日経産業新聞フォーラム2008

オンラインサービスにおける顧客の安全を約束するセキュリティー

～安全の可視化と利便性維持とは～

ネットワーク社会の進展で、私たちの生活の利便性は飛躍的に向上した。インターネットを活用したオンライン取引も増加、そのため安心・安全に取引を行うセキュリティー対策が求められている。そういった中、このほど日経産業新聞フォーラム2008「オンラインサービスにおける顧客の安全を約束するセキュリティー～安全の可視化と利便性維持とは～」が開催された（主催＝日本経済新聞社、協賛＝日本ベリサイン）。フォーラムでは日本銀行決済機構局企画役の中山靖司氏が「金融業務と情報セキュリティー技術。現状と今後の展望」をテーマに講演。続くセッションではそれぞれの立場からセキュリティー向上と利便性の維持や、その取り組みについて紹介された。

基調講演

金融業務と情報セキュリティー技術
現状と今後の展望

日本銀行
決済機構局企画役
中山靖司氏

安全であることを分かりやすく表示

金融業界は比較的オンライン化を早く進めた業界の一つであり、安定性とセキュリティーに優れたメーンフレームや専用回線などを活用してきた。かつては金融ハイテク犯罪が発生することはほとんどなく、暗号化や電子署名が使われることはまれであった。

しかしこの十年で状況は一変。金融機関もオープン環境やネットワークでサービスを提供し、インターネットバンキングや電子マネーといった新しいサービスも登場した。

増えるネットバンキング

いまやインターネットバンキングは、金融機関にとって重要なチャネルの一つになっている。二〇〇七年三月末現在の口座数は約二千四百万口座、インターネット専業銀行も社会に定着しつつある。電子商取引の決済や公共料金の支払い、家計簿ソフトと連動したアプリケーションなどサービスは多様化している。

そうした中、偽造キャッシュカードをはじめとする金融ハイテク犯罪が問題化。〇三年にはインターネットバンキングのIDとパスワードが盗まれ、口座から預金が不正に引き落とされるという事件が起こった。

その後メールに添付された不正プログラムを知らずに実行した結果、スパイウエアが埋め込まれいつの間にかIDとパスワードがネットワーク越しに盗み出されるなどの犯罪も発生している。手口は複雑・巧妙化し、実態が分かりにくくなっているため、気づかずにいる被害者もいるかもしれない。現在ではセキュリティーを確保するには、暗号化や電子署名、ICカードや生体認証といった新しい技術を適切に活用していくことが必要となっている。

利便性とのバランス考慮

フィッシング詐欺はこれまで不特定多数に向けた単純なメールやスパイウエアを使ったものが主流であったが、最近では標的を絞るようになってきた。攻撃者がサーバーと利用者間に介在して情報を盗んだり、情報を改ざんする中間者攻撃も発生。将来どのような攻撃が登場するか予測は難しいが、いち早く対策を講じるには最新の犯罪手口を認識しておくことが重要である。

これらの対策として、本人認証の強化は必須だ。本人認証の方法は暗証番号やパスワードのような「知識」、鍵・カードといった「所有物」、生体認証のような「本人固有の特徴」によるものの三つに分けられる。このうち二つ以上を組み合わせて認証する多要素認証が当たり前になりつつある。

一方、利便性とのバランスを考慮することも大切だ。例えばリスクベース認証では、いつもと違うIPアドレスから接続するといった不審な挙動があると、追加の認証を要求するなどより確実な本人確認を行う。通常は面倒がないよう必要最低限の認証しか行わないが、危険を察知したときだけ追加的に認証を増やすというバランスの取れた手法だ。

本人認証の強化とともにもう一つ重要な対策が、顧客が不正なサイトにアクセスしないようにすること。これまでSSL証明書を使った暗号化通信が行われていれば安全と思われていたが、最近はそうとも言い切れない。紛らわしいドメインを取得して、SSL証明書を導入しているケースもある。

そこで注目されているのが「EV SSL証明書」。これはSSL証明書の一種で、法人として登記されているかなどの実在確認に関する審査基準が厳しくなっているものだ。最新のブラウザーでは証明書が導入されているとURLを表示するアドレスバーが緑色になり、その右側に企業名が表示される。一方、赤色が表示されると危険なフィッシングサイトなどの可能性が高い。

このようにブラウザーの基本機能だけでひと目で安全を確認できるのがポイントだ。追加的な導入コストがそれほど必要ない割にははっきりとした効果が期待できることもあり、今後企業の標準的な対策になると思われる。

多様な技術組み合わせる

もう一つ注目されるのが、産業技術総合研究所が開発した「パスワード相互認証方式」。これは本人認証とサイト認証の両方を行うもので、多要素認証だけでは防ぎきれない中間者攻撃にも有効だ。こうしたセキュリティー技術がインターネットの標準機能としてブラウザーに搭載されるようになれば、フィッシング対策の有効な手段になるかもしれない。

セキュリティーの基本は、リスクの所在と大きさを正しく認識し、これをコントロールすることだ。リスクをゼロにすることは不可能であり、あらかじめ想定した許容範囲に抑え込むとの考え方が現実的だ。その際利便性やセキュリティーレベル、コストのバランスにも配慮する必要がある。

情報セキュリティーは、さまざまな要素技術を組み合わせて総合的に実現されるものだ。金融機関は、その情報セキュリティー対策の実効性を正しく評価するとともに適切な情報開示を行い、時には第三者の客観的な評価を受け、顧客からの信頼性を向上させるよう努力し続けていくことが必要である。

セッション①

勝機をつかみ、成長を維持するための
セキュリティー向上とユーザー利便性の維持

日本ベリサイン
執行役員
マーケティング本部長
柴田　斉氏

EV SSL証明書や二要素認証
インターネットの安心・安全提供

インターネットは検索やブログの閲覧、オンラインショッピングの利用など、もはやインフラとして定着している。しかし利用に関して不安を感じているユーザーは多い。

ベリサインはインターネットの安心・安全を構築するために一九九五年に米国で誕生、翌年に日本法人が設立された。現在世界七十五カ国でビジネスを展開、日本ではサーバー証明書をはじめとする認証ビジネスのリーディングカンパニーである。

当社が昨年実施したインターネットユーザーの調査では、「オンラインショッピングでID・パスワードを不正に利用される不安」「フィッシングサイトなどで個人情報漏えいが心配」といった回答が多かった。

サービスを提供する企業には、顧客のこのような不安を和らげる対策が必要である。セキュリティーの難しいところは利便性を損なわず、できるだけ分かりやすく対策を講じることだ。安全を可視化できるように提供することは、インターネット上の安全性を高めるだけではなく、ブランド構築とロイヤルティーを高める役割を果たす。

アドレスバーが緑色に

セキュリティーの見える化には当社も提供しているEV SSL証明書が有効だ。インターネットエクスプローラー7・0などでアクセスするとアドレスバーが緑色に変化する。これまでブラウザーの下に表示されていた鍵マークがアドレスバーのすぐ横に表示され、ウェブサイトを運営している組織名、発行した認証局が表示される。企業などのホームページにアクセスしようとするとき、検索結果の上位サイトがフィッシングサイトの可能性もある。サイトの実在性を証明することはサイトに訪問した顧客を離反させない要素でもある。すでに金融業界をはじめ、多くのイーコマースやインターネットサービス分野で「EV SSL証明書」が導入されている。

そのほか、メール配信元の実在性を証明する「セキュアメールID」がある。電子証明書による電子署名をメールに付与することで電子メールの発信者を確認できるサービス。メールの送信元の実在性が日本ベリサインによって認証された企業・組織であることと、電子メールの内容が通信途中で改ざんされていないことを、顧客は特別な知識なしに確認できる。

ユーザーIDとパスワードを使った二要素認証も提供している。登録したパスワードに加えトークンなどによりその都度生成する使い捨てのパスワードを組み合わせることで強固な認証となる。そのためパスワードなどを推測されることや不正取得されることが起こりにくい。ユニークなのは、OATHというオープン規格を採用していること。この規格は世界中で取り組まれている二要素認証を活用した認証強化法の標準になっている。標準技術をベースとしたオープンアーキテクチャーによって既存のインフラとの統合が容易で、将来にわたって拡張できるメリットがある。

