参考資料６－１

# トラストサービス検討ワーキンググループ（第５回）　議事要旨

## １　日　時

平成 31 年４月 15 日（月）10:00～12:00

## ２　場　所

総務省８階　第１特別会議室

## ３　出席者

（構成員）手塚主査、宮内主査代理、新井構成員、小笠原構成員、小川構成員、楠構成員、繁戸構成員、柴田構成員、袖山構成員、谷構成員、西山構成員、中村氏（古屋構成員代理）、宮崎構成員

（ヒアリング対象者）GMO グローバルサイン株式会社稲葉氏、セコム株式会社　IS 研究所伊藤氏、一般社団法人セキュア IoT プラットフォーム協議会松本氏

（オブザーバー）吉田内閣官房情報通信技術総合戦略室参事官、中村法務省法務専門官、布山経済産業省情報プロジェクト室係長、河本経済産業省サイバーセキュリティ課課長補佐、大澤一般財団法人日本情報経済社会推進協会センター長（山内常務理事代理）

（総務省）竹内サイバーセキュリティ統括官、泉大臣官房審議官、木村参事官（総括担当）、近藤参事官（国際担当）、赤阪参事官（政策担当）、豊重サイバーセキュリティ統括官室参事官補佐、小笠原大臣官房企画課長、山路データ通信課長、飯倉情報通信政策課調査官、小高情報システム管理室長、寺田外国人住民基本台帳室長

## ４　配付資料

資料５－１　GMO グローバルサイン株式会社　提出資料
資料５－２　セコム株式会社　IS 研究所　提出資料
資料５－３　一般社団法人セキュア IoT プラットフォーム協議会　提出資料
参考資料５－１　トラストサービス検討ワーキンググループ（第４回）議事要旨

## ５　議事要旨

（１）開　会

（２）議　題

①　前回会合の振り返り

事務局から参考資料５－１に基づき、前回会合の振り返りが行われた。

②　関係者ヒアリング（前半）

稲葉氏から資料５－１について、伊藤氏から資料５－２について説明が行われた。

③　意見交換（前半）

関係者ヒアリング（前半）の後、意見交換が行われた。主な意見等は次のとおり。

宮崎構成員：稲葉氏の資料に、CA/Browser Forum のねらいとして、「EV SSL を QWAC と同格化させたい」との記載があるが、CA/Browser Forum にとってどのようなメリットがあるか。

稲葉氏：ウェブサイトの一番厳格性の高い証明書として EU の QWAC （Qualified Website Authentication Certificate）と同格化することで、EV SSL の普及を図るきっかけとしたいということが考えられる。

宮崎構成員：CA/Browser Forum 側もヨーロッパ側も、双方接近したいという動機を持っているということか。

稲葉氏：そのように認識している。ヨーロッパの QWAC は eIDAS 規則という法体系のもとで位置づけられた証明書である一方、CA/Browser Forum は民間のスタンダードに過ぎないというギャップをどのように解消していけるか、ETSI や Web Trust のメンバーを含めたフェース・ツー・フェース・ミーティングで議論がされているところ。

手塚主査：国レベルで eIDAS 規則の中で決めてきたルールと、民間側からつくり上げてきた厳格な EV SSL をどのようにハーモナイズするかという点が現在議論されているという認識でよいか。

稲葉氏：然り。

柴田構成員：CA/Browser Forum のガイドラインを監査する仕組みはどのようなものか。

稲葉氏：ブラウザベンダー各社が出すルート証明書の搭載要件の中に、CA/Browser Forum の Baseline Requirements や EV SSL の監査を受けなくてはならない旨が規定されており、Web Trust が実際の監査を行っている。Web Trust のタスクフォースは主にアメリカやカナダの公認会計士協会から構成されており、IT や PKI に詳しい人をオーディターとして認定し、そのオーディターが監査をしている。

柴田構成員：ヨーロッパでは ETSI や eIDAS 規則をベースに監査機関が法的に位置付けられている一方、CA/Browser Forum の Web Trust は民間の制度という認識でよいか。

稲葉氏：然り。

宮内主査代理：ウェブサイトにサーティフィケートを発行する際、自然人に対してサーティフィケートを発行する際とは、認証局においてどのような違いが

あるか。また、監査についても、自然人に対する監査とウェブサイトに対する監査とで何か違いがあるか。

さらに、日本語の法人名をローマ字表記にした際の課題について、現状ではどのような対応が具体的にされているか。自然人であってもローマ字表記は確定したものがあるとは限らないが、自然人の場合と法人の場合、それぞれどうされているか。

