SOCレポート

1.1 はじめに

IIJでは、2016年にセキュリティブランド「wizSafe（ウィズセーフ）」を立ち上げ、お客様が安全にインターネットを利用できる社会の実現に向けて日々活動しています。過去Vol.38[*1]の「SOCレポート」ではwizSafeの中核である情報分析基盤について、Vol.42[*2]では2018年に明らかとなった脅威と情報分析基盤を用いた新たな取り組みを紹介しました。今回は2019年におけるセキュリティの主要なトピックについて第1.2節で振り返り、取り上げたトピックに関連する脅威について情報分析基盤上で観測したものを第1.3節で紹介します。

1.2 2019年セキュリティトピックス

ここでは、2019年の主要なセキュリティトピックの中から、SOCが注目したものを表-1にピックアップしてまとめます。

＊1　Internet Infrastructure Review（IIR）Vol.38（https://www.iij.ad.jp/dev/report/iir/038/01.html）。
＊2　Internet Infrastructure Review（IIR）Vol.42（https://www.iij.ad.jp/dev/report/iir/042/01.html）。

表-1 2019年セキュリティトピックス

月	概要
1月	**国内のインターネットサービス企業が提供するファイル転送サービスにおいて、第三者の不正アクセスに起因する個人情報の漏えいが発生した。約480万件の会員情報が影響を受けたとされ、サービスを2020年3月31日に終了すると発表された。** "「宅ふぁいる便」サービス終了のお知らせ（2020年1月14日）" https://www.filesend.to/
2月	**総務省及び国立研究開発法人情報通信研究機構（NICT）は、容易に推測可能なパスワードを入力するなどの方法により、サイバー攻撃に悪用される恐れのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」を2月20日から開始した。** "IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施" http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html "IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施" https://www.nict.go.jp/press/2019/02/01-1.html
3月	**3月8日をもって「Coinhive」のサービスが終了した。仮想通貨の度重なる仕様変更や市場価値下落などの要因により、経済的にサービスを継続することが難しくなったとのこと。**
3月	**海外のPCメーカが管理するサーバがAPT（Advanced Persistent Threat：持続的標的型）攻撃を受けた。この攻撃により、同社製ノートパソコンに付随するユーティリティを利用しアップデートを実行した一部のユーザへ、悪意のあるコードを含むファイルが配信されていた。** "ASUS response to the recent media reports regarding ASUS Live Update tool attack by Advanced Persistent Threat (APT) groups" https://www.asus.com/News/hqfgVUyZ6uyAyJe1
4月	**国内の高等教育機関などで利用される"ac.jp"ドメインが、取得資格を満たさない第三者により取得され、成人向けWebサイト開設に利用されていたことが発覚した。ドメイン登録時の資格要件確認に不備があったとのこと。公共性の高いドメインの信頼性確保は重要であることから、総務省は再発防止策などを要請した。** "株式会社日本レジストリサービスに対する「.jp」ドメイン名の管理・運用に係る措置（要請）" http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000152.html
5月	**リモートデスクトップサービスに存在するリモートコード実行の脆弱性（CVE-2019-0708）、通称「BlueKeep」が公開された。マルウェアの感染拡大に重大な影響を与える脆弱性であるとの判断から、サポートが終了したOSに対してもセキュリティ更新プログラムが提供された。11月には実際にBlueKeepを悪用した攻撃も観測された。** "CVE-2019-0708 | リモート デスクトップ サービスのリモートでコードが実行される脆弱性" https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708
5月	**セキュリティ企業3社が不正アクセスを受け、セキュリティソフトウェアの開発ドキュメントやソースコードを含む機密情報が流出した可能性があることが発表された。後日、一部企業では、本事象による影響を受けていないことが確認された。** "Top-Tier Russian Hacking Collective Claims Breaches of Three Major Anti-Virus Companies" https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies
6月	**FreeBSD及びLinuxカーネルに、細工されたSACKパケットを受信することでカーネルパニックを引き起こす可能性のあるTCPベースの脆弱性（CVE-2019-11477）、通称「SACK Panic」を含む複数の脆弱性が存在することが発表された。**
7月	**バーコード決済サービスにおいて、一部のアカウントが第三者による不正アクセス及び不正利用の被害を受けたと公表された。複数端末からのログインに対する対策や二要素認証を含む追加認証の検討が不十分であったことなどが原因として挙げられている。本事件を受け、同サービスは9月30日をもって廃止された。** "「7pay（セブンペイ）」サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について" https://www.sej.co.jp/company/important/201908011502.html
7月	**国内の仮想通貨取引所において、約30億円分の仮想通貨が不正流出したことが公表された。流出した仮想通貨は、いずれもオンライン環境下で管理される「ホットウォレット」にて保管されており、その秘密鍵が窃取・不正利用されたと見られる。** "（開示事項の経過）当社子会社における仮想通貨の不正流出に関するお知らせとお詫び（第三報）" https://contents.xj-storage.jp/xcontents/AS08938/8a8b8ec7/f5b1/445e/a543/eade0775d325/140120190716472191.pdf
7月	**国内の自動車製造・販売会社の内部情報を格納した全文検索エンジンElasticsearchが外部から認証不要で参照できる状態であったことが公表された。格納されていた内部情報は、従業員の個人情報や内部ネットワーク、端末情報など約40GB分に上った。** "Honda Motor Company leaks database with 134 million rows of employee computer data" https://rainbowtabl.es/2019/07/31/honda-motor-company-leak/
8月	**2019年4月以降に報告された複数のSSL VPN製品の脆弱性を狙った攻撃が活発化した。8月にはBlack Hat USA 2019にて脆弱性に関する詳細が公開されたほか、PoCや当該脆弱性を悪用した攻撃の観測情報も報告されている。SOCにおいても、Pulse Secureの脆弱性（CVE-2019-11510）を悪用した攻撃通信を観測した。** "OVER 14,500 PULSE SECURE VPN ENDPOINTS VULNERABLE TO CVE-2019-11510" https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/
9月	**エクアドル国民2,000万人超の情報を格納した全文検索エンジンElasticsearchが外部から認証不要で参照できる状態であったことが発表された。** "Report: Ecuadorian Breach Reveals Sensitive Personal Data" https://www.vpnmentor.com/blog/report-ecuador-leak/
9月	**Wikipedia、Twitch、Blizzardの各サーバに対するDDoS攻撃が発生した。一連の攻撃はMirai亜種とみられるボットネットにより引き起こされていた。**
11月	**JPCERT/CCは、マルウェアEmotetに関する注意喚起を行った。2019年10月後半から、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ファイルによる感染被害の報告を多数受けているとのこと。SOCでは2019年9月末より活発な活動を観測している。** "マルウエア Emotet の感染に関する注意喚起" https://www.jpcert.or.jp/at/2019/at190044.html
12月	**複数の企業が、マルウェアEmotetに感染したことを公表した。感染した端末に保存されたメールアドレスやメール本文が漏えいした可能性があり、各企業を装った不審なメールの添付ファイルやURLリンクを開かないように注意喚起を行っている。**
12月	**自治体がリース契約満了に伴い返却したサーバから、データ削除前のハードディスクが盗難に遭っていたことが発覚した。当該ハードディスクはリース会社がデータ消去を委託している企業の社員により横領され、オークションサイト上で出品・落札されていた。** "リース契約満了により返却したハードディスクの盗難について" https://www.pref.kanagawa.jp/docs/fz7/prs/r0273317.html
12月	**海外のSNSに登録された2億6700万件超のユーザ情報が、認証不要で外部から閲覧可能なElasticsearchサーバ上に公開されていたことが報告された。** "Report: 267 million Facebook users IDs and phone numbers exposed online" https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/

