2019年の情報セキュリティ動向

安部 広夢 ●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

金融機関を騙るフィッシングメールおよびSMSによる不正送金被害の急増、サイバー攻撃における継続したランサムウエアの悪用のほか、脆弱性を悪用した攻撃事例が複数確認された。

■セキュリティインシデントの報告件数

2019年1月から12月までに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1万8070件（前年は1万5751件）であった（資料4-1-1）。前年と比較して、「スキャン」および「ウェブサイト改ざん」の報告件数が減少した一方で、「フィッシング」の報告が増加した（資料4-1-2）。フィッシングサイトの報告件数は前年比50％の増加になっており、中でも、国内ブランドを装ったフィッシングサイトの増加が顕著だった。

■個人ユーザを対象とした攻撃

●実在する組織から送られたメッセージを装った偽サイトへの誘導

2019年も2018年に引き続き、実在する組織を装ってメールやSMS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、ユーザがメールやSMS本文中に記載されたリンク先にアクセスすると、攻撃者によって準備されたフィッシングサイトへ誘導される。誘導されたフィッシングサイトにおいてアカウントやパスワードなどの情報を入力すると、攻撃者に入力した情報が窃取される。フィッシングサイトは半数近くがHTTPSに対応していたり、正規サイトで使用されているドメイン名のドットをハイフンに置き換えたりするなど巧妙に似せているケースが多かった。

また、フィッシングによって窃取されたアカウント情報を悪用したとみられる不正送金が2019年9月ごろから急増し、各銀行などが注意喚起[1]を出した。警察庁の注意喚起[2]によると、8月まで毎月の不正送金被害額は約6,700万円以下で推移していたが、9月に4億円を上回り、その後も月を追って増加した。

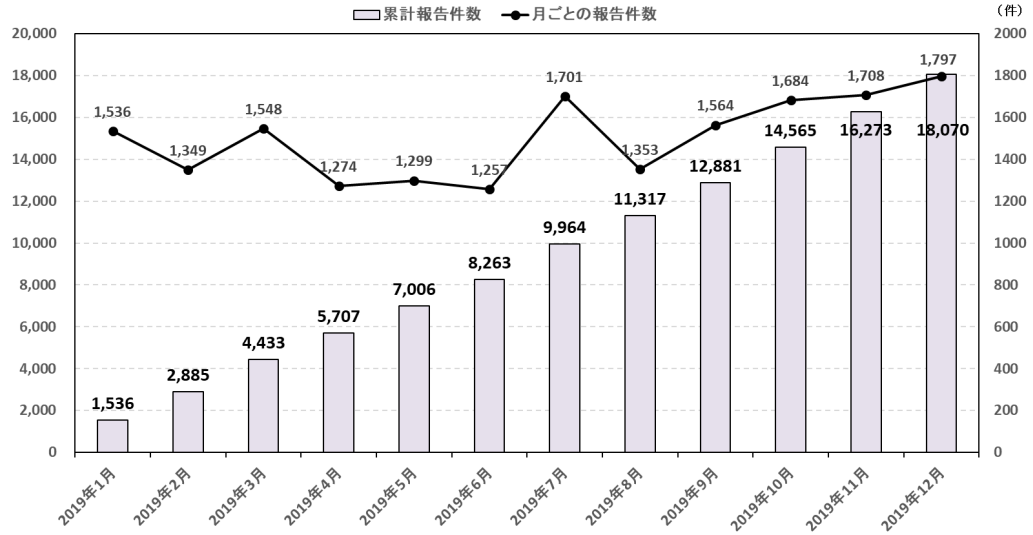
こうした被害にあわないよう、来るはずのないメールやSMSを疑ってかかり、受信したメッセージ中のURLをクリックせず、メッセージ内容を確認する必要がある場合は、メールやSMS本文中に記載されているURLを使わず、あらかじめ確認してブックマークした正規のURLや正規のアプリを使うように心掛けたい。

■法人や組織を対象とした攻撃

●マルウエアの動向

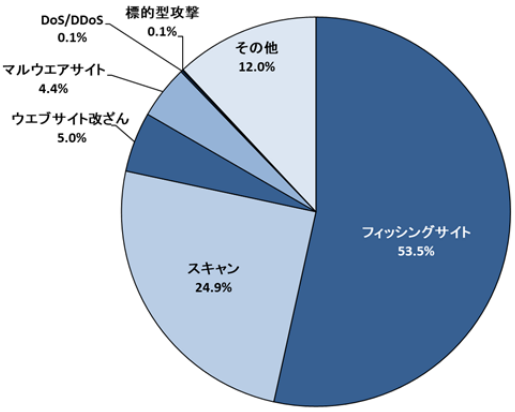
2017年にランサムウエアWannaCryに感染する被害が日本国内でも多く見られた。その後、様々なランサムウエアが新たに確認されている。2019年ではGandCrabやSodinokibi、Ryukなど

