令和５年11月７日
JPAAWG6th General Meeting

サイバー空間をめぐる情勢と警察の取組
～フィッシング対策を中心に～

警察庁サイバー警察局
サイバー企画課

青木　稔

本日の議題

1　サイバー空間をめぐる情勢

2　フィッシングの現状

3　警察庁におけるフィッシング対策

本日の議題

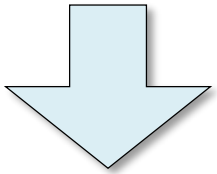
1　サイバー空間をめぐる情勢

2　フィッシングの現状と対策

3　警察庁におけるフィッシング対策

サイバー空間をめぐる情勢

- デジタル化社会の到来に伴い、サイバー空間の公共空間化が加速
- フィッシング被害等に伴うクレジットカード不正利用被害やインターネットバンキングに係る不正送金被害の急増
- ランサムウェア被害も高水準で推移
- 国家を背景に持つサイバー攻撃の発生　など



サイバー空間における脅威については
極めて深刻な情勢が継続

本日の議題

1　サイバー空間をめぐる情勢

2　フィッシングの現状

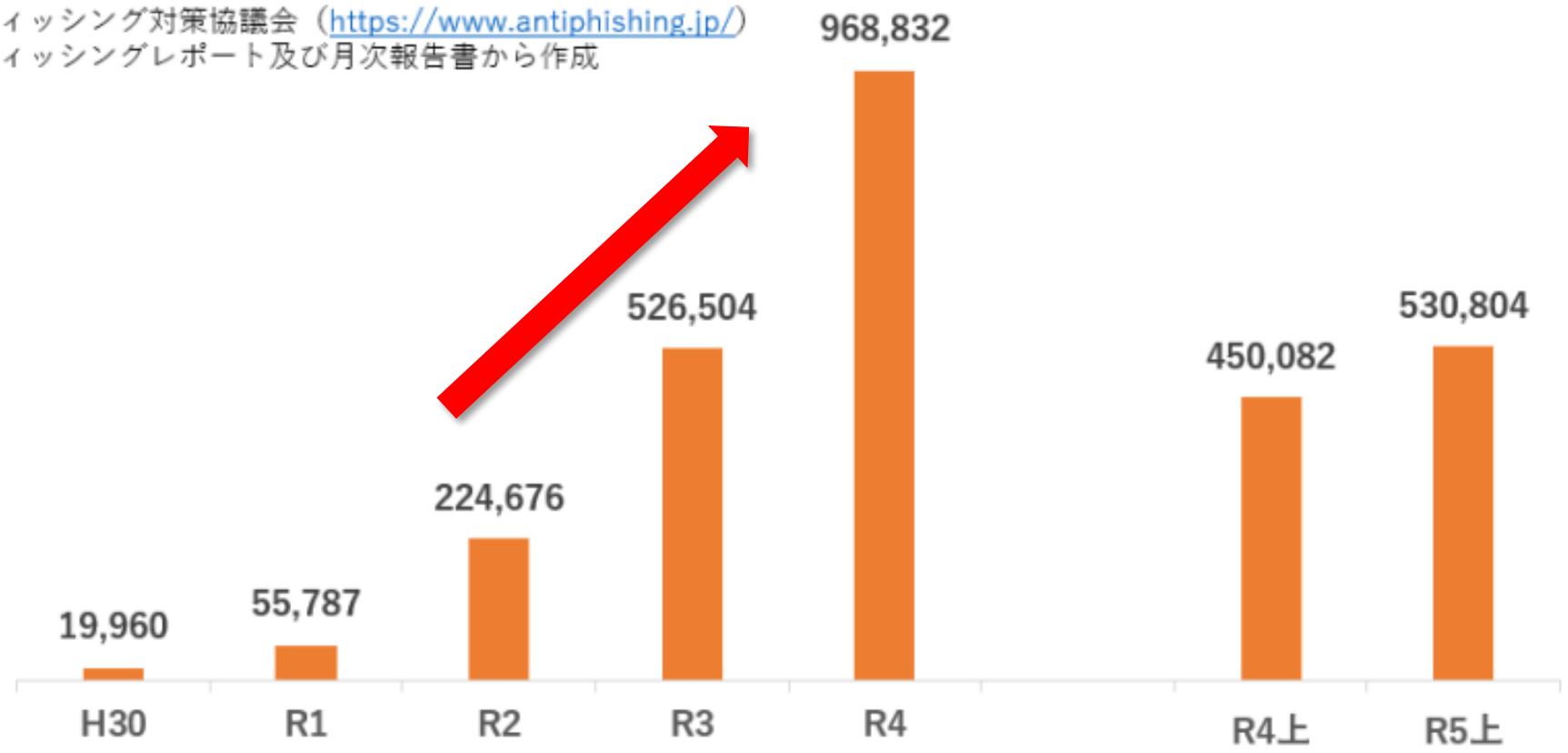
3　警察庁におけるフィッシング対策

フィッシングの増加

- フィッシング報告件数は右肩上がりで増加
- フィッシングで騙られた企業は、クレジットカード事業者、EC事業者を装ったものが多い

フィッシング報告件数（件）

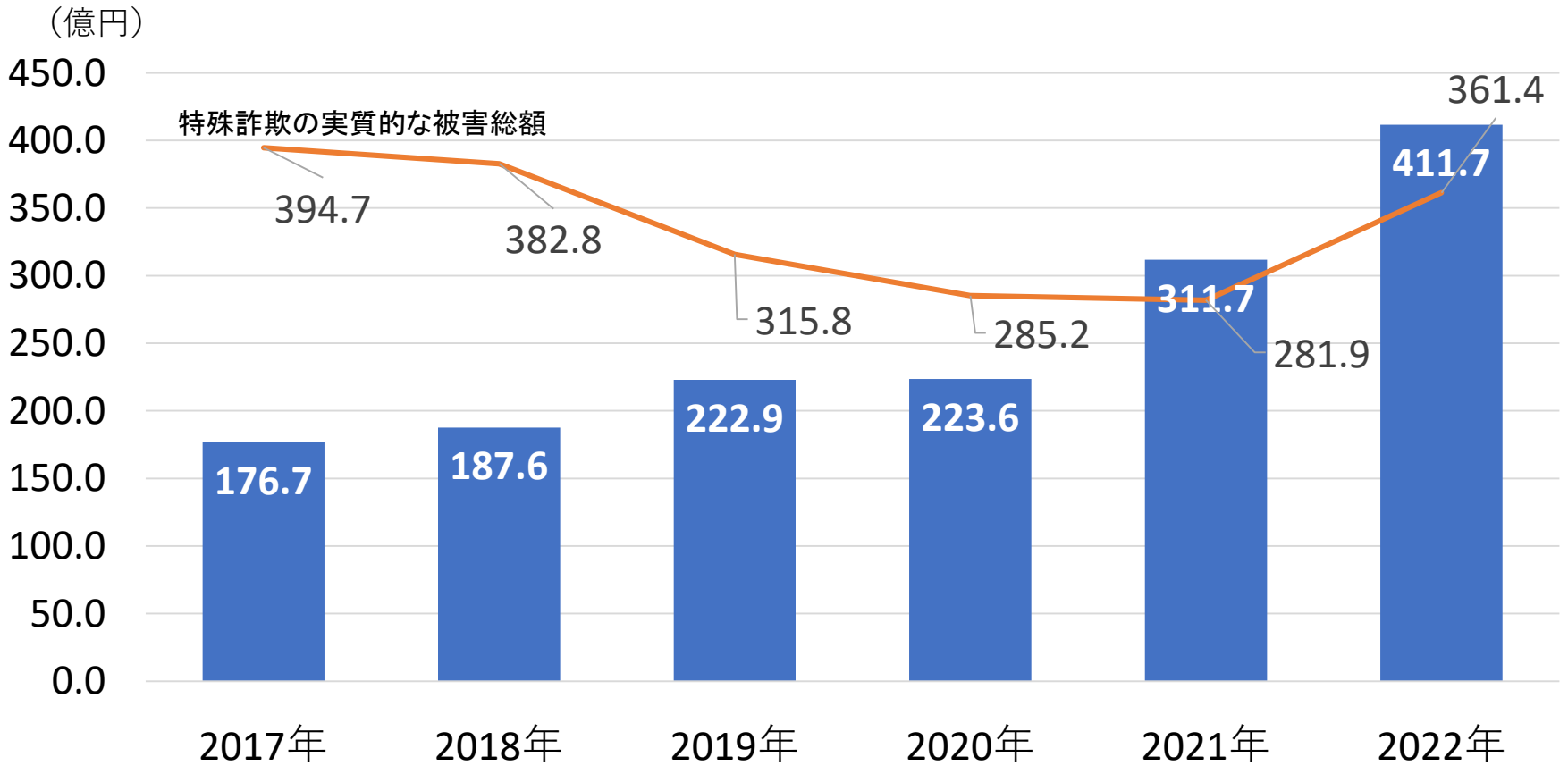
フィッシング対策協議会（https://www.antiphishing.jp/）
フィッシングレポート及び月次報告書から作成



