GlobalPlatformの最新標準化動向 ——IoT時代のセキュアコンポーネント

庭野（にわの） 栄一（えいかず）
NTTセキュアプラットフォーム研究所

ICカードの国際標準化組織として設立されたGlobalPlatformも標準化対象を多様なSE（Secure Element），そしてトラステッドな実行環境TEE（Trusted Execution Environment）と対象をデバイスに拡大しています．さらには近年のIoT（Internet of Things）そしてエコシステム化の流れを受けて，提供する機能をアプリケーション管理からデバイスの信頼性管理へと拡げつつあります．ここでは最近，設立以来の組織改編を行ったGlobalPlatformのIoT・エコシステム時代に向けた最新の取り組みについて紹介します．

ICカードとは，CPUやメモリなどコンピュータと同様の機能を有し，耐タンパ性という外部からの攻撃に対して強いハードウェア特性を持つセキュアコンポーネントです．利用者認証や暗号化などのセキュリティ処理や安全なデータ管理などに利用されます．

現在，決済系（ICクレジットカードなど），通信系（SIMカード），交通系（Suicaなど），職域系（入退室用IC社員証），公共系（電子パスポート，マイナンバーカードなど）など非常に多くの分野で利用されています．

GlobalPlatform（GP）[1]はこのようなICカード内のアプリケーションプログラム管理に関する国際標準化組織として1999年に設立された団体です（**図1**）．特にICカード発行後にICカード発行者とサービス提供者が協調してリモートかつセキュアにICカードに対してアプリケーションを搭載・管理することを可能にした，セキュアコンポーネント関連では世界最有力の業界標準化団体です[2]．

設立以来，GPは対象となるセキュアコンポーネントをICカードからeSIM（embedded Subscriber Identity Module）などの多様なSE（Secure Element）[3]のほか，デバイス内にデバイスOSとは独立なトラステッドな実行環境TEE（Trusted Execution Environment）[4]に拡大するなど，現在では管理対象がデバイスレベルまで及んでいるのが重要な点です．さらにはSEのファームウェアの更新，SE/TEEに対する認定プログラムの創設，など標準化内容の拡充が進んでいます．

このため，近年では従来のICカード系のチップ業者やICカード業者，通信業者など伝統的なSE関係の業者のほかに，ARMなどのモバイルデバイス系チップ関連業者，Apple，Samsung，Qualcommなどモバイルデバイス関連の業者が積極的に貢献していることが重要な動きとなります．現在世界中から約100社のステークホルダが参加しています．

さて，ローエンドからハイエンドの多種多様かつ膨大な数のIoT（Internet of Things）デバイスが，ダイナミックに追加・接続され，連携・制御されていくようなIoT環境の拡大とエコシステム化が進展しています．

このような複雑かつダイナミックな環境の出現により，コネクティッドカーの乗っ取りによる外部からの不正なハンドル操作，医療機器の不正操作，家庭のデジタルカメラを踏み台としたDDoS（Distributed Denial of Service）攻撃など，多くのサイバー攻撃に関する実証やインシデント事例が報告され，IoTデバイスの脆弱性問題が指摘され始めています．

そこで，近年多種多様なIoTデバイスに対する真正性など，デバイスの信頼性をどのように担保するかが大変重要な課題として注目されてきています．

このような状況においてGPはさまざまなデバイスベンダとデジタルサービスの提供者が協調して高信頼かつ安全にデバイス管理を行えるよう，セキュアコンポーネントの役割を利用者認証からデバイス認証へと拡張しようとしています．

このためIoT，デバイス認証関連の要件レベルの検討に着手していましたが，最近1999年設立以来の技術委員会の改編を行い，デバイス認証関連の技術仕様を定める「TPS（Trusted Platform Service）委員会」を設置しました．

■アドバイザリカウンシル

GPでは技術仕様を策定する前に，要件を議論する場として，アドバイザリカウンシルが設けられています．現在，このアドバイザリカウンシルはマーケット関連，地域関連のタスクフォースで構成されています．

