キャッシュレス社会の安全・安心の確保に向けた検討会報告書

令和６年３月21日
警察庁サイバー警察局

キャッシュレス社会の安全・安心の確保に関する検討会報告書

目　次

はじめに……1
１　情勢認識及び課題……2
１．１　キャッシュレス社会の進展とその被害状況……2
１．２　警察の取組……5
⑴　関係機関等と連携した注意喚起……6
⑵　ＤＭＡＲＣの導入促進……7
⑶　ウイルス対策ソフト等による警告表示等の推進……9
⑷　ＳＩＭスワップ対策の推進……10
⑸　国際共同捜査等の推進……11
２　キャッシュレス社会の安全・安心の確保のため方策……13
２．１　被害に遭わないための環境整備……13
２．１．１　利用者に直接届く注意喚起の実施……13
２．１．２　フィッシングサイト等にアクセスさせないための方策……15
⑴　送信側におけるＤＭＡＲＣの導入促進等……15
⑵　受信側におけるＤＭＡＲＣの導入促進等……17
⑶　フィッシングサイトのテイクダウン促進……18
⑷　次世代認証技術（パスキー）の普及促進……19
２．１．３　ＩＤ・ＰＷを窃取された場合でも被害に遭わないための方策……20
⑴　ＥＣ加盟店等との情報連携の強化……21
⑵　暗号資産交換業者への不正送金の防止……23
⑶　コード決済に関する被害防止……25
２．２　警察における対処能力の向上……26
２．２．１　先端技術の活用等によるフィッシング対策の高度化・効率化……26
⑴　フィッシングサイトの特性を踏まえた対策の高度化……26
⑵　生成ＡＩを活用したフィッシングサイト判定の高度化・効率化……27
２．２．２　被害企業等との情報共有による捜査の推進……28
２．２．３　国内外の関係機関等との連携強化……29
⑴　トラステッド・フラッガー制度の活用……29
⑵　フィッシング対策の高度化・効率化に関する連携強化……30
２．２．４ 警察の捜査により得られた情報の被害防止対策への活用推進……30

⑴　ＥＣ加盟店等との情報連携の強化【再掲】 30
⑵　警察の捜査により得られたクレジットカード情報の活用推進..... 30
おわりに..... 32

はじめに

朝出勤のため交通系ＩＣカードで地下鉄に乗車し、コンビニエンスストアではコード決済を使いコーヒーを購入する。帰宅前にスーパーマーケットにおいてクレジットカードで夕食の食材を購入し、帰宅後にインターネットバンキングを利用して忘れていた英会話の月謝を振り込む。今や多くの人々が日常生活の中でほとんど意識することなく“キャッシュレス”の恩恵を享受している。キャッシュレス決済比率の堅実な増加も、そうした社会の変化を如実に示している。

その一方で、キャッシュレス社会における被害の状況に目を向けると、極めて深刻なものとなっている。令和５年のクレジットカードの不正利用の被害額は９月時点で 401.9 億円であり、前年同期比では 30.1%増加しており、厳しい情勢にある。また、令和５年のインターネットバンキングに係る不正送金被害は、被害額・被害件数ともに過去最多と言う文言では表現し尽くせないほどの急増をみせている。そして、これら被害の要因の一つとして考えられるのがフィッシングであり、その報告件数も急増している状況にある。

これまで警察では、キャッシュレス社会の安全・安心を確保するため、国境を越えて敢行されるフィッシング事案等の捜査、実態解明、国際共同捜査の推進、被害実態・手口等を踏まえた対策の要請、関係機関等と連携した注意喚起の実施等によって、クレジットカードの不正利用や不正送金を実行した犯罪者の検挙、被害の未然防止・拡大防止等を推進してきている。

しかし、現下の情勢を踏まえると、官民連携を深化し、例えば、これまでの官民における情報共有スキームの転換や、生成ＡＩ等の先端技術の積極的な活用等、更に踏み込んだ先制的な対策を図る段階に来ていることに疑いの余地はない。そして、そうした対策強化の検討に当たっては、キャッシュレス社会のスキームや構造的課題を理解し、被害の具体的な発生状況、各事業者が保有する情報や対策の現状等を把握して、対策を強化するポイントを明確化するなど、様々なステークホルダー間での情報収集・意識共有が重要である。すなわち、警察部内の議論だけではなく、有識者による多様な観点や現場での経験からの議論が不可欠である。

こうしたことから、警察庁では、キャッシュレス社会における様々な被害に対して、官民連携の更なる推進等による効果的な対策について検討することを目的として、「キャッシュレス社会の安全・安心の確保に関する検討会」を、令和５年 11 月から令和６年２月までに計３回開催し、金融業界、ＥＣ業界、法曹界、学術界、セキュリティ関係団体等の各分野の有識者による幅広い視座、深い知見を基に議論を重ねてきた。

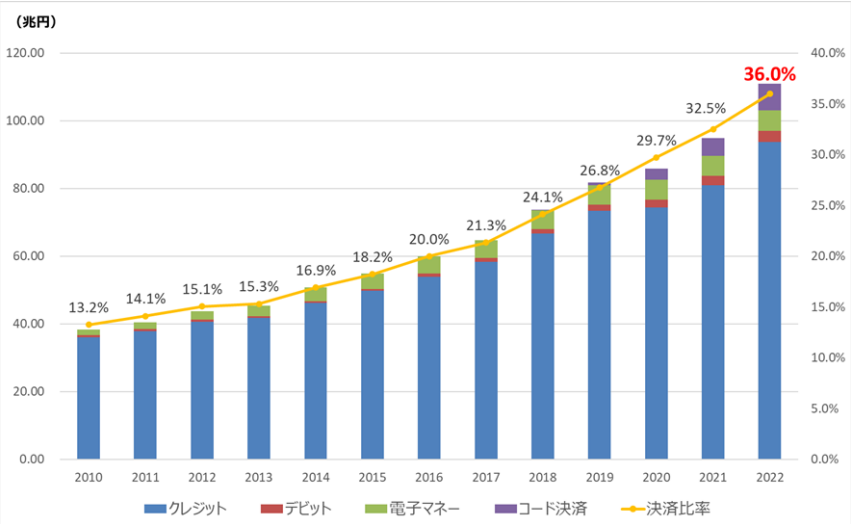
本報告書は検討会での議論の結果を取りまとめたものである。

１　情勢認識及び課題

１．１　キャッシュレス社会の進展とその被害状況

キャッシュレス決済（クレジットカード決済、デビットカード決済、電子マネー決済及びコード決済[1]をいう。以下同じ。）は、現金（紙幣・硬貨）を使用しなくとも取引ができ、物理的な制約である「モノ・時間・情報量」から解放されるという特性を持っている[2]。

我が国における民間最終消費支出に占めるキャッシュレス決済比率は、決済におけるモバイル端末の利用拡大等に見られる「消費者のライフスタイルの変化」、ＡＩ、高速通信、ブロックチェーン等の「新たな技術の進展」、「社会全体でのデジタル変革」という３つの大きな環境変化[2]も相まって、毎年確実に上昇を続けており、令和４年におけるキャッシュレス決済の比率は 36.0%、決済額は 111 兆円となっている。クレジットカード決済に加え、コード決済の比率が顕著に増加していることも注目に値する。



（兆円）	暦年	2016	2017	2018	2019	2020	2021	2022
①クレジット	決済額	53.9	58.4	66.7	73.4	74.5	81.0	**93.8**
	比率	18.0%	19.2%	21.9%	24.0%	25.8%	27.7%	**30.4%**
②デビット	決済額	0.9	1.1	1.3	1.7	2.2	2.7	**3.2**
	比率	0.3%	0.4%	0.4%	0.6%	0.8%	0.9%	**1.0%**
③電子マネー	決済額	5.1	5.2	5.5	5.8	6.0	6.0	**6.1**
	比率	1.7%	1.7%	1.8%	1.9%	2.1%	2.0%	**2.0%**
④コード決済	決済額	-	-	0.2	1.0	3.2	5.3	**7.9**
	比率	-	-	0.1%	0.3%	1.1%	1.8%	**2.6%**
キャッシュレス合計（①+②+③+④）	決済額	60.0	64.7	73.5	81.9	85.8	95.0	**111.0**
	比率	20.0%	21.3%	24.1%	26.8%	29.7%	32.5%	**36.0%**
民間最終消費支出	額	299.9	303.3	305.2	305.8	288.6	292.0	**308.5**

我が国のキャッシュレス決済額及び比率の推移

（経済産業省：https://www.meti.go.jp/press/2023/04/20230406002/20230406002.html）

1 店舗に設置されているＱＲコードを利用者のスマートフォンで読み取る、又は利用者がＱＲコードやバーコードを提示して店舗が読み取ることで決済を行う決済手段をいう。

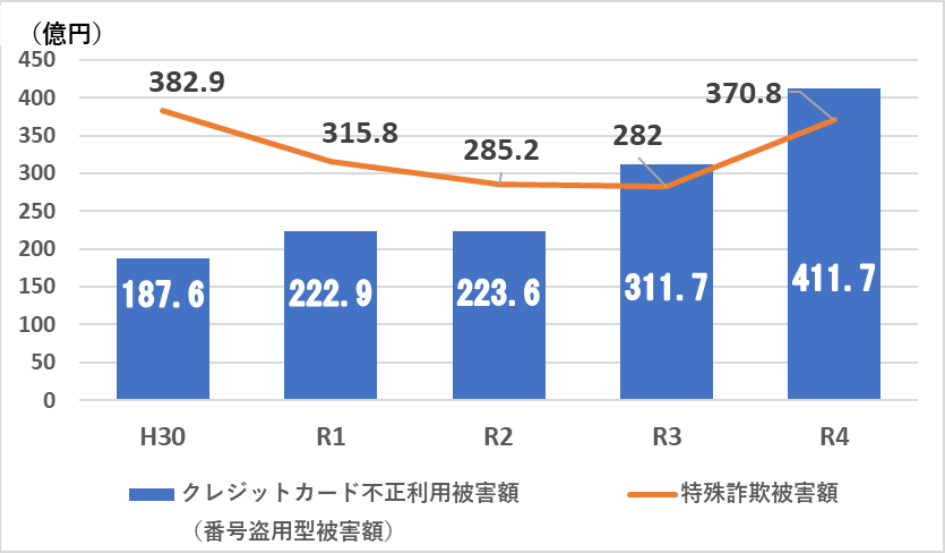
2 「キャッシュレスの将来像に関する検討会とりまとめ」（令和５年３月商務・サービスグループキャッシュレス推進室）

一方で、こうした社会の変化と呼応するかのように、キャッシュレス決済やインターネットバンキング等（以下「キャッシュレス決済等」という。）に関する被害も増加し続けている。特に深刻な被害が発生している分野については概ね次のとおりである。

①　クレジットカードの不正利用

一般社団法人日本クレジット協会（以下「日本クレジット協会」という。）によると、令和４年におけるクレジットカードの不正利用被害額は 436.7 億円で、そのうち番号盗用型の被害額は 411.7 億円であり、令和４年における特殊詐欺被害額（370.8 億円）を上回っている。また、令和５年１月から９月におけるにおけるクレジットカードの不正利用被害額は 401.9 億円と、過去最多に迫るペースで増加している。

こうした被害の内訳を見ると、クレジットカード番号盗用による被害が 90%以上となっており、フィッシングサイト（偽のログインサイト）によりクレジットカード番号等の情報を盗み取る手口も確認されている。

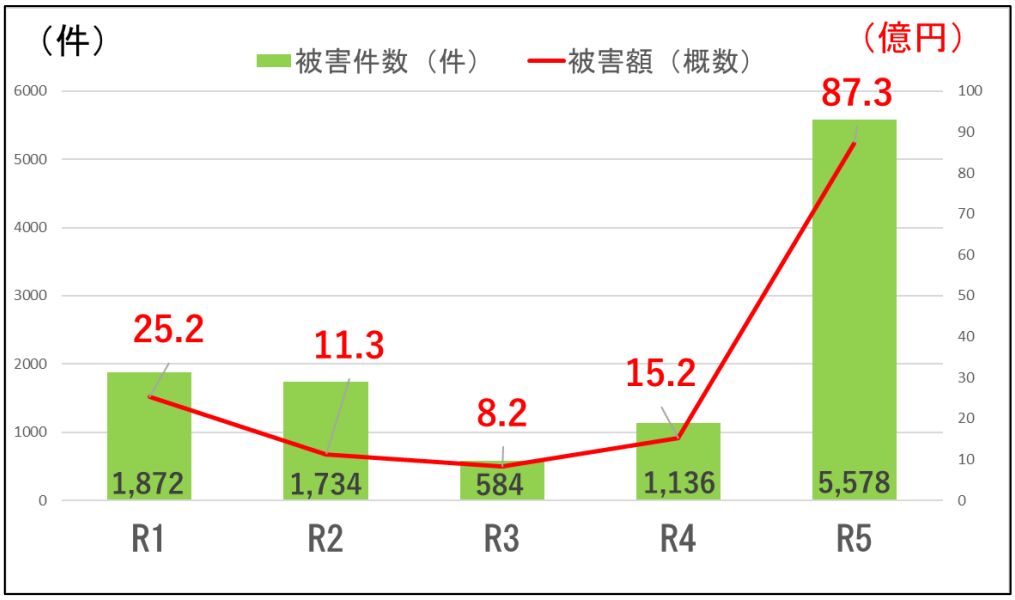


クレジットカード不正利用被害額（番号盗用型被害額）と特殊詐欺被害策の比較

（「クレジットカード不正利用被害額」は日本クレジット協会の統計資料から引用）

②　インターネットバンキングに係る不正送金

インターネットバンキングに係る不正送金事犯については、令和５年は発生件数が 5,578 件 、被害総額は約 87 億円と急増し、いずれも過去最多となった（それぞれ前年比で 391%、474%増加）。被害者の大部分は個人であり、そのうち 40 代から 60 代の被害者が約６割を占めている。インターネットバンキングに係る不正送金事犯の手口は様々であり、また、情勢や対策等に合わせて手口が変化することがあるが 、令和５年においては、その被害の多くがフィッシングによるものとみられており、金融機関を装ったフィッシングサイトへ誘導する電子メール等が多数確認されている。



