UNISYS

IoT時代に備えるサイバーセキュリティ

企業におけるサイバーセキュリティの戦略と対策

日本ユニシス株式会社
アウトソーシング企画統括部セキュリティ技術部
遠藤　英幸

BITS 2015
NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

本日の内容

1. はじめに
2. セキュリティ意識の変革が必要
3. IoT
4. IoTへのサイバーアタック
5. 変革が必要な背景
6. どう変わればいいのか
7. まとめ

自己紹介

遠藤　英幸

日本ユニシス株式会社

アウトソーシング企画統括部セキュリティ技術部

UCSIRT POC

1987年日本ユニシス（株）入社

過去　　オブジェクト指向言語および実行環境の開発

アウトソーシング基盤構築などを担当

現在　　システム開発におけるセキュリティ品質統制

脆弱性情報ハンドリング、セキュリティ事故対応

セキュリティコンサルティング等のセキュリティサービス全般

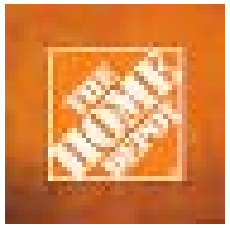
保有資格：　CISSP

社外活動：　情報処理技術者試験委員

1. はじめに

- 2013年から2014年にかけて、クレジットカード情報を含む、大量の個人情報事件が頻発

7000万件！



6000万件！

  - セキュリティ対策をしていたにもかかわらず

- 従来のセキュリティ対策では、なぜいけないのか

Change!

2. セキュリティ意識の変革が必要

- Amit Yoran氏（RSA社長）

RSA Conference | Where the world talks security

“2014年はセキュリティベンダの敗北の年だった”

“セキュリティに対する考え方を変えなければならない”

Change!

- Keren Elazari氏 (サイバーセキュリティアナリスト)

CODE BLUE

“サイバースペースにはWWWだけがあるのではない”

“攻撃者は創造的で革新的で協調的である” “私たちもそうであるべき”

Change!

2. セキュリティ意識の変革が必要

- Christopher Young氏 (Intel Security Group GM)

RSA Conference | Where the world talks security

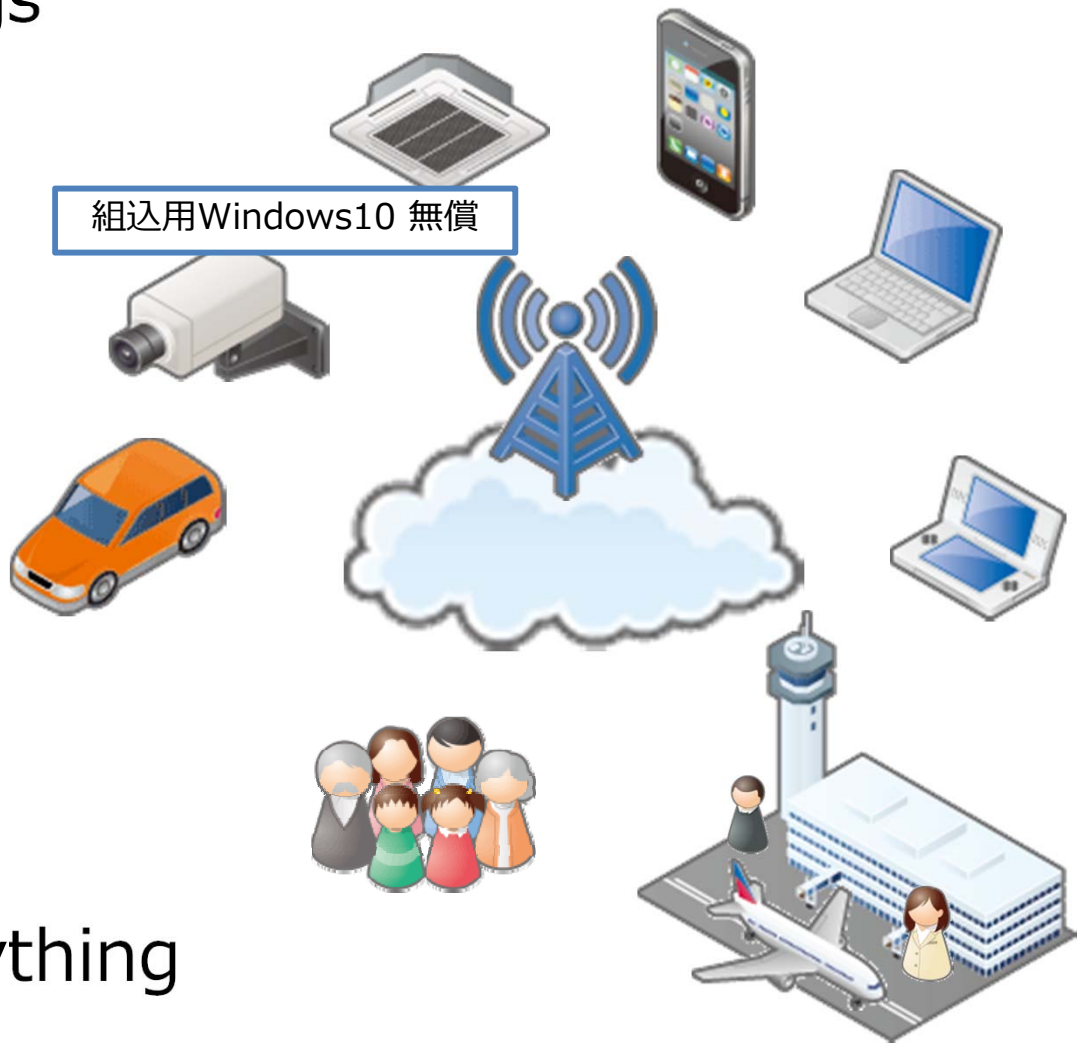
“攻めのセキュリティへ”

