# 複数 IoT デバイスの位置関係に起因する脆弱性の複合現実感技術を用いた検出・可視化

# An MR-based Detection and Visualization System of Location-based IoT Security

情報工学専攻 赤坂 優馬
Information and System Engineering Yuma AKASAKA

## 1 序論

IoT 家電は, 情報セキュリティの観点からは 2 つの脆弱性がある. 第一に, ファームウェア/ソフトウェアの自動更新のない IoT デバイスは, セキュリティホールとなる恐れがある. 第二に, IoT デバイスを複数使用している場合, 複合要因により, 単体の IoT デバイスでは発生しない脆弱性を引き起こす可能性がある. 例えば, スマートスピーカなどの音声入力デバイスには, 攻撃音声という音声コマンドを埋め込めんだ音声によって不正操作される脆弱性が存在し, ハッキングされた音声出力デバイスが聴覚範囲内にある場合, 攻撃音声を用いて攻撃される可能性がある. この攻撃を防ぐためには, IoT デバイスの位置情報を使用して, 音声入力デバイスを攻撃音声の届く範囲に配置しないように警告して, 攻撃音声の届かない範囲に配置させる必要がある.

そこで本研究では, 次の 2 つを目的とする. 第一に, IoT デバイスの脆弱性と対策をユーザに分かりやすく提示し, IoT デバイスの脆弱性についての知識を深めさせ, 対策を行えるよう支援する. 第二に, IoT デバイスの位置情報を取得し, デバイス同士の位置関係によって生じる脆弱性について警告する. この 2 つの目的を達成するために, 本研究では複合現実感 (Mixed Reality, MR) を用いてユーザに, IoT デバイスの脆弱性を分かりやすく伝え, 対策を促すシステムを提案する. このシステムは, ユーザに IoT デバイスの脆弱性を理解させ, IoT デバイスについての知識を向上させることを目標とする. 目標の達成度の確認にはユーザアンケートを実施する. ユーザに提案システムを体験させた後に, IoT デバイスの脆弱性の理解しやすさ, 脆弱性の対策の行いやすさなどを評価させる. また, 各アンケート項目は実験前までのセキュリティ意識が十分ではないユーザから過半数の高評価を得た場合に目標達成とする.

## 2 複合現実感の概要

文献 [1] に従えば, MR とはコンピュータ内に構築される仮想世界を現実世界の情報で強化する拡張仮想感という概念と, 現実の環境とそこから得られる様々な知覚情報に, コンピュータが生成した仮想物体や情報を現実世界の中に表示する技術である拡張現実感とを統合し包含する概念である. 本研究では, IoT デバイスの位置情報を取得し, MR を用いて IoT デバイスに脆弱性情報を重畳表示することで, ユーザの脆弱性に対する理解度の向上を目指す.

## 3 IoT デバイスに対する脅威

家庭用のブロードバンドルータ, スマートスピーカ, 監視カメラ等の機器はオープンソースソフトウェア（Open Source Software, OSS）を利用して作られていることが多い. OSS はコミュニティの慣習から, 脆弱性が発見された場合は開発元から直ちにパッチが公開されるのが一般的である. しかし, パッチや更新の適用は OSS を利用したソフトウェアやシステムの開発者・利用者に委ねられていることが多く, そのため適切な対応が行われないことが起きやすい. また IoT デバイスの場合, ファームウェアの更改がなかなか進まない, 出荷の際に最新化せずに当初のままのファームウェアで出荷されるケース, 機器のサポート期間が終了しファームウェアの更新版や修正パッチがリリースされないケースもある. さらに, 家庭用の IoT デバイスの場合は, 購入後の管理者は利用者本人になることが多く, ファームウェアの更新・設定作業は, 一般の利用者側に委ねられている [2]. このため, 利用者に IoT デバイスのセキュリティ意識がないと, 不正操作やマルウェアを用いたサイバー攻撃の被害を受ける. サイバー攻撃を防ぐためには, 管理者であるユーザに

脆弱性を分かりやすく伝え, 対策を促すことが必要である.

