フィッシング対策ガイドライン2024の概要と改定ポイント

フィッシング対策協議会 技術・制度検討WG / JPNIC　木村泰司

2023年度フィッシングレポートより

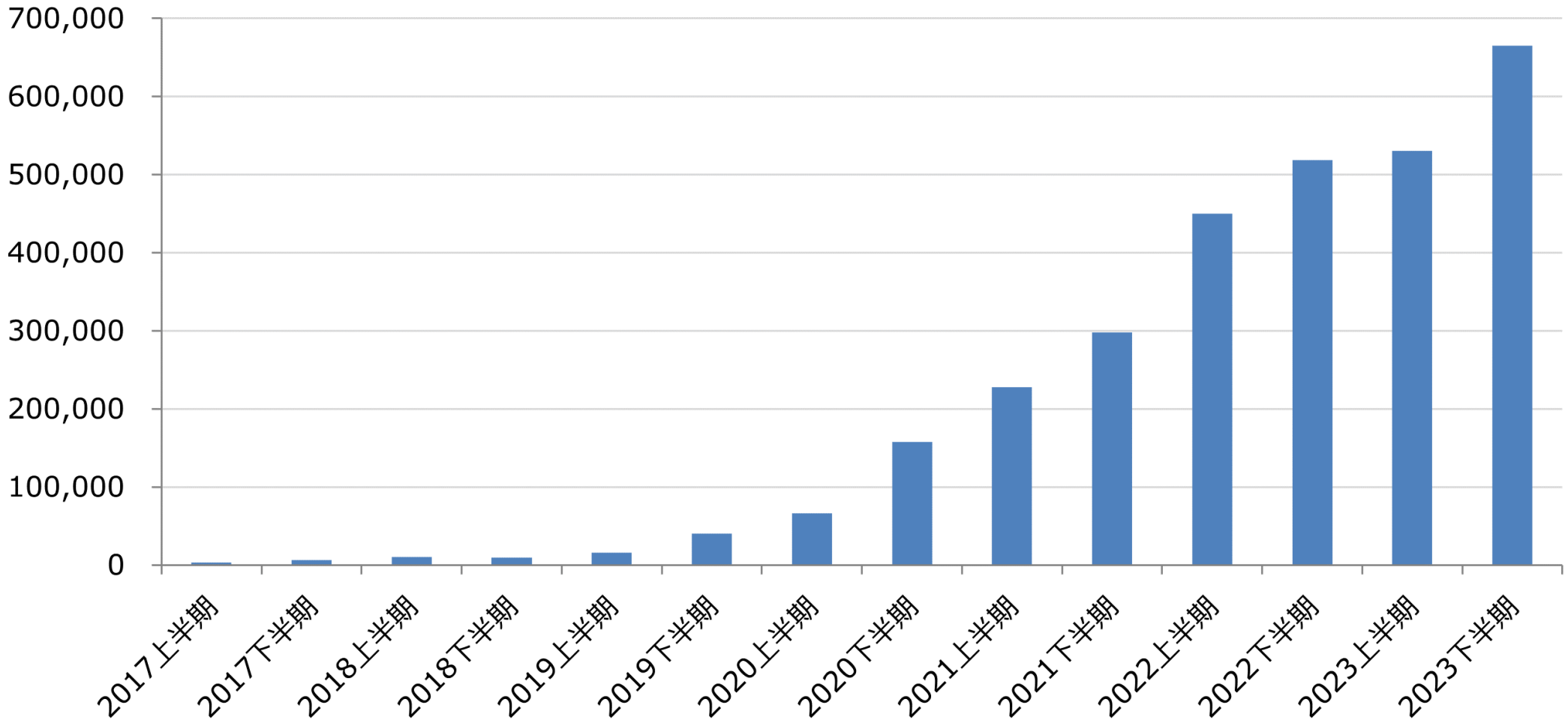

図1-1 国内のフィッシング情報の届け出件数
フィッシング対策協議会、フィッシング報告状況（月次報告書）（閲覧日：2024年2月20 日）より

2023年度フィッシングレポートより

フィッシング情報の届け出件数について、2023年は前年と比較して増加した（図 1-1）。**ECサイト大手、クレジットカード会社**のほか、**マイナポイント事務局など公共サービス、交通系サービス**のなりすましが報告されている。

警察庁の発表 によると、2023年上半期は、ランサムウェア被害の件数が高水準で推移している。また、**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も急増**している。2023年上半期のインターネットバンキングに係る不正送金被害は、**年間の被害件数と比較しても過去最多、被害総額も過去最多に迫る状況**である。

