「Ｉ・ＴＯＰ横浜」 キックオフイベント

「IoT Security READY!! IoT機器・IoTサービスのセキュリティ強化と検証」

「スマートホームにおける脆弱性の実態」
～ハッキングデモを交えて～

2017年6月20日

（一社）重要生活機器連携セキュリティ協議会
Connected Consumer Device Security Council （CCDS）

代表理事　荻野　司　博士（工学）

CCDSのご紹介

- 名称：一般社団法人 重要生活機器連携セキュリティ協議会
  - 英名：Connected Consumer Device Security council (CCDS)
- 設立：2014年10月6日
- 会長：徳田英幸（慶應大学 教授、内閣府セキュリティ補佐官）
- 代表理事：荻野 司（京都大学 特任教授）
- 理事：後藤厚宏（情報セキュリティ大学院大学 教授、SIP：PD）
  長谷川勝敏（イーソル㈱ 代表取締役社長）
  服部博行（株式会社ヴィッツ 代表取締役社長）

- 会員数：144（正会員以上：44、一般会員：73、学術系：16、協賛:11）

- 主な事業：
  1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
  2. 生活機器の安全と安心を両立するセキュリティ技術の開発
  3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
  4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

CCDS Members

- Total number of members: 144 (as of April, 2017)
  - Executive Members: 27

    HITACHI Inspire the Next, JVCKENWOOD creates excitement & peace of mind, OKI, OMRON, RICOH
  - Regular Members: 17

    AISIN comCruise, DNP, Deloitte. デロイトトーマツ, FUJITSU, muRata, NTT Communications Transform. Transcend., Paloma, Panasonic
  - General members: 73,

    ALPINE Driving Mobile Media Innovation, ALPS, Calsonic Kansei Driven by Inspiration and Innovation, clarion, FURUKAWA ELECTRIC, gemalto, INTEC TIS INTEC Group, I-O DATA, KASPERSKY, KOKUYO, KDDI, KDDI Research, NEC, NTT AT, Pioneer, SONY, THALES, TOSHIBA, TEC, TREND MICRO, UL Underwriters Laboratories
  - Academic members: 16
    - Hiroshima City Univ., Keio Univ., Nagoya Univ., Univ. of the Ryukyus, Yokohama Nat'l Univ., Inst. of Information Security, Japan Adv. Inst. of Science and Technology, Nat'l Inst. of Adv. Industrial Science and Technoloty (AIST), Nat'l Inst. of Information and Communications Technology (NICT), Nat'l Inst. of Informatics, etc.
  - Liaison members: 11
    - Computer Software Assoc. of Japan, Internet Assoc. of Japan , Japan Network Security Assoc., Japan Cloud Security Alliance, etc.

増え続けるIoTのセキュリティ脅威

生活を脅かすサイバー攻撃が増加を続け
攻撃の手口や標的は多様化

Miraiボットネットによる大規模なDDoS攻撃

世界中で感染は100万台以上

IoT機器へ拡大
影響範囲拡大

台湾製ホームルータの脆弱性による個人情報の漏えい

米FTCとASUSの間で訴訟に発展

メーカー責任

商業衛星をマルウェアでハッキング

国家間の懸案事項に

テロへの利用を想起

参考☞「付録①」

あたり前になっているハッキング

DEFCON:IoT Village：コンテスト事例

- ハッキングコンテスト
  - コンシューマー製品のハッキング大会（ワークショップ）
    - 家庭用ルータ（ASUS, Zyxel 社）
    - 防犯カメラ（Netgear, Forscam 社）
    - 赤ちゃんモニター（Samsung 社）
    - Wi-Fi対応血圧モニター（Blipcare 社）
    - Wi-Fi対応体重計（Fitbit Araia 社）
    - タイムカード記録装置（ZK Software 社）
    - NAS（Apple社タイムカプセル）
    - ガレージ開閉装置（Chamberlain 社）
    - 電気錠（LockState, Hysoon 社）
    - 冷蔵庫（Samsung 社）
    - おもちゃ（HappyCow社
      カメラ付き戦車模型（Wi-Fi接続））
    - 2016年はドローンが追加

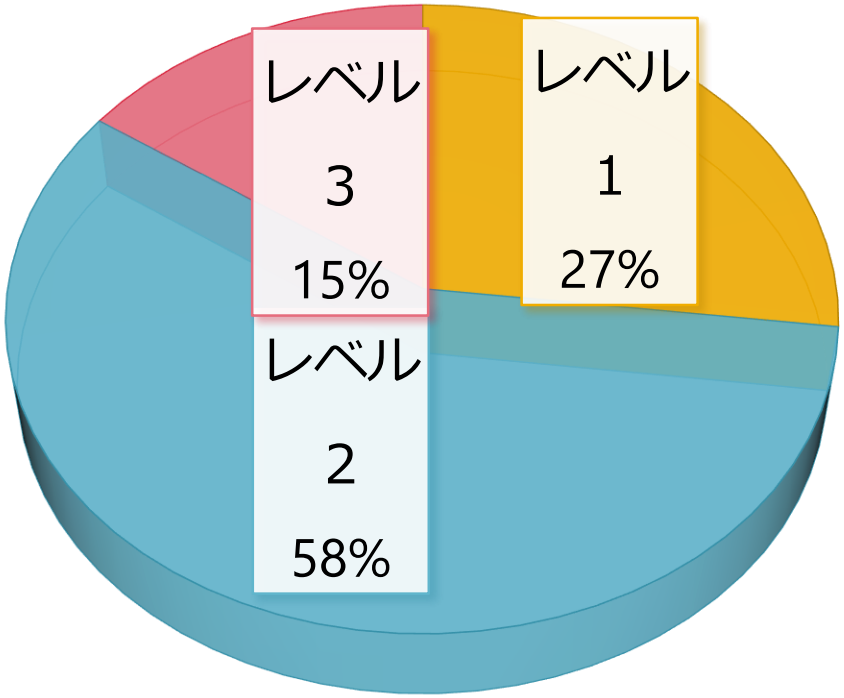
OSSでどこまでできるの？

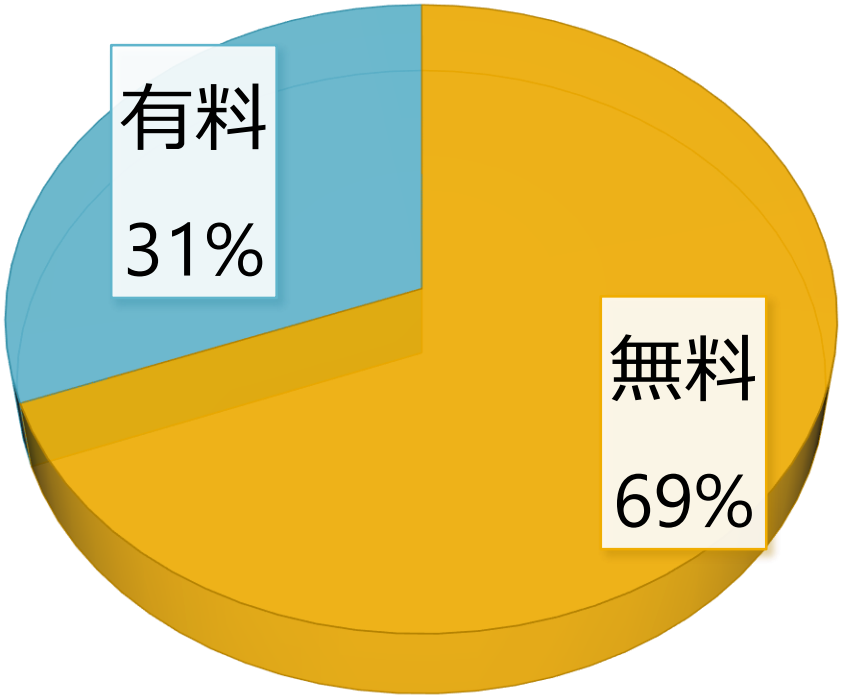
- 調査内容
  - 脆弱性の現状
  - 脆弱性検証手段
- 調査手段
  - 一般的な手段で入手可能な情報を元にして調査
  - インターネット上の情報を基本として調査を実施
- 調査対象
  - 21種類の脆弱性に関して調査
  - 26種類の攻撃ツールを調査
- 調査結果
  - 攻撃方法の類型化
  - 攻撃ツールの難易度判定

