「スマートフォン利用シーンに潜む脅威 Top10 2023」ガイド

【第一回】フィッシング・スミッシング メール対策

【第一版】

2024 年 3 月 31 日

日本スマートフォンセキュリティ協会（JSSEC）
利用部会

文書管理番号 JSSEC-R-20240331-1

■制作■

JSSEC スマートフォン利用シーンに潜む脅威 Top10 2023 選定委員

委員長	松下 綾子	アルプスシステムインテグレーション株式会社
構成員	北村 裕司	サイバートラスト株式会社
	中村 丈洋	株式会社 SHIFT SECURITY
	本間 輝彰	KDDI 株式会社
	三池 聖史	ユニアデックス株式会社

（社名五十音順）

文書管理番号 JSSEC-R-20240331-1

目 次

1. はじめに 2

1.1. はじめに 2

1.2. 本ガイドの利用にあたって 2

1.3. 本ガイドの目的 2

1.4. 想定読者 3

1.5. 対象とする範囲 3

2. フィッシングを取り巻く、「情報」と「人」の相関図 4

3. 被害にあわないための対策・被害にあった時の対応 5

3.1. 周囲での体験 5

3.1.1. 【事例解説】ビッシング詐欺 6

3.1.2. 【事例解説】スミッシングを用いたリバースビッシング詐欺 7

3.1.3. 【事例解説】巧妙化するフィッシングメール　生成 AI の利用 8

3.1.4. 【事例解説】巧妙化するフィッシングメール　URL 偽装 8

3.2. 「その時、どうしたの？どうなった？」「ところで、どうして問題に気付いたの？」 9

3.3. 「どのような対策が考えられるか」、「どうすればよかったのか」 10

3.3.1. 【対策解説】BIMI によるブランドロゴ表示 13

3.3.2. 【対策解説】パスワードマネージャによるサービス利用 14

3.3.3. 【対策解説】パスキー（FIDO2 ～ 例：指紋・顔認証）の利用 15

3.3.4. 【対策解説】利用履歴の追跡 16

4. おわりに　～　いま私たちにできること 17

1. はじめに

1.1. はじめに

一般社団法人日本スマートフォンセキュリティ協会（JSSEC：会長 佐々木 良一）は、2011 年に設立されました。それ以来、急速に普及したスマートフォンは、ビジネスや個人の生活において重要な役割を果たしてきました。

利用部会（部会長：松下 綾子）は、利用者の視点からセキュリティに関する検討を行い、この 10 年以上の間に脅威がどのように変化しているかを再評価することの重要性を認識しました。その結果、「スマートフォン利用シーンに潜む脅威 Top10 2023」（以下、スマホ利用 10 大脅威 2023）を選定し、2023 年 2 月 28 日に発表しました。

さらに、スマホ利用 10 大脅威 2023 で選定された脅威に対処するため、被害を未然に防ぐ方法や被害発生時の対処方法を利用者視点で提唱する必要があると考え、JSSEC 会員企業の有志とワークショップを開催しました。このワークショップでは、各利用シーンにおける経験談の共有や安全対策に関する議論を行い、それらをもとに本ガイドが作成されました。

本ガイドは、スマホ利用 10 大脅威 2023　第 1 位のスミッシングメールと、第 4 位のフィッシングメールに焦点を当てて作成したもので、詐欺被害の影響をできるだけ抑制するための手助けとなる内容となっています。

1.2. 本ガイドの利用にあたって

本ガイドは、利用部会で行われた JSSEC 会員によるワークショップでの意見をまとめたものです。また、「スマートフォン」と「タブレット」を包含する言葉として「スマートフォン」を用います。

なお、記載された内容は今後の状況によって変更の可能性があります。

1.3. 本ガイドの目的

スマートフォンを安全に利用するにあたっては、技術的対策で 100%防ぐことは不可能であり、利用者一人一人がスマートフォン利用時の危険性を十分理解し、適切な判断を行うことが重要です。

利用者一人一人が、今回選定した脅威について十分理解していただけることを期待しています。

さらには、若い世代に対して企業や組織、両親や教育関係者が適切な指導ができず、相談すべき相手

が友人しかいないという問題も明らかであることから、企業や組織の責任者・担当者や教育関係者や保護者の方々には、現状を理解した上で、適切な指導に役立てていただきたいと考えています。

1.4. 想定読者

本ガイドは、主に以下の読者を対象としています。

(1) 企業や組織においてスマートフォンを導入する責任者・企画担当者
(2) 企業や組織においてスマートフォンを導入する際にセキュリティポリシーを策定する責任者、担当者
(3) 企業や組織においてワークスタイル変革を推進する責任者・企画担当者
(4) スマートフォンの利用者
(5) スマートフォン利用者の指導者、教育関係者、保護者

