社会活動部会主催のJNSA会員限定勉強会

証券口座乗っ取りにおける認証システムと補償の問題

--20年前の偽造キャッシュカード問題から考える証券口座乗っ取り問題―

2025年7月29日

松本　泰　NPO JNSA フェロー

証券口座乗っ取りにおける認証システムと補償の問題

- 証券口座の乗っ取り被害が深刻化し、被害補償の可否や責任の所在が社会的な議論を呼んでいます。
- 実は、こうした問題は初めてではありません。約20年前、日本では「偽造キャッシュカード問題」が大きな社会問題となり、金融機関と利用者の責任分担をめぐる混乱の中、最終的には預金者保護法が議員立法により成立し、一定の補償ルールが制度として整備されました。
- 本セミナーでは、この「偽造キャッシュカード問題」の経緯と教訓を振り返りながら、現在の「証券口座乗っ取り問題」と比較し、オンラインサービスにおける認証システムの設計、利用者の責任、そして今後の制度的対応のあり方について考察します。
- また、2025年7月15日の公表された金融庁監督指針改定案、日本証券業協会のガイドライン の改正案について被害を加速させているフィッシング詐欺の進化と現状にを鑑み考察します。

証券口座乗っ取りにおける認証システムと補償の問題

- （1）イントロ
  - 不正取引５０００億円の衝撃
- （2）20年前の偽造キャッシュカード問題
  - サイバー犯罪における被害者補償のあり方と、提供する認証システムのあり方
- （3）偽造キャッシュカード問題から考える証券口座乗っ取り問題
- （4）証券口座乗っ取り問題の対応の動向
  - 2025年7月15日の公表された金融庁監督指針、日本証券業協会のガイドラインの改正案についてのコメント
  - → 2025年現在、最も厳しい業界ガイドライン案なのでインターネット上のサービスの今後を考える上で参考になります。
- （5）「ウェブサイトが真正なウェブサイトであることの証明」は可能なのか？
  - 欧州のアプローチの紹介

イントロ

証券不正売買５０００億円の衝撃？？

証券口座乗っ取りで株価操縦、被害招いた「人任せ」対策

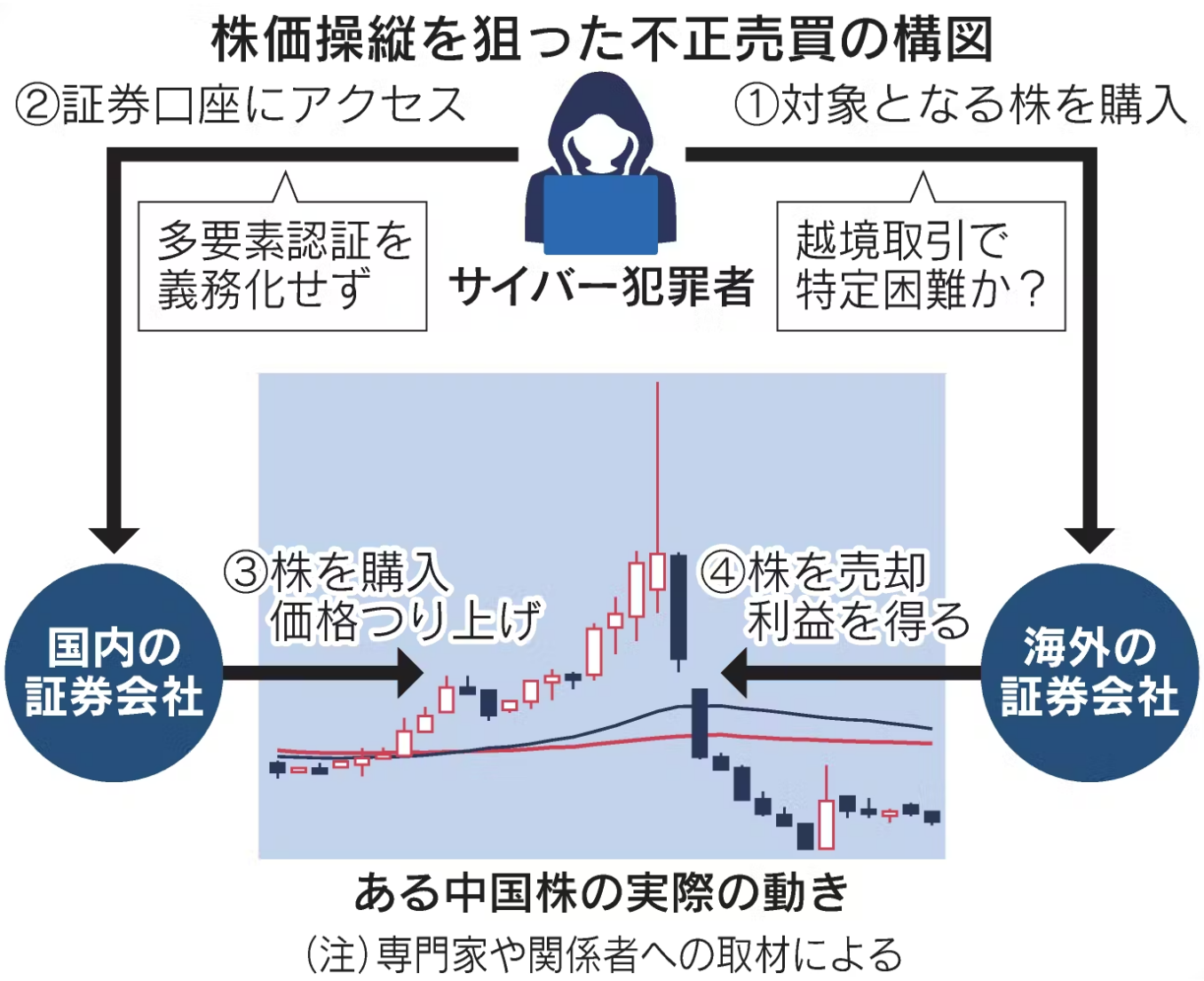
編集委員　須藤龍也

須藤 龍也　＋フォローする

2025年6月25日 5:00 [会員限定記事]

保存

サイバー犯罪者が証券口座を乗っ取り、株価を操縦して利ざやを稼ぐ不正売買に証券業界が揺れている。すでに5千億円を超えた被害はなぜ、起きてしまったのか。専門家や関係者への取材で浮かび上がった犯罪の全体像を検証すると、「人任せ」とも言える業界のサイバー対策の実情が見えてきた。この意識を改めない限り、再発防止の道のりは険しい。



出典:
https://www.nikkei.com/article/DGXZQOCD17BGQ0X10C25A6000000/

この記事は有料会員限定記事です

証券口座乗っ取り、SBI・楽天・松井は原則2分の1補償　対面と対応割れる

証券口座乗っ取り ＋フォローする

2025年7月25日 15:20 (2025年7月25日 17:09更新) [有料会員限定記事]

保存

インターネット証券のSBI証券と楽天証券、松井証券は25日、証券口座の乗っ取り事件を巡り、顧客に被害額の原則2分の1を補償すると発表した。SBIと楽天は全被害者に一律で1万円の見舞金も渡す。野村証券など対面大手は不正に取引された株を元通りにする原状回復で補償する。ネット証券と対応が分かれることになる。

SBIと楽天は近く顧客へ補償の方針を伝える。被害のピークだった4月までの計4000件ほどの不正...

出典:
https://www.nikkei.com/article/DGXZQOUB239J00T20C25A7000000/

補償に関して、証券会社の足並みが揃わない？？

この記事は有料会員限定記事です

証券口座乗っ取り、対策不備ならサービス停止を　金融庁が要請へ

証券口座乗っ取り ＋フォローする

2025年7月26日 17:00 [有料会員限定記事]

保存

証券口座の乗っ取り事件を受け、金融庁と警察庁は近く金融業界全体へ不正アクセス対策の強化を要請する。強固な認証システムの導入を求め、安全性が確保できないサービスは停止の検討を促す。一連の事件は金融サービスの信頼を揺るがしかねず、早急な対策が必要と判断した。

要請は被害が確認された証券業界だけでなく、銀行や保険、暗号資産（仮想通貨）交換業を含むほぼ全ての金融機関の業界団体に出す。法的拘束力はないが各...

金融庁は、証券会社以外にも強固な認証システムの導入を求める？？

出典:
https://www.nikkei.com/article/DGXZQOUD088RV0Y5A700C2000000/

金融庁が公表している被害の状況

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

	2025/1	2025/2	2025/3	2025/4	2025/5	2025/6	合計
不正取引が発生した証券会社数（社）	2	2	5	9	16	7	ー
不正アクセス件数	170	116	2,308	5,351	3,274	1,539	12,758
不正取引件数	96	54	945	2,932	2,329	783	7,139
売却金額（億円）	約2	約0.9	約163	約1,554	約1,109	約215	約3,044
買付金額（億円）	約0.8	約0.8	約142	約1,361	約996	約166	約2,666

- 被害額の大きさからして、補償の切り分けは大きな課題。この補償の法的根拠となるものはあるのか？（無いから結果的に大きな被害を被るに至ったのではないか？）
- 被害が顕著になる前に対策を取ることが出来れば、その後の大きな被害は防げたのでは??

金融庁が公表しているインターネットバンキングの被害と補償

偽造キャッシュカード等による被害発生等の状況について（令和７年６月10日）
https://www.fsa.go.jp/status/higaijyoukyou/index.html

○　被害発生件数

（単位：件）

	令和３年度	４年度	５年度	６年度	対象期間計
偽造キャッシュカード	25	54	14	14	7,685
盗難キャッシュカード	9,797	11,045	9,084	6,936	149,203
盗難通帳	30	19	13	19	3,546
インターネットバンキング	403	2,038	6,737	10,337	30,389
連携サービス	450	559	451	296	1,794

○　平均被害額

（単位：万円）

	令和３年度	４年度	５年度	６年度	対象期間計
偽造キャッシュカード	174	82	385	194	82
盗難キャッシュカード	79	77	80	78	67
盗難通帳	113	83	90	78	166
インターネットバンキング	283	140	174	156	156
連携サービス	11	14	25	27	18

○　インターネットバンキング

（単位：件）

被害発生年度	処理方針決定済				
		補償		補償しない	
令和３年度	401	229	(57.1%)	172	(42.9%)
４年度	2,023	1,549	(76.6%)	474	(23.4%)
５年度	6,649	5,206	(78.3%)	1,443	(21.7%)
６年度	4,992	3,208	(64.3%)	1,784	(35.7%)
対象期間計	24,889	19,296	(77.5%)	5,593	(22.5%)
	-	-	(注)(86.0%)	-	-

- インターネットバンキングの被害は年々増加している。R6年度では、161億円程度？？？
  - 5000億の衝撃
- 被害の7割程度、補償されている。補償の根拠は？？？