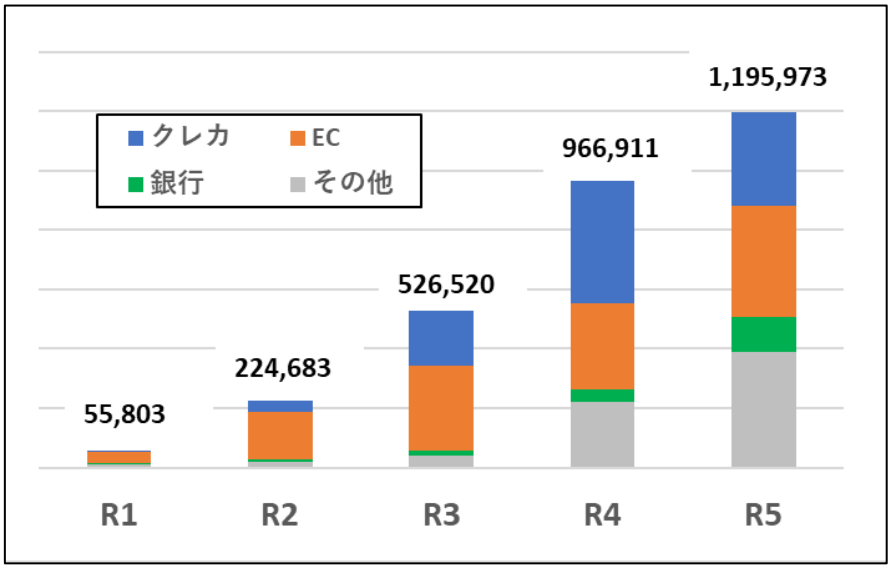
インターネットバンキングに係る不正送金被害の発生状況

（警察庁：令和５年におけるサイバー空間をめぐる脅威の情勢等について）

③　フィッシングの増加

フィッシング対策協議会によると、フィッシングの報告件数も右肩上がりで急速に増加しており、令和５年におけるフィッシング報告件数は 1,195,973 件と４年前の令和元年の約 21 倍となっている。

フィッシングに悪用されるブランドは、クレジットカード、ＥＣサイト及び金融機関が多くを占めていることを踏まえると、フィッシングが、前述したクレジットカードの不正利用やインターネットバンキングに係る不正送金の主要因の一つと見ることが極めて自然ではないかと考えられる。



フィッシング報告件数

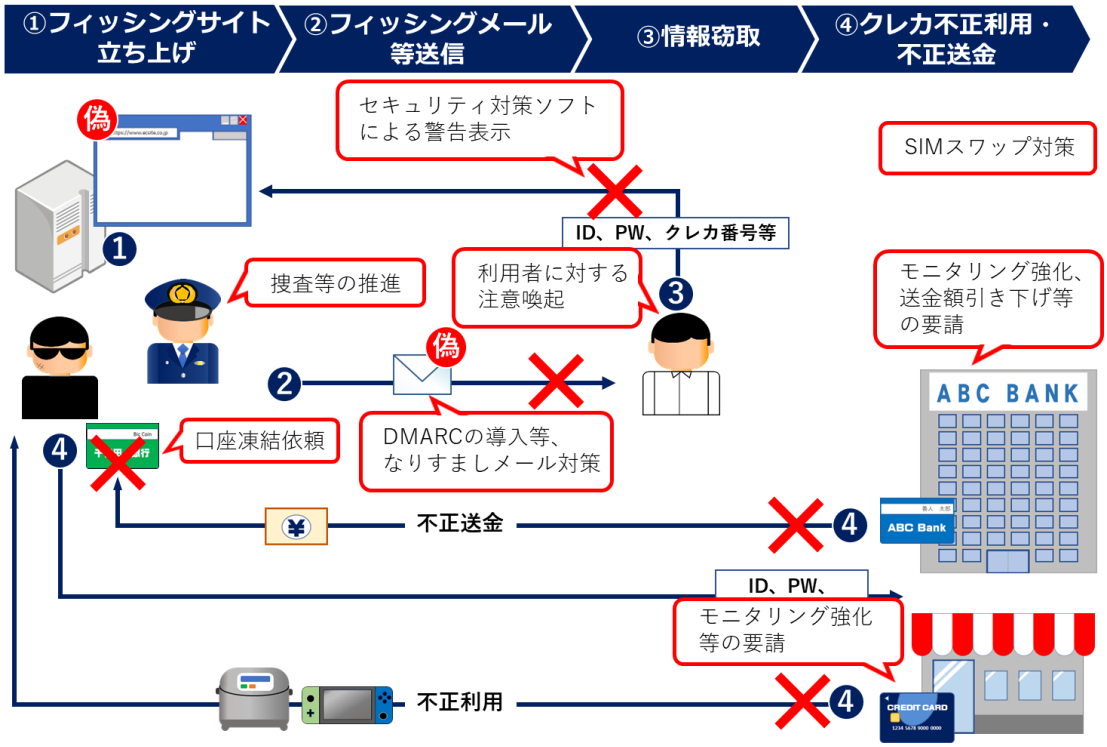
（フィッシング対策協議会の提供資料から作成）

１．２　警察の取組

サイバーセキュリティを確保するためには、攻撃をフェーズごとに細分化して分析し、それぞれのフェーズの特徴を踏まえた対策を講じることが有効であるとされている。Lockheed Martin が作成したサイバー攻撃の行動段階を構造化して整理したサイバー・キル・チェーン（Cyber kill Chain®）[3]等が有名であるが、フィッシング対策においても、攻撃を幾つかのフェーズに分解し、それぞれのフェーズの特徴を基に最適な対策を重層的に講じることが効果的であろう。

フィッシングに関しては、４つの攻撃フェーズに分解することが可能である。すなわち、「①フィッシングサイトの立ち上げ」、「②フィッシングメール等の送信」、「③情報の窃取」、「④クレジットカードの不正利用、不正送金」であり、各攻撃フェーズにおいては、例えば、「①なりすまされた事業者の知的財産権等の侵害被害」、「②サービス利用者における情報、金銭の窃取被害」、「③サービス提供事業者のシステムに対する不正アクセス被害」、「④サービス利用者の被害補填等に伴う金融機関、ＥＣ加盟店等における金銭的被害」が発生している。

それぞれのフェーズにおいて、警察において実施している取組は次の概要のとおりである。



フィッシングの各攻撃フェーズを踏まえた取組の概要

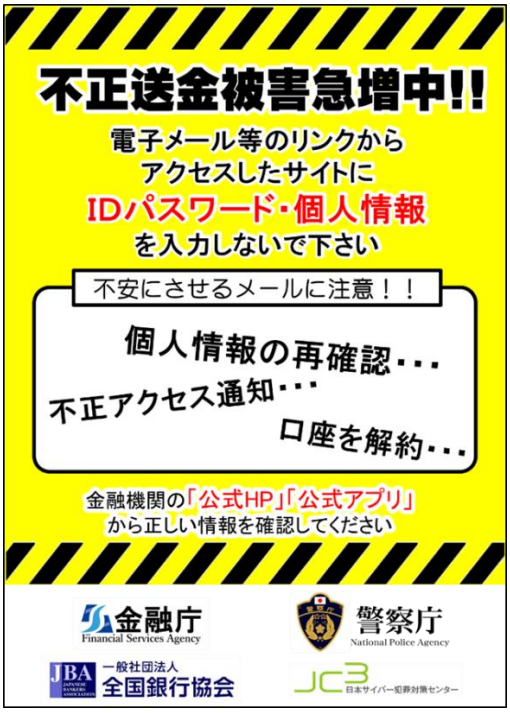
以下、警察の取組について詳述する。

3 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

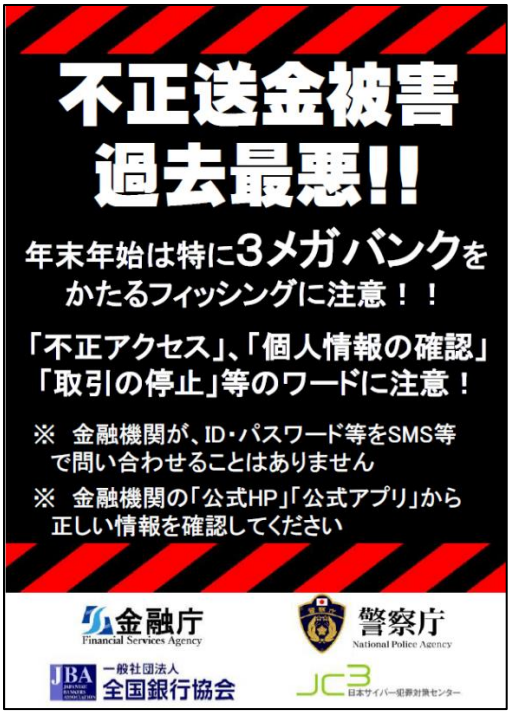
⑴　関係機関等と連携した注意喚起

警察においては、国民や企業等がサイバー事案の被害に遭わないよう、サイバー事案の捜査や実態解明から得られた情報を分析し、情勢や手口、被害の拡大・防止対策について、総務省、経済産業省、消費者庁、独立行政法人国民生活センター等の関係機関や、一般財団法人日本サイバー犯罪対策センター（以下「ＪＣ３」という。）、一般社団法人全国銀行協会（以下「全国銀行協会」という。）、日本クレジット協会等の関係団体と連携し、警察からのみならず、様々なチャネルを通じて、注意喚起を実施している。

具体的には、令和５年８月及び 12 月に、金融庁、全国銀行協会、ＪＣ３と連携し、不正送金被害が急増している状況等について、国民に対して注意喚起を実施した。



令和５年８月の注意喚起文の一部



令和５年 12 月の注意喚起文の一部

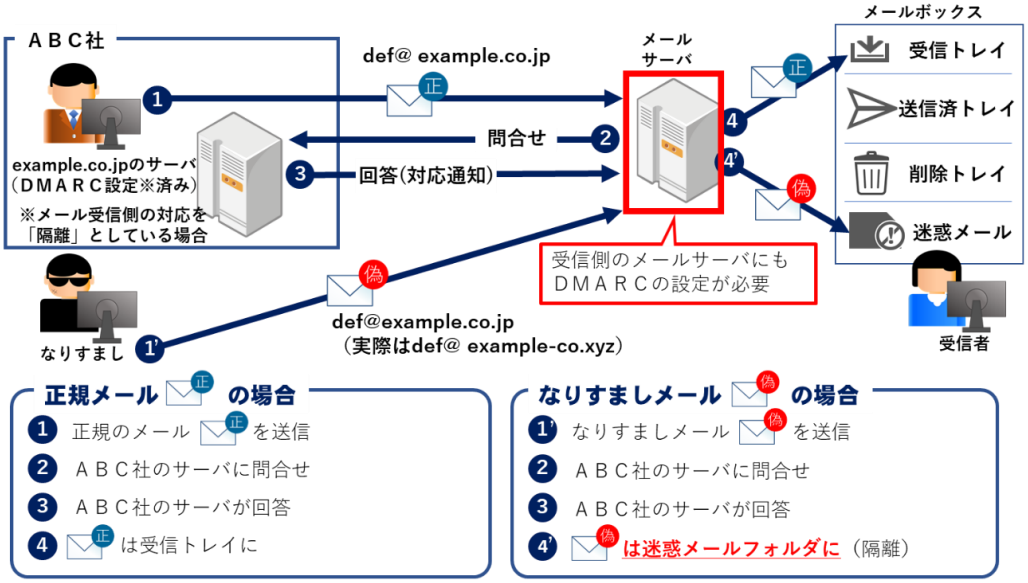
さらに、令和５年２月には総務省、金融庁及び経済産業省と連携しフィッシングに関し注意喚起したほか、外国人留学生が帰国に際して預貯金口座を不正に譲渡している事案が確認されていることから、令和５年６月には、出入国在留管理庁、金融庁及び文部科学省と連携し不正送金に悪用される口座売買に関し、複数言語による注意喚起を実施している。

関係省庁と連携した注意喚起

⑵　ＤＭＡＲＣの導入促進

フィッシング対策においては、利用者に対する注意喚起を実施することに加え、フィッシングメールが利用者に届かない環境を整備することが重要であることから、警察庁においては、関係機関、関係団体等と連携し、なりすましメール対策として送信ドメイン認証技術の一つであるＤＭＡＲＣ[4]の導入を促進している。

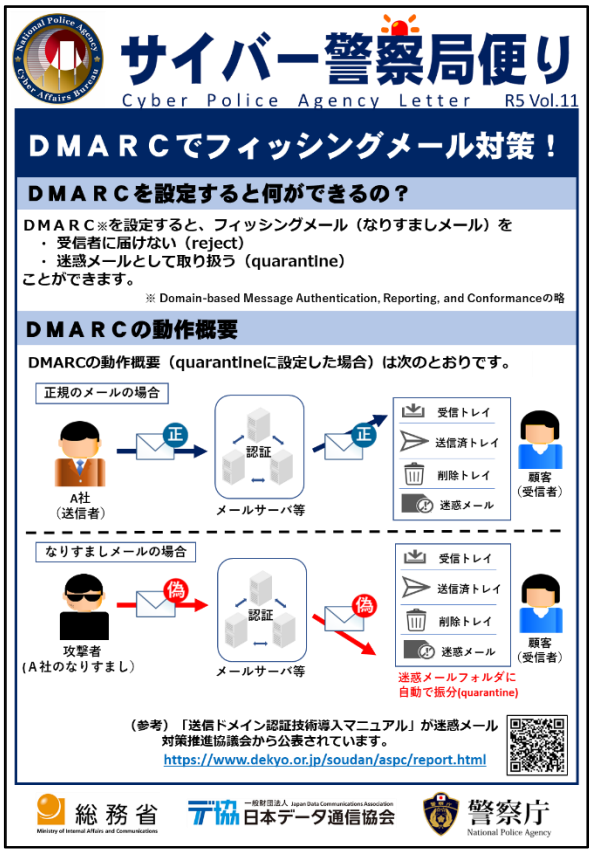
4 「Domain-based Message Authentication, Reporting and Conformance」の略。受信したメールのドメイン名が送信者（ヘッダ From）のドメイン名と一致している場合は、認証成功としてメールボックス上の受信トレイに配信し、送信者のドメイン名と一致しない場合は、認証失敗として迷惑メールフォルダに格納する（quarantine）ことやメールボックスに配送しない（reject）ことを可能とする技術である。