1.5. 対象とする範囲

本ガイドは、スマートフォンを利用する個人が対処できる範囲と、それを取り巻く環境について解説しています。

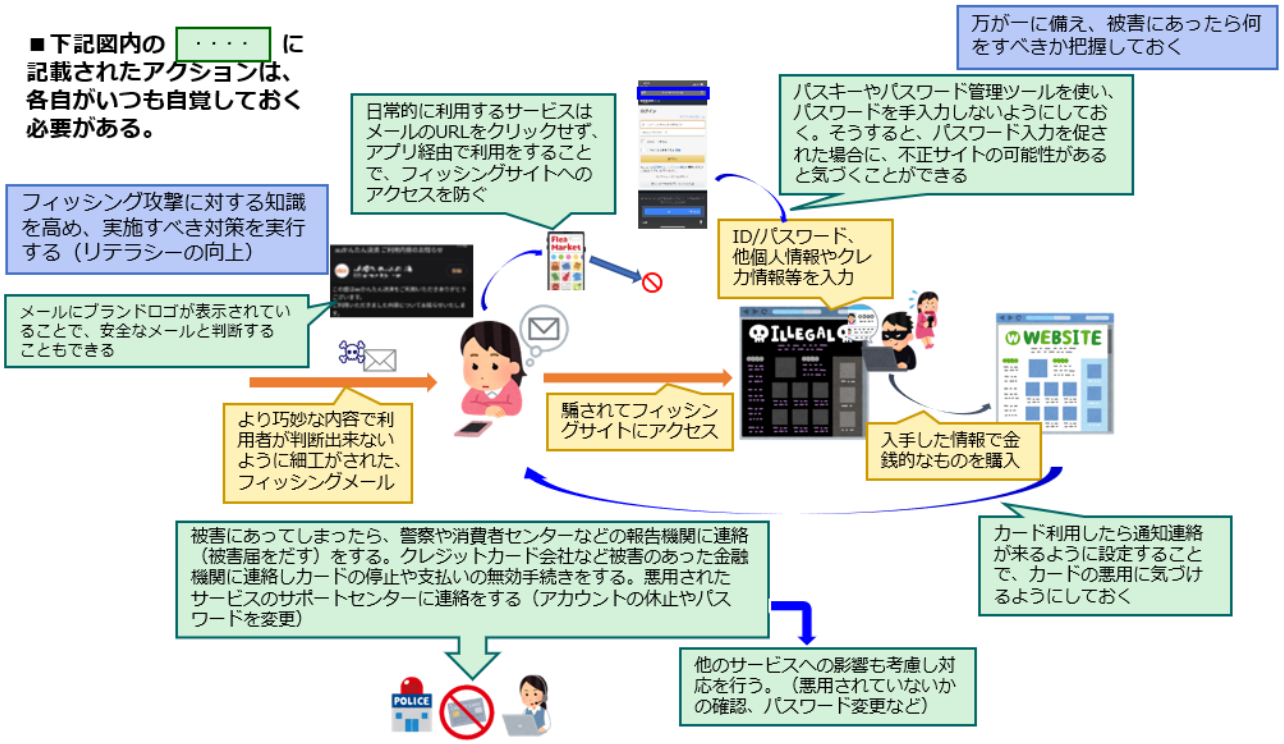
2. フィッシングを取り巻く、「情報」と「人」の相関図

フィッシング詐欺は、ますます巧妙化しています。攻撃者は、信頼できる組織や、金融機関を装ったメールを送信し、受信者に対して不正なリンクをクリックするよう求めます。リンクをクリックすると、偽のウェブサイトが表示されますが、利用者はこれを本物のサイトと誤認し、ID やパスワード、クレジットカード情報などの個人情報を入力してしまいます。このようにして、攻撃者は、利用者の個人情報やクレジットカード情報を不正に入手し、結果として金品を奪うことがあります（図 2-1　フィッシングを取り巻く、「情報」と「人」の相関図 参照）。

フィッシングの中でも、メールではなく SMS を利用した手法は特に、スミッシングと呼ばれます。

これらの攻撃に対しては、様々な対策が考えられます。次章以降では、フィッシング被害の事例、その派生事例、それらの被害を防ぐにはどうすればよいか、について説明します。

図 2-1　フィッシングを取り巻く、「情報」と「人」の相関図



3. 被害にあわないための対策・被害にあった時の対応

フィッシング対策を検討するにあたり、最初に、自分や周囲の体験談、および、その時の一次対応内容を議論しました。

3.1. 周囲での体験

自分が直接「詐欺被害にあった」という声もありましたが、多くは周囲の体験談の見聞でした。また、一般的に認知されているフィッシング詐欺の事例のみならず、多種多様な体験も挙げられました。