1.3 観測情報

本節では、情報分析基盤を活用して明らかになった、2019年の特筆すべき活動について取り上げます。

1.3.1 外部公開されたElasticsearchサーバからの情報漏えい

■ Elasticsearchと情報漏えい事件

2019年は大規模な個人情報の漏えいが度々発生しました。中でも全文検索エンジンElasticsearchの設定不備による情報漏えいが目立った印象です。第1.2節で紹介したセキュリティトピックスでも、Elasticsearchに関連した情報漏えい事件を3件取り上げています。掲載した事件のほかにも、2019年1月には米国のクラウドデータ管理会社の顧客情報[*3]、2019年5月にはパナマ国民の約90%の情報[*4]が含まれていたElasticsearchサーバが外部から認証なしでアクセス可能な状態であったことが報告されています。いずれも流出した情報の量が多く、数百万件を超える情報や数十GB以上のデータが流出しています。

Elasticsearchは、Elastic社を中心に開発されているApache Luceneを基盤としたオープンソースの全文検索エンジンです[*5]。分散型システムで、並行して大量のデータを処理することで高速な検索を実現します。そのため、大規模な情報を扱う際に選択されることも少なくなく、セキュリティインシデントが発生すると流出する情報の量も多くなる傾向があると考えられます。また、ElasticsearchではRESTful APIが提供されており、HTTPプロトコルでデータの検索や操作が可能です。HTTPアクセスする際のポート番号はデフォルトで9200/TCPが用いられます。

SOCでは、アクセス可能なElasticsearchサーバを探索していると思われる9200/TCPへのスキャン通信が2019年に増加したことを観測しています。

■ 観測情報

図-1にIIJマネージドファイアウォールサービスにて観測された9200/TCPへのスキャン通信の件数及び送信元IPアドレス数の推移を示します。通信件数の値は年間に観測した9200/TCP宛てスキャン通信の合計を100%として正規化した当該通信の割合を記載しています。

図-1において、9月21日から10月31日にかけてのスキャン通信の増加が目立ちます。この41日間で発生した9200/TCPへのスキャン通信は、2019年の1年間に発生したスキャン通信の約23.37%を占めており、1日あたりの送信元IPアドレス数はピーク時で30,394件まで増加しています。これは1月1日のIPアドレス数(308件)と比較すると約98.68倍の数値です。この時期にElasticsearchに関する脆弱性は発表されておらず、スキャン通信が増加した明確な理由は分かっていません。

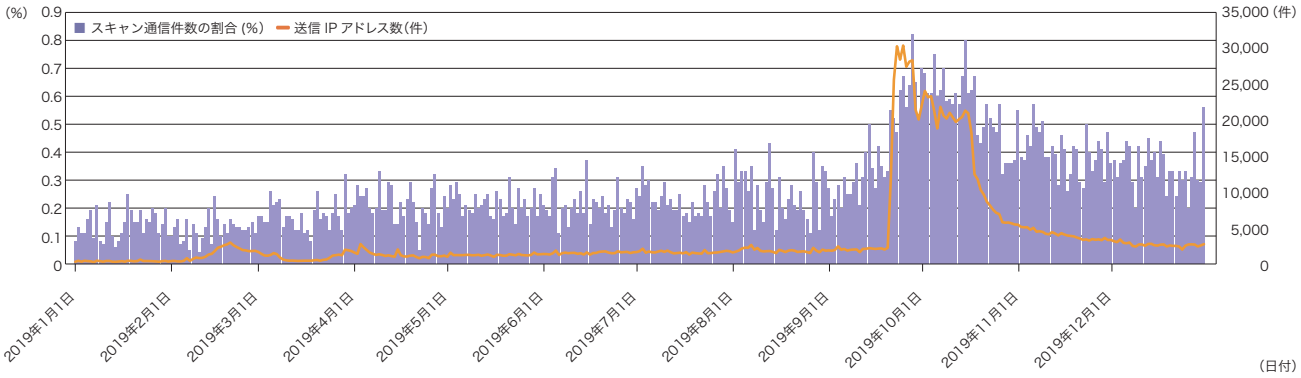

図-1 9200/TCPへのスキャン活動(2019年1月～12月)

＊3 techcrunch(https://techcrunch.com/2019/01/29/rubrik-data-leak/)。
＊4 securityaffairs、"Personally identifiable information belonging to roughly 90% of Panama citizens were exposed on a poorly configured Elasticsearch server."(https://securityaffairs.co/wordpress/85462/data-breach/panama-citizens-massive-data-leak.html)。
＊5 Elasticsearch(https://www.elastic.co/jp/elasticsearch)。

スキャン通信が増加する直前の9月16日にエクアドル国民2,000万人超の情報が閲覧可能であったとの報道がされており、この事件を契機とした増加である可能性も考えられますが、関連性を示す明確な証拠は見つかっていません。

