2020年の情報セキュリティ動向

石井 泰鷹 ●一般社団法人JPCERTコーディネーションセンター 早期警戒グループ 脆弱性アナリスト

COVID-19を題材としたフィッシングに加え、Emotetの感染やSSL-VPNのアカウント情報公開など、組織活動に影響を与えるインシデントが複数確認された。

■インシデントの報告件数

2020年1～12月にJPCERTコーディネーションセンター（JPCERT/CC）に報告されたコンピューター・セキュリティ・インシデント（以下、インシデント）の件数は4万3823件（前年は1万8700件）であった（資料4-1-1）。中でも「フィッシングサイト」の報告は前年と比較して84%と、大幅に増加した（資料4-1-2）。また、2019年と同様に国内ブランドを装ったフィッシングサイトが多く見られた。

■個人ユーザーを対象とした攻撃

●実在する組織を装った偽サイトへ誘導するメッセージ

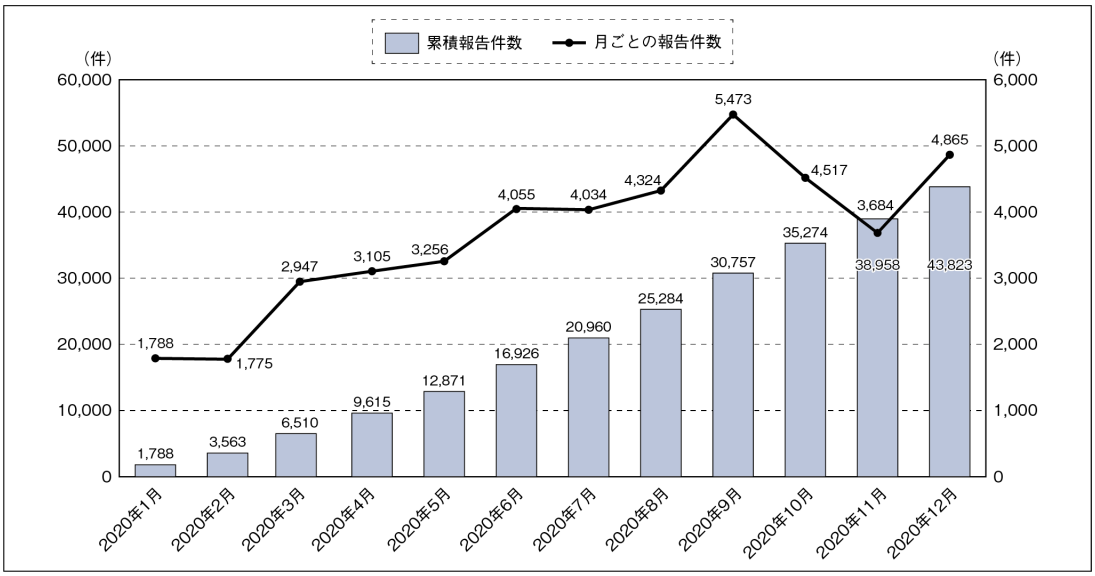
2020年も前年に引き続き、実在する組織を装ってメールやSMSでメッセージを送り付け、フィッシングサイトへ誘導する攻撃が多数報告された。この攻撃では、ユーザーがメッセージ内に記載されたリンクにアクセスすると、攻撃者が用意したフィッシングサイトへ誘導される。誘導先のウェブサイトでは、登録情報（IDやパスワードなど）をはじめその他の個人情報を入力させ、窃取しようとする。不正なアプリケーションのダウンロード案内が表示されるケースも確認されている。

フィッシング対策協議会の報告によると、フィッシングサイトの特徴として、一度に複数取得したとみられるドメインが使用されるケースや無料のダイナミックDNSサービスを使用したケースがみられた。そうしたサービスを用いてメールごとに、または短時間で誘導先のURLが変えられていたため、フィッシングサイトの報告数が増加した。こうしたウェブサイトは、数回のアクセスでアクセス不能になったり、短時間で停止することが多かったりすることが確認されている[1]。これは、セキュリティベンダーなどからの調査やフィッシングサイトと認識されることにより、攻撃の成功確率が低下することを避けるための手口だと考えられる。

