoT and Smart Infrastructuresというトピックで複数のドキュメントを発行しています。

ENISAのドキュメントでは、まずリスク認識を行った上で要求事項を記載しており、トピックに関わるリスクにどのようなものがあるかの理解の参考になります。

*このページの内容は、英語の紹介ページの内容を翻訳し日本語としての言い回しを調整しています。

ENISAの研究 ～IoT とスマートインフラ概要～

スマートインフラストラクチャは、エネルギー、公共輸送、公共安全など、さまざまな活動領域からの複数の運用者で構成されている。

彼らは物理的世界と相互作用するデータ制御機器である「サイバー・フィジカル・システム」を導入し、運用している。彼らは、成熟度に応じていくつかのスキームでデータを共同して交換している。

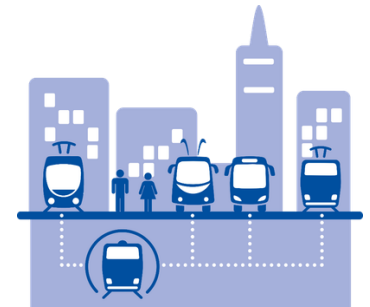
サイバーフィジカルデバイス（物理世界と相互作用するソフトウェア制御のデバイス）の使用は、経済と市民の安全に新たなリスクをもたらす。

最近の動向では、IoTを導入することによって、スマートインフラに移行する重要インフラ事業者が見られる。彼らはサービスの質を向上させるために遠隔管理と大きなデータに投資している。

ENISAは、優れたセキュリティプラクティスを見出し、事業者、製造業者、意思決定者に推奨事項を提案することによって、スマートインフラストラクチャをサイバー脅威から守るためのガイダンスを作成している。

ENISAは以下の領域で分野別のアプローチをとっている。

- スマートカー
- スマートホーム
- スマートシティ



No	名称	和訳	発行
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	2015年12月01日
2	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	2016年01月12日
3	Cyber security for Smart Cities	スマートシティのサイバーセキュリティ	2016年01月12日
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	2016年11月24日
5	Securing Smart Airports	スマート空港の確保	2016年12月16日
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	2017年01月13日
7	Baseline Security Recommendations for IoT	IoTのベースラインセキュリティ推奨事項	2017年11月20日

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>

Security and Resilience of Smart Home Environments

- レポートの項目(1)



スマートホーム環境のデバイスとサービスの開発、ホームネットワークでの利用、製品のEOLに関するグッドプラクティスを説明している

No	項目	概要	Page
1	はじめに	トピックを紹介し、このドキュメントの概要、ターゲットとする利用者、採用された方法論について説明	08~11 (4P)
2	スマートホーム環境	「スマートホーム」の定義。デバイス、サービス、テクノロジーの種類とこれらの環境に対する脅威	12~15 (4P)
3	主な発見事項	スマートホームのエコシステムにおけるセキュリティについて、調査研究において発見された主要な事項	16~20 (5P)
4	セキュアなスマートホーム環境のためのグッドプラクティス	スマートホームのコンテキストにおいて、既存の脅威を緩和するために適用されるセキュリティのグッドプラクティスの全体像を定義。	21~21 (1P)
5	スマートホームデバイスとサービス開発におけるグッドプラクティス	本報告書の中心的内容。スマートホームを構成するデバイスとサービスの開発を確実にするためのベストプラクティス	22~42 (21P)
6	ホームエリアネットワークでのデバイス統合に関するグッドプラクティス	スマートホーム環境でデバイスを安全に統合・連携するためのグッドプラクティス	43~47 (5P)
7	製品寿命(EOL)までの利用に関するグッドプラクティス	スマートホーム環境に配置された製品の運用と保守のためのセキュリティのグッドプラクティス	48~52 (5P)

Annex A～Dも参考になる

No	項目	概要	Page
8	推奨事項	スマートホーム環境のセキュリティとレジリエンスを強化するための重要な推奨事項	53~56 (4P)
-	Annex	Annex A：スマートホーム環境に関する追加の詳細事項 Annex B：脅威とグッドプラクティスとのマッピング Annex C：グッドプラクティスチェックリスト Annex D：ユーザ理解のためのトピックの例	-

Security and Resilience of Smart Home Environments

- 挙げられている推奨事項



推奨事項として記載されている内容自体は特殊な内容ではない

対象者	No	推奨事項
主にベンダー、学者、 および研究を資金提供する政策 立案者	1	すべての利害関係者は、最低限のセキュリティ要件についてコンセンサスに達するべき
	2	業界調査および公的資金によるイニシアティブは、スマートホームおよびIoTに関連する研究開発プロジェクトにサイバーセキュリティを組み込むべき
主にベンダー、政策立案者、 業界団体、消費者団体	3	業界は、セキュリティ主体のビジネスモデルをサポートすべき
ベンダー、消費者団体、 および国内のサイバーセキュリ ティ機関	4	すべての主体がセキュリティ意識を高めるために貢献すべき
欧州委員会および加盟国の政策 立案者	5	政策立案者は、スマートホーム環境の法的側面を明確にすべき

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

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 Transport

URL

<https://www.enisa.europa.eu/publications/good-practices-recommendations>

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

-レポートの項目



インテリジェントな公共交通機関を確保する必要性が中心であり、その次に環境の説明、グッドプラクティスの説明が続く

No	項目	概要	Page
1	はじめに	トピックを紹介し、このドキュメントの概要、ターゲットとする利用者、採用された方法論について説明	09~12 (4P)
2	インテリジェントな公共交通機関の環境	インテリジェントな公共交通機関を定義している。主要な立法環境、インテリジェントな公共交通機関における重要なビジネス及び社会的機能、主要な資産の識別など、インテリジェントな公共交通機関の環境について説明	13~20 (7P)
3	インテリジェントな公共交通機関を確保する必要性	インテリジェントな公共交通機関に影響を与えるサイバー脅威を特定し整理し、インテリジェントな公共交通機関に固有の新しいサイバー脅威の脆弱性を挙げる	21~33 (13P)
4	インテリジェントな公共交通機関を確保するためのグッドプラクティス	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を強化するためのグッドプラクティス	34~39 (6P)
7	ギャップ分析	インテリジェントな公共交通機関を保護するためのギャップの特定と分析(既存の政策面、法律面、運用面、雇用面から)	40~42 (3P)
8	推奨事項	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を強化するための重要な推奨事項	43~47 (5P)
-	以下、付録	Annexes	-

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



- 推奨事項(1)

幅広い内容が推奨事項として記載されている

対象者	No	推奨事項
インテリジェントな公共交通機関の意思決定者 (EC : European Communities と MS : Member States)	1	ECとMSの機関は、インテリジェントな公共交通機関 (IPT)サイバーセキュリティに関するパブリック/プライベートな コラボレーションを促進 すべき
	2	ECとその機関は、国レベルおよびEU全体共通の IPTセキュリティへのアプローチの開発を促進 すべき
	3	ECとMSは、他の活動分野で行われたセキュリティの努力を統合し 集約 すべき
	4	ECとMSは、IPTの調和した サイバーセキュリティ基準の開発 を促進すべきで
IPTオペレータ (IPT事業者)	5	IPTオペレータは、サイバーセキュリティをコーポレートガバナンスに 統合 すべき
	6	IPTオペレータは、ホリスティックなサイバーセキュリティと安全上のリスクと 統合された企業戦略の策定 をすべき
	7	IPTオペレータは、外部契約者および依存関係を含む環境における マルチステークホルダーのサイバーセキュリティのリスク管理 を実施すべき

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

- 推奨事項(2)



対象者	No	推奨事項
IPTオペレータ (IPT事業者)	8	IPTオペレータは、 サイバーセキュリティの要件 を明確かつ定量的に指定すべき
	9	IPTオペレータは、組織のサイバーセキュリティプロセス、慣行およびインフラを レビュー すべき
製造業者および ソリューションプロバイダー	10	製造業者とソリューションプロバイダは、IPTエンドユーザのサイバーセキュリティ要件を満たす製品/ソリューションを作成すべき
	11	製造業者とソリューションプロバイダーは、IPTソリューションに適用するIPT特有サイバーセキュリティ要件の開発に協力すべき
	12	製造業者とソリューションプロバイダは、リスクと脆弱性について信頼できる情報共有プラットフォームを開発すべき
	13	製造元およびソリューションプロバイダは、システムと製品、ソリューションの セキュリティガイダンス を提供すべき

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

発行	2016年01月12日
参考別紙	なし
Topic	IoT and Smart Infrastructures : Smart Infrastructure
URL	https://www.enisa.europa.eu/publications/smart-cities-architecture-model

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るようにされており、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。

Cyber security for Smart Cities

- レポートの項目



環境や資産の定義、スマートシティのアーキテクチャの定義とアーキテクチャに基づいた説明が中心となっている

No	項目	概要	Page
1	はじめに	トピックを紹介し、このドキュメントの概要、ターゲットとする利用者、採用された方法論について説明	08~10 (3P)
2	スマートシティ環境	インテリジェント・パブリック・トランスポート(IPT: インテリジェントな公共交通)とサイバーセキュリティスマートシティに焦点を当てたスマートシティ (SC)環境について説明している。これらには、IPT事業者や利害関係者だけではなく、データ交換をする他の関係者も含む	11~16 (6P)
3	スマートシティにおける輸送セクターのアーキテクチャ	スマートシティにおける輸送セクターのアーキテクチャモデルを説明している。都市の成熟度に応じて輸送セクターのアーキテクチャがどのように異なるかについて説明	17~25 (9P)
4	スマートシティにおける脅威	輸送セクターのアーキテクチャにおけるサイバーセキュリティに重点を置いたレイヤについて説明	26~32 (7P)
6	セキュリティのグッドプラクティス	公共交通機関におけるサイバーセキュリティのグッドプラクティスを提示	33~37 (5P)
7	主な発見事項	調査研究において発見された主要な事項を要約	38~41 (4P)
8	推奨事項	スマートシティのサイバーセキュリティを強化するための推奨事項	42~44 (3P)
-	Appendix A,B	Appendix A:意図的な攻撃とグッドプラクティスの関連付け Appendix B:事故とグッドプラクティスの関連付け	-

主要な発見事項として挙げられている事項は以下の通り、内容から挙げられているのは現状の課題と考えて良い

No	主要な発見事項
1	スマートシティにおけるコラボレーションが未定義
2	スマートシティにおけるデータ交換のための参照アーキテクチャの欠如
3	スマートシティにおけるサイバーセキュリティに対する認識が低い
4	脅威とインシデントに関する横断的情報共有の欠如
5	IPTにおけるサイバーセキュリティの知識と費用は非常に低い
6	サイバーセキュリティ対策の遅れ
7	意識を高めることでサイバーセキュリティを向上

Cyber security for Smart Cities

- 推奨事項



推奨事項は対象、記載内容ともに幅広い内容となっている

対象者	No	推奨事項	対応する 主要発見事項
自治体	1	自治体は、調和のとれたサイバーセキュリティフレームワークの開発を支援すべき	1,2,4
欧州委員会と 加盟国	2	欧州委員会と加盟国は、業界、加盟国、および加盟国間のサイバーセキュリティにおけるナレッジの交換と協力を促進すべき	1,3,4,7
	3	欧州委員会と加盟国は、すべての主体の責任を明確にすべき	2,6
IPT事業者	4	IPT事業者は、セキュリティ要件を明確に定義すべき	6,7
製造元 およびソリュー ションベンダー	5	製造元およびソリューションベンダーは、製品にセキュリティを統合する必要がある	5,6
IPTの運営者 および地方自治体	6	IPTの事業者および地方自治体は、上級管理職のサイバーセキュリティにおける責任を明確にすべきで	3,5,6,7
	7	IPTの運営者および地方自治体は、サイバーセキュリティに対するより高い支出を配分すべき	5,6
スマートシティの 標準化組織	8	スマートシティの標準化組織は、スマートシティの成熟度レベルにサイバーセキュリティを統合する必要がある	2

