重要 IoT デバイスへの PKI 電子認証の実装

ーセキュア IoT 基盤が形成するトラストチェーンー

松本 義和[†*]　辻井 重男[‡]　白水 公康[†]　瀬瀬 考平[†]

概要：IoT 機器のライフサイクルマネジメントの実現に向けて，PKI 電子認証の技術を用いた Trust Anchor と Root of Trust の検証を進めてきた．半導体などの専用チップに安全に鍵を書き込み，その鍵を繋ぎ合わせていくことでデバイスのトレーサビリティを実現できる．信頼される認証局が鍵を管理していくことで信頼の鎖，すなわちトラストチェーンが形成される．AI やビッグデータと連携して次世代 ICT を形成する IoT 機器の，製造から廃棄に渡るライフサイクルをトラストチェーンで実現していくための技術的な実装を提案する．

キーワード：IoT，PKI，電子認証，セキュリティ，トラストチェーン

Implementing PKI Electronic Certification on Critical IoT Devices

Yoshikazu Matsumoto[†]　Shigeo Tsujii[‡]　Kimiyasu Shirouzu[†]　Kohei Sese[†]

Abstract: To realize the life cycle management of IoT devices, we have been verifying Trust Anchor and Root of Trust using PKI digital authentication technology. Device traceability can be realized by writing keys securely on dedicated chips such as semiconductors and connecting the keys together. A chain of trust, that is a trust chain, is formed by a trusted certificate authority managing the keys. We propose a technical implementation to realize the life cycle from manufacturing to disposal of IoT devices that form next-generation ICT in cooperation with AI and big data in a trust chain.

Keywords: IoT, PKI, Digital Authentication, Security, Trust Chain

1. 求められるモノの認証（以下、課題）

1.1 IoT 機器がもつ潜在的な脆弱性

IoT（Internet of Things）機器は，単体の機能に加え，インターネットを介したサービスと連携する．インターネットには常に多くの脅威が存在し, PC やモバイル端末で経験してきたセキュリティ対策のほぼ全てが IoT 機器にも必要といえる．IoT 機器への直接的な攻撃に加え，IoT サービスへの攻撃や IoT 機器を利用した攻撃など，今後新たな攻撃手法が次々と登場してくることが想定できる．

①IoT 機器への攻撃
- プログラムの改ざん
- リバースエンジニアリング

②IoT サービスへの攻撃
- データ盗聴
- データ改ざん
- IoT 機器のなりすまし
- 架空デバイスによるなりすまし

③複合的な攻撃
- 乗っ取られた機器による DDoS 攻撃

これらの攻撃は，IoT 機器がもつ潜在的な脆弱性を狙ったものが多い．インターネットの脅威に対する IoT 機器のセキュリティ機能の欠落，すなわち防御機能がない IoT 機器が続々と生産され続けていることにある．

1.2 IoT サービスに対する脅威と対策例

IoT 機器を利用した IoT サービスでは，インターネットの利用に対するセキュリティ対策に加え，当然ながら IoT 機器そのものへのセキュリティ対策も必要となる．代表的な脅威と，これに対する対策例をまとめる．

† 一般社団法人セキュア IoT プラットフォーム協議会
Secure IoT Platform Consortium.
‡ 中央大学研究開発機構
Chuo University. Research and Development Initiative.
* yoshikazu.matsumoto@cybertrust.co.jp

© 2019 Information Processing Society of Japan

①データに対する脅威

データ盗聴	脅威	プライバシー情報の漏洩
	対策	位置情報，バイタル情報，監視映像，収益情報などのプライバシー情報は，通信路の暗号化により保護
データ改ざん	脅威	クラウドサービスに送信されるデータを改ざんし，クラウドサービスの誤動作や不正アクセスに利用する．
	対策	送信データに対して電子署名を行うことにより，データの真正性を担保する
デバイスのなりすまし	脅威	機器のなりすましにより，センサーから故意に正常/異常信号を送信し，動作を妨害する
	対策	デバイス証明書等，なりすましが困難な方式による認証を推奨 ※製造番号，機器固有番号（UUID,IMEI 等），MAC アドレス等は，容易になりすましが可能

②プログラムに対する脅威

プログラム改ざん	脅威	プログラムの改ざん，不正プログラム混入により，制御の乗っ取り，データの盗聴が可能となる
	対策	プログラムは，電子署名により，改ざん防止を施すとともに，製造元の正当性も評価した上で更新する
プログラムの漏洩	脅威	制御プログラムが悪意ある第三者に渡った場合，制御ノウハウ等，企業機密の漏えいや，リバースエンジニアリング等により，内部構造，認証機構が解析され，攻撃に利用される
	対策	正規のデバイス以外からの制御プログラムの取得要求を拒否すべく，厳密な認証を行う．

③インターネットサービスに対する脅威

不正デバイス接続	脅威	悪意ある第三者によるクラウドサービスへの接続を許した場合，脆弱性を突いた攻撃により，クラウドサービス上の情報漏えいにつながる恐れがある
	対策	正規のデバイス以外からのサービスへのアクセスを拒否すべく，厳密な認証を行うことを推奨する

④IoT 機器に対する脅威

IoT 機器への攻撃	脅威	脆弱性を突いた攻撃等により，IoT 機器へ侵入し，機器のなりすまし，データや認証情報，プログラム情報の盗難，機器の不正操作を行う
	対策	FW・WAF によるアクセス制限，IPS・IDS による侵入検知，防御，セキュアブート，改ざん検知機構，マルウェア対策による不正プログラム検知，監視機構による異常検知・通知・動作停止，OTA による脆弱性対策プログラムの配付等が挙げられる また，物理侵入への対策としては，耐タンパ技術の適用が挙げられる

1.3 IoT 機器特有のセキュリティ上の課題

PC やモバイルデバイスと比較して，IoT 機器には特有のセキュリティ上の課題がある．まずはほとんどの IoT 機器は低リソースであり，高いスペックが要求されるセキュリティ機能が実装できない．難解な課題といえるが，対策としては，IoT ゲートウェイ等により段階的な保護を実現することが有効ではないだろうか．ログ解析や攻撃分析などはクラウドなどのリソースを活用するなど，IoT 機器単体での対策ではなく，複合リソースによるセキュリティ実装が現実的といえる．また，IoT 機器の多くは無人運転（自動稼働）であり，攻撃に対して被害に気が付きにくいという特性をもつ．遠隔監視やセキュリティパッチの適用などが効果的といえるが，個体を管理していくには大幅にコスト上昇してしまう．より強固なセキュリティ対策が求められる中，頑丈な筐体に加え，個体識別ができる要素が必要になってきている．

2. RoT の実現

2.1 RoT の要件

RoT（信頼の起点：Root of Trust）とは，機器の信頼性を保証するためのハードウェアおよびソフトウェアのコンポーネントを指す．NIST（アメリカ国立標準技術研究所）では，RoT の要件を以下のとおり定義している．

・攻撃に対し，安全な設計がされていること
・小さく，かつ，保護されていること
・ハードウェアで保護することが望ましい

また，RoT は以下のセキュリティ上重要な機能を提供する．

・ソフトウェアの正当性検証
・暗号鍵を保護する
・デバイス認証を実行する

このため，必然的に PKI による実装が現実的であり，結

果的にリーズナブルな構築が実現できる．

3. RoT の実装モデル

3.1 要件を満たす H/W の選定

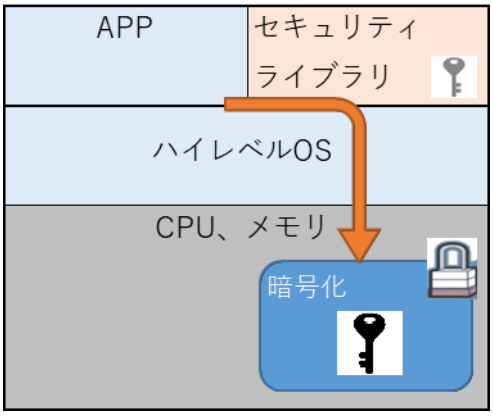
RoT を実現するにあたり，運用も含めた機能要件を整理する．ここでは IoT 機器を制御する OS と，この OS を起動させるためのブート機能，耐タンパ機能といった IoT 機器に特有の要件が登場する．機器の大小や機能面での差分は考慮せず，多くの IoT 機器に共通なものを列挙する．

- SoC システムレベルのブートより前に，Secure HW RoT からのブートが行われること→「HW Secure Boot」
- オンチップ/オフチップの書換え不可なメモリ上で，機密データを保護する機能が提供されること
- 製造時のセキュリティ保護のために，HW RoT によって保護されている「テスト」モードによる，HW ブートをサポート
- 機能/データのプロビジョニングに対する信頼の委任を可能にする（信頼関係のない二者間の信頼を確立する）
- 認証されたサービス/アプライアンス間のセキュアな双方向通信機能を提供すること
- 接続されたデバイスのプロビジョニングと管理を行う機能

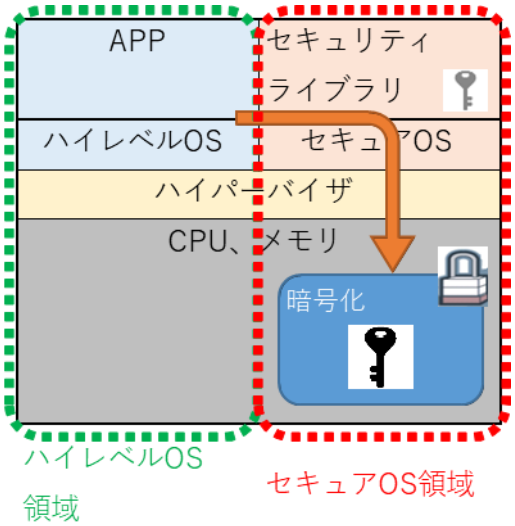
3.2 RoT の実装

RoT の実装は OS の構成によって大きく 3 種類のモデルで実現できる．それぞれのセキュア領域にクレデンシャル（秘密鍵）を搭載し，不正な利用からの防御も可能とした．

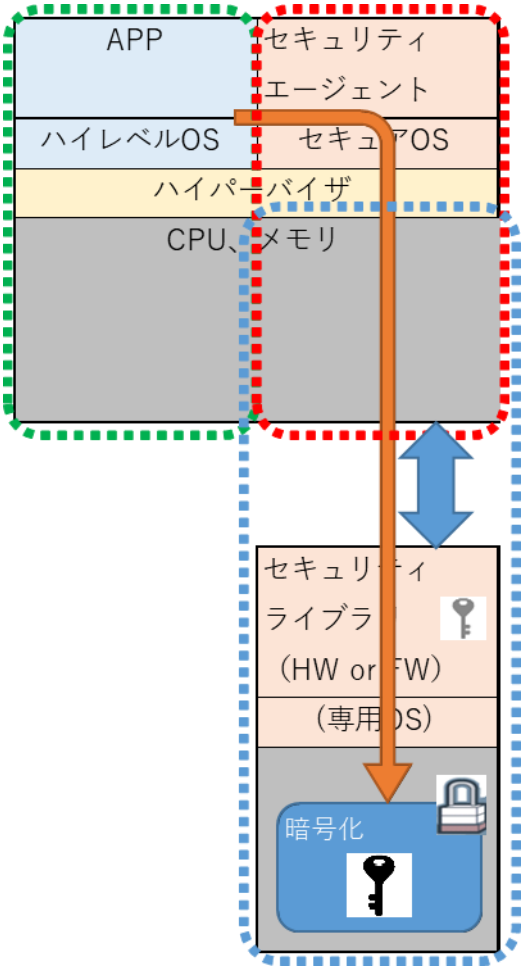
①シングル OS 構成 : OS のアクセス制御で保護し，セキュリティライブラリを乗っ取られた場合，暗号鍵を取り出すことが可能



②仮想 OS 構成：ハイパーバイザーのアクセス制御で保護し，ハイパーバイザーを乗っ取られた場合，暗号鍵を取り出すことが可能



③HW セキュア領域 : HW が独立しており，SW レベルの乗っ取りでは暗号鍵をとりだすことができない



4. ３つの鎖（チェーン）

4.1 トラストチェーン（要素）

トラストフレームワークには，信頼の起点を保証する Trust Anchor が存在する PKI に基づくトラストモデルと，特定の権威に依存せずネットワーク上で台帳を共有する集

合によりトラストモデルを形成するブロックチェーンが存在する.攻撃者がトラストフレームワークを攻撃するとき，PKI におけるトラストモデルには Trust Anchor となる認証局の可用性を損なわせたり認証局の秘密鍵そのものを詐取したりするなどが考えられ，またブロックチェーンのトラストモデルにはネットワーク上の多数の台帳を攻撃する必要がある．いずれも極めて困難な攻撃手法となるが，実現不可能ではない.

PKI に基づくトラストモデルにおいて，電子証明書を発行する認証局がユーザーや検証者にとって信頼できるのもかが重要になってくる．認証局が悪意をもつ者に運営され，悪用のための電子証明書が発行されてしまった場合，ユーザーも含め検証者はこれが正しいものかを見極めるための手段をもつ必要がある．SSL/TLS では，多くのインターネットブラウザが信頼のできる認証局の情報を予めアプリケーションに組み込むことで幅広いユーザー層にセキュリティ機能を提供している．また，WebTRUST の規格も広がりを見せており，Web サイトが能動的に安全であることをアピールしている．このように安全な Web サイトと危険な Web サイトを視覚的な効果でユーザーに知らしめる仕組みには電子証明書が使用される．WebTRUST による厳格な審査によって，悪意をもつ者には信頼されている認証局からは電子証明書を発行できない. したがって WebTRUST の認定を受けている認証局は Trust Anchor になりうる．Root 認証局と中間認証局などで構成される多段階構造のトラストモデルでは，上位の認証局が下位の認証局を信頼することで「信頼の連鎖（トラストチェーン)」を形成している．これに WebTRUST の認定が加わることで, 悪意のない信頼できるトラストチェーンが完成する．トラストチェーンは，ユーザーと検証者に対し，第三者機関である認証局が信頼を保証する. IoT デバイスの RoT に格納される Trust Anchor がトラストチェーンであるためには,

・RoT からトラストアンカーが取り出せないこと

・不正が発覚した場合に，ただちに失効できること

となり，この２点を同時に満たすことで，当該の RoT は世の中にただ一つの Trust Anchor を持ち，信頼のできる認証局から発行されたと証明できる.

4.2 ブロックチェーン（技術）

ブロックチェーンでは，利用者の認証に加え，利用者の識別，トランザクションの認可（承認）に非対称鍵暗号を利用している．ブロックチェーンのアカウント番号には公開鍵暗号が使われており，そのアカウントに関連付けられている資産にアクセスできるのは，秘密鍵を所有している者だけとなる.別のアカウントに資産を譲渡するためには，トランザクションデータに元来の所有者の秘密鍵を使って作成されたデジタル署名を含ませることで可能となる．このことからも，秘密鍵あるいは秘密鍵を使ったデジタル署名が，正当な所有者を立証する唯一の手段である．したがって，アカウントが所有する秘密鍵が，他の誰かに渡ったときにブロックチェーンのセキュリティは破綻する.

ブロックチェーンには通信の安全性など多様なセキュリティ技術が実装されているが，アカウント番号に関連付けられた資産を保護する手段は非対称鍵暗号のみであり，秘密鍵の紛失や資産の漏えいなどから保護するセキュリティ対策は存在しない．そのため，トランザクション履歴をブロックチェーンデータ構造に組み込むことで，改ざんや偽造からの保護を可能としている．正しくは改ざんや偽造を検知する仕組みであり，インシデントを防止することはできない．そこで，ブロックチェーンにおける秘密鍵を RoT で保護することで，悪意のある第三者からの不正を防ぐことができると考えられる．秘密鍵という電子データを，物理的な RoT に格納することで「所有」という認証要素と，さらに秘密鍵を活性化する際に PIN コードを要求することで「記憶」，あるいは指紋などの「バイオメトリクス」といった認証要素との組み合わせで多要素認証が実現できる.

許可型ブロックチェーン（permissioned blockchain）において，書き込みアクセスの権利を付与するノードに対して，このような RoT を搭載した機器を指定することができるのであれば，非常に高い機密性を担保しながら高い本人性も維持できるセキュアなブロックチェーンが実現できる.

4.3 サプライチェーン（応用）

IoT デバイスの製造には，複数の工程がある．部品それぞれに製造工程があるとともに，加工や組み立てなどの工程で工場あるいは企業そのものが異なる場合がほとんどである．このような IoT デバイスの製造におけるサプライチェーンでは，潜在的なセキュリティリスクが存在する.例えば厳格なセキュリティ領域で製造された部品であれ，第三者の出入りが自由な作業領域で組み立てが行われば，スパイチップなどの異物が混入される可能性は否定できない．全ての部品が RoT をもち，Trust Anchor が検証できるのであれば，サプライチェーンにおける不正の多くを防ぐことできる.

5. 謝辞

本論文発表は，総務省ＳＣＯＰＥ「IoT デバイス認証基盤の構築と新 AI 手法による表情認識の医療介護への応用について」の研究開発（181603006)」の一環として行ったものであり，研究委託を頂いた総務省に謝意を表する.

文　献

[1] 一般社団法人　次世代社会システム研究開発機構，“IoT 白書，”2016 年度版，pp.614-620，Feb.2016

[2] IoT 推進コンソーシアム，“IoT セキュリティガイドライン ver1.0，”, pp.4-5, Jul.2016.

[3] 重要 IoT デバイスへの PKI 電子認証の導入－セキュア IoT 基盤の導入に向けて－