SQiP
Software Quality Profession

IoT時代の品質保証

～つながる世界の中で品質保証はどうなっていけばいいのか～

2017　ソフトウェア品質保証部長の会
IoT時代の品質保証グループ

東芝デジタルソリューションズ㈱	内海　俊行
エプソンアヴァシス株式会社	江口　達夫
リコーITソリューションズ㈱	里富　豊
NECソリューションイノベータ株式会社	杉野　晴江

(50音順)

アブストラクト

- IoT時代の品質保証について、
何から手をつければよいのかお困りではありませんか？

- 特に困っているメンバで集まり、このテーマで検討を進めて参りました。その結果として、IoT時代での現在の日本の状況と晒されているリスクが分かってきました。その内容や、我々が感じた危機感を皆様にも感じていただきたく、品質保証として解決すべき課題とその取り組み方法を提言致します。

- この発表を期に、時代にあった品質保証で、
「安心、安全な日本」を一緒に目指しましょう。

アジェンダ

１．そもそも、“IoT時代”って？

２．“IoT時代”の困りごと

2-1．利用者側は？

2-2．価値提供する側は？

３．IoT時代の品質保証

3-1．今日から始めよう

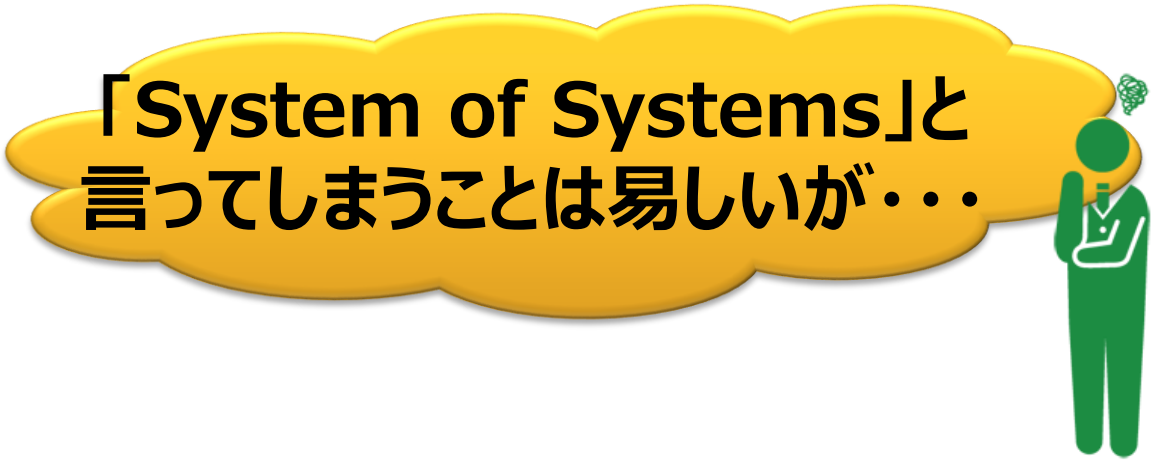
3-2．導かれる課題

４．まとめ

1．そもそも“IoT時代”って？

- 「モノ」が Internet につながり、
  自らが世界を観察、特定、理解するようになる

- さらに「モノ」と「モノ」が
  Internet を通じてつながる



2．“IoT時代”の困りごと

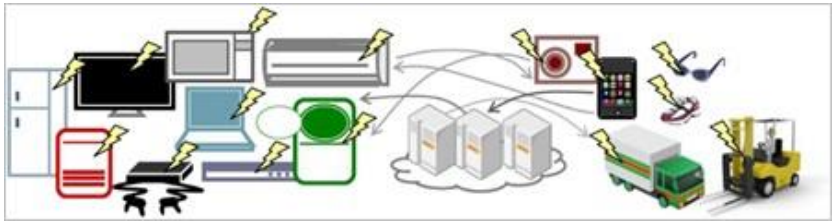
「つながる世界」の到来

引用：つながる世界の開発指針

~安全安心なIoTの実現に向けて
開発者に認識してほしい重要ポイント~

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター

（１）想定しないつながりが発生する



（２）管理されていないモノもつながる

（３）身体や財産への危害がつながりにより波及する

（４）問題が発生してもユーザーにはわかりにくい

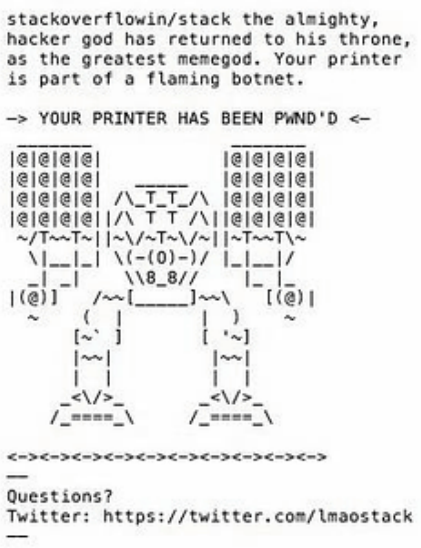
“つながり”の把握やリスクの発見、機器やシステムの管理が難しい。

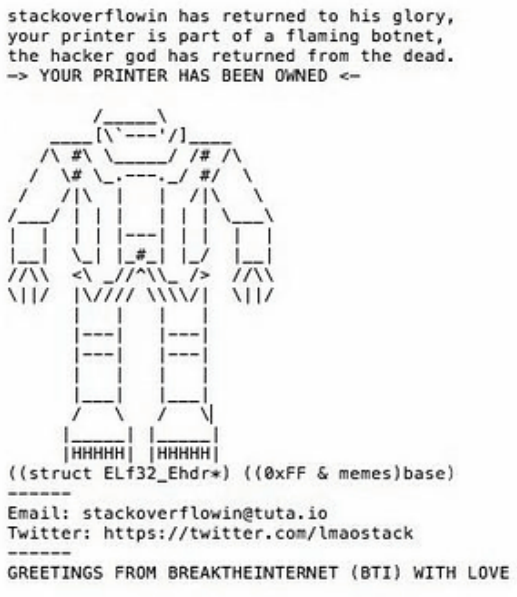
2．“IoT時代”の困りごと

実例！

2017年2月、ネットワークに接続されている15万台の複数各社の**プリンタがハッキング**され、一斉に意図せぬ文書が印刷された。

目的は、ファイアウォールなどのセキュリティ対策をせずにプリンタをオンラインで公開する危険性を指摘するため



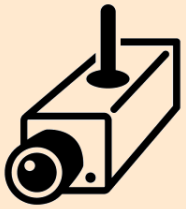
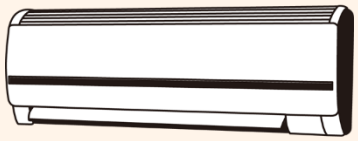


出典：ギズモード・ジャパン 2/17(金) 21:10配信
http://www.gizmodo.jp/2017/02/hacker-claims-he-hacked-150-000-printers.html

IoTセキュリティに、もっと関心持って！

2．“IoT時代”の困りごと

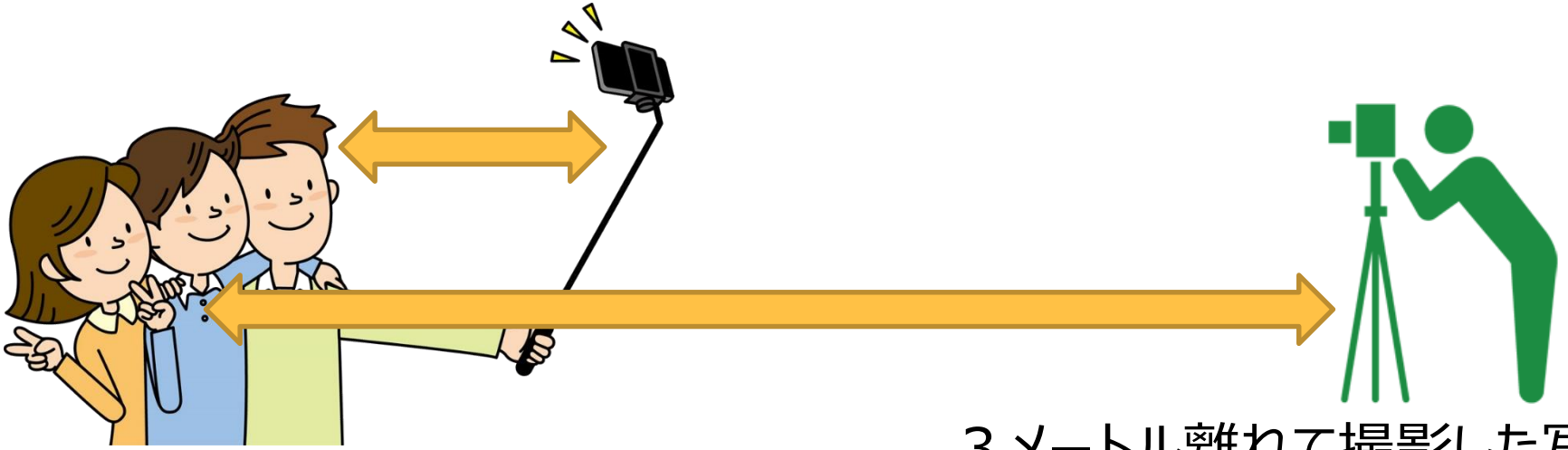
悪意のある者が・・・

つながるリスク例	想定例	対策例
悪意ある者がつなげてしまう 	防犯カメラが乗っ取られ閲覧される 	• サイバー攻撃を検知する機能搭載 • サイバー攻撃を受けやすい脆弱プログラムが見つかればネット経由でソフト更新 • 利用者がＰＷを設定しないと使えない仕様 • サイバー保険(※)に入る (※)サイバー攻撃でIoT機器の制御ができなくなり、工場の生産が止まってしまった場合に逃した利益や情報漏えいなどで生じた損害を補償
	家電製品を狙ったサイバー攻撃 	

出展：
2017/1/26日本経済新聞「サイバー攻撃保険　拡充」
2017/1/25日本経済新聞「サーバー攻撃「家電」標的」より

2．“IoT時代”の困りごと

指紋・顔・眼球も複製可能！



３メートル離れて撮影した写真からでも、**指紋読み取り可能**

出展：国立情報学研究所
http://www.nii.ac.jp/news/release/2017/0317.html

SNSへの実名・電話番号登録、写真投稿等により**“悪意のある第三者”の攻撃対象**となってしまう

2-1. 利用者は？

- **安心・安全・快適さを損なわれたくない**
- **満足・感動がほしい**

- **変化をのぞまない**
  - 慣れ、変わらないことの価値
  - セキュリティ対策として、本人認証行為が増える等、手間が増えるのは嫌
    ・・・等々

2-1. 利用者は？

リスクはあるけど・・・

- **リスクをわかっていながらも目をつぶっている**
- **リスクを意識的に意識しないようにしている**
- **リスクだったことを忘れている**

- **価値がリスクを凌駕している（リスク＜価値）**
  - 例：SNS＝人同士の”つながり” に価値を見出している
- **リスクがSafetyまで脅かす可能性に気が付いていない**(もしくは無視している)

2-2. 価値提供する側は？

「リスク ＜ 価値」に甘えてませんか？

利用者の 自己責任 ということにして・・・

2-2. 価値提供する側は？

実例）システムベンダーはどこまで責任を負うのか

経産省・IPAが注意喚起すれば当事者の意思に関わらず義務になる！？

ウェブにおける商品受注システム（受注金額：890万円）

- 2011年04月：サーバへの不正アクセス、顧客クレジットカードの不正利用が発覚
- 2011年10月：委任契約の債務不履行があったとして、顧客への謝罪や売上減少等、約1億900百万円の損害賠償請求訴訟を提起
- 2014年01月：東京地方裁判所が被告に2,262万円の支払を命じる判決

・「対応しません」という意志表示をしないと、認めたということになってしまう。

– 『特別な指示をしなくても，既知の脆弱性に対し，当時の技術水準に応じた対策がなされたプログラムが提供されることを通常期待するはず』

– IPAから対策を行うよう注意喚起がされている

契約書の記載がなくても「プロとしての知見ありながら、コメントしなかった」として
SIベンダとしてのプロの注意義務を広く捉える傾向がある。
ただ、基準はないため、自分達で考えていくしかない。