マーケット関連のタスクフォースとしては，コンシューマIoT，インダス

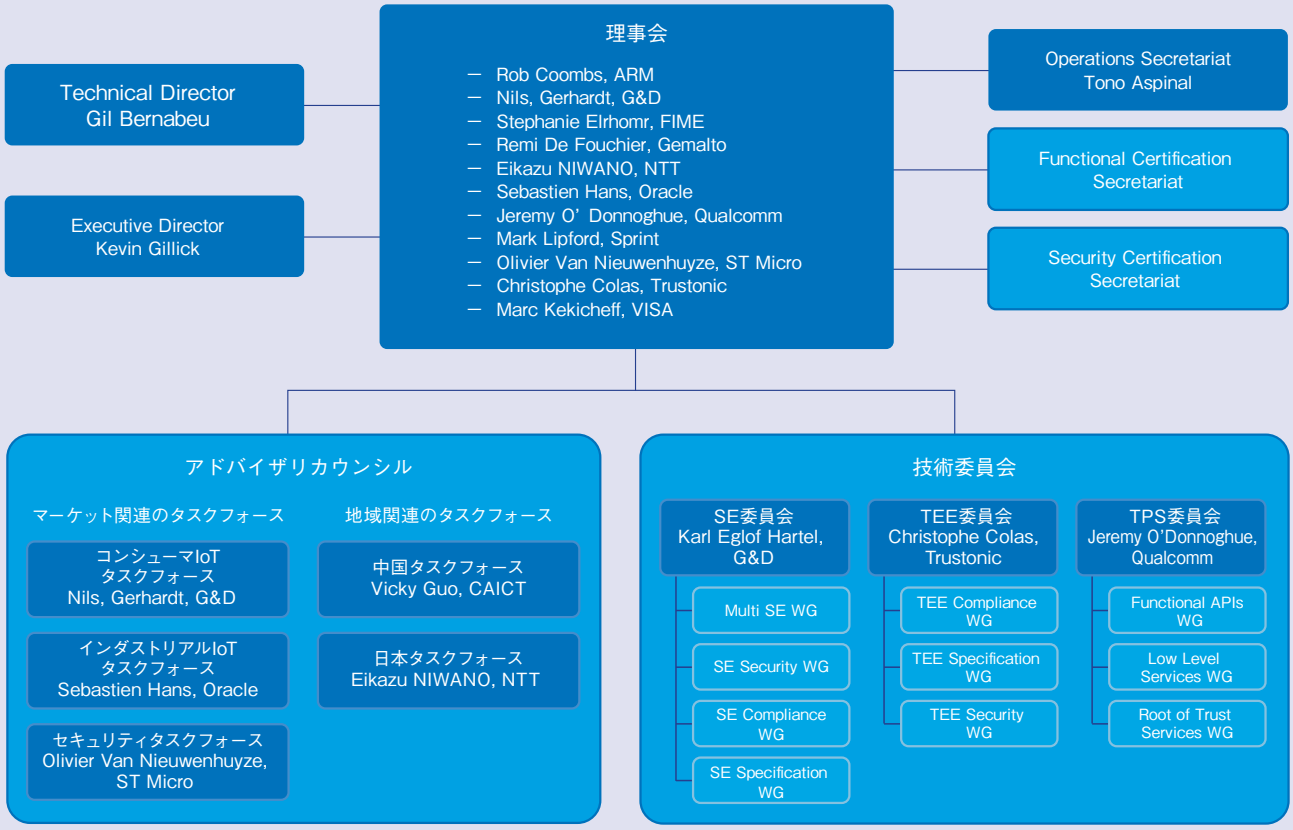


図1　GlobalPlatform組織構成

トリアルIoT，セキュリティの3つのタスクフォースが存在し，それぞれウェアラブルデバイスなどのコンシューマ系IoT分野，Industory4.0などのインダストリアル系IoT分野，そして信頼の基点（Root of Trust: RoT）と信頼の連鎖・最新暗号サポート（多様な最新暗号対応，デバイスに応じた軽量暗号サポートなど）などの議論が行われています．

地域関連のタスクフォースは地域に拠点を有するメンバが中心となり，GP情報，地域事情の共有や地域要件・展開の検討，地域発信の技術などの議論がなされており，現在，中国，日本2つのタスクフォースが存在しています．