2023年度フィッシングレポートより

APWG（Anti-Phishing Working Group）の調査によれば、2023年のフィッシング届け出件数は、2020年下半期をピークに減少していたが2022年下半期に増加した。**2022年下半期以降は減少傾向にある（図 1-6）**。

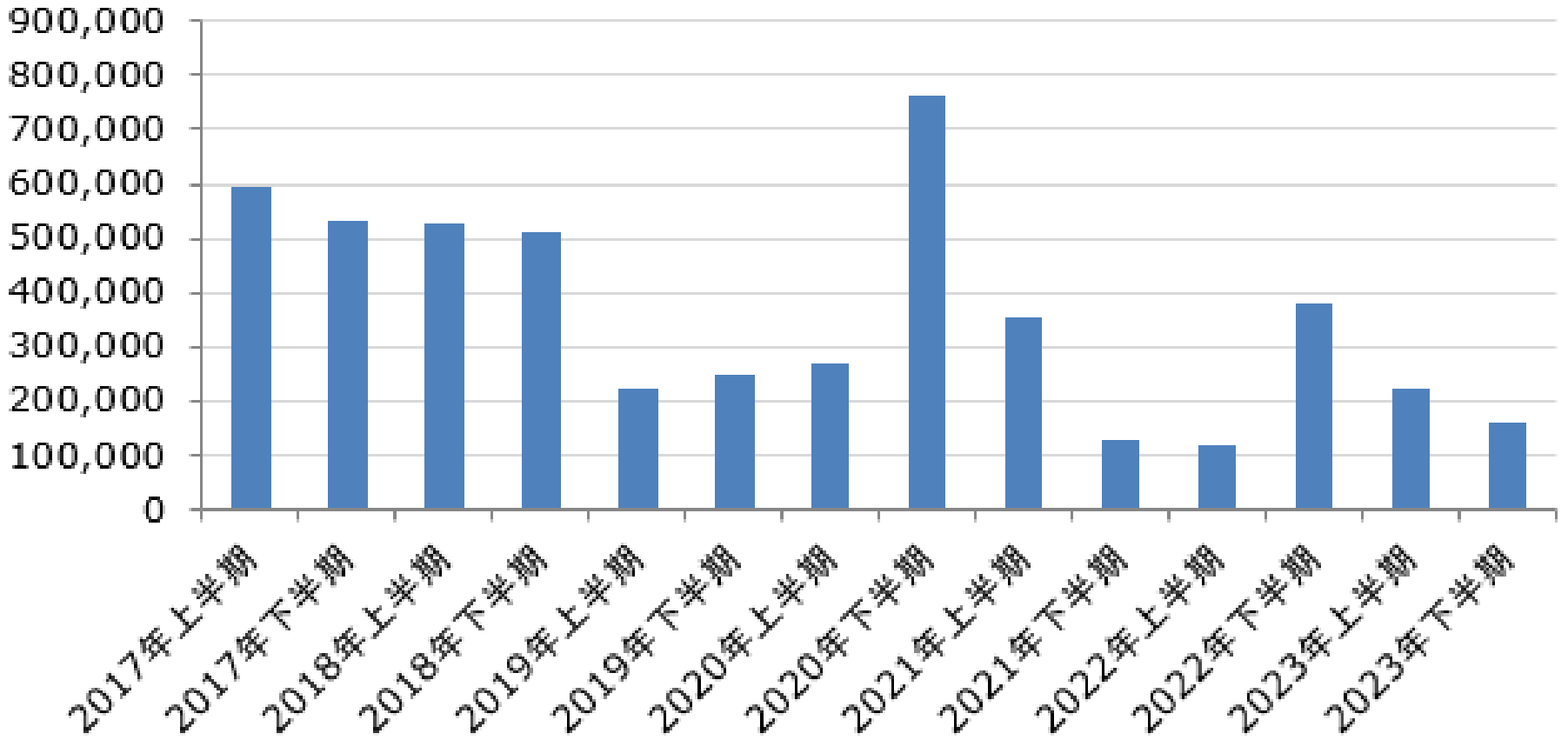

図 1-6　APWG へのフィッシングメール届け出件数[7]

フィッシング対策ガイドライン

フィッシング対策協議会　Council of Anti-Phishing Japan｜報告書類｜ガイドライン
https://www.antiphishing.jp/report/guideline/