ＤＭＡＲＣの概要

警察庁は、令和４年９月、金融庁と連名で、全国銀行協会等に対し、ＤＭＡＲＣの導入やフィッシングサイトのテイクダウン等を含む不正送金対策の強化を要請したほか、令和５年２月、総務省及び経済産業省と連名で日本クレジット協会に対してもＤＭＡＲＣの導入を要請しており、加えて、令和５年７月、全国銀行協会等の会員金融機関に対し、被害を踏まえたフィッシングの手口やその対策について具体的に示した上で、フィッシング対策の強化を要請した。また、各種の講演会や注意喚起資料において、ＤＭＡＲＣの概要、導入手順等について説明するとともに、ＤＭＡＲＣの導入への理解促進を行っている。

FIT 大阪 2023 における講演（令和５年９月）



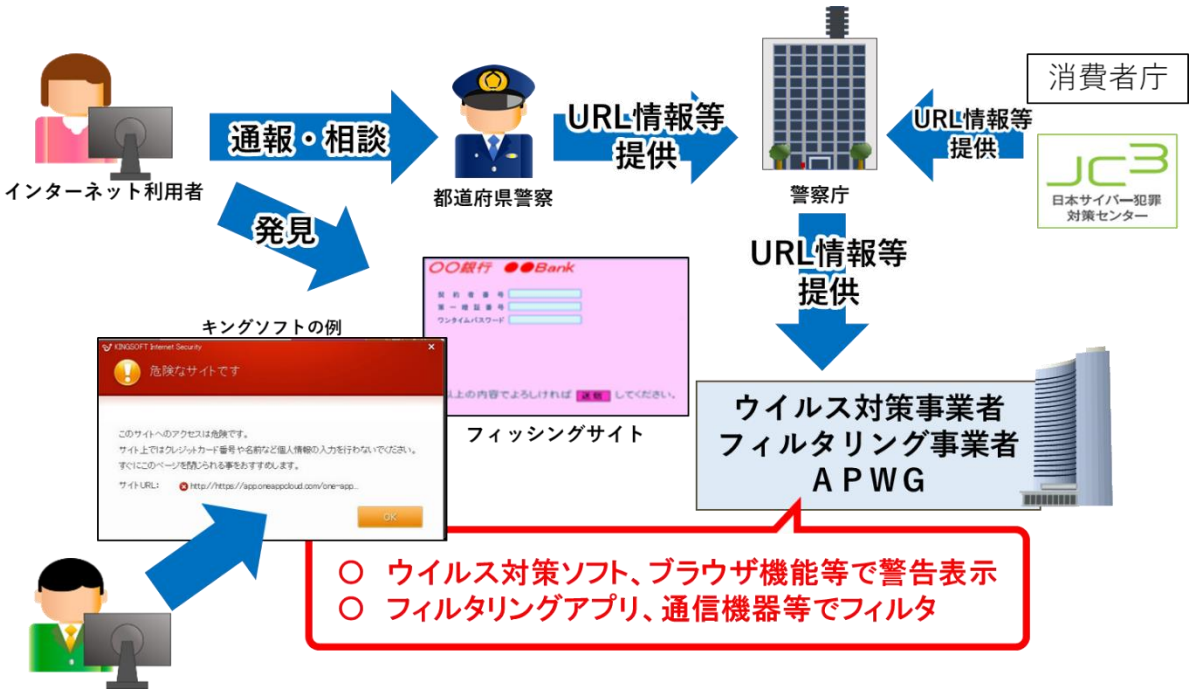
「サイバー警察局便り」による注意喚起（令和５年７月）

⑶　ウイルス対策ソフト等による警告表示等の推進

ＤＭＡＲＣの導入等のなりすましメール対策を実施したとしても、一定数の利用者にはフィッシングメールやフィッシングを目的としたＳＭＳ[5]（以下「フィッシングメール等」という。）が届いてしまうことが想定される。こうした場合に備え、被害者がフィッシングメール等に記載されたＵＲＬを押下した場合であっても、フィッシングサイトにアクセスしないようにすることが重要である。

そこで、警察庁では、都道府県警察のサイバーパトロール、インターネット利用者等からの通報・相談やＪＣ３や消費者庁等からの情報提供により、警察庁に集約されたフィッシングサイトのＵＲＬ等の情報を、ウイルス対策ソフト事業者やフィルタリング事業者、国際的なフィッシング対策の団体であるＡＰＷＧ（Anti-Phishing Working Group）（以下「ウイルス対策ソフト事業者等」という。）に提供することで、ウイルス対策ソフトやブラウザ機能等による警告表示、フィルタリングアプリケーションや通信機器によるフィルタリングに活用している。

5 ショート・メッセージ・サービス



フィッシングサイトの警告表示等による対策

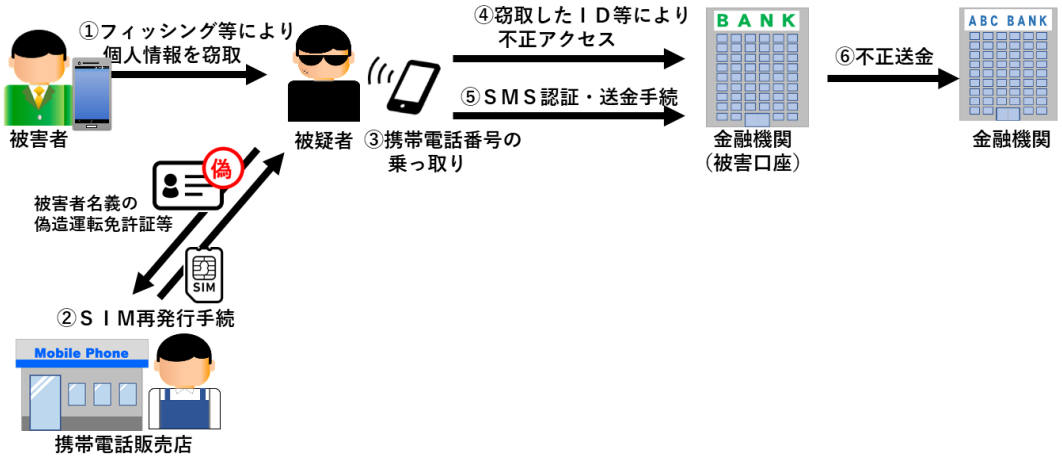
⑷　ＳＩＭスワップ対策の推進

インターネットバンキングに係る不正送金事犯においては、送金時の本人認証の強化策として一部の金融機関が導入しているＳＭＳ認証[6]を回避するため、一時期、ＳＩＭスワップと呼ばれる手口が利用されていた。ＳＩＭスワップとは、ＳＭＳ認証を回避するため、例えば、店舗に赴き「ＳＩＭカード[7]を紛失した。」などと申し述べた上で、偽造した本人確認書類を提示してＳＩＭカードの再発行を依頼し、不正にＳＩＭカードを入手する手口である。犯罪者は、不正に入手したＳＩＭカードのＳＭＳに二段階認証として送付を受けた認証番号を使って、不正送金を行っていた。

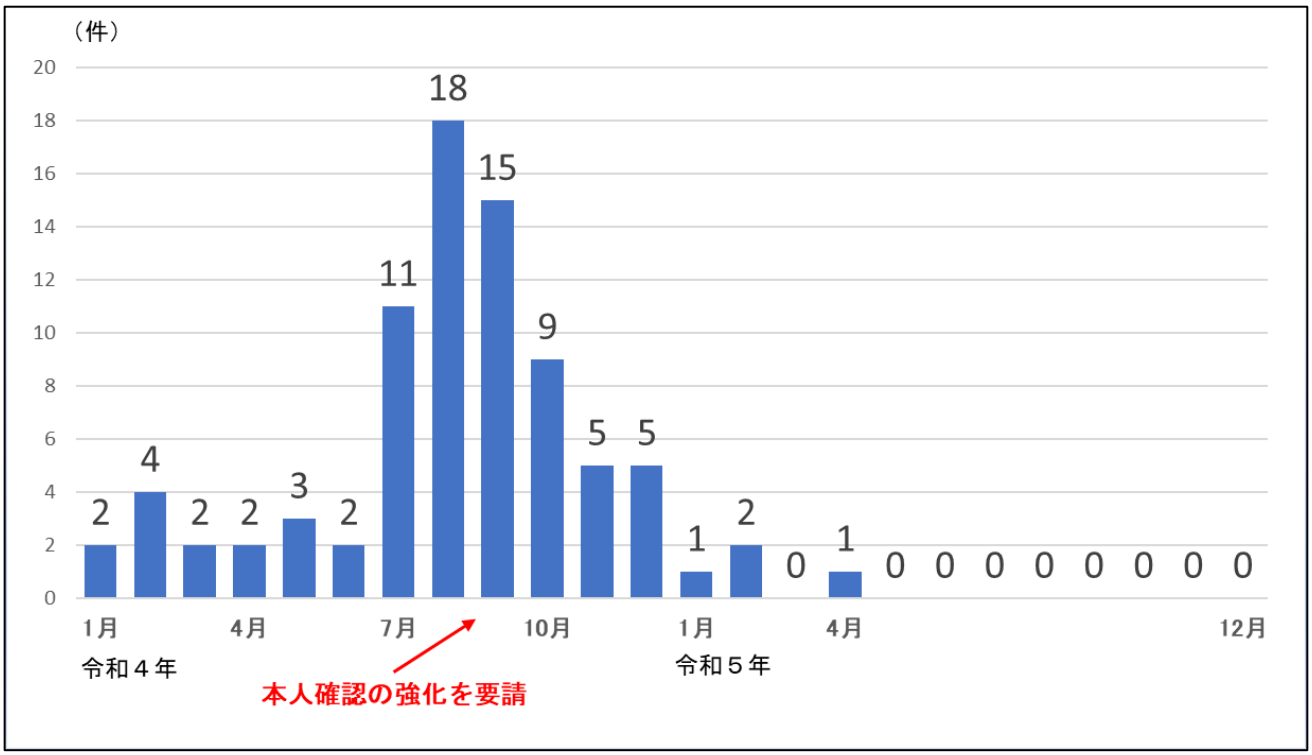
ＳＩＭスワップによるインターネットバンキングの不正送金被害が増加したことを踏まえ、警察庁において、令和４年９月、総務省と連携し、ＳＩＭカードの店舗での再発行時等における本人確認の強化を大手携帯電話事業者に対し要請した。その結果、令和５年１月以降、ＳＩＭスワップによる被害が激減し、令和５年５月以降、ＳＩＭスワップによる不正送金被害は確認されていない。

6 入力された電話番号宛てにＳＭＳで認証番号を通知し、認証画面で当該認証番号の入力を求めることで、入力された電話番号を登録本人が利用していることを確認する認証方式をいう。

7 「Subscriber Identity Module」の略で、各携帯会社と利用者の契約の証明となり、スマートフォンに差し込むことなどで通信サービスを利用できるようにするもの。（総務省：https://www.soumu.go.jp/menu_seisaku/ictseisaku/keitai_portal/gimonkaiketsu.html）



ＳＩＭスワップの概要



ＳＩＭスワップに係る不正送金発生状況

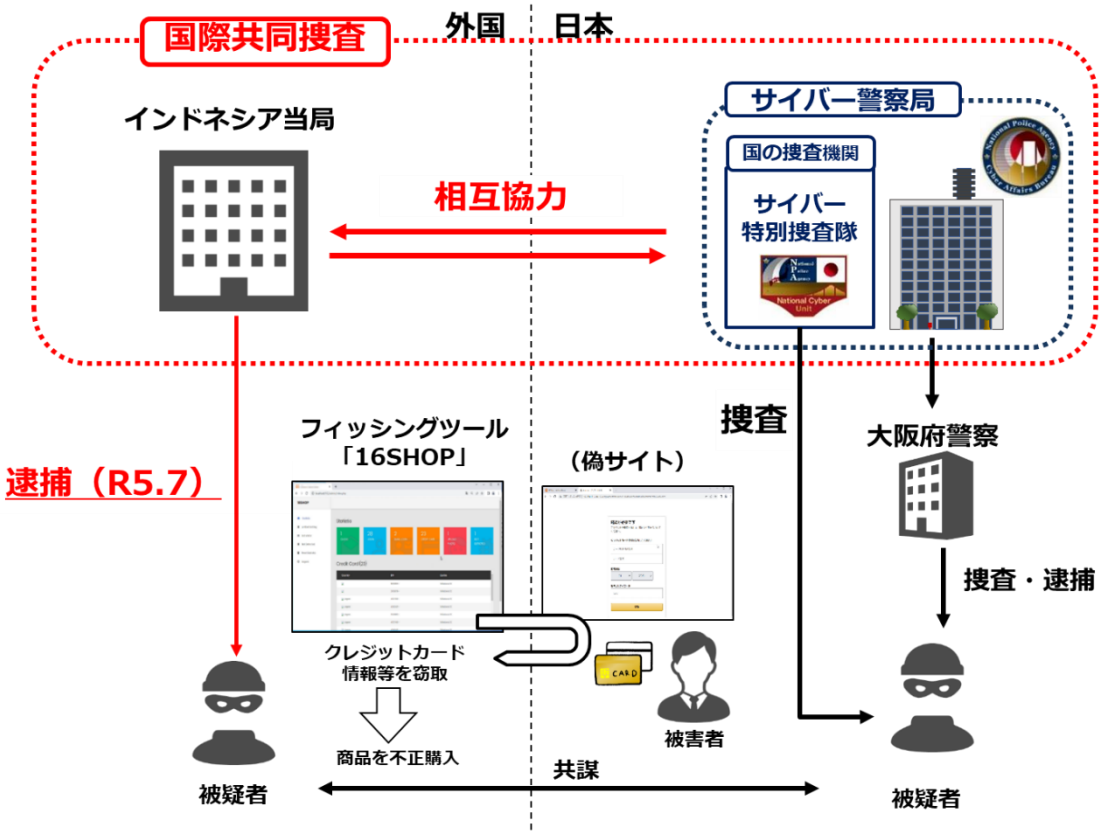
⑸　国際共同捜査等の推進

サイバー空間における脅威が極めて深刻な情勢であることを踏まえ、令和４年４月、国の捜査機関であるサイバー特別捜査隊が警察庁関東管区警察局に設置された。サイバー特別捜査隊においては、都道府県警察が初動捜査により得た情報について、高度な技術を用いて更なる分析・解析等を行っている。また、国境を越えて行われるサイバー事案に対しては外国捜査機関と連携して対処することが不可欠であることから、サイバー特別捜査隊ではこれら