偽造キャッシュカード問題等に対する対応状況

https://www.fsa.go.jp/status/higaijyoukyou/index.html

偽造キャッシュカード等による被害発生等の状況

- 偽造キャッシュカード等による被害発生等の状況について（令和７年６月10日） NEW
- 偽造キャッシュカード等による被害発生等の状況について（令和７年３月28日）
- 偽造キャッシュカード等による被害発生等の状況について（令和７年２月５日）
- 偽造キャッシュカード等による被害発生等の状況について（令和６年11月８日）
- 偽造キャッシュカード等による被害発生等の状況について（令和６年６月25日）
- 偽造キャッシュカード等による被害発生等の状況について（令和６年３月26日）
- 偽造キャッシュカード等による被害発生等の状況について（令和６年１月31日）

１．対象期間

以下の期間に発生した被害について、犯罪類型ごとに集計しています。

■偽造キャッシュカード犯罪：平成12年４月から令和７年３月

■盗難キャッシュカード犯罪：平成17年２月から令和７年３月

■盗難通帳犯罪：平成15年４月から令和７年３月

■インターネットバンキング犯罪：平成17年２月から令和７年３月

■連携サービス犯罪：令和２年10月から令和７年３月

証券口座犯罪の集計はない

お問い合わせ先

金融庁　Tel：03−3506−6000（代表）

監督局　銀行第１課（内線3329、3698）
銀行第２課（内線3699、3229）
協同組織金融室（内線3385、3373）
郵便貯金・保険監督参事官室（内線2614、3264）

「証券課」は、担当外

令和７年７月15日
金融庁

「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）の公表について

金融庁では、「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）を別紙のとおり取りまとめましたので、公表します。

本件は、証券会社のウェブサイトを装ったフィッシングサイト等で窃取した顧客情報（ログインIDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が多発したことを踏まえ、インターネット取引における認証方法や不正防止策を強化するために、所要の改正を行うものです。

具体的な改正内容については、（別紙１）～（別紙４）を御参照ください。

また、フィッシング詐欺対策については、メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページのURL やログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く。）、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる、送信ドメイン認証技術の計画的な導入、フィッシングサイトの閉鎖依頼等、提供するサービスの内容に応じた適切な不正防止策を講じているか。

https://www.fsa.go.jp/news/r7/shouken/20250715/20250715.html

（１）ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時におけるフィッシングに耐性のある多要素認証の実装及び必須化
（３）フィッシング詐欺等被害未然防止のための措置

https://www.jsda.or.jp/about/public/bosyu/files/20250715_guideline_public.pdf

「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正について（案）

2025 年 7 月 15 日
日 本 証 券 業 協 会

１．改正の趣旨

本協会では 2021 年３月に、インターネット取引における証券取引口座の開設時から出金に至る各段階における不正防止、脆弱性対策や情報管理、不正利用時の対応等についての具体的な留意事項を「インターネット取引における不正アクセス等防止に向けたガイドライン」（以下、「ガイドライン」）として取りまとめた。

また、2021 年７月には、会員の外部委託先の従業員による不正アクセス・出金が発生したこと等を踏まえ、ガイドラインにおける外部委託先の顧客情報に係る安全管理措置等について、より具体的な事項を定めるための改正を行ってきたところである。

今般、公的個人認証サービス利用や多要素認証の普及・定着などインターネット技術の利活用に係る環境の変化に加え、昨今、フィッシング及びマルウェアにより、顧客情報（ID、パスワード等）が窃取され、インターネット取引において不正アクセス・なりすまし取引等により、従来の不正出金ではなく、不公正取引に悪用されている事案が発生したことを踏まえ、ガイドラインの改正を行うこととする。

２．主な改正箇所

（１）ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時におけるフィッシングに耐性のある多要素認証の実装及び必須化（ガイドライン Ⅳ．１．（２）①）

（２）不正売買、不正出金等を防止・検知するための設定等の利用状況確認等（ガイドライン Ⅳ．１．（３））

（３）フィッシング詐欺等被害未然防止のための措置（ガイドライン Ⅳ．４．（１）～（６））

（４）顧客の被害拡大・二次被害等を防止するための周知・注意喚起等（ガイドライン Ⅳ．７．（２））

（５）その他所要の改正を行う。

証券口座乗っ取りの主な経緯

- 2024年12月　　香港で類似する事案があった？？
- 2025年１月22日-SBI証券　中国株式（香港株）の一部銘柄の新規買付停止
- 2025年2月21日　楽天証券　約款改訂（免責について）　　→　証券会社は、補償に否定的？？？
- 2025年４月3日　　金融庁　　インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています
- 2025年4月16日　日証協会長「多要素認証、基本義務化を」　口座不正対策　　日本経済新聞
  - https://www.nikkei.com/article/DGXZQOUB1670I0W5A410C2000000/
- 2025年4月18日　　日本証券業協会
  - 【重要】インターネット取引サービスを利用する投資家の皆様へ「不正アクセス・不正取引の被害急増のお知らせと　大切な資産を守るためのお願いについて」
- 2025年4月25日　日本証券業協会
  - 多要素認証の設定必須化を決定した証券会社
- 2025年５月２日　日本証券業協会
  - 今般のインターネット取引サービスにおけるフィッシング詐欺等による証券口座への不正アクセス等による対応について（
  - 証券口座乗っ取り 大手10社 被害状況に応じ顧客に補償する方針
  - https://www3.nhk.or.jp/news/html/20250502/k10014795491000.html
- 2025年5月9日　　証券口座乗っ取り、被害補償は証券会社負担に　賠償保険金下りず　日本経済新聞
  - https://www.nikkei.com/article/DGXZQOUB025SU0S5A500C2000000/
- 2025年7月15日
  - 金融庁　「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）公表
  - 日本証券業協会　「インターネット取引における不正アクセス等防止に向けたガイドライン」 の改正について （案）公表

20年前の偽造キャッシュカード問題

- 2004年から2005年にかけて社会問題化
  - → 現在の証券口座乗っ取り問題と類似した社会問題化
- 金融庁「偽造キャッシュカードスタディグループ」
  - 2005年２月２２日から2005年6月16日までに１９回開催
  - 2005年６月２４日（金）　最終報告書公表
- 2005年8月　議員立法「預貯金者保護法」が成立

偽造キャッシュカード問題は、日本におけるサイバー犯罪とは認識されていないかもしれない。しかし2025年現在のサイバー犯罪との類似性は高く、また、現在のインターネットバンキングにおける補償の考え方は、この偽造キャッシュカード問題に端を発している。→　過去の歴史上の重要なインシデントの事例として理解されるべき。

偽造キャッシュカード問題

- 偽造キャッシュカード問題
  - 磁気カードのスキミング装置（スキマー（skimmer））によるスキミング
    - 磁気ストライプカード（magnetic stripe card）
- 偽造キャッシュカード問題の技術、制度、ビジネスの対応
  - 制度の対応
    - 預金者保護法（2005年8月成立、2006年２月 施行）
      - 偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律
      - 偽造・盗難カード使用により被った損害を補償の枠組み
  - ビジネス的対応
    - 取引限度額の引き下げなど
  - 技術的対応
    - ICキャッシュカードなどの普及など
- 2005年　偽装キャッシュカード問題
  - 利用者のキャッシュカード（マグネットカード）が、スキミングにより情報が抜き取られ、利用者は、この事に気が付かない。スキミングされることは、預金者の過失なのか？
- 2025年　証券口座乗っ取り問題
  - ユーザ・パスワードが、フィッシングにより情報が抜き取られ、利用者は、この事に気が付かない。フィッシングされることは、証券口座利用者の過失なのか？

【ケース1】ゴルフ場の貴重品ボックスからキャッシュカードを抜き取りスキミングされる

（年齢不明　被害者多数）　貴重品ボックスの暗証番号をキャッシュカードと同じ番号にしていて

犯人は、ゴルフ場を利用していたお客さまがゴルフ場の貴重品ボックスに入れていたキャッシュカードをスキミングすることで、磁気記録情報を盗みとって偽造キャッシュカードを作成した。

貴重品ボックスには、暗証番号を設定している手元を隠し撮りするために、気が付かない位置に小型のビデオカメラが設置されており、犯人はその情報を使って貴重品ボックスを開けていたが、貴重品ボックスに設定した暗証番号はキャッシュカードの暗証番号と同一のものであったことから、後日、偽造されたキャッシュカードにより、お客さまの口座から多額の現金が不正に引き出されてしまった。

また、キャッシュカード自体は、犯罪の発覚を遅らせるために、貴重品ボックスに戻されていた。

【このケースの特徴】

・貴重品ボックスの暗証番号をキャッシュカードの暗証番号と同じ番号に設定する場合が多いことを狙った犯行です。

・キャッシュカード自体は盗まれていない(戻されている)ことから、発覚が遅れる場合が多いです。

出典：
https://www.jp-bank.japanpost.jp/crime/pdf/inf_crm_pdf_skimming1.pdf

- 分業化・エコシステムのステークホルダー？
- スキミング装置を設計する人
- スキミング装置を製造する人
- スキミング装置を販売する人
- スキミング装置を購入してスキミングする人（ここでの犯人）
- スキミングデータ格納済みスキミング装置を買う人
- 偽造キャッシュカーを作る人
- 出し子
- 集金する人？？

ビジネス化の過程　ニッチな犯罪 -> 分業化 -> エコシステム化 -> 被害の急増

【ケース2】 整体院やマッサージ店において従業員がキャッシュカードを抜き取りスキミングされる

（年齢不明　被害者多数） 会員カードの暗証番号をキャッシュカードと同じ番号にしていて

お客さまが整体院で整体サービスを受けている最中、従業員だった犯人がお客さまの手荷物が入ったロッカーを勝手に開け、バックに入れていたキャッシュカードをスキミングすることで、磁気記録情報を盗み取って偽造キャッシュカードを作成した。

犯人は、店に登録してある会員情報から名前や生年月日等を不正に入手しており、キャッシュカードの暗証番号が会員情報から類推される番号（生年月日等）であったことから、後日、偽造されたキャッシュカードにより、お客さまの口座から多額の現金が不正に引き出されてしまった。

また、キャッシュカード自体は、犯罪の発覚を遅らせるために、バックの中に戻されていた。

【このケースの特徴】

・生年月日等がキャッシュカードの暗証番号に設定されるケースが多いことを狙った犯行です。

・キャッシュカード自体は盗まれていない（戻されている）ことから、発覚が遅れる場合が多いです。

出典：
https://www.jp-bank.japanpost.jp/crime/pdf/inf_crm_pdf_skimming1.pdf

- 従業員だったとされる犯人→アルバイト感覚のスキミングする人？
  - スキミング装置を購入
  - お客様のキャッシュカードをスキミング
  - スキミングを繰り返す
  - スキミングデータが溜まったスキミング装置を売る

【ケース 1】 銀行の店舗外に設置されているATMを使用したら・・・

（年齢不明　被害者多数） ATMにスキミング機（小型読取装置）・小型カメラが取り付けられていた

お客さまが商業施設で買い物をしているとき、その施設に設置されたATMで、自分が利用している銀行のキャッシュカードを使って預金を引き出した。

しかし、そのATMのカード挿入口には、カードをスキミングするための小型読取装置が取り付けられており、磁気記録情報が盗み取られた。

また、ATMコーナーにも暗証番号を入力している手元を隠し撮りするために、気が付かない位置に小型のビデオカメラが設置されており、お客さまが暗証番号のキーを押している手元を隠し撮りされていた。そのため、後日、偽造されたキャッシュカードと、隠し撮りされた暗証番号により、不正に預金が引き出されてしまった。

【このケースの特徴】

- ATM自体にスキミングの読取装置を、ATMコーナーに小型カメラを設置し、お客さまのカードを詐取することなく、カード情報および暗証番号を盗み取ることで犯行を行います。
- 利便性向上のため、ATMはその銀行のカードだけでなく、提携金融機関のキャッシュカードやクレジットカード（キャッシング）でも利用できることが多いので、1 台のATMで被害が発生した場合でも、影響は複数の金融機関におよぶこともあります。
- キャッシュカードやクレジットカード自体は盗まれていないことから、発覚が遅れる場合が多いです。

偽造キャッシュカードの社会問題（2005年）、しばらく経った2010年代に流行った手口。

2025年現在のフィッシングの進化に似ている。

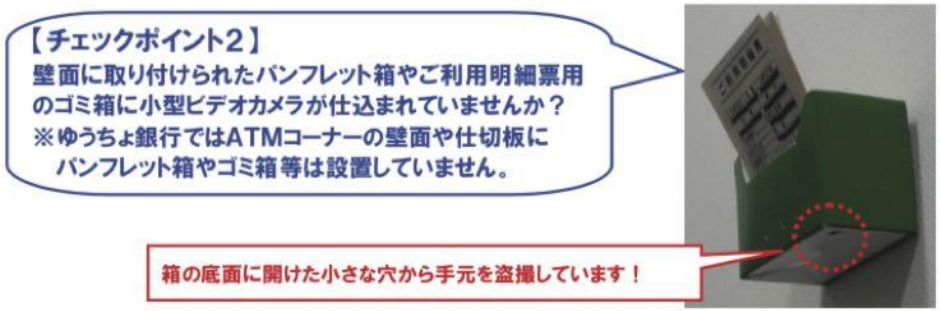
出典:
https://www.jp-bank.japanpost.jp/crime/pdf/inf_crm_pdf_skimming2.pdf

スキミング被害防止のため、ATM利用時にはご注意ください！

最近、商業施設の ATM コーナーに設置された他行の ATM において、スキミング装置や小型ビデオカメラを設置して、偽造カードから現金を不正に引き出す事件が発生しています。

万が一、ゆうちょATMに不審な機器が設置されていた場合はご利用を中止し、ゆうちょ銀行または郵便局の社員、コールセンターにお問い合わせください。

【カード挿入口へのスキミング装置設置イメージ】



【小型ビデオカメラ設置イメージ】

出典
https://www.jp-bank.japanpost.jp/crime/pdf/inf_crm_pdf_skimming.pdf

「偽造キャッシュカードスタディグループ」

- 2005年２月２２日から2005年6月16日までに１９回開催

出典：
https://www.fsa.go.jp/singi/singi_fccsg/member.html

偽造キャッシュカード問題に関するスタディグループ　メンバー

座　　長	岩原　紳作	東京大学大学院法学政治学研究科教授
メンバー	川地　宏行	専修大学法学部教授
	中尾　誠	㈱三井住友銀行執行役員事務統括部長 （第１回～第９回）
	平田　淳	㈱みずほ銀行事務統括部長 （第 10 回～第 19 回）
	姫野　和弘	警察庁生活安全局生活安全企画課都市防犯対策官
	日和佐　信子	雪印乳業㈱社外取締役、前全国消費者団体連絡会事務局長
	松本　貞夫	明治大学法科大学院教授
	松本　勉	横浜国立大学大学院環境情報研究院教授
	松本　恒雄	一橋大学大学院法学研究科教授
	松本　泰	セコム㈱ＩＳ研究所主席研究員
オブザーバー	米谷　達哉	日本銀行金融市場局決済・市場インフラ企画担当総括参事役 （第１回～第６回、第 11 回～第 14 回、第 19 回）
	岩下　直行	日本銀行金融研究所情報技術研究センター長 （第７回～第 10 回、第 15 回～第 18 回）
	吉田　徹	法務省民事局参事官（第１回～第６回）
	筒井　健夫	法務省民事局参事官（第７回～第 19 回）
	郡山　信	(財)金融情報システムセンター監査安全部長 （第１回、第２回）
	久木田　弘好	(財)金融情報システムセンター監査安全部主任研究員 （第３回～第 19 回）
	喜入　博	金融庁情報化統括責任者（ＣＩＯ）補佐官
	杉浦　宣彦	金融庁金融研究研修センター研究官
事 務 局	金融庁監督局	

全銀協の幹事会社？

松本が４人

現京都大学教授

監査業界で長らく活躍されていた

中央大学大学院戦略経営研究科教授

担当した銀行第１課の当時の課長は、前金融庁長官の遠藤俊英氏
銀行第１課の当時の課長補佐は、現財務省審議官の渡辺公徳氏

偽造キャッシュカード問題に関するスタディグループ

- 2005年２月２２日（火）　第１回
  - 岩原座長より、検討項目（座長メモ）について説明
  - 金融庁より、「偽造キャッシュカードに関する金融庁の対応について」について説明
- 2005年2月25日（金）　第２回
  - 柳田邦男氏より、偽造キャッシュカード犯罪及び被害の問題点について説明
- 2005年３月４日(金)　第３回.　法的対応の議論
  - 川地委員より、キャッシュカードの不正使用をめぐるドイツの法状況について説明
  - 岩原座長より、偽造その他無権限キャッシュカード等取引に関する英米仏等の法制について説明
  - 金融庁より、民法第４７８条とＡＴM引出しの適用事例等について説明
- 2005年４月１５日(金)　第９回　技術的対応の議論
  - 岩下オブザーバより、偽造キャッシュカード問題の現状とその対策について説明
  - 松本勉委員より、金融取引における生体認証について説明
  - 松本泰委員より、偽造キャッシュカード問題と認証システムの考察について説明
- 2025年６月１６日　第１９回　最終回
- 2005年６月２４日(金)　最終報告書公表

2005年2月25日（金）　第２回
柳田邦男氏より、偽造キャッシュカード犯罪及び被害の問題点について説明
https://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050225-singi_fccsg/01.pdf

- (1) カードデータを盗む技術の進歩
  - １ 暗証番号を盗む技術
    - のぞき、手の動き、盗撮、回線のブランチ、旧カードの磁気データ etc
  - ２ カード番号を盗む技術
    - スキミング、カードそのもの、回線のブランチ etc
  - ３ 偽造カード作成技術
  - ４ スキミング装置、盗撮カメラ、解読機等の入手容易
- (2) 銀行のセキュリティ対策の不備と怠慢、捜査への非協力
- (3) 警察の捜査の怠慢
- (4) 行政によるセキュリティ対策の制度化の遅れ
- (5) 預金者の関心と具体的注意の稀薄

発売日： 2004/12
https://www.amazon.co.jp/キャッシュカードがあぶない-柳田-邦男/dp/4163667202

- 2025年時点において、サイバー犯罪は複雑化しているが、それが故に、証券口座乗っ取り問題にしても、類似した視点で対応を考えられないと、問題解決にならないのでは？
- 技術自体は、もともと大したことはない。被害の顕著化は、犯罪のエコシステム化。

2005年３月４日(金)　　第３回.　法的対応の議論

金融庁より、民法第４７８条とＡＴＭ引出しの適用事例等について説明

https://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050304-singi_fccsg/03.pdf

○民法第 478 条

「債権ノ準占有者ニ為シタル弁済ハ弁済者ノ善意ナ①リシトキニ限リ其効力ヲ有ス②」

（趣旨）

本条の趣旨は、債務の弁済という日常頻繁に行われる取引を敏速かつ簡便に処理するため、準占有者に対して行った弁済も一定の要件の下に有効としたものとされる。

①「債権の準占有者」とは、取引観念の上からみて真実の債権者と信じさせるような外観を有する者。

②　条文上は、弁済者の無過失を要求していないが、判例上は同条により弁済が有効とされるのは弁済者が「善意かつ無過失」の場合に限るとされている。

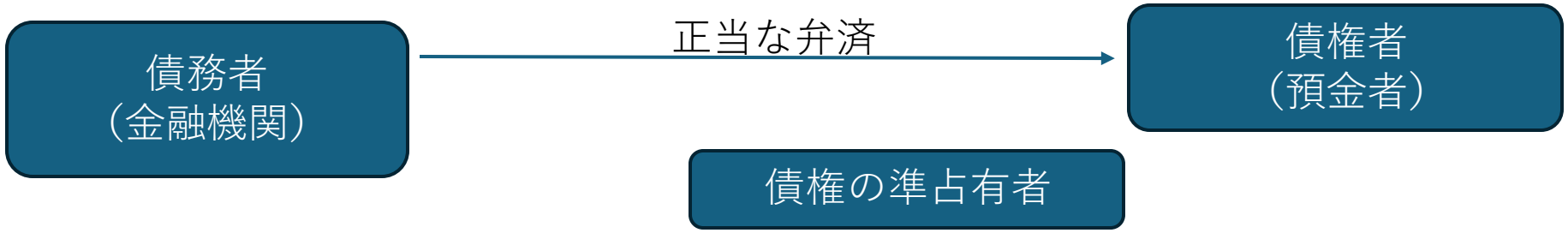
※　なお、同条は債務の弁済についての一般的な規定であり、キャッシュカードの利用に関する約款がある場合は、その約款が有効である限り、約款の定めに従うこととなる。

2004年の民法改正（民法現代語化）は、民法の文言を平仮名・口語体に改められたが、2005年ではまだ？？

趣旨を「平仮名・口語体」で説明されても。。。よくわからない。そもそも、ATM、キャッシュカードとどう関係があるのか？？？

結局のところ、「約款の定めに従う」なのか？

2005年当時の松本は、偽造キャッシュカード問題における補償問題などに関して、明治時代の法律の解釈を議論していたことに、とっても驚いた＆違和感を感じた（その意味、意義が理解できなかった）



偽造キャッシュカード問題に関するスタディグループ（第３回）議論の概要
2005年３月４日（金）
https://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050304-singi_fccsg.html

- もともと民法第478条は、弁済期限が到来した債務について、債務者（銀行）において債権者（預金者）が分からないために履行遅滞が生じることを防ぐため、債務者（銀行）保護の観点から、債務者（銀行）が善意無過失であればその弁済を有効と扱う規定となっており、債権者（預金者）の過失については論じていない。（中略）このため民法第478条の枠内だけで補償の問題を考えることは難しいのではないか。
- 日本では、預金の払戻しは預金債務の弁済と捉えている。しかし、ドイツでは、預金の払戻しは、預金債務の弁済ではなく、銀行が預金者の指示に従い行う現金化という事務処理であり、銀行が預金者に現金を交付した後に、事務処理に要した費用の償還として銀行が預金者の口座から当該金額を引き落とすものと捉えている。この考え方に立てば、債務の弁済ではないため民法第478条を適用する必要はなく、日本においてもこうした解釈は可能と考えられる。
- また、民法第478条を適用することを前提とした場合であっても、本来同条は、民法第480条と関連付けて考えると、誰が債権者であるかに関する認証システムを債権者が主導して作っている場合を前提にしているのではないか。ところが預金については、誰が債権者（預金者）であるかに関する認証システムについて、債務者である銀行が主導して作っている。これは民法第478条の前提とは異なると考えられることから、預金については、同条の適用を否定できるのではないか。
- 他方、従来から、預金通帳による不正払戻しの事案において民法第478条を適用する最高裁判例が積み重ねられているので、同条の適用が当然視されている
- 法律の適用面において、民法第478条のみで事案を処理することの当否については、議論の余地はありうる。民法第478条は債務弁済に関する一般的基本法であり、預金債権についてこの規定だけで問題解決することは困難ではないか。