フィッシング対策ガイドラインの構成と使い方

第1章　ご説明

改定ポイント１
コンテンツへの動線の見直し

第2章　本WGメンバーによって特に重要として選ばれた「重要５項目」
- Webサイト運営者等、フィッシングに対する対策を事前に行うために

第3章　詳細やより強い対策を講じるための「要件」
- 詳細やより強い対策を講じるための事項

改定ポイント２
情勢を受けた項目の削減

第4章　フィッシング対策マニュアル
- ガイドライン項目を実施するために必要な手順や情報

改定ポイント３
新設

第5章　利用者におけるフィッシング対策
⇒ 利用者向けガイドライン

第6章　付録
- 「プロバイダーへのテイクダウン要請文例」「事業者におけるNG集」「制作・送信に関するガイドラインに含めるべき内容」**「フィッシング対策チェックリスト」**

付録H フィッシング対策チェックリスト

重要項目1	◎	利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること
		□ **メール送信に使うドメイン名についてDMARC等の送信ドメイン認証技術を導入している(必須)。** □ VMC等の**ブランドアイコンが表示される仕組みを導入している(推奨)**。 □ **送信メールの送信者が正規かどうかが分かる**ようにS/MIMEを導入している(推奨)。
重要項目2	◎	利用者に送信するSMSにおいてはなりすましが起きにくいサービス（国内で直接接続される送信サービス等）を利用し、発信者番号を利用者に告知すること
		□ 使っている**発信者番号を利用者に告知している(必須)**。 □ **なりすましが起きにくいSMSサービスを利用している(推奨)**。
重要項目3	◎	複数要素認証を要求すること
		□ **複数要素認証を採用している(必須)**。 □ **資産の移動（振り込み等）の実行前に再認証**を行っている(推奨)。
重要項目4	◎	ドメインは自己ブランドと認識して管理し、利用者に周知すること
		□ 自組織に割り当てられている**ドメイン名を把握している(必須)**。 □ **ドメイン名のライフサイクル管理**をしている。ドロップキャッチの対策をしている(必須)。 □ ある**部署もしくは発注先などによって勝手にドメイン名が設けられたり使われたりしないように管理**している(必須)。 □ 利用者に**サービスで使っているドメイン名を周知**している(推奨)。
重要項目5	◎	フィッシングについて利用者に注意喚起すること
		□ **フィッシング詐欺が起きている場合にはその旨を周知**している(必須)。 □ フィッシング詐欺についての**注意喚起を行うWebページ等**を設けている(推奨)。

利用者が正規メールとフィッシングメールを判別可能とする対策（参照：3.3.1）

要件1	◎	利用者が確認できるように利用環境と分かりやすい説明に配慮した上で、どのように確認すればいいのかを分かりやすく端的に説明すること。
		□ **利用者が正規メールと判別できる**ようにBIMI等のブランドのロゴや公式マーク、S/MIMEを使った電子署名を施すなどしている。**なりすましメールが送られているときに利用者が判別できる**ようにしている。 □ どのように**確認すればいいのかを説明**している。
要件2	◎	外部送信用メールサーバーを送信ドメイン認証に対応させること
		□ 外部送信用のメールサーバは**SPF、DKIM、DMARC等の送信メールドメイン認証技術に対応**している。 □ BIMIを導入している。
要件3	◎	利用者へのメール送信では、制作・送信に関するガイドラインを策定し、これに則って行うこと
		□ **社内や組織内でメール作成に関するガイドラインを策定**している。
要件4	◎	利用者に送信するSMSには国内直接接続の配信、または、RCS準拠サービスを利用すること
		□ **SMSには国内直接接続の配信、または、RCS準拠サービスを利用**している。

フィッシング被害を拡大させないための対策（参照：3.3.3）

要件5	◎	利用者が安全にサービスを利用する環境を整えるように促すこと
		□ **メールやSMSに記載されたURLもしくは検索結果のURLを利用させない、それを前提としない**形を取っている。 □ 利用者には正規のWebサイトであることを確認頂いた上で**ブックマーク**して頂くようになっている。
要件6	◎	**複数要素認証を要求すること**
		□ ワンタイムパスワードといった所有認証、指紋や顔認証といった生体認証を組み合わせた複数要素認証を求めるようにしている。 □ ポイントや資産の移動操作実行時には複数要素認証を求めるようにしている。
要件7	◎	**資産の移動に限度額を設定**し、変更・移動時は通知を行うこと
		□ 資産の移動機能（ポイント交換や他金融機関への振込み、商品の購入など）については上限を設け、制限を超えた時には利用者に連絡するようになっている。 □ **資産の移動等が行われたときに利用者に通知**を行っている。
要件8	◎	利用者の通常とは異なるアクセスや登録情報の変更や登録情報の変更に対しては**追加のセキュリティを要求する**こと
		□ 利用者の通常とは異なるログインや登録情報の変更が行われる場合には、第二認証や第三認証を求めるようにし、次の操作に進めないようにしている。
要件9	○	重要情報の表示については制限を行う
		□ クレジットカード番号やデビットカード番号は下4桁など一部だけの表示に留めている。
要件10	◎	不正利用も含めた**アクセス履歴の可視化**
		□ 利用者がそのサイトへの過去のアクセス履歴（複数回）を確認できるようにしている。 □ アクセス履歴にはユーザアクション、接続時刻、接続時間、接続端末（PC、スマートフォンなど）およびアクセス元IPアドレスを含む。