これらの事例と具体的な攻撃内容について、「表 3-1　フィッシング詐欺における攻撃の事例」 の通りまとめました。

表 3-1　フィッシング詐欺における攻撃の事例

<table>
<tr><th>事例</th><th>攻撃手法</th></tr>
<tr><td>怪しい日本語はだいぶ減ってきている。元のテンプレートを流用しているケースや、ChatGPT のようなサービスを利用するケースもある。後者は短文であればほぼ問題ない文章となる。</td><td rowspan="2">攻撃をより巧妙にすることで、利用者が判断出来ないように細工をする。
● 従来
➢ 当選しました
➢ 支払いしてください
➢ マルウェアに感染しました
● 最近
➢ 「セキュリティを更新してください」「セキュリティを確認してください」など、内容を確認すべきと思わせるように洗練されてきた。
➢ セキュリティ意識が高い人でも確認したくなる内容へ進化</td></tr>
<tr><td>リンク先 URL の文字列については、ギリシャ文字による偽装や、誤 URL 補正サービスなどお節介なサービスがあり、見破るのはほぼ不可能。</td></tr>
<tr><td>WhatsApp で、ボイスコールのワン切りがあった。</td><td rowspan="2">リバースビッシングと呼ばれる音声詐欺で、利用者から電話をかけさせて、発信先になりすまして対応を行い騙す攻撃。</td></tr>
<tr><td>音声に誘導することでいかなるフィルターも迂回する（オレオレ詐欺に近いが入口が SMS など）という海外事例がある。</td></tr>
<tr><td>Facebook のコメント欄で「お友達になりませんか」など緩い勧誘がある。</td><td rowspan="2">典型的ななりすまし、詐欺</td></tr>
<tr><td>ロマンス詐欺が増えている。「台湾から日本に行きたいんですが」といった、異性からの書き込み。</td></tr>
</table>

また、議論の中で、フィッシング詐欺に派生する攻撃事例についても話が挙がったため、これらを「表 3-2　フィッシング詐欺に派生した攻撃の事例」の通りまとめました。

表 3-2　フィッシング詐欺に派生した攻撃の事例

事例	攻撃手法
サポート詐欺が増えている。	高齢者や IT 知識がない人を狙った詐欺。 正規のサポート代理業者も外国人を利用していることがあり、相手が日本人ではない（つたない日本語）からといって詐欺だとすぐに疑えない事情もある。 類似として、ポップアップ詐欺や偽警告・偽契約詐欺対策などのテーマも要注意。 https://www.jssec.org/column/20230913.html https://www.jssec.org/column/20210412.html
“QR コード”を攻撃ベクタにするという話もある。 中国での事例として、シェアサイクルサービス用の QR コードの上に犯罪者が自分の口座への送金 QR を貼ったというニュースがあった。	画像を張り付ける詐欺。 サービス提供者側もホログラフなどコピー防止の仕組みと併用するなどの必要がある。

3.1.1. 【事例解説】ビッシング詐欺

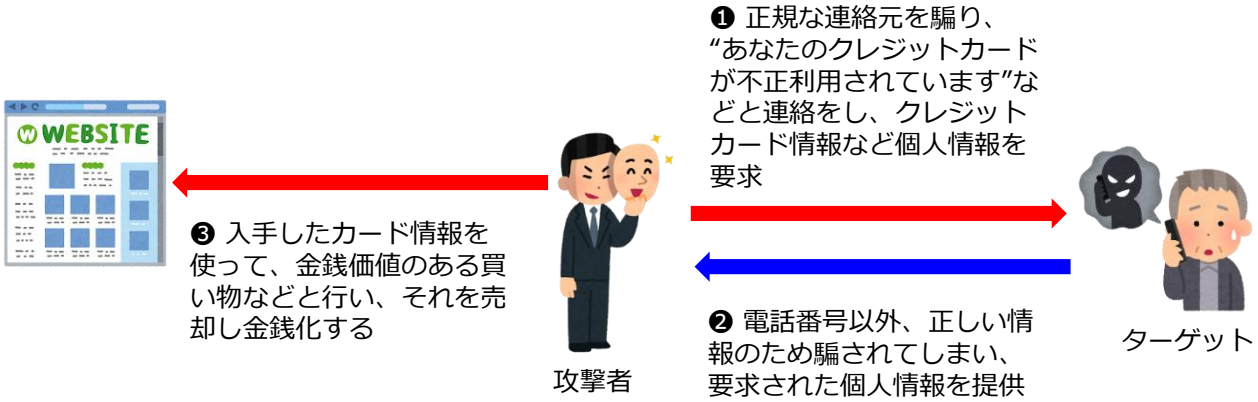
ビッシング（Vishing）は、Voice Phishing の略であり、音声を使ったフィッシング詐欺の一種です。この手法は、通常のフィッシング詐欺と同様に、利用者から個人情報や金銭を騙し取ることを目的としています。

一般的な手法として、攻撃者は利用者に対して「クレジットカードが不正利用されている」といった偽の連絡を行い、その後、個人情報の入手を試みます（図 3-1　ビッシング詐欺の攻撃の流れ　参照）。

攻撃者は、事前に利用者についての個人情報（住所や家族構成など）を入手していることがあり、この情報を利用して信頼性を高め、「正しい情報を提供している」と利用者が騙されやすくなるように仕向けます。

この手法は、電話を通じて行われるため、利用者は攻撃者の話す内容に騙される可能性が高まります。その結果、利用者は自分の情報が漏洩したと捉え、攻撃者の指示に従ってしまうことになります。

図 3-1　ビッシング詐欺の攻撃の流れ



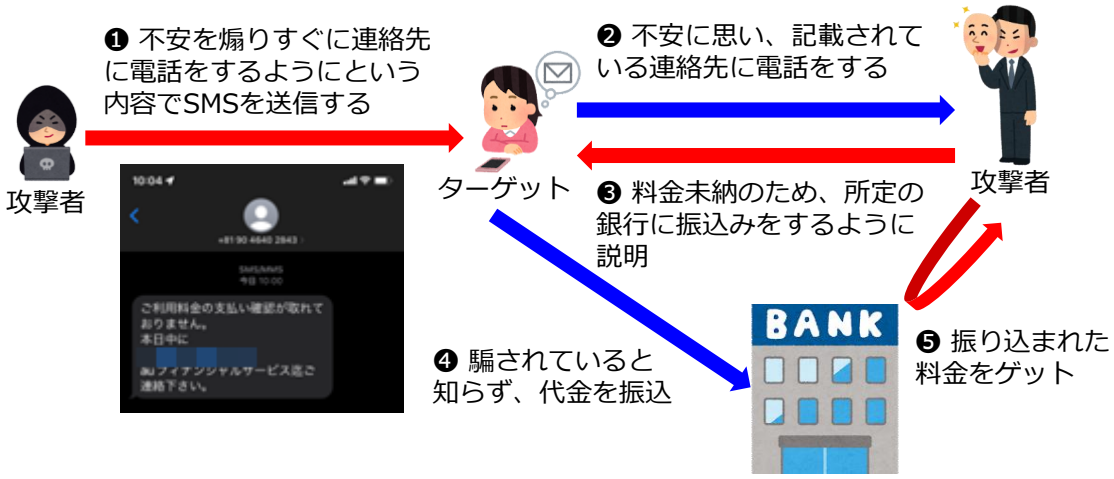
このような手法に対処するためにも、一呼吸おいて冷静になり、まずは正規の連絡先に確認して自分状況を検証してください。個人情報や重要な情報を提供する前に、慎重に確認作業を行うことが重要です。

なお、振り込め詐欺もビッシング詐欺の一種と考えられます。

3.1.2. 【事例解説】スミッシングを用いたリバースビッシング詐欺

リバースビッシングは、音声詐欺の古典的な手法の一つです。最近は、スミッシングと組み合わせた手法が急増しています。この手法は、不安を煽る内容を含んだ SMS を送信し、指示された連絡先に電話をかけさせます。この連絡を受けた攻撃者は、親身に対応し、相手を騙して金銭の振込を要求すると同時に個人情報を搾取します（図 3-2　スミッシングを用いたリバースビッシング詐欺の攻撃の流れ参照）。

図 3-2　スミッシングを用いたリバースビッシング詐欺の攻撃の流れ



上述のように、利用者が SMS を受け取り「クレジットカード情報が漏洩した可能性がある」といった不安を煽る内容に接した後、SMS に記載された電話番号に連絡を取ってしまうという、というのが典型的な手法です。そしてこの電話先で攻撃者は、信頼を得るために親切で理解がある役を演じて利用者を騙し、個人情報を収集して金銭を要求します。

この手法に対処するために、SMS や電話での突然の連絡には慎重に対応することが重要です。事前に自分が得ていない情報や、認識していない要求には、最大限の注意を払いましょう。

少しでも不審な連絡を受けた場合には、公式の連絡先を通じて状況を確認することが大切です。

3.1.3. 【事例解説】巧妙化するフィッシングメール　生成 AI の利用

生成 AI を悪用して、フィッシングメールの文面を作成する手法が確立されつつあります。この手法により、詐欺に使われる文章がより洗練され、フィッシングメールとしての認識が難しくなる可能性が高まっています。

具体的には、生成 AI の自然言語処理や文章生成技術を駆使して、信憑性の高い文章を自動的に作成することが可能になっています。これにより、フィッシング詐欺は以前よりも巧妙になり、利用者がそのメールを本物と間違える可能性が増しています。

生成 AI を悪用することで、攻撃者は従来よりも遥かに自然な文章を作成し、個人情報や機密情報を騙し取るための手法を進化させつつあります。このため利用者は、より慎重になり、正規の情報源からの確認を行うことが重要となっています。

3.1.4. 【事例解説】巧妙化するフィッシングメール　URL 偽装

フィッシング詐欺の単純な手法としては、たとえば、本物の URL "sample.example" を模倣するため" sampie.example " のように、"l" を "I" に置き換えて類似したドメインを使用する手法が挙げられます。

この時、利用者は一見すると本物のサイトと見分けがつかず、誤って偽のサイトにアクセスしてしまう可能性が高まります。

図 3-3　"l" を "I"の置き換え事例

また、文字コードを利用した URL 偽装では、本物の URL "docomo.com" を模倣するために、ギリシャ文字のオミクロン（O）を使用した "docomo.com" のような手法が使われます。この "O" はギリシャ文字のオミクロンであり、通常の "O" との微妙な違いを利用者が見分けるのは困難です。これにより、利用者は本物の URL と間違え、偽のサイトにアクセスする可能性が高まります。