伊藤氏：法人に EV 又は OV 証明書を発行する場合は、申請する権限を持っているであろうとされている人からの申請を受けて発行する。発行の際は登記簿等も参照はするが、本当に申請者が申請する権利のある人であるかということに関しては、申請者の肩書等を見て判断している。人と組織との結びつきや権限の委譲等を確認できるシステムがあるのが理想ではある。自然人の場合もほぼ同様である。監査の際には、以上のようなプロセスが正しく行われているということを監査法人が確認する。

ローマ字表記については、ROBINS を確認すればわかるものもあるが、その場で担当者が判断せざるを得ないのが現状。今後、EV 証明書や OV 証明書の需要が増えた際にはより大きな問題となるだろう。

手塚主査：認証局の証明書を法人として発行する場合に、英語表記がないことが問題であったため、JIPDEC が作った、法人認証基盤に相当するデータベースである ROBINS に登録することによって、CA/Browser Forum にも認めてもらうという手続が行われてきたという経緯がある。しかし、公的なレベルのトラストアンカーではなく、民間の自由な判断のもとで使われているのが実情。

西山構成員：EU Trusted List に登録された Qualified のサーバ証明書の事業者と EV 証明書などで認められたサーバ証明書の事業者の間には、それぞれ国の認定制度と民間の認定制度に応じたものという意味でギャップがあるものの、EU は CA/Browser Forum に対するガバナンスに積極的に参加し、そのギャップを埋めようとしている。現在の CA/Browser Forum のチェアマンは、ギリシャの HARICA という認証局の方である。また、EV 証明書と Qualified 証明書のギャップを埋めるべく、例えば、EU のトラストリストを Firefox に取り組むプラグインが Mozilla から発行されており、そのプラグインを実行すると、EU のトラストリストに登録された QWAC を発行している事業者であるかどうかが機械的に確認できるようになっている。日本としても CA/Browser Forum のガバナンスに積極的に関与するとともに、EU において国家が認めたウェブサーバ証明書の発行事業者がトラストリストに載っているように、日本としてどの事業者のサーバ証明書が信頼できるものと認めるか、国としての認定制度の枠組みの中で議論することが必要。

手塚主査：ウェブ認証について CA/Browser Forum という民間団体の実施基準のみに則って我が国として進めていくか、国として公的なルールを作った上で CA/Browser Forum と連携するかは大きな論点。中国は自前のトラストリスト

を作っている。EU は、eIDAS 規則に基づいたトラストリストを作成しつつ、CA/Browser Forum ともうまく連携しようとしているという国際的な動きがある中で、我が国としてどのようにしていくか。

新井構成員：ウェブサイト認証は、URL というウェブ上の住所との結びつきが重要であり、制度としての検討が必要。英語表記についてもしっかり管理していく制度が必要ではないか。英語表記の確認の際、ROBINS だけでなく、国税庁の法人番号は参照しているか。

伊藤氏：弊社では、国税庁の法人番号は参照していない。

新井構成員：国税庁の法人番号の英語表記登録を参照することも含めて制度化を考えることが必要。また、CA/Browser Forum のガバナンスに積極的に参加し、日本の特殊な事情を表明していくべき。

伊藤氏：英語表記に関しては、日本語表記と英語表記がきちんとマッチングしている妥当性や、悪用されないようになっているかも確かめる処理が必要であるため、個別に確認するのは効率が悪く、一括したデータベースで処理し、それを参照できるようにするのがよいだろう。

④　関係者ヒアリング（後半）

松本氏から資料５－３について説明が行われた。

⑤　意見交換（後半）

関係者ヒアリング（後半）の後、意見交換が行われた。主な意見等は次のとおり。

宮内主査代理：普及の課題として、「電子署名法における認定認証業務相当の認定制度の検討」が挙げられているが、認定認証業務では、本人が確かに名乗っているとおりの人かどうかの確認、すなわちエンティティの確認がメインで行われるが、IoT 機器の証明書を発行する場合、その対象であるエンティティは何であり、どのようにそのエンティティを確認することになるか。

松本氏：今後、認証局において、どのメーカーにどの証明書を何個発行するかという審査が必要になるところ、大手の製造業であれば、EV の審査等と同様にすぐに審査ができるが、例えば委託先の町工場等の審査については審査基準が必要であり、政府から審査基準の提示があるのが望ましい。