クレジットカード不正利用の情勢

クレジットカード情報を窃取するフィッシングサイトの増加等により、クレジットカード不正利用が増加

クレジットカード不正利用（番号盗用）被害額（億円）

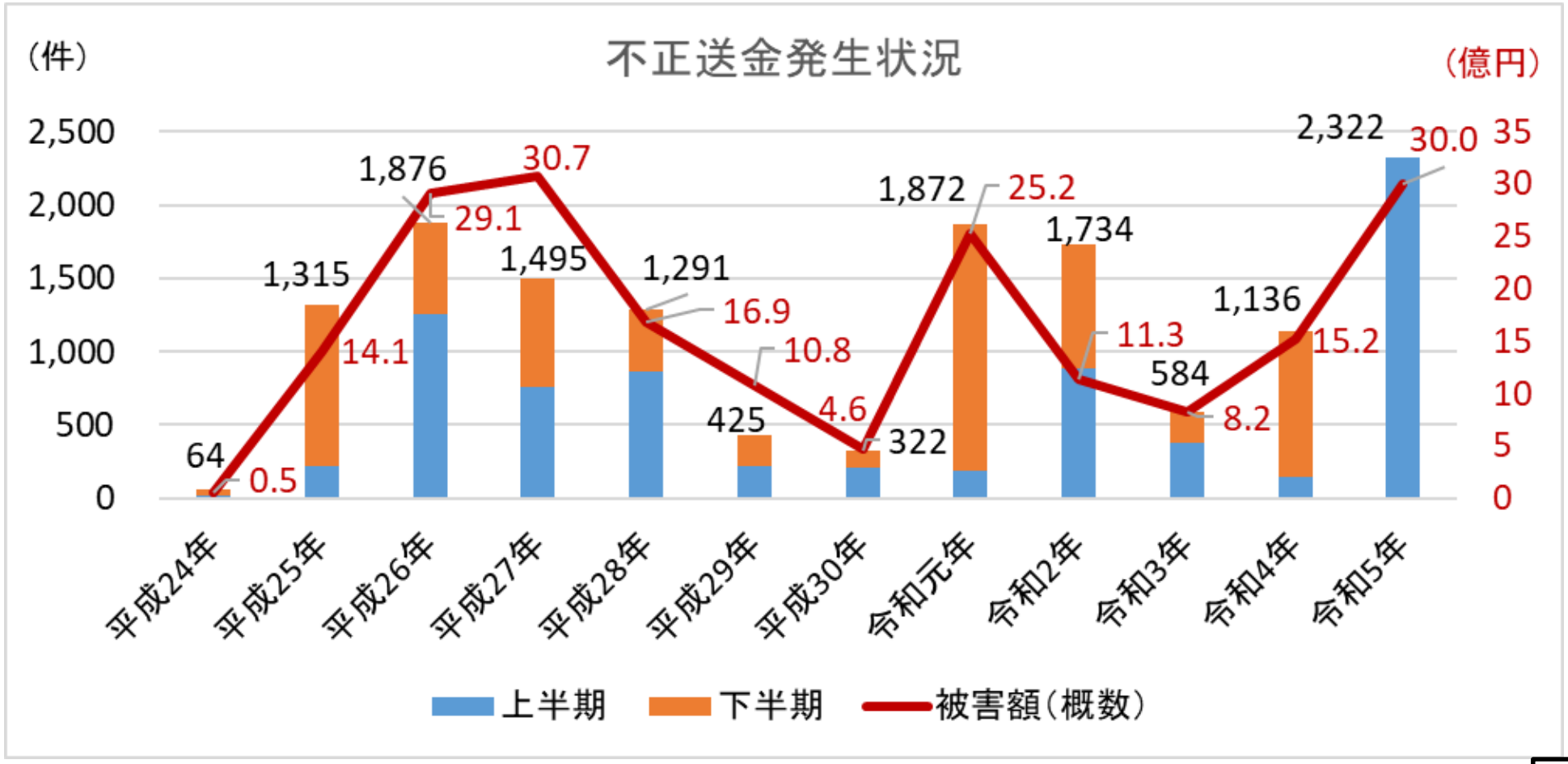


「一般社団法人日本クレジット協会　クレジットカード不正利用被害額の発生状況」
「警察庁　特殊詐欺の認知・検挙状況等について」より作成

インターネットバンキング被害再増加

令和5年上半期の被害は、年間の件数と比較しても

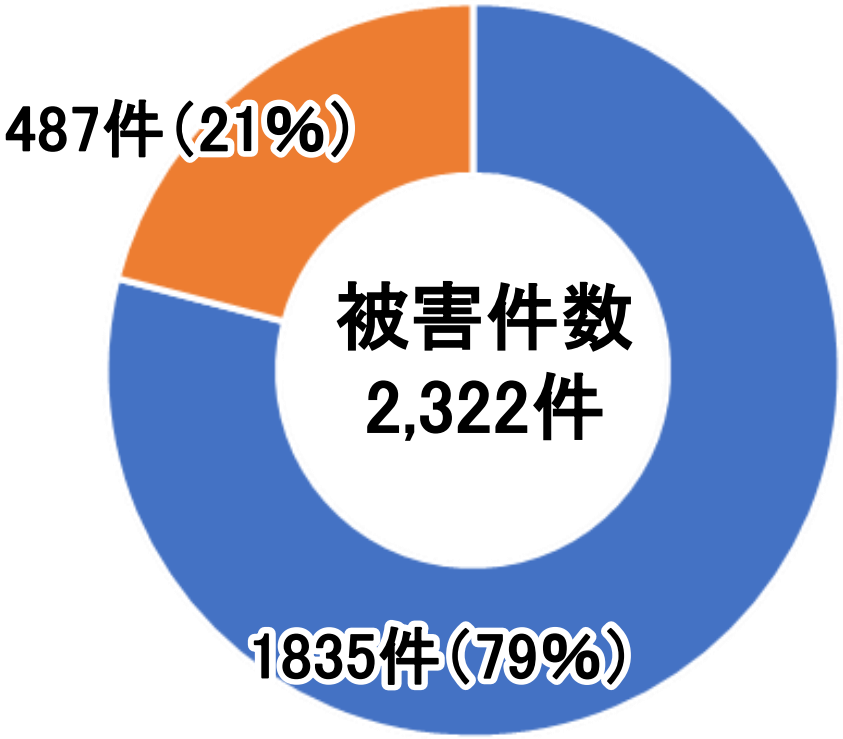
- ○ 被害件数は過去最多　　：2,322件
- ○ 被害額も過去最多に迫る　：約30.0億円

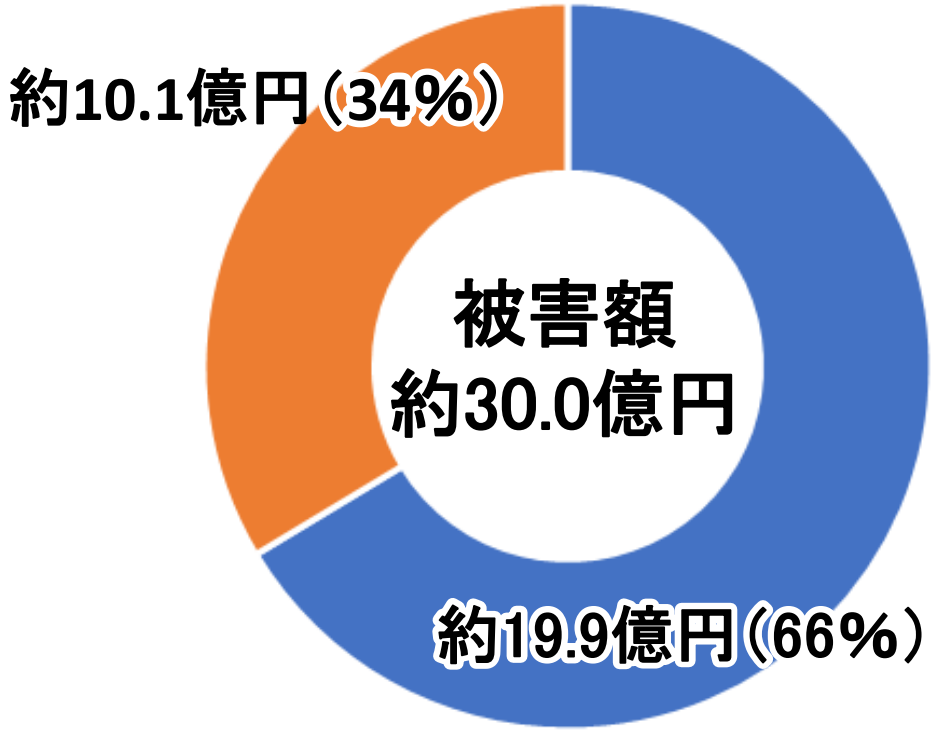


※数字は令和5年8月4日時点の暫定値

被害金融機関の内訳

被害金融機関の多くは、ネット専業銀行、信託銀行が占める





■ ネット専業・信託銀行　■ その他金融機関

※数字は令和5年8月4日時点の暫定値

不正送金被害に係るフィッシングメールの主な内容(１)

■利用制限

- ○ お振り込み手続きの**一時制限**について。
- ○ 重要　緊急　**入金制限**のお知らせ。
- ○ **お取引を規制**させて頂きました。規制解除するには下記へアクセスし手続してください。
- ○ インターネットバンキングにおける**入出金を規制**します。解除はこちら。
- ○ お客様の口座のご利用を**一時停止**しております。本人確認手続きをお願いします。

■取引内容確認

- ○ **お取引目的等のご確認**のお願い。
- ○ 犯罪収益移転防止法に基づき、**お取引を行う目的等を確認**する必要があります。
- ○ 長く利用していないので**ログインをして更新**してください。
- ○ 必ずご回答ください/**お客様情報等の確認**について。
- ○ アップグレードを実施しており、**個人情報を再確認する必要**があります。
- ○ セキュリティシステムの大幅なアップデートによる**個人情報の再確認**してください。

不正送金被害に係るフィッシングメールの主な内容(２)

