インターネットバンキングを取り巻く犯罪動向

日本銀行　決済機構局　中山靖司

（参考）預金者保護法（2005年8月成立 、2006年2月施行）

▽預金者に故意・重過失があれば、補償されない（金融機関に立証責任）

▽預金者に故意・重過失のない場合の取扱い

取引形態 （個人預金者の取引）			新法
カード	偽造		100%補償
	盗難	預金者に故意・過失のない場合	100%補償
		預金者に過失がある場合（金融機関に立証責任）	75%補償
窓口取引、インターネットバンキング			新法の対象外（注）

（注） 新法の附帯決議では、**政府、金融機関その他の関係者は、例えば、**インターネットバンキングにかかる犯罪等**については、**「速やかに、その実態の把握に努めその防止策および預貯金者等の保護のあり方を検討し必要な措置を講ずること」とされている。

フィッシング（Phishing）とは

- 「フィッシング（Phishing）」とは、銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ID、パスワード等）を入力させるなどして個人の金融情報を不正に入手するような行為。その情報を元に金銭をだまし取られる被害が発生するおそれがある。

- 最近では、様々な手口が増えており、スパイウェア等も含め、IDやパスワードなどの個人情報を詐取する行為全般を指すことも多い。

国内における事案

- 2003年2月　「キーロガー」ソフト
  - 不特定多数の人が利用するインターネットカフェのパソコンに、利用者の操作履歴を記録する「キーロガー（key logger）」ソフトが仕掛けられ、盗まれたIDとパスワードを使って預金が不正に引出された＜A銀行＞。
- 2005年7月　スパイウェア
  - インターネットバンキングを利用する顧客のパソコンが、電子メールで送られてきた不正プログラム（スパイウェア）に感染。ID等を盗まれ、預金が他人の口座に不正に振り込まれた＜B銀行、C銀行、D銀行、E信金＞。
  - その後、法人顧客宛てに、スパイウェア入りのCD-Rを送りつける犯罪も．．

- 2004年11月-2005年7月　フィッシング
  - 実在の金融機関名等を騙って、ID等の入力を促す内容のフィッシングメールが不特定多数の顧客に送付された＜F㈱、G銀行、H銀行＞。

フィッシングの被害状況①

- 日本では、これまでに数千万円の被害規模。
- 一方、警察庁が2005年7月に発表した資料によると、米ガートナー社調べとして、「米国では年間で約7,300万人が平均50件以上のフィッシングメールを受け取り、その被害額は約9億3千万ドル（約1,000億円）に達している」としている。

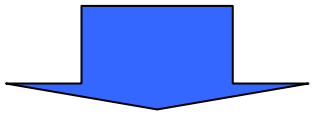
フィッシングの被害状況②

- 海外ではサービス停止に追い込まれた例も
  - フィッシングによってアカウント情報を詐取した攻撃者が、口座にアクセスすることを防ぐため、緊急避難的にオンライン・バンキングのサイトを一時的に閉鎖した例。

