IMES DISCUSSION PAPER SERIES

金融業界における情報システムの脆弱性検知と情報共有

岩下 直行（いわした なおゆき）

Discussion Paper No. 2005-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
http://www.imes.boj.or.jp

IMES Discussion Paper Series 2005-J-6
2005 年 4 月

金融業界における情報システムの脆弱性検知と情報共有

岩下 直行（いわした なおゆき）*

要　旨

ネットワークを経由して提供される金融サービスが一般的なものとなるにつれて、金融業界にとって、情報システムのセキュリティ対策が益々重要な課題となってきている。金融業界の情報システムは、偽造キャッシュカードによる不正預金引出しから、フィッシング詐欺、インターネット・バンキングの不正取引に至るまで、様々な脅威にさらされている。金融業界にとって、こうした脅威の原因となっているシステムの脆弱性を正確かつタイムリーに検知し、その是正に戦略的に対応していくことが必要となってきている。金融業界全体の問題として、脆弱性の検知とその情報共有のための体制整備に向けた話し合いを始めるべき時期に来ていると考えられる。

本稿では、金融業界において、情報システムの脆弱性を早期に検知したうえで、その情報を業界内で適切に共有していくために、どのような対応が考えられるかについて検討する。

キーワード：脆弱性、情報セキュリティ対策、脆弱性関連情報届出制度、
偽造キャッシュカード、インターネット・バンキング
JEL classification: L86、L961、Z00

* 日本銀行金融研究所情報技術研究センター（E-mail: iwashita@imes.boj.or.jp）

本論文は、2005 年 3 月 29 日に日本銀行で開催された「第 7 回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。

目　　次

１．はじめに――銀行の金融ハイテク犯罪への対応

歴史的建造物として各地に保存されている古い銀行の建物には、頑丈な外観を持つものが多い。かつて銀行は、レンガ造りや花崗岩の外装、鉄格子のはまった窓、堅牢な金庫等によって、自らが、地震や火災、強盗などの脅威に対して高い安全性を持っていることをアピールしてきた。その頑丈な外観は、銀行の顧客にとって信頼の象徴であった。

しかし、現代の銀行が直面しているのは、そのような物理的な脅威だけではない。深夜のコンビニ ATM に挿入される偽造キャッシュカード、無差別に顧客に送りつけられるフィッシング詐欺[1]メール、インターネット・カフェのパソコンに仕掛けられたキー・ロガー[2]等、銀行を脅かす新手の金融ハイテク犯罪の手口が次々に出現している。これらの新しい脅威は、ネットワークを伝わり、遠隔地から銀行の情報システムを攻撃する。金融サービスに対する攻撃の技術が従来よりも高度なものになればなるほど、銀行にとって、情報システムのセキュリティ対策が重要な経営課題となってくる。

金融業界は、コンピュータによるネットワーク・システムを最も早い時期に整備した業種であった。1960 年代の第一次オンライン・システムに始まり、1970 年代には銀行内部の事務を飛躍的に合理化する第二次オンライン・システムが構築された。現在利用されているキャッシュカードや CD/ATM の基本設計は、第二次オンライン・システム構築時から 30 年間にわたって維持されてきたものである。1990 年代にインターネットが普及する以前は、コンピュータ・ネットワークといえばまず第一に銀行のオンライン・システムが挙げられる程の存在であり、その頑健性、安全性に疑いが差しはさまれることはほとんどなかった。銀行は、頑丈な建物によって守られるその物理的なセキュリティと同様に、情

---

[1] フィッシング（phishing）詐欺：　銀行等の利用者を、銀行が発信したように装った電子メールや偽のウェブサイトに誘導して暗証番号やクレジットカード番号を入力させ、個人情報を搾取する詐欺。

[2] キー・ロガー（key logger）：　キーボードからの入力を監視して記録するソフトウエア。元々はシステム開発に利用されるツールだったが、最近ではこっそりパソコンに仕掛けて利用者のパスワードを盗むなど、悪用される事例が増えている。

報システムのセキュリティについても、十分な安全性が確保されていると信じられてきた。

しかし、偽造キャッシュカード問題、フィッシング詐欺事件、インターネット・バンキングでの不正送金など、新手の金融ハイテク犯罪の手口をみせつけられた結果、銀行のセキュリティに関する顧客の信頼が揺らぎつつある。

もちろん、銀行は、こうした顧客の不安を解消すべく、様々な対策を打ち出してはいる。しかし、金融ハイテク犯罪の手口は高度化しており、常に最新のセキュリティ対策を講じていくことは、銀行にとっても容易ではない。銀行は、かつて、レンガ造りの建物でその信頼性をアピールしていたように、今、自らの情報システムのセキュリティ対策の信頼性について、顧客に積極的にアピールすることが期待されている。しかし、いったいどうすれば、顧客の信任を得ることができるのだろうか。

