IoTがサイバー攻撃のターゲットにされる理由

2018年2月26日

株式会社ラック
武田　一城

はじめに

（この講演の主旨）

本日の主旨

＜サイバー攻撃とは何なのかを理解する＞

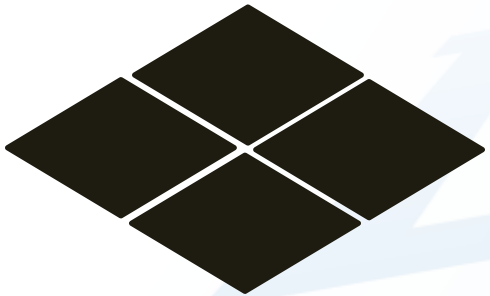
なぜ、サイバー攻撃は繰り返されるのか？	攻撃の目的は何なのか？	ターゲットは何なのか？

- **IT**：20年以上のIT分野のサイバー攻撃の現実を知る
- **IoT**：IoTのセキュリティ面での課題を理解する


サイバー攻撃の現実を
理解することで、
IoTを安全に利用できる
（適切なIoTセキュリティ対策が実現する）

自己紹介

武田一城 なんて言う名前なので・・・



武田だわ

＋

＝

いかにも

あの県

出身な感じですが！

自己紹介

千葉県出身

（風林火山とか関係なし）

株式会社 ラック

トップレベルのセキュリティ技術を駆使した
ITトータルソリューションで、未来をきり拓く

設立	2007年10月1日
代表者	代表取締役社長 西本 逸郎
資本金	10億円
売上高	連結 371億円（2017年3月期）
従業員数	連結 1,734名（2017年4月1日現在）
上場市場	東京証券取引所JASDAQ
事業内容	セキュリティソリューションサービス システムインテグレーションサービス 情報システム関連商品の販売およびサービス

LAC
ともに、イキル

自己紹介

ざっくり言うと・・・

サイバー攻撃を受けた際に、最も

頼りになる企業のひとつ

（SOCサービスを1998年に開始など）

24時間/365日対応の
マネージドセキュリティサービス

JSOC JAPAN SECURITY OPERATION CENTER

自己紹介

緊急対応
担当者

●サイバー救急センター

サイバー救急センターは、サイバー攻撃によって被害を受けた企業・組織の緊急対応を24時間365日実施している最前線でサイバー攻撃に対応するサービスです。

●被害の拡散防止
●情報（証拠）の保全
●調査・解析

被害者

自己紹介

セキュリティ対策の不都合な真実--5年に一度しか来ないベンダーの正体

武田一城 (ラック) 2017年06月19日 07時00分

いいね！ 1,124　ツイート　G+　B! 50　Pocket 142

印刷　メール▼　ダウンロード▼　クリップ

PR 見失うな！働き方改革は何のため？「生産性」を担保する機能とセキュリティ
PR 【動画】脆弱性に対するパッチを適用できない・・・そんなときの対処法は？
PR "問題なく動いて当然"なネットワーク--実現のカギは「DHCP/DNS」にあり！
PR ちょっと待った！メーカーに頼るその前に--IT機器の保守の延伸

本連載「企業セキュリティの歩き方」では、セキュリティ業界を取り巻く課題、問題点をひもときながら、サイバーセキュリティを向上させていくヒントを提示する。

ベンダーにもセキュリティ人材がいない

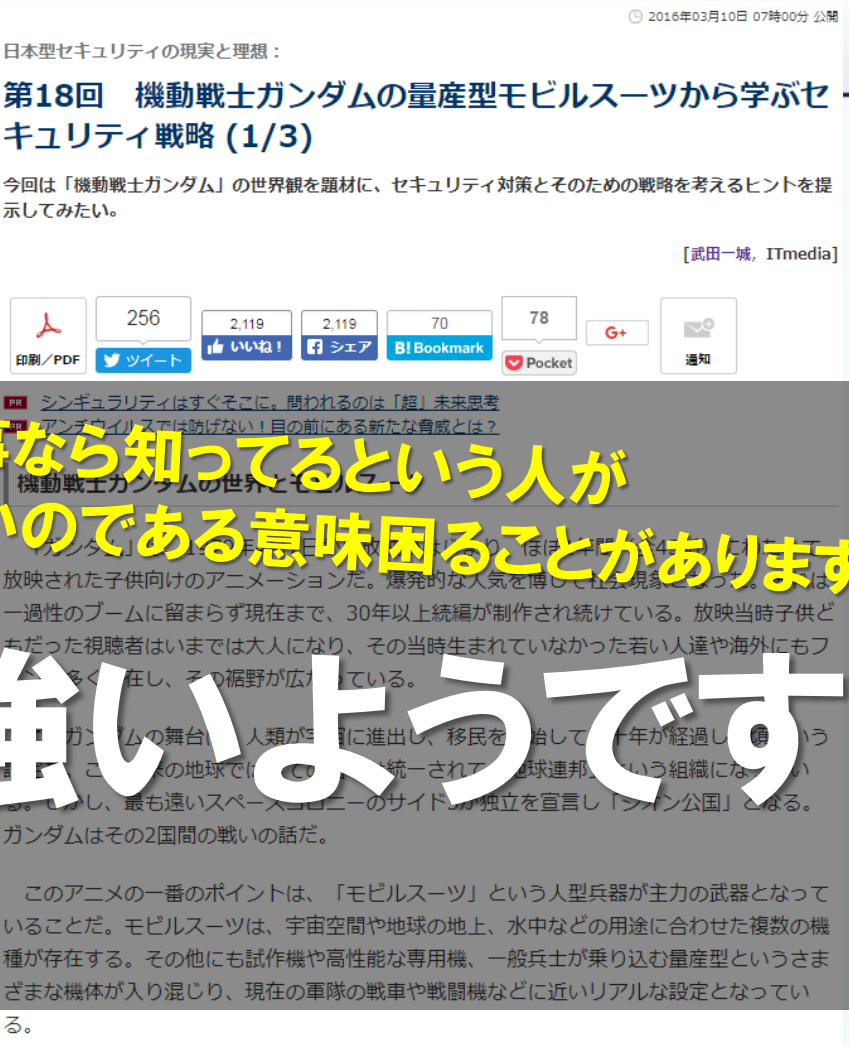
前回は、日本企業が表向きは多層防御のセキュリティ対策を講じていながら検知しても対処ができない「セキュリティマネジメント不在」の状況を、今回は、なぜセキュリティ対策製品を提供するベンダーがその状況を看過しているかについて述べる。

セキュリティマネジメントの状況は、ユーザー企業に進歩が見られなかった。セキュリティ製品を提供しているベンダーが、なぜこの状況を看過しているのだろうか。

答えは簡単だ。それは、ユーザー企業にセキュリティマネジメントがいないのと同様に、セキュリティ製品を提供しているベンダー側にも該当者がいないか、いたとしても非常に少数だからである。つまりユーザー企業もベンダー側も、同じ状況に陥っているというのが、問題の根を深くしている。

