第 2 章　電子認証フレームワークに関する調査研究について

内容

- PKI と利用上のノウハウ
- 電子認証の普及と BCP
- 電子認証フレームワークとは
- 電子認証に関するガイドライン等の状況

ほか

2. 電子認証フレームワークに関する調査研究について

2.1. 調査研究の背景

近年、インターネットは情報インフラとして認知されるようになっている。日本におけるインターネットの普及は 1990 年代に遡るが、その中で World Wide Web（以下、Web と呼ぶ）の普及は大きな原動力であった。2005 年現在、携帯電話を使って Web の閲覧をしたり電子メールをやりとりしたりできることは、もはや常識と言えるだろう。Web や電子メールはインターネットで使われているアプリケーションの一部に過ぎないが、これらを使って提供されるサービスは数多い。Web や電子メールはこれまで物理的な媒体で実現してきた広告やダイレクトメールを非常に高い費用対効果で代替するツールであるだけでなく、インターネットの双方向性を生かしたサービスを提供するプラットホームでもある。Web を使ったアプリケーションサービスは、しばしば「Web アプリケーション」と呼ばれる。

Web アプリケーションの発展は、特に商用 Web サイトに見ることができる。まず目に留まるのは広告であろう。ユーザが過去にアクセスした商品の情報を元に関連する商品を表示したり、他のユーザの購買履歴を元に、ユーザに「おすすめ」したりする。ユーザが商品に関する情報交換をするための掲示板が設置されていて、そこに書き込まれた商品レビューに対する評価の仕組みもある。様々な商品検討の材料が提供される上に、商品の購入は非常に簡単である。一般的に「カート」と呼ばれる仕組みで、一度クレジットカード情報等の支払い情報と商品の送付先の住所を登録しておけば、商品を選択して「購入」をクリックするだけで購入できてしまう。あとは商品が届くのを待つだけである。購入後は、商品の配送状況が電子メールで通知されたり、ユーザの好みを考慮した関連商品の広告が届いたりする。

小売の商用 Web サイトの他にも、Web アプリケーションによる各種サービス提供が行われるようになってきた。政府が取り組んでいる電子申請や電子入札、教育機関における資料の閲覧サービス、医療機関等で構築されている「Web ポータル」は、その構造上、ほぼ全て Web アプリケーションの仕組みが使われていると言える。民間企業の、顧客に対する各種申し込み等を含めると、企業や個人にとって日常的な活動に密着したサービスが Web アプリケーションで提供されつつあると言える。しかし、ユーザの利便性が高まる一方、これは非常に危険な状況ができつつあるとも言える。最もわかりやすい問題は、ID の盗用である。ID とはユーザを識別するためにコンピューター・システムがユーザを識別する為に割り当てる番号や記号のことで、対面で確認のできないインターネット越しのユーザを識別するために使われる。ID は、本来ユ

ーザ本人だけに使われるべきものであるが、もし他のユーザを別のユーザの ID を利用できてしまうと問題が起こる。前述した小売の商用 Web サイトの場合には、自分が注文していない商品が他人に勝手に注文されてしまったり、商品の届け先が変更されていて、支払いを負わされてしまったりすることが考えられる。企業活動で使われる ID の盗用が起きると被害は更に大きくなると考えられる。ID を盗用されたユーザが被害を受けるだけでなく、システムを提供しているサービス会社側でも発生した損害の賠償責任が問われ、信用の失墜も起こる。ID の盗用が起こるとユーザ側にもサービス提供者側にもメリットはない。Web アプリケーションの普及によって、日常的な活動が他人になり変わられてしまう危険性が大きくなる。

ID の盗用は人的な要素が大きく影響するため、完全に防止することは難しい。例えばパスワードが他人に知られた時に、ユーザ自身が気づくことは不可能であろう。しかし ID の盗用をより困難にし、盗用が起こった場合に追跡調査ができるようにするような対策を講じることはできる。例えばオンラインで本人を確認する「認証」を行うとき、パスワードだけでなく IC カードも使うようにすれば、ユーザはその IC カードが盗まれたことに気づいた時点で、その ID が悪用されないように利用を一旦停止するなどの対処ができる。また、そもそも偽の ID の発行が行われたような場合でも、その登録の記録が残っていれば何が原因であったのかを後になってから調べ、責任の所在を明らかにすることができる。

