JNSAの考えるIoTセキュリティの課題と対策

2016年10月26日

日本ネットワークセキュリティ協会(JNSA) IoTセキュリティWG
武田　一城(日立ソリューションズ)

本講演の主旨

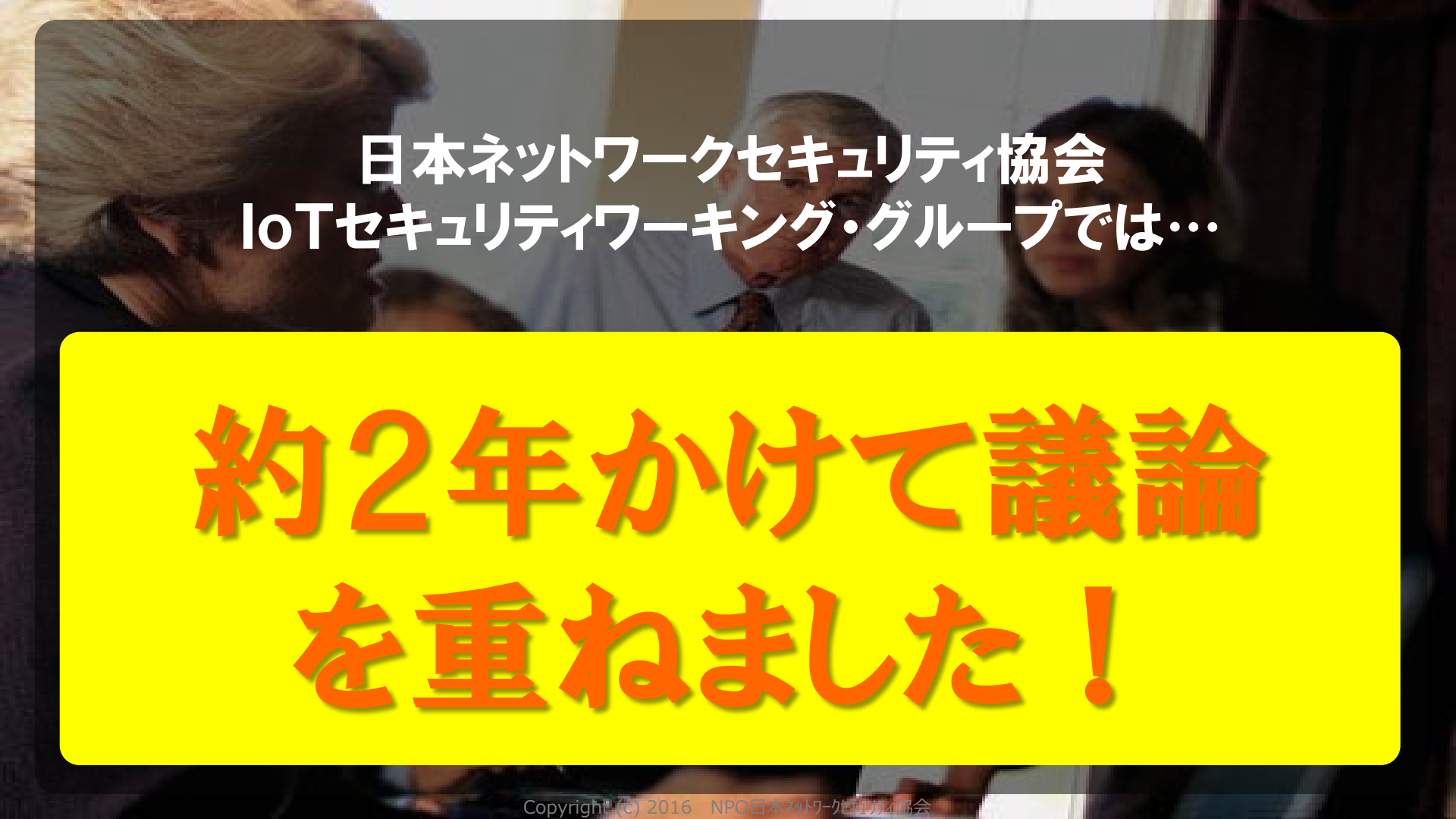
- 何年もの間、サイバー攻撃の脅威が叫ばれ続けている。
- 数多くのセキュリティ対策が施されているが、改善されない。
- IoTが急激に普及する兆しがある。
- ITだけでも大変なのに、今後はIoTも守らなければならない。