機関と情報交換を行うなど国際共同捜査を推進して重大サイバー事案への対処に当たっている。

例えば、クレジットカードの不正利用事案やインターネットバンキングに係る不正送金事案の中には、被害金が暗号資産に交換され、移転される事案もみられており、サイバー特別捜査隊では不正な暗号資産取引を俯瞰的に分析することなどにより、実態解明の取組を推進している。

また、令和５年７月、フィッシングサイト作成ツール「16SHOP」を用いた国際的なクレジットカード情報不正取得・利用事案について、サイバー特別捜査隊等がインドネシア国家警察と連携して捜査を実施し、インドネシア国家警察において、同国在住の被疑者を逮捕している。



国際的なクレジットカード情報不正取得・利用事案の概要

２　キャッシュレス社会の安全・安心の確保のため方策

ますます高度化・巧妙化する手口や複雑化・多様化するサービスの登場を踏まえると、キャッシュレス社会の安全・安心を確保するためには、これまでのように被害の状況や手口を基にした注意喚起や被害防止対策を行うだけでは足りず、サービスごとにきめ細やかな注意喚起を実施することに加え、例えば、事業者において犯罪者のフィッシングに係るコストを高めるセキュリティ対策を講じるなど、利用者が日常生活を営む中で意識しなくとも被害に遭わない環境整備を更に推進することが重要である。

同時に、警察の捜査能力や情報収集・分析能力を高度化し、迅速化・効率化により犯罪者の検挙や実態把握を更に推進し、犯罪発生の芽を事前に摘み取ることも重要である。犯罪者の検挙や実態解明は、事業者等における対策に資する情報を把握することができることから、被害に遭わない環境整備にも繋がる側面もある。

そこで、本検討会においては、「被害に遭わないための環境整備」及び「警察における対処能力の強化」の観点から、具体的な方策について議論した。

これら２つの観点は、キャッシュレス社会の安全・安心に向けて、決して独立して個々に推進すべきものではなく、いわば「車の両輪」として推進すべきものである。一方で、効果的な対策を講じるために課題を分析し、本質を理解する上で、課題や対策を構造化することもしばしば有効である。本報告書においても、そうした課題分析上の要請に加え、読み手の理解促進の観点から、便宜的に２つの観点に分けて記載している。

警察庁においては、本報告書を踏まえた施策を推進するに当たっては、「被害に遭わないための環境整備」と「警察の対処能力の強化」を有機的に連動させて実施する必要があることを銘記いただきたい。

以下、本検討会において議論した方策を示す。

２．１　被害に遭わないための環境整備

「被害に遭わないための環境整備」として、１．２において述べた各フェーズを念頭に、主に「被害者に直接届く注意喚起の実施」、「フィッシングサイト等にアクセスさせないための方策」及び「ＩＤ・パスワード（以下「ＰＷ」という。）を窃取された場合でも被害に遭わないための方策」について、それぞれ具体的に検討した。

２．１．１　利用者に直接届く注意喚起の実施

警察では、これまでサイバー空間の情勢等に応じ、被害の情勢や手口に関し注意喚起を実施してきた。

しかし、こうした注意喚起は、その性質上、抽象的・総論的な内容に留まらざるを得ないが、サービスが多様化している中、注意喚起がサービスの利用者に正確に届いていない状況

が生じていると考えられる。例えば、不正送金事犯が急増していることや、その対策として「メールに記載されているＵＲＬからアクセスしたウェブサイトにＩＤ・ＰＷを入力しない」、「公式のウェブサイトやアプリからログインする」ことなどを示したとしても、インターネットバンキングの利用者において、自分に向けた注意喚起であることを正しく認識できない状況に陥っているのではないかと思われる。ただでさえ、こうした注意喚起には正常性バイアスが働き、自分が被害に遭う可能性を正しく理解できない場合がある。抽象的・総論的な注意喚起であればなおさらであろう。

また、フィッシングを実行する犯罪者は、事業者が新たなサービスを開始したタイミングや税金・公共料金の支払時期を鋭敏に捉え、フィッシングサイトへ誘導するメッセージの内容や攻撃対象を変えるなど巧妙に犯罪を実行している状況が窺われる。

こうした状況を踏まえると、様々な年齢層のサービスの利用者が自分のこととして危機感を持ち、フィッシングメール等に対する行動の変容を促すことができるよう、関係機関・団体や被害企業等、幅広い関係者で連携して注意喚起することで、話題性を高め、報道機関等に取り上げられるようにすることや、利用者の年代等に応じてタッチポイントが異なることを踏まえ、動画サイト、デジタルサイネージ等様々な媒体を効果的に活用するとともに、必ずしも一度で届くとは限らないことから繰り返し実施することにも配意する必要がある。このほか、例えばフィッシングメールの件名や文面、被害者のセキュリティ対策の実施状況等の具体的な事例を示すなどフィッシングの実態や特徴、サービスの内容等を踏まえた注意喚起を行う必要がある。

もちろん、レピュテーションリスク等を懸念し、警察と連携した注意喚起を敬遠しがちな被害企業等も少なからず存在することから、警察から被害企業等に対し、利用者の保護等の観点から粘り強くその必要性、効果等について説明をし、その理解と協力を取り付けることが重要であろう。被害企業等との連携なくして効果的な注意喚起は難しいことを今一度しっかりと受け止めていただきたい。

また、１．２⑴に掲載した注意喚起チラシにあるように、金融機関では「ＩＤ・ＰＷをＳＭＳ等により問い合わせることはない」ことを、警察や金融庁、全国銀行協会等の関係団体や金融機関において、繰り返し周知徹底を図る必要もある。

一方で、個別の具体的な注意喚起にのみ執心してしまうと、問題が矮小化されてしまうことも懸念される。要は、バランスを取ることが重要であり、「森だけを見て木を見ない」ことも問題だが、「木を見て森を見ない」ことも問題である。引き続き、サイバー空間でどういった事象が起きているかを把握し、抽象的・総論的な注意喚起を適時に実施することを、おざなりにしてはならない。

２．１．２　フィッシングサイト等にアクセスさせないための方策

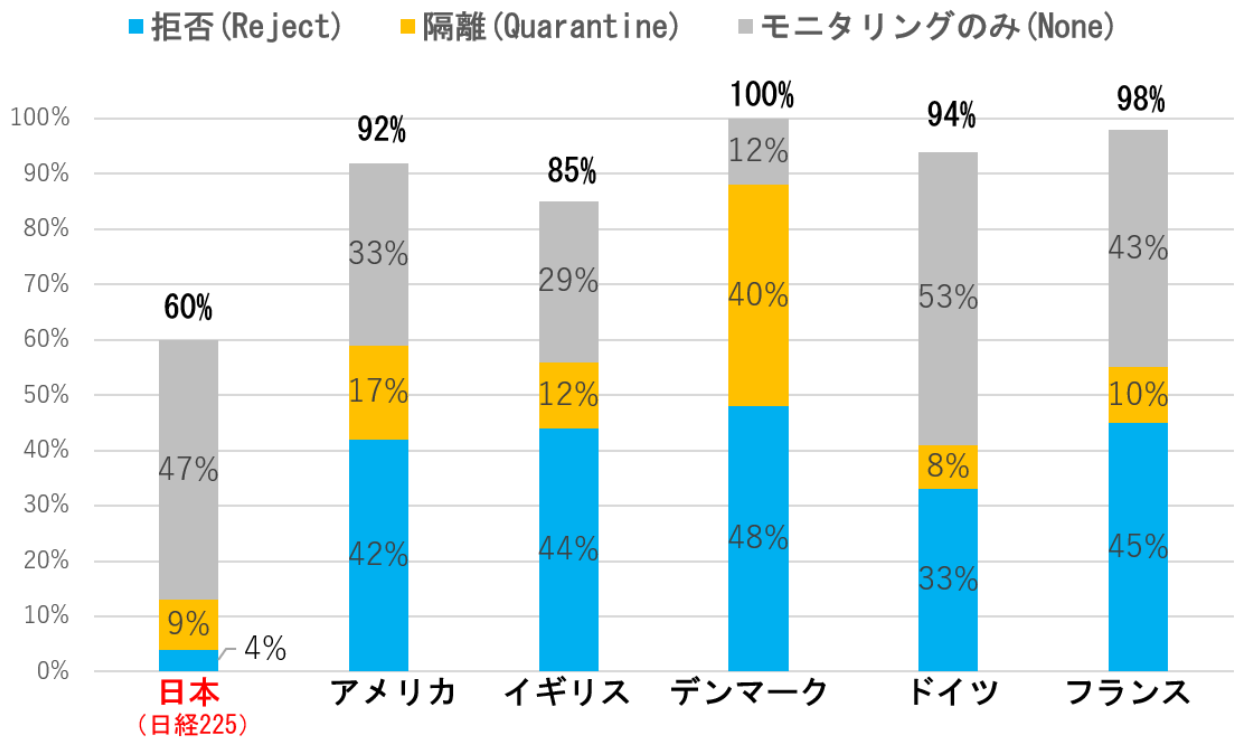
ひと昔前の「不自然な日本語」が混在していたものと異なり、最近のフィッシングメール等やフィッシングサイトは非常に巧妙に作成されており、その真偽を人間の目で判断することは困難であることが多い。また、フィッシングメール等は、「不正アクセスを検知した」、「取引を停止した」といった文面を採用することにより、利用者を不安にさせるなどして正常な判断能力を失わせ、「(フィッシング) サイトにアクセスして詳細な内容を確認しなければならない」といった心理にさせるようなものが多い。

こうしたことから、フィッシング対策においては、被害者への注意喚起に工夫を凝らすだけでは十分ではなく、そもそもフィッシングメール等の真偽を利用者に判断させる状況に至る前に、技術的な対策により、利用者にフィッシングメール等が届かない環境や、利用者がフィッシングメール等に記載されているＵＲＬにアクセスしたとしても、フィッシングサイトにアクセスできない環境を整備することが肝要である。

⑴　送信側におけるＤＭＡＲＣの導入促進等

利用者にフィッシングメールが届かない環境を整備するためには、送信ドメイン認証技術（ＤＭＡＲＣ等）の広範な普及が必要不可欠である。送信ドメイン認証技術はドメイン名単位で送信者情報が正しく設定されているかを確認する技術であり、それだけをもってフィッシングメール対策に完璧を期すことはできないが、少なくとも送信ドメイン認証技術が普及することにより、送信ドメインの詐称ができない環境が整備されることになる。

ところが、民間企業の調査によれば、我が国の民間企業（日経 225 社）におけるＤＭＡＲＣ導入状況は、世界の主要各国における主要な企業の導入状況と比較しても大きく遅れを取っていることが判明している。また、ＤＭＡＲＣを導入している企業の内訳を見ると、受信拒否（reject）や隔離（quarantine）といった設定にしていない企業が大半を占めており、実質的なＤＭＡＲＣの導入状況は非常に低調であると言わざるを得ない。



主要国のＤＭＡＲＣ導入率と日経 225 企業における導入状況（2023.12 調査）

（「日本プルーフポイント株式会社：https://www.proofpoint.com/jp/blog/email-and-cloud-threats/Global-DMARC-Adoption-Rate-Survey-2023」の掲載データから引用）

こうした状況を踏まえ、警察庁においては、関係機関等と連携し、金融機関やクレジットカード業界に対するＤＭＡＲＣ導入を含めたフィッシング対策強化の要請を行っているが、ＤＭＡＲＣの導入を更に促進するためには、総務省、経済産業省及び消費者庁と連携し、関係団体に対し、引き続き、対策を実施するよう働き掛ける必要がある。

併せて、一般社団法人日本経済団体連合会等の経済団体との連携強化により、民間事業者に対するフィッシング対策の強化を要請する必要がある。関係省庁からの関係団体への要請を垂直的な取組とすると、経済団体からの要請は業界横断的であり水平的な取組と整理されるが、いずれにしても、こうした取組は網目のように重層的に実施することが効果的である。