脆弱性診断に利用できるOSSの種類

場所	• リモートからの攻撃 • ローカルでの攻撃 • Proxyを利用しての攻撃
攻撃ツールの種類	• DoS攻撃 • SQLインジェクション • XSS（クロスサイトスクリプティング） • Proxy • Password attack
ライセンス形態	□無償　□有償
攻撃ツールの難易度	• 難易度１（GUIなどで利用可能。特別な知識などは不必要 • 難易度２（shellスクリプトなどと組み合わせて検証する。若干の知識が必要） • 難易度３（Ruby,python,java,Cなどのプログラムと組み合わせて検証。高度な知識が必要）

OSSのライセンス形態と難易度



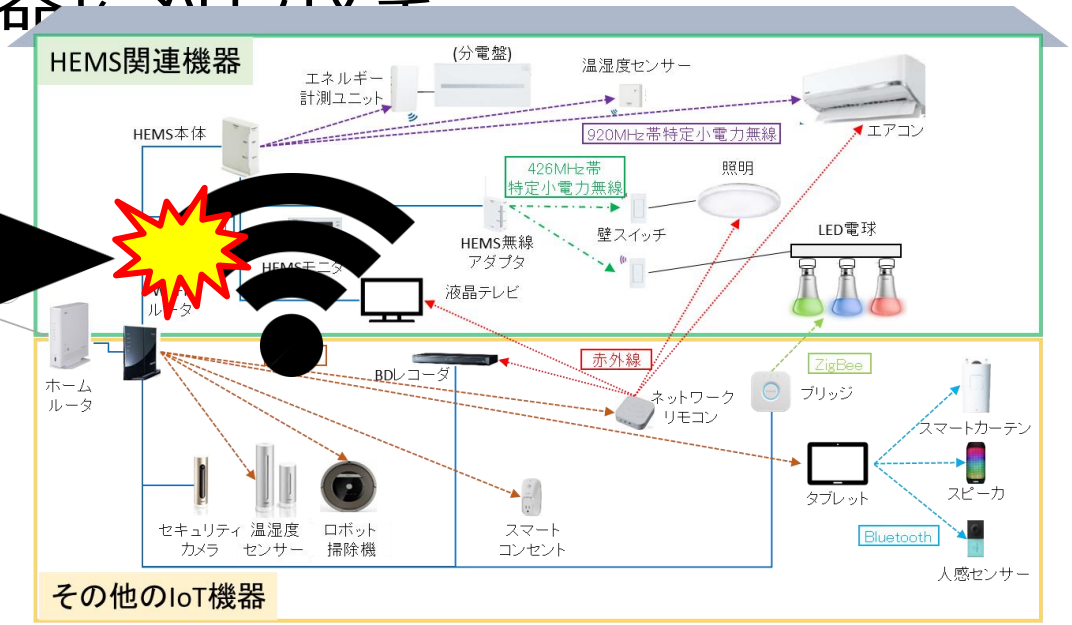


安価で比較的高度な知識が無くても利用可能なことが判明

悪意の想定

- シチュエーション
  - 近隣の住人がWiFiをハックし、宅内ネットワークへの侵入するところから開始
  - 宅内ネットワークへの不正侵入に成功し、接続されている機器に対し攻撃