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

発行	2016年11月24日
	<p>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。</p> <p>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。</p> <p>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。</p>
参考別紙	なし
Topic	Critical Infrastructures and Services : Health IoT and Smart Infrastructures : Smart Infrastructure
URL	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Cyber security and resilience for Smart Hospitals

- レポートの項目



脅威分析(リスク分析、脅威シナリオ)が中心となっており、その基礎となっているスマート病院の環境の項目が多い

No	項目	概要	Page
1	はじめに	トピックを紹介し、このドキュメントの概要、ターゲットとする利用者、採用された方法論について説明	06~08 (3P)
2	スマート病院	スマート病院の環境について説明。病院が、その目的を追求するために「スマート」な効果がもたらす保護すべき重要な資産を明らかに、情報セキュリティに関する規制の枠組みとガイドラインを特定	09~17 (9P)
3	脅威とリスク分析	本報告書では、脅威とリスク分析に対する資産中心のアプローチを取っており、本セクションでは、主要な資産と脆弱性に基づいた潜在的な攻撃ポイントと脅威の種類を説明	18~29 (12P)
4	脅威シナリオ	病院のスタッフに対するソーシャルエンジニアリング攻撃、デバイスへの物理的タンパリング、マルウェア感染、機器の盗難、病院サーバーへのサービス拒否攻撃の、5つの攻撃シナリオについて説明	30~44 (15P)
5	セキュリティのグッドプラクティス	脅威からスマート病院を保護するために利用できるコントロールと復旧措置について記述。病院と産業界がそれぞれ実施する対策は異なっていると結論	45~51 (7P)
6	推奨事項	病院の役員、業界関係者、政策立案者を対象とした、具体的かつ実践可能なグッドプラクティスの例	53~55 (3P)

これら未解決の問題は、医療向けのIoTコンポーネントのサイバーセキュリティを強化するために必要なこととされるが、記載されている問題の粒度やカテゴリは統一されていない

No	未解決の問題
1	独自デバイスのコントロールの欠如
2	自動資産インベントリ発見ツールの必要性
3	アプリケーションホワイトリスト（認可されたソフトウェアとバージョンのリスト）技術の欠如
4	安全な構成の確保の必要性
5	システムの検証と認証のためのクライアント証明書必要性
6	トレーニングや意識向上プログラムの欠如
7	安全なチャンネル上のサーバー、ワークステーション、ネットワーク装置などのリモート管理
8	標準化とIT技術のスピード
9	費用対効果の内訳の重要性

「未解決の問題」と各対象者への推奨事項と関連付けて説明されている

No	推奨事項	対応する 未解決の問題
病 院		
1	サイバーセキュリティのための効果的な組織ガバナンスを確立	1,3,4,6,9
2	最先端のセキュリティ対策の実装	1,2,3,4,7,9
3	病院内のIoTコンポーネントに特有のITセキュリティ要件の適用	5,7,8,9
4	NIS(Network Information Security)製品への投資	1,2,3,5
5	情報セキュリティの共有メカニズムを確立	3,6,8
6	リスクアセスメントと脆弱性評価	4,5,7
7	ペネトレーションテストと監査を実行	4,5,7
8	マルチステークホルダーコミュニケーションプラットフォーム (ISAC) や他の情報共有方法をサポート	2,3,4,5
業 界		
1	既存の品質保証システムにセキュリティを組み込む	4,5
2	テスト活動に第三者を関与させる	5,9
3	重要なインフラストラクチャコンポーネントに医療機器規制を適用することを検討	5,7
4	医療への情報セキュリティ基準の適用をサポート	8

Securing Smart Airports

スマート空港の確保

Securing Smart Airports

発行	2016年12月16日
参考別紙	Good practices mind map Smart Airports asset groups and assets Threat Taxonomy Simple Threat Taxonomy
Topic	Critical Infrastructures and Services : Critical Information Infrastructures IoT and Smart Infrastructures : Smart Transport
URL	https://www.enisa.europa.eu/publications/securing-smart-airports

Securing Smart Airports

- レポートの項目



環境や資産の定義、脅威分析(リスク分析、脅威シナリオ)が中心となっており、対応するグッドプラクティスの記載がその次に多い

No	項目	概要	Page
1	はじめに	トピックを紹介し、このドキュメントの概要、ターゲットとする利用者、採用された方法論を説明	09~12 (4P)
2	スマート空港のサイバーセキュリティにおける重要な側面	スマート空港の定義と主要な立法環境、スマート空港およびスマート空港における重要資産の識別など、スマート空港のコンテキスト	13~21 (9P)
3	主要な資産グループと資産	スマート空港で保護される主要な資産グループと資産の概要	22~24 (3P)
4	脅威とリスク分析	スマート空港内の主要な資産に影響を与える重要なサイバー脅威を特定し整理している。スマート空港に固有の新しいサイバー脅威の脆弱性についての議論と攻撃の例	25~32 (8P)
5	脅威シナリオ	机上での研究と専門家へのインタビューの両方で確認された三つの詳細な攻撃シナリオ	33~41 (9P)
6	セキュリティのグッドプラクティス	空港内のサイバーセキュリティを強化するためのグッドプラクティス	42~46 (5P)
7	ギャップ分析と改善領域の特定	空港内のサイバーセキュリティにおける既存のギャップの識別と分析では、これまでの知見との比較分析	47~49 (3P)
8	推奨事項	スマート空港のセキュリティとレジリエンスを強化するための重要な推奨事項	50~52 (3P)

Securing Smart Airports

- 推奨事項



推奨事項自体は特殊な内容ではない

対象者	No	推奨事項
空港の意思決定者 (CISO,CIO,ITディレクター、事業責任者) および空港情報セキュリティ専門家	1	安全のためのサイバーセキュリティの優先順位付け
	2	明確な空港のサイバーセキュリティの姿勢を確立し、適切な役割とリソース配分、グッドプラクティスのモニタリングに基づいてサイバーセキュリティポリシーとプラクティスを修正
	3	ネットワークベースの総合的なリスクと脅威管理のポリシーとサイバーセキュリティのプロセスの実装
政策立案者	4	共通のガイドライン、基準、指標、意識の啓発と促進
	5	スマート空港のサイバーセキュリティに関するナレッジ交換
	6	スマート空港におけるサイバーセキュリティの認定および第三者監査の開発の促進
業界代表者	7	サイバーセキュリティ標準の開発における主要な利害関係者とのコラボレーション
製品とソリューション提供者	8	空港運営者と協力し、サイバーセキュリティの要件に合わせた製品やソリューションを開発

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

発行	2017年01月13日
参考別紙	なし
Topic	IoT and Smart Infrastructures : Smart Transport
URL	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

Cyber Security and Resilience of smart cars

- レポートの項目



脅威とリスク分析およびギャップ分析とグッドプラクティスを中心となっており、Appendixも参考になる

No	項目	概要	Page
1	はじめに	トピックを紹介し、このドキュメントの概要、主要な立法環境、ターゲットとする利用者、採用された方法論について説明	08~12 (5P)
2	スマートカーの主な側面	スマートカーの定義、スマートカーのアーキテクチャや資産などスマートカーのコンテキスト環境について説明	13~23 (11P)
3	脅威とリスク分析	スマートカーのサイバーセキュリティの主要な資産に影響を与える重要なサイバー脅威を特定し整理。スマートカーのサイバーセキュリティに固有の新しいサイバー脅威の脆弱性についても議論し、攻撃の例を説明	24~43 (20P)
4	ギャップ分析とグッドプラクティス	スマートカーのサイバーセキュリティにおける既存のギャップの識別と分析、スマートカーのサイバーセキュリティを強化するためのグッドプラクティスを提示。	44~56(13P)
5	推奨事項	スマートカーのサイバーセキュリティとレジリエンスを強化するための重要な推奨事項がの提示	57~61 (5P)
-	Appendix A, B	Appendix A:攻撃シナリオの詳細なリスク評価 Appendix B:グッドプラクティスの詳細	-

Cyber Security and Resilience of smart cars

- 推奨事項



推奨事項として記載されている内容自体は特殊な内容ではない
主に情報共有と評価に視点が置かれている

対象者	No	推奨事項
スマートカーメーカー、ティア、アフターマーケットベンダーのための推奨事項	1	スマートカーのサイバーセキュリティを向上。業界の主体は、製品のセキュリティを効果的に向上させる優れた方法の確立
	2	業界関係者間の情報共有を改善。情報共有のコミュニティはすでに存在しており、この努力を追求
	3	セキュリティ研究者や第三者との交流を改善。業界の主体は、特にセキュリティドメインからの第三者との接触を強化すべき
スマートカーメーカー、ティア、アフターマーケットベンダー、保険会社のための推奨事項	4	業界関係者間の責任を明確化。高度に階層化された環境における企業主体は、セキュリティ問題が発生した場合に、それぞれの責任を明確にするプロセスの定義
業界団体および団体のための勧告	7	グッドプラクティスの技術基準に関するコンセンサスの確立
	8	独立した第三者評価スキームの定義
業界団体、協会、セキュリティ会社のための勧告	9	セキュリティ分析用のツールを構築し、業界の主体は、セキュリティテストとセキュリティ監視ツールの構築によって、セキュリティテストのスキルを直接向上

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

発行	2017年11月20日	
	<p>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。</p> <p>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。</p> <p>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。</p>	
参考別紙	なし	
Topic	IoT and Smart Infrastructures : Internet of Things (IoT)	
URL	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot	

Baseline Security Recommendations for IoT

- レポートの項目



他のIoT関連の報告書と同様の構成で、IoT環境やその構成要素の定義、脅威とリスク分析が主体

No	項目	概要	Page
1	はじめに	報告書の概要と目的の定義とそれを達成する方法論	11~17 (7P)
2	IoTによるパラダイム	IoTの主要要素と環境の定義	18~29 (12P)
3	脅威とリスク分析	主要な、脅威・脆弱性・リスク・攻撃シナリオの分析	30~45 (16P)
4	セキュリティ対策と グッドプラクティス	報告書の対象範囲における、識別された主要なセキュリティ対策の開発、マッピング、分類	46~52 (7P)
5	ギャップ分析	ギャップと今後の課題	53~56 (4P)
6	IoTサイバーセキュリティを改善するための 高水準な推奨事項	5章で挙げられたギャップと今後の課題に対し、開発されたセキュリティ対策との対応	57~60 (4P)
-	GlossaryとAnnex A, B	Glossary Annex A: セキュリティ対策/グッドプラクティスの詳細 Annex B: セキュリティ対策と脅威のマッピング Annex C: レビューされたセキュリティ基準と参考文献 Annex D: IoTセキュリティインシデントの記述	-