# 4　提案手法

## 4.1　概要

本研究では, MR を用いて, IoT デバイスのセキュリティと脆弱性への対策を重畳表示するシステムを提案する. 提案システムでは, 透過型 HMD である HoloLens を用いる. このシステムでは, HoloLens のマッピングデータから IoT デバイスの位置情報を取得し, 脆弱性データベースと対策履歴から現在の IoT デバイスの状態を参照し, ユーザに IoT デバイスの脆弱性の対策を提示する. システムはユーザに対して, IoT デバイスの危険度を色で, かつ, 脆弱性の対策を文章で提示する. ユーザは現実の IoT デバイスを見ることで, 重畳表示された IoT デバイスの状態を示す仮想のオブジェクトを見られ, その IoT デバイスのセキュリティ状態を直感的に理解できる. また, IoT デバイスに脆弱性がある場合には, ユーザが対策を読むことで容易に実行できる. システムの流れを図 1 に示す.

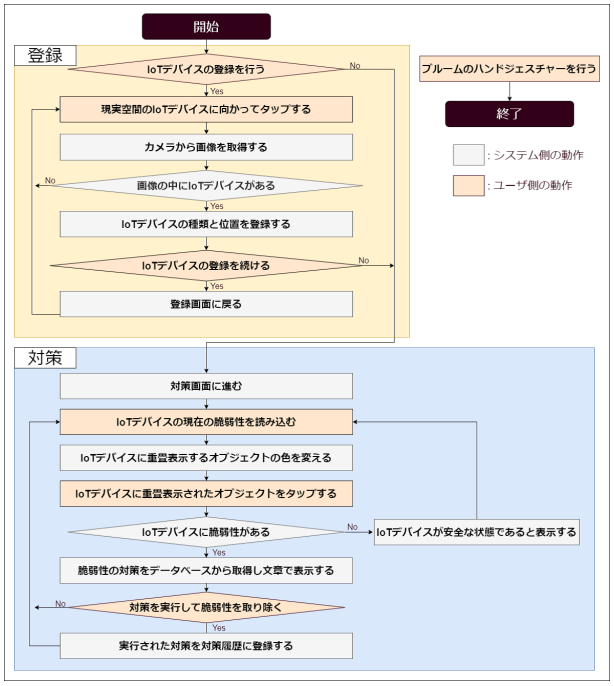


図 1: 提案システムの流れ

## 4.2　データベースの詳細

提案システムでは, 2 種類のデータベースによって IoT デバイスの脆弱性とユーザによる対策の履歴を管理する. IoT デバイスの脆弱性を登録したデータベースのレコードは, 脆弱性の種類, 脆弱性をもつ IoT デバイスの名称, 脆弱性があるか判断する条件, 脆弱性の危険度, 脆弱性の対策で構成される. ユーザが行った対策の履歴を保存するデータベースのレコードは, 対策を実行した日時, 実行された対策, 実行された IoT デバイスの名称で構成される. 複数デバイスに起因する脆弱性をデータベースに登録する際には, 脆弱性があるか判断する条件に, 近くにあると脆弱性が発生してしまう IoT デバイスの名称を登録する.

脆弱性を表示するときは, まず, 登録されている IoT デバイス名で脆弱性データベースを検索し, そのデバイスが持っている脆弱性をすべて参照する. その脆弱性の種類とデバイス名で対策履歴を検索し, 登録されていない最も危険度の高い脆弱性を, デバイスに発生している可能性がある脆弱性としてユーザに提示する. 提示した情報をもとにユーザが対処を実行し, 対処実行完了ボタンをタップすることで, 表示していた脆弱性を対策履歴に登録する. これによって, IoT デバイスに直接問い合わせることなく脆弱性の情報を管理する.

## 4.3　提案システムの特徴

提案システムの特徴を以下に述べる.

- 複数のデバイスに起因する脆弱性について警告できる.
- IoT デバイスの位置情報を取得できる.
- ネットワーク上から確認が難しい脆弱性にも対応している.
- 脆弱性の危険度について重畳表示されたオブジェクトの色から直感的に理解できる.
- マーカなどの事前準備が必要ない.
- 複数の脆弱性を持っているデバイスがあるときに, 表示するのは一つの脆弱性であり, 複数ある場合にはその中で危険度が最も高い脆弱性のうちの一つのみ表示される.

# 5　実装

図 2 に IoT デバイスの登録画面を, 図 3, 4, 5 に提案システムの脆弱性の対策画面を示す.