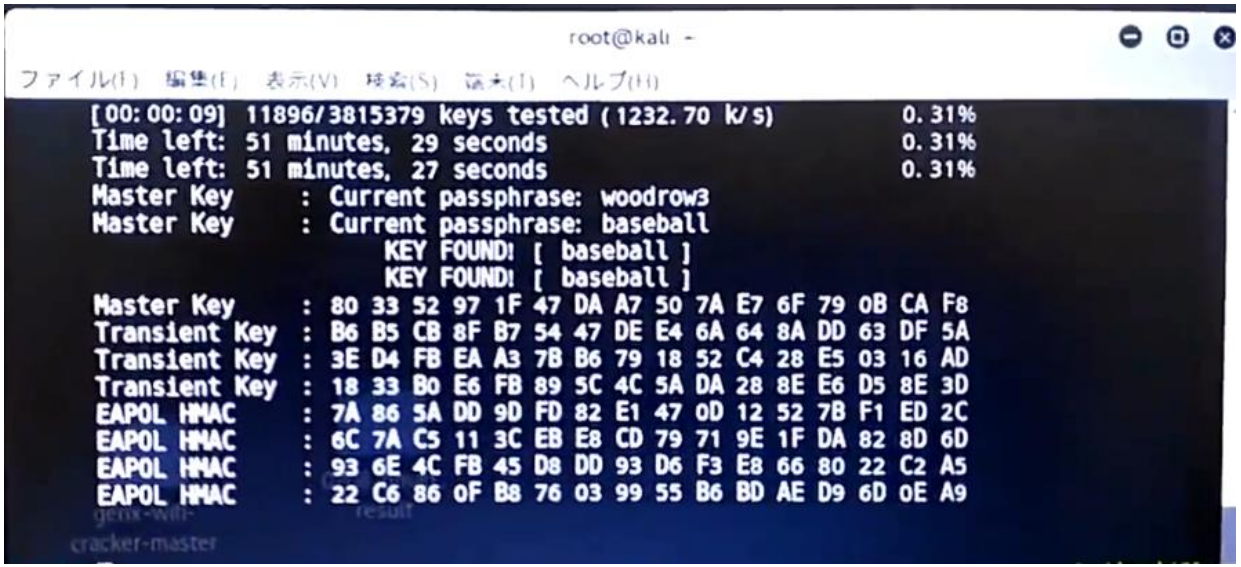
悪意を持った近隣に住人



検証

① WiFiへの不正接続

- ツール：aircrack

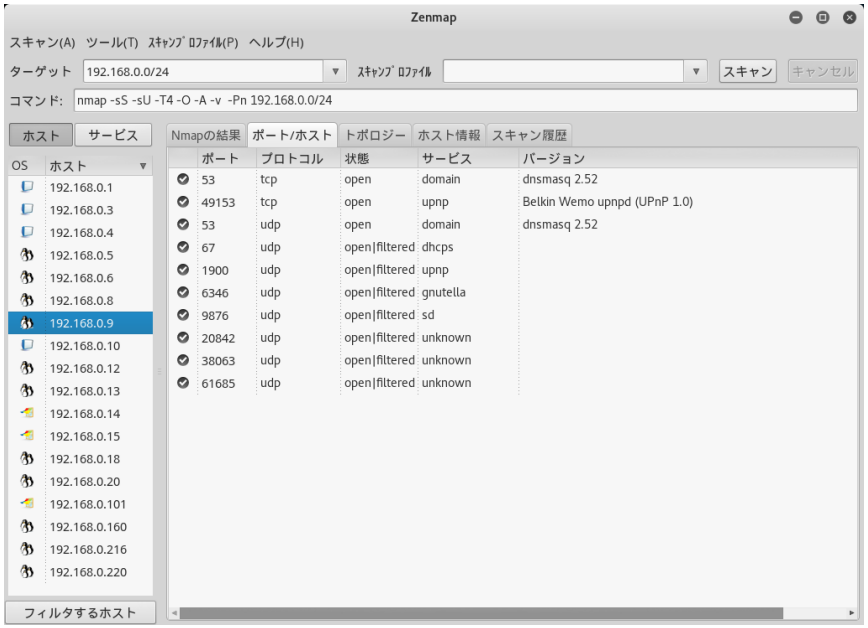


- ✓ WEP・WPA2の両方で解析に成功
- ✓ WPA2は辞書攻撃でパスフレーズを解析

検証

② 宅内のネットワークに侵入し接続されている機器をスキャン

- ツール：Zenmap



- ✓ 空ポートだけでなくOSや想定機器を表示

検証

③ 発見された機器への不正ログイン
(パスワード解析：ブルートフォース)

