RAPID7

RESEARCH

National/Industry/Cloud Exposure Report (NICER) 2020

最新のインターネット環境に関する包括的なセキュリティ調査 2020年度

目次

エグゼクティブサマリー

Rapid7の2020年版National / Industry / Cloud Exposure Report（NICER）は、最新のインターネットに関する最も包括的な調査です。世界的なパンデミックや不況の中で、Rapid7のリサーチチームが、刻々と変化するインターネットリスクの状況について、データに基づいた分析を行うことで、インターネットの世界を形成している相互接続の技術に潜んでいる外部公開の方法、および設定に関する弱点（サイバーエクスポージャー）の発生率と地域的な分布を測定しました。さらに実用的なデータを提供するため、調査結果を国、業界、プロトコル別に分け、またパンデミックやクラウドへの移行などの技術的変化の影響を追加しました。これにより行政当局や、事業部門、研究開発部門は、脆弱性、改善または改悪した点、およびインターネットの安全性の強化について、対策の立案で必要となる分析を行うことが可能になります。

インターネットから見るグローバルパンデミック

2020年中頃には、コンピューターサイエンス分野は通常扱わないようなウイルスの発生に世界が対応することになりました。それは、COVID-19の生物学的パンデミック[1]と、それによるロックダウンの直後に続いた景気の低迷です。Rapid7は、以前よりインターネットと世界中のセキュリティ状況に関する調査を計画していましたが、今となっては急速に、そして無秩序に世界の形を変えている、このような前例のない混乱の時代を捉える、珍しい機会を得ることになりました。

まず私たちが答えを見つけるべきだと考えたのは、「パンデミック、ロックダウン、そして雇用喪失が、どのようにインターネットの特徴や構成に影響したか」ということです。人々がオフィス、コワーキングスペース、学校に行けなくなり、在宅での仕事や学習モデルに突然切り替わったため、「とりあえず物事を機能させる」ことを急ぎました。そのため、公共のインターネットには、急いで展開された構成が不十分かつ、全体的に安全性に欠けたサービスが復活すると予想していました。本プロジェクトに向けて4月と5月のデータ収集を開始した際、自宅と職場間のファイル共有に、数千万という新しいWindows SMBサービス、インターネット全体のバックアップデータを収集するrsyncサーバー、およびTelnetベースのコンソールを提供する未構成のIoTデバイスに関する懸念が拭えませんでした。

しかし2020年は悪いものだけでなく、 良い驚きにも満ちた年です。実に、SMB、Telnet、rsyncなどの安全性が非常に低いサービスと、中核的なメールプロトコルの個体数が、2019年の水準よりも減少したことが分かりました。一方、SSH（セキュアシェル）やDoT（DNS over TLS）など安全性が低いプロトコルに替わる、安全な選択肢は増加しました。つまり、地域間の違いや、懸念すべき程度のサイバーエクスポージャーが明らかにあり、 それについては後に詳細を見ていきますが 、サービスの安全性という点では、インターネット全体が正しい方向に向かっているようです。

これは率直なところ、衝撃的な結果です。世界的な病気と不況という災害、そしてそれらがもたらす不透明感は、インターネットの根本的な性質に明白な影響を与えていないように思われます。これは、まだパンデミック、不況、およびリモートワークの導入拡大による影響が完全に把握できていないためという可能性もあります。Rapid7は今後もモニタリングを続け、状況の展開を報告いたします。

シルバーシティの神話

一方、クラウドは今まで以上に「インターネット上の問題」を抱えるようになりました。Platform-as-a-Service（PaaS）とInfrastructure-as-a-Service（IaaS）のプロバイダなら、中小企業でもプロレベルで管理と保守が行われたサーバーインフラを展開し、想像できる限りありとあらゆるインターネットのベンチャービジネスを運用できるようできます。インターネット上で、設計的に安全ではないサービスが減少したのは、クラウドプロバイダによるものだと予想していました。単純に世界的なクラウドプロビジョニングの大手が、コンテナ化された安全設計のソフトウェアを展開できる完璧なアーキテクチャーの「シルバーシティの神話」、つまりは、天空にそびえるまばゆい銀色の都市を構築できるものと想像していました。

しかし、そうではありませんでした。実際には、クライドプロバイダは多くの場合、従来のオンプレミス環境でIT部門が苦戦しているのと同じ問題に悩まされているのでした。プロバイダが持つドキュメンテーションやデフォルト設定ですら、必ずしも安全にインターネットサービスの設定と実行を行うための近道という訳ではないのです。また、パッチ処理がされていない、または最新ではないUbuntu（およびその他のLinuxディストリビューション）のと、これらのネットワークにインストールされたサービスの数から、「見て見ぬふり」という考え方が多くのユーザー間で一般化しているように見えます。この結果から、インターネットの安全性が、依然としてできるだけ早く物事を機能させて進めたいという要求に追いついていないという事実に気付かせられます。

[1] COVID-19は、厳密に言うとSARS-CoV-2で、単に「コロナウイルス」とも呼ばれます。

国別ランキング

調査結果をまとめるにあたり、収集したコンピュータの情報をネットワークオペレータ以外でも理解できるようにする方法を考える必要がありました。自律システム「AS4809」は、インターネットルーティングの仕組みに詳しい人にとっては聞きなれた名称かも知れませんが、分かりやすくするため、単純に「中国に」あるコンピュータと呼ぶことにします。また、IPアドレスが物理的に世界のどこにあるかというジオロケーションに、かなりの時間を費やしました。しかしながら、物理的な世界では普遍性、実証性において不十分なため、経度と緯度の座標ではなく、「デンマーク」や「グリーンランド」といった馴染みのある場所の名前を使用しています。

最後に、本レポートでは地域を説明するのに「国」という言葉を使用していますが、他の名付けられた地球上の地域を指すことがあります。その場合、特別な行政領域、科学的な保護区域、または他国の領土といった政治的ステータスは区別していません。算入の基準は単純に、「この地域はISO 3166 3-alphaの国名コードがあるかどうか」です。[2] 国名コードがある場合は、政治的現状に関係なく、調査目的のために「国」と見なします。例えば、「香港」（HKG）のような地域は、このレポートにも出てきます（香港はサイバーエクスポージャーの面で興味深い点がいくつかあります）が、一方、設定が不十分なインターネットに接続されたデバイスが多くあるにもかかわらず、「カリフォルニア」は出てきません。

もし、世界中で「最もサイバーエクスポージャーが多い」国を知るためだけに本レポートをお読みになっている場合は、以下の説明と表を見るだけで答えが分かるようになっています。

サイバーエクスポージャーが最も高い国

以下の表では、リストの上位国（エクスポージャーの状態が悪い）国を重点的に下記の指標を使って計算した、サイバーエクスポージャーが最も高い国を示しています。

- **全体の攻撃面**（調査期間中に使用されていて、何かを露出させたIPv4の合計数）。
  根拠：IPアドレスの多さ＝攻撃対象の多さ。
- **特定のサービスにおけるエクスポージャーの合計。**具体的にはSMB、SQL サーバーおよびTelnet。*根拠：*これらは決して露出させてはいけません。
- **全サービスを通して存在する個別のCVE数。**
  *根拠：*既知の脆弱性の多さ＝露出の多さ。
- **脆弱性率分布の中心。**脆弱性率とは、脆弱性を伴うエクスポージャーのあるサービスまたはエクスポージャーのあるサービスの数を指します。**根拠：**エクスポージャーのあるサービスすべてを通して高い脆弱性率が、ランクの低下につながるはずです。
- **最大の脆弱性率。**
  *根拠：*前段階を経た後に残った全ての関係を断つため、最も脆弱性率が高い国にペナルティを加点する。

露出度が最も高い上位50か国

ランク	国	ランク	国
1	米国	26	スウェーデン
2	中国	27	インドネシア
3	韓国	28	南アフリカ
4	イギリス	29	シンガポール
5	ドイツ	30	ポーランド
6	ブラジル	31	コロンビア
7	ロシア	32	サウジアラビア
8	日本	33	ベネズエラ
9	カナダ	34	アラブ首長国連邦
10	イラン	35	モロッコ
11	イタリア	36	ポルトガル
12	アルゼンチン	37	アルジェリア
13	台湾	38	オーストリア
14	オーストラリア	39	ニュージーランド
15	スペイン	40	ルーマニア
16	フランス	41	ウクライナ
17	インド	42	スイス
18	トルコ	43	チリ
19	香港	44	マレーシア
20	メキシコ	45	ノルウェー
21	ベトナム	46	チュニジア
22	オランダ	47	ベルギー
23	エジプト	48	クロアチア
24	タイ	49	ハンガリー
25	アイルランド	50	ギリシャ

[1] https://www.iso.org/iso-3166-country-codes.html

予想通り、私たちのランキング方法ではIPスペースが広い国が上位に選ばれています。米国と中国が「最も露出のある」国の1位と2位というのは、驚くべき結果ではありません。興味深く、そしておそらく驚くべき結果は、最も露出が高いとされた3位から50位までの順位です。例えば、カナダとイランはどちらも精巧かつ広範なインターネットを保有していますが、カナダの人口はイランの半分以下です。それでも、カナダとイランの露出率は非常に似ており、カナダが僅差でイランを抜いて9位となっています。

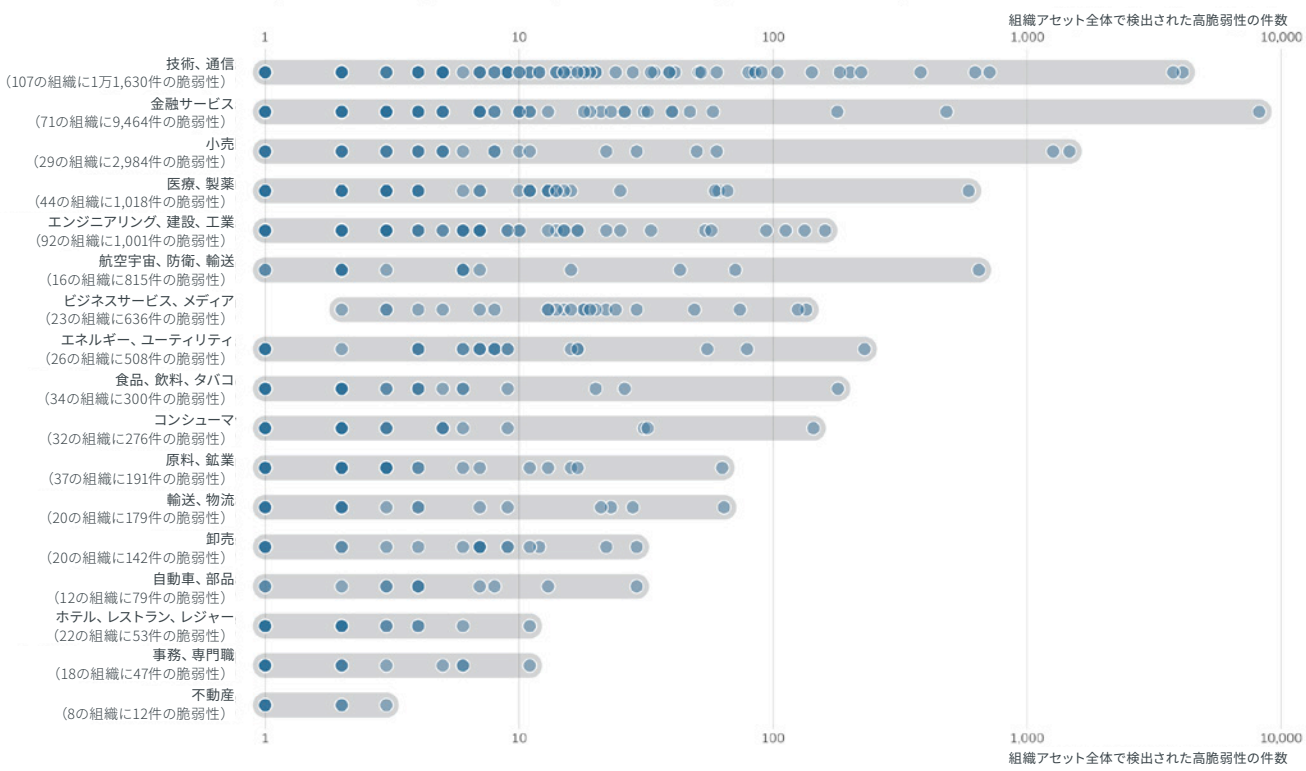
さらなる深堀レポート

今後で、日本やラテンアメリカなど、特定の国や国のグループを詳しく調べた補足レポートを作成する予定です。さらに、これら以外に、詳しく調査したい特定の国や地域がある場合は、お知らせください。

業界別ランキング

2019年に、Rapid7は米国のFortune 500、英国のFTSE250＋、ドイツのプライムスタンダード320社、オーストラリアのASX200、そして日本の日経225のセキュリティ体制を調べたレポートシリーズ、「業界別サイバーエクスポージャーレポート（ICERs）」を作成しました。すでにこのような好業績で資金力の高い上場企業1,500社を特定していたことから、業界別にグレード付け、順位付けしました。

RAPID7 INDUSTRY 1500 組織の高脆弱性分布



上記の表にある点は企業を、X軸上の位置はインターネットに面する攻撃面のコンポーネントで発見された重大な脆弱性の数を表しています。これらのコンポーネントは、Webサーバーからキャッシュサーバー、そしてこれらのサービスが実行されているオペレーティングシステムまでを含みます。

弱点の多くは、管理が行き届いていないApache HTTPのWebサーバーで、「お決まりの問題点」（例：DNS、SMTP、SSH）などが続きます。

ベンダー	サービス	重大な脆弱性を持つインスタンス数
Apache	HTTPサーバー	14,830
Squid	キャッシュサーバー	3,822
OpenBSD	OpenSSH	3,626
Debian	Linux	3,123
ISC	BIND（DNS）	2,460
RedHat	Linux	434
Apache	Tomcatサーバー	205
Exim	Exim（SMTP）	162
Canonical	Ubuntu	160
nginx	nginx Webサーバー	133

Apacheのコンポーネント（ここではHTTPDのWebサーバーとJavaサーブレットランナーを指す）には、nginxなどに比べてかなり古く、多くの企業にとって可視性や管理性のない「アプライアンス」の一部となっているという明らかな欠点があります（ITとセキュリティ部門がエクスポージャーの管理を強化するためには、「ソフトウェアのBOM（部品表）」[1]のようなものが必要となります）。

グラフは全体的な分布を示していますが、これらのサービスを露出している個体数が比較的把握できていることから、業界別ランキングのアプローチは国別ランキングと若干異なります。これらの企業は十分な資金力があり、その大半が規制枠組みを遵守しなければならず、独自の情報技術および情報セキュリティの専門家を有しています。多くは創業から10年以上経過しており、対象企業の全てが基礎的なITおよびサイバー衛生を実践しています。

これらを念頭に置いたうえで、汚れやネズミの侵入のサイバー版を、各業界グループに見られた「高」（CVSS8.5以上）脆弱性の数字として定義し、[2]ニューヨーク市がレストランの格付けを行うのと同様に、アルファベットを割り当てました。[3]割り当てられたアルファベットは、業界ごとのエクスポージャーの高さの対数平均で決定されています（一部の業界は他よりも企業数がはるかに少なく、また業界によっては数百、数千に上るアセットのエクスポージャーに関与しているため）。結果は表3の通りです。

業界	グレード
航空宇宙、防衛、輸送	A
自動車、部品	A
小売	B
ビジネスサービス、メディア	B
輸送、物流	B
卸売	B
不動産	B
エネルギー、ユーティリティ	C
食品、飲料、タバコ	C
コンシューマ	C
ホテル、レストラン、レジャー	C
事務、専門職	C
技術、通信	D
金融サービス	D
医療、製薬	D
エンジニアリング、建設、工業	D
原料、鉱業	D

過去12カ月ほどを振り返ると、発生した侵入やランサムウェアのほとんどが、グレード「D」の業界に集中していることから、同業界が他業界に後れを取っていることは当然だといえます。

[3] https://www.ntia.gov/SBOM
[4] 各インデックスマップの業界内訳が、どのように標準化された業界に分類されているかについては、付録の「調査方法」を参照してください。
[5] https://www1.nyc.gov/site/doh/services/restaurant-grades.page

一方、「完璧」に近い業界はなく、サイバー衛生という点では各地域に掲載されている企業は、さらなる努力が必要であるということが前回のICERから分かりました。これは、Apache HTTPDの高エクスポージャーの80%が、3年から14年前のバージョンであるという事実からも明らかです。

バージョン	リリース年	数	割合
2.4.6	2013	3,222	21.73%
2.2.15	2010	2,162	14.58%
2.2.27	2014	1,357	9.15%
2.4.29	2017	1,177	7.94%
2.2.3	2006	1,100	7.42%
2.4.18	2015	1,098	7.40%
2.2.22	2012	711	4.79%
2.4.7	2013	397	2.68%
2.4.25	2016	389	2.62%
2.2.31	2015	377	2.54%

それでも、悪いことばかりではありません。ICER全体で1,500社近くが所有するパブリックIPv4スペースをマッピングしたところ、重大なエクスポージャーがあったのは、 611社（40%以下） と少数でした。老朽化するITアプリケーションやインフラを、最新のコンポーネントに置き換える企業が増えると同時に、この割合はさらに低下すると見込んでいます。

インターネットセキュリティの分類

サイバーセキュリティ分野の進歩が実証され、トレンドが正しい方向に進んでいる一方、進化のスピードは遅いままです。コネクテッドテクノロジー利用の大幅な拡大、自動化された非標的型攻撃のまん延、極めて精巧で資金力の高い攻撃者、そしてシステムの複雑化という観点から見ると、進歩の速度は遅すぎるといえます。私たちは、サイバーセキュリティーを（障害物ではなく）ビジネスを成功させる重要な手段、また安全で安定した社会の構築に欠かせない要素と捉え、努力を続ける必要があります。

そこで、私たちがビジネスを行い、文化を表現し、また日々の生活を送る上でこれまで以上に頼りとする、この先進的なグローバル通信ネットワークの全体的なセキュリティ体制には、どのような特徴があるのかを見てみましょう。最終的には、本レポートで審査した24のプロトコルすべてで測定された、4つの基準にまとめられます。その基準とは、インターネットをベースとするサービスの設計、展開、アクセス、保守です。

暗号化への対応

インターネットは1960年代に発明され、1990年代に急激に拡大し、21世紀を通じて成長と変化を続けています。その進化の中で、多くの大学、企業、および個人が、公共ネットワークを通したデータの送受信における新たなソリューションを開発してきました。しかし、サービスの設計にセキュリティの概念がある程度組み込まれるようになったのは最近のことです。インターネットの新しいサービスを設計するうえで最も重要な要素は、2つの機能を備えた最新の暗号化技術を取り入れることです。暗号化の第1の機能は、コミュニケーションとデータの機密性を高め、パブリックインターネットを横断する際に盗難や変更されないようにすることです。第2に、暗号化によるコントロールが、安全な会話に関わるマシンや人のアイデンティティを確立することです。 つまり、 銀行のマシンだと名乗るものが本当にそうであり、銀行側もあなたが本当にあなた自身であると確かめることです。 「クリアテキスト」通信と呼ばれる、 暗号化が使用されていない状況では、機密性およびアイデンティティのどちらも、有意義な形で証明することはできません。

- *調査結果：*24種類のサービスプロトコルの技術評価により、世界中に流されている情報の全体のうち、**暗号化されていないクリアテキストプロトコルが、決して例外的な少数派ではなく、依然として多数派となっています。**つまり、プレーンテキストのHTTPサーバーが、HTTPSサーバーより42%も多いことが判明しました。300万ものデータベースが安全でないクエリを待機し、290万のルーター、スイッチ、サーバーがTelnet接続を受け入れています。
- *推奨事項：*インターネットに接続する場合は、暗号化を行う必要があります。これは、データ、サービスのID、すべてに当てはまります。

サービスの展開

これは、私たちが最も時間と努力を費やして測定する領域です。 インターネット上にはどのようなサービスがあり、誰がそのようなサービスを受けられるのかを見ます。インターネットは分散型のオープンデザインで作成されましたが、この開放性は諸刃の剣です。一方では、インターネット全体の破壊を非常に困難にします。一部が破損、破壊されても、インターネットというのは単純にその破損部分を迂回して、他のサービスやユーザー向けに機能し続けます。その反面、悪意のある攻撃者が操作するものも含め、すべてのコンピュータは他のコンピュータにアクセスしたり情報交換を行ったりできるのです。そのため、データベース、コマンド、コントロールコンソールなど、誰もがアクセスできるはずではないサービスや、外部の人には全く関係のないサービスを見つけた場合、それを危険な露出としてマークします。

- *調査結果:* **安全でないサービスの数が過去1年間で減少した**ことは良いニュースです。つまり、数百万単位の人がテレワークへ突然移行したことと、在宅環境でIoTデバイスが継続的に増加していることで新たにTelnetやSMBなどの安全でないサービスが外部に公開されているにもかかわらず、SMB、Telnet、rsyncなどのリスクの高いサービスが平均で13%減少し、懸念されていた大惨事は免れました。
- *推奨事項:* 対策の継続です。ISP、企業、および政府は、これらの不適切なサービスをインターネットから排除するために引き続き協力を行う必要があります。

コンソールアクセス

インターネットの構築で最初に行われたのは、リモートシステムのオペレーターが、遠隔のコンピュータにログインし、コマンドを実行し、結果を得られるようにすることでした。リモートアクセスの対象となるコンソールの安全性よりも接続性の方が重要でした。今日、コンソールアクセスを見つけると、セキュリティの専門家はそのエントリポイントを懐疑的に見る傾向があります。少なくとも、Telnet、SSH、RDP、およびVNCのコンソールは、何かしらの二要素認証やコントロールを組み込むことで、インターネットベースの攻撃者に対する耐性を強化するべきです。通常、仮想プライベートネットワーク（VPN）コントロールを組み込むことで、直接的なアクセスの可能性を排除することができます。攻撃しようとする者はまず、暗号化によってセキュアになったVPN層を破らなければ、パスワードを試したり、認証の脆弱性を悪用したりするコンソールを見つけることもできないからです。そういった最初の防衛線が欠けているサービスでは、「ドアノブをガチャガチャ」と動かしてみて、ロックがどれほど頑丈かを確かめるような攻撃者を安易に受け入れてしまいます。自動化された攻撃では、1秒間に世界中にある何千ものドアノブに手をかけることができるのです。

- *調査結果:* インターネット上で、現在もアクティブで利用可能な**Telnetサーバーをほぼ300万個**も検出しました。それらの多くは、**コアルーティングとスイッチングギア**に関連しています。その数は300万を超えています。リモートコンソールアクセスはインターネットの基本的な設計上のゴールです。しかし、インターネットをうまく動作させるのに最も重要な役割を担っているルーターとスイッチにとっては、このような古代的な技術に依存させたままにしておく理由がありません。
- *推奨事項:* Telnet、SSH、RDP、VNCはすべて、少なくとも1つのセキュリティレイヤーを追加する必要があります。つまり、多要素認証を導入するか、またはVPN接続環境でのみ使用可能にするべきです。

ソフトウェアのメンテナンス

私たちはよくインターネットについて、世界中で情報を交換する仕組みという観点から話をします。しかしながら、この仕組みの耐久性が非常に高いのだということを思い出してください。これらは、消耗期間があるような物理的にピストンやギアで構成されているものではなく、主に個体で構成され動力部品のない電子機器です。機械的な動作を伴うとしても冷却ファンの部品くらいのものです。このような仕組みは、インシデントや人間による操作なしで何年も稼働し続けることができます。当然のように動作する機能のようにも見えるかも知れませんが、実際にはこれが過信を招くことがあります。これらのハードウェアを動作させる複雑なソフトウェアには、パッチ、アップグレード、そして最終的にはハードウェアの交換という形での定期的なメンテナンスが必要です。セキュリティと安全な設計概念に関する知識と理解が深まるにつれ、そのビジネス、学術、または文化に関する要件を満たすために、新しいソフトウェアを展開する必要が生じます。残念ながら、多くのインターネットサービス分野で、定期的メンテナンスが大きく欠如していることが分かりました。数十年前の脆弱性のままのソフトウェアが使用されており、悪用されるのは時間の問題です。

- *調査結果：***パッチとアップデートへの対応はさらに遅くなってきています。**実際に悪用が起きていることが報告されている最新のサービスに対してもそのことが言えます。これはとりわけ、例として、360万ものSSHサーバーが、5〜14年経過した脆弱なバージョンを使用した電子メールの処理とリモートコンソールアクセスを行っている部分に当てはまります。さらに厄介なのは、米国、英国、オーストラリア、ドイツ、および日本の上場企業が、とりわけ**金融サービス**と**通信**において、既知の脆弱性を抱え、パッチ適用されていないサービスを驚くほど多数ホスティングしていることです。外部公開されている資産の全体に対してCVEを評価しました。ふんだんな資金と専門知識を持った人材を抱えた巨大な組織であるにもかかわらず、このレベルの脆弱性のサイバーエクスポージャーに関しては、世界的に不況が襲いかかってきている時代に改善される可能性は低いでしょう。
- *推奨事項：*すべてのソフトウェアにはバグがあり、パッチ処理が必要であることから、企業はインターネットに面するインフラに定期的なパッチ作業時間と稼働停止スケジュールを組み込む必要があります。

インターネットに迫る災害

上記のようなインターネットエンジニアリングの観点から、さらなる努力が必要なことは明らかです。この1年間でインターネットは徐々に改善され、現代のインターネットにあふれる生物学的および経済的な危機、脆弱性、そしてエクスポージャーには耐えているように見えます。このようなエクスポージャーは、不十分な設計の古いソフトウェア、重要な「バックエンド」サービスの過剰な有用性、コントロールされていないオペレーティングシステム・コンソールのアクセスポイントと定期的なパッチやアップグレードといったメンテナンスの欠如を通して、深刻なリスクをもたらし続けます。

さらに、インターネットベースの攻撃者が、このような設計、展開、アクセス、保守の欠点を十分に把握しており、すでに何の報いも受けずに、インターネット上の弱い標的を悪用していることは、私たちも分かっています。有効な「インターネット警察」がパトロールをしているわけではありません。つまり、インターネットインフラの安全性は、世界中のITおよびサイバーセキュリティの専門家、そして彼らへの技術の伝授、訓練、助言、そして金銭的援助にかかっているのです。

これは、とても重要な調査結果です。24種類のそれぞれのプロトコル、コンソールアクセス、ファイル共有、電子メール、グラフィカルリモートアクセス、データベースサービス、コアインターネットインフラストラクチャ、およびWebの7つのサービスカテゴリについて、具体的で実用的なセキュリティアドバイを提供します。本レポートから、他に何も得るものがなかったとしても、これだけは理解して頂きたいと思います。インターネットは、自動的に金銭や文化を生成する機械ではないということです。その裏には、高い技術力を持った多くの犯罪者やスパイから日々攻撃されながらも、インターネットの健全性を保とうとする多くのプロたちの奮闘があるのです。

政策担当者の役割

世界各国の政府で規制の推進や施行、予算と調達の優先付け、および助成金の監督に携わる政策担当者は、インターネットのセキュリティにおいて重要な役割を担っています。セキュリティは技術だけでなく、進化を続けるセキュリティの世界に関する最新かつ正確な情報、また複雑なセキュリティの課題のソリューションについて専門家の指示を仰いだインセンティブ、情報共有、そしてリーダーシップの融合によって実現されます。では、立法行政機関はどうすればそのような調査結果を学ぶことができるでしょうか。その答えがここにあります。

NICER2020は、本質的に欠陥がある、またはインターネットに露出するにはあまりにも危険な FTP、Telnetなどオープンでセキュリティが不安定など、官民両セクターの安全性に直接的影響 を与えるプロトコルのリスクと、世界的な拡大状況をまとめたものです。政策立案者は、現在のインターネットに関する調査をまとめた本レポートを参考に、十分な情報を持ったうえで、オンラインのプライバシー、セキュリティおよび安全性に関する意思決定を行うことができます。この情報を官民における組織的な高リスクプロトコルへの依存軽減、既知の脆弱性やエクスポージャーの回避、また**よりセキュアなプロトコルの導入を推進するのにご活用ください。活用方法の例をいくつかご紹介します。**

- セキュリティやプライバシーに関する規制の施行において、特定の高リスクプロトコルやソフトウェアアプリケーションの使用に関するガイダンスを示す
- 政府のITシステム内にある高リスクプロトコルやアプリケーションを審査し、政府システムのプロトコルの安全性強化と近代化を進める
- 政府のITシステムで検知されているエクスポージャーを軽減するため、各省庁の取り組みを監督する
- 問合せ、監査、その他民間部門のセキュリティに関連するアクションにある危険なプロトコルへのエクスポージャーを考慮する
- 既知のエクスポージャーや危険なプロトコルの地域的拡散状況データを活用し、多国間の脅威に関する情報共有を強化する
- クリアテキスト、国家の安全保障、経済、消費者保護に対する危険かつ本質的に安全でないプロトコルやアプリケーション影響、またエクスポージャーの低減で組織が直面する課題に関して、さらなる研究を指示する

エクスポージャーの測定：プロトコルごとの分析

ここからは、7種類のサービスにおける TelnetからDNS-over-TLSまで、全24のプロトコルを詳細にわたって分析します。まず、各プロトコルを提供するサービスの原数値を、2019年の同時期と比較します。次に、各プロトコルのセクションで、そのプロトコルの「TLDR」（概要）を以下の項目に沿ってまとめます。

- プロトコルの目的
- 見つかったサービスの数
- 当該プロトコルの一般的なプロフィール
- ビジネス機能でプロトコルに替わるもの
- 当該プロトコルに関するアドバイス
- 展開の観点から、状況が改善または悪化しているかどうか

以上の概要の後、これらのプロトコルを国別、クラウド別、バージョン別に、調査結果のデータと分析を行います。これらの分析は、それぞれが優れた研究論文にもなり得る内容ですが、ここではそれをすべてお読みいただけます。それでは、サイバーセキュリティという名の深海に一緒に潜っていきましょう。

前年比で見るインターネットサービス

ある時点のエクスポージャーを見ることにも多くのメリットがありますが、Rapid7 Labsチームは、*多くの変化が生じたことから*、2019年4月と2020年4月の比較に非常に興味がありました。

レポートの作成では、グローバルパンデミックと差し迫る世界的不況に関して、人々が在宅勤務を余儀なくされたことで「RDPサーバーが増加する」ものの、GUIコンソールへのアクセスは引き続き必要であるとか、遠隔の労働力を組み込むために人々が慌ててWindowsのワークフローを再構成したことから、「SMBが急増する」など、いくつかの仮説を立てました。結局、私たちの *予想は大きく外れました*。以下の表では、2020年の調査対象となったプロトコルが、2019年の同時期のサンプル調査と比較して増減、 主に減少 していることが分かります。

SONAR 調査	ポート	2019	2020	変化	割合
SMB	445	709,715	594,021	-115,694	-16.30%
Telnet	23	3,250,417	2,830,759	-419,658	-12.91%
rsync	873	233,296	208,882	-24,414	-10.46%
POP3	110	4,818,758	4,335,533	-483,225	-10.03%
SMTP	25	6,439,139	5,809,982	-629,157	-9.77%
IMAP	143	4,296,778	4,049,427	-247,351	-5.76%
SMTP	587	4,220,184	4,011,697	-208,487	-4.94%
RDP	3389	4,171,666	3,979,356	-192,310	-4.61%
POP3S	995	3,887,033	3,717,883	-169,150	-4.35%
IMAPS	993	4,008,577	3,852,613	-155,964	-3.89%
MSSQLサーバー	1434	102,449	98,771	-3,678	-3.59%
SMTPS	465	3,592,678	3,497,791	-94,887	-2.64%
DNS (Do53)	53	8,498,166	8,341,012	-157,154	-1.85%
FTP	21	13,237,027	13,002,452	-234,575	-1.77%
NTP	123	1,653,599	1,638,577	-15,022	-0.91%
FTPS	990	443,299	460,054	16,755	3.78%
SSH	22	15,890,566	18,111,811	2,221,245	13.98%
DNS over TLS (DoT)	853	1,801	3,237	1,436	79.73%

表の説明を行う前に、少なくともコアサービスに関連した部分では、**インターネットの安全性が向上している**ということを喜んでお伝えします。ひねくれ者のセキュリティのプロとして、書き慣れない文章です。しかし、データはうそをつきません。では結果を見ましょう。

まず、「変更の割合」の列で、ハイライトされていないサービスがいくつかあります。付録の「**調査方法**」のセクションにある通り、インターネットのスキャンには危険が伴います。私たちは過去6年にわたってあるスキャンがどのように「おかしい」かを理解するのに十分なスキャンデータを収集しました（クラウドプロバイダのダイナミックサービスプロビジョニング増加に伴い、年々悪化しています）。Project Sonarの各調査にはそれぞれの精度範囲がありますが、全体的に+/-4%の差異がある場合、何かが「上がった」または「下がった」という絶対的な記述ができないということになります。しかしながら、ほとんどのサービスの数値は、その範囲から大きく外れていました。

Microsoft SMBは、主にISPによるSMBポートのブロックにより、エクスポージャーは20%近く減少しました。しかし、現在もSMBサービスを露出しているWindowsやLinuxシステムは50万件以上もあるので、喜ぶのは*まだ早い*です。

過去4年間にわたり、皆さまに使用をやめるよう訴えてきたTelnetが15%近く減少したことは喜ばしいことです。しかしまだ、残りの280万というかなりの数のルーターやスイッチといったデバイスがTelneによって露出されています。このようなサービスが1999年の設定モードのままだからと言って、私たちまでその年に縛られるべきではないのです。

人々が自身のメールインフラをホストすることを止めているのは、喜ばしいことです。このように、Outlook 365やG Suiteなど、プロフェッショナルなメールサービスのホストへの移行は、突然のロックダウンにより加速されたという可能性もありますが、メールの中央集中化はそれ以前から始まっており、今後も続くと予想しています。

SSHが13%増加したことについては、少し懸念があります（SSHサービスと、それをホストするオペレーティングシステムの脆弱性がいかに深刻かについては、**SSH**セクションを参照してください）。今後は、Linuxの流通がUbuntuを模倣し、安定したリモートシステムの接続には、SSHと同等またはそれ以上に安全でセキュアなWireGuard[6]を採用することで接続性も向上し、時間の経過とともにSSHが減少することを期待しています。

最後に、DoTサーバー数が過去1年間に2倍近くに増加したことは想定していたことで、2021年にはさらに2倍（またはそれ以上）になると見込んでいます。

このように、パンデミックによるロックダウンや経済的な不透明感の中で、人々の働き方やインターネットの利用が大幅に変化したものの、インターネット自体の性質や特徴に大きなシフトは見られませんでした。結局のところ、インターネットは世界的な災害を考慮して設計されており、その点では素晴らしい仕事をしているようです。

次は、プロトコル別の分析に移ります。いつも通りの悲観的な見方に戻りましょう。

コンソールアクセス

当初、「I」が大文字だった時代のインターネットの目的は、1つのテキストベース型端末からもう1つの端末への接続を容易にして、オペレータが「ここ」でコマンドを入力して、「あっち」で実行できるようにすることでした。私たちは通常、（小文字の「i」で始まる）インターネットを、（大文字の「W」で始まる）World Wide Webとは区別ができない、読み取り専用テキスト、画像、音声、動画にあふれたものとして考えます。インタラクティブなマルチメディアアプリケーションができたのは、しばらく後のことです。リモートシステムのログインインターフェースに接続することが、最初のインターネットの基本的な機能でした。このリモートターミナルへのアクセスという遺産は現在も残っていますが、あまり良いものではありません。

TELNET（TCP/23）

最初のコンソールプロトコルではありませんが、最も厄介なものです。

TLDR

説明：	今日インターネットで使われている中で、最も古いリモートコンソールアプリケーションの1つです。
数：	282万9,555のノードを検出しました。 合計36のサービスグループで38万9,528（13.7%）にRecogフィンガープリントがありました。
脆弱性：	不思議なことに、リモートコード実行型の脆弱性は少なかったものの、デフォルトの認証情報と盗聴の機会は多くありました。
アドバイス：	決してTelnetをインターネットに露出させてはいけません。
代替手段：	SSH（セキュアシェル）は、最も分かりやすいTelnetの代替手段ですが、それ以前にコンソールアクセスをインターネットに露出するということについて考えてください。
傾向：	改善傾向。エクスポージャーは2019年から13%減少しました。

[6] <https://www.wireguard.com/>

調査結果の詳細

RFC 15の時代、[7]Telnetは「ネットワークシステムプリミティブ周辺のシェルプログラムで、リモートホストにあるテレタイプまたは同様の端末がサービングホストのテレタイプと同じように機能できるようにするもの」と説明されていました。このRFCからも分かるように、これは元々一時的なソリューションであり、「より洗練されたサブシステムがそのうち開発される」と考えられていました。しかし、ミルトン・フリードマンの言葉を借りるとすれば、一時的な解決策ほど永続的なものはないのです。リモートコンソールアクセスは、今日のインターネットでも求められており、最も基礎的なレベルでそれを実現してくれるTelnetが、50年経った今もまだ使われているのです。

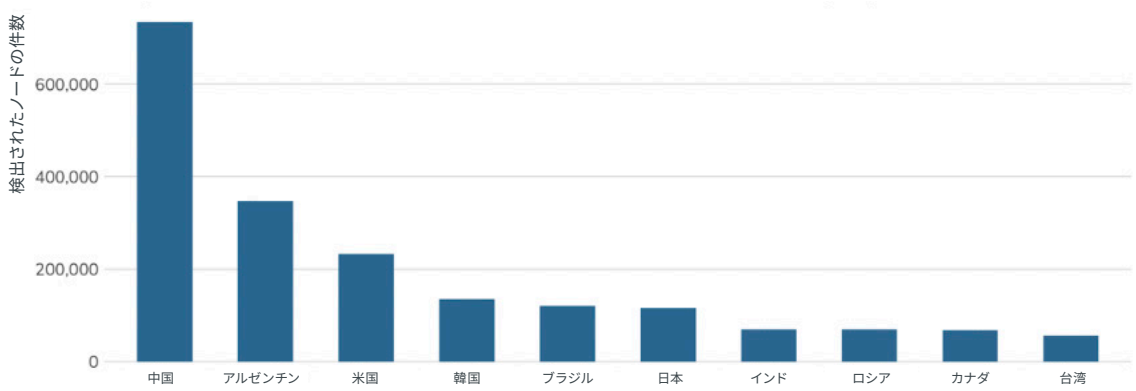
エクスポージャー情報

半世紀にもわたって使用されている割に、表向きには（サーバーとしての）Telnetが経験した脆弱性の危機は比較的少ない。CVEデータを軽く見ても、CVSSスコアが5以上の脆弱性は10件しかありませんでした。しかし、Telnetには根本的な欠陥がいくつかあります。1つは、通常ほぼクリアテキストプロトコルであるため、認証情報（ユーザー名とパスワード）とデータの両方が受動的盗難の危険にさらされます。また、もし攻撃者がトラフィックに中間者攻撃（MITM）を仕掛けられる立場になった場合、ストリーム内でコマンドやレスポンスを置き換えることも比較的容易です。本質的に、Telnetにはセキュリティに関する保証を、ほぼまたは全くしていないため、逆に言えば、コード自体の脆弱性は比較的低いことになります。

