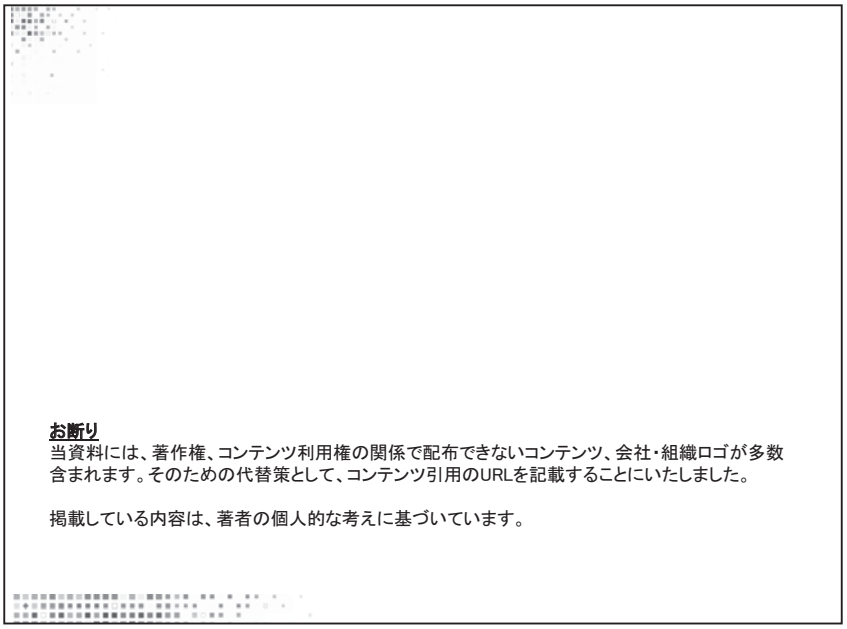
特別セミナー講演３

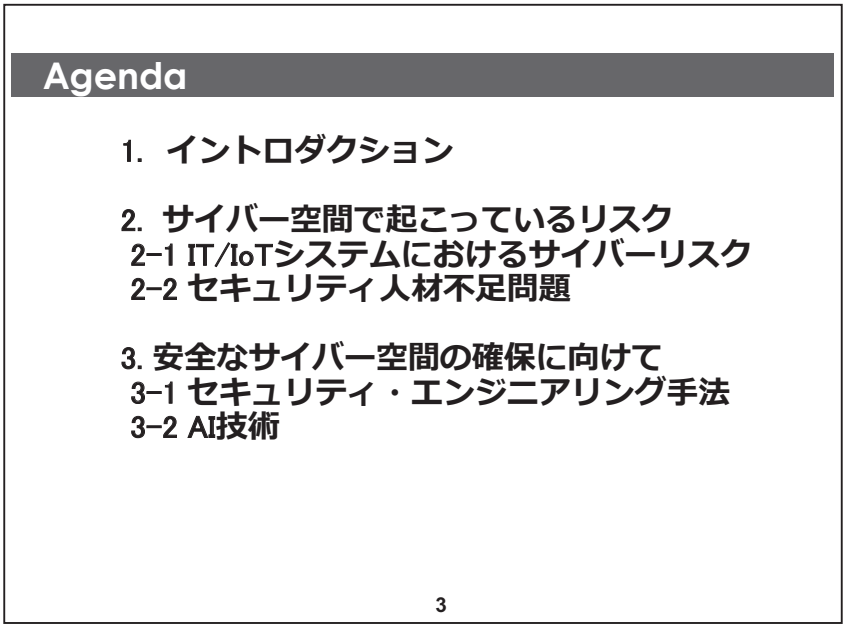
IoT のセキュリティと AI の考え方

セキュリティ・アーキテクト　**大西　克美**

IoTシステム対するサイバー攻撃の事例が増加し、火急な対応が必要な時代になっています。

このセッションでは、実際のお客様事例を元に、安全なIoTシステムの設計方法、AI技術の適用方法をご紹介します。





Agenda

1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

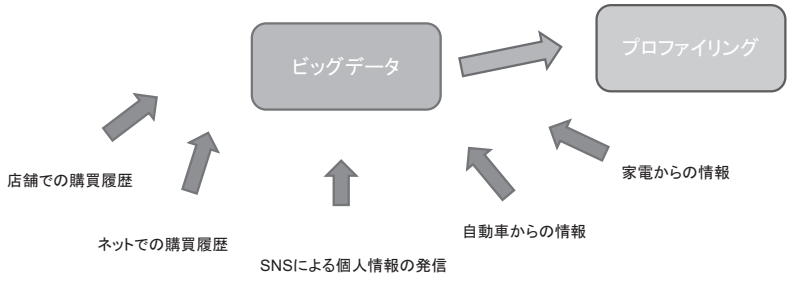
3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

4

なぜ、つなげたい/つながりたい??

