基般

3. トラストと暗号技術の関係性

島岡政基（セコム（株）IS 研究所）

暗号技術に必要なトラスト

社会におけるトラスト

我々は日々何気なく社会生活を営んでいるが，これはさまざまな前提の上に成り立っており，信頼もその１つといえる．信頼には，たとえば家族や友人に対する人格的な信頼もあれば，貨幣制度や公権力に対するシステム的な信頼もあるだろうし，意識的な信頼，無意識的な信頼もあるだろう．信頼論の古典「信頼（Vertrauen）」[1]の著者 Niklas Luhmann も「信頼は社会生活の基本的な事実である．（中略）こういうこと（社会生活）が可能であるのは，我々が他者や社会に対して一定の信頼をおいているからにほかならない」と述べている．Luhmann いわく信頼は「社会的な複雑性を縮減するメカニズムの１つ」であり「不十分な知識に基づきながら人格システムや社会システムに対する予期を生み出す」ことと述べるとともに，「信頼すべき他者や社会の構造に関する知識が必要」と述べている．筆者なりの解釈で平易に説明するならば，「人が相手を信頼する」とは「相手が（ある文脈において）自分の予測する通りに振る舞うはずである」と期待する行為であり，社会生活を円滑に営むための手段と捉えることができる．本稿では，この「社会生活を円滑に営むための行為としての信頼」を明示的に**トラスト**と呼ぶことにする．

暗号技術を支えるトラスト

現代の情報通信技術は社会基盤化が進み，そこでは当たり前のように暗号技術が広く使われている．交通系非接触 IC カードの偽造対策や格納されるデータの保護，ネットショッピングなどのなりすましサイト対策や暗号化通信などさまざまなところで多くの場合は無意識のうちに暗号技術を使っている．

暗号技術に限らず，我々は今やさまざまな情報システムを活用して社会生活を営んでいるが，その情報システムの仕組みをいちいち理解して利用している人々はそれほど多くはないだろう．つまり我々は，情報システムが提供する機能を把握しつつ，その仕組みまでは理解していない，という「不十分な知識」の下で，システムが「ちゃんと機能するはず」という期待を持っているのである．

暗号技術も同様で，それが提供する機能（たとえば秘匿や認証，署名など）が確実に提供されるはずという期待を持っていると考えられる．しかし一方で，利用者は決して盲目的に期待をしているわけではなく，さまざまな仕組みの組合せによってこうした期待が成立する．

本稿では，事例をベースに暗号技術のトラストがどのように成立しているのかを解説するとともに，今後の IoT（Internet of Things）時代の到来によって，このトラストがどう変化するのかについて考察していく．

暗号技術と暗号鍵

暗号技術に対するトラストについて述べる前に，まずは簡単に暗号の仕組みについて説明しておく．

暗号技術の基本は，任意の平文に対してある処理を行い，暗号文に変換する暗号化処理と，その暗号文をもとの平文に復元する復号処理によって構成される．一般に暗号アルゴリズムと呼ばれるものは，この暗号化処理と復号処理の手順を規定したものであり，AES（Advanced Encryption Standard）や RSA（3 人の発明者 Rivest, Shamir, Adleman の頭文字）などが代表的である．

暗号文は第三者に解読されては困るもので，復号

処理には何らかの秘密情報を必要とする．この秘密情報がいわゆる鍵であり，およそ現代の暗号技術は暗号アルゴリズムが同一でも鍵さえ異なれば復号できない仕組みになっている．このため暗号アルゴリズムは必ずしも秘匿する必要がなく，機密管理すべきは鍵のみと考えればよい☆1．