■不正アクセス通知

- ○ 【緊急】××銀行が**不正利用を検知**しました。
- ○ 別の国からあなたのアカウントへの**ログインの試みが検出**された。
- ○ インターネットバンキングに**不正なアクセス**がありました。口座の確認をしてください。
- ○ 【重要】普段と異なる環境からの**ログインを検知**しました。
- ○ 【××銀行】アカウント**異常活動の通知！**

■期限を迫る

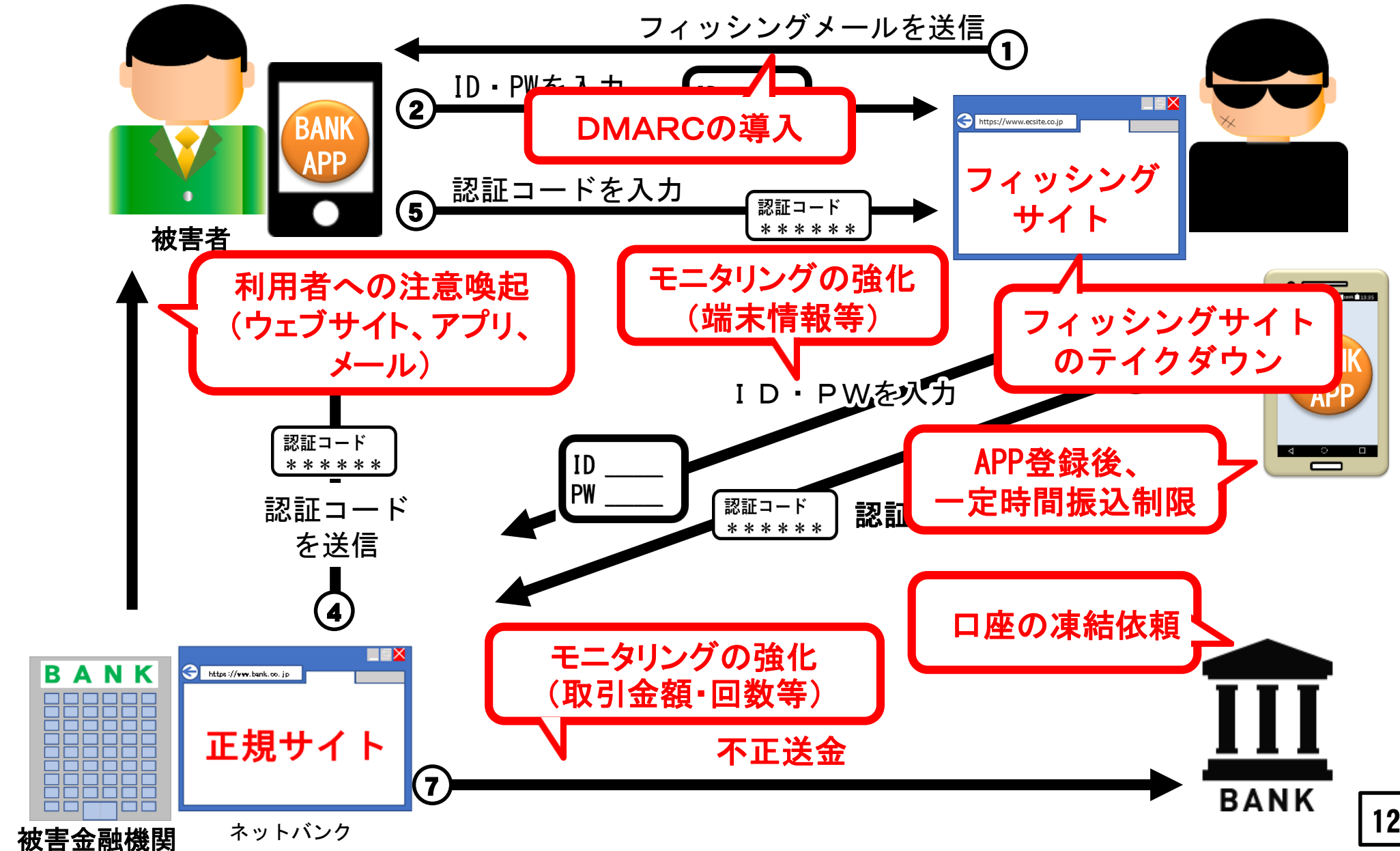
- ○ 取引制限について **××までにご回答いただけない場合**、お客様のご回答に著しい不足がある場合、もしくはご回答から当社規約第8条（禁止事項）に抵触すると判断した場合、やむを得ず、**お客様の口座を解約**させていただくことがございますので、あらかじめご了承ください。
- ○ お客様の取引を規制させていただきました、解除するには下記リンク先にアクセスし手続きしてください。**××までにご回答がない場合**はお客様の口座が解約されるかもしれません。

不安を煽り、本人確認を求め、認証情報・個人情報を窃取する内容

フィッシングの手口と対策について（概要）

	フィッシングサイト立ち上げ	フィッシングメール等送信	情報窃取	不正送金等実行
攻撃者の行動	○ 新規ドメインを取得 ○ 標的とする金融機関のサイトに模したフィッシングサイトを構築	○ ダークウェブ等からメールアドレスや電話番号を入手 ○ 入手したメールアドレス等にフィッシングメール、SMSを送付		○ 窃取した情報を用いて、正規のサイトへアクセスし、不正な送金を実行 ○ 詳細な利用者情報や身分証を用いてカードローン等から借り入れ
利用者の行動		○ フィッシングメールやSMSを受信 ○ メール等に記載のリンクをクリック（フィッシングサイトへのアクセス）	○ 口座番号やID・PW等を入力 ○ 住所、生年月日、職業、年収等個人情報を入力 ○ 運転免許証やマイナンバーカード等の写真をアップロード	
事業者の対策	○ 継続的なフィッシングサイトの調査とテイクダウン	○ 利用者への被害状況等を踏まえた注意喚起 ○ DMARC等の送信ドメイン認証導入	○ 利用者への被害状況等を踏まえた注意喚起 ○ 継続的なフィッシングサイトの調査とテイクダウン	○ 過去の取引履歴や利用している端末情報、不審な宛先への送金等不審な取引の監視（モニタリング） ○ 二要素認証やリスクベース認証の導入等、認証強化 ○ 取引完了後に利用者へ取引内容を通知

