日本銀行金融機構局　金融高度化センター
ITを活用した金融の高度化に関するワークショップ
第2回「金融取引チャネルとセキュリティ」

2014年11月26日

ネットバンキングのセキュリティ

日本銀行 金融研究所 情報技術研究センター
(Center for Information Technology Studies)
中山　靖司

※本資料の内容や意見は、報告者個人に属し、日本銀行や金融研究所の正式見解を示すものではありません。

目次

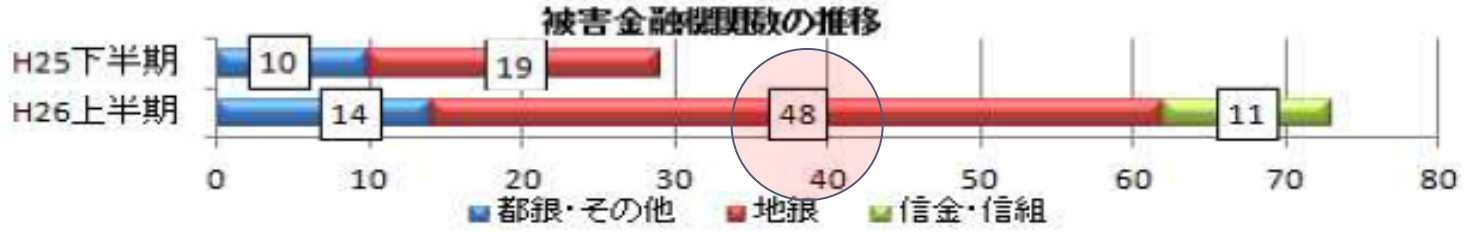
1. ネットバンキングを使った不正払出の増加

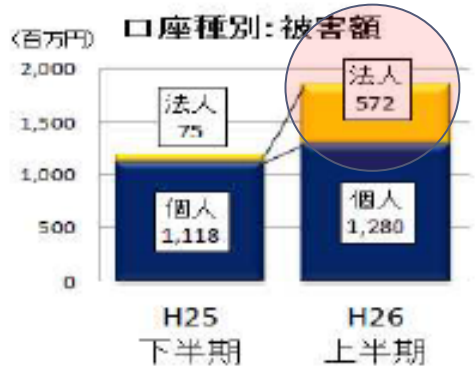
ネットバンキングを使った不正払出の増加

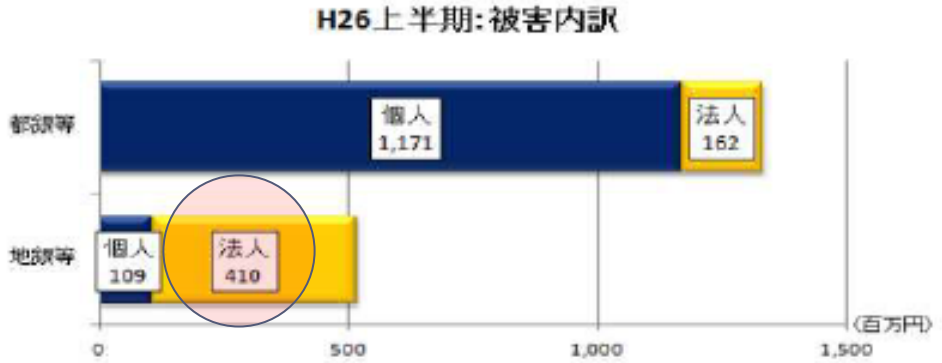
平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況について

平成26年9月4日
警察庁

期間	件数	被害額
H26上	1,254	約18億5,200万円（約148万円/件）
H25下	1,098	約11億9,300万円（約109万円/件）
H25上	217	約2億1,300万（98万円/件）







- その被害額は、**偽造キャッシュカードによる不正な現金の引出しが社会問題となった2005年の規模（個人口座8.2億円＜全銀協発表＞）を上回っている。**

  => 金融機関が補償に応じているため、偽造キャッシュカードの時ほど騒がれてはいない。

口座種別毎の被害状況

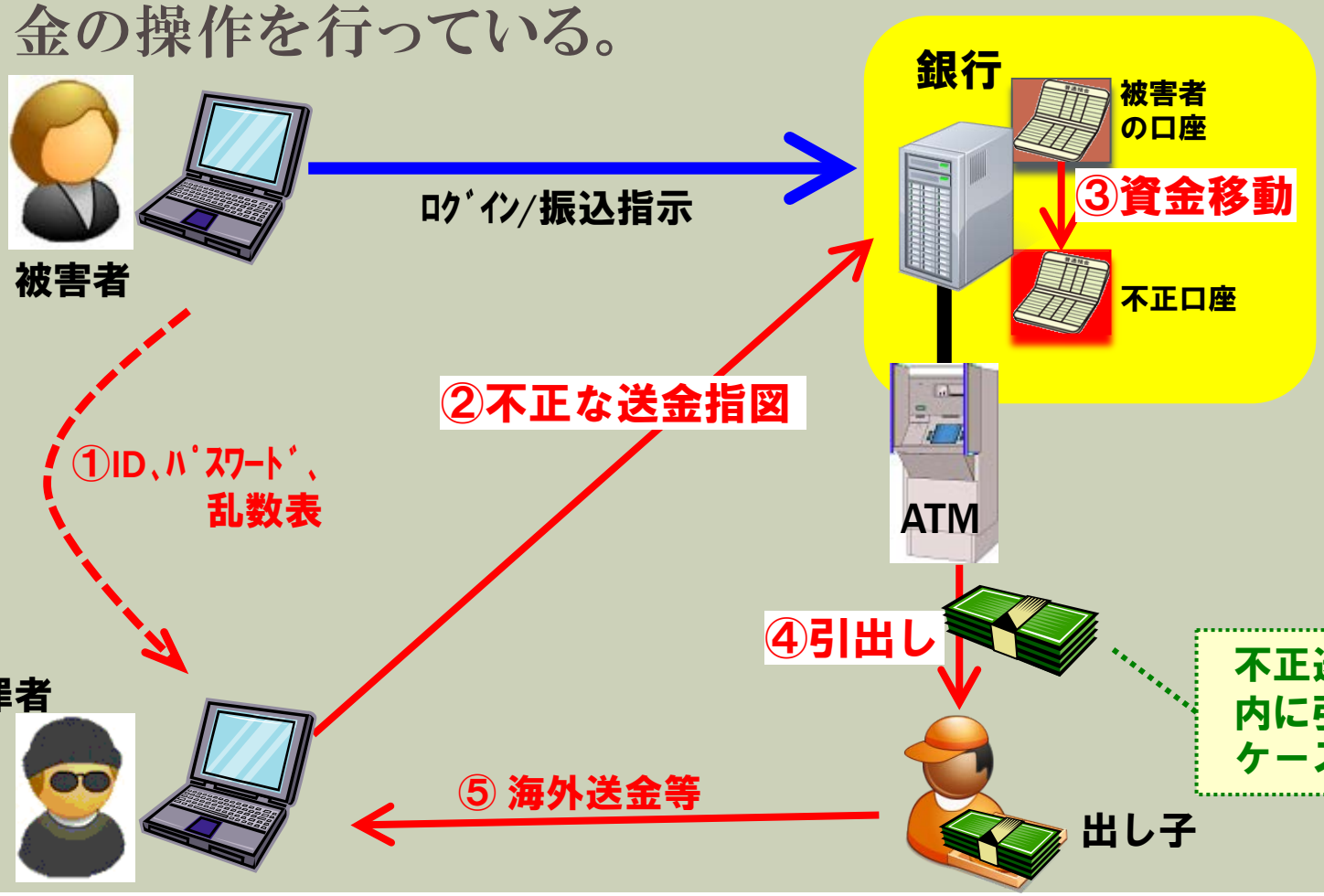
口座種別	平成25年下半期			平成26年上半期		
	都市銀行等	地方銀行等	合計	都市銀行等	地方銀行等	合計
個人	約10億4,300万円（87.4%）	約7,500万円（6.3%）	約11億1,800万円（93.7%）	約11億7,100万円（63.2%）	約1億900万円（5.9%）	約12億8,000万円（69.1%）
法人	約3,500万円（2.9%）	約4,000万円（3.4%）	約7,500万円（6.3%）	約1億6,200万円（8.8%）	約4億1,000万円（22.1%）	約5億7,200万円（30.9%）
合計	約10億7,800万円（90.3%）	約1億1,500万円（9.7%）	約11億9,300万円（100.0%）	約13億3,300万円（72.0%）	約5億1,900万円（28.0%）	約18億5,200万円（100.0%）

－－　ID/パスワード盗取からPC乗っ取りへ　－－

2. 不正払出手口の変化

（従来型）ネットバンキングの不正払出の流れ

■IDとパスワードを入手した犯罪者が本人に成り済まして送金の操作を行っている。



どうやって、IDとパスワードが取られるのか？

- **不正手口①－フィッシング**
  - フィッシングサイトの数が、2013年末から急増。
  - フィッシングサイトに誘導するフィッシングメールも、今では（比較的）流暢な日本語に対応。
  - 大手検索サイトの検索結果画面に邦銀のフィッシングサイトへのリンクが表示された例も。
- **不正手口②－ウイルス**
  - ID／パスワード等を盗聴し、外部に送信するウイルス。
  - ネットバンキングを狙ったウイルスが年々増加。
  - 脆弱な正規のWebサイトが改ざんされ、ウイルスを仕組まれるケースが増加。
- **不正手口③－ウイルスとフィッシングの融合**

基本的なフィッシングの一例

③ID、ﾊﾟｽﾜｰﾄﾞ等の不正入手

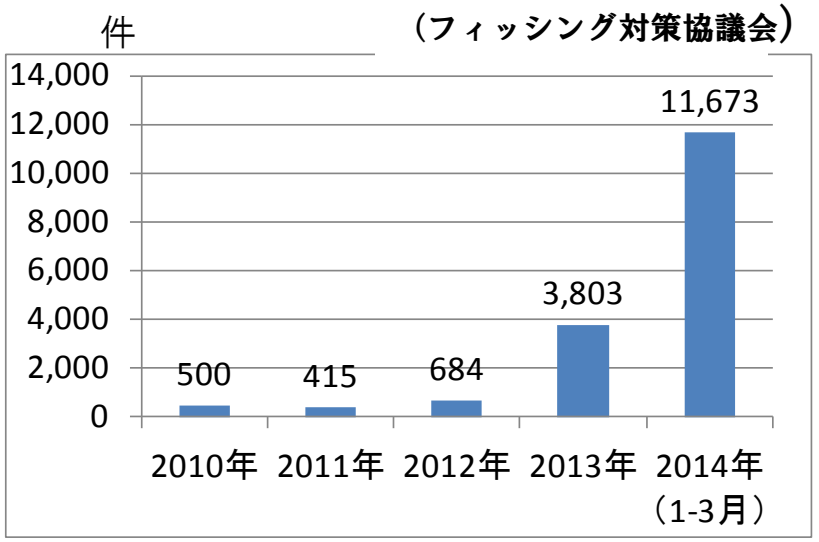
犯人

ID, パスワード

②偽ホームページにアクセス

被害者

①偽ﾎｰﾑﾍﾟｰｼﾞへの誘導ﾒｰﾙ送信

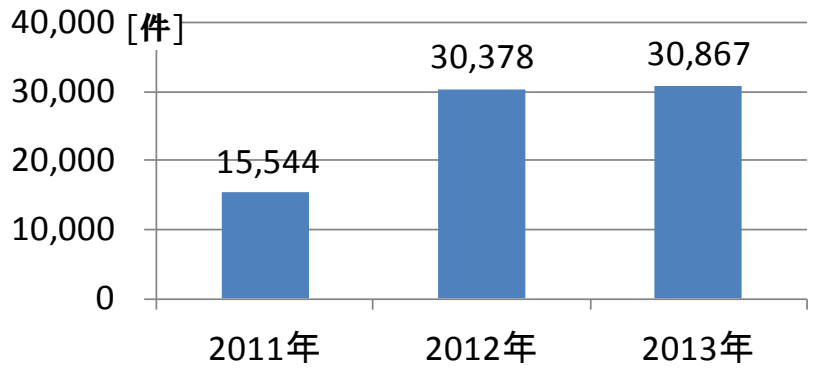


フィッシングサイトの報告件数

PCのウイルス感染

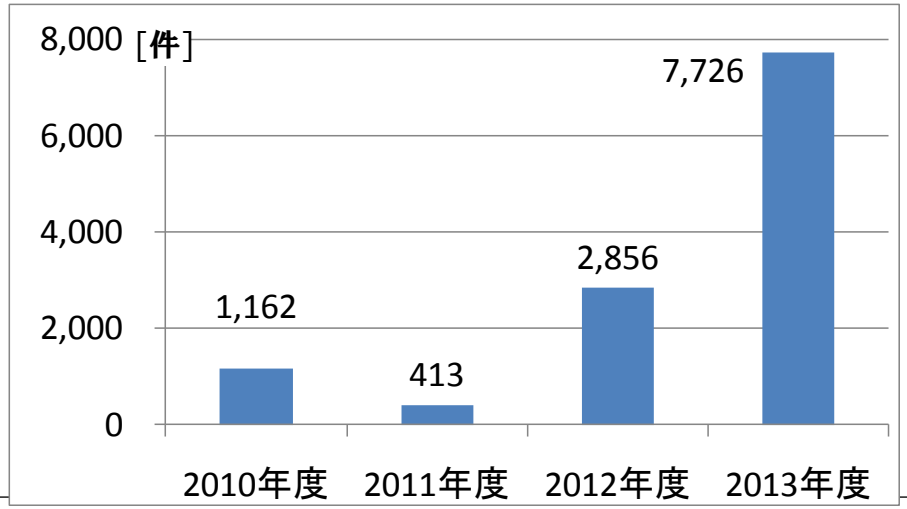
■ ネットバンキングを狙ったウイルスが年々増加。

ネットバンキングを狙ったウイルスの報告件数（IPA）



■ 脆弱な正規のWebサイトが改ざんされ、ウイルスを仕組まれるケースが増加。

Webサイトの改ざんの報告件数（JPCERT）

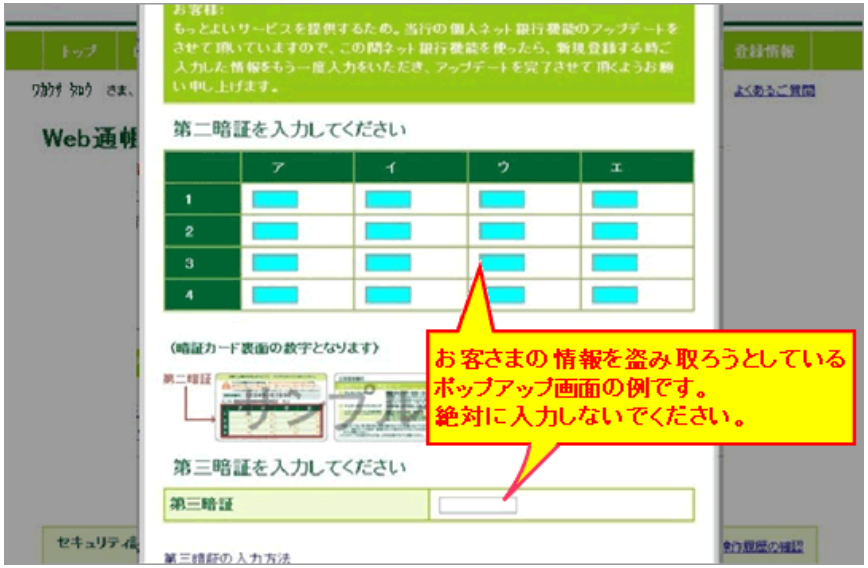


ウイルスに感染する経路は、
メール（90%）、
Web（8%）、
ダウンロードファイル（1%）

（2013年、IPA）

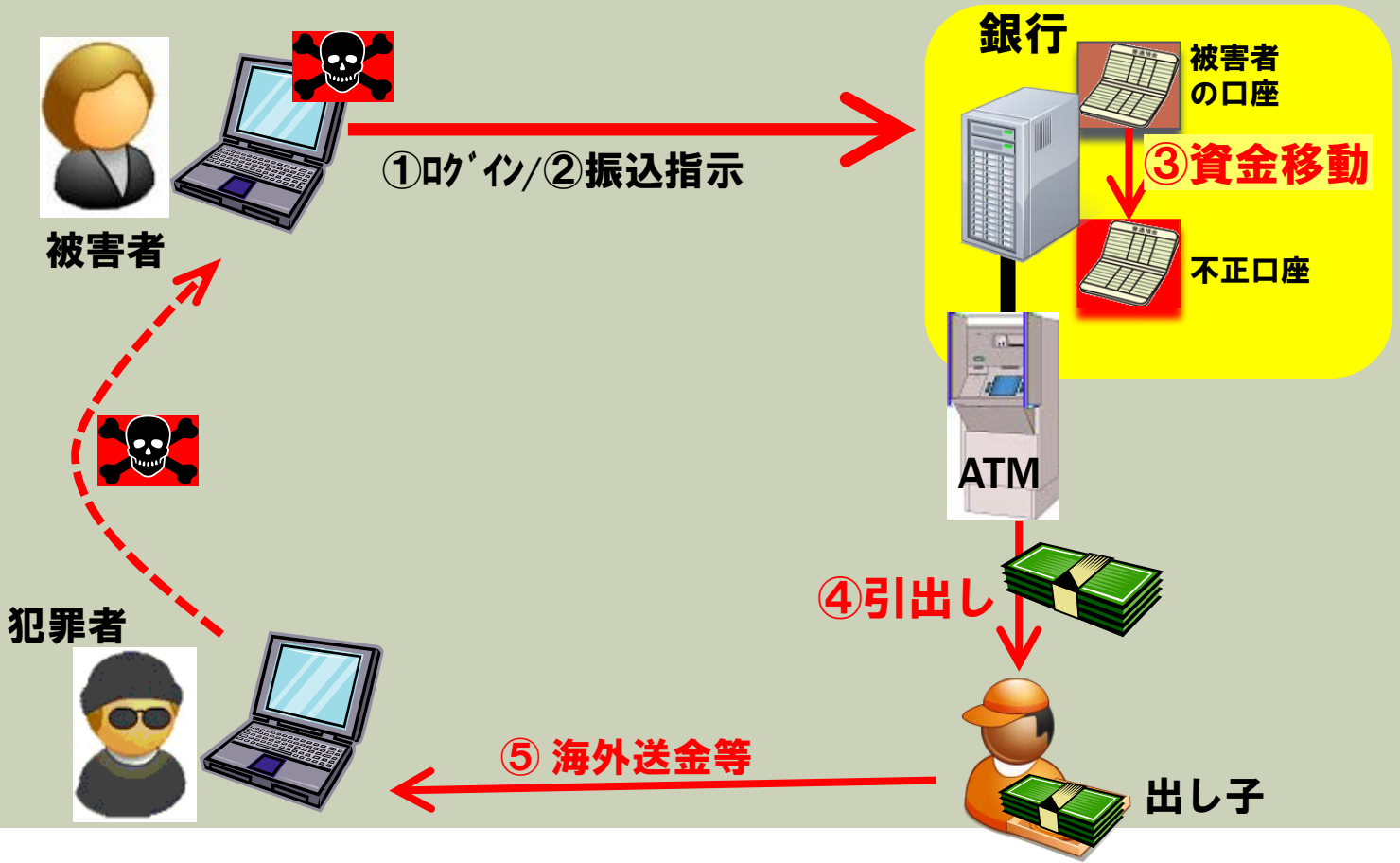
ウイルスとフィッシングの融合

- 利用者がネットバンキングにアクセスすると、ウイルスが画面表示のHTML文に不正コードを挿入し、ログイン画面等で乱数表や秘密の質問等の入力を促すポップアップ画面を表示させる等の手口。
  ーー（ID盗取型MitB<Man-in-the-Browser>攻撃）



（最新型）ネットバンキングの不正払出の流れ

- ウイルスが利用者のパソコンを乗っ取り、本人の意思に反して送金の操作等をしている（MitB攻撃）。



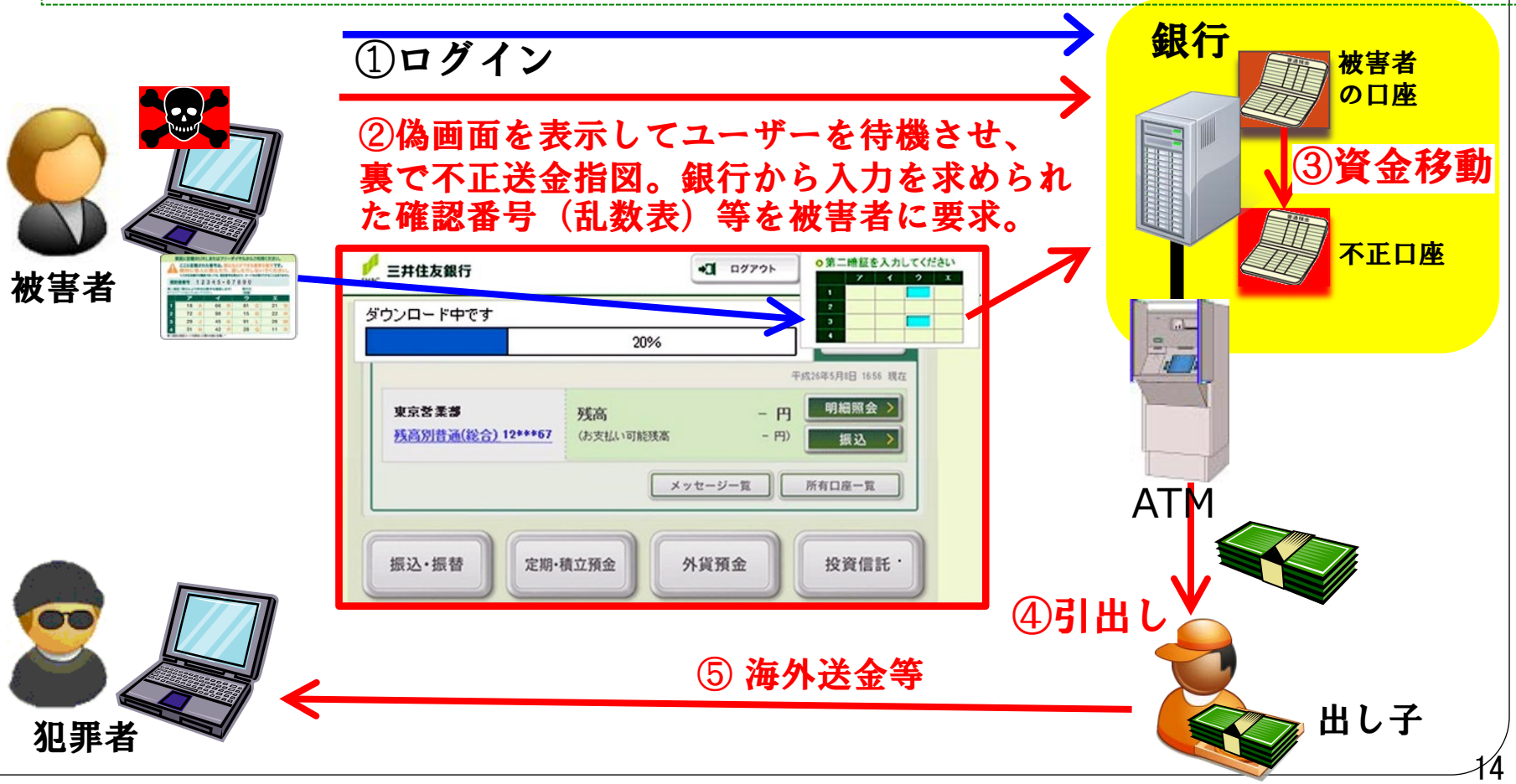
どうやって、本人の意思に反する操作を行うのか？

- **不正手口④－ウイルスが裏で気づかれないように勝手に送金を指示**
  - 本人がID/パスワードを入力してログインした後にウイルスが活動を開始するため、 犯罪者はIDやパスワードを盗む必要もない。
- **不正手口⑤－ウイルスがユーザーの取引を改ざん**
  - 不自然な画面が表示されること等が一切ないため、ユーザーが事前に気づくことは極めて困難。

ウイルスが勝手に送金指図を行う一例

- 本人による正規のログイン後に、裏で気付かれないように勝手な送金指示を行う（取引偽造型MitB攻撃）。

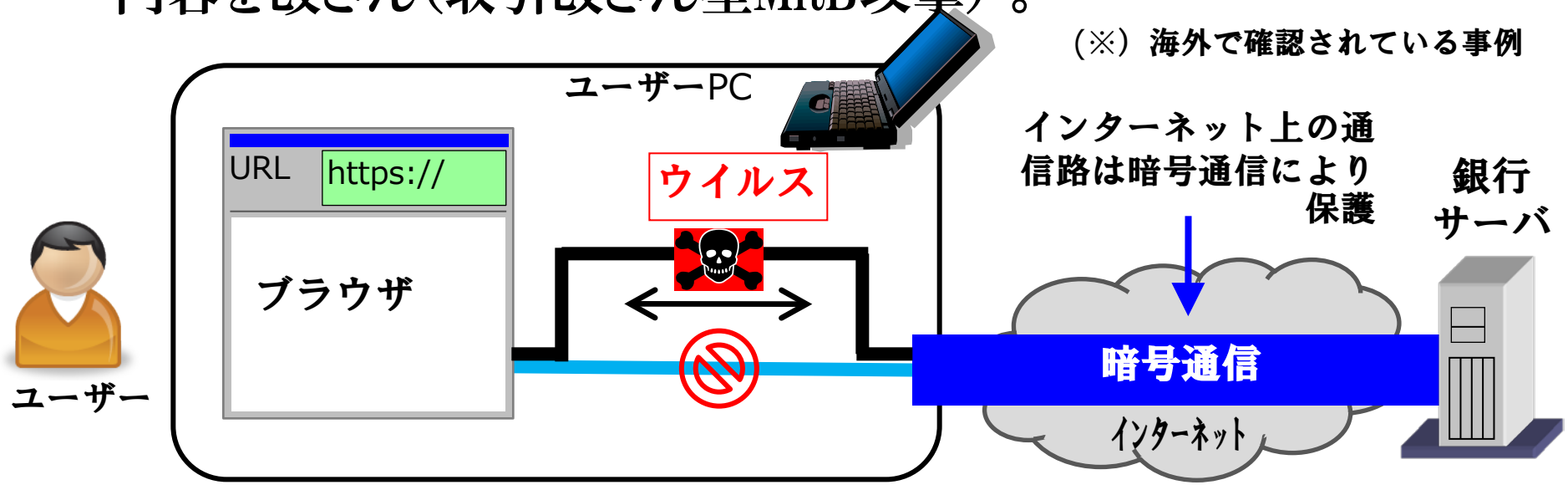
（※）乱数表だけでなく一定時間ごとに生成されるパスワード<OTP>も以下と同様の仕組みで無力化。



ウイルスがユーザーの取引を改ざんする仕組み

- ユーザー本人によるログイン後、取引のタイミングになったところで、ウイルスが活動を開始。通信に割り込み、表示画面や送信内容を改ざん（取引改ざん型MitB攻撃）。

（※）海外で確認されている事例



・「口座Aに1万円」との送金指図が、ウイルスによって「口座Xに100万円」と改ざんされ、銀行サーバに送信
・銀行からの確認画面も改ざんされ、元の指図「口座Aに1万円」と表示されるため、ユーザーは攻撃に気付かない

- こうしたMitB攻撃の可能性は、日本銀行でも2006年に指摘(※)している
（※）日銀レビュー2006-J-14 「インターネットバンキングの安全性を巡る現状と課題」

国内外のMitB攻撃の発生段階

ID盗取型 ⇒ 取引偽造型 ⇒ 取引改ざん型

高度 →

（海外）

取引改ざん型MitBも発生 ： 2008年頃から発生

- 米、独、伊、蘭等で大規模発生（*2012年1～3月頃*）
  - －－ 攻撃のほとんどが同一の犯行組織によるものと考えられ、一連の事件は総称して「Operation high roller」と呼ばれている。
  - －－ 不正送金総被害額は60億円～2000億円と試算されている（60以上の金融機関が被害）

（国内）

ID盗取型MitB ： *2012年10月下旬頃*

取引偽造型MitB ： *2014年春頃*

取引改ざん型MitB ： 未確認

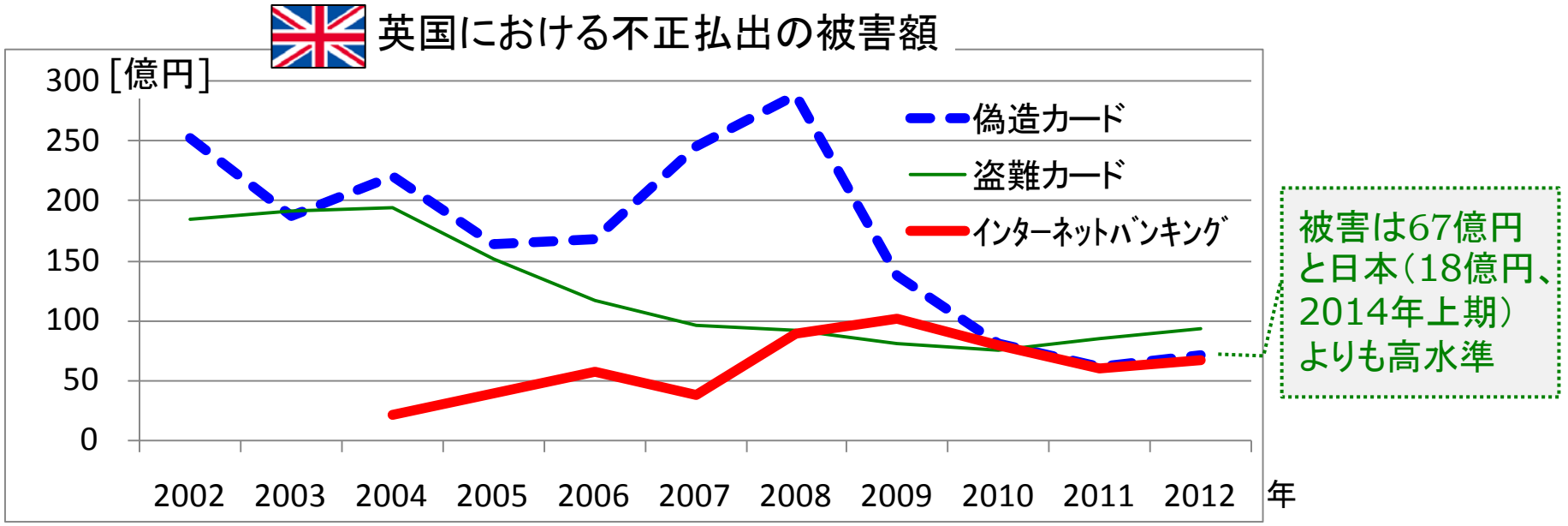
3. 被害急増の背景と海外動向

被害急増の背景として考えられることは色々あるが．．．

- **攻撃ツールの流通**
  フィッシングサイト作成キットやバンキングウイルス作成ツールがインターネット上に安価に出回るようになり、偽造キャッシュカード等他の犯罪よりコストパフォーマンスがよくなりつつある。
- **不正送金した資金を現金で引き出す方法等の確立**
  —— 「振り込め詐欺」や「偽造キャッシュカード」等の犯罪で使われている「出し子」を使った方法が、ネットバンキングの不正送金後の現金引出しでも活用され始めた。
  —— 日本のATMの現金引出し限度額が海外に比べ高いことも一因。
- **日本語の壁の低下**
  日本語の壁があると言われていたが、日本語が（比較的）堪能な協力者が犯罪集団に加わるようになってきたと考えられる。

最大の理由は、日本のセキュリティが海外に比べ相対的に甘くなっていることかも．．．

- **海外から日本へターゲットが移行しつつある可能性**
  従来、海外での被害が中心であったが、一部で、乗っ取り型ウイルス等の最新の手口にも対応した**不正送金対策が進んだため**、ターゲットを日本にも広げつつある。



（Financial Fraud Action UK）

英国大手行における対策の導入状況

- 大手5行が、時刻同期型OTPではなく、振込先等の情報に紐付いた取引認証コードを生成する専用機器を導入。また、3行が、ウイルス対策ソフトを無償提供。

銀行名	HSBC	BARCLAYS	LLOYDS BANK	Standard Chartered	RBS The Royal Bank of Scotland
取引認証機器	Secure Key  振込毎。振込先（下4桁）に紐付く認証コード（6桁）	PINsentry  振込先の登録のみに使用（認証コード8桁）	 振込毎。振込先/金額に紐付く認証コード（8桁）	 振込毎。振込先/金額に紐付く認証コード（8桁）	Card-Reader  振込先の登録のみに使用（認証コード8桁）。
ウイルス対策	Trusteer [Trusteer Rapport] インターネットバンキングに特化したウイルス対策ソフトを無償提供	KASPERSKY [Kaspersky Internet Security] 一般的な大手ウイルス対策ソフトを無償提供	一般的な大手ウイルス対策ソフトを紹介	なし	Trusteer [Trusteer Rapport] インターネットバンキングに特化したウイルス対策ソフトを無償提供等

シンガポールにおける対策の導入状況

- シンガポール銀行協会（ABS）は、2012年12月までに、リスクの高い取引（新規振込等）について「取引認証」を導入することを示し合せ（2012/1月）。
- シンガポール金融管理庁（MAS）は、「TECHNOLOGY RISK MANAGEMENT GUIDELINES（2012/6月）」で、取引認証等の適切な対策を講じることを定めている。

ICカードに、ディスプレイとボタンを搭載。

中国における対策の導入状況

- ＜中国人民銀行　電子取引ガイド(第1号)＞2005.10
  インターネットバンキング業務では、PKI電子証明書及び電子署名を利用しない限り、個人ユーザ：1000元/1回、5000元/1日の支払額を超える事ができない（法人ユーザ：50000元/1回）。
- ＜中国人民銀行ネットバンキングシステム情報セキュリティ共通基準＞2012.5
  ネットバンキングにおける情報セキュリティ問題を分析した上で、技術、管理、運用の3方面から、基本と強化の2段階の対策を3年以内に達成するよう金融機関に要求。ワンタイムパスワードトークンやUSBトークン等の物理認証デバイスについて、具体的な技術基準を規定。トランザクション署名を基本機能として要求。

- 中国の4大銀行（中国農業銀行、中国工商銀行、中国銀行、中国建設銀行）が取引認証を行う専用機器＜対話型USBトークン＞を導入。
  －－　単一口座へ振込する場合は、対話型USBトークンのトランザクション署名機能で振込先口座、振込先名前、金額をトークンの液晶画面で確認してから、振込処理を実行。
  －－　対話型USBトークンは70元程度で販売。中国では金融機関支店網が充実していないこともあり、インターネットバンキングへのニーズが高いほか、利用者も自分の預金は自分で守るという意識が高いとのこと。

ICBC(中国工商銀行<総資産額中国第1位>)の場合

- 複数の認証方式を提供し、利用する方式により送金の上限金額を変えている。

対話型USBトークン
トランザクション電子署名

USB-Shield – best choice of Personal Internet Banking security

USB-Shield is a security tool to authenticate the identity of customers through digital certificates. It has been granted a national patent, and is the highest security-level ID authentication tool in the e-banking sector. The general USB-Shield is applicable to mobile phones, computers and other devices.

OCRA仕様
トランザクションOTP署名

導入実績2000万個？

ICBC e-Password Device – product used in different channels

ICBC e-password device is a new electronic banking security product that comes with a power supply and password generation inside, an external display and a digital keypad.

スクラッチカードによる
ワンタイム認証

E-Banking Code Card – new E-Banking security tool

E-Banking Code Card is a new electronic banking security tool specially designed for online banking users with full consideration on security and cost.

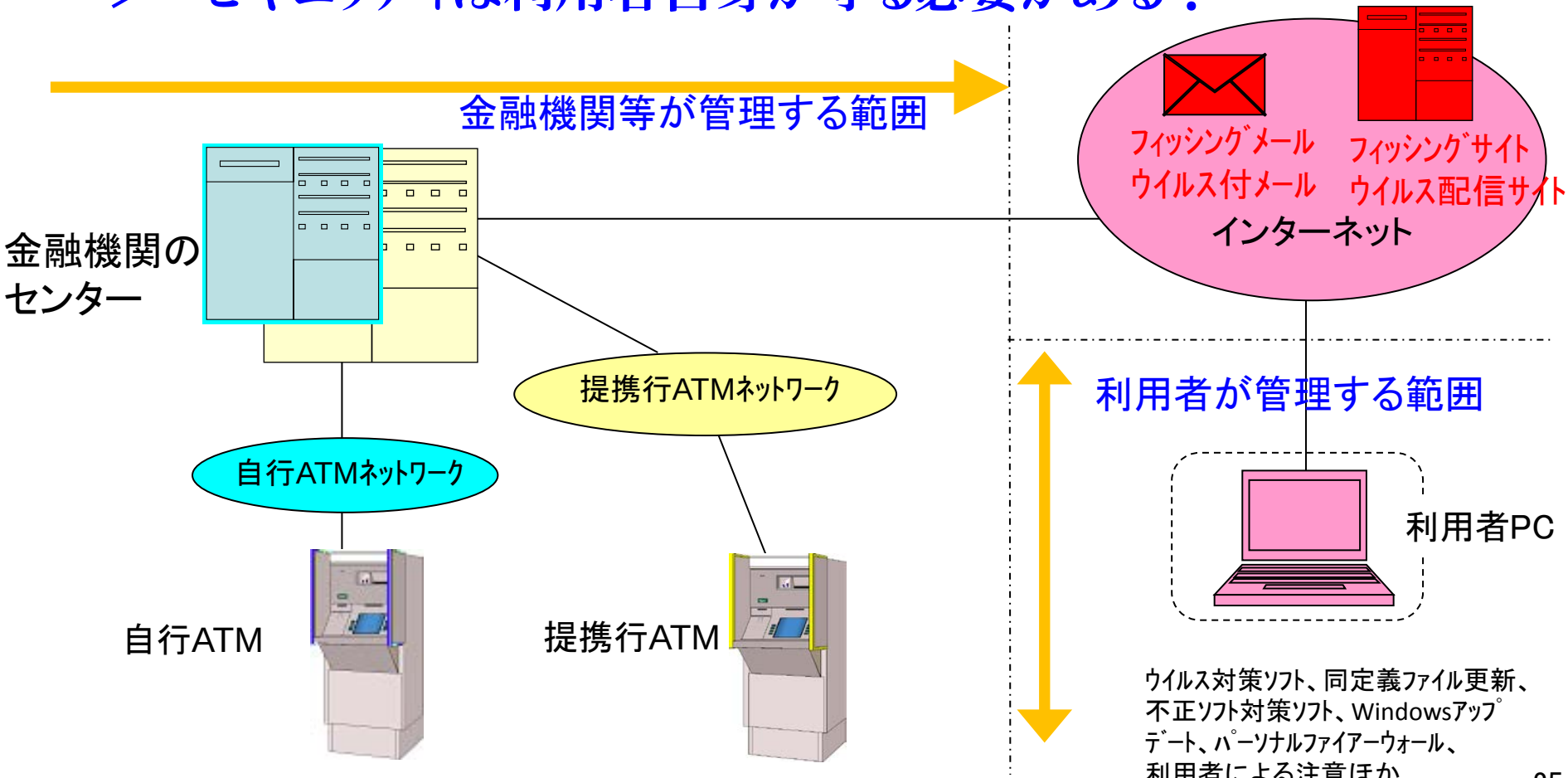
※ICBCホームページより

①金融機関が採用すべき不正送金対策
②金融機関の預金補償
③リスクを下げるための他の対策例

4. 不正払出への対処

ネットバンキング特有の対策の難しさ

◆キャッシュカードを使ったATM取引とは異なり、端末（利用者のPC等）が金融機関の管理範囲外にある。
＝＞　セキュリティは利用者自身が守る必要がある！



MitB攻撃への様々な対策

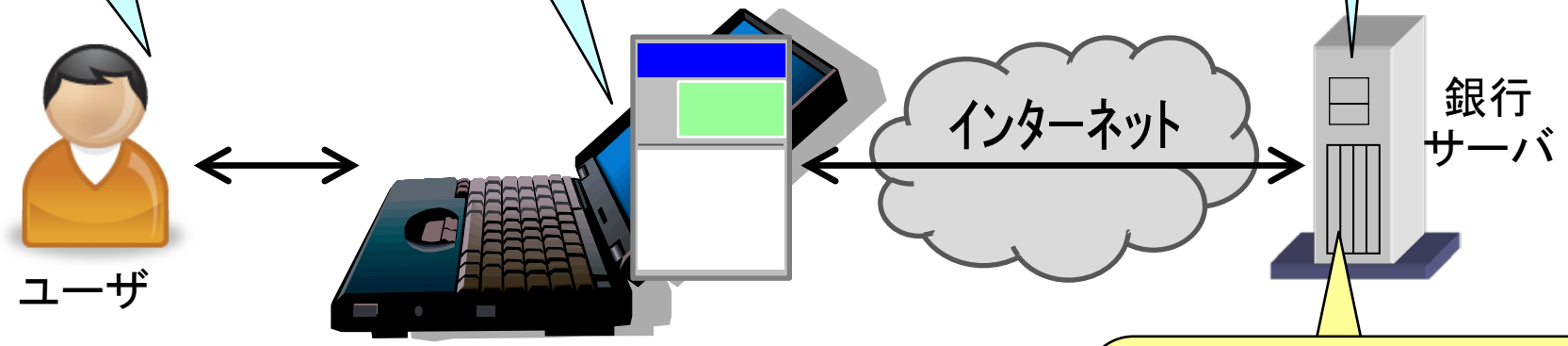
目的：攻撃防止

ユーザの啓蒙

・*怪しいサイト、メールに注意*
・不審に感じたらID等を入力しない

・*ウイルス対策ソフトの利用*
・*OSやブラウザのセキュリティパッチの適用*
・インターネットバンキング専用に用意したPCの利用
・USB等で保護された専用環境を立ち上げ
・ブラウザの保護

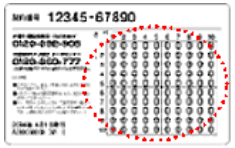
・**取引認証**
・取引パターンに基づく不正取引の検知（リスクベース認証）
・振込先の事前登録



被害軽減
・振込限度額の引下げ
事後検知
・振込結果(振込先・金額)の通知

①金融機関が採用すべき不正送金対策

- 従来は、取引指図を行った人が正規の顧客かどうかを確かめる「本人認証」を強化する対策（ID/パスワードのみに頼らない認証）が中心（多要素認証等の導入）。
  ――ID/パスワード盗取型にはある程度有効な対策。



- しかしながら、利用者が行った取引が勝手に改ざん等される可能性まで考えると「本人認証」だけでは不十分。取引の内容が正規のユーザーの意図したものかどうかを確認する「取引認証（トランザクション署名、多端末を用いた確認等）」を速やかに導入することが必要。
  ―― 利便性に配慮するのであれば、新規振込先登録にのみ取引認証を行うという工夫の余地もある。

取引認証の導入は海外ではあたりまえになりつつあり、国内でも導入は必須

- ただし、日本では「取引認証」を導入ないし導入を準備している金融機関はわずか。

- 取引認証（広義）にも様々な方法がある。

（方法A）取引認証機器による方法・・・セキュリティカード、スマホアプリ、 ICカード＋カードR/W＜欧州型＞

（方法B） SMS（ショートメッセージ）や電話（音声）で取引内容と確認コード（TAN：Transaction Authentication No.）を送信し、取引内容を確認して確認コードを入力しない限り取引を成立させない方法。

（方法C）他経路（スマホ）でも取引内容を確認する多端末認証。

※国内ネット銀行で導入事例あり

取引認証等の方法

主となる取引手段

ブラウザ

①取引指図

④TAN＋取引承認／取引中止

銀行サーバー

③TANを手入力

③TANを手入力

（方法A）TAN生成

②独立したデバイスで、取引内容に応じたTANを生成し、取引認証として使用

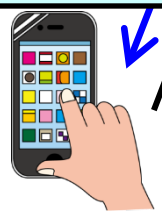
- **専用リーダにICカード挿入**
- PINを手入力
- **振込先、金額を手入力**
  ⇒8桁の数字（TAN）の表示

（方法B）TAN受信

②携帯電話等の**受信機能のみ**を使い、銀行サーバから受付けた取引内容とそれに応じたTANを受信

携帯電話等

（方法C）別端末で取引承認

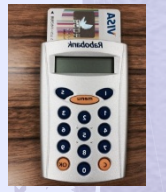


スマートフォンの専用アプリで②サーバが受付けた取引内容を確認した上で、③取引を承認

取引認証の導入を進めるにあたって

- 各行がそれぞれ対策を始めると、預金者は保有する金融機関の口座の数だけ取引認証機器等を持つ必要があり煩雑！
- ICカードを使うタイプで取引認証方法の共通化ができると、カードリーダーライタを共用できるというメリットも。
  ＝＞ベルギーやオランダをはじめとする欧州の事例
  －－全行が機器を配る必要がないコストメリットも。

EMV-CAP



- キャッシュカードのIC化を進め、取引認証でも使用すると便利だが。

－－キャッシュカードのIC化はなかなか進んでいない。ICカードに強制的に切り替えるためにはどうしたらよいのかを考える時期かも。

②金融機関の預金補償

- 現時点では、金融機関は経営判断としてセキュリティ対策を採用するより、被害を補償することで預金者に迷惑をかけない道を選択している。

- 金融機関は、預金者に「（重）過失がない」と認められる場合、（保護対象ではないが）預金者保護法の趣旨に則り、不正払出の被害について補償している。
  - 預金者に「（重）過失がない」と認められるかどうかは、「補償要件、補償基準を満たすかどうか」で判断。

インターネット・バンキングに係る補償の対象・要件・基準等について

（別紙3）

<table>
<tr><th>項　目</th><th>盗難通帳（参考）</th><th>インターネット・バンキング
（モバイル・バンキング、テレホン・バンキングを含む。）</th></tr>
<tr><td>1．補償対象</td><td colspan="2">個人のお客さま</td></tr>
<tr><td rowspan="3">2．補償要件</td><td colspan="2">金融機関への速やかな通知</td></tr>
<tr><td colspan="2">金融機関への十分な説明</td></tr>
<tr><td>捜査当局への盗取の届出</td><td>捜査当局への被害事実等の事情説明（真摯な協力）</td></tr>
<tr><td rowspan="3">3．補償基準</td><td colspan="2">預金者無過失 ⇒ 全額補償</td></tr>
<tr><td>預金者過失あり ⇒ 75%補償※
(1) 通帳を他人の目につきやすい場所に放置するなど、第三者に容易に奪われる状態に置いた場合
(2) 届出印の印影が押印された払戻請求書、諸届を通帳とともに保管していた場合
(3) 印章を通帳とともに保管していた場合
(4) その他お客さまに上記と同程度の注意義務違反があると認められる場合</td><td rowspan="2">預金者過失あり・重過失 ⇒ 個別対応
・インターネットの技術やその世界における犯罪手口は日々高度化しており、そうした中で、各行が提供するサービスは、そのセキュリティ対策を含め一様ではないことから、重過失・過失の類型や、それに応じた補償割合を定型的に策定することは困難である。したがって、補償を行う際には、被害に遭ったお客さまの態様やその状況等を加味して判断する。</td></tr>
<tr><td>預金者重過失 ⇒ 補償せず
(1) 他人に通帳を渡した場合
(2) 他人に記入、押印済みの払戻請求書、諸届を渡した場合
(3) その他お客さまに上記と同程度の著しい注意義務違反があると認められる場合
※上記(1)および(2)については、病気の方が介護ヘルパー（介護ヘルパーは業務としてこれらを預かることはできないため、あくまで介護ヘルパーが個人的な立場で行った場合）などに対してこれらを渡した場合など、やむを得ない事情がある場合はこの限りではない。</td></tr>
<tr><td>4．その他</td><td colspan="2">金融機関への通知が被害発生日の30日後まで行われなかった場合、親族等による払戻の場合、虚偽の説明を行った場合、戦争・暴動等の社会秩序の混乱に乗じてなされた場合は補償を行わない。</td></tr>
</table>

（※）銀行によって特に取り扱いが異なるとみられる事項。

②金融機関の預金補償（続き）

- 補償要件ははっきりしているが、補償基準を明確に定めることは難しいとして、個別判断としている。

- ほとんどの金融機関は注意喚起を行っているが、何を怠ると（重）過失に相当するのかは分からない。
  そうした中でも、一歩踏み込んで、全額補償が受けられない場合がある過失の具体例を示す金融機関もある。
  ＝＞預金者にとって分かりやすい！

例

インターネットバンキング被害においてお客様の重大な過失となりうる場合（ある金融機関Aの例）

重大な過失となりうる場合とは、故意と同視しうる程度に注意義務に著しく違反する場合であり、その事例は典型的には以下のとおりです。

(1) 他人に譲渡・貸与したパソコンや携帯電話が不正使用された場合
(2) 他人にログインID・ログインパスワード・確認用パスワードを渡した場合
(3) ログインID・ログインパスワード・確認用パスワードを他人の目に付きやすい場所に放置した場合
(4) その他、上記と同等の重大な過失が認められる場合

例

過失となりうる場合（ある金融機関Bの例）

①推測されやすいパスワードを設定してる場合

②ID及びパスワードを容易に第三者が認知できるような形でメモなどに書き記し、かつ「お客さまカード」とともに携行・保管していた場合

③IBの利用環境・接続環境に関して改善するよう具体的、複数回にわたる働きかけが行われたにもかかわらず、IBの利用環境・接続環境に改善がみられなかった場合

④ログインした状況で操作端末から離れた結果、被害が発生したとみられる場合

⑤その他お客さまに上記と同程度の注意義務違反があると認められた場合

例

金融機関の注意喚起の例(ある大手行)

パスワード・ご契約カードは重要な情報ですので厳重な管理をお願いします。以下のような事項に該当しますと、補償が難しい場合もございますので、決して行わないようご注意ください。銀行員がパスワードを電話や店舗外でお伺いすることは絶対にありません。

1. パスワードやご契約カードの内容を他人に知らせた場合やご契約カードを他人に渡した場合。
2. パスワードを生年月日・住所の番地・電話番号・自動車のナンバー・同じ数字等他人に類推されやすい番号にしていた場合や同じパスワードを他のお取引に使用していた場合。
3. ご契約カードを他人の目につきやすい場所に放置する、パスワードやご契約カードの内容をメモなどに書き記す・パソコン等に保存する等、第三者に容易に奪われる状態に置いた場合。

例

金融機関の注意喚起の例（続き）

お客さまの大切な情報を盗まれないよう、パソコン・インターネットのセキュリティにも十分ご注意ください。

1. ご利用のパソコンのOS・ブラウザソフトを更新し、セキュリティパッチを適用する、ウイルス対策ソフトは最新のパターンファイルを更新する等、ウイルスの感染やスパイウエアの侵入にご注意ください。
2. ご利用のパソコンにパスワードを設定することをおすすめします。
3. 無線LANやブロードバンドルータ等、ネットワークのセキュリティの設定を確認してください。
4. 身に覚えのない電子メールはフィッシング詐欺の可能性があります。メールやメールに添付されているファイルを開いたり、リンクをクリックしたりしないでください。電子メールへの返信やリンク先のウエブサイトにはパスワード等の重要情報を入力なさらないようご注意ください。なお、当行からお客さまのID・パスワード・口座番号・暗証番号等の重要情報を電話や電子メール等でおたずねすることはありません。当行からお送りする一部の電子メールには、電子署名をつけてお送りしております。
5. 無料ソフトをダウンロードする際や不審な電子メールの添付ファイルを開くことによりスパイウエアが侵入する可能性もありますのでご注意ください。
6. ファイル交換ソフトの使用は十分な知識がないと危険です。
7. インターネットカフェやホテル等に設置されている不特定多数の方が使用するパソコンではスパイウエアに侵入されている場合や手元のキー操作を盗み見される可能性がありますので、〇〇ダイレクトをご利用にならないようおすすめします。

預金補償基準を分かりやすく

- （重）過失となり得る場合とはどんな場合なのかを利用者にもう少し具体的に示すべきではないか？
  - もっとも、預金者に「（重）過失がない」と判断される状況は、世間の常識、社会通念の変化によって変わっていく可能性があるもので留意が必要。
  - 非推奨環境（WindowsXP等）ではサービスが稼働しないようにすることも必要ではないか。

- 預金者は、不正払出の被害者となるという万が一の時に備え、補償が受けられるよう、「（重）過失がない」と認められる最低限の対策を行うようになることが期待される。

③リスクを下げるための他の対策例

1. 被害にいち早く気付かせるよう工夫する
2. 必要以上に預金者にリスクを負わせない
3. パスワードの管理方法について

－－　パスワードについても単なる注意喚起ではなく、金融機関にもできることや、もっとユーザーに濃淡をつけて伝えるべきこともあるはず。

1. 被害にいち早く気付かせる

①月1回は残高や取引履歴を確認できるようにする。

- 預金者保護法では、補償対象期間は、被害を金融機関に通知した日から遡って30日まで。

②ログインの度に前回ログイン履歴はもちろん失敗履歴も簡単に確認できるようにする。

- 前回ログイン日付に心当たりがなければ金融機関にすぐに連絡してもらう。

③なんらかの取引があった時に事前に登録したメールアドレスに通知してくれるサービスを提供する。

2. 必要以上にリスクを負わせない

①振込／振替等の限度額を必要な範囲内で、できるだけ低く設定してもらう（使わないならゼロに）。

- 残高照会のみで資金移動ができないサービスも有効。

②預金のすべてをリスクに晒さないようネットバンキングで扱える預金を口座の中で別段管理する方法も。

- ネットバンキングのサービスを受けられない口座を用意して使い分けるのも一案。

３.パスワードの管理方法について

①パスワードは推測されにくいよう適切に設定させる

- ログイン試行回数には制限があるため、少なくとも預金者の個人情報等から容易に類推されにくいものにさせる。
- リバースブルートフォース攻撃への対策として、パスワードは安易に設定されがちなもの（1234,qwer等）には設定できないようにシステム的に制限する。
- 漏えいして2年以上たったパスワードを使っている場合は補償対象外とする金融機関がほとんどのため、「2年経つ前にパスワードを変更しないと不利益を被る可能性があること」を宣伝すべき。

②パスワード等を自分だけがアクセスできる状態のメモに記録したりPCの中に保存することは止むを得ないが、少なくともパスワードそのものをそのままの形では記録しないように推奨する（一部を変換する等）。

③一部にログインIDを自由に設定できる金融機関があるが、パスワードリスト攻撃を受ける可能性が高まるのでやめるべき。

- 独自のお客様番号をIDとして利用している分には同攻撃には安全。

5. 最後に

金融機関にとってのバランス

- 金融機関は、セキュリティ対策は利便性とリスクとコストのバランスを考えて経営判断しているというが、個々の前提が変わると結論も変わる可能性。
  - セキュリティ対策にかかるコストは、セキュリティ以外の販売促進費用（宣伝費）等から捻出する等の工夫の余地はないのか（ノベルティグッズとして自行名入りの取引認証用のICカードR/Wを配布するベルギーやオランダの事例）。
  - 一律に被害を補償するということは、結果的に、対策を適切に行っている個人が相対的に不利益を被ることにはならないか？
  - やるべきことをやらないために、反社勢力に金銭が流れる状況を放置しているとの見方を受けないか？　コンプライアンスの観点。
  - コストをかけた抜本的な対策を採らず、利用者の利便性を著しく低下させることになる運用等により、その場凌ぎの対応をしている面はないか？　都度振込の即時処理の停止等。

預金者にとってのバランス

- 金融機関は、利用者の利便性を損なうことに繋がる対策には慎重だが、一方で不安を感じて利用を控えている預金者がいることも事実。
  - 利用者が、サービスの利用や対策の導入の有無を判断できるようにすべきではないか？
    ＝＞利用者が利便性とリスクとコストのバランスを判断できるように、正しく情報提供するとともに、対策の選択肢を提供すべきではないか。
- 利用者のセキュリティリテラシーに応じたレベルのサービスの提供という考え方も（預金者を不必要なリスクに晒すべきではない）。
  - 金融機関が提供する認証機器の利用有無、利用者PCのセキュリティ対策の状況等に応じて振込上限金額を変えるという発想。
  - テストでリテラシーを評価し、結果に応じて提供するサービス内容を変える等。
  - 金融機関は、利用者に自分の預金は自分で守るというインセンティブを持たせる方法を考えるべき。結果的に、セキュリティより利便性を重視する利用者へも配慮可能か。

memo