資料4-1-1　インシデント報告件数の推移（2019年1～12月）



出典：「JPCERT/CC インシデント報告対応レポート」をもとに作成（インシデント報告対応レポート（JPCERT/CC、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（2019年1～12月）



フィッシング	10,857件（+5,857件）	↗
スキャン	5,052件（－ 887件）	↘
ウェブサイト改ざん	1,013件（－ 42件）	↘
マルウェアサイト	902件（+ 576件）	↗
DoS/DDoS	30件（+ 12件）	↗
標的型攻撃	19件（－ 7件）	↘
制御システム関連	7件（－ 70件）	↘
その他	2,430件（－ 548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」をもとに作成

のランサムウエアが観測され、継続してランサムウエアが攻撃に使用されることが確認された。また、以前から確認されていた感染力の高いマルウエアEmotetが、ランサムウエアと併用されるよう

になり、結果的にランサムウエアの被害を拡大した。Emotetは2019年で最大級の脅威となった。

ランサムウエアGandCrabは2018年1月に初めて観測され、復号ツールが公開されるとすぐに対抗したバージョンが開発されるなどし、2019年末までに5回バージョンアップされた。2019年1月に観測された事例においては、スパムメールに画像ファイルを装ったZipファイルが添付されており、Zipファイルに格納されているファイルに記載されたJavaScriptを実行することでGandCrabなどのマルウエアがダウンロードされる。また、スパムメールは当初、件名が「Love you」などであったが、その後、日本の芸能人の名前など日本人が関心を持つ件名へと変化した。スロバキアのセキュリティ企業ESET社の調査[3]によると、2019年1月頃時点では、ESET社製品によるGrandCrabに関連するスパムメールの検知数の95%が日本国内でのものだった。その後、2019年6月にはGandCrabの製作者が、十分な収入を得られたとの理由で活動停止を発表[4]した。

2019年4月頃には、新しいランサムウエアであるSodinokibiの情報[5]がシスコ社から公開された。Sodinokibiは、コードや、ファイル暗号化後に生成されるランダムなURLの生成方法などにおいてGandCrabと類似しているとの指摘がある。感染経路は、GandCrabと同様にメールが使用されるほか、Oracle Weblogicの脆弱性（CVE-2019-2725）を悪用する攻撃や、RDP（Remote Desktop Protocol）を介してネットワークにアクセスし、ハッキングしたMSP（Managed Service Provider）コンソールを使用して展開するなどのケースが確認されている。日本でも、2019年7月にカスペルスキー社が感染を確認したとの情報[6]を公開し、感染させようとしたインシデント事例をJPCERT/CCでも確認した。

2019年10月頃には、マルウエアEmotetが国内外問わず多数観測され、JPCERT/CCにおいてもEmotetの感染に関する相談を多数受けた。Emotetの感染経路として、実在の組織や人物になりすましたメールに添付されたWord文書ファイルが使用されるケースが多い。また、多くの日本企業からEmotetに感染したことが原因と思われるなりすましメールの送信に関する注意喚起が公開され、急激に感染が広がっている様子が確認された。Emotetは2014年ごろから確認されており、当初はオンラインバンキングマルウエアとして認知されていた。2018年頃より、感染した端末のメールアカウントなどを窃取し、そのアカウントになりすましてメールを送信することで感染を拡大させるようになった。さらに、2019年においては他のマルウエアに感染させるダウンローダとしての役割など、様々な機能を有するようになった。たとえば、Emotetによりマルウエアtrickbotなどに感染させられ、結果としてランサムウエアRyukに感染するなどの挙動[7]が確認された。

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の基本的なセキュリティ対策が重要となる。また、2019年も多数観測されたランサムウエアなど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の受けない場所にデータのバックアップデータの取得および世代管理をすることも重要となる。

●標的型攻撃

2019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報告がJPCERT/CCに合計19件（前年は26件）寄せられた。