新型コロナウイルス感染症（COVID-19）を題材にし、給付金やマスク販売などをかたったフィッシングサイトが登場したことも、2020年の世相を反映した攻撃であった。こうしたウェブサイトについて金融庁などから注意喚起が出されている[2]。COVID-19に限らず誰もが興味を持つ内容が悪用されるケースがあることを、インターネット利用時や受信メッセージの確認時には注意したい。

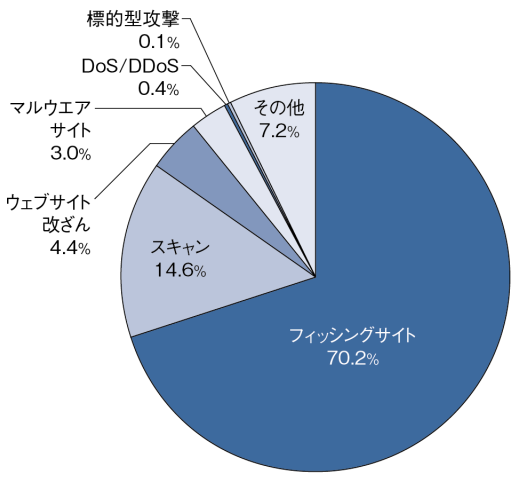
2020年12月には、内閣府消費者委員会から「フィッシング問題への取組に関する意見」が公表された[3]。対策に取り組む関係省庁である警察庁、総務省、経済産業省、消費者庁に対して、

資料4-1-1　インシデント報告件数の推移（2020年1～12月）



出典：JPCERT/CC、「インシデント報告対応レポート」（https://www.jpcert.or.jp/ir/report.html）

資料4-1-2　インシデント報告件数のカテゴリ別内訳（2020年1～12月）



フィッシング	19,961件（＋9,104件）	↗
スキャン	4,161件（　－891件）	↘
ウェブサイト改ざん	1,261件（　＋248件）	↗
マルウエアサイト	865件（　－37件）	↘
DoS/DDoS	104件（　＋74件）	↗
標的型攻撃	34件（　＋15件）	↗
制御システム関連	0件（　0件）	→
その他	2,061件（　－369件）	↘

※（）内の数値は前年同期間からの変動値

出典：JPCERT/CC、「インシデント報告対応レポート」（https://www.jpcert.or.jp/ir/report.html）

フィッシングメールの受信防止対策の普及促進、および効果検証や不正アクセス禁止法などに基づく取り締まりの強化など、フィッシング対策に関する意見が示された。

■法人や組織を対象とした攻撃

●マルウエアの動向

2019年に引き続き、マルウエア「Emotet」に感染させる大規模な攻撃活動が国内外問わず観

測された。感染手段としては、実在する組織や人物になりすまして発信したメールに添付されたWordファイルのマクロ機能が使用されることが多い。さらに、他のマルウエアに感染させるダウンローダーとしての役割など、Emotetはさまざまな機能を有している。具体的には、マルウエア「TrickBot」「Qbot」などに感染させ、最終的にランサムウエアに感染させるといった攻撃が確認されている。

2020年2月にEmotetの配布活動はいったん停止したが、同年7月に再開された（資料4-1-3）。配布停止期間中に機能拡充をしたとみられ、その一例としてメール本文の取得サイズの上限が16KBから無制限になったと報告されている[4]。さらに、配布再開後は感染拡大の手口が巧妙化している。たとえば、感染用のWordファイルを正規のメールから窃取したファイルと共に添付して送付する事例や、パスワード付きzipファイルに圧縮し送付することでウイルススキャンの回避を試みたと思われる事例などが観測されている[5]。

2020年10月に、Emotetと同様にメールを感染手段とするマルウエア「IcedID」のメール配布が広範囲に観測された[6]。

こうしたマルウエアの感染を予防するためには、組織内への注意喚起やセキュリティ製品の定義ファイルを定期的にアップデートするなど、基本的なセキュリティ対策が重要である。また、2020年も多数観測されたランサムウエアによる被害を最小化するために、異なるネットワークや物理的に影響を受けない場所に複数世代のバックアップを取得しておくことも有用な対策である。

●標的型攻撃

2020年も標的型攻撃が相次いだ。国内の組織を標的とした標的型攻撃に関連したインシデントは、JPCERT/CCに合計34件（2019年は19件）報告された。

2020年7月には、Lazarusと呼ばれる攻撃グループが国内外のさまざまな業界に対する標的型攻撃を行ったとの報告があった。Lazarusは、複数のマルウエアやツールを利用している。たとえば、横断的侵害にはファイル操作やシェルコマンド実行などの機能を持つマルウエア「BLINDINGCAN」[7]やWindows実行ファイル化したSMB経由でリモートホストにアクセスするPythonツールを使用していることが確認されている[8]。

