転ばぬ先のIoTセキュリティ
～コウカイする前に知るべきこと～

体系的なIoTセキュリティへの取り組み方

2017年 11月 29日
NRIセキュアテクノロジーズ株式会社
ストラテジーコンサルティング部
熊白　浩丈

講師紹介

熊白　浩丈
(Hirotake Kumashiro)

ＮＲＩセキュアテクノロジーズ株式会社
ストラテジーコンサルティング部
マネージャー
上級セキュリティコンサルタント

専門
- 情報セキュリティ監査／システム監査
- SIRT(CSIRT、PSIRT、機密管理）構築、運営支援
- 情報セキュリティ インシデント対応支援
- PCIDSS、セキュリティルール評価・策定

○ 主な支援 / 活動内容

情報セキュリティ監査／脆弱性検査

- 金融機関　：大手金融機関における情報セキュリティ監査
- 金融機関　：大手金融機関における委託先情報セキュリティ監査
- 大手流通企業　：委託先監査、グループ会社情報セキュリティ監査多数
  ：情報セキュリティ格付審査、委託先情報セキュリティ監査
- オフショア開発　：情報セキュリティ監査（シンガポール、インド、中国）
- 大手物流会社　：情報セキュリティ監査、情報セキュリティ評価
- 上場メーカー　：セキュリティポリシー策定、情報セキュリティ評価
- 各社　：不正侵入調査、インシデント対応支援

セキュリティコンサルティング

- CSIRT構築　：CSIRT立ち上げ、運営支援 多数
- PSIRT構築　：PSIRT立ち上げ、運営支援多数
- インシデント対応　：情報漏えい事件対応支援
- オフショア開発　：監査を踏まえた対応計画策定支援
- 各社　：情報セキュリティ規程類 策定支援
- 大手食品メーカー　：委託先管理規程策定支援
- 流通企業　：外部アクセスポイントポリシー策定
- データセンター　：SOC2レポート策定支援

講師紹介

- 作家の「井上ひさし」 さんが生前に繰り返し言っていた言葉です。

「むずかしいことをやさしく、やさしいことをふかく、
ふかいことをおもしろく、おもしろいことをまじめに、
まじめなことをゆかいに、
そしてゆかいなことはあくまでゆかいに」

- コンサルタントとしてお客様に向き合う際にも通じること。
  座右の銘にしています。
  本日は宜しくお願いいたします。

会社概要　NRIセキュアテクノロジーズ株式会社

NRI 野村総合研究所グループにおける情報セキュリティ専門の中核企業

- **本社所在地：東京都千代田区大手町1-7-2　東京サンケイビル**
- **代表取締役社長　小田島　潤**
- **設立：2000年8月1日**
- **資本金：4．5億円**　　※サービス提供は１９９５年より開始

- **拠点**
  - **東京（本社）**
  - **横浜（テクニカルセンター）**
  - Irvine, CA（**北米支社**）
- **グループ会社**
  - 株式会社ユービーセキュア（**東京都港区**）
- **社員数**（連結）：398名　（単体）：343名

- **資格取得者数**
  - 高度情報処理技術者 ： のべ464名 （うち情報セキュリティスペシャリスト 195名）
  - CISA(Certified Information System Auditor) ： 80名
  - CISM(Certified Information Security Manager) ： 41名
  - CISSP(Certified Information Systems Security Professionals) ： 38名
  - GIAC(Global Information Assurance Certification) ： のべ168名

- ＩＳＯ／ＩＥＣ 27001認証取得

IS 75215 / ISO 27001:2013

- サービス提供実績
  - 官公庁、金融、流通、製造、製薬、 通信、マスコミ 等500社以上に運用サービスを提供
  - 一次的なスポットサービスを含めると2000社以上にサービス提供

（2017年10月1日現在）

はじめに

このセッションのゴール

テーマ１　IoT系ガイドラインの効果的・効率的な運用

- 自社への適用に関する勘所がわかる。
  - ガイドラインの利活用の目的
- どのようなIoTガイドラインがあるかがわかる。
  - 適用セグメントによって、求められるものが異なる