電子認証の技術は、IDの盗用のような被害を防止する対策となる技術である。パスワードも電子認証技術の一種で特定の情報を「知っていることによる認証」である。その他にICカードなどの認証トークンを用いた「物を持つことによる認証」、指紋や虹彩などユーザの「特徴による認証」などの分類がある[1]。電子認証の技術は、しばしば暗号技術の発展の一環として捉えられることがある。例えば、暗号技術の発展によって元々のメッセージを解読することが難しくなり、従ってメッセージを送った本人になりすますことが難しくなる、といった捉え方である。しかし実際にその暗号技術を使ってシステムを運用させるにはいくつかの落とし穴がある。例えば、暗号化に使われた暗号鍵のデータは、本人しか知らない情報かどうかが確認されていないかも知れない。また元々本人だと思われていた人が実は本人でなかった時、その間違いの原因を突き止めて再発を防ぐ対策が取られているか、といったことである。

これらのことから、認証技術の利用には認証技術そのものの他に、適切に運用していくためのノウハウのようなものが必要であると考えられる。Web アプリケーション

[1] 「Network Security: Private Communication in a Public World」、Charlie Kaufman、Radia Perlman、Mike Speciner、ISBN: 0130614661

の多くで使われているパスワードを上記の暗号鍵に置き換えると、多くの落とし穴が考えられる。アクセスしているユーザが本物かどうか、その判断にはどのようなチェックが行われたのかといった点である。このようなノウハウに則って運用されなければ認証技術はその効果をほとんど発揮しない。Web サーバの認証で使われている電子証明書の技術である PKI も同様のことが言える。

2.2. PKI と利用上のノウハウ

PKI は ITU-T の X.500 ディレクトリサービスの為の認証技術で、X.509 で勧告され標準化された技術である。X.509 の初版である 1988 年版には、既に認証情報の失効（ID の失効）の情報を伝達する仕組みが入っている。パスワードシステムに比べると処理は複雑であるものの、様々な利用場面が考えられる基盤の概念を規定している。1990 年代に入ると IETF で RFC（Request for Comments）としても策定された。現行の RFC3280 では電子証明書の検証方法の詳細がより明確になるなどしている。PKI は基盤的な技術で、特定のアプリケーションに特化した電子認証のために考慮されたものではない。そのため同一の認証情報、PKI の場合には「電子証明書」を、複数のアプリケーションで利用できるため応用性が高い。例えば複数の Web サーバにアクセスするときに一度認証手続きを踏むだけで複数のサーバにログインできる「Single Sign On」の実現に利用できる。

しかし電子証明書の発行手続きにもノウハウが必要である。PKI を使った認証では、認証手続きを受けるもの、例えばユーザは、実際に認証手続きを受ける前に電子証明書を発行してもらっておく必要がある。もし実際とは異なるユーザに電子証明書が発行されてしまうと、それ以降、本来のユーザになりすませることになってしまい認証の意味がない。電子証明書を身分証明書だと捉えると、その運用には新たな観点が必要となる。現実社会における身分証明書は発行に必要な手続きの種類は少なく、例えば日本国内のパスポートであれば、ほぼ一定の確からしさは推測できる。しかし PKI の「サーバ証明書」の場合は状況が違ってくる。サーバ証明書を発行する電子認証サービスは多数存在しており、運営主体も様々で、各々が独自の発行手続きを取っている。するとユーザにとっては見た目が同じサーバ証明書でも、確からしさは様々であるはずである。

すなわち、ユーザが証明書の信頼の程度を識別できるような指針が必要だと考えられる。PKI のような高度な認証技術を多くのユーザに普及することを考えると、このような指針や認証技術の運用ノウハウは、オープンなドキュメントとしてまとめられる必要があると考えられる。