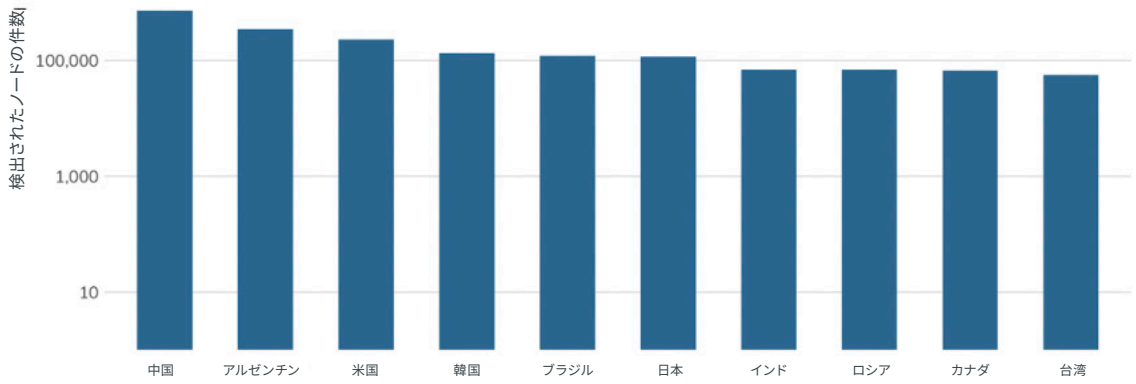
Telnetに関するさらに大きな問題は、実際にはデフォルトのユーザー名とパスワードがありがちなもの過ぎるため、Telnetサーバーを目にすると、誰もがそうであると考えるということです。これが、2016年のMiraiワームの中心的な仮設です。Miraiは、Telnetでよく使われるデフォルトのユーザー名とパスワードの短いリストを使い、TwitterやNetflixなどのインターネット大手を、事実上偶然にも襲うことができました。

以下の表では、中国が単独で非常に深刻なTelnet問題を抱えており、それにアルゼンチンと米国が続いていることが示されています。

コンソールアクセスにおける上位10か国：TELNET（23）



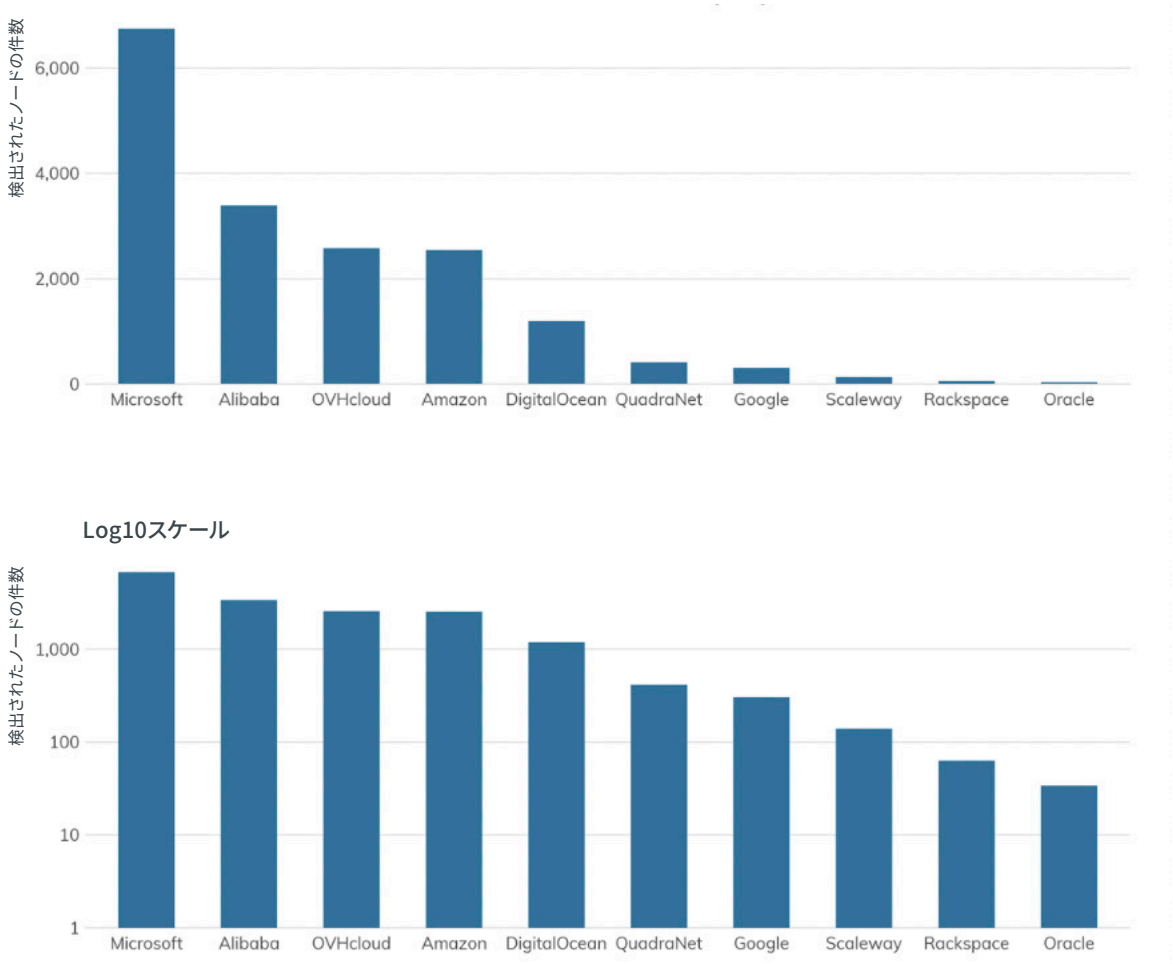
Log10スケール



[7] 人の暦でいうと、1969年9月になります。

クラウドサービスプロバイダがTelnetを一切使用しないというのが理想ですが、ある程度の進歩が見られます。ランキングのトップは、7,000件のエクスポージャーがあるMicrosoft Azureです。Windowsプラットフォームは通常Telnetサーバーが内蔵されていないことから、これは少し妙な結果です。

クラウドプロバイダのコンソールアクセス：TELNET（23）



インターネット上で見つかったTelnetのインスタンスで、ベンダー別に確信をもって識別できたもののうち、以下の表では、最低1万件のレスポンスノードがSonarに表示されたベンダーのサービスを示しています。

ベンダー	数
Cisco	278,472
ファーウェイ	108,065
MikroTik	73,511
HP	70,821
Ruijie	17,565
ZTE	15,558

これらの数値で興味深いのは、インターネットに露出されているTelnetサービスのほとんどが、コアネットワーキングギアベンダーと深く関係していることです。CiscoとHuaweiは、ともに世界最大手のルーターメーカーで、すべてのTelnetサービスの合計数を占めています。さらに、Ciscoのデバイスの14%、そしてファーウェイのデバイスの11%が、現在でもデフォルトの認証情報でアクセスできるということが示されています。このような、世界中の数千にも上る組織の中枢が十分に保守されていないというのは残念な結果で、これらのデバイスはすべて、すでに攻撃されていると見なされるべきです。

Telnetがいまだにインターネット全体で広く使われている一方、一部のISPが、比較的気軽にサービスを提供していることが分かります。以下の表は、ネットワーク内で1万件以上のTelnetサービスをホストしている地域的ISPを示しています。さらに、これらのエクスポージャーの大半は、クライアントベースのエクスポージャーではなく、ISPが提供するコアルーティングとスイッチングギアがホストとなっています。このようなやり方（または見落とし）は、これらのプロバイダを発信元または発信先とするクライアントのネットワークトラフィックを、攻撃の危険にさらします。

ISP/プロバイダ	数	以下に割り当てられたASN
Telecom Argentina	1,320,360	AR
China Telecom	282,897	BY、**CN**、GB、HK
中国聯合通信	183,290	**CN**、GB、HK
Tencent	130,620	CN
Korea Telecom	81,392	KR
Cox Communications	78,442	US
アルテリアネットワーク	68,598	JP
LG UPlus	56,434	KR
British Telecom	53,020	**GB**、NL
AT&T	43,517	BR、CZ、DM、MR、RO、TH、US
HiNet	42,150	TW
Guangdong Mobile	39,197	CN
Claro	37,469	**BR**、CL、ES、MX、PA
Uninet	37,204	AZ、**MX**
VNPT	35,640	VN
中国移動通信	35,247	**CN**、HK、RU
Hathway IP Over Cable Internet	33,428	IN
Telefonica Brazil	30,270	BR
Columbia Telecom	27,865	RU
CenturyLink	26,998	US
NTT Communications	26,757	AU、BR、HK、**JP**、MM、MY、SG、US
Total Pay Telecom	26,448	MX
Alestra	23,679	MX
Algar	23,546	BG、**BR**
Charter Communications	23,124	US
Irideos	22,570	IT
RCS & RDS	22,422	RO

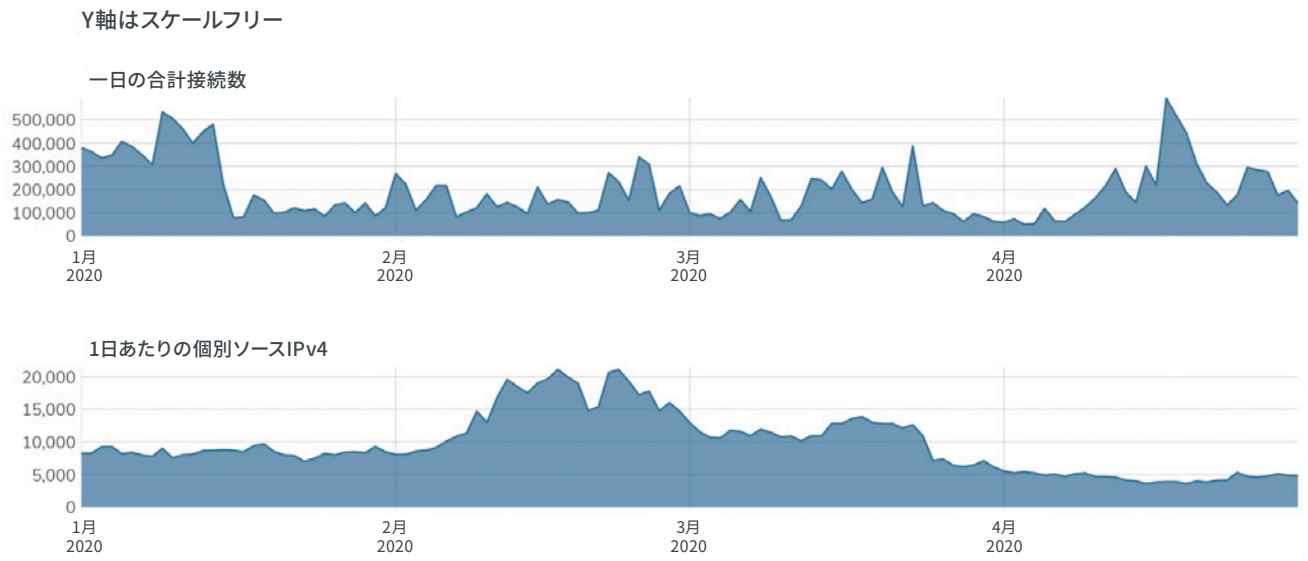
ISP/プロバイダ	数	以下に割り当てられたASN
Indonesia Telecom	19,920	ID
Rostelecom	19,597	RU
Orange	19,562	BD、BE、BF、BR、CD、CF、CI、CM、ES、EU、**FR、**GN、GW、IN、MD、MG、ML、NE、PL、RO、RU、SK、TN、UG
Corbina Telecom	19,071	RU
Vodafone	18,760	AU、CZ、**DE、**EG、ES、EU、FJ、GB、GH、GR、HU、IE、IN、IS、IT、MT、NL、NZ、PT、QA、RO、TR
Daisy Communications	18,028	GB
フリービット株式会社	17,590	JP
Turk Telekom	17,446	TR
Telecom Italia	17,042	IT、SM
Triple T Broadband	16,936	TH
Primus Telecommunications Canada Inc	16,732	CA
Comcast	15,980	DO、**US**
Verizon	15,926	GB、**US、**ZA
True Internet	15,394	TH
Compañía Dominicana de Teléfonos S. A.	15,317	DO
TalkTalk	15,120	GB
TekSavvy Solutions Inc.	15,041	CA
Telefonica De Espana	14,366	ES
Hong Kong Broadband Network LTD	13,839	HK
Level 3	13,008	BD、HK、**US**
HGC Global	12,222	HK
SK Broadband	11,972	KR
Cable & Wireless	11,550	EU、**GB、**PA、SC

攻撃者の視点

Telnetは、強力な認証や暗号化などのセキュリティコントロールが完全に欠如していることから、インターネットには全く不向きです。標準外のポートにTelnetを隠すことも、一般的には意味がありません。単にファイヤーウォールが23番ポートのエクスポージャーを禁じているという理由から、最新のTelnetスキャナは、80番や443番ポートなどにTelnetが潜んでいることは十分承知しているのです。今日、Telnetはセキュリティが低いまたは全くない低品質のIoTデバイスに最も関連付けられているものです。そのため、これらのデバイスをインターネットに露出するということは、少なくとも、その組織には厳格なセキュリティ体制がないことを示します。

ハニーポットネットワークを見る限り、攻撃者はMirai攻撃が数十万台のデバイスをオフラインに追いやってから4年経った今でも、積極的にTelnetサービスを探し続けています。以下に示されているトラフィックの約90%は、一般的なユーザー名とパスワードで試行された基本的アクセスです。急増が見られる部分は、公開されている他の認証情報のダンプから引き出した、新しいユーザー名とパスワードの組み合わせを使用したクレデンシャルスタッフィング攻撃の集中を表しています。[8]

TELNET（TCP/23）HEISENBERGの活動



アドバイス

ITとITセキュリティチームは、標準的なTelnetポートのブロックとディープ・パケット・インスペクション（DPI）ソリューションの両方を通じて、できる限りネットワーク上のTelnetトラフィックを両方向でブロックしてください。また、Telnetサービスの監視を続け、攻撃的なデバイスを追跡してTelnet接続を無効にする必要があります。Telnetを最新のインターネットに露出しなければならない理由はありません。稀に、ネットワークオペレーターがインターネット上でテキストベースのコンソールに誰かをログインさせたいという場合には、十分に保守されたSSHサーバーの方が、はるかに信頼性が高く、柔軟で、安全です。

クラウドプロバイダは、上記の組織と同様のオペレーションを実践するべきです。全てのTelnetトラフィックを、自動的な技術的手段によってデフォルトで禁じることです。現在もTelnetを頼りにしているというクライアントがいるかも知れませんが、その場合は、丁寧かつ確実に、SSHベースの代替手段に切り替える必要があります。最終的に、Telnetを利用しているクライアントが、最新版のWindows、OSX、Ubuntu Linuxにデフォルトでアクセスできないのには理由があります。ですから、ホストされたマシンにTelnetがないことで困る人はほとんどいません。

政府のサイバーセキュリティ機関は、コアネットワークオペレーションのハードウェアに不当な量のTelnetアクセスを提供するISPを積極的に追跡し、そのようなオペレーターには厳しく注意し、必要であればSSPのセットアップ方法が記載された危険回避のための通知を発行してください。ISPは、現時点ですでに把握しているべきです。

[8] 関連するXKCD：https://xkcd.com/2176/、「ハッキングの仕組み」

セキュアシェル（SSH）（TCP/22）

まさに名前に「セキュア」が入っています。

TLDR

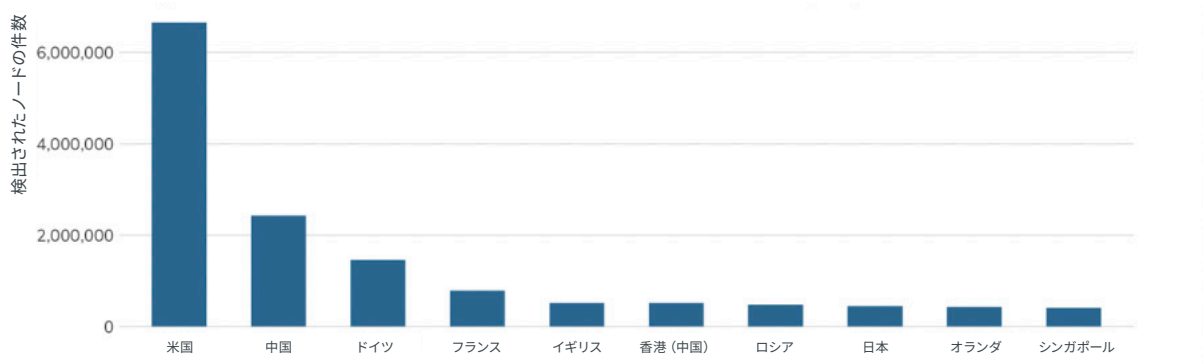
説明：	SSHは通常、Telnetに替わる安全な手段ですが、事実上どのようなプロトコルも暗号化セキュリティという、温かくて安心できる毛布で包むことができます。
数：	1,787万456のノードを検出しました。 1,703万3,109（95.5%）にRecogフィンガープリント（合計36のサービスグループ）がありました。
脆弱性：	Telnet同様、SSHと関連付けられるエクスポージャーは通常、デフォルトのパスワードとパスワードの再利用が原因です。また、SSHは特定のオペレーティングシステムの暗号ライブラリに存在する脆弱性を表面化させる傾向があります。
アドバイス：	SSHを慎重に展開し、安全なパスワードやプライベートキーの生成と保守に備えたシステムを確立してください。
代替手段：	代替手段もいくつかありますが、SSHは無料のオープンソースで、かつ学術的および商業的なソフトウェア開発者のネットワークによって十分に保守されています。SSHの代替手段として妥当なものは、特にSSHが安全でないプロトコルもカバーできることを考えると、考えにくいというのが現実です。
傾向：	改善しているかどうか不明。2019年からは14%増加しているものの、それが十分であるかどうかは不明です。

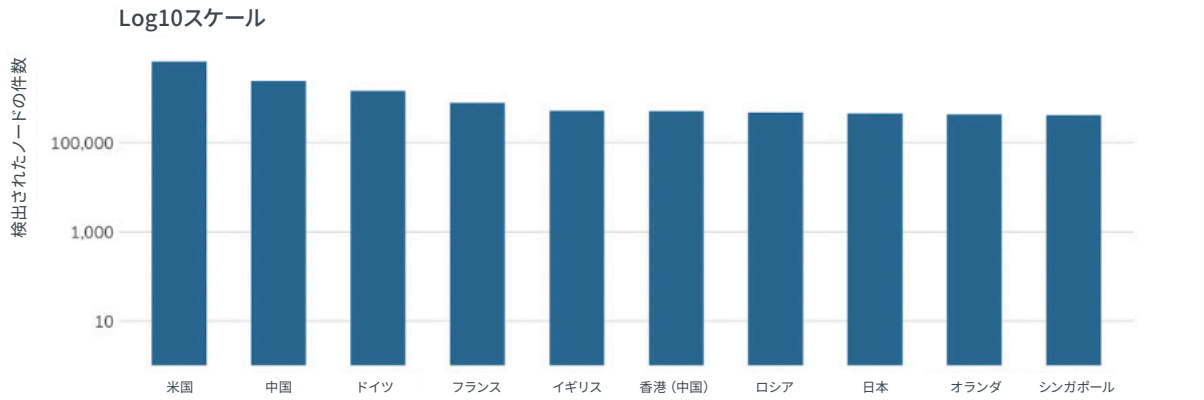
調査結果の詳細

一般的にSSHと呼ばれるセキュアシェルは、Telnet、rlogin、FTPなどのクリアテキストプロトコルに対抗する、認証情報の受動的盗難防御手段として1995年に設計および開発され、一般に広がりました。単純に暗号化の安全性を備えた、Telnetの一時的な代替手段として一般的に考えられていますが、アプリケーションのSSHスイートは、ファイル送信のSCPなどのネイティブアプリケーションやSSHトンネリングを通して、事実上どのようなプロトコルも、安全なものにしたり、置き換えたりできます。

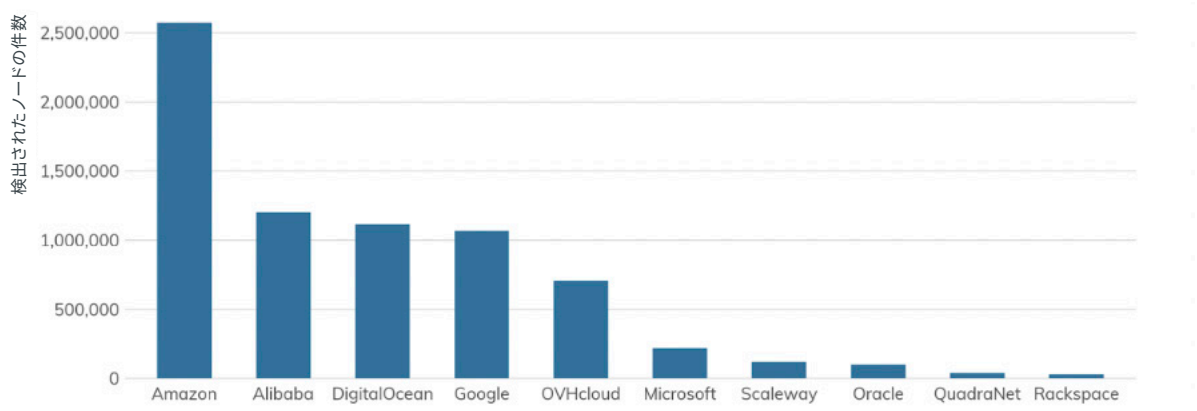
本レポートの分析で注目すべきポイントの1つは、SSH展開が今やTelnetのエクスポージャーを6対1の割合で上回ったという事実です。インターネットからの直接的なコンソールアクセスが最も賢明な手段ではない一方で、このような露出されたシェルの85%がセキュアシェルで、あらゆる盗難、スプーフィング、およびトランジット内のデータ操作を排除するということを、人々が理解したと受け取れます。インターネット、そして中でも米国中のネットワークオペレータを褒めたいです。 米国のSSHサーバー（660万）とTelnetサーバー（わずか23万2,000）のエクスポージャー比率は、28対1になりました。これを中国の3対1（SSHが240万、Telnetが73万4,161）と比較してみてください。SSHがコンソールアクセスと他のプロトコルの安全性確保を可能にする一方、Telnetはほぼコンソールアクセスのみに使用されているということを考えると、米国の比率は素晴らしいものです。

コンソールアクセスにおける上位10か国：SSH（23）

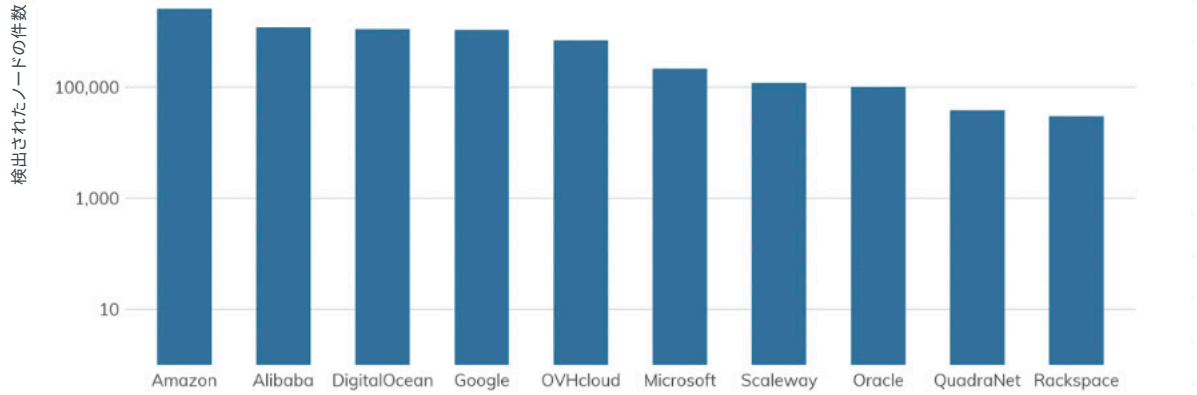




クラウドプロバイダのコンソールアクセス：SSH（22）



Log10スケール



エクスポージャー情報

より複雑で、明確にセキュリティを保証するSSHにも、独自の脆弱性があります。メモリ安全性が備わっていない言語で書かれた他のネットワーク同様、従来型のスタックバッファオーバーフローが発生する場合があります。さらに新たな脆弱性は、実装時にデフォルト以外の設定オプションの組み合わせに表れたり、コミュニケーションを安全にするためSSHが使用する暗号ライブラリ内の脆弱性を通して発生することがあります。しかし最も一般的なSSHの脆弱性はよく、Telnetから（正しく）離れたIoTデバイスに搭載された、ベンダーが提供する変更不可能なユーザー名、パスワード、そしてプライベートキーと関連付けられます。これはつまり、暗号の使用だけでセキュアシェルが魔法のように安全なものになるわけではないということです。SSHがよく使われる環境では 、なぜかパスワードの再利用が一般的であるため、パスワードとプライベートキーを保護することは、本当に安全なSSHベースのインフラを維持するうえで重要となります。

上記の通り、管理者やデバイスメーカーも、可能な限りクリアテキストのものではなく、オープンで無料のSSHを標準化するよう、強く推奨されています。IoT、OT、ICS機器は特に、安全なサービスを実行する暗号化のオーバーヘッドに対応するのに必要なローカルリソースが足りないと言われています。しかし、もしそれが本当なら、このようなデバイスはそもそもインターネットに接続されたネットワークに露出されるべきではありません。上記でも述べましたが、デフォルトの再利用されたパスワードなど安全性の低いプラクティスを、単純にクリアテキストプロトコルから「安全な」プロトコルと移行するだけでは不十分です。暗号がもたらす安全性は、使用する主な材料の質によるのです。

インターネットで発見されたSSHサービスのうち、以下の表にあるものが99.9%以上を占めています（ここでは最低1,000のフィンガープリント可能なサービスのみを表示）。

サービス FAMILY	数	割合
OpenSSH	15,747,821	92.238%
Dropbear	1,250,254	7.323%
SSH	37,884	**0.222%**
WinSSHD	10,408	0.061%
WeOnlyDo	6,510	0.038%
iLO	6,495	0.038%
セキュア FTPサーバー	3,507	0.021%
NetScreen	2,298	0.013%
埋め込みSSHサーバー	2,044	**0.012%**
SSH Tectia Server	1,942	0.011%
libssh	1,586	0.009%
VShell	1,064	0.006%

攻撃者の視点

SSHはTelnetよりも優れたコンソールアクセス方法を提供しますが、それでも多くの機能を備えたただのソフトウェアにすぎません。SSHの機能には、ログインが成功した後、コマンドプロンプトが表示されることで、攻撃者がクレデンシャルスタッフィングを実行（盗まれた認証をSSHに使用するなど）できるため、脆弱性がサービス自体を攻撃するというものもあります。そのため、Telnetで説明したものとほぼ同じ内容を繰り返すことになります（皆さまの貴重なお時間を無駄にはしません）。

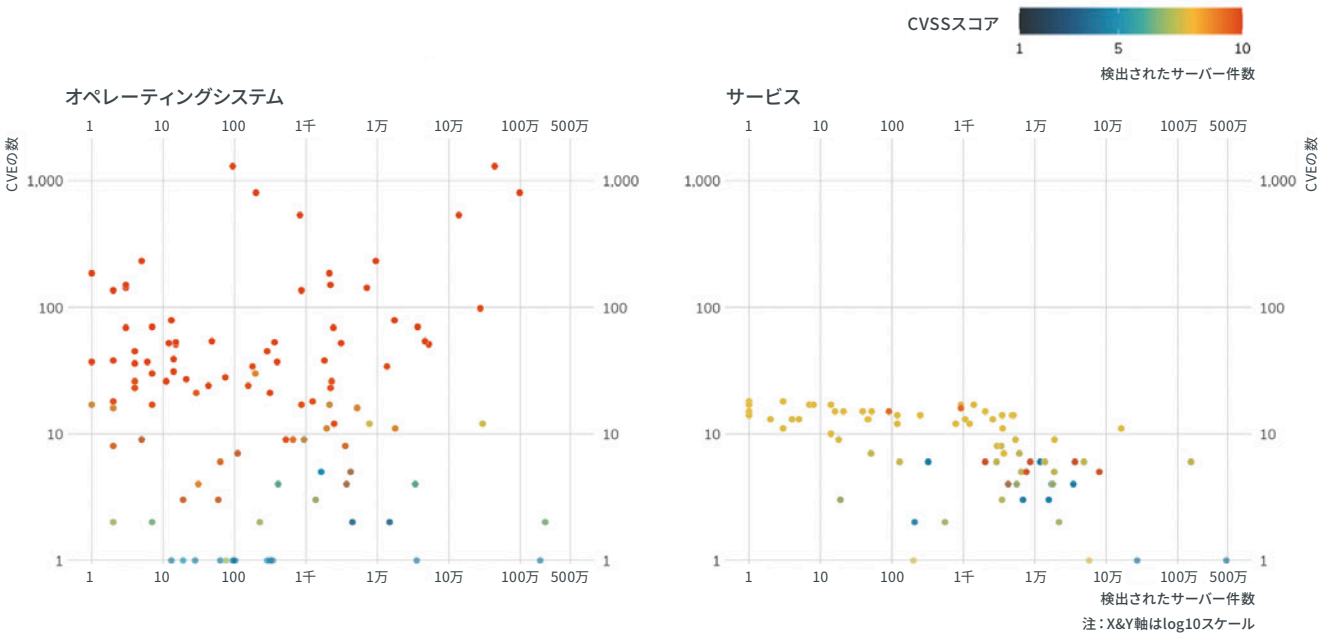
ここでできることは、フォーカスを露出されたSSHサービスに関連する脆弱性と、露出されたSSHサービスがどれほどの情報を攻撃者に与えるか、という2点に集中させることです。

OpenSSHで最も普及しているのは、バージョン7.5です。12月にリリース4周年を迎え、9つのCVEがあります。上位20のバージョンにはすべて、CVEが2〜32個あります。つまり、冷酷なインターネットに露出されている何百万個というシステム全体で、パッチ管理が大きく欠けているということです。

バージョン	数	リリース	CVEの数
7.4	4,784,909	2016年12月19日	9
7.6p1	2,286,132	2017年10月3日	8
7.2p2	1,928,745	**2016年3月10日**	**13**
5.3	1,535,299	2009年10月1日	32
7.4p1	1,023,278	2016年12月19日	8
6.6.1	609,661	2014年3月15日	22
6.6.1p1	558,341	2014年3月15日	22
6.7p1	485,255	2014年10月6日	22
7.9p1	341,816	**2018年10月19日**	**2**
7.5	271,083	2017年3月20日	9
8	195,587	2019年4月17日	2
4.3	161,884	2006年2月11日	40
6.0p1	145,874	2012年4月22日	26
7.9	141,982	2018年10月19日	7
8.1	99,243	2019年10月9日	2
5.9p1	88,520	2011年9月6日	26
6.4	79,966	2013年9月8日	28
7.7	79,399	2018年4月2日	9
7.8	67,960	2018年8月24日	8
8.2	59,804	2020年2月14日	3

「だからどうした」と思われるかもしれません。（インターネット上のエクスポージャーについて意見を述べる際、定期的に自問することです。）エクスポージャーに関する別の視点が、答えに導いてくれるかも知れません。

OS/サービス別の重大性が示されているCVE • TELNET (23) & SSH (22)



上記の数字には、かなりの情報が詰め込まれていますので、ここで2つ目のポイント（SSHサービス[9]がどれほどの情報を攻撃者に与えるか）を掘り下げてみましょう。

左パネルに表示されている「オペレーティングシステム」は、Sonar SSH接続から取得したデータ（以下に列挙）のみから、どのオペレーティングシステムが使用されているかが分かるということです。それぞれの点は、オペレーティングシステムの1つのバージョンを表しています。X軸上の位置は、私たちが見つけたサーバーの数、Y軸上の位置は、それに割り当てられたCVEの数です。重大度は色で表示されています。このグラフには、かなり多くのCVSS 8以上があります。つまり、これらのシステム（オペレーティングシステムレベル）には、優先度の高い脆弱性が多くあるということです。

右パネルも同じで、SSHバージョン（1つは上に列挙）です。数の違いは、Recogのカバレッジ[10]、と、1つのオペレーティングシステムが異なるバージョンのSSHを実行できるという事実の両方によるものです。そのため、オペレーティングシステムカテゴリまでの集約数の方が多くなります。SSHサービス内の重大な脆弱性は少ないものの、下よりも7以上、つまり非常に優先度の高いものが多くあります。

敵はこの情報を利用して、どの経路で攻撃するか、そして宝箱に追加するべく悪用できる脆弱性をマッピングします。総合的に、攻撃者がこのSSHに関するレポートを読んだら面白いと思います。

[9] この図はTelnetとSSHの両方をカバーしていますが、ほとんどのフィンガープリントはSSHのものです。

[10] SSH Recog <https://github.com/rapid7/recog/blob/master/xml/ssh_banners.xml>

OS	バージョン	数
Ubuntu	18.04	2,220,456
Ubuntu	16.04	1,890,981
Ubuntu	14.04	533,725
Ubuntu	19.1	52,026
Ubuntu	12.04	48,705
Ubuntu	19.04	36,451
Ubuntu	10.04	16,757
Ubuntu	17.1	9,467
Ubuntu	15.04	7,086
Ubuntu	17.04	5,183
Ubuntu	16.1	3,536
Ubuntu	8.04	3,314
Ubuntu	12.1	2,408
Ubuntu	11.04	2,276
Ubuntu	10.1	2,201
Ubuntu	18.1	2,192
Ubuntu	13.04	2,131
Ubuntu	14.1	2,117
Ubuntu	11.1	1,807
Ubuntu	9.1	1,234
Ubuntu	9.04	861
Ubuntu	15.1	860
Ubuntu	8.1	393
Ubuntu	6.04	303
Ubuntu	7.1	285
Ubuntu	7.04	195
Ubuntu	5.1	29
Ubuntu	5.04	5

OS	バージョン	数
Debian	9	975,722
Debian	8	436,149
Debian	10	274,752
Debian	7	137,363
Debian	6	46,054
Debian	7.8	38,543
Debian	4	17,279
Debian	5	13,526
Debian	3.1	3,089
Debian	11	1,361
Debian	3	362
MikroTik	2.9	419
vxWorks	5.1.0p1	911
vxWorks	6.9.0	288
vxWorks	1.10.0	285
vxWorks	1.8.4	47
vxWorks	6.8.0	40
vxWorks	1.12.0	24
vxWorks	6.5.0	22
vxWorks	6.0.9	14
vxWorks	6.6.0	8
vxWorks	6.0.2	7
vxWorks	7.0.0	2

OS	バージョン	数
FreeBSD	11.2	23,503
FreeBSD	12	19,360
FreeBSD	9	17,646
FreeBSD	11.1	4,687
FreeBSD	9.2	4,193
FreeBSD	8.1	3,681
FreeBSD	7.1	2,468
FreeBSD	10.4	2,179
FreeBSD	8.3	1,939
FreeBSD	8.4	1,627
FreeBSD	10	937
FreeBSD	8	656
FreeBSD	6	521
FreeBSD	4.9	312
FreeBSD	5.3	155
FreeBSD	4.11	110
FreeBSD	4.7	74
FreeBSD	5.5	63
FreeBSD	4.8	43
FreeBSD	5.2	21
FreeBSD	5	14
FreeBSD	4.6	14
FreeBSD	5.1	11
FreeBSD	4.5	7
FreeBSD	4.3	6
FreeBSD	4.4	4

アドバイス

ITとITセキュリティチームは、クリアテキスト端末とファイル転送プロトコルが見つかり次第、積極的にSSHの代替手段へと切り替えてください。交換することが不可能であれば、そのようなデバイスはパブリックインターネットから削除してください。

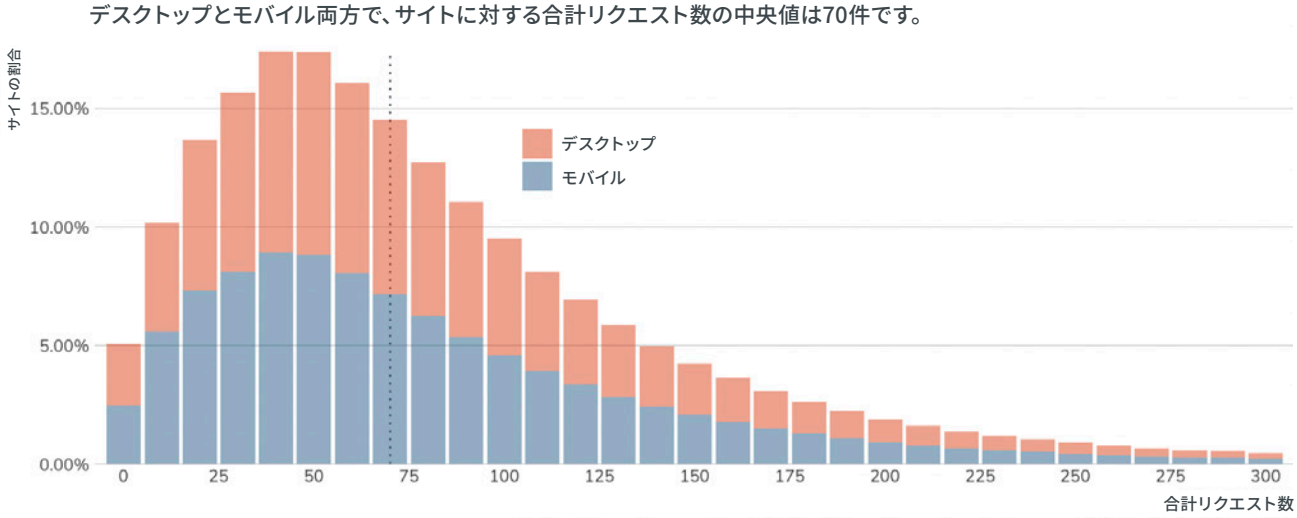
クラウドプロバイダは、あらゆる種類のコンソールやファイル転送アクセスの簡単なデフォルトとしてSSHを提供し、クライアントがどのように他のプロトコルをSSHトンネルに組み込むことができるかを、具体的な例とデフォルトで安全な設定方法を示した参考資料とともに供給してください。