IoTが本格普及されたら・・・

何が脅威となり、何を守るべきなのか？

根源的な
そもそも論から
話をはじめました。

そのため・・・



日本ネットワークセキュリティ協会
IoTセキュリティワーキング・グループでは…

約2年かけて議論を重ねました！

そして、やっと完成したのが…

本講演の主旨

情報セキュリティの専門家としてたどり着いた結論

129ページ
の大容量

本講演の主旨

本講演では、このJNSAのIoTセキュリティWGが・・・

IoT分野のセキュリティにおいて
何を守るべきターゲットとしたのか？

とその課題と対策を説明します。

Ans. コンシューマ向けIoT機器！

Contents

1. 情報セキュリティとIoTの関係
2. IoTの普及と課題
3. 狙われるコンシューマ向けIoT機器
4. コンシューマ向けIoTのガイドを作成した理由

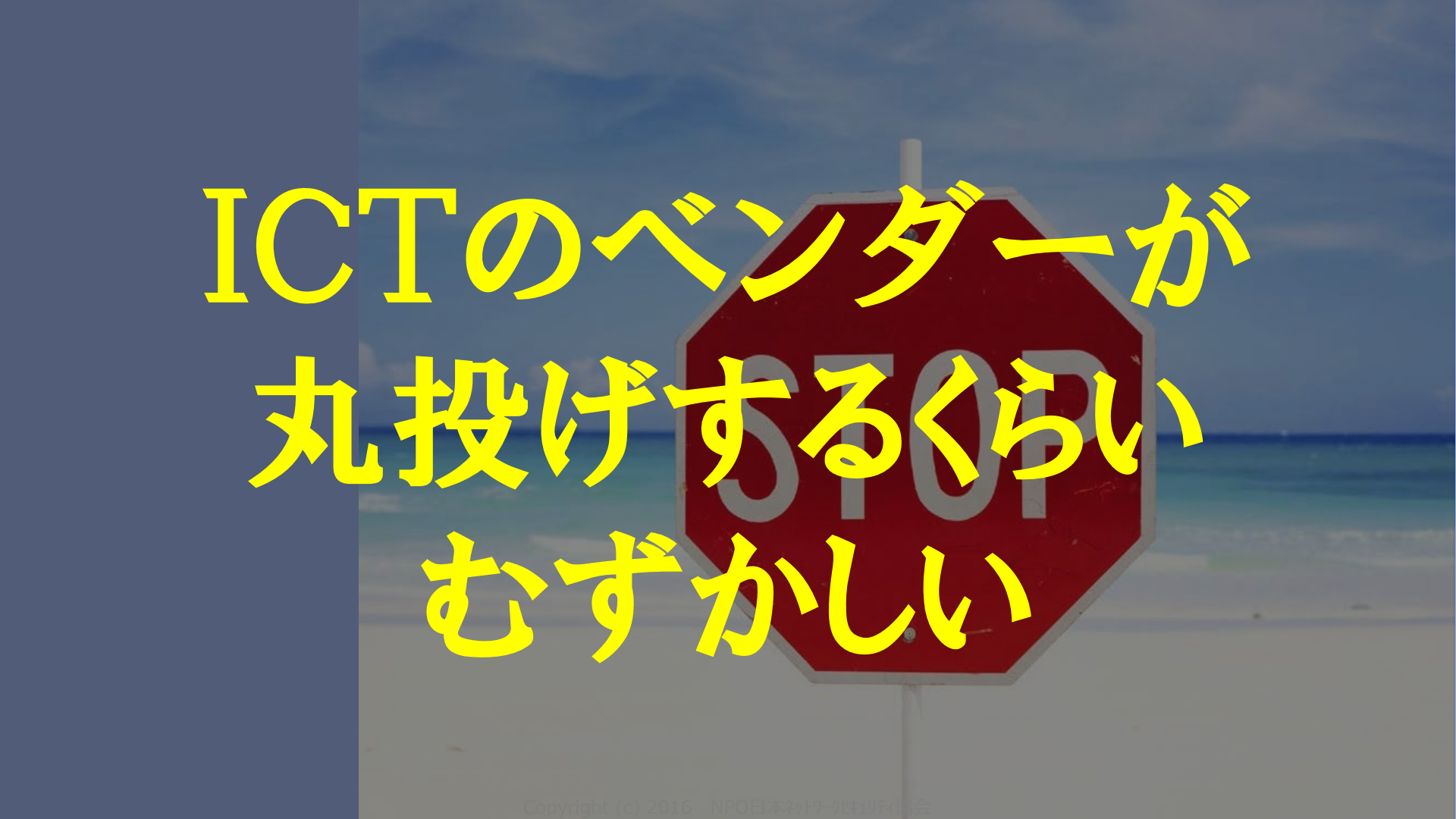
1．情報セキュリティとIoTの関係

Question 1 ：

情報セキュリティは むずかしい？

・・・そう思われる方は挙手をお願いします！

ICTのベンダーが丸投げするくらいむずかしい



1．情報セキュリティとIoTの関係

欧米のような外資系企業では、ビジネスの重要な武器であるＩＣＴは、自社内でＳＥを雇用し、社内で人材を育成します。しかし日本企業では、伝統的に情報システム部門が窓口となって外部のＩＣＴベンダーに業務委託します。そして、そのベンダーでもセキュリティ技術者が潤沢にいないこともあって、さらにそこだけセキュリティ（専業）ベンダーに業務委託することも珍しくありません。

1．情報セキュリティとIoTの関係

もちろん・・・

すべての条件を
満たす人は非常に少ない

Question 2 ：

情報セキュリティを理解し対策するにはどうしたら良いか？

「・・・ウチはこんな風に成功した！」という方は挙手をお願いします！

1. 情報セキュリティとIoTの関係

1．情報セキュリティとIoTの関係

CISSP

情報セキュリティ
スペシャリスト
（情報処理安全確保支援士）

CISA

①これらのセキュリティ資格を勉強して取得する！
②社内で人材を育成する！
③良いセキュリティコンサルを見つける！

これらのようなことは、もちろん
大事で有効ですが・・・

現実問題としては難しい

（ヒト・モノ・カネのリソースが世界レベルで絶対的に足りない！）

1. 情報セキュリティとIoTの関係

SQLインジェクション

内部犯行

DDOS攻撃

ゼロディ攻撃

標的型攻撃

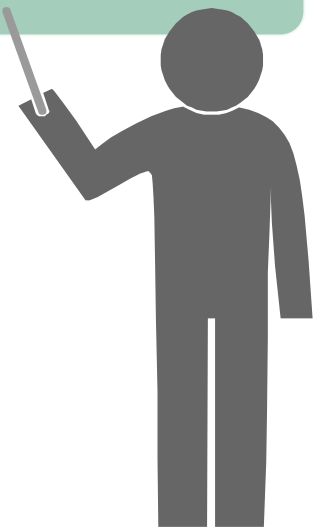
Winny

ランサムウェア

クラウドコンピューティング

フィッシング詐欺

このようなサイバー攻撃の
猛威は収まる気配がありません。



そして…

IoTが本格的に普及するとさらに拡大します！

1. 情報セキュリティとIoTの関係

SQLインジェクション

内部犯行

DDOS攻撃

ゼロディ攻撃

標的型攻撃

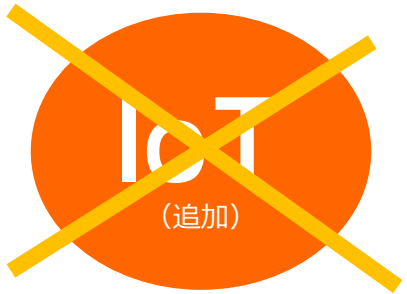
Winny

ランサムウェア

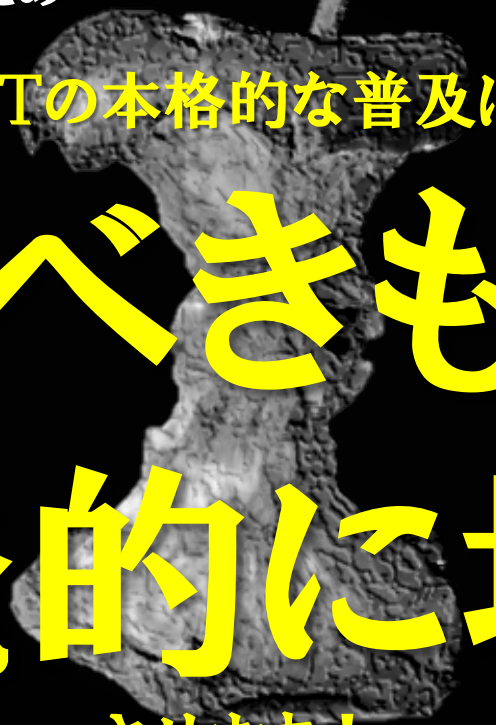
クラウドコンピューティング

フィッシング詐欺

しかし、IoTはこれまでの攻撃や脅威のひとつに追加されるという単純なものではないと思います。



IoTはモノのインターネット言われています。つまり、人間が介さなくても、どんどんモノがインターネットにつながる仕組みです。その結果、ICTの世界と現実世界が融合していくはずです。そのため・・・



IoTの本格的な普及は

守るべきものを爆発的に増大

させます！

2. IoTの普及と課題

2. IoTの普及と課題

● 世界中で拡大するIoT

200億を超えるIoT機器

世界で2020年までにインターネットにつながるモノの数

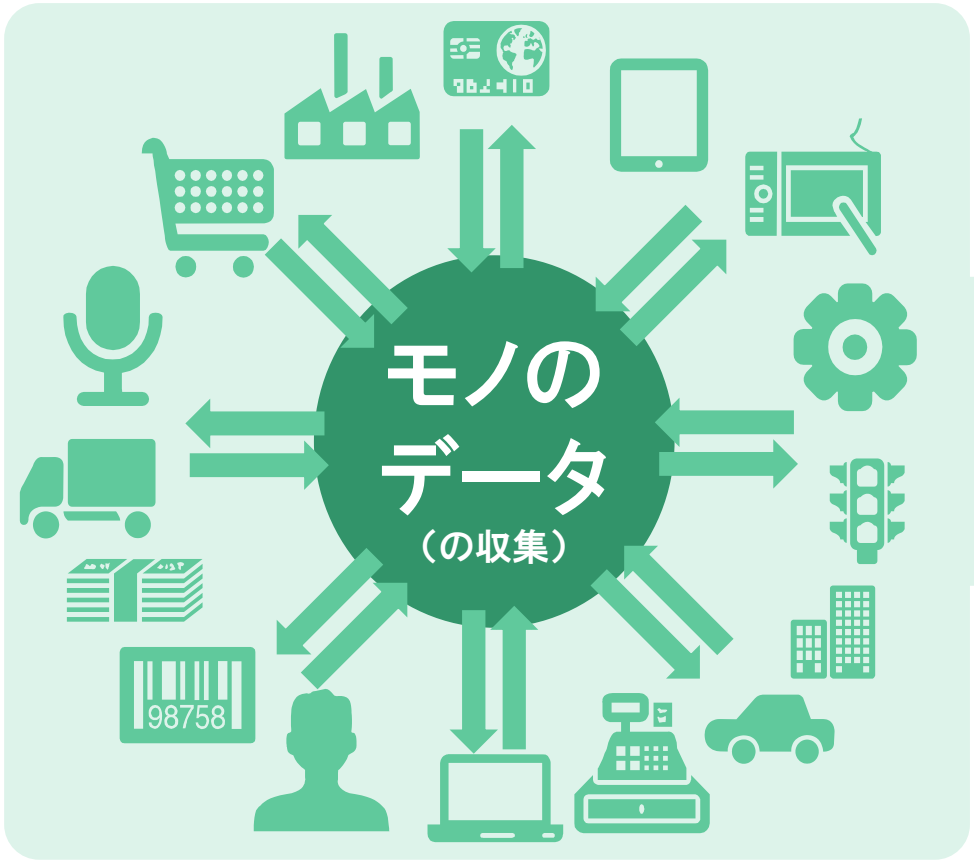
Internet of Things

（モノのインターネット ⇒ データで未来を予測し価値が生まれる時代）

日本では将来の

「成長戦略の柱」

2. IoTの普及と課題



ICTの世界へ

ICTの世界だからこそ
大量のデータ
解析が可能

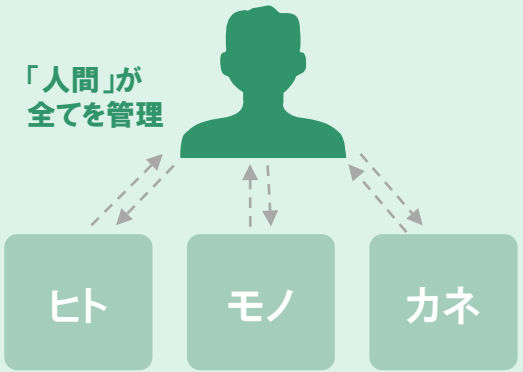
新たな価値を生む

2. IoTの普及と課題

【 ICT導入以前 】

ヒト・モノ・カネの経営リソースの管理をそれぞれ人間が行っていた時代。“情報”は紙などで人間が手計算して、管理していた。

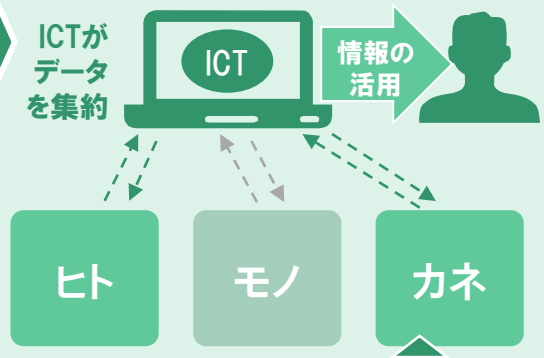
その昔、情報はすべて人間が「手計算」して「紙で管理」していた



【 ICT導入後 】

ICTの導入により、ヒト・モノ・カネの経営リソースのデータが定量的に集約されることで管理しやすくなった。ICTにより、情報は収集・管理しやすく、活用しやすくなった。

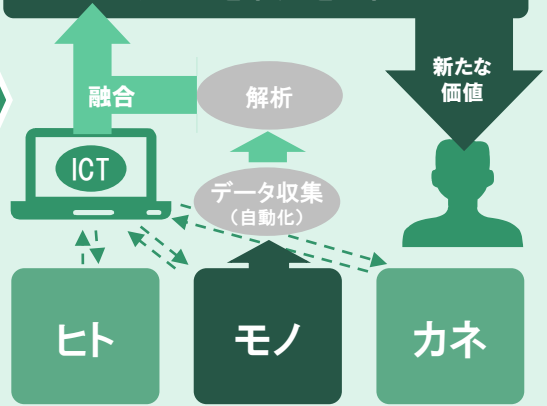
モノのデータは収集する方法がなくそのまま置き捨てられていた



【 ICT＋IoT導入後 】

ICTのみの時代の情報活用は、データは人間が入力するかwebで生成されたものに限定。IoTは、モノから現実に起きたさまざまな事象のデータを収集・解析することによる「新たな価値の創造」を実現させる。

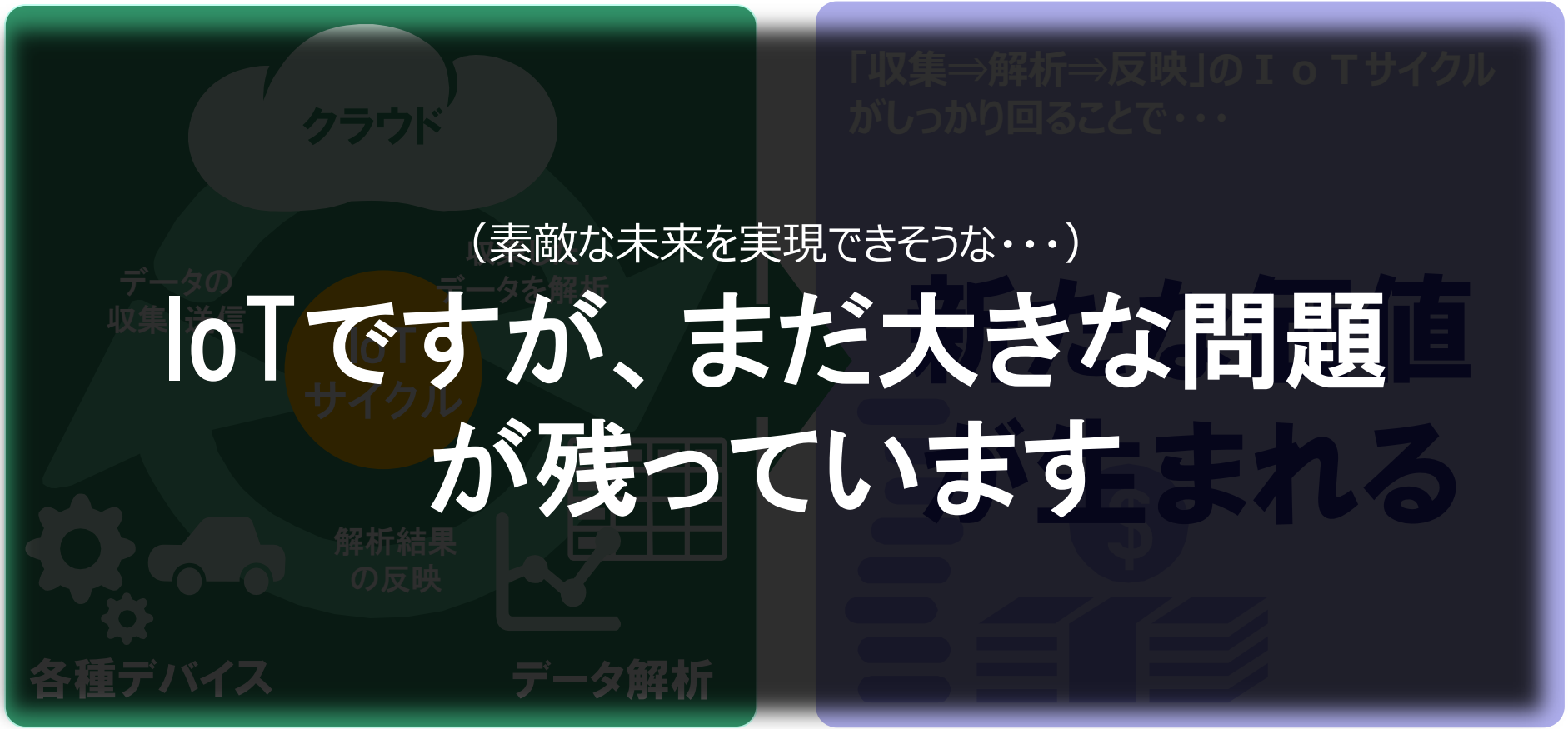
IoTはICTから置き去りにされていたモノのデータを活用を可能にした



FinTechとして進化中

IoTはモノのデータをICTにつなげ、情報活用を進化させる

2. IoTの普及と課題



（素敵な未来を実現できそうな・・・）

IoTですが、まだ大きな問題が残っています

IoTデバイスの管理ができない問題

ＩＣＴでは、数百～数千台の端末（ＰＣやタブレット）も管理しきれずに、端末部分の脆弱性を突かれて、標的型攻撃を受けています。時に数百万台にもなる可能性がある
ＩｏＴデバイスの管理は、将来的に必ず大きな問題になります。