図 2: IoT デバイスの登録

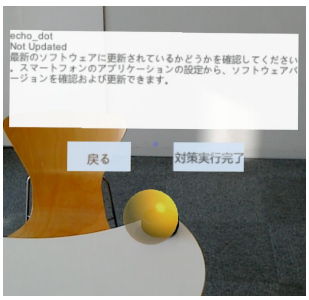


図 3: ソフトウェアの更新

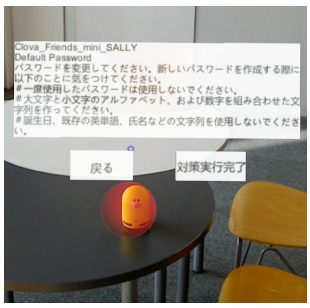


図 4: パスワードの設定

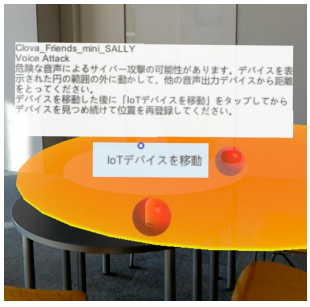


図 5: 位置関係に起因する脆弱性

## 6 評価実験と考察

### 6.1 アンケート結果

目標の達成度を測定するため, ユーザ 16 人に提案システムを使用してもらい, アンケートを行った. まず事前アンケートで, 普段セキュリティを意識しているか聞き, セキュリティ意識の比較的低い 9 人をグループ A とし, 比較的高い 7 人をグループ B とした. アンケートの評価は, 値が小さいほど高評価で値が大きいほど低評価である. 結果を表 1〜7 に示す.

表 1: 提案システムの操作性について

| 質問項目 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1.1 デバイスを登録する操作 | 4 | 5 | 5 | 2 | 0 |
| 1.2 脆弱性を対策する操作 | 3 | 7 | 4 | 2 | 0 |

表 2: 表示方法の分かりやすさについて

| 質問項目 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 2.1 ソフトウェアの更新 | 5 | 9 | 2 | 0 |
| 2.2 パスワードの設定 | 5 | 9 | 2 | 0 |
| 2.3 攻撃音声への対策 | 8 | 5 | 3 | 0 |

表 3: 対策方法の文章の分かりやすさについて

| 質問項目 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 3.1 ソフトウェアの更新 | 5 | 10 | 1 | 0 |
| 3.2 パスワードの設定 | 8 | 6 | 2 | 0 |
| 3.3 攻撃音声への対策 | 5 | 8 | 3 | 0 |

表 4: 色で表示した危険度の分かりやすさについて

| 質問項目 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 4.1 ソフトウェアの更新 | 10 | 6 | 0 | 0 |
| 4.2 パスワードの設定 | 10 | 6 | 0 | 0 |
| 4.3 攻撃音声への対策 | 10 | 6 | 0 | 0 |

表 5: 位置関係に起因する脆弱性への理解について

| 質問項目 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 5.1 脆弱性への理解度 | 6 | 10 | 0 | 0 |

表 6: 提案システムに使用したデバイスについて

| 質問項目 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 6.1 視野の広さ | 0 | 3 | 1 | 2 | 10 | 0 |
| 6.2 重量の軽さ | 2 | 4 | 5 | 4 | 1 | 0 |

表 7: 使用によるセキュリティ意識の変化

| 質問項目 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 7.1 セキュリティ意識の変化 | 1 | 10 | 4 | 1 | 0 |

### 6.2 考察

#### 6.2.1 提案システムの操作性について

表 1 の項目 1.1, 1.2 において, 操作を間違えず行えたユーザは過半数となった. 残りのユーザは, ボタンのタップ操作をミスした, 認識されなかったと答えている. この原因として, 事前のタップ操作練習が不十分であったことが考えられる. 練習では視線に追従するオブジェクト 3 個とその場から動かないオブジェクト 3 個を問題なくタップできれば終了としていたが, より多くの回数のタップを練習させて操作に慣れさせる必要があると考えられる. また, 項目 1.2 でミスしたユーザの中には, 位置関係に起因する脆弱性の対策方法の操作が複雑だと答えた者がいるため, 操作方法を改善する必要がある.

#### 6.2.2 提案システムの脆弱性の表示方法について

表 2 の項目 2.1, 2.2, 2.3 は, グループ A と B 両方の過半数のユーザが高評価を与えた. つまり, ユーザに IoT デバイスの脆弱性を分かりやすく伝えるという目標は達成できたといえる. しかし, 脆弱性の種類や対策方法が分かりづらかったと回答したユーザもいる. これらのユーザは, セキュリティに詳しくない人は対策文だけでは理解が困難だという意見や, 視線の操作のために首が痛くなったと答えている. この結果から, より複雑な脆弱性に関しては提案システムでは理解度が上がらない可能性が考えられるが, 今回使用したレベルの脆弱性であれば, 多くのユーザが理解できると言える. また, ボタンに対してカーソルを合わせるために視線を動かすという動作が負担になり, 対策文を読むことに集中できなくなる可能性が考えられるが, デバイスに慣れることで負担は軽減されると予想される. また, 項目 2.3 で分かりづらかったと回答

したユーザは, 表 6 の項目 6.1 において, デバイスの視野の狭かったと答えており, 位置関係に起因する脆弱性の対策のための円が, 分かりづらかった可能性が考えられる. そのため, 将来的にデバイスの視野角が広がればより評価が上がると思われる.