復号処理だけでなく暗号化処理においても鍵が必要となるが，復号処理と暗号化処理で同じ鍵を用いる方式を共通鍵暗号方式，異なる鍵を用いる方式を公開鍵暗号方式と呼び，それぞれの概要を**図 -1** に示す．第三者に暗号文を解読されないためには，復号処理に用いる鍵を機密管理しておく必要がある．公開鍵暗号方式の場合は，暗号化処理に用いる鍵は機密管理する必要がないという意味で公開鍵（Public Key）と呼ばれ，対称的に復号処理に用いる鍵は私有鍵（Private Key）と呼ばれる．この公開鍵は私有鍵と一意に紐付けられ，両者の組合せは鍵ペアと呼ばれる．なお，共通鍵暗号方式の場合は，両処理に用いる鍵は秘密鍵（Secret Key）と呼ばれる．

また，暗号技術を自分自身のために利用する場合を除けば，暗号化処理を行うものとそれを復号するものは別のものということになる．暗号化処理を行うものを Relying Party（RP），復号処理を行うものを Trusted Party（TP）と呼ぶ．

このように暗号技術の構成要素は，暗号アルゴリズムと鍵に大別され，鍵の種類などは暗号方式によって異なるものの，鍵（秘密鍵ないし私有鍵）を機密管理する必要がある，という点はどの暗号技術であっても変わらない．特に，共通鍵暗号方式においては，後述のように公開鍵暗号と組み合わせて使うのでない限りは，その共通鍵を TP と RP 間で事前共有する必要がある．しかし，以下のような課題があり，実装・運用上しばしば大きな制約となる．

（ア）鍵の情報量（多くの場合 128bit 以上）的にディジタルメディアによる媒介が不可欠．

（イ）情報通信網を介して共有する場合は，通信網における盗聴・なりすましリスクを考慮する必要がある．

（ウ）秘密鍵を共有するすべての RP が機密管理する必要がある．

（エ）RP ごとに秘密鍵を使い分ければ TP の鍵管理コストが煩雑になる．

（オ）TP が秘密鍵を更新すれば RP も合わせて更新する同期管理が必要となる．

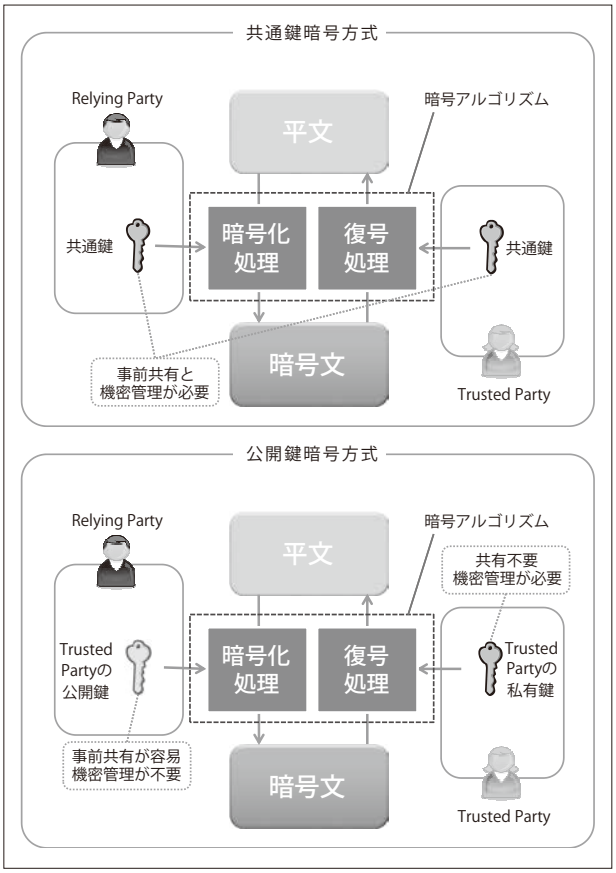

図 -1　共通鍵暗号方式と公開鍵暗号方式

これに対して公開鍵暗号方式では，鍵を機密管理する必要があるのは TP のみでよい．さらに，公開鍵暗号を応用した Diffie-Hellman などの鍵確立（Key Establishment）アルゴリズムを用いれば，秘密鍵を TP/RP 間で安全に共有することが可能となり，共通鍵暗号も合わせて利用することが可能である．

一方で，TP の公開鍵は共通鍵暗号同様に RP と共有する必要がある（公開鍵暗号の場合，共有ではなく配布と呼ぶ方が一般的である）．共通鍵暗号と

☆1 知財問題や攻撃へのヒントを最小化するために暗号アルゴリズムを秘匿しているものもないわけではない．

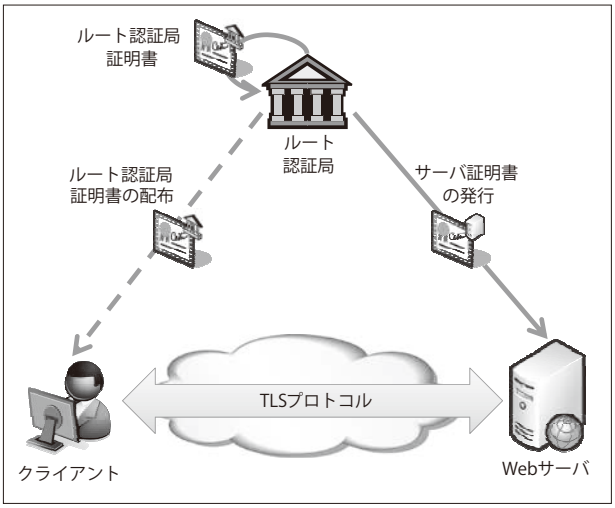

図 -2　サーバ認証の概念

異なり，公開鍵なので盗聴リスクは気にしなくてよいが，なりすましリスクは依然残っている．また，共通鍵と同様に公開鍵を更新したり失効すれば，RP にもその情報が適切に伝えられる必要がある．

つまり，公開鍵暗号方式における課題は，1）私有鍵の機密管理，2）公開鍵の安全な配布・管理に集約されると言ってよいだろう．

こうした公開鍵暗号方式の利点を活かしつつ上記 2 点の課題を解決して広く普及した実装例として，Web のサーバ認証などに用いられる Web PKI（Public Key Infrastructure）がある．公開鍵暗号方式が前述のように共通鍵暗号方式と比べれば扱いやすくなったのは間違いないが，広く社会で利用されるためには前述の課題 2 点を解決する必要がある．次章では，この Web PKI が社会で広く利用されるためのポイントは何だったのか，どのようなトラストがそこには必要とされているのか，について明らかにしていく．

Web PKI を支えるトラスト

暗号技術に対するトラストがよく形式化され，かつ実用化されている事例として Web のサーバ認証などに用いられる Web PKI がある．主要な Web ブラウザや OS のベンダは，各製品にあらかじめいくつかのルート認証局（の証明書）を組み込んでおり，これらの認証局はパブリック認証局と呼ばれる．Web PKI は，これらパブリック認証局をルート認証局として構成される一連の認証局によって証明書を発行・管理する基盤である．

サーバ認証の仕組み

本稿で扱うサーバ認証は，TLS（Transport Layer Security）と呼ばれるセキュア通信プロトコルで規定されている認証方法で，ネットバンキングやオンラインショッピングサイトを中心に広く普及している．サーバ認証は，Web ブラウザなどのクライアントがインターネット経由でサーバにアクセスするにあたり，サーバがなりすましでないことを確認するために用いる．この確認は，①サーバ証明書に記載されたサーバの名称等の確認と，②当該サーバが生成する署名の検証によって実行される．

署名は公開鍵暗号の一応用で，私有鍵を持つ TP のみが署名を行うことができ，公開鍵を入手した RP であれば誰でもこの署名が改ざんされていないことを検証することができる．

サーバ証明書は，認証局と呼ばれる発行者から主体者であるサーバに対して発行されるもので，サーバの公開鍵および名称等に対して発行者の私有鍵で署名されている．

認証局は，ルート認証局と呼ばれる最上位の認証局と，その下位に複数の中間認証局を持つ階層構造を持つことができる．サーバ証明書は最下位の中間認証局から発行される．

クライアントは所与の（ルート）認証局の公開鍵（証明書）を用いてサーバ証明書を検証することで，当該証明書の改ざんや，不正な認証局によるサーバ証明書の偽造を検知することができる．

このように階層構造の PKI においては，ルート認証局の鍵ペアがトラストの起点となり，このような存在はトラストアンカーと呼ばれる．

サーバ認証の概要と，認証局の階層構造を**図 -2** および**図 -3** にそれぞれ示す．

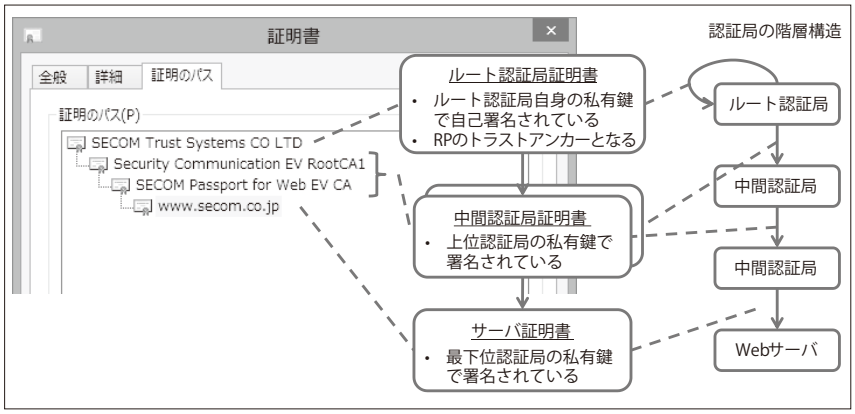

図-3　認証局の階層構造

パブリック認証局

一般のルート認証局が，その私有鍵の機密管理にパブリック認証局として主要なWebブラウザやOSに組み込まれるためには，これらのベンダが示す要件を満たし審査を受ける必要がある．要件は組込みベンダによって多少の違いはあるものの，いずれにも共通するのは，WebTrust for CA（Certification Authority）など認証局運用に関する何らかの監査規準への準拠をルート認証局に求めている点にある．

これらの監査規準では，認証局が持つ私有鍵の機密管理について，①（所定の）安全な暗号アルゴリズムを利用すること，②耐タンパ性を備えた暗号モジュールを利用すること，③堅牢な物理セキュリティ環境での運用の3点を要求しており，それぞれ設計レイヤ，実装レイヤ，運用レイヤで対策すべき要件と捉えることができる．

①では，暗号アルゴリズムの深い知見を有する機関（たとえば前述のAESを策定した米NIST[☆2]（National Institute of Standards and Technology）や，日本であれば電子政府推奨暗号リストを策定している暗号技術検討会[☆3]（CRYPTREC）など）の評価を受けた暗号アルゴリズムの利用が求められる．②では，NISTが策定する暗号モジュールのセキュリティ規格FIPS（Federal Information Processing Standardization）140においてレベル3以上の認定を取得したHSM（Hardware Security Module）の利用が求められる．HSMは暗号鍵を格納管理する装置で，暗号鍵を外部に一切読み出すことなく，暗号鍵を利用する一連の処理はすべて装置内で完結できるように実装されたハードウェアである．FIPS 140 レベル3では，耐タンパ性として物理的な改ざん耐性，すなわち密閉された装置を物理的に開封すれば自動的に暗号鍵を消去する機構が求められる．③では，最低でも4層以上の物理的なセキュリティゾーンを用意し，物理的な破壊や電磁波放射の対策などを行うとともに，論理アクセス物理アクセスともに個人単位での認証認可を行うなど，厳格な物理セキュリティ対策が求められる．

このようにパブリック認証局は，その私有鍵の機密管理を保証するために，これら①～③の準拠性についてWebTrust for CAなどの資格監査人による監査を毎年受けている．そして，①～③が明文化され，その準拠性を客観的に評価できることこそがパブリック認証局を支えるトラストであるといえる．

パブリック認証局組込みベンダ

ルート認証局をパブリック認証局として自社製品にあらかじめ組み込むWebブラウザやOSのベンダのことを，ここでは（パブリック認証局）組込みベンダと呼ぶことにする．前述のとおり組込みベンダによってそれぞれに組込みポリシーを規定しており，それぞれに細かな違いはあるものの，本質的な違いはないといえる．詳細かつよく整理された例としてはマイクロソフト社のMicrosoft Root Certificate Program[☆4]が挙げられる．

各組込みベンダは，パブリック認証局を各製品に組み込んでおくことで，その公開鍵の安全な配布を実現できるとともに，製品のオンラインアップデートの中でこれらパブリック証明書の更新や無効化な

☆2 http://www.nist.gov/itl/csd/ct/
☆3 http://www.cryptrec.go.jp/
☆4 http://aka.ms/rootcert/

どを行っている．いわばWeb PKIにおけるトラストアンカー管理の役割を担っている．

パブリック証明書の更新は，組込みベンダの求める要件が変わった場合（暗号アルゴリズムの移行など）にパブリック認証局側がこれに応じる形でパブリック証明書を更新することもあれば，パブリック認証局側の都合（ルート証明書の有効期限切れなど）でパブリック証明書を更新することもある．組込みベンダは，これらの更新を受けて各ベンダの対象製品（Webブラウザや OS）に対して更新パッチを提供している．一方の無効化は，要件を満たせなくなった認証局をパブリック認証局から除外（無効化）するもので，最たる典型例は2011年に外部からの不正侵入を受け多数の証明書不正発行事件に至ったオランダの認証局 DigiNotarである．組込みベンダらは同事件発覚後直ちに各製品に対して緊急更新パッチを提供し，同認証局は無効化された．

Web PKIが普及した要因として，パブリック認証局を信頼するWebブラウザや OSの提供元であるベンダがこうしたトラストアンカー管理の役割を担ったこと，また組込みベンダ（Apple, Google, Microsoft, Mozillaなど）が認証局に対して十分にガバナンスを効かせられる立場にあったことなどが挙げられるだろう．さらに，これら組込みベンダは世界的にも有数のベンダであり，（各論として議論の余地はあると認識しているが）総論としてこれらに対しては既存の社会システムによって一定のガバナンス，つまり組込みベンダが不正を行えば社会的リスクが大きいという抑止力が期待できることも大きなポイントだったのではないだろうか．

IoT時代の暗号技術とトラストの関係

ここまで，Web PKIを事例に暗号とトラストの関係性について述べてきたが，これからのIoT時代はその関係性が大きく変わる可能性がある．

私有鍵の機密管理

従来のクライアント環境は，パスワードにしても，パスワードに使い捨てパスワードなどを組み合わせた多要素認証にしても，人による操作を前提としていた．つまりクライアント側の端末にはこれまで鍵は必須ではなかった．これに対してIoTでは多くの場合，人による操作を想定せず自律的に動作することを想定していると考えられるため，サーバ側がクライアントである機器を認証するためには何かしらの鍵が機器側にも必要となると考えるのが自然である．これはすなわち「私有鍵の機密管理」が強い物理セキュリティ環境を用意可能だったサーバ側だけでなく，クライアント側にも求められるようになる大きな変化といえる．

またIoTでは，膨大な数の機器を流通させるために従来よりも大幅に機器単価を低く抑えることが求められ，加えて必ずしも有人管理下で稼働するとも限らないなど，低い物理セキュリティ環境の下で動作することを前提に設計しなければならない．

