日本銀行金融高度化セミナー資料

金融機関を取り巻く最近のサイバー脅威動向と求められる対策

2020年10月

日本銀行 金融機構局

日本銀行
BANK OF JAPAN

本日のご説明内容

1. 「サイバーセキュリティに関するアンケート」結果のポイント

2. 最近のサイバー脅威動向の変化と求められる対策

「サイバーセキュリティに関するアンケート」の概要

- 実施時期：2019年9月

  —— 同様のアンケートを2017年4月に実施

- 対象：日本銀行の当座預金取引先金融機関等のうち402先

  —— 内訳は、銀行134先、信用金庫249先、系統中央機関4先、金融商品取引業者7先、証券金融会社1先、短資会社3先、資金清算機関1先、金融商品取引清算機関2先、その他1先

- 回収率：100％

⇒ 調査結果を金融システムレポート別冊「サイバーセキュリティの確保に向けた金融機関の取り組みと課題」として公表（2020年1月）

URL: https://www.boj.or.jp/research/brp/fsr/data/fsrb200131.pdf

アンケート結果のポイント

- 同様のアンケート調査を実施した2017年4月時点と比べ、多くの金融機関がサイバーセキュリティの確保を経営上の重要課題と捉え、体制整備や技術対策などの取り組みを進めている
- もっとも、サイバーセキュリティの企画に携わる要員が引き続き不足しているほか、グループベースでの啓発・教育・訓練の取り組みに改善の余地がみられる
- 脆弱性診断やシステムへの攻撃試行等による検査、コンティンジェンシープランに基づく訓練について、前回調査時以降の改善が十分に進んでいない先が少なくない
- 新たなデジタル技術の導入に伴う対応についても、パブリッククラウドで経営上重要なシステムを構築したり、重要な情報資産を扱う場合に必要となる追加的な管理体制の整備が、一部の先では十分に進んでいない
- サイバー攻撃により被害を受けることを前提とした訓練の実施など、対応が急がれる項目については、優先的な経営課題として取り組む必要

金融庁による働きかけ

【令和元事務年度金融行政方針（2019年8月）より抜粋】

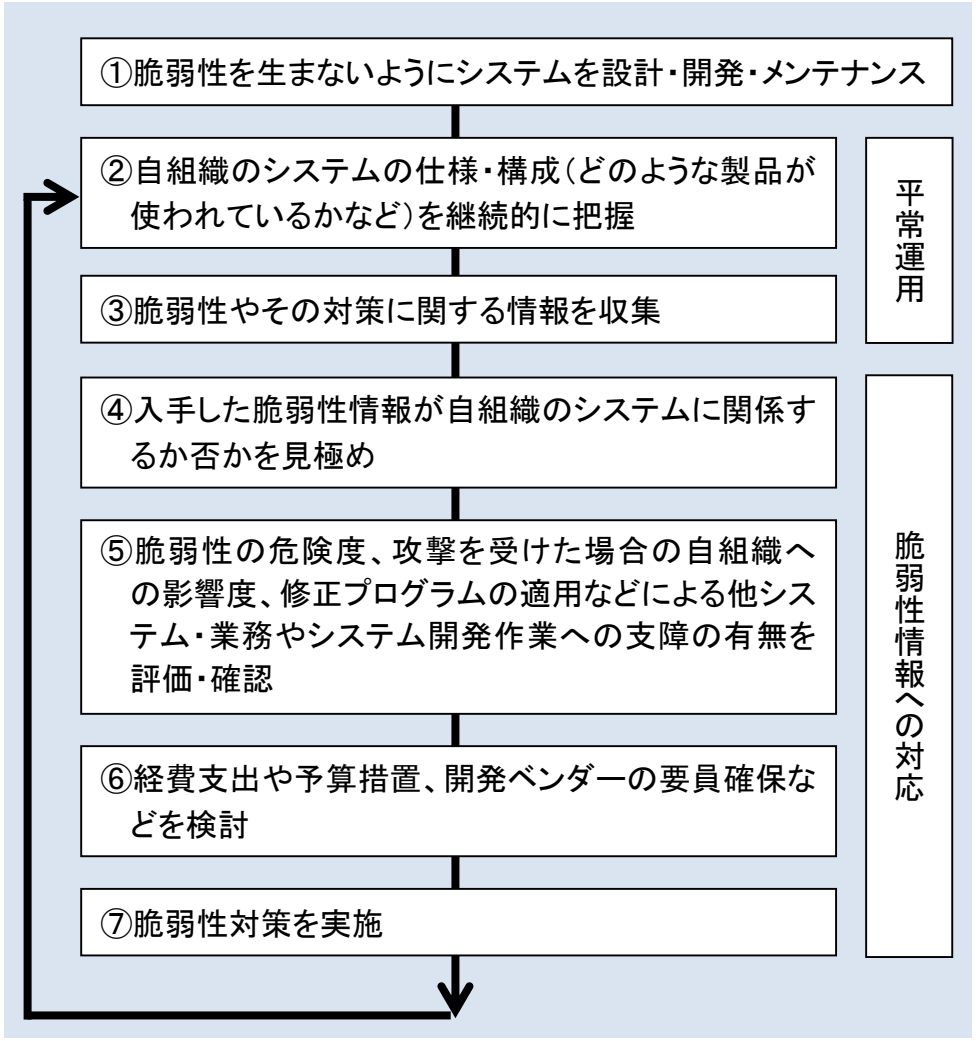
「・・・サイバーの脅威に適切に対応していくために、サイバーセキュリティ対策の実効性強化に取り組む。中小金融機関に対しては、脆弱性診断等の活用、サイバーセキュリティ演習への参加を通じて、サイバー攻撃からの防御・インシデント対応能力の強化を図る。大手金融機関に対しては、TLPTの深度を更に高めるなど、サイバーセキュリティ対策のより一層の高度化を促す。さらに、連携会議も活用し、連携手順の整備や演習等を通じた業界全体の連携態勢の強化を図る。」