Baseline Security Recommendations for IoT

- レポート概要(1) -IoTの定義とIoTの要素



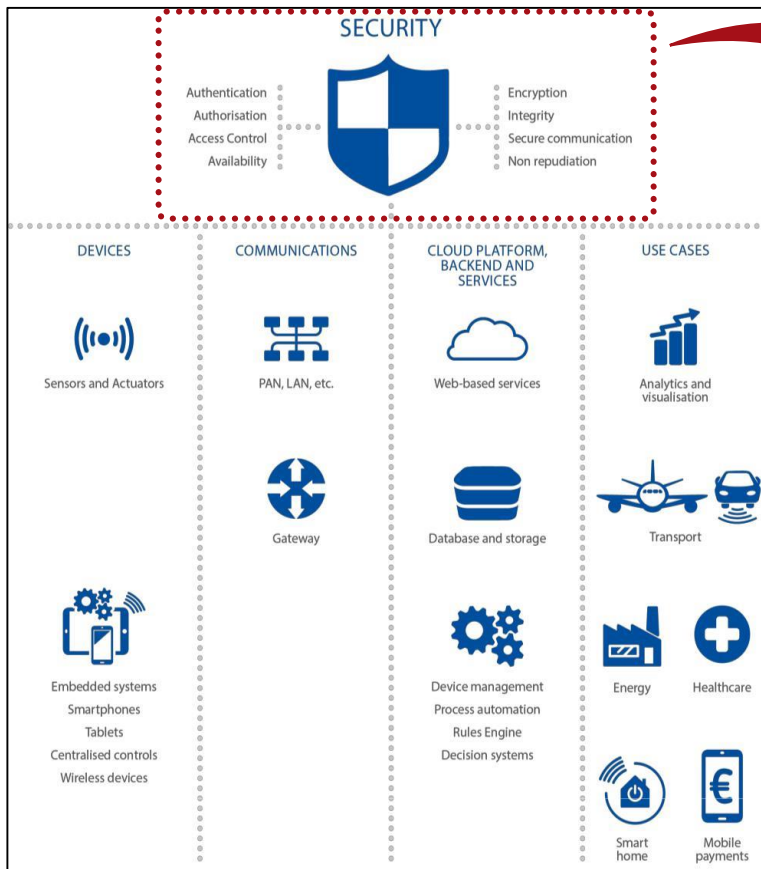
レポートによるIoTの定義：合理的な意思決定ができる、センサーとアクチュエータが相互接続されたサイバーと物理のエコシステム

No	IoTの要素	要約
1	IoTのモノ Things in the Internet of Things	「モノ」は物理的かつ仮想的なオブジェクトで、通信ネットワークを介してコミュニケーションし、インテリジェントシステムで管理され、監視および制御するために自律的に「モノ」に接続可能
2	合理的な意識決定 Intelligent decision making	IoTは意思決定が必要な行動の概念を必ず含み、合理的な意思決定は情報に依存 意思決定によって行動し、新しい情報をエコシステムに供給する事があり、このプロセス全体は、コンテキストの認識と適応、自律性、自己最適化などをサポート
3	センサー及びアクチュエータ Sensors and actuators	センサーとアクチュエータはIoTの基本要素 入力装置の機能は、環境およびそのコンテキストに関する情報をセンサーから得て処理され、アクチュエータは出力ユニットとして処理された情報に基づいて動作
4	組込みシステム Embedded systems	センサーとアクチュエータの機能やネットワーク機能、ソフトウェアを実行する機能は、独自のデータ処理を実行する処理ユニットに基づく組込みシステムによって実現される
5	コミュニケーション Communications	IoTのエコシステムで使用されるプロトコルの選択は、そのユースケースの要件によって異なり、通信システムは無線または優先ベースのいずれでもよく、それぞれ独自の規格で定義されている

Baseline Security Recommendations for IoT

- レポート概要(2) -IoTハイレベルリファレンスモデル

レポートでは、複数のアーキテクチャ定義を分析し基本要素を抽出し、これらの複数のアーキテクチャの主要要素を含むリファレンスモデルを定義している



SECURITY/セキュリティ	
Authentication	認証
Authorization	認可
Access Control	アクセスコントロール
Availability	可用性
Encryption	暗号化
Integrity	完全性
Secure Connection	セキュアコネクション
Non repudiation	否認防止

Figure 4:IoT High-level reference model

Baseline Security Recommendations for IoT

- レポート概要(3) - セキュリティの考慮事項



レポートでは、セキュリティの考慮事項として次の11点を挙げている(1-6)

No	セキュリティの考慮事項	要約
1	非常に大きな攻撃面 Very large attack surface	IoTに関する脅威とリスクは多様であり急速に変化しており、市民の健康、安全およびプライバシーへの脅威の影響は非常に広い
2	限られたデバイスリソース Limited device resources	大部分のIoTデバイスは限られた能力しか持たず、IoTで従来のセキュリティプラクティスを適用しようとする技術的な制約のためにリエンジニアリングが必要
3	標準と規制の断片化 Fragmentation of standards and regulations	新しい技術の出現により、断片的で遅い標準の採用とIoTのセキュリティ対策、グッドプラクティスの導入における規制の懸念
4	広範囲な展開 Widespread deployment	近重要インフラを構成するレガシーインフラの上にIoTを採用してスマートインフラに移行するのが近年のトレンド
5	統合されたセキュリティ Security integration	全ステークホルダの視点と要件は矛盾する可能性があり、異なるIoTシステム・デバイスは、異なる認証ソリューションに基づくことができるため、それらは統合され相互運用性を担保出来なければならない
6	安全面 Safety aspects	アクチュエータがあるためIoTのコンテキストでは非常に関連性があり、セキュリティの脅威は物理的な世界に影響を与える

Baseline Security Recommendations for IoT

- レポート概要(4) - セキュリティの考慮事項



レポートでは、セキュリティの考慮事項として次の11点を挙げている(7-11)

No	セキュリティの考慮事項	要約
7	低コスト Low cost	IoTデバイスおよびシステムの低コスト化は、セキュリティの観点から影響が大きく、製造業者はセキュリティ機能を制限することがある
8	専門知識の欠如 Lack of expertise	新規ドメインのため、IoTサイバーセキュリティに適したスキルと専門知識を持つ人々が不足
9	セキュリティアップデート Security updates	ユーザインターフェイスの特徴から、従来のアップデートメカニズムが利用できないため、セキュリティアップデートの適用が困難
10	安全でないプログラミング Insecure programming	他のドメインよりも高い「市場投入期間」短縮の圧力や予算の制約によって、IoT製品の開発企業は実現すべきセキュリティやプライバシー対策よりも機能性とユーザビリティを重視
11	不明瞭な責任 Lack of expertise	大規模で複雑なサプライチェーンは、責任の所在が不明確な場合、事故発生時にあいまいさや矛盾が生じる可能性がある コンポーネントが複数の当事者によって共有されていた場合、セキュリティをどのように管理するかという問題は解決されず、責任を強制することは別の大きな問題を生む

Baseline Security Recommendations for IoT

- レポート概要(5) - セキュリティ対策とグッドプラクティス



レポートでは、3カテゴリの24個のセキュリティ対策を挙げている

No	カテゴリ	セキュリティ対策	対訳
1	ポリシー Policies	<ul style="list-style-type: none">• Security by design• Privacy by design• Asset Management• Risk and Threat Identification and Assessment	<ul style="list-style-type: none">• セキュリティバイデザイン• プライバシーバイデザイン• 資産管理• リスクと脅威の分析
2	組織的、人的、 プロセス的対策 Organisational, People and Process measures	<ul style="list-style-type: none">• End-of-life support• Proven solutions• Management of security vulnerabilities and/or incidents• Human Resources Security Training and Awareness• Third-Party relationships	<ul style="list-style-type: none">• EOL サポート• 実績のあるソリューション• セキュリティ上の脆弱性やインシデントの管理• 人事、セキュリティトレーニングと動機づけ• サードパーティとの関係
3	技術的対策 Technical Measures	<ul style="list-style-type: none">• Hardware security• Trust and Integrity Management• Strong default security and privacy• Data protection and compliance• System safety and reliability• Secure Software / Firmware updates• Authentication• Authorisation• Access Control - Physical and Environmental security• Cryptography• Secure and trusted communications• Secure Interfaces and network services• Secure input and output handling• Logging• Monitoring and Auditing	<ul style="list-style-type: none">• ハードウェアセキュリティ• 信頼性と完全性の管理• 強力なデフォルトセキュリティとプライバシー• データ保護とコンプライアンス• システムの安全性と信頼性• セキュアなソフトウェア/ファームウェアアップ デート• 認証• 認可• アクセス制御 - 物理的、環境的セキュリティ• 暗号化• 安全で信頼できる通信• セキュアなインターフェイスとネットワーク サービス• 安全な入力および出力処理• ロギング• 監視と監査

Baseline Security Recommendations for IoT

- レポート概要(6) - 脅威の分類法で特定されたすべての脅威



レポートでは、7カテゴリの25個の脅威を挙げている

No	カテゴリ	脅威	対訳
1	悪意のある活動/乱用 Nefarious activity / Abuse	<ul style="list-style-type: none">MalwareExploit KitsTargeted attacksDDoSCounterfeit by malicious devicesAttacks on privacyModification of information	<ul style="list-style-type: none">マルウェアエクスプロイトキット標的型攻撃DDoS悪意のあるデバイスによる偽造プライバシーへの攻撃情報の変更
2	盗聴/傍受/ハイジャック Eavesdropping / Interception / Hijacking	<ul style="list-style-type: none">Man in the middleIoT communication protocol hijackingInterception of informationNetwork reconnaissanceSession hijackingInformation gatheringReplay of messages	<ul style="list-style-type: none">中間者攻撃IoT通信プロトコルハイジャック情報の傍受ネットワークの偵察セッションハイジャック情報収集メッセージの再生
3	停止 Outages	<ul style="list-style-type: none">Network OutageFailures of devicesFailure of systemLoss of support services	<ul style="list-style-type: none">ネットワーク停止デバイスの障害システムの障害サポートサービスの喪失
4	損害/損失 (IT資産) Damage / Loss (IT Assets)	<ul style="list-style-type: none">Data / Sensitive information leakage	<ul style="list-style-type: none">データ/機密情報の漏洩
5	障害/機能不全 Failures / Malfunctions	<ul style="list-style-type: none">Software vulnerabilitiesThird parties failures	<ul style="list-style-type: none">ソフトウェアの脆弱性サードパーティの障害
6	災害 Disaster	<ul style="list-style-type: none">Natural DisasterEnvironmental Disaster	<ul style="list-style-type: none">自然災害環境破壊
7	物理的攻撃 Physical attacks	<ul style="list-style-type: none">Device modificationDevice destruction (sabotage)	<ul style="list-style-type: none">デバイスの変更デバイスの破壊 (妨害)

Baseline Security Recommendations for IoT

- レポート概要(7) -IoTに対する攻撃シナリオ



レポートでは、IoTに対する攻撃のシナリオとして、10個のシナリオを挙げている

No	IoTに対する攻撃シナリオ	重大度
1	コントローラとアクチュエータとの間のネットワークリンクに対する攻撃	High~Crucial
2	センサーに対して、センサーによって読み取られた値またはその閾値および設定を変更する攻撃	High~Crucial
3	アクチュエータに対して、通常の設定を変更または妨害する攻撃	High~Crucial
4	IoTの管理システムに対する攻撃	High~Crucial
5	プロトコルの脆弱性の悪用	High
6	デバイスに対して、コマンドをシステムコンソールに注入する攻撃	High~Crucial
7	踏み台攻撃	Medium~High
8	IoTボットネットを利用したDDoS攻撃	Crucial
9	脆弱性の利用による、電源操作とデータ読取り	Medium~High
10	ランサムウェア	Medium~Crucial

Baseline Security Recommendations for IoT

- レポート概要(8) - 7つの要求事項



レポートでは、以下の7つの要求事項を挙げている

No	推奨事項	対象者
1	IoTのセキュリティの推進と規制の調和	IoT業界、プロバイダー、製造業者、協会
2	IoTのサイバーセキュリティの必要性に対する意識の向上	IoT業界、プロバイダー、製造業者、協会、学界、消費者団体、規制当局
3	IoTのセキュアなソフトウェアおよびハードウェア開発のライフサイクルにおけるガイドラインの策定	IoT開発者、プラットフォームオペレータ、業界、製造業者
4	IoT エコシステム全体の相互運用性に対するコンセンサスの達成	IoT業界、プロバイダー、製造業者、協会、規制当局
5	IoT セキュリティに対する経済的なインセンティブと行政を通じたインセンティブの強化	IoT業界、協会、学界、消費者団体、規制当局
6	セキュアなIoT 製品とサービスのライフサイクルマネジメントの確立	IoT開発者、プラットフォームオペレータ、業界、製造業者
7	IoTのステークホルダー間の責任の明確化	IoT業界、規制当局