例 2

https://www.example.com

https://www.example.com

■参考：ギリシャ文字一覧

小文字	大文字	読み	読み	小文字	大文字	読み	読み
α	A	alpha	アルファ	ν	N	nu	ニュー
β	B	beta	ベータ	ξ	Ξ	xi	クサイ
γ	Γ	gamma	ガンマ	ο	O	omicron	オミクロン
δ	Δ	delta	デルタ	π	Π	pai	パイ
ε	E	epsilon	イプシロン	ρ	P	rho	ロー
ζ	Z	zeta	ゼータ	σ	Σ	sigma	シグマ
η	H	eta	イータ	τ	T	tau	タウ
θ	Θ	theta	シータ	υ	Y	upsilon	ウプシロン
ι	I	iota	イオタ	φ	Φ	phi	ファイ
κ	K	kappa	カッパ	χ	X	chi	カイ
λ	Λ	lambda	ラムダ	ψ	Ψ	psi	プサイ
μ	M	mu	ミュー	ω	Ω	omega	オメガ

図 3-4　ギリシャ文字をつかった偽装の例

3.2. 「その時、どうしたの？どうなった？」「ところで、どうして問題に気付いたの？」

被害の体験を踏まえ、実際にどのような対応をすべきだったのかという観点でも議論を行いました。なぜ被害にあったか、どうして被害に気付いたか、以下の通りまとめました。

表 3-3　なぜ被害にあったか、その問題にどうして気付いたか

事例	
事例 1	● 銀行を名乗るフィッシングに引っかかったことがある。カード引き落としの被害にあった。 ● ただ、カード決済前に支払いを止めてもらい被害は無かった。 ● メールアドレスが全く違うことに途中で気づいたので、カード会社に連絡して回避できた。そうでなければ危うかった。
事例 2	● たまたま荷物の集荷を頼んでいた日に、郵便局を騙るフィッシングメールを受けたら騙されそう。
事例 3	● フィッシングに気付くのは、アクセス後が多いだろう。パスワードを入力した後に、あれ？と思うかもしれない。

事例 4	● 被害があったとき、 - 気づくのが遅れるような工夫がある。例）その後に遷移する先のサイトのロゴもそっくりに作ってある。 - 通知設定を変えてしまう。例）通知設定が解除されたことで通知が来ず、「通知が来ないから大丈夫」として気づくのが遅れる。 - 購入履歴を削除する。

◀TOPIC ： バイアスの 1 つは、「タイミング」▶

例えば、銀行からの連絡が予定されている日に、銀行をかたるフィッシング詐欺の情報に接すると、本物だと信じ込んでしまうかもしれません。攻撃者は情報を広くばらまくことで、そうした人たちを騙すチャンスをつかもうとします。最近のフィッシングメールやサイトは非常に巧妙であり、知識のある人でも騙されることがあります。だからこそ、受け取った情報には常に疑いの目を持ち、不審な場合には公式の情報源から確認することが大切です。

3.3. 「どのような対策が考えられるか」、「どうすればよかったのか」

フィッシング詐欺やスミッシングから、完全に身を守る抜本的な解決策はありません。ワークショップでの意見をまとめると、「表 3-4　有効と考えられる対策 」のような結論に至りました。

