

# パスワード及びログの保存設定に着目した IoT デバイスにおけるファームウェアの安全性調査

Investigation of firmware security in IoT devices with a focus on password and log storage settings

川島佑介・ネットワーク分科会・情報セキュリティ大学院大学

## RQ IoT機器は本当に安全なのか？

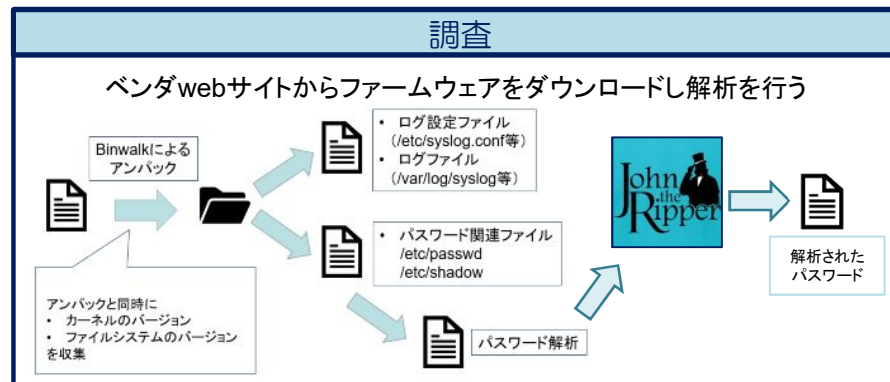
## 貢献

- ・関連研究で不足している部分の調査を実施した
- ・大規模調査のための予備調査を実施した

### 背景

IoT機器は様々な分野で数多く使われているが、その安全性には問題がある

弱い初期パスワード	適用されない更新パッチ	物理的ハードニングの欠如
十分に保存されないログ	脆弱性を含まないままの製品	ベンダや機器の信頼性



### 関連研究

様々な研究が存在するが、**ログとパスワード**の調査が十分行われていない

	D.D.Chenら	山本朝花ら	Ruotong Yuら	白石周暮ら
アーキテクチャの種類	○	○	○	○
カーネルのバージョン	○	○	○	○
ファイルシステムのバージョン	×	○	×	○
アプリケーションの種類とバージョン	○	○	×	○
適用されている攻撃緩和策	×	×	○	○
動的な脆弱性調査	○	○	×	×
カーネルやアプリケーションに古いバージョンが使われる理由	×	×	×	○
開発の際にセキュリティを阻害する要因	×	×	×	○
ログの保存設定	×	×	×	×
パスワード設定	×	×	×	×

### 調査結果

各種情報を調査し、パスワード解析を行いパスワードの強度を確認した

項目	結果
カーネルの抽出	6件
ファイルシステムの抽出	10件
ログの保存設定	無し
パスワード設定	4件 (うち3件が解析可能)

※ いずれも母数は収集した42件のファームウェア

**ログの保存される機器は存在せず**

- ・ etc/syslog.conf (syslogの設定ファイル) 1件
- ・ 「/var」ディレクトリは、「/dev/null」へとリダイレクト
- ・ ログローテーション設定 無し

**パスワードは脆弱な状況**

- ・ shadowファイルの使用 1件
- ・ パスワード桁数5桁以内 3件
- ・ 英字もしくは数字のみのパスワード 1件

### まとめ

<b>成果</b>	<ul style="list-style-type: none"> <li>・ ログの保存設定やパスワードの強度などについて調査を行った</li> <li>・ ファームウェアの収集や解析の自動化などの今後の課題が明らかになった</li> </ul>
<b>今後</b>	<ul style="list-style-type: none"> <li>・ デバイスごとの固有ログの調査を行う (IPカメラ固有のログ等)。</li> <li>・ 大規模調査を行い、国やベンダごとの脆弱性等についての傾向を分析する</li> </ul>