参考

その他参考になる文献について説明します。

◆ 「ITmediaエンタープライズ」 記事

ビッグデータ利活用と問題解決のいま：欧州にみるスマートシティのサイバーセキュリティ

<http://www.itmedia.co.jp/enterprise/articles/1605/10/news008.html>

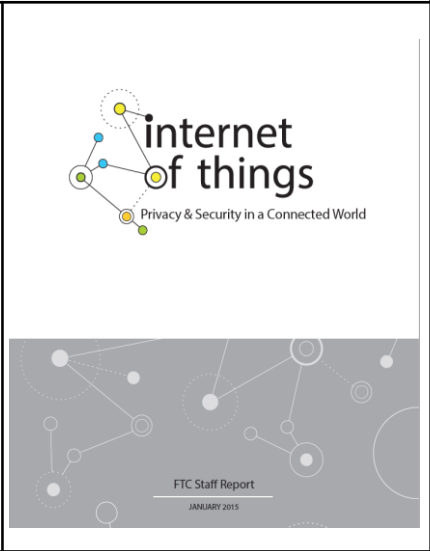
上記の記事では以下の3つの文献について触れられている。

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
2. 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
3. Architecture model of the transport sector in Smart Cities
スマートシティのサイバーセキュリティ

Internet of things Privacy & Security in a Connected World

つながる世界のIoT プライバシーとセキュリティ

Internet of things Privacy & Security in a Connected World

発行	2015年	
	<p>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)</p> <ul style="list-style-type: none">・ 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、ウェアラブル」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	

Internet of things Privacy & Security in a Connected World



報告書の構成

No	項目	Page
1	要約 Executive Summary	1~
2	背景 Background	1~
3	IoTとは何か？ What is the “Internet of Things”?	5~
4	ベネフィットとリスク Benefits & Risks	7~
5	典型的でプライバシーに基づくアプリケーション例 Application of Traditional Privacy Principles	19~
6	法規制 Legislation	47~
7	結論 Conclusion	55~

Internet of things Privacy & Security in a Connected World

- 米国FTC(連邦取引委員会)にとってIoTとは何か？



FTCのミッションとの一致：消費者保護

No	推奨事項	ノート
1	商業圏での消費者保護のため、 (我々の) IoTの議論は、「消費者に販売されたり、消費者によって使用される」デバイス (B2C向け) に限定	B2Bの議論はしない：ホテルや空港でのセンサーネットワーク、 広範なM2M通信を可能にする在庫、機能、効率を追跡するビジネスなどは考えない

Internet of things Privacy & Security in a Connected World

- IoTのベネフィット (利益)



No	分野	ベネフィット	課題
1	ヘルスケア	<ul style="list-style-type: none"> • 病院まで行かなくて済む • 病院、ケア設備での長期滞在をなくす • 患者は、介護者、親戚、医師にアプリを通じて健康データを提供 • 接続された健康機器は「より豊かな情報源」を提供し「生活の質と安全性」を向上 • 「診断／治療」のために患者は医者にデータを送信、「病気の予防／改善」可能な医療システム • より「効率的／運転コスト」を削減「豊富なデータ」による”変革” 	<ul style="list-style-type: none"> • ヘルスデータのプライバシー問題が発生 • FDA（アメリカ食品医薬品局）による「砂糖使用を減らす」という動きにも繋がる
2	エネルギー	<ul style="list-style-type: none"> • スマートメータは、「エネルギー管理者」に屋内外の電気の使用量を提供「どの家電が使われているか」の把握、制御が可能 • エネルギー利用プランが提供可能 • 屋外（プールなど）水漏れを検知 	-
3	車 (移動手段)	<ul style="list-style-type: none"> • ソフトウェア「ダウンロード」で「更新」の実現 • センサーで道路状態（安全性）を通知 • リアルタイム診断によってディーラーに行くべきかを通知、非車検制度を実現 • インターネットラジオ、ナビゲーション、気象情報、交通状況、スマホは「スターター」やがて「ビルトイン」 • 将来は自動運転、シェアードカーへ 	-

Internet of things Privacy & Security in a Connected World

- IoTのセキュリティリスク



No	脅威	リスク
1	個人情報の不正アクセス	<ul style="list-style-type: none"> スマートテレビは、消費者によるインターネットサーフィンを可能にし、ノートPCやデスクトップコンピュータと同様に、物品購入／写真共有ができ、脆弱性によってコンピュータ同様の危険（テレビに保存された情報、テレビを介して送信された情報を含む）にさらされる スマートテレビ、その他のデバイスは機密性の高い金融口座、パスワード、その他の種類の情報を含むため、脆弱性を利用した個人情報の盗難や不正行為 消費者が自宅に多くのスマート機器を設置することで、侵入者が個人情報を侵害する可能性のある「脆弱性の数」が増加
2	不正使用	<ul style="list-style-type: none"> 特定のデバイスのセキュリティ脆弱性が攻撃を容易にする可能性と消費者のネットワークまたは他のシステムへの攻撃 侵害されたIoTデバイスを使用したサービス攻撃は、より多くのデバイスに効果的 接続されたデバイスを使用した悪意ある電子メール送信 攻撃者は自分のコントロール下にあるIoTデバイスが増加するにつれて、脆弱性を用いて「サービス攻撃に使用できるデバイス」を増やせる
3	他のシステムへの攻撃	-
4	安全（セーフティ）リスクを創出	-

権限のない人がセキュリティの脆弱性を悪用、場合により物理的安全性のリスク

No	脅威	リスク
1	不正アクセス・不正使用	<ul style="list-style-type: none"> インスリンポンプが遠隔からハッキングされ薬を摂取できなくなる 車に非接触のまま、車載コンピュータネットワークへアクセスされ、テレマティクスユニット、エンジンおよび制動装置を遠隔制御される 完全に自動化された自動車、自動化された物理的オブジェクトとでは一般的になる インターネットカメラ/ベビーモニターへの不正アクセスによる物理的安全性の懸念 ヘルスケア機器などによって収集されたデータへの不正アクセスにより、時間経過とともにユーザーの位置を追跡による物理的安全性の懸念 泥棒が遠隔からスマートメーターのエネルギー使用量を住宅所有者の家から離れてアクセスし安全に窃盗を行う

IoTデバイスの潜在的なリスクは、家庭用コンピュータのセキュリティよりも難しい？

リスク

セキュリティアップデートは全く無く、消費者は購入直後のデバイスのサポートを受けないか脆弱なまま

背景

IoT市場に参入する企業はセキュリティ上の問題に対処した経験をもつ

いくつかのIoTデバイスは高度に洗練されているが、他の多くは安価かつ本質的に使い捨てである。そのような場合で脆弱性が発見された場合、製造後のソフトウェアの更新・パッチが困難または不可能な場合がある

アップデートが利用可能であっても”多くの消費者はそれを耳にしない”

多くの企業（特にローエンドのデバイスの開発企業）では継続的なサポートやソフトウェアを提供する経済的インセンティブがない

IoTから生まれるプライバシーリスク

- セキュリティ上のリスクに加えてIoTでのリスクの中には、正確な地理的位置情報、財務情報などの重要な個人情報、アカウント番号、健康情報、インターネットとモバイル商取引、その他の個人情報、習慣、場所、および時間の経過に伴う身体状況など
- 機密情報を直接収集していないエンティティ
 - ビックデータ解析による問題
- 少数のデバイスでも生成できる膨大な量のデータ
 - 1万人未満の世帯がある会社のIoTホームオートメーション製品を使用すると世帯につき1日に”1億5000万の離散データ”を得られる（世帯毎に6秒で1データを得る）

膨大な量の詳細なデータによるプライバシーリスク

- 膨大な量の詳細なデータは、少ないデータでは不可能な分析を実行できる
 - 既存のスマートフォンセンサを使用して様々な推測ができる。例えば、ユーザの気分、適応力、人格、双極性障害、人口統計（性別、婚姻の有無、ステータス、ジョブステータス、年齢など）、喫煙習慣、全体的な幸福感。パーキンソン病の進行、睡眠パターン、幸福度、運動のレベル、身体的活動や運動の種類など
- 推論は消費者に有益なサービスを提供するために使用できるが、誤用される可能性がある
- 「機密性の高い行動パターンの収集を可能にする」それらは「許可されていない方法」またはそれらが「許可されていない個人」によって行われる危険性
- 一般的なプライバシーリスクの存在は、細かいデータ収集と関連している。豊富なデータを用いた動向把握は、環境デバイスからの意図しない”底引き網のようなデータ収集”を生み出す

企業によるプライバシー侵害

- 企業はデータを使ってクレジット、保険、雇用の決定する
 - 保険会社が保険金を回収することを可能にするプログラムがあり、運転習慣に関するデータ「ハードブレーキ」、マイルの数、費やされた時間、深夜から午前4時までの運転などが保険料率の設定に役立つ
- 信用／保険／雇用決定のためのデータは、利益をもたらす可能性がある
 - より安全な運転者が自動車保険の料金を下げることが可能にし、消費者のクレジットへのアクセスを拡大できるが、一方で問題は、消費者の知識や同意がなされず、データの正確性を保証できなくなる
- 消費者は健康トラッカーを使用してもよいが健康関連の目的のためだけに集められたデータは、将来的に健康保険や生命保険に値を付けたり、ユーザーの信用や雇用への適合性に使われる
 - 例えば、良心的な訓練者は良い信用リスクまたは良い従業員を作る
- そうしたタイプの意味決定を「他がする企業に好ましい指示に従えない、またはしない」特定のグループに対して体系的に偏る、または保護された集団に対して差別的な実行に導くという懸念がある

法律による問題

- 公正な信用報告法（以下「FCRA」）：消費者データの使用する一定の制限に関する、クレジット、保険、または雇用、または同様の目的のために使用される
 - データの正確性の確保、消費者による情報アクセスなども報告に含まれる

ただし

- FCRAは一般にIoTデバイスをカバーしない
 - 独自のインハウス分析を行うメーカーも対象外
 - 企業デバイスを使用し、消費者の接続された顧客から「直接データを収集」し、そのデータを使用して社内のクレジット、保険などを作成し、適格性の決定する等
- 例えば、保険会社は、消費者ウェアラブルフィットネストラッカーからデータを提出するオプションを提供、健康保険料を引き下げる
 - つまり、FCRAの規定が提供する、情報にアクセスして情報エラーを修正する能力を要求するなどは、IoTでは適用されないことがある

製造業者や侵入者による盗聴

- 製造業者または侵入者が、遠隔から「盗み聞き」またはプライベート空間に侵入する
- 企業は「IoTデータをいかに見るか」を考えている
 - 暗号化されていないスマートメーター装置から送信されたデータなどを見る→個人がどのテレビ番組を見ていたかを判断することができる
- セキュリティカメラの脆弱性

セキュリティとプライバシーに対して認知できるリスクは、それが現実に無くても、完全なポテンシャル（可能性）に適合する技術を必要とする消費者の信頼を覆しうるし、結果的にIoTの普及率を低くするだろう

- 「プライバシーとデータ保護の原則の促進」がIoTサービスの社会的受容を確実にするために最も重要である

Internet of things Privacy & Security in a Connected World

- 通知と選択肢(1)



消費者とのインターフェースが無ければ選択肢（オプション）の提供は不可能であり、また万能の手法も存在しない

選択肢	概要
販売視点での選択肢	自動車産業（の参加者の意見）では、購入時にオプトイン選択を提供する
チュートリアル（個別指導）	Facebook ではプライバシー設定ページにて消費者を案内するビデオチュートリアルを提供、IoTデバイス製造者は自動車の例と同様に消費者に説明と選択肢を提供できる
装置にコードをつける	製造業者はQRコードまたはバーコードをつけ、スキャン時にWebサイトのインターフェースを利用し消費者を適切なデータ実行によってWebに誘導し、選択肢を与える
設定時での選択	多くのIoTデバイスは初期設定ウィザードを持ち、企業は明確で目立った意味あるプライバシー選択肢を提供できる