企業目線：マーケティング分析、顧客囲い込み
消費者目線：特典、新しいユーザー体験

AI技術により
洞察/ 助言/ 提言/ 指示/ ・・・



5

AI技術とビッグデータがもたらす新しい価値

重要インフラ

重要サービスを支える機器群

つながる機器、システムは安全なのか？（セキュリティの観点）

私たちの個人情報は安全に管理されているのか？（プライバシーの観点）

6

Agenda

1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

7

Agenda

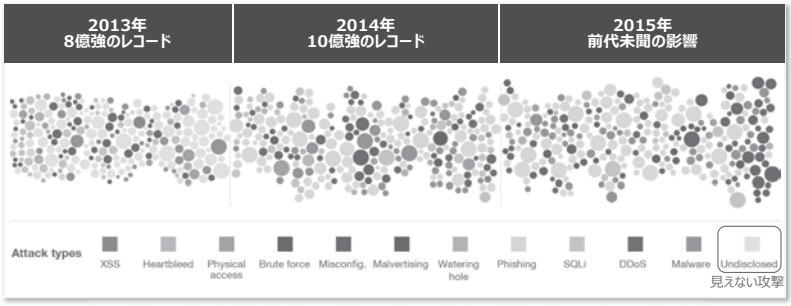
1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

8

2-1. IT/IoTシステムにおけるサイバーリスク



資料出典： IBM X-Force レポート

なぜ、「見えない攻撃」が多いのか？
 →監視するログが少なすぎる
 →攻撃を判断する要員の経験値が不十分である

現時点では、IOTデバイスはモニタリングされる準備ができていない

9

IoT機器がサイバー攻撃の対象に

セキュリティ対策が十分でないIoT機器に対して、カンファレンス、論文などでハッキング事例が数多く紹介されています

防犯カメラ/ 監視カメラ
自動車
医療機器

資料出典：
http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/
https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf
http://www.popsci.com/technology/article/2012-10/hacker-attackers-could-reverse-pacemakers-distance-delivering-deadly-shocks

10

IoT・制御システムもサイバー攻撃の対象に

重要インフラもターゲットになることで、サイバーリスクはITを超えた社会問題になりつつある
IoTシステムに対する攻撃、IoTを利用した攻撃も増加中

- 2013年　NYダム制御システムに対するイランのサイバー・ハッキング
- 2015年　ウクライナ西部でサイバー攻撃による大規模停電(6時間、70万人に影響)
- 2015年　走行中のクルマ乗っ取りに成功（140万台のリコール）
- 2016年　監視カメラを経由した覗き見サイト公開（http://www.insecam.org/）
- 2016年　Miraiマルウェア：IoTデバイスを踏み台にした世界最大規模（数千万アドレス）のDDoS攻撃
- 2016年　経済産業省「今後のサイバーセキュリティ政策」を発表
  - 「国民の生命や社会システム全体に甚大な被害が発生する可能性があり、国家として対応を強化すべき課題」と認識
- 2017年　日本の大手製造業でランサムウェアに感染、甚大な被害をもたらす

パンドラの箱を空けたら、SF映画の世界に迷い込んでしまった！

11

参考）IoTシステムに対する攻撃手法

- Plain old software bugs (buffer overflows, SQLi, XSS, …)
- No transmission encryption (e.g., plain HTTP)
- Weak encryption (home brewed?)
- Key storage on device (symmetric encryption)
- Simple username/password
- Backdoor accounts
- Too many exposed services / lack of hardening
- No firmware integrity checks