2月中旬と4月上旬についても、一時的なスキャン活動の増加が見られます。送信元IPアドレス数は2月20日と4月3日に一時的に3,000件近くまで増加していました。2月19日に、Elastic社からElasticsearchの脆弱性(CVE-2019-7611)[*6]が公表されており、それを起因としたElasticsearch稼働サーバの探索と推測されます。CVE-2019-7611はアクセス許可に関する脆弱性で、悪用された場合、情報の取得や改ざんが行われる可能性があります。また、この時期に発生したElasticsearchへの攻撃についてCisco Systems社のセキュリティ部門であるTalosからレポートが公開されています[*7]。レポートによると過去に発表された脆弱性(CVE-2014-3120、CVE-2015-1427)を狙った攻撃が観測されていたようです。

年間を通したトレンドとしても、9200/TCPへのスキャン通信は全体的に増加傾向があります。12月における1日あたりの通信件数の平均は、1月平均の0.14%から0.35%と約2.46倍の増加、送信元IPアドレス数は1月平均の384.74件から2702.10件と約7.02倍も増加しています。同様の傾向は警察庁が公開している定点観測レポート[*8]でも見られ、Talosのレポートと同様にCVE-2015-1427を狙ったものと考えられる攻撃が紹介されています。

■ 対策

2019年に大きく報道されたElasticsearchに関連する情報漏えい事件のほとんどは、設定不備により認証不要でアクセス可能であったことが原因です。インターネット側からのアクセスが不要な場合はファイアウォールなどで9200/TCPを含む不要な通信を拒否したり、必要な場合も信頼できるIPアドレスからのみ接続を許可し適切な認証を設けるなど基本的な対策が重要です。また、Talosや警察庁のレポートにあるように、過去の脆弱性を狙う攻撃も依然として観測されています。システムに関連する脆弱性情報が公表された際には、システムへの影響を確認の上、修正プログラムの適用も併せて必要となります。

1.3.2 DDoS攻撃の観測

IIJでは様々な手法のDDoS攻撃を観測・対処しています。本項では、2019年のDDoS攻撃のトピックを取りまとめます。はじめに2019年にIIJが対処したDDoS攻撃のうち、IIJ DDoSプロテクションサービスで検出した攻撃についてまとめます。次に2019年に話題となった攻撃手法を取り上げ、最後に2019年に話題となった攻撃手法における国内の被害事例に関して、観測情報と併せて紹介します。

＊6 Elastic、"Security issues"(https://www.elastic.co/jp/community/security)。
＊7 Cisco Talos、"Cisco Talos Honeypot Analysis Reveals Rise in Attacks on Elasticsearch Clusters"(https://blog.talosintelligence.com/2019/02/cisco-talos-honeypot-analysis-reveals.html)。
＊8 警察庁、「Elasticsearch の脆弱性を標的としたアクセスの増加等について」(https://www.npa.go.jp/cyberpolice/important/2019/201910021.html)。

■ 2019年DDoS攻撃観測サマリ

2019年9月では、Wikipedia、Twitch、BlizzardへのDDoS攻撃が話題となりました。ここでは、2019年にIIJが対処したDDoS攻撃のうち、IIJ DDoSプロテクションサービスで検出した攻撃について取りまとめます。表-2にIIJ DDoSプロテクションサービスで検出した攻撃の件数や通信量を示します。

表-2の中で、TCPを用いた攻撃はSYN Flood攻撃やSYN/ACKリフレクション攻撃があり、UDPを用いた攻撃はUDP Amplification攻撃とUDP Flood攻撃があります。UDP Amplification攻撃では利用されるアプリケーションプロトコルにいくつか種類が存在し、DNS、NTP、LDAPなどがあります。

DDoS攻撃の発生件数は月単位で1日あたりの平均を算出していますが、2019年にはDDoS攻撃が顕著に活発な月はありませんでした。1秒あたりのパケット数が最も大きかったのは5月で、最も長い攻撃は1月に発生していました。また、最大パケット数が比較的大きかったのは5月、7月、12月でしたが、攻撃の最長時間は1時間未満に収まっていました。毎月の最大通信量及び最大攻撃時間で利用された攻撃種別の多くはLDAPやDNSを用いたUDP Amplificationが目立っています。

■ 2019年のDDoS攻撃トピック

表-2で紹介した攻撃手法のほかにも、DDoS攻撃として利用できる新手法がいくつか話題となりました。ここでは、2019年に話題となったDDoS攻撃の手法について、3つのキーワードを用いて紹介します。

- Web Services Dynamic Discovery（WSD）
- Apple Remote Management Service（ARMS）
- SYN/ACKリフレクション

1つ目のWSDは、Simple Object Access Protocol（SOAP）によって特定のネットワーク帯において対象のサービスを検出したり、データのやり取りを実現したりするプロトコルです。利用するポートは3702/UDPで、OSがWindows Vista以降のパソコンやプリンタなどで利用されていることが知られています。このプロトコルを利用したDDoS攻撃の可能性は、zeroBS GmbHにて示されています[*9]。なお、3702/UDPに対してインターネット上から応答を返すIPアドレス数は約63万個存在していたことが確認されています[*10]。SOCでは、2019年8月に3702/UDPに対するスキャン活動の増加を観測しています[*11]。図-2では、2019年にSOCで観測した当該ポートへのスキャン活動の推移を示します。なお、通信件数の値は年

表-2 2019年 DDoS観測情報サマリ

月	月間の件数（1日平均）	最大秒間パケット数（万）	最大通信量		最長攻撃時間	
			帯域	手法	時間	手法
1	13.58件	約179万	17.38Gbps	DNS Amplification	3時間20分	SYN Flood
2	15.75件	約284万	27.89Gbps	LDAP Amplification	1時間18分	LDAP Amplification
3	14.00件	約652万	19.30Gbps	SSDP Amplification	2時間32分	SSDP Amplification
4	22.96件	約97万	9.21Gbps	DNS Amplification	41分	DNS Amplification
5	16.16件	約886万	39.29Gbps	LDAP Amplification	41分	DNS Amplification
6	10.93件	約148万	8.11Gbps	SSDP Amplification及びSYN/ACKリフレクション	30分	SSDP Amplification及びSYN/ACKリフレクション
7	16.41件	約738万	75.67Gbps	DNS Amplification	38分	NTP Amplification
8	18.10件	約91万	8.77Gbps	LDAP及びDNS Amplification	1時間35分	UDP Flood
9	19.20件	約130万	11.71Gbps	LDAP及びDNS Amplification	43分	NTP Amplification
10	22.09件	約310万	23.09Gbps	LDAP及びDNS、NTPなどのAmplification	1時間56分	LDAP Amplification
11	13.36件	約70万	8.24Gbps	UDP Flood	25分	UDP Flood
12	10.38件	約607万	61.34Gbps	LDAP及びDNS Amplification	38分	NTP Amplification