政府のサイバーセキュリティ機関は、特にIoTについて、暗号化されていない他の手段ではなくSSHの使用を積極的に推進してください。このような組織は、TelnetとFTPがまだ一般的な分野での商業的なSSHの活用を奨励することもできます。さらに、サイバーセキュリティの専門は、健全なキー管理を奨励し、SSHが有効になっているデバイスに、長い間使われているデフォルトのパスワードとキーを内蔵させないようにすることも可能です。

ファイル共有

インターネットの初代ユーザーたちがコンソールアクセスを得たら、次はリモートシステムとファイルを送受信する方法が必要でした。ファイル共有は、自分のデバイスにエンコードされた動画をストリームしたり、猫の写真をたくさん見たり、またはキャッシュされていないページを訪問する度に約70個のファイルがダウンロードされるウェブサイトとインタラクトしたりと、現代のインターネットトラフィックの大半を占めるものです。[11]

HTTPアーカイブコレクションにおける、サイト別リクエスト合計数の分布



出典：httpparchive.org（2020年5月1日）<httparchive.org/reports/page-weight?start=latest&view=list>

現代のインターネットにおけるファイル共有の種類は、Webリソースの要求だけではありません。本レポートでは、この「ファイル共有」という広範なサービス分類で、以下の3種類のサービスについて調査しました。

- ファイル転送プロトコル（FTP）（TCP/21）と「セキュア」FTP（TCP/990）
- Server Message Block（SMB）（TCP/445）
- Rsync（TCP/873）

これらのサービスには、インターネット上のエクスポージャーという点で、それぞれ独自の安全性に関する問題があります。まずは2種類のFTPについて説明します。

[11] 出典：HTTP Archive、2020年4月 https://httparchive.org/reports/page-weight?start=latest&view=list

FTP (TCP/21)

分かりにくいデータチャネル交渉シーケンスと、完全なクリアテキスト。うまく行く わけがありません。

TLDR

説明：	FTPは元々、RFC 114で標準化され、当時のプロトコルの多くと同様、認証とデータ転送ではクリアテキストに依存しています。従来、FTPはTCP/21をコントロールチャンネルに使用しており、クライアントとサーバは、「アクティブ」または「パッシブ」モードで実際のデータ転送を行う2つ目のチャネルを交渉します。そのため、ファイヤーウォール管理者を悩ませ続けてきました。
数：	12,991,544のノードを検出しました。 6,645,633 (51%) にRecogフィンガープリント (合計20のサービスグループ) がありました。
脆弱性：	フィンガープリントのほとんどに、関連するエクスプロイトコードのあるDoSと、RCEに記録されたAuth/Unauthの脆弱性があり、いくつかのバックドアも残っています
アドバイス：	Telnetのセクションで述べたことは、すべてFTPにも当てはまります。パブリックに露出されたネットワークにFTPを見つけた場合、当該組織がパブリックコンピューティングという昔の遺産を使用しており、成熟したセキュリティプログラムの恩恵を受けていないということは間違いないと言えます。
代替手段：	現在、有用なFTPの代替手段はいくつかあります。SFTPは本質的にSSHにラップされたFTPで、一方FTP/SはHTTPS同様、SSLの層にラップされたものです。一般的にファイル転送では、SSHトンネリングのSCPとrsyncが良いソリューションであり、今日ではもちろん、世界中のエンタープライズネットワークでHTTPSベースのファイル共有アプリケーションが十分に確立されています。つまり、昔のプロトコルにこだわるべき理由はないということです。
傾向：	変化なし。2019年から、統計的に有意義な変化はありませんでした。

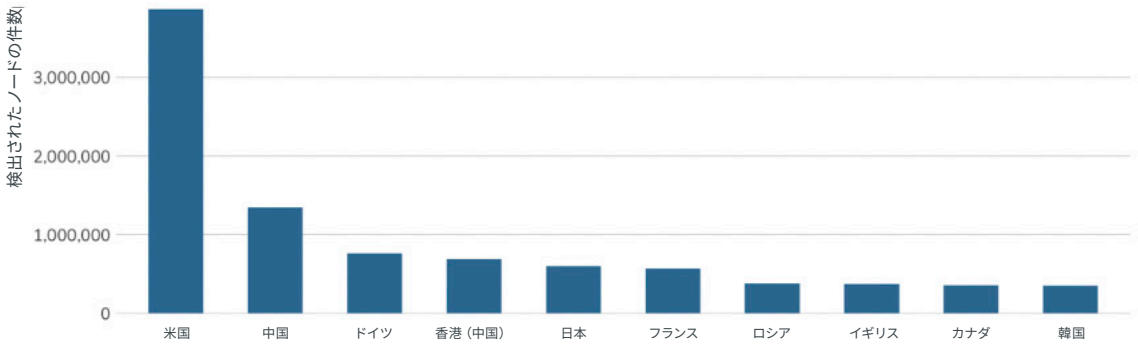
調査結果の詳細

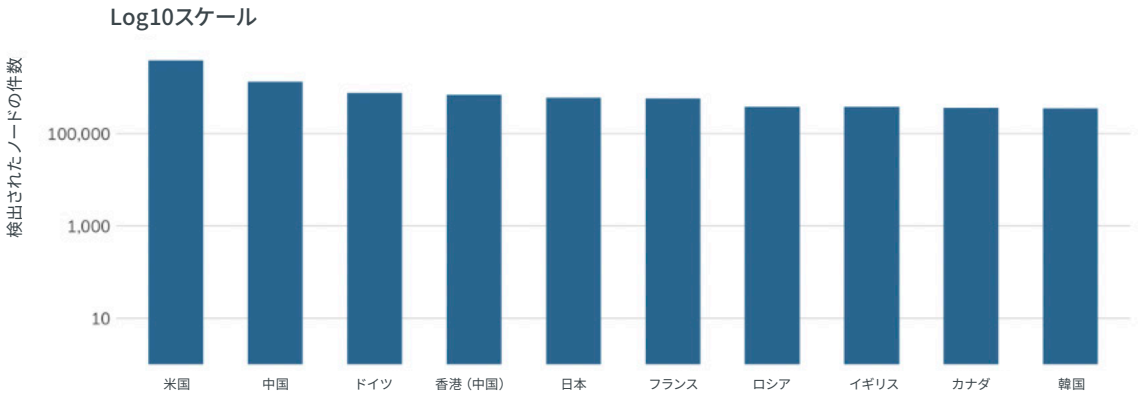
FTP (TCP/21のバリアント) は1972年に、「シンプルかつスムーズで、容易に実装できるプロトコルデザインで、maxi-HOST、mini-HOST、Datacomputerユーザーの多様なニーズを満たす」ために開発されました。[12] これは、クリアテキストのコマンド駆動型プロトコルで、その実用性以上に生き残っています。特に今では、ブラウザ開発の大手2社が、サポートを中止した、または中止する計画です。[13]

[12] RFC 354 <https://tools.ietf.org/html/rfc354>

[13] Mozillaの発表<https://groups.google.com/forum/#!msg/mozilla.dev.platform/FqCZUT9ay_o/jt4DLRDjAwAJ>
とGoogleの発表<https://www.chromestatus.com/feature/6246151319715840>

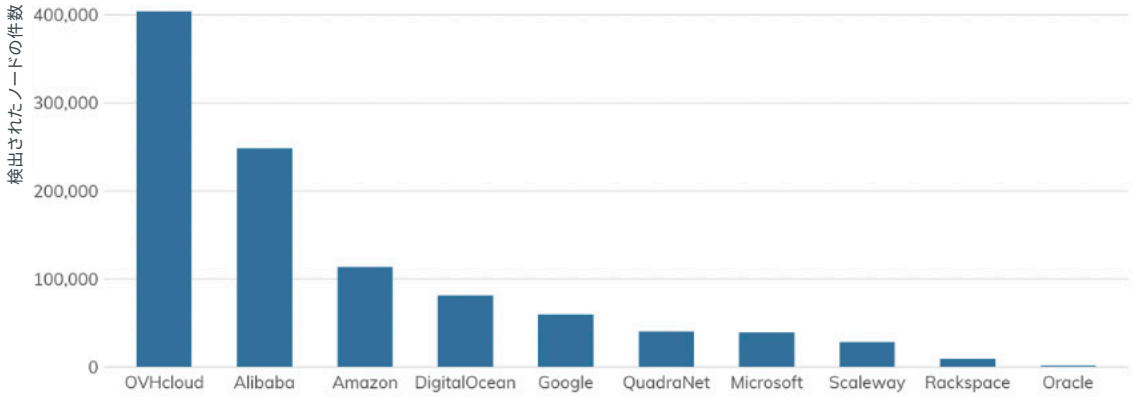
ファイル共有における上位10か国：FTP（21）

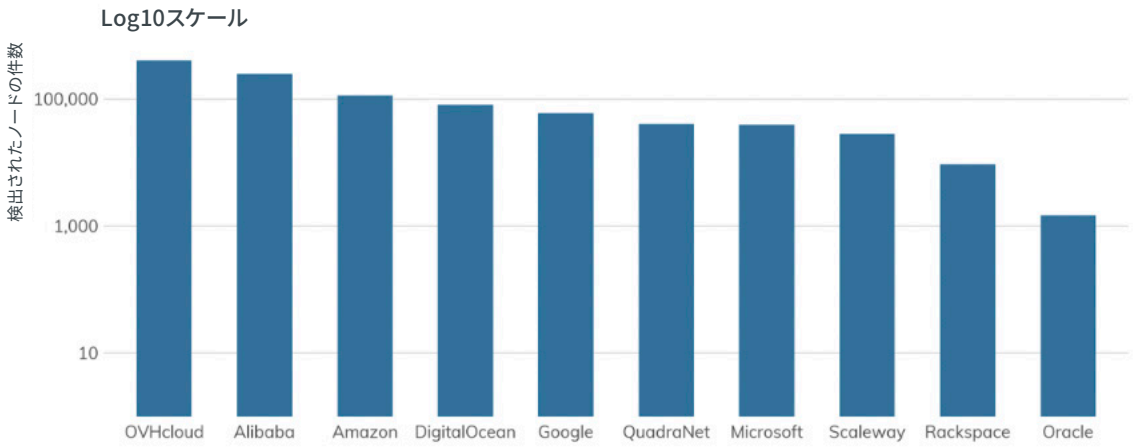




プロジェクトSonarでは、1,300万件弱（1,299万1,544）のアクティブなFTPサイトが見つかりました。前回のNational Exposure Index調査と比べ、2,000万件以上の減少となりました。FTPのインターネットへの露出では、米国が第1位で、390万件近くのホストが「OPEN」を待っています。

クラウドプロバイダのファイル共有：FTP（21）





少し驚いたのは、FTPはクラウド環境に大きなプレゼンスがあり、Alibaba、Amazon、OVH、Azureが発見されたノードの約13.5%をホストしているということです。

さらに詳しく調べると、AlibabaがLinux[14]とWindows[15]の両方で「FTPサイトの構築」方法を詳細にわたって説明しており、またAmazonが新しいFTPサービスを提供していることが分かりました。[16]同様に、OVH[17]とMicrosoft[18]にもFTPに関する文書があり、OVHに至っては、クライアントに対して、ウェブコンテンツのファイル管理にFTPを利用することを積極的に奨励しています。

さらにすべてのプロバイダに、FTPを搭載するか、または簡単にインストールできるというベース画像（前述の役に立つ文書から）があります。そのため、クラウド環境におけるFTPエクスポージャーの高さは、当然と言えます。

[14] Alibaba Cloud FTPセットアップ手順：Linux <https:/www.alibabacloud.com/help/ja/doc-detail/92048.htm>

[15] Alibaba Cloud FTPセットアップ手順：Windows <https:/www.alibabacloud.com/help/ja/doc-detail/92046.htm>

[16] Amazon AWS FTPの発表 <https://aws.amazon.com/jp/blogs/news/new-aws-transfer-for-ftp-and-ftps-in-addition-to-existing-sftp/>

[17] OVH FTP文書 <https://www.ovh.co.uk/web-hosting/ftp.xml>

[18] Microsoft FTP文書 <https://docs.microsoft.com/ja/azure/app-service/deploy-ftp>

エクスポージャー情報

2020年に容認できるFTPの利用方法はただ1つです。それは、どちらかというとパブリックなデータで、匿名のFTP[19]ダウンロードを提供することです。クリアテキストの認証情報が露出されないのは、このような使い方だけです（それでもトランジット中のデータは露出されます）。それ以外の使用方法は、すべて不安定かつ安全でないと見なし、避けてください。FTPはネイティブのチェックサムや他のエラーチェックをファイル転送で行わないため、この方法ですら、トランジット内のデータが中間者攻撃で容易に変更されるため、危険が伴います。

それでも、インターネットには数百万というFTPサーバーがあります。私たちはいくつかのフィンガープリントを検出することができました。[20]以下の表は、認証済みや匿名のものを含むFTPの世界を、かなり忠実に表しています。

サービス	数
Pure-FTPd	3,102,834
ProFTPD	1,011,310
IIS	823,696
vsFTPd	661,034
Bftpd	420,023
FileZilla FTP Server	415,147
Firewall-1	66,686
Serv-U	55,392
Multicraft	29,610
SmbFTPD	15,800
Gene6	10,260
ucftpd	6,928
Twisted	6,826
inetutils	4,239
WS_FTP	4,231
TBS FTPサーバー	4,199
AOS	3,548
Unified Security Gateway	3,401
Nepenthes（ハニーポット）	303
JetDirect	166

最後の列は読み間違いではありません。166件のプリンターがFTPサービスをインターネットに露出しているのです。おそらく、より心配するべきなのは、FTPを露出しているUbiquiti UniFi Square Gateway（ファイアウォール）3,401件です。

FTPサーバーのうち14種類で、比較的簡単にバージョン番号のフィンガープリントが行えます。その95%を、vsFTPd、ProFTPD、Bftpd、およびFilezillaが占めています（つまり210万件のFTPサーバーが、露出されたシステムの17%近くを占めているということ）。各種類の全バージョンをまとめるのは、膨大な作業になるため、トップ5のバージョンをコメント付きでまとめました。

VSFTPD	数
3.0.2	221,481
3.0.3	165,776
2.2.2	164,761
2.0.5	43,347
2.3.5	16,598

バージョン3.0.3が最新のもので、RCEの観点からは安全だと考えられます。しかし、3.0.2には中程度のリモートエクスプロイトのCVEが1つあります。[21]バージョン2.2.2は2011年のもので、DoS CVEがあります。[22]バージョン2.0.5は2008年にリリースされ、危険な（認証済みの）リモートCVEがあります。[23]

PROFTPD	数
1.3.5a	118,672
1.3.5b	100,941
1.3.4a	59,089
1.3.5	57,364
1.3.5e	45,756

ProFTPDで最も普及している 1.3.5/a/b の3バージョンには、リモート攻撃者に任意ファイルの読み書きをできるようにする、非常に危険なCVE[24]があります。1.3.4.aには、たちの悪いDoS CVE[25]があり、またその次の1.3.5eには認証された攻撃者が特定の設定下でディレクトリ構造を再設定できるようにする、低重度CVE[26]があります。

[19] RFC 1635 <https://tools.ietf.org/html/rfc1635>

[20] Recog FTP フィンガープリント <https://github.com/rapid7/recog/blob/master/xml/ftp_banners.xml>

[21] CVE-2015-1419 <https://attackerkb.com/topics/SLwQqWdCzX/cve-2015-1419>

[22] CVE-2011-0762 <https://attackerkb.com/topics/pMUfmyuiTA/cve-2011-0762>

[23] CVE-2007-5962 <https://attackerkb.com/topics/nqTlyFr916/cve-2007-5962>

[24] CVE-2015-3306 <https://attackerkb.com/topics/1Qhi2ndx91/cve-2015-3306>

[25] CVE-2013-4359 <https://attackerkb.com/topics/YdjqLThxlh/cve-2013-4359>

[26] CVE-2017-7418 <https://attackerkb.com/topics/g2r203lfxR/cve-2017-7418>

BFTPD	数
2.2	310,906
3.8	90,088
1.6.6	12,733
4.4	1,725
2.2.1	1,713

FILEZILLA	数
0.9.60 beta	190,673
0.9.41 beta	138,349
0.9.46 beta.	9,500
0.9.59 beta	9,030
0.9.53 beta	8,017

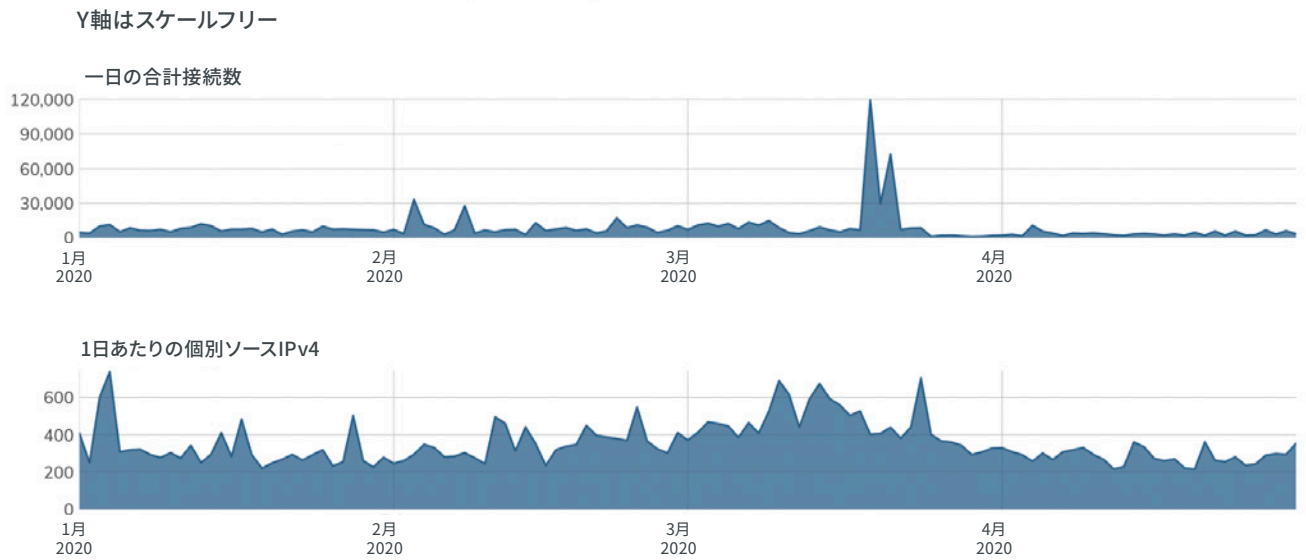
バージョン2.2 (11月でリリース11周年を迎える) には、便利なDoS CVEがあります[27]。残りのバージョンには、ログインしたユーザーが 悪用できるメモリ破損CVE[28]があります。

驚くべきことに、FileZillaのトップ5のバージョンにはCVEありませんでしたが、これらは非常に古いものです。

攻撃者の視点

Project HeisenbergにはFTPのハニーポットがありませんが、よく発生するTCP/21の接続試行はすべて捕えています。

FTP (TCP/21) HEISENBERGの活動



この活動では、攻撃者がC2インベントリに追加できる、ノード上の悪用できるサービスを探すか、または攻撃者やリサーチャーが盗難できるドキュメントを探します。いずれのシナリオでも、これ以上システムを犠牲にしない方が良いでしょう。

[27] CVE-2009-4593 <https://attackerkb.com/topics/DybJGgFgGI/cve-2009-4593>

[28] CVE-2017-16892 <https://attackerkb.com/topics/ShHL7hn1QT/cve-2017-16892>

アドバイス

ITとITセキュリティチームは、内部および外部両方でFTP（TCP/21）の使用を避けてください。このクリアテキストプロトコルは本質的に安全性が低く、はるかに安全で優れた新しい代替手段があります。システム間ファイル転送では、FTPの「S」バージョン（FTPSまたはSFTP）や、（できれば）広いクライアントおよびサーバーサポートのあるSCPが、より安全でかつ手早い代替手段です。よりインタラクティブに使用するには、商業的に利用でき、HTTPS上で動作するオープンソースのファイル共有ソリューションも多くあります。本当にインフラコンポーネントでFTPファームウェアの更新が必要な場合は、少なくともエンドポイントがインターネットに面していないことを確認し、認証情報が除かれないように内部のVPNゲートウェイで隠すことを検討してください。

脆弱性のスキャンや、パブリックにおける攻撃面のモニタリングの際はFTPもフラグしてください。調達プロセスでは、ソリューションのサポートでFTPが含まれている、またはFTPを必要とするかを確認し、その情報に基づいて安全な製品やサービスを選ぶようにしてください。

クラウドプロバイダは、安全性が非常に低いサービスの設定に関する親しみやすい文書を提供するのではなく、FTPがインストールされていない、またはデフォルトで有効になっていないベース画像だけを提供して、FTPの使用を避けるように呼びかけてください。サービス文書やその他の指示書は、明確にFTPの使用を止めさせ、露出されたFTPが見つかった際には、ユーザーに関連する通知ができる定期的なサービスの提供をプロバイダは検討してください。可能であれば、FTPプロトコル自体、またTCP/21はデフォルトでブロックし、標準のSaaSサービスからは必ず外してください。

政府のサイバーセキュリティ機関は、代替サービスの提案とともにFTPの危険性に関するガイダンスを提供してください。エクスポージャーセクションで述べた通り、インターネットに面したFTPシステムのかなりの数で、認証されていないRCEの脆弱性が見つかっています。これは、攻撃者が選びやすい標的、そしてFTPサービスが露出されている各国の公共インフラの本質的な弱点となります。

FTP/S（TCP/990）

TLDR

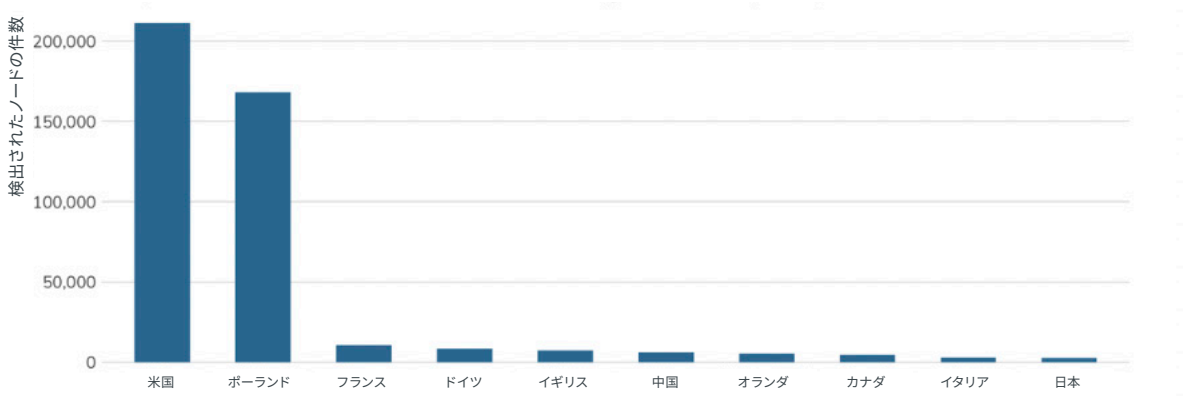
説明：	FTPですがSSLにラップされています。単にSSL層にラップされたHTTPであるHTTPSと非常に似ています。
数：	45万9.907件のノードが検出されました。 8万4,607件（18%）にRecogフィンガープリント（合計10件のサービスグループ）があります。
脆弱性：	検出されたのは主にDoSの脆弱性のフィンガープリントですが、Auth/UnauthのRCEも少しありました。IISについては、「Webサーバー」セクションで別に説明があります。
アドバイス：	FTP/Sは認証のみを暗号化し、ファイル転送はクリアテキストのままであるため、代わりにSFTPを使用してください。
代替手段：	SFTP、SCP、SSHにラップされたrsync、またはHTTPSベースのファイル共有アプリケーション
傾向：	FTP同様、変化なし

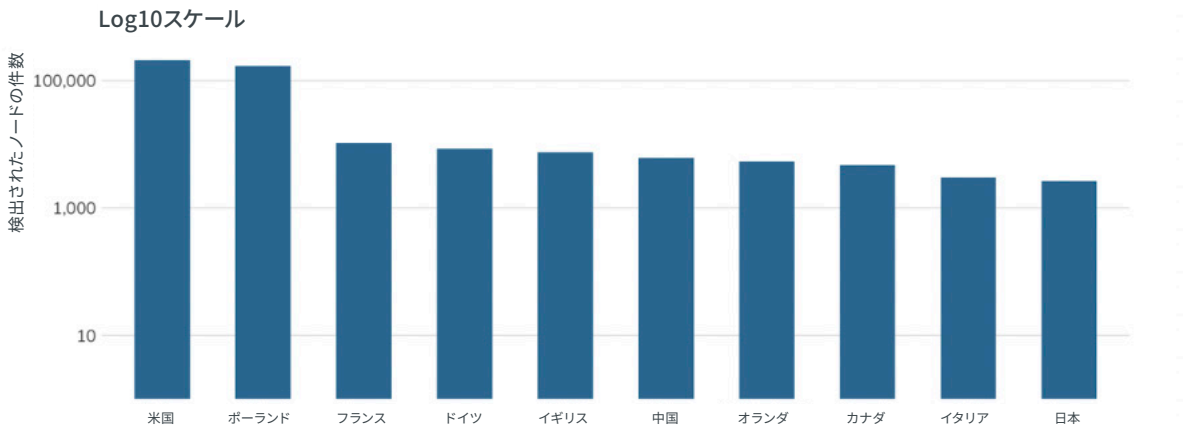
調査結果の詳細

FTP/S（TCP/990のバリアント）は1997年に、前のセクションで説明したFTPプロトコル[29]に残るセキュリティ問題を解決するために開発されました。本質的には、FTPのやや安全なバージョンです。残念ながら、安全になるのはログインだけで、ファイル転送は盗難に対する保護や、トランジット内の変更が全くないまま、クリアテキストで行われます。もう1つの利点は、FTP/Sサーバーが（HTTPSサーバー同様）暗号化の確実性を持ってアイデンティティを主張できることですが、これにはクライアントが実際に証明書の詳細を確認し、証明書の識別が失敗したときに正しい対策を講じなければなりません。

[29] RFC 2228 <https://tools.ietf.org/html/rfc2228>

ファイル共有における上位10か国：FTPS（990）





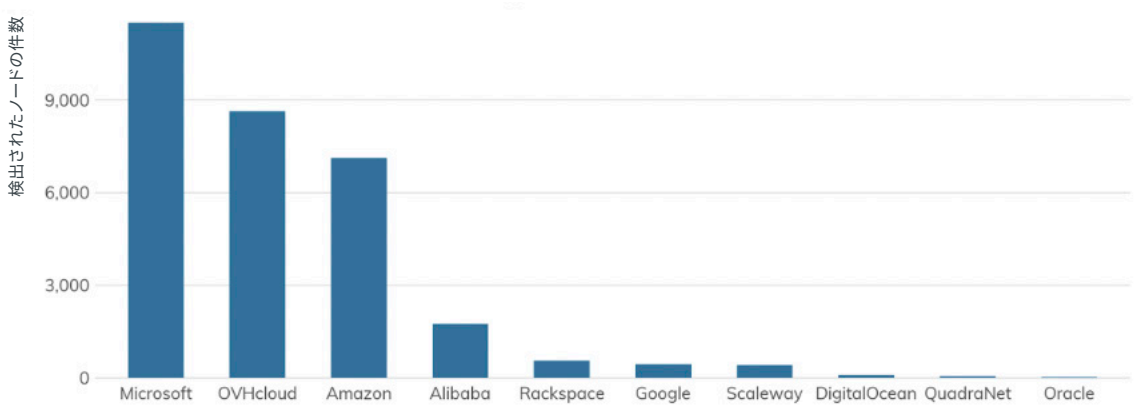
FTP/Sが、安全性の低い従兄弟とほぼ同じながらも、使用する上では比較的安全であることを考えると、より広く使われていると思うかもしれませんが、そうではありません。Project Sonarでは、パブリックインターネットで普通のFTPサーバーが何百万も見つかったのに対し、FTP/Sはわずか50万ノードでした。考えられる大きな1つの理由は、FTP/Sのプロセスで、HTTPSで前ほど単純ではなくなったTLS証明の作成、インストール、定期的な更新の必要性です。[30]

FTP/Sは米国に集中していますが（主にAzureが広く普及しているためで、これについては後に説明します）、ポーランドではhome.plのホスティングプロバイダーが従来のFTPからの切り替えに尽力しています。[31] 他のクラウドプロバイダにも是非このような文書化の努力をしていただきたいです。

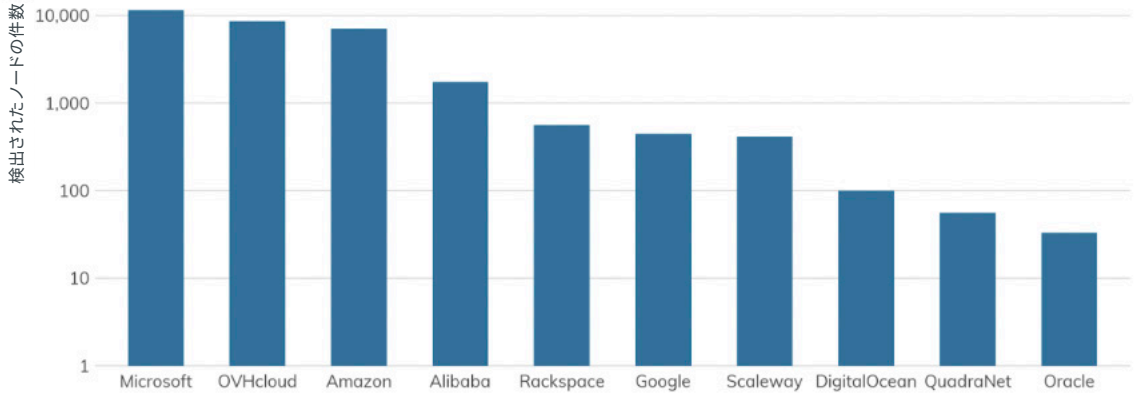
[30] これは、ボブとトッドの2人ともが同意してくれた、Let's Encryptに対する最小限の称賛です。

[31] Home.plのFTP/Sドキュメント <https://pomoc.home.pl/baza-wiedzy/bezpieczne-polaczenie-ftps-z-serwerem-w-home-pl>

クラウドプロバイダのファイル共有：FTPS（990）



Log10スケール



残念ながら、home.plは本レポートに記載されている調査で、トップ10入りするには十分なノードが露出されませんでいたが、Microsoft同様、正しいことを行っています。前述のFTP文書に加え、彼らには専用のFTP/S設定と指示書があり、「エクスポージャー」セクションの表から察することができる通り、IISでFTP/Sを有効化するのが非常に簡単です。

このような努力があっても、ユーザーはおそらくFTP/SではなくSCPを使用していると思われます。SCPはトランジット内のファイルコンテンツだけでなく、ログイン認証情報も暗号化するからです。

[32] Microsoft Azure FTP/Sドキュメント <https://docs.microsoft.com/ja-jp/azure/app-service/deploy-ftp>

エクスポージャー情報

Recogがフィンガープリントできた利用可能なFTP/Sサービスは、わずか8万4,697件（18%でした）が、FTP/Sで利用できる明示的な設定パラメータがあり、証明書の要求とインストールにはGUIが備わっているため、今回はIISの「勝ち」となりました。

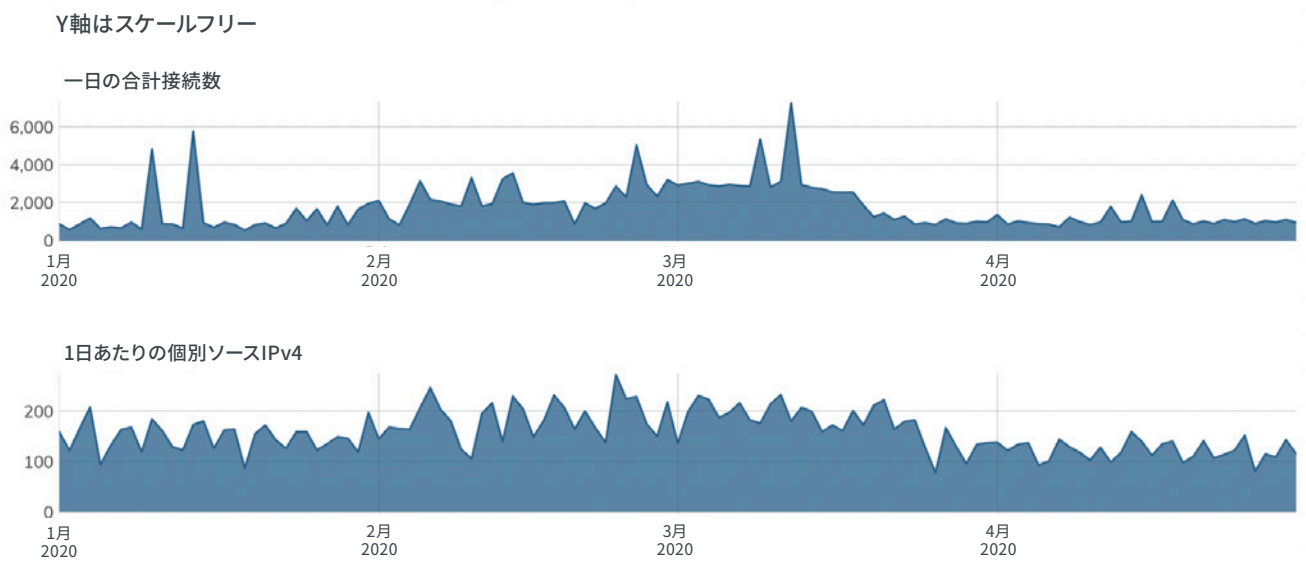
多くのFTP/Sサーバーが FTPとFTP/Sサーバーの機能を備えているため、同じ脆弱性が適用されます。IISについては、本レポートの「Webサーバー」セクションで詳しく説明します。

攻撃者の視点

FTP/Sはあまり使用されていません。これは一般的に、攻撃者やリサーチャーからそれほど注目されないことを意味します。プロジェクトHeisenbergの調査では、この仮定が補強されました（FTP同様、FTP/Sでもインタラクションの多いハニーポットがないため、原数値の合計と独自の時系列カウントを攻撃者と研究者の活動の代替値としました）。

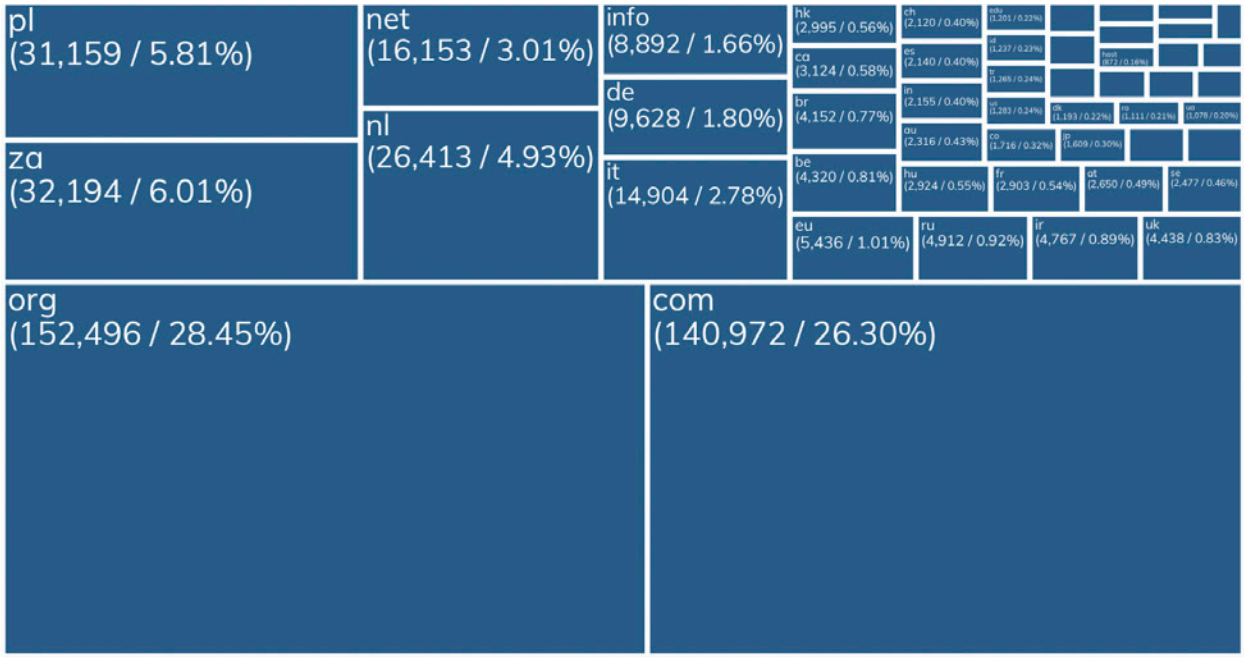
サービス	数
IIS	38,314
FileZilla FTP	33,147
Serv-U	7,092
ProFTPD	1,697
vsFTPd	1,420
Pure-FTPd	1,184
WS_FTP	1,110
Gene6	623
Bftpd	19
Twisted	1

FTP/S（TCP/990）HEISENBERG の活動



デフォルトのポートでFTP/Sを露出させるだけでなく、パブリックDNSのFTPS...tldのエントリ数の多さを考慮すると、攻撃者はDNSエントリで簡単にこれらのシステムを見つけられます。

TLDによる「FTP」で始まるDNSエントリ



アドバイス

ITとITセキュリティチームは、内容がほぼ同じであるため、FTPセクションのアドバイスに沿ってください。いつも事前に暗号化されたファイルを送信している、またはアップロードやダウンロードするコンテンツが機密情報でない（または中間者に覗かれたり変更されたりすることが気にならない）のであれば、もう少しの間FTP/Sの使用を続けられるかもしれません。

クラウドプロバイダは、home.plの例に倣い、安全なファイル転送に関するFTP/Sの可能性や限界を明確に説明してください。FTP/Sに依存しているシステムがあったとしても、クラウドプロバイダはSSH上のSCPやrsyncなど、総合的なソリューションを積極的に推進する必要があります。

政府のサイバーセキュリティ機関は、安全なファイル転送に関するFTP/Sの可能性や限界を明確に説明し、代替サービスを提案してください。「FTPエクスポージャー」のセクション（FTP/Sにも適用）で述べているように、比較的少ない、インターネットに面するFTP/Sシステムにも、認証されていないRCEの脆弱性が存在しており、攻撃者が選びやすい標的、そしてFTPサービスが露出されている各国の公共インフラの本質的な弱点となります。

SMB（TCP/445）

こだわる人はSMBを選びます。

TLDR

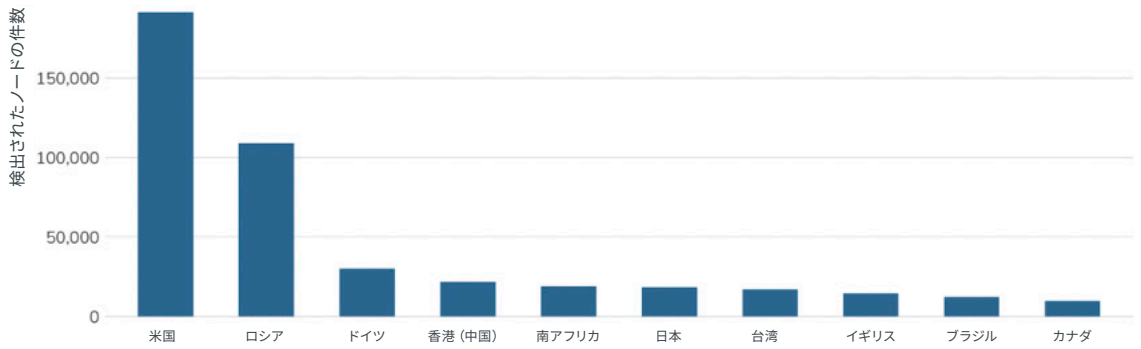
説明：	SMBはWindows全体のプロトコルですが、通常はWindowsベースのファイル転送に使用されます。
数：	59万3,749 件のノードを検出しました。[33]
脆弱性：	インターネット史上、最も破壊的なワームは、何らかの方法でSMBを使用しています。
アドバイス：	ルーティング不可能なローカルネットワーク外でのSMBへの直接アクセスは、一般的に禁止されるべきです。
代替手段：	通常、SMBがファイルホスティングを意図する場合、HTTPSベースのファイル共有で解決できますが、ほとんどのSMBエクスポージャーが偶然発生しています。
傾向：	改善傾向。何ということでしょうか。主にISPのおかげで、エクスポージャーは2019年から16%減少しました。

[33] WannaCryがいかに破壊的であったか、また、パブリックインターネットに対するEternalBlueの攻撃がいかに執拗であったかを受け、政府とISPは共同で、139番と445番ポートへのアクセスをブロックしてSMBのエクスポージャーを緩和しようと取り組んでいます。インターネットに入り込もうとするノードは、おそらく59万4,000件近くありますが、ISPがうっかりしてファイヤーウォールのルールを削除してしまわない限り、それは叶わないでしょう。

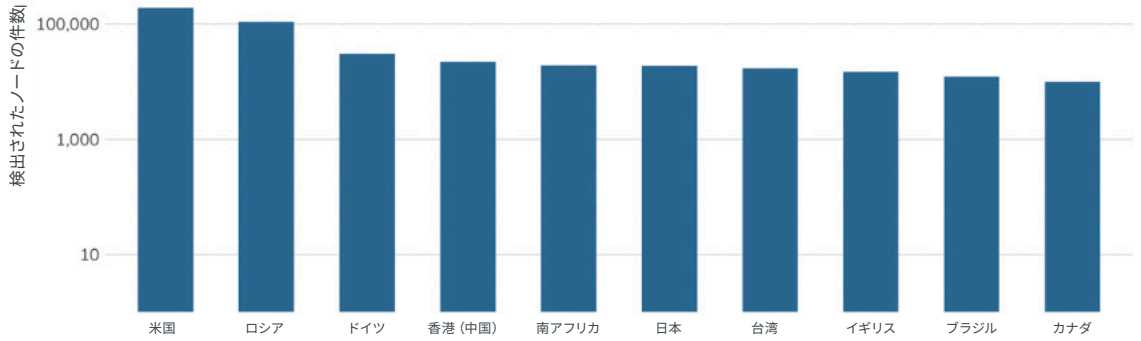
調査結果の詳細

SMBは、世界中のネットワークオペレータにとって、今でも頭痛の種です。元々、NetBEUIやIPX/SPXなどのローカルエリアネットワークプロトコルで動作するように設計されたSMBv1は、他のインターネットが動作する通常のTCP/IPネットワークに移植されました。それ以降、SMBv2とSMBv3がリリースされています。SMBは主に、認証、ファイル共有、印刷サービス、プロセスコントロールなどでWindowsベースのコンピュータに関連付けられますが、同時にSambaやNetsmbなど、Windows以外のオペレーティングシステムの実装でも使われています。交渉可能な暗号化機能があるバイナリプロトコルとしては、複雑なプロトコルです。この複雑性、また初期の独特な性質やオペレーティングシステムカーネルとの深い結びつきから、リモートコード実行（RCE）を可能にするセキュリティの脆弱性を発見するのに最適です。これに加えて、デスクトップオペレーティングシステムとしてのWindowsが世界的に人気であることから、バグハンターやエクスプロイターにも人気のターゲットであり続けます。

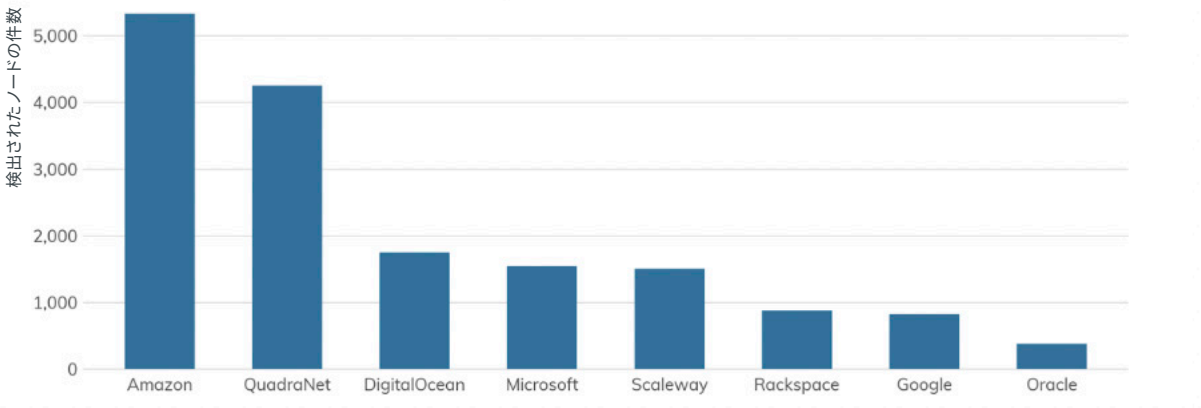
ファイル共有における上位10か国：SMB（445）



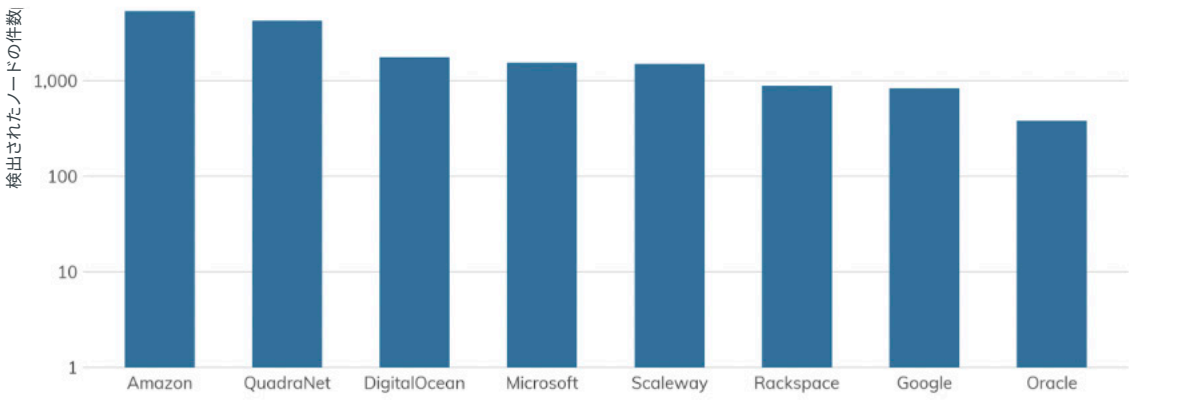
Log10スケール



クラウドプロバイダのファイル共有：SMB（445）



Log10スケール



エクスポージャー情報

最も良く知られている脆弱性、エクスプロイト、および野放しのワームが、何らかの形でSMBを活用しています。WannaCryとNotPetyaは、SMBが悪用と感染の中心となった、最も新しいイベントの2つです。過去に発生したSMBベースの攻撃には、NachiおよびBlasterワーム（2003年～2005年）があり、今後のSMBベースの攻撃には、SMBGhostが含まれると見られています。[34]バグに加え、SMBの意図的な特徴（特に自動ハッシュパス）が、無防備な被害者からパスワードのハッシュを盗むのに理想的なメカニズムにとなります。また、SMBシェア（ネットワークに露出されているファイルのディレクトリ）は、サーバーの不十分な管理や、使いやす過ぎるネットワークアタッチストレージ（NAS）を通し、引き続き事故的にインターネットに露出され続けています。

利用可能なSMBサービスのほとんどがWindowsベースであることは予想通りですが、右の表からは、少数派であるWindows以外のSMBもある程度見られます。

SMBサーバーの種類	数
Windows（サーバー）	298,296
Linux/Unix/BSD/SunOS（Samba）	170,095
Windows（デスクトップ）	110,340
QNAP NASデバイス	10,164
その他/ハニーポット	1,914
Apple Time Capsule、またはmacOS	1,465
Windows (Embedded)	703
Keenetic NAS	647
プリンター	386
Zyxel NAS	6
EMC NAS	5

[34] 本レポートが作成される直前に、SMBGhost、別名CVE-2020-0796にはパッチがあてられました。通常90日間とされる大規模な悪用までの猶予終了までのカウントダウンは始まっています。詳しくは、https://attackerkb.com/topics/2LCXe3EPAZ/cve-2020-0796---smbghostをご覧ください。

ご覧のとおり、これらのWindows以外のノードは通常、主にWindows環境で使用されているNASシステムの一種であり、ニアラインバックアップシステムの維持を行うものです。これらがWindowsシステムを攻撃するものと同じエクスプロイトに対して脆弱である可能性は低いものの、このような**バックアップがインターネットに露出されている**というだけでも、次にランサムウェアの波が襲ってきたら、これらのネットワークオペレータは非常に苦労することになります。

自動インストール

インターネットに露出されているWindowsマシンから、Sonarスキャンに見られるワークグループストリングの原点について、少し学ぶことができます。以下のリストは、これらのマシンのほとんどが、デフォルトの「WORKGROUP」というワークグループを使用しており、その他は標準の無人インストールで自動生成されたものです。SMBがとても珍しいもので、インターネットに露出するのが安全だったまるで魔法のような世界では、これらのマシンは手動で設定され、定期的にパッチが当てられていると思われていたかもしれません。

しかし実際にはそんなことはありえません。 これらのWindowsオペレーティングシステムは、おそらく自動的にインストールおよび設定され、インターネットへの露出については特に気にされることもありませんでした。そのため、エクスポージャーはほぼ間違いなく偶然の産物で、特別な、非常に重要なビジネス機能を果たしていないことになります。さらに、これらのアフターマーケットでデフォルトのWORKGROUPは、WindowsまたはSambaベースのビルドが生産環境で使われているかのヒントを与え、攻撃者にこれらのシステムを狙わせることにもなります。

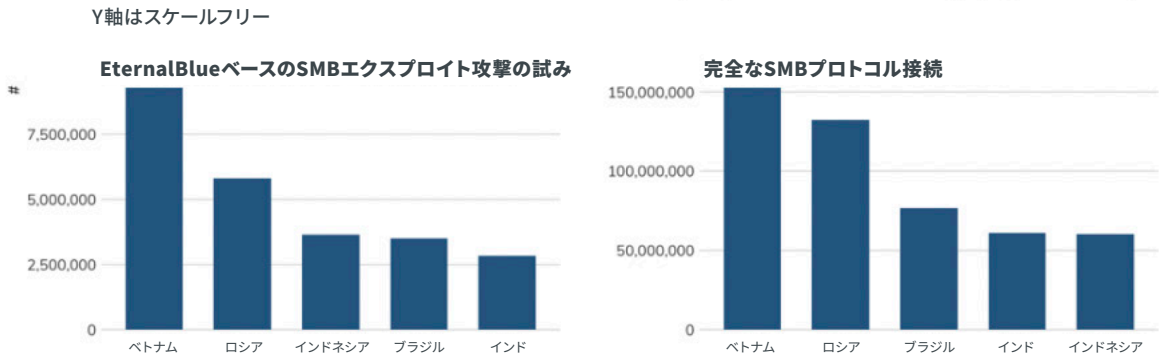
ワークグループ名	数
WORKGROUP	204,014
WIN-<string e.g. 4RGO6K0U19F>	98,153
MICROSO-<string e.g. HCBD8KK>	27,213
SERVER[####]	15,721
HK-<number e.g. 2723>	12,823
IPアドレス	10,367
DESKTOP -<string e.g. HUDL8UO>	7,203
HKSRV[####]	6,160
RS-<string e.g. A2-084	6,017
XR-<string e.g. 20190714REWT>	4,448
QNSERVER[####]	4,067
PC-<string e.g. HCBD8KK>	4,034
CCSERVER[####]	3,807
SVR-<number e.g. 20191106VUM>	3,303
MYGROUP	3,269
MSHOME	3,060
SRV*	2,910
SERVER	2,476
VM*	2,186
TKO[####]	2,088

攻撃者の視点

暗号化やその他のセキュリティコントロールのバージョンや設定に関係なく、SMBは今日のインターネットには不適切です。信頼性を確保するには複雑すぎるため、犯罪者にとって悪用するのにとても魅力的な重大な脆弱性であり続けています。それでも、SMBは今でもあらゆる規模のオフィス環境で重要なネットワークレイヤーであり、TCP/IPにネイティブであるため、ネットワークの誤設定でSMBベースのリソースを直接インターネットに露出してしまうことも考えられます。すべての組織はネットワークのイングレスおよびイーグレスフィルタでSMBトラフィックを継続的に点検し、 部外者がSMBトラフィックを誤って露出されたリソースに送信することを防ぐだけでなく、内部のユーザーが、過失によりSMB認証トラフィックを外部に漏洩させないようにする必要があります。

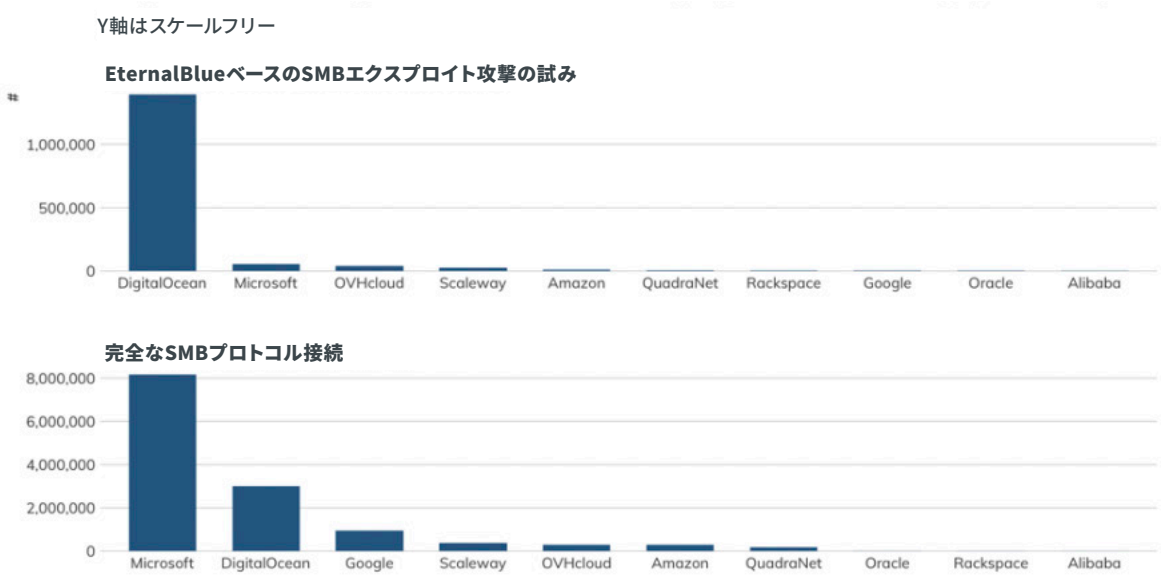
調査期間中、約64万件のIPアドレスが、ハイ・インタラクション型SMBハニーポットを訪れましたが、これをSMB犯罪者の大群として考えるのではなく、これらの接続の大半は、インターネット上にある無人のマシンからであるということを覚えておいてください。結局のところ、それがワームのやり方です。このような接続のうち、（pwnedではなく）攻撃者が個人的に所有するマシンがソースであると考えられるのは、ごくわずかです。これを念頭に置いたうえで、私たちのハニーポットトラフィックから、現在どの国がWannacryのようなSMBベースのメガワームに露出されているかが大体分かります。リストの上位国は、ベトナム、ロシア、インドネシア、ブラジル、そしてインドでした。

PROJECT HEISENBERG　発信国別に見る悪意のあるSMBアクティビティ（2020年4月）



クラウドプロバイダ間では、状況はさらに顕著です。Digital Oceanから私たちのハニーポットへの接続の約150万件が、WannaCryを支えているエクスプロイトのエターナルブルーによるものでした。一方、Microsoft Azureがソースとなっていた（エターナルブルーではない）接続は、約800万件でした（そのうちの約12%にあたる120万件ほどが、Azureでの設定ミスによる偶然の接続でした）。Digital OceanとAzureの攻撃トラフィックと偶然のトラフィックの間に、なぜこれほど大きな相違があるのかはまだ分かっていません。しかし、MicrosoftがAzureのデフォルトオファリングが、MSS17-010に沿ってパッチされていることを厳しく徹底している一方で、Digital Oceanはパッチの徹底をそこまでしておらず、ユーザーベースに定期的なメンテナンスを任せているということが理由として考えられます。

PROJECT HEISENBERG ソースクラウド別に見る悪意のあるSMBアクティビティ（2020年4月）



アドバイス

ITとITセキュリティチームは、VPN接続されたネットワーク以外の組織とのSMBアクセスを双方向で禁じ、また外部に面した既知のIPアドレススペースで、設定ミスのあるSMBサーバーがないかを定期的にスキャンしてください。

クラウドプロバイダは、クラウドリソースへのSMBアクセスを禁じ、少なくともSMBアクセスの外部リソースへのアクセスを定期的に調べてください。ハニーポットへのSMBを通した、Microsoft Azureからのインバウンド接続のうち約15%が攻撃やプローブではなく、実は設定ミスであることを考えると、Azureは特にこの一般的な欠陥を認識し、現在見られるレベルにまでSMBを偶然露出するのを不可能にするべきです。

政府のサイバーセキュリティ機関は、自国のSMBへのエクスポージャーを正確に把握し、定期的なスキャンや、SMBアクセスが発見された際にはそれをシャットダウンする通知プログラムを確立してください。これは特に、ハニーポットソースリストの上位国に当てはまることです。

RSYNC (873)

初期のインターネットエンジニアリングの事故ともいえます。

TLDR

説明：	[暗号化]認証あり、またはなしのクリアテキストファイルまたはディレクトリ転送サービス。
数：	208,882件のノードを検出しました。 すべてにRecogバージョンのフィンガープリントがありました。
脆弱性：	rsyncサービスには、長年にわたり、目立った脆弱性がいくつかあります。しかし、中でも最も重大なのは、ユーザーが認証情報を必要とせずに、もしくは、弱いまたは暗号化されていない認証情報を使ってインターネットに露出し、その直後に自己暗号化されていない機密ファイルの転送にrsyncを使用するものです。
アドバイス：	是非使用してください。しかし、使用できるのはSSHトンネルのみです。エンドツーエンドの暗号化により、インターネットに露出サービスを1つ減らすことができるからです。
代替手段：	いくつかの代替手段がありますが、rsync-over-SSHは、バックアップやあるシステムから別のシステムへのファイル転送を行うのに適した安全な方法です。FTPやFTPS、またRCPなどのレガシーツールではなく、rsync-over-SSHの検討を強くお勧めします。
傾向：	改善傾向。昨年に比べ、露出されたrsyncシステムの数は11%近く減少しました。

調査結果の詳細

rsyncサービスは誕生から24年経ち、人間でいえば米国でレンタカーを借りれるほどの年になりました。多くのネットワークプロトコルと異なり、rsyncはプロトコル自体にはIETFのRFCはありませんが、Uniform Resource Identifier (URIですが、URLだと考えても結構です) が知られるようになり、この尊いプロトコルは少なくともURIスキームで部分的なRFCステータスを獲得しました。[35]rsyncにはドキュメンテーションがあり[36]、最新のインターネット上で広く使われており、ソフトウェアとオペレーティングシステムミラーやファイルシステムを人々に活用させ、バックアップを実行することで （後に説明します）、 かなりの数のホームネットワークアタッチストレージ (NAS) を露出させています。

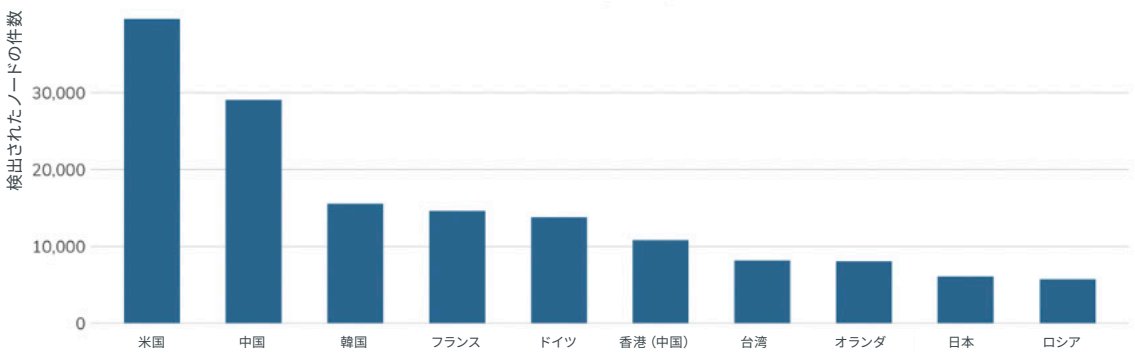
Rapid7のJon HartとShan Sikdarは、2018年にrsyncのエクスポージャーについて詳しく調査しましたが、[37]それから現在までにはわずかな変化しか見られません。そのため、重複する調査は行わず、その変化に注目します。

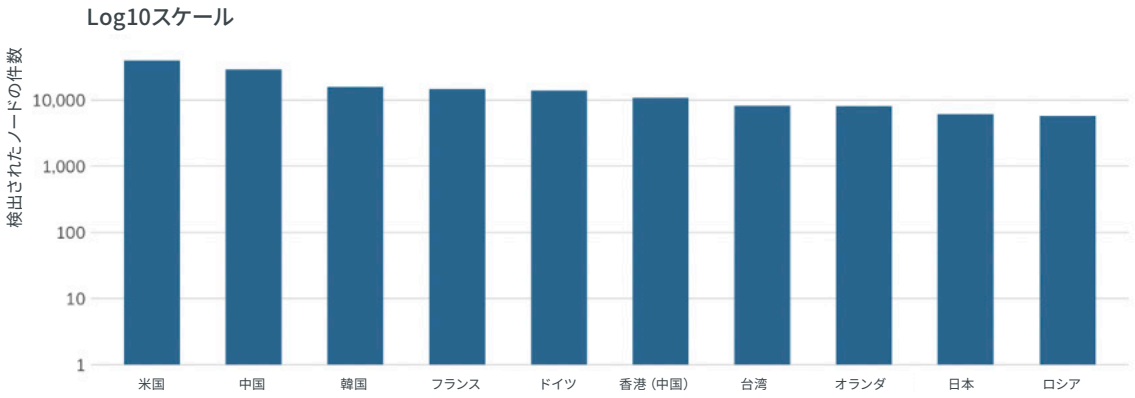
[35] RFC 5781 <https://tools.ietf.org/html/rfc5781>

[36] rsyncアルゴリズム <https://rsync.samba.org/tech_report/>

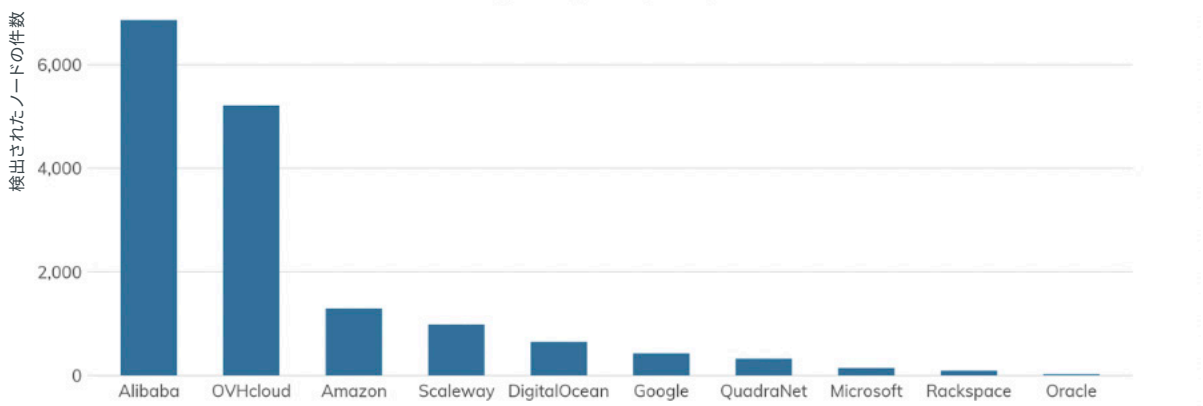
[37] Rsunk your Battleship: An Ocean of Data Exposed through Rsync <https://blog.rapid7.com/2018/12/21/rsunk-your-battleship-an-ocean-of-data-exposed-through-rsync/>

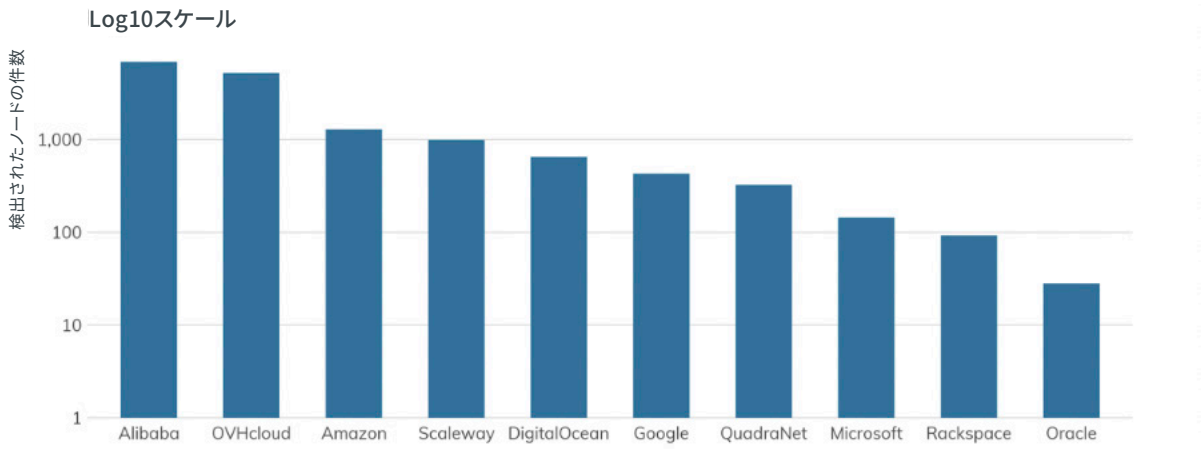
ファイル共有における上位10か国：RSYNC（873）





クラウドプロバイダのファイル共有：RSYNC（873）





なぜ中国のAlibabaとフランスのOVHが他のプロバイダに比べて大きなrsyncのプレゼンスを持っているのかと疑問に思っている方は、「クラウド」に馴染みのない人々がジャンプスタートする際に頼りとする、それらのドキュメント[38]やサービス[39]を見れば分かります。残念ながら、両方のクラウドがデフォルトで平凡なrsyncを使用していますが、少なくとも、SSHトンネルを通して実行の安全性を高められるということに言及しています。

[38] Alibaba rsyncドキュメント <https://www.alibabacloud.com/help/ja/doc-detail/54016.htm>; <https://www.alibabacloud.com/blog/speeding-up-network-file-transfers-with-rsync_594337>

[39] OVH「クラウドアーカイブ」（rsyncに基づく） <https://us.ovhcloud.com/public-cloud/cloud-archive/>

エクスポージャー情報

露出されたrsyncシステムの半分以上（約57%）が、10年前のプロトコル（バージョン30）で実行されており、オペレーティングシステムが10年以上も同じままで、他の脆弱性に悩まされているということが分かります。プロトコルのバージョン31が最新のものですが、これは少し誤解を招く可能性もあります。バージョン31は、2013年にリリースされました。プロトコルのバージョン30と31以外では、本当に古いバージョンが急激に減少しています。

RSYNC プロトコルバージョン	数
30	117,629
31	80,391
29	7,596
26	2,654
28	510
31.14[40]	45
27	36
24	8
34	7
32	2
20	1
25	1
29	1
31.12	1

rsyncエクスポージャーの20%以上が家庭向けISPスペース（トップ25は以下のリストに記載）にあることから、これまでのセクションとは少し方向を変える必要があります。これらのほとんどは、オンラインストアや大箱の家電量販店で見たことのあるブランドのNASデバイスです。これがなぜ重要なのかについては、次のセクションで説明します。

ISP	数
HiNet	5,316
Korea Telecom	5,300
中国聯合通信	4,583
China Telecom	4,528
Vodafone	4,389
Orange	4,274
Deutsche Telekom	2,245
Comcast	1,994
Tata Communications	1,355
Charter Communications	1,306
Swisscom	810
Verizon	732
NTT Communications	727
Telia	643
Virgin Media	626
中国移動通信	550
Cogent	489
Rostelecom	473
AT&T	412
Rogers	394
Cox Communications	383
CenturyLink	193
Hurricane Electric	165
Level3	102
China Tietong	92

[40] 見る限り、31.14と31.12という唯一小数点数を持つバージョンは、Buffalo NASデバイス特有のものです。なぜこのように記されているのかは分かりません。

コアのrsyncサービスには暗号化がないため、 認証を含む すべての操作は、クリアテキスト上で行われます。つまり、TelnetやFTPと同じくらい危険ということです。このプロトコルは、非クリアテキスト認証の使用をサポートするために拡張されていますが、ファイル転送はいまだにクリアテキストで行われるため、正しいネットワークポジションを覗けば、データを盗むことが可能です。

しかし、rsyncを露出させることが本当に危険である理由の1つは、攻撃者に対して盗めるファイルや、乗っ取る価値があるかも知れないオペレーティングシステムがあることを知らせてしまうということです。

攻撃者の視点

rsyncは「ファイルあります！」という大きなネオンサインで、また露出されたrsyncの大部分が家庭用ISPネットワークにあることから、攻撃者はそのようなIPアドレスにある他のサービスとの関連性を探り、露出されているシステムの種類を把握できます。

なぜこのような家庭用rsyncシステムがインターネット上にあるのでしょうか。QNAPなどのベンダーは、このようなNASデバイスを使いやすくするために、「myQNAPcloud」のようなサービスを作ります。これにより、ユーザーは「nameyouwant.myqnapcloud.com」を作成して、インターネット上で自分のデバイスにアクセスできるようになるのです（これを行うには、自宅のルーターに少なくとも1つの穴を開けなければいけません）。また、保存した動画や音楽を視聴できる便利なモバイルアプリもあります。Sonar FDNS調査では、12万5,000件以上のmyqnapcloud.comエントリが見つかりました。攻撃者がデータを収集するのは非常に簡単なのです。つまり、12万5,000件以上のQNAP NASユーザーが、攻撃者に自宅の（IP）アドレスを渡して、昔ながらの「Welcome」と書かれたマットを入り口に敷いいているようなものです。

残念ながら、QNAP（および他のNASベンダー）は、7つの認証されていないリモートコード実行に関連するもの（中でも最新のものがひどい）を含む脆弱性については、これまで十分な対策を講じていませんでした。[41]これらの脆弱性はrsync上で露出されてはいないものの、前述の通り、NASデバイスがある可能性が高いことを示す大きな目印になります。

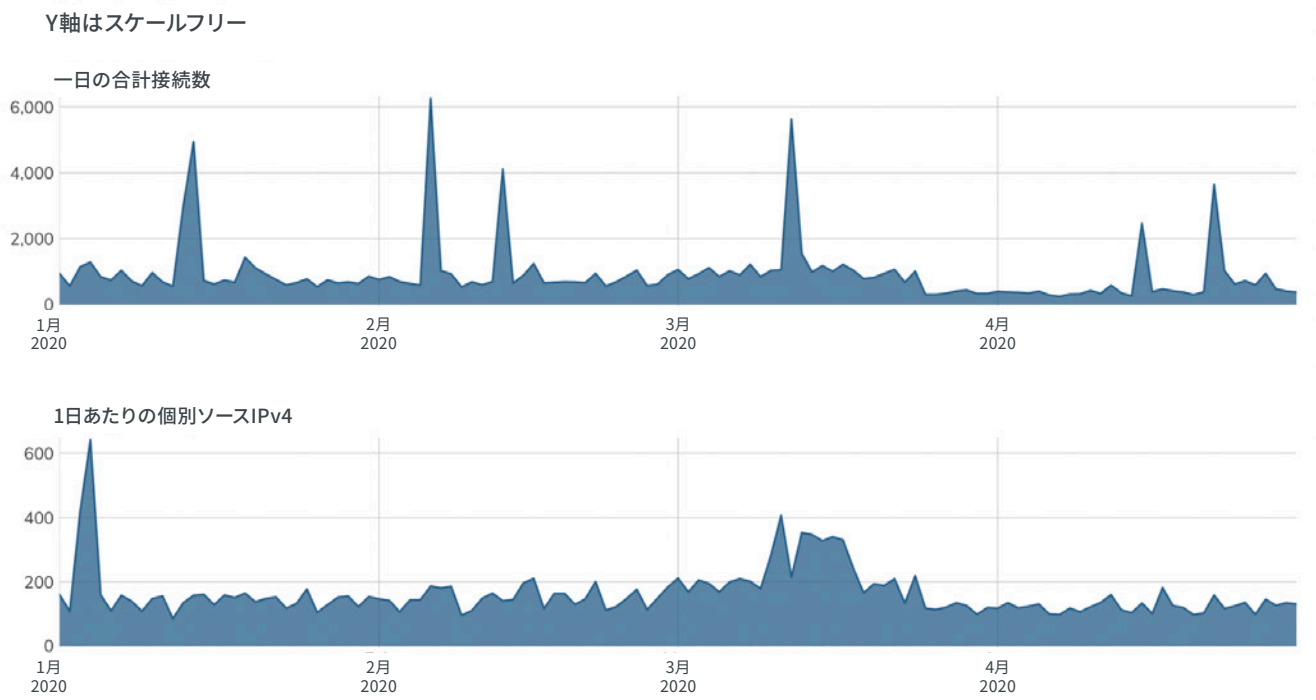
攻撃者はこのようなデバイスを、インターネット上の他の悪意のあるアクティビティ（DDoS攻撃など）の開始ポイントとして使用し、これらのデバイス上のすべてのファイルをロックして、消費者グレードのランサムウェア攻撃を行うこともあります。

ご覧のとおり、rsyncといった1つの純粋なサービスを露出することで、大きなトラブルを引き起こす可能性があるのです。

Heisenbergのハニーポット隊には、rsyncのハイ・インタラクションハニーポットはありませんが、TC/873への接続試行はすべて見つけ、侵攻する新たなrsyncのエンドポイントを探しているリサーチャーや攻撃者の定期的なインベントリスキャンを観察しました。

[41] QNAP Pre-Auth Root RCE <https://medium.com/bugbountywriteup/qnap-pre-auth-root-rce-affecting-450k-devices-on-the-internet-d55488d28a05>

RSYNC（TCP/873）HEISENBERGの活動



アドバイス

ITとITセキュリティチームは、決して従来のrsyncを使用せず、常にそれを甘いチョコレートのような安全なシェルに包んでください（つまり、証明書ベースの認証されたSSHセッションをトンネリングする場合にのみ使用してください）。機密情報にrsyncを使用するのに、他に安全な方法はありません。全くです。

クラウドプロバイダは、証明書ベースの認証済みのSSH以外のrsyncサービス以外は提供しないでください。既存の安全性が低いサービスは、できるだけ速やかにフェーズアウトしてください。このような、どこにいても暗号化するという世界に近づくうえで、最も分かりやすいな道は、rsync-over-SSHを始める方法が例とともに示された、十分に保守されていて見つけやすいドキュメントを提供することです。反対に、rsyncを裸で実行する方法についてのドキュメントは最低限に留めるか、または全く必要ありません（過ちをどうしても犯したいというユーザーは、昔のように頑張ってマニュアルを読めば良いのです）。

政府のサイバーセキュリティ機関は、消費者、クラウドプロバイダ、そして組織に対し、証明書ベースの認証されたSSHトンネルを通したrsyncサービスの使用を定期的に、かつ強く奨励してください。また、クラウドプロバイダやNASベンダーと協力し、そのようなプラットフォームからのrsyncエクスポージャー被害を根絶してください。

電子メール

現在のような形式の電子メールは、ネットワークとコンピュータ間のメッセージ転送におけるSMTP標準として出現し、1981年11月、RFC 788に記載されました。メールは少なくともその10年前から使用されていましたが、システムやネットワーク間のプロトコルやアプリケーションは大きく異なるものでした。メールを統一して一般化したのはSMTPであり、現在でもその進化は続いています。

クライアント側では、長年にわたって習慣に変化が見られます。1990年代には、Client-to-Serverプロトコルグループの一種であるPOP（Post Office Protocol）とIMAP（Internet Message Access Protocol）が主流でした。世界的にWorld Wide Webに移行していった際に、スタンドアロン型のメールユーザーエージェント（MUA）ではなく、ウェブメールに人々が目を向けたことから、その利用はわずかの間減少しました。この傾向は、メールサーバーとの通信にIMAPv4を主に使用するAppleおよびAndroid製モバイルデバイスの台頭に伴い、逆転しました。

SMTP (25/465/587)

SMTPにある「シンプル」というのは皮肉です。

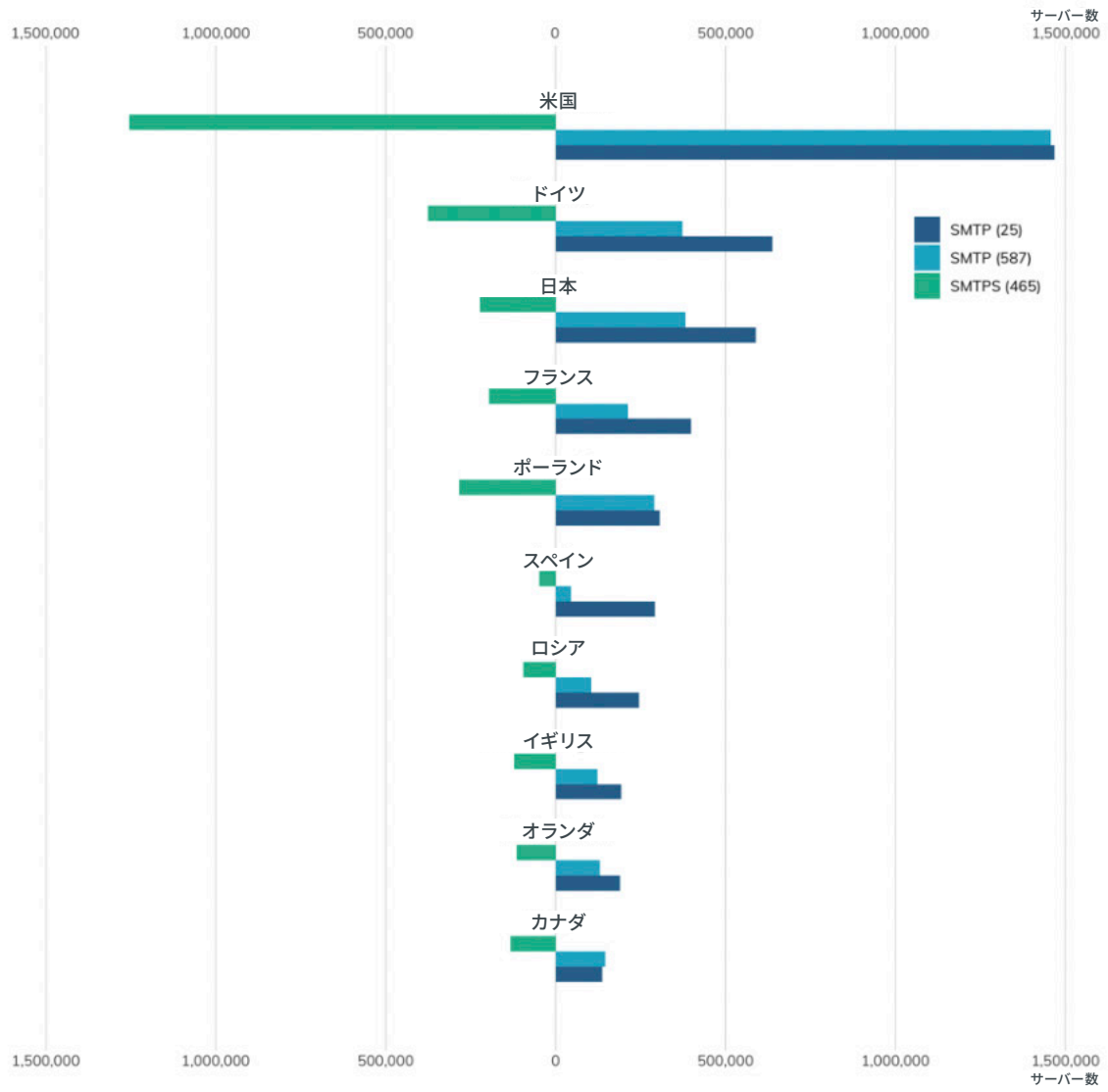
TLDR

説明：	通常クリアテキストで、ネットワーク間のメール配信のテキスト型スタンダードです。
数：	225番ポートで検出されたノード580万5,012件、587番ポートが400万7,931件、465番ポートが349万4,067件。合わせて、1,330万7,010件のサービスノードです。 そのうち302万3,486件 (52%) にRecogフィンガープリント (合計43件のサービスグループ) がありました。
脆弱性：	ネイティブでクリアテキストというメールの特性が、このプロトコルのセキュリティに関する主な懸念です。メールはまた、ユーザーにパスワードの公開やマルウェアの実行をさせるフィッシングによく使われる手段です。最後に、今日展開している人気の高いメールサーバー、EximとMicrosoft Exchangeには、少なくとも2つ重大な脆弱性があります。
アドバイス：	メール管理者は、リリースされ次第セキュリティパッチを適用することを徹底し、速やかにDMARCの反スプーフィングコントロールを実装してください。
代替手段：	メールをGoogleやMicrosoftなどのクラウドプロバイダにアウトソーシングすることは、これほど重要なインターネットインフラを効果的に維持するコストを比較すれば、多くの場合正しい選択です。
傾向：	改善傾向 (25/587) 。自身のメールをホストするという変わった人は減っています。

調査結果の詳細

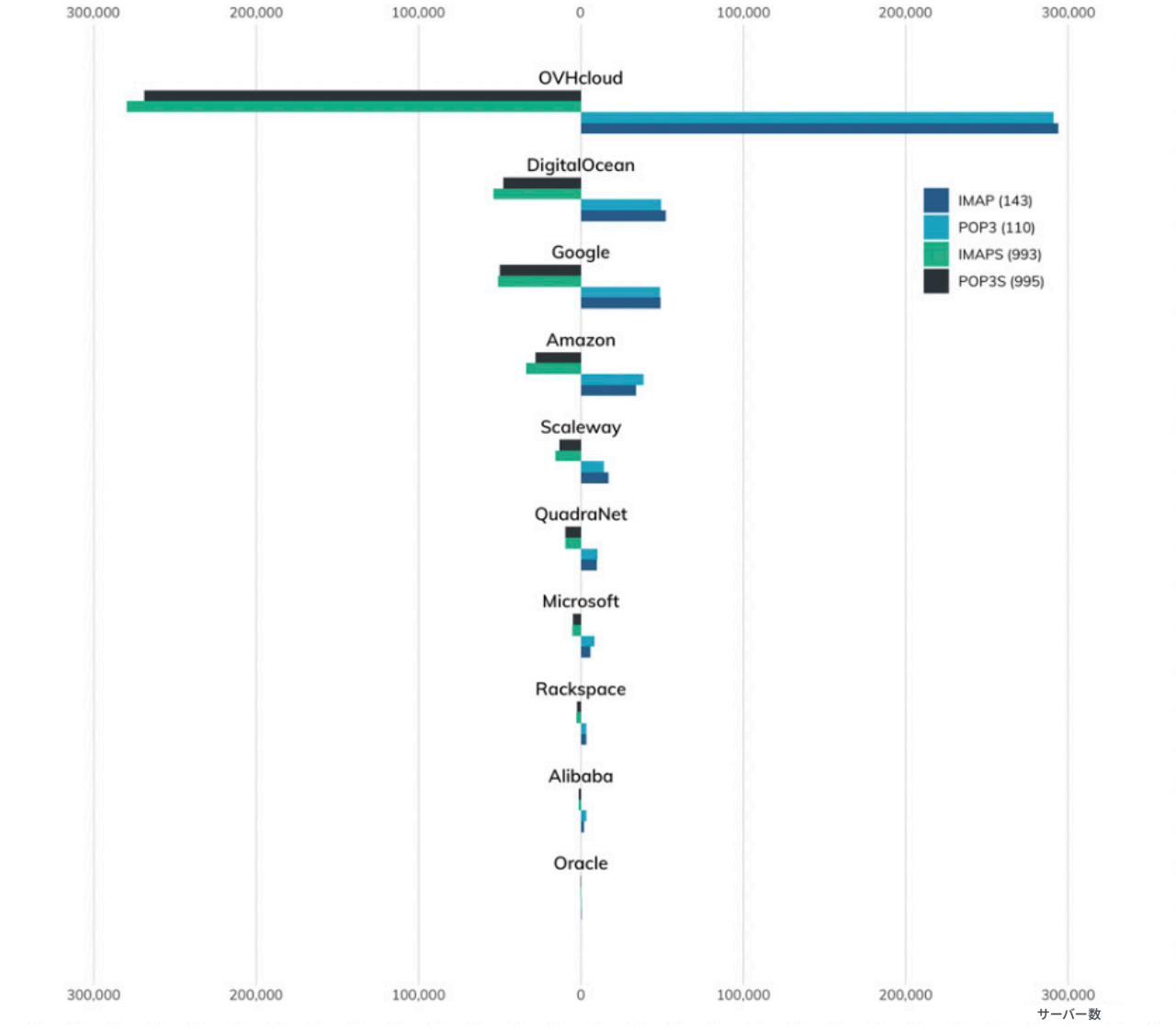
SMTPは従来、STARTTLSと呼ばれるセキュアプロトコル交渉がオプションであるクリアテキストですが、現在では、SMTPSとしても知られる、SSLにラップされたSMTPが増えています。以下のグラフと表は、25番ポート上のSMTP、587番ポート上のSMTP (SMTPからSMTPへのメッセージ中継のためのもの) 、そして465番ポート上のSMTPSの分布を示しています。

国別で見る暗号化と非暗号化メールサービスの比較（上位10か国）



国	SMTP (25)	SMTP (587)	SMTPS (465)
米国	1,467,077	1,456,598	1,253,805
ドイツ	637,569	373,266	375,526
日本	589,222	382,133	222,633
フランス	398,390	212,937	196,177
ポーランド	306,368	289,522	284,297
スペイン	291,844	44,435	48,694
ロシア	245,814	104,709	95,972
イギリス	193,073	121,902	122,069
オランダ	189,456	129,690	115,211
カナダ	137,342	146,323	132,133

クラウドプロバイダ別で見る暗号化と非暗号化メールサービスの比較



プロバイダー	SMTP (25)	SMTP (587)	SMTPS (465)
OVHcloud	317,584	248,695	236,772
Amazon	95,175	32,579	31,438
DigitalOcean	74,097	46,521	41,234
Scaleway	30,876	15,332	12,594
QuadraNet	29,282	18,200	8,667
Google	29,030	50,422	50,561
Microsoft	14,945	5,576	2,790
Rackspace	8,459	2,511	1,841
Alibaba	5,729	3,863	3,826
Oracle	1,274	509	345

トップレベルのドメインについては、SMTPの大半がドットコムランドにあることが分かります。 ドットコムに登録しているMXレコードは1億件以上で、dot-de、dot-net、dot-orgはMXレコードがそれぞれ約1,000万と、急激に減少しています。

エクスポージャー情報

何十個ものSMTPサーバーがあり、それぞれが設定、スパムフィルタリング、およびセキュリティに独自の方法を持っています。フィンガープリントできるSMTPサーバーでトップとなったのは、インストール数が100万件以上のPostfixで、それにExim、Exchange、そして信頼できるSendmailが続いています。以下は、私たちが明確に認識した全SMTPサーバーのリストです。 メール管理者は、昔からあるもののあまり使われていない、Lotus DominoやZMailerなどのメールサーバーがお分かりになるでしょう。もしあなたがこれらのメールサーバーをお使いなら、なぜこれほど報われない仕事を単純に専用のメールサービスプロバイダに託さないのかを、しっかり考えてください。

SMTPグループ	数
Postfix	1,679,222
Exim	759,799
Exchange Server	182,263
Sendmail	180,812
Mail Server	84,262
IIS	58,720
Ecelerity Mail Server	25,206
MDaemon	14,404
Connect	10,447
IMail Server	5,354
Pro	3,462
IBM Domino	3,445
Twisted	1,999
UTM	1,926
WinWebMail	1,879
Email Security	1,867
ListManager	1,785
Lotus Domino	1,734
David	1,490
PowerMTA	1,239
CCProxy	675
MailSite	305

SMTPグループ	数
Post.Office	275
VPOP3	245
ZMailer	205
GroupWise	176
Check Point	78
WinRoute	43
Messaging Server	40
VOPMail	24
IntraStore	22
Internet Mail Server	18
NTMail	17
Mercury Mail Transport System	15
FWTK	9
SLMail	8
FTGate	4
Internet Mail Services	4
VM	3
Mail-Max	2
AppleShare IP Mail Server	1
MERCUR	1
WebShield	1

最後に、Eximメールサーバーを見てみましょう。インターネット上で人気のあるソフトウェア同様、あらゆる種類のバージョンがあります。しかし、他の人気ソフトウェアとは異なり、Eximのバージョニングは非常に動きが速く、 スキャンの時点で最新だったのは、Eximのv4.93でしたが、発表する頃にはすでに4.94が出ていました。一方、最新バージョン（4.93）とそれより1つ前のバージョン（4.92.x）の人気を比べると、その差は10万の桁であり、Eximに向けられた政府諜報機関の厳しい監視の目を考慮すると、この差は非常に困ったものです。どれほど問題かというと、米国家安全保障局がEximの管理者に対し、「Sandwormグループ」による悪用を回避するため、可及的速やかにパッチとアップグレードを行うようにと勧告したほどです。[42]具体的に、悪用された脆弱性はCVE-2019-10149で、バージョン4.87から4.91に影響します。スキャンを行った時点では、インターネットに露出されていた、 そのようなサーバーは8万7,500件見つかりました。これは、全Eximサーバーのうち約5分の1ですが、メールサーバーにおける露出された脆弱性は、一気に「直ちにパッチを当てるべき」脆弱性のリストのトップに上る傾向にあります。

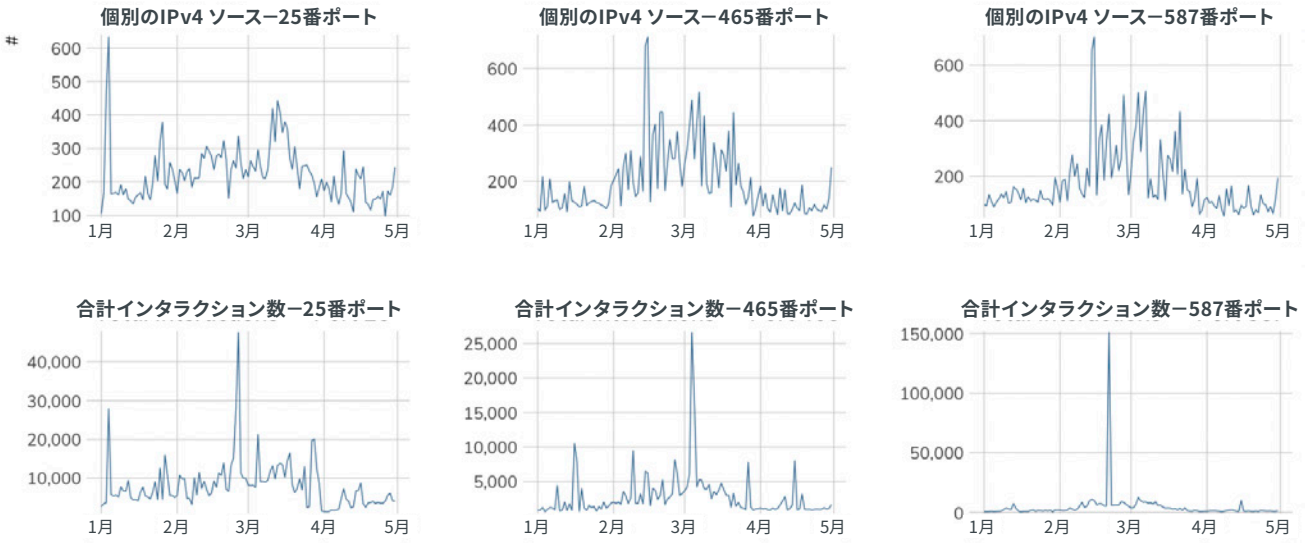
EXIMバージョン	数
4.92	243,647
4.93	106,977
4.92.3	89,980
4.93.0.4	52,467
4.91	42,953
4.84_2	37,332
4.89	36,159
4.90_1	28,542
4.86_2	18,678
4.92.2	17,118
4.8	9,673
4.87	8,539
4.72	7,836
4.82	7,732
4.76	6,409

[42] https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf

攻撃者の視点

攻撃者がSMTPの脆弱性に割り当てる価値の高さを考えれば、SMTPのハニーポットにある脅威アクターで、かなり定期的なスキャンが行われているのは驚くことではありません。

PROJECT HEISENBERG SMTPインタラクションの試行



日付	SMTPポート	数	割合	プロバイダー
2020年2月15日	25	518	12.92%	Sprint（ポーランド）
2020年2月15日	25	514	12.82%	China Telecom
2020年2月15日	25	409	10.20%	Tele Asia Hosting
2020年2月15日	465	4,337	99.18%	DigitalOcean
2020年2月15日	587	4,568	99.65%	DigitalOcean
2020年2月26日	25	32,495	73.97%	Hostwinds
2020年2月26日	25	6,504	14.81%	Sprint（ポーランド）
2020年2月26日	25	2,730	6.21%	Tamatiya Eood Hosting
2020年2月26日	465	851	69.36%	DigitalOcean
2020年2月26日	465	344	28.04%	Web Hosted Group
2020年2月26日	587	948	94.33%	DigitalOcean
2020年3月25日	25	4,930	41.55%	Microsoft 365
2020年3月25日	25	1,481	12.48%	Locaweb Hosting
2020年3月25日	25	509	4.29%	Hurricane Electric
2020年3月25日	465	415	95.62%	DigitalOcean
2020年3月25日	587	408	97.14%	DigitalOcean

日付	SMTPポート	数	割合	プロバイダー
2020年5月9日	25	1,180	58.13%	Vietnam Telecom
2020年5月9日	25	195	9.61%	Zumy Communications
2020年5月9日	25	159	7.83%	China Telecom
2020年5月9日	465	6,641	94.91%	Microsoft 365
2020年5月9日	465	326	4.66%	DigitalOcean
2020年5月9日	587	316	95.18%	DigitalOcean

アドバイス

ITとITセキュリティチームは、MicrosoftのOffice 365やGoogleのG Suiteなど、既成のメールプロバイダに変換することを真剣に検討してください。独自にメールを管理することは、動作不能、パッチ管理、そして重複するバックアップなどは、順調な時でさえ大きな苦痛を伴うネットワーク管理タスクです。それに加え、スパムやフィッシングとの戦いでは、リソースが常に食われてしまいます。この分野における既成のプロバイダは、スパムとフィッシング対策、優れたアップタイムの達成において、実績があります。

クラウドプロバイダは、SSLにラップされたSMTPというデフォルト設定から、SMTPを設定する方法に関して、信頼性の高い文書をユーザーに提供してください。これは、MicrosoftやGoogleなどのプロバイダが、ホストするメールソリューションにユーザーを取り込むため、少し宣伝になってしまうような文書を挿入することに、43私たちが反対しない唯一のケースです。

政府のサイバーセキュリティ機関は、誰もが単にサービス可能なメールインフラを管理するうえで問題を抱えており、それなりの規模で本当に優秀な仕事ができている組織はごくわずかです。コンテンツベースの攻撃に関して、専門家はDMARCなど最低限の技術的防御の導入と、フィッシング詐欺の認識と予防に関するユーザー教育を引き続き呼びかけてください。

IMAP (143/993) とPOP (110/995)

スパムとされるメールの割合は、たった55%です。

TLDR

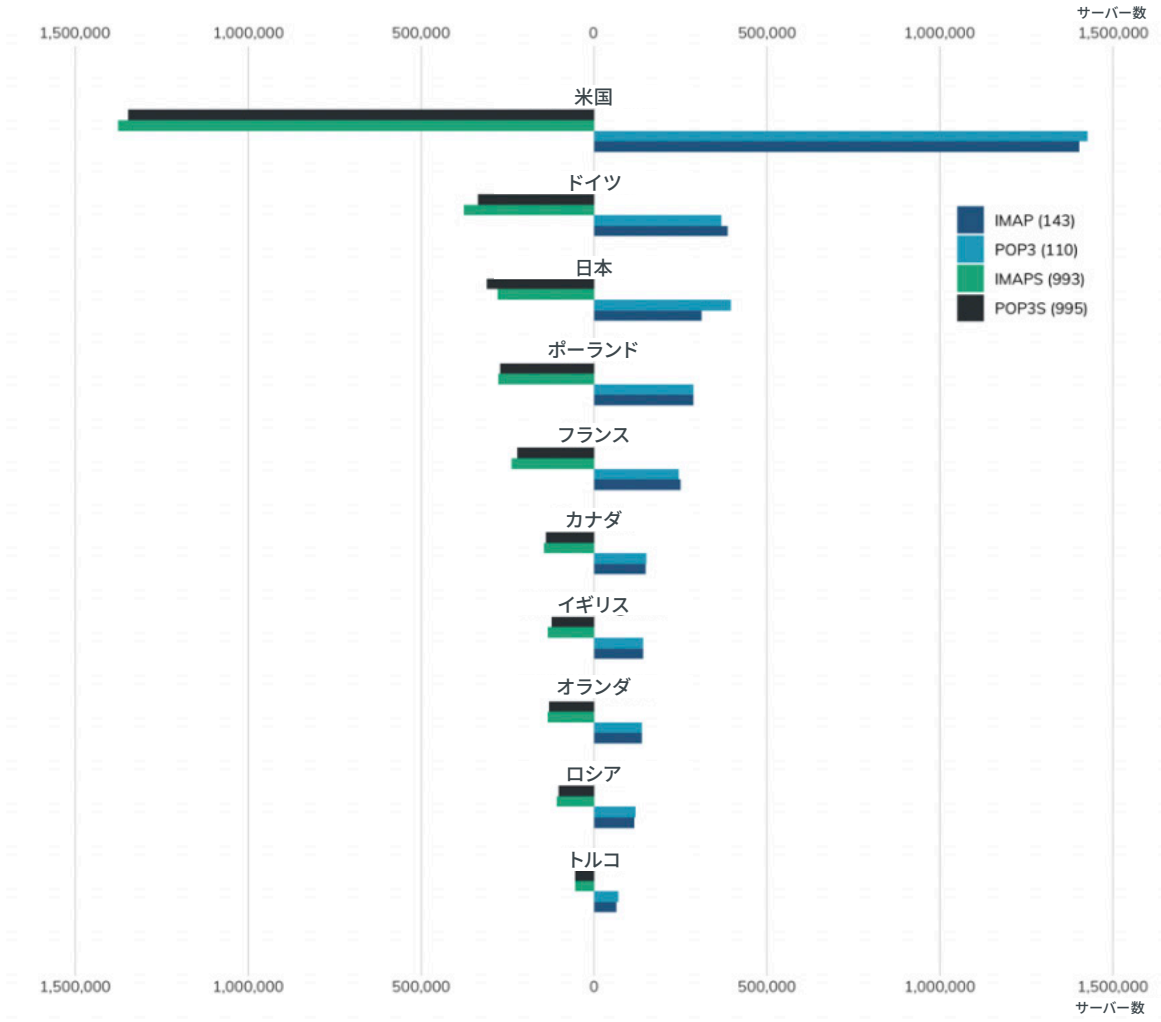
説明：	メールを読んだり送信したりする際、ほぼ毎回使われるステートフルなプロトコルのInternet Message Access Protocolと、一括ダウンロードのメール版のように機能するPost Office Protocolです。
数：	TCP/143でクリアテキストIMAPインスタンスを実行するノード404万5,472件と、暗号化テキストIMAPSを実行するノード384万8,675件を検出しました。 クリアテキストPOPを実行するノード433万1,314件と、暗号化テキストPOPSを実行するノード371万4,171件。 324万919件にRecogフィンガープリント（合計9件のサービスグループ）がありました。
脆弱性：	二要素認証（2FA）が事実上すべての実装で欠けていると、IMAPとPOPが深刻なパスワードの集中攻撃の的になる可能性があります。
アドバイス：	IMAPとPOPアカウントがアプリ固有のパスワードで設定されていることを確認してください。POPサービスの完全な廃止を検討してください。
代替手段：	可能な限り、IMAPではなく、SSLラッピングのIMAPSを優先的に使用してください。
傾向：	改善傾向。2019年に比べ、露出されたメールクライアントサービスは4〜11%減少しました。

[43] その場で作ったかばん語

調査結果の詳細

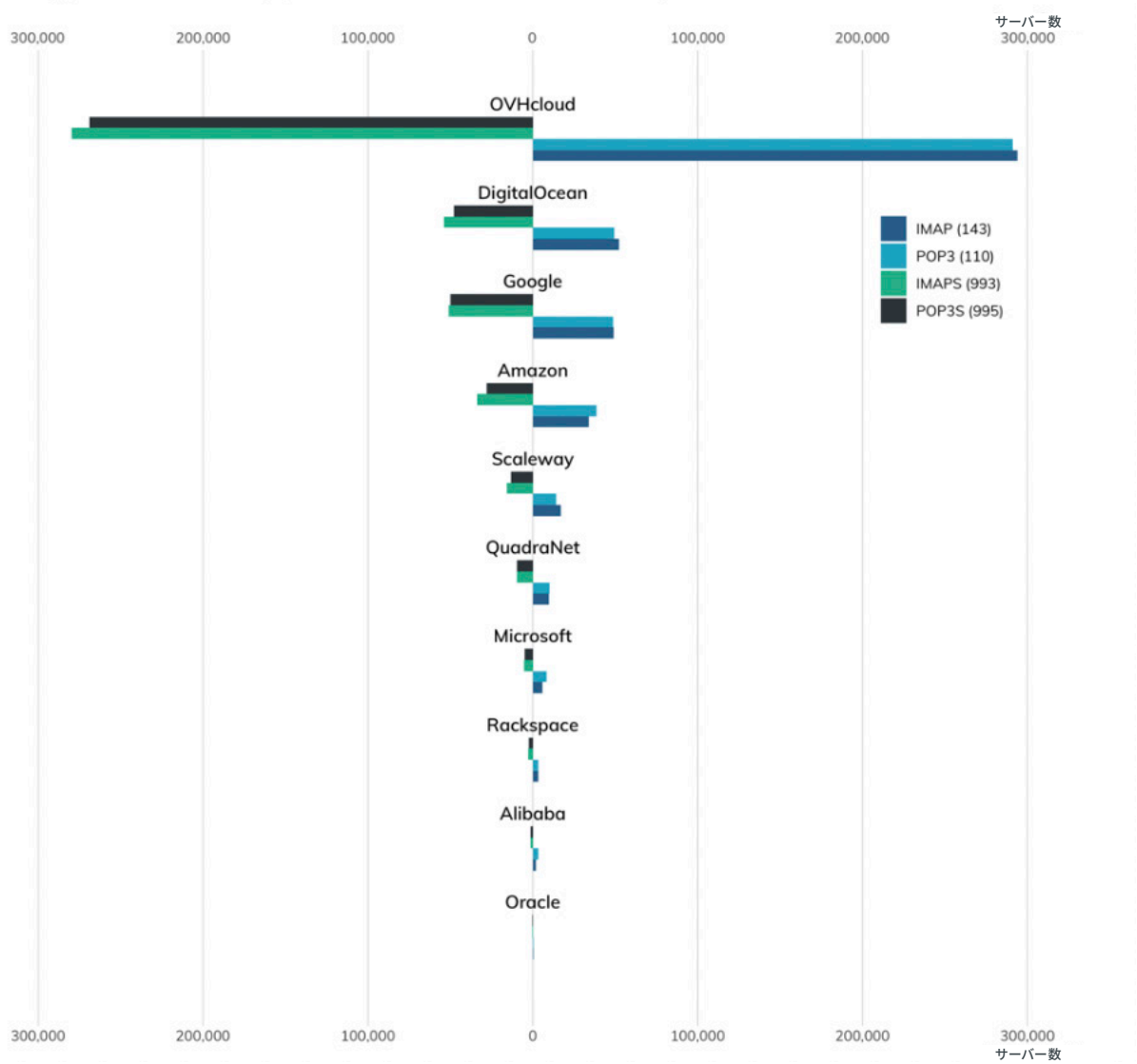
SMTPは、組織へのメールインバウンドを処理するもので、一方POPとIMAPは、読んで返信するために、そのメールを回収している個々のユーザーのアクションを処理します。SMTPと同様に、これらのサービスのクリアテキストおよび暗号化されたバージョンの普及を詳しく調査し、その結果を全体および国とクラウド別にして以下のグラフに示しました。

国別で見る暗号化と非暗号化メールアクセスサービスの比較（上位10か国）



国	IMAP (143)	IMAPS (993)	POP3 (110)	POP3S (995)
米国	1,402,707	1,376,546	1,427,119	1,347,756
ドイツ	386,092	376,780	367,597	336,128
日本	310,159	279,196	396,123	309,619
ポーランド	286,820	278,183	286,957	272,185
フランス	251,024	238,042	244,940	221,815
カナダ	149,171	145,738	150,229	139,814
イギリス	142,433	134,132	141,653	122,933
オランダ	138,202	134,078	138,549	130,015
ロシア	116,758	108,308	119,790	102,058
トルコ	65,526	55,545	69,857	54,418

クラウドプロバイダ別で見る暗号化と非暗号化メールアクセスサービスの比較



プロバイダー	IMAP (143)	IMAPS (993)	POP3 (110)	POP3S (995)
OVHcloud	293,785	279,854	290,942	268,917
DigitalOcean	52,410	53,909	49,531	47,715
Google	48,863	51,040	48,793	50,133
Amazon	33,859	33,934	38,619	28,002
Scaleway	17,062	15,632	14,117	13,187
QuadraNet	9,763	9,744	10,115	9,495
Microsoft	5,797	5,201	8,474	4,810
Rackspace	3,418	2,812	3,391	2,564
Alibaba	2,000	1,399	3,355	1,248
Oracle	342	361	327	283

エンドユーザーがアクセスできるメールプロトコルでは、選択肢が少ないものの、ベンダーごとのIMAPサーバーをフィンガープリントできました。

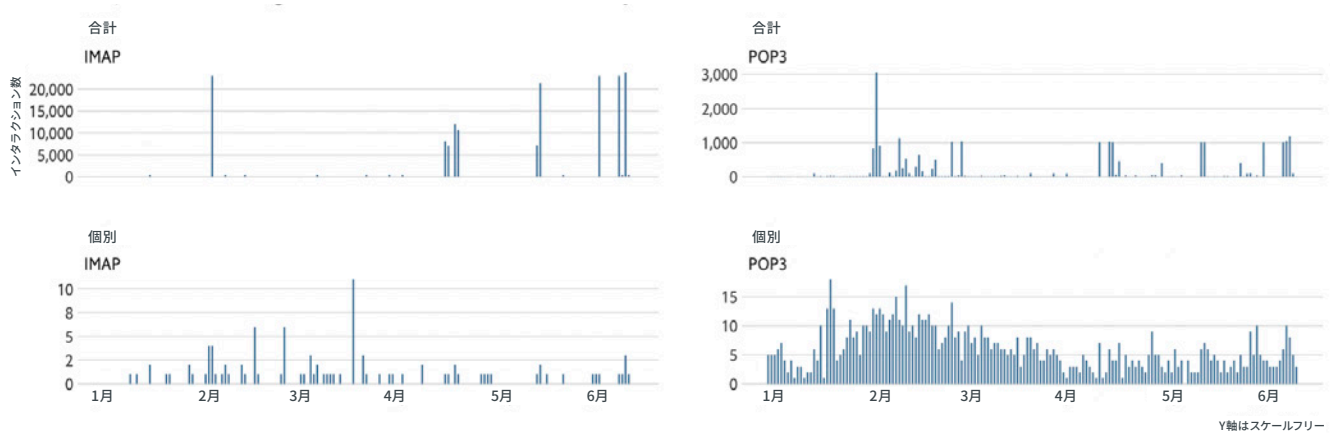
IMAP/POPグループ	数
Dovecot	3,068,391
Courier MTA	103,604
Exchange Server	37,448
Cyrus MTA	12,671
Qpopper	9,809
Bigfoot Email Tools	6,153
Lotus Domino	1,102
CCProxy	896
E-mail Services	845

それでも、バージョンごとのテレメトリはほとんどありません。IMAPとPOPは、事前に認証された方法でこの情報を開示しないことが多く、私たちにはバージョンからそれなりの正確性を得るのに有効なテクニックがありません。

攻撃者の視点

以下のグラフは、ハニーポットのIMAPとPOPへの接続を表しています。はじめはスパイクが外れ値に見えるかも知れませんが、IMAPとPOPのプロビングは実際、常に尖っているもののようです。理由は分かりませんが、これらのスキャンには統計用語でいう「高い季節性」があります。 つまり、他のプロトコルのスキャンで通常みられる恒常性ではなく、バーストが発生する傾向にあるということです。

PROJECT HEISENBERG IMAP/POP3インタラクションの試行



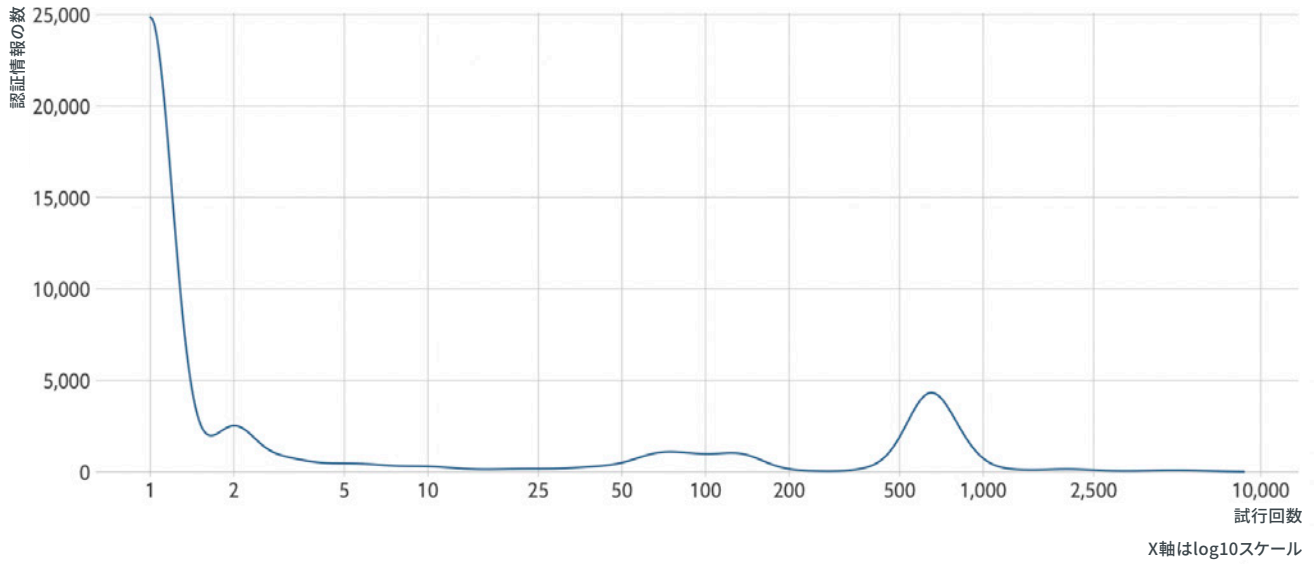
調査期間中、IMAPとPOPで施行された特有のユーザー名は、約7,500件でした。

施行されたユーザー名のトップ20は以下の通りです。

1.	admin	11.	postmaster
2.	test 12.	12.	mail
3.	webmaster	13.	abuse
4.	backup	14.	service
5.	info	15.	spam
6.	marketing	16.	master
7.	contact	17.	helpdesk
8.	support 18.	18.	mailing
9.	office	19.	newsletter
10.	sales	20.	recruit

これらのユーザー名が、それぞれ4,000〜8,000回試行されました。興味深いことに、ほとんどの実行で各ユーザー名が1度だけ試されていますが、攻撃者は、1回で1つのユーザー名と500〜1000個のパスワードを試すこともありました。

特定のログインが試された回数



アドバイス

ITとITセキュリティチームは、独自のオンプレミス型メールインフラを管理するコストを、金銭面だけでなく時間や専門知識の観点からも、定期的にチェックしてください。できる限り、Outlook 365やGoogle G Suite（TLSがデフォルトでサポートしているクライアントメールサービス）など、専門的なメールプロバイダへの移行を検討し、アップタイム保証やスパム排除を「他人に任せる」という恩恵を享受してください。

クラウドプロバイダも同様に、人々を独自のメールインフラを維持することから遠ざけ、合理的で安定した代替手段を検討することを、ユーザーに奨励してください。少なくとも、クラウドプロバイダの文書は、POPとIMAPの違いと、なぜそれらが必要でないのかを明確に説明し、ユーザーをTLSにラップされたクライアントメールサービスに導いてください。

政府のサイバーセキュリティ機関は、クリアテキストのIMAPとPOPプロトコルに代わる強力な暗号化手段を提唱し、POPとIMAPは多くの場合、多要素認証による安全性が確保されていないことからパスワードテストに便利なバックドアであるという事実を一般に周知徹底してください。

リモートアクセス

ここで、はっきりと伝えなければならないことがあります。コンソール端末のセッションで説明した内容は多くのタスクにとって役に立ちません。皆さんと同様に、私たちもコマンドラインのファンですが、最新のITエコシステムでは、リモートデスクトップやサーバー環境のグラフィカルユーザーインターフェース（GUI）の方が有効です。従来の（つまり、ブラウザベースでない）デスクトップアプリケーションにリモートアクセスを与えるにしても、イントラネットリソースへのアクセスを防ぐにしても、さらに完全なデスクトップのインタラクティブセッションの遠隔利用を有効にするにしても、これらのソリューションが真のニーズを満たし、Get Stuff Done™のような組織作りに役立ちます。

この現実を認識したうえで、非常に人気の高い2つのリモートアクセスサービスについて見てみました。

- Virtual Network Computing（VNC、TCP/5900）
- Microsoft Remote Desktop（RDP、TCP/3389）

拝啓、X-Window様、大変申し訳ありません、貴君の時代は終わりました。今後は、天文学研究室とハリウッド映画のハッキングシーンでご活躍ください。

VNC (5900 & 5901)

これはRFBですが、どういう訳か誰もそう呼びません。

TLDR

説明：	Remote Framebufferプロトコルを使用して、キーボード、ビデオ、マウスの完全なインタラクティビティをリモートシステムで可能にする、グラフィカルデスクトップ共有システムです。
数：	34万7,940件のノードが検出されました。[44] 34万7,932件（99.99%）に、フィンガープリントバージョンがありました。
脆弱性：	VNC製品を扱うすべてのベンダーで、最低37件あります。
アドバイス：	VNCを直接インターネットに露出させないでください。
代替手段：	VNCを使用しなければならない場合は、SSHトンネルでVNCを実行してください。