また、ここ何年かセキュリティ関連の執筆を多数しているので、ご存知の方も多いかもしれません

自己紹介



2016年03月10日 07時00分 公開

日本型セキュリティの現実と理想：

第18回　機動戦士ガンダムの量産型モビルスーツから学ぶセキュリティ戦略 (1/3)

今回は「機動戦士ガンダム」の世界観を題材に、セキュリティ対策とそのための戦略を考えるヒントを提示してみたい。

[武田一城，ITmedia]

印刷／PDF　256 ツイート　2,119 いいね！　2,119 シェア　70 B! Bookmark　78 Pocket　G+　通知

PR シンギュラリティはすぐそこに。問われるのは「超」未来思考

PR アンチウイルスでは防げない！目の前にある新たな脅威とは？

機動戦士ガンダムの世界と

放映された子供向けのアニメーションだ。爆発的な人気を博して社会現象となった。は一過性のブームに留まらず現在まで、30年以上続編が制作され続けている。放映当時子供だった視聴者はいまでは大人になり、その当時生まれていなかった若い人達や海外にもフ多く存在し、その裾野が広がっている。

ガンダムの舞台は人類が宇宙に進出し、移民を始めて数十年が経過した頃という設定。この地球では統一された地球連邦という組織になっている。しかし、最も遠いスペースコロニーのサイドが独立を宣言し「ジオン公国」となる。ガンダムはその2国間の戦いの話だ。

このアニメの一番のポイントは、「モビルスーツ」という人型兵器が主力の武器となっていることだ。モビルスーツは、宇宙空間や地球の地上、水中などの用途に合わせた複数の機種が存在する。その他にも試作機や高性能な専用機、一般兵士が乗り込む量産型というさまざまな機体が入り混じり、現在の軍隊の戦車や戦闘機などに近いリアルな設定となっている。

この記事なら知ってるという人が
結構多いのである意味困ることがあります。

特に・・・

この印象が強いようです

※機動戦士ガンダムは、株式会社サンライズの登録商標です。

とりあえず、
質ではなく

手数で
勝負しています

（ここ数年のセキュリティ関連の寄稿は私が最多だと思います）

自己紹介

常識破りのIoTセキュリティ

本格普及間近のIoT、今できるセキュリティ対策は？

武田 一城＝ラック／JNSA IoTセキュリティWG　2017/06/05　ITpro

目次一覧

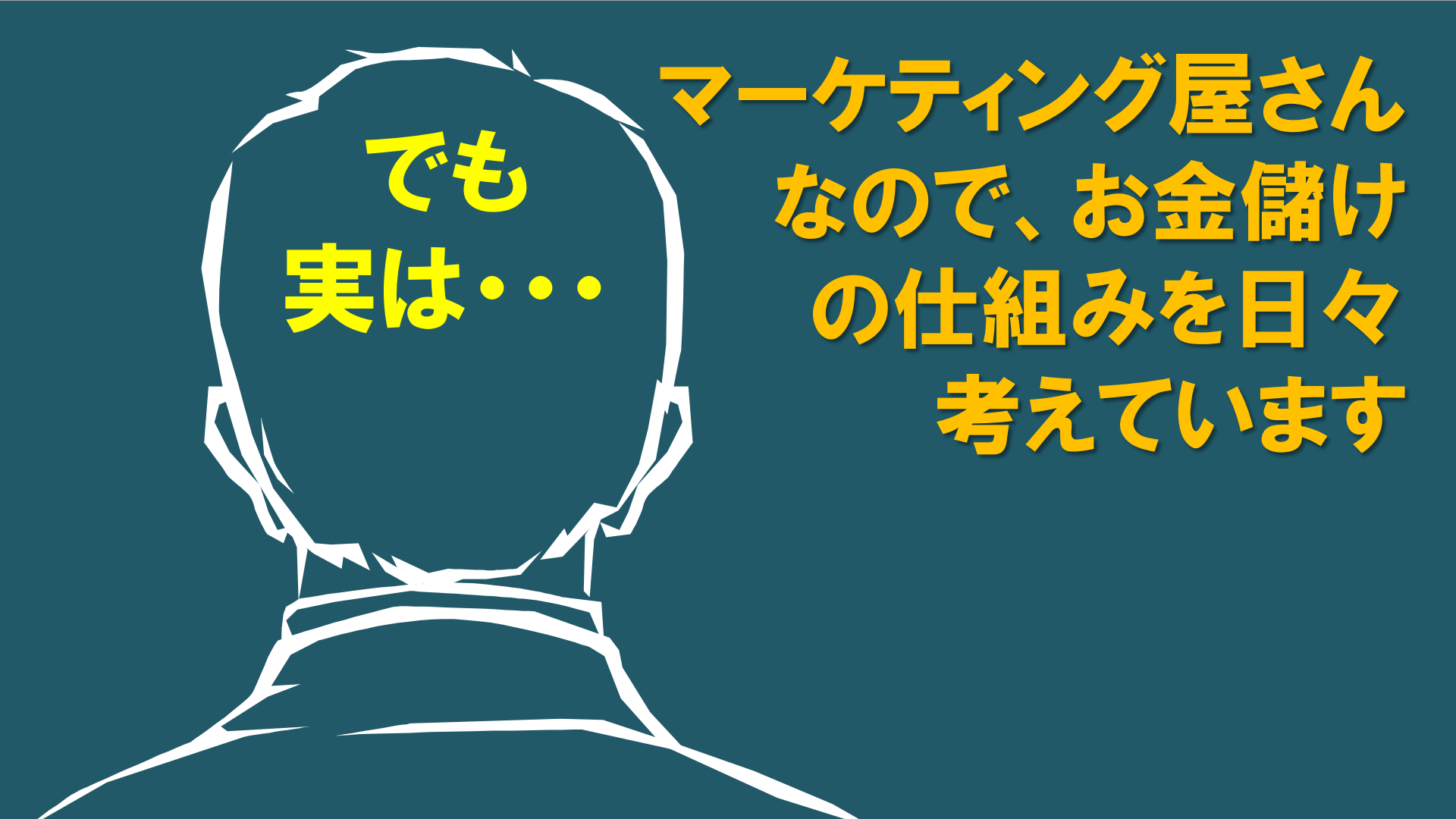
IoT（インターネット・オブ・シングズ）という言葉がここ数年で一気に広まった。だが、実際に社会へ普及させるにはは大きな課題がある。課題の1つは通信コストだ。

これまでのインターネット活用の主役はヒトだった。接続するデバイスもPCやスマートフォンというヒトが利用するものだった。通信でやり取りするものは、ヒトが使いやすく楽しむためのリッチなコンテンツが中心となる。そのため通信インフラには広帯域と高品質なものが求められ、1台当たり数千円（月額）の通信費が必要だった。

しかし、モノの通信には、それほどの広い帯域や高い通信品質は必要ない。IoTでやり取りするのは数値や少量のテキストデータだからだ。そのため、LTEや3Gなど既存の携帯電話系の通信インフラは、IoT環境ではオーバースペックとなってしまう。