Change!

- 自社がどのような脅威に晒されているのかを知る
- 攻撃を分析して対策を立てる

3. IoT

- IoT：Internet of Things
  - モノのインターネット
    - PC
    - スマホ
    - 自動車
    - テレビ
    - コピー機
    - 防犯カメラ
    - スマートメーター
    - ドローン
- IoE：Internet of Everything
  - すべてのインターネット



2020年には500億のモノが接続されるとの予想！

4. IoTへのサイバーアタック

- NAS：Network Area Storage
  - telnetでアクセス可能なNAS
- ホームルーター
  - UPnPの設定ミス
- 自動車
  - 制御装置への侵入
- 冷蔵庫、テレビ
  - スパムメールの送信
- ペースメーカー
  - 制御装置への侵入
- ドローン
  - 制御装置への侵入

電子タバコも例外ではない

5. 変革が必要な背景　- 1

- 現在のセキュリティソリューションでは、完全に防ぐことはできない攻撃が増加
  - ウイルス対策ソフトの回避
  - IPS／IDSの回避
  - 正当なアカウントの使用
  - IoTの闇の部分

サイバーアタックは分業化され、市場を形成
- マルウェア開発
- ボットネットレンタル
- 実行犯

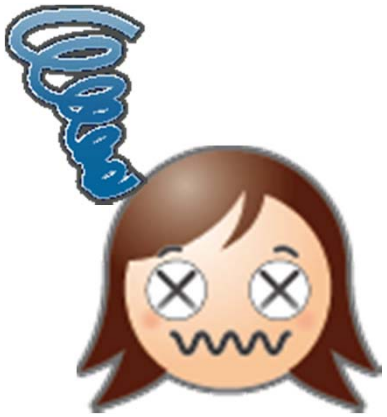
5. 変革が必要な背景　- 2

- ウイルス対策ソフトの回避
  - 堅牢化
    - ファイルを削除しても再生成
    - プロセスを切っても再生成
    - システムプロセスへの寄生
  - パターンマッチングの回避
    - 暗号化や難読化が高度化
    - 99%のゴミコードと、1%の実コード
    - 復号鍵の隠蔽
  - サンドボックスの検知手法の高度化
    - サンドボックス内での動作変更による検知回避