出展：システムベンダのセキュリティ対策義務より
～東京地裁平成26年1月23日判決（平23(ワ)32060号）を素材として～
スクワイヤ外国法共同事業法律事務所　弁護士　武田勝弘
http://www.softic.or.jp/semi/2014/5_141113/index.html

2-2. 価値提供する側は？

サイバーセキュリティも気にしないと・・・

出展元	タイトル
経産省	サイバーセキュリティ経営ガイドライン（Ver1.0）
経産省	ソフトウェア等脆弱性関連情報取扱基準（改正）
IoT推進コンソーシアム 総務省/経産省	IoTセキュリティガイドラインVer1.0
IPA	サイバーセキュリティ経営ガイドライン解説書（Ver1.0）
IPA	情報セキュリティ早期警戒パートバーシップガイドライン
IPA	ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル
IPA	つながる世界の開発指針
JPCERT/CC	高度サイバー攻撃（APT）への備えと対応

・・・etc

3．IoT時代の品質保証

様々な武器があることを知り、活用しよう！

3-1. 今日から始めよう

- **全従業員**に、つながることによるリスクを知ってもらう
- リスク検討に有用な、様々な手段を知ってもらう
- 社内に推進体制を作って、検討を始めよう

経営者層への対応理解

教育

プロセス改善

引合･受注 → 要件定義 → 設計･製造 → 運用

3-2. 導かれる課題

- セキュリティ投資へのリターンは見え難く、経営者がリーダシップを取らなければ積極的には話がでない。

課題①：経営層のリスク理解度向上

  - さまざまなルールや認証ができたらそれに対応する、ではなく、現在社会で発生しているリスクを正しく認識し、それに対して後手にならないように手を打っていくことが大切。
  - そこは売上や利益とは別の次元。
  - 品質保証のメンバーは、経営層の理解を助け、正しい方向へ導く。

3-2. 導かれる課題

経営層のリスク理解度向上に向けて！

出展：独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター
http://www.ipa.go.jp/sec/reports/20160324.html

P.16「1.3 開発指針の目的と使い方 － (1)開発指針の目的」
開発者だけでは対応が難しい事項については **経営者** や保守者に参照可能な内容となっている。

大項目		指針
方針	4.1 つながる世界の安全安心に企業として取り組む	指針 1　安全安心の基本方針を策定する
		指針 2　安全安心のための体制・人材を見直す
		指針 3　内部不正やミスに備える
保	4.4 市場に出た後も守る設	指針 13　自身がどのような状態かを把握し、記録する機能を設ける

P.32「4.1 つながる世界の安全安心に企業として取り組む」
つながる世界の安全安心は、機器やシステムの開発企業にとっては存続にかかわる課題であるため、開発者のみならず **経営者** もリスクを認識する必要がある。
P.33「[指針１]安全安心の基本方針を策定する」
P.35「[指針２]安全安心のための体制・人材を見直す」

3-2. 導かれる課題

サイバーセキュリティの確保は経営者が果たすべき責任の一つ

サイバーセキュリティ経営ガイドライン

【3原則】
1．経営者のリーダーシップが重要
2．自社以外(ビジネスパートナー等)にも配慮
3．平時からのコミュニケーション・情報共有

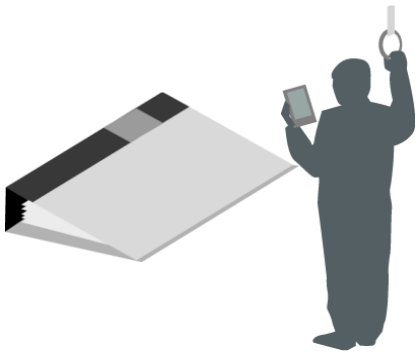
【重要10項目】
①サイバーセキュリティ対応方針の策定
②リスク管理体制の構築
③リスクの把握、目標と対応計画策定
④PDCAサイクルの実施と対策の開示
⑤系列企業ビジネスパートナー
⑥予算の確保、人材配置・育成
⑦ITシステム管理外部委託先
⑧情報収集・共有
⑨定期的な演習の実施
⑩被害発覚後の開示体制整備

出展：経済産業省
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバーセキュリティ経営ガイドライン　解説書

ガイドラインの内容を補足し、
実施方法が具体的に解説されている

出展：独立行政法人情報処理推進機構 技術本部セキュリティセンター
http://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html



3-2. 導かれる課題

- 今後出てくるであろう、脆弱性への対応方針をお客様と合意

  課題②：契約時の責任範囲明確化

  ・システム化計画フェーズ（受注前）での契約方針策定

- 「開発指針」はつまるところ「しくみ」や「注意点」、すなわち「プロセス」

  課題③：プロセスを変えていく

  ・業務分析フェーズでのリスク対策範囲の明確化
  ・上流設計フェーズでのセキュリティ脅威分析、対策方針の決定
  ・下流設計フェーズでの対策方針の具体化、テスト計画策定
  ・実装フェーズでのソースコード解析
  ・運用段階での注意喚起、インシデント発生時の対応　　など

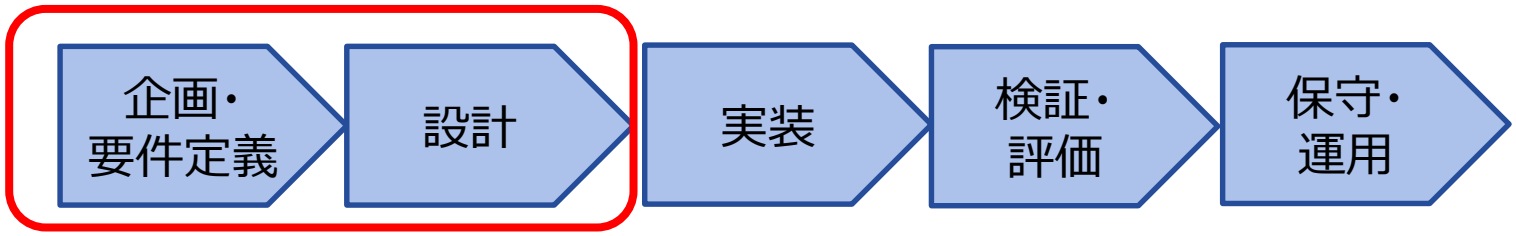
3-2. 導かれる課題

- 脆弱性を生まない設計を実現する

課題④：「Security　by Design」

●セキュリティ・バイ・デザインの定義（NISC）

「情報セキュリティを企画・設計段階から確保するための方策」



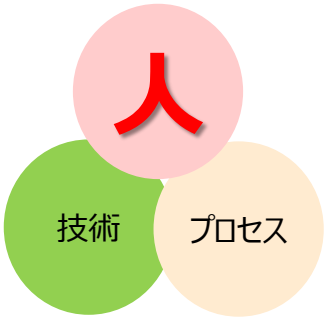
“情報セキュリティ”ではなく、“セキュリティ”とすれば
IoT製品やサービスにも適用できると考えられる。

出展：
「IoT時代」のセーフティ＆セキュリティ　by　デザイン
～アシュアランスケースとコモンクライテリア(ISO/IEC15408)によるセキュリティの品質保証を考える～
情報セキュリティ大学院大学　　金子朋子

3-2. 導かれる課題

- もうひとつ大切なことは「プロセスに込める心」、そして提供側も利用側も「社会のリスクを気にすること」、すなわち「意識」

課題⑤：提供側と利用側の意識変革（品質へのこだわり）



・自身のためのこだわり
・自社のためのこだわり
・エンドユーザ・社会のためのこだわり
・お客様企業のためのこだわり

4.まとめ

IoT時代の品質保証

経営者自らのリーダーシップ

①経営層のリスク理解度向上

⑤提供側と利用側の意識変革

④Security by Design

③開発プロセスを変えていく

②契約時の責任範囲明確化

リスクを知る

最後に

IoT時代の品質保証・・・

ご清聴ありがとうございました