もう一つの課題は電源だ。ヒトが利用するスマートフォンであれば、都度充電すればよい。だが、ヒトが行けない場所にこそIoTが必要という要件も多いだろう。そのため、電池交換せずに数カ月や数年単位での稼働が求められる。

本日のメインテーマ


でも
実は・・・
マーケティング屋さん
なので、お金儲け
の仕組みを日々
考えています

数字が語る
サイバー攻撃の現実

（３つのセンセーショナルな数字でセキュリティの現実を理解する）

＜1つ目の数字＞

97%

※または9割以上

Answer

97%

未知の脅威が侵入している企業の割合

＜2つ目の数字＞

205日

Answer

205日

セキュリティ侵害が発生してから組織がその侵入を発見するまでの平均日数

※FireEye社による発表(2015/10/29)


＜3つ目の数字＞
55%

55%

Answer

アンチウィルスソフトが検知できないマルウェア

※Symantec社による発表(2014/5/7)

なので、2014年5月7日は、
アンチウィルスソフト
の命日らしい・・・。

3大AVソフトベンダーのVPの公式発言なので・・・

数字が語るサイバー攻撃の現実

97%

ほとんどの企業は何らかの形で侵入されている

（たぶん、皆さんだけが例外である可能性は少ない）

205日

皆さんが気づく前に攻撃者は深く侵入している

（外部との境界付近から、時間をかけて内部の重要な機密情報にたどり着く）

55%

もう、アンチウィルスソフトだけでは防げない

（検体が見つかっていないマルウェアの検知は、アンチウィルスソフトの構造上難しい）

かなりの大ダメージ！

では、防御側は蹂躙されるのを待つだけなのか？

対策はあります。攻撃者の行動を理解し、その実態を知ることが防御対策の第一歩！

もちろん
推測

攻撃者の実態

（セキュリティ対策は「攻撃者が何がしたいのか？」を把握することからはじまる）

攻撃者の実態

そもそも・・・

（１）誰が攻撃しているのか？
（２）なぜ攻撃するのか？
（３）どうやって攻撃するのか？

攻撃者の身になって考えることが重要

攻撃者の実態

（1）誰が攻撃しているのか？

実はこのパターンが多い（？）

不良

ハッキングおたく

サラリーマン

（2）なぜ攻撃しているのか？

ほとんどが金銭目的！

（攻撃者は、サイバー攻撃分野に特化した起業家のようなもの）

サイバー攻撃 ＝ 儲かるビジネスモデル

※資本主義の富の集中への反発や宗教・思想やイデオロギーで攻撃している場合もある！

（3）どうやって攻撃するのか？

攻撃者は、常に高い効果（利益）を得やすい攻撃手法を次々に考案する。そして、さらに改善を加える。

より儲かりやすい攻撃へと進化を続ける

まるで優良企業のような改革・改善

攻撃者の実態

防御側

【10年以上前の古いまま】

防御側は時代遅れの古い防備だけで安心しきっている。ツギハギで多少の修正は行っているが、防御思想も守り方も良く分かっていない。
装備だけでなく、守るノウハウもなく攻撃側との差は開くばかり・・・。

人材不足

限られた費用

格差拡大

攻撃側

【攻撃力の向上を持続】

攻撃側は攻撃手法もどんどんレベルアップさせている上に、特に防御側の弱点を突くノウハウを貯めている。常に組織化され、方法や手法をブラッシュアップすることで、より効率的な攻撃ができるようになっている。