事業者における対策　～手口を踏まえた対策



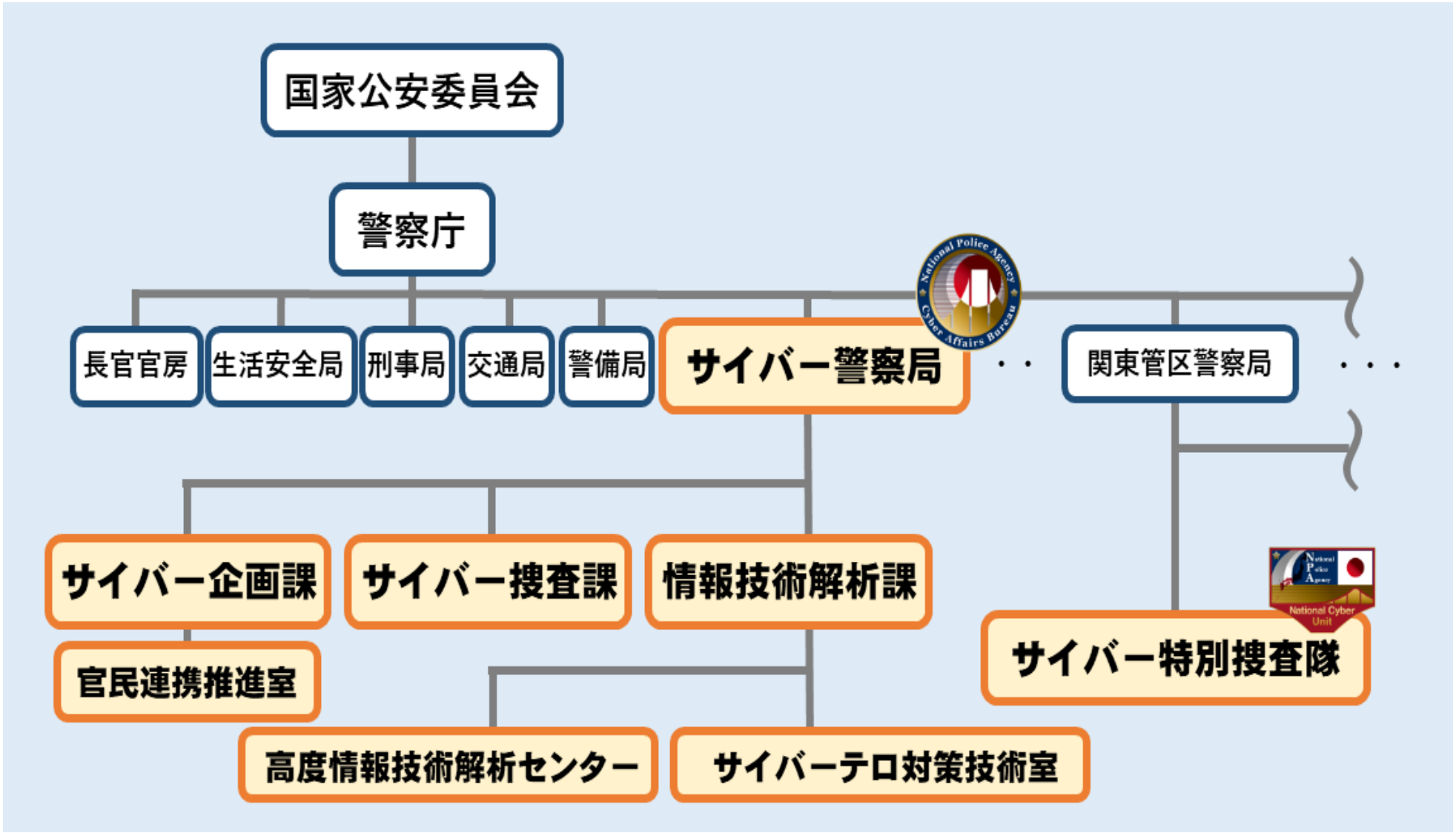
本日の議題

1　サイバー空間の情勢

2　フィッシングの現状と対策

3　警察庁におけるフィッシング対策

サイバー警察局・サイバー特別捜査隊の設置



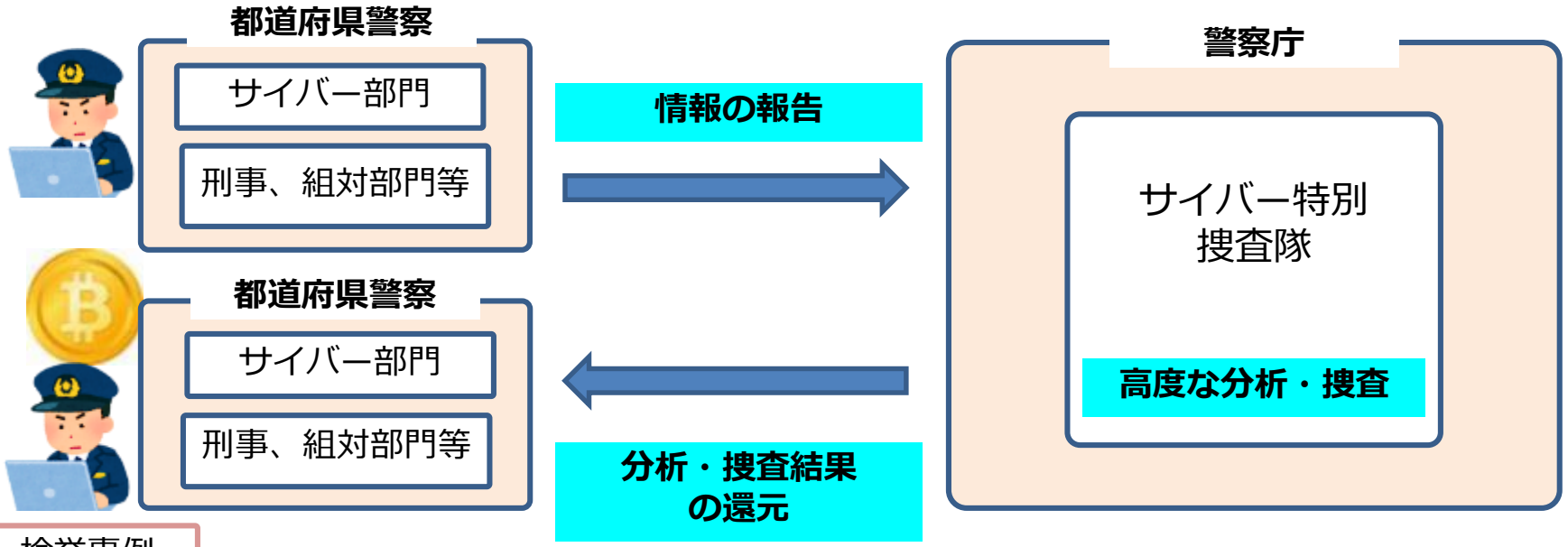
サイバー事案の取締り（暗号資産に係る捜査）

◆　犯罪に使用された暗号資産に係る情報の高度な分析・捜査

○　組織犯罪対策部門等と連携して、犯罪に使用された暗号資産に係る情報をサイバー特別捜査隊において分析することで捜査の進展に寄与

○　ユーロポールが主催する暗号資産捜査の実践型研修プログラム等にサイバー特別捜査隊隊員が参加することで、海外の先進的な捜査に関する知見・技能を習得

都道府県警察とサイバー特別捜査隊の連携状況



検挙事例

組織犯罪対策部門等と連携し、犯罪に使用された暗号資産に係る情報について高度な分析・捜査を実施した結果、2023年５月、サイバー保険を名目とした架空料金請求詐欺事件について、サイバー特別捜査隊において暗号資産追跡の支援を行い、愛知県警察などの合同捜査本部が被疑者２名を逮捕した。