■技術委員会

GPにおいて標準仕様を定める組織が技術委員会です．最近，ICカードから拡大を続けてきたセキュアコンポーネント関連の検討状況を反映して，名称を「カード委員会」から「SE委員会」，「デバイス委員会」から「TEE委員会」へと変更しました．もっとも注目される動きが前述した新たにデバイスの信頼性を検討する「TPS委員会」の設置で，セキュアコンポーネントを活用したデバイスの信頼性が検討テーマとなります．

GPはこれらの委員会を通じてマーケットやデバイスの種類によらずに，デバイスベンダやデジタルサービス提供者が協調してセキュアなデジタルサービスを提供することをめざしています．そのために，認証，コネクティビティ，プライバシ，セキュリティにかかわる次の3つの技術を提供しています．

① デジタルサービスの保護
② デジタルサービスのセキュアリモート管理
③ セキュアコンポーネントの認定（認証）

デジタルサービスの保護

まず最初のGP技術ですが，セキュアコンポーネントを活用したデジタルサービスや資産の保護で，デジタル資産（指紋や認証・暗号鍵などのクレデンシャル）の保護やそのためのセキュリティサービス（認証など）を提供していることです．

次のようにさまざまなマーケットの要件に対応する2つのセキュアコンポーネント技術を標準化することでこれを実現します．

■SE

1つはICカードを含む耐タンパ

ハードウェアとしてのセキュアエレメントです．これには外部からリーダ・ライタなどを通じて端末と連携するICカードやUSBトークンが含まれます．もう1つのタイプがモバイルデバイスなどの内部で利用されている，SIM，smart SD，eSE（eSIM，eUICCなど），さらにはチップセット（SoC: System on Chip）と統合されたiSE（integrated SE）などが含まれます．

また，モバイルデバイス内の複数のSEに対するアクセスの標準化も進展しており，モバイルアプリケーションからSEにアクセスするためのAPI（Application Programming Interface）として，OMAPI（Open Mobile API）が規定されています．また，モバイルデバイスはNFC（Near Field Communication）[*1]という近接通信技術をサポートしていますが，NFCを通じてモバイルデバイスのカードのエミュレーション環境HCE（Host Card Emulation）や多様なSEにアクセスするための仕組みCEE（Contactless Card Emulation Environment）もNFCフォーラムや欧州電気通信標準化機構（ETSI：European Telecommunications Standards Institute）と共同で検討されています．その他，SEのファームウェアのアップデート，特にGSMA（GSM Association）[*2]からの要望を受けてiSEのOSを上位と下位に分離するVPP（Virtual Primary Platform）という仕組みも新たな項目として検討が進展しています．

現在，220億（市場の41%）のGP準拠SEが展開されていますが，特にIoT関連で注目すべき点としてはGSMAがGPを活用したeUICCのリモートプロビジョニングの仕様を公開し，モバイルオペレータやコネクティッドカー向けに自動車業界がこの仕組みを採用していることです．

■TEE

一方で，SEのような耐タンパハードウェアに加えて，携帯電話などのようなデバイスに，従来のOSとは独立したセキュアな実行環境を提供するTEE（**図2**）の標準化が進展しており，デバイスOSより高いセキュリティを保証します．トラステッドアプリケーションといわれる認定されたソフトウェアのみが実行され，完全性やデータアクセス権の保護などエンド・ツー・エンドのセキュリティを保証します．

TEEはアプリケーション，デバイスOS，SEとのインタフェースを有するほか，Trusted UI（TUI）と呼ばれるマン・イン・ザ・ブラウザを回避するための高信頼なユーザインタフェース環境を提供します．

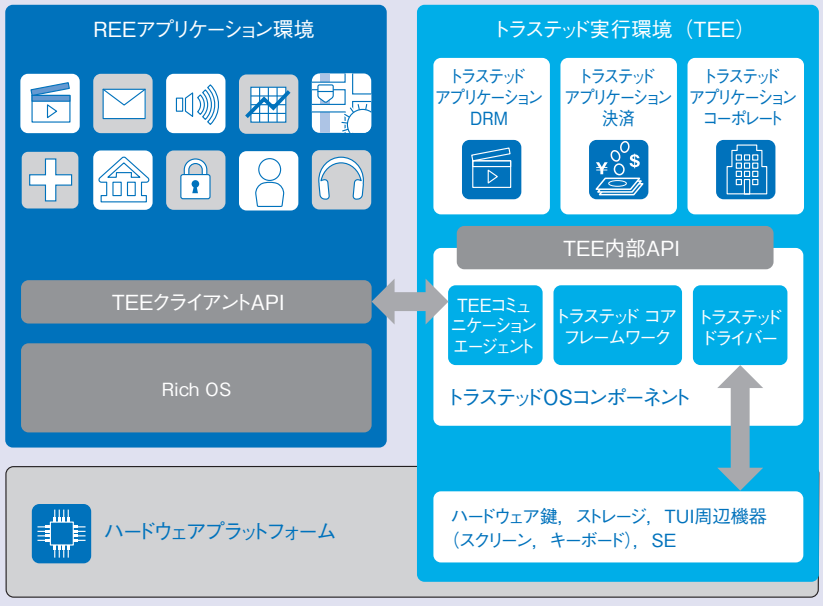
現在，TEEは生体認証処理や映像コンテンツのDRM（Digital Rights Management）処理，決済など高い安全性を要求されるアプリケーションに利用されているほか，IoT推進コンソーシアム[*3]が規定した「IoTセキュリティガイドライン1.0」[(5)]などで触れられており，展開が進展しています．

■サービス保護に関する4つの特徴

デジタルサービスおよび資源の保護のために，この2つのセキュアコンポーネントが提供する4つの特徴について述べます（**図3**）．

まず，1番目は「信頼の基点」をセキュアコンポーネント内に管理することでデバイスOSと分離されたセキュアな実行環境を提供していることです．

2番目がマルチアクタ（デバイスベンダとデジタルサービス提供者等）による，セキュアコンポーネント内の



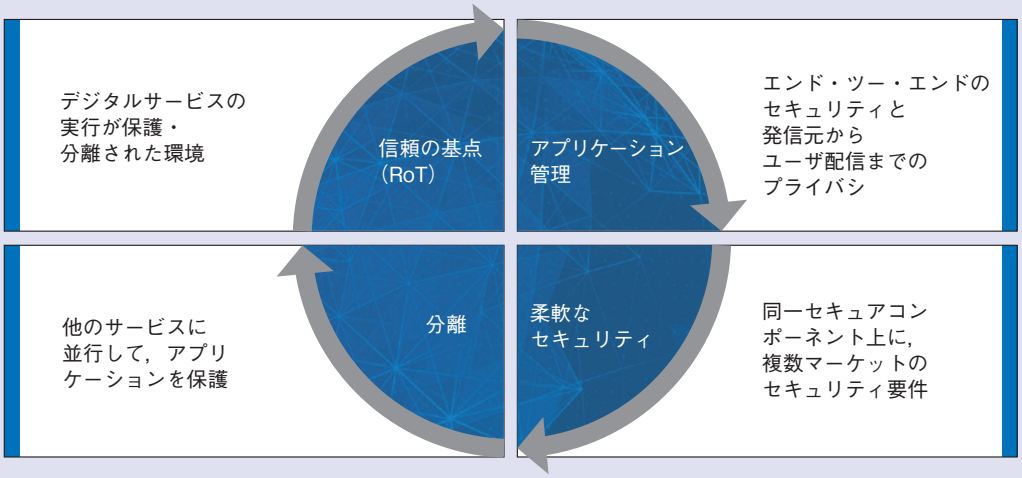
出典：GlobalPlatformより作成

図2　TEEのアーキテクチャ

＊1　NFC: 既存の複数の非接触ICカードの通信規格を包含した無線通信規格で，非接触ICカード機能やリーダ・ライタ機能，機器間通信機能などが利用可能．

＊2　GSMA: GSM方式の携帯電話システムを採用している移動体通信事業者や関連企業からなる業界団体．

＊3　IoT推進コンソーシアム：産学官が参画・連携し，IoT推進に関する技術の開発・実証や新たなビジネスモデルの創出推進するための体制を構築することを目的として設立した団体．



出典：GlobalPlatformより作成

図３　サービス保護に関する４つの特徴

「アプリケーション管理」をエンド・ツー・エンドでセキュアに実行できることです．SEのファームウェアも管理資源の対象となります．

３番目が，複数のマーケットセクタ共通の「セキュリティサービス」を同一のセキュアコンポーネント上で柔軟に追加・提供できることです．

最後に，複数のデジタルサービス提供者が同一セキュアコンポーネント上で，それぞれが「分離・独立した領域」を管理することができることです．

デジタルサービスのセキュアリモート管理

GP技術の次はリモート管理が可能であることです．特にIoT環境ではセンサも含めてさまざまな場所にIoTデバイスが設置されるため，これを実地で長期的に管理することは極めて困難です．そこで，リモート管理機能が非常に重要となってきます．GP技術により，IoTデバイスに組み込まれたeSIMなどのSEをリモート環境においてエンド・ツー・エンドで安全に管理することができます．

セキュアコンポーネントの認定（認証）

さらなる技術としてGPはSE/TEE向けに機能認定，TEE向けにセキュリティ認定のプログラムを提供しています．これに関係して，生体認証を含む多要素認証の標準化を推進するFIDOアライアンス*4との連携も開始され，FIDOアプリケーション（鍵・アプリケーション）をセキュアコンポーネントを含めたデバイス内環境にどのように構成・管理するかの方法や，この構成に関するセキュリティ認定の必要性の議論が開始されています．

一方，サイバーセキュリティ関連ではエコシステム化の進展による部品のサプライチェーン問題に対して，ハードウェアも含めた認定の仕組みが重要であるとの議論が世界中のいろいろな組織で盛んになされています．IoT・エコシステム時代を迎え，セキュリティバイデザインと併せてこの認定のスキームが今後より重要となってくるものと考えます．

デバイスの保護～デバイストラストアーキテクチャ

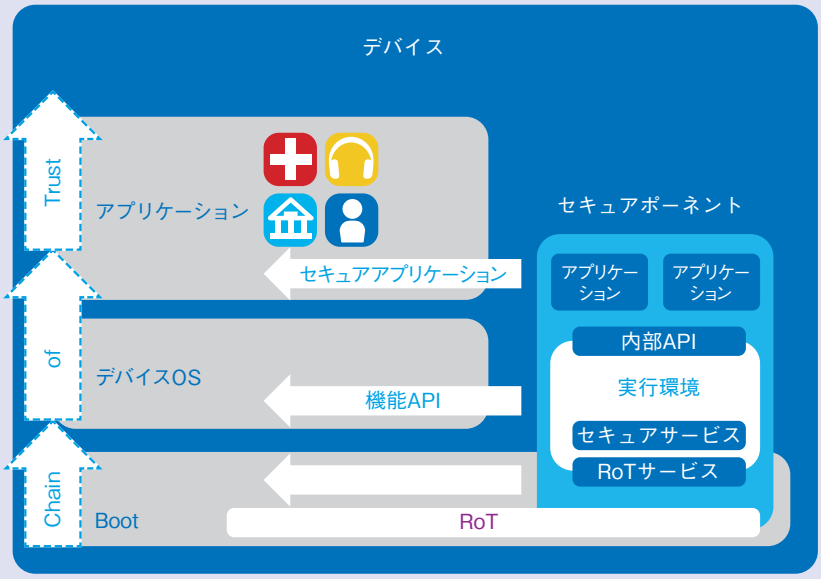
さて，ここからがGPが開始した最新の取り組みである「デバイスの保護」に関するものです．今後のIoT環境，エコシステム環境の拡大に伴うサイバーセキュリティ対策の１つとして大変重要な鍵となります．

デバイスの保護とは，デバイスの真正性保証も含めたデバイスの信頼性に関する仕組みのことであり，今後TPS委員会にて標準仕様が規定されます．

デバイスの保護に関しては，従来からトラステッドコンピューティングの一環として，TCG（Trusted Computing Group）*5がTPM（Trusted Platform Module）を活用したソリューションを標準化してきましたが，GPはセキュアコンポーネントを活用した汎用的な仕組みとしてIoTデバイス等に展開していくことを考えています．

繰り返しになりますがセキュアコン

＊4　FIDOアライアンス：生体認証など多要素認証の標準化組織．
＊5　TCG：セキュアブート機能を有するTPMの検討を推進する団体．



出典：GlobalPlatformより作成

図4　デバイストラストアーキテクチャ

ポーネントの特徴は，マーケットやデバイスによらずに，デバイスのベンダやデジタルサービスの提供者が，セキュリティ機能を含むさまざまなアプリケーション（およびSEの場合ファームウェア）をセキュアコンポーネント内にリモートで追加・更新できることにあります．このようにセキュアコンポーネントを活用して，デバイスの信頼の基点，信頼の連鎖，リモートデバイス構成証明サービスが提供できるため，マルチアクタ環境で高信頼，安全，そして柔軟にデバイスを管理することが可能になります[6]．

このデバイス保護の仕組みをデバイストラストアーキテクチャ（DTA: Device Trust Architecture）[7]と呼んでおり，デジタルサービス保護のためのセキュアコンポーネントと一体で検討が進められようとしています（**図4**）．

今後の展望 ～IoT時代に向けて

さて，GPの強みは非常に多くの標準化組織と連携していることです．従来のICカード，金融，通信系の標準化組織のほか，最近ではIoT関係でGSMA/OneM2M*6や自動車関係でCCC（Car Connectivity Consortium）*7と連携を進めています．さらに，他の耐タンパハードウェア関連では，デバイスの信頼性についてTCGと信頼の基点・連鎖などセキュアブートを汎用化するための仕組みの検討を開始するとともに，他の耐タンパハードウェアとして特にサーバ系の鍵管理・暗号処理で用いられるHSM（Hardware Security Module）との関係整理も始めています．

IoT・エコシステム時代を迎えて，この流れを進展させていく必要があります．ただし，この分野は制度面・文化的背景の違いにより，業界・地域ごとにニーズが異なると思われるため，今後は業界・地域ごとのニーズ・ユースケース分析とそれぞれの業界・地域における標準化組織との連携というものがさらに重要になってくると思っています．ここからさらにスマートシティなどのような「クロスセクタ×クロスリージョン」による標準化や認定が重要となります．そしてこの業界・地域特性に応じた他の耐タンパハードウェア関連団体との連携もさらに重要となると考えます．

また，技術面においては，このような多様なステークホルダ（開発者，運用者，サービス提供者，利用者），多様なデバイス・システム（およびその構成要素）がダイナミックかつ分散的につながる環境においては，IDおよび実体の情報を管理する「IDコンポーネント」を，「セキュアコンポーネント」を活用してどのように構造化・配置し，どのように真正性・信頼性を管理・認定し，どのような仕組みによって評価・認証していくのか，についての研究開発と標準化が重要となってくると思っています．

最後になりますが，これまでNTTはセキュアコンポーネントに関してPKI（Public Key Infrastructure）を用いた管理に対する貢献を果たしてきましたが，今後もこのような分散セキュリティ技術応用によるIoTセキュリティ・サイバーセキュリティ分野への貢献を図っていきます．

*6　OneM2M: IoTプラットフォームの標準化を進めるために開始された共同プロジェクト・標準化団体．
*7　CCC:スマートフォンと車内接続のための標準に関する業界団体．

■参考文献

(1) https://globalplatform.org/
(2) 庭野・五郎丸："GlobalPlatformにおける標準化動向，" NTT技術ジャーナル，Vol.18，No.9，pp.76-79，2006.
(3) GlobalPlatform："Introduction to Secure Elements，" May 2018.
(4) GlobalPlatform："Introduction to Trusted Execution Environments，" May 2018.
(5) IoT推進コンソーシアム・総務省・経済産業省："IoT セキュリティガイドラインver 1.0，" 2016.
(6) GlobalPlatform："Deploying and Protecting Digital Services with Chains of Trust，" May 2018.
(7) GlobalPlatform："Introduction to Device Trust Architecture，" July 2018.