⇒ 脆弱性検査（脆弱性診断やシステムへの攻撃試行等）、コンティンジェンシープランに基づく演習・訓練について、アンケート実施後に改善が進んだことが期待される

⇒ これらの検査・訓練を継続的に実施するとともに、確認された課題を解決し、改善に繋げていくプロセスを確立することが重要

脆弱性検査（脆弱性診断や攻撃試行等）はなぜ必要か

▽脆弱性に対するリスク管理プロセス（例）



設計・開発・メンテナンス時に意図しない箇所で脆弱性が残存するリスク

一部のシステムの構成を正確に把握せず脆弱性が残存するリスク

情報収集が不十分で自組織に関連する脆弱性情報を見落とすリスク

脆弱性の自組織への影響等を誤って評価するリスク

↓

<u>脆弱性検査は左記のリスク管理プロセスを補完</u>し、システムに残存する脆弱性を早期に識別し対処できるようにすることが目的

コンティンジェンシープランに基づく演習・訓練の重要性

- *金融セクターのサイバーセキュリティに関するG7の基礎的要素*（2016年）

  要素5：インシデント発生時の対応（Response）

  「・・・金融機関や当局が、あるいはこれらの主体が共同で行う演習は、より効果的なインシデント対応につながるものである。演習を行うことで、金融機関と当局は、とりうる意思決定が互いの能力 ― 重要なもの、そうでないものを含めた機能・サービス・業務を維持する能力 ― にどのような影響を与えるのかを把握することができる。」

- *Effective Practices for Cyber Incident Response and Recovery*（金融安定理事会、2020年）

  45. Exercises, tests and drills.

  “Organisations conduct tests on a regular basis, such as tabletop exercises and live simulations, to validate and improve the knowledge as well as understanding of resources regarding their CIRR [cyber incident response and recovery] activities and capabilities, and more in-depths drills to assess the robustness of their CIRR plans and procedures. …”

本日のご説明内容

1. 「サイバーセキュリティに関するアンケート」結果のポイント

2. 最近のサイバー脅威動向の変化と求められる対策

最近のサイバー脅威動向の変化（1）

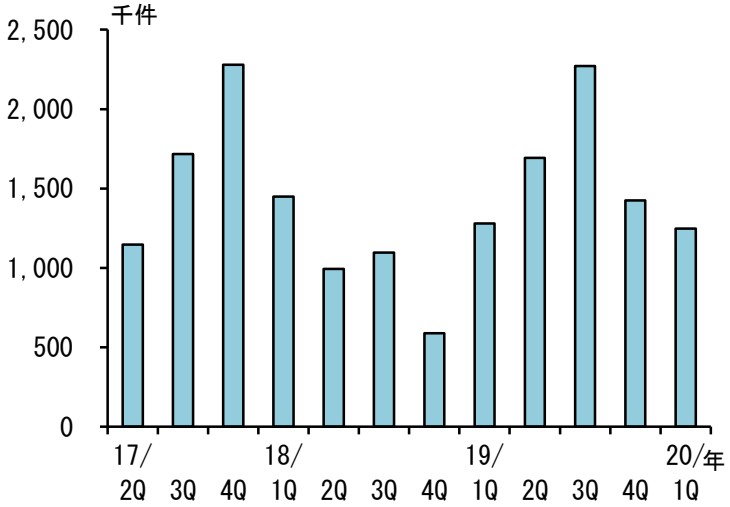
ランサムウェア攻撃の凶悪化

- 金融セクター以外で大きな感染被害が生じる事案が多発

  ―― 金融セクターでも、海外では情報漏えいのほか、銀行の全支店が閉鎖に追い込まれた事案の報道も

- 「ビッグゲームハンティング」（犯行グループが要求する身代金相場の高騰）

▽ 新たなランサムウェアの件数



（注）マカフィー社で検知した件数（全世界ベース）
（出所）マカフィー「McAfee Labs 脅威レポート」

背景にある二つの変化

- ランサムウェアおよび連携する他のマルウェアによる攻撃力の上昇
  - 「人手によるランサムウェア攻撃」（情報処理推進機構）
    - ✓ 侵入後、事前に重要な端末やサーバ等（例えば、業務継続に影響を及ぼすもの）を探し出したうえで効果的にランサムウェアに感染させる手口（バックアップデータが同時に狙われることも）
  - 「二重の脅迫」（同）
    - ✓ ランサムウェアにより暗号化したデータを復旧するための身代金要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開するなどと二重に脅迫する攻撃方法
  - 連携する他のマルウェアの潜伏能力・情報収集能力の向上
    - ✓ 例えば、Emotet（媒介マルウェア）によるTrickBot（データ収集・窃取マルウェア）の展開 → TrickBotによるRyuk（ランサムウェア）の展開
- メール以外の侵入経路を悪用する機会の増加（後述）

求められる対策（1）
「基本に忠実に」＋「備えが重要」

- OS・ソフトウェアのアップデート、修正プログラム適用
- 不審な添付ファイルの開封・リンクのクリックを行わない、またそのための役職員の啓発
- 定期的なバックアップデータ取得、オフラインでの保管
- データ復旧にかかる時間とコストの事前見積もり

  ―― 暗号化されていないバックアップデータが残っていたとしても、復元には相応の時間とリソースを要する可能性

- 利用するアプリケーションおよびアプリケーションのインストール・使用権限の絞り込み
- 不審メールの検知・監視機能の強化の検討
- 悪質なIPアドレスとのアクセス遮断

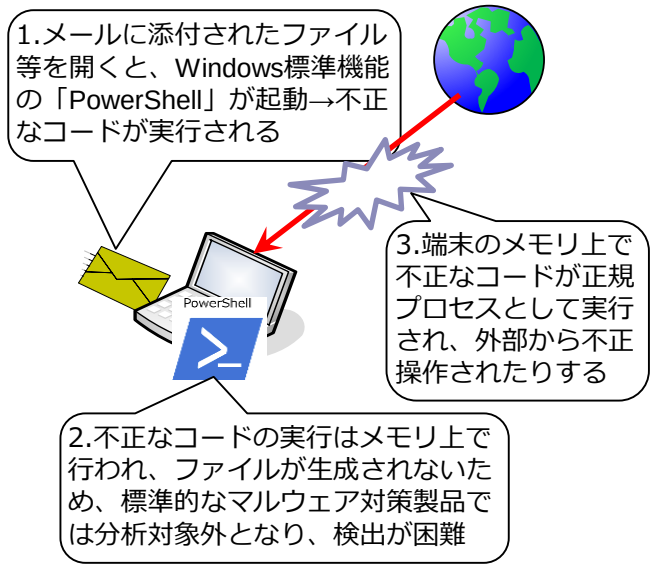
最近のサイバー脅威動向の変化（2）

ファイルレス攻撃の著増・一般化

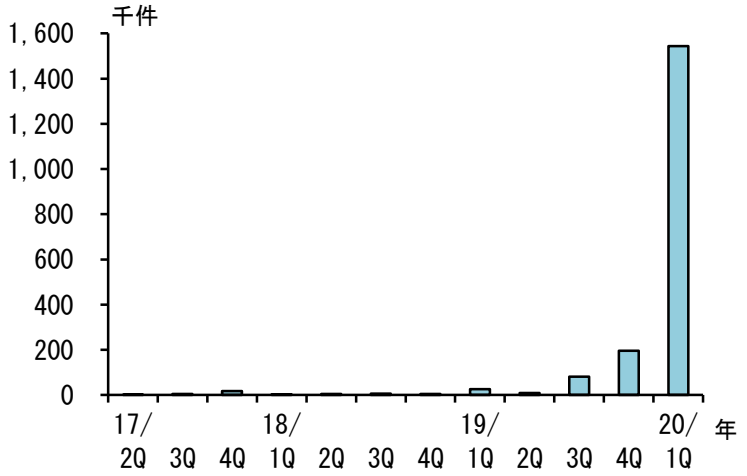
- マルウェアがディスク上の実行ファイルとしてではなく、システムのメモリ内部に存在 → 標準的なマルウェア対策製品では検知が困難
- OSに元々備わっている機能を利用（例えば、PowerShellは本来はシステム管理の目的で利用するWindowsの標準機能）

▽ ファイルレス攻撃の例（PowerShellマルウェア）

（イメージ）



（新たなPowerShellマルウェア）



（注）マカフィー社で検知した件数（全世界ベース）
（出所）マカフィー「McAfee Labs 脅威レポート」

求められる対策（2）

抜本的回避または侵入される前提での検知能力向上

- （可能であれば）悪用される可能性のあるツールの無効化
- 最重要な情報資産におけるネットワーク分離の検討
- 振舞い検知など高度な機能を有するセキュリティ対策ソフトの導入の検討
- ログの監視・分析機能の強化の検討

最近のサイバー脅威動向の変化（3）

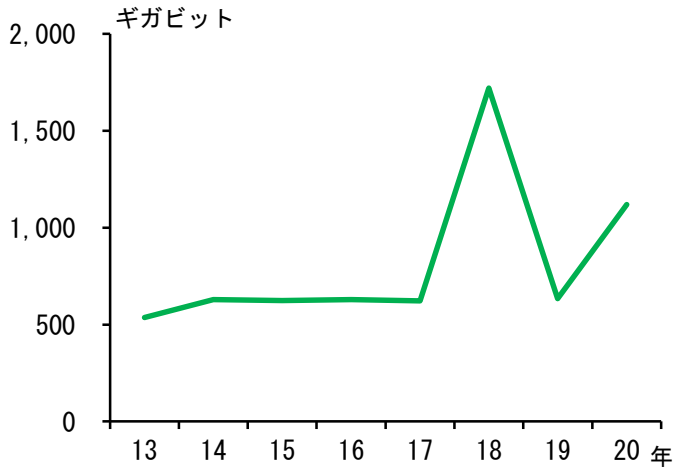
暗号資産の支払いを要求するDDoS攻撃の再来

- 2019年～2020年に、特定のサイバー犯罪グループを名乗る者などによる攻撃予告および攻撃が国内外の金融セクターで発生

  ―― 攻撃者は、攻撃を中止する条件として暗号資産の支払いを要求

- わが国の金融機関を狙った攻撃も確認されているが、大きな被害には至っていない（ただし、海外の一部金融セクターでは深刻なシステムの機能停止に見舞われた事例も存在）

▽ DDoS攻撃の攻撃規模の推移



（注）各年で観測された1秒当たりの不正通信量の最大値
（2020年は1～9月）
（出所）NETSCOUT社脅威レベル解析システム（ATLAS）

求められる対策（3）

完全な防御は困難との前提に立ったリスク軽減

- 不審な通信を迅速に遮断
- 導入済みの対策で防御しきれないことを前提とした（代替策への移行を含む）コンティンジェンシープランの整備と、訓練・演習による実効性の確認
- 業務継続上の重要性に応じた、コンテンツデリバリーサービスなど攻撃の影響を緩和するための高度な対策の導入の検討

最近のサイバー脅威動向の変化（4）

リモート接続にかかる脆弱性を狙った攻撃の増加

- 新型コロナウイルス感染症の感染拡大に起因したテレワークの拡がりが影響

  —— VPN（仮想プライベートネットワーク）装置への負荷が過大となり、利用を停止していた旧型のVPN装置を再利用したところ、旧型装置に潜んでいた脆弱性を狙う攻撃を受けた事例も存在

- 攻撃者にとって、次の経路をメールに代わる侵入口として活用する機会が増加
  - RDP（リモートデスクトッププロトコル）
  - VPN装置

- わが国の金融セクターでは大きな被害がみられていないが、国内の他セクターや海外の金融セクターの一部において、リモート接続にかかる脆弱性の悪用により、認証情報の流出やランサムウェア攻撃につながった可能性が指摘されている

リモート接続にかかる脆弱性の具体例

- Windowsのリモートデスクトップサービスの脆弱性（CVE-2019-0708）

  —— 遠隔の第三者によるRDP経由のサーバ乗っ取りが可能となる可能性

- 米Pulse Secure社のVPN製品の脆弱性（CVE-2019-11510）

  —— 遠隔の第三者がVPN装置上の任意のファイルを読み出し可能となる可能性

- 米Citrix Systems社のVPN製品の脆弱性（CVE-2019-19781）

  —— 遠隔の第三者が内部の任意のファイルにアクセス可能となる可能性

求められる対策（4）

脆弱性情報の収集と迅速な検討・対応

- 修正プログラムの迅速な適用（適用できない場合には代替のリスク軽減策の実施）
- 使用していないサービスの無効化または通信ポートの遮断
- 不正通信の検知・監視機能の強化の検討
- リモート接続に関する権限を必要最小限に抑制
- 重要な外部委託先（含む再委託先）がテレワークを実施している場合には、同様の対策が講じられていることの確認

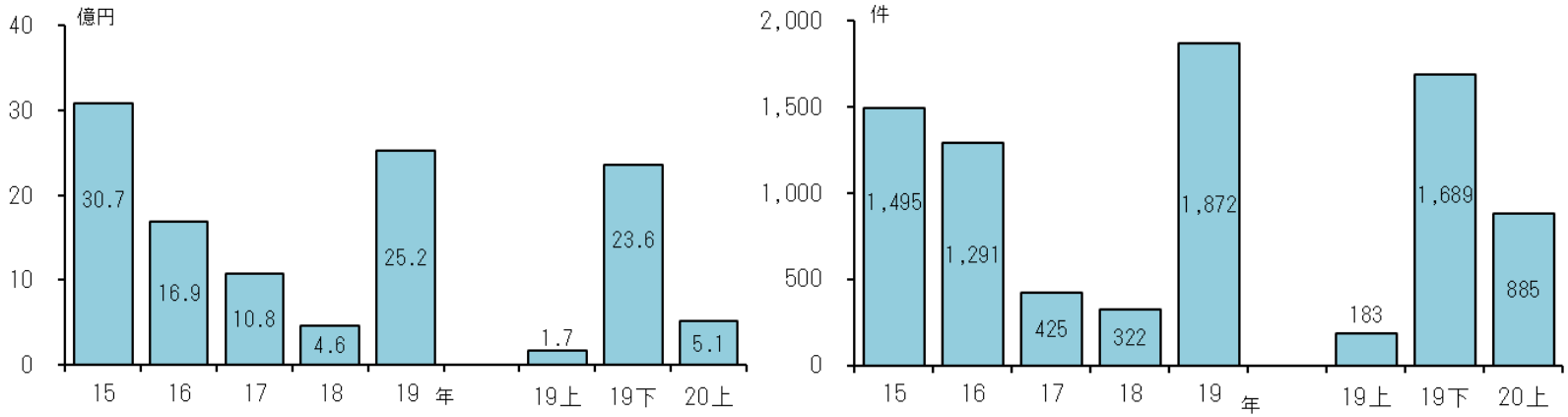
（参考）金融庁・日本銀行による通知「新型コロナウイルス感染症対応としての在宅勤務（テレワーク）拡大に伴うサイバーセキュリティ上の留意点について」（2020年4月21日付）

最近のサイバー脅威動向の変化（5）

顧客の預金等を狙った攻撃の再活発化

- わが国のインターネットバンキングにかかる預金等の不正引き出し金額・件数は、二要素認証を突破するフィッシング詐欺の流行により、2019年後半から著増。2020年入り後は、金額ベースでは減少しているが、発生件数は依然多い

▽ インターネットバンキングにかかる預金等の不正な引き出し金額・件数の推移

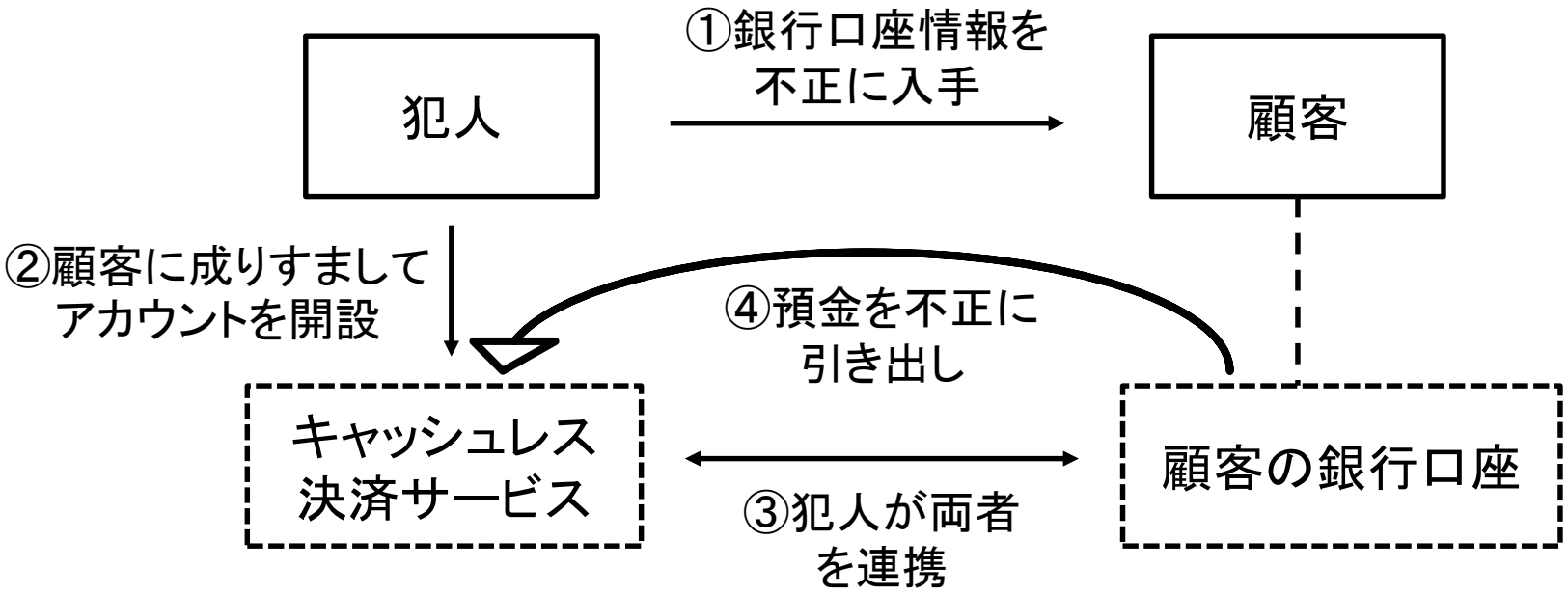


（出所）警察庁

- 最近、キャッシュレス決済サービスを悪用した預金等の引き出し、オンライン証券口座からの資金引き出し等の被害が目立っている

例１：キャッシュレス決済サービスを悪用

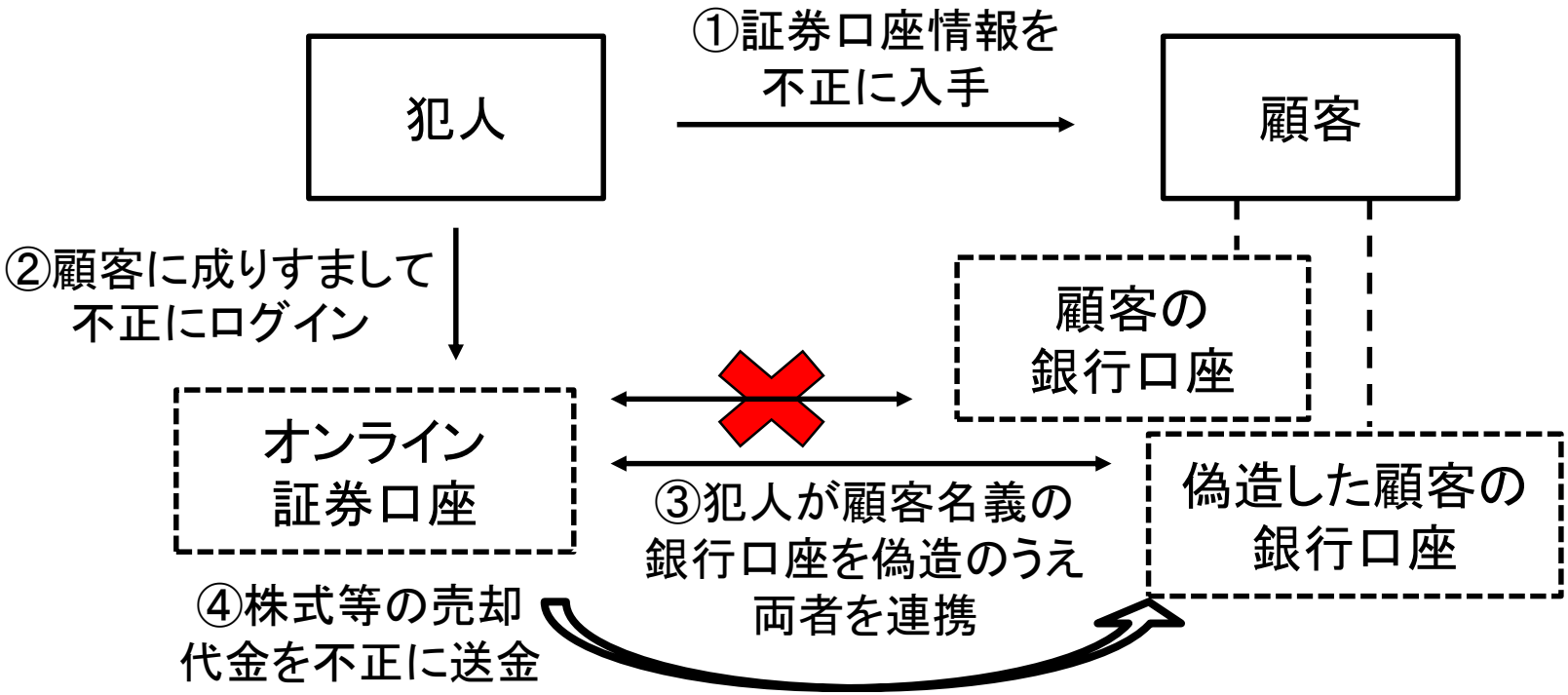
（イメージ図）



―― 銀行側では、サービスの連携（上図の③）時の本人確認が十分ではなかった（知識＜記憶＞の一要素のみによる認証）ところに課題

例2：オンライン証券口座から資金を不正に引き出し

（イメージ図）



―― 金融商品取引業者側ではサービスへのログイン時の認証等の仕組みが、銀行側では口座開設時の本人確認が、それぞれ十分でなかったところに課題

求められる対策（５）

顧客のオンライン取引にかかる本人確認・認証条件の強化

- キャッシュレス決済サービス等とのサービス連携方法に関するセキュリティ上の問題の有無の確認および必要に応じた対策（認証条件等）強化の検討
- 銀行口座開設時における本人確認の強化の検討
- 攻撃を受けることを前提としたダメージコントロール（利用限度額の抑制等）の検討
- フィッシング等のサイバー攻撃の可能性を高めうるオンライン取引にかかるウェブ画面への入力項目（4桁暗証番号等）に関する（中長期的な）見直しの検討

ミニマムスタンダード vs. ベストプラクティス

- 監督当局からの要求水準が切り上がった場合、金融機関は対応が求められる（ミニマムスタンダードの考え方）
- 他方、ベストプラクティスは、各主体が考える問題

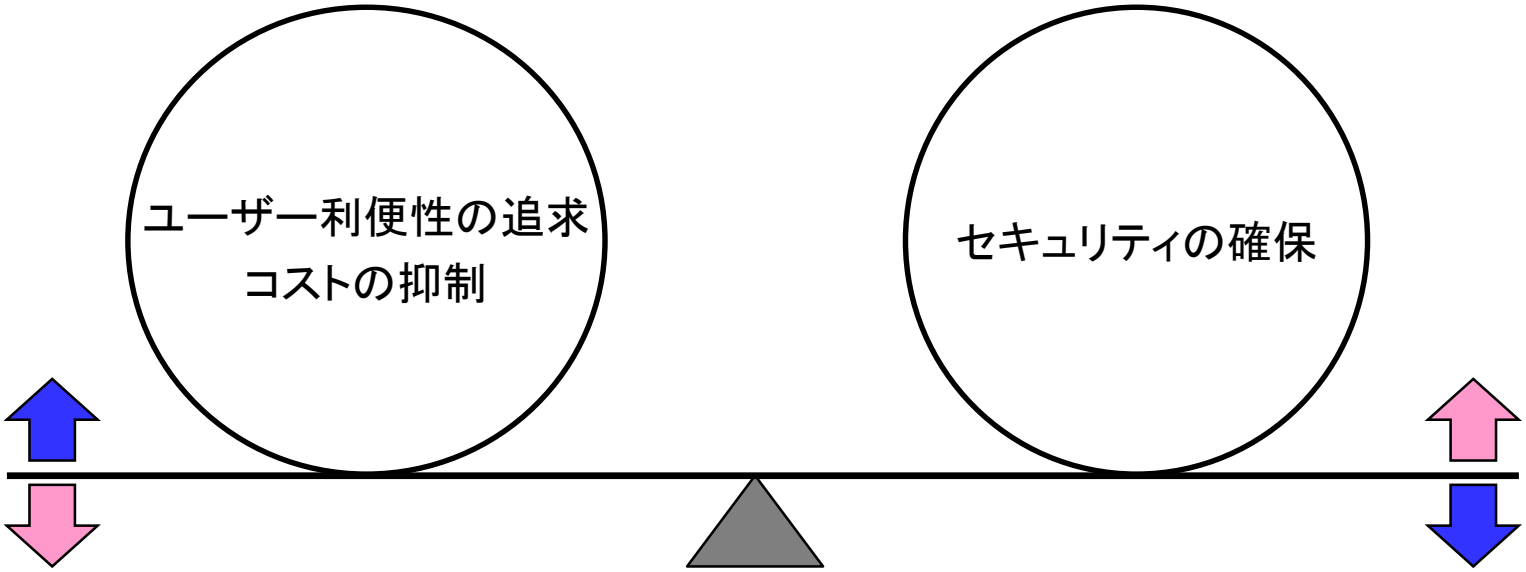
（例）

- 二要素認証でも突破されるリスクがあるとすればどうすべきか
  - リスクを受容する
  - リスクを軽減し、残余部分を受容する
  - リスクを受容せず、さらに高度な防御策を講じる
- リスクの変化をどのようにモニタリングするか
- リスクがどこまで変化したらどのように対応するか

（参考）NIST SP800-63-3（Digital Identity Guidelines）

- 米国政府機関向けのガイドラインであるが、わが国の金融機関にとっても有用な考え方を提供
- 同ガイドライン中の「認証およびライフサイクル管理」によれば、Authenticatorは次の9種類に分類可能
  - 記憶シークレット（パスワード等）
  - ルックアップシークレット（乱数表等）
  - アウトオブバンドデバイス（SMS認証等）
  - 単一要素OTPデバイス（ハードウェアOTPトークン等）
  - 多要素OTPデバイス（Touch IDにより有効化するOTPアプリ等）
  - 単一要素暗号ソフトウェア（クライアント証明書等）
  - 単一要素暗号デバイス（USBドングル等）
  - 多要素暗号ソフトウェア（指紋認証により有効化するクライアント証明書等）
  - 多要素暗号デバイス（指紋認証により有効化するUSBドングル等）
- 認証の信頼レベルを、①上記の9種類のうち一つ利用、②単独で多要素を満たすもの一つまたは単一要素のもの二つの組み合わせ、③②の要求に加え、「暗号鍵の所持」、「ハードウェアベース」の要求を満たす組み合わせ、の3段階に分類（③の信頼レベルが最も高い）

デジタライゼーションを進める際のセキュリティ確保の視点



- 上図の左右の均衡を図る考え方（トレードオフ論）が一つの視点
  - ―― 「ユーザー利便性の追求やコストの抑制という目的に照らして適切な支出か」（経営リスク領域）、「リスクや起こりうる被害が組織としての許容範囲内にとどまっているか」（システムリスク領域）という異なる要求を満たす最適解を見極める必要
- リスクの態様が変化した時（例えば、Web口座振替の収納企業の中にSMS認証やメール認証を使って本人確認を行う資金移動業者が加わった時）には、相応のセキュリティ強化を検討する必要

サイバーセキュリティと組織の意思決定

- *金融セクターのサイバーセキュリティの効果的な評価に関するG7の基礎的要素*（2017年）

  パートA・アウトカム2：組織的な意思決定にサイバーセキュリティの視点が組込まれている

  「・・・サイバーセキュリティを各主体の通常の意思決定過程に組み入れること（特に、早くからサイバーリスク管理を意思決定過程に含めること）は、各主体の組織全体にわたる戦略的なアウトカムに好影響を与える。・・・新たな製品・サービスを開発する際や、既存の技術・インフラを活用する業務運営の有効性を評価する際には、サイバーセキュリティは戦略的な考慮を要する重要事項であると認識すべきである。・・・」

- *サイバーセキュリティの確保に向けた金融機関の取り組みと課題*（日本銀行金融システムレポート別冊、2020年）

  Ⅱ．1．（2）組織体制

  「・・・金融機関がデジタル技術を活用した新しい顧客サービスや業務改革等を進めるなかにあっては、サイバーセキュリティの十分性や適切性にかかる検証が、同時並行的に行われていくことが望ましい。・・・」

セキュリティ確保が経営上の優位性になるとの視点も重要

- キャッシュレス決済等とのサービス連携時の認証問題への取り組み強化は、（相応のセキュリティ対策のもとで構築した）既存のインターネットバンキングの仕組みへの接近を意味し、必ずしも利便性の低下をもたらすとは言えない
- 認証に関する追加的なセキュリティ対策が、オンライン取引全体に対する信頼感の高まりに寄与し、中長期的にユーザー利便性やコスト面の改善につながる可能性もある

ご清聴ありがとうございました

本資料の中で示された内容や意見は、日本銀行の公式見解を示すものではありません。

本資料に関する照会先

日本銀行　金融機構局　考査企画課　システム・業務継続グループ　伊藤
phone: 03-3664-4333
email: csrbcm@boj.or.jp