7　不正アクセスを防ぐための新たな技術

(1) ワンタイムパスワードによる認証

ワンタイムパスワードは、多要素認証における「知識：自分だけが知っているもの」、「所持：自分だけが持っているもの」、「属性：自分自身」のうち、「所持」により個人認証を強化するものである。

インターネットバンキング等の遠隔地にあるコンピュータから、ネットワークを通じてサービスを提供するサーバにアクセスした場合、フィッシング、スパイウェア、キーロガーなどにより、ID やパスワードを盗まれる危険性があり、固定の ID やパスワードでは、なりすましにつながることになる。

ワンタイムパスワードは、1 回限りで無効となる使い捨てのパスワードが都度に生成されるため、第三者によるパスワード悪用などのリスクは小さくなる。

ワンタイムパスワードを生成するには、専用機器によるハードトークンか、携帯電話などにインストールするソフトトークンを利用する。ハードトークンでは、キーホルダータイプの小型ものが製造されており、ソフトトークンでは、携帯電話を利用することが主流となっている。

専用機器によるハードトークンは、トークン自体がスパイウェアに感染することもないため安全性が高いが、コストや配布方法の問題に加え、紛失の危険がある。携帯電話によるソフトトークンでは、専用機器を利用しないためコストが低いが、利用者自身がダウンロードやインストールをしなければならないことや、携帯電話を買い換えた場合には登録変更の手続きが必要など利用者への負担が大きい。紛失の危険は、ハードトークンと同様である。

ワンタイムパスワードは、サーバとトークンとの時刻同期を利用する。一定時間ごと（約 30 秒～1 分のタイプが多い）に異なる数字が生成され、液晶画面に表示される。生成されたパスワードは、ボタンを押したときのみ液晶画面に表示される仕組みである。利用者は、表示されたパスワードをコンピュータに入力し、サーバ側で正規のユーザからのものであるかどうかを確認する。パスワードが万が一盗まれたとしても、そのパスワードの有効期間は最大でも 1 分しかなく、次回は利用できない使い捨てタイプであるため、高い安全性が保持できる。

製品としては、RSA セキュリティ株式会社の「SecurID」が代表的なものであり、導入企業も多い。国内外のデファクトスタンダードになっている。

但し、ワンタイムパスワードでも防げない「中間者攻撃（man-in-the-middle attack）」というようなタイプの攻撃手法もでてきている。これは、通信を行う二者の間に割り込んで、両者が交換する公開情報を自分のものとすりかえることにより、気付かれることなく盗聴したり、通信内容に介入したりするものであり、使い捨てのパスワードでも危険性があることが明らかになっている。

(2) リスクベース認証

「リスクベース認証」は、利用者の利用環境（利用者コンピュータのデバイス情報、IP アドレス、ISP、接続タイプなどのネットワーク情報など）やアクセスログ（口座の利用状況やアクセスの時間帯・場所など）から利用者の行動パターンをリアルタイムで総合的に分析し、不正利用の懸念があるアクセスを検知した場合には追加認証を行い、本人確認の確度を高めるものである。

万が一、利用者の ID やパスワードが第三者に知られ、不正な第三者が利用者の普段の利用環境とは異なる環境からアクセスしてきた場合には、追加で認証を行うことで、第三者による不正利用防止に有効な対策どなる。

追加認証は、デバイス ID の入力、ハードウェア・ソフトウェアトークン、トランザクション署名、チャレンジ質問、または電話やメール、SMS によるアウトオブバンド認証などで行えるが、チャレンジ質問による追加認証が多くなっている。これは、事前に登録しておいた「合言葉」と「答え」で認証を行うため、利用者の操作性にも配慮した新しい認証方式となっている。

不正利用の懸念がないアクセスには、追加認証は要求されないため、高いセキュリティと利用者の利便性を両立させる。さらに、ワンタイムパスワードの専用トークンの配布に比べ、導入コストを低減することが可能である。しかし、時間や場所のリスクを軽減できるが、取引が発生するごとに要求される認証ではないため、取引のリスクの低減につながらないという面もある。