２．偽造キャッシュカード問題とその教訓

2005 年初に大きく報じられた偽造キャッシュカードによる預金引出しは、銀行が長年培ってきた情報システムのセキュリティ対策に対する信頼を大きく損なう事件であった。全国銀行協会によれば、2002 年度まではほとんどみられなかった偽造キャッシュカードによる預金引出しが、2003 年度以降急増し、2004 年 4 月～12 月の 9 ヶ月間で 307 件、8 億円に達した（表 1 参照、全国銀行協会[2005]）。2005 年 1 月に、ゴルフ場の貴重品ロッカーからキャッシュカードを盗み出してスキミングする手口で不正預金引出しを行っていたグループが逮捕され、マスコミで大きく報道されるなど、国民の関心が集まった。

表1：「いわゆる偽造キャッシュカードによる預金等引出し」に関するアンケート結果

（対象：正会員・準会員180 行）

時 期	件 数（件）	金 額 (百万円)
2001年度	1	19
2002年度	3	13
2003年度	92	277
2004年 4月～ 6月	53	188
2004年 7月～ 9月	68	271
2004年10月～12月	186	348

備考：1. アンケート結果は、自行の預金者からの申出があり、ジャーナル等を確認した結果、偽造キャッシュカードによる預金引出しである可能性が高い、もしくは偽造カードによるローンの借入れである可能性が高いと判断できたケースをカウント。
2. 「時期」とは、偽造キャッシュカードにより預金等引出しが発生した時期。
3. 「件数」は、原則として預金名義人単位。

出典：全国銀行協会 [2005]

偽造キャッシュカード問題は、年間被害額で高々数億円のオーダーであり、過去に発生したクレジットカードやプリペイドカードの偽造犯罪が百億円オーダーであったのと比べて、特に規模が大きいとはいえない。しかし、過去のカード偽造事件では、主としてカード発行者、システム運営者が損失を被ったのに対し、偽造キャッシュカード事件では、不正に預金が引き出された預金者個人に損失が発生し、被害額が補償されなかったことから、預金者の誰もが被害者になり得ると理解されたため、人々の不安が高まり[3]、社会問題化してしまった。

全国銀行協会は、IC カードや生体認証などの新技術の導入、被害者への補償などを内容とする対策を表明したほか、2005 年 3 月現在、関係者の間で様々な対応策に関する検討が進められている。

そもそも、様々なカードを偽造する技術の裾野が広がる中で、磁気ストライ

[3] マクロミル社が 2005 年 2 月に実施した、「銀行カードの安全についてのネットリサーチ結果」によると、20 才以上のキャッシュカードを利用する銀行預金者 1034 名のうち、約 9 割が、「キャッシュカードを使用することが不安を感じている」と回答している。
http://www.macromill.com/client/r_data/20050210bank/20050209bank.pdf

プ方式のキャッシュカードと４桁の暗証番号の組み合わせでは、最大で１日当たり数百万円もの預金引出しが可能となる認証手段としては十分な強度を持たないことについては、数年前から本シンポジウムでも指摘してきた[4]。金融業界もこうした問題が存在しうることは認識しており、全国銀行協会は、1988 年に IC カードの業界標準を制定し、その後の技術進歩に合わせて累次の改訂を行うなど、新技術の導入の準備を進めていた。しかし、実際には、(1) 過去 30 年間、磁気ストライプカードと暗証番号という技術が大きな問題もなく利用され続けてきたため、IC カードなどの新しい技術に移行するきっかけがつかめなかったこと、(2) 従来の技術が金融業界全体の基本インフラとして利用されてきたため、業界内の幅広い合意がなければ新しい技術への移行が難しかったことから、IC カードや生体認証などの新技術の導入にかかる意思決定が先送りされてしまったという側面があったことは否定できない。

今回、偽造キャッシュカード事件が社会問題化したことから、新技術の導入が急速に進む見通しとなった。しかし、批判を受けて新技術の導入を迫られるという事態は、金融業界にとって決して望ましいことではない。短期間で結論を出す必要があるため、新技術に関する十分な評価ができないのではないか、技術の選択を誤り将来に禍根を残すのではないか、といった心配もある。本来であれば、金融業界が自らの判断で、将来発生しうる脅威を想定して、既存の技術の脆弱性を評価し、十分なセキュリティ・マージンとリード・タイムを確保したうえで、戦略的に新しい技術に移行していくというのが望ましい展開で

[4] 例えば、1999 年 11 月に日本銀行で開催された第２回情報セキュリティ・シンポジウムでは、銀行のキャッシュカードと暗証番号による認証方式の見直しの必要性について、次のように指摘している（松本・岩下[2000]）。

「…(a)様々な技術革新によって印鑑、印影、各種印刷物、磁気カード等の偽造が容易になっていること、(b)暗証番号の盗用や推定が巧妙に行われるようになっていること、(c)金融機関側も、店舗の人員削減等により、従来ほどのセキュリティ対策への配慮が期待できないおそれがあること、等を考えると、「これまで大丈夫だったので、これからも大丈夫」と判断することには慎重であるべきと思われる。したがって、既存の金融取引で利用される認証方式についても、磁気カードよりも安全性の高い IC カードの採用や、暗証番号に加えてバイオメトリック認証を導入するといった選択肢について、検討のスコープを広げていくべきであろう。」

あった。

金融業界は、情報システムに巨額の投資をしているが、技術革新が進めば、既存の技術が陳腐化していくのは道理である。磁気ストライプカードの仕様が30 年間維持されてきたということ自体、例外的な現象であって、業界内で利用するインフラ技術は、定期的に更改を行っていかなければならない宿命にあるといえる。今回の偽造キャッシュカード問題を奇貨として、今後、銀行の情報システムの脆弱性を正確かつタイムリーに検知し、その是正に戦略的に対応していくための体制を構築していくことが望ましい。そのための議論を始めるべき時期ではないだろうか。

３．インターネット・バンキングのセキュリティを巡って

偽造キャッシュカード問題と並んで、銀行が提供しているインターネット・バンキングへの攻撃を巡る話題も、最近、マスコミで盛んに報じられている。大手銀行の名前を騙ったフィッシング詐欺メールや、インターネット・カフェのパソコンに仕掛けられたキー・ロガーを用いて、インターネット・バンキングのログイン ID やパスワードを盗み出そうという試み等である。インターネット・バンキングを提供するウェブページのプログラム（ウェブアプリケーション）に攻撃を受けやすい問題点があるという指摘が聞かれることも少なくない。こうした問題についても、金融業界としての正確な認識と対応が必要となっている。しかし、こうしたインターネット・バンキングのセキュリティを巡る問題は、何故か、「銀行の提供する情報システムの脆弱性」と位置付けられないで論じられることが多いように思われる。

インターネットを通じた取引が急速に拡大した現在においても、銀行にとって、インターネットがどの程度大切なインフラなのかについて、コンセンサスが得られているとはいえない。銀行の情報システムの基幹ともいうべき勘定系システムは、インターネット技術ではなくレガシー技術で動いており、銀行のシステム化戦略の中心は、やはりレガシー技術が担っていると理解されている。レガシー技術に基づいて提供された情報システムは、そのネットワーク全体が

銀行に管理されているので、万一障害が発生して機能しなくなれば、これを解消する義務は銀行側にある。しかし、インターネットで接続している場合、ネットワークが接続している先は顧客が管理する領域であり、どのようなシステム構成になっているか分からないから、障害が発生しても、その原因の特定や責任の切分けが難しい。従来の銀行の情報システムを担当してきた立場からみると、インターネットは管理できないネットワークなのである。

同様の議論は、社会の重要インフラ[5]における情報セキュリティ対策を検討するプロセスで良くみられる。重要インフラとされる業種のうち、例えば電力、運輸、ガスなどは、その基幹システム（制御系）はインターネット技術に依存していないといわれており、仮に、インターネットを経由して攻撃を受けても、基幹システムに問題は生じにくいとされることが多い。

同様に、金融業界も、その根幹となる勘定系のシステムはレガシー技術を利用して構築されており、伝統的な脆弱性対策がとられている。しかし、金融業界における顧客とのインターフェース部分には、インターネット技術が広く利用されており、この部分については、新たな脆弱性対策が必要とされている。顧客とのインターフェースといっても、顧客の指示に基づき資金の授受を行うというのが銀行の業務の基本である以上、仮に、そこに障害があれば、業務全体が滞ることになるし、万一、インターフェース部分で不正な取引が実施されてしまうと、その取引を引き継ぐシステムが正常でも全体としては正しくない処理をしてしまうことになる。こう考えると、金融業界は、電力、運輸、ガスといった他の重要インフラと比べて、インターネットの脆弱性の影響をより深刻に受けるという意味で、「インターネットにコミットしてしまった業界」ということができるだろう。

そのような観点からは、金融業界は、インターネット経由でサービスを提供する際のセキュリティ対策について、少なくとも他の重要インフラと比較して

[5] 高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）の下に設けられたセキュリティ基本問題委員会第２分科会では、重要インフラの情報セキュリティ対策強化について検討が行われている。同分科会には、金融・通信・電力・運輸・ガス等の重要インフラ事業者等の関係者が参加している。

より真剣に取り組んでいく必要がある。具体的には、銀行の情報システムの脆弱性を検知し、その情報を金融業界内で共有していく仕組みが、今、必要とされているといえよう。

４．銀行の情報システムにおける「脆弱性」とは何か

(1) 脆弱性という言葉の意味

「銀行の情報システムの脆弱性を検知する」という場合の「脆弱性」という言葉は多義的であるため、その意味するところを明確にしておく必要がある。

「脆弱性」は、英語の vulnerability の訳であり、「傷つきやすさ」、「攻撃に対するもろさ」を意味する言葉であるが、日本語においては、情報システムのセキュリティとの関連で使用されることが多い。

(2) 狭義の脆弱性

情報システムの「脆弱性」という言葉が広く認知されるようになったのは、インターネットの普及によって、多くの人々がインターネットに接続された情報機器にアクセスできるようになったこと、および、そこに接続されたパソコン、サーバ等の分散系の情報機器のシステムに多くのセキュリティ・ホールが存在し、それを突いたウィルスや不正アクセス行為が横行していたことに端を発する。ウィルスや不正アクセス行為の被害が増加する中で、必ずしもシステムに詳しくない一般ユーザをも巻き込んで、情報機器のセキュリティを向上させるために、情報システムに対する攻撃手法の仕組みや危険性を包み隠さず公開しようという、「フルディスクロージャー（Full Disclosure）[6]」という考え方が広まった。現在では、ソースコードレベルで情報が公開されているソフトウエア製品も増えており、それ以外のソフトウエア製品についても、脆弱性が指摘されると、詳細な情報が公開され、問題点を修正するプログラムや攻撃回避方法に関する情報が、一般に提供されるのが普通となってきた。このようにして指摘、共有されているのが、ソフトウエア製品の脆弱性情報である。

セキュリティ関連のウェブサイトには、毎日のように、「某 OS に新しい脆弱

[6] Bruce Schneier [2001]

性」、「某サーバ・プログラムに重大な脆弱性、アップデートを強く勧告」といった情報が掲載されている。多くの場合、この脆弱性とは、「特定のソフトウエア製品の欠陥」を意味している。

企業のネットワーク管理者の立場からみると、脆弱性とは、自ら管理するネットワークで利用されているソフトウエアが安全か否か、もし問題があるとすれば、それはどの程度の深刻さで、どのような対応策があるのかを確認するための情報、と受け止められている。

また、個人ユーザの立場からみると、脆弱性とは、放置しておくと自分のパソコンがウィルスに感染しやすくなるような問題、と受け止められていると思われる。かつては、個人ユーザが OS の脆弱性を気にすることなど考えられなかったが、2003 年 8 月にブラスター・ワーム[7]と呼ばれるウィルスの大規模な感染が発生して以来、個人ユーザであっても、「Windows の脆弱性情報が出たら、Windows Update を実施する」ことが常識となりつつある。

こうした「ソフトウエア製品のセキュリティの脆弱性」を、比較的厳密に定義したものとしては、マイクロソフト社のウェブサイトに掲載されている、次の説明が挙げられる（Microsoft TechNet アーカイブ [2005]）。

【狭義の脆弱性】

セキュリティの脆弱性とは、製品の適切な使用による場合でも、攻撃者によるユーザーシステムに対する特権の不正行使、操作の制限、システム上のデータの損傷、および許可されていない信頼の偽装を防止不能にする、製品に含まれる問題である。

この定義では、製品の不適切な使用によって攻撃が可能となることは脆弱性ではないとされている。また、この定義の追加説明において、ソフトウエア製品仕様上の弱点（例えば、仕様として鍵長 40 ビットの共通鍵暗号が利用されている結果、そのシステムへの攻撃が容易になること）が脆弱性に含まれないこ

[7]ブラスター・ワーム（Blaster worm）： 2003 年 8 月 12 日に発生した、Microsoft Windows NT/2000/XP の脆弱性（MS03-026）を利用したワーム（自己増殖を繰り返す性質を持つ、コンピュータ・ウィルスの一種）。

とが明示的に説明されている。このような定義となっているのは、脆弱性の定義に合致するか否かによって、セキュリティ・パッチをリリースする必要が生じるという、ソフトウエア製品の供給者側の特殊事情があることを理解する必要があるだろう。

(3) 広義の脆弱性

一方、こうしたシステム技術の供給者側からの定義とは別に、システム技術の需要者側の立場からは、脆弱性をより広い概念で捉えることが一般的である。そのような例として、企業のリスク・マネジメントの文脈で利用されている、次のような定義が挙げられる（日本セキュリティ・マネジメント学会 [1990]）。

【広義の脆弱性】

企業資産に損害の原因となる脅威を生ぜしめたり、損害を拡大せしめるシステム環境上の特性。

(4) 届出制度の対象となる脆弱性

一方、脆弱性関連情報届出制度（後述）のための経済産業省の告示においては、ソフトウエア等（ソフトウエア製品およびウェブアプリケーション）を対象とする脆弱性を、次のように定義している（経済産業省 [2004]）。この定義は、狭義と広義の中間的な範囲が対象となっている。

【届出制度の対象となる脆弱性】

ソフトウエア等において、コンピュータ・ウィルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

(5) 脆弱性概念の比較

そこで、これらの異なる脆弱性概念を比較し、本当に検討が必要とされている脆弱性の範囲がどこにあるかを検討してみよう。

ある情報システムに脆弱性があるということは、その情報システムの構築過程別に区分すれば、

①そのシステムが採用している要素技術（仕様)、

②それを実装したソフトウエア製品（メーカー実装)、

③それを利用して構築した業務アプリケーション（ユーザ実装)、

④それを実際に運用して行う業務サービス（運用[8]）

のいずれかひとつ以上に問題があることになる。広義の脆弱性を前提とすれば、この①～④の全過程で、攻撃の原因となり得るような「脆弱性」が存在しうることになる。そこで、前記の 3 つの定義にかかる脆弱性を①～④の過程別に分けて書き入れると、次の表 2 のようになる。

表 2：脆弱性の 3 つの定義とその対象に含まれる技術の範囲

	①要素技術（仕様）	②ソフトウエア製品（メーカー実装）	③業務アプリケーション（ユーザ実装）	④業務サービス（運用）
狭義の脆弱性	×	○	×	×
広義の脆弱性	○	○	○	○
届出制度の対象となる脆弱性	×	○	△（ウェブアプリのみ）	×

（備考）表中の「○」は対象に含まれる、「×」は対象に含まれないことを意味している。「△」は部分的に含まれる場合もあることを意味している。

狭義の脆弱性と届出制度の対象となる脆弱性は、脆弱性に対して対策を講じるソフトウエア等の供給者側の立場から問題点を特定するために、②と③の実装面に着目して脆弱性を規定している。マイクロソフト社が明示的に説明しているとおり、例えば、鍵長 40 ビットの共通鍵暗号を利用する仕様になっているソフトウエア製品の場合、その技術が正しく実装されている限り、仮にそのソフトウエア製品を利用した結果として情報システムが脆弱になったとしても、それはマイクロソフト社の製造したソフトウエア製品のメーカー実装における脆弱性ではないとされる。ソフトウエア製品の技術仕様が公開されている限り、

[8] 情報システムを脆弱なものとするのは、システム的な要因だけでなく、機密情報の管理体制や運用ミス等の人為的な要因もあり得る。こうした脆弱性を、システム的なものと区別して、「人為的脆弱性」と呼ぶこともある。

構築する情報システムにどのような仕様のソフトウエアを採用するかは、ソフトウエアの利用者側の問題となる[9]。

この違いは、どちらが正しいというものではない。マイクロソフト社は、ソフトウエア製品の提供者として、その製品実装に欠陥がない限り、「脆弱性」という言葉は使わないと決めているというだけのことである。しかし、利用者からみると、利用している個々のソフトウエア製品に（狭義の）「脆弱性」がないとしても、適切な要素技術を選択できなかったり、利用者の段階での実装・運用に問題があれば、自らが提供する情報システムが脆弱なものとなってしまう可能性があることには注意が必要である。

５．金融業界における脆弱性対策のあり方

４節での検討を踏まえると、金融業界が脆弱性と位置付け、検知と情報共有を行っていくべき脆弱性の範囲は、できるだけ広くとっておくことが適当であると思われる。ソフトウエア製品に関する狭義の脆弱性については、汎業界的な枠組みで情報を入手できることを前提とすれば、むしろ、金融業界としては、狭義の脆弱性に含まれない領域に注力すべきではないだろうか。

例えば、４節(5)の整理で、「①要素技術（仕様）」と整理した技術の中には、暗号アルゴリズムやハッシュ関数、生体認証の基礎技術等が含まれる。それらの脆弱性については、主として、学者・研究者が検知作業を担当し、その情報は学術雑誌などで共有されることが多い。金融業界は、これまで、そうした情報をさほど積極的に収集してきたわけではなかったが、高度な技術を利用した情報システムを用いて金融サービスを提供していく立場からは、こうした脆弱性の問題を看過していくべきではない。金融業界において実際に利用されている要素技術に脆弱性が発見された場合、その事実と影響範囲を業界内に迅速に伝える枠組みが必要であろうと思われる。

[9] ただし、経済産業省の告示の定義において、ウェブアプリケーションの脆弱性については、①仕様および④運用が原因となった脆弱性が含まれる余地があり得る。

一方、「③業務アプリケーション（ユーザ実装）」と整理した技術の中には、個別性の高い情報システムが多く含まれ、外部からの脆弱性の指摘や情報共有にそぐわないものも多い。これは、「④業務サービス（運用）」と整理した部分も同様である。

しかし、偽造キャッシュカード事件の経験等を踏まえれば、こうした技術領域についても、どのような脆弱性が存在しうるかを検討し、各銀行が自らの業務システムや運用状況をチェックできることが望ましい。例えば、金融情報システムセンター（FISC）が発刊している「金融機関等コンピュータシステムの安全対策基準」には、金融機関が利用する情報システムの設備・運用・技術面の安全対策について記述されているが、この資料の改定作業を通じて、過去に発生した攻撃事例の整理や、それらを踏まえた脆弱性情報の共有を推進していくことが考えられよう。

６．経済産業省の脆弱性関連情報届出制度について

こうした観点からみて注目すべき動きが、2004 年 7 月に始まっている。経済産業省が「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）を公示し、脆弱性関連情報届出制度が開始されたのだ。

この制度は、各種ソフトウエア製品（OS、ブラウザ、ウェブサーバ等）に加え、インターネット上で提供されるインターネット・バンキング、オンライン証券取引を始めとする様々なウェブアプリケーションについて、不正アクセスや個人情報漏洩などの原因となる「脆弱性」を発見した人が、受付機関である情報処理推進機構（IPA）に通知し、その内容を確認して、ウェブサイトの管理者やソフトウエア製品の開発者に通知し、脆弱性の是正を促すという仕組みである。ソフトウエア製品の製品開発者への連絡および公表にかかる調整機関として、JPCERT コーディネーションセンター（JPCERT/CC）が指定されている（図 1 参照）。また、IPA、JPCERT に加え、電子情報技術産業協会、情報サービス産業協会、日本パーソナルコンピュータソフトウェア協会、日本ネットワーク

セキュリティ協会の 4 団体が連名でガイドラインを発表し、IT ベンダー各社に積極的に脆弱性を検知、報告するよう働きかけている。

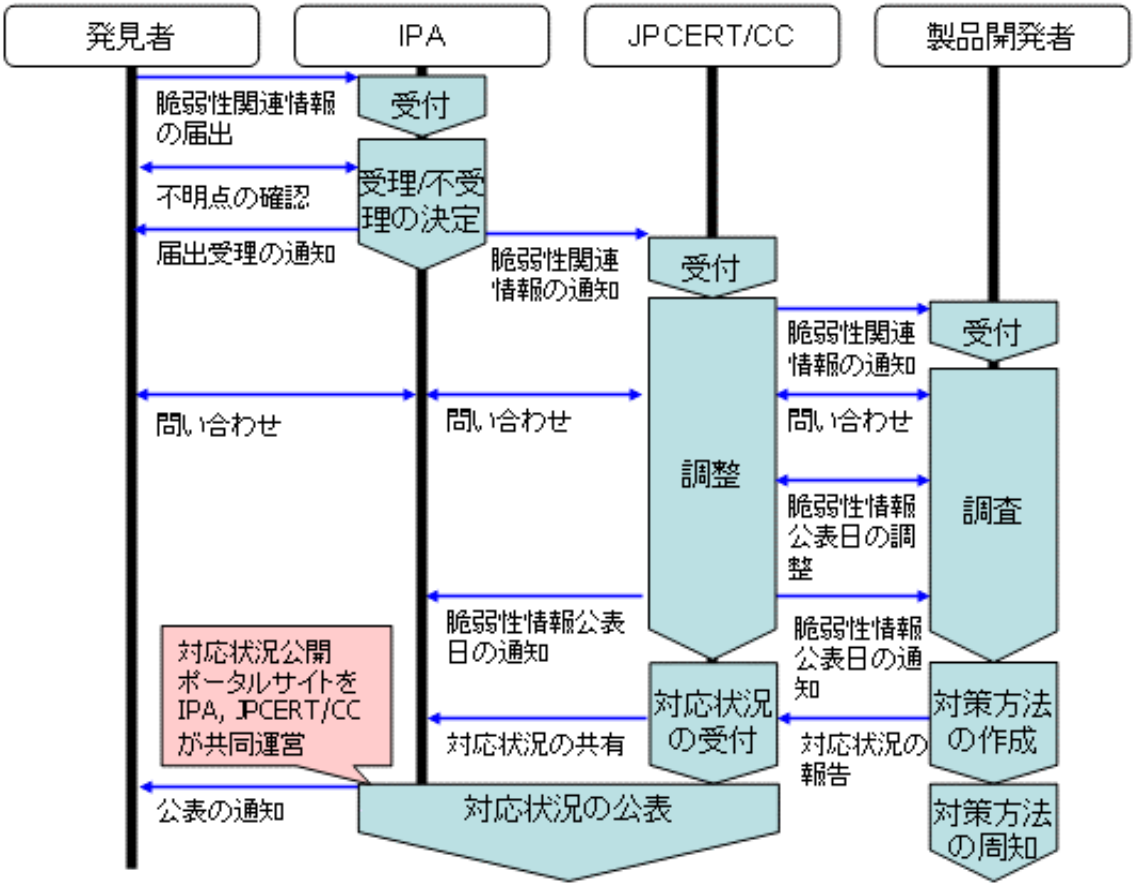
こうした IT ベンダーによる脆弱性の検知は、海外におけるインターネット利用者の自発的な動きから始まったものである。特に、OS やサーバ用ソフトウエアについては、脆弱性を検知し、その情報を共有して攻撃を回避しようという枠組みが整備され、関係者の地道な努力により、実際に幅広く活用されている。元々、ウィルスの制作や不正アクセスを試みる攻撃側は、攻撃対象のソフトウエア製品の脆弱性にかかる情報を相互に交換して攻撃に役立ててきたといわれていた。そこで、防御側もこうした「脆弱性の検知と情報共有」の枠組みを作ることで、ウィルスや不正アクセスを防御する側も様々な情報を入手でき、ウィルス感染や不正アクセスを効率的に排除することができるようになったのである。今回の届出制度は、こうした自発的な取組みを補完するものである。

今回の届出制度は、IT ベンダーが中心となった汎業界的な動きであるが、金融機関が提供しているウェブサイトも脆弱性検知の対象となっていることから、金融業界にも影響を与えるものと思われる。これまで、インターネット・バンキングのウェブサイトについては、個人の管理するメーリングリストやブログなど、非公式なルートで問題点が指摘されることが多かったが、そのような指摘については、金融機関が必ずしも真摯に指摘を受け入れるとは限らなかった。新しい制度の下では、IPA が仲介者として機能し、指摘内容の確認も行うので、ウェブサイト管理者としても、指摘を受け入れやすくなるものと考えられる。

ただし、ウェブサイトの脆弱性については、その内容が公開されるとは限らないため、同様の脆弱性を抱える複数のサイトが存在しても、一遍には是正されないという問題がある。ウェブサイトのセキュリティについては、何らかの形で脆弱性にかかる技術情報が共有される仕組みとすることが望まれよう。

図 1　脆弱性関連情報届出制度の概要

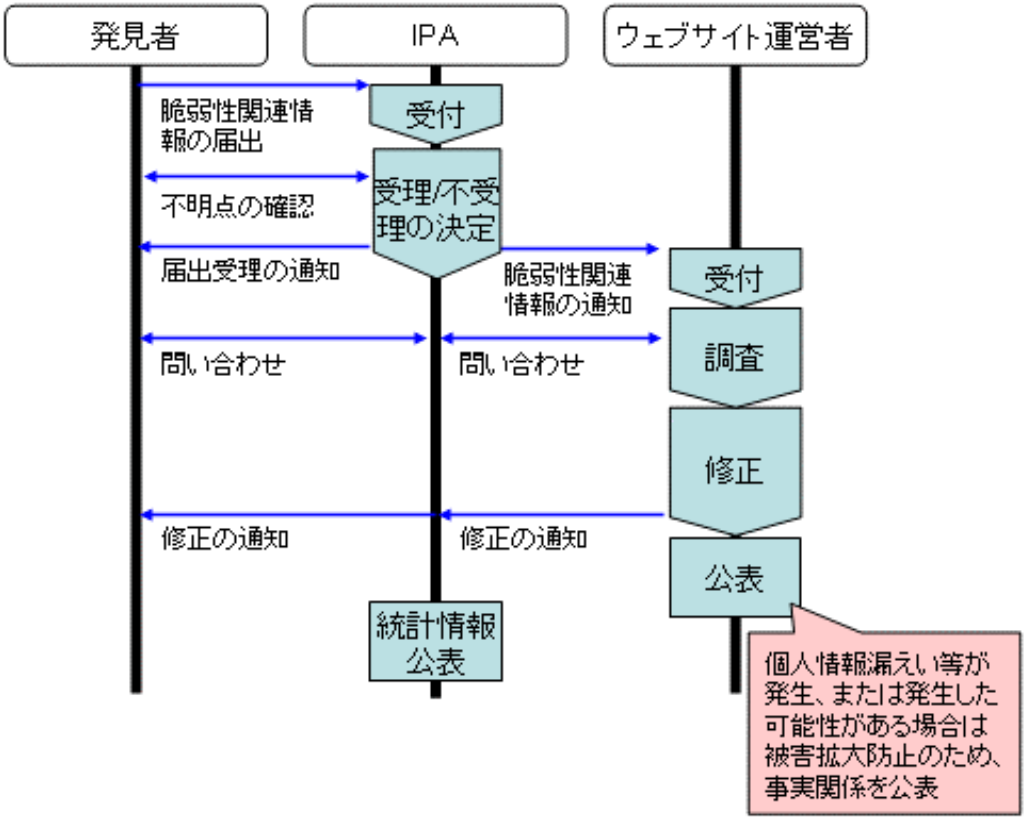
(1) ソフトウエア製品の脆弱性関連情報の取扱いプロセス



対象：OS やブラウザなどのクライアント PC 上のソフトウエア、データベース管理システム、ウェブサーバなどサーバ上のソフトウエア、ソフトウエアを組み込んだ汎用的なハードウエア製品。
IPA に届出られた脆弱性関連情報は、既に報告されていないか確認が行われ、取扱いが妥当と判断された場合に、情報を JPCERT に通知する。JPCERT は、別途用意された製品開発者

登録リストから、受け付けられた情報に関係するベンダーに連絡を行う。

(2) ウェブアプリケーションの脆弱性関連情報の場合



対象：インターネット上のウェブサイトで稼働している、電子申請やインターネット・バンキング等のウェブアプリケーション。
受付機関は IPA だが、JPCERT を経由せずに、IPA が直接ウェブサイト運営者と調整を行う。ソフトウエア製品の脆弱性とは異なり、脆弱性があったかどうかについて公表する義務はない。

資料：情報処理推進機構セキュリティセンター[2005]

７．脆弱性関連情報届出制度と金融業界の対応

脆弱性関連情報届出制度のように、インターネット上の様々な脆弱性を検知

し情報を共有する汎業界的な仕組みが整備される中で、金融業界としては、どのような対応をしていけばよいのだろうか。

そもそも、金融業界の情報システムは、偽造キャッシュカードによる不正預金引出しから、フィッシング詐欺、インターネット・バンキングの不正取引に至るまで、様々な脅威にさらされている。銀行は、こうした脅威の原因となっているシステムの脆弱性を的確に検知し、適切に対処していくことが求められている。こうした情報システムに対する脅威のうち、コンピュータ・ウィルス、サーバ・プログラムやハードウエアの欠陥を突いた攻撃など、「どのユーザにも発生しうる一般的な攻撃」については、金融業界も、脆弱性検知と情報共有に関する汎業界的な対策を積極的に利用していくべきだろう。銀行は、適切なウィルス検知ソフトの導入、サーバ・プログラムへのパッチ適用、ハードウエアの組み込みソフトウエアの更新など、一般企業向けに提供されている情報セキュリティ対策を着実に実施することにより、システムの脆弱性を是正していくことができる。ウェブアプリケーションの脆弱性が指摘されれば、これを適切に是正していけばよい。銀行が管理している情報システムの重要性を前提とすれば、銀行は、こうした汎業界的な脆弱性検知と情報共有についても、迅速かつ徹底した対応をとることが要請されている。なお、汎業界的な脆弱性については、実際には、その対策を IT ベンダーやセキュリティ対策を専門とするサービス事業者に委ねることも可能な部分も多いと考えられる。

これに対し、偽造キャッシュカードによる不正預金引出し、フィッシング詐欺、インターネット・バンキングでの不正送金のように、「銀行のシステムに固有の攻撃」に対しては、そもそもどのように脆弱性を検知するか、その情報をどのように共有するかについて、まだ何も決まっていない。この結果、脆弱性の検知と是正が遅れ、被害の拡大を招く惧れがあるほか、業界としての適切なセキュリティ対策に関するコンセンサスが醸成されないという問題もある。

こうした「銀行のシステムに固有の攻撃」については、誰よりもまず、銀行自らがその対策を検討する責任を負っている。銀行の社会的責任やレピュテーション・リスクをも考慮して、どこまでコストを掛けてセキュリティ対策を講

じていくか、各銀行が判断しなければならない。そのためにも、トラブルの原因となった脆弱性を適切に検知するとともに、業界内で適切に情報を共有し、脅威に対抗する有効な対策を講じていく必要があるだろう。

ここで海外に目を転じてみよう。例えば、フランスでは、1980 年代に、磁気ストライプカードの偽造に苦しんだため、国を挙げて IC カード化に取り組んだ結果、国内の銀行取引カードを全て IC カード化することに成功している。ドイツでは、磁気カードに独自の偽造防止技術を組み入れることによって、スキミングの被害を抑制している。

米国では、金融業界を挙げて、情報セキュリティ技術の検討と実装を進めている。例えば、暗証番号を暗号化するために利用していた DES 暗号が脆弱化した際に、米国政府に新たな標準暗号技術の作成を働きかけ、自らトリプル DES 暗号の標準化を行った。こうして米国金融業界で標準化された技術が、他国で利用されているのである。

脆弱性の検知と情報共有についても、米国での取組みが参考になる。業界内で脆弱性情報を検知、共有する仕組みとして、運輸、通信、金融などの重要インフラを担う業界において、ISAC（Information Sharing and Analysis Center）と呼ばれる組織が設立されている。なお、日本でも、情報通信業界が、2002 年 7 月に Telecom-ISAC Japan を組成し、活動を開始している。

８．おわりに

銀行は、情報技術のユーザであってメーカーではない。銀行が実際のシステム構築作業を IT ベンダーに担当させている以上、システムの中身についてどこまで知っておくべきなのかという点は、従来から様々な議論があった。しかし、最近発生した幾つかの事件は、銀行が技術の中身やその脆弱性を知悉しているか否かにかかわらず、銀行が提供するサービスに不具合があった場合、銀行が指弾を受けるという当然の事実を改めて認識させるものであった。

金融業界が巨大な情報システムを管理する装置産業になってしまっている以上、そこで利用されている技術を分析・研究し、脆弱性を検知し、脅威を未然

に取り除くことは、金融業界自身の責務といえる。金融業界は、個々の金融機関がネットワークで結ばれることによって、単独では果たし得ない、重要な機能を担っているが、これは同時に、個々の金融機関のシステムに問題が発生すると、業界全体にその影響が及ぶというリスクを抱えていることを意味する。こうした環境においては、金融業界全体として、情報システムの脆弱性に対処していくことが必要となってくる。

キャッシュカードやインターネット・バンキングに対する金融ハイテク犯罪が増加している実態を踏まえると、銀行は、自らの情報システムの脆弱性を正確かつタイムリーに検知し、その情報を業界内で適切に共有し、その是正に戦略的に対応していくための体制を早急に構築していくことが必要となっている。金融業界全体の問題としても、こうした体制整備に向けた話し合いを始めるべき時期に来ているのではないだろうか。

【参考文献】

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準』、2003 年 10 月

経済産業省、『ソフトウエア等脆弱性関連情報取扱基準』、平成 16 年経済産業省告示第 235 号

情報処理推進機構セキュリティセンター、『脆弱性関連情報に関する届出について』、2005 年 2 月
http://www.ipa.go.jp/security/vuln/report/index.html

全国銀行協会、『いわゆる偽造キャッシュカードによる預金等引出しに関するアンケート結果』、2005 年
http://www.zenginkyo.or.jp/news/17/pdf/news170222_2.pdf

日本セキュリティ・マネジメント学会、『セキュリティ・マネジメント・ハンドブック』、1990 年 4 月

松本勉・岩下直行、「金融業務と認証技術：インターネット金融取引の安全性に関する一考察」、『金融研究』第 19 巻別冊第 1 号、pp.1-14、日本銀行金融研究所、2000 年 4 月

Microsoft TechNet アーカイブ、『「セキュリティの脆弱性」の定義』、
https://s.microsoft.com/japan/technet/archive/community/columns/security/essays/vulnrbl.mspx（アクセス日：2005 年 3 月 25 日）

Schneier, Bruce, "Full Disclosure", Crypto-Gram Newsletter, November 15, 2001,
http://www.schneier.com/crypto-gram-0111.html#1