残念ながら、特効薬のような対処法は存在しませんが、個々の利用者が複数の対策を理解し、注意深く行動することが不可欠です。

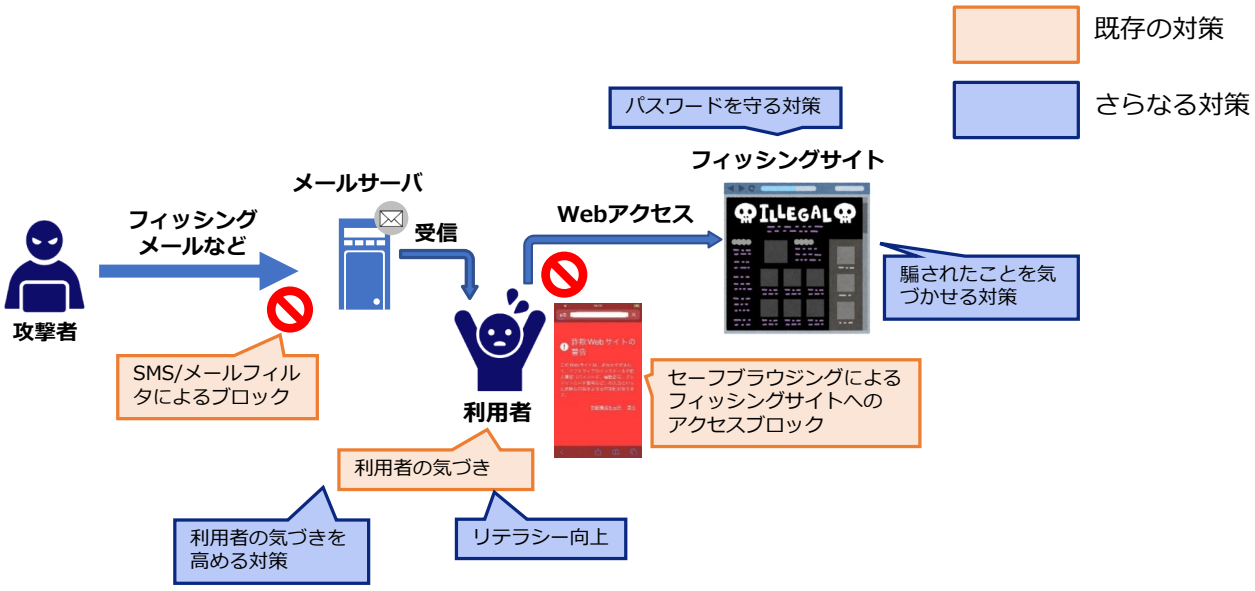
表 3-4　有効と考えられる対策

対策	具体例
リテラシー向上	フィッシングメールという攻撃があることを理解し、下記の対応することが重要となります。 ● メールや SMS、SNS に記載されたリンクからはログインしない。ブックマークを利用する。 ➢ SMS 等のリンクは決してクリックしないというメッセージを普遍的に発することが大事 ➢ 「URL を掲載しない」「URL は開かない」はサービス提供部門としては、推奨が難しいという課題もある ● 家族には「SMS に対してはリアクションを取るな、詐欺だと思え（知らない番号に限らず、海外からだと偽装が可能）」という指導をしている。 ● ブックマークからのみログインする。

	● 基本的にはリアクションしない。 ● スマートフォンアプリからのみ利用する。
BIMI によるブランドロゴ表示 - 利用者の気づきを高める対策	● 本文だけでフィッシングと見抜くことは無理がある、おそらく不可能だろう。 ● メールについては BIMI などのメールへのブランドロゴ表示の普及で見分けやすくなる可能性がある。
パスワードマネージャの活用 - パスワードを守る対策	● パスワードマネージャの活用が現実的。 ● パスワードを入力しない -> 覚えない ➢ 自分でパスワードを覚えていなければ、入力を求められた時に「フィッシングサイトかも」と疑えるし、うっかりログインするのを回避できそう。 ➢ 権限移譲タイプ（OAuth）のフィッシングには十分ではない可能性もあるので、要注意。
パスキー（FIDO ～ **例:**指紋・顔認証）の利用 - パスワードを守る対策	パスキー（FIDO2 ～ 例:指紋・顔認証）で認証する。 ➢ 利用できるか否かはサービス提供者に依存する。ユーザが使いたくても使えない場合もあるので、サービス毎に確認が必要。
利用履歴の追跡 - 騙されたことを気づかせる対策	● カード利用したら、リアルタイムに通知連絡が来るように設定する。 ● 支払いや金融資産を管理する。カード明細等を確認する。 ➢ 家計簿アプリ等の資産管理アプリを使う。しかし家計簿アプリ自体の信頼性担保は必要。

また、上記の対策を攻撃内容の流れからまとめると、「図 3-5　フィッシング攻撃と対策の流れ」の通りになります。

図 3-5　フィッシング攻撃と対策の流れ



さらに、実際に被害にあった事例を参考に、「その時どうすればよかったのか」という議論を行った結果、下記に示すような意見が集まりました。

表 3-5　被害にあった時にどうすればよかったのか

事例	
事例 1	● キャリアの SMS には、「不審な SMS を報告する」といった機能があるので活用する。 ※Android はキャリアプロファイルによる。 ※iOS は iMessage にはデフォルト機能あり。 ● メールもサービス提供各社が報告機能などを提供しているので、これら機能を活用する。
事例 2	● 送信元が不明なメールや SMS は、いったん保留する。急を要すると感じた場合は、別ルートで事実確認を行う。
事例 3	● フィッシングに引っかかったかもしれないと思った時は、知見のある知り合いや消費者センターへ相談する。 ➢ 「知見のある知り合い」というのは、その人の思い込みかもしれないので危険性あり。公的な機関への相談を推奨したい。

フィッシング詐欺を防ぐためには、サービス提供者やプラットフォーム提供者の責任も大きいとの声がありました。例えば、パスワードの安全性を高めるために、FIDO2 やパスキーの利用が推奨されていますが、対応しているサービスはまだ一部であり、未だにセキュリティ対策が不十分なサービスが存在しています。また、BIMI を使ったメールへのブランドロゴ表示に関しては、メールを送信するサービス事業者、メールサービス提供者の双方での対応が必要となります。しかし、どちらも対応しているのは一部です。

従って、サービス提供者、メッセージサービス提供者、そして利用者、すべてのステークホルダーが利用シーン改善に向けた努力を継続して行う必要があります。

3.3.1. 【対策解説】BIMI によるブランドロゴ表示

BIMI（Brand Indicators for Message Identification）は、メールに送信元ブランドの公式ロゴを表示させることで、受信者に対してメールの正当性を示すための仕組みです。これにより、受信者はロゴの表示を通じて、送信元が正規のものであることを確認しやすくなります。BIMI の実装には VMC（Verified Mark Certificate）証明書が必要であり、これが攻撃者の悪用を困難にする利点もあります。VMC 証明書は、送信元が信頼できるかどうかを検証するための証拠となります。