宮内主査代理：電子証明書のコモンネームは何になるか。会社の名前が入るのか、個々の機器の名前が入るのか。

松本氏：機器一個一個のシリアルナンバーやメーカー名、製品のロット等の様々な組合せが考えられる。

宮内主査代理：ある IoT 機器にあるサーティフィケートを発行したということはどのように確認できるか。

松本氏：固定鍵を基準に証明書を発行するので、固定鍵と証明書がペアになっていることを確認するが、認証局の今の機能だけでは困難な部分があるため、プラットフォームという形で、データベースや検索エンジン等と組み合わせたシステムとして､実証を行おうとしているところ｡認証局とHSMが連携し、固定鍵に合った証明書が発行できたかどうかを、ログも含めて確認できる仕組みが必要。

宮内主査代理：アップデートの際には、署名鍵、すなわちIoT機器の持つ秘密情報のアップデートも行われるか。

松本氏：固定鍵を想定しており、最初の鍵は変更しない、アップデートできないポリシーとすることを想定。

宮内主査代理：証明書をアップデートするときにも、鍵が変わらないという前提で発行されるということか。

松本氏：然り。

宮内主査代理：PKIの前提となっていた、同じ鍵に対する証明書は二度とつくらないというスキームとはかなり考え方が変わってくるというイメージか。

松本氏：固定鍵を基準に、時間のパラメータを入れて証明鍵を生成することで、同じ鍵はつくらない仕組みを設けることを想定している｡Over The Air(OTA)を使ってアップデートするときのアップデートモジュールも、何かしらの署名を確認することで、正しいものであることを確認できる仕組みを実現しようと考えている。アップデートモジュールの方を認証し、OTAを使って降ってくるパッチが正しいかどうか、例えば、ウイルスではないかどうか、メーカーが本当に発行したものかどうかを確認することを想定している。

西山構成員：トラストアンカーはどこになるか。製造プロセスでIoT機器に証明書を埋め込む場合、例えば、ある自動車メーカーのプライベート認証局のようなものをたてて、そのメーカーから生産されるものだけに証明書を埋め込むことになるが、メーカーの認証局の正当性をどう確認するかという問題が出てくるため、何かしらのトラストアンカーとひもづく形でメーカーの認証局の正当性が確認できるスキームが必要になるのではないか。また、そのメーカーの認証ドメインで、関連する町工場のIoT機器に同じように証明書を埋め込むことができるだろうか。

　もう一点、Over The Airでアップデートするとなると、IoT機器のスキームとは別に、Wi-Fiが繋がらないとアップデートができないのではないかという側面についても、何か整理はされているか。

松本氏：トラストアンカーについても議論がされているところ。発売元又は製造元のメーカーがピラミッド構造の一番上にいるトラストアンカーや行政や地方自治体による認定制度等、何パターンも考えられる。

　Over The Airを実行する場合のネットワーク環境に関して、インターネットに繋がらないものはIoT機器と捉えていない。また、今後5Gの時代が

到来した際にも、トラストチェーンのモデルができれば、接続元の確認ができる仕組みが実現できるのではないか。一方で、世の中に出たときにはインターネットにつながっていたが、数年たってつながらなくなってしまったIoT機器が、５年10年たって、久々につながるときに一番リスクがあると考えており、そのときはPKIの技術を使った証明書の更新を行える仕組みができればよいのではないかと考えている。

西山構成員：後者の質問は、例えば、IoT機器が埋め込まれている自動車が、Wi-Fiが繋がらない場所で、エンジンがかからないといったことが起こらないか懸念されたので、念のために質問した次第。

小川構成員：IoT機器への証明書の組み込みについては、AzureやAWSでも既に行われているところ、今回の検討で一番メインとなるのは、IoT機器をセキュアな空間に入れるべきか否かの判断か、ライフサイクルも含めての検討か、ご教示いただきたい。今回の検討の新規性はどこにあるか。

IoT機器の廃棄に関して、データの出所を後で追跡や検証する際には、検証する鍵が必要になるため、そのような鍵も含めて全て破棄するべきではないとも考えられるが、その点に関する検討はされているか。

人や法人の活動において何かを証明する際、コストの観点から、TLSやSSLを全てに用いることは必要か。例えば、IoT機器のセンサーからある一時の温度を送るためだけにTLSを張ったり、証明書を使うことが正しいか、あるいはニーズがあるかといった検討はされているか。