5. 変革が必要な背景　- 3

- IPS／IDSの回避
  - 攻撃パターンの多様化
    - シグネチャの解析による検知回避

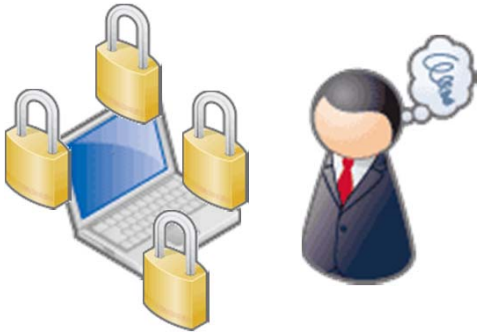
  - 緩慢な攻撃
    - 単位時間当たりの閾値による検知回避
  - 攻撃の分散化
    - 攻撃元IPアドレスが特定できない



5. 変革が必要な背景　- 4

- 正当なアカウントの使用
  - ID／パスワードの事前窃取
    - 外部サイトで流出した情報の使用
    - マルウェア侵入初期における盗聴活動
    - フィッシング、ファーミングによる事前窃取

  - 極めて困難な不正ログインの検知
    - 最小限のログイン失敗回数
  - 利便性の呪縛
    - 敬遠される多要素認証、多段階認証の採用



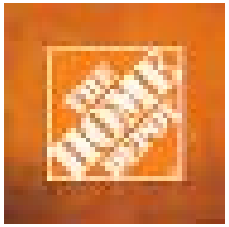
5. 変革が必要な背景　- 5

- IoTの闇の部分(1)
  - モノ（設計者）と利用者の技術力のギャップ
    - どんな情報を保持しているのか知らない
    - 攻撃を受けたり踏み台になったときの影響が想像できない

  - 困難な脆弱性の完全除去
    - 見落とし
    - 新しい攻撃方法の発見

5. 変革が必要な背景　- 6

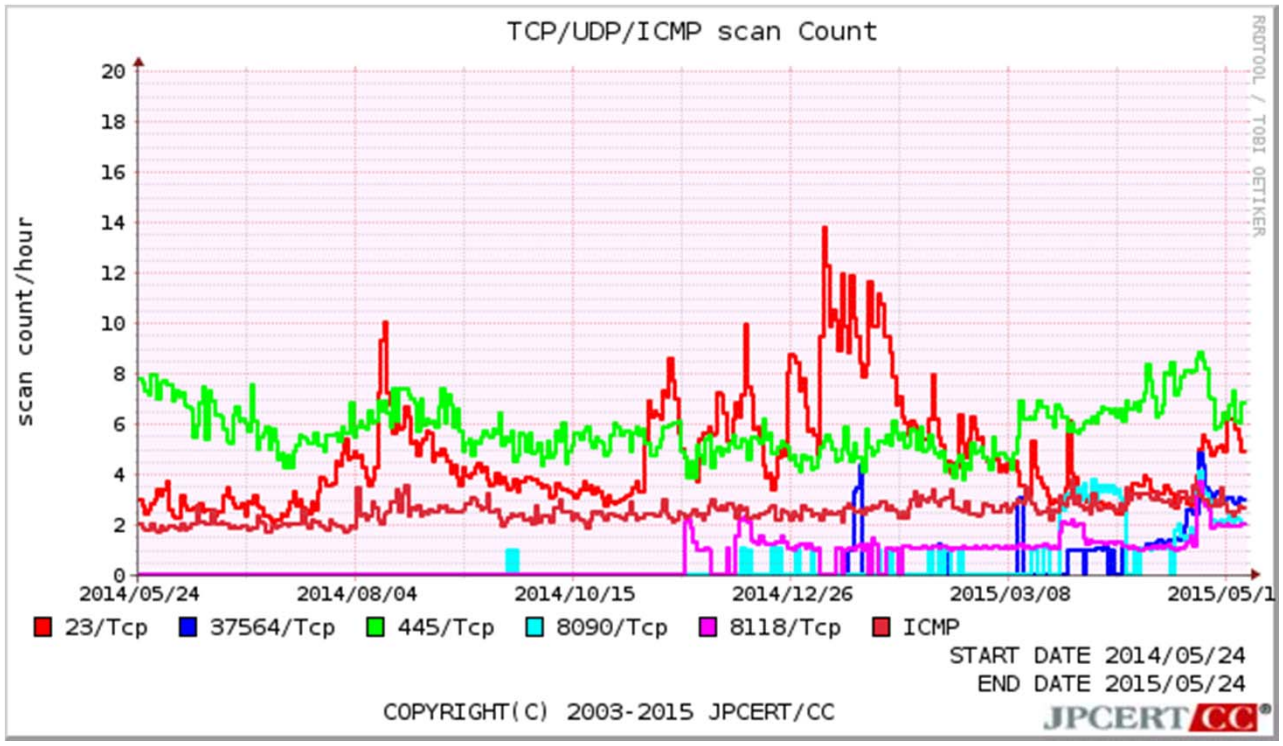
- IoTの闇の部分(2)
  - 様々なデバイスの接続
    - 対策レベルの低いデバイスからの侵入
    - 他の接続されているモノへの侵入の踏み台