テーマ２　PSIRTの枠組み

- 最近よくきく「PSIRT」の触りを理解した。
  - PSIRTに取り組むにあたっての最低限必要な機能とは

目次

テーマ１　IoT系ガイドラインの効果的・効率的な運用（30分）

1．IoTシステムとガイドラインの位置づけ

2．ITとは異なるセキュリティ対策

テーマ２　PSIRTの枠組み　（10分）

４．PSIRTのいま

1.　IoTシステムとガイドラインの位置づけ

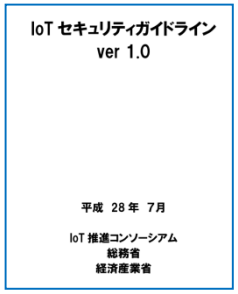
1. IoTシステムとガイドラインの位置づけ

釈迦に説法ですが・・・

そもそも「ガイドライン」とは何なのか？

「指針」　＝　物事を進めるうえで頼りになるもの
　　参考となる手引き
「基準」　＝　望ましい性質や水準

望ましい方向に進む手掛かり・目安になるもの
（Mustではなく、ShouldやBetter）


IoT セキュリティガイドライン
ver 1.0

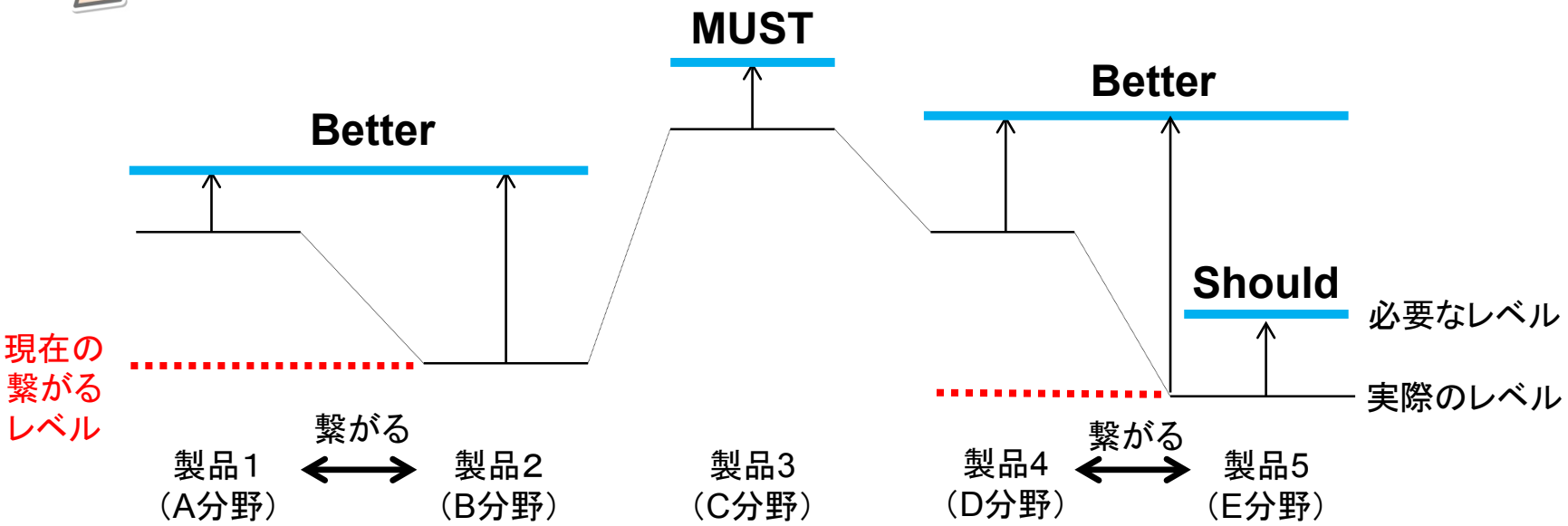
平成 28 年 7月

IoT 推進コンソーシアム
総務省
経済産業省

本ガイドラインは、IoT 機器やシステム、サービスの供給者及び利用者を対象として、サイバー攻撃などによる新たなリスクが、モノやその利用者の安全や、個人情報・技術情報などの重要情報の保護に影響を与える可能性があることを認識したうえで、IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたものである。本ガイドラインを活用することにより、IoT 機器やシステム、サービスの供給者や利用者が自己の役割を認識しつつ、分野ごとの性質に応じたセキュリティ確保の取組が促進されることを期待するものである。