2019年6月には仮想通貨事業者を狙ったと考

えられる標的型攻撃の報告があった。この攻撃にはメールが使用され、メールに含まれた短縮URLのリンクをクリックするとクラウドサービスからZipファイルがダウンロードされる。ダウンロードされたZipファイルに格納されたショートカットファイルに指定した短縮URLにアクセスさせるコマンドが含まれており、ユーザがこのショートカットファイルを開くことでコマンドが実行されてマルウエアに感染する。

標的型攻撃では、用いられるマルウエアや侵入手口が標的組織ごとにカスタマイズされているため、一般化された方法で攻撃を検知することは難しい。FireEyeの調査[8]によると、アジア太平洋地域におけるセキュリティ侵害の発生から検知までに要した日数の中央値は2018年において204日（2017年は498日、2016年は172日）だった。前年度の統計から改善されているものの、検知までに半年以上の時間を要している。

そのため、すでに侵入されている可能性を念頭に、早期検知に配慮した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、運用状況の把握が重要である。また、発生したセキュリティ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を行い、サイバー攻撃への備えを進めていただきたい。

●脆弱な製品に対する攻撃の事例

2019年も脆弱性情報は多数公表されており、ベンダーや調整期間による公表後すぐに攻撃に悪用されるケースも確認された。また、また、セキュリティアップデートなどの対策なしに脆弱性が長期間放置され、それに対する攻撃を受けて被害に到った複数の事例も確認された。

2019年1月に特定のホスティングサービスを利用している5000近いWebサイトが改ざんされた。このホスティングサービスは共有型サービスであり、改ざんの手口は特定の利用者が設置したWordPressのアカウントが容易に推測可能だったため攻撃者に踏み台とされ、WebサーバのOSの脆弱性が悪用された不正アクセスだったと公表[9]された。

次に、2019年10月にはウイルスバスターコーポレートエディションに対する攻撃事例に関連した注意喚起[10]がトレンドマイクロ社から出された。法人向けに提供されている製品であり、影響範囲を考慮しJPCERT/CCでも注意喚起[11]を公開した。

さらに、2019年5月ごろにマイクロソフト社から注意喚起があったリモートデスクトップサービスの脆弱性や、2019年9月ごろにJPCERT/CCが注意喚起[12]を公開したSSL VPN製品の脆弱性が同年9月から11月ごろにかけて悪用されたことが確認[13]された。

本項で記載した脆弱な製品に対する攻撃のうち、ウイルスバスターコーポレートエディションの脆弱性に関しては、情報が公表されてからすぐに攻撃の悪用が確認された。また、その他の脆弱性に関しては、脆弱性情報およびセキュリティアップデートが公開されてから約半年以上の時間が経過してから攻撃に悪用され、被害にあったケースが確認された。

脆弱性への対策の基本はセキュリティアップデートである。しかし、アップデートを適用する前に検証を行うなど、時間を要する場合には、暫定的な回避策を講じる必要がある。また、セキュリティ製品の導入や、アクセス制限をするなど基本的な対策とともに、セキュリティアップデートの運用ポリシーなどを定め、早期にセキュリティアップデートが実施できる体制を築くことが重要となる。

●サイバー攻撃をにおわせた脅迫

2019年もサイバー攻撃をにおわせた脅迫が確認された。2018年は主に個人ユーザを対象とし「漏洩した秘密情報を公開されたくなければ金を払え」と仮想通貨を要求する脅迫メールだったが、2019年においては2017年に見られた金融機関を対象とした「DDoS攻撃をされたくなければ金を払え」と仮想通貨を要求する脅迫メールが再び確認された。

2017年に確認された仮想通貨を要求する脅迫メールはArmada Collectiveを名乗る攻撃グループから主に中国や韓国の金融機関に対して送信された。実際に、攻撃グループが指定した支払い期限の前や当日にメールを受信した組織に対して最大で40Gbps程度のDDoS攻撃が行われるケースが確認[14]された。観測した攻撃はNTP Amplification、TCP SYN Flooding、ICMP Floodingなど一般的なDDoS攻撃に使用される手法だった。

2019年に確認された脅迫メールはロシアの攻撃グループFancy Bearを装って金融機関に対して送信[15]された。2017年と同様に支払期限より前に最大60Gbps程度のDDoS攻撃が行われたことが確認された。一方で、2019年においては金銭を支払わなかったことによってDDoS攻撃が行われたとの情報はない。また、観測した攻撃は一般的なDNS、NTP、CLDAPに加え、WS DiscoveryやApple Remote Management Serviceを使用した2019年に新たに確認されたDDoS攻撃が含まれていた。