=> ITでは有名な攻撃／脆弱性の利用であり、特段の違いがあるわけではない

安全な製品を作る手法を確立する

ITで培った知見・技術をIoTに適用する

12

Miari IoTボットネット

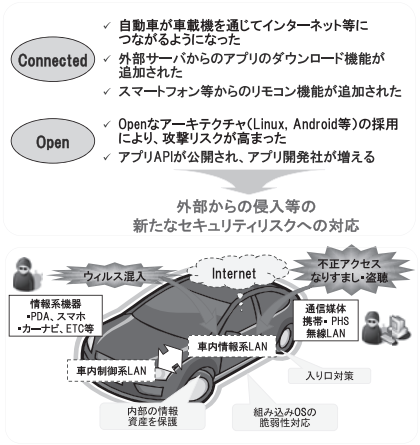
セキュリティ対策が十分でないIoT機器を利用したサイバー攻撃が話題になりました

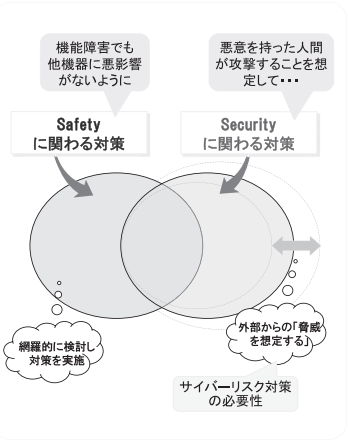
資料引用：IBM Security Intelligence
https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins /

13

何故IoTデバイスが狙われる？（自動車の例）

・自動車が何かとつながることで、外部からの脅威が発生します
・その脅威は、Safety対策でカバーできない想定外の攻撃を仕掛けてきます





14

自動車に対するサイバー攻撃発生！

ホワイトハッカーが走行中の自動車に対するハッキングデモを実施。
日本でも大きな話題となり、経産省などのガイドなどでも引用される有名なハッキング事例となっています

米国におけるハッキング事例

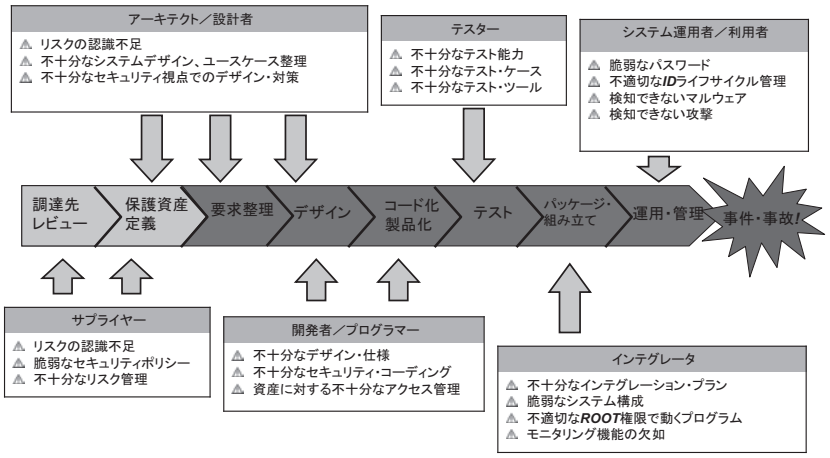
考察：ロボット、制御機器、IoTデバイスなどを遠隔操作して、人類を攻撃できないか？
→ 遠隔操作で走行に影響を与えるハッキングには成功済み
→ 製造業に根付いている"Fail Safe"という概念の限界

資料引用
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

15

セキュリティ事件・事故が発生する理由

各専門分野におけるセキュリティ視点の欠落



16

2-2. セキュリティ人材不足問題

セキュリティ対策が進まない理由の一つに、セキュリティの人材不足の問題があります。
2020年では、約20万人のセキュリティ技術者が不足していると報告されています

人材不足の統計資料

資料出典：**経産省「IT人材の需給に関する推計」**
http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

17

Agenda

1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

18

セキュリティの設計、実装は難しいでしょう？

→ 匠の技・経験にだけ頼るのは危険です

セキュリティだけでも大変なのに、プライバシー対策なんて・・・

製造社と利用者の責任範囲は？

周囲にセキュリティを知っている人がいないのですが・・・

→ セキュリティもシステム・エンジニアリングしましょう

19

3-1 セキュリティ・エンジニアリング手法

計画、設計段階からセキュリティ対策、プライバシー対策の実施が必要です。
それを実践するためには、過去の経験だけではなく、「エンジニアリング」を実施することです。

セキュリティ対策の範囲、高度はリスクの大きさ、ビジネス用途で決定されます。
例えば、家庭でペットを眺めるためのWebカメラと空港などのテロ対策向けの防犯カメラでは、サイバー攻撃に対するセキュリティレベルが違うことになります。

