

# 在宅IoMT利用における家庭用ネットワークセキュリティ —患者・家族向けガイドの設計と検討—

Home Network Security for At-Home IoMT Use:  
Design and Assessment Patient-and Family-Oriented Guide

中井太郎・ネットワーク分科会・情報セキュリティ大学院大学

abstract-As IoMT adoption grows, cyberattacks increasingly threaten patient safety, especially in home care where devices rely on household networks. This study identifies home-network threats and security requirements for IoMT and proposes a practical patient/family guide covering setup steps and operating rules, then assesses feasibility by aligning it with existing guidelines.

## 研究成果の概要

- 在宅IoMTにおける脅威を医療安全の観点から体系化
- 患者・家族が状況ごとに実行可能な利用者向けガイドを設計
- 使い方についての記載の有無を既存のガイドラインと比較評価

## 背景

1. IoMTの拡大
2. 在宅医療の進展
3. 接続先とリスクの変化
  - 閉域網→家庭内LAN
  - 情報漏洩→医療安全

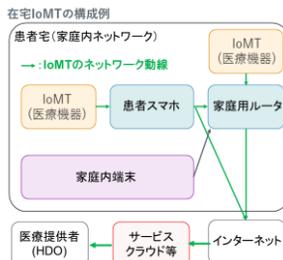
## 既存ガイドラインの整理と課題

- 医療機関向け  
医療機関内の管理が対象。在宅環境対策は患者への説明や連絡体制の整備。
- 製造業者向け  
Security by Designの要求。脆弱な環境前提の設計。
- 消費者向け  
一般家電を想定。医療機器に求める高可用性・完全性とは不一致

患者・家族が状況ごとに実行可能な具体的な運用ガイドが不足している。

## 脅威の整理と医療安全への影響

- 在宅のリスク: 一般IoTの混在、設定不備、物理的アクセス
- 脅威モデルの整理: 攻撃元をインターネット、家庭内LANなど類型化
- 医療安全への直結: 改ざん・NW障害・なりすまし等の侵害は、誤診や搬送遅延に直結



## 提案ガイドとコンセプト

- 医療安全を最優先
- 家庭環境の制約を前提
- ITリテラシーが高くなくても実行可能
- 導入時、定期点検、困ったときの3局面

### 在宅IoMTを安全に使うガイドライン

対象: 患者宅 (IoMT Edge Network+家庭用ネットワーク運用) 想定: 1日に不慣れた患者・家族  
重要: 体調が悪い・緊急時は医療安全を最優先し、緊急要請または医療機関へ連絡する

- | 導入時 (最初に1回)  | 定期点検 (毎月1回)  |
|--|--|
| <input type="checkbox"/> 連絡先を記入 (医療機関/メーカー/緊急)                 | <input type="checkbox"/> ルータの更新 (ファームウェア) を確認する        |
| <input type="checkbox"/> Wi-FiはWPA2またはWPA3、長いパスワードにする          | <input type="checkbox"/> スマホOSとIoMTアプリを最新にする           |
| <input type="checkbox"/> ネットワーク設定をパスワードで変更する                   | <input type="checkbox"/> 使っていない機器はWi-Fiをオフにし、電源も切る     |
| <input type="checkbox"/> IoTデバイス管理をパスワードで変更する                  | <input type="checkbox"/> 設定ルールを確認 (伊勢川流しなど、設定を勝手に変えない) |
| <input type="checkbox"/> IoMT専用Wi-Fi (ゲスト/別SSID) における (可能な範囲で) | <input type="checkbox"/> 医療者からのお知らせを確認する               |
| <input type="checkbox"/> 暗号化不要なリモート管理をOFFにする                   |  |
| <input type="checkbox"/> 公的アプリのみ使用し、2段階認証があればONにする             |  |
| <input type="checkbox"/> スマホに画面ロック (PIN+生体) を設定する              |  |

### 困ったとき (まず医療安全)

- 体調が悪い場合、医師より先に医療機関へ連絡 (または急診)
- 設定変更がわからない/変更できない/変更できない場合は医療機関へ連絡 (または急診)
- ① まずルータとスマホを再起動 (機器本体の初期化・設定変更は医療者の指示があるまで行わない)
- ② 公式アプリでエラー表示と対処法をメモ
- ③ 医療者へ報告 (待たせながら、いつからか、表示内容)
- 不要なメール・電話で困った状況を報告してはならない (医療機関・メーカーを名乗ってはいけません)
- スマホ紛失時: 通信会社の紛失手続、端末の遠隔/強制ロック、IoMTアカウントのパスワード変更、医療機関へ連絡

### 連絡先

医療機関 (担当/窓口)	メーカー/サポート

注: 医療機関の設定変更・ファームウェア更新は、医療機関またはメーカーの指示に従う。

## 評価・結論

6つのフェーズを設定し、各ガイドラインの利用者向け手順の具体性を定量的に評価。

文書群	P1(導入前)	P2(初期設定)	P3(日常運用)	P4(更新・脆弱性対応)	P5(異常時対応)	P6(廃棄・譲渡)
一般消費者IoT	△	◎	○	○	△	△
医療機関向け	○	△	△	△	△	△
遠隔医療向け	△	△	○	△	△	△
メーカー向け	△	△	△	△	○	○
IoT製品基準	◎	△	△	○	△	△
患者啓発	△	△	○	○	○	×
提案ガイドライン	△	◎	○	○	◎	×

## 強み

- P2: ルータ設定や端末管理をチェックリスト化
- P5: 医療安全を優先したフローの提示、既存の消費者向け基準の欠落を補完