Vol.2020-DPS-182 No.29
Vol.2020-CSEC-88 No.29
2020/3/12

スマート家電に適したPKIの運用方法の考察

山川 大貴[1,a)]　猪俣 敦夫[2]　上原 哲太郎[3,b)]

概要：現在，スマートサービスと呼ばれる様々なシステムやスマートスピーカ等を始めとしたデバイスが我々の生活に急速に普及しつつある．これらの多くは，スマートフォン上のアプリからクラウドを経由して，デバイスの遠隔操作や状態監視のためのセンシング機能等を提供している．さらにインターネットを利用することからその安全性を考慮し，クラウドに存在するサーバとスマート家電等の間の通信にはサーバ認証と内容の秘匿化のためにPKIの仕組みを利用したSSL/TLS通信が使用されていることが一般的である．本研究では，スマート家電における通信方式のセキュリティに着目し，スマート家電の実機を用いた調査を行いその安全性について議論する．スマート家電とクラウドサーバ間で実際にやり取りされている通信を観測したところ，対象としたスマート家電によりPKIの運用方法が異なっていることが判明した．これらの結果を踏まえて各運用方法のリスク分析を行い，今後のスマート家電に適した運用方法について考察を与える．

1. はじめに

近年，様々なものをネットワーク接続しIoT化することで，IoTデバイスから様々なデータを大量に収集することが可能になり，収集したデータを有効活用して新たな価値を提供するスマートサービスという新しいビジネスモデルが誕生した．今回は，スマートサービスの中でもスマートハウスに注目し，ネットワーク接続されているスマート家電のネットワークセキュリティを考える．一般的に外部サーバと通信する際には送信元認証と通信内容の秘匿化のためにTLS通信を利用することが多く，サーバ証明書にはパブリック認証局が発行したものを利用するのが一般的である．TLS通信はPKI(Public Key Infrastructure)を利用し，今まで接続をしたことがない機器同士が通信する際に信頼できる第三者として認証局が送信元の身元を保証していることで成り立っている．しかし，スマート家電は接続先のサーバが事前に決まっているなど，一般的なブラウザとWebサーバのやり取りとは異なる側面があるため，スマート家電に特有の運用要件があると考えた．そこで，本研究では現在のスマート家電がどのようにPKIを運用しているのか調査し，その結果を分析した後，スマート家電に適したPKIの運用方法について考察を与える．

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

2. 研究背景

2.1 スマート家電の動向

総務省の令和元年度版情報通信白書[1]によると，2021年に世界で約448億台のIoT機器が普及すると予測している．IoT製品の例としては，スマートフォンのアプリを利用して遠隔地から家電の稼動状態の確認や機器の操作をできるスマート家電が挙げられる．図1は，スマート家電が企業のクラウドサーバを経由してスマートフォンアプリと通信する例を示す．スマートフォン・スマート家電とクラウドサーバ間の通信はスマート家電の操作命令や機器の状態の情報などのやり取りに使用される．そして，各通信には利用者のプライバシーの観点から，送信元の認証と通信内容の秘匿化のためにPKIの仕組みを利用したSSL/TLS通信が利用されていることが多い．

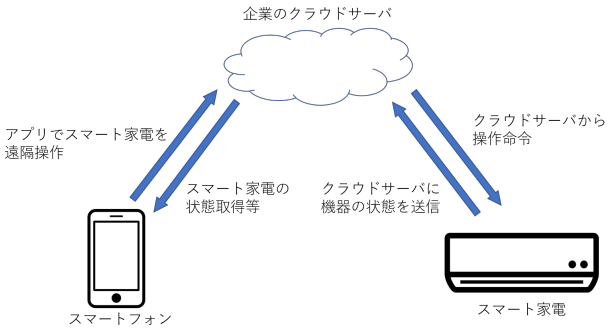

図 1 スマート家電のモデル図

2.2 サーバ証明書の更新ミスの事例

サーバ証明書に適用されている暗号アルゴリズムの危殆化を考慮した上で，暗号鍵の鍵長サイズや有効期限を設定する必要がある．また，CA/Browser Forum の Baseline Requirements は 2018 年 3 月 1 日以降に発行するサーバ証明書の期限を 825 日よりも短くすることを定めている [2]．しかし，人為的なミスやシステム構成が問題でサーバ証明書が更新されず，期限切れを起こすことでシステム障害の発生に繋がる可能性がある．サーバ証明書の更新ミスが原因で発生したシステム障害の事例を 2 件取り上げる．1 つ目は 2018 年 12 月 6 日に発生したソフトバンク社の約 3060 万回線に及ぶ大規模な通信障害である [3]．原因はコアネットワーク内のエリクソン製の MME(Mobility Management Entity) で利用されていた証明書の期限切れであった．ソフトバンク社が緊急的な対処として，TLS 通信を利用していないバージョンにダウングレードしたことにより，通信障害は復旧している．2 つ目は 2018 年 11 月 24 日に発生した 144Lab 社のうんこボタンの不具合である [4]．144Lab 社がサーバ証明書の更新を忘れたことが原因で証明書の有効期限が切れたため，機器とサーバ間の通信ができなくなった．通常は新しいサーバ証明書を更新するだけで通信は回復するが，今回の事例ではサーバ証明書のフィンガープリントを機器にハードコードしていたため，通信の復旧ができなかった [5]．さらに，ファームウェアアップデートにも TLS 通信を利用していたため，直接ファームウェアを書き換える方法しかなく，不具合に対して全品回収という対応を取っている [6]．

2.3 サーバ証明書の検証ミスの事例

PKI による送信元認証では，サーバ証明書の署名を証明書の発行者である認証局の公開鍵で検証して，サーバ証明書の公開鍵が証明書の作成者 (Subject) のものであることが保証されていることが大切である．しかし，現実には実装に置いてサーバ証明書の公開鍵が適切に検証されていない場合がある．日本テレビ放送網が提供する Android アプリ “日テレニュース 24”や iOS 版 LINE でサーバ証明書の検証不備による脆弱性が発見された．[7][8] このように，サーバ証明書の検証が正しく行われていない場合，不正なサーバ証明書を利用した中間者攻撃が成立する．

2.4 関連研究

武田ら [9] は 2007 年当時の情報セキュリティに関する最新動向をまとめているが，その中でスマート家電のセキュリティについて分析を行っている．はじめに，スマート家電を機能別にグループ分けし，機器をインターネットに接続した場合に想定される脅威を列挙した後，脅威に対抗するために必要な対策を述べている．その後，新たなセキュリティアーキテクチャとして，ネットワークオペレータによるスマート家電のセキュリティ管理を提案しており，利便性を高めるために家電メーカに機器の遠隔操作と管理が可能となるアプリケーションの開発を提言している．武田らの提案方法はスマート家電の利用者がセキュリティの知識を持たないことを前提とした上で，ネットワークセキュリティの管理を専門家に委託し，スマート家電の操作等を利用者が遠隔操作できるように提案していることから，図 1 のような，現在のスマート家電の通信モデルに似ているものであると言える．Daniel ら [10] は 2009 年 8 月に Marsh Ray が発見した安全でない再ネゴシエーションを悪用した中間者攻撃や 2011 年に Duorg と Rizzo により発見された BEAST 攻撃など，今までの SSL/TLS プロトコルに対する攻撃について解説している．その後，PKI の仕組みや計算機の計算能力の向上によって認証局の鍵長に必要なビット数が増えてきたことを示しながら，SSL/TLS プロトコル・PKI 全体の変遷について述べている．そして，PKI の信頼性を強化するための方法として，証明書のピンニング技術を取り上げ，様々な側面から各ピンニング技術を分析している．論文内で比較しているピンニング技術を以下に示す．

- Certificate Transparency
- Sovereign Keys
- Trust Assertion for Certificate Keys
- Certification Authority Authorization
- HTTP Strict Transport Security and HTTP Public Key Pinning Protocol
- DNS-Based Authentication of Named Entities

様々な状況を仮定し，IoT 機器の特徴を考慮した上で各ピンニング技術を比較した結果，各運用や管理コストの側面から DANE を利用するのが良いと結論づけている．Daniel らはパブリック認証局を利用しつつ，セキュリティを強化する方法を模索していたが，本研究ではメーカが独自のプライベート認証局を運用する場合についても着目し，それも併せて分析している．

3. 予備実験

本研究でスマート家電に適した PKI の運用を考えるために，普段スマート家電が通信している企業のクラウドサーバがどのようなサーバ証明書を利用して TLS 通信を行っているのか知る必要がある．そこで，予備実験としてスマート家電と通信しているサーバ証明書の情報を異なるメーカ A 社，B 社の機器から取得した．取得するために構築した実験環境を図 2 に示す．スイッチングハブのポートミラーリング機能を利用し，スマート家電とクラウドサーバ間の通信内容を観測することにした．観測結果より，スマート家電と接続しているクラウドサーバの IP アドレスが判明するため，OpenSSL の TLS 通信のクライアント機能を使用して，クラウドサーバのサーバ証明書を取得する．

取得したサーバ証明書の情報を調査したところ，A 社はパブリック認証局に署名されたサーバ証明書，B 社は信頼できる第三者ではなくメーカのプライベート認証局に署名されたサーバ証明書であった．また，パブリック認証局に署名された A 社の証明書は約 2 年間，プライベート認証局に署名された B 社の証明書は約 20 年間の有効期限が設定されており，A 社と B 社の証明書の運用方法が異なるため，各運用方法をスマート家電に適用した場合の分析をすることにした．

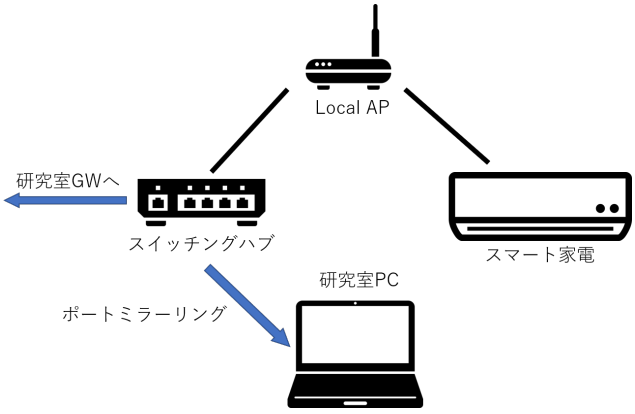

図 2　予備実験の環境

4. スマート家電に適用された証明書の解析

4.1 パブリック認証局に署名された証明書の特徴

本章では，パブリック認証局に署名されたサーバ証明書をスマート家電との通信に利用している場合の長所と短所を述べる．

4.1.1 長所

パブリック認証局を利用している場合の長所を下記に示す．

(1) 証明書の発行元 (トラストアンカ) が一般的な信頼を得ている
(2) 最長 825 日で更新が必要なため，定期的に暗号アルゴリズム等の見直しができる

(1) は証明書チェーンの最上位に位置するトラストアンカが証明書利用者が定めているルート CA 証明書プログラムの元で運用されているので，一般的な信頼を得ていることを示す．ルート CA 証明書プログラムの例として Mozilla 社の Mozilla Root Store Policy[11] を紹介する．Mozilla Root Store Policy の中で認証局に対して，第三者機関である WebTrust for CA や ETSI の監査を受けることを要求している．

(2) は CA/Browser Forum の Baseline Requirements[2] に規定されているサーバ証明書の有効期限が 825 日であるため，更新のタイミングで暗号アルゴリズム等の見直しができるので，証明書が危殆化する前に更新を行えることを示す．

4.1.2 短所

パブリック認証局を利用している場合の短所を下記に示す．

(1) 証明書の発行と更新に費用がかかる
(2) 短いライフサイクルで証明書を運用するので更新ミスの危険性がある

(1) は商用の認証局から発行されるサーバ証明書を利用する場合，証明書の発行と更新時に費用がかかることである．

(2) は最長でも 825 日という期間でサーバ証明書を更新する必要があるため，2.2 節で紹介したような更新忘れによって発生する通信障害が起こる可能性が高いことを示す．また，結果的に否決されたが，Google 社は現行の最長 825 日よりさらに短い期間を定めるように Baseline Requirements の改定の提案を行っており，今後も証明書の有効期限の短縮が議論に上がる可能性はある [12]．

4.2 プライベート認証局に署名された証明書の特徴

本章では，プライベート認証局に署名されたサーバ証明書をスマート家電との通信に利用している場合の長所と短所を述べる．また，証明書の有効期限は十分に長い期間が設定されているものとする．

4.2.1 長所

プライベート認証局を利用している場合の長所を下記に示す．

(1) 証明書の発行や更新にかかる費用が無料
(2) 長いライフサイクルで証明書を運用するので更新ミスの危険性が低い
(3) クライアント側でプライベート認証局の証明書のみ保持して運用する場合，攻撃される可能性のある範囲を限定できる

(1) は証明書の発行を自社で行うので，OpenSSL[13] を利用してプライベート認証局を作成することが考えられる．そして，OpenSSL はオープンソースであるため，証明書の発行や更新時に費用がかからない．

(2) はプライベート認証局で発行する証明書の有効期限は自社で決められるため，証明書の有効期限を長く設定できることを示す．今回，取得した B 社の証明書には有効期限が 20 年間に設定されていた．つまり，証明書を発行してから 20 年間の間は証明書作成時に利用している暗号技術が危殆化しない限り，証明書を更新する必要がない．したがって，2.2 節で紹介したようなサーバ証明書の更新ミスによる通信障害が起こる可能性を低下させることができる．

(3) は，サーバ証明書の発行にかかわる可能性のあるパブリック認証局はルート認証局と中間認証局を合わせると数多く存在する．そして，認証局も攻撃を受ける可能性があり，攻撃される恐れのある範囲は広いと言える．一方で，プライベート認証局の証明書のみ保持して運用する場

合，サーバ証明書の発行者は一意に決まるため，認証局の証明書が攻撃を受ける範囲は限定される．このように認証局を指定し証明書チェーンを限定することで，不正な証明書を利用した中間者攻撃を防ぐ技術として HPKP(HTTP Public Key Pinning) がある [14].

HPKP はクライアント側に証明書チェーン上の証明書の公開鍵を保持させ，再び Web サーバと接続するときに提示された証明書チェーン上に自身が持っている公開鍵情報と一致する情報が存在しているか確認することで，不正な証明書を利用した中間者攻撃の対策を行っている．初めてクライアントがサーバに接続するときには，サーバが HTTP レスポンスヘッダに証明書チェーン中の中間認証局の証明書などの公開鍵情報と Web サーバを紐付ける情報を付与し，クライアント側に一定期間記憶させている．しかし，HPKP の欠点として，証明書の更新によってピンニングの値が変わる場合は新しいピンニングを設定する必要があり，運用を間違えると古いピンニングの値をクライアントが持っている間は通信ができないという問題点がある．さらに，ピンニングの有効期限が切れたタイミングで，ドメインの乗っ取り等により攻撃者が用意した正規ドメインの偽 Web サイトを作成された場合，偽 Web サイトのピンニングをクライアントに保存される危険性もある．一度，保存された偽 Web サイトのピンニング情報は有効期限が切れるまで，クライアント側で保存されているので，乗っ取られたドメインで作成された Web サイトにしか接続できない状態になる．Google 社は HPKP の危険性を考慮した結果，Chrome72 から HPKP のサポートを廃止している [15].

今回のプライベート認証局を利用した TLS 通信も，クライアント側で保持しているプライベート認証局の証明書の更新ミスが発生した場合は TLS 通信ができなくなるため，更新作業を適切に行うことが大切となる．また，万が一証明書の更新ミスが発生した場合はクライアント側が保持している証明書の入れ替えをスムーズにできるような仕組みが必要である．

4.2.2 短所

プライベート認証局を利用している場合の短所を下記に示す．

(1) 証明書に利用している暗号技術が危殆化する可能性
(2) 発行している証明書の信頼性が担保できないこと
(3) 送信元が詐称される可能性

(1) は証明書のライフサイクルを長くするので，証明書の運用中にコンピュータの性能向上や暗号技術に新しい脆弱性が発見される可能性があることを表す．そのため，使用している既存の証明書を脅かすような情報の収集を常に行い，証明書が危殆化した場合に既存の証明書を失効させ，新しい証明書に更新できるような仕組みを持っておく必要がある．

(2) はプライベート認証局であるため，パブリック認証局に求められている監査プログラム等を受けることを強制されていない．したがって，認証局の運用方法や発行している証明書の質はプライベート認証局を運用している会社に依存している．

(3) はプライベート認証局が発行している証明書の署名検証をするために，本来クライアント側が持っておくべきプライベート認証局の証明書を保持しておらず，適切な証明書検証を行っていない場合は送信元の詐称ができる可能性があることを示す．つまり，正規の証明書のフィールドを模倣した偽の証明書を用いて，クライアントに対して普段接続しているサーバになりすました中間者攻撃を行えるということである．もし，攻撃が成功した場合はクラウドサーバとやり取りしている暗号化された通信内容の漏洩や改ざんをされる恐れがある．

5. 追加実験

本研究ではプライベート認証局に署名されたサーバ証明書を利用して TLS 通信を行っているスマート家電に対して追加実験を行った．実験の内容は普段使用しているサーバ証明書のフィールド情報を限りなく似せた証明書を作成し，利用することで企業サーバになりすました通信を行い，スマート家電がどのような挙動をするのか観測した．

5.1 実験方法

第 3 章の予備実験で取得したサーバ証明書のフィールドをもとに OpenSSL[13] を用いて偽のサーバ証明書を作成した．正規のサーバ証明書と偽のサーバ証明書のフィールドの相違点を表 1 に示す．プライベート認証局やサーバの鍵情報が必要なフィールド (Subject Public Key Info など) 以外はフィールド情報を正規のサーバ証明書と同一にすることができた．したがって，認証局の公開鍵を用いた署名検証を行っておらず，サーバ証明書の Subject や Issuer フィールドで正規の証明書かどうかを判断している場合，今回作成した証明書を正規の証明書だと誤認して TLS コネクションが成立する．

その後，偽サーバ証明書を利用した通信を対象のスマート家電と行うために，作成した実験環境を図 3 に示す．スマート家電と研究室 PC を直接接続する必要があったため，研究室 LAN 内に新しい LAN 環境を構築した．Raspberry Pi 内では dnsmasq[16] を使用して，DHCP サーバと DNS サーバを動かしている．そして，DNS サーバの設定で企業のクラウドサーバのドメイン名と研究室 PC の IP アドレスを紐付けすることで，スマート家電から研究室 PC に対して接続試行するようになる．研究室 PC 内ではオープンソースの Web サーバである Nginx[17] を利用している．Nginx の設定で作成した偽サーバ証明書を指定することで，スマート家電からの Client Hello に対して偽サーバ証明書

表 1 作成した証明書と実際の証明書との対応表

証明書のフィールド	作成した証明書との相違
Version	○
Serial Number	○
Signature Algorithm	○
Issuer	○
Validity	○
Subject	○
Subject Public Key Info	鍵を作成するアルゴリズムのみ正規の証明書と同一にできた
X509v3 extensions	証明書の拡張要素は正規の証明書と同一にできたが値は異なる

の提示をするようにした．

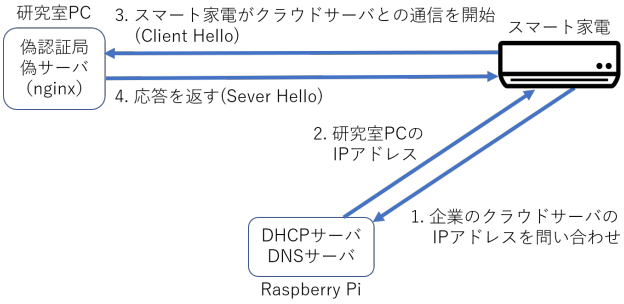

図 3 追加実験の環境

5.2 実験結果

図 3 の実験環境で観測したパケットの概要を図 4 に示す．通信プロトコルは TLS のバージョン 1.2 であった．最初はスマート家電から研究室 PC に対して Client Hello メッセージが送られ，サーバから Sever Hello メッセージや証明書情報が格納されている Certificate メッセージ等が返答される．しかし，図 4 に示しているとおり，サーバからのパケットを受け取った直後にスマート家電は RST パケットを送信している．そのため，5.2 節で危惧していた企業のサーバになりすました通信は成功しなかった．したがって，サーバ証明書の検証が正しく行われていることが判明した．Alert メッセージを送信せずに RST パケットを送っているのは，スマート家電の製造元の実装方法に依存していると考えられる．

6. スマート家電に適した PKI の運用

本研究では，スマート家電に適した PKI の運用として，各メーカーがプライベート認証局を運用し，自社のプライベート認証局が発行した証明書を利用した TLS 通信を行うことを提案する．さらに，プライベート認証局を運用すると，発行するサーバ証明書の期限を自社で決められるため，スマート家電のライフサイクルより長い期限を設定することで，サーバ証明書の更新ミスの可能性を減らせるようになる．また，サーバ証明書の検証のためにスマート家電内にトラストアンカとしてプライベート認証局の証明書を保持することをピンニングと呼ぶことにする．理由はサーバとスマート家電間の TLS 通信で使用する証明書を発行する認証局を固定しているからである．

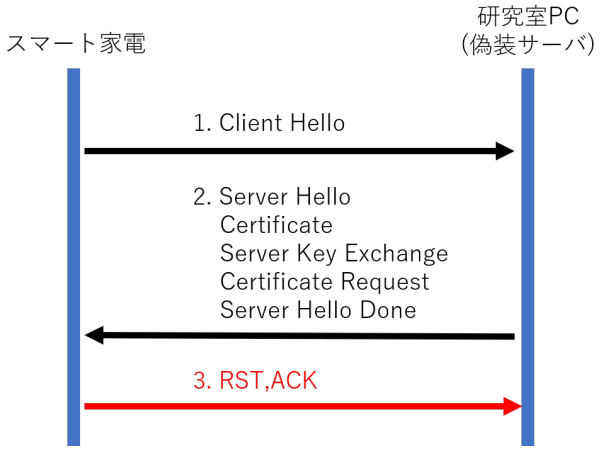

図 4 観測した TLS 通信の概要

6.1 運用する際に必要な要素

スマート家電に適した PKI の運用をする際に必要な要素を下記に示す．

(1) 長期間耐性のある暗号技術を利用した証明書の作成
(2) プライベート認証局の秘密鍵を厳重に管理
(3) プライベート認証局の証明書が危殆化した際に，スマート家電にピンニングされた証明書をアップデートできる環境の提供

(1) は更新ミスの危険性を減らすために，長期間有効なサーバ証明書を発行するので，プライベート認証局の自己署名証明書と認証局が発行するサーバ証明書に使用する暗号技術も証明書の危殆化対策として，長期間耐性のあるものを選ぶ必要があることを示す．サーバ証明書に使用する暗号技術を検討する際には，CRYPTREC の暗号技術評価委員会が毎年公開している報告書を参照し，電子政府推奨暗号リストなどから選ぶと良い [18]．特に，プライベート認証局の鍵長は十分な長さを持つべきである．

(2) はプライベート認証局の秘密鍵が危殆化すると，運用している PKI の仕組み全体に影響が及ぶため，厳重に管理しなければいけないことを表す．そのため，認証局の秘密鍵の管理に HSM(Hardware Security Module) を利用するなど，鍵の管理方法をよく考える必要がある．

(3) はプライベート認証局の証明書が有効な間に，何らかのアクシデントでプライベート認証局の秘密鍵が漏洩した場合や量子コンピュータの登場により，使用している暗号アルゴリズムに対する計算能力が想定外に向上することで，証明書が危殆化する可能性がある．プライベート認証局の証明書が危殆化すると，スマート家電は攻撃者に

よって接続されてしまうため，普段の暗号化された通信内容が漏洩してしまう．したがって，プライベート認証局の証明書が予期せず危殆化した際に，プライベート認証局の証明書を即座に作り直し，同時にスマート家電にピンニングされている証明書も更新する必要がある．一般的に IoT 機器は OTA(Over The Air) アップデートにより，ファームウェアを更新している．スマート家電にピンニングされている証明書を更新するときにも OTA アップデートを用いることが自然であると考えられるが，特に重要なことはアップデート内容の完全性の確保である．そこで，本研究ではファームウェアアップデートのバイナリの完全性を保証するために電子署名を行うことを提案する．この際，OTA アップデートに使用するキーペアは複数用意し，スマート家電に公開鍵を持たせることで，いずれかの公開鍵を用いた署名検証ができるようになる．

7. おわりに

本研究では，はじめにスマート家電の基本的な通信のモデル図を示し，クラウドサーバとスマート家電間で PKI の仕組みを利用した TLS 通信が利用されていることを述べた．そして，TLS 通信で使用されるサーバ証明書の更新ミスや検証ミスの事例を挙げ，一般的に利用されているパブリック認証局を利用した PKI の運用が難しいことを示した．予備実験として，スマート家電とクラウドサーバ間でどのような通信が行われているか観測したところ，自社のプライベート認証局が発行した証明書を利用している機器とパブリック認証局が発行した証明書を利用している機器があることがわかった．そこで，プライベート認証局を利用した場合とパブリック認証局を利用した場合のそれぞれの特徴を長所と短所に分けて整理し，スマート家電に適した PKI の運用方法を考察することにした．その結果，あらかじめ送信元と送信先が決まっているスマート家電においては各メーカーでプライベート認証局を運用し，プライベート認証局が発行したサーバ証明書を利用することを推奨し，その根拠について述べた．今後は，スマート家電だけではなく IoT 機器全般が PKI の運用をどのように行っているか傾向を知るために，多種多様な IoT 機器とクラウドサーバ間でやり取りされている通信を観測する予定である．また，今回扱ったスマート家電以外の IoT 機器で，機器が普段通信を行っているサーバが利用しているサーバ証明書を模倣し，第 6 章のようにクライアントに対して中間者攻撃を行い挙動を確認することで，証明書検証を正しく行っているのか確認する予定である．

参考文献

[1] 総務省:令和元年度版情報通信白書，総務省 (オンライン)．https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/pdf/01honpen.pdf．閲覧日:2020-2-9.
[2] CA/Browser Forum:Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum(Online). https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.7.pdf. 閲覧日:2020-2-11.
[3] ソフトバンク株式会社:ソフトバンク株式会社 上場記者会見，YouTube(Online). https://www.youtube.com/watch?v=Gu7xMCllCbM. 閲覧日:2020-2-12.
[4] 株式会社 144Lab:うんこボタン，うんこボタン (Online). https://unkobtn.com/. 閲覧日:2020-2-12.
[5] 高橋睦美:IT の過去から紡ぐ IoT セキュリティ:ソフトバンク障害は “他人事”ではないデジタル証明書のヒヤッとする話 (3/3), ITmedia(Online). https://www.itmedia.co.jp/news/articles/1812/21/news038_3.html. 閲覧日:2020-2-18.
[6] はなまる:うんこボタンのブログ うんこボタン不具合のお詫び，Ameba(Online). https://ameblo.jp/unkobtnmom/entry-12421736847.html. 閲覧日:2020-2-12.
[7] JVN:JVN#01236065 Android アプリ「日テレニュース 24」における SSL サーバ証明書の検証不備の脆弱性，JVN(Online). https://jvn.jp/jp/JVN01236065/. 閲覧日:2020-2-16.
[8] JVN:JVN#75453852 iOS 版 LINE における SSL サーバ証明書の検証不備の脆弱性，JVN(Online). https://jvn.jp/jp/JVN75453852/index.html. 閲覧日:2020-2-16.
[9] 武田 圭史，Nicolas CHRISTIN, Davar PISHVA. 情報セキュリティに関する取り組みについての最新動向. 知能と情報 (日本知能情報ファジィ学会誌), Vol. 19, No. 3, pp. 200–208, 2007.
[10] Daniel Díaz-Sánchez, Andrés Marín-Lopez, Florina Almenárez Mendoza, Patricia Arias Cabarcos, and R. Simon Sherratt. TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications. *IEEE Communications Surveys and Tutorials*, Vol. 21, No. 4, pp. 3502–3531, oct 2019.
[11] Mozilla:Mozilla Root Store Policy, Mozilla(Online). https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/. 閲覧日:2020-2-14.
[12] CA/Browser Forum:BALLOT SC22-REDUCE CERTIFICATE LIFETIMES[V2], CA/Browser Forum(Online). https://cabforum.org/2019/09/10/ballot-sc22-reduce-certificate-lifetimes-v2/. 閲覧日:2020-2-11.
[13] The OpenSSL Project:OpenSSL Cryptography and SSL/TLS Toolkit, OpenSSL(Online). https://www.openssl.org/. 閲覧日:2020-2-15.
[14] IETF:Public Key Pinning Extension for HTTP, RFC7469(Online). https://tools.ietf.org/html/rfc7469. 閲覧日:2020-2-18.
[15] Google, Remove HTTP-Based Public Key Pinning (removed), Chrome Platform Status(Online). https://www.chromestatus.com/feature/5903385005916160. 閲覧日:2020-2-19.
[16] Simon kelley:Dnsmasq, Dnsmasq(Online). http://www.thekelleys.org.uk/dnsmasq/doc.html. 閲覧日:2020-2-16.
[17] F5 Networks,inc:Nginx Port of F5, Nginx(Online). https://www.nginx.com/. 閲覧日:2020-2-16.
[18] CRYPTREC:暗号技術評価委員会 (2013˜), CRYPTREC(Online). https://www.cryptrec.go.jp/eval_cmte.html. 閲覧日:2020-2-18.