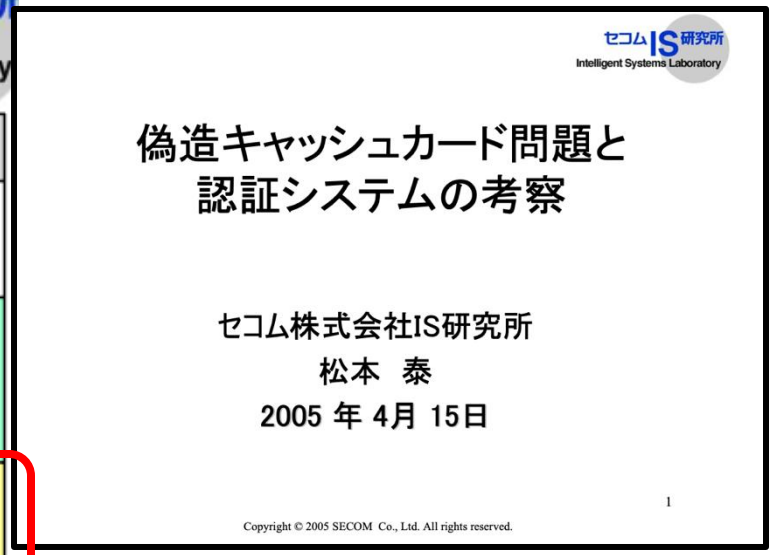
2005年４月１５日(金)　　第９回　　技術的対応の議論
松本泰委員より、「偽造キャッシュカード問題と認証システムの考察」について説明

金融機関の認証システムに関する考察

認証における利用者の義務と金融機関の責任

セコムIS研究所 Intelligent Systems Laboratory

カテゴリ	紛失	盗難	偽造
責任の所在	預金者の責任	預金者の責任とは言い切れない??	金融機関の責任が大きい。
起こり易さ（磁気ストライプ）	預金者の管理次第	預金者の管理次第	スキミングが容易に行なわれる。スキミングを100%防ぐことは困難
起こり易さ（ICカード）	預金者の管理次第	預金者の管理次第	偽造自体が困難。
発覚のタイミング	比較的早い	比較的早い	遅い
悪用のタイミング	比較的遅い	早い	早い。暗証番号の入手方法を隠すために時間をおく場合も考えられる。
暗証番号の漏洩	財布、手帳などに暗証番号を一緒に紛失	巧妙な手口。 財布、手帳など暗証番号を一緒に盗難	巧妙な手口で暗証番号を入手
事件発覚後の預金者の対応	紛失を早期に届ければ被害の可能性は少ない	盗難を早期に届ければ被害を最小減に留められる可能性が高い	発覚のタイミングが比較的遅いため対応は困難であるが早期に届けるべき


セコムIS研究所 Intelligent Systems Laboratory

偽造キャッシュカード問題と
認証システムの考察

セコム株式会社IS研究所
松本　泰
2005 年 4月 15日

1

https://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/03.pdf

2005年４月１５日(金)　第９回　　技術的対応の議論
松本泰委員より、「偽造キャッシュカード問題と認証システムの考察」について説明
発表資料とともに提出した文書　　NIST SP 800-63の紹介も行っている。

偽造キャッシュカード問題と認証システムの考察

目次

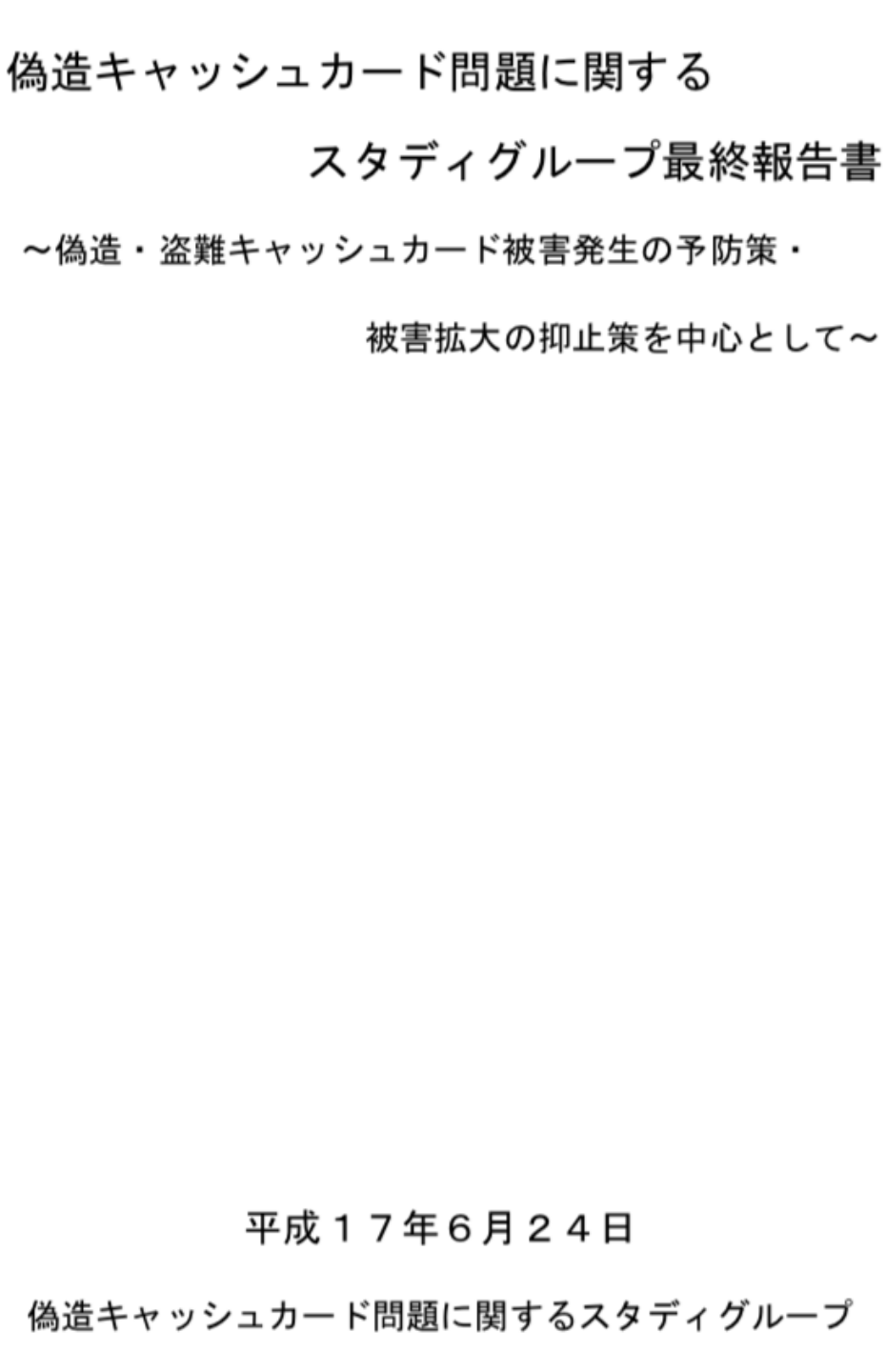
https://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/03.pdf

4.1 認証における利用者の義務と金融機関の責任

キャッシュカードの偽造による被害が社会的な問題になるほどに、金融機関に対しての対応が強く求められてきた。こうしたこともあり補償に関連して「偽造キャッシュカード問題に関するスタディグループ」の中間取りまとめにおいても、３つの大きな原則が述べられている。

○ 偽造キャッシュカードが使用されたことによる損害は、原則として金融機関が負担
○ 但し、預金者の責に帰すべき重大な事由がある場合には、預金者が
○ 預金者の帰責事由については、金融機関に立証責任。

補償の考えかたが示されたことは大きな進歩である。こうした補償を前提キャッシュカードの認証のあり方について検討する必要がある。補償を行なうだけでは、犯罪が減る方向に向かう訳ではなく、根本的な問題が解決されたわけではない。上記の原則により金融機関の責任がより大きくなり、金融機関によりセキュアな認証システムの提供が望まれるところであるが、現実的に、預金者が何の管理に対する義務を果たさずともセキュリティを保てる夢の認証システムはあり得ない。補償を行なうことは、預金者がカード管理や暗証番号の管理を軽視する方向に向かうモラルハザードを生む可能性も指摘されている。金融機関が正当な理由で預金者の帰責事由についての立証ができる認証システムがあるべきであるが（後略）


偽造キャッシュカード問題に関する

スタディグループ最終報告書

～偽造・盗難キャッシュカード被害発生の予防策・

被害拡大の抑止策を中心として～

平成１７年６月２４日

偽造キャッシュカード問題に関するスタディグループ

2005年6月24日

- 報告書の目次

- I.　これまでの検討の経過
- II.　我が国におけるATMシステム及び被害発生の予防策等の現状
- III.　海外の状況
- V.　具体的な被害発生の予防策等
- VI.　終わりに

出典：
https://www.fsa.go.jp/news/newsj/16/ginkou/f-20050624-4/01.pdf

偽造キャッシュカード問題に関するスタディグループ 最終報告書　　2005年 6月24日

- VI. 終わりに
  - 金融機関のシステムやネットワークを巡っては、その技術が日進月歩であ るー方で、犯罪技術についても常に巧妙化が進んでいる状況にある。このよ うな中で、金融機関は、随時、技術の動向を注視し、必要なシステム・セキ ュリティ対策を講じていく必要がある。
  - (略)
  - なお、本スタディグループは、ATMシステムに関わる問題を中心に検討 してきたが、窓口における預金取引(盗難通帳の問題を含む)、インターネ ットバンキング、デビットカードの諸問題についても注視していく必要があ るとの意見が出された。その際、
  - 1　窓口における預金取引については、現行の本人確認の方式は、印鑑による認証を基本とする我が国の商慣習にも関わる重大な問題であ り、その検討にあたっては窓口での本人確認手続き等の実務の対応 及び利用者利便への影響を考慮する必要があること
  - 2　インターネットバンキングについては、利用される端末が金融機関 の管理下にないこと、また、電子商取引一般との整合性について考慮する必要があること
  - 3　デビットカードについては（略）

最終報告書の記述　　６．盗難キャッシュカード被害に関する補償のルール案
＃預金者保護法では、その思考過程はわからないので重要
＃多分、2005年以降に、このような包括的な考察はなされた来なかったのはないか？