2003年12月　X銀行（英）
2005年10月　Y銀行（ニュージーランド）
2005年10月　Z銀行（スウェーデン）

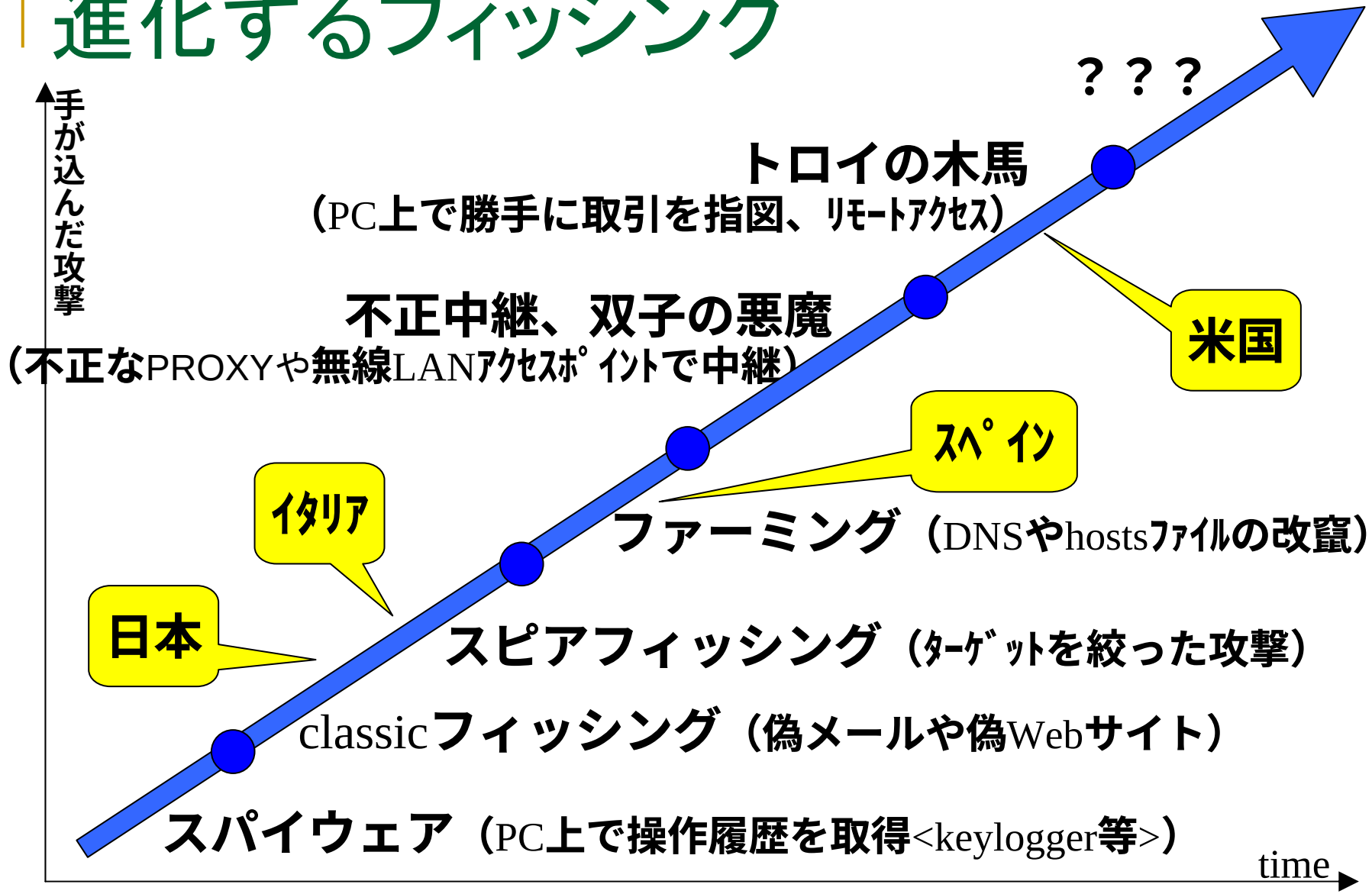
フィッシングの傾向

- 万国共通に行われている個人を標的とする犯罪。
- 使用されているツールもほとんどのものが共通。
- グローバルに国境を越えて行われている組織犯罪であり、不正に送金された資金の流れも類似（ICPOによればバルチック地域の国に集中）。
- 海外では日本をはるかに凌ぐ被害規模となっている。



海外の動向を参考にしつつ、対策を講じるべき

進化するフィッシング


手が込んだ攻撃
？？？
トロイの木馬
（PC上で勝手に取引を指図、ﾘﾓｰﾄｱｸｾｽ）
不正中継、双子の悪魔
（不正なPROXYや無線LANｱｸｾｽﾎﾟｲﾝﾄで中継）
米国
ｽﾍﾟｲﾝ
ｲﾀﾘｱ
ファーミング（DNSやhostsﾌｧｲﾙの改竄）
日本
スピアフィッシング（ﾀｰｹﾞｯﾄを絞った攻撃）
classicフィッシング（偽メールや偽Webサイト）
スパイウェア（PC上で操作履歴を取得<keylogger等>）
time