このような脅迫を受けた場合は、攻撃者の要求には応じず、冷静に対応することを心掛けたい。2017年や2019年に確認された脅迫メールの場合、実際にDDoS攻撃が行われる可能性があるため、攻撃が発生した場合の対応体制の確認や、攻撃への対策や利用している対策サービスの状況確認を推奨する。また、被害を最小化するために外部から接続可能なサーバやサービスの制限が重要となる。

■社会・インターネット基盤に影響をもたらす攻撃

●DDoS攻撃

2019年も継続してDDoS攻撃が観測された中で、主な手法は様々なプロトコルを使用したUDP Amplification攻撃だったが、一時的にTCP SYN/ACKリフレクション攻撃の観測が急増した。また、新たにWS-Discoveryを使用したDDoS攻撃が確認された。そして、これまでもクラウド、ホスティングサービスはDDoS攻撃の標的とされていたが、2019年においては利用者の多いAWSがDDoS攻撃によって一部のサービスに影響を受けた。

インターネットイニシアティブ社によるとTCP SYN/ACKリフレクション攻撃が2019年10月末ごろに急増したことが確認[16]された。この攻撃において複数の国がターゲットとなっており、ターゲットとなる送信元アドレスの偽装にはCarpet Bombingと呼ばれる攻撃手法が多く用いられ、宛先ポートとして80/tcpと443/tcpが多くを占めるなどの特徴があった。イスラエルのセキュリティ企業ラドウエア社やJPCERT/CCのインターネット定点観測システムでも同様のTCP SYN/ACKリフレクション攻撃を観測しており、広い範囲で攻撃が行われたことが推察される。

2019年に新たにDDoS攻撃に使用されたWS-Discoveryはローカルネットワーク上のサービスを探索する技術仕様であり、SOAPによってデバイスの探索と接続をする。WS-Discoveryを使用している製品は多岐にわたり、Windows Vista以降のパソコンやプリンタ、IPカメラなどで使用されている。WS-DiscoveryはUDPベース

のプロトコルであり、増幅率が最大500程度[17]と非常に効率的にDDoS攻撃が行うことが可能となっている。

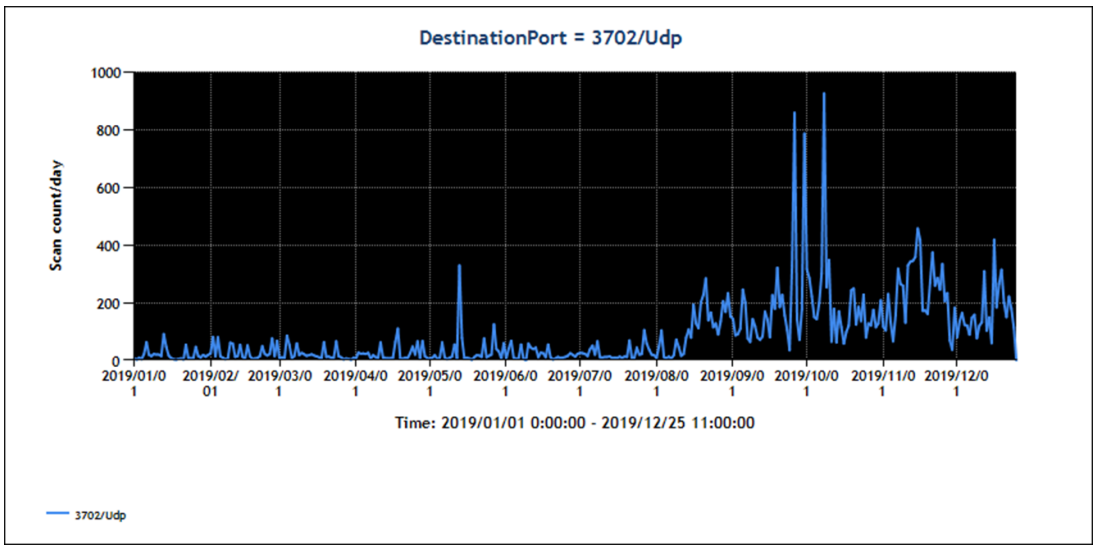
2019年5月にネットスカウト社がこのプロトコルを使用した攻撃を観測[18]しており、9月頃にはアカマイ社でもゲーム業界をターゲットとしてWS-Discoveryを使用した最大35GbpsのDDoS攻撃が行われたことが観測[19]された。WS-Discoveryで使用される3702/udpポートに対するスキャンが、攻撃が確認された5月頃と9月から10月頃に増加している様子をJPCERT/CCのインターネット定点観測システムにおいて確認（資料4-1-3）した。