こうした要請に加え、一般社団法人日本データ通信協会（以下「日本データ通信協会」という。）やフィッシング対策協議会等の関係団体と連携し、ＤＭＡＲＣのレポート分析方法に関するガイドラインを作成するなど、各事業者等において導入への敷居を低くするための取組も忘れてはならない。現状は、ＤＭＡＲＣの設定等については、日本データ通信協会から「送信ドメイン認証技術導入マニュアル」[8]が公表されているが、運用に必要なＤＭＡＲＣレポートの分析方法については、インターネット上で公表されている資料は極めて少ない。

8 https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf

何を導入すれば良いかが分かっていても、導入・運用する方法が分からない状況では、導入は促進されないであろう。

なお、一部のグローバルなメールサービスを提供している通信事業者において、一定件数以上のメールをメールサービスに送信する場合には、フィッシングメール等から受信者を保護するために送信側でＤＭＡＲＣの導入を必須とする取組を開始した。ＤＭＡＲＣを導入していない行政機関や事業者等は、重要なメールが届かなくなる可能性があることから、ビジネス上の要請としてＤＭＡＲＣを導入する必要に迫られている。今後、こうした取組は他のメールサービスにも広まることが予想されることから、ビジネス促進の観点からもＤＭＡＲＣの導入は不可欠であることを伝えることも効果的である。

また、ＢＩＭＩ（Brand Indicators for Message Identification）等の公式マーク表示サービスも活用されつつある。ＢＩＭＩとは、メールを送信した企業のブランドアイコンが受信メールフォルダに表示される技術であり、ＤＭＡＲＣの導入を前提としていることから、なりすましメール対策において、ＤＭＡＲＣを補完するものと整理できる。ＤＭＡＲＣを導入した場合は、なりすましメールには効果的であるが、「なりすましていないメール」（メールアドレスを詐称していないメール）には効果が期待できず、受信者のメールフォルダに届いてしまう可能性がある。そうした際には、利用者が自ら判断せざるを得ないが、ブランドアイコンの付与の有無がメールの真贋判断において大きな手助けとなるからである。

公式マーク表示には、ＢＩＭＩのほか、ＮＴＴドコモが実施しているものなど幾つか挙げられるが、企業ブランドの認知率上昇が期待できることから、ビジネス促進の観点からも併せて普及することが望ましい。

⑵　受信側におけるＤＭＡＲＣの導入促進等

ＤＭＡＲＣの運用には、送信側のみだけでなく受信側の対策も必要になるが、日本データ通信協会の調査によれば、一部の電気通信事業者が提供するメールサービスにおいては、受信側におけるＤＭＡＲＣ機能の提供がなされていない[9]。フィッシングメールを受信するのは、多くの場合は業務用のメールではなくプライベートで利用するメールであることを踏まえると、携帯電話事業者やＩＳＰ（インターネットサービスプロバイダー）、フリーメールアドレスを提供する事業者等（以下「通信事業者等」という。）において、受信側のＤＭＡＲＣ機能を提供してもらうことは必要不可欠である。仮に送信側においてＤＭＡＲＣの導入が促進されたとしても、受信側での対応が進まない限りは、その効果が十全に得られない。

こうした受信側のＤＭＡＲＣ対応については、通信事業者等における設備投資等も必要であり、導入までの相応の時間と運用に関する費用負担が発生するが、安全なサービスを提供

9 https://www.dekyo.or.jp/soudan/contents/auth/index.html

するという社会的な責任を果たす観点や、安全なサービスを選択できるという消費者のニーズを満たす観点からも、通信事業者等において早急に進める必要があろう。

具体的には、警察庁において、総務省と連携し、通信事業者等に対し、ＤＭＡＲＣ等のなりすましメール対策の早期の導入を要請するべきである。併せて、前述した「一定件数以上のメールを送信する場合にはフィッシングメール等から受信者を保護するためにＤＭＡＲＣの導入が必要であるといった取組」についても、導入するよう働き掛けるべきである。

また、スミッシング（ＳＭＳによってフィッシングサイトに誘導する手口をいう。）対策の観点からは、ＳＭＳを受信できるアプリケーションにおける対策強化も重要である。この点、ＪＣ３が大手携帯電話事業者にフィッシングサイトに関する情報を提供し、当該大手携帯電話事業者においてフィッシングサイトへ誘導するＳＭＳの受信を自動で拒否する機能を提供している[10]が、こうした取組を広げていくべきである。この点、警察庁においては、総務省が開催する検討会等[11]にオブザーバーとして参加していることから、総務省や大手携帯電話事業者等と連携して、より実効性のある対策が実現されるよう検討を進めていただきたい。

⑶　フィッシングサイトのテイクダウン促進

ＤＭＡＲＣの導入と並行して、フィッシングサイトをテイクダウン（閉鎖）する活動も、推進する必要がある。フィッシングメール等のＵＲＬにアクセスした場合であっても、既にアクセス先のフィッシングサイトがテイクダウンされていれば、被害に遭うことはない。

フィッシングサイトのテイクダウンについては、警察庁において、金融庁と連携し金融機関に、また、経済産業省や総務省と連携しクレジットカード会社に実施要請を行っているが、引き続き、関係省庁等と連携し、関係団体等に対して、なりすまされている事業者等が自らのサービスの利用者保護の観点からフィッシングサイトのテイクダウンに取り組む必要性についても理解を促進し、テイクダウンを実施するよう働き掛けるべきである。

また、フィッシングサイトのテイクダウンに関しては、サイバー防犯ボランティアの活動にも注目したい。サイバー防犯ボランティアは、都道府県警察が委嘱し、主に①小中学校や高齢者等に対する教育活動、②広報啓発活動、③インターネットの環境浄化を行う団体であり、令和５年末現在で、全国で 308 団体が活動している。フィッシングサイトのテイクダウンは、インターネットの環境浄化の一環として、それぞれのサイバー防犯ボランティアの特性等に応じて、精力的に行われている。

---

10 https://www.jc3.or.jp/news/2022/20220113-424.html

11 「不適正利用対策に関するワーキンググループ」
（https://www.soumu.go.jp/main_sosiki/kenkyu/ICT_services/02kiban18_02000315.html）

こうした取組に加え、ＪＣ３では、専門的な知識を持たない人であってもプラットフォーム事業者等に対してテイクダウンの依頼(abuse通報)を行うことができるツール「Predator」を開発し、サイバー防犯ボランティア等に提供するとともに、令和６年２月から３月にかけてサイバー防犯ボランティア向けの「フィッシングサイト撲滅チャレンジカップ」（後援：警察庁、経済産業省）を実施するなど、フィッシングサイトのテイクダウンに関する気運を高める取組を進めている。警察としてもこうした取組を積極的に後押しし、より幅広い主体がフィッシング対策に参画できる環境を整備していただきたい。

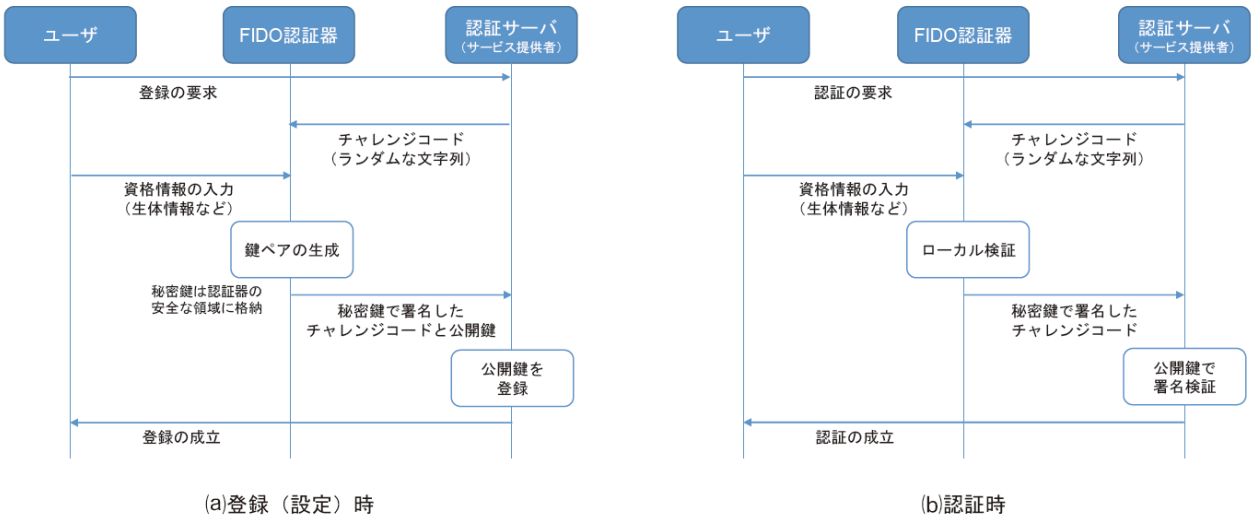
「フィッシングサイト撲滅チャレンジカップ」の実施状況

⑷　次世代認証技術（パスキー）の普及促進

フィッシングサイトにアクセスさせないための対策としては、１．１．２で掲げたフィッシングサイトの警告表示のように、フィッシングサイトを「ブラックリスト」化するほか、正規のサイトを「ホワイトリスト」化することも有効である。

そうした観点からも、ＩＤ・ＰＷの窃取を目的とするフィッシングへの対策として、パスワードレス認証である「パスキー（Passkey)」という技術が注目を集めている。

パスキーとは、FIDO Alliance（ファイド・アライアンス）とWeb標準化団体のW3C（The World Wide Web Consortium ）により規格化されている「FIDO認証資格情報（クレデンシャル)」のことであり、詳細は技術書等に譲るが、認証資格情報とともにパスキーが作成されたウェブサイトのドメイン名がメタデータ（RPID ：Relying Party IDentifier）として保存されており、認証時にこのドメインと完全一致又は後方一致しないと認証されないなど、フィッシングサイト等の正規サイト以外においては認証が機能しないといった観点から、認証情報の漏えいリスクを低減できる効果があるとされている。その他、公開鍵暗号方式によるマルチデバイス認証であることや、生体認証等のパスワードレスな認証との連携が実装されるなど、従来の認証技術に比してセキュリティが強固であり、次世代の認証技術として普及が進められている。



パスキーによる認証（FIDO 認証）の流れ

（「ドコモ テクニカルジャーナル Vol.28 No.1 Apr.2020」から抜粋）

パスキーについては、Apple や Google、Microsoft 等のベンダーが実装したことで普及に向けた下地が整備されつつあるが、我が国においては、ＮＴＴドコモのｄアカウントやメルカリ[12]、Yahoo! JAPAN ID[13]等において一部採用されているものの、まだ普及が十分ではない。

フィッシングサイトにアクセスした場合であっても、ＩＤ・ＰＷを窃取されないようにするためには、利用者の利便性に配意しつつ、こうした技術の普及促進を図ることが肝要であり、警察庁において関係省庁と連携し、金融機関やＥＣ加盟店等のサービスにおけるパスキーの採用や、利用者に対するパスキーの利用（生体認証等の利用）を働き掛ける必要がある。

なお、全ての利用者がパスキーへ移行するには相応の時間を要し、それまでの間は、ＩＤ・ＰＷによる認証を使う利用者も併存することから、パスキーへの移行段階として、生体認証等、ＰＷを使用しない認証方式を選択するよう、利用者に呼びかけることも重要であると考えられる。

２．１．３　ＩＤ・ＰＷを窃取された場合でも被害に遭わないための方策

フィッシングメール等に関する対策を強化した場合であっても、フィッシングメール等からフィッシングサイトにアクセスし、ＩＤ・ＰＷ等を入力してしまう被害者が一定数いることから、仮にＩＤ・ＰＷ等が窃取されたとしても、個人や事業者における不正送金やクレジットカードの不正利用等の実質的な被害が発生しないようにすることも重要である。

12 https://about.mercari.com/press/news/articles/20230414_passkeys/
13 https://www.lycorp.co.jp/news/archive/Y/ja/ja20230314_B.pdf

こうした観点から、ＥＣサイトにおける本人認証が強化（EMV® 3-D セキュアの導入原則化等）される予定である[14]など、事業者側の被害防止対策が強化されているところであるが、これに加え、事業者における被害防止対策に資する情報の更なる活用が鍵となると考えられることから、ここでは主に「ＥＣ加盟店等におけるクレジットカードの不正利用防止」、「金融機関における暗号資産交換業者への不正送金対策」、そして「コンビニエンスストア等におけるコード決済の不正利用防止対策」に関し、ＩＤ・ＰＷを窃取され、当該ＩＤ・ＰＷが不正に利用されそうになった場合でも、被害を水際で防止するために有効であると考えられる方策について述べる。

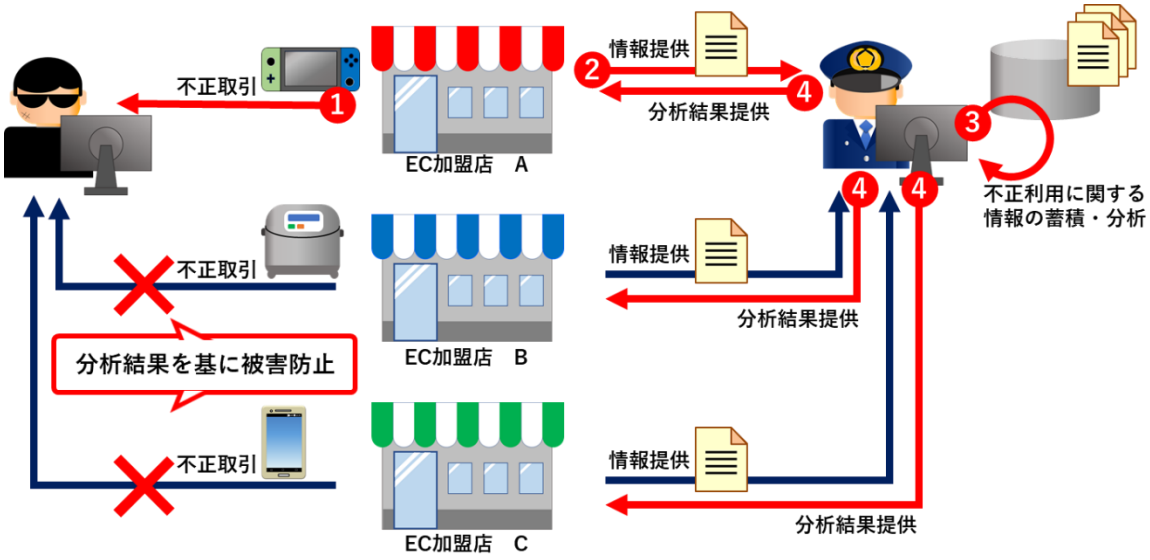
⑴　ＥＣ加盟店等との情報連携の強化

ＥＣ加盟店においては、不正取引に関するアカウント情報（氏名、住所、電話番号、メールアドレス等）、クレジットカード番号、配送先住所等や、取引日時、取引商品、取引金額等（以下「不正取引に関する情報」という。）を、それぞれの個人情報の取扱いに関する指針等に基づき、不正取引やアカウントの不正取得等の被害防止対策に活用している。