自社の「ガイドライン」は何のために定めるのか？

自社製品（分野ごと）のセキュリティ品質・水準を
一定に担保するための道しるべ・基準

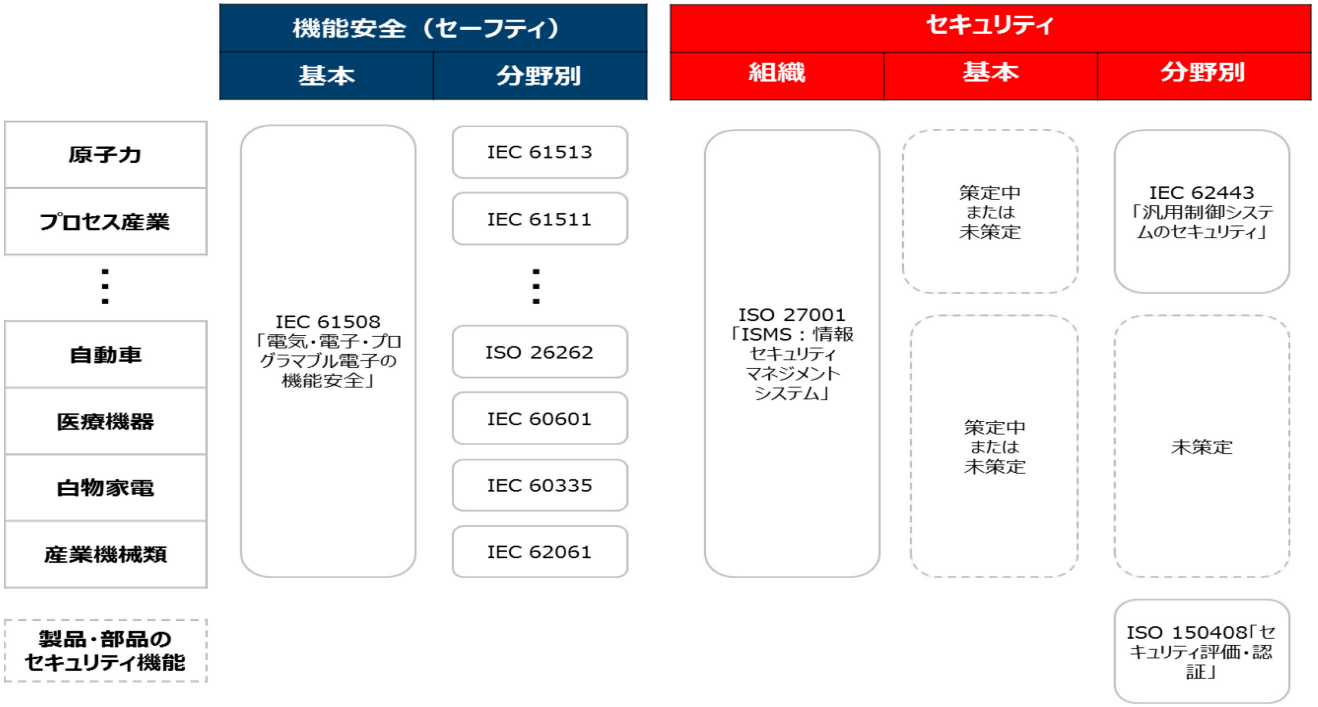


製品ポートフォリオに応じた
“MUST”・“Should”・” Better ”

2. ITとは異なるセキュリティ対策

2．ITとは異なるセキュリティ対策

これからIoTに参入しようとしている企業、すでにIoTを市場にリリースしている企業がセキュリティを考えた時、「セーフティ」規格とは異なり、「セキュリティ規格」はまだ策定途上にある。



引用元：CCDS:IPA ET West2016 ブースプレゼン
機能安全とセキュリティ 発表スライドより一部加工

2．ITとは異なるセキュリティ対策

一方、「ガイドライン」や「レポート」はここ数年で多数発行されている。（一部抜粋）

対象	発行団体	ガイドライン概要		
		名称	発行年（最終更新）	ガイドライン概要
IoT全般	OWASP	OWASP IoT Security Guidance	2016年 (2017年)	メーカーや開発者がIoTの安全な製品やアプリケーションの構築、また消費者によるIoT製品の製品の購入に役立つ3種類のガイダンス。 各ガイダンスは、包括的な考慮事項のリストではなく、そのように扱われるべきものでもないが、このガイダンスの基本事項を確実にカバーすることでIoT製品のセキュリティ向上、安全なIoT製品の購入に役立つ。
IoT全般	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	2016年	IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。各指針等においては、具体的な対策を21個の要点としてまとめている。
IoT全般	CSA(Cloud Security Alliance)	Security Guidance for Early Adopters of the Internet of Things(IoT)	2015年	IoT機能を実装する組織に推奨されるセキュリティコントロールとサンプルユースケースを提供している。これらのコントロールは、IoT固有の特性に合わせて調整されており、アーリーアダプター企業はこの新技術に関連する多くのリスクを緩和できる。
・Connected Home ・Wearable Tech	OTA（Online Trust Alliance）	OTA IoT Trust Framework	2016年 （2017年）	IoTトラストフレームワーク（IoT Trust Framework）では、「security and privacy by design」が製品開発の開始からの優先事項であり、全体的に取り組まなければならないことを説明している。また、このフレームワークの遵守は規制要件を上回るものではなく、法律や規制への準拠を意味するものではない。なお、スマートホーム・接続された家電や消費者向けのウェアラブル技術をスコープとしている。
IoT全般	GSMA	GSMA IoT Security Guidelines	2016年、2017年	サービスのライフサイクル全体を通じてセキュリティのベストプラクティスが実装されることを確実にするために、安全性の高いIoTサービスを開発するための方法論を示すもので、IoTサービスにおける一般的なセキュリティへの脅威と弱点を軽減する方法についての推奨要件を説明している。
IoT全般	CIS	CIS Critical Security Controls (Version 6.1): IoT Security	2015年 （2017年）	Critical Security Controlsは、情報セキュリティ対策とコントロールのベースラインを示したコンセンサスドキュメントである。IoTに関する20個のコントロールが記載されている。
IoT全般	IPA	つながる世界の開発指針	2016年	製品の開発時に考慮すべき安全安心に関わる事項を指針としてとりまとめたものである。各指針は、取組みの「ポイント」、背景の「解説」及び具体的な「対策例」から構成されている。すべてのポイントを検討することで、つながる世界のリスクを低減することを目的としている。
IoT全般	NISC	IoT セキュリティのための一般的枠組	2016年	将来、個々のシステムが相互に接続されることを見据え、セキュリティ・バイ・デザイン(Security by Design)の思想で設計、構築、運用されることが不可欠である。こうしたことを合理的に実現させるためには、早急にすべての IoT システムにかかる設計、構築、運用に求められる事項を一般要求事項としてのセキュリティ要件の基本的要素を明らかにすることを目的としている。

２．ITとは異なるセキュリティ対策

IoTシステムは人命にかかわるシステムも多く、セキュリティを担保するために**トップダウンのアプローチ**で抜け漏れの無い対策を施すべきである。
　＃下記を全部足し算して、漏れの無い対策を・・・