フィッシングに起因する犯罪の検挙（国外被疑者の検挙）

国際共同捜査

外国　日本

インドネシア当局

相互協力

サイバー警察局

国の捜査機関

サイバー
特別捜査隊

National Cyber Unit

捜査

大阪府警察

逮捕（R5.7）

フィッシングツール
「16SHOP」

（偽サイト）

捜査・逮捕

クレジットカード
情報等を窃取

CARD

被害者

商品を不正購入

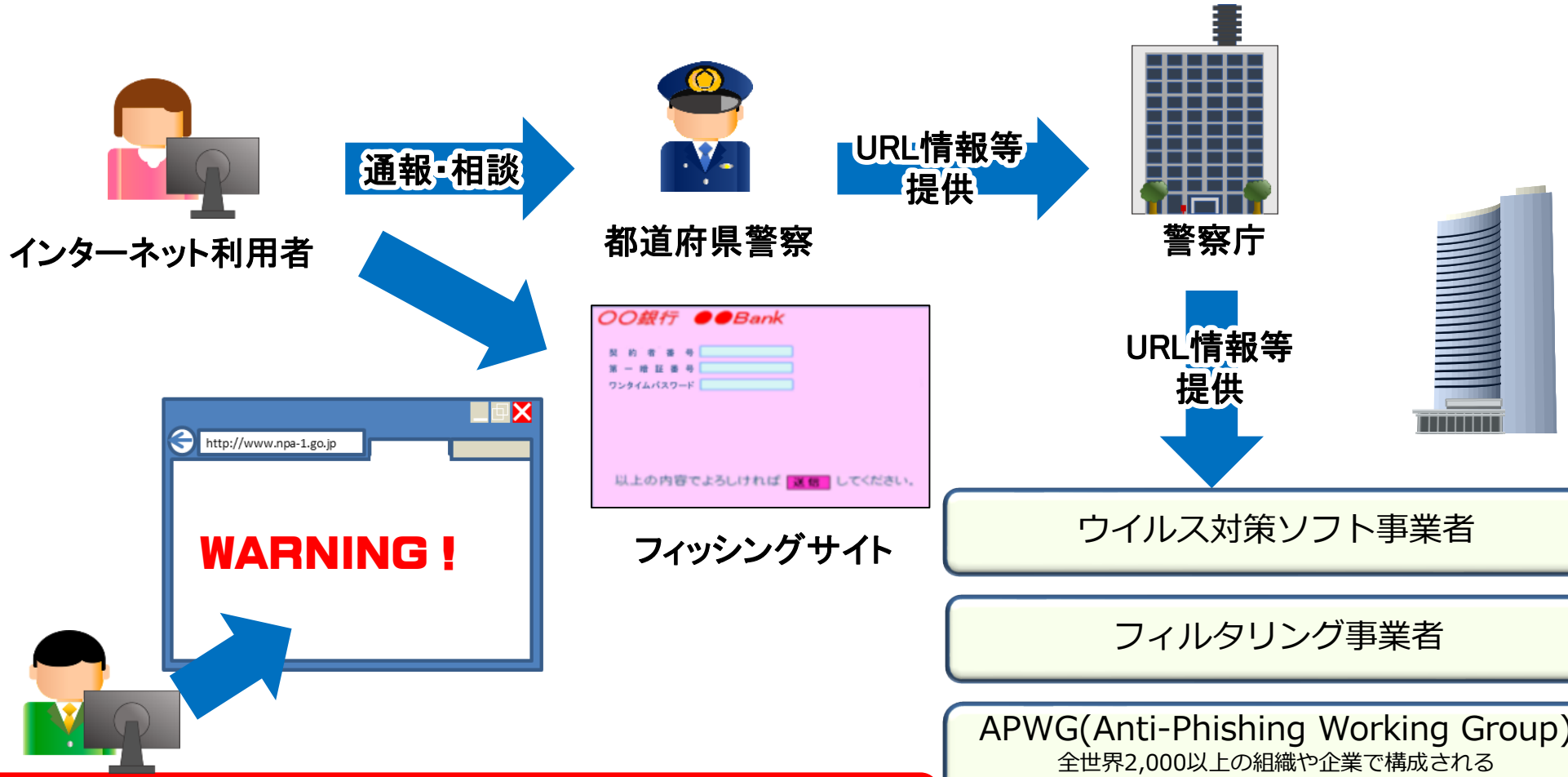
共謀

被疑者

被疑者

警察におけるフィッシング対策①　警告表示

警察庁からウイルス対策事業者等にフィッシングサイトのURL情報等を提供し、警告表示等に活用

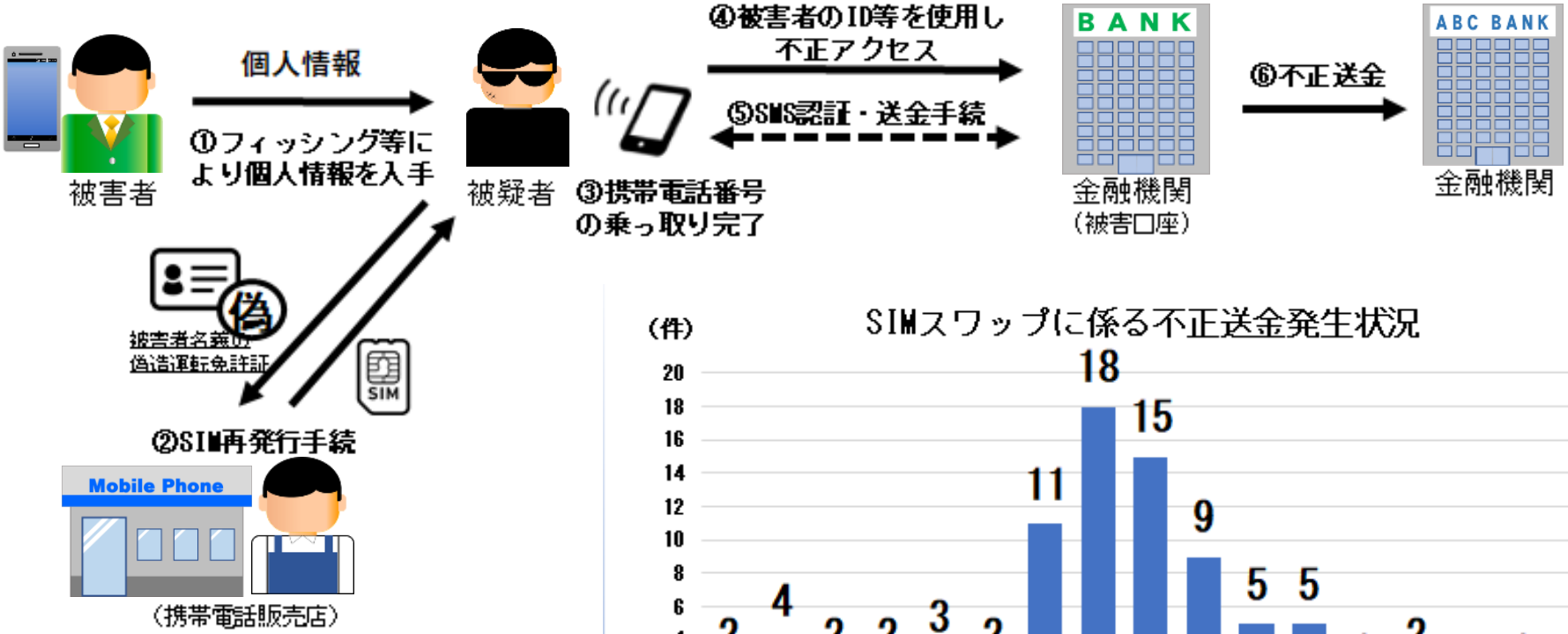


○　ウイルス対策ソフト、ブラウザ機能等で警告表示
○　フィルタリングアプリ、通信機器等でフィルタ

警察におけるフィッシング対策②　ＳＩＭスワップ対策

SIMスワップ（※）によるインターネットバンキングの不正送金被害が増加したことを踏まえ、総務省と連携し、携帯電話事業者において本人確認手法を強化等し、SIMスワップを防止（令和４年９月～）

（※）実在する人物になりすまして店舗に来店し、本人確認資料として偽造した運転免許証等を使い、SIMカードの再発行等を行うことで、携帯電話番号を乗っ取る手口



インターネットバンキング被害再増加に関する注意喚起

令和５年８月８日
警　　察　　庁
金　　融　　庁

フィッシングによるものとみられるインターネットバンキングに係る
不正送金被害の急増について（注意喚起）

令和５年４月にインターネットバンキングに係る不正送金事犯による被害急増に関する注意喚起を実施するとともに、被害金融機関と連携し対策を講じているものの、その後も被害は拡大し続け、８月４日時点において、令和５年上半期における被害件数は、過去最多の2,322件、被害額も約30.0億円となっています。
（平成24年から令和４年の数値は確定値、令和５年上半期の数値は、同年８月４日時点における暫定値である。）

被害の多くはフィッシングによるものとみられます。具体的には、金融機関（銀行）を装ったフィッシングサイト（偽サイト）へ誘導する電子メールが多数確認されています。このような電子メールやSMSに記載されたリンクからアクセスした偽サイトにID及びワンタイムパスワード・乱数表等のパスワードを入力しないよう御注意ください。

また、一般社団法人全国銀行協会及び一般財団法人日本サイバー犯罪対策センター（ＪＣ３）の各ウェブサイトにおいても注意喚起を実施していますので御参照ください。

【掲載場所】
・一般社団法人全国銀行協会ウェブサイト
https://www.zenginkyo.or.jp/topic/
・一般財団法人日本サイバー犯罪対策センターウェブサイト
https://www.jc3.or.jp/threats/topics/article-507.html

不正送金被害急増中!!

電子メール等のリンクから
アクセスしたサイトに
IDパスワード・個人情報
を入力しないで下さい

不安にさせるメールに注意！！

個人情報の再確認・・・
不正アクセス通知・・・
口座を解約・・・

金融機関の「公式HP」「公式アプリ」
から正しい情報を確認してください

金融庁 Financial Services Agency
警察庁 National Police Agency
JBA 一般社団法人 全国銀行協会
JC3 日本サイバー犯罪対策センター

注意喚起等

サイバー警察局便り　(不定期・月２回程度)

サイバー警察局便り
Cyber Police Agency Letter　R5 Vol.11

ＤＭＡＲＣでフィッシングメール対策！

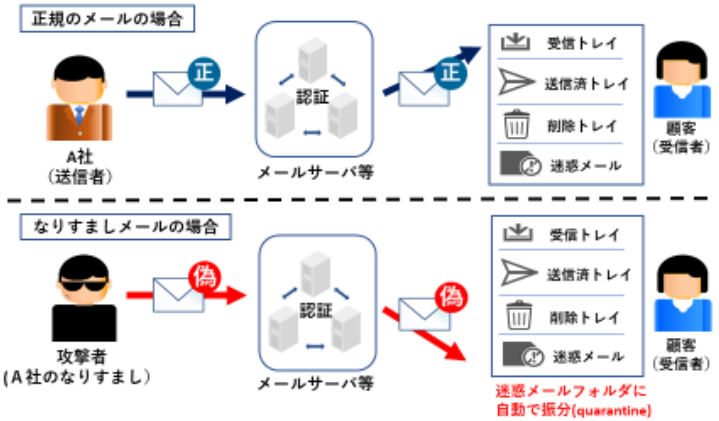
ＤＭＡＲＣを設定すると何ができるの？

ＤＭＡＲＣ※を設定すると、フィッシングメール（なりすましメール）を
・ 受信者に届けない（reject）
・ 迷惑メールとして取り扱う（quarantine）
ことができます。