2.3. 電子認証の普及と BCP

日本における PKI の利用に関しては、電子署名の分野について 2001 年に「電子署名及び認証業務に関する法律」が施行されて以降、関連の手続き等に対する常識的な想定事項が作られつつある。それに対し、電子認証の分野ではガイドラインなど実践の規範となるべきドキュメントがない状態にある。Web における SSL/TLS の証明書を用いた認証は一般にも普及しつつあるが、これに反してフィッシング詐欺などの脅威は高まりつつある。電子認証の技術が適切に利用されれば、サーバのなりすまし行為が直接的な被害の原因であるフィッシングを防止できると考えられる。電子認証の技術は、Web ブラウザに実装されていてもそれがこれらの不正行為を防げるような方法では利用されていないのが現状である。

電子認証サービスに関する利用・運用の指針やガイドラインがないことは、リスクに応じた対策を講じることを困難にしているとも言える。ユーザはリスクが高い場合と低い場合とを区別することが難しく、リスクが高い場合でも個人情報を入力してしまったりする。これでは電子認証の技術を利用する意味が薄れてしまい、今後の電子認証の普及を阻害する要因ともなりかねない。

一方、これまで IETF 内の PKIX WG において PKI の基本的なプロファイルやプロトコルの策定が行われてきている。しかし PKI の利用場面では、もはや基本的なプロファイルだけでは足りず、「有効で目安となる使い方」の情報が必要とされている。この Best Current Practice はほとんど蓄積されておらず、PKI を利用してシステムを構築している SI 業者や開発者において短期的な開発方法が用いられるなど、PKI の利点を生かしきれていない状況がある。そこで、この PKI に関する「有効で目安となる使い方」をまとめるべく、民間組織が策定活動に参加して業界での Best Current Practice を策定し、ガイドラインとしてとりまとめることが期待されている。

2.4. 電子認証フレームワークとは

電子認証フレームワークとは、「有効で目安となる使い方」を民間組織が中心となって業界での Best Current Practice を策定する仕組みである。2004 年度、IP アドレス認証局の調査研究を行っている際に、認証技術の専門家による議論の中で必要性が明らかになってきたもので、認証技術の適切な普及に欠けている部分であると考えられている。この仕組みの具体的なあり方は本調査研究を通じて明らかにしていくが、これまでに判明している状況の中では、例えるならば IETF の Best Current Practice 版だと考えられている。

電子認証の技術の利用には、各業界に共通の基盤的要素と業界やアプリケーション毎の応用的要素がある。各々の要素に対して「有効で目安となる使い方」を集約することで、業界に共通のノウハウ、または該当業界におけるデファクトスタンダードとなるノウハウがドキュメント化されることが考えられる。その為には、IETF におけるプロトコルの標準化活動と同様に、民間組織によって主体的な活動を行い、利用場面やアプリケーションに即したガイドラインを迅速に策定していく必要がある。

すなわち電子認証フレームワークは、民間組織における電子認証の適切な利用を促進するための枠組みである。

2.5. 電子認証に関するガイドライン等の状況

電子認証の利用や運用に関するノウハウをドキュメント化していくことを考えるにあたり、内容やその策定仕組みとしてどのようなものが必要になってくるのか、という点がポイントになる。ここでは既に明らかになっているガイドライン等の策定に関わる状況について述べる。

（1） 民間で利用できるガイドライン・ドキュメントの欠如

はじめに挙げられる点は、政府機関における電子認証のガイドライン・ドキュメントが国内外において整備されつつある中で、民間サービスで利用できるものが存在しないことである。現在、日本で電子認証に関して利用できる適切なガイドライン・ドキュメントが存在しない。具体的な状況としては以下に示す。

- 米国では e-Authentication Guidance で定められた 4 段階のレベルのレファレンスがある、日本では同様のレベル付けはない。
- 監査基準を一種のガイドラインとして捉えると、WebTrust for CA などが該当するドキュメントとして挙げられる。しかし CP（Certificate Policy – 証明書ポリシ）を規定していなかったり、現在の要求水準からは不足と思われる項目が少なくなかったりする。
- 現状では日本国内で提供されている電子認証サービスおいて、セキュリティに関する保証レベルを評価することができない。認証業務の安全性レベルは、電子認証サービス毎に独自に設定されるもので、ユーザがサービスごとの安全性レベルを比較するにはエンドユーザにはわかりくい CPS を読んだり、認証局の監査報告書を見たりする必要がある。そのため、ユーザは費用の高いサービスがセキュリティも高いと認知されるなど、実態に即したサービスの評価がなされていない。