プライバシーに関しても、冒頭に紹介したように、個人情報を積極的に発信する世代が台頭しています。よって、昔ながらの一律的な規制ではなく、用途や時代のニーズにマッチした設計が必要になっています。

「Secure by Design」／「Privacy by Design」を実践するにはエンジニアリングが必要
- →想定される脅威を網羅的に整理する手法
- →整理したリスクを評価し、対策の必要性を検討する手法
- →体系化したセキュリティテストの手順、方法
- →PDCAサイクルを適用した脆弱性管理

20

各局面で実施すべきセキュリティ対策

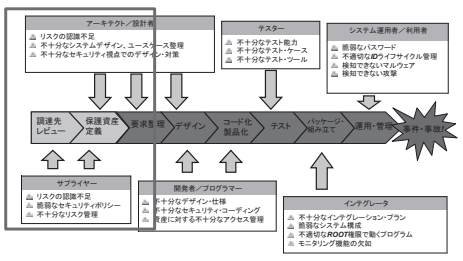
1.計画局面

・守るべき資産の定義・確認
- 製品の商品性、安全性
- 各社のブランド
- 製品に含まれる個人情報　など

・利用用途に応じたリスクの定義
- サービス停止
- 情報漏えい　など

・製品に整備すべきセキュリティ技術の洗い出し
- 侵入検知システム
- フィリタリング技術
- データ暗号化・匿名化　など

・サプライヤーへの調達要求
- サイバー観点からの脆弱性に対する保証範囲
- 責任範囲の明確化（ソフトウェア脆弱性＝欠陥とは言えないケース）



21

各局面で実施すべきセキュリティ対策

2.設計・開発・製造局面

・セキュリティ設計

　セキュリティ要件の整理と設計

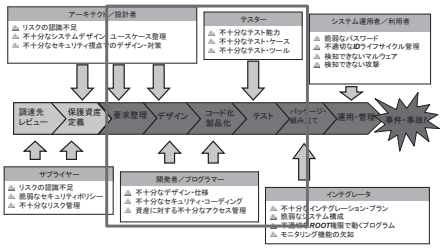
　プライバシー要件の整理と設計

・セキュリティ・テスト

　コード検証

　仕様確認テスト

　攻撃者目線でのハッキングテスト



　エンドツーエンドでのセキュリティテスト（特に、ITシステムとの連携時）　など

　　例）監視カメラで録画された自宅映像をスマホのアプリケーションを利用して閲覧する

　　　監視カメラの録画データが改ざんされる？

　　　アプリケーションを提供するサーバーが攻撃を受けてサービスが停止する？

　　　スマホがハッキングされて、第三者に自宅映像を盗聴される？　など

各局面で実施すべきセキュリティ対策

3.利用・運用局面

・セキュリティ知識を有しない利用者対応

　初期値：利便性＜セキュリティ

　遠隔保守の可否

・脆弱性対応

　脆弱性情報の入手

　リスクの評価