※ Domain-based Message Authentication, Reporting, and Conformanceの略

ＤＭＡＲＣの動作概要

DMARCの動作概要（quarantineに設定した場合）は次のとおりです。



（参考）「送信ドメイン認証技術導入マニュアル」が迷惑メール対策推進協議会から公表されています。
https://www.dekyo.or.jp/soudan/aspc/report.html

総務省　日本データ通信協会　警察庁 National Police Agency

サイバー警察局便り
Cyber Police Agency Letter　R5 Vol.12

フィッシングの被害拡大中！！

そのメールは本物ですか？

フィッシングメール（なりすましメール※）のリンクをクリックして、
※なりすましのSMSも含みます。
「銀行預金を不正に送金された」
「クレジットカードを不正に利用された」
という被害が後を絶ちません。

フィッシングメールの特徴

☑ **正規のメールと見分けることが困難。**
☑ **【重要】、【不正アクセスを検知】、【取引を制限】**等のタイトルで**不安にさせ、リンクをクリックさせようとする。**
☑ 宅配業者、金融機関、通信事業者、ネットショップ、官公庁等の**実在の企業等を装う。**

フィッシング被害に遭わないためには？

- **メールやＳＭＳに記載されたリンクをクリックしない。**
- **内容を確認するときは、公式サイトやアプリを利用する。**
- **携帯電話会社等の迷惑メッセージブロック機能を活用する。**

《 フィッシングメール対策動画 》

制作：めじろんおおいた見守り隊

制作：サイバー防犯ボランティア島根大学

総務省　金融庁 Financial Services Agency　経済産業省 Ministry of Economy, Trade and Industry　警察庁 National Police Agency

サイバー事案の被害情報の把握・共有

- ○ **サイバー事案に係る捜査**
- ○ **捜査機関としての実態解明**
- ○ **被害実態の調査**
- ○ **防犯対策への活用**

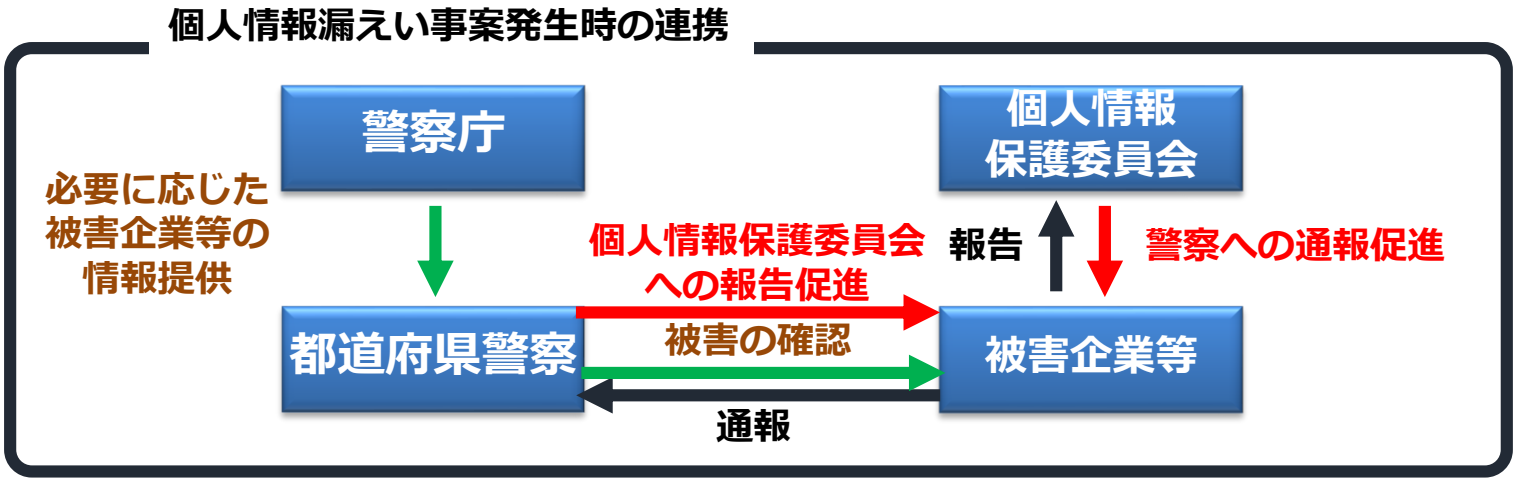
いずれにおいても、通報・相談が不可欠

- ○ **関係機関等との覚書の締結**等による通報・相談の促進
- ○ 都道府県警察の**インターネット上の通報・相談窓口の統一化**
- ○ **統一マニュアルの配布や定期的な教養の実施**等による、各都道府県警察における通報・相談への適切な対応の徹底
- ○ **被害の報告に係る様式等の統一**に向けた関係機関等との調整
- ○ ＪＣ３、損害保険会社等を介した**被害実態等の情報共有**

関係機関等との連携推進

◆　サイバー事案の被害の潜在化防止に向けた取組の推進

○　個人情報保護委員会と不正アクセス事案のうち個人情報の漏えい等発生時の警察への通報・相談を促進等する覚書を締結（2023年３月）



○　経済産業省や公益社団法人日本医師会等とも覚書を締結し、サイバー事案の被害の潜在化防止に向けた取組を推進

◆　ランサムウェア被害防止対策の推進

○　教育分野、医療分野におけるランサムウェア被害防止のため、厚生労働省、文部科学省と連携した対策を推進（医療機関に対する講演の実施、文部科学省と連名の事務連絡の発出等）

警察における今後の対応

・フィッシングサイトの傾向を踏まえた把握と提供

・ＤＭＡＲＣ等なりすましメール対策の普及促進

・フィッシングに起因する不正送金事犯やクレジットカード不正利用に関する被害防止対策の推進
（関係機関、関連団体、民間企業等と連携した対策）

・警察の対処能力の強化

おわりに

- フィッシング（スミッシング）件数の急増
- 手口はますます巧妙化・複雑化する傾向に
- 顧客への注意喚起は重要。しかし、顧客への注意喚起だけではフィッシングの被害の拡大防止は不可能
- 各事業者で技術的な対策を重層的に講じてもらう必要

⇒　省庁間や官民の間の壁を払拭した連携・情報共有とあらかじめ対策が重要