（2） 脅威の高度化

電子認証におけるセキュリティ上の脅威としては、以下の状況が認められる。

- Web における SSL/TLS の安全な利用については、検証できない証明書を信用しないなどの普及啓発が進みつつあるが、正式な証明書を用いたフィッシングサイトが出現するなど、電子認証の利用に際して利用者に求められる知識も高度化しつつあり、適切な利用を阻害する原因となりかねない。

（3） 日本の認証に固有の条件

上記(1)(2)の状況に加え、ガイドライン・ドキュメントを策定する活動を行う場合、日本では以下のような事情を考慮する必要がある。欧米で規定されたものをそのまま適用できない。

- 人を対象とした認証の場合、欧米諸国では個人名での認証のみを考えればよいのに対し、日本では個人名のほかに、役職名による認証を行う場合がある。これは特に法人などを対象とした認証サービスを行う場合には欠くことのできない条件となる。

2.6. 日本におけるこれまでの取組み

電子認証を対象としたガイドライン・ドキュメントに関連するこれまでの取組みとして、以下の事例が挙げられる。

（1） 認証局運用ガイドライン（電子商取引実証推進協議会（ECOM））

1.1.1.3(2)で示したように、ISO（International Organization for Standardization）や IETF 等で検討されている電子認証もしくは認証局に係わる各種のガイドラインの内容や、ECOM（Next Generation Electronic Commerce Promotion Council of Japan）内で認証局の実験を行ったプロジェクト等からの意見をもとに 1998 年 10 月に策定されたガイドラインである。

（2） 保健医療福祉分野PKI認証局 証明書ポリシ（厚生労働省）[2]

保健医療福祉分野においてサービス提供者及びサービス利用者への署名用公開鍵証明書を発行する「保健医療福祉分野 PKI 認証局」による証明書発行（失効も含む）に

[2] 保健医療福祉分野PKI認証局 証明書ポリシ
http://www-bm.mhlw.go.jp/shingi/2005/04/dl/s0401-1a.pdf

関してその適用範囲、セキュリティ基準、審査基準等の一連の規則を定めるものである。厚生労働省における医療情報ネットワーク基盤検討会での審議を経て、2005 年 4 月に策定された。引き続き、公開鍵基盤認証局の整備と運営に関する専門家会合での検討が続けられている。

（3） 時刻認証基盤ガイドライン（タイムビジネス推進協議会）[3]

これまで時刻の証拠能力の担保に関してはその重要性に反して指針が存在しなかったことを問題意識として、政府・地方公共団体におけるタイムスタンプの利用に焦点を置いて 2003 年 3 月に策定された。タイムスタンプに関するガイドラインとして利用側における要件、提供側における技術基準、運用基準等を規定している。

（4） 電子認証ポリシーガイドライン（日本 PKI フォーラム）

現在、日本PKIフォーラムの相互運用技術検討部会ポリシーサブワーキンググループにおいて検討が進められている。電子認証に必要とされるセキュリティレベル、信用レベル等について国内及び海外の調査を実施し、事業化において必要とされる電子認証のポリシについて検討することが予定されている。[4]

2.7. 電子認証フレームワークに期待されること

電子認証フレームワークは諸外国のガイドラインと異なり、民間組織に利用されることを想定する。民間組織による電子認証を踏まえて、電子認証フレームワークに期待されるニーズを以下に挙げる。

（1） 電子認証の適用用途からのニーズ

電子認証フレームワークの適用が望まれている用途としては、以下が挙げられる。

- ユーザ認証
  民間組織内、または組織間のユーザ認証の保証レベルを明らかにし、企業間取引において利用できるようなユーザ認証の制度面の整備が必要とされている。大学間のユーザ認証の連携や、医療分野における認証の連携、企業間取引の際に有効とみなされるユーザ認証の保証レベルなどである。

[3] タイムビジネス推進協議会, 時刻認証基盤ガイドライン, 2003.3.
[4] 日本PKIフォーラム 2005 年度活動計画
http://www.japanpkiforum.jp/info/plan/2005/pl_sougo.htm

- IP アドレス認証
  JPNIC において取り組んでいる IP アドレス認証局は、日本国内の ISP の業務管理者や業務担当者の認証を行うための電子証明書の発行を行っている。この電子証明書は必ずしも自然人を対象としたものではない。ユーザが対象組織に所属していることを確認したり、個人の匿名性を確保しつつ不正発見時の追跡を可能にしたりすることを目的としている。いわゆる「三文判 PKI」の一種と考えられる電子認証である。このような電子認証は既存のユーザ認証システムに組み込みやすく、電子認証の適切な利用を促進しうるものだが、業界内でのデファクトとしての認知が欠如しているなど制度面での整備が必要となる分野である。
- サーバ認証
  サーバを対象とした認証についてはこれまでも行われているが、その認証の保証レベルや業界における認知については上記の IP アドレス認証と同様、あいまいである。一様に Web ブラウザの「鍵マーク」が表示されることで一部の業界ではよしとされている面があるが、実際にはこれはサーバの成りすましをユーザに気づかせることができない、間違った認識である。電子認証の保証レベルなど、業界内での整備が必要である。
- 法人の役職名による認証
  日本の法人においては幅広く行われている承認形態でありながら、欧米にはない慣習である。社内や特定の取引関係グループの内部など、これまでも限られた範囲内での認証サービスにおいては、役職名による認証の有効範囲を内部的に決定することで実現されてきたケースも多いが、電子認証サービスの普及に際しては、より普遍的な規範となるべきものが求められる。

（2） 電子認証フレームワークの仕様に関するニーズ

一方、フレームワークが提供すべき仕様に関するニーズとしては、これまで示してきたように日本国内では電子認証サービスの比較において、セキュリティに関する保証レベルを評価することができないことから、以下のバリエーションに応じた電子認証サービスを提供するためのフレームワークを用意することが求められていると考えられる。

- 電子認証に関係する役割の整理
  電子認証の技術を利用するには、サービス提供者とサービス利用者の他に、認証サービス事業者や監査人等の関係組織がある。またアプリケーションベンダーは出荷時に、特定の認証局を信頼する設定にしておくことが多い。その他に、実際に電子認証の設計を行うのが、システム・インテグレーターやソリューション・ベンダーと呼ばれる業者であることが多い。電子認証の適用にあたって関係組織の整理を行う必要がある。
- 保証レベル
  民間組織における認証の安全レベルは、特定の基準に則って形成されるよりも、

サービスに必要な最低限のものとして設定されると考えられる。従って、諸外国の政府のガイドラインのようにすべてが準拠性を要することが適するとは考えにくい。業界に共通する部分は準拠性を以って適切な普及を図りつつ、業界毎の部分は各業界のセキュリティ文化の向上を図りつつ規定する必要がある。

2.8. 電子認証フレームワークのあり方に関する調査事項

電子認証フレームワークのあり方に関して調査研究を実施するにあたり、「電子認証の運用に関するドキュメントに関する基本調査」と「電子認証の技術とドキュメント策定プロセスに関する調査」を行った。

電子認証の運用に関するドキュメントに関しては、既存の電子認証の運用に関わるガイドライン・ドキュメントについての基本調査を行った。本調査では、ガイドラインと捉えられる既存のドキュメントについて諸外国及び日本国内の状況を踏まえて調査を行った。

電子認証の技術とドキュメント策定プロセスに関しては、電子認証技術である PKI のプロトコル策定動向について、IETF のミーティングに参加し調査を行った。また IETF においてドキュメント策定プロセスの見直しに関わる活動が始まっているため、関連 WG に参加し動向を調査した。

次章では、電子認証技術である PKI の国際動向について述べ、その状況を受けて行ったこれらの基本調査については第 3 章で述べる。