松本氏：Azureのように、クラウドサービスのミドルウエアから電子証明書が発行されるものも多く存在している。今回の検討では、リッチOSやリッチなハードウェアといった電子証明書の埋め込みができるものではなく、メモリ領域が小さいものを対象にしている。小さな固定鍵のレベルであれば入れることができることが判明してきているので、いきなり証明書をRoot of Trustに入れるのではなく、まずは小さな鍵が盗まれないような形で証明書をコントロールするという設計思想。

破棄のときの鍵の扱いについても検討しているところ。破棄した瞬間から、鍵は利用できなくなり、ログに関しても信頼性が失われていくため、振る舞いも含めたログのとり方については今後検討したい。

モノに証明書を入れる場合、例えば一日に一回や一月に一回、センサーのデータを上げるときだけ、SSLやTLSのセッションを張ることもありえる。データの通信を暗号化するだけであれば、サーバ証明書を活用すればよいが、データを上げる機器を認証するクライアント認証も今後必要になるだろう。

小川構成員：暗号化通信をしないパターンも検討しているということでよいか。

松本氏：然り。

新井構成員：IoT機器の認証を制度化するとした場合、認定の対象は鍵だけか、工場自体も含まれるか等、何を制度化すべきか。

認証の際に確認する結びつきの限界はどこか。モノ一つ一つを認証するか、ある工場が ISO 等の規定を確認するといったことで工場を認証するか。

PKI を使うのは重いのではないか。ID ベース暗号といった、より軽い方法があるのではないか。

松本氏：制度化に関して、ある証明書が正しいところから発行されていることを最終的には確認したいため、認証局をどのように審査すべきかが課題。現在は、メーカーにプライベート認証局を立てることについて検討を進めている。また、製造ラインが正しいかどうかの確認も重要であり、監査や審査の基準も必要。固定鍵をチップにインストールするときに、正しい製造ラインでインストールされたかが信頼の基点になると考えている。

認証の際の結びつきについて、どのレベルで何を認証するかも重要。ライフサイクルマネジメントの中で、IoT 機器に変なチップが載っていることを確認できるようにしたいというところから検討を始めており、どのようにチェックするのがよいか、今後検討したい。

電子証明書にトラストアンカーやそこから発行されたチェーンを含めると PKI は非常に重い。ビットコインのようなブロックチェーンを使ったものや、ハッシュを追い続ける方法など、他の手段もありえる。一方、PKI には様々なログがとれたり、情報に付加価値をつけられるといったメリットがあるため、PKI を使ったモデルでまずはチャレンジしようとしているところ。

谷構成員：セキュア IoT プラットフォームでの検討の対象が、人命にかかわる重要 IoT 機器とのことであるが、重要 IoT 機器の基準はあるか。

松本氏：具体的な基準はまだ無く、将来的には重要インフラの IoT 機器で使われていくべきという提言である。現在は、見守りカメラから実証を始めようとしている。

谷構成員：見守りカメラから始めようとした理由は何か。

松本氏：PKI をチップに入れ込む実装例がまだ数種類しかなく、その中の一つに見守りカメラがあるため。

手塚主査：コスト面はアプリケーションとの関係で様々な見方があるため、本ワーキンググループで議論するのは難しいところもあるだろう。一方、本ワーキンググループでも既に議論になっている法的根拠やトラストアンカーという観点では、信頼できる発行元をどうやって担保するかという点が一番重要ではないかと考えるが、その点について意見を伺いたい。

松本氏：検討の目標として、悪意のある人間が IoT 機器を製造するリスクを防ぐということがある。この IoT 機器は正しいもので、この IoT 機器は悪いものといったシグナルを発することができることが期待される。

手塚主査：特に認証局といったトラストアンカーの信頼度をどのように担保するかが重要になるということか。

松本氏：ご指摘のとおり。

中村氏：サーバ証明書については、運用者側、例えばウェブサービスであれば、ウェブサービスを行う法人の認証として証明書が載っているように、サービサーの証明書と理解。IoT 機器の認証の議論について、製造者側の証明書を載せるという議論であったが、サーバ側の証明書について、技術革新等を背景に証明書の更新頻度が早くなり、監査等の負荷が増えている中、IoT 機器のクライアント側については、IoT 機器を納品した後は、本来納品された側が管理者になるところ、どこまでを製造者側の証明書の範囲とするか、納品後は証明書自体を切りかえる運用ができるか等、コスト負担者の見直しは検討されているか。

松本氏：御指摘の点は、制度面も含め非常に重要な検討課題の一つ。IoT 機器のライフサイクルマネジメントを行う際の課題の一つとして、瑕疵担保期間が長くなったことも踏まえ、製造側の瑕疵をどのように担保すべきかということがあるところ、メーカー側の保証の中で PKI を使えないかという議論もある。メーカーの責任と利用者の責任は分けて考えて行く必要があるが、まだ検討段階である。

小笠原構成員：EV 証明書の議論にせよ、IoT 機器の認証の議論にせよ、製造企業や発行対象企業といったように、「企業」を中心に証明書が議論されているように感じる。前回の e シールの議論と同様、企業で証明書を発行することが、ビジネス上必要になってきているのではないか。今後のインターネット上のビジネスにおいて、データの信憑性という議論に際しては、法人に対する証明書がやはり重要。トラストアンカーという観点で見た場合にも、法人自体の信頼性をどのような形で担保するか、一般の利用者も信頼できるように法的根拠をつけることが重要ではないか。

宮内主査代理：見守りカメラで実証を始めているという話があったが、不特定多数とのやりとりが発生するから PKI を使うものと考えられるところ、見守りカメラのような製品であれば、製造元企業のサーバとセキュアな通信ができれば良く、不特定多数からアクセスするということはないとも考えられる。そのような製品で PKI ベースの認証を行うことの意義と、どのような実証を行おうとしているかをご教示いただきたい

伊藤氏：最近の IoT カメラはサーバ証明書を搭載していることが多い。例えば、子どもを見守るカメラであれば、スマホのウェブブラウザから直接カメラにアクセスしたいという要望があり、その際はカメラがサーバとなるので、サーバ証明書が必要となる。現在松本氏が想定しているカメラは、クライアント証明書かもしれないが、将来的には、見守りカメラのユースケースとして、サーバ証明書があるほうが利用者にとって大きく便利になる。

宮内主査代理：知らないところにデータを送ることを防ぐため、クライアントであるカメラが、スマホのようなアクセスしてくる側の機器を認証することが必要である一方、スマホから見ても、偽のカメラに接続することを防ぐ必要

があるため、双方向の認証が必要ということか。

伊藤氏：然り。双方向の認証が必要であるから、PKI ベースの認証も必要となる。

手塚主査：企業の証明書を検討するにあたって、信頼できる発行元、すなわちトラストアンカーから証明書を出すことについて、国の制度レベルにするか、企業の実施基準で行うかを検討する必要があるだろう。今までの議論を踏まえると、制度化した方がエンドユーザーとしても安心して使えるのではないかという意見が多数の構成員から出ている。

柴田構成員：電子署名やタイムスタンプ、e シール、IoT 機器、それぞれ状況は異なっている一方で、データのトラストが重要であることは明確。将来的にはトラストサービスを構成する技術も変革し、それに伴った運用も変わっていくことが予想されるが、ヒトやモノの認証がバラバラに行われているのが現状。制度化して一つの枠組みとして継続して提供できる基盤を作った上で、様々な認証をその枠組みに入れていくスキームをつくっていくことが必要。

宮崎構成員：我が国の電子署名法は、認証局を認証する枠組みであるが、松本氏からは、認証局だけでなく、鍵や発行手順、発行対象も含めた認証についての提案があった。ヨーロッパでは、署名の生成装置についても基準を定め、あるレベル以上のものを使うかどうかで区別をしており、我が国においても、認証局だけではなく、鍵をどう機器の中に組み込むかや、対象となる機器が何かといった点も含めて制度化すべき。

手塚主査：リモート署名についても同様の議論があったが、我が国では、実印を登録した後の管理についてルールは全く無い。一方、電子の世界では、秘密鍵と公開鍵のペア鍵について、登録する公開鍵ではなく、秘密鍵の管理についてルール化がされていないという課題がある。電子証明書であれば、秘密鍵は IC カードに入れて安全に保持しようという方向になっている。IoT 機器について、松本氏から説明があったように、ハードウェアで管理、ソフトウェアで管理といった、四つほどのレイヤに分けた Root of Trust の考え方が示されている。これらの動きも踏まえつつ、どのようにルール化していくか、検討する必要がある。証明書の発行と鍵の管理について、ヒトやモノ等の認証には共通点があることも踏まえ、制度を検討していく必要がある。

⑥　その他

事務局から、次回の日程について説明があった。

（３）閉会

以上