①　警察への被害届等を補償を求めるための前提とする。

②　金融機関に故意又は過失がない場合であっても、（現行約款等の考え方を改め、）預金者に故意又は過失がない場合は、金融機関が損害を補償することとする。

③　立証責任については、キャッシュカードが盗難されて現金が引き出されるに至った事情については預金者にしか分からず、また、システム提供者としての責任を果たしていたかは金融機関にしか分からないため、前者の立証責任は預金者に、後者の立証責任は金融機関に課す。

しかしながら、こうしたルール案の場合、特に、預金者にとっては、盗難されたことについての帰責事由がないことの立証は実際には困難であることが多いため、一般人としての通常の注意義務を果たしていた場合であっても、補償されない事態が想定される。また、全ての盗難被害について、個々のケースごとに立証を行うことは預金者、金融機関双方にとって実務上の負担が極めて大きいことが懸念される。

したがって、損失負担のルール案の策定に当たっては、上記「前提となる考え方」でも述べたように、理論的な妥当性のみならず、実行可能性についても配慮することが必要であると考えられ、 その観点から以下のような点を満たすルール案が適当ではないか。

①　過失責任の原則をベースとしつつも、預金者・金融機関の公平性に十分配慮しつつ、大量の事故を処理する観点から、基本となる対応方針を定めた上で、さらに当事者の過失が明らかな場合については、それに応じた負担を求めることとする。

②　そのために、可能な限り外形基準による認定を行い、負担が大きい個別の過失認定を行う場合を限定していくこととする。

③　モラルハザード回避の観点から、両当事者に犯罪予防に対する適切なインセンティブを与える仕組みとする。

預貯金者保護法　　2005年8月成立、2006年２月 施行
偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律
https://laws.e-gov.go.jp/law/417AC1000000094

- （目的）
- 第一条　この法律は、偽造カード等又は盗難カード等を用いて行われる不正な機械式預貯金払戻し等による被害が多数発生していることにかんがみ、これらのカード等を用いて行われる機械式預貯金払戻し等に関する民法（明治二十九年法律第八十九号）の特例等について定めるとともに、これらのカード等を用いて行われる不正な機械式預貯金払戻し等の防止のための措置等を講ずることにより、これらのカード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護を図り、あわせて預貯金に対する信頼を確保し、もって国民経済の健全な発展及び国民生活の安定に資することを目的とする。
- （定義）
- 第二条　この法律において「金融機関」とは、次に掲げるものをいう。
- 一　銀行
- （略）　＃→　証券会社は含まれない
- （カード等を用いて行われる機械式預貯金払戻し等に関する民法の特例）
- 第三条　民法第四百七十八条の規定は、カード等その他これに類似するものを用いて行われる機械式預貯金払戻し及び機械式金銭借入れ（以下「機械式預貯金払戻し等」という。）については、適用しない。ただし、真正カード等を用いて行われる機械式預貯金払戻し等については、この限りでない。
- （偽造カード等を用いて行われた機械式預貯金払戻し等の効力）
- 第四条　偽造カード等を用いて行われた機械式預貯金払戻しは、…

証券会社は、含まれない
（対象外）

預貯金者保護法も、民法第478条の特例という建て付け

2008年　銀行無過失の場合でもお客さまに過失がないときは原則補償
→ インターネットバンキングにも適用

2008年2月19日

各　位

全国銀行協会

申し合わせ

「預金等の不正な払戻しへの対応」について

全国銀行協会（会長　奥 正之　三井住友銀行頭取）は、今般、預金者保護法※、同法附則および附帯決議を踏まえ、盗難通帳やインターネット・バンキングによる預金等の不正な払戻しが発生した際に、銀行無過失の場合でもお客さまに過失がないときは原則補償する旨の申し合わせを別添のとおり行いましたのでお知らせいたします。

- 「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」

以　上

出典：
https://www.zenginkyo.or.jp/news/2008/n2933/

2008年　銀行無過失の場合でもお客さまに過失がないときは原則補償
→ インターネットバンキングにも適用

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)

項　目	盗難通帳（参考）	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。）
1. 補償対象	個人のお客さま	
2. 補償要件	金融機関への速やかな通知	
	金融機関への十分な説明	
	捜査当局への盗取の届出	捜査当局への被害事実等の事情説明（真摯な協力）
3. 補償基準	預金者無過失 ⇒ 全額補償	
	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	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。
	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。	
4. その他	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。	

(※)銀行によって特に取り扱いが異なるとみられる事項。

https://www.zenginkyo.or.jp/fileadmin/res/news/news200219_4.pdf

2025年　インターネットバンキングなどの補償に関する現状の法的解釈
→ 多分、法的には、「証券口座乗っ取り問題」への適用は難しい（民法第478条の適用は困難ではないか？）

項目	キャッシュカード・ATM	インターネットバンキング
法的根拠	預金者保護法で明記	預金者保護法の趣旨＋指針・ガイドライン
補償	原則あり（過失なし）	原則あり（過失なし）
制限条件	利用者に「重大な過失」があると補償対象外	同様に「利用者の過失」の要件あり

立証責任の変化

時代	預金者が立証すべきこと	金融機関が立証すべきこと
預金者保護法以前	銀行に過失があったこと	なし（事実上有利）
預金者保護法以後（2025年現在の解釈）	重過失でなかったこと（場合による）	適正な確認手続き（利用者の認証）だったこと

20年前の偽造キャッシュカード問題から考える

証券口座乗っ取り問題

- 被害額の大きさからして、補償の切り分けは大きな課題。この補償の法的根拠となるものはあるのか？？
- 被害が顕著になる前に対策を取ることが出来れば、その後の大きな被害は防げたのでは??
  - → このためには、預金者保護法のような補償の枠組みは必要だったのではないか？？

過去からの歴史的経緯

- 明治時代
  - 民法第478条
- 2004年まで
  - 預金通帳による不正払戻しの事案において民法第478条を適用する最高裁判例が積み重ねられてきた。　→　　判例に基づいた対応
- 2004年
  - 偽造キャッシュカード問題　　エコシステム化による犯罪の急増
- 2005年　預金者保護法
  - ＃立証責任が金融機関側へ
- 2008年　金融機関
  - インターネットバンキングの補償においても預金者保護法の趣旨を反映
- 2025年
  - 証券口座乗っ取り問題

被害額の大きさからして、補償の切り分けは大きな課題。この補償の法的根拠となるものはあるのか？（無いから結果的に大きな被害を被るに至ったのではないか？）

- 預金者保護法＆民法第478条
  - 証券会社は、預金者保護法の対象外
  - 証券会社と口座利用者の関係は、民法第478条の債権者、債務者の関係とは異なる？？
  - 同様に『2008年の全銀協「銀行無過失の場合でもお客さまに過失がないときは原則補償」』も、適用外
  - →．他に根拠となる法律があるのかどか？？？（松本は、分からない）
- 管轄官庁の金融庁
  - 金融庁
    - 監督局
      - 銀行１課、銀行２課　　→　　全国銀行協会(全銀協)
      - 証券課　　→　　日本証券業協会
  - 多分、過去からの経緯から鑑みて「預金者保護法」に準じた対応を示唆？？（指導？？）
    - 日本証券業協会の自主的なガイドラインの策定？？？？？
    - → 2025年7月15日の監督指針改定案、日証協のガイドライン改定案
    - →　しかし、「補償」には、触れられていない。

被害が顕著になる前に対策を取ることが出来れば、その後の大きな被害は防げたのでは??

- 対策を遅らせた証券会社の意識
  - 今回の証券会社の意識は、2005年の偽造キャッシュカード問題以前の金融機関の意識に近い??
    - 証券会社も被害者という意識が強かった???
    - 約款の「免責事項」で「弱い認証システム」を正当化???
- （証券サービスに）預金者保護法のような補償の法的枠組みがあれば
  - 口座利用者の過失に対する立証責任を果たすことが可能な「認証システム」を提供する根拠が生じる（と思う）。
  - ２要素認証の導入が、他の証券会社にお客様を取られるといったことがなくなった??

まとめ

- 20年前の「偽造キャッシュカード問題」は、サイバー犯罪という認識はないかもしれないが、「証券口座乗っ取り問題」などのサイバー犯罪の構図と大きく変わらない。
- 20年前に行われた「偽造キャッシュカードスタディグループ」における議論は、正に「今」必要なのではないか？
  - 特に金融機関の責任、利用者の責任、補償も含めた制度対応の議論
  - そもそも犯罪を減らすためのフレームワークのあり方
- 適切な補償のフレームワークは、結局のところ 「認証システム」を提供するサービスプロバイダーにとっても中長期的は、とっても重要

証券口座乗っ取り問題の対応の動向

2025年7月15日の公表された

- 金融庁「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）
- 日本証券業協会の「インターネット取引における不正アクセス等防止に向けたガイドライン」 の改正について （案）」

→ 2025年現在、最も厳しい業界ガイドライン案なのでインターネット上のサービスセキュリティの今後を考える上で参考になります。

注目するべきは、
- フィッシングに耐性のある多要素認証
- フィッシング詐欺等被害未然防止のための措置

令和７年７月15日
金融庁

「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）の公表について

金融庁では、「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）を別紙のとおり取りまとめましたので、公表します。

本件は、証券会社のウェブサイトを装ったフィッシングサイト等で窃取した顧客情報（ログインIDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が多発したことを踏まえ、インターネット取引における認証方法や不正防止策を強化するために、所要の改正を行うものです。

具体的な改正内容については、（別紙１）～（別紙４）を御参照ください。

また、フィッシング詐欺対策については、メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページのURL やログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く。）、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる、送信ドメイン認証技術の計画的な導入、フィッシングサイトの閉鎖依頼等、提供するサービスの内容に応じた適切な不正防止策を講じているか。

https://www.fsa.go.jp/news/r7/shouken/20250715/20250715.html

（１）ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時におけるフィッシングに耐性のある多要素認証の実装及び必須化
（３）フィッシング詐欺等被害未然防止のための措置

https://www.jsda.or.jp/about/public/bosyu/files/20250715_guideline_public.pdf

「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正について（案）

2025 年 7 月 15 日
日 本 証 券 業 協 会

１．改正の趣旨

本協会では 2021 年３月に、インターネット取引における証券取引口座の開設時から出金に至る各段階における不正防止、脆弱性対策や情報管理、不正利用時の対応等についての具体的な留意事項を「インターネット取引における不正アクセス等防止に向けたガイドライン」（以下、「ガイドライン」）として取りまとめた。

また、2021 年７月には、会員の外部委託先の従業員による不正アクセス・出金が発生したこと等を踏まえ、ガイドラインにおける外部委託先の顧客情報に係る安全管理措置等について、より具体的な事項を定めるための改正を行ってきたところである。

今般、公的個人認証サービス利用や多要素認証の普及・定着などインターネット技術の利活用に係る環境の変化に加え、昨今、フィッシング及びマルウェアにより、顧客情報（ID、パスワード等）が窃取され、インターネット取引において不正アクセス・なりすまし取引等により、従来の不正出金ではなく、不公正取引に悪用されている事案が発生したことを踏まえ、ガイドラインの改正を行うこととする。

２．主な改正箇所

（１）ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時におけるフィッシングに耐性のある多要素認証の実装及び必須化（ガイドライン Ⅳ．１．（２）①）

（２）不正売買、不正出金等を防止・検知するための設定等の利用状況確認等（ガイドライン Ⅳ．１．（３））

（３）フィッシング詐欺等被害未然防止のための措置（ガイドライン Ⅳ．４．（１）～（６））

（４）顧客の被害拡大・二次被害等を防止するための周知・注意喚起等（ガイドライン Ⅳ．７．（２））

（５）その他所要の改正を行う。

フィッシングに耐性のある多要素認証
→　口座利用者の過失に対する立証責任を果たすことが可能な「認証システム」

- 20年前の偽造キャッシュカード問題
  - 磁気ストライプカード
    - スキミング耐性がないため、所持による認証になっていない。
  - ICカード
    - スキミング耐性があり、所持による認証として適切。口座利用者の過失の立証を明確にしやすい。
- 2025年　　証券口座乗っ取り問題
  - ユーザID、パスワード
    - フィシング耐性がない。高度化するフィッシングの現状を考えるとフィッシングに引っ掛かることを証券口座ユーザの過失とすることは困難に。また、利用者の過失を証券会社が立証することは難しい。
  - メール・SMSを使った２要素認証（２段階認証）
    - リアルタイムフィッシングの耐性に欠ける。所持による認証としては、弱い。
    - メールセキュリティに頼ることになるので、実質、証券会社が利用者の過失を立証することは難しい（そもそも、メールアカウントの乗っ取りが増加している）
  - FIDO2など　（実質、スマートフォンのFIDO2Platform Authenticatorの利用）
    - ＃現状は、ベストプラクティスかもしれないが、スマフォのセキュリティなどの依存しているため利用者の過失を証券会社が立証出来ないケースもあるかもしれない点を、運用も含めてよく考察する必要がある。

「フィッシング耐性のある認証」の定義??

NIST SP 800-63B Revision 4　July 2025　「フィッシング耐性（phishing resistance）」

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf

- 3.2.5.　フィッシング耐性　　Phishing Resistance
- フィッシング攻撃は、SP 800-63Bでは「検証者なりすまし(verifier impersonation)」と呼ばれていたもので、不正な検証者やRP(（Relying Party）が、不注意な認証者(unwary claimant)を騙して偽の認証器（ authenticator）を提示させるようとする試みです。
- SP 800-63の以前のバージョンでは、フィッシング攻撃に耐性のあるプロトコルは「強いMitM耐性（中間者攻撃耐性）」とも呼ばれていました。
- フィッシングという用語は、類似した攻撃の多種多様な形態を説明する際に広く使用されています。本文書では、フィッシング耐性とは、認証プロトコルが、認証秘密情報（authentication secrets）や有効な認証器（authenticator）出力情報を、認証者の注意に依存することなく、偽の検証者（impostor verifier）に開示しない能力を指します。
- 認証者（claimant）が偽の検証者に誘導される方法は、この定義には関係ありません。例えば、認証者が検索エンジン最適化（SEO）経由で誘導されたか、メールで促されたかに関わらず、その攻撃はフィッシング攻撃とみなされます。
- 承認された暗号アルゴリズムは、必要に応じてフィッシング耐性を確立するために使用しなければなりません。この目的で使用される鍵は、[SP800-131A]の最新版（本公開日時点では112ビット）で指定される最低限のセキュリティ強度を提供しなければなりません。
- 認証器（Authenticators ）の出力を手動で入力する認証方法（例：アウトオブバンド認証器やワンタイムパスワード認証器）は、フィッシング耐性がありません。それは、認証器の出力を認証対象のセッションに結び付けないからです。例えば、偽の検証者が認証器の出力を検証者に転送し、認証に成功する可能性があります。　**1
- フィッシング耐性には2つの方法が認識されています。チャネルバインディングと検証者名バインディングです。チャネルバインディングは、検証者名バインディングよりも安全であるとされています。なぜなら検証者証明書の誤発行や不正使用に脆弱ではないためです。
- しかし両方の方法はフィッシング耐性の要件を満たしています。

**1　「リアルタイムフィッシング」の耐性

4. フィッシング詐欺等被害未然防止のための措置 → これらは、本当に効果があるのか

- 【スタンダード】
  - フィッシング詐欺被害未然防止の観点から、以下の（１）から（６）について実施する。
  - また、フィッシング詐欺対策の情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等、金融庁・警察当局等から提供された犯罪手口に係る情報などを活用することが考えられる。
  - (1) 顧客へ送信する電子メールのドメインを特定し、DMARC 等の送信ドメイン認証技術の計画的な導入を行う。また、DMARC レポート等の確認等を行った上で、ポリシーは「reject」にする。
  - (2) 共通ショートコード9を利用し、Web サイト上又はアプリケーション上等で当該共通ショートコードを公開する。
  - (3) 自社を騙るフィッシングサイトについて、そのアクセス制限のためのテイクダウン（閉鎖）活動を行う。
  - (4) ドメインは自己のブランドと認識し、以下の①から③を中心に適切に管理する。
    - ① 自組織に割り当てられているドメイン名を把握・管理する。
    - ② ドメイン名のライフサイクルを管理する。また、ドロップキャッチやサブドメインテイクオーバー等の攻撃に対する対策を実施する。
    - ③ 顧客に対し、サービスで使用するドメインに関する周知を行う。
  - （５） 利用者がアクセスしているウェブサイトが真正なウェブサイトであることの証明を確認できるような措置を講じる。
  - （６） メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページのURL やログインリンクを記載しない（法令に基づく義務を（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く）。
- 【ベストプラクティス】
  - 顧客が各社からの正規のメールだと判断できるように、以下を実施することが望ましい。
  - ① 電子メールにブランドのロゴや公式マークが表示されるよう、BIMI への対応を行う。
  - ② 顧客へ何らかの通知を行う場合のメールについて、S／MIME による電子署名を付与する。

4. フィッシング詐欺等被害未然防止のための措置 －

証券口座乗っ取り問題においては、送信ドメイン認証技術は、無力だったかもしれない。メーラのUIの問題も大きい。

- 【スタンダード】
  - フィッシング詐欺被害未然防止の観点から、以下の（１）から（６）に
  - また、フィッシング詐欺対策の情報の収集に当たっては、金融関係団体や金融情報 センターの調査等、金融庁・警察当局等から提供された犯罪手口に係る情報などを活用することが考えられる。
  - （1）顧客へ送信する電子メールのドメインを特定し、DMARC 等の送信ドメイン認証技術の計画的な導入を行う。また、DMARC レポート等の確認等を行った上で、ポリシーは「reject」にする。
  - （2）共通ショートコード9を利用し、Web サイト上又はアプリケーション上等で当該共通ショートコードを公開する。
  - （3）自社を騙るフィッシングサイトについて、そのアクセス制限のためのテイクダウン（閉鎖）活動を行う。
  - (4) ドメインは自己のブランドと認識し、以下の①から③を中心に管理する
    - ① 自組織に割り当てられているドメイン名を
    - ② ドメイン名のライフサイクルを管理する。 対策を実施する。
    - ③ 顧客に対し、サービスで使用するドメイン

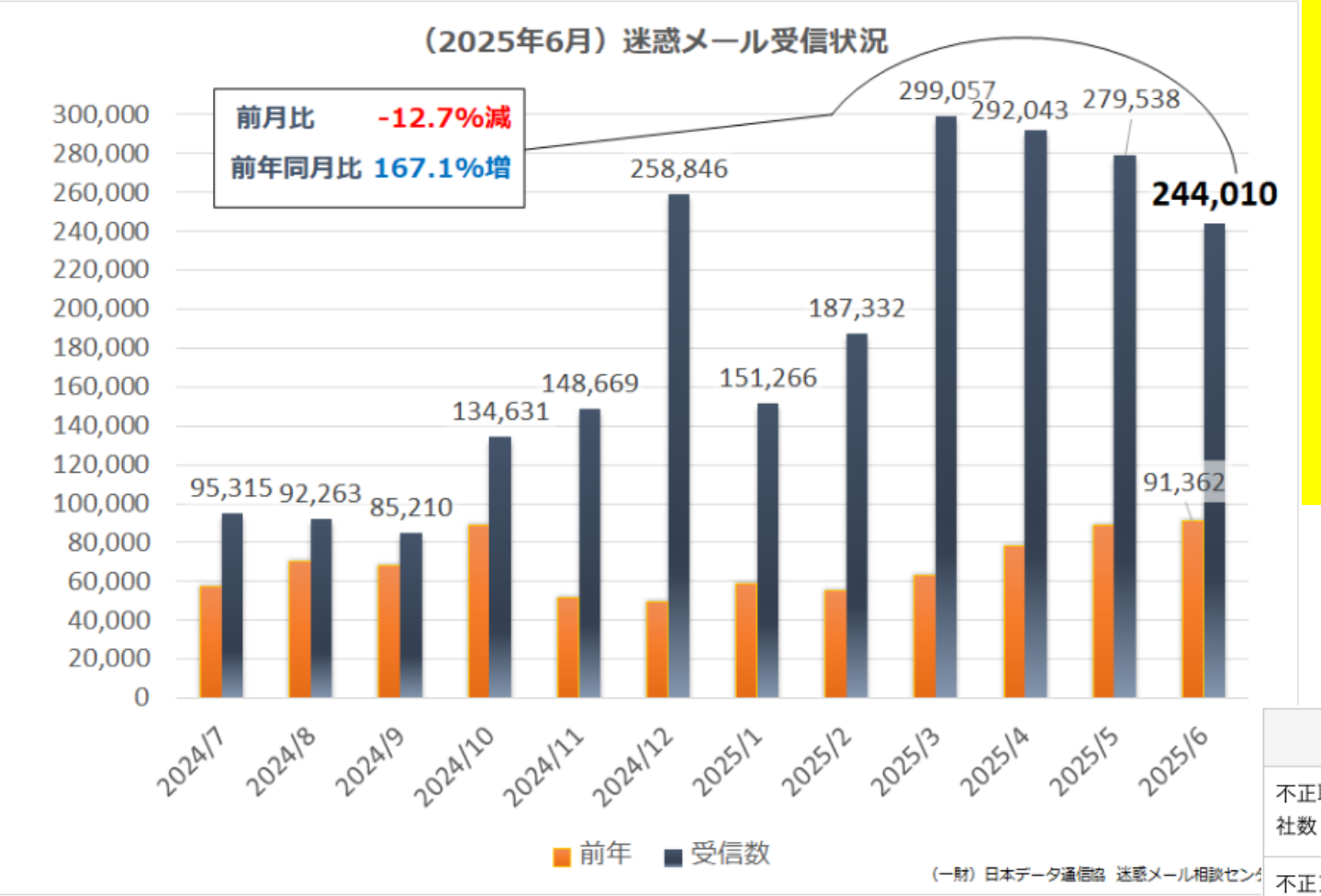
フィッシングサイトは、ほぼ全て、短命ドメインであり非常に短時間で立ち上げ、短時間で閉鎖される。モグラ叩き的なテイクダウンだけでは対策になっていない。なぜそのようなことが可能になっているの理解が重要

  - （５） 利用者がアクセスしているウェブサイトが真正なウェブサイトであることの証明を確認できるような措置を講じる。
  - （６） メールや SMS（ショートメッセージサ 内にパスワード入力を促すページのURL やログインリンクを記載しない（法令に基づく義務を（法令に基づく や に必要な場合など、その他の代替的手段を採り得ない場合を除く）。

そもそも真正ウェブサイトとは何か？、証明は誰ができるのかの理解が重要

- 【ベストプラクティス】
  - 顧客が各社からの正規のメールだと判断できるように、以下を実施することが望ましい。
  - ① 電子メールにブランドのロゴや公式マークが表示されるよう、BIMI への対応を行う。
  - ② 顧客へ何らかの通知を行う場合のメールについて、S／MIME による電子署名を付与する。

今時のフィシングメールの状況



出典：
https://www.dekyo.or.jp/soudan/contents/activities/statistics/2025/report202505.html

- 2025年現在の「迷惑メール」は、ほぼ、フィッシングメール（SPAMメールは、すでに死語かも）
- 2025年3月のフィッシングメールの多くは、証券口座乗っ取りを目的としたもの
- 2025年５月のフィッシングメールの多くは、証券会社の対策の文面
- 2025年6月に「迷惑メール」が減っているのは、「迷惑メール対策」の成果ではない。証券会社の２要素認証の導入などにより証券口座乗っ取りが難しくなったため

出典：
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

	2025/1	2025/2	2025/3	2025/4	2025/5	2025/6	合計
不正取引が発生した証券会社数（社）	2	2	5	9	16	7	―
不正アクセス件数	170	116	2,308	5,351	3,274	1,539	12,758
不正取引件数	96	54	945	2,932	2,329	783	7,139
売却金額（億円）	約2	約0.9	約163	約1,554	約1,109	約215	約3,044
買付金額（億円）	約0.8	約0.8	約142	約1,361	約996	約166	約2,666

5月2日に顧客に補償をする方針を決めたとるする大手10社のDMARCポリシー
2025年6月16日に調査　→　最近設定した可能性もあるが、

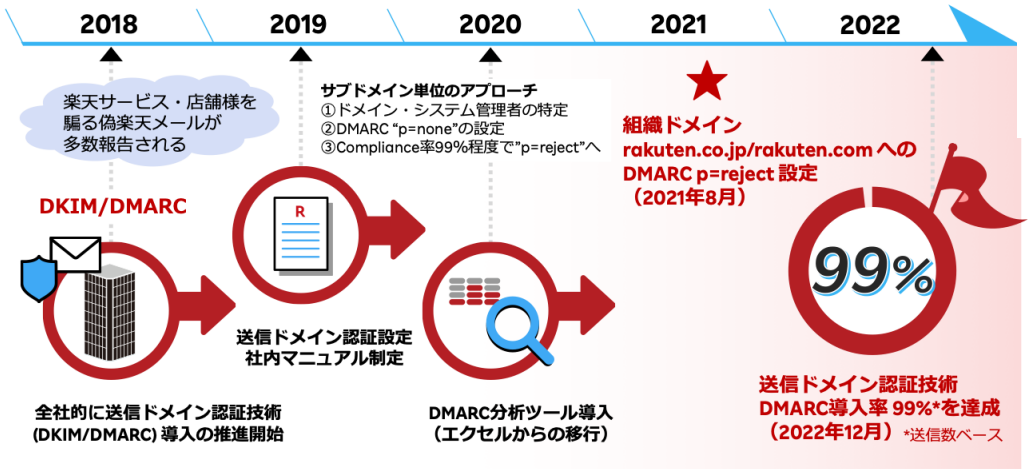
			DMARCポリシー
1	楽天証券	rakuten-sec.co.jp	p=reject
2	SBI証券	sbisec.co.jp	p=quarantine
3	野村證券	nomura.com	p=reject
4	大和証券	daiwa.co.jp	p=reject
5	松井証券	matsui.co.jp	p=reject
6	マネックス証券	monex.co.jp	p=none
7	三菱ＵＦＪモルガン・スタンレー証券	sc.mufg-terrace.com	p=none
8	ＳＭＢＣ日興証券	mail.smbcnikko.co.jp	p=reject
9	みずほ証券	email.mizuho-sc.com	p=none
10	三菱UFJeスマート証券	kabu.com	p=none

実際に標的とされ、また大きな被害を受けたのは
楽天証券（p=reject）、SBI証券(p=quarantine)、野村證券(p=reject)の３社

最新フィッシング動向とDMARC運用のポイント
- 楽天におけるDMARC対応の歩みとBIMIの導入 -

2023年1月26日
楽天グループ株式会社
テクノロジーマネジメントディビジョン
情報セキュリティ・プライバシーガバナンス部
高田 加菜江

楽天サービスにおけるDMARC対応の歩み



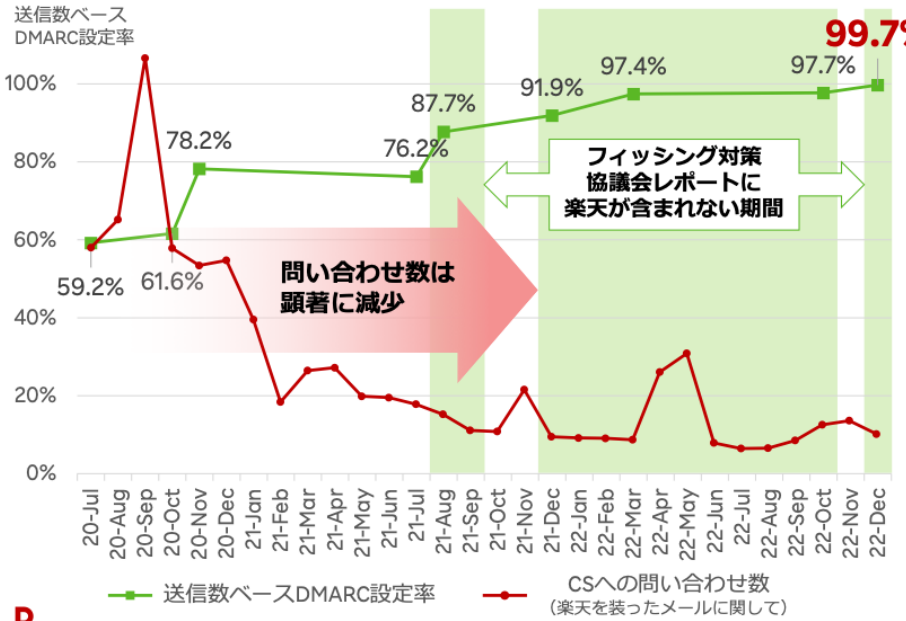
R

4

出典：
https://www.janog.gr.jp/meeting/janog51/wp-content/uploads/2022/12/JANOG51_DMARC_高田さん.pdf

DMARC "p=reject" 適用の効果と課題

DMARC設定率とカスタマーサービスへの問い合わせ数の比較



問い合わせ状況

- 不定期にスパイクが発生
- このメールは本物か、という問い合わせが多い

➢ ユーザ自身でメールを判別できる仕掛けが必要

偽メールの傾向

- 非楽天ドメインを使用（見た目のみ楽天）

➢ DMARCでは対応できない、非楽天ドメインによる偽メールへの対策が必要

R

5

ここが狙われた

楽天証券をターゲットとしたフィッシングメールが激増したと考えられが、それは、楽天グループ（楽天証券を含む）が、SPF /DKIM /DMARCなどによる対策を行わなかったためではない。

様々なタイプのフィッシングメール？？？

SPAMメールサービス
SPAM判定されやすい

SPAM
メールサーバ
DMARC p=non

短命ドメイン偽メールサーバ
短命なのでSPAM判定されにくい？

偽メールサーバ
SPF/DKIM設定
DMARC p=non

乗っ取りメールアカウント

正規のメールサービス

送信メールサーバ
SPF/DKIM設定
DMARC p=reject

From 詐称した場合
正規証券のDMARC p=reject
は有効に働く
“DMARC p=non”の企業が習われるされる根拠？？？

From ドメインの詐称を行わない（表示名：display-name は詐称）
この場合は、正規証券の
DMARC p=reject は、無力

正規証券
SPF/DKIM設定
DMARC p=reject

正規証券 2
SPF/DKIM設定
DMARC p=non

受信メールサービス

メーラのUIの問題
表示画面が狭いスマートフォンなどのメーラーに問題が多い？？？

「4. フィッシング詐欺等被害未然防止のための措置」に対する素朴な疑問（根本的な？？？）疑問

- 偽メールサーバ、偽Webサーバを非常に短時間に立てることが可能な理由は、そもそもトラストのない審査などが不要なドメイン発行にのみで構築可能なことにある
  - ドメイン発行のみに依存している送信ドメイン認証（SPF/DKIM/DMARC）は、それだけでは、本質的な解決にはならないのでは？
  - 同じく、偽Webサーバは、ほぼすべて、Let‘s Encrypt （DV証明書）は無料の TLS 証明書を利用しており、これもドメイン発行にのみ依存している
  - ドメインの発行のみに依存している限り「真正なウェブサイト」「真正なメールサーバ」の判別は付かないのではないか？
- （時間もかかる）審査があるのは　　→　普及しない（と思われている）
  - メールサーバ
    - BIMI(Brand Indicators for Message Identification)
  - Webサーバ
    - EV証明書　（OV証明書も審査は行っていが審査基準がない）
  - BIMI＆EV証明書は、多くの組織にとっては、必要ないが、フィッシングの対象となるような組織、法人にとっては、区別が付いて欲しいと考えるはず
- BIMI＆EV証明書が有効に働くためには
  - これらが機能するためには、ブラウザーベンダー、メーラーベンダーによる、判別可能なUIの実装が必須

「ウェブサイトが真正なウェブサイトであることの証明」は可能なのか？

欧州のアプローチの紹介

eIDAS2.0　45条　　2024年5月成立

ウェブブラウザプロバイダーは、証明書（QWAC：Qualified Website Authentication Certificates）で証明されたアイデンティティデータと追加の証明された属性がユーザーフレンドリーな方法で表示されることを保証する必要がある。

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

「真正なウェブサイト」の意味をもう少し深掘りする必要がある。
証明された属性　→　欧州の金融監督機関が、「認可した金融機関」であることを証明
この証明された属性（金融機関であることを）ユーザーフレンドリーな方法で表示されることを保証

フィッシング サイトと正規サイトの区別がつけばフィンシングメールも減る？？

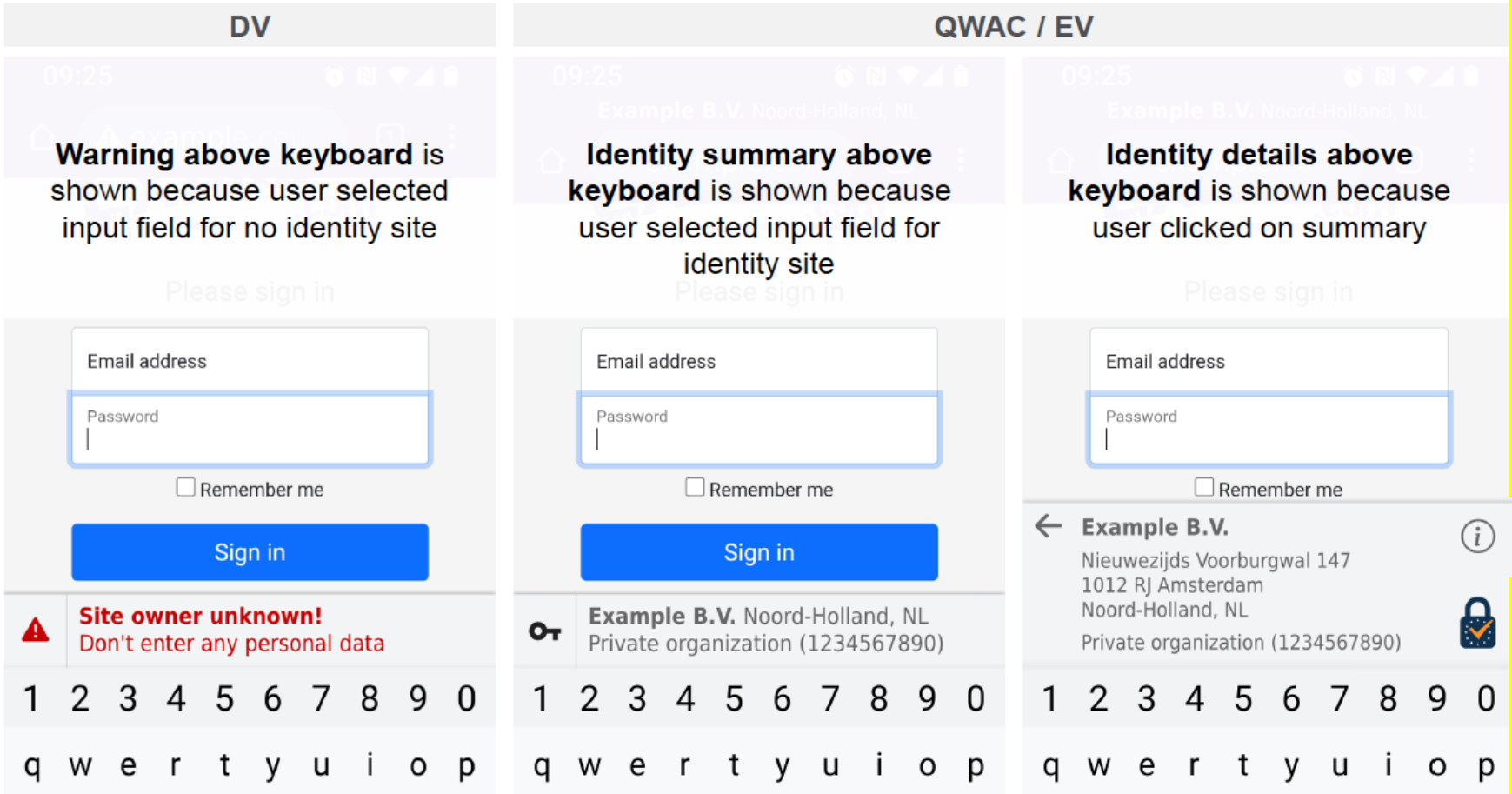
- インターネットメールの散々な状況
  - ＃溢れかえるフィシングメール
    - メールのコストは、極めて安価だが、安価になるほどに、フィシングメールが増加する
    - 正当なメールを運用するためのコストは、上昇する一方
- フィッシングサイトの問題　→　偽メールサーバと類似
  - フィッシングの対象となる正規サイトは、金融機関とか証券会社とか極わずかに対して偽Webサーバは、山のようにあり、その区別がつかない。。。。。
  - 偽Webサーバは、ほぼ、すべて、Let‘s Encrypt は無料の TLS 証明書を利用
- 欧州のeIDAS2.0のQWAC
  - フィッシングの対象とならないような普通のサイトは、Let’s Encrypt の無料 TLS 証明書で何ら問題はないが、フィッシングの対象となる正規サイトは、金融機関とか証券会社とかは、偽Webサーバとか有象未曾有のサイトとは、区別がついて欲しい訳はず。
  - 欧州のeIDAS2.0 では、QWAC（Qualified Website Authentication Certificate）というやつを使って、多分、そのサイトの金融機関とか、医療機関とか、区別できるような仕組みを提供しようとしている。
  - この区別は、Webブラウザが表示することになるが、そうした仕組みが、Webブラウザに実装される（eIDAS2.0が、このことを要求している）。
  - eIDAS2.0の成立時、Webブラウザベンダーが、猛烈に反対していたこともあり、あまり情報が出てこないのですが、現在、検討は、進んでいるぽい。
  - →　なぜ、日本では、類似する議論が皆無なのか？？　→　むしろEV証明書（QWAC）などを批判している人が多い

https://www.slideshare.net/slideshow/etsi-esi-activities-fesa-ecats-2025-05-14-pdf/279151528

eIDAS2.0　45条　　2024年5月成立
ウェブブラウザのプロバイダーは、証明書（QWAC：Qualified Website Authentication Certificates）で証明されたアイデンティティデータと追加の証明された属性がユーザーフレンドリーな方法で表示されることを保証する必要があります。

情報入力時に警告するUIをブラウザに実装

Summary of EU compliant data entry interfaces



このスライドは、2021年、eIDAS2.0案が提出された後のChris Bailey, Entrustの提案

2024年に、ETSIにおいて、Web Authentication Task Forceが活動を開始しており、2025年現在もUIに関する検討は行われていると考えられる。

2024年6月 Google は、デジタル証明書のセキュリティを維持するため、Entrust の証明書をディストラストすることを発表している。
https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

出典：　Designing the new eIDAS 2 browser UI
https://www.enisa.europa.eu/events/trust-services-forum-ca-day-2021/ca-day-presentation/05_chris-bailey_20210900-ca-day-designing-the-new-eidas-2-browser-ui.pdf

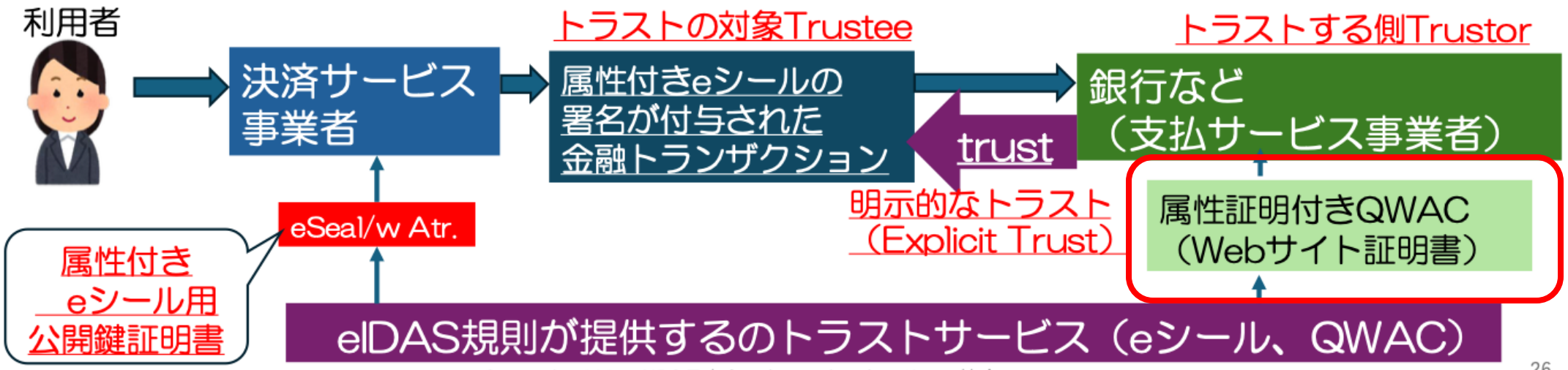
フィッシングのターゲットなるWebサイトの識別
EUのデジタルアイデンティウォレットで検討されているQWACによる属性証明
→ EUのデジタルアイデンティウォレットでは「証明された属性」によるアクセス制御が検討されている

- 従来からのEV証明書への批判
  - 正規の法人であれば、金さえ払えば証明書を発行しているので、信頼できる法人とは限らない（実際、そのようなサイトが作られたし、そもそもの法人登記が甘い国がある）
  - → 正規の法人によるWebサイトが、本当に、真正なWebサイトなのか？
- EUのデジタルアイデンティウォレットで検討されているQWACによる属性証明
  - 個人のDIWのアクセス先の明示（アクセス制御・制限も行う） -> Draft 段階
  - relying party role が public administration、trust service providers、qualified trust service providers、public sector attestation issuer、banks and credit institutions
  - other regulated institutions on EU .. その他。。。

欧州のPSD2における（トラスト）な金融トランザクションの考え方

＃ここでは、「金融トランザクション」をトラストの対象（Trustee）と捉える

- PSD2（Payment Services Directive 2）とは、欧州連合（EU）が2018年に施行した決済サービスに関する指令であり、決済サービスの透明性と競争の促進
  - 多対多の関係にある「決済サービス事業者」と「銀行など（支払サービス事業者）」間のトランザクションデータ（このトラストを如何に実現するのか）
- 属性付きeシール証明書は、欧州の金融監督庁が与えた属性（許可番号）の証明も行われている
  - → Trustworthinessは、許認可を行なっている欧州の金融監督機関の役割が大きい
  - → Trust メカニズムは、トラストサービスが発行するeIDAS 規則の(属性付き）eシールなどの役割
- 利用者は、欧州の決済エコシステムにおけるPSD2のような制度・トラスト管理に暗黙のトラストを置く



出典：https://www.iwsec.org/scis/2025/_img/page/YasushiMatsumoto_SCIS2025_InvitedTalk.pdf

欧州の金融管轄官庁により証明された属性（許認可された決済サービス事業者、支払いサービス事業者）によるアクセス制御（QWACを利用）は、欧州のPSD２で既に利用されている。

まとめ

まとめ
横行するフィッシングに対抗することは出来るのか？？

- 証券口座乗っ取りは、フィッシング攻撃を大きく進化させた可能性がある。フィッシング対策は、これまでの取り組みだけでは足りないかもしれない。そもそもの「真正なウェブサイト」「真正なメールサーバ」をどのように判別するのか？そこから考える必要がある。
- 進化するフィッシング攻撃は、認証システムの要求も高度化させている。単純な２要素認証から、フィッシング耐性（リアルタイムフィッシングに対する耐性）もある認証の要求へ
- 2025年7月15日の公表された金融庁監督指針改定案、日本証券業協会のガイドライン の改正案は、証券業界に留まらず、金融業界全体に波及する可能性がある。