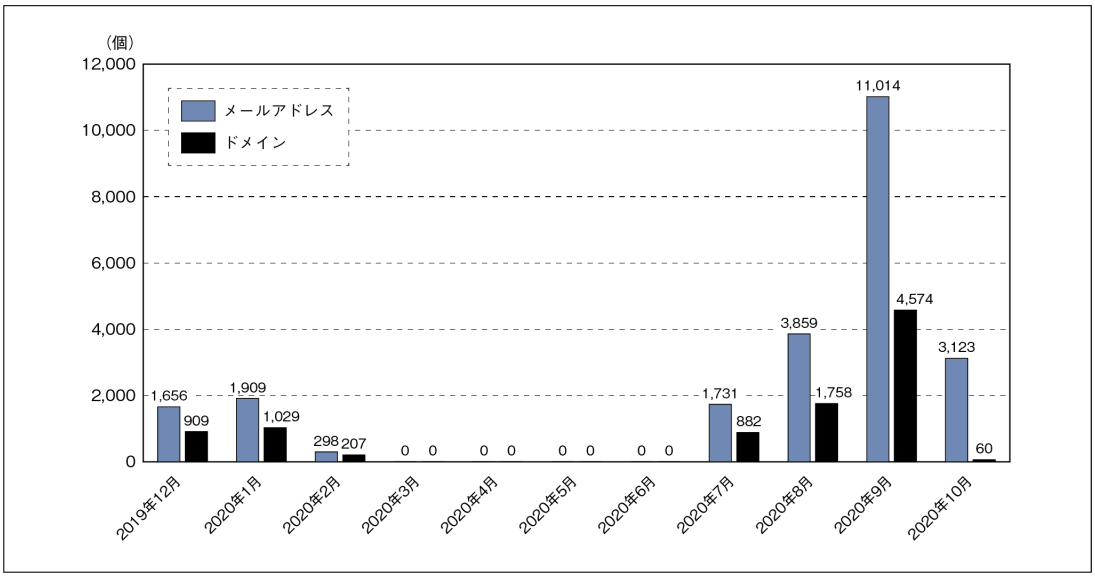
標的型攻撃は攻撃手口が巧妙で、侵入を完全に防ぐことは難しい。侵入されることを前提に、早期に検知するための日頃からの備えが重要だ。具体的には、まずは自組織における各種ログ（ProxyやFirewall、Active Directoryなど）の定期的な調査や端末の管理状態の確認など、システムの利用状況を把握する。また、発生したインシデントに対処するためにCSIRTをはじめとした社内体制の整備やJPCERT/CCなど外部組織との連携について検討を行い、サイバー攻撃への備えを進めていただきたい。

●機器の脆弱性を悪用し窃取した認証情報の公開

複数のネットワーク製品において、SSL-VPN機能に内在する脆弱性の悪用が2019年に引き続き確認された。2020年8月、米パルスセキュア製のPulse Connect Secureの脆弱性（CVE-2019-11510など）を悪用して取得したとみられるユーザーの認証情報が公開されていたことが報道された。同年10月には、米フォーティネット製品に関連したユーザー認証情報の公開が確認されている[9]。上記の公開された情報に掲載されている国内の組織に対して、JPCERT/CCは通知および対策の実施依頼をしている。

上記の脆弱性はいずれも2019年前半に公表さ

資料4-1-3　Emotetに感染しメール送信に悪用される可能性のある.jpドメインのメールアドレスの推移



出典：ばらまきメール回収の会のデータを基にJPCERT/CCが作成

れたものであり、製品ベンダーや専門機関からの脆弱性情報や注意喚起がユーザーに届いておらず、対策が実施されていないケースが少なくない実情が見えた。

脆弱性の放置は時として大きなインシデントに発展するケースが考えられるため、アップデートや回避策の速やかな適用が望ましい。さらに、普段からバージョンを含め利用製品を把握し、管理者を定めて不具合時の影響の範囲などを認識するとともに、バージョンアップ体制・手順などを整理し、新たに公表される脆弱性情報に備えることが不可欠である。ネットワーク構成の検討やアクセス制限など、ネットワーク上での基本的な対策も重要である。