【出典】ITメディアEterprize

①高度な攻撃

経験値

経験値　経験値

経験値　経験値　経験値

②効率的な攻撃

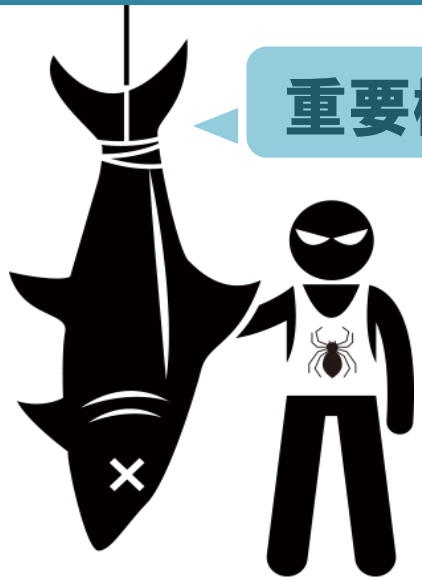
攻撃ツール

脆弱性情報

闇市場

攻撃者の実態

標的型攻撃（APT攻撃）



難易度が高いが、成功すれば
大きな収益が見込めるビジネス

二極化
の傾向

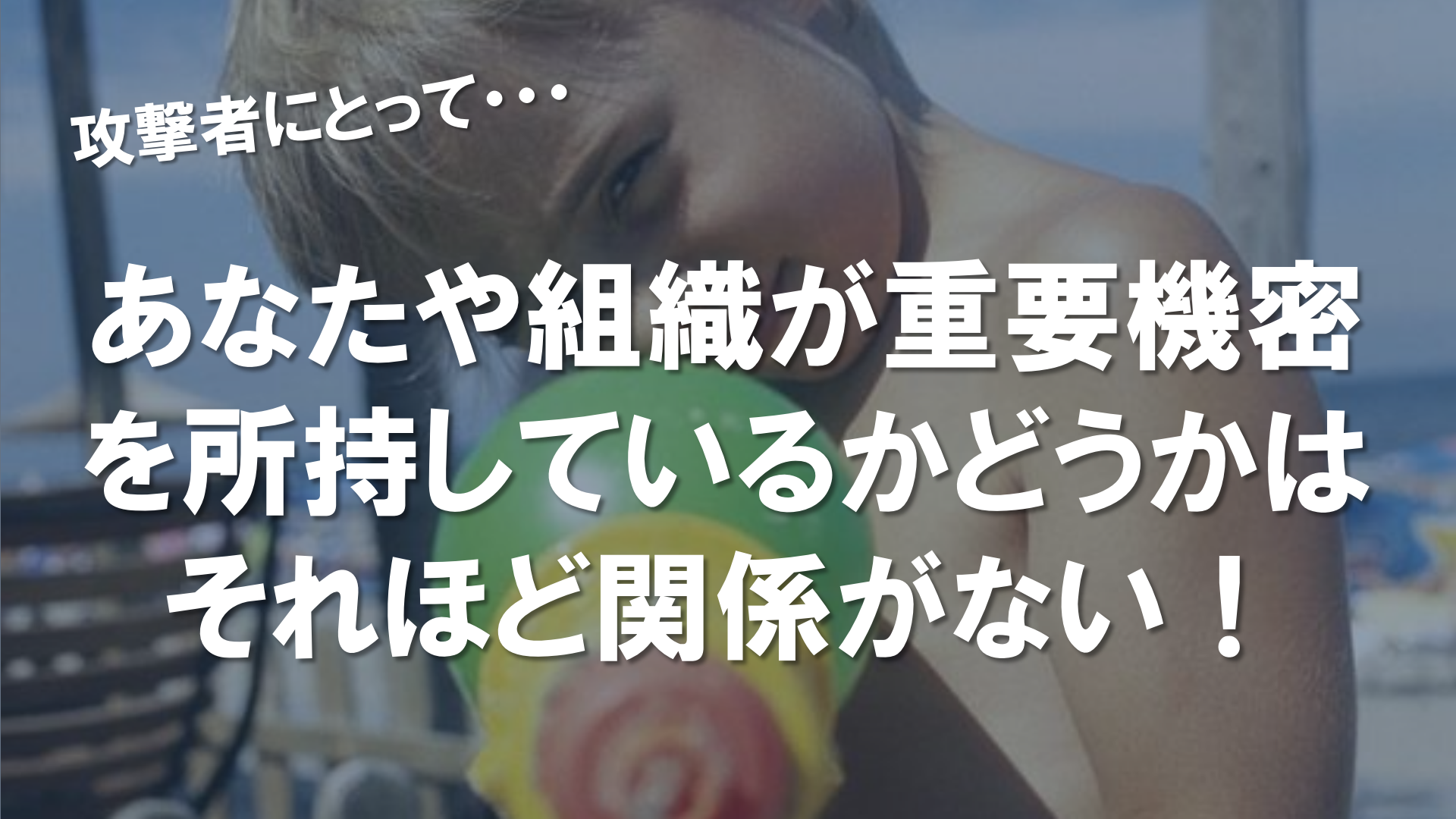
弱い箇所を狙う攻撃

コツコツと定期収入が
得られる手堅いビジネス

※マーケティング観点からの私見です。

【出典】ITメディアEterprize


このことから何が
わかるかと言うと・・・


攻撃者にとって・・・
あなたや組織が重要機密
を所持しているかどうかは
それほど関係がない！

つまり、

サイバー攻撃によって、儲かる仕組みが出来てしまうと、

誰もが攻撃される可能性がある！

攻撃者の実態

たとえば、

ビットコインなどの仮想通貨の登場

（これによって全てのPCとサーバが攻撃対象となった）

攻撃者の実態

1. ランサムウェアの決済

リスクの少ない身代金の受領が可能になった！

（攻撃者はランサムウェアをばら撒き、感染させるだけで自動的に利益を得ることが可能）

2. ビットコインマイナー

ビットコインの計算をすると報酬がもらえる

（攻撃者はサーバ等のリソースを悪用し、ビットコイン採掘の報酬を不正に受け取る）

攻撃者の実態

注意　**ただし、ビットコインの存在自体が悪ではない。**

＜ご参考＞

実は、現在の通貨も金本位制を前提とする金兌換の仕組みのはずが、いつの間にか各通貨毎の兌換をやめてしまった。以前は、基軸通貨だったドルとの交換による裏づけで実質的な金兌換・・・の筈だったが、米国ニクソン大統領時代（1971年）に政策転換され、ドルの兌換は停止された。

※そもそも、現在の貨幣という存在自体がすでにあやふやであり、大国による為替操作も行われている（？）

インターネットのように、仮想通貨もなくては
ならないものになる可能性がある技術のひとつ

ただし、最近こんな事件があったので、一般の人は非常に怪しいものだと感じているはず・・・。

CoinCheckでのXEM不正送金（2018年1月26日）

～被害総額5億2,300万ZEM（580億円相当）、発行数の5%、被害者数：約26万人～

Zaifで20億BTCを0円で購入（2018年2月16日）

～「簡単売買」のシステム異常で訂正処理したため被害ゼロ、BTCの発行数は2,100万BTC～

仮想通貨（暗号通貨）は、本来の決済の仕組みとは、大きく異なる賭け事の対象となってしまった

（野放しの金融事業は非常に儲かることを証明。反面、仕組みが未整備で高リスク）

少々横道に逸れたので
本題に戻すと・・・

サイバー攻撃は世界規模のビジネスとなり、機密情報の窃取目的だけではなくなった

（技術の進歩や仮想通貨は、それを後押ししたに過ぎない）

そのため、

うちには、重要な情報など
無いので狙われない！

むしろ・・・

（大きな利益が得られる重要機密情報は、もちろん狙われますが…）

脆弱な箇所が狙われる

※脆弱な箇所こそ優先して狙う「脆弱性ファースト」な状況かも？

脆弱な箇所とは？

（脆弱であることが攻撃者とターゲットとなり得る）

どのようなところが狙われるのか？

（どのようなところが脆弱になりやすいのか？）

Answer（個人的な考察）

クラウド

IoT

脆弱な箇所とは？

クラウドが脆弱になりやすい理由

クラウドコンピューティングが技術的な制約などで、オンプレミスよりもセキュリティレベルが低くなるということはほとんどない。むしろ、オンプレミスのサーバーによく見られるSSHなどの脆弱性などは、セキュリティ設定を厳しくしていることで、**むしろ強固な場合も多い**。