ドメイン名に関する配慮事項（参照：3.3.4）

要件11	◎	ドメイン名を自社のブランド戦略の一貫として考えること
		□ **ドメイン名の管理を内部統制**のプロセスの中に含めている。 □ Webサイトで用いるドメイン名および**送信するメールの送信者アドレスのドメイン名は同一**である(推奨)。
要件12	◎	使用するドメイン名と用途の情報を利用者に周知すること
		□ フィッシング対応を行う国内外のベンダー、調査機関、事業者、アナリスト等に向けて、**正規ドメインと用途（サービス名）を示している**。 □ サービスとは違うドメイン名を使用する場合は送信ドメイン認証技術でドメイン名を保護している。
要件13	◎	**ドメイン名の登録、利用、廃止にあたっては、自社のブランドとして認識**して管理すること
		□ ドメイン名管理のためのルール・手順を社内で確立している。

フィッシングへの備えと発生時の対応（参照：3.3.5）

要件14	◎	フィッシング対応に必要な機能を備えた組織編制とすること
		□ 事前準備、**役割分担および連絡・レポート体制を明確化**している。 □ フィッシング被害が発生してしまった際の**行動計画（対応フロー）を策定**している。 □ フィッシングについて組織内で連絡や連携が取れるようになっている。 □ サービス運用部門と協力し、ログなどの分析結果からの**状況把握と対策の効果測定**を行っている。
要件15	◎	フィッシング被害に関する対応窓口を明記すること
		□ 利用者からの情報提供を受ける**フィッシング報告窓口**を設けており、利用者のために明記している。 □ 利用者に多大な被害が及ぶサービス（金融系、クレジットカード系、キャッシュレス決済サービス等）の場合、アカウントの利用制限（停止）依頼や事故の被害を報告できる24時間受付窓口を設置している。
要件16	◎	フィッシングの手法および対策に関わる**最新の情報を収集**すること
		□ 情報サイトのセキュリティコーナーやウイルス情報のサイトを確認している。
要件17	◎	フィッシングサイトへの**対応方法を整備**しておくこと
		□ URLフィルターの申告方法（テイクダウンよりも即効性が期待できるため）を定めている。 □ テイクダウンのアプローチ方法（自社、社外業者）を定めている。 □ 発生中のフィッシングサイトを利用者に注意喚起する実施手順を定めている。

利用者への啓発（参照：3.3.6）

要件18	◎	利用者が実施すべきフィッシング対策啓発活動を行うこと
		☐ 正規のメールおよびSMSか否かを判断する助けとなるよう**フィッシングに関する注意喚起や啓発**を行っている。 ☐ 正規メールのみに表示されるアイコンなど「見てわかる」方法を中心に、**図やスクリーンショット、漫画などで分かりやすく表現**している。
要件19	◎	フィッシング発生時の利用者への連絡手段を整備しておくこと
		☐ フィッシングが発生したときに**WebやSNSなどに注意喚起を掲載**できるようになっている。 ☐ SNSでの通知のために**公式アカウントを取得**している。 ☐ 通知のできる**公式アプリを採用**している。

フィッシング被害の発生を迅速に検知するための対策（参照：3.4）

要件20	○	Webサイトに対する不審なアクセスを監視すること
		□ **ログインの失敗が多発するなど不審なアクセスを監視**している。 □ 自社のサイトを構成する以下の資産に対して異なるドメイン名からの参照が行われていないかを監視している。
要件21	◎	フィッシング検知に有効なサービスを活用すること
		□ インターネット上の不正活動を24時間体制でモニタリングし、**URLフィルターへの登録やテイクダウンを行う商業サービスを利用**している。 □ 事業者特有の文字列を含むドメイン名の事業者以外からの登録状況のモニタリングや検知・通知サービスを活用している。
要件22	◎	**DMARCレポートやバウンスメールを監視**している。
		□ DMARCレポートを収集・分析し、自社ドメインがなりすましをされているか、また、されていた場合のメール送信元のサーバーや配信規模を把握できるようになっている。 □ DMARC未対応の場合は、バウンスメールを監視し、フィッシングの兆候を検出できるようになっている。

ご意見をお寄せください。