■社会・インターネット基盤に影響する攻撃

●ドメイン名登録情報に対する攻撃

サブドメインの乗っ取りや、ドメイン改ざんが行われた事例も確認された。たとえば、Subdomain Takeoverと呼ばれる攻撃により、被害企業が過去に利用していたと思われるサブドメインへのアクセス時に、当選詐欺のウェブページが表示されるといったものが複数報告された[10]。CNAMEレコードを利用してサブドメインの参照をCDNサービスのドメインに転送設定していたが、その後、CDNサービス契約を解除し放置されているドメインに対して、この攻撃手法が使われる。攻撃者が、その放置されたドメインでCDNサービス契約をすることで乗っ取りが可能となる。

ほかにも、仮想通貨事業者を狙ったドメイン改ざん事案も複数報じられている。たとえば、利用しているドメイン登録サービスの管理ツールの脆弱性を悪用して管理者アカウントを乗っ取り、NSレコードやMXレコードが改ざんされる事例が公表された。

Subdomain Takeoverを防ぐために、CDNサービスの解約時には設定したCNAMEレコードの削

除も忘れずに実施することが必要である。ドメイン改ざんに対しては、DNSサーバーの設定やドメイン名の定期的な監視、ドメイン管理者アカウントの認証に多要素認証を用いるなどの検討が重要である。

●DDoS攻撃による脅迫

2020年も、DDoS攻撃の実施停止と引き換えに仮想通貨による送金を要求する脅迫行為が国内外で確認された[11]。標的になった対象は、2019年は金融機関のみだったが、2020年はそれ以外の組織にも広範囲に拡大した。要求に応じないまま支払期限を過ぎてもDDoS攻撃が行われない事例もある一方で、脅迫メールを受信後、即座にDDoS攻撃が行われたケースを複数確認している。

こういった攻撃に備えて、攻撃発生時の対応手順や体制、利用している対策サービスの状況を確認しておくことを推奨する。脅迫を受けた場合には、安易に攻撃者の要求には応じず、冷静に対応することも心掛けたい。

1. 2020/04 フィッシング報告状況（フィッシング対策協議会）（https://www.antiphishing.jp/report/monthly/202004.html）
2. 新型コロナウイルスに乗じた犯罪にご注意ください！（金融庁）（https://www.fsa.go.jp/news/r1/ginkou/20200407/20200407.html）
3. フィッシング問題への取組に関する意見（内閣府）（https://www.cao.go.jp/consumer/iinkaikouhyou/2020/1203_iken.html）
4. Emotet Trojan Begins Stealing Victim's Email Using New Module（Bleeping Computer）（https://www.bleepingcomputer.com/news/security/emotet-trojan-begins-stealing-victims-email-using-new-module/）
5. マルウェアEmotetの感染拡大および新たな攻撃手法について（JPCERT/CC）（https://www.jpcert.or.jp/newsflash/20200090401.html）
6. 緊急セキュリティ速報：マルウエア「IcedID」に注意（トレンドマイクロ）（https://www.trendmicro.com/ja_jp/about/announce/announces-20201110-01.html）
7. 攻撃グループLazarusが使用するマルウェアBLINDINGCAN（JPCERT/CC）（https://blogs.jpcert.or.jp/ja/2020/09/BLINDINGCAN.html ）
8. 攻撃グループLazarusがネットワーク侵入後に使用するマルウェア（JPCERT/CC）（https://blogs.jpcert.or.jp/ja/2020/08/Lazarus_malware.html）
9. Fortinet社製FortiOSのSSL VPN機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について（JPCERT/CC）（https://www.jpcert.or.jp/newsflash/20201012701.html）
10. JPCERT/CCインシデント報告対応レポート2020年7月1日～2020年9月30日（JPCERT/CC）（https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf）
11. DDoS攻撃を示唆して仮想通貨による送金を要求する脅迫行為（DDoS脅迫）について（JPCERT/CC）（https://www.jpcert.or.jp/newsflash/2020090701.html）
New Zealand Stock Exchange suffers day four disruption following DDoS attacks（ZDNet）（https://www.zdnet.com/article/new-zealand-stock-exchange-suffers-day-four-disruption-following-ddos-attacks/）

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2021年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp