分散個体群を認証するための秘密分散法要件の一検討

山澤昌夫[1,2] 五太子政史[1] 山本 博資[1] 松本義和[2] 白水公康[2] 豊島大朗[2] 瀬瀬考平[2] 近藤 健[3]
辻井 重男[1,2]

概要：5G に象徴されるように，通信技術の急激な進歩により，あらゆるものがインターネットに接続される時代が到来した．それに伴って，接続されたモノ，IoT(Internet of Things) に対するサイバーセキュリティの確保は，極めて重要な課題となっている．ここ数年は， 5G のサービスの開始や，データ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大していること等，環境の変化も著しい [1]．こうした環境下，IoT 機器の脆弱性については，セキュリティ・バイ・デザインの考えのもと製造段階からの IoT 機器のセキュリティ機能埋込み，と言う考え方が重要とされている．セキュア IoT プラットフォーム協議会と中央大学研究開発機構は， IoT 機器の真正性を担保するトラストアンカー（TA：Trust Anchor）の埋込み，ライフサイクルマネジメント（LCM：Life Cycle Management) に関する実装方式の開発，普及の推進活動を行っている [2]．その中核となるのが，IoT 機器の真正性を担保する TA であるが，その認証機能における機能力は，装置を構成する要素個々まで及ぶものではない．しかし，IoT 機器におけるこれまでのインシデント例からは，装置の構成要素それぞれについても，真正性を担保する仕組みが求められている現状である．全ての部品がルートオブトラスト (ROT：Root of Trust) をもち，TA が検証できるのであればよいが，そうでない時の対策が望まれる．本論文では，TA に結びつけた秘密情報を秘密分散法により分割し，分散片を各部品へ配置し，分散片による検証機能のカバー範囲拡大施策を提案している．

An Optimum Secret Share Method for Gross Authentication of A Device Group

MASAO YAMASAWA[1,2] MASAHITO GOTAISHI[1] HIROSUKE YAMAMOTO[1]
YOSHIKAZU MATSUMOTO[2] KIMIYASU SHIROUZU[2] DAIRO TOYOSHIMA[2] KOHEI SESE[2]
TAKESHI KONDO[3] SHIGEO TSUJII[1,2]

1. IoT 機器の脅威と望ましい対応

IoT 機器を利用する 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．

IoT 機器の LCM 過程（図１）において考察すると，IoT 機器に対する脅威は，設計・製造段階，出荷後のサービス運用（利用シーン），廃棄の段階時においてそれぞれ異なる．

特に，利用者の手元に届くまでの過程において，悪意のあるコードや本物に限りなく似せて作られた模造品が紛れ込む事象が確認されている．このような脅威に対しては，以下のような対応が望ましい．

- データ・プログラムに対する脅威
  データやプログラムに対する脅威は「改ざん」や「誤動作」が代表的なものとなる．
  これらに対しては，送信データやプログラムへの電子署名により，機器の安全性やデータの真正性を担保することができる．
  また，製造後や出荷後に発見されるプログラムの脆弱性に対しては，都度セキュリティパッチを適用していくことで新たな脅威への対応ができてくる．データやプログラムに対する脅威は「改ざん」や「誤動作」が代表的なものとなる．これらに対しては，送信データや

[1] 中央大学研究開発機構
Chuo University, Research and Development Initiative
[2] セキュア IoT プラットフォーム協議会
Secure IoT Platform Consortium
[3] 中央コリドー ICT 推進協議会
CCC21ICTCouncil

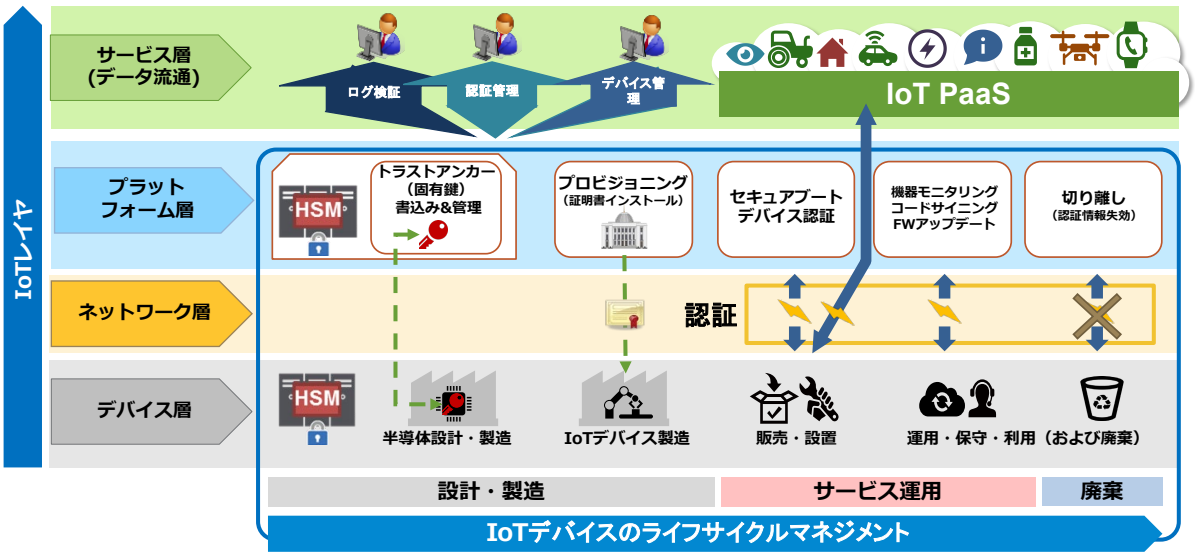

図 1　セキュリティバイデザインとライフサイクルマネジメント（LCM：Life Cycle Management）.
IoT デバイスは，設計・製造過程を経て，フィールドに出，サービス・運用される．運用が終了すると，廃棄される．その間、一環してセキュリティが担保されるよう IoT レイヤの各層における活動が必要である．

プログラムへの電子署名により，機器の安全性やデータの真正性を担保することができる．

- インターネットサービス，IoT 機器に対する脅威.
  インターネットサービスに接続する IoT 機器には，厳密な認証を実装することで，ここから生成されるデータの真正性が担保される．

IoT 機器の製造には複数の工程があり，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．即ち，組み立て環境しだいでは，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のである．このように，IoT 機器のセキュリティ対策には認証と真正性の担保が非常に重要となる．

全ての部品が後述する ROT をもち，TA が検証できるのであればよいが，そうでない時の対策が望まれる．本論文で述べる部品への秘密情報分散は，その施策として提案した．これにより，分散片による TA 機能のカバー範囲拡大が期待できる．

この認証機能のカバーする範囲は，実際は機器の一部である．IoT デバイスの製造には，複数の工程があり，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．即ち，組み立て環境しだいでは，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のである．

全ての部品が RoT をもち，TA が検証できるのであればよいが，そうでない時の対策が望まれる．本論文で述べる部品への秘密情報分散は，その施策として提案した．これにより，分散片による TA 機能のカバー範囲拡大が期待できる．

2.　IoT 機器が実装すべきセキュリティ機能

IoT 機器として組み立てられる前段階において，各 IoT 機器に必ず組み込まれるいわゆる IC チップに普遍的なクレデンシャルを埋め込むことでトレースの信頼度を確実なものにすることができる．これを IoT 機器におけるルートオブトラスト（Root of Trust：信頼の起点）と呼ぶ．

RoT は元来，米 NIST（アメリカ国立標準技術研究所）が規定する定義であり，デバイスの信頼性を保証するために設計されているが，当然ではあるものの IoT デバイスに対しても適用できる．ここでは，IoT 機器の RoT に期待するセキュリティ機能を以下の 3 点とした．

a．ソフトウェアの正当性検証ができる
b．暗号鍵（クレデンシャル）を保護できる
c．デバイスの識別に利用できる

RoT に格納されるクレデンシャルをトラストアンカー（TA：認証の基点）と呼ぶことにする．TA は，PKI のように電子的な証明の立証が連鎖した構造を持つ認証基盤を使うときに用いられ，したがって，TA の概念は IoT 機器のトレースには最も適しているといえる．

図 2 に「Trust Anchor」と「Root of Trust」のイメージを示す．

IoT 機器の製造段階から廃棄までのプロセスをトレースしていくためには，この RoT と TA が保証されなければならない．一般に桁数の小さいクレデンシャルは，情報セ

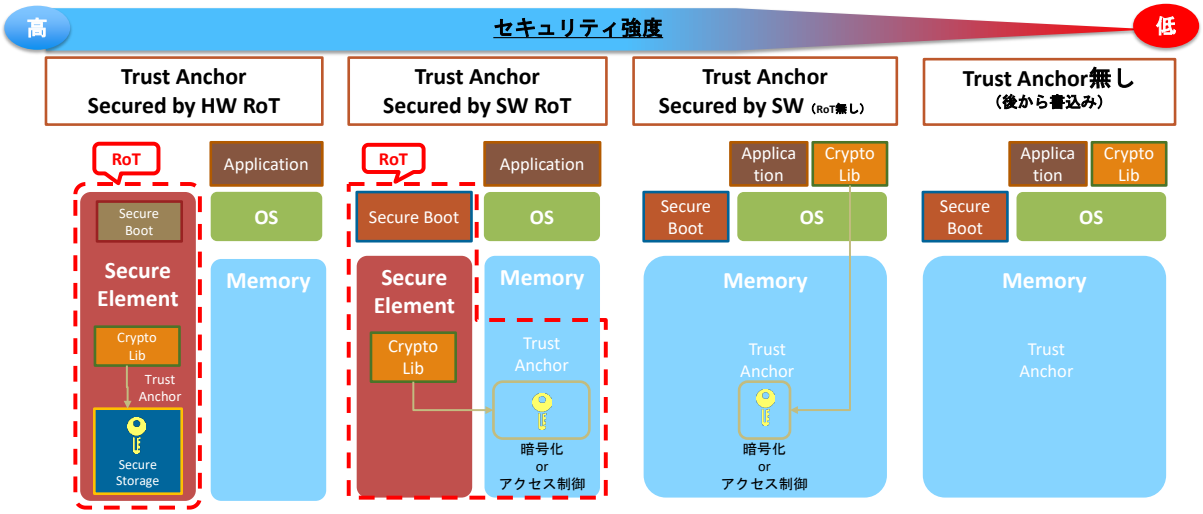

図 2　「Trust Anchor」と「Root of Trust」のイメージ．
ROT（Root of Trust）の組込み方によりセキュリティ強度が左右される．耐タンパー領域を持つセキュアエレメントに格納する形態（左側の図）が最もセキュリティ強度が高い．右方に向かって TA に対する防御が弱まる．

キュリティの観点からは脅威に対して弱いとされる．短いパスワードのように類推されやすく，データとして一定の大きさをもった TA を，如何に安全に利用できるかが RoT の信頼度となる．また，同時に以下のセキュリティ要件を満たすことが必須といえる．

要件-1　RoT から TA が取り出せないこと

要件-2　漏えいや不正が確認された場合に TA を直ちに失効できること

この 2 点を実装することにより，当該の RoT は世の中にただ一つの TA を持つ信頼の起点と成る．これらは，IoT 機器におけるセキュリティ要件として，欠かすことができないものである．

では，この TA にはどのような形式の電子データが適しているのか．一般に，IoT 機器に搭載される RoT には多面的な制限が存在する．特に容量の制限については，製品の価格や性能に大きく影響を及ぼすため設計時に多くの配慮を要する．脅威に対するコスト面へのリスクヘッジともなるが，いわゆる安価な IC チップにも格納できるサイズの電子データも選択できなければならない．

容量の大きな IC チップの RoT には，固有の電子証明書を TA として格納することがベストとなるが，電子証明書は電子データとしては比較的大きなものとなり，ローコストな IC チップには実装は難しい．このような IC チップには，必要最小限の電子データを格納することとなるが，このクレデンシャルとしての TA には一定のセキュリティ強度が保たれることが，RoT の設計に必要となる．そこで，RoT に求められる要件を以下のようにまとめた．

要件-3　攻撃に対し，安全な設計がされていること

要件-4　小さく，かつ，保護されていること

要件-5　ハードウェアで保護することが望ましい

これらを同時に満たす新たな技術が求められる．

3.　サービス開始，運用，廃棄フェーズにおけるセキュリティ上の脅威と課題

IoT 機器は，単体の持つセンサー類からデータ等が集積され，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，これまでに 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 機器への代表的な攻撃を，以下のようにまとめる．

(1) IoT 機器の脆弱性を狙った攻撃
- プログラムの改ざん
- リバースエンジニアリング

(2) IoT サービスへの攻撃
- データの盗聴
- データの改ざん
- 利用者のなりすまし
- 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く，製造時の正常性だけでは検知が困難である．

また，多くの IoT 機器は前述のとおり低リソースであり，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．加えて，IoT 機器の多くは無人運転（自動稼働）であり，攻撃を検知しにくいといった特性をもつ．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なコスト上昇が想定され，より強固なセキュリティ対策が求められる中，安全性に富む筐体に加え，個体識別ができる要素が必要になってきている．

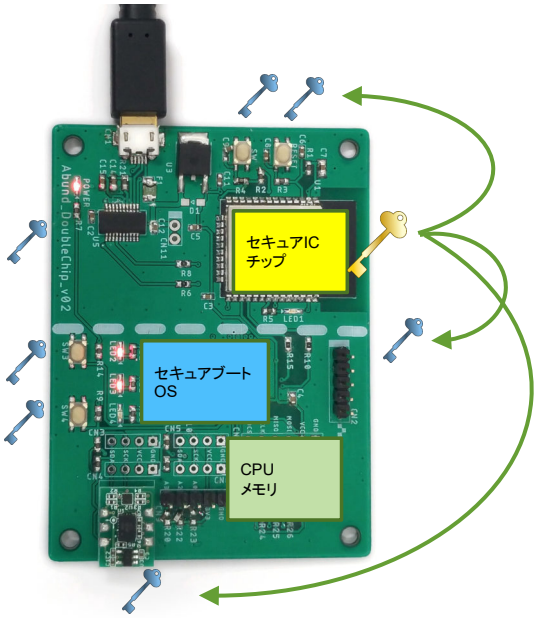

図 3　セキュア PCB のイメージ．
RoT（Root of Trust）の情報（図中の大きな鍵）と関連付けたサブ情報（図中の小さな鍵）を用いて、適切な運用を行うことで全体の正当性を担保する方式が，処理能力見合いのセキュリティ強度を担保するのに有用と考えられる．

4.　クレデンシャルの分散の考察

このように，IoT 機器を取り巻く脅威のすべてからは単一のセキュリティ対策では防御が困難である．しかしながら，IoT 機器の重要部位である CPU や IC チップが搭載された IC ボードの真正性あるいは真贋が保たれることで，設計・製造時には混入していなかったセンサー類や部位，誤動作の予兆などが検知可能となると考えた．

図 3 に示すとおり，既述のセキュアな IC チップのクレデンシャル，あるいはこのクレデンシャルを使用して生成したシークレットキー（図中の大きな鍵）を，真正性が求められるセンサーなどの部位に分割して（図中の小さな鍵）配付することで，すべてが揃うことで実行されるコマンドなどを動作させることができる．また，異常検知などセキュリティのみならず多岐のシーンでの活用も見込まれる．ただし，これらの鍵が偽装されるリスクは大きく，安全な鍵配付などの管理の仕組みが必要不可欠となる．

上位認証局が発行する証明書を付加した TA により，RoT が構成されるのだが，それを組込む対象が「IoT デバイス」としても，図 4 に示すように種類は，モバイル端末，オフィスのプリンタ，工作機械，コネクティッドカー，ドローン，ウェアラブルデバイス，センサー/カメラ，･･･，等々，多岐にわたる．

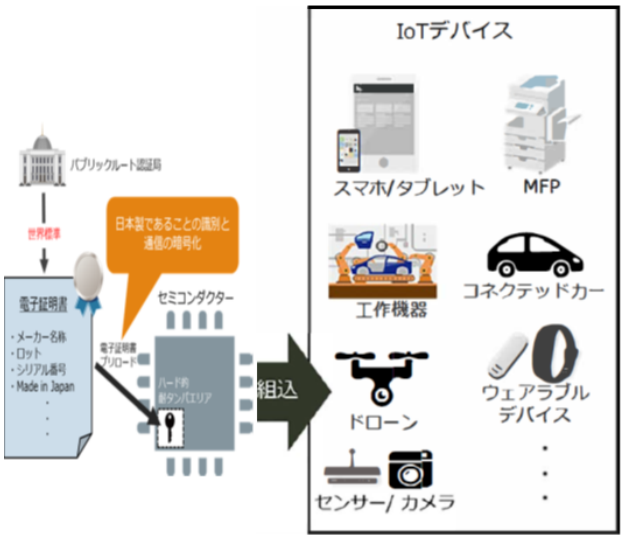

図 4　RoT の組込み対象のイメージ [5].
RoT（Root of Trust）の組み込み先は，モバイル端末，オフィスのプリンタ，工作機械，コネクティッドカー，ドローン，ウェアラブルデバイス，センサー/カメラ，･･･，等，多岐にわたる．

このような環境で，図 3 のようなイメージの PCB 上で図 2 の ROT として，「セキュア IC チップ」が実装されることになるのだが，応用分野すべてで，分散実装が望ましいというわけではない．

しかしながら，監視カメラやドローン等，実装コストが重要と思われる応用分野，ならびに，工作機械，車載装置等，真正性を担保がとりわけ重要となる応用分野では，分散実装も取り得るオプションの一つと考えられる．

そのような場合，図 3 の「ちいさな鍵」の所要個数，それを作り出したり，戻したりする時の方式計算量などが，つぎの検討事項となる．

より具体的には，

項目-1　分割数
素子数としてどのくらいまでサポートしなければならないのか．

項目-2　分割片のサイズ
素子に格納できるサイズと安全性とのトレードオフ．

項目-3　安全性
分散片の情報漏洩性と分割法．

もちろん，図 4 にあるように，多岐にわたる応用分野にたいして，一意的に決められるものとは思えないが，ウェアラブルデバイスのような小型機器，センサー/カメラ，ド

ローンタブレットなどの中型機器，工作機械や MFP(Multi-Function Printer) などの大型機器に分類して考察すれば，ある程度の目安が得られると思われる．

表 1 に検討例を示す．

表 1 分散法適用の検討要件

システム	項目- 1	項目- 2	項目-3
小型機器	一桁台	<32B	強安全性
中型機器	～10	<1kB	強安全性
大型機器	二桁台	<2kB	強安全性

5. まとめ

TA（トラストアンカー）に結びつけた秘密情報を秘密分散法により分割，分散片を各部品へ配置して，分散片による検証機能のカバー範囲を拡大する，という一施策を提案した．別途報告する秘密分散法の具体的実現方法を適用し，実システムへの応用を考えていきたい．

参考文献

[1] サイバーセキュリティタスクフォース “IoT・5G セキュリティ総合対策,”pp.10-12, Aug. 2019.

[2] 松本義和, 辻井重男, 白水公康, 瀬瀬考平, “重要 IoT デバイスへの PKI 電子認証の実装－セキュア IoT 基盤が形成するトラストチェーン－,” Computer Security Symposium 2019, pp.808-811, 21-24 October 2019.

[3] 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.

[4] 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.

[5] 一般社団法人セキュア IoT プラットフォーム協議会, “協議会設立プレスリリースー IoT 時代の安心安全なモノづくりを目指して－”, 2017.