このような取り組みにより、受信者はメールで送信元のブランドロゴが表示されると、それが正当であることを確信しやすくなります。つまり、受信者はブランドロゴの表示を通じて、そのメールが安全であることを認識しやすくなります。これにより、フィッシングメールやその他の悪意あるメールから保護される可能性が高まります。

図 3-6　BIMI によるブランドロゴ表示の例

ブランドロゴを表示するには、送受双方で BIMI に対応する必要がありますが、対応しているサービスがまだ少ないのが現状です。

そのため、フィッシングに悪用されているサービスプロバイダー各社での導入が期待されています。

3.3.2. 【対策解説】パスワードマネージャによるサービス利用

パスワードマネージャを使用することで、パスワードを安全に管理できます。また、サービスへのログイン時には、パスワードマネージャが自動的に ID やパスワードを入力します。この機能により、利用者はパスワードを手動で入力する必要がなくなり、セキュリティが向上します。

さらに、もしもパスワードが自動的に入力されないサイトがあれば、それはフィッシングサイトである可能性があります。この特性により、ユーザは自動入力の動作を通じて、不正なサイトに対する判断が容易になります。そのため、パスワードマネージャを使用することで、安全なパスワード管理とフィッシングサイトからの保護が期待できます（図 3-7　パスワードマネージャによる判別例 参照）。

また、パスワードマネージャの情報は、クラウド上に保存することで、スマートフォンを盗難・紛失してもクラウドのアカウント（Apple ID や Google アカウントなど）を使って復旧することが可能です。しかしながら、クラウドのアカウントが流出するとパスキーも搾取される可能性があるため、クラウドのアカウントは他人に漏れないように厳重に管理することが重要となります。

図 3-7　パスワードマネージャによる判別例

3.3.3. 【対策解説】パスキー（FIDO2 ～ 例：指紋・顔認証）の利用

パスキーは、サービス利用時にログイン ID とパスワードの利用で行っていた方法に代わる安全な認証方法で、スマートフォンに設定した生体認証やパターンを使ってログインができるようになります。

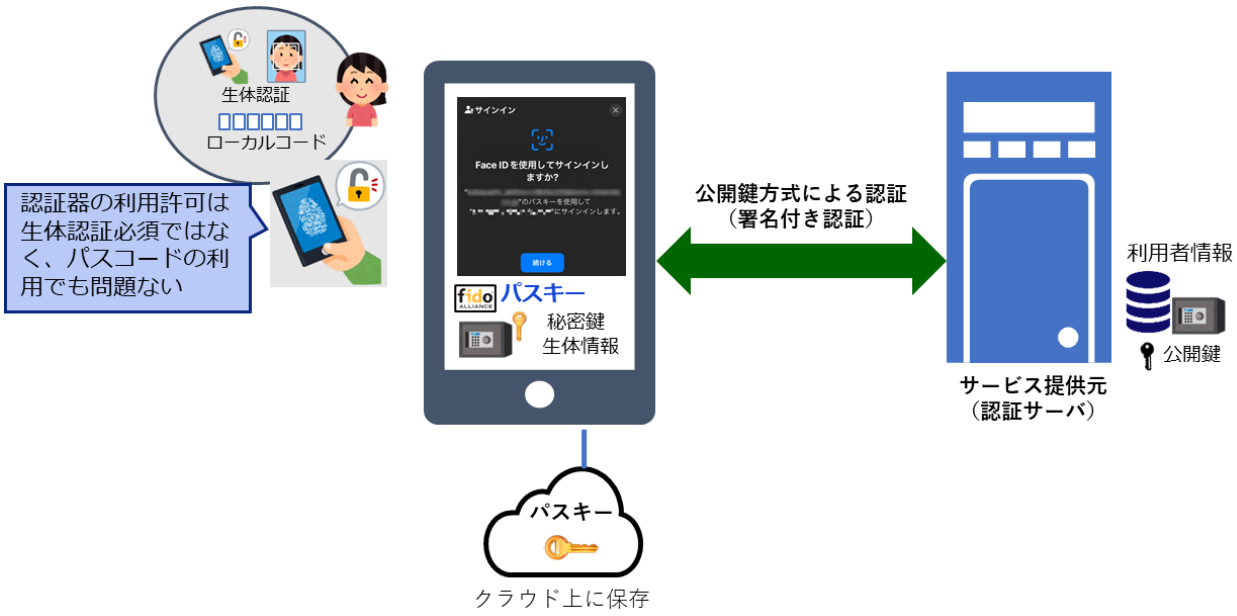
パスキーとは、FIDO2 と呼ばれる技術を利用しており、認証する際に指紋や顔などの生体認証を使うため、「指紋や顔認証によるログイン」、「生体認証によるログイン」などと呼ばれることもあります。