米国では、2005 年 10 月に連邦準備制度理事会、連邦預金保険公社（FDIC）、米信用組合局（NCUA）、通貨監督官事務所（OCC）、貯蓄監督局（OTS）の 5 機関から構成された連邦金融機関調査評議会（Federal Financial Institutions Examination Council : FFIEC）が発表した合同ガイダンス「インターネットバンキング環境における認証」で、加盟銀行に対して、オンラインバンキングを単一要素による認証から二要素認証にするよう推奨された。正式な法令ではなく、法的義務はないが、これによりワンタイムパスワードやリスクベース認証への機運が高まった。

(3) 生体認証

生体（バイオメトリクス）認証は、人間の身体的特徴（指紋、虹彩、顔など）や行動的特徴（動作や癖など）を用いて行う個人認証技術である。

ID、パスワード、トークンによる認証では、忘却や紛失によって本人でも認証できなくなったり、漏洩や盗難によって不正な第三者になりすまされて認証される恐れがある。生体認証は、長いパスワードや複数のパスワードを覚えたり、トークンを持ち歩いたりしなくてもよいため利便性があり、紛失、盗難、忘却といったリスクも低い。自分自身の特徴で認証を行うため、セキュリティが高いとい

うメリットがある。

その反面、生体情報は生涯不変なため、一度でも情報が漏洩すると致命的なリスクを負うことにもなる。生体情報はパスワードのように一旦漏洩したとしても取り替えることができないということが最大のデメリットとなる。また、誤認証がゼロではないことやなりすましが可能なことも指摘されている。

オンライン上のサービスで生体認証を利用する場合には、利用者のコンピュータに生体認証を行うためのデバイスが必須であり、配布方法やコストの問題もある。加えて、サービス提供者側においても、生体情報を安全に管理するためのコストなど負担は大きいといえる。

(4) 携帯電話を利用した認証

携帯電話を利用した認証では、コンピュータと携帯電話を連携させ、携帯電話のメール機能を利用して認証を行う事によりセキュリティの精度を向上させる個人認証システムが利用され始めている。サービスを提供しているサイトにて、携帯電話のメールアドレスを登録し、そのメールアドレスに届いたメールに記載されている URL に携帯電話からアクセスすることで、ユーザ認証が完了するものである。ソーシャルネットワーキングサービス（SNS）「GREE」の 会員登録などで実際に利用されている。

携帯電話のカメラ機能を利用し、サービスを提供しているサイトにて表示される二次元バーコードを読み取るという個人認証もでてきている。これは、利用者がコンピュータからサービス提供サイトで ID とパスワードを入力すると、コンピュータの画面に「QR コード（2 次元バーコード）」と「バーコード番号」が表示される、利用者は、カメラ付き携帯電話のバーコード読み取り機能でそれを解読する。2 次元バーコードには、特定の URL が書き込んであり、携帯電話のインターネット接続機能で「パスワード」認証を使い、特定のサイトにアクセスすることで、コンピュータからアクセスしているサイトの認証が得られる仕組みである。表示される 2 次元バーコードは、ログイン時に生成し、表示する。

携帯電話を使うことで、「携帯電話の端末 ID」と「ユーザ・パスワード」の 2 つのキーを利用して、不正アクセスを防ぐ。また、携帯電話インターネット接続に、パスワード認証を用いることで、携帯電話を紛失したり、盗難にあっても、保護できる特徴があるという。

(5) IC カードを利用した認証

IC カードを利用した認証は、国税電子申告・納税システム（e- Tax）に代表される公的個人認証サービスにも利用されている個人認証方式である。

IC カードによる個人認証では、利用者のコンピュータに接続した IC カードリ

ーダから、IC カードを読み込んだ状態でなければログインできない仕組みになっており、事前に登録したパスワードを入力させることが多い。

IC カードによる認証では、専用トークンに比べて低コストである、IC カードの券面を身分証明書にすることができる、カードリーダに IC カードを読み込んだ状態で認証できるというメリットがあるが、貸し借りができることや、IC カードを読み込んだ状態のまま離席すると第三者の利用が可能になるといったデメリットもある。また、利用者のコンピュータに IC カードリーダが必要であり、そのコストを誰が負担するのかといった問題もある。