しかし

構造や仕様、適正な設定方法を理解しなくても簡単にシステムが稼動してしまい、管理ができない

脆弱な箇所とは？

IoTが脆弱になりやすい理由

ITはインターネットが普及し始めてから四半世紀の歴史があり、過去に多くの事件や事故があった。そのため、**ITを守るノウハウの蓄積**は一定レベルある。

しかし

IoTを守るためのノウハウはメーカーにも利用者にもない

特に、今後のIoTは非常に
危険かもしれません。

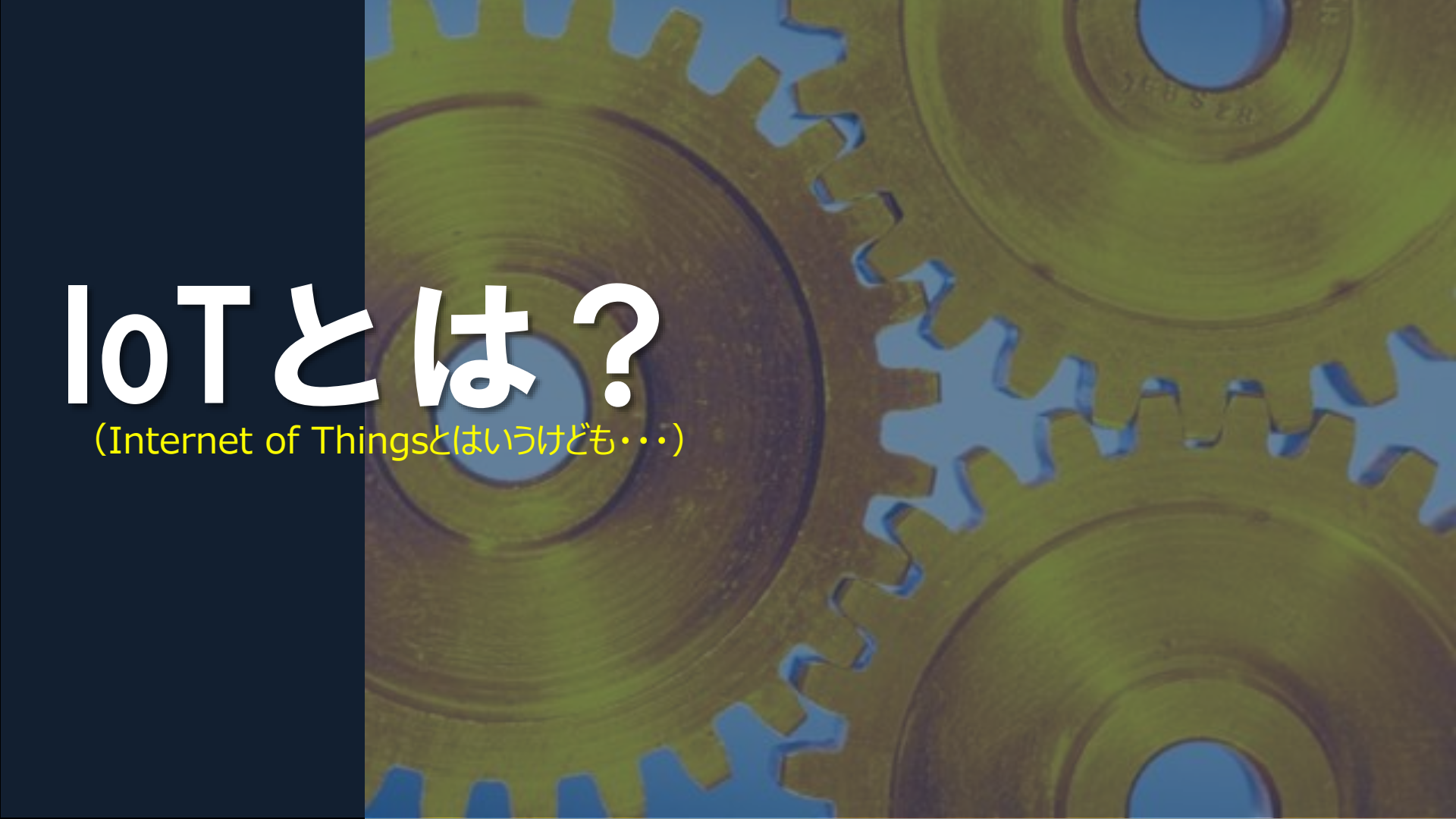
なぜなら・・・

脆弱な箇所とは？

ごく単純に・・・

IoTデバイスが多すぎて管理できない

ＩＴ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。


IoTとは？
（Internet of Thingsとはいうけども・・・）

IoTとは何か？

大雑把に言うと・・・

IT以外でインターネットに接続される全てを指す言葉

IoTとは？

その中でも、
この3つがIoT
の代表例

- 組込み系
- 制御系
- プロセス系

IoTとは？

組込み系

様々な機器にコンピュータが組み込まれた専門用途の機器とそのシステム

- キオスク端末
- カーナビ
- 自動車（センサーの進化）
- 情報家電
- 産業用機械

制御系

機器やシステムが動作する際のタイミングや順序などを制御するシステム

- 交通システム
- 工場の生産ライン

プロセス系

大規模な製造業などで用いられる温度、圧力、流量などを適正値に合わせて制御するシステム

- 石油化学プラント
- 素材精製

IoTとは？

管理すべき端末の数がこれまでのITと比較にならない！