  - 困難な修正プログラム適用
    - 大量のデバイス
    - 多様な接続形態
    - 必要最小限のリソース

5. 変革が必要な背景　- 7

- IoTの闇の部分(3)
  - モノがモノを攻撃／負の連鎖
    - 攻撃者がWebカメラを攻撃 (マルウェア)
    - WebカメラがNASを攻撃 (Port 23:telnet)
    - NASがNASを攻撃 (Port 8080:http)



6. どう変わればいいのか -1

- セキュリティーソリューションを過信しない
  - セキュリティソリューションは、攻撃者によって攻略されるもの
  - もちろん、これまでの対策は必要！

攻撃は今もされている

いつかは被害を受ける

Amit Yoran氏（RSA社長）

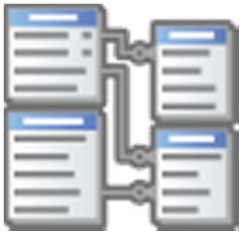
RSA Conference | Where the world talks security

“2014年はセキュリティベンダの敗北の年だった”
“セキュリティに対する考え方を変えなければならない”

Change!

6. どう変わればいいのか -2

- 積極的な防御
  - SIEM (Security Information and Event Management) の活用
    - さまざまなログの積極的分析
    - 不足しているログの洗い出し



  - SOC (Security Operation Center) による攻撃の分析と対策立案
    - どんな攻撃を受けているのか
    - どんな対策が有効か

Christopher Young氏 (Intel Security Group GM)

RSAConference | Where the world talks security

“攻めのセキュリティへ”

Change!

6. どう変わればいいのか -3

- 事故に備える体制の整備
  - CSIRT (Computer Security Insident Response Team) によるダメージコントロール
    - 組織化／人材育成
    - 脆弱性情報の収集
  - CSIRT連携
    - モノの増加に伴い、単独での対応がより困難に
    - 日本シーサート協議会の加盟数の増加
      - 2010年　18チーム
      - 2014年　45チーム
      - 2015年　85チーム

Keren Elazari氏 (サイバーセキュリティアナリスト)

CODE BLUE

“攻撃者は創造的で革新的で協調的である” “私たちもそうであるべき”

Change!

7. まとめ

- これまでの対策は必要

ウイルス対策

監視

パッチ適用

- IoTによるサイバーセキュリティ対策への影響
  - システムの構成要素にさまざまなモノが追加
    - どこが弱いのか
- 事前対策／事後対策の強化
  - 脆弱性情報の収集
  - 積極的防御
  - 被害の極小化と復旧期間の短縮

Change!

UNISYS

Foresight in sight

ご清聴ありがとうございました

BITS 2015
NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM