Vol.2020-CSEC-91 No.10
Vol.2020-SPT-40 No.10
Vol.2020-EIP-90 No.10
2020/11/25

ECHONET Liteのクラス別リスク評価に基づいたセキュリティ対策

山川 大貴[1,a)]　沖本 貴志[2,b)]　猪俣 敦夫[3]　上原 哲太郎[2,c)]

概要：現在，家庭内の家電や設備機器の最適制御を行うことでエネルギーを効率的に利用する仕組みを導入したスマートハウスが注目されている．スマートハウスには HEMS(Home Energy Management System) と呼ばれる家庭内のエネルギー利用を管理する設備がしばしば導入される．HEMS において広く使われている通信プロトコルとして ECHONET Lite がある．本研究では，ECHONET Lite 対応機器にセキュリティ機構が実装されているか現状を確認することを目的として，実機を用いた調査を実施した．調査対象としては HEMS コントローラの入手が困難であったため，スマート家電を用いた．調査の結果，対象機器では送信元認証や通信経路の秘匿化は行われておらず，ECHONET Lite を用いて攻撃が可能であることが判明した．一方で，ECHONET Lite を悪用して生じる被害の種類や深刻度は機器に実装されているクラスの機能に依存しているため，各クラスのリスク評価を行う必要があると考えた．そこで，ECHONET Lite の仕様で定義された全てのクラスに対して，攻撃による被害額に着目したリスクアセスメントを行い，その結果に応じたセキュリティ対策を行うことを提案する．

Class-based Risk Assessment and Security Measures against Vulnerabilities on ECHONET Lite

1. はじめに

近年，地球温暖化の進行を抑止するため，エネルギー利用の効率化によって，総エネルギー消費量を減少させることが求められている．家庭においては家電や住宅設備を最適に制御してエネルギー消費量を削減する HEMS が注目されており，その実現には異なるベンダで製造された機器間で相互通信できる必要がある．そこで，機器間の共通の通信プロトコルとして ECHONET Lite が策定され，対応した家電が普及している．しかし，ECHONET Lite ではセキュリティに関する規定がないため，セキュリティ機構をベンダが実装する必要がある．そのため，ECHONET Lite におけるセキュリティ機構の実装状態を実機を用いて調査する．また，ECHONET Lite では各機器の機能をクラスとして定義しており，クラスによってはセキュリティ機構を実装する優先順位が実装にかかるコストを考慮すると低いものもあると考えられる．一方で，全クラスの優先順位をつけるための指標がないことが問題である．したがって，本研究では指標を示すことを目的として，各クラスの攻撃シナリオを想定し，攻撃の発生確率と影響を考慮したリスクアセスメントを実施した．

[1] 立命館大学大学院 情報理工学研究科
[2] 立命館大学 情報理工学部
[3] 立命館大学 総合科学機構研究機構，大阪大学
[a)] yamakawa@cysec.cs.ritsumei.ac.jp
[b)] okimoto@cysec.cs.ritsumei.ac.jp
[c)] t-uehara@fc.ritsumei.ac.jp

2. 研究背景

2.1 ECHONET Lite

ECHONET Lite は HEMS コントローラが様々な家電・住宅設備と相互接続する際に利用する共通の通信規格である [1]．通信ミドルウェアは OSI 参照モデル上においてセッション層，プレゼンテーション層に位置づけられている [2]．また，ECHONET Lite の送信形態は個別送信と一斉同報送信の 2 種類があり，特定のノードに対して ECHONET Lite フレームを送信する個別送信の場合にはトランスポート層以下のアドレスを用いて送信先を指定する．一斉同報送信は同一サブネット内のすべての ECHONET Lite ノードに対してマルチキャストまたはブロードキャストを用いて ECHONET フレームを送信することである．

Vol.2020-CSEC-91 No.10
Vol.2020-SPT-40 No.10
Vol.2020-EIP-90 No.10
2020/11/25

次に，ECHONET Lite ノード，機器オブジェクト，クラスとプロパティの関係性について説明するため，各関係性を図 1 に示し，電文形式も図 2 に示す．

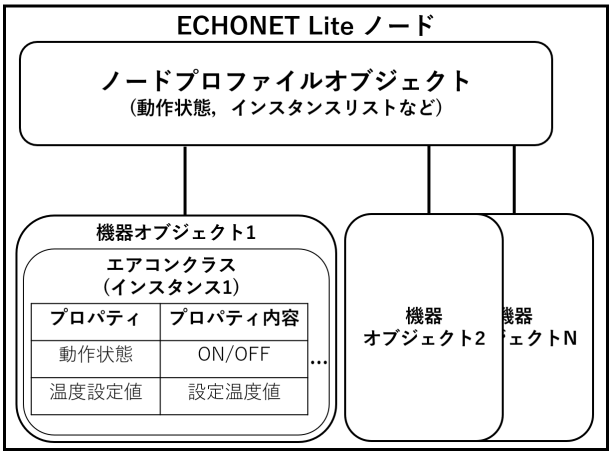

図 1 ノード/機器オブジェクト/クラス/プロパティの関係性

EHD1	：ECHONET Lite電文ヘッダー1	(1B)
EHD2	：ECHONET Lite電文ヘッダー2	(1B)
TID	：トランザクションID	(2B)
SEOJ	：送信元ECHONET Liteオブジェクト指定	(3B)
DEOJ	：送信先ECHONET Liteオブジェクト指定	(3B)
ESV	：ECHONET Liteサービス	(1B)
OPC	：処理プロパティ数	(1B)
EPC	：ECHONET Liteプロパティ	(1B)
PDC	：EDTのバイト数	(1B)
EDT	：プロパティ値データ	(PDCで指定)

図 2 ECHONET Lite の電文形式

ECHONET Lite ノードはメーカ情報等のノードとしてのプロファイル情報をノードプロファイルオブジェクトとして保持している．そのため，他の ECHONET Lite ノードがプロファイルの情報を書き込んだり，読みだしたりする際には DEOJ(送信先 ECHONET Lite オブジェクト指定) にノードプロファイルオブジェクトを指定する．機器オブジェクトは機器として持つ動作機能を保持している要素で各オブジェクトの仕様はクラスとして定義されている．ECHONET 機器オブジェクト詳細規定 [3] で 118 個のクラスが定義されており，各クラスが持つ機能に関してはプロパティとして定義されている．プロパティでは操作方法であるアクセスルール，クラスを実装する際に対象プロパティが実装必須かどうか，プロパティ値が更新されたときに状態変化時アナウンスとして他の機器に対して一斉同報送信するか等が規定されている．

最後に，本研究の調査とリスクアセスメントを説明する際に重要な電文形式の要素である ESV(ECHONET Lite Service) と EPC(ECHONET Lite Property) について説明する．ESV では ECHONET Lite ノードに対する操作方法を指定でき，主な ESV の定義として Get/Set/INF_REQ の 3 つがある．ESV の各定義とその説明を下記に示す．

- Get は設定されているプロパティ値を読み出す
- Set はプロパティに値を書き込む
- INF_REQ はプロパティ値を通知することを要求する (返答は一斉同報送信)

ECHONET Lite ノードは ECHONET Lite フレームを受け取った際に DEOJ でどのクラスとインスタンスに対する操作命令なのか判断し，ESV の値によって操作方法，EPC の値によってどのプロパティに対する操作命令なのか判断する．

2.2 関連研究

城間・井上ら [4] はスマートハウス内で通信する機器の経路を起点にリスク特定を行う手法を提案している．この提案では，スマートハウス内にある機器の通信データの内容が通信しているインターフェースや通信プロトコルによって異なることに着目しており，インターフェースや通信プロトコルごとにたどりつく保護資産を導出している．例えば，ホームゲートウェイに対して無線 LAN ポートで UPnP プロトコルによって通信する場合，たどり着ける保護資産として端末名や WAN 側の IP アドレスなどが導出できる．しかし，井上らの研究では下位の伝送メディアの差異をアプリケーション層から隠蔽して利用できる ECHONET Lite 通信ミドルウェアが想定されていない．そのため，本研究は通信に利用されるインターフェースやプロトコルではなく，攻撃される ECHONET Lite クラスの特徴を考慮したシナリオを想定し，どのような被害が発生するかによってリスク特定を行った．

3. 提案

ECHONET Lite では通信経路の暗号化や送信元認証の規定はされておらず，ECHONET Lite より下位レイヤである OSI 参照モデルのトランスポート層以下でのセキュリティ機構を利用することをセキュア通信の実現指針として示している [5]．表 1 に紹介されているセキュリティ機構の一覧を示す．推奨されているセキュリティ機構の中には，IPsec や DTLS といった通信経路の暗号化や送信元認証を実現できる機構があるため，すべての ECHONET Lite 対応機器に対してそれらのセキュリティ機構を実装することで ECHONET Lite を安全に利用することができる．一方で，機器にセキュリティ機構を実装する場合，人件費等の追加費用が発生するため，機器の機能を考慮してセキュリティ機構の実装を優先順位をつけて対応することが重要であると考えられる．したがって，ECHONET 機器オブジェクト詳細規定 [3] で定義されている全クラスに対して，ECHONET Lite を悪用して生じる被害の深刻度や攻撃する難易度を基にリスクアセスメントを実施し，その結果に

表 1 通信レイヤのセキュリティ機構

通信レイヤ	セキュリティ機構
トランスポート	DTLS (Datagram Transport Layer Security)
ネットワーク	IPsec(Security Architecture for Internet Protocol) RFC5191
データリンク	WEP(Wired Equivalent Privacy) WPA(Wi-Fi Protected Access) WPA2(Wi-Fi Protected Access2) AES-CCM(Advanced Encryption Standard Counter with CBC-MAC) IEEE802.1X