消費者とのインターフェースが無ければ選択肢（オプション）の提供は不可能であり、また万能の手法も存在しない

選択肢	概要
管理ポータル／ダッシュボード	初期設定での選択肢に加えて、IoTデバイスにおいて消費者が設定／再訪できるプライバシー設定メニュー例えば、モバイル環境ではAppleとGoogle（Android）はダッシュボード手法を提供、位置情報や連絡先（Apple）などのデータ要素に基づく手法、または個々のアプリに囲まれた手法（Android）、コネクテッド家電機器のための「コマンドセンター」も同様のプライバシーダッシュボードを組み込むことができる 適切に実装されたダッシュボードアプローチは、どの情報を共有するかを決定する明確な方法である
アイコン	デバイスはインターネット接続のオン／オフを切り替えるトグルを伴う形で、アイコンを使用し重要な設定／属性を迅速に伝える。
消費者要求に基づく アウトオブバンド通信 (帯域外通信)	表示または利用者の注意が限定されている場合に重要なプライバシー情報とセキュリティ設定を別チャンネルで伝えることができる (例えば、ある家電製品では重要な情報を電子メールまたはテキストで受け取るようにデバイスを設定することができる)

消費者とのインターフェースが無ければ選択肢（オプション）の提供は不可能であり、また万能の手法も存在しない

選択肢	概要
一般的なプライバシーメニュー	上記で説明した特定の設定と選択のタイプに加えて、デバイスとその消費者は選択肢を「パケット（小包）」にまとめることができる。設定の明確かつ顕著な説明を伴う「低プライバシー」、「中」、「高」などのより一般的な設定が必要な場合がある
ユーザー経験に基づく手法	IoTデバイスに紐づく消費者行動の学習に適応した方法で、パーソナライズ（個別化）の選択に基づく（例として、2つ以上のデバイスを提供する製造業者は、消費者の好みを1つのデバイス（「第三者に第三者に情報を送信しない」）を使用してデフォルトを設定、別のものに優先する。別の例として、家電「ハブ」のような単一装置は、消費者の家庭内ネットワークのデータをローカルに格納することで、消費者の以前の動作での選好を学習し将来のプライバシーの選好を予測する新しいアプライアンスを提供する

Internet of things Privacy & Security in a Connected World

- プライバシーとセキュリティの法律(1)



委員会スタッフが議会にプライバシーとセキュリティの法制化を促す一方、既存のツールを活用しIoT企業が新規デバイスおよびサービス開発においてセキュリティとプライバシーを考慮するよう活動を継続する

利害関係者	概要
法執行機関	委員会は、FTC法、FCRA、児童オンラインプライバシー保護法、HI-TECH法の健康違反通知規定、その他IoTに適用される法律を施行する。委員会は違法とみなされる場合、権限を行使しなんらかのアクションを実行する。(TRENDNet事件は、欧州委員会の最初のIoTケース。IoTを製造する企業のケース、すなわち合理的なセキュリティを維持しないデバイス、プライバシー慣行に照らした虚偽表現、FCRAの要件に違反するクレジット、雇用、保険、その他の適格性の決定などを引き続き探索する。スタッフは、強力なFTCの法執行機関の存在がコネクテッドデバイスの製造と販売を行う企業の適切なプライバシーとセキュリティ保護の慣行を奨励する助けになると信じている
消費者 およびビジネス教育	消費者は、自分のIoTのプライバシーに関する詳細情報を得る方法を理解する必要がある (IoTデバイスに接続するホームネットワークを保護する方法、デバイスの使用方法、利用可能なプライバシー設定について)。これにより、企業、特に中小企業はIoTデバイスを合理的に保護する方法に関する追加情報の恩恵を受ける。委員会のスタッフはこのエリアで新しい消費者およびビジネス教育資料を開発する予定

委員会スタッフが議会にプライバシーとセキュリティの法制化を促す一方、既存のツールを活用しIoT企業が新規デバイスおよびサービス開発においてセキュリティとプライバシーを考慮するよう活動を継続する

活動	概要
複数の利害関係者グループへの参加	現在、委員会のスタッフは、IoTに関連するガイドラインを検討中の様々なグループと協力している（例：NTIAの顔認識のガイドラインを検討している複数のステークホルダーグループ、およびスマートメーターのガイドラインを作成する省庁のマルチステークホルダー）法律がない場合でも、これらの努力はコネクテッドデバイスの開発企業のベストプラクティスにつながり、消費者に大きな利益をもたらす。委員会スタッフは引き続きマルチステークホルダー・グループに参加し、IoTに関連するガイドラインを開発する
政策提言 (アドボカシー)	委員会のスタッフは必要に応じてアドボカシーの機会を探す。他の機関、州議会、裁判所と協力して、この分野における保護を促進する。とりわけ、スタッフはこのレポートで説明したプライバシーやセキュリティの問題のベストプラクティスを他の政府機関は確実に考慮している

- IoTは消費者に多くの利益をもたらす消費が基本的な方法に基づく技術と相互作用する方法を変化させる可能性がある。現状理解するのが難しいが、将来、IoTは仮想世界と物理世界を融合させる可能性が高い
- セキュリティとプライバシーは、センサーやデバイスが現在の親密な空間（家庭、車、ウェアラブル、撮造物、身体など）への普及導入にとって、特別な難題
- 日々の生活の中の物理オブジェクトは、より人間を検出し、観測情報を共有するが、消費者は恐らくプライバシーを守り続けるだろう
- 欧州委員会の職員はIoTに関与する適切なセキュリティとプライバシーの保護を促進するために引き続き法律を執行し、教育を行い、消費者と企業、そして消費者の支持者、業界、学者、他のステークホルダーなどに関わるだろう
- 同時に、我々はデータセキュリティの制定と幅広いプライバシー保護法に基づいてIoTに関するさらなる自主規制の努力を急ぐ

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

IoTデバイスの安全性確保のための現在のベストプラクティクス

Best Current Practices for Securing Internet of Things 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**を列挙している。

[\[Docs\]](#) [\[txt\]](#) [\[pdf\]](#) [\[Tracker\]](#) [\[Email\]](#) [\[Nits\]](#)

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>

Best Current Practices for Securing Internet of Things Devices

- 以下の属性でまとめている



No	ポイント	内容
1	対象レイヤ	ソフト・ハードウェアの記載が中心
2	対象者	IoT (Internet of Things) デバイスの開発やファームウェアアップデートを作成するベンダー
3	対象インダストリー	共通
4	文書の位置付け	国際標準： Internet Draftとして公開されている
5	詳細度評価	概要レベル： ニーズにより各デバイスに固有のセキュリティの考慮事項があるため、本文書では特定の技術的解決策の推奨は避け、すべてのデバイスに適用される最小要件を述べている

Best Current Practices for Securing Internet of Things Devices

- レポートの項目



IoTデバイスは、ニーズにより各デバイスに固有のセキュリティの考慮事項があるため、本文書では特定の技術的解決策の推奨は避け、すべてのデバイスに適用される最小要件を述べている

No	項目	概要	Page
1	Introduction	IoTに関わるセキュリティインシデントが多く発生している中、それらのインシデントを予防するために、行うべき最小限のセキュリティ要件を紹介し、本文書での用語を定義	03~05 (3P)
2	Design Considerations	インターネットに接続されたデバイスは、許可なく意図しない目的で使用されるような攻撃から自分自身を保護するべきとして、設計、暗号、認証等について考慮すべき点を述べている	05~11 (7P)
3	Implementation Considerations	デバイスのセキュリティに必要な実装として、製品に暗号品質乱数を生成するためのソリューションを含まなければならない	11 (1P)
4	Firmware Development Practices	ファームウェアの開発の要件として、コード・バグ管理やセキュリティテストにシステムを利用することを推奨し、セキュリティバグ、脆弱性等の定期的なチェックを推奨	12 (1P)
5	Documentation and Support Practices	製品販売後のセキュリティ対応の為のアップデートの作成、サポート期間の設定、バージョン管理、情報提供方法等	12~13 (2P)
6	Security Considerations	ドラフト段階の為、作成途中	13 (1P)
7	IANA Considerations	ドラフト段階の為、作成途中	14 (1P)
8	Acknowledgements	ドラフト段階の為、作成途中	14 (1P)
9	References	参照RFC番号及びURL	15 (1P)

Best Current Practices for Securing Internet of Things Devices

- 設計上の考慮点



No	ポイント	内容
1	General security design considerations (一般的なセキュリティ設計)	IoTデバイスのセキュリティを確保するために意図しない外部からのアクセスや認証情報・受信情報の保護等を行う そのために製品に存在する脅威を分析を行い、標準化・確立されているアルゴリズム、プロトコルを使うべき
2	Authentication requirements (認証要件)	デバイスは、認証に使用される秘密を保護するように設計されなければならないとしている、認証機構に対するDoSに耐えうる設計をすべき
3	Encryption Requirements (暗号化要件)	インターネットに接続されたデバイスは、暗号化する機能をサポートし、適切な強度の暗号を利用すべきとしている。ただし、認証情報は絶対であり、他の情報に関しては要検討
4	Firmware Updates (ファームウェアアップデート)	デフォルトで自動アップデート機能を提供すべきとして、段階的な更新およびアップデート時の認証を取り入れるべき
5	Private key management (秘密鍵管理)	秘密鍵を利用した認証の場合、デバイスごとの秘密鍵はデバイス上で生成されるべきであり、デバイスの外部に公開されるべきではない
6	Operating system features (オペレーティングシステムの機能)	ファームウェアに、メモリ区画化技法を実装し、使用許可のないプロセスによるメモリ領域の読み取り、書き込み、実行を防止するように設計されるべきとしている。また、ファームウェアの特権を最小化し、アクセスする必要のない部分から特権コードとデータを分離するように設計されるべき

- この文書はIETFのインターネットドラフトであり、文書の効力は発行日から6ヵ月の間のみとしている
- bcp-00は2016/10/31に発行、2017/5に失効した。
- その後、bcp-01が2017/7/3に発行されたが、2018/1/4に失効している
- IETFの仕組み上、内容が有用とされるとRFC番号が振られて恒常的に参照可能なドキュメントとなるとしているが、確認できていない
<https://www.nic.ad.jp/ja/basics/terms/ietf.html>

Industrial Internet Security Framework

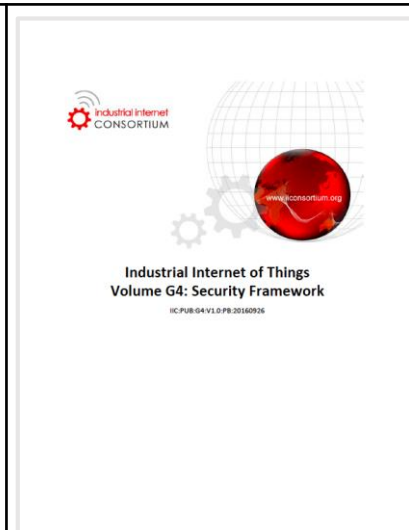
インダストリー インターネット セキュリティ フレーム
ワーク

Industrial Internet Security Framework 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含めたベストプラクティスで構成されている。想定すべきリスクと対策の概論が記載されているが、ベストプラクティスと謳いつつ、日本人が期待するすぐに使えるものではなく、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>