表 3 の項目 3.1, 3.2, 3.3 は, グループ A と B 両方の過半数のユーザが高い評価を選択しているが, 項目 3.2, 3.3 のグループ B に分かりづらかったと答えているユーザがいる. この理由として, パスワードを設定する際に, 入力した文字列の強度をリアルタイムに評価できるシステムの方が分かりやすいという意見と, 位置関係に起因する脆弱性の対策で IoT デバイスを動かした際の操作が分かりづらかったという意見があった. パスワードの強度の評価は, このシステムでは難しいが, 強度の高いパスワードをランダムに生成する機能があれば, より評価が上がる可能性が考えられる. また, IoT デバイスを動かす方法をより直感的にすると評価が上がると思われる.

表 4 の項目 4.1, 4.2, 4.3 は, 全てのユーザが高い評価を選択している. このことから, 提案システムの色を IoT デバイスに重畳表示する危険度表示は有用であると言える. しかし, 視線に追従する UI が邪魔になる場面があったと答えたユーザがいる. このため, UI の動きを制限する, UI を一時的に小さくする, といった機能を追加すれば, より評価が上がる可能性が考えられる.

#### 6.2.3 位置関係に起因する脆弱性について

表 5 の項目 5.1 において, 全てのユーザが位置関係に起因する脆弱性の理解に対して高評価である. しかし, 理解度が少し低いユーザもいる. この原因として, 6.2.2 でも述べた, 視野角の狭さから位置関係に起因する脆弱性を提示する円が分かりづらかった可能性と, IoT デバイスを動かす際の操作が分かりづらかった可能性が考えられる. この 2 つの点を改善することで, ユーザの位置関係に起因する脆弱性の理解度がより高くなると思われる.

#### 6.2.4 システムの総合評価

表 7 の項目 7.1 において, 過半数のユーザがセキュリティ意識が向上したと回答した. このことから, 提案システムはユーザのセキュリティ意識を高めるために有用であると言える. また, HoloLens を今回初めて使用したというユーザもセキュリティ意識が向上したと回答しており, HoloLens を使ったことがないユーザに対しても有用であると示せた. しかし, グループ A に比べて, グループ B のセキュリティ意識の向上が少ないことが見られた. これは, もともとセキュリティ意識が高い人のセキュリティ意識をさらに高めることは難しいからだと思われる.

## 7 結論

本研究では, 複数の IoT デバイスの位置関係に起因する脆弱性を警告でき, かつ, IoT セキュリティに詳しくないユーザのセキュリティ意識を向上させるシステム作りを目的とし, MR を用いて IoT デバイスに脆弱性の危険度と対策を重畳表示するシステムを作成した. 提案システムは, HoloLens を用いて IoT デバイスの脆弱性とその対策を知れる. しかし, 操作方法が分かりづらい箇所があり, 改善する必要がある.

アンケート結果から, 提案システムを使用することでユーザのセキュリティ意識を向上させられることを示せた. また, MR を用いて IoT デバイスの脆弱性を重畳表示することの有用性を示せた. 今後の課題としては, 操作方法の改善, 複数の脆弱性があるときの表示方法, UI の改善が挙げられる.

## 謝辞

本研究を通じ, 懇切丁寧な御指導, 御鞭撻, 及び多くの御支援を賜りました, 中央大学理工学研究科情報工学専攻牧野光則教授に深く感謝致します. また, よき同僚として御協力いただいた同輩諸氏, アンケートにご協力いただいた方々に御礼申し上げます.

## 参考文献

[1] 田村秀行, 大田友一: “複合現実感”, 情報映像メディア学会誌, vol.52, no.3, pp.266-272, 1998.

[2] BUSINESS COMMUNICATION : “桑名レポート：サイバーセキュリティの現場から 7. IoT 機器の脆弱性と対策”, https://www.bcm.co.jp/solution-now/cat-solution-now/cat-now-sybersecurity/2019-03_1753/ (最終アクセス 2020 年 3 月 1 日)