将来どんな手口が出てくるか予想が困難

（こんな手口もあるという例）

- 2004年10月、欧州の○○銀行で不正アクセスがあり、ロンドン事務所から約2億2000万ポンド（約451億 円）を盗もう という試みがあったことを英国の国家ハイテク犯罪部(National Hi-tech Crime Unit: NHTCU) が明らかにした。
- 犯行グループ は、清掃員として事務所に入りこみ、スパイグッズのような器具、**ハードウェアのキーロガー**をキーボードのUSBポートに仕掛けていた。器具は英国で20ポンド（4100円）程度と安価で、見た目にもケーブルと同化して目立たないため、こうした器具が世の中に存在することを知らない人にとっては気づきようがないものであった。
- 不正にアクセスされた情報は**口座番号、パスワード**などの機密情報。同行によれば、10件の口座から世界中の銀行の口座に送金しようとする資金盗難の試みがあったが、犯行グループは送金には失敗したとのこと。

（Hardware Keyloggerの例）

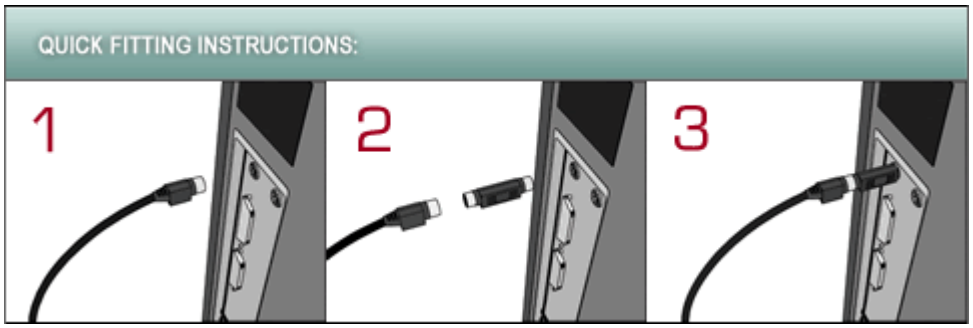
①USBケーブルタイプ

↑↓ﾊｰﾄﾞｳｪｱｷｰﾛｶﾞｰの製品例

装着前

装着後

②コネクタプラグタイプ

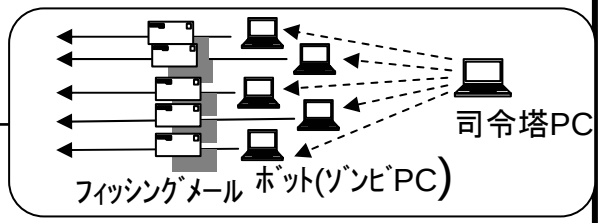


取り付けは簡単

Supply Chain?

分業化が進むフィッシング

①	ﾒｰﾙｱﾄﾞﾚｽ収集業者	ﾌｨｯｼﾝｸﾞﾒｰﾙ送り先のﾒｰﾙｱﾄﾞﾚｽを収集し販売。 ――特定のｻｰﾋﾞｽ利用者等のﾀｰｹﾞｯﾄが絞られているほど高価。
②	ﾎﾞｯﾄﾈｯﾄ貸出し業者	ﾌｨｯｼﾝｸﾞﾒｰﾙの送信等に使用するﾎﾞｯﾄﾈｯﾄを時間貸し。 ――国内でも40～50台に1台はﾎﾞｯﾄに感染している可能性。
③	ﾌｨｯｼﾝｸﾞﾂｰﾙ作成業者	ﾌｨｯｼﾝｸﾞｻｲﾄやﾒｰﾙを作成するためのﾂｰﾙを販売。
④	ﾌｨｯｼﾝｸﾞ実行者	ﾌｨｯｼﾝｸﾞﾒｰﾙ送信し、顧客の金融情報を収集、闇市場で販売。
⑤	犯罪組織 不正な振替え 引出し／送金 ﾏﾈｰﾛﾝﾀﾞﾘﾝｸﾞ	購入した顧客情報を使って管理口座に資金移動。 管理口座から資金を引き出して、組織に送金。 送金された資金を洗浄。



日本銀行 BANK OF JAPAN

フィッシングに対抗するには

①	ﾒｰﾙｱﾄﾞﾚｽ収集	顧客のﾒｰﾙｱﾄﾞﾚｽの一覧等の個人情報の漏洩対策
②	ﾎﾞｯﾄﾈｯﾄ貸出し	ﾎﾞｯﾄPC撲滅のため、利用者を啓蒙（ｳｨﾙｽ/ ｽﾊﾟｲｳｪｱ対策ｿﾌﾄ, ﾊﾟｰｿﾅﾙﾌｧｲｱｳｫｰﾙ等の対策を推奨）
③	ﾌｨｯｼﾝｸﾞﾂｰﾙ販売	早期に販売ｻｲﾄを発見し、閉鎖
④	ﾌｨｯｼﾝｸﾞｻｲﾄ開設	早期にﾌｨｯｼﾝｸﾞｻｲﾄを発見し、閉鎖 ｻｰﾊﾞを乗っ取られ、ﾌｨｯｼﾝｸﾞｻｲﾄとして使われないよう脆弱性対策
	ﾌｨｯｼﾝｸﾞﾒｰﾙ送信	ｽﾊﾟﾑﾒｰﾙ対策（S/MIME、senderID、DomainKeys）
	ﾌｨｯｼﾝｸﾞﾒｰﾙ受信	ｽﾊﾟﾑﾒｰﾙﾌｨﾙﾀﾘﾝｸﾞ等 利用者の啓蒙（ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ対策）
	ﾌｨｯｼﾝｸﾞｻｲﾄ	ﾌｨｯｼﾝｸﾞｻｲﾄ警告ﾂｰﾙ 利用者の啓蒙（ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ対策）

フィッシングに対抗するには（続き）

⑤	不正アクセス	本人認証の強化 端末認証の実施 不正取引監視
	不正な振替指図	振込先を事前登録先に限定
	資金移動	振込み限度額の引下げ 不正の早期検知（前回ログイン時刻の表示、取引結果のメール通知）

フィッシングに対抗するには各セクターの協力が不可欠

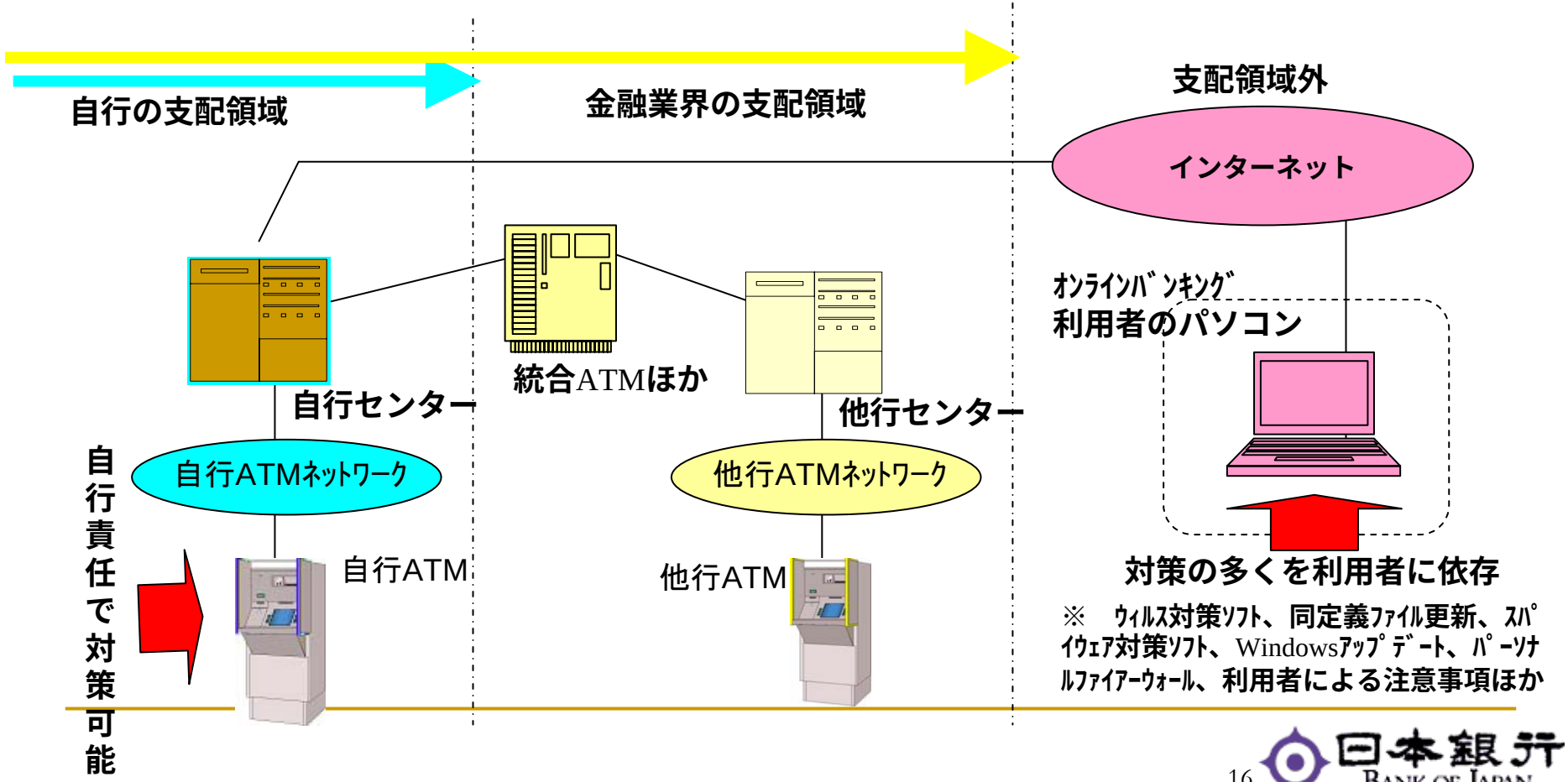
- 通信業者（インターネットプロバイダー）
  - 送信者を騙るﾌｨｯｼﾝｸﾞﾒｰﾙを禁止する技術の導入（senderID、DomainKeys）、不正サイトの早期発見/削除
- 公的機関
  - 犯罪行為取締り、業界指導等
- 金融機関
  - 後述
- 利用者
  - リスクに対するアウェアネスの向上（各セクターから働き掛け）

フィッシング対策（金融機関）

- 利用者の啓蒙
  - 各金融機関のホームページ上等での注意喚起。
- セキュリティ対策の強化
  - 不正の早期検知（不正監視、前回ログイン時刻の表示、取引結果のメール通知）
  - メールやサイトの正当性確認手段の提供
  - 本人認証等の強化
- リスクに応じた利便性/サービスのバランス
  - 振込み限度額の引下げ。
  - 振込先を事前登録先に限定。
- 業界内の協力

利用者啓蒙の大切さ

- 利用者のパソコンを取引端末としているため、セキュリティ対策は利用者のITリテラシーに依存する面が小さくない。



本人認証の強化

- フィッシングによる被害は最終的には「成りすまし」による不正な資金移動指図によって行われるため、本人認証の強化（リスクレベルに応じた認証）が有効。
- また、認証方式のセキュリティレベルや被害発生時の補償の範囲に応じた利用限度額の設定も有効。

（これまでの金融機関の対応例）

- 複数のパスワード
- ソフトウェアキーボードの導入
- 乱数表を使ったパスワード入力
- 「使い捨てパスワード（ワンタイムパスワード）」の導入等
- Tan（TransAction Number：使い捨てパスワード一覧表）の導入（ドイツ）
- IPアドレスによる接続端末の制限ほか

二要素認証の必要性

- ただし、前述の対策でもマウスの操作を記録されたり、操作時の画面のイメージが漏洩したり、通信パケット自体を記録されると防ぎきれないため、二要素認証等を利用することとすることが望ましい（二要素認証が万全というわけではないが．．．）。
- 海外では、二要素認証の必要性に言及する公的機関も多い。例えば、米では連邦金融機関検査審議会<FFIEC>が、2006年末までに二要素認証を導入するよう通告。
- もちろん、「有効」な二要素の組合せでないと意味がない。
  - 二重パスワードは二要素認証とは呼べない
  - スクラッチカード型のﾜﾝﾀｲﾑﾊﾟｽﾜｰﾄﾞはｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞには弱い
  - トークンを使ったワンタイムパスワード発生装置は比較的有効か

問題はコスト．．．　最終的には経営判断．．．

二要素認証とは？

- 二つの異なる方法を組み合わせて行う認証方法（厳密には、以下のうち、異なる分類に属する二方法の組合せ）。
  - ①本人知識によるもの
  - ②本人所有によるもの
  - ③本人固有の特徴によるもの（生体認証）

認証の分類	知識	所有	個人の特徴	
			身体的特徴	身体的特性
具体例	暗証番号、パスワード	IDカード、鍵	顔、掌型、網膜、虹彩、指紋、静脈	筆跡、声紋、キーストローク
留意事項	忘却したり他人に知られたりする惧れ	遺失、盗難の惧れ、複製が困難なことが前提	時間経過等により特徴が変化する惧れ、生体からしか抽出できない情報であることが必要（残存指紋等は使えないこと）	

トランザクション監視と情報共有

- 不正検知システムの高度化（不正が疑われるトランザクションの監視）
- フィッシングに関する情報（不正アクセス元等）の業界内での共有
- 金融分野におけるCEPTOAR機能（Capability for Engineering of Protection, Technical Operation, Analysis and Response：情報共有・分析機能）の活用

（以下参考）

フィッシングと法規制（国内）

フィッシング自体を取り締まる法律は未整備。

- 警察庁では、詐欺/窃盗に至らない段階（偽のホームページの開設等）で、防止、検挙することが何よりも重要とし、フィッシング行為自体を業務妨害罪、著作権法（複製権侵害、公衆送信権侵害等）違反等で検挙するよう努める方針を発表（2004年12月）。

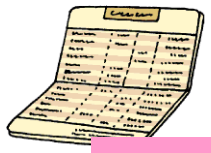
警視庁ハイテク犯罪対策総合センターは、インターネットサービス会社「ヤフー」のＨＰを勝手に複製し、会員のパスワードなどを入手するフィッシング詐欺を行っていた大阪市の会社員（42）を、著作権法違反容疑で逮捕した。同センターによると、フィッシング詐欺事件の摘発は全国で初めて。

国内関連法令による検挙の可能性

②偽ホームページの開設
（著作権法違反、不正競争防止法違反、業務妨害罪？）

①架空名義口座開設or購入
（改正本人確認法違反）

被害者口座



架空名義口座

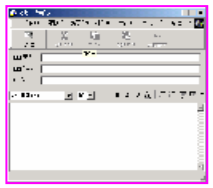
ATM

⑤不正な資金移動指図
（不正ｱｸｾｽ禁止法違反、
電子計算機使用詐欺罪）

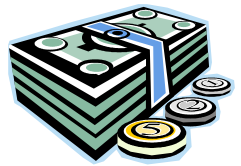
ID,PassWord

④ID、ﾊﾟｽﾜｰﾄﾞ等の不正入手
（？？？）

被害者



犯人



⑥現金引出し
（窃盗罪）

③偽ﾎｰﾑﾍﾟｰｼﾞへの誘導ﾒｰﾙ送信
（業務妨害罪、電子ﾒｰﾙ送信適正化法違反？）

官公庁（国内）の対応

- 利用者の啓蒙の推進
  - 内閣官房、警察庁、金融庁、総務省、経済産業省が連名で注意喚起の通知を発出（「夏休み期間における情報セキュリティにかかる注意喚起～ ﾌｨｯｼﾝｸﾞやｽﾊﾟｲｳｪｱへの対応について ～」<17年7月20日>等）
- フィッシングサイトの早期発見・削除への貢献
  - 警察庁：全国の警察にフィッシング・ダイヤル110番を設置
  - 総務省：ISP（ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ）を中心メンバーとするフィッシング対策推進連絡会を組織し、フィッシングサイトの発見／削除を推進
- フィッシング詐欺に関する情報共有・分析体制の強化
  - 経済産業省：フィッシング対策協議会を立ち上げ、フィッシング事例の収集／分析、同ホームページ上での事例紹介、海外機関との連携等を実施