	CSA+OTA+FTC+FBI+ENISA+GSAMA+OWASP+IEEE+IPA								
①デバイス	○		○	○		○		○	
②NW		○	○	○	○	○	○	○	○
③PF	○	○	○		○	○		○	○
④マネジメント			○			○	○		○

２．ITとは異なるセキュリティ対策

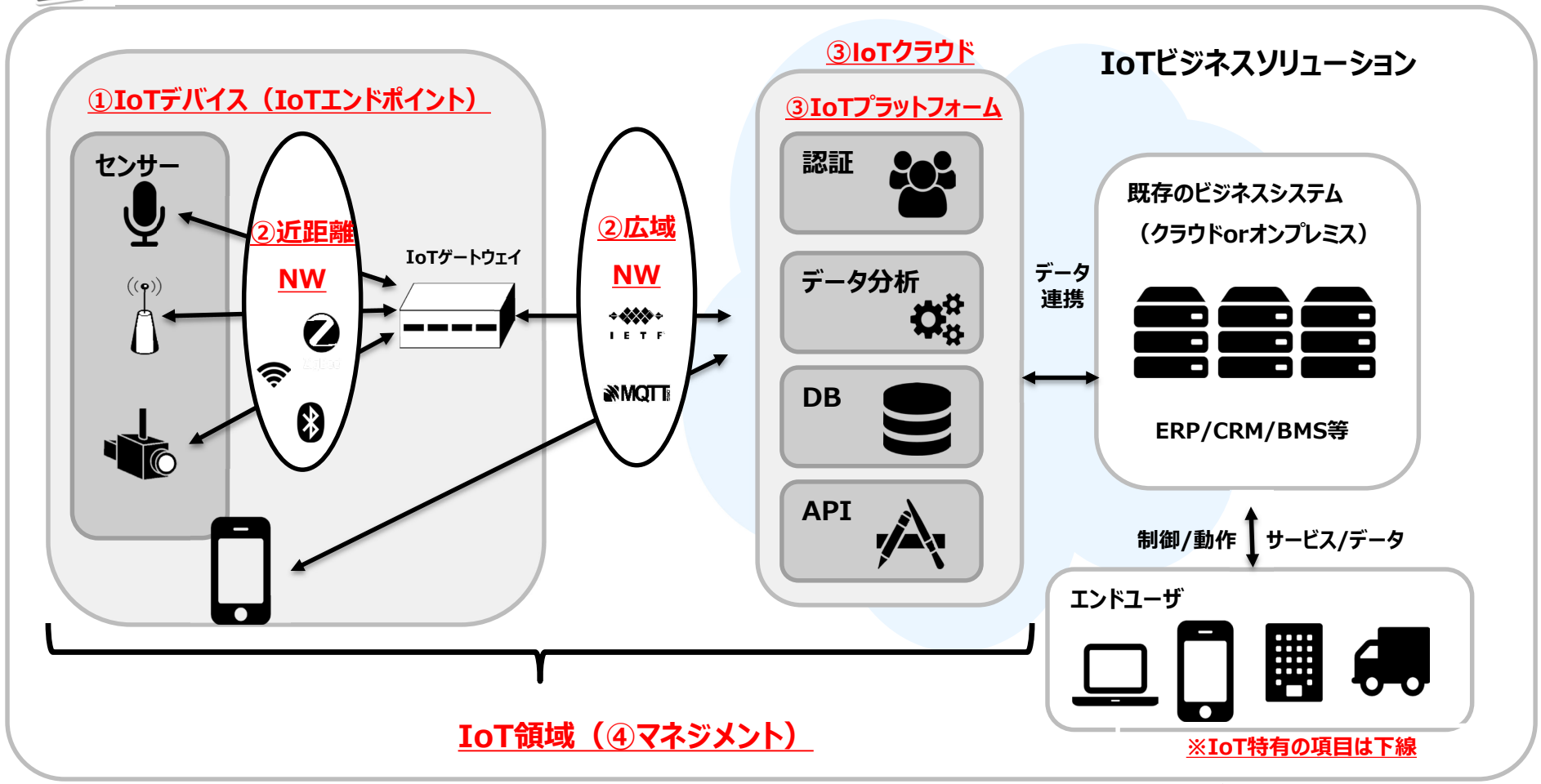
トップダウンアプローチ（ベースライン型アプローチ）

メリット：
手戻りが少なく、網羅性が担保できる。
マーケットインした製品等についても、一定の確認は行えている。

デメリット：
時間と手間がかかる。
網羅的にセキュリティを担保するために、どの範囲・深さまで調査すれば良いのかスコープを判断することが非常に難しい

制御システムはセキュリティを守る必要性が高いが、機能安全のように確立された国際基準のような基準が存在しない。
トップダウンアプローチで全体最適を目指すことは、限られた時間で行うには難しいアプローチであると考える。

一般的にIoTシステムは、下記の4つの構成要素（①～④）で構成される。



2．ITとは異なるセキュリティ対策

下記に記載したガイドラインは、それぞれ、どの構成要素に詳しいかの特徴がある。

	米国				欧州	グローバル			国内
	CSA	OTA	FTC	FBI	ENISA	GSAMA	OWASP	IEEE	IoT推進コンソーシアム
①デバイス	○		○	○		○		○	
②NW		○	○	○	○	○	○	○	○
③PF	○	○	○		○	○		○	○
④マネジメント			○			○	○		○