- ツール：Hydra

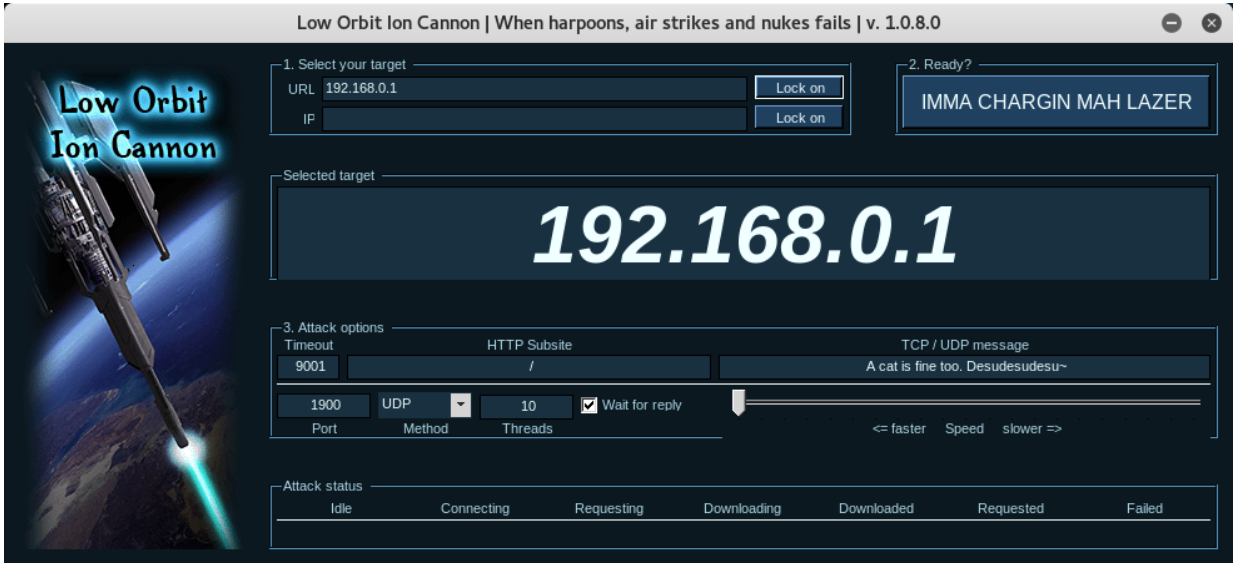
```
root# hydra -V  -t 1 -l "root"  -P ~/comment/hydra_pass_ap/fasttrack.txt 192.168.0.216 http-get /get/top.cgi
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illega
l purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-02-09 18:15:53
[DATA] max 1 task per 1 server, overall 64 tasks, 187 login tries (l:1/p:187), ~2 tries per task
[DATA] attacking service http-get on port 80
[ATTEMPT] target 192.168.0.216 - login "root" - pass "ccds" - 1 of 187 [child 0]
[ATTEMPT] target 192.168.0.216 - login "root" - pass "P@55w0rd" - 2 of 187 [child 0]
[ATTEMPT] target 192.168.0.216 - login "root" - pass "P@ssw0rd!" - 3 of 187 [child 0]
[ATTEMPT] target 192.168.0.216 - login "root" - pass "0101" - 4 of 187 [child 0]
[80][http-get] host: 192.168.0.216   login: root   password: 0101
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-02-09 18:16:00
```

- ✓ 空ポートに対しログイン情報(ID/Pass)を総当たりして解析

検証

④ ログインできない機器にDoS攻撃

- ツール：LOIC・ostinato・Gatling



- ✓ IoT機器の動作を妨害

⑤ 脆弱性スキャン

- ツール：OWASP ZAP・OpenVAS

(商用版：Nessas)

- ✓ 既知の脆弱性を発見

検証ツールによる実証（動画）

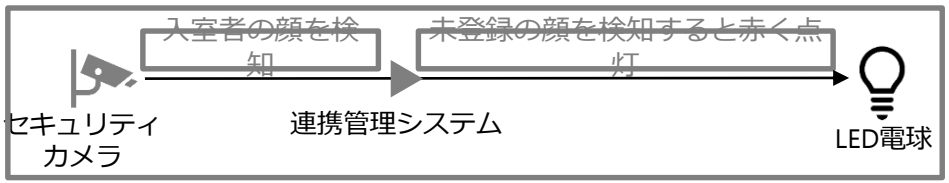
- DoS攻撃によるセキュリティカメラ(侵入検知)と照明との連携機能阻害の例
- ・実機テストベッドに設置した機器に対し検証ツールで攻撃し、連携動作への影響を検証
  ・仮想テストベッドにて同じ状況をシミュレーションし結果を比較

■実機テストベッドでの検証結果

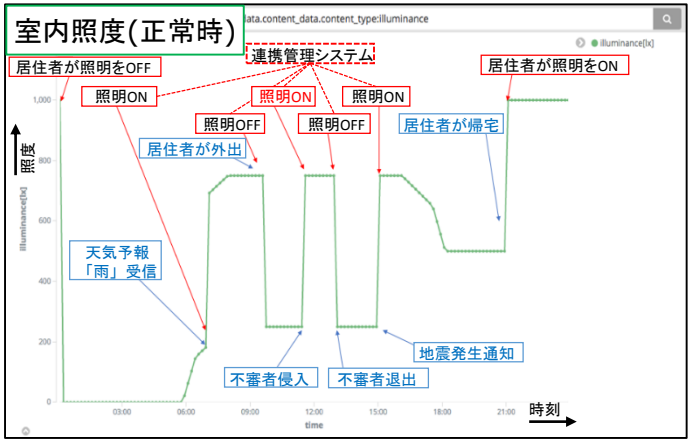
DoS攻撃を使って不審者検知を妨害

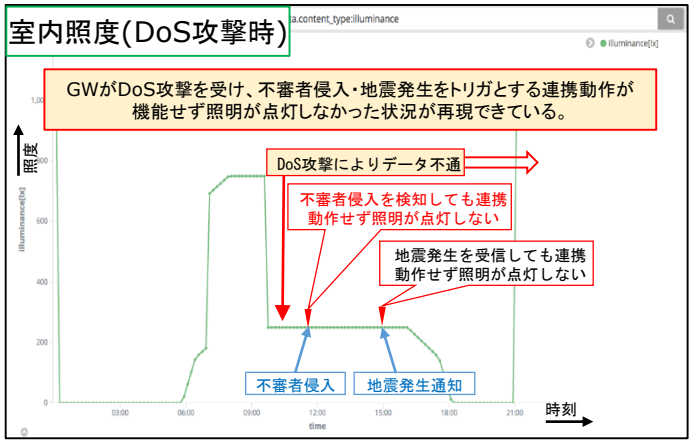
ツール提供：CCDS

連携動作設定



■仮想テストベッドでの検証結果





まとめ

- 1つのツールで検証するのではなく、複数のツールを組合わせて検証することが重要
- ツールの組合わせにはノウハウが必要

告知：脆弱性トライアルプログラム

対象：IoT機器、（不随するシステムは応相談）
期間：2017年7月～2017年12月
募集件数：10種類まで
（CCDS会員企業を優先）

トライアル開始時期：上記期間内にて調整
脆弱性検証期間：約1週間
検証方法：CCDS保有ツールにより実施
検証結果：依頼者、実施者、CCDSにてＮＤＡ
検証者：（株）マストトップ社（CCDS会員）
費用：無償

連絡先　info@ccds.or.jp