こうした情報は、組織的に複数のＥＣ加盟店等に対して不正取引が行われる場合があることを踏まえると、他のＥＣ加盟店等における被害防止対策にも有用である場合があると考えられる。

そこで、警察において、ＥＣ加盟店等から不正取引に関する情報の提供を受け、複数のＥＣ加盟店等を横断した分析を行うことにより、被害防止対策を講じるために有益な情報を掘り起こし、これをＥＣ加盟店等に還元することで、ＥＣ加盟店等において自社で独自に実施するよりも効果的な被害防止対策を講じることが可能となる。

14「クレジットカード・セキュリティガイドライン【4.0版】」
（https://www.meti.go.jp/press/2022/03/20230315001/20230315001.html）



不正取引に関する情報の共有による被害防止対策

しかし、現状では、ＥＣ加盟店等において、不正取引に関する情報を警察に提供することについて、利用規約等で第三者提供について同意を得ている場合であっても[15]、利用者の個人情報及びプライバシーの保護への配慮等の観点から、極めて抑制的に行われているとの指摘がなされている。具体的には、チャージバック（クレジットカード会社がＥＣサイト等での売上を取り消すこと）が確定した後に不正取引に関する情報を提供する場合など、不正取引が発生した時点から相当程度の時間が経過した後に実施していることが挙げられる。企業等において、利用者の個人情報及びプライバシーの保護に重点を置いて対応することはコンプライアンス確保の観点から不可欠である一方で、正確で具体的な不正取引に関する情報を警察や他の事業者に可能な限り早期に共有することが犯罪抑止の上で極めて重要であることからすると、改善の余地があるものと考える。例えば、ＥＣ加盟店等において不正取引が疑われる要素を検知した時点で、不正取引である蓋然性を速やかに確認し、蓋然性が高いものについて警察や他のＥＣ加盟店等と共有するくらいのスピード感が必要であろう。

こうしたチャージバック後の情報共有とならざるを得ない状況を改善し、ＥＣ加盟店等から不正取引に関する情報の警察への提供を促進するため、警察庁において、個人情報保護委員会事務局と調整した上で、個人情報保護法（平成 15 年法律第 57 号。以下「個人情報保護法」という。）の規定上、個人データの第三者提供の本人同意を得ることができない場合であっても、財産の保護のために個人データの提供が可能となる蓋然性が高いケースを整理することが望ましい。また、必要に応じて、個人情報保護委員会が作成しているガイドライン等において、警察への個人データの提供が可能となるケースやその際の具体的な条件を明記

15 個人情報保護法上、個人情報取扱事業者は、原則として、予め本人の同意を得ることなく、個人データを第三者に提供してはならないとされている。

することも効果的と考えられるところ、警察庁において、個人情報保護委員会事務局と実現に向けた調整を積極的に推進していくことが期待される。

同時に、個別のサービスの特性や規模に応じてそれぞれのＥＣ加盟店等の考え方も異なることから、並行して個別のＥＣ加盟店等との連携を進め、利用者の個人情報及びプライバシーの保護と被害防止対策とが両立する形での警察への不正取引に関する情報の提供を着実に実現するべきである。

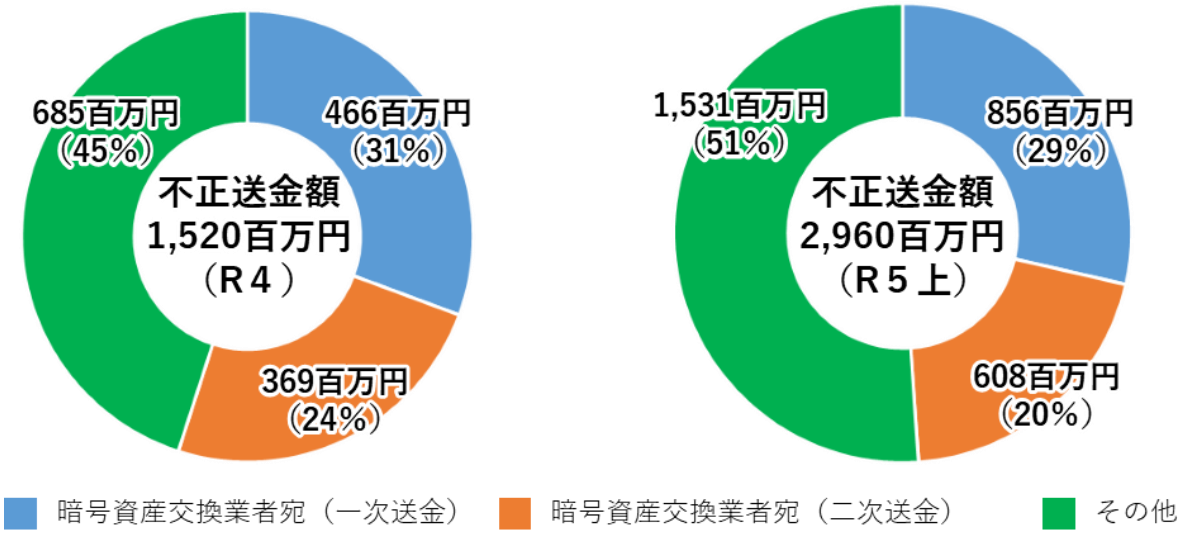
また、本人の同意を得ることなく個人データを第三者提供することが可能と言い切れないケースにおいても、警察への不正取引に関する情報提供を可能とするため、事業者等において、利用規約等に具体的に「どういった取引が発生した場合に、どういったデータを警察に提供する」といったことを記載し、個人データを含む不正取引に関する情報の第三者提供に関する同意をあらかじめ得るなどの取組を実施することも考えられる。

なお、第三者提供への同意の有無や提供する情報の個人データへの該当性によらず、こうした取組に対する利用者の理解を得て、また、顧客に対する説明責任を果たし透明性を確保するという観点から、不正取引に関する情報を警察へ提供していることなどを、定期的にウェブサイト等において公表することも望ましい。あらかじめ警察への不正取引に関する情報を提供する場合があることを周知することで、犯罪者に対して「警察と連携して対策を推進している」ことを示すことにもつながり、そのＥＣサイトでの不正取引を忌避させる副次的な効果も期待できる。このような取組により、様々な事業者において、警察への情報提供に関する理解が促進され、更に取組が推進されることが期待される。

⑵　暗号資産交換業者への不正送金の防止

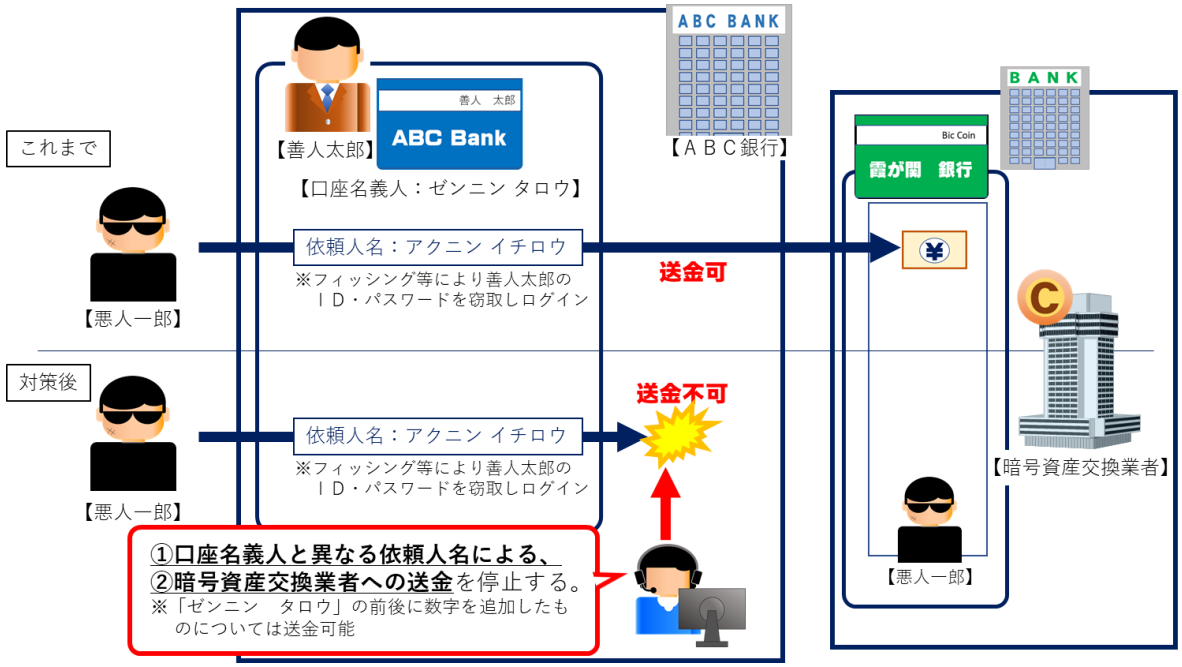
フィッシングによるものとみられるインターネットバンキングに係る不正送金事犯においては、ＩＤ・ＰＷが窃取されたインターネットバンキングのアカウントから暗号資産交換業者の金融機関口座への不正送金が多数確認されている。警察庁によると、令和５年の不正送金に関する被害額（約 87.3 億円）の実に約半分が、暗号資産交換業者の金融機関口座に不正送金されていることが判明している。

暗号資産交換業者においては、暗号資産のアカウントの名義と同一の名義による送金のみを受け付ける仕様としていることから、暗号資産交換業者の金融機関口座への不正送金は、被害者（不正アクセスされた金融機関口座）の名義から変更して行われる（異名義送金）が、一部の金融機関を除き、現在はこのような異名義送金を停止できていない。



暗号資産交換業者の口座への不正送金の割合

こうしたことから、本検討会における議論を踏まえ、警察庁において、令和６年２月、金融庁と連名で、全国銀行協会等に対して、「暗号資産交換業者の金融機関口座に対し、送金元口座（法人口座を含む。）の口座名義人名と異なる依頼人名で行う送金については、振込・送金取引を拒否する」ことや、「パターン分析のためのルールやシナリオの有効性について検証・分析の上、抽出基準の改善を図るなど、暗号資産交換業者への不正な送金への監視を強化する」ことなど、利用者保護のための更なる対策の強化に取り組むよう要請している[16]。



暗号資産交換業者への不正送金対策

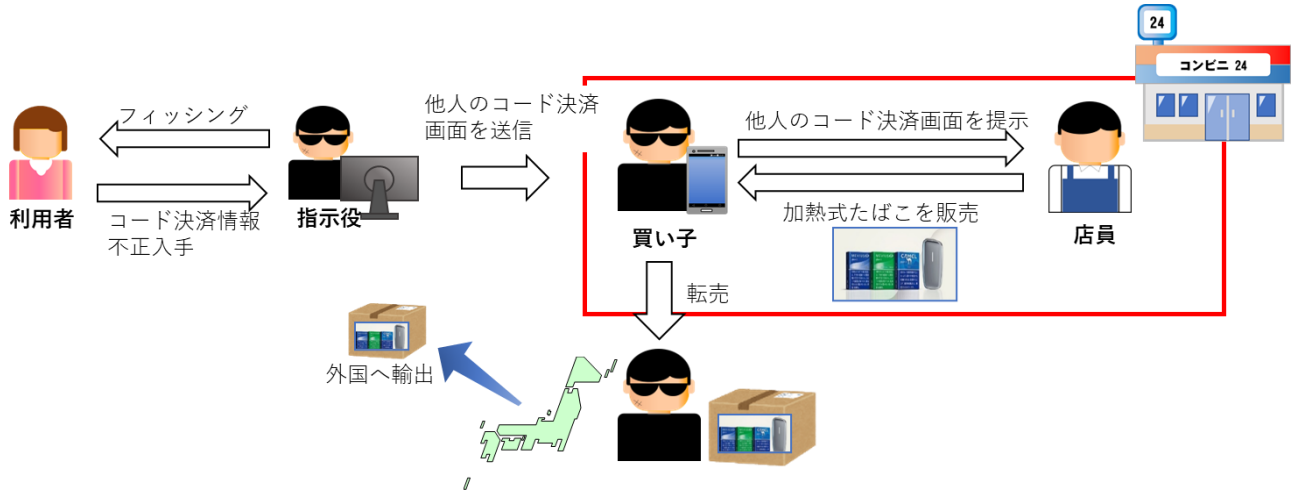
16 警察庁「暗号資産交換業者への不正送金対策の強化に関する金融機関への要請について」
https://www.npa.go.jp/bureau/cyber/koho/news/20240206.html