Virtual Network Computing（VNC）サービスは、1999年に（AT&Aのせいで閉鎖された）Olivietti & Oracle Research Labで作られ、Remote Framebuffer（RFB）プロトコル[45]を使用して、遠くにあるデスクトップまたはサーバーのGUIに連れて行ってくれます。macOSで「スクリーン共有」機能を使用すれば、VNCの実行や使用の感じが分かります。独自の、カスタムVNCのクライアントサーバーソリューションを持つベンダーは何十社もあり、すべて同じ基礎プロトコルの上に構築されています。

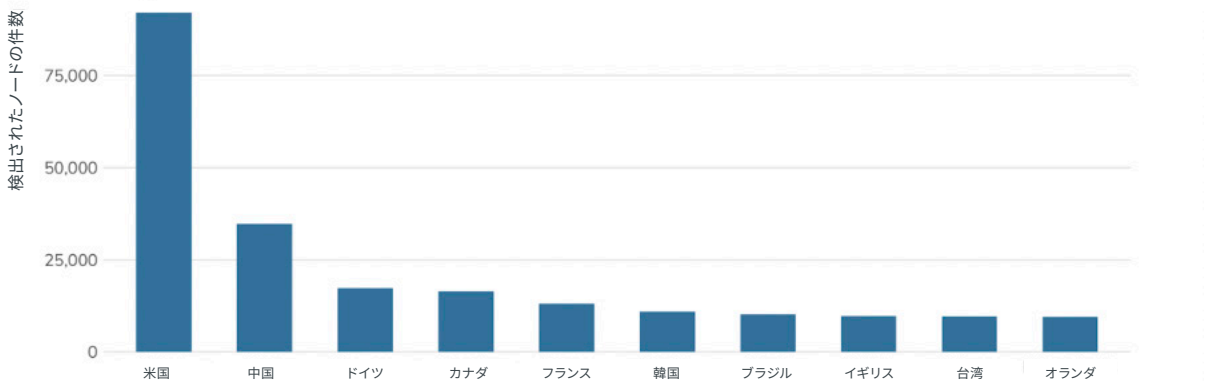
[44] 5,900番と5,901番ポートのみを対象にした調査ですのでご注意ください。

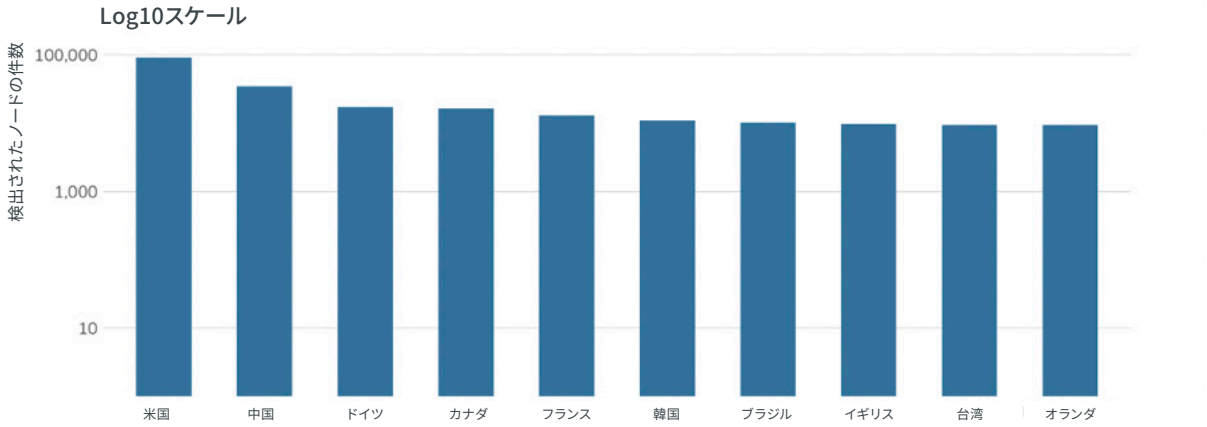
[45] RFC 6143 <https://tools.ietf.org/html/rfc6143>

調査結果の詳細

Project Sonarは、5,900件のデフォルトポートと人気のある代替ポートで、34万7,940件のVNCサーバーを見つけました。その他のソースで、さらに大きな数字を見たことがあるという場合（具体的には、素晴らしいKasperskyのサマリーペーパー[46]）、VNCはインターネットの未開拓地にある多くのポートにも存在しているため、そのような数字もおそらく正確なものです。理由はどうであれ、VNC実装は、設計上の決定として、IANAが割り当てたポート番号を厳密に遵守しません。つまり、エクスポージャーのベースラインとして私たちの数字を使うことはできます。一方、少なくとも60%近くのVNCユーザーがサービスで最も一般的なポートを使うという結果が出ていますが、国やネットワーク別の分布を一般化し過ぎるのは避けた方が良いでしょう。

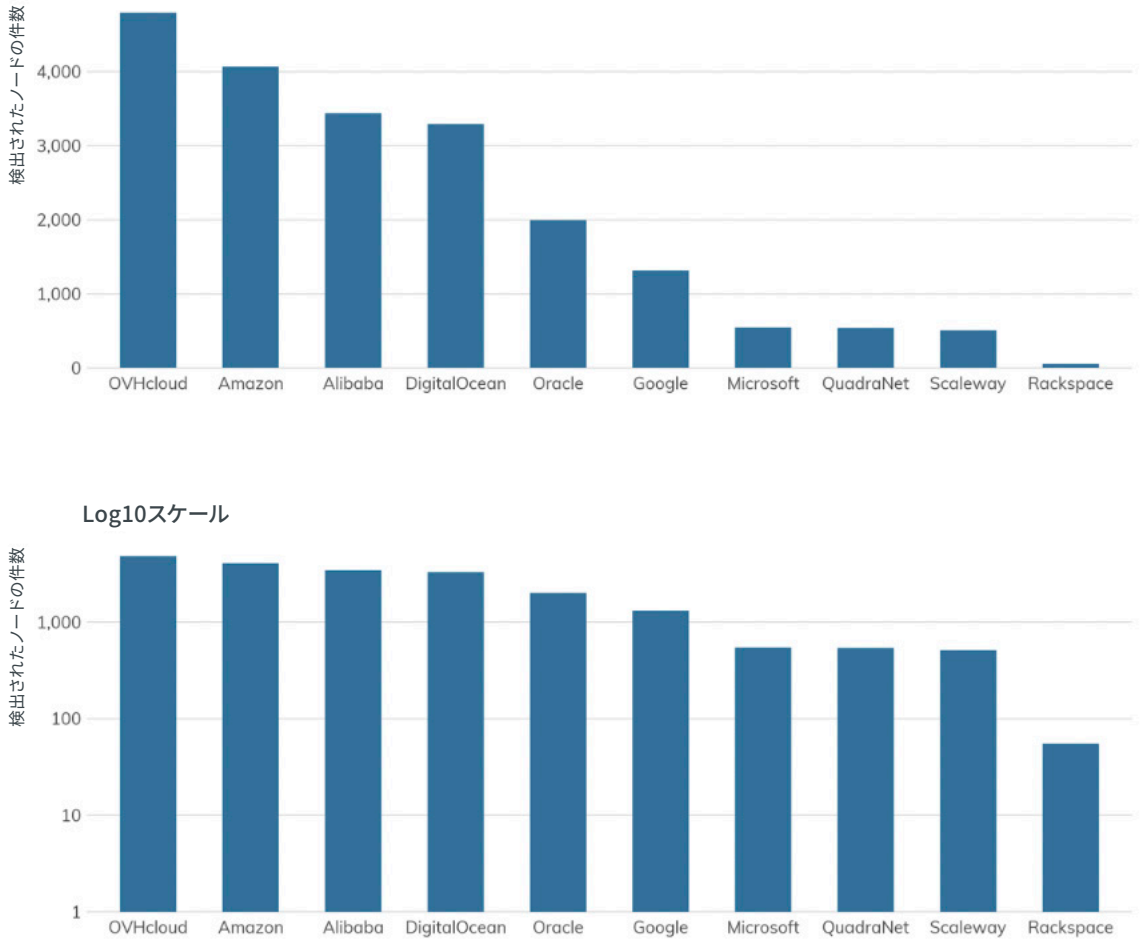
リモートアクセスの上位10か国：VNC（5,900+5,901）





[46] Kasperskyは2019年11月に素晴らしいVNC脆弱性調査レポートを発表し、当時インターネットには60万件のVNCに似たノードがあった可能性を指摘しました。
<https://ics-cert.kaspersky.com/reports/2019/11/22/vnc-vulnerability-research/#_Toc22133279>

クラウドプロバイダのリモートアクセス：VNC（5,900+5,901）



ここでは、OVHがリードしています。これは、「VNCを通してパブリッククラウドインスタンスにアクセスする方法」[47]に関する「便利な」サポートページがあるためです。VCNにはルートユーザーとしてログインするため、このページにはルートユーザー用のパスワードの設定方法も記載されています。これは多くの規制基準に違反しており、本当に泣きたくなります。

AmazonもAlibabaやDigitalOceanに並び、[49]わざわざ攻撃面を広げる手助けをしています。[50]これで、クラウドエクスポージャービューで彼らが「トップ4」となった理由がお分かりになるでしょう。

[47] OVH VNCサポートページ <https://support.us.ovhcloud.com/hc/en-us/articles/360002208690-How-to-Access-a-Public-Cloud-Instance-via-VNC>

[48] AWS VNCサポートページ <https://aws.amazon.com/premiumsupport/knowledge-center/ec2-linux-2-install-gui/ >

[49] Alibaba VNCサポートページ <https://www.alibabacloud.com/blog/how-to-install-and-configure-vnc-on-an-alibaba-cloud-ecs-instance_595135>

[50] DigitalOcean VNCサポートページ <https://www.digitalocean.com/community/tutorial_collections/47>

エクスポージャー情報

本レポートのいくつかのセクションでもそうだったように、VNCにおけるビジネスおよび家庭用ISPのエクスポージャーについて話す必要があります。なぜなら、これが全エクスポージャーのうち大きな割合を占めているからです。以下のISP/プロバイダは、発見されたVNCノードの合計30%を占めました。

ISP/プロバイダ	数
China Telecom	20,143
AT&T	12,202
British Telecom	11,410
Charter Communications	9,985
Orange	9,415
Comcast	9,229
Telefonica De Espana	6,758
HiNet	6,661
Korea Telecom	6,017
中国聯合通信	5,604
Vodafone	5,508
Deutsche Telekom	5,075
Telecom Argentina	4,980
Uninet	4,549
Cox Communications	4,056
CenturyLink	3,686
Telecom Italia	3,620
SK Broadband	3,574
NTT Communications	3,497
Host Europe GmbH	3,466

すでにお聞きになったことがあるかも知れませんが、これらのノードは主に、内部ネットワークの何かに、迅速なリモートアクセスを必要とする企業か、または遠隔で自宅システムにアクセスしたい、家庭ユーザーです。

認証情報を推測しようとするのは、どのような方法であっても米国ではCFAA[51]の違反になります。調査チームはオレンジ色の囚人服を着たくはないので、ログインが必要なシステムの数を調べることはできません。また、画像に機密情報が含まれていた場合、多くの地域でプライバシー法の違反となるため、スクリーンショットを撮ることもできません。

発見されたサーバーの52%がRFBのバージョン3.8（最も新しいRFBのスタンダード）を使用しており、次に多かったのは何らかのmacOSを使用しているというのが19%でした。これは、Apple製のコンピュータが、ある程度の数字で現れる可能性が高い、数少ないプロトコルの1つです。VNC上では、adminインターフェースを露出している数十台の*マルチファンクションデバイス*[52]*も見つかりました。*

攻撃者の視点

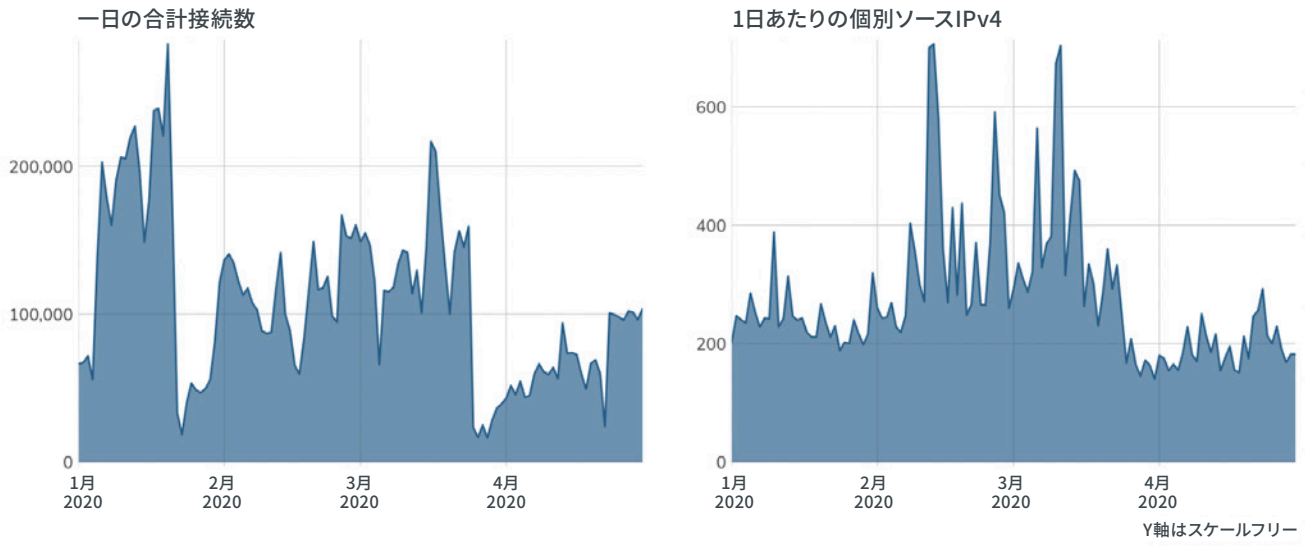
数年間にわたり、VNCの全バージョンで多くのバグが見つかっていますが[53]、幸い、そのほとんどは認証済みのセッションがなければ効果が出ません。しかしながら、「ダークウェブ」にはただ試行されるのを待っている80億以上の認証情報が出回っています。

[51] https://www.law.cornell.edu/uscode/text/18/1030

[52] 最近流行っている、プリンターのかっこいい呼び方です。

[53] libvnc <https://attackerkb.com/search?q=libvnc>、TightVNC <https://attackerkb.com/search?q=tightvnc>、TurboVNC <https://attackerkb.com/search?q=TurboVNC>、UltraVNC <https://attackerkb.com/search?q=UltraVNC>

VNC（TCP/5900+5091）HEISENBERGの活動



他のサービス同様、Heisenbergハニーポットネットワークでは VNCサービスを取り上げていません。そのため、上記のグラフに示されているのは、日和見主義的なスキャンまたは組織の設定ミス（AWS、GoogleまたはRackspaceで、あると思っていたIPアドレスにない、かつて所有していたVNCサーバーを狙うなど）です。

接続の試行回数が多いことから、VNCをインターネットに露出する際は十分に注意して、一度も使用されたことのない強力な認証情報でパッチが当てられていないVNCサーバーコードを使用し、さらに多要素認証で安全性を強化してください。[54]

アドバイス

ITとITセキュリティチームは、すべてのVNCアクセスをVPN接続やSSHトンネルの背後に置き、絶対にVNCを直接インターネットに露出させないようにしてください。VNCアクセスのあるホストをパブリックインターネットで使用するには、設定や維持で気を付けるべきことが多くあります。

クラウドプロバイダは、VNCを裸のまま使用することは避けるように呼びかけ、VNC-over-SSHなど、より安全でコスト効率の高いソリューションをユーザーに提案してください。当然ながら、セキュリティが強化されたVNCのクライアントやサーバーのセットアップはありますが、チュートリアルやセットアップガイドの多くは、ユーザーの攻撃面を広げるだけのものです。

政府のサイバーセキュリティ機関は、VNCの安全な使用方法のガイダンスを定期的に公開し、VNCの脆弱性開示を監視し、また時宜を得たアラートを発行して、インターネットサービスプロバイダに少なくともデフォルトポート（5900）ではVNCアクセスをブロックするよう奨励してください。

[54] RealVNCの便利な2FAガイドは https://help.realvnc.com/hc/en-us/articles/360002250077-Introduction-to-Multi-Factor-Authentication- をご覧ください。

リモートデスクトップ — RDP (3389)

これはVNCに似ていますが、マイクロソフト寄りのものです。

TLDR

説明：	システム間のグラフィカルユーザーインターフェース（GUI）接続のためにMicrosoftが開発した独自のプロトコルです。デフォルトのポートはTCP/3389ですが、どのオープンポートでもホストできます。
数：	397万9,356件のノードを検出しました。 4万4,540件（1.1%）にRecogオペレーティングシステムフィンガープリント、397万4,474件（99.8%）にセキュリティスキームのRecogフィンガープリントがありました。
脆弱性：	2019年の春、Microsoftが発表したCVE-2019-0708[55]（BlueKeep）を含む、多くのリモートコード問題があります。
アドバイス：	「常にオン」である必要がある場合は、RDPをVPN接続に置きます。RDPを断続的に使用できる場合は、RDPを露出するすべてのノードが推奨されている仕様に沿って完全にパッチで強化されていることを確認し、多要素認証を利用してください。
代替手段：	これは、リモートシステムに遠隔アクセスするうえでMicrosoftが推奨するソリューションです。宣伝通りに動作するため、代替手段は特にありません。このようなアクセスを必要とする場合は、「**アドバイス**」セクションのガイダンスに従ってください。
傾向：	若干の改善傾向。2019年の測定から、RDPは5%近く減少しました。

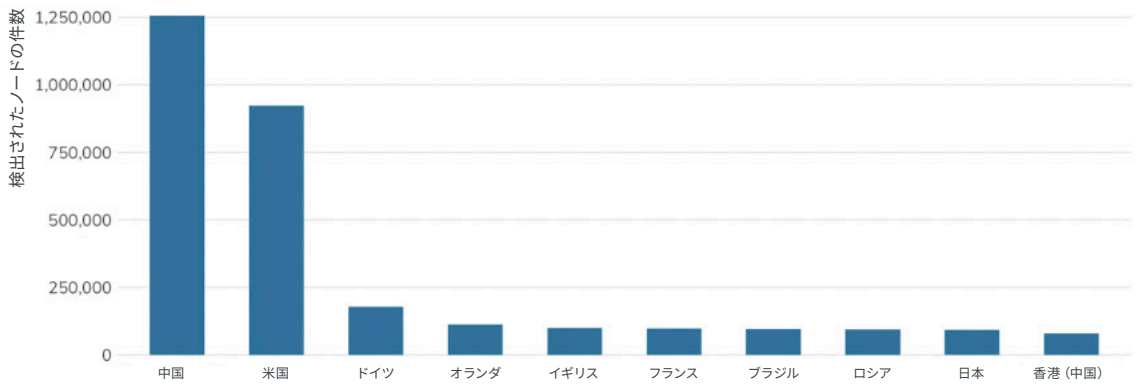
WindowsXP（2001）の導入により、多くの発明が生まれました。例えば、マルウェアの広範におよぶ分布、ブルースクリーンによるデータ損失、また、リモートデスクトップ接続を介して他のWindowsXPシステムのキーボードビデオマウス（KVM）接続を容易に得られるという新たな機能などです（以前は「端末サービス」と呼ばれていましたが、Microsoftはそれが気に入らなかったようです）。これはXP以降すべてのWindowsバージョンに搭載されており、ほとんどのユーザーが遠隔でWindowsシステムにアクセスする際、主にこの方法を使っています。サイバーセキュリティ関係者の多くは、Microsoft Remote Desktopについて話す時は、 RDP（リモートデスクトッププロトコル）のショートカットを使用します。

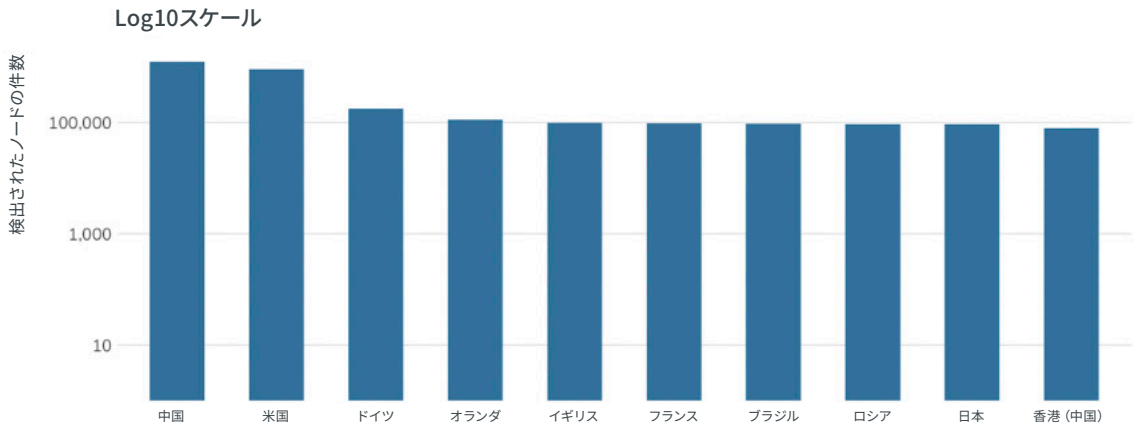
調査結果の詳細

Project Sonarは、400万件弱の活発なRDPノードを発見しました。そのうちの4分の1以上が中国に帰属するネットワークです。

[55] BlueKeep/CVE-2019-0708 <https://attackerkb.com/topicsl/cve-2019-0708>

リモートアクセスの上位10か国：RDP（3,389）





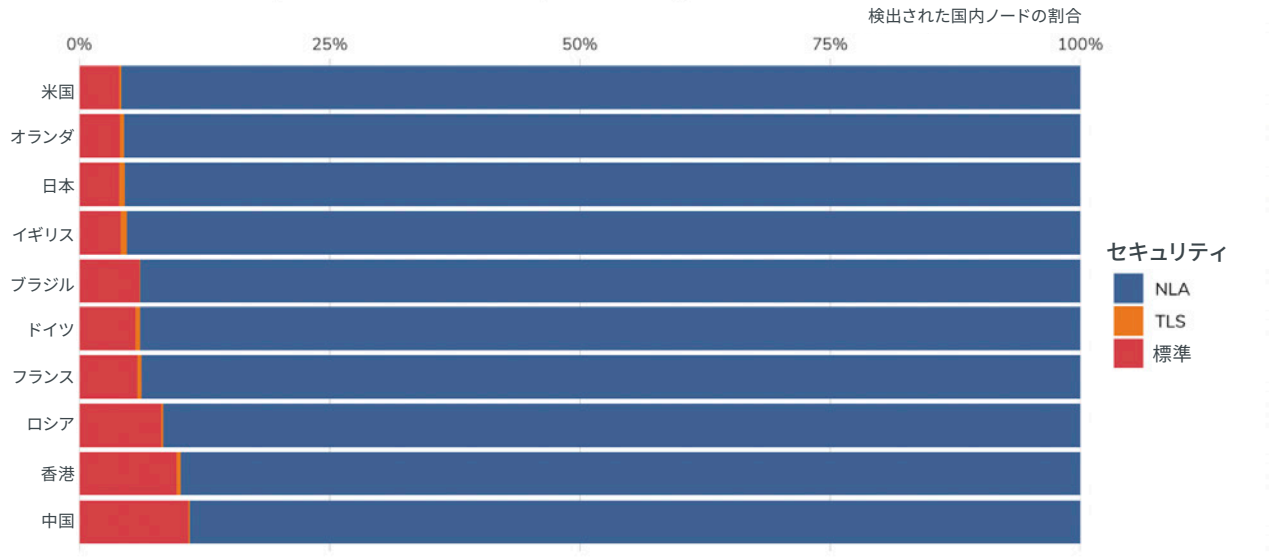
エクスポージャー情報

当然のことながら、RDPノードの約4分の1が、調査対象のクラウドプロバイダネットワーク内にありました。Microsoft Azureがトップになると予想していましたが（Windowsですから）、 接続しなくてもこのようなリモートシステムは利用できるという訳です。ですから、AzureがホストするRDPが3位だったことを知ったときは、驚きました。3位と言っても、クラウドの巨人であるAmazonとAlibabaに次いでいるので、これは強力な3位です。

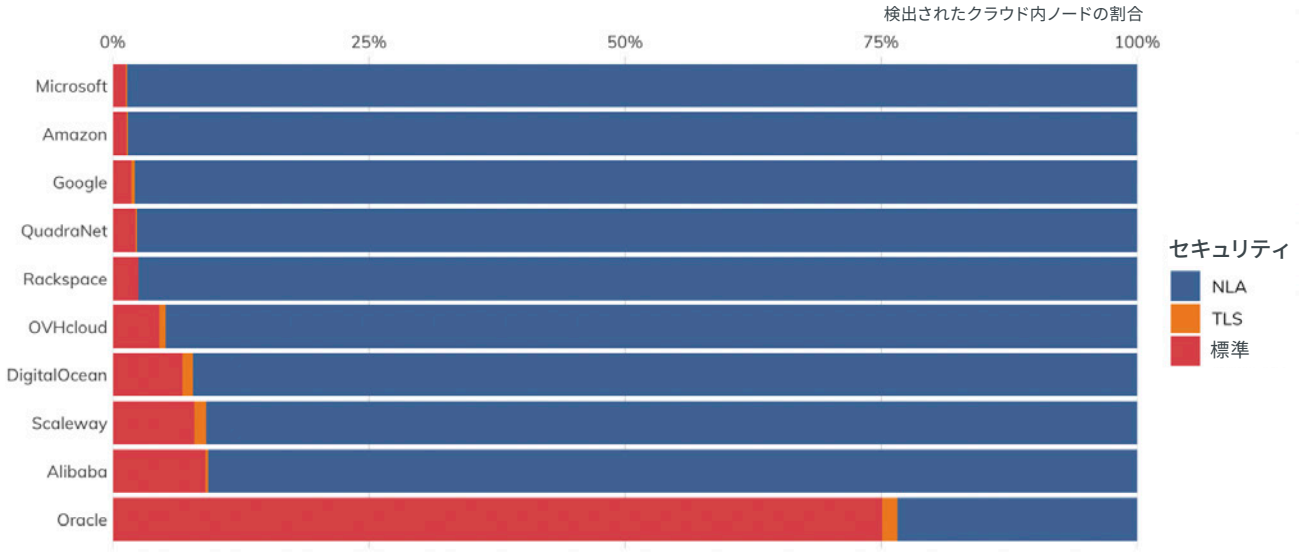
RDPはどこにでもあり、その数は（VNCの40万弱に対し、400万以上で）VNCを一桁上回っています。 前述の「クラウド」使用の場合以外では、中小企業がビジネスクラスのISP接続で、または事業がリモートアクセスや管理に、さらに小売り業者が日常的な管理業務でポイントオブセールスのRDPを有効にするなどの使用方法があります。またホームユーザーの間でも、家庭用PCへのリモートアクセスを有効化するうえで、ファイヤーウォールに時間をかけて穴をあけるのに、使いやすいとされています。このような遍在性が、設定ミスのまん延や脆弱性と重なり、攻撃者にとって理想的な標的となるのです。これについては次のセクションで説明します。

RDPセッションにはさまざまな[56]設定方法があります。Project Sonarは、「標準」または「レガシー」、「ネットワークレベル認証」（NLA）、そして「トランスポート層セキュリティ」（TLS）の3つのステートを認識できます。「標準」というのはあたかも列車事故の発生待っている状態で、（定期的にパッチを当て、多要素認証のある安全な設定を利用しているという前提で）NLAとTLSはどちらも、セッションの安全性を確保するのに非常に役立ちます。また、トップ10の国におけるノード比率の高さと、より安全な接続オプションがクラウドに使用さていることから、ほとんどの家庭およびビジネスクラスユーザーが、それを理解したように見えます。

国別で見るRDPセキュリティ使用率



クラウドプロバイダ別で見るRDPセキュリティ使用率



一方、クラウドの仕組みはそれぞれ異なり、安全なセキュリティモードの使用という点では、Oracleクラウドのユーザーが最下位となっています（これもクラウド内のノード比率から見て判断）。これは、おそらくRDPを有効化する際のデフォルト設定が原因だと思われます。

[56] リモートデスクトッププロトコル、基本的な接続性とグラフィックスリモート <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/5073f4ed-1e93-45e1-b039-6e30c385867c>

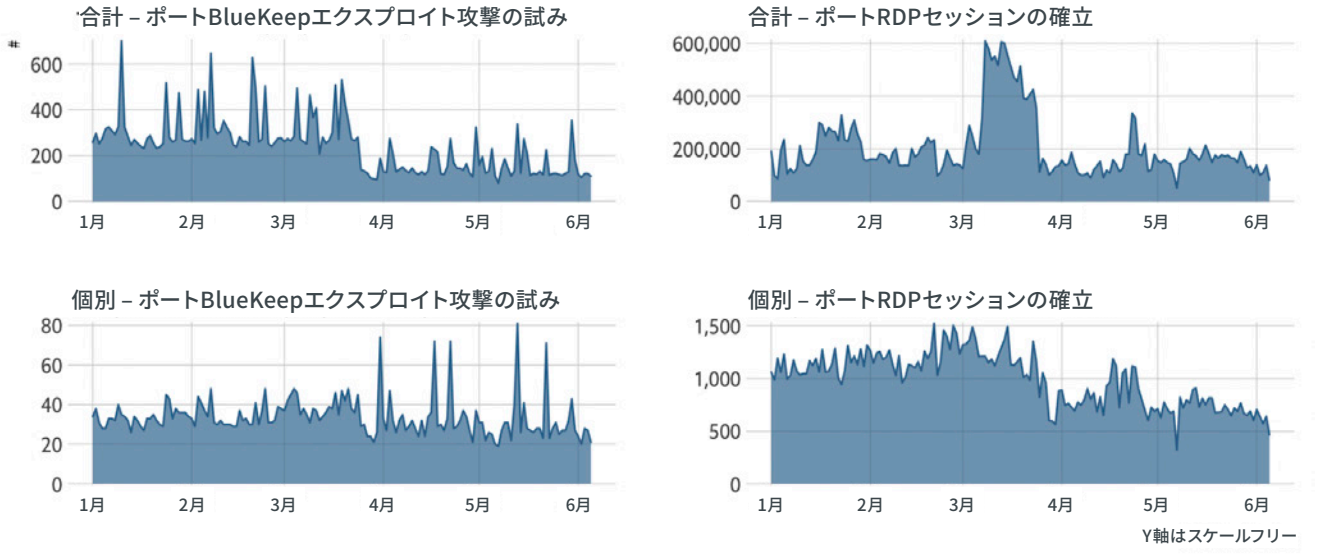
攻撃者の視点

このプロトコルは、ハニーポットがしっかりとカバーしており、RDPセッションの確立とBlueKeep経由でのRDP悪用の試みという2つの領域に注目します。

2019年の春にMcrosoftが発表した、RDPにおける認証されていないリモートコード実行の欠陥である BlueKeepは、かなり悲観視されていたものの、ほぼ終息しました。これは、人々が実際にパッチを当て、NLAセキュリティに切り替えたためだと考えられます（国およびクラウド別の調査結果にも表れており、また調査対象となったRDPの92%がNLAを使用していたことも分かっています）。BlueKeepがいわれていたほどの悪夢にならずに済んだのは、すべてのレベルで早期に行われた、一貫した正しい警告のおかげだったと私たちは考えています。

BlueKeepの活動の証拠がないという訳ではありません。しかし、BlueKeepの使用よりも、クレデンシャルスタッフィングの試行の方がはるかに多く見られています。

PROJECT HEISENBERG　RDPアクティビティ



上記の図から学べることが4つあります。

- BlueKeepの数が非常に少ないということ。
- 悪意のあるユニークなソースホストの数が少ないということ。
- RDPの活動が不変であるということ。
- 攻撃者は、2020年のパンデミックにより米国がロックダウンを始めた頃、幸運が訪れるかもしれないと考えていました。

2020年1月1日から2020年4月30日までの間に、HeisenbergはBlueKeepベースのエクスプロイトの使用を試みた、またはハニーポットネットワークに対してクレデンシャルスタッフィングを行った、個別ソースのIPアドレスを8,500件以上見つけました。これらのユニークなIPv4アドレスの11%がDigitalOceanに由来していますが、悪意のあるRDPトラフィックすべてのうち16%が、オランダのホスティングプロバイダであるHostkeyから来ています。これら2つのネットワークソースが目立つ一方、1,310件の個別の自律システム（ASes）が悪意のあるソースをホストしているため、非難を目を向ける場所は多くあります。

アドバイス

ITとITセキュリティチームは、GUIリモートアクセスのためにどうしてもRDPを使用するという場合は、RDPをVPNに置くことを検討してください。RDPを直接インターネット上に置く必要がある場合は、必要に応じて行うようにし、RDPが露出されている全てのシステムにパッチが適用されており、多要素認証によってRDPの設定ができるだけ強力であることを徹底してください。

クラウドプロバイダは、かなり安全なデフォルトを確保し、弱い設定でRDPを展開したユーザーに対し、定期的な注意喚起を行ってください。ユーザーが一定期間だけ簡単にRDPを有効化できるようにすることは、クレデンシャルスタッフィング攻撃の予防に大きく役立ちます。インターネットを少しでも安全にするため、プロバイダは悪意のあるトラフィックを監視し、地域のCERTと協力して、可及的速やかに悪意のあるノードをシャットダウンさせてください。

政府のサイバーセキュリティ機関は、引き続きRDPの危険性と、安全な使い方の徹底について、人々への啓蒙活動を続けてください。悪意があるとしてよく知られるソースがあることから、セキュリティ機関は地域のCERTやホスティング/クラウドプロバイダと連携し、悪いトラフィックをリモートホストに侵入する前に止められるようにしてください。

CITRIX ADC/NETSCALER (TCP/VARIAOUS)

これはVNCと似ていますが、例えて言うなら、Plan9がベル研究所から抜け出して、人気者になったようなものです。

TLDR

説明：	Microsoft Remote Desktopと同様の クライアント/サーバーテクノロジー で、アプリケーションやオペレーティングシステムデスクトップ環境全体へのリモートアクセスを提供します。
数：	62,998件のノードを検出しました。 62,998件 (100%) にRecogサービスバージョンのフィンガープリントがありました。
脆弱性：	多いです。最近では、[57]2020年1月以降、認証されていないリモートコード実行の重大な脆弱性が広く悪用されています。
アドバイス：	是非使用してください。しかし、パッチを当て、多要素認証を使用してください。
代替手段：	Microsoft Remote Desktop、VNCなど、よく使われているVPNで使われる同様のソリューション。

Citrixは1989年に設立され、長年にわたって多様なリモートアクセスソリューションを開発してきました。最新のCitrix ADC (アプリケーション配信コントローラ) とNetScalerソリューションは、Microsoft Remote Desktop Servicesインフラを使用して、仮想アプリケーションやデスクトップをリモートユーザーに配信します。組織には、単なるなリモートデスクトップよりも堅牢なアクセスコントロールを設定することが可能で、Citrixのアプリケーション配信プロセス内では、それをさらに高速化させ、Remote Desktopセッションよりも消費する帯域幅を少なくする最適化が可能です。

調査結果の詳細

HTTPとNTPサーバーがCitrixシステムであることを通知するようになっているため[58]、インターネット上で当該システムを認識するのは想像以上に簡単です。これにより、Rapid7 Labsのリサーチャーが、インターネット上のCitrixシステムの普及を追跡することは容易でした。また、2020年3月にはダウンロード可能なCitrixクライアントのバージョンフィンガープリントに基づいて、サーバーのバージョンフィンガープリントを見つける方法を開発しました (もう一度いいますが、Citrixが自社のシステムを認識可能しています) 。

Labsチームが時間をかけてこのような取り組みを行ったのは、攻撃者が危険なリモートコード実行の脆弱性[59]にパッチを当てていないシステムを攻撃し続けていて、私たちはさまざまな技術のパッチ適用率をモデルする多くのプロジェクトを進めているからです。

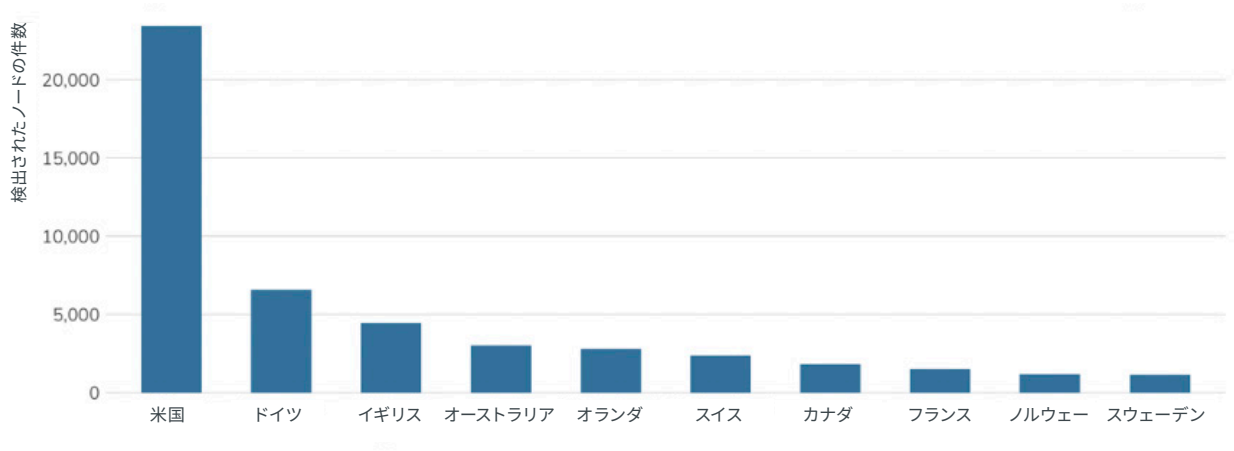
トップ10にある他の多くの国と異なり、中国はCitrixシステムのインターネット面露出で、スウェーデンすら破れませんでした。

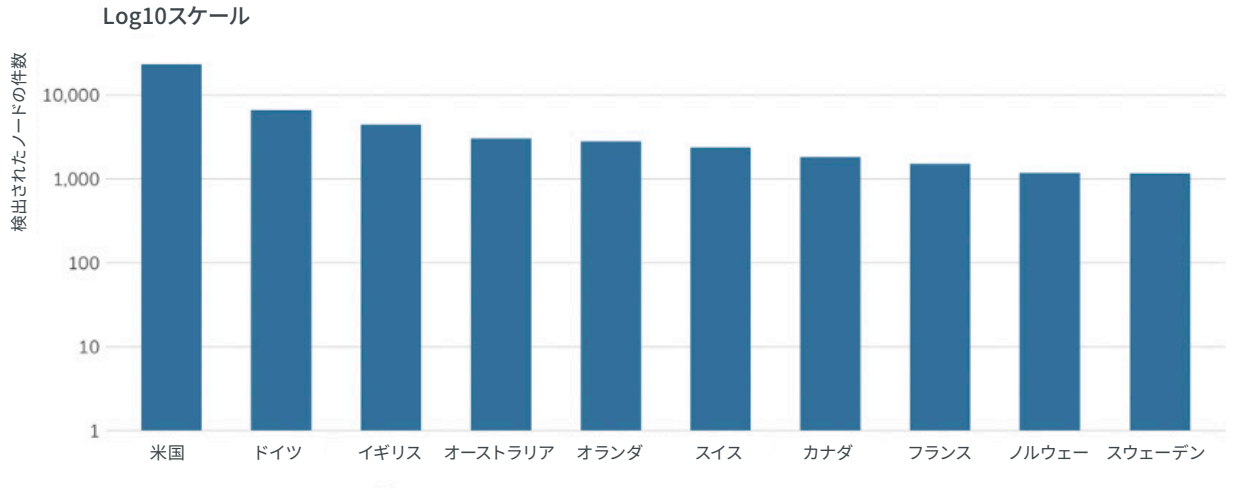
[57] Citrix NetScalerの積極的な悪用 (CVE-2019-19781) : 知っておくべきこと <https://blog.rapid7.com/2020/01/17/active-exploitation-of-citrix-netscaler-cve-2019-19781-what-you-need-to-know/>

[58] Citrix向けRecogフィンガープリント <https://github.com/rapid7/recog/search?q=citrix&unscoped_q=citrix>

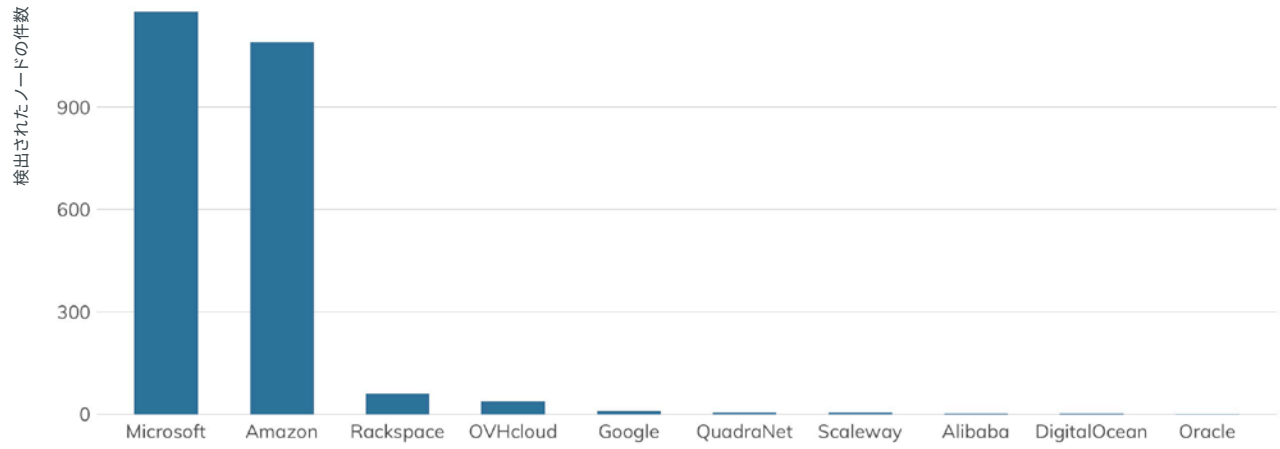
[59] CVE-2019-19781 <https://attackerkb.com/topics/x22buZozYJ/cve-2019-19781>

リモートアクセスの上位10か国：CITRIX ADC/NETSCALER（多種）

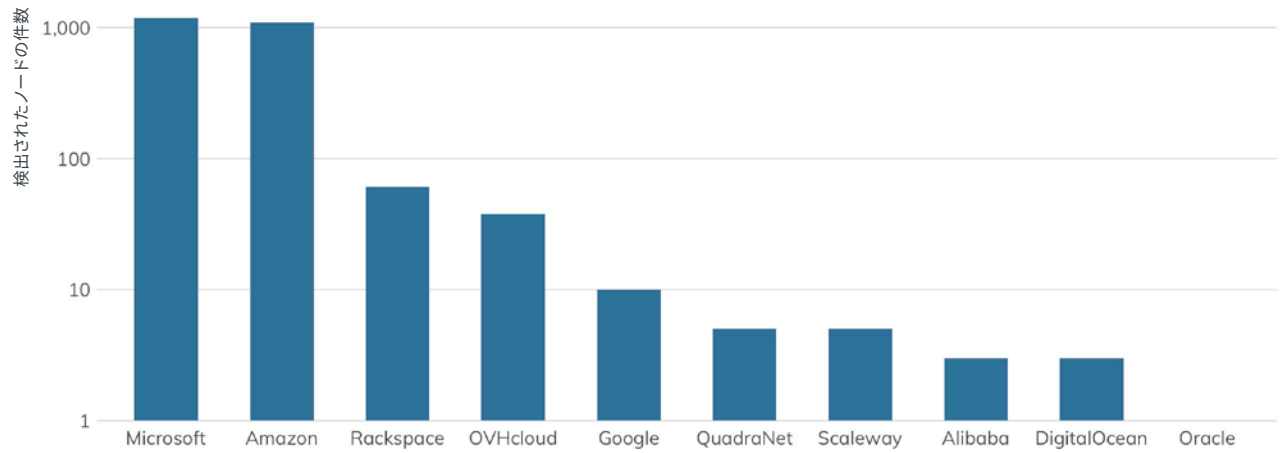




クラウドプロバイダリモートアクセス：CITRIX ADC/NETSCALER（多種）



Log10スケール



クラウド環境にCitrixが欠如しているというのは、この技術が通常、ほぼ企業やビジネス環境のみで見られる仮想デスクトップ基盤（VDI）に関連付けられることから、納得できます。

エクスポージャー情報

積極的に悪用されている脆弱性や、そのような状況に関する政府の定期的な警告[60]を考慮すると、インターネットに面するCitrixサーバーが完全にパッチ適用されている、または緩和策があると思うかもしれません。（またしても）それは間違いです。しかしこの場合、状況はそれほど悲観的ではありません。

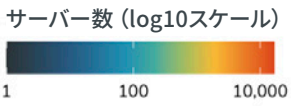
[60] US-CERT 「Citrix CVE-2019-19781の検知」 <https://www.us-cert.gov/ncas/alerts/aa20-031a>

CITRIX ADC/NETSCALERシステムの地理的分布

パッチ済み

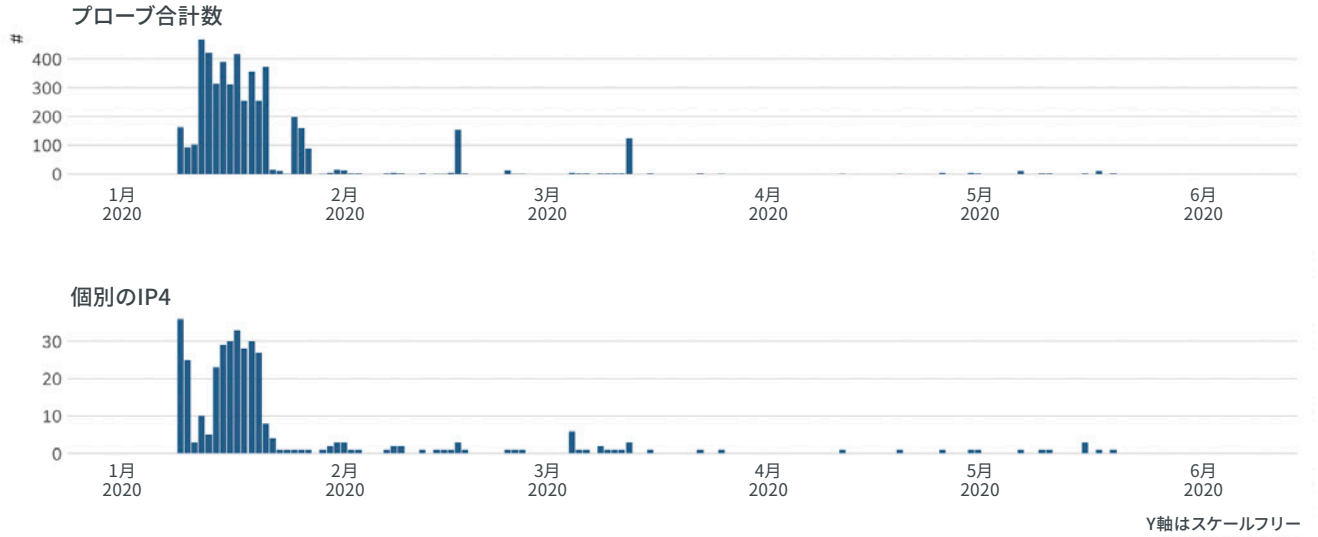
脆弱

脆弱/旧式



私たちのバージョンフィンガープリント技術では、インターネットに面するCitrixシステムの73%にパッチが当てられている、または緩和策が整っていることが分かりました。残りの27%は、脆弱、またはひどく時代遅れである（それにより他にも問題を抱えている）という状況です。パッチ率を73%まで引き上げるには、5か月かかりました。

CITRIXシステム向けの攻撃者プローブ



Heisenbergハニーポットノードの大半はクラウド環境にあり、 これまでに見たように 、それは通常、Citrixの居場所ではありません（少なくともパブリックインターネットのクラウドセグメントでは）。1月に、悪用できるシステムを頻繁に探している攻撃者やリサーチャーを捕まえましたが、そのアクティビティは（完全に止まっていはいないものの）下火になりました。

私たちのハニーポットはCitrixをエミュレートしないため、アクティビティの不足は攻撃者のインベントリスキャン後、ノードが無視されているためだと考えられます。攻撃者はまた、初期のインベントリリストを使っているか、すでにパッチ処理に長時間かかった、数千というシステムに足場を持っているのかも知れません。

アドバイス

ITとITセキュリティチームは、ベンダーからの通知やCVEレポートをくまなく監視し、可及的速やかにCitrix環境にパッチを適用してください。過去18カ月間では、リモートアクセス技術を標的にする攻撃が増えていることから、これらのシステムで、より詳細なログイン設定でモニタリングを強化するのも良いアイデアです。

Citrixはクラウド環境向けのソリューション[61]も提供していますが、その使用はあまり普及していないようなので、**クラウドプロバイダは**現状の対策を引き続き行うだけで十分です。

政府のサイバーセキュリティ機関はこれまで通り、Citrixのようなリモートアクセス技術における脅威アクターの活動や、脆弱性の深刻さに関する意識向上の取り組みを続けてください。

[61] 例：https://www.citrix.com/global-partners/amazon-web-services/citrix-workspace-on-aws.html

データベース

誕生以来、コンピュータは情報の整理で重要な役割を果たしてきましたが、1960年代に、主にIBMのSABRE[62]システムが成功したこと、そしてそれが旅行の予約方法に改革をもたらしたことで、大きく飛躍しました。E.F. Coddが70年代に、現在リレーショナルデータベース管理システム（RDBMS）として知られる、つまりキーによって接続されている情報の正規化された表に関して説明する、基礎的文書を発行しました。それ以降、私たちはあらゆる種類のデータベースタイプの誕生を見てきましたが、本レポートでは、RDBMS、そしてシンプルでありながらパワフルなKey-Valueストレージシステムという2つの一般的なタイプに注目します。

リレーショナルデータベースは素晴らしい技術で、今後も長く使われるでしょう。だからと言って、インターネットに露出するべきではありません。決して。通常なら、安全にWebアプリケーションの背後に置かれるべきデータベース機能の偶発的な露出は、つまりのところ、 SQLインジェクション という脆弱性です。実際にデータベースにアクセスするために必要な認証スキームに関係なく、世界中の誰でもアドレス可能なオープン接続がデータベースにある必要はありません。そうしてしまうとかえって問題を招くことになります。

データベースをインターネットに露出するのは、本質的に無分別で、頭痛を引き起こすものです。良くないことです。残りの本セクションは、それがどれほど危険であるかを示す、分析だと思って読んでいただきたいと思います。

MYSQL (3306)

私のSQL、あなたのSQL、皆のSQL。

TLDR

説明：	断片的な歴史を持つ、人気の高いオープンソースのリレーショナルデータベース管理システムです。
数：	282万6,541件のノードを検出しました。 281万7,028件（99.66%）にRecogフィンガープリント（合計4件のベンダーグループ）がありました。
脆弱性：	1,000以上で、CVSSスコアはばらばらです。
アドバイス：	是非使用してください。しかし、パッチを適用し、インターネット上で外部公開しないでください。

代替手段：PostgreSQL、Microsoft SQL Server、Oracleプロパー、および他のRDBMS。

MySQLの断片的な歴史についてだけで、論文を書けるほどです。元々は、オープンソースの統一されたコードベースとして始まり、 Oracleに買収されてからは、 MariaDB[63]、Percona[64]、Google Cloud SQL[65]などのバリアントが出現しました。これらはすべて、MySQLの仲間ですが、バージョニングはそれぞれ異なります。ベンダーごとに分析する場合は、検出されたノードの98%を占める、正式なOracle MySQLのバリアントとMariaDBに注目します。

調査結果の詳細

ポーランドは、Home.plというホスティングプロバイダの存在で、ドイツをわずかに追い抜いて3位となりました（前述したように、Home.plのおかげで完璧とは呼べないデフォルト設定がFTP調査で検知されました）。露出されたMySQLのうち、米国が34%を占め、15%の中国と距離を空けています。

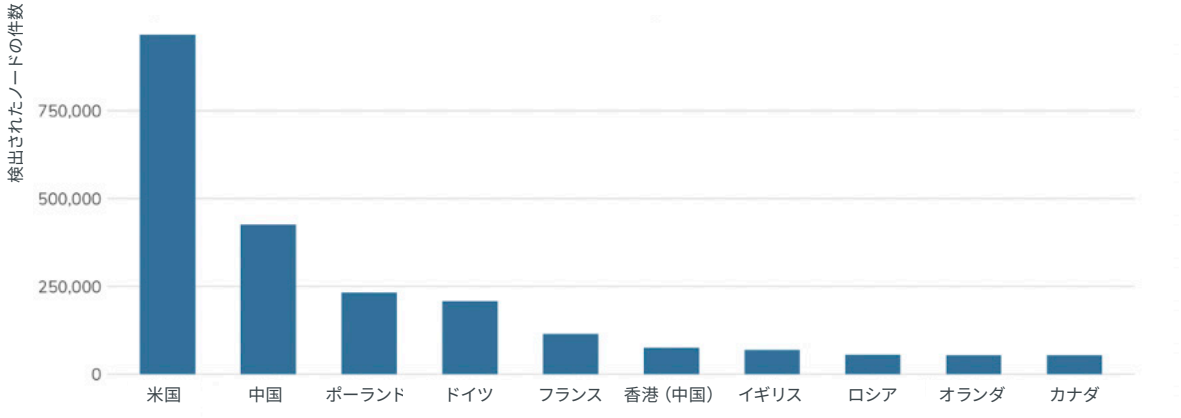
[62] <https://en.wikipedia.org/wiki/Sabre_(computer_system)>

[63] <https://mariadb.org/>

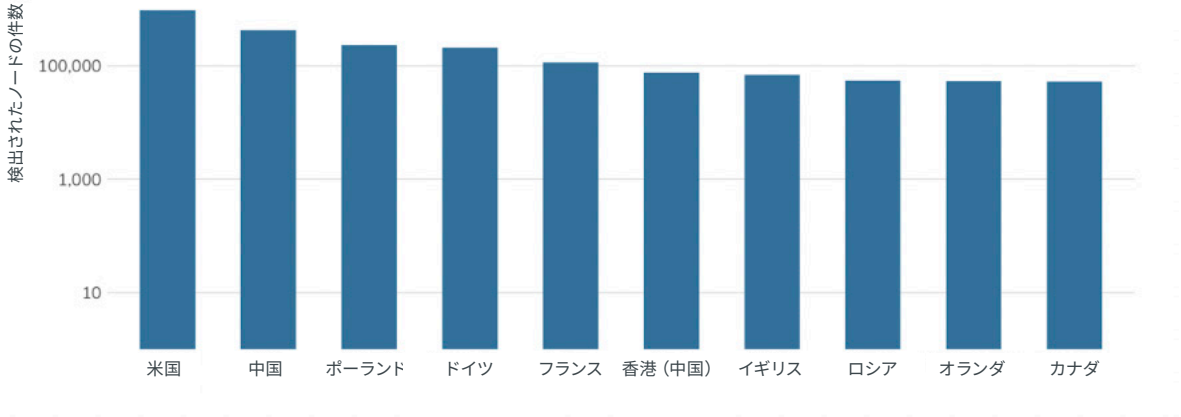
[64] <https://www.percona.com/>

[65] <https://cloud.google.com/sql>

データベースの上位10か国：MYSQL（TCP/3306）

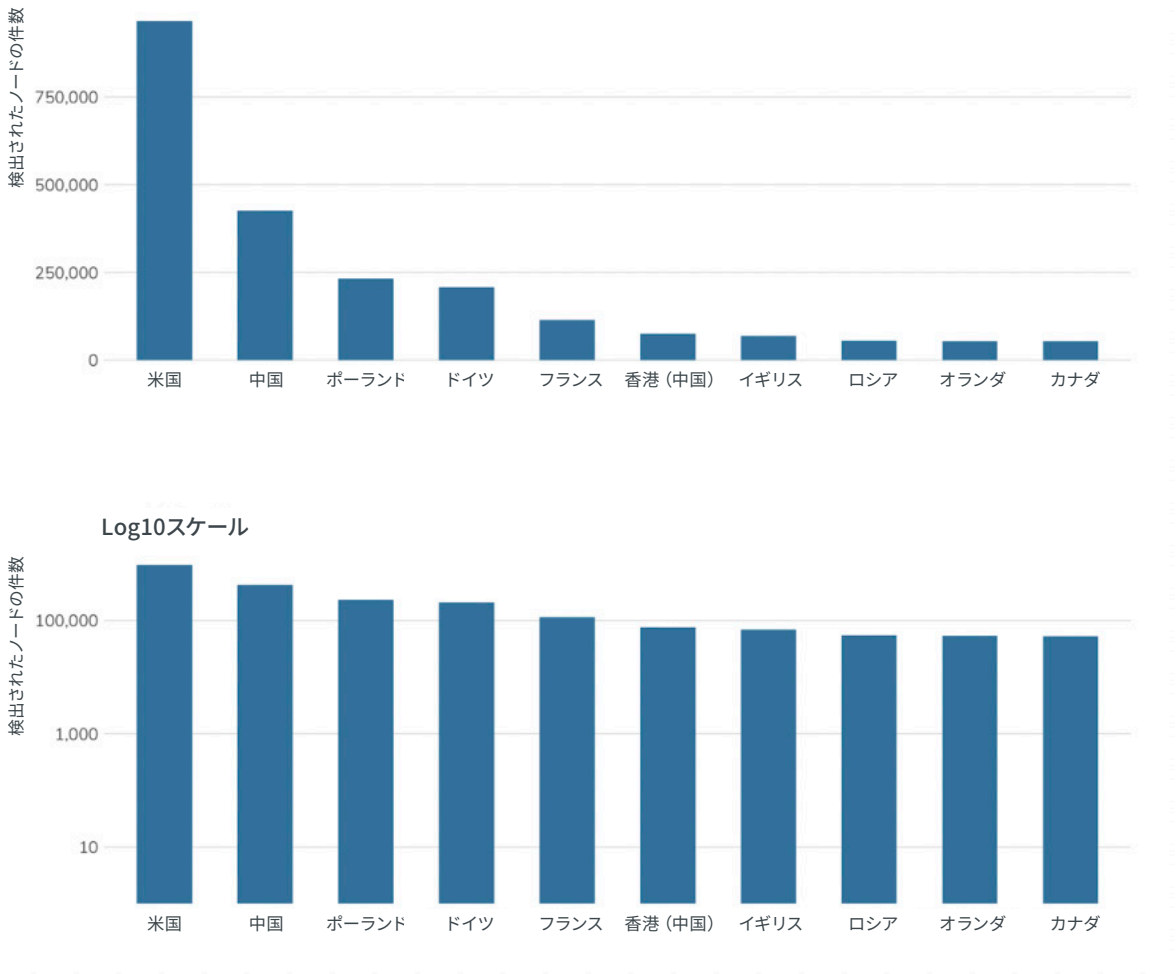


Log10スケール



Alibabaには、Oracle MySQLとMariaDBの両方の画像がありますが、AsparaDBが管理するサービスの中に、MySQLに似た独自のものを提供しています。[66]Amazonも同様の状況で、[67]またOVHもターゲット化されたMySQLを提供しています。[68]これらのプロバイダ3社には、提供する画像やサービスに安全なデフォルト設定があり、MySQLの安全性確保について十分な文書も揃っていることから、クラウドエクスポージャーでトップ3に並ぶのは不思議に思えます。これは、彼らがインターネット上にMySQLを表示させるよう、わざわざ努力をしているか、もしくは設定で大きなミスを犯したかのどちらかです。

クラウドプロバイダデータベース：MYSQL（TCP/3306）



本レポートは主に「ホスティング」プロバイダまたはコロケーション企業ではなく、クラウドプロバイダに注目していることから、本セクションには少し色を足す必要があります。露出されたインスタンスの件数では、コロケーション企業のUnified Layer[69]が（OVHを破り）14万5,967件、ホスティングプロバイダのGoDaddy[70]が（他のプロバイダを抜いて）10万1,775件となりました。

MySQLインスタンスを露出している自律システムは17,876件あり、そのうち3つのサーバーの中央値と156件のサーバーの平均値もあるため、エクスポージャーに関して非難するべきものは多くあります。

[66] AsperaDB <https://www.alibabacloud.com/product/apsaradb-for-rds-mysql>

[67] Amazon MySQLのサービス <https://aws.amazon.com/jp/rds/mysql/>

[68] OVH MySQL <https://www.ovh.co.uk/cloud-databases/>

[69] Unified Layer <https://unitedlayer.com/>

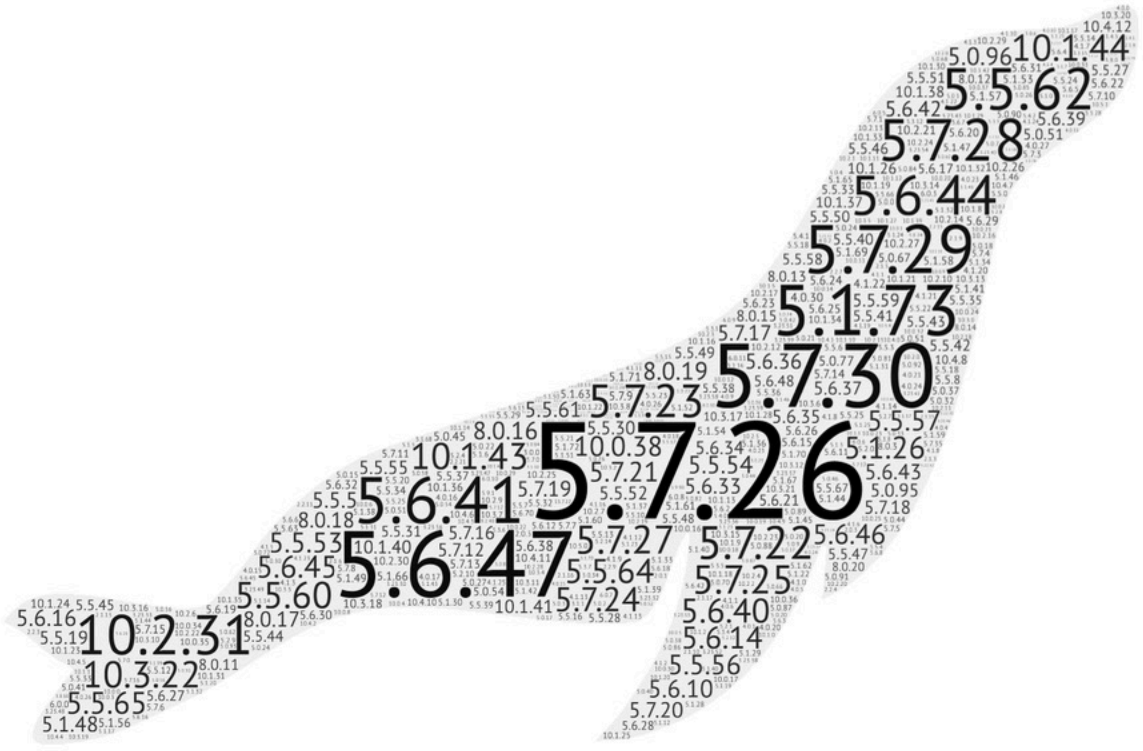
[70] GoDaddy <https://www.godaddy.com/>

エクスポージャー情報

本レポートでは、1,600通りのベンダーとバージョンの組み合わせがあります。これは、ベンダーを Oracle、MariaDB、Google、Percona、そして「その他」のグループにまとめた場合です。インターネット上には200万以上のインスタンスが発見されたことから、MySQLを自身でうまく管理できている人はいないといえるだけの十分なデータがあります。そうです、あなたのことです。どうぞ、ノートパソコンのコマンドプロンプトか、よく使うサーバーに「mysqld -version」と入力してください（どこかで実行しているのは分かっています）。著者の1人で、 シールドを持った変わった人間 もそれをしましたが、同じことをしましたが、彼ですら最新のMariaDBリリースから2パッチポイント遅れているのです。[71]

つまり、そこなのです。パッチ管理が難しいのです。しかし、「localhost」にしか露出されていないローカルのノートパソコンインスタンスにパッチを当てないことと、*インターネットに直接接続されている*MySQLインスタンスにパッチを当てないことでは、大きく異なります。

それでもまだ、バージョンの分布がどうかを見たいとお考えでしょう。これには（分布が広大なため）少し工夫して、ワードクラウドを作り、MariaDBのロゴに重ねました。あざらしのロゴマークがとても良いからです。



バージョン5.7.26は、2019年4月25日にリリースされました（他のバージョンの元となるOracleバージョン）。

バージョン5.7.26には、中程度の脆弱性が13件あり、一方、5.7.30は2020年4月27日にリリースされたので、本レポート作成時には比較的新しいものになります。Oracleは、8.0.x（基本的には5.8.xと同じ）、5.7.x、5.6.xを、それぞれ技術的に大きく違うことから、正式に枝分けしています。さらに分かりにくいことに、MariaDBは5.6.xから10.0.xに飛びました。10.xリリースで最も知られているのは10.2.31です。これは、2020年1月にリリースされ、（5月にリリースされた）10.2.32に取り替えられました。MariaDB自体は、バージョン10.0.xから10.4.xまでを続けています。

この文章を理解するのが困難だったというのであれば、データベースのパッチ管理がいかに難しいかが理解できたということです。なぜなら、パッチ管理は、似たようで異なる、小数点が並ぶねじれた迷路だからです。ですから、*MySQLをインターネットで外部公開するのはやめましょう。*

[71] 念のために言っておきますが、「brew update && brew upgrade」ではかなりのタイピングをします。

攻撃者の視点

HeisenbergにはMySQLのハニーポットがありません。また、MySQLの接続試行の性質が、意図的な攻撃や、（設定ミスではあるが）自分が所有していると勘違いした誰かが、合法的に通信しようとした際の、怪しい接続を見分けることを困難にします。つまり、ここにグラフを掲載したところで、質問がさらに増えるだけだということです。

あえて言うとすれば、Heisenbergは一般的に、TCP/3306で1日当たり1万～3万件の、中央値が約250の個別ソースIPv4からのTCP接続を見つけます。MySQLをスキャンしている他のリサーチャーによる、このような（毎日の）接続は、ほんの一握りです。私たちのハニーポットノードは主にクラウドIPスペースにあるため、設定ミスのクライアントが5～15%を占めます。

お伝えできることは、2019年に攻撃者らが、インターネットに面するMySQLサーバーを狙ったランサムウェア作戦[72]を開始したこと、そして、私たちが見つけたMySQLサーバーで、悪意のあるアクターが試行できる何十億という認証情報が出回っているということです。ですから、MySQLをパブリックサーバーで使うことは、考え直していただきたいと思います。

アドバイス

ITとITセキュリティチームは、パブリックIPアドレスでMySQLをホストせず、MySQLのベンダーとバージョンの組み合わせを1つ選び、それを会社全体の標準にすること（そしてパッチ処理を行うこと）を強くお勧めします。MySQLにはよく、「アプライアンス」が付属しています。調達チームと連携し、どのバージョンが使用中のソリューションにバンドルされているか、また新しいMySQLリリースが発表されたら、適宜アップデートを行う旨を、ベンダーがきちんと伝えるように確認してください。

クラウドプロバイダは、安全で管理の行き届いたMySQLと互換性のあるサービスを引き続き提供し、独自にMySQLインフラをホスティングしているユーザーに関連する脅威を緩和する手助けをしてください。MySQLディストリビューションのある、ベンダーが管理するディスクイメージは、新リリースの発表後すぐにアップデートし、ベンダーはレガシーバージョンのアップデートが必要である旨を、ユーザーに伝えてください。

政府のサイバーセキュリティ機関は、MySQLを安全にホストする方法を有意義な方法で指導し、新たな攻撃作戦を発見した場合は、適宜通知を行ってください。 さらに、クラウドプロバイダ、ホスティングプロバイダ、およびISPと連携して、MySQLがパブリックインターネットに接続するのを防ぐよう取り組んでください。

MICROSOFT SQL SERVER（MS SQL）（UDP/1434）

SELECT TOP 1 * FROM quippy_subtitles

TLDR

説明：	Microsoftが開発したリレーショナルデータベース管理システム。データベースのプロパーはTCP（通常は1433番ポート）で動作しますが、この調査では（MS SQLが実際どこにあるかを指し示す）MS SQL Discoveryサービスを使用しました。
数：	9万8,771件のノードを検出しました。 9万8,771（100%）が、バージョンとその他の設定情報を、認証されていないリクエストで返しました。
脆弱性：	1999年以降86件で CVSSスコアは8.5以上、リモートコード実行の欠陥があったものが45件ありました。
アドバイス：	是非使用してください。しかし、決してインターネット上で外部公開しないでください。
代替手段：	PostgreSQL、MySQL、Oracle、およびその他のリレーショナルデータベース管理システム。
傾向：	現状のまま。2019年から特に変化はありませんでした。

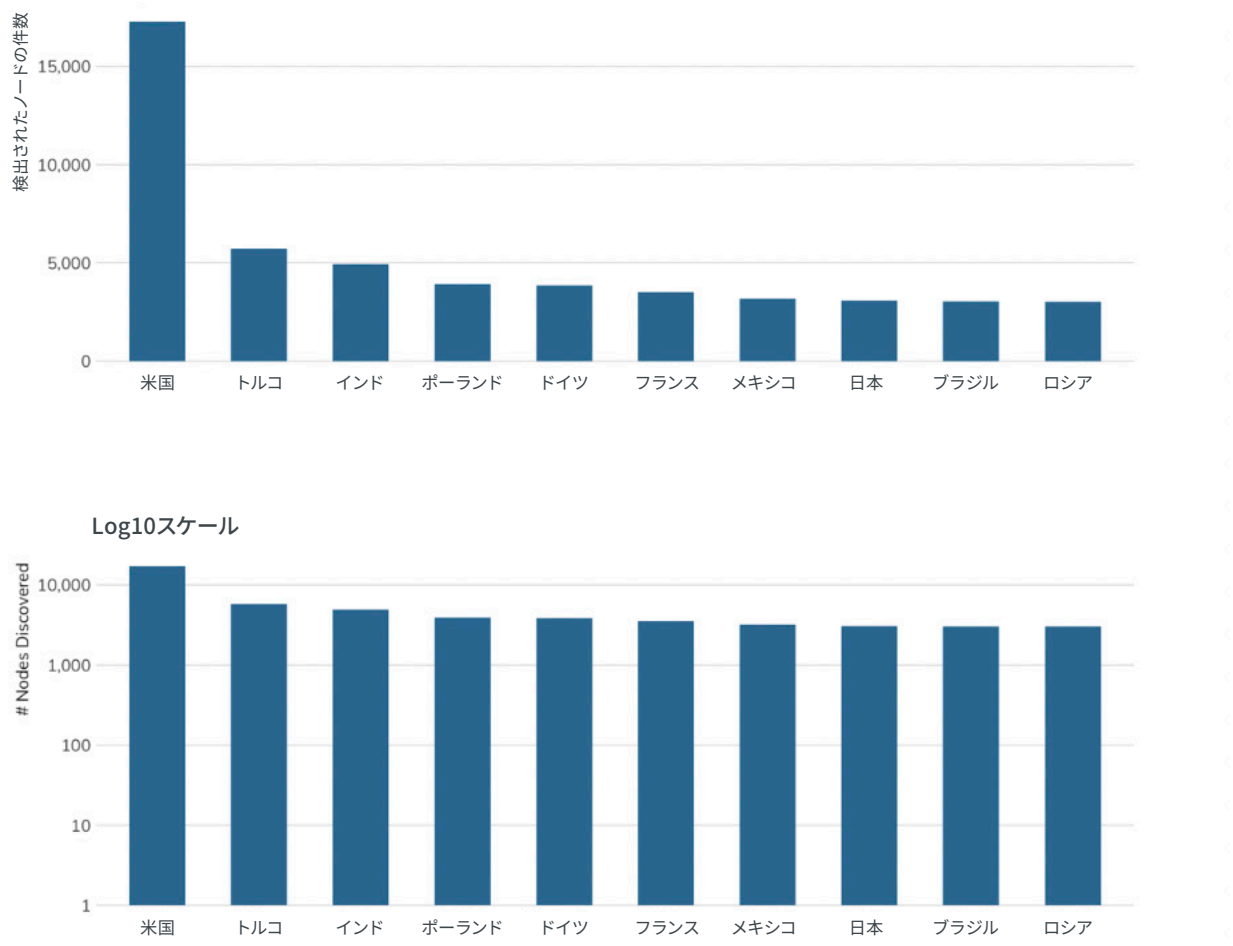
[72] <https://news.sophos.com/en-us/2019/05/24/gandcrab-spreading-via-directed-attacks-against-mysql-servers/>

OS/2オペレーティングシステム用16ビットサーバーであるMicrosoft SQL Server 1.0は、 1989年に最初にリリースされました（まだ生まれていなかったという方も多いでしょう）。Microsoft Windowsオペレーティングシステム（NT）の最初のバージョンは、1993年にリリースされたSQL Server 4.2でした。現在、Microsoftは、Azureクラウドデータベースサービスに加え、2012、2014、2016、2016、2017、2019という5つの主要なバージョンに対応しています。大企業では、必ずと言ってよいほど、MS SQLがどこかで作動し、何らかのビジネスやタスクを支えています。

調査結果の詳細

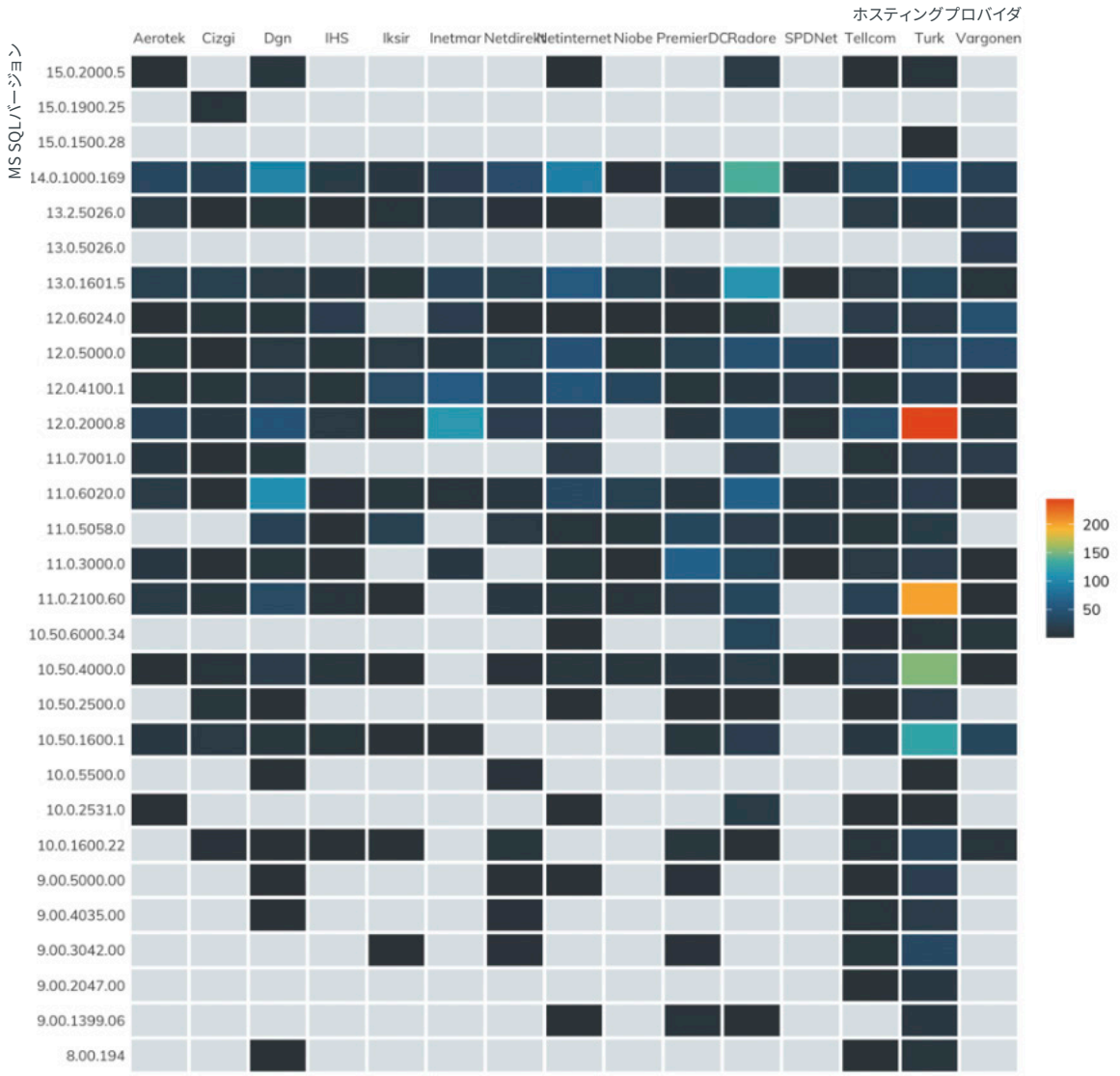
決してどのようなデータベースも（意図的なAPIサービス経由でない限り）インターネットに露出してはいけないにもかかわらず、Project Sonarでは、9万9,000件近くが（一切の認証なしで）サービスに関する詳細を公開できる状態でした。これは、MySQLセクションで見たものと比べて、 ごく小さな数字 （2桁の差）です。この違いは、MS SQL Severが有料なのに対し、MySQLが*無料*であることが理由だと考えられます。

データベースの上位10か国：MS SQL（TCP/1434）



トルコがトップ10入りすること、さらに大国を凌いで2位のスポットを取るというのは珍しいことです。そこで少し結果を掘り下げてみると、トルコのホスティングプロバイダのユーザーは、Microsoft SQL Serverをインターネットに露出するのが*大好き*であるということが分かりました。トルコのエクスポージャーの75%をプロバイダが占めており、（以下の通り）非常に多様なSQL Serverのバージョンが見られました。同様に、インドでも国内のエクスポージャーの75%をホスティング業者が占めています（SQL Serverの合計バージョン数は35件）。ポーランドも、ドイツとほぼ同じ数のSQL Serverを露出していることから、注目に値します。 大手ISP兼ホスティングプロバイダである Orange Polskaは、ポーランドにおけるSQL Serverエクスポージャーの50%を占めています。また、Orangeのネットワークからのエクスポージャーの35%を、販売、会計、人材管理を手掛ける大手のSaaS企業が占めています。

トルコのホスティングプロバイダで露出されているMS SQL SERVERバージョンの範囲



イスタンブールのどこかの大学で、人気の高いデータベース管理コースがあり、そのトレーニング施設でMicrosoft SQL Serverの露出を推奨しているのでしょうか。ご存じの方がいましたら、それを止めるように説得するので、是非教えてください。

調査対象のクラウドプロバイダにおけるMicrosoft SQL Serverのエクスポージャーに関しては、Microsoftが1位になると考えるのが普通です。しかし、少し遡ってMicrosoft AzureがAzure Database Service[73]を提供していることを思い出せば、なぜそれほど多くのSQL Serverインスタンスをインターネットに露出していないのかが理解できます。外部からAzure Database Serviceに話しかけるのは、非常に困難だからです。

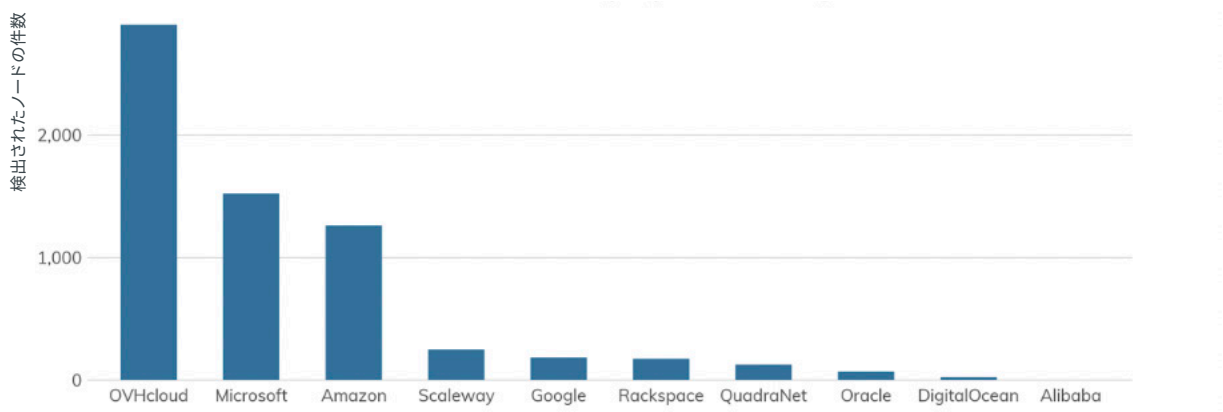
OVHはAmazon同様、SQLServerにコスト効率の高い、既製のイメージを提供することに力を入れています。[74][75]しかし、MS SQLを独自にホストするという点ではOVHのコストが低く、これが1位の座を獲得した理由だと思われます。

[73] https://azure.microsoft.com/ja-jp/services/sql-database/

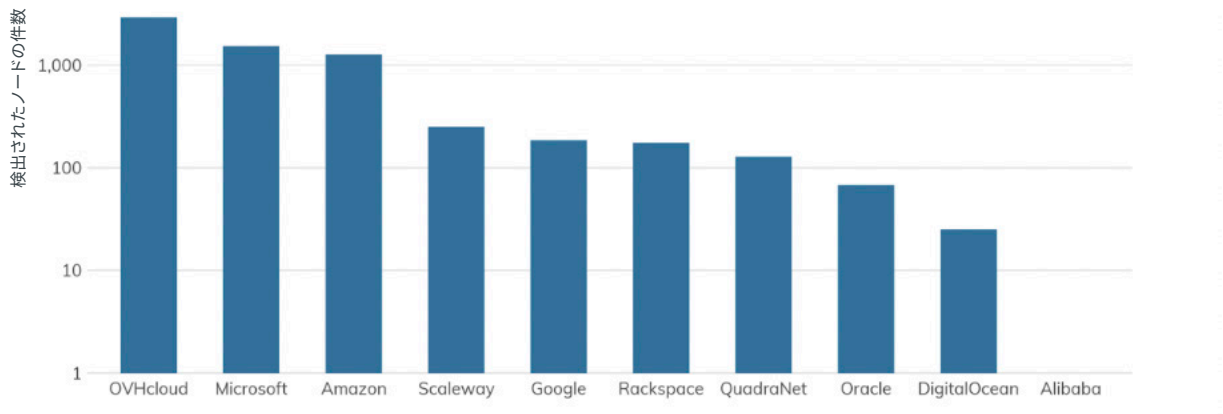
[74] https://www.ovh.com/world/dolvated-server/distributions/sql_server.xml

[75] https://aws.amazon.com/sql/

クラウドプロバイダデータベース：MS SQL（UDP/1434）



Log10スケール



エクスポージャー情報

これらのシステム全体で、Microsoft SQL Serverのユニークなバージョンが54件見つかり、そのうちの20件がエクスポージャーの95%を占めています。赤色のセルは、SQL Serverのメインバージョンに対応していないことを示しています。緑色のCVEセルは、脆弱性がパッチ処理された時期を示します。「Vintage」とは、リストされているバージョンのリリース日を意味します。

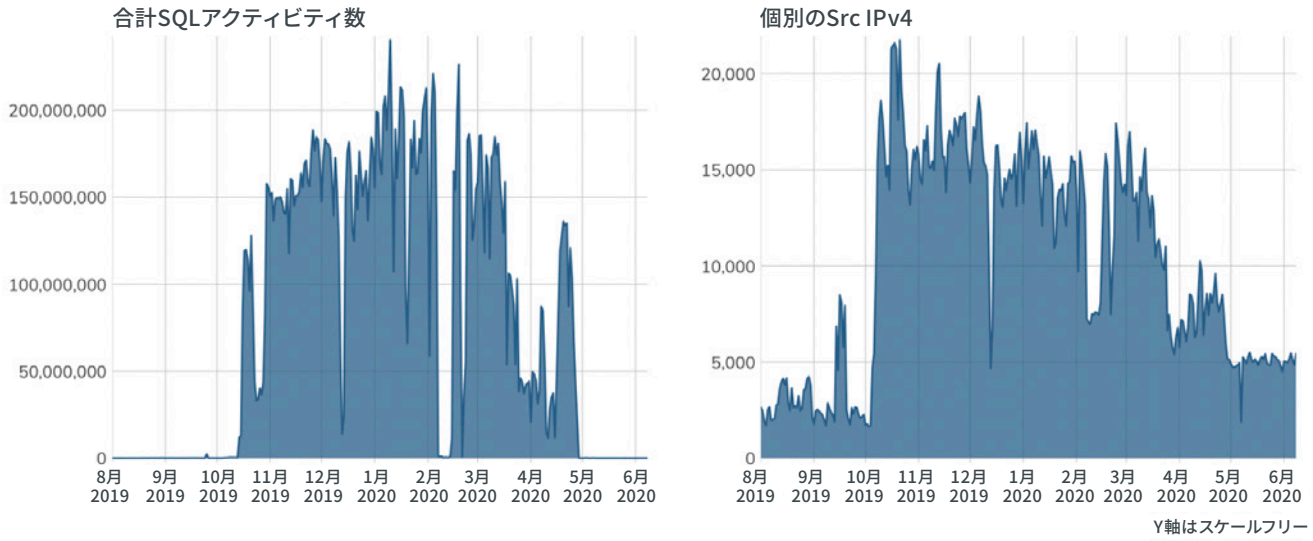
バージョン	数	割合	SQL SERVER	VINTAGE
12.0.2000.8	12,149	12.30%	SQL Server 2014 RTM	2014年4月1日
14.0.1000.169	10,398	10.53%	Microsoft SQL Server 2017 RTM	2017年10月2日
11.0.2100.60	9,378	9.49%	SQL Server 2012 RTM RTM	2012年3月6日
10.50.1600.1	7,880	7.98%	SQL Server 2008 R2 RTM RTM	2010年4月21日
10.50.4000.0	7,420	7.51%	SQL Server 2008 R2 Service Pack 2 (SP2)	2012年7月26日
12.0.5000.0	6,218	6.30%	SQL Server 2014 Service Pack 2 (SP2)	2016年7月11日
13.0.1601.5	6,132	6.21%	Microsoft SQL Server 2016 RTM	2016年6月1日
12.0.4100.1	4,454	4.51%	SQL Server 2014 Service Pack 1 (SP1)	2015年5月14日
11.0.6020.0	3,445	3.49%	SQL Server 2012 Service Pack 3 (SP3)	2015年11月23日
10.50.2500.0	3,153	3.19%	SQL Server 2008 R2 Service Pack 1 (SP1)	2011年7月11日
8.0.194	3,011	3.05%	SQL Server 2000 RTM (SPなし) RTM	2000年11月30日
9.0.5000	2,998	3.04%	SQL Server 2005 Service Pack 4 (SP4)	2010-12-17
12.0.6024.0	2,901	2.94%	SQL Server 2014 Service Pack 3 (SP3) 最新SP	2018年10月30日
11.0.3000.0	2,629	2.66%	SQL Server 2012 Service Pack 1 (SP1)	2012年11月6日
11.0.7001.0	2,551	2.58%	SQL Server 2012 Service Pack 4 (SP4) 最新SP	2017年10月5日
11.0.5058.0	2,356	2.39%	SQL Server 2012 Service Pack 2 (SP2)	2014年6月10日
13.0.5026.0	2,209	2.24%	Microsoft SQL Server 2016 Service Pack 2 (SP2)	2018年4月24日
10.0.1600.22	1,721	1.74%	SQL Server 2008 RTM	2008年8月7日
9.0.4035	1,643	1.66%	955706 SQL Server 2005 Service Pack 3 (SP3)	2008年12月15日
9.0.1399	1,168	1.18%	SQL Server 2005 RTM	2005年11月7日

注目すべき点は、サポートされているバージョンはどれも、最新のパッチリリースではないということです。MS SQLを無謀にもインターネットに露出している人は、そもそもサイバー衛生を心がけていないと予想されます。そのため、このような人々が最新のパッチを維持しているというのは、少し楽観的な考えです。

攻撃者の視点

攻撃者は、よくSQL Serverを狙いますが、2019年10月以降は、執拗なクレデンシャルスタンシングとSQL実行作戦を大々的に展開しています（本当は2018年ですが、本格的な開始が2019年でした）。[76]

MSSQLサーバーのHEISENBERG アクティビティ



Project Heisenbergの高対話型MS SQLハニーポットは、MS SQL Serverの不正ともいえる配信に、バックドア7[77]が仕掛けられている可能性があるという報道が出始めてから間もなく、このような活動に文字通り圧倒されました。1日6,300万件以上の認証アクセス試行と、それに続くさまざまなSQLコマンドシーケンスが見つかりました（ハニーポットが攻撃者のログインを許した場合）。これが2月に減少したことと、何かしらの公開アクションに相関関係があるのかについて、Rapid7 Labsはまだ解明していません。しかし、この作戦はまだ終わりません（Guardicoreの報道以降、多くの攻撃者がやり方を変えていますが）。

これを聞けば、MS SQL Serversを直接インターネットにつなげるには、いつも以上の注意が必要だと納得できるでしょう。

アドバイス

ITとITセキュリティチームは、決してMS SQL Serverのインスタンスを直接インターネット上には置かないでください。また、パッチ管理に関しては、32,000件のパッチ処理を行わなかった人々より、さらにしっかりと仕事をしてください。内部SQL Serverインスタンスへのアクセス管理者は、認証の不正を追跡し、認証情報ダンプにあるユーザー名と一致するアカウントは、すべて強制的にパスワードをリセットしてください。あえていう必要はないかもしれませんが、攻撃者の作戦や、インターネット上のSQL Serverの残念な状況を考慮すれば、デフォルトのアカウントを有効化したり、デフォルトの認証情報を使用することは、やめましょう。

クラウドプロバイダは、安全でプライベートなMicrosoft SQL Serverの管理サービス引き続き提供し、プロバイダが管理する画像が、常に最新のパッチレベルにあることを徹底してください。古くなった、そして特にサポートされていないイメージを使っているユーザーには、この問題を放置した場合の危険性について、定期的にコミュニケーションを取ってください。

政府のサイバーセキュリティ機関は、MS SQL Serverに対する作戦を追跡し、個人、組織、および管轄内の人々が攻撃の可能性を検知できるよう、適宜通知してください。MS SQL Serverのパッチ適用と、パブリックインターネットで使用してはいけないことについては、特に重点的に認知向上および啓蒙に取り組んでください。

[76] Vollgarキャンペーン <https://www.guardicore.com/2020/04/vollgar-ms-sql-servers-under-attack/>

[77] <https://www.scmagazine.com/home/security-news/gaming/skip-2-0-backdoor-malware-provides-magic-password-to-access-mssql-accounts/>

REDIS (6379)

非リレーショナルデータベースでも、インターネット上にあってはいけません。

TLDR

説明：	2009年に作成された、スケーラビリティとパフォーマンスに特化したインメモリベースのキーバリューデータベースです。
数：	10万2,801のノードを検出しました。
脆弱性：	2013年以降のCVEは12件ですが、CVEだけではRedisのエクスポージャーの全容は分かりません。
アドバイス：	是非使用してください。ただ、パブリックインターネットには露出させないでください（元々そのように作られていないからです）。
代替手段：	etcd[78]とmemcached[79]は、Redisと似た特性を持つ、インメモリベースのキーバリューストアです。

Redisは、必要なデータを常にメモリ内やディスク上に置くという考えを根本的に変え少なくとも一般化しました。オンディスク版の目的はただ1つ、高可用性設定における同期に使用するインメモリ版を再構築することだけです。「NoSQL」[80]データベースのカテゴリーで非常に人気が高く、Twitter、GitHubやその他、スケールの大きい多くの環境でのプロダクションに使用されています。

[78] <https://etcd.io/>

[79] <https://memcached.org/>

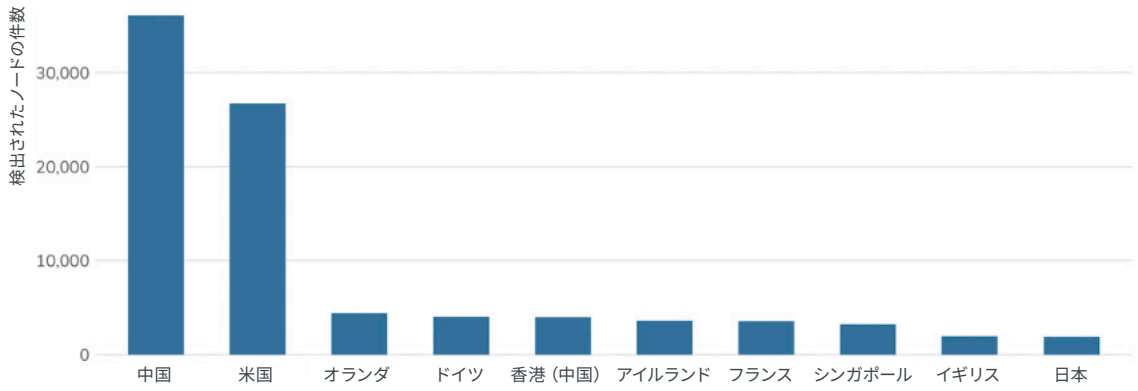
[80] <https://ja.wikipedia.org/wiki/NoSQL>

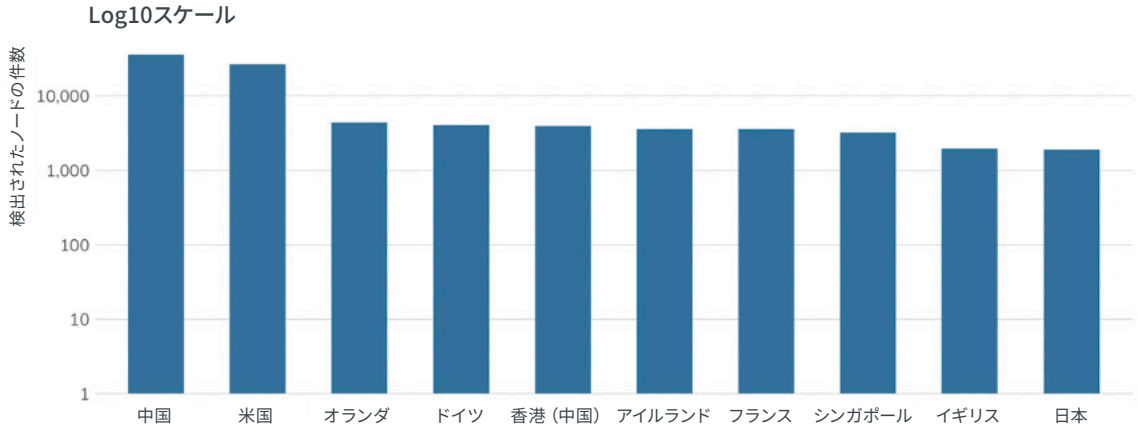
調査結果の詳細

Project Sonarは、パブリックインターネットで10万2,801件のRedisインスタンスを発見しました。Redisが他のデータベース同様、インターネットに露出されるべきではないことを考えると、驚くべき数字です。

第1位は中国で、この背景にはRedisプロトコルを完全にエミュレートするTencentDB[81]の存在があります。中国でRedisと互換性のあるノードのうち、1万5,000件以上が、Tencentの自律システムに由来しています。

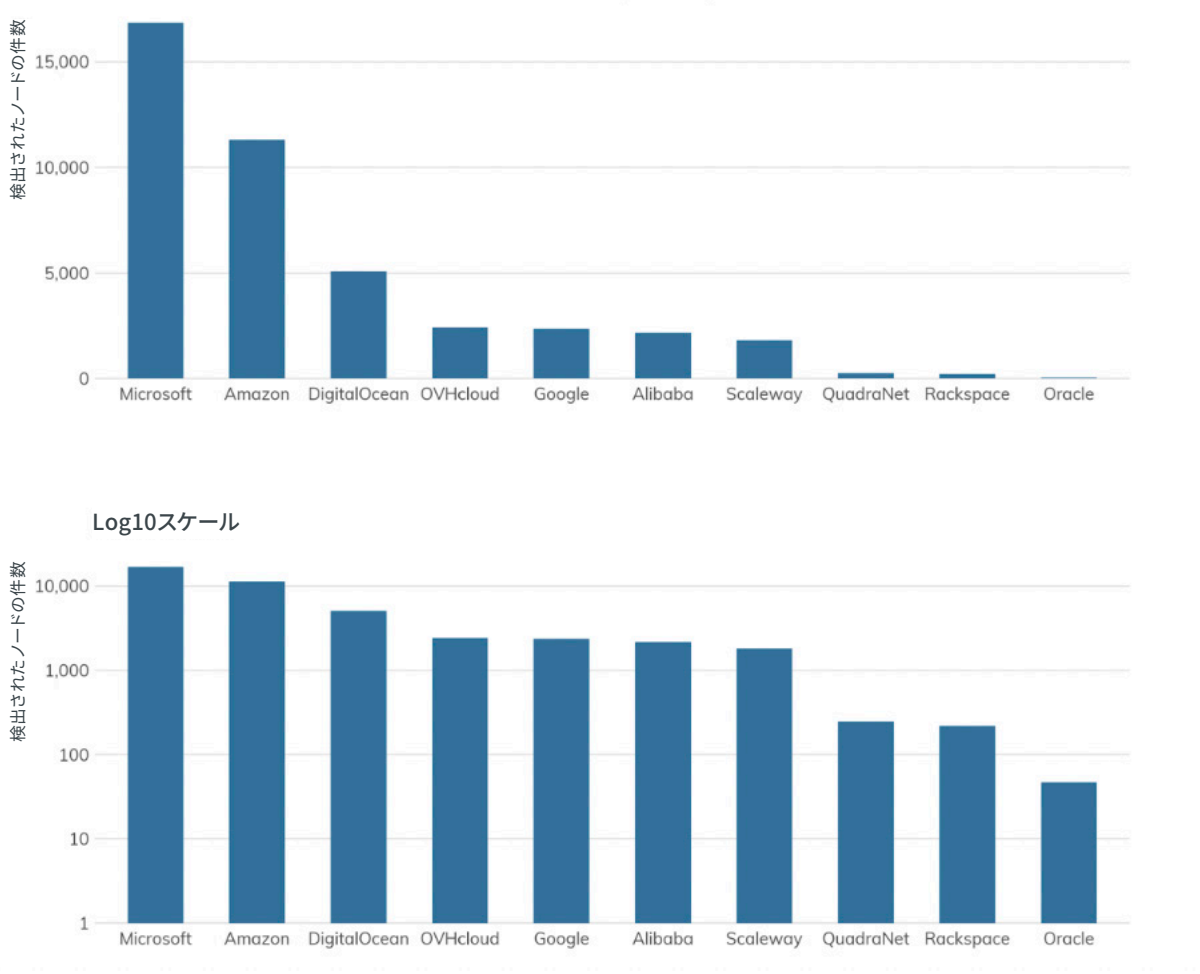
データベースの上位10か国：REDIS（6379）





[81] <https://intl.cloud.tencent.com/product/crs>

クラウドプロバイダデータベース：REDIS（6379）



クラウド環境でRedisを見つけることには、それほど驚きません。今日では多くのパブリックWebアプリケーションがクラウドにあるからです。Microsoftは、Azure CacheサービスでRedisに大きく依存するため、1位となっています。[82]またAmazonは、RedisとRedis互換性のあるElasticCacheサービスに対する、直接的なAWSサポート[83]により、2位にランクインしました。[84]

しかし、クラウドの数が少ないように感じるという場合は、「エクスポージャー情報」のセクションを読んでください。

[82] Azure Cache for Redis <https://azure.microsoft.com/ja/services/cache/>

[83] AWS：Redis <https://aws.amazon.com/jp/redis/>

[84] ElasticCache <https://aws.amazon.com/jp/elasticache/>

エクスポージャー情報

TLDRで述べたように、RedisのCVEはあまり多くありません（1つだけ[85]非常に重大なものがありました）が、Redisの最大の弱点は、 デフォルトで 全てのネットワークインターフェースにバインドするということです。[86]つまり、Redisインスタンスかクラスタをあえて安全にしなければ、同じネットワークセグメントにアクセスできる人ならだれでも対話できてしまうということです（これについては後に説明します）。Redisの開発者であるantirezは、SSHの仕組みに関する少しの知識があれば、わずか5秒ほどで安全でないRedisインスタンスへのリモートアクセスを得られることを証明しました。[87]

Redisは、ポートを変更したり、認証を必要にするよう設定したり、TLSトンネルをラッパーにしたりしてサービスをセキュアにできますが、インターネットに接続する理由は何もありません。インターネット（デフォルトのポート）にある10万件以上の状態を見てみましょう。

REDISサーバーの状態	数	割合
認証が必要	77,050	74.95%
リターンドバージョン	13,590	13.22%
実行が保護されている	9,255	9.00%
エラーが発生	2,765	2.69%
IPホワイトリスト	130	0.13%
ビジー状態が報告された	11	0.01%

リモートRedisインスタンスへの侵入がいかに容易かを考えると、約75%のサーバーで認証が必要というのは心強いです。許可なしに認証情報をテストすることは禁止されているため、それらの認証情報がどれほど強力かは分かりません。また、9%のシステムが「保護」モードで実行されているというのも前向きな結果です。バージョン3.2.0以降、Redisはデフォルト設定で実行され（全てのインターフェースがバインドされている）、アクセスにパスワードが必要ない場合、特別な「保護モード」に入り、ループバックインターフェースからのクエリにのみ返信し、その他のインターフェースからのクエリにはエラーメッセージを返します。

Redisインスタンスの約13%から（INFOリクエストを通して）バージョンなどの情報を抽出し、112の異なるバージョンストリングをカウントすることができました。そのうち30件が、見つかったバージョンの90%をカバーしています。

REDISバージョン	数	割合
3.0.504	2,303	21.25%
3.2.12	1,314	12.12%
5.0.8	878	8.10%
5.0.7	843	7.78%
3.0.6	793	7.32%
3.2.100	728	6.72%
4.0.9	657	6.06%
3.0.503	364	3.36%
5.0.5	327	3.02%
3.0.501	235	2.17%
2.6.12	212	1.96%
2.8.17	191	1.76%
5.0.3	188	1.74%
5.0.6	175	1.62%
3.2.6	169	1.56%
4.0.14	160	1.48%
3.0.7	158	1.46%
3.2.8	122	1.13%
3.0.500	109	1.01%
2.8.4	106	0.98%
5.0.4	98	0.90%
2.8.19	93	0.86%
3.2.11	91	0.84%
2.8.23	85	0.78%
4.0.11	83	0.77%
3.2.9	81	0.75%
3.2.10	78	0.72%
3.0.5	72	0.66%
3.0.1	70	0.65%
4.0.10	55	0.51%

[85] CVE-2015-4335 <http://attackerkb.com/cve-2015-4335>

[86] Redisクイックスタート <https://redis.io/topics/quickstart#:~:text=By%20default%20Redis%20binds%20to,is%20a%20big%20security%20concern.>

[87] Redisセキュリティに関するいくつかのポイント <http://antirez.com/news/96>

バージョン3.0.504がこれほど多い理由の1つは、安全性が不十分なTencentDBインスタンス（他にもありますが、報告されているバージョンの1つと思われるもの）です。それは、Azure Managed Cacheが終了する前にリリースされた最後のバージョンでもあります。[88]

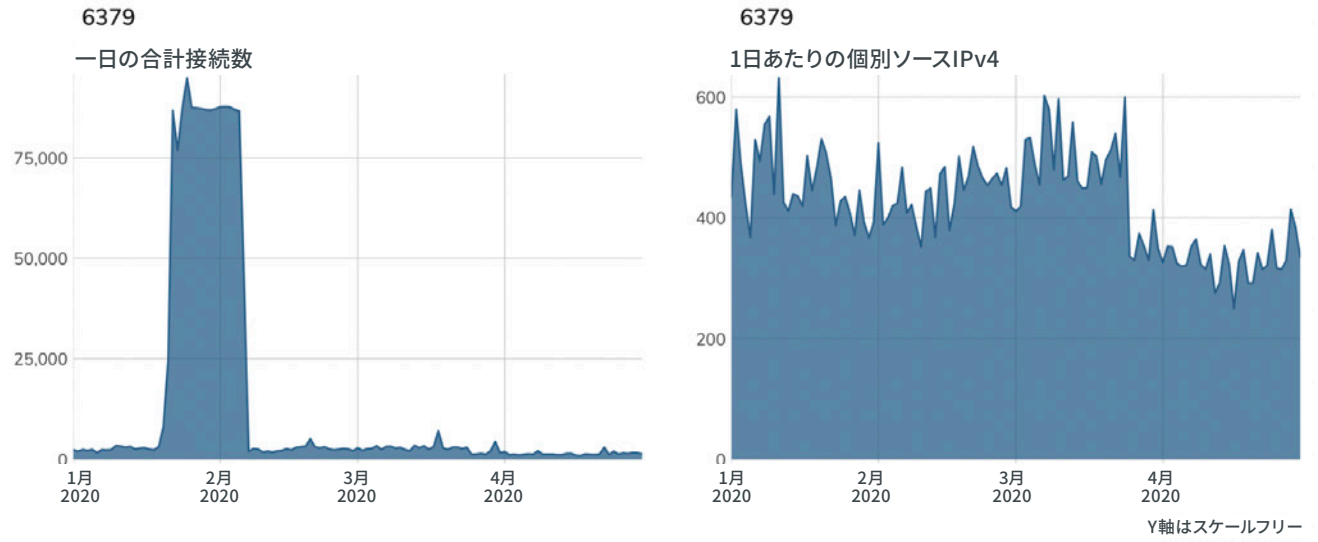
最後にここで注目すべき点は、2020年4月の調査時点で最新だったバージョンは5.0.8でしたが、これは実にRedisで3番目によく使われているものだということです。しかし、調査が発表された時点で、Redisは既にバージョン6.0.5をリリースしていました。Redisのバージョン番号は、速いペースで増えていきます。

攻撃者の視点

安全でないRedisインスタンスに侵入するのが、いかに容易かを考えると、新しいホストを獲得して悪意のあるアクションを実行したり、身代金を要求したり、仮想通貨のマイナーをインストールしたりと、攻撃者があらゆる手段で襲ってくるのは当然のことです。[89]

Project HeisenbergはRedisをエミュレートしませんが、初期の不完全なプロキシとして6379番ポートへのTCP接続を試すことで、攻撃者が本当に、インターネット上で露出されたRedisノードを探しているのかを確認できます。

REDIS（TCP/6379）HEISENBERG アクティビティ



異常なスパイクが見られたこと、またRedisが「1つのパケットに好きなだけ多くのコマンドを詰め込める」タイプのプロトコルであるということから、私たちは調査期間中のパケットキャプチャについて調べたくなりました。

その結果、確かに期間中、特にRackspaceハニーポットノードで、多くのRedisリクエストを受け取ったことが分かりました。また、Redisクラスタのレプリケーション設定で、誤ってHeisenberg のIP（当時の）を組み込み、5GB近くのWebサーバーカウントデータを送り、1時間あたり平均1,700件のRedis PUBSIHリクエストを作成した人がいたようです。

ここで、Redisインスタンスをセキュアにするだけでなく、クラスタ設定も厳密に管理することを改めてお願いします。うっかり自身のデータ5GB を、何も知らないセキュリティリサーチャーに漏らしてしまわないように。

[88] Microsoft Redis リリースアーカイブ <https://github.com/microsoftarchive/redis/releases>

[89] 露出されたRedisインスタンスのリモートコード実行、仮想通貨マイニングへの悪用 <https://blog.trendmicro.com/trendlabs-security-intelligence/exposed-redis-instances-abused-for-remote-code-execution-cryptocurrency-mining/>

アドバイス

ITとITセキュリティチームは、プロダクションでRedisを実行するための、プレイブックとオートメーションを確立してください。また、アプリケーション開発の段階で、デベロッパーがRedisを適切に設定し、セキュアでないインスタンスを露出して攻撃者に悪用されることのないよう、徹底してください。インターネットに直接接続するRedisインスタンスがあってはいけません。

クラウドプロバイダは、管理するRedisサービスが、独自のデフォルトでセキュアになっており、そうでなければ実行できないようにしてください。結局のところ、Redisはセキュリティよりもオープン性とユーザビリティを優先するように設計されています。Redisがプリインストールされているマシンイメージが提供されている場合、それらのイメージをRedisが各リリースに合わせてアップロードし、またイメージのユーザーに、展開しているノードをアップグレードする必要があるということを通知してください。

政府のサイバーセキュリティ機関は、Redisを安全に実行し、Redisシステムに入り込もうとする悪意のあるアクターを監視するためのガイダンスを提供してください。

MEMCACHED (UDP/11211)

使いやすいDDoSの方法であり、NoSQLデータベースです。[90]

TLDR

説明：	通常、地理的に分散するウェブサイトアセットのキャッシングに使用される、インメモリベースのキーバリューストアです。
数：	6万8,3376のノードを検出しました。 8,337件 (100%) にバージョンフィンガープリントがありました。
脆弱性：	2011年以降、13件のCVEがありますが、DDoS攻撃を増幅させるという厄介な問題があります。これは「エクスポージャー情報」セクションで詳しく説明しています。
アドバイス：	是非使用してください。ただし、インターネットに露出させないでください。
代替手段：	Redisとetcdは、memcachedと似た特性を持つ、インメモリベースのキーバリューストアです。

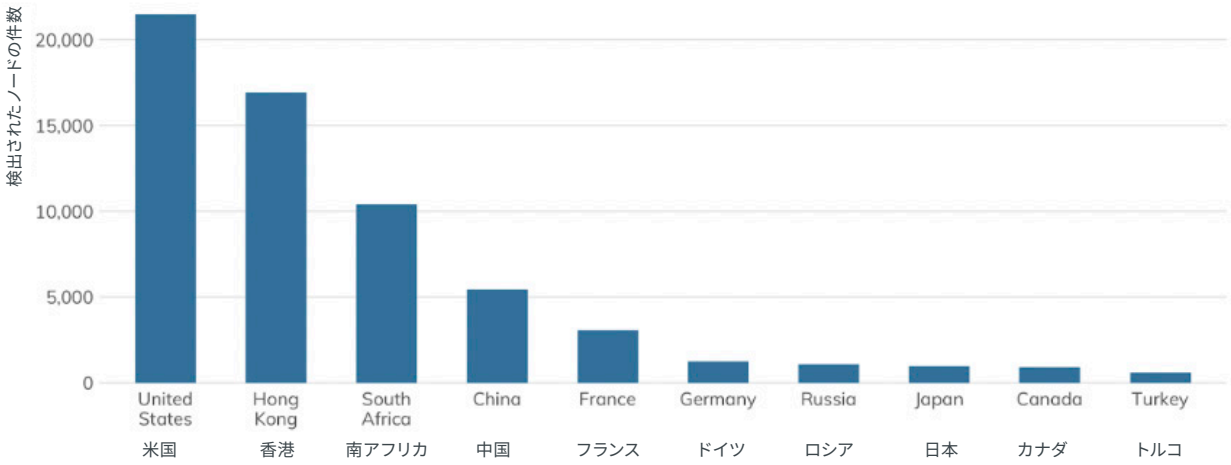
Memcachedは、データベースコール、APIコールまたはWebページのレンダリングによって呼び出される、任意データの細かいチャンク (ストリングとバイナリオブジェクト) 用のインメモリキーバリューストアです。シンプルなデザインによる展開の速さと開発の容易さで、人気があります。

調査結果の詳細

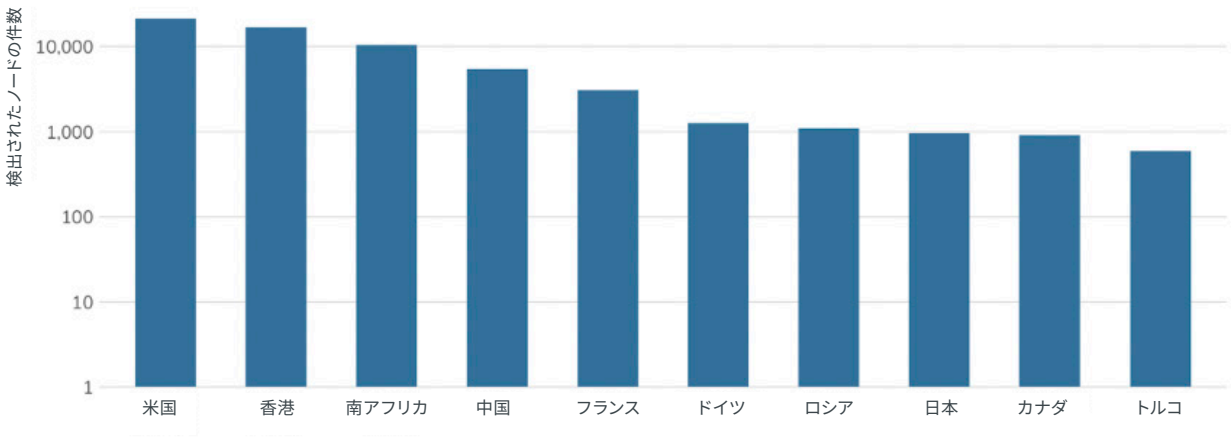
Project Sonarでは、露出されたmemcachedホストが6万8,337件見つかりました。他のエクスポージャーリストのトップ10には姿のなかった南アフリカが3位にあることに驚きました。SAノードのほとんど (97%) は、Icidc Network (87%) とInternet Keeper Global (10%) の2つの自律システム内にあります。また各自リスシステム内のホストの多くは、nginxとSSH両方のエクスポージャーカウントが似ています。

[90] ミルクに入れてもサクサクのままです。

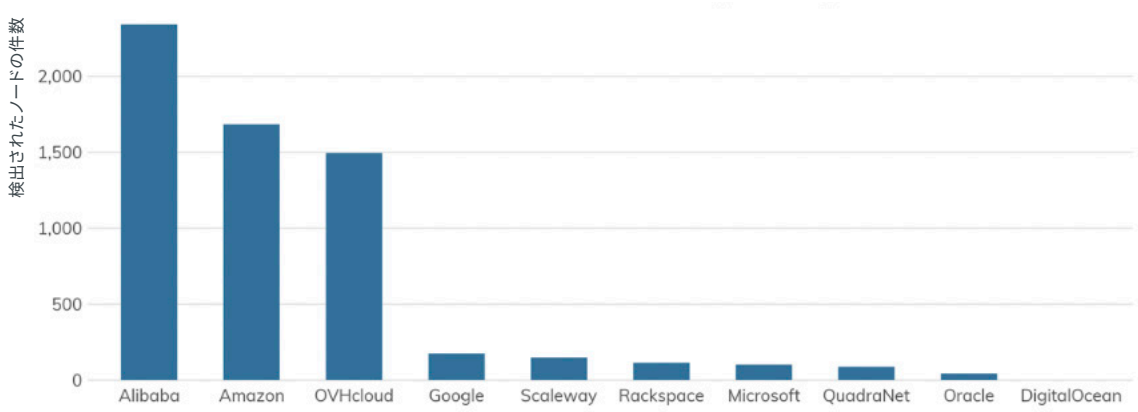
データベースの上位10か国：MEMCACHED（11,211）

