パネル討論
「IoTで新たに出現した セキュリティリスクと対策を語る」

2017年2月13日
(株)IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp/

1

（1）自己紹介

福岡出身：　香椎中学➔福岡高校➔東京大学
1970年　東芝入社
社内計算機利用環境企画・構築・活用指導・支援
情報セキュリティ研究開発企画・推進、事業支援
2007年　（株）IT企画設立
事業支援活動（3社の顧問・相談役）
大学教育活動（2校の情報セキュリティ講師）
研究開発活動（1機関の研究員）
研究対象分野：
サイバーセキュリティ、IoT、FinTech

2

（2）IoTセキュリティ事件と攻撃サービス/ツールの紹介

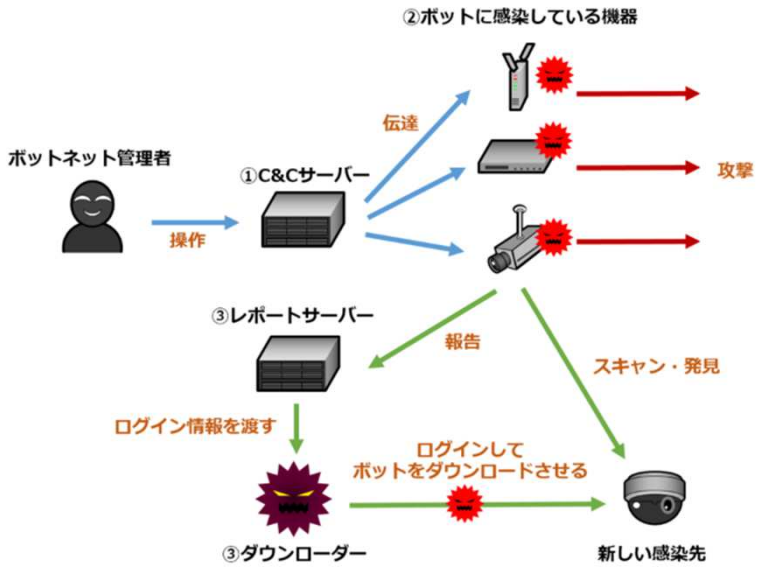
KrebsOnSecurityサイト攻撃（2016年9月）

＊IoTからのDDOS攻撃により、一時閉鎖へ

＊vDOS関係者・利用者からの反撃か
vDOS運営容疑で2人の青年（18歳）を
イスラエル当局が逮捕

＊IoT向けマルウェアMiraiが使用されていた模様

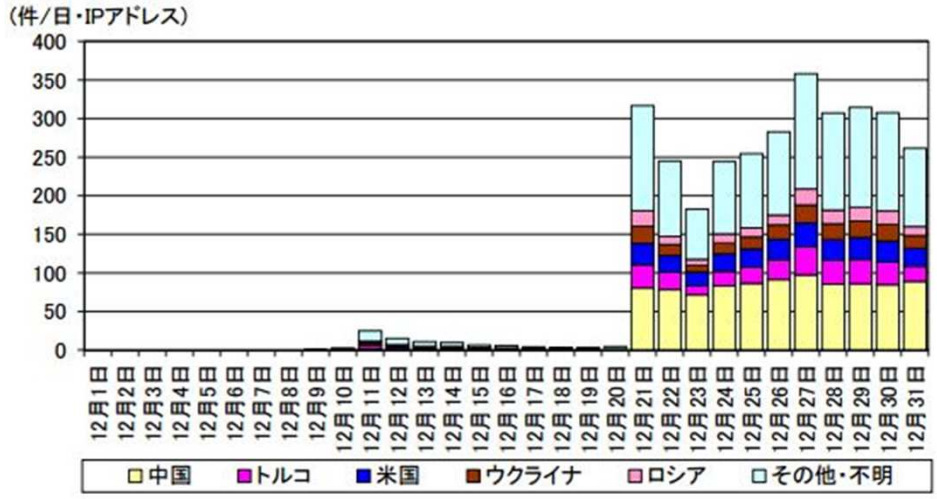
IoT向けマルウェアMiraiの動き



出典：http://www.atmarkit.co.jp/ait/articles/1611/08/news028.html

4

（3）日本でもIoT機器を対象としたMiraiボットの亜種等からの感染活動とみられるアクセスが急増



宛先ポート23231/TCPに対するアクセス件数（発信元国・地域別推移）

警察庁：インターネット観測結果等（平成28年度12月期）

5

（4）IoTシステム特有のセキュリティ課題

IoT機器本体そのものの課題

＊インターネット接続想定せず：不十分なセキュリティ機能

＊処理能力が不足：十分なセキュリティ機能搭載不可

＊ライフサイクルが長い：セキュリティ対策の危殆化

機器設置環境に起因する課題

＊物理的に保護されていない環境に設置：
　盗難や破壊・改ざん、機器・電源・通信故障のリスク大

システム構築・運用・管理上の課題

＊セキュリティ課題を十分認識していない事業者・利用者

＊影響範囲が広く、影響の度合いが大きい

6

（5）IoT機器およびシステムの開発・構築・運用者の社会的責任

- ボット化されたIoT機器、IoTシステム構築事業者、IoTシステム運用・サービス事業者の社会的責任は重大！
- 不十分なセキュリティ対策でインターネットへ接続するということは、犯罪者（攻撃者）の行為に加担・助長する行為！
- 道義的責任はもちろんだが、悪意があれば刑事責任を、悪意が無くとも損害賠償責任は問われる時代に！

7

（6）IoTシステムのセキュリティ対策

①IoTシステムモデルの明確化
- **リスク分析・対策選定、Security/Privacy by Design**
- **IoT機器/IoTシステムの役割分担・多層防御**

②認証・秘匿機能は不可欠
- **IoT機器認証、データ認証・保護**
- **軽量認証・秘匿技術**

③Attack Surfaceの最小化
- **弱小デバイスの隠ぺい**
- **既存インターネットセキュリティ技術の活用**

④IoT機器の通信特性を利用した対策
- **通信相手の限定・なりすまし対策（パケットフィルタリング/uRPF)**
- **外部からの制御ニーズに応じた対策**

⑤システム長寿命への対応
- **安全・確実なリモート更新/リモート監査**

⑥監視・管理責任の明確化
- **階層的特定・追跡性**

8

終

ご清聴、ありがとうございました。

9