● 世界中で拡大するIoT

530億個

2020年までにつながるモノの数（Gartner調査）

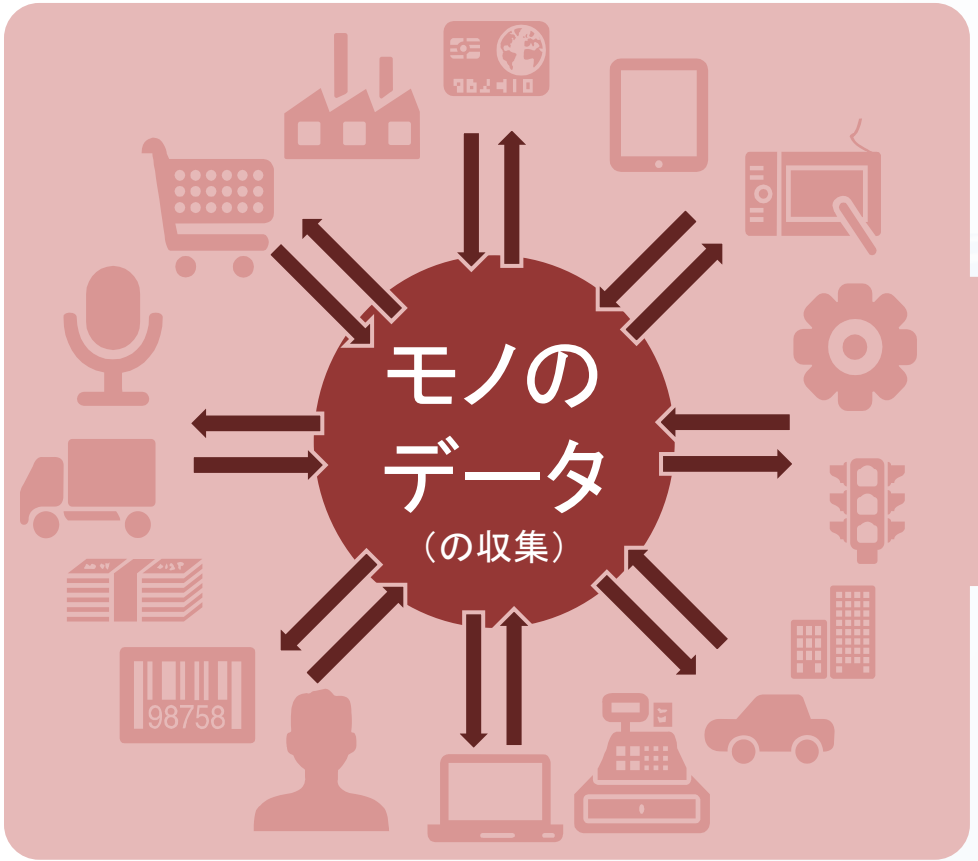
3.04兆＄

2020年の世界の市場規模（IDC調査）

Internet of Things

（によって、物理世界とサイバー空間が繋がる）

脆弱な箇所とは？



ITの
世界へ

POINT

ITの世界だからこそ
大量データの
収集・解析が可能

物理世界と
サイバー空間が融合

IoT時代はセキュリティよりも・・・

セーフティが問題になる

ディスプレイの向こう側の問題だけではなくなる！

それでも・・・

世界中で儲かるビジネスと考えられている
IoT拡大のスピードがセキュリティ対策のために
停滞することは、まず無いでしょう。

なぜなら・・・

進化のスピードを落とすことは
ビジネスでの負けに直結するから

（そもそもIoTを守れる人材育成からはじめる必要がある）

IoTへの攻撃

（横浜国立大学の吉岡先生の調査）

昨年のこのセミナーでの基調講演

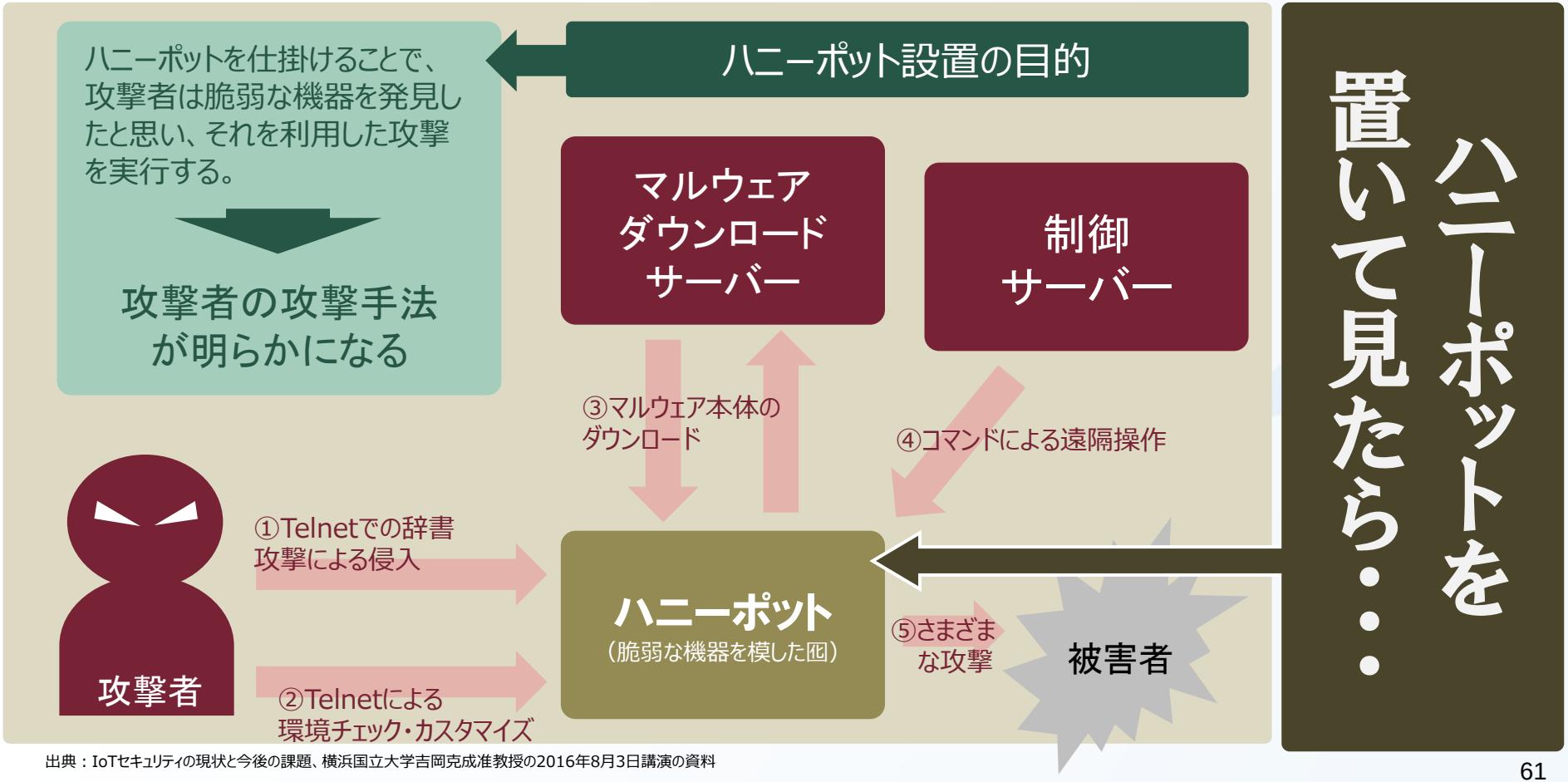
横浜国立大学

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

IoTへの攻撃



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

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の応答で判断した不正アプリケーション）

めっちゃ
攻撃された

IoTへの攻撃

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･･･

攻撃される理由は、脆弱なシステムというだけで充分

現時点のIoTにおける

脆弱性の最大の原因はTelnet

（開放された２３番ポートから、攻撃者はIoT機器を自由に操作できる）

IoTへの攻撃

Telnetは、本来インターネットに開放してはいけないもの

（インターネット以前のクローズドなネットワーク環境での利用を想定したもの・・・。ITの分野では常識）

IoT機器の製造元と利用者の双方が、インターネットに接続する際の最低限の常識を知らない状況

IoTへの攻撃

現時点で、IoT機器は非常に脆弱な状態で放置されており、攻撃者に都合の良い環境を提供してしまっている

このままでは、IoT機器が

サンドバッグのような状態になってしまう・・・

ただし、勘違いしては
いけないのは・・・

Telnetを塞ぐことが
IoTセキュリティ対策ではない

Telnetの対策は、玄関に鍵をかける程度の**当たり前の対応**でしかない

IoTのセキュリティ対策

IoTのセキュリティ対策

まだIoTでは収益をあげていない

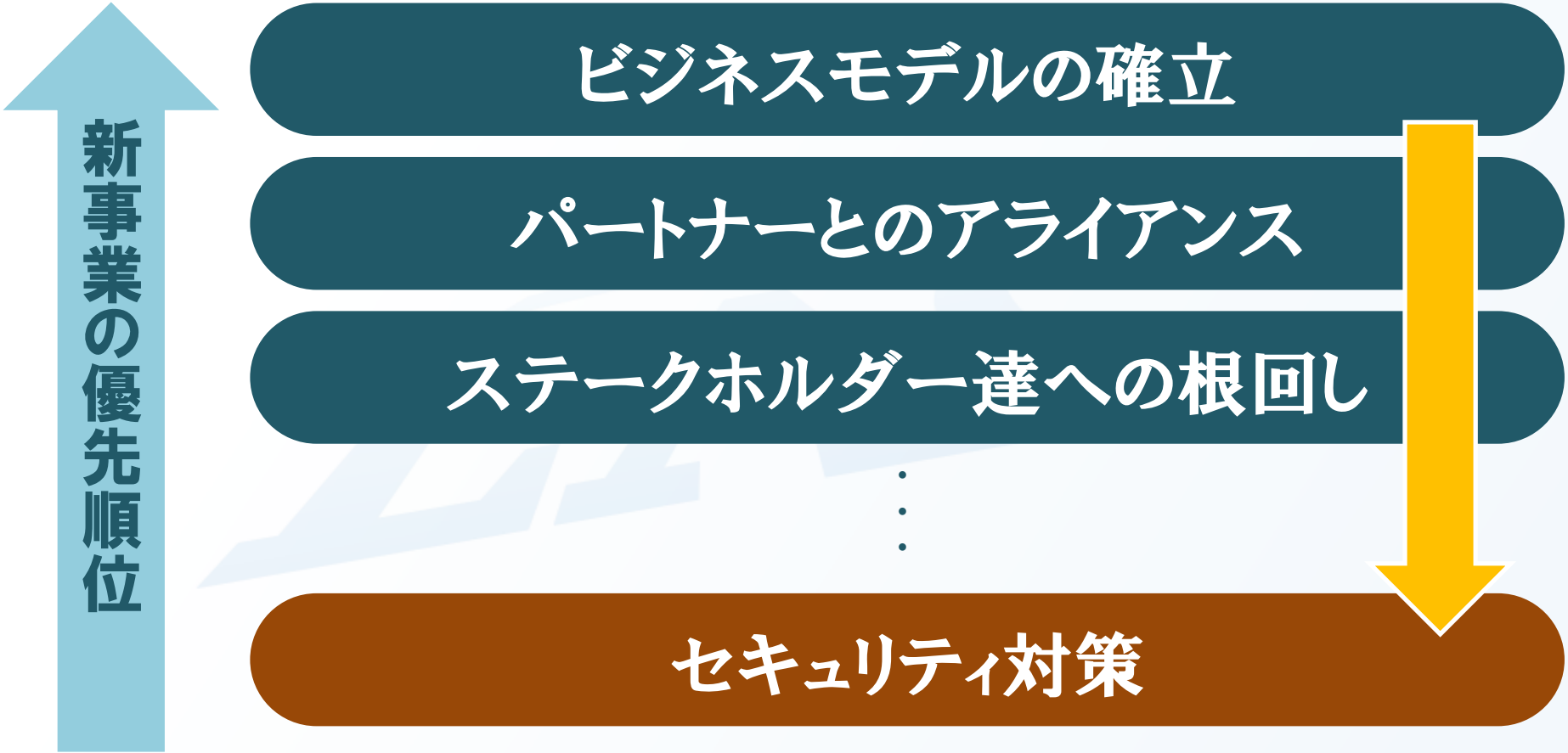
現時点では大問題は発生していない

何を守るべきかが定まっていない

製造メーカーも利用者も世界と繋がることのメリットに夢中！
（しかし、それにどのようなリスクをあるかという危機意識は希薄・・・）

実は、ITのセキュリティ対策もすでに四半世紀ほどの歴史がありますが、1,000億円級の重要機密を持つグローバル企業級や公共・金融などの意識の高い企業を除くと、まだまだセキュリティ対策はもちろん危機意識も充分とは言えない状態・・・。

IoTのセキュリティ対策



実際、サイバー攻撃の
危機意識の実感は湧きにくい・・・。

（そして、実際セキュリティ対策は難しい。）

セキュリティ対策は専門家に任せたい

（正確には、制御系技術者に既に丸投げされている）

しかし、

制御系やプロセス系、組込み系に詳しい

セキュリティ対策人材は非常に少ない

（ITのセキュリティ専門家も、この分野のセキュリティ対策ではそれほどあてにならない）

だからと言って、まだ八方塞がり
という状況ではありません

IoTのセキュリティ対策

危機意識の啓蒙のために、現状の危ない部分のお話をしましたが・・・

それでも、現時点でのIoTは、非常に重要なインフラ以外は「攻撃されやすい特に脆弱な機器」への攻撃が主流です。

つまり

一定のセキュリティ対策をするだけで防げるレベルの攻撃

（発電所を含む大規模プラント、医療機器ほかの命に関わるようなIoTを除く）

逆に、それが出来ていないとセキュリティ機能不全で・・・

リコールの対象にもなる

帰社したら、経営者にこれを是非言ってください。一番効く筈です。

IoTのセキュリティ対策

IoTをビジネスとして考える時には、「セキュリティ対策は製品品質を高めることと同様」と考えることが最も実感しやすいと思われます。

その品質を実現するためには・・・・

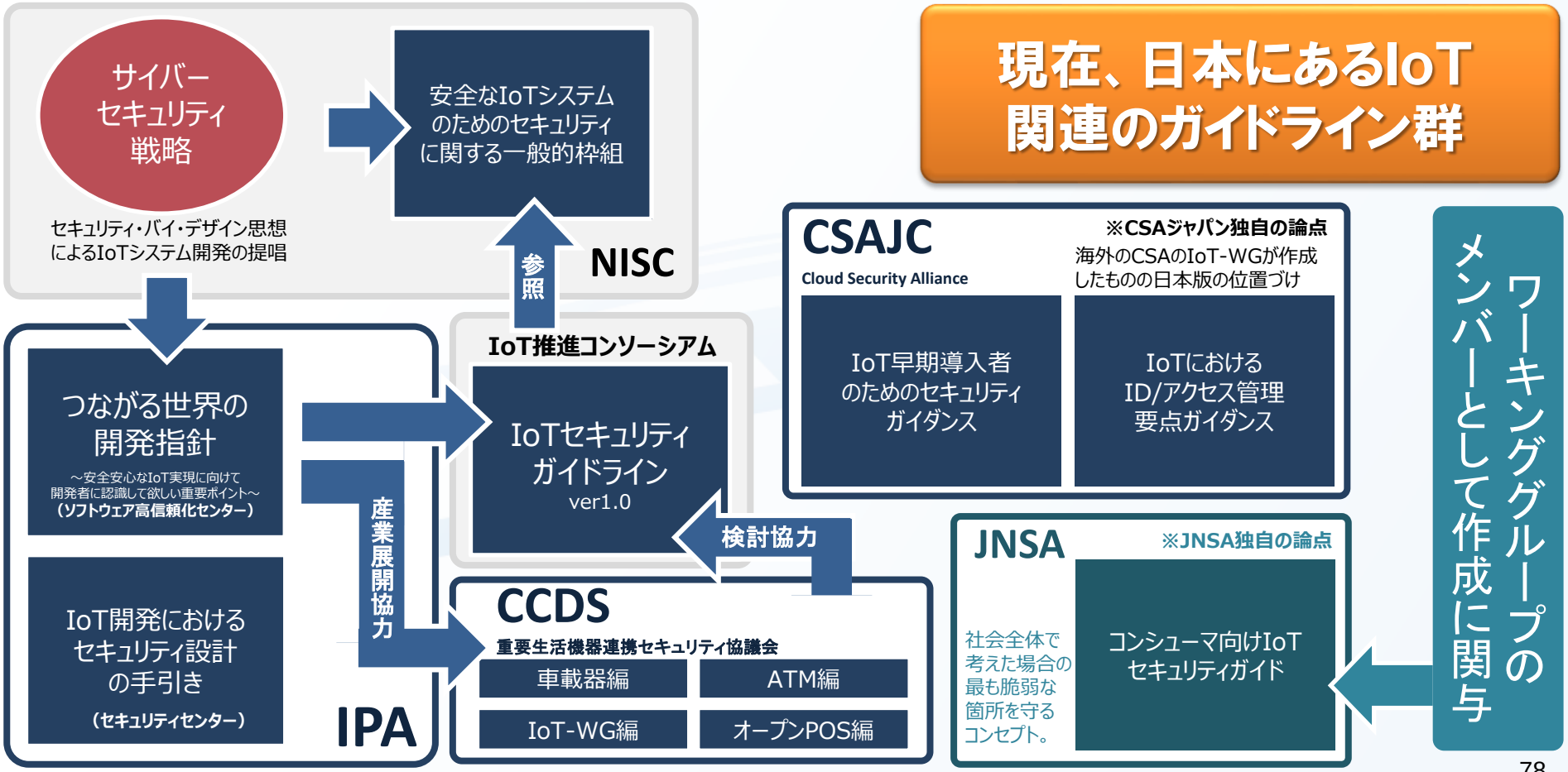
なにを
守るべきか？

どうやって
守るべきか？

守れなかったら、どうなってしまうか？
（をきちんと認識しておくことです）


そして、
IoTを守るための動きは
既にいくつも開始されています

IoTのセキュリティ対策



さらに・・・

情報処理推進機構と総務省からIoTセキュリティに関する資料が公開

（10月2日、3日）

IoTのセキュリティ対策

重要インフラの制御システムを守るためのリスク分析に特化したガイドと実施例

<ガイド>
350頁

<実施例>
70頁

非常に理にかなった内容ですが

合計420ページと、かなり大容量

【出典】https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

IoTのセキュリティ対策


別紙

IoT セキュリティ総合対策

平成 29 年 10 月

サイバーセキュリティタスクフォース

サイバーセキュリティタスクフォースによる
「IoTセキュリティ対策に関する提言（2018年4月発表）」

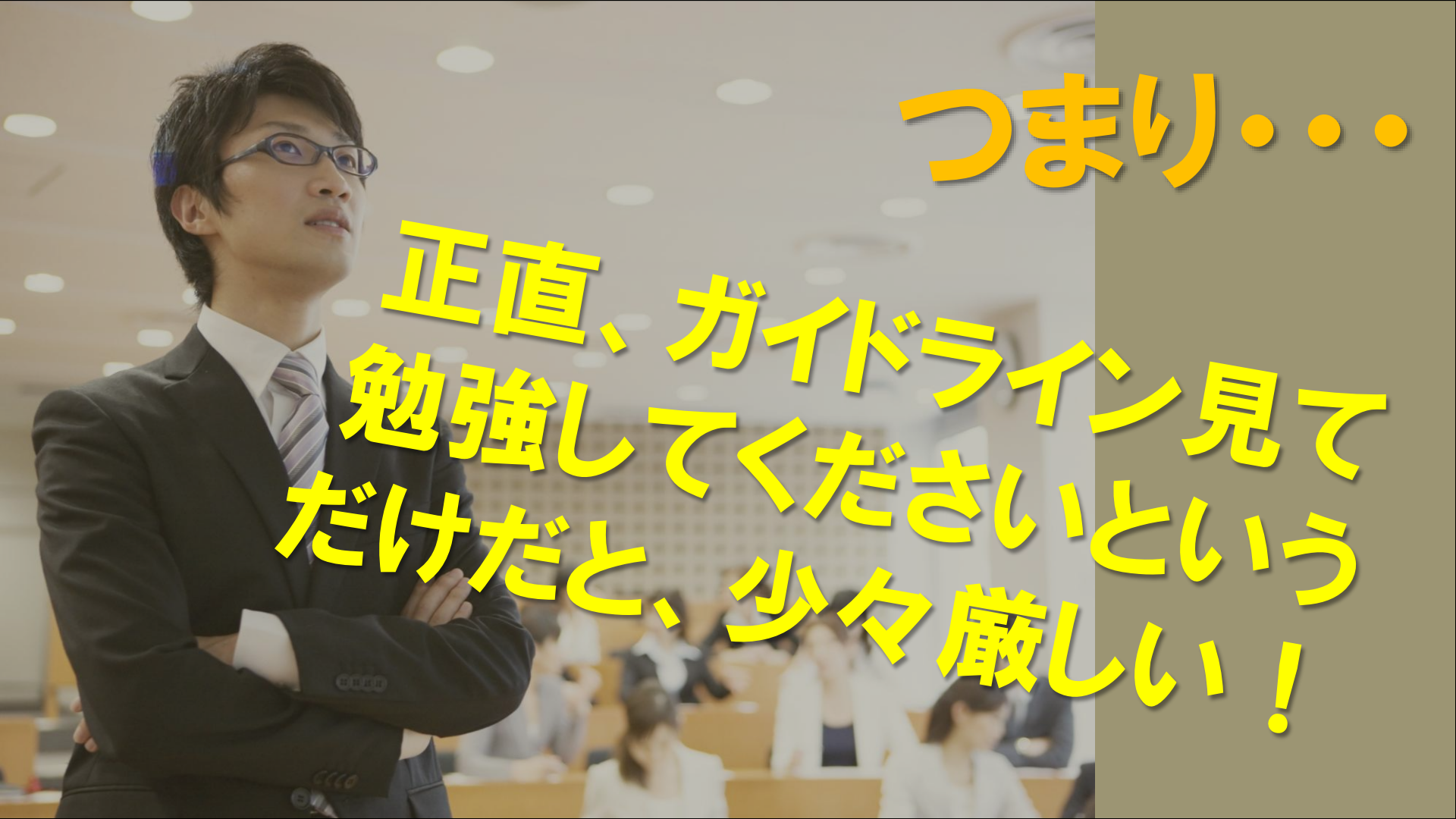
上記を踏まえつつ、総合的な視点での対策を講じる

～具体策～

- （１） 脆弱性対策に係る体制の整備
- （２） 研究開発の推進
- （３） 民間企業等におけるセキュリティ対策の促進
- （４） 人材育成の強化

ただし、研究開発や国際連携など一般の方には少々とっつきにくい

【出典】http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html


つまり・・・
正直、ガイドライン見て
勉強してくださいという
だけだと、少々厳しい！

なので、

今回はIoT機器を守るために

具体的に何を学ばなくてはならないか？

をテーマに本セミナーを企画しました

【Point】この後の3つの講演でその説明をします！

ガイドラインラッシュから国際標準の動向

伊藤 公祐 氏（一般社団法人 重要生活機器連携セキュリティ協議会（CCDS））

IoTセキュリティ評価のためのチェックリストを使った取り組み

輿石 隆 氏（JPCERT コーディネーションセンター（JPCERT/CC））

IoTセキュリティ時代のCSIRT

原子 拓 氏（日本CSIRT協議会（NCA）/株式会社ラック）

つまり・・・

IoT
守るためには
何学ぶ？

本日のセミナーでは、これを理解して頂きたい

（JNSAのIoTセキュリティWGのセミナー企画者としてのお願い）


IoTがサイバー攻撃の
ターゲットにされる理由
ご清聴ありがとうございました。

Thank you. Any Questions ?