応じたセキュリティ対策を行うことを提案する．本研究で行ったリスクアセスメントにおける，各クラスに行うリスク特定とリスク分析のフロー図を図 3 に示す．ここで行うリスクアセスメントは，各クラスで攻撃シナリオを想定し被害の種類を分類した後，プロパティを抽出することでリスク特定を行う．リスク分析では，攻撃による被害の影響と発生確率を定量化し，スコア算定式によって各クラスのリスクのスコアを算出する．ここでは，被害の影響を，異なる被害の種類で影響の大小関係を比較するための共通の指標として被害額によって定量化する．最後に，算出されたスコアを順序付けた表にまとめ，順序の妥当性について検討する．

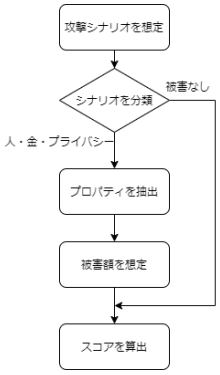

図 3 リスク特定とリスク分析のフロー図

4. 調査

本研究では，各クラスのリスクアセスメントを実施する前に ECHONET Lite 機器に対して実際に攻撃が可能か実機を用いた調査を実施した．今回，HEMS コントローラが入手困難であったため，調査した機器は ECHONET Lite に対応したスマート家電である．調査対象の機器を表 2 に示す．エアコンと空気清浄機は動作状態や風量設定など各機能を ECHONET Lite を用いて制御できる．コントローラとは ECHONET Lite を利用する他の機器の状態取得や機器に対して操作命令を出す機能を有している機器である．

表 2 調査対象の機器

会社名	A 社	B 社	C 社
機器	エアコン	空気清浄機	コントローラ

4.1 調査方法

調査方法は研究室 PC と機器を研究室 LAN に接続し，研究室 PC と機器間で ECHONET Lite を用いた通信を試みて機器の挙動を観察し，通信内容を観測した．仮に，通信内容が平文でやり取りされていれば，通信経路の暗号化は行われていないことが判明する．さらに，ECHONET Lite で送信した操作命令通りに機器を制御できていれば，送信元認証の機能が機器に実装されていないことがわかる．機器に ECHONET Lite の機能としてどのプロパティが実際に実装されているか事前に知るために，Set プロパティマップと Get プロパティマップの取得を行う．Set プロパティマップとは機器に値を設定できるプロパティ一覧のことで，Get プロパティマップは機器に設定されている値を取得できるプロパティの一覧である．また，C 社のコントローラが他の ECHONET Lite 機器を管理対象に追加する際の機器間の通信方法に着目し，偽の存在していない機器を追加できるか試みた．

4.2 調査結果

調査対象のすべての機器に対してポートスキャンを実施したところ，3610 番 (UDP) ポートが開いていることがわかったため，UDP 通信で各機器と通信を行った．ECHONET Lite では UDP 通信をする際にはマルチキャストアドレスとして 224.0.23.0 を利用することが定められている [2]．そのため，一斉同報送信をする際には送信先アドレスに 224.0.23.0 を設定した．

4.2.1 A 社:エアコン

機器の電源状態を取得するパケットを送信した結果，機器から応答パケットを受け取ることができた．通信内容を確認したところ，平文で通信されており，通信経路の暗号化は機器に実装されていないことが判明した．次に，電源を操作するパケットを送信した結果，電源の ON/OFF を切り替えられたことから，任意の機器がエアコンの状態取得や値の設定が可能であるため，送信元認証も実装されていないことがわかった．さらに，機器の状態取得を取得するパケットを大量に送信して，機器に対する DoS 攻撃のテストを行った結果，パケットを送信している間はスマートフォンアプリ側で機器の状態取得ができなくなった．

4.2.2 B 社:空気清浄機

機器の電源状態を取得するパケットを送信した結果，機器から応答パケットを受け取ることができなかった．しかし，電源を操作するパケットを機器に送信すると，電源の ON/OFF を切り替えられたことから，任意の機器が空気清浄機に対して値を設定でき，送信元認証が実装されてい

ないことがわかった．次に，機器が制御命令を受け取ったときに送信する通知の通信内容を確認したところ，平文で通信されており，通信経路の暗号化は機器に実装されていないことが判明した．また，機器に設定されている値を読み出すパケットに関して一切応答がなかった．ECHONET 機器オブジェクト詳細規定 [3] では，空気清浄器クラスの電源状態の取得は実装必須となっているため，今回の結果はメーカの実装が仕様に沿っていない可能性がある．

4.2.3 C 社:コントローラ

機器の電源状態の取得するパケットを送信した結果，機器から応答パケットを受け取ることができた．通信内容を確認したところ，平文で通信されており，通信経路の暗号化は機器に実装されていないことが判明した．次に，コントローラの開発元が提供しているスマートフォンアプリでコントローラに追加できる機器の一つに太陽光発電機があったため，今回は太陽光発電機をコントローラの管理する機器に追加するときに考えられる攻撃方法を説明する．1 つ目はコントローラに偽機器を追加させる方法である．まず，通信経路の暗号化が実装されていないことからコントローラが機器を追加する際の通信フローや各通信が送信されるタイミングを事前に知ることができる．コントローラが管理する機器 (以下，クライアント) を追加する際の通信フローを図 4 に示す．ECHONET Lite ノードは基本的に自身の IP アドレスを取得した後，インスタンスリスト通知を一斉同報送信する [2]．したがって，偽クライアントも太陽光発電機クラスのインスタンスリストを一斉同報送信すると，コントローラは通知したインスタンスクラスに対して Get プロパティマップを要求してきた．その後は図 4 のようにコントローラから求められる情報を太陽光発電機クラスに合致するように返答するとアプリケーション側で偽クライアントの追加が成功できたことを確認できた．2 つ目は既にコントローラの管理下にある機器から偽クライアントにコントローラの管理対象機器を変更する方法である．図 4 の識別番号を応答する際に，既にコントローラの管理下にある機器の識別番号になりすまして通信を行うことで，コントローラの管理対象機器が変更されたことを確認できた．

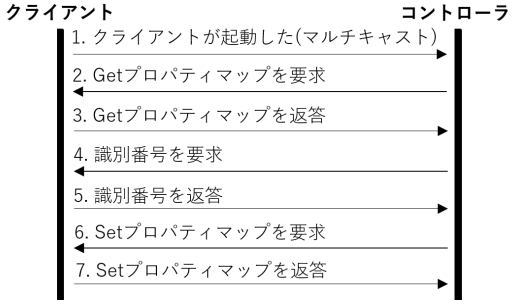

図 4 コントローラが管理する機器を追加する際の通信フロー

5. リスクアセスメント

4.2 節の調査結果より，セキュリティ対策がなされてない場合，通信内容の傍受，任意の機器からの制御などの攻撃が可能であることが判明した．そのため，ECHONET Lite よりも下位レイヤの，表 1 にあるセキュリティ機構を使用した通信を行うよう対策を施さなければならない．しかし，対策には人件費などの追加コストが発生する．一方で，攻撃される機器によって攻撃シナリオが異なるため，攻撃による被害の影響や発生確率も異なる． したがって，セキュリティ対策を施す順序を付けることが可能である．ここでは，全クラスに対してリスクアセスメントを行い，リスクを定量化して各クラスにスコアを与える． 算出されたスコアによってリスクの脅威の順序を明確にする．

5.1 リスク特定

リスク特定を行う前提として，攻撃者は LAN 内に侵入し，ECHONET Lite 機器に対して任意の制御が可能であるとする．そして，ECHONET Lite 機器オブジェクト詳細規定 [3] に記載されている全クラスに対して攻撃シナリオを想定する．攻撃シナリオが想定できないクラスは “被害なし”に分類する．次に，攻撃シナリオが想定されたクラスを，被害の種類によって “人・金・プライバシー”に分類する．これらの定義を表 3 に示す．この攻撃シナリオの実現に最低限必要であるプロパティを抽出し，これをキープロパティと呼ぶ．また，キープロパティを利用した攻撃よりも被害は小さいが攻撃に利用される可能性があるプロパティを抽出し，このプロパティを危険プロパティと呼ぶ．ただし，抽出するプロパティに動作状態は含めない．動作状態とは，機器の動作が ON/OFF である，または機器が制御受付が可能/不可能であることを示すプロパティである．

動作状態プロパティを用いた攻撃は動作状態を OFF から ON に切り替えることで，不必要なエネルギーを消費させる攻撃が想定できる．この場合，全てのクラスで被害の種類が “金”に分類されるため，プロパティから動作状態を除外した．

センサを規定したクラスでは，センサが計測した値をどのように他の機器が利用するかによって攻撃シナリオが異なる．ここでは，各クラス単体で想定した攻撃シナリオについてリスクアセスメントを行う．そのため，ここではセンサに対するリスクアセスメントは行わないものとした．

5.2 リスク算定式

全クラスに対して，リスクの深刻度を算出する．ここでは，リスクを影響と発生確率に分割して分析を行う．筆者らが考えたリスクのスコア算定式を次に示す．

表 3 攻撃シナリオの種類の定義

分類	定義
人	機器を制御することで人体に危害が与えられる
金	機器を制御することで使用，もしくは獲得エネルギーを変動させる 機器になりすますことで偽のエネルギー消費量，もしくは獲得量を発信する
プライバシー	機器を制御，もしくは通信を傍受することでプライバシー情報を抜き取る

表 4 パラメータの値

分類	R		A		S	
	必須	任意	Set	Get	必須	任意
プライバシー	3	1	3	1	0.8	1
人 or 金	3	1	1	3	1	0.8

$$Score = D \cdot R \cdot A \cdot S \cdot (1 + Num \cdot 0.1)$$

リスクの影響を表すパラメータは D，発生確率を表すパラメータは R，A，S，Num である．各パラメータは，D が攻撃シナリオによって発生する最大被害額の桁数，R がキープロパティの実装必須，A がキープロパティのアクセスルール，S がキープロパティの状態変化時アナウンスの実装必須によって値が決定される．また，Num はキープロパティと危険プロパティの総数である．R，A，S の設定値を表 4 に示す．設定値が大きいほど，リスクの脅威が大きいことを示している．

5.2.1 被害の影響

攻撃による被害の影響 D を，全クラスで攻撃シナリオによる最大被害額を算出し，この被害額の桁数によって定量化した．この被害額の想定方法は被害の種類によって大きく異なる．

まず，攻撃シナリオの被害の種類が “人”であるクラスについて述べる．“人”に分類された攻撃シナリオによる被害は，人命を落とす可能性があるものと人命には関わらないが負傷する可能性があるもので分類した．人命を落とす可能性があるシナリオには，火災を起こさせたり，人を殺害させたりする攻撃シナリオが該当する．この被害額は逸失利益で算出し，逸失利益の算出方法を次に示す．

$$\begin{aligned} \text{逸失利益} = &\text{基礎収入} \\ &\times \text{ライプニッツ係数} \\ &\times (1 - \text{生活費控除}) \end{aligned}$$

逸失利益の算出に用いる基礎収入と年齢は日本人の平均値をとる．厚生労働省の令和元年賃金構造基本統計調査 [6]，総務相統計局の平成 27 年国勢調査人口等基本集計結果の概要 [7] より，基礎収入と年齢はそれぞれ 369.24 万円，43.1 歳である．ライプニッツ係数は国土交通省の就労可能年数とライプニッツ係数表 [8] より求める．生活費控除は 40 % とした．

人命に関わらないが負傷する可能性があるシナリオとは，攻撃によって命を落とすことはないが怪我を負う可能性がある場合のことである．ここでは，被害者は怪我によって 7 日間の通院をする必要があると仮定する．通院費を Co-op 共済の医療保険 [9] より，一日あたり 1,500 円とした．したがって，このシナリオの被害額は 10,500 円である．

次に，攻撃シナリオの被害の種類が “金”であるクラスについて述べる．金額の算出は月当たりで行う．これは，電気やガス，水道の料金は月ごとに請求され，攻撃が発覚するのはこの請求時と考えられるからである．被害の種類が “金”である攻撃シナリオは電力やガス，水流メータの値を任意に変更するシナリオ，機器のエネルギー消費を増大させるシナリオと機器の生産エネルギーを減少させるシナリオの 3 つに分類できる．

メータの値を任意に変更するシナリオとは，LAN 内のメータと機器の ECHONET Lite プロトコルを用いた通信を横取りして偽の情報を流す攻撃のことである．例えば，攻撃者が電力メータの通信を横取りしたとき，エネルギーのベンダに対して消費したエネルギー量を増大させて通知することで，通常より高額な料金を請求させることが可能である．このような攻撃では任意の消費エネルギー量を他の ECHONET Lite 機器に通知することができるが，その値には上限がある．1 億円のような法外な電気料金になるよう情報を送信すると，LAN 内に侵入して機器に対して攻撃していることが露呈する．したがって，考え得る範囲内で請求できる最大料金を算出しなければならない．メータの種類は電力量，ガス，水流量の 3 種類である．ここでは請求可能な最大料金を，電力量メータは関西電力の従量電灯 A 早見表 [10] の最大値，ガスメータは大阪ガスの一般料金の H 料金 [11]，水流量メータは大阪市水道局の水道料金表 [12] の用途が一般用である料金表で 1001 立方メートル の料金とした．

機器のエネルギー消費を増大させるシナリオは，機器を最大消費電力で稼働させ続けてエネルギー消費を増大させる攻撃と夜間の安価な電力の使用を制限する攻撃の 2 種類がある．エネルギー消費を増大させる攻撃では，その機器の月当たり消費エネルギー量を算出し，それにあたる料金を被害額とした．例えば，消費電力が 1 時間当たり 94 W である機器の月当たりの消費電力量は 67680 W である．これを関西電力の従量電灯 A 早見表 [10] と照合すると 1,517 円となる．夜間の安価な電力を制限する攻撃とは，昼間より夜間の電力料金が安価であることを利用して昼間に使用する電力を夜間に貯蓄，または使用する機器に対して，夜間の稼働を停止させ，料金の高い昼間の電力を使用させる攻撃のことである．ここでは，夜間の電力料金が昼間よりも安価な料金プランである，関西電力のはぴ e タイム R [13] を適用しているとして，夜間と昼間の電力料

金の差額を被害額とした．このプランでの夜間と昼間の料金は 13.76 円の差がある．夜間が 8 時間であるから，被害額は 1 日当たり 110.08 円となり，月当たり 3,302.40 円となる．

機器の生産エネルギーを減少させるシナリオとは，太陽光発電などの発電を行う機器に対して，発電させないよう制御する攻撃のことである．この場合，攻撃による被害は本来生産できるはずだった電力量である．したがって，被害額を機器が月当たりに生産できる電力量を算出し，これを関西電力の従量電灯 A 早見表 [10] と照合した金額を被害額とした．

最後に，攻撃シナリオの被害の種類が “プライバシー”であるクラスについて述べる．この攻撃シナリオによる被害額を JO モデル [14] によって算出する．JO モデルによる個人情報価値の算定式を次に示す．

$$\begin{aligned}\text{漏えい個人情報価値} = {} & \text{漏えい個人情報価値} \\ & \times \text{情報漏えい元組織の社会的責任度} \\ & \times \text{事後対応評価}\end{aligned}$$

JO モデルに関する研究として，山田道洋らによる個人情報漏えいによる損害額の新しい数理モデルの提案 [15] がある．この研究では，JO モデルの算出式やその係数が専門家による経験則から決められたものであるため，JO モデルの信頼性は低いと指摘されていた．そのため，過去の個人情報流出に関するインシデントを調査，解析して新たな数理モデルが提案された．しかし，この提案モデルで対象とされた個人情報には，現在，ECHONET Lite でクラスとして定義されている体重計に関するものが含まれていない．よって，山田道洋らによって提案されたモデルより体重の漏えいを考慮している JO モデルの方が被害額の算出式として適正であるとした．

5.2.2 攻撃の発生確率

リスクの発生確率を算出するパラメータはキープロパティの実装の必須 A，アクセスルール R，状態変化時アナウンスの実装の必須 S，キープロパティと危険プロパティの総数 Num がある．ここでは，表 4 にある，それぞれのパラメータの設定値について述べる．

キープロパティの実装必須のパラメータ R は，キープロパティが実装必須であればそのプロパティは確実に実装されており，攻撃に利用される可能性が高いため，必須であるときに値を大きくしている．アクセスルールのパラメータ A と状態変化時アナウンスのパラメータ S では，被害の種類が “プライバシー”かそれ以外で設定値が異なる．

被害の種類が “人”，もしくは “金”であるとき，機器を任意に制御すること，もしくは通信を横取りして偽の情報を送信することで攻撃が成立する．機器の制御は Set コマンドを送信することで実現できる．偽の情報を送信するには，通信を横取りした後でプロパティデータを通知，もしくは他の機器から Get コマンドで要求されたときに応答することで実現できる．機器を制御する攻撃は偽の情報を送信する攻撃と比較して，機器の通信を横取りする必要がないため攻撃が容易である．よって，キープロパティのアクセスルールが Set であるときにパラメータ A の値は大きくなる．また，状態変化時アナウンスが実装されていた場合，値が変化したことが他の機器に通知されるため攻撃されたことを検知できる．状態変化時アナウンスが実装必須であるとき，リスクの発生確率が低減されることからパラメータ S の値を 0.8 とした．

被害の種類が “プライバシー”であるとき，この攻撃目標は情報を読み出すことである．したがって，攻撃は機器に対して Get コマンドを送信してプロパティを読み出すか状態変化時アナウンスによって機器が通知したパケットを受け取ることによって成立する．機器に対して Set コマンドを送信した場合は，プロパティの値が変化するのみであり，機器の情報を読み出すことはできない．そのため，プロパティのアクセスルールが Get のとき，状態変化時アナウンスが実装必須であるときにパラメータ R，S の値を大きくしている．

算定式のパラメータ R，A，S の値はキープロパティの規定によって，表 4 のように決定される．ただし，キープロパティが複数あるとき，算定式に用いるパラメータを選定しなければならない．キープロパティは攻撃シナリオを実現するために最低限必要なものである．つまり，全てのプロパティを制御して初めて攻撃が成立する．攻撃の実現には攻撃難易度が高いプロパティを利用する必要があるため，パラメータ R，A，S の値はそれぞれ値が低いものを選択する．例えば，キープロパティが 2 つあり，それぞれプロパティの実装が必須，任意であったとする．この場合，実装が任意であるプロパティが実装されていなければ攻撃は実現できない．そのため，実装必須のパラメータ R は表 4 より 1 となる．

また，被害の影響では，危険プロパティによる攻撃は考慮されていない．危険プロパティの個数が多いほど攻撃が発生する可能性が高くなる．しかし，危険プロパティを用いた攻撃はキープロパティを用いた攻撃よりも被害の影響が小さいものである．よって，危険プロパティとキープロパティの影響の差を考慮するため，危険プロパティとキープロパティの総数に 0.1 の重みを付ける．ただし，プロパティの個数が 10 未満の場合，0.1 の重みを付けるため値が 1 以下となる．この場合，乗算するとスコアが小さくなりリスクが低減されたかのように捉えることができる．そのため，最低スコアとして 1 を加算する．

5.3 考察

リスク算定式によってリスク分析を行った結果の上位 40

クラスを付録 A.1 に示す．ただし，スコアは小数点以下を切り上げている．付録 A.1 より，各クラスのリスクを定量化することによって，セキュリティ機構を実装する優先順位を考える際の指標を示した．また，スコアの算出例を次に示す．

$$\begin{aligned}
\text{家庭用エアコン} &= 5\cdot 3\cdot 3\cdot 1(1+25\cdot 0.1) \fallingdotseq 158\\
\text{電動シャッター} &= 8\cdot 3\cdot 3\cdot 0.8(1+12\cdot 0.1) \fallingdotseq 127\\
\text{体重計} &= 4\cdot 3\cdot 3\cdot 0.8(1+2\cdot 0.1) \fallingdotseq 35\\
\text{電力量メータ} &= 5\cdot 1\cdot 3\cdot 1(1+4\cdot 0.1) \fallingdotseq 21
\end{aligned}$$

家庭用エアコンは，R，A，S の値が最大値であり，キープロパティと危険プロパティの総数も 25 と全てのクラスの中で 2 番目に大きいため，スコアの順位は 1 位となっている．また，電動シャッターに対してはシャッターの開け閉めの制御による攻撃が可能であるため，人を殺害する可能性がある．逸失利益によって算出した被害総額は 8 桁と全てのクラスで最大値であるため，電動シャッターは上位になっている．これらに比べ，体重計はパラメータ D とプロパティ総数 Num ，電力メータはパラメータ R と Num の数値が小さいため下位にある．このように，全てのクラスに対してリスクの大小の順序を付け，セキュリティ対策の優先度を付けることができた．そのため，スコアが大きいクラスが実装されている機器から順に通信経路の暗号化や送信元認証を行うようセキュリティ対策を施す優先順位が高いことが明確にできた．

また，本研究では，攻撃によって発生する被害が大きいクラスのスコアが高くなることを目的としてリスク分析を行った．特に，人命を落とす可能性があるシナリオが想定されたクラスのスコアが上位になることが望ましいと考えた．付録 A.1 に示した結果を見ると，電動雨戸・シャッター，電動窓などのシャッターや扉を開閉させることで人を殺害する攻撃が想定できるクラスは Score が 100 以上となっており，上位にある．しかし，家庭用エアコンや蓄電池クラスの順位を見ると，これらのクラスでは電力の消費や生産値を変更させる攻撃が想定され，パラメータ D の値は 5 であるにも関わらず，パラメータ D が 8 であり，パラメータ R，A の値が同値である電動シャッターや電動窓クラスよりも順位が高い．これは，家庭用エアコンや蓄電池クラスでは，パラメータ Num の値がそれぞれ 25，28 となっており，全クラスで最上位の値となっているためである．筆者らが考えたリスク算定式では Num の値に 0.1 の重みを付けているが，被害の影響が大きいものを上位にすることを目的とする場合，重みを 0.1 よりも小さくする必要があると言える．しかし，プロパティの実装数が多くなると攻撃に利用されるプロパティが増える．そのため，危険プロパティ数が大きいほど攻撃の発生確率は上昇することから，重みを極端に小さくするべきではない．よって，この重みの適正な値については検討が必要である．

また，攻撃シナリオは筆者が想定したものによるため，攻撃による被害の影響は主観的に定量化されていると言える．攻撃シナリオが異なるとリスクアセスメントの結果は変化する．したがって，攻撃シナリオの想定時に主観性を排除する必要があると言える．

6. おわりに

本研究では，ECHONET Lite に機器間を安全に通信するためのセキュリティに関する規定がなく，下位レイヤでセキュリティ機構を機器に実装する必要があることを述べた．そこで，本研究では ECHONET Lite 対応機器にセキュリティ機構が実装されているか確認することを目的として，実機を用いた調査を実施した．その結果，機器にセキュリティ機構が実装されていないことが判明したため，疑似攻撃を行うことで攻撃によって発生する影響を示した．攻撃された際の被害を考慮すると，ベンダは機器にセキュリティ機構を実装する必要があるが，機器に実装されているクラスによってリスクの影響や発生確率が異なる．そのため，クラスごとにクラスの特徴を考慮した攻撃シナリオを特定し，そのリスクを定量化してセキュリティ機構を実装する優先順位を明らかにした．ただし，このリスクアセスメントは筆者らが想定した攻撃シナリオに依存しており，主観的な視点によって決められていると言える．今後は，想定する攻撃シナリオに客観性を持たせるため，複数の専門家によって想定された攻撃シナリオからリスクアセスメントを行う予定である．

参考文献

[1] Echonet consortium:echonet lite specification 第 1 部 echonet lite の概要，echonet consortium(オンライン), July 6 2018. Version 1.13，閲覧日:2020-10-21.
[2] Echonet consortium:echonet lite specification 第 2 部 echonet lite 通信ミドルウェア仕様, echonet consortium(オンライン), July 6 2018. Version 1.13，閲覧日:2020-10-21.
[3] Echonet consortium:appendix echonet 機器オブジェクト詳細規定 releasen，echonet consortium(オンライン), Sep 25 2020. 閲覧日:2020-10-21.
[4] 城間 政司, 井上 博之．スマートハウス向け情報機器のリスクアセスメントにおける資産導出手法．Technical report, Computer Security Symposium 2017, 2017. 閲覧日:2020-10-26.
[5] Echonet consortium:echonet lite システム設計指針第 2 版 (日本語版)，echonet consortium(オンライン), June 24 2019. 閲覧日:2020-10-21.
[6] 令和元年賃金構造基本統計調査　結果の概況 ＞賃金の推移．https://www.mhlw.go.jp/toukei/itiran/roudou/chingin/kouzou/z2019/dl/01.pdf. 閲覧日:2020-9-20.
[7] 平成 27 年国勢調査 人口等基本集計結果 結果の概要．https://www.stat.go.jp/data/kokusei/2015/kekka/kihon1/pdf/gaiyou1.pdf. 閲覧日:2020-9-20.
[8] 就労可能年数とライプニッツ係数表. https://www.mlit.go.jp/pubcom/01/pubcom63/pubcom63_4.pdf. 閲覧日:2020-9-20.

[9] 《たすけあい》｜医療コース:特長｜加入をご検討の方｜コープ共済. http://coopkyosai.coop/thinking/lineup/tasukeai/medical/feature.html. 閲覧日:2020-9-20.
[10] 従量電灯A料金早見表 [関西電力] ＞２０２０年１１月分. https://kepco.jp/ryokin/unitprice/ju_a_hayami/~/media/B7AB685523204EAABA02AEEA9CFC3E7E.ashx. 閲覧日:2020-9-20.
[11] 最新の料金表(一般料金). https://wwwe5.osakagas.co.jp/custserv/ryokinhyo1001.html. 閲覧日:2020-9-20.
[12] 大阪市水道局：水道料金の仕組みと料金表（水道をお使いの皆さまへ＞水道料金）. https://www.city.osaka.lg.jp/suido/page/0000321790.html. 閲覧日:2020-9-20.
[13] はぴｅタイムＲ｜電気｜関西電力　個人のお客さま. https://kepco.jp/ryokin/menu/hapie_r/. 閲覧日:2020-9-20.
[14] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ. 情報セキュリティインシデントに関する調査報告書 別紙第 1.0 版, p5-11. https://www.jnsa.org/result/incident/data/2016incident_survey_attachment_ver1.0.pdf. 閲覧日:2020-9-20.
[15] 山田道洋, 菊池浩明, 松山直樹, 乾孝治. 個人情報漏洩の損害額の新しい数理モデルの提案. 情報処理学会論文誌, 2018.

付　　録

A.1 リスク分析の結果

順位	クラス名	Score
1	家庭用エアコン	158
2	蓄電池	137
3	電動雨戸・シャッター	133
4	電動シャッター	127
5	電動窓	127
6	浴室暖房乾燥機	126
7	電動ゲート	121
8	電動玄関ドア・引戸	121
9	床暖房	90
10	電気温水器	87
11	電気錠	87
12	散水器 (庭用)	87
13	電気自動車充放電器	70
14	電動ブラインド・日よけ	65
15	炊飯器	63
16	業務用ガスヒートポンプエアコン室内機	61
17	電気自動車充電器	52
18	業務用パッケージエアコン室内機 (設備用除く)	51
19	業務用ショーケース	49
20	食器洗い乾燥機	44
21	オーブンレンジ	41
22	洗濯乾燥機	36
23	体重計	35
24	レンジフード	34
25	クッキングヒータ	34
26	スマート電力量サブメータ	33
27	電気便座	33
28	ファンヒータ	33
29	電気暖房機	30
30	燃料電池	30
31	高圧スマート電力量メータ	27
32	低圧スマート電力量メータ	27
33	水流量メータ	24
34	瞬間式給湯器	23
35	空調換気扇	23
36	電力量メータ	21
37	衣類乾燥機	21
38	Household small wind turbine power generation	20
39	冷凍冷蔵庫	18
40	電気ポット	18