2．ITとは異なるセキュリティ対策

IoTの構成要素（桃色軸）に応じて、右に○がついているガイドラインの要素を参考にする。

	米国				欧州	グローバル			国内
	CSA	OTA	FTC	FBI	ENISA	GSAMA	OWASP	IEEE	IoT推進コンソーシアム
①デバイス	○		○	○		○		○	
②NW		○	○	○	○	○	○	○	○
③PF	○	○	○		○	○		○	○
④マネジメント			○			○	○		○

例：自社製品がIoTデバイスの場合

	米国				欧州	グローバル			国内
	CSA	OTA	FTC	FBI	ENISA	GSAMA	OWASP	IEEE	IoT推進コンソーシアム
①デバイス	○		○	○		○		○	
②NW					○	○	○	○	○
③PF					○	○		○	○
④マネジメント			○			○	○		○

全部見る必要はない。
5つのガイドラインから絞る。

・IoTの構成要素から、○をプロットしているものを参考にする。

例：自社製品がIoTデバイスの場合

	米国				欧州	グローバル			国内
	CSA	OTA	FTC	FBI	ENISA	GSAMA	OWASP	IEEE	IoT推進コンソーシアム
①デバイス	○		○	○		○		○	
②NW					○	○	○	○	○
③PF					○	○		○	○
④マネジメント			○			○	○		○

全領域に配慮されたもの＋
詳しいもの・粒度の細かいもの
を組み合わせる。

・5つを全部見るのも大変・・・
上記だと「GSMA＋CSAでまずは見てみる」など
必要最小限の材料でアプローチしてみる。

２．ITとは異なるセキュリティ対策

ボトムアップアプローチ（足元のリスクベース型アプローチ）

メリット：
現状のクリティカルな脅威に対して迅速に対応することが出来る。

デメリット：
抜け漏れがあった場合に、大きな手戻りが発生する可能性がある。
マーケットイン済みの商品に影響が生じる可能性がある。

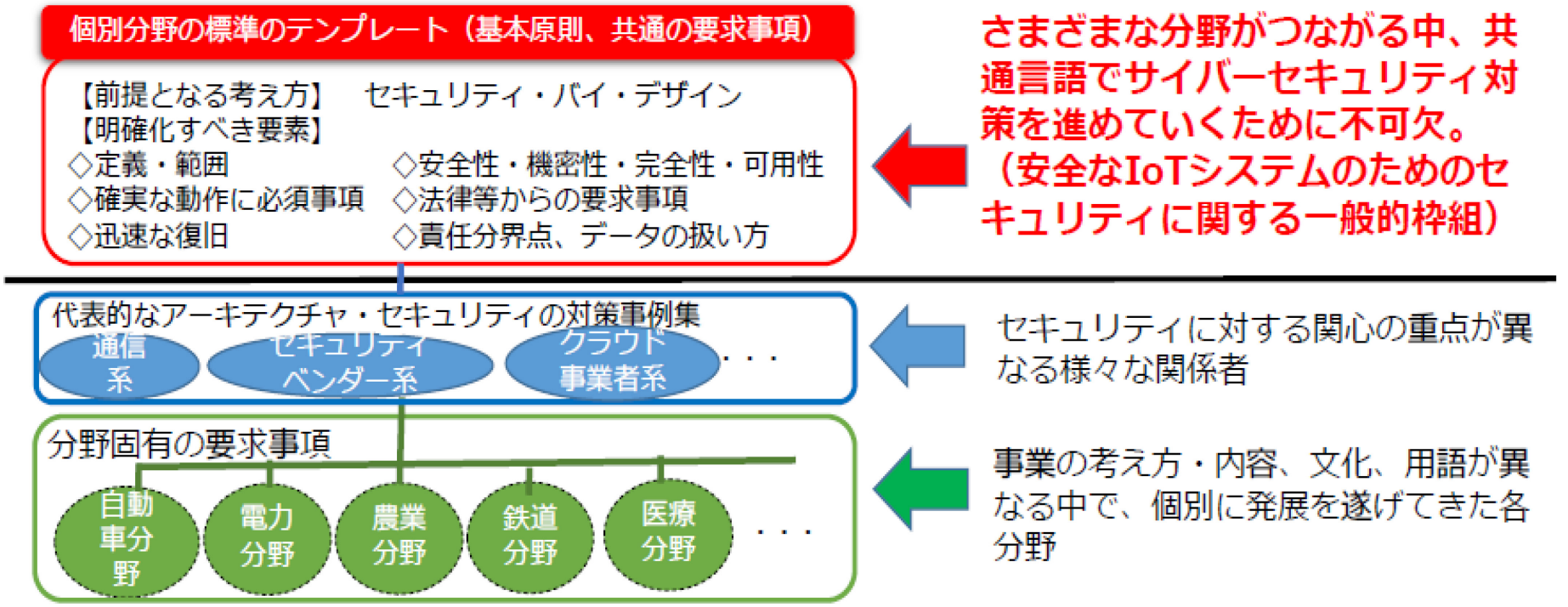
多角的に多くのプロダクトを扱っている企業では、網羅的に全てのプロダクトに対してトップダウンで適用したいと思う企業が多いが、まずは例示したガイドライン用いて「ボトムアップアプローチでプロダクトごとの個別最適を目指してみる」ことをお勧めする。

ここでは、比較的汎用的に記載されたガイドラインをピックアップしているが、ガイドラインで詳しく書かれている項目、粒度は異なっている。実際にガイドラインを活用する際は上記のような特徴を踏まえて組み合わせることをお勧めする。
結果的に早くプロダクトのリリースもできる。
当該プロダクトに最適なセキュリティの担保が出来ると考えられる。

2．ITとは異なるセキュリティ対策

更に･･･分野固有のガイドラインも出ており、該当するガイドラインの確認も必須となる。

【安全なIoTシステムのためのセキュリティに関する一般的枠組】（2016年8月 NISC）



・「自動車の情報セキュリティへの取組みガイド」第2版
・スマートメーターシステムセキュリティガイドライン（JESC）
・電力制御システムセキュリティガイドライン（JESC）
・医療機器サイバーセキュリティ技術報告書

出所：安全なIoTシステムの創出に向けた取組（NISC）

2．ITとは異なるセキュリティ対策

ボトムアップアプローチでまずやってみる。
トップダウンアプローチで網羅性を担保。
いずれにしても、独自要件の追加・修正は必須！

トップダウン

STEP1
汎用的なガイドラインにある記載を列挙し、IoTガイドラインに記載のある対策一覧を作成する。

STEP2
全ての対策一覧から、事業特性、自社（製品特性）に応じた適用の要否を判断し、要・不要を明示したガイドを作成。

ボトムアップ

STEP1
対象事業全域に共通する汎用的なガイドラインからIoTの構成要素で○がついているものをピックアップする

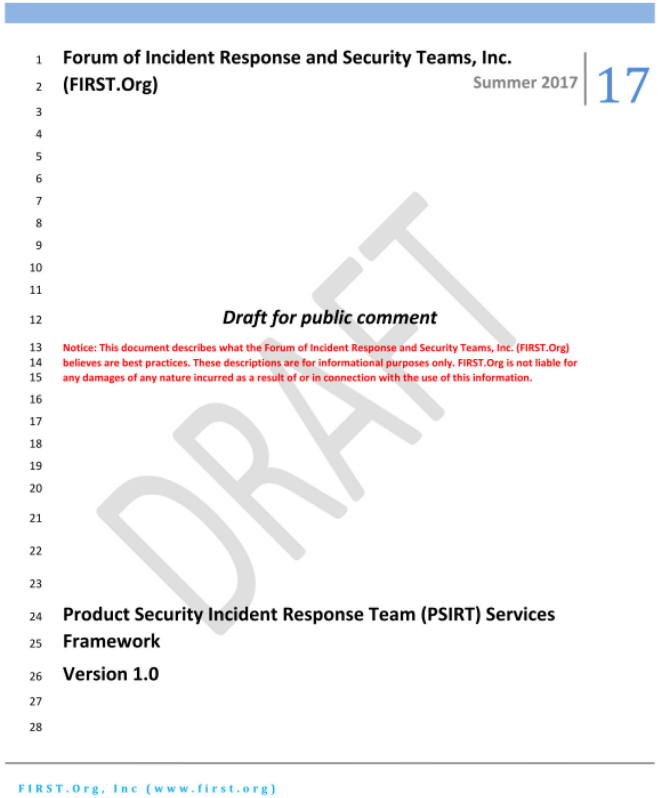
STEP2
該当するガイドラインから必要な項目をピックアップして、自社（製品）仕様のガイドラインを策定する。

STEP3
事業特性・製品特性に応じた独自要件の追加／修正を行い、充実化を図る

3．PSIRTのいま

3. PSIRTのいま

現時点では、確立したフレームワークはなし。
FIRST が”PSIRT Services Framework“パブコメ中



Forum of Incident Response and Security Teams, Inc.
(FIRST.Org)
Summer 2017 | 17

Draft for public comment

Notice: This document describes what the Forum of Incident Response and Security Teams, Inc. (FIRST.Org) believes are best practices. These descriptions are for informational purposes only. FIRST.Org is not liable for any damages of any nature incurred as a result of or in connection with the use of this information.

DRAFT

Product Security Incident Response Team (PSIRT) Services Framework
Version 1.0

FIRST.Org, Inc (www.first.org)