要請した対策の強化に取り組むまでには、体制強化やシステム改修を要することから、全ての金融機関において実現されるまでには相応の期間を要することが見込まれる。警察庁においては、要請したことをもって対策の終着地点とすることなく、金融庁と連携し、定期的に実施状況等を確認し、その結果を全ての金融機関に対して還元するとともに、未実施の金融機関に対しては、個別に根気強く対策の必要性を説明するなど、継続的に金融機関に対して対策を強化するよう要請すべきである。

⑶　コード決済に関する被害防止

コード決済については、政府による消費税率引き上げに伴う「キャッシュレス・ポイント還元事業」の推進、マイナンバーカードの普及などに向けた「マイナポイント事業」の実施やコード決済サービス提供会社による大規模なポイント還元キャンペーンに加え、新型コロナウイルス感染症の感染拡大防止の気運と相まって、決済金額が大きく伸びており、現在では、デビットカードの決済額を上回る規模となるなど、キャッシュレス決済の一角を占めるまでに日常的に活用されている。

こうした利用拡大を背景として、フィッシング等により窃取されたコード決済サービスのアカウントが、コンビニエンスストアや薬局等の店舗で不正利用されることも増加していることから、コード決済サービスの不正利用の水際防止を目的として、事業者等において対策を講じる必要がある。



コンビニ等の店舗におけるコード決済不正利用対策

そこで、本検討会の議論を踏まえ、警察庁は、令和５年 11 月、一般社団法人日本フランチャイズチェーン協会に対して具体的な犯罪手口の情報を提供するとともに、店舗における対応等を教示した。こうした被害は、薬局等においても確認されていることから、引き続き、同様の取組を他の業種に対しても実施する必要がある。

加えて、コード決済は店頭に犯罪者（出し子）が赴く必要があることから、防犯カメラの店頭や店外（駐車場等）への設置を推進することにより、こうした被害を含め、コンビニエンスストア等における犯罪の発生抑止が期待できる。また、実際に被害が発生した場合においても、防犯カメラの映像等が捜査において重要となるが、コンビニエンスストアの防犯カメラの映像の保存期間が短いために、被害状況が確認できなかった事例も確認されていることから、警察としても、業界団体と連携し、防犯カメラの設置や映像の保存期間の延長について働き掛けるべきである。

２．２　警察における対処能力の向上

サイバー事案の捜査を行う上で、官民連携の深化の観点からも警察の対処能力の強化が必要不可欠であることは論を俟たない。

また、被害に遭わないための環境整備を推進するためには、サイバー空間をめぐる情勢や犯罪の手口等に加え、個別の不正取引に関する情報等、警察が保有する情報を企業等に適時に提供することが重要であり、すなわち、警察において「被害に遭わないための環境整備」に資する情報を如何に収集・分析し、民間企業等に提供できるようにするかが鍵となる。

そこで、本検討会において、「警察における対処能力の強化」として、「先端技術の活用等によるフィッシング対策の高度化・効率化」、「被害企業等との情報共有による捜査の推進」、「国内外の関係機関等との連携強化」及び「警察の捜査により得られた情報の活用推進」について、それぞれ具体的に議論した。

２．２．１　先端技術の活用等によるフィッシング対策の高度化・効率化

警察における対処能力の向上のためには、警察で進めている対策の内容を踏まえ、高度化や効率化を図るために、民間の研究結果や製品を積極的に導入する必要がある。

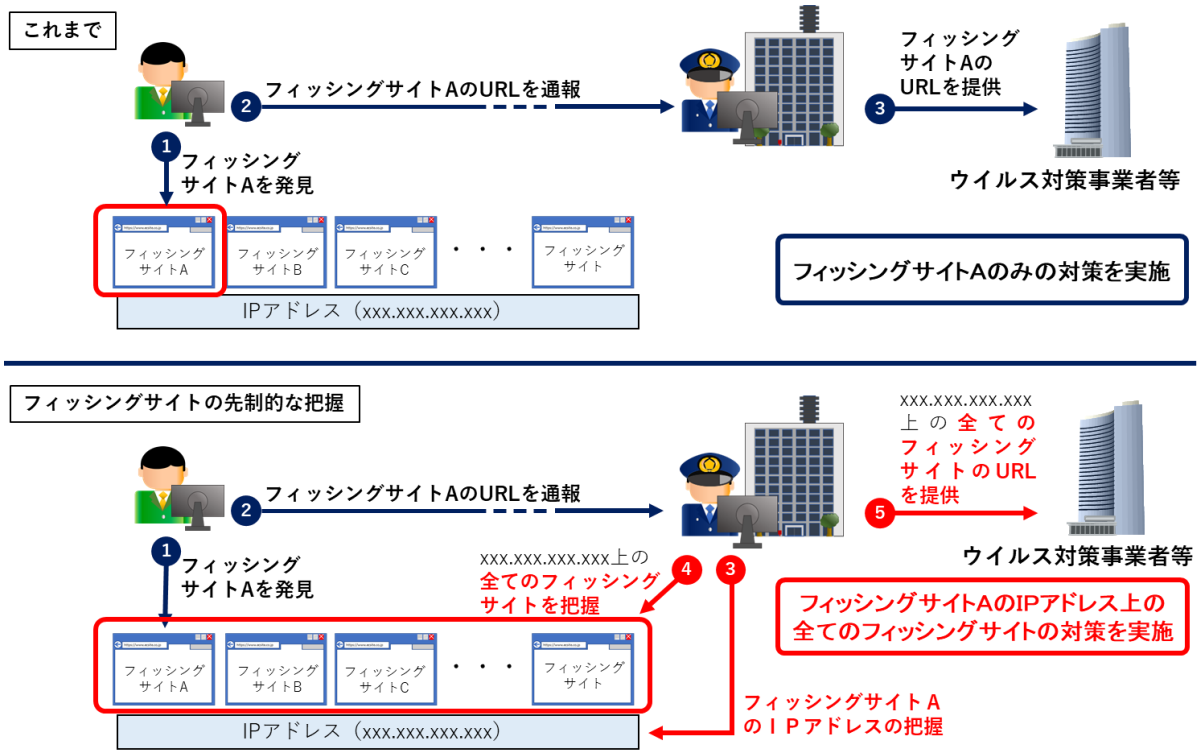
⑴　フィッシングサイトの特性を踏まえた対策の高度化

フィッシングメール等を利用者に届かない環境を整備することが重要であることは、先に述べたとおりであり、警察においては、インターネット利用者の通報・相談やＪＣ３等からの情報提供により集約したＵＲＬ情報等をウイルス対策事業者等に提供している。逆に言うと、ウイルス対策事業者等に提供している情報は、被害に遭ったインターネット利用者等から提供された情報等のみであり、雨後の筍のように次から次と乱立するフィッシングサイトへの対策としては、事後的な対応と言わざるを得ない。

ここで、フィッシングサイトの構築に関しては、一定の傾向があることが報告されている。例えば、複数のフィッシングサイトが１つのＩＰアドレス上に構築されていることが挙げら

れるが、中には、１つのＩＰアドレス上に、数百のフィッシングサイトが構築されている例も把握されている。

こうした傾向の全てを本報告書に記載することは控えるが、いずれにしても、警察において、フィッシングサイトの構築に関する傾向を基に、例えば同一ＩＰアドレス上のサイトを自動収集できるツール等を活用して把握するなどにより、通報・相談等により情報提供されたフィッシングサイトだけでなく、未だ警察に通報等がなされていないフィッシングサイトについて把握して警告表示等を実施するなど、先制的なフィッシングサイト対策を行うことが望まれる。



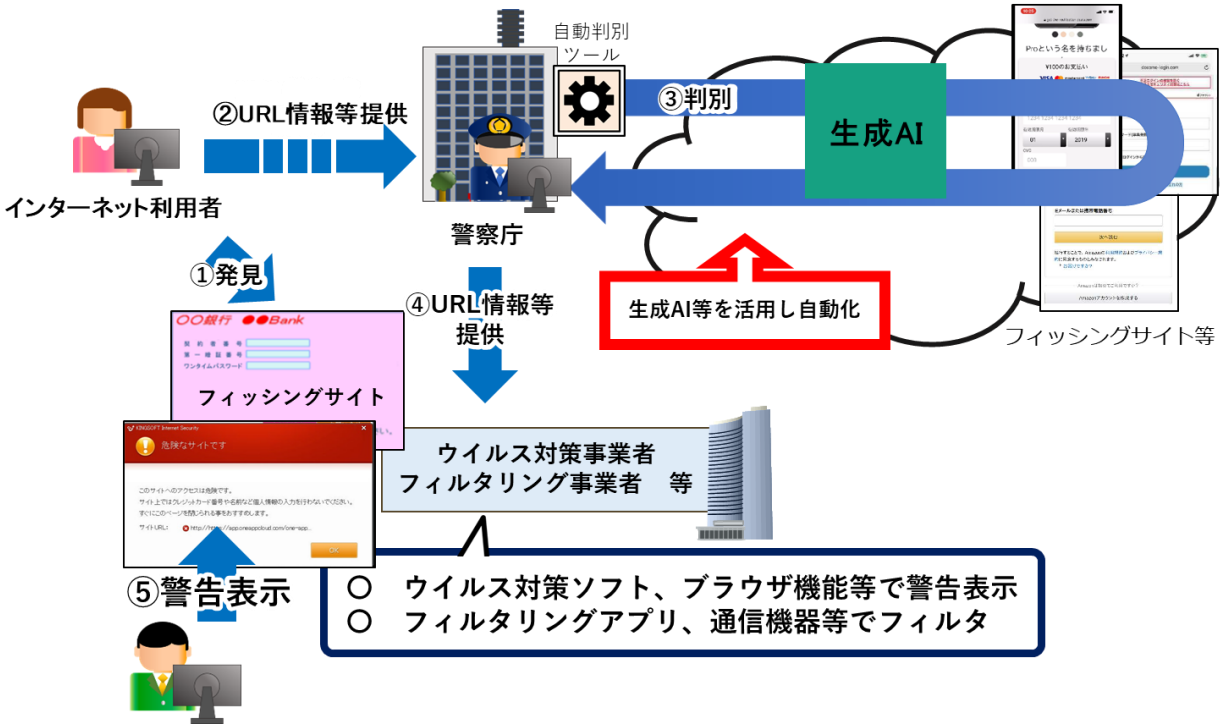
フィッシングサイトの傾向を踏まえた対策の推進

⑵　生成ＡＩを活用したフィッシングサイト判定の高度化・効率化

１．２⑶において記載したとおり、フィッシングサイトのＵＲＬ等の情報は、令和５年には警察庁からウイルス対策ソフト事業者等に約 49 万件提供している。こうした情報に関するフィッシングサイト該当性の判別は人の手によって行っており、フィッシング報告件数の増加に伴って警察庁における業務量が増大している状況である。また、⑴に記載した先制的なフィッシングサイトの把握を推進すると、今後は、ますます大量の情報について、フィッシングサイト該当性を判別することが求められる。

こうした中、民間企業において ChatGPT 等の生成ＡＩを用いたフィッシングサイトの判別について研究が進められている。その研究結果を見ると、98%以上の高い精度で、フィッシ

ングサイトの判別ができるとしているものも存在している[17]。警察庁においても、こうした最先端の技術を積極的に活用し、業務の高度化・効率化を行うべきである。



生成ＡＩを活用したフィッシングサイト対策の高度化

他方、生成ＡＩ等を活用した対策を実施する中で、誤判定により正規のサイトをフィッシングサイトと判定して警告等を表示してしまう可能性もあることから、サイト運営者等から是正申告を受け付ける窓口を設置するとともに、リカバリーに関する措置を設けることも重要である。

また、ウイルス対策ソフト事業者等において提供を受けた情報を効率的に対策に活用できるよう、提供する情報の判別方法や形式について、あらかじめ警察庁からウイルス対策ソフト事業者等に説明することも重要である。

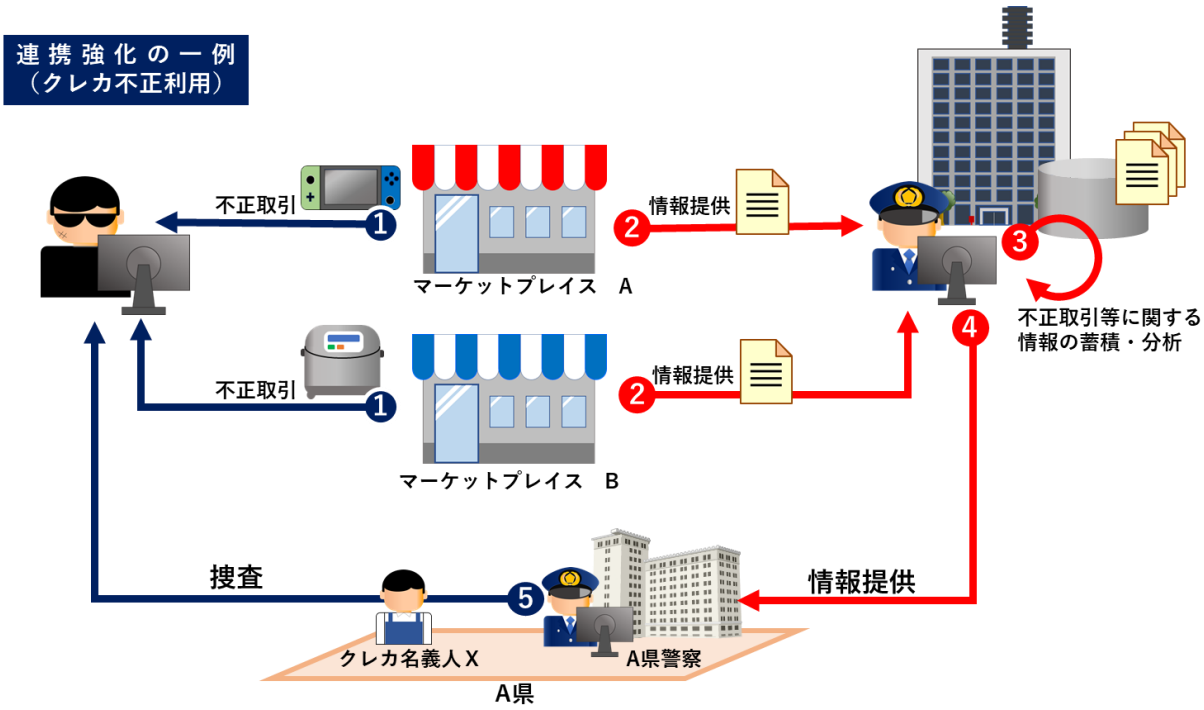
２．２．２　被害企業等との情報共有による捜査の推進

ＥＣ加盟店等が保有している不正取引に関する情報は、被害拡大防止に向けた取組のみならず、都道府県警察やサイバー特別捜査隊による捜査にも活用することができると考えられる。不正取引であることが、それ単独又は他の情報と突き合わせることにより、合理的に疑われる場合は、当該不正取引に関する情報を警察に提供し、捜査に活用してほしいと考えているＥＣ加盟店等は、警察が想像するよりも多い。