＊9 zeroBS、"Analysing the DDOS-Threat-Landscape, Part 1: UDP Amplification/Reflection"（https://zero.bs/analysing-the-ddos-threat-landscape-part-1-udp-amplificationreflection.html）。
＊10 zeroBS、"New DDoS Attack-Vector via WS-Discovery/SOAPoverUDP, Port 3702"（https://zero.bs/new-ddos-attack-vector-via-ws-discoverysoapoverudp-port-3702.html）。
＊11 wizSafe、「wizSafe Security Signal 2019年8月 観測レポート」（https://wizsafe.iij.ad.jp/2019/09/746/）。

間に観測した3702/UDP宛てスキャン通信の合計を100%として正規化した当該通信の割合を記載しています。

図-2より、8月13日頃から当該ポートへのスキャンが増加していることが確認できます。また8月19日から8月末にかけて、当該ポートへのスキャン活動を実施する送信元IPアドレス数が増加しており、スキャン活動の増加は、BinaryEdgeの調査報告と概ね一致します。2月17日に発生した当該ポートへの通信を試みる送信元IPアドレス数の増加理由は定かではありませんが、2月19日にWS-Discoveryを用いたDDoS攻撃が発生していたことをBaidu, Inc.がレポートしています*12。このことから、WS-Discoveryを用いたDDoS攻撃は少なくとも2月頃には利用されていたと考えられます。しかし、国内で話題となったのは2019年9月になってからです。また、US-CERTのUDP Amplification Factorの資料においても、9月に公開された記事を引用する形で12月になってから追記されています*13。そのため、WS-DiscoveryがDDoS攻撃で本格的に利用されはじめたのは、実際に攻撃に利用され始めた数ヵ月後であったと考えられます。

2つ目のARMSは、Apple Remote Desktop（ARD）で利用されているサービスで、ARDはMacOSの複数端末をリモートから制御するためのアプリケーションです。ARMSは3283/UDPを通して、管理コンソールからのコマンドなどの命令を受信します。このARMSをインターネット上に公開している端末は、約4万台存在していたことが確認されています*14。図-3では、2019年にSOCで観測した当該ポートへのスキャン活動の推移を示します。なお、通信件数の値は年間に観測した

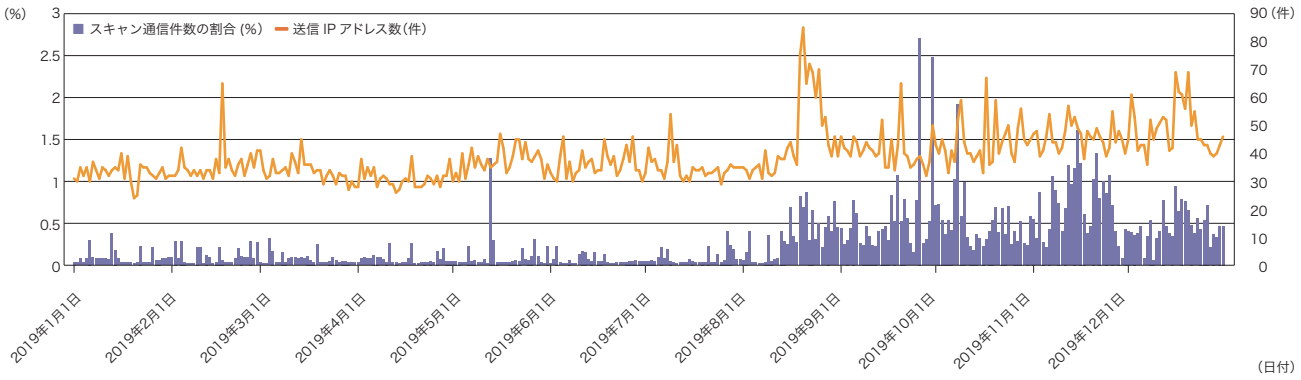

図-2 3702/UDPにおけるスキャン通信と送信元IPアドレス数の推移（2019年1月～12月）

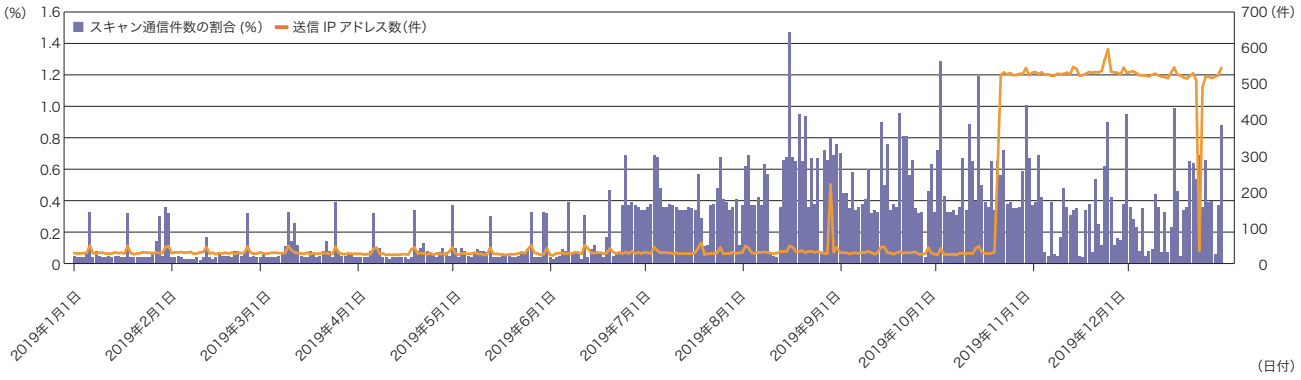

図-3 3283/UDPにおけるスキャン通信と送信元IPアドレス数の推移（2019年1月～12月）

*12 百度安全指数、"基于ONVIF协议的物联网设备参与DDoS反射攻击"（https://bsi.baidu.com/article/detail/128）。
*13 CISA、"Alert (TA14-017A)"（https://www.us-cert.gov/ncas/alerts/TA14-017A）。
*14 ZDNet、"macOS systems abused in DDoS attacks"（https://www.zdnet.com/article/macos-systems-abused-in-ddos-attacks/）。