行動パターンの異常検知

リスクベース認証は、オンラインサービスを利用する一人ひとりの顧客の行動パターンを自己学習する。異常な行動パターンが検知されたときに、追加の認証を要求する。

サイトで勝機をつかむためのセキュリティー対策とは、顧客にとって安全性が分かりやすく表示されること。事業者側の対策だけでなく、顧客自身が脅威から身を守るための対策も必要だ。そのために啓発活動は重要で、継続して取り組むことが大切である。当社はより使いやすいセキュリティーを提供し、安心・安全なネットワーク環境を構築するために努力していく。

セッション②

オンライントレードにおける情報セキュリティー
～信頼性向上に向けた大和証券の取り組み～

大和総研
証券システム統括部長
田中宏太郎氏

SSL使った暗号化通信を活用
「脅威の見えない化」に人的対策

ネットと店舗を両輪に

大和証券は一九八六年にパソコンホームトレードを開始。九六年四月からインターネット株式取引である「ダイワ・ダイレクト」を開始している。これを皮切りに日本でもインターネットを活用したオンライントレードが幕を開けたと評価されている。

インターネット株式取引は百二十店舗、業界最大規模の四百五十席のコールセンターでサポート。この体制が万が一のシステム障害時にも有効となっている。それは、店舗・コールセンターで緊急受注ができるなど、顧客への影響を最小限に抑制できるからだ。

インターネット株式取引のような電子商取引のセキュリティー上のリスクは主に四つある。取引情報を盗み見られる「盗聴」、取引情報が書き換えられる「改ざん」、第三者が本人のふりをして取引する「なりすまし」、取引事実を否定する「否認」である。

これらの対策にはまず、SSLを使った暗号化通信を活用している。本人認証時にはログインパスワードが必要だが、一定回数間違えるとログインをロックしている。ロック時やログインパスワード失念時は、支店やコールセンターで本人確認後、仮パスワードを発行する。このパスワードは口座開設時に登録した住所に配達記録郵便で送付するため、不正入手は困難である。

また取引画面では最終確認画面で、ログインパスワードとは別の暗証番号の入力が必要である。この暗証番号の変更はネットでは不可能である。万一の場合、有価証券を売却して換金し、出金するケースが考えられるが、ATM出金時にはダイワカードが、店頭では届け印が必要である。ウェブ出金（振込）時は、口座開設時に指定した預貯金口座が対象になるため、任意の口座を指定できない。

利用者の確認負担軽減

「情報セキュリティ白書2007年版」によると、最近の傾向として「脅威の見えない化」が進行している。昨今の脅威は、「悪意を持った犯罪へ」「標的型攻撃へ」「脆弱（ぜいじゃく）性を狙う方法へ」「人間の心理を突いた巧妙な攻撃へ」と変貌（へんぼう）してきており、利用者が意図せず情報流出の被害を拡大させているという。セキュリティー対策のうち、人的対策がより重要になってきているといえる。

人的対策として急務なのが多様化するフィッシング対策だが、注目されるのがEV SSL証明書だ。世界標準の認証ガイドラインに基づき、運営サイトの実在性を確認する方法が厳密に規定されている。インターネットエクスプローラー7・0を搭載していれば緑色のバーが出るので、視認性に優れている。

サイトの安全性確保と利用者の確認負担を軽減することは、運営者の責務であるとの認識から、EV SSL証明書をダイワのオンライントレードでも導入している。サイトを運営する大和証券と証明書を発行する認証局であるベリサインのロゴが交互に表示される。業界一位の実績と携帯電話への対応が進んでいるため、日本ベリサイン製を採用。ウィンドウズ・ビスタやXPにも対応していることなども選択の理由だ。

システム障害やセキュリティー事故は自社内にとどまらず、社会的影響を及ぼす可能性がある。これらを情報システムのリスクととらえ、適切にコントロールすることが、企業にとってますます重要な経営課題となっている。