このように2019年においても新たな手法を加えながらDDoS攻撃が継続して確認されており、アカマイ社が確認した事例のように特定の業界がターゲットとなったケースとTCP SYN/ACKリフレクション攻撃のように広い範囲に対して行われたケースが確認された。さらに、大規模なクラウドサービスを提供しているAWSのDNSサーバもDDoS攻撃の影響を受ける事例があった。

DDoS攻撃の標的にされた場合、それを逃れることは難しい。だが、事前にそうした事態に備えて、事業への影響を評価し、重大な影響があれば少しでもそれを軽減するために、顧客対応部門や広報部門などと連携した全社的な対応策を整備しておくことが望ましい。

1. インターネットバンキングの不正送金の被害に注意（JC3）
https://www.jc3.or.jp/topics/banking/phishing.html
2. 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）（警察庁）
https://www.npa.go.jp/cyber/policy/caution1910.html
3. 「Love you（ラブ・ユー）」マルウェア、日本を標的にした大規模な攻撃を展開 (ESET)
https://www.eset.com/jp/blog/welivesecurity/love-you-malspam-makeover-massive-japan-targeted-campaign/
4. GandCrab ransomware operation says it's shutting down（zdnet）
https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/
5. Sodinokibi ransomware exploits WebLogic Server vulnerability（Cisco Talos）
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
6. Sodin ransomware exploits Windows vulnerability and processor architecture（Kaspersky）
https://securelist.com/sodin-ransomware/91473/
7. Emotet´s Central Position in the Malware Ecosystem（Sophos）
https://news.sophos.com/en-us/2019/12/02/emotets-central-position-in-the-malware-ecosystem/
8. M-TRENDS2019（FireEye）
https://www.fireeye.jp/content/dam/collateral/jp/rpt-mtrends-2019.pdf
9. 【アルファメール/アルファメールダイレクト】お客様ご利用のWeb環境に対する不正アクセス発生のご報告（1/25 11:35更新）（大塚商会）
https://mypage.otsuka-shokai.co.jp/news/detail?linkBeforeScreenId=OMP20F0102S01P&oshiraseNo=0000001172
10. 【注意喚起】ウイルスバスターコーポレートエディションの脆弱性（CVE-2019-18187）を悪用した攻撃を確認したことによる最新修正プログラム適用のお願い（トレンドマイクロ）
https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=3592
11. ウイルスバスターコーポレートエディションの脆弱性（CVE-2019-18187）に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2019/at190041.html
12. 複数のSSL VPN製品の脆弱性に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2019/at190033.html
13. CVE-2019-0708：「BlueKeep」脆弱性を狙い、仮想通貨マイナーを増やす攻撃が確認される（tenable）
https://jp.tenable.com/blog/cve-2019-0708-bluekeep-exploited-in-the-wild-to-deliver-cryptocurrency-miner
14. Armada Collectiveを名乗る攻撃者からのDDoS攻撃に関する情報（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2017062901.html
15. RDoS attacks by fake Fancy Bear hit banks in multiple locations（Group-IB）
https://www.group-ib.com/blog/fakeapt28
16. TCP SYN/ACKリフレクション攻撃の観測（2019年10月）（IIJ）
https://sect.iij.ad.jp/d/2019/11/051516.html
17. UDP-Based Amplification Attacks（CISA）
https://www.us-cert.gov/ncas/alerts/TA14-017A
18. INTELLIGENCE REPORT: POWERED BY ATLAS

資料4-1-3　3702/udp（WS-Discovery）へのスキャン（2019年1～12月）



出典：JPCERT/CC のインターネット定点観測システム TSUBAME のデータをもとに作成

（NETSCOUT）
https://www.netscout.com/sites/default/files/2019-07/SECR_010_EN-1901%20%E2%80%93%20NETSCOUT%20Threat%20Report%201H%202019%20%E2%80%93%20Web.pdf

19. 解き放たれた、新しいDDoS攻撃ベクトル35 GbpsのWSD攻撃（Akamai）
https://blogs.akamai.com/jp/2019/09/ddos-35-gbps-wsd.html

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～2020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