ここ数年、情報セキュリティ対策のトレンドだった標的型攻撃なども管理しきれないPCやスマートフォンのように

「数が多く管理・対策がしきれない脆弱な箇所を狙った」もの・・・。

でも・・・

IoT機器の数はPCなどの比ではない！

機器のコントロールができなくなる

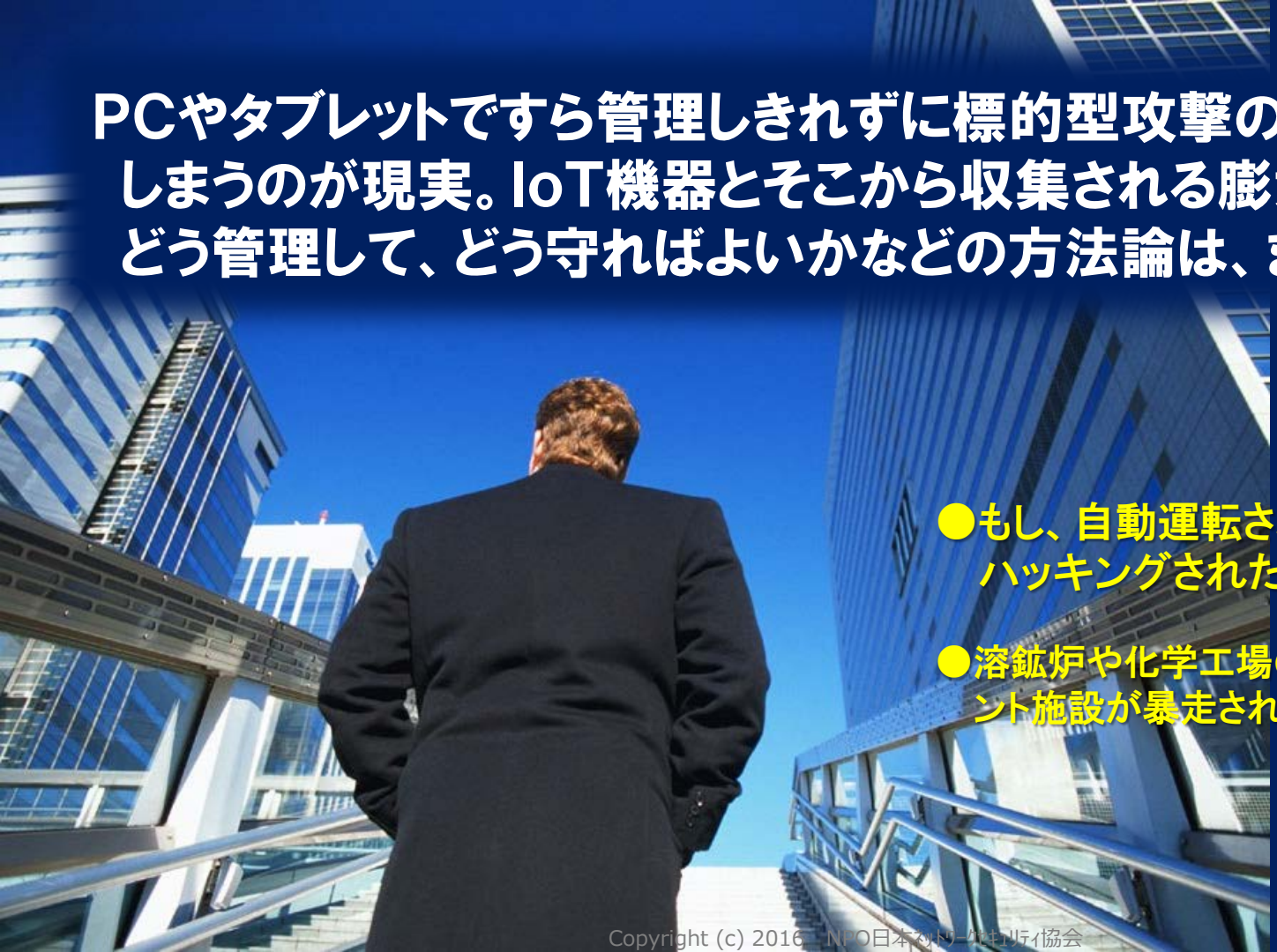
（何らかの理由で機器が制御不能になった場合、自動車の自動運転や工場設備などの安全が保てなくなる）

機器の不正動作による
データの信頼性が低下する

（不正動作等を管理する仕組みがなければ、せっかく収集したデータ精度が悪く解析の意味がなくなる）

膨大なIoTデバイスの管理がしきれなくなる

（野良IoTとも呼ばれる問題）



PCやタブレットですら管理しきれずに標的型攻撃の対象にされてしまうのが現実。IoT機器とそこから収集される膨大なデータをどう管理して、どう守ればよいかなどの方法論は、まだ未確立。

- もし、自動運転されている自動車がハッキングされたらどうするか？
- 溶鉱炉や化学工場のような大規模なプラント施設が暴走されられたらどうするか？

3. 狙われるコンシューマ向けIoT機器

3. 狙われるコンシューマ向けIoT機器

なぜ、コンシューマ向けの
機器が狙われるのか？

どこに狙いを定めて
何をするのかは攻撃者次第！

たとえば…

出口対策の難しさ

（2011年に発生した標的型攻撃の対策の目玉で特効薬のようにもてはやされました）

セキュリティ対策側が想定した「出口」を
はたして攻撃者は通ってくれるでしょうか？

（家に入った空き巣がどこから出て行くかと同じ理屈です。ホントに出口対策は完了してるのでしょうか？）

つまり、攻撃者の身になって想像するしかない！

3. 狙われるコンシューマ向けIoT機器

攻撃者の気持ち
（私だったらバージョン）

サイバー攻撃は生活のための手段
（愉快犯やイデオロギーによる攻撃もあるが、サイバー攻撃全体での絶対数は多くない）

経済活動は費用対効果が重要
（キャッシュフローや効率が重視され、規模が大きくなるとプロジェクト管理の要素も必要）

成功率の高い弱い箇所へ攻撃
（高採算で高効率な攻撃を行うためには成功率をあげることが近道）

3. 狙われるコンシューマ向けIoT機器

※国家安全保障に関わるシステムや重要インフラは除く

標的型攻撃

当たったら大きいが失敗した場合は、
収入がゼロとなりリスクが高い

どちらを
選択する？
（私だったらバージョン）

弱い箇所を狙う攻撃

コツコツと収益を得ながら最適な
ビジネススキームができる

3. 狙われるコンシューマ向けIoT機器

攻撃者の動向を
調べている所を探して
みたら・・・ あった！

〔本日の基調講演〕

吉岡克成先生の研究成果

（ハニーポットを設置した脆弱なIoT機器への攻撃の状況調査）

[出典]「IoTセキュリティの現状と今後の課題（2016年8月3日公開）」横浜国立大学　吉岡克成　准教授

たった半年間に、横浜国立大学に行われた攻撃が・・・

約60万台

（IPアドレスによる区別した台数）

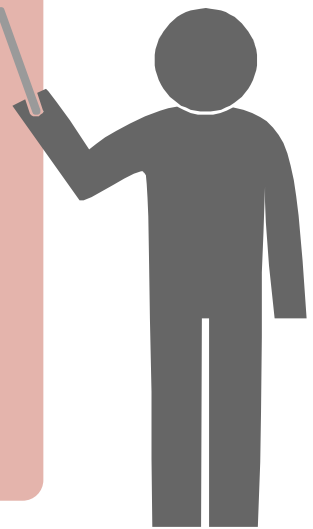
500種類超

（webおよびtelnetの応答で判断した種類）

3. 狙われるコンシューマ向けIoT機器

もちろん、そんな多くの機器が1つの大学に
攻撃(アクセス)する理由があるはずはない・・・。

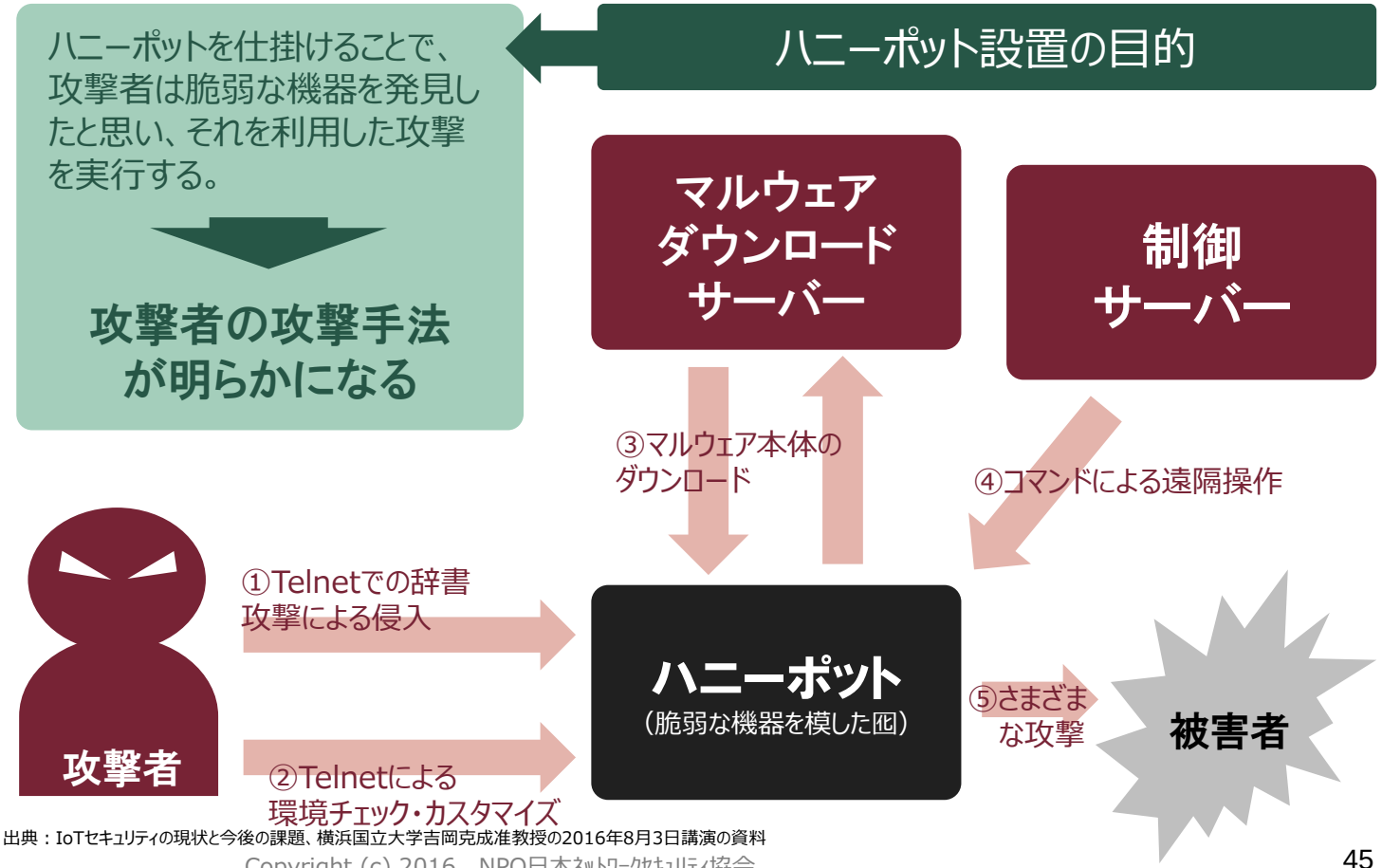
つまり・・・
攻撃者は常に脆弱な箇所を
狙っていることがわかった！



3. 狙われるコンシューマ向けIoT機器

JNSA

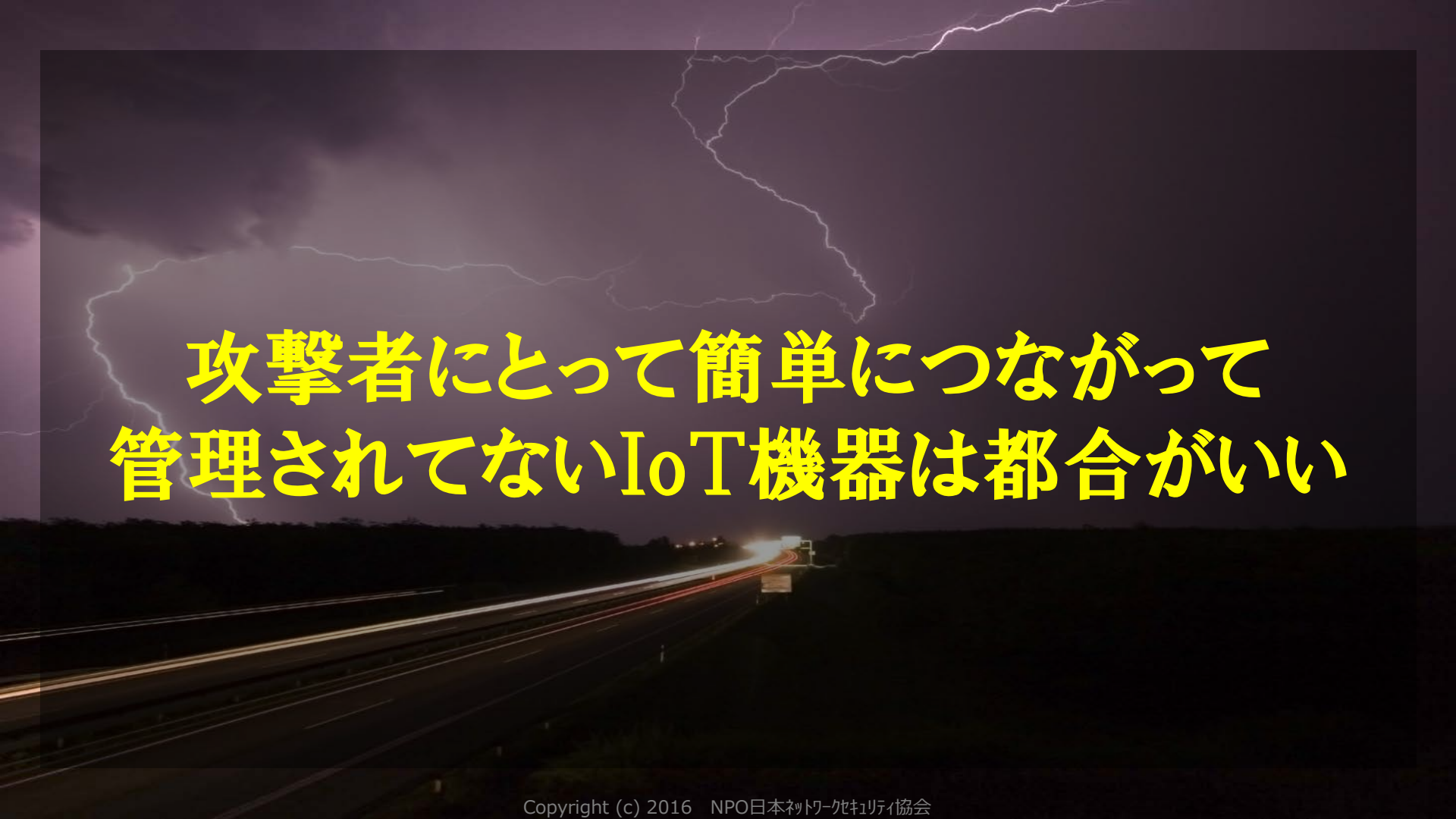
基調講演の復習



出典：IoTセキュリティの現状と今後の課題、横浜国立大学吉岡克成准教授の2016年8月3日講演の資料

原因はTelnet

（開放された２３番ポートは、ライオンの檻に迷い込んだ野うさぎのようなもの）



4. コンシューマ向けIoTのガイドを作成した理由

IoTは核施設や大規模プラントからおもちゃレベルまで多種多様・・・

しかし、攻撃者は確実により脆弱な箇所を狙っている。

無防備なコンシューマ向けの機器が攻撃者のターゲットになりやすい！

4. コンシューマ向けIoTのガイドを作成した理由

情報セキュリティの専門家としてたどり着いた結論

コンシューマ機器開発者向けセキュリティガイドを作成しました！

4. コンシューマ向けIoTのガイドを作成した理由

ガイド作成メンバー

阿部真吾	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
杉浦昌	日本電気株式会社
玉木誠	SCSK株式会社
洞田慎一	JPCERTコーディネーションセンター
福田尚弘	パナソニック株式会社
松岡正人	株式会社カスペルスキー
兜森清忠	オブザーバ
桐山隼人	オブザーバ

*五十音順

4. コンシューマ向けIoTのガイドを作成した理由

JNSA

訴求点 → **コンシューマ向け機器の危険性の認知**
（IoTの重要インフラ部分については各業界団体で標準化プロセスなどが既に検討されている）

ターゲット → **コンシューマ向け機器の開発者**
（一般利用者にガイドに沿った特殊な設定変更や管理などは難しく現実的ではない）

ガイドの構成 → **IoTの概要と具体的対策**
（特に後半は各機器のシステム構成などをわかりやすく記載）

4. コンシューマ向けIoTのガイドを作成した理由

1. Internet of Things(IoT)の概要
1-1.市場動向と未来予測
1-2.IoTの技術
1-3.IoTの制御技術の例

2. IoTセキュリティの現状
2-1.セキュリティとプライバシー
2-2.デバイスとシステムのセキュリティ
2-2-1.IoTのセキュリティ（組込み系）
2-2-2.IoTのセキュリティ（無線系）

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

3. ベンダーとしてIoTデバイスを提供する際に検討すべきこと

4. ベンダーが、ユーザーのIoT利用に際して考慮すべきこと

4. コンシューマ向けIoTのガイドを作成した理由

JNSA

Point **脅威一覧表**（IPAの定義に基づく脅威分析の一覧表）

本ガイドでは、IPAが発行した「自動車の情報セキュリティへの 取組みガイド」を元に、IoT デバイスへの脅威を以下のように定義した。これを異なるデバイスに当てはめて脅威分析を行いました。（参考資料：http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_guide_24.pdf）

● **利用者による操作に起因する脅威**

1.操作ミス	デバイスやシステムを誤動作させられてしまう
2.ウィルス感染	デバイスやシステムが有する情報やデータが漏れるか誤動作させられてしまう

● **攻撃者による干渉に起因する脅威**

3.盗難	デバイスが盗まれてしまう
4.破壊	デバイスが破壊されてしまう
5.盗聴	通信内容を他人に知られてしまう
6.情報漏えい	知られたくない情報を盗まれてしまう
7.不正利用	他人にシステム、デバイス、ネットワークを使用されてしまう
8.不正設定	他人にシステム、デバイス、ネットワークを設定変更されてしまう
9.不正中継	無線や近接による通信内容を傍受されるか、書き換えられてしまう
10.DoS攻撃	システム、デバイスの機能やサービスが利用できなくなる
11.偽メッセージ	偽メッセージによるシステム、デバイスが誤動作してしまう
12.ログ喪失	動作履歴が無いため、問題発生時に対処方法がわからなくなる

IPAがまとめた
12種類の脅威を・・・

5つの状態に分類し
ライフサイクルを一覧化

4. コンシューマ向けIoTのガイドを作成した理由

JNSA

【横軸】 5つの状態（ライフサイクル）

【縦軸】 十二種類の脅威（IPAの定義）

利用者による操作に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
操作ミス	• IoT デバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 • 意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能をOFF にしてしまい通信情報が盗聴される、等	• ID、パスワード、通信先などデフォルト設定の確認・変更機能を実装する • 通信の暗号化機能はデフォルトONにする（特にroot権限やコマンド、レスポンスのやりとり） • テスト（試行）による動作確認を実装する	• 定期的な認証情報の更新ができる • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • ログの取得による不正動作の検知ができるようにする	• 通信先などの異常を自動検知してメール等で通知する • 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• 動作監視（モニタリング） - ランプ - 遠隔通知 • 認証情報に有効期限を設ける	• デバイス内の設定の初期化ができるようにする • 廃棄時は物理的に読み出し不可にするようガイドする • ラベルや注意書き等、システムの構成や制御内容、取扱うデータ、管理者などが類推可能となるおそれのある情報を削除するようガイドする
ウイルス感染	• 利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフト ウェア（マルウェア等）等に感染することによりひきおこされる脅威 • IoTデバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	• ボード購入元の信頼性を確認する（ウィルスが仕込まれていないか） • ネットワークなど安全な環境下で設定を行うようガイドする • 実際のシステムに接続する前にセキュリティの設定が行われるようにする • 最新のセキュリティパッチを適用されるようにする	• 定期的なウィルスチェックができるようにする ・製造元からの脆弱性情報を配信する • ログの取得による不正動作の検知ができるようにする	• 動作状況のわかりやすい表示 • 安全なシーケンスで再起動を実行するようにする • 安全な停止、入出力やネットワークの切り離しができるようにする	• 定期的なウィルスチェックができるようにする	• 連携先に廃棄を連絡するガイドまたは機能を実装する

汎用マイコンボード
（①設定ミス、②ウィルス感染）

4. コンシューマ向けIoTのガイドを作成した理由

JNSA

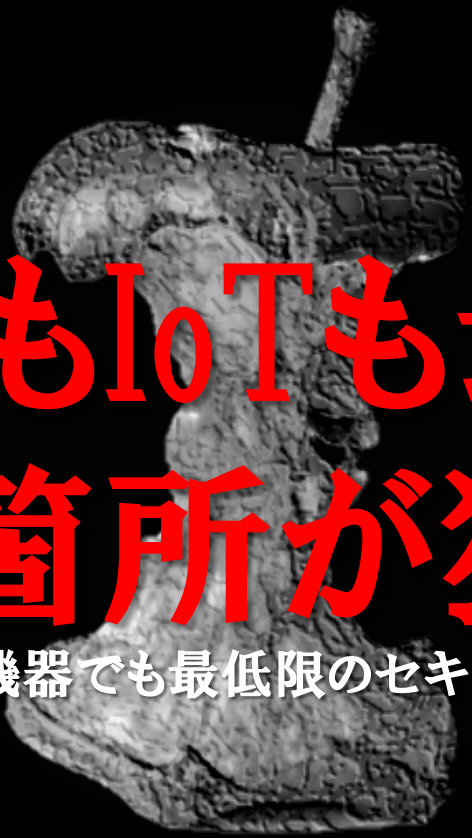
スマートテレビ
汎用マイコンボード
ウェアラブルデバイス
ネットワークカメラ

これらの利用者に
セキュリティ対策を
委ねることは難しい

コンシューマ向けIoT機器の開発者向けの3つのメッセージ

- デフォルト設計を セキュアに！
- 問題発生を 想定する
- 廃棄まで 責任をもつ

繰り返しになりますが・・・



ICTもIoTも最も脆弱な箇所が狙われる

ので、コンシューマ向け機器でも最低限のセキュリティ対策が重要です。

4. コンシューマ向けIoTのガイドを作成した理由

JNSA

JNSAのガイド
はこちら！

別の組織に任せる
（決して放置していいわけではない）

どちらを
選択する？
（JNSAバージョン）

狙われやすい脆弱な箇所へのセキュリティ対策

これが・・・

（ＪＮＳＡ　ＩｏＴセキュリティＷＧで対処が必要と考えた）

現時点でのIoTセキュリティの課題と対策です

もちろん、重要インフラを守る組織との摺り合わせが必要です。

休憩後の

パネルディスカッションへつづく

（今回が日本で組織を越えた“ほぼはじめての”話し合いになります・・・。）

ご清聴ありがとうございました。

END

JNSAの考えるIoTセキュリティの課題と対策

日本ネットワークセキュリティ協会（JNSA） IoTセキュリティWG
武田　一城（日立ソリューションズ）