技術的には，耐タンパ性を備えたSE（Secure Element）と呼ばれるICチップが，携帯電話やスマートフォンなどのモバイル通信端末に抜挿可能なSIM（Subject Identity Module）カードとして，またPCのマザーボードなどに直付けするTPM（Trusted Platform Module）として[☆5]広く普及しているが，IoTに求められる機器単価によってはこのSEのコストを吸収することはまだまだ容易ではない．

また，低い物理セキュリティ環境における私有鍵の機密管理は，技術的に新しいチャレンジが必要になると考えられる．有人管理下にないということは，物理的な不正アクセスを排除することが難しくなる．もちろん耐タンパ性を持つSEなどであれば一定の効果を発揮するが，耐タンパ性装置に有効なサイドチャネル攻撃の実証研究も報告されており，今後耐タンパ性装置が普及してくれば攻撃も本格化・高度化してくることが予想される．

サイドチャネル攻撃とは，暗号モジュールを侵襲せずに動作状況をさまざまな物理的手段で観測することで秘密情報の取得を試みる攻撃手法である．物

☆5 正確にはTPMはSEではないが，ここでは耐タンパ性を備えたICチップという広義で捉えるものとする．

理的手段が必要なため，従来の強い物理セキュリティ環境であれば本質的な脅威ではなかったが，弱い物理セキュリティ環境では検討すべき有意な脅威として捉える必要が出てくるだろう．サイドチャネル攻撃対策として，ハイディングやマスキングといったサイドチャネル情報の価値を低減させる対策も検討されているものの，コスト増の問題や，未対策機器が一定数流通してしまえばそれらの移行についても考慮する必要があるなど，今後の研究開発における喫緊の課題として取り組む必要があると考えている．

トラストアンカー管理

Web PKI から学びとれる知見として，トラストアンカー管理を担うステークホルダの理想的な条件には，

- トラストアンカー管理のモチベーションがあること
- RP に対して遠隔更新可能なスキームがあること
- RP，TP やほかの関係者を含むエコシステムの中で十分な支配力があること
- トラストアンカー管理を行うステークホルダ自身はエコシステムの中だけでなく，既存の社会システムの中で RP から信頼されやすい立場にあること

などが挙げられる．

また，もう一点重要なポイントとして，トラストアンカーを配布する範囲（トラストドメイン）が挙げられる．Web PKI は，不特定多数のユーザがアクセスすることを想定した Web サーバのためのものだったため，トラストアンカーを配布する対象も不特定多数であり，結果としてパブリックなトラストドメインを確立した．一方の IoT では，不特定多数のステークホルダ（ユーザおよび機器）がアクセスする機器よりも，特定のステークホルダのみにアクセスを許可する機器の方が多くなるのではないだろうか．こうしたトラストドメインの広さや規模によっても，トラストアンカー管理の役割を担うものは変わってくるだろう．

時代に応じたトラスト

暗号技術が社会で利用されるようになってきたが，その典型例である Web PKI を紐解いてみると，そこには暗号技術を支えるトラストがあった．両者が出会うことによって，その複雑な仕組みが縮減され，暗号技術の詳しい理解なしにその恩恵を享受できるようになったのだといえる．一方 IoT 時代を迎えると，暗号技術を支えるトラストもまた変化することが予想される．それぞれの時代に応じたトラストを確立することが重要であり，暗号技術を社会に浸透させていくにはトラストの理解は不可欠といえるだろう．

参考文献

1）Niklas, L 著，大場　健，正村俊之 訳：信頼―社会的な複雑性の縮減メカニズム，勁草書房（1990）．

（2015 年 8 月 7 日受付）

島岡政基（正会員）■ m-shimaoka@secom.co.jp

1998 年慶應義塾大学大学院理工学研究科修士課程修了．同年セコム（株）入社，2004 年より同 IS 研究所．2005 ～ 10 年まで国立情報学研究所特任准教授（後に客員准教授）を兼務．認証基盤とトラストの研究開発に従事．博士（情報学）．