公的個人認証サービスでは、多要素認証の所持（IC カード）、知識（パスワード）に加えて、PKI 認証を用いることにより安全性を高めている。

(6) PKI 認証

PKI（Public Key Infrastructure、公開鍵暗号基盤）とは公開鍵暗号方式を利用したセキュリティ基盤のことであり、PKI 認証はこの PKI を利用した個人認証の仕組みである。

公開鍵暗号方式では、対になっている「公開鍵」と「秘密鍵」の 2 つの暗号鍵を利用する。この 2 つの鍵の組み合わせを「鍵ペア」と呼び、「片方の鍵（公開鍵（または秘密鍵））で暗号化した情報は、もう片方の鍵（秘密鍵（または公開鍵））でないと復号できない」ようになっている。

暗号化用途で PKI を利用する場合は、例えば秘密のメッセージを送受信する際には、送信者は受信者が公開している公開鍵を入手してメッセージの暗号化を行う。暗号化されたメッセージは受信者の持つ秘密鍵でしか復号できないため、途中で第三者に傍受されても中身を解読されることはない。

認証用途で PKI を利用する場合は、例えば利用者 A が Web サイトでログイン認証する際には、サイトから送られてきたチャレンジコードに対して、利用者 A は自分の秘密鍵 A で暗号化したレスポンスを送り、サイト側にて利用者 A の公開鍵 A で復号化して照合することによって、アクセス者が確かに秘密鍵 A を持った利用者 A であることを認証する。

PKI 認証は高いセキュリティレベルの認証を実現できるが、利用方法は複雑であり、利用者のリテラシーがある程度高くなければ利用は難しいといえる。利用者の利便性の向上を図らないかぎり、インターネットバンキングやネットショッピングなど、利用者のリテラシーが多様な場面では早期に導入を図ることは難しいといえる。

(7) 3D セキュア

3D セキュアは、クレジットカードによるインターネットでの決済に利用される

本人認証サービスであり、クレジットカード情報の盗用による第三者のなりすましといった不正利用を防止する仕組みである。VISA（VISA 認証サービス）、MasterCard（SecureCode）、JCB （J/Secure）といった大手クレジット会社で導入が開始されている。

従来、オンラインショッピングなどの決済にクレジットカードを利用する場合、利用者が入力した「クレジットカード番号」や「有効期限」などから、そのクレジットカードが有効であるかどうかを確認する。3D セキュアでは、それらの情報に加えて、本人しか知らないパスワードを入力することで、クレジットカードの利用者以外の第三者に不正に利用されていないかどうかを確認することができる。

利用者は、事前にクレジット会社にパスワードを登録するだけで簡単に利用できる。

ショッピングサイトなどのサービス提供者は、3D セキュアに対応した認証ページを作成し、クレジット決済を行う際、利用者にクレジット会社に事前登録したパスワードを入力させ、認証を行う。パスワードは、クレジット会社に暗号化されて送信される。これによって、従来より安全にオンライン上での買物ができる。

ただし、現在 3D セキュアに対応したクレジットカードを発行しているのは大手だけであり、まずは、すべてのクレジット会社でこの新しい技術に対応したカードが発行されるよう業界全体の取り組みが必要となる。

また、利用者側も、クレジット会社に登録してあるパスワードを失念している人が多いため、3D セキュアを必須にするには、周知徹底の期間が必要となる。

実際の店舗における買物においても、クレジットカードで決済する場合に、サインで本人確認するか、パスワードで本人確認するかを聞かれることも多くなってきており普及は早いと見られる。