なお、パスキーで利用する生体認証は、「パスキーを使って認証を行ってよいか」を確認するものです。つまり、まるで鍵を使って扉を開けるようなイメージです。

そして実際の認証では、スマートフォンとサーバの間で公開鍵暗号方式と呼ばれる署名検証技術を使って、より高いセキュリティレベルで情報をやり取りします。そのため、パスワードを使わずに安全にサービスにログインすることが可能となります。

さらに、パスキーは、Google Drive や iColud などのクラウド上に保存することで、スマ―トフォンを盗難・紛失してもクラウドのアカウント（Apple ID や Google アカウントなど）を使って復旧することが可能です。また、クラウドを経由して複数のデバイスでパスキーを共有することも可能となっています。しかしながら、クラウドのアカウントが流出するとパスキーも搾取される可能性があるため、クラウドのアカウントは他人に漏れないように厳重に管理することが重要となります。

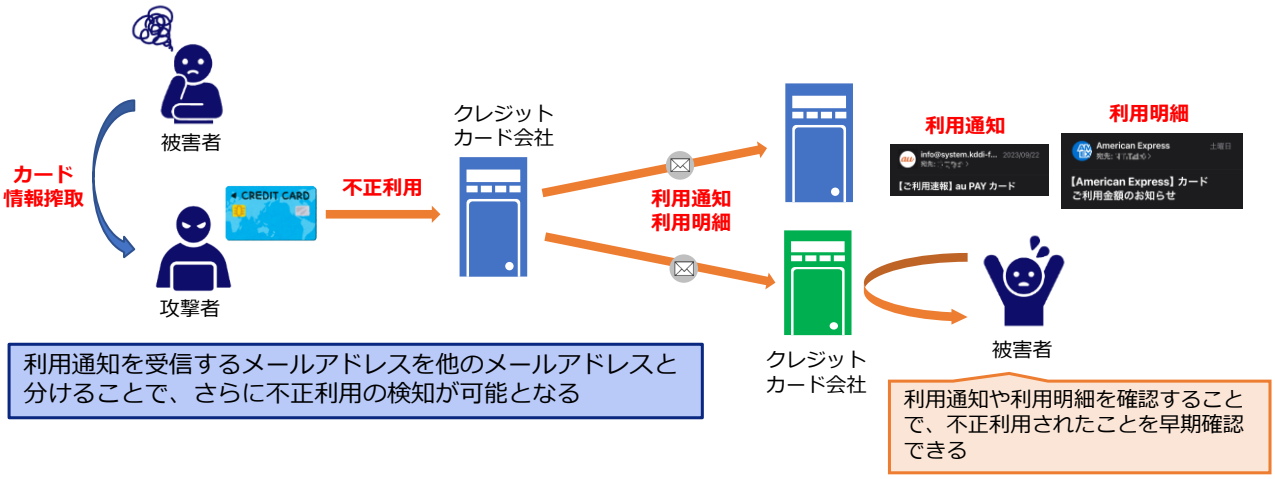
図 3-8　パスキーを使った認証の流れ



3.3.4. 【対策解説】利用履歴の追跡

カードを利用した際に利用通知を設定しておくことで、不正利用を素早く発見できます。不正利用があった場合、リアルタイムで利用通知が送信されるため、利用者は迅速にその内容を確認し、不審な取引を見つけることができます。また、定期的に利用明細を確認することも重要です。これらの手法を組み合わせることで、不正利用に早急に対処することができます（図 3-9　カード利用歴通知によるカード悪用の検知の流れ 参照）。

図 3-9　カード利用歴通知によるカード悪用の検知の流れ



4. おわりに　～　いま私たちにできること

スマートフォンの利活用にあたって、セキュリティを強化しフィッシング被害から身を守るためには、以下の点に留意することが重要です。

1. **リンクは慎重に**:「怪しいリンクはクリック厳禁！」SNS やメールの本文に、ログインや電話を促す内容があったら特に要注意。自信がない場合は絶対にクリックしないで！公式アプリやブックマークから安全にアクセスしましょう。

2. **パスワードマネージャを活用して自動入力**:「パスワードは覚えない！入力しない！」スマートフォンのパスワードマネージャで自動入力しましょう。フィッシンサイトへのパスワード入力予防に役立ちます。

3. **パスワードは自分で作らず自動生成**:「パスワードの生成も、パスワードマネージャにお任せ！」たくさんの複雑なパスワードを作るのは至難の業。パスワードマネージャに任せれば、個別のパスワードを自動生成してくれます。パスワードの使いまわし防止に役立ちます。

4. **不安を感じたら即行動を:**「もしもの時は、パスワード変更＆相談！」不安があったらすぐにパスワード変更しましょう。カードの取引明細等を確認し、怪しい取引や不審な情報を見つけたらサービス提供者（カード会社や銀行など）や公共機関に速やかに相談。被害を最小限に抑えるための手助けが受けられます。

5. **セキュリティ機能をフル活用**:「不正アクセスから身を守るために！」各サービスのセキュリティ機能を使って、アカウントをしっかり守りましょう。たとえば、各サービスで多要素認証やパスキーが利用可能なら、利用しましょう。