Industrial Internet Security Framework

- レポートの項目



No	項目	概要	Page
1	Overview	文書の目的や適用範囲（IIRAで規定）、想定利用者、IICの他の文書との関連を解説	11-12
2	Motivation	IIoT、IT/OTの融合に伴う安全対策の重要性	13
3	Key System Characteristics Enabling Trustworthiness	対象となるシステムの特徴を理解することで、弱点とその対策が明らかになり、堅牢なシステムのための五つの要素の関連を解説	15-20
4	Distinguishing Aspects of Securing the IIoT	ITとOTの融合に伴い、システムの特徴が変化する。いままでとは異なる状況に合わせるための基礎的な考え方を解説	21-24
5	Managing Risk	IIoTはビジネスの文脈で語るが、ビジネス上のリスクの扱い方についての基本を解説	27-34
6	Permeation of Trust in the IIoT System Lifecycle	ライフサイクルや信頼など、IIoTの複雑な構成を解説	36-43
7	IISF Functional Viewpoint	通信、データなどの保護など、IISFの構造と構成要素についての解説	46-58
8	Protecting Endpoint	エンドポイント保護を、ハードやCPU、仮想化環境などの技術、ライフサイクルやサプライチェーンの影響を加味した包括的に解説	60-80
9	Protecting Communications and Connectivity	ITネットワークと制御ネットワーク、各種プロトコルや無線通信規格など踏まえて代表的な対策を解説	82-95
10	Security Monitoring and Analysis	セキュリティ状態の監視プロセス、予知や検知などIRのためのプロセスなどの概説	96-103
11	Security Configuration and Management	セキュリティ環境の構成や変更と管理についての概論	105-120
12	Looking Ahead – The Future of IIoT	継続して本文書の更新を進めていく基となるのはテストベッド	121
13	Annexes (A to G)		125-150

Industrial Internet Security Framework

- 目的：Trustworthinessの実現

Trustworthinessを実現するために五つの要素を適切に扱うことで脅威に対抗することができる

実現するための要素
Security
Safety
Reliability
Resilience
Privacy

脅威
Attacks
Errors
Disruptions
Faults

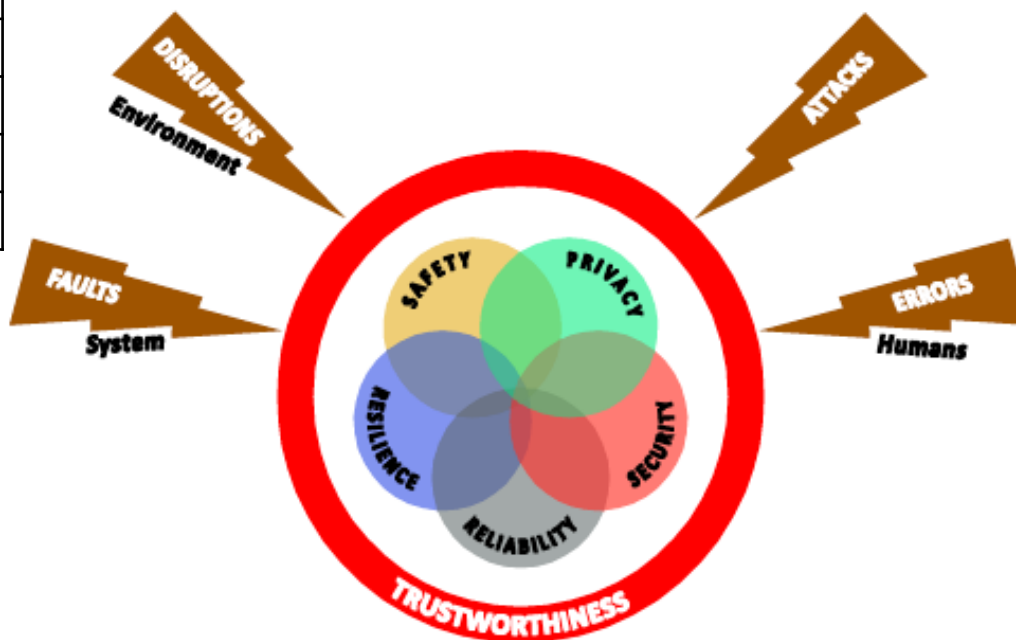


Figure 3-1: Trustworthiness of an IIoT System

Industrial Internet Security Framework - IIoTシステムはITとOTの融合

IIoTのセキュリティはITとOTで実現

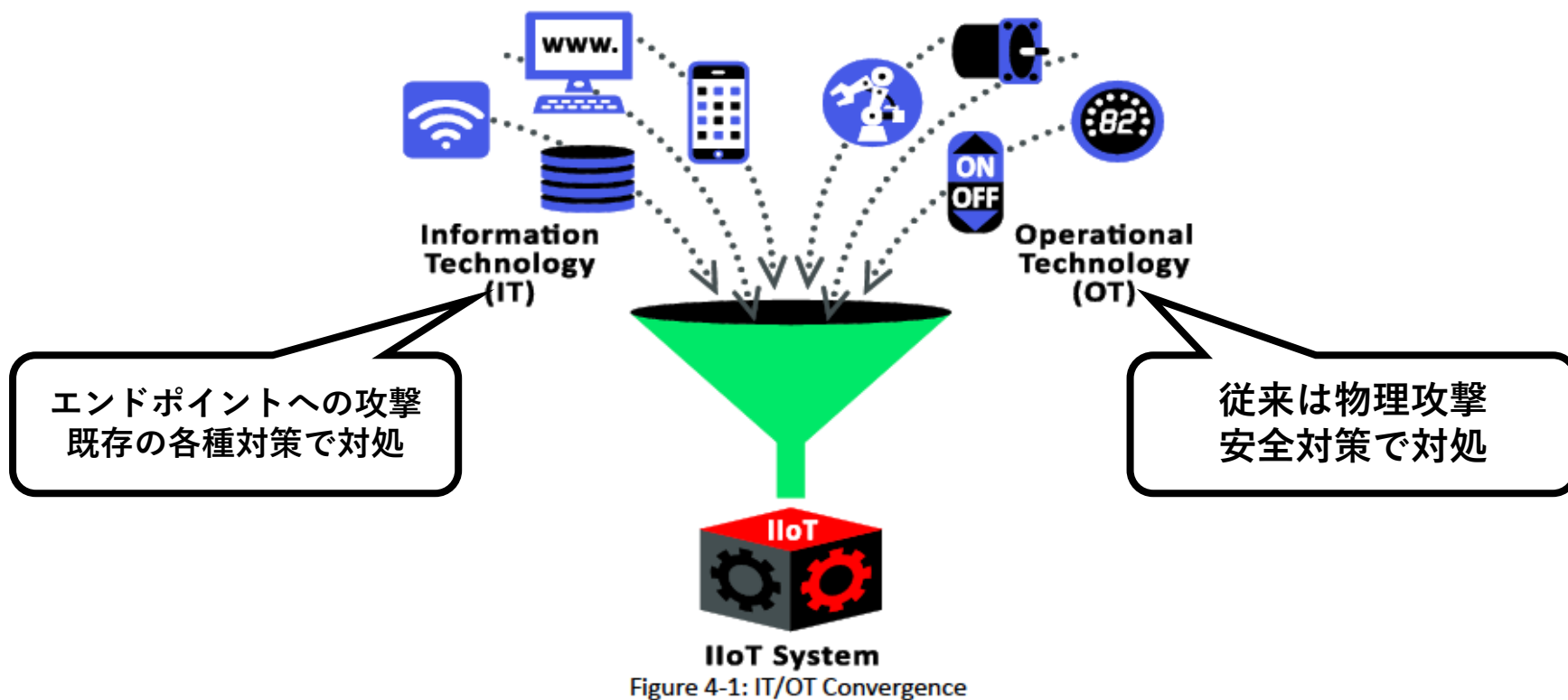
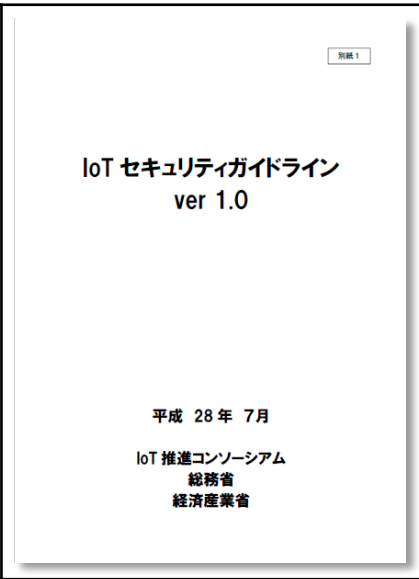


Figure 4-1: IT/OT Convergence

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	2016年07月05日初版
	
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/

IoTセキュリティガイドライン

- ガイドラインの項目



方針、分析、設計、構築・接続、運用・保守の各段階で21の要点を提示している

No	項目	概要	Page
—	はじめに	この文書の書かれた状況や期待事項の定義を行っています。	01~02 (2P)
1	背景と目的	この文章の背景について、「動向と近年の脅威事例」→「IoT特有の6つの性質」という流れで説明しています。 この文章の目的について、IoTのイメージや対象読者について説明しています。対象読者については、供給者（経営者、機器メーカー、システム・サービス提供者／企業利用者）、利用者のそれぞれで何章を読むべきかが定義されています。	03~11 (9P)
2	IoTセキュリティ対策の5つの指針	「方針」、「分析」、「設計」、「構築・接続」、「保守」の大項目について、5つの指針と、21の要点について対策例を交えて具体的に解説を行っています。 主に供給者向けの内容となっており、どのような理由で対策を行うべきかが解説されています。	12~54 (42P)
3	一般利用者のためのルール	IoT機器を利用する一般利用者向けに、利用者の視点で気をつけるべき事項が5つのルールにまとめられています。	55~56(2P)
4	今後の検討事項	今後に向けて検討が必要な項目について具体例が記載されています。	57~58 (2P)
	付録	略称一覧	-

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る。

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る。

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紐付けられており、客観性がある資料となっている。

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る（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る）。



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>

IoT開発におけるセキュリティ設計の手引き

- 手引きの項目



IoTのセキュリティ設計について具体例を使って説明を行っている

No	項目	概要	Page
1	はじめに	本文書のねらいとその背景を説明しています。	06~08(3P)
2	本書におけるIoTの定義	本文書でIoTセキュリティを検討するためにモデル化したIoTの全体像と、その構成要素について説明しています。	09~11(3P)
3	IoTのセキュリティ設計	IoTのセキュリティ設計の手順である、脅威分析と対策検討、さらにセキュリティ対策の一つである脆弱性への対応について、説明しています。	12~24(13P)
4	IoT関連のセキュリティガイド	IoTのセキュリティを検討する上で参考となるIoT関連のセキュリティガイドとして、OWASP、OTA、GSMAのガイドを紹介しています。	25~30(6P)
5	IoTシステムにおける脅威分析と対策検討の実施例	IoTシステムの脅威分析と対策検討について、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題材にして、具体的に説明しています。対策については、OWASP、OTAのガイドの要件との紐付けも行っています。	31~61(31P)
6	IoTセキュリティの根幹を支える暗号技術	適切な暗号技術を導入しても、鍵の取り扱いに不備があれば、その脆弱性をついた攻撃が行われることを述べています。	62(1P)
-	付録	付録A. OWASP Internet of Things Projectの成果概要 付録B. OTAIoT Trust Frameworkの概要 付録C. IoTにおける暗号技術利用チェックリスト 付録D. 「つながる世界の開発指針」と本書の対応	-

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）	
<p>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。</p>		
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	

つながる世界の開発指針

- 指針の項目



方針、分析、設計、保守、運用の各段階で17の開発指針を提示している

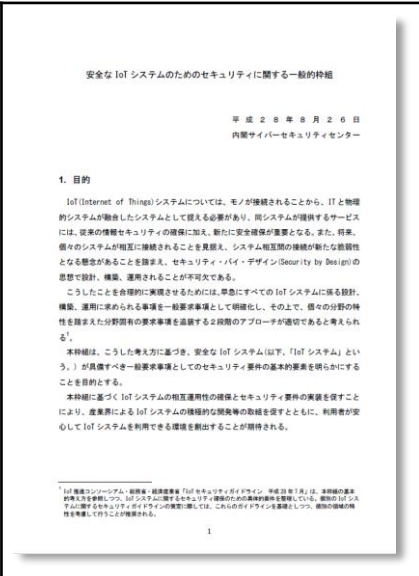
No	項目	概要	Page
	はじめに	この文書の読んで欲しい読者層の明示や安全安心の定義を行っています。	01~07 (7P)
1	つながる世界と開発指針の目的	本開発指針の目的について、「つながる世界とは何か」→「つながる世界では、何が危ないのか」→「本開発指針は何を目指すのか」という流れで説明しています。	08~18 (11P)
2	開発指針の対象	本開発指針が既存のIoT規格とどのような関係があり、どのような位置付けのもとでIoTのどの部分に焦点を当てているかを説明しています。	19~26 (8P)
3	つながる世界のリスク想定	開発指針策定の前提となるIoTのリスクについて、IoTをどのような軸で整理し、どのような手順でリスクの想定を行ったかを説明しています。	27~31(5P)
4	つながる世界の開発指針	17の開発指針について、対策例を交えて具体的に解説を行っています。分析、設計というIoTシステムの開発だけでなく、そのシステムを保守、運用、さらにはその前提となる企業の方針まで、網羅的に指針を定めています。	32~88 (57P)
5	今後必要となる対策技術例	開発指針を実現するために今後必要になることが想定される対策技術について、説明している。	89~93 (5P)
-	おわりに、付録A	A1. 本開発指針の活用方法 (チェックリスト) A2. 開発指針の導出手順 A3. つながる相手の品質判断の例 A4. つながる機器の異常検知の例	-

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	
	<p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none">・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	

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

- 枠組の項目



枠組として、基本原則とその取組方針を示している

No	項目	概要	Page
1	目的	本枠組の目的とその背景、また本枠組の促進により期待される効果を説明しています。	01
2	検討の視点	本枠組を検討するに当たって重要な視点（安全性の考慮、IoTシステムの集合体“System of Systems(SoS)”と捉えること）を提示しています。	02
3	基本原則	本枠組のベースとなる基本原則を明確化するとともに、IoTシステムのセキュリティ確保のためにシステムの設計・開発、構築、運用・保守の各段階で明確化すべき項目を、6段階に分けて説明しています。	02~03
4	取組方針	本枠組を促進していくための取組方針を7つに分けて示しています。 1. 要求事項の明確化 2. IoTシステムのモデル化 3. リスクに応じた対応 4. 性能要求と仕様要求の適切な運用 5. 段階的・継続的アプローチ 6. 役割分担及び連携した対処のあり方の明確化 7. その他運用ルールの検討	03~04
5	留意事項	本枠組における留意事項を説明しています。	05

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

- 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>

INTERNET OF THINGS : RISK AND VALUE CONSIDERATIONS

- レポートの項目



本文書はホワイトペーパーとして発行されておりページ数は多くない

No	項目	概要	Page
1	モノのインターネット：リスクと価値の考察	まえがき。本ホワイトペーパーのサマリが記載されています。	04 (1P)
2	モノのインターネットとは何か?	IoTの定義、IoTによって得られるビジネスにおける価値やリスクについて概要を説明しています。	05 (1P)
3	成熟そして採用	ISACAが、本ホワイトペーパーを発行する前に実施した調査結果にもとづいて、IoTは黎明期ではなく既に成熟しており、組織におけるIoT取り組みが始まっている事が説明がされています。	06~07 (2P)
4	価値の提供	IoTに取り組むことによって価値を得ている事例を説明しています。また、リスク管理の専門家以外は、IoTのビジネス価値を重視しそのリスクを軽視しがちであることについて触れられています。	08(1P)
5	リスクとリスク軽減	IoTに取り組むことによって価値が得られる反面、新たなリスクを抱えることになることが記載されています。IoTデバイスのユーザーに関連するリスクを挙げてそれぞれについて説明しています。	09~11 (3P)
6	専門家が問うべき質問	得られる価値とリスクを受けて、IoTに取り組む組織においてアシュアランス、セキュリティ、リスク管理の実務者(専門家)が問うべき9つの質問を挙げています。	13(1P)
7	何をすべきか、何をすべきでないか	これまでの説明を要約した表を記載しています。	12(1P)
8	結論	おわりに。IoTは非常に巨大な可能性を秘めており、既に普及し始めているが益々利用が広がる。IoTに取り組むことによって抱えるリスクについても気遣う必要があることが述べられています。	13(1P)

INTERNET OF THINGS : RISK AND VALUE CONSIDERATIONS

-リスク項目



新しい技術、プロセス、ビジネス方法はリスクを増加させる可能性があり、IoTはその普及によりこれらのリスクを大幅に増加させる可能性があるとして、下記3カテゴリを挙げている

リスクカテゴリ	リスク項目
ビジネスリスク	健康・安全
	法令・コンプライアンス
	ユーザプライバシー
	予想外の費用
オペレーショナルリスク	機能への不適切なアクセス
	シャドールーザ
	パフォーマンス
テクニカルリスク	デバイスの脆弱性
	デバイスのアップデート
	デバイスの管理

INTERNET OF THINGS : RISK AND VALUE CONSIDERATIONS

- 9つの問い



IoTに取り組む組織が考えるべき下記9つの問い、ビジネス価値とリスク両方の考慮などが特徴的

No	9つの問い
1	ビジネスの観点からデバイスをどのように使用し、どのようなビジネス価値を期待するか？
2	どのような脅威が予想され、どのように緩和できるか？
3	誰がデバイスにアクセスでき、そのアイデンティティはどのように確立され、証明できるか？
4	攻撃や脆弱性が発生した場合にデバイスをアップデートするプロセスはどのようなものか？
5	デバイスに関連する新しい攻撃や脆弱性の監視は誰が担当するか？
6	リスクシナリオを評価し、予想されるビジネス価値と比較したか？
7	どのような個人情報がIoTデバイスによって収集、保存、処理されるか？
8	情報が収集されている個人は、収集され使用されていることを知っており、同意を得ているか？
9	データは誰と共有されるか？

INTERNET OF THINGS : RISK AND VALUE CONSIDERATIONS

- 結論



結論として、「すべき事、してはならない事」が整理されている

何をすべきか

- 脅威モデルの準備
- ビジネス価値の評価
- 全体的な評価とリスク管理
- リスクと効果のバランスを取る
- 全てのステークホルダーに予想される使用方法の通知
- ビジネスチームとの早期からの連携
- 全てのステークホルダーの関与と徹底的な計画の立案
- 既存のセキュリティと運用保護との統合
- 可能性のあるプライバシーへの影響を分析するために、デバイスによって収集され、送信される情報を調査し文書化
- ステークホルダーと、情報がどのように共有され、どのような状況でどのように共有されるのか、どのように関係するかについての協議

何をすべきでないか

- 他のステークホルダーに相談することなく迅速に展開
- セキュリティやプライバシーなど、既存のポリシー要件の無視
- 規制義務の無視
- ベンダー（ハードウェア、ソフトウェア、ミドルウェアなど）が特定の使用法やセキュリティ要件を考えているとの誤まった仮定
- デバイス固有の攻撃や脆弱性の無視
- プライバシーの考慮不足、またはエンドユーザーから収集/送信されるデータの隠ぺい

NIST SP 800-160

Systems Security Engineering

システムズ セキュリティ エンジニアリング

NIST SP 800-160 Systems Security Engineering



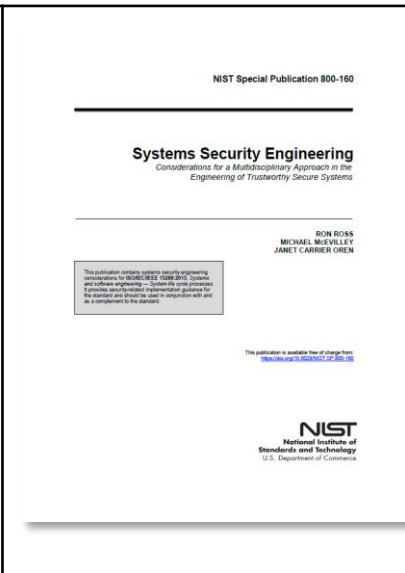
発行

2016年11月

システムのセキュリティ・エンジニアリングの概念や考え方から、システムの各ライフサイクルプロセスでセキュリティをどのように組み込むべきかなどを記述した包括的なガイドである。IoTに特化した記述はない。

特定の実装を提供するのが目的ではなく、各システムやアプリケーションに必要なセキュリティ機能を特定するためのカタログあるいはハンドブックとして使うことを推奨している。

全体にセキュリティは単独で考える要件・機能ではなく、システム全体の中で考慮され検討されるべきという考え方が示されており、ライフサイクルプロセスについてはISO/IEC/IEEE 15288 Systems and software engineering -- System life cycle processesを参照して記述されている。



参考別紙

なし

Topic

NIST SP 800-160 Systems Security Engineering

URL

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>

NIST SP 800-160: Systems Security Engineering

- レポートの項目



No	項目	概要	Page
1	INTRODUCTION	文書の目的や適用範囲、想定読者などを解説	1-6
2	THE FUNDAMENTALS	Systems security engineering の規範についての解説、システムと構成要素、環境やあらゆる運用環境についての定義の確認と、セキュリティの観点でどのように保護を実現するか、妥当性やアーキテクチャ、トラストワージネスや保証についてなどについて。概念についての解説。	8-24
3	SYSTEM LIFE CYCLE PROCESS	ISO/IEC/IEEE 15288 標準を拡張したライフサイクルプロセスの検討に基づく解説。こちらも概論のため、実用的な内容にまで噛み砕かれていない。	26-152
4	APPENDIX A, B, D, E, F, G	リファレンスおよびグロッサリー、略称などの補足	157-164

ITU-T Recommendation Y.4806 Security capabilities supporting safety of the Internet of things

IoTの安全をサポートするセキュリティの能力

ITU-T Y.4806

Security capabilities supporting safety of the Internet of things



発行

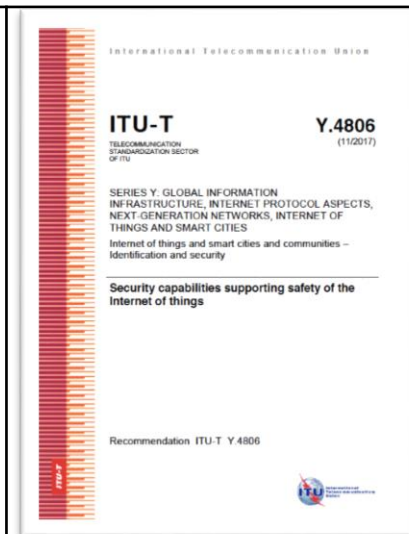
2017年11月

IoTがもたらすセキュリティ上の脅威を分類し、それぞれがどのように「安全」に影響をもたらすかについて検討している。

また、ITU-T Y.4401/Y.2068 で示したセキュリティ能力がどのようにIoTの安全に役立てることができるかについて提示している。

あくまでも推奨であることを明確にするため、Recommendation と明記しているが、想定される脅威に対してどのような対処が可能かについて例示している点からより多くの人に理解しやすいと思われる。

ITU-TはYで始まるシリーズを、100～4999まで個別のテーマに即して提供しておりPDFで入手できる。



参考別紙

なし

Topic

ITU-T Y.4806 Security capabilities supporting safety of the Internet of things

URL

<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13391>

ITU-T Y.4806

- 項目



No	項目	概要	Page
1	Scope	Y.4401で定義したセキュリティ上の脅威を元に安全への影響を検討したものであるのが本文書であると宣言。また、対象は安全が重要となるIoTが対象としている	1
2	References	[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012) [ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014) [ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015) を参照	1
3	Definitions	主要な用語の参照先	1-2
4	Abbreviations and acronyms	IoTなどの略語などを説明	3
5	Conventions	なし	3
6	Classification of security issues in the Internet of things by their impact vector	本書の重要な章で、IoTの影響の有無 (Impact Vector) について概念をベクターを用いて説明している。ここで、V:Virtual (仮想)、T:Thing (モノ)、P:Physical (物理) を用いて分類している	6-10
7	Security threats affecting safety in the Internet of things	安全に影響のあるセキュリティ上の脅威を五つに分類して説明	10-11
8	Security capabilities for supporting safety in the Internet of things	上記への対策の基本はY.4401では6種類あるとしている。Communication security capability [C-7-1]、Data management security capability [C-7-2]、Service provision security capability [C-7-3]、Security integration security capability [C-7-4]、Mutual authentication and authorization security capability [C-7-5]、Security audit security capability [C-7-6].	12-32
9	Appendix I	特定された脅威に対する対処の例示だが、上章とは直接関連しないが本書の中ではもっともわかりやすい。脅威と対策が一覧で例示されている。	33
10	Bibliography	-	-

OTA IoT Trust Framework(V2)

OTA IoT トラスト フレームワーク (V2)

OTA IoT Trust Framework(V2)

発行

2017年1月

IoT向けセキュリティ機能のフレームワーク（一種のチェックリスト）である。Online Trust Allianceというインターネットの技術革新や活力促進を支援する非営利団体が作成した。

モノのインターネット（IoT）デバイスの開発者や購入者、販売業者向けの製品開発やリスクマネジメントのガイドの役割を果たし、将来のIoT認証プログラムの基礎となるように作成したとされている。

デバイスのライフサイクルセキュリティの方針を示し、消費者がIoTデバイスの購入を決める際の判断材料になることを目標に掲げる。

IoT Trust Frameworkには37の指針が含まれており、それらは4つの主要なカテゴリーに分類される。



参考別紙

なし

Topic

IoT Trust Framework

URL

<https://otalliance.org/initiatives/internet-things>

OTA IoT Trust Framework(V2)

- カテゴリー(1)



IoT Trust Frameworkには37の指針が含まれており、それらは4つの主要なカテゴリーに分類される

項目	説明
セキュリティ (1～9)	<ul style="list-style-type: none">• 全てのデバイスやそのアプリケーション、バックエンドクラウドサービスに適用可能• これらは、厳格なソフトウェア開発のセキュリティプロセスの活用、デバイス上で保存や送信が行われるデータに関するセキュリティ指針の遵守、サプライチェーンの管理、ペネトレーションテストと脆弱性報告のプログラムを含む• さらなる指針では、ライフサイクルセキュリティのパッチの要件について概説
ユーザーアクセスと認証 (10～14)	<ul style="list-style-type: none">• パスワードとユーザー名の全ての暗号化の要求• 独自のパスワードを設定したデバイスの出荷• 一般的に受け入れられるパスワード再設定のプロセスの実装• 『総当たり (ブルートフォース)』攻撃によるログインの試みを防止する際に役立つメカニズムの統合の要求

OTA IoT Trust Framework(V2)

- カテゴリー(2)



項目	説明
プライバシーと情報開示、 透明性 (15~30)	<ul style="list-style-type: none">• 一般的に容認されているプライバシー指針に準拠することの要求• (製品の) パッケージ、販売場所、オンラインの掲示において目立った情報開示を行う• 工場出荷時設定に復元できる機能を提供• EU General Data Protection Regulation (GDPR/EU一般データ保護規則) やChildren's Online Privacy Protection Act (COPPA/児童オンライン・プライバシー保護法) などを含めた(これらの規制に限らず)、適用される規制要件に準拠• インターネットに接続されていないとき、その製品の機能や機能にどのような影響が出るのか開示
通知、およびそれに関連した ベストプラクティス (31~37)	<ul style="list-style-type: none">• デバイスのセキュリティを維持する鍵は、脅威について、また必要とされる行動について迅速にユーザーへ通知するメカニズムやプロセスを持つこと• 指針には「セキュリティの通知を行うためのメール認証の要件」が含まれており、また、そのメッセージは全ての世代、あらゆる読解力のユーザーにも分かるように明確に書かれていること• 不正改造を防止する加工が施された造りや、ユーザー補助の要件を強調

OTA IoT Trust Framework(V2)

- セキュリティ(1~9)



1. デバイスと関連するアプリは一般的なセキュリティ機能やプロトコルをサポートする
2. すべての通信（有線無線に関わらず）暗号化をサポートする
3. IoTをサポートするサーバーのサイトはセキュリティ対策や脆弱性対を継続的に実施し 一年に一度はペネトレーションテストを行う
4. 出荷後の脆弱性対応や脅威を公開するなどの対策をする Bug Bounty制度も検討する
5. セキュアなソフトウェアやハードウェアのUpdateの仕組みを持つ
6. IoT関連ソフトウェアの開発プロセス・ライフサイクルを確立する
7. サービス・クラウドプロバイダーのリスクアセスメントを行う
8. 使用しているライブラリーやソフトウェアなどのリストを作りメンテナンスする
9. 運用のための機能（外部インターフェース）は最小限とする

OTA IoT Trust Framework(V2)

- ユーザーアクセスと認証 (10~14)



1. デフォルトで、システムが生成するユニークなパスワードやワンタイムパスワードなど強力な認証を利用
2. セキュアな証明書を資格情報として使用することも可能。必要に応じて、管理者アクセス、デバイスとサービスの間の認証、工場リセット時にもユニークなパスワードを使用する必要がある。一般的に受け入れられているやり方でIoTアプリケーションの認証情報の再設定方法を提供すること。ユーザーパスワードが存在しない多要素認証（電子メールや電話など）を使用して、クレデンシャルを再設定するためのパスワードや方法をサポートする
3. 合理的な回数以上に無効なログイン試行があった場合、ユーザーおよびデバイスのサポートアカウントをロックまたは無効にすることにより、「ブルートフォース攻撃」やその他の不正なログイン試行（自動ログインボットなど）から保護する
4. 安全な認証または域外通知を利用して、ユーザーにパスワードのリセットまたは変更をされたことを通知する
5. ユーザーのパスワードを含む認証情報は、隠ぺい、ハッシュ、および暗号化されるものとする。それは格納されているすべての資格情報に適用され、不正アクセスや総当たり攻撃を防止する

15. プライバシー、セキュリティ、サポートのポリシーは、買い物、アクティベーション、ダウンロードなどを実行する前に準備されていて、見つけやすくわかりやすいものに。わかりやすくする手法の具体例あり
16. セキュリティやサポートの期限の開示、消費者が購入する前にわかるよう製品寿命とともに。IoTには必ずしもPatchが当てられないとわかっている。そういったリスクも伝えておくべき
17. どのような個人情報・機微情報が収集されるか開示
18. バックエンドサービスの停止で、物理的なセキュリティ機能への影響だけでなくどの機能がどのように使えなくなるかを開示
19. データの保持期間について開示
20. IoTデバイスがほかの機器やプラットフォーム・サービスに接続することを通知するかユーザーへ確認 (confirm) を要求
21. IoTデバイスの所有者の変更とデータの移行について公開
22. 消費者の個人情報を第3者と共有する場合は明確な同意を得る

OTA IoT Trust Framework(V2)

- プライバシーと情報開示、透明性 (15～30)



23. プライバシーにかかわる情報を消費者が確認、修正でき、工場出荷状態にリセット可能
24. データ収集源と独立している（関係がない）また同意されたプライバシーポリシーに反しない限り、個人情報（売買も転送もしない）とコミットする。 そうでない場合は同意を取得
25. 使用に先立ってプライバシーポリシーを読んだ時点で消費者が無償で返品ができるよう返品可能な期間を明示
26. ポリシー拒否あるいはオプトアウトにより消費者がどのような機能を使えなくなるかを明示
27. 国内外の規制を遵守
28. プライバシーポリシーの変更履歴を公開
29. デバイスの利用停止、紛失、売却時にデータを削除する機能の提供を推奨
30. デバイスの利用停止、紛失、売却時にデバイスをリセットする機能の提供を推奨

31. エンドユーザーの通信は e-mailやSMSに限らずスパフィッシングやなりすましを防止するために認証プロトコルを採用、個人情報扱う通信には、SPF, DKIM and DMARCを実装
 - SPF : Sender Policy Framework
 - DKIM : Domainkeys Identified Mail
 - DMARC : Domain-based Message Authentication, Reporting & Conformance
32. Email通信については180日以内にDMARCポリシーの発行を推奨
33. Email通信を使用するIoTベンダーはトランスポートレベルでのセキュリティの実装を推奨
34. デバイスに物理的なタンパー対策の実装を推奨
35. 障害者（視覚・聴覚・身体）の利便性についての考慮を推奨
36. エンドユーザーがセキュリティやプライバシーの問題発生に気づき、デバイスの寿命やリコールに気がつくアプリの通知などの一般的なユーザーの理解できる通知プロセスの開発
37. サイバー攻撃などの問題発生とその対応について消費者への通知方法を少なくとも年1回見直す

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。

Category	IoT Security Consideration
11: Insecure Web Interface	<ul style="list-style-type: none">Ensure that any web interface in the product disallows weak passwordsEnsure that any web interface in the product has an account lockout mechanismEnsure that any web interface in the product has been tested for XSS, SQL and CSRF vulnerabilitiesEnsure that any web interface has

参考別紙

なし

Topic

OWASP IoT Security Guidance

URL

https://www.owasp.org/index.php/IoT_Security_Guidance

OWASP IoT Security Guidance の項目



チェックするポイントは以下のカテゴリーに分けられている。
(Manufacturer / Developer/ Consumer の各ガイダンス共通)

No	項目
I1	Insecure Web Interface / 安全ではないWebインターフェース
I2	Insufficient Authentication/Authorization / 不十分な認証・認可
I3	Insecure Network Services / 安全でないネットワークサービス
I4	Lack of Transport Encryption / 通信の暗号化の欠如
I5	Privacy Concerns / プライバシーの問題
I6	Insecure Cloud Interface / 安全でないクラウドインターフェース
I7	Insecure Mobile Interface / 安全でないモバイルインターフェース
I8	Insufficient Security Configurability / 不十分なセキュリティ設定
I9	Insecure Software/Firmware / 安全でないソフトウェア・ファームウェア
I10	Poor Physical Security / 貧弱な物理セキュリティ

Manufacturer IoT Security Guidance の項目例 (安全でないWebインターフェース)



記載されている内容自体は特殊な内容ではなく、最新の動向を踏まえてアップデートされるものである

内容

Webインターフェースが弱いパスワードを許可しないようにする。

Webインターフェースがアカウントロックアウトの機構を持つこと。

Webインターフェースに対して、クロスサイトスクリプティング、SQLインジェクション、クロスサイトリクエストフォージェリに対する脆弱性のテストを行うこと。

Webインターフェースは転送される情報を守るができるようにHTTPSを使用することができるようにしておくこと。

Webインターフェースを保護するためのWebアプリケーションファイアウォールの機能を含めること。

Webインターフェースによりデフォルトのユーザ名とパスワードを変更できるようにしておくこと。

**各自が一通り目を通しておくことに意義のあるものであり
詳細は原典を参照されたい**

□ レポート作成メンバー：

輿石隆	JPCERTコーディネーションセンター
酒井美香	日本IBMシステムズ・エンジニアリング株式会社
柴田康広	日本プロセス株式会社
玉木誠	SCSK株式会社
長坂啓司	日本プロセス株式会社
福田尚弘	パナソニック株式会社
細田将	セコム株式会社
松岡正人	株式会社カスペルスキー

*五十音順、所属は作成時のもの

- 本レポート中で引用している写真・図版や各種情報などの引用元と著作権はそれぞれの引用元をご参照ください
- 本レポートを引用する際には日本ネットワークセキュリティ協会に事前にご連絡ください

<お問い合わせ>

- 本ハンドブックに関する引用・内容についてのご質問はJNSAウェブサイト上の「引用連絡および問い合わせフォーム」からご連絡ください
- 引用のご連絡に対する承諾通知は返信いたしませんので予めご了承下さい
- 報告書についてのFAQもございますので、引用。お問い合わせの際はご参照ください

<http://www.jnsa.org/faq/incident.html>

- お問い合わせフォーム
引用連絡及び問い合わせフォーム
<https://www.jnsa.org/aboutus/quote.html>