　社外に対する公表

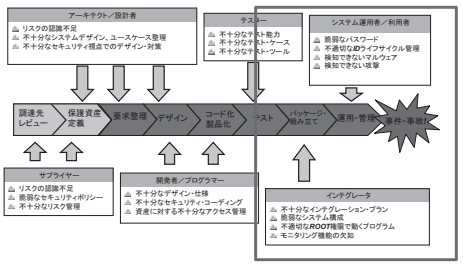
　修正ソフトウェアの配布・適用

　品質不具合対応（リコール？）

・保証範囲

　ソフトウェアに対する保証期間

　有料vs無償の分岐点



3-2 AI（Artificial Intelligence）技術

サイバー攻撃に対するAI技術の適用事例を、IBMの事例をもとに紹介します

アナリストを支援：

外部データの迅速な使用

パワフルな洞察の入手

新しい傾向とパターンの発見

脅威の正確な分析

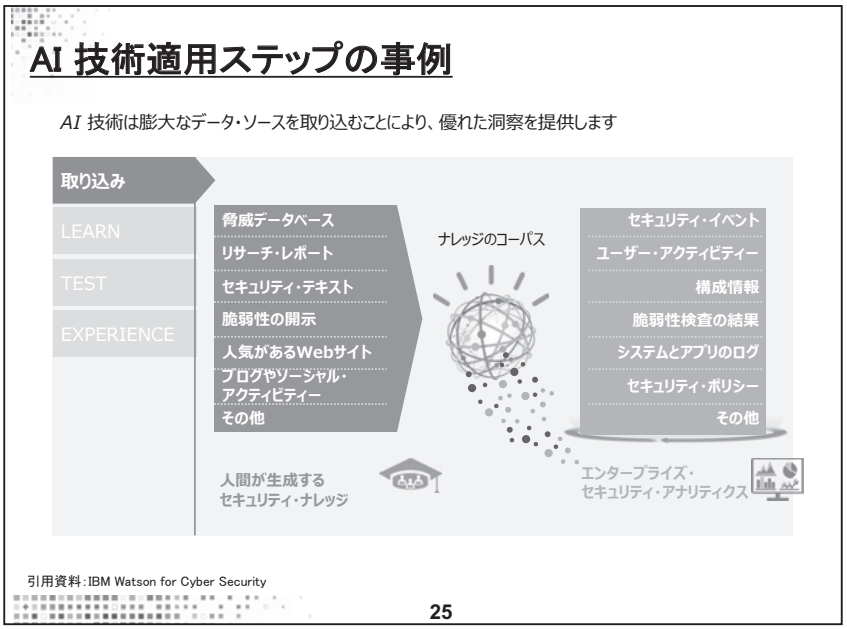
時間と資源の節約

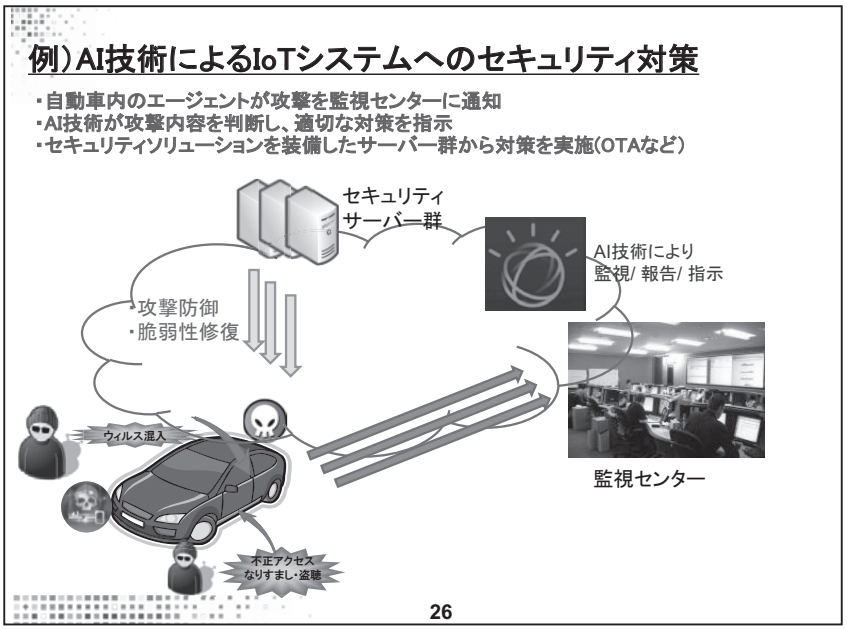
セキュリティ・アナリストの経験不足を補填

セキュリティ技術者の学習時間を節約

　→「見えない攻撃」の解決の糸口

引用資料：IBM Watson for Cyber Security





■当資料のコンテンツ引用URL

資料10（出典）

・http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/
・https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf
・http://www.popsci.com/technology/article/2012-10/hacker-attackers-could-reverse-pacemakers-distance-delivering-deadly-shocks

資料11

・http://www.insecam.org/

資料13（引用：「IBM Security Intelligence」）

・https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/

資料15（引用）

・http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

資料17（出典：経産省「IT人材の需要に関する推計」）

・http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html