17　「ChatGPT はフィッシングサイトを検出できるか」https://jp.security.ntt/tech_blog/102ih4e

しかし、２．１．３⑴に記載しているとおり、利用者のプライバシー保護の観点等から、ＥＣ加盟店等から警察への不正取引に関する情報の提供は抑制的に行われており、こうした情報を横断的に分析し、捜査に活用することが必ずしもできていない状況が窺われる。不正取引やフィッシング等に関する情報提供を促進して捜査を推進するためには、個人データを事業者から第三者に提供することができるケースを明示的に整理することが必要である。

こうしたことにより、警察庁において、複数のＥＣ加盟店等から不正取引に関する情報を集約し、横断的な分析を行い、犯罪者をあらかじめ特定した上で都道府県警察と連携し捜査するなど、組織的かつ業者横断的に敢行される犯罪に対し、効率的かつ効果的な捜査を行うことが可能となると考えられる。



被害企業等との情報共有による捜査の推進

また、提供された不正取引に関する情報は、非常に大量になることが予想されることから、その分析に当たっては、ＡＩ等のデジタル技術を活用して高度化・効率化すべきである。

２．２．３　国内外の関係機関等との連携強化

⑴　トラステッド・フラッガー制度の活用

ブラウザやＳＮＳサービスを提供する一部のプラットフォーム事業者では、「トラステッド・フラッガー（Trusted flaggers）」として、政府機関やホットライン等から提供を受けた情報について優先的に対応してコンテンツの削除、警告表示やフィルタリングを実施する枠組みが設けられている。

警察においては、ウイルス対策ソフト事業者等におけるこうした枠組みの拡大を促進し、被害を受けた事業者と情報共有しながら、ウイルス対策ソフト事業者等に提供したフィッシングサイトの情報を迅速にフィルタリングや警告表示等に反映してもらうなど、国内外の関係事業者と連携した対策を推進するよう検討すべきである。また、プラットフォーム事業者側においても、警察等からの情報提供を積極的に受け、被害防止対策に活用していく意識が醸成されることが期待される。

⑵　フィッシング対策の高度化・効率化に関する連携強化

ブラウザ事業者等が機械学習によるフィッシングサイトの検知等に関する研究を実施しているほか、国内外の事業者や団体等にも関連する知見が蓄積されていることから、警察とこうした事業者等の双方におけるフィッシング対策の高度化・効率化に向けて、情報共有を推進するとともに、必要に応じて人事交流を促進するなどの連携強化を推進すべきである。

２．２．４ 警察の捜査により得られた情報の被害防止対策への活用推進

⑴　ＥＣ加盟店等との情報連携の強化【再掲】

ＥＣ加盟店等において保有する不正取引に関する情報を警察に提供し、警察において複数のＥＣ加盟店等を横断した分析を行うことにより、被害防止対策を講じるために有益な情報を抽出し、これをＥＣ加盟店等に還元することにより、ＥＣ加盟店等において効果的な被害防止対策を講じることについては、２．１．３⑴において述べた。

警察においては、ＥＣ加盟店等から提供される不正取引に関する情報に加え、当然のことながら、捜査や国際連携等により収集した情報を保有している。一方で、捜査が正に進展し、又は捜査が見込まれる事案においては、捜査は潜行すべきものであることから、ＥＣ加盟店等に対して被害防止の観点から情報を提供することが困難な場合が多く、また、捜査によって犯罪者を検挙することは何にも増して被害の抑止になることも理解している。それでも、捜査には所要の時間も必要となることを踏まえると、必要最小限の範囲でＥＣ加盟店等に対して、新たな被害者を生まない対策に資する情報を提供するよう努めていただきたい。それこそが、情報提供により未然防止されるであろう事案について捜査を行う必要がなくなり、警察におけるリソースの最適な活用にも繋がるものと期待されるからである。

そのためには、どのような情報であれば、捜査に支障を及ぼすことなく、ＥＣ加盟店等に提供することが可能か、あらかじめ整理しておく必要がある。

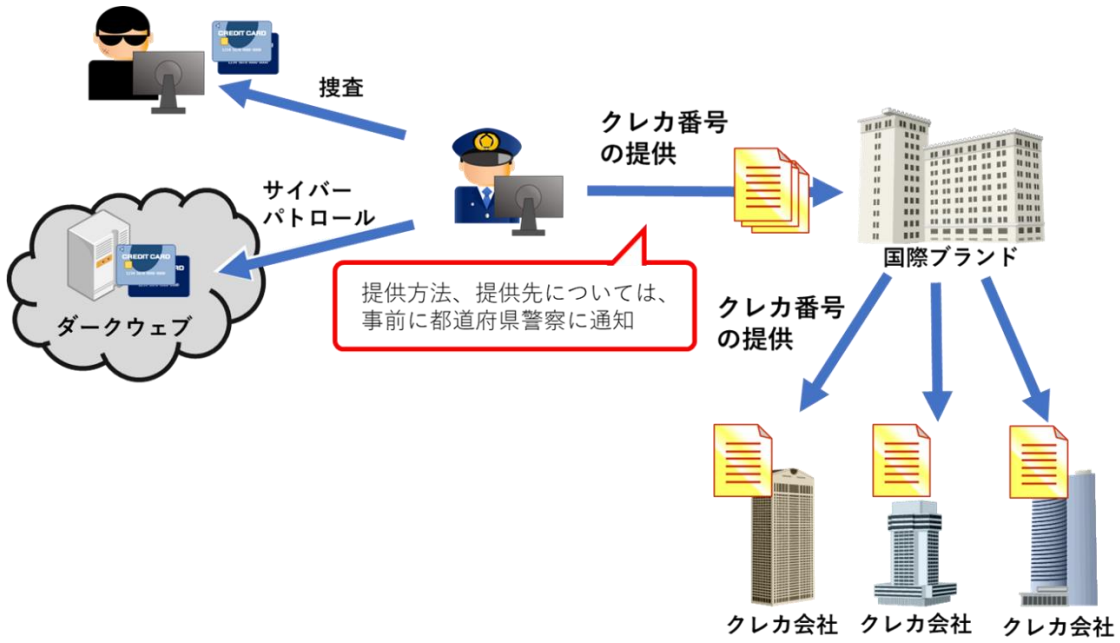
⑵　警察の捜査により得られたクレジットカード情報の活用推進

クレジットカードの発行は、VISA、Mastercard、JCB といった国際ブランドがライセンスを与えたクレジットカード会社（イシュア：issuer）が実施している。国際ブランドにおい

ては、クレジットカード情報の不正取得の被害に関する情報を収集し、悪用される恐れが明確であると判断したクレジットカードについてはイシュアに提供し、イシュアにおいて当該クレジットカードの利用停止等の被害防止対策を実施している。

都道府県警察では、これと同様に、捜査等においてクレジットカードの情報を把握した場合は、イシュアに当該情報を提供し、被害防止対策を依頼している。しかし、当該情報提供に際しては、各イシュアに対して情報提供ごと（事案ごと）に個別に連絡し、それぞれのイシュアから指定された異なる方法により情報を提供していることから、警察における業務負担は非常に大きいものがあり、迅速な提供が困難な状況となっている。

こうした状況を改善し、より迅速・効果的なクレジットカードの不正利用対策を実施するため、例えば、捜査等によりクレジットカード番号等の情報を把握した場合、国際ブランドに当該クレジット番号等を提供し、国際ブランドが各イシュアに対して情報提供することにより被害防止対策に活用することができるといった枠組みを構築することが望まれる。



国際ブランドと連携したクレジットカード不正利用防止対策

なお、利用目的以外の目的のために外国に所在する第三者へ保有個人情報を提供する場合は、個人情報保護法第 71 条の規定に基づく必要があることから、国際ブランドへの情報提供の枠組みを検討するに当たっては、こうした規定についても留意する必要がある。

おわりに

本検討会では、進展するキャッシュレス社会において、クレジットカードの不正利用やインターネットバンキングに係る不正送金といった被害の防止や捜査等に効果的と考えられる方策について、主に「被害に遭わないための環境の整備」と「警察における対処能力の向上」という２つの観点から議論を行い、整理した。

サイバー空間における警察の諸活動は大きな意義があり、社会的な影響力も大きいものがある。捜査や実態解明によるサイバー空間における情勢の全体像と個別の事象（事件）の両方を把握できる立場を生かし、全体を俯瞰しつつ個別具体的な対策を講じ、場合によっては、関係機関と連携して法令や指針等の改正を行うなど、法執行と施策の企画立案を行うことができる数少ない機関だからである。そして、令和４年４月のサイバー警察局やサイバー特別捜査隊の設置が、民間からの期待を増幅させ、大きなうねりとなりつつある。

一方で、誤解を恐れずに言うと、被害防止等の観点からサイバー空間で警察が単独でできることは決して多くはない。実空間と異なり、サイバー空間を構成する多くの要素は、公的なものではなく民間企業によるものであるからである。本報告書に記載した提言のうち、特に「被害に遭わないための環境の整備」に向けては、業界団体や事業者等の理解や協力を仰がなくては、実現にこぎつけるのは困難なものばかりである。

そういった観点から、官民連携の深化に当たっては、単に警察から事業者等に対応を求めるだけではなく、例えば、事業者等がその対応に関して利用者への説明責任を果たせるよう、要請の背景、合理的な理由、期待する効果等について丁寧に説明することや、所管省庁と連携して業界全体に向けて対応要請を行い、また、国民に対しても理解を求めることにより、個社ではなく業界全体として対応する機運を高めるなど、事業者等における対策を後押しする環境を整えることを忘れてはならない。

もちろん、事業者等において「提供サービスの環境浄化に努め、安心して利用できるサービスを提供することは企業等の社会的責任である」との意識を持つことは極めて重要である。「自助」だけでは限界があるが、「公助」や「共助」が「自助」に先んじることは決して健全なあり様とは言えないからである。各界に属する我々としても、民間企業等における社会的責任に関する意識の醸成に向けて、あらゆる機会を捉えて啓蒙していきたい。

また、グローバル化が加速度的に進む現代においては、地理的な制約を受けないサイバー空間の安全・安心の確保には、他の分野にも増して、国際連携の深化も不可欠な要素である。それには、各国の制度を踏まえて対応する必要があることから、サイバー警察にあっては、引き続き国際動向にも鋭敏であっていただきたい。

我が国経済の更なる発展には、キャッシュレス社会の安全・安心の確保は、もはやなくてはならない前提条件となっている。しかし、残念なことに、キャッシュレス社会を取り巻く

情勢は深刻な状況が続くと見込まれる。サービスの多様化やグローバル化、多くのステークホルダーの関与が、問題を複雑にしている。生成ＡＩ等の先端技術の積極的な活用は、一つの重要な処方たり得るであろうが、それでも特効薬は少なく、対症療法のみが唯一の解決策であるものもあろう。現行の法制度では対処が難しい点も生じている。被害の未然防止・拡大防止に向けて迅速な対応を行う観点から、サイバー空間における警察の対応の在り方等についても、新たな法制度を含め検討する段階に来ているかもしれない。

また、本検討会では、キャッシュレス社会の安全・安心の確保に関する課題への対策のうち、特に、注意喚起やフィッシング対策といった利用者の目から見えるものに着目して検討を進めた。他方、グローバル化やデファクトスタンダード化の進展、クラウド技術の普及等により、システム・サービスの連携が進み、サービス相互の依存度が急速に高まりつつある。これに伴い、サイバー空間上で提供されるサービスの中には、あたかもあらゆるサービスの認証基盤として活用されているものが登場していることなどから、利用者であっても自身の情報がどのサービスでどの様に活用されているかを容易に把握することがますます困難になるといった構造的な課題（ブラックボックス化）も生じている。なかには、そうした構造的な課題に端を発していると考えられる事案等も発生していることから、利用者の目から見えにくい課題への対応についても、今後検討を進めていただきたい。

いずれにしても、キャッシュレス社会の安全・安心の確保には、警察や関係省庁の「官」、民間企業や業界団体の「民」、そして「利用者」の三者が協働し、理解をはせつつも、時にお互いの立場からの意見をぶつけ合い、それぞれの責任を十全に果たし、「官民連携を深化」させること以外には実現できる道はない。多分に険しい道であることは想像に難くない。クレジットカードの不正利用やインターネットバンキングに係る不正送金が被害のピークを迎えては減少し再度増加したように、ゴールと見える頂を越えてはその先にも更なる頂が見えるといった行程の連続であろう。しかし、歩み続ける以外の選択肢はない。

もちろん、我々も、それぞれの専門分野から、引き続き警察に対する支援、助言等や関係業界との橋渡し、そして、関係団体への積極的な提言を行うなど、長い歩みを共にする覚悟でいる。

そして、本報告書が、そうした長い道程の確かな道標となることを切に望んでいる。