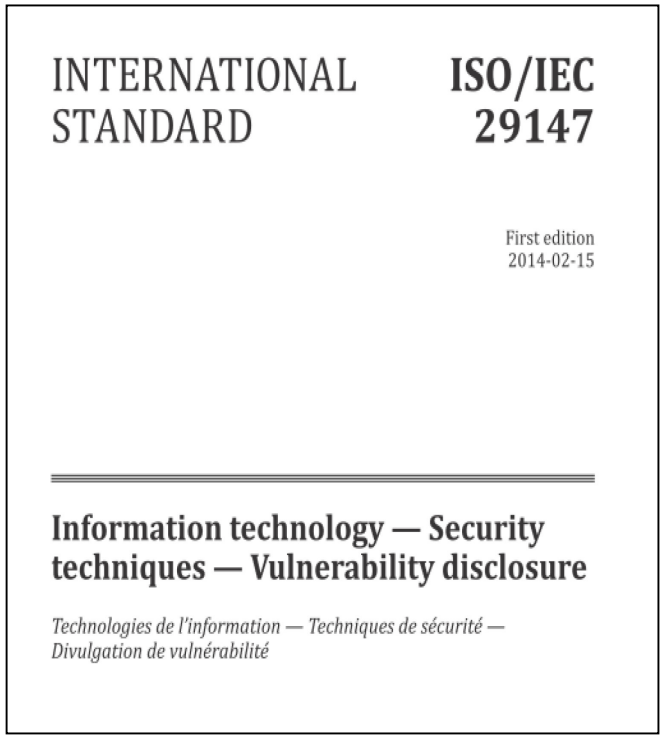
1. 関係者のマネジメント
   - 外部コミュニティ、組織
   - セキュア開発ライフサイクル
2. 脆弱性認識、把握
   - 脆弱性の報告
   - 利用プロダクト脆弱性情報の監視
3. 脆弱性判断、分析
   - 脆弱性の特定
   - 脆弱性情報の管理
4. 脆弱性対応
   - アップデートリリース計画
   - インシデント対応
5. 情報公開
   - アップデートリリース計画
   - 外部公開
6. 訓練、教育

抜粋

※1 FIRST (Forum of Incident Response and Security Teams) はCSIRTの国際連合体に相当するフォーラム
※2 2017/9時点でパブリックコメント版だが、PSIRTの活動の全体を俯瞰して整理したガイドライン

3. PSIRTのいま

脆弱性マネジメントに特化したものだと
ISO/IEC 29147 ： 脆弱性の公開
ISO/IEC 30111 ： 脆弱性ハンドリング

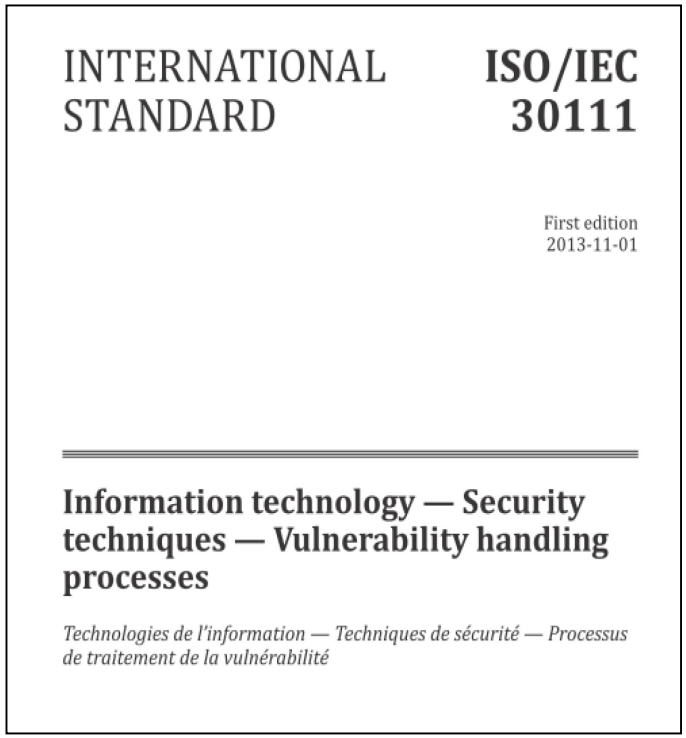

INTERNATIONAL STANDARD

ISO/IEC 29147

First edition
2014-02-15

Information technology — Security techniques — Vulnerability disclosure

Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité


INTERNATIONAL STANDARD

ISO/IEC 30111

First edition
2013-11-01

Information technology — Security techniques — Vulnerability handling processes

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

3．PSIRTのいま

前段の枠組みにとらわれず、
①～③の全てをPSIRTの枠組みでとらえている例もある

■ 整備すべき内容

- 1．対策方針
- 2．技術開発
- 3．標準化活動
- 4．会社ルール
- 5．人材育成

■ 対応分類

① 開発

出荷前に適切な製品企画・開発・製造を行うこと

- リスクレベルの定義
- 設計・開発・評価の基準と標準化
- 評価の実施（リスクアセスメント）
- 脅威の想定と対策レベルの策定

② 脆弱性対応

出荷後の脆弱性を把握・影響判断・対応して、セキュリティレベルを適切に維持すること

- 情報の収集
- 対応レベルの判断、対応

③ インシデント対応

インシデント発生時に速やかに対応すること

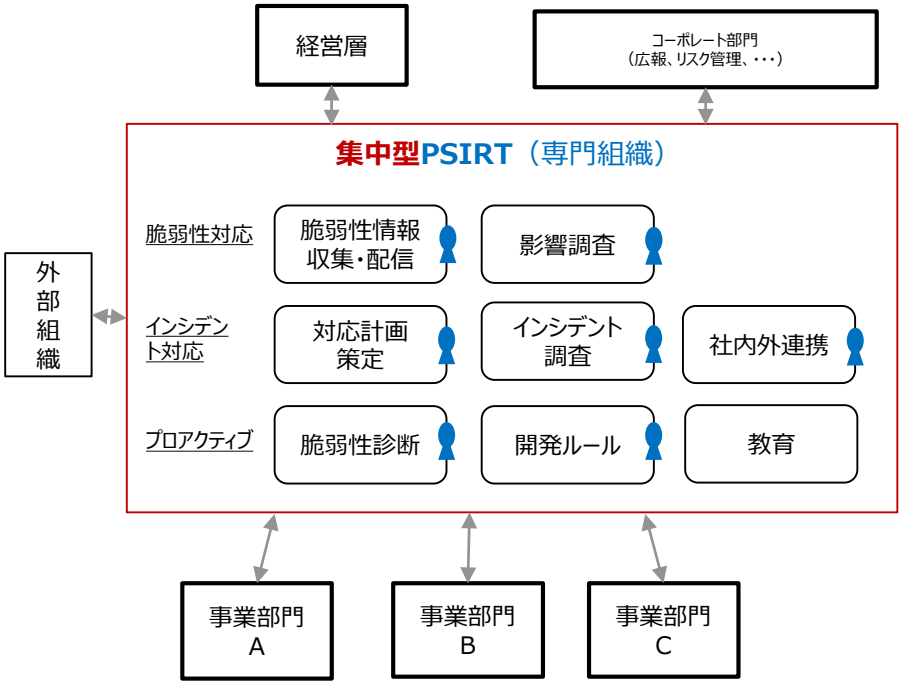
- 対応レベルの判断、対応
- 関係者への連絡・報告、公表

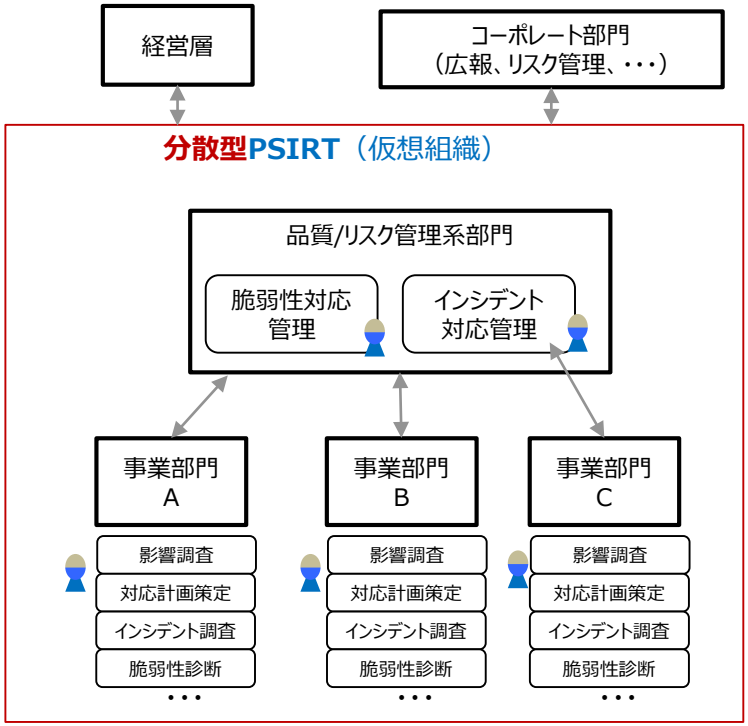
出荷前（Proactive）
企画 ・ 設計 ・ 開発

出荷後（Reactive）
運用 ・ 廃棄

4. PSIRTのいま

PSIRTの体制構築パターン大きく3つ
- 集中型　：　１つの組織に集中的に機能を配置
- 分散型　：　既存の各部門に機能を割り当てる
- ハイブリッド型　：　集中型と分散型の良いとこどり型





4．PSIRTのいま

PSIRTの活動に取り組む前に・・・
まず自社でできていることはどれでしょう？
必要な役割と責任を整理すると、既にPSIRTがあるといえる会社も・・・

■ 整備すべき内容

1．対策方針

2．技術開発

3．標準化活動

4．会社ルール

5．人材育成

■ 対応分類

① 開発

出荷前に適切な製品企画・開発・製造を行うこと

- リスクレベルの定義
- 設計・開発・評価の基準と標準化
- 評価の実施（リスクアセスメント）
- 脅威の想定と対策レベルの策定

② 脆弱性対応

出荷後の脆弱性を把握・影響判断・対応して、セキュリティレベルを適切に維持すること

- 情報の収集
- 対応レベルの判断、対応

③ インシデント対応

インシデント発生時に速やかに対応すること

- 対応レベルの判断、対応
- 関係者への連絡・報告、公表

出荷前（Proactive）
企画 ・ 設計 ・ 開発

出荷後（Reactive）
運用 ・ 廃棄

4. PSIRTのいま

この後、アイオーデータの島田様から、PSIRTの実際をお話いただけます。

先ほどお見せしたスライドで、機能俯瞰を頭に浮かべつつ

- どこの機能を担うような組織設計になっているのか？
- その組織ではどのような制度・運用設計になっているのか？

に着目して聞いていただけるとよいのではないかと思います。

4. 最後に

このセッションのゴール

テーマ１　IoT系ガイドラインの効果的・効率的な運用（30分）

- 自社への適用に関する勘所がわかる。
  - ガイドラインの利活用の目的
- どのようなIoTガイドラインがあるかがわかる。
  - 適用セグメントによって、求められるものが異なる

テーマ２　PSIRTの枠組み　（10分）

- 最近よくきく「PSIRT」の触りを理解した。
  - PSIRTに取り組むにあたっての最低限必要な機能とは

ご清聴ありがとうございました。