3283/UDP宛てスキャン通信の合計を100%として正規化した当該通信の割合を記載しています。

図-3より、6月24日頃から当該ポートへのスキャンが増加していることが確認できます。また、10月22日頃からスキャン活動を実施する送信元IPアドレス数が増加しています。したがって、NetScout Systems, Inc.のレポートが公開される[*15]数日前からスキャン活動が増加していたことが分かります。

3つ目は、SYN/ACKリフレクション攻撃です。これは、TCPのthree-way handshakeの過程において、送信元アドレスを偽装したSYNパケットを多数のアドレスに同時に送信し、その応答であるSYN/ACKパケットを利用して送信元アドレスに対してDDoS攻撃を行う手法です。図-4にSYN/ACKリフレクション攻撃の全体像を示します。

SYN/ACKリフレクション攻撃の発生から、被害者に被害が発生するまでの流れを以下に説明します。図-4と併せてご覧ください。

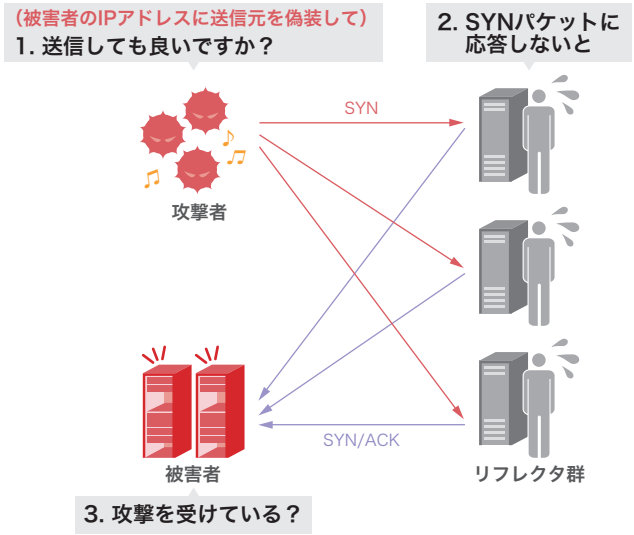

図-4 SYN/ACKリフレクション攻撃の全体像

1. 攻撃者は攻撃に使用するSYN/ACKパケットを発生させるために、送信元IPアドレスを攻撃対象に偽装し、送信元を偽装したSYNパケットをリフレクタに送信する。
2. three-way handshakeにおいて、そのSYNパケットに対してリフレクタはSYN/ACKパケットで応答する。
3. SYNパケットの送信元IPアドレスは偽装されていることから、リフレクタが返送したSYN/ACKパケットが被害者となるIPアドレス宛に届くことで攻撃が実現される。

本攻撃をSOCで観測したのは2018年で、小誌Vol.42の「1.2.2 SYN/ACKリフレクション攻撃」にて説明しています[*16]。このSYN/ACKリフレクション攻撃は、2006年頃にはTCP Amplification攻撃としてしられていた攻撃手法です[*17]。2014年には、SYN/ACKパケットやRSTパケット、PSHパケットを実装上発生しうる一般的な数よりも多く再送する端末がインターネット上で発見されました[*18]。実際に2014年に発見された端末を利用しているかは定かではありませんが、攻撃の原理としては同一のものです。SOCでは、SYN/ACKパケットを用いたTCP Amplification攻撃をSYN/ACKリフレクション攻撃と呼んでおり、7月頃から11月頃にかけて頻繁に観測されるようになりました。

これら2019年に話題となった3つの攻撃手法は、パケットの送信元を被害者に偽装し、リフレクタと呼ばれるDDoS攻撃を行うための踏み台を利用することが大きな特徴です。このような特徴を持つDDoS攻撃はDistributed Reflection Denial of Service（DRDoS）と呼ばれています。DRDoS攻撃の場合、攻撃者はリフレクタとして利用できるホスト及びポートを事前に調査し、悪用を試みます。そのため、DRDoSで利用できるポートが、インターネット上で誰からでもアクセスできてしまう場合、DRDoSのリフレクタとして利用されてしまう恐れがあります。WSDやARMSのようなDRDoS攻撃の場合には、送信元及び被害者だけに対策を求めるのではなく、リフレクタにおいても可能な対応策を取る必要があります。DRDoS攻撃の

＊15 NETSCOUT、"A Call to ARMS: Apple Remote Management Service UDP Reflection/Amplification DDoS Attacks"（https://www.netscout.com/blog/asert/call-arms-apple-remote-management-service-udp）。
＊16 Internet Infrastructure Review（IIR）Vol.42（https://www.iij.ad.jp/dev/report/iir/042/01.html）。
＊17 RFC 4732、"Internet Denial-of-Service Considerations"（https://tools.ietf.org/html/rfc4732#section-3.1）。
＊18 USENIX、"Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks"（https://www.usenix.org/system/files/conference/woot14/woot14-kuhrer.pdf）。

場合、リフレクタとなっているサーバの管理者は、DDoS攻撃の標的ではありませんが、被害を受けているサーバやネットワークなどに対する攻撃に意図せず加担してしまいます。したがって、インターネット上で不必要にポートを開けていないかを確認し、意図したアクセスのみを許容する設定にしておくことが重要です。このことは、不正アクセスだけでなくDDoS攻撃で利用される可能性のあるリフレクタを削減することにも繋がるため、DDoS攻撃における攻撃者の行動を制限できる可能性が高まります。ただし、DRDoS攻撃の手法にはリフレクタとしてアクセス制御が容易でないものが存在します。それがSYN/ACKリフレクション攻撃です。その理由は次の「SOCによる観測状況」で説明します。

■ SOCによる観測状況

2019年には、先述した3つの攻撃手法による日本国内の組織やサービスを狙ったDDoS攻撃が発生しました。ここでは日本国内で発生したDDoS攻撃のうち、2019年に話題となった事例について、SOCで観測した情報を加えて解説します。日本国内の組織を狙ったWSD及びARMSを用いたDDoS攻撃は、2019年10月のJPCERT/CCの注意喚起に[*19]示されています。本事例は、DDoS攻撃にWSD及びARMSが用いられていただけでなく、仮想通貨を要求する脅迫メールが届く事例であることが判明しています。このような金銭目的と考えられる脅迫文を用いてDDoS攻撃を示唆する試みは、Ransom Denial of Service（RDoS）と呼ばれています。このRDoSは2019年だけでなく、2017年にも話題となった事例です[*20]。攻撃のアクターは両年の事例において同一であるかは定かではありませんが、少なくとも2017年には公表されていなかったWSDとARMSを用いたDDoS攻撃が2019年の事例で利用されていることは事実です。図-2及び図-3と併せて考えると、少なくともDDoS攻撃で用いられる攻撃インフラは悪用可能なプロトコルに順次適応していると考えられます。

SYN/ACKリフレクション攻撃が日本国内の企業に向けたDDoS攻撃で利用された事例として、表-2の6月の最大通信量・最長攻撃時間を記録した攻撃が挙げられます。SYN/ACKリフレクション攻撃の大きな特徴は、リフレクタとして任意のTCPポートが利用されるため、WSDやARMSのように特定のポートに紐づくサービスを悪用するものではありません。そのため、Webサーバで一般的に利用される80/TCPや443/TCPなどが利用されます。例えば、インターネット上に公開しているWebサーバ上のコンテンツは、幅広く閲覧してもらうために何処からでもアクセスできることが重要になります。この場合、ファイアウォールは意図して誰でもアクセスできる設定になっているはずです。この前提の上で、SYN/ACKリフレクション攻撃のリフレクタとして利用された場合、リフレクタ側では容易にアクセス拒否することが難しいと考えられます。図-5に、2019年にSOCで観測したSYN/ACKリフレクション攻撃のリフレクタとして利用されたTCPポートの割合を示します。

図-5から分かる通り、SYN/ACKリフレクション攻撃で利用されるTCPポートは、80/TCP及び443/TCP、またSimple Mail Transfer Protocol（SMTP）として利用される25/TCPです。これらは全体の95%以上を占めます。また、Othersには、21/TCPや22/TCP、587/TCPなどが多く含まれています。従って、SYN/ACKリフレクション攻撃で利用される踏み台となるポートは、インターネット上から比較的自由にアクセスしやすいTCPポートが対象となっていることが分かります。図-5で示したとおり、外部からのアクセスを許容するサービスが稼働しているTCPポートが踏み台とされやすいため、アクセス制御によって、リフレクタ側でSYN/ACKリフレクション攻撃に対処することが難しいものと考えられます。

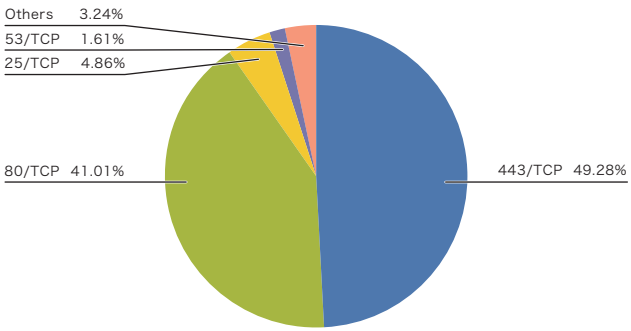

図-5 SYN/ACKリフレクション攻撃におけるリフレクタで利用されたポートの割合

*19 JPCERT CC、「DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて」（https://www.jpcert.or.jp/newsflash/2019103001.html）。
*20 radware、"Fancy Bear DDoS for Ransom"（https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/fancybear/）。

しかし、SYN/ACKリフレクション攻撃への対処の難しさはこれだけではありません。SYN/ACKリフレクション攻撃は、攻撃に関わりのある端末や被害者など、基本的にネットワーク全体を俯瞰してみなければ判断しにくいものです。実際にリフレクタとなっている個々のホストには攻撃端末からSYNパケットが大量に届くため、リフレクタして利用されているホストの管理者からはSYN Flood攻撃を受けているものと判断してしまう恐れがあります。その場合にブラックリスト方式でSYNパケットの送信元を永続的に遮断すると、DDoS攻撃が収束した後に被害者のIPアドレスから遮断設定を行ったホストへアクセスができなくなります。これはSYN/ACKリフレクション攻撃の副次的な被害と考えることが出来ます。

SYN/ACKリフレクション攻撃で国内の端末をリフレクタとして利用された事例は、SOCの情報発信サイト「wizSafe Security Signal[*21][*22][*23][*24]」にまとめています。なお、これらの事例は、リフレクタ視点で観測したSYN/ACKリフレクション攻撃であり、被害者視点の情報ではありません。そのため、SYN/ACKリフレクション攻撃における攻撃規模を全て示しているわけではないことにご留意ください。

1.3.3 Emotet

■ Emotetの概要

2019年の後半からは、メールを悪用して感染活動を行うEmotetと呼ばれるマルウェアが話題になりました。このマルウェアが最初に報告[*25]されたのは2014年、当時トレンドマイクロ社に在籍していたJoie Salvio氏によるものでした。当初、金融機関の情報を狙うバンキングトロジャンとして活動していたEmotetは、次第にその形態を変化させボットネット化していきました。更にモジュール化によるワーム機能の獲得により、様々なマルウェアやランサムウェアを拡散する能力を備えました。これにより近年では、金融機関の情報だけではなく、機密情報も盗み出すマルウェア（TrickbotやZeuSなど）をダウンロードさせるように変化してきました。また、Emotetを起点にダウンロードされた情報窃取の機能を持つマルウェアにより、ターゲットとなるシステムに侵入することで、最終的にRyukと呼ばれているランサムウェアのペイロードを実行する攻撃が報告されています。これらのマルウェアにより窃取した情報を元にターゲットとなるシステムに侵入し、Ryukと呼ばれるランサムウェアのペイロードを実行する多段攻撃triple threat[*26]についても報告が上げられています。このような変化に伴い、攻撃のターゲットも公共機関や民間企業へと変化を見せています。

国外の観測[*27]では、2019年6月頃からEmotetで使用されていたC2サーバの休眠が確認されていましたが、活動の休止は長くは続きませんでした。2019年8月末には当該サーバの活動再開が報告されており、同9月以降、IIJのメールゲートウェイサービス「IIJセキュアMXサービス」においてもEmotetへの感染を誘導する悪意あるメールの検出が増加していました。

SOCの観測では、Microsoft Word（doc）形式の添付ファイルを悪用した感染活動を多数確認しています。その後、別の感染経路として、メール本文にEmotetに感染させるdocファイルをダウンロードさせるURLを記載したメールが増加しました。

---

*21 wizSafe、「wizSafe Security Signal 2019年7月 観測レポート」（https://wizsafe.iij.ad.jp/2019/08/717/）。
*22 wizSafe、「Servers.comを狙ったDDoS攻撃の観測」（https://wizsafe.iij.ad.jp/2019/10/764/）。
*23 wizSafe、「2019年10月 TCP SYN/ACKリフレクション攻撃の観測事例」（https://wizsafe.iij.ad.jp/2019/12/820/）。
*24 wizSafe、「2019年11月 TCP SYN/ACKリフレクション攻撃の観測事例」（https://wizsafe.iij.ad.jp/2019/12/839/）。
*25 TREND MICRO、"New Banking Malware Uses Network Sniffing for Data Theft"（https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/）。
*26 cybereason、"RESEARCH BY NOA PINKAS, LIOR ROCHBERGER, AND MATAN ZATZ"（https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware）。
*27 cBLEEPINGCOMPUTER、"Emotet Botnet Is Back, Servers Active Across the World"（https://www.bleepingcomputer.com/news/security/emotet-botnet-is-back-servers-active-across-the-world/）。

Emotetへの感染を誘導するdocファイルを開くと、Wordの初期設定状態では図-6に示すような「コンテンツの有効化」を促すメッセージが表示されます。そして「コンテンツの有効化」を許可することによりマクロが実行されます。なお、Wordの設定でマクロを有効化している場合には、図-6のような画面は表示されず、マクロは自動で実行されます。そして、マクロが実行されるとマルウェア配布サーバよりEmotetがダウンロードされ、感染へと繋がります。

一度感染すると、Emotetは感染を永続化するために、新しいサービスに自身をコピーし、自動実行されるように設定します。その後、感染したPCの情報窃取やC2サーバへの通信を行います。窃取される情報にはメール本文やアドレスのデータなどが含まれており、Emotetへの感染を誘導するメールにはこれらの情報を悪用し、メールの返信を装うものがあります。これが感染を広げる原因の1つになっています。前述のtriple threatと呼ばれる多段攻撃の例からも分かるとおり、Emotetは他のマルウェアの入り口として機能するため、最終的な被害は今後更に変化すると考えられます。

■ 観測情報

以下では、SOCにおけるEmotetの観測状況について報告します。

まず2019年9月から12月に検出した攻撃について、Emotetに関連する検出とその他の検出に分けた積み上げグラフを図-7に示します。図の横軸は日付を、縦軸は集計対象期間における合計検出件数を100%として正規化した割合を表します。

図中で、最初にEmotetの検出が目立つのは9月27日です。その後は10月の16日、17日、23日、24日に多く検知しています。11月に入ると、これまでの月と比べ多くの日数、割合でEmotetを検出しています。また、検出は平日に集中する傾向が見られます。12月3日から4日にかけて集計期間中の検出

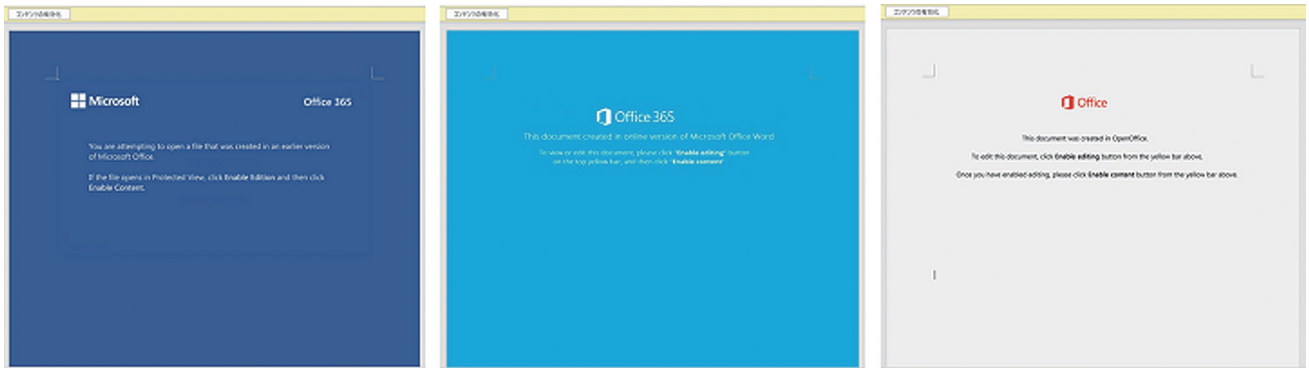

図-6「コンテンツの有効化」を促す画面の例

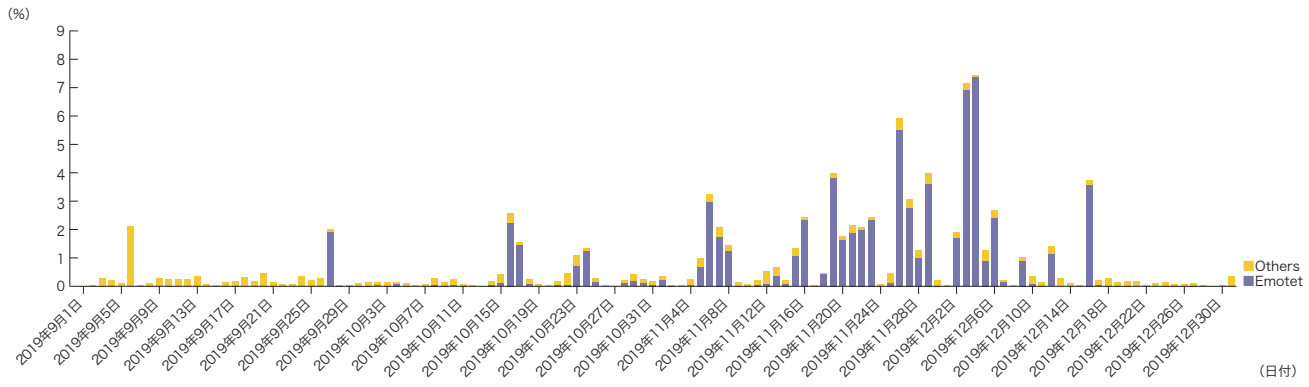

図-7 メール受信時のマルウェア検出傾向(2019年9月～12月)

ピークを迎え、その後16日のスパイクを最後に、12月中はIIJセキュアMXサービスにおける検出が落ち着きました。

しかし、それと入れ替わるように、IIJセキュアWebゲートウェイサービスでは、Emotetに関連する検出が増えています。図-8には横軸に日付、縦軸に12月中のEmotetに関連する検出合計を100%として正規化した当該通信の割合を示します。

図-7のメールでの検出が落ち着いた直後の12月17日から数日間、図-8ではEmotetに関連する検出の割合が増加しています。これらの通信は、Emotetに感染させるためのdocファイルをダウンロードする試みであることを確認しています。また、IPAからはEmotetに感染させるための不正なURLリンクを記載した日本語メールが12月10日頃より確認されたとの注意喚起[*28]が出されており、図-8に示した検出が開始した時期と一致しています。従って、図-8で検出した通信は、Emotetの拡散を目的としてメール本文に記載されたURLにアクセスしたものであると考えられます。

次に、SOCで観測したEmotetへの感染を誘導すると見られるメールのうち、件名に日本語を含むものを表-3に示します。なお、表-3では主要なものだけを取り上げており、全てのメールを網羅しているわけではない点にご注意ください。

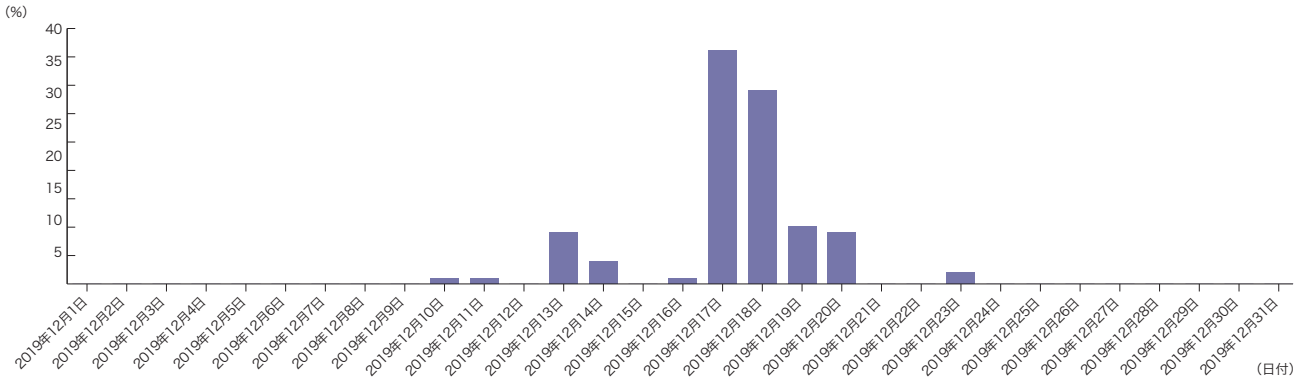

図-8 HEUR:Trojan.MSOffice.SAgent検出割合の推移(2019年12月)

表-3 件名に日本語を含みEmotetへの感染を誘導する不審メールの情報

件名	添付ファイル名	備考
12 月賞与	<日付>.doc	<日付>にはYYYYMMDDの形式でメール受信日が入ります 件名の末尾には日付、人名、組織名が入る場合があります
[本日 23:59 まで]amazon.com に更新割引クーポンが発行されました	<日付>_<ランダムな英数字>.doc	
ご入金額の通知	<ランダムな英数字> <日付>.doc	
ご請求書発行のお願い	<ランダムな英数字> _<日付>.doc	
ドキュメント	<ランダムな英数字>-<日付>.doc	
メッセージを繰り返す	賞与支払届.doc	
リマインダー	12月賞与.doc	
気づく	2019冬・業績賞与支給.doc	
最後のオプション	請求書送付のお願い <ランダムな数字>-<日付>.doc	
支払通知	メリークリスマス <日付>.doc	
助けて		
情報		
新バージョン		
請求書送付のお願い		
領収書		

*28 独立行政法人情報処理推進機構、「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」(https://www.ipa.go.jp/security/announce/20191202.html#L11)。

表-3に示したようにメールの件名には、「気づく」・「助けて」・「情報」など1単語だけの表現や請求書・領収書を装ったものなど様々なバリエーションがあります。また、ブラックフライデーのシーズンにはECサイトの割引クーポンを装った件名や、年末には件名もしくは添付ファイル名に「賞与」・「クリスマス」といった時期に合わせた単語が用いられるようになりました。

■ 対策

前述のとおり、Emotetは感染端末から窃取したメール情報を元に、返信を装うなどして感染を拡大させるためのメールを送付します。そのため、受信者が送信元メールアドレスや本文から違和感を感じたり、不審であるかどうかを判断したりすることが困難な場合があります。感染を予防し被害を最小限に抑えるためには、まず、Wordの設定を確認の上、マクロの自動実行を設定している場合には無効化します。また、問題がないと判断できないメールに添付されているファイルを不用意に開かないこと、添付ファイル内のマクロを手動で有効化しないことも重要です。更に、US-CERTでは入り口での予防として、マルウェアに利用されることのある拡張子やアンチウイルスソフトでスキャンできない形式のファイルを添付したメールの受信を禁止するポリシーも有効であるとされています[*29]。それ以外にも、適切な権限設定や送信ドメインの認証を行うことなどが推奨されています。

1.4 おわりに

本レポートでは、2019年に国内で話題となったセキュリティ事件を取り上げ、いくつかの事例をSOCで観測している情報と併せて紹介しました。本章で取り上げた事例のほかにも様々なセキュリティ脅威を日々観測しています。1.2節及び1.3節で取り上げた事件や事象に関わらず、適切に状況を把握し、対処することが重要となります。1.3.1項で取り上げたElasticsearchにおける事案などACLで対処できる内容のものもあれば、脆弱性におけるパッチの適用、1.3.3項のようなマクロの有効化を安易に実施しないという個人における対策も存在します。SOCでは、引き続き様々なセキュリティ事件や脅威について、wizSafe Security Signal（https://wizsafe.iij.ad.jp）にて定期的に情報共有しており、日々のセキュリティ業務に還元していただけたら幸いです。

執筆者：
守田 瞬（もりた しゅん）
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター データアナリスト

執筆者：
本部 栄成（ほんぶ えいせい）
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター データアナリスト

執筆者：
山口 順也（やまぐち じゅんや）
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター データアナリスト

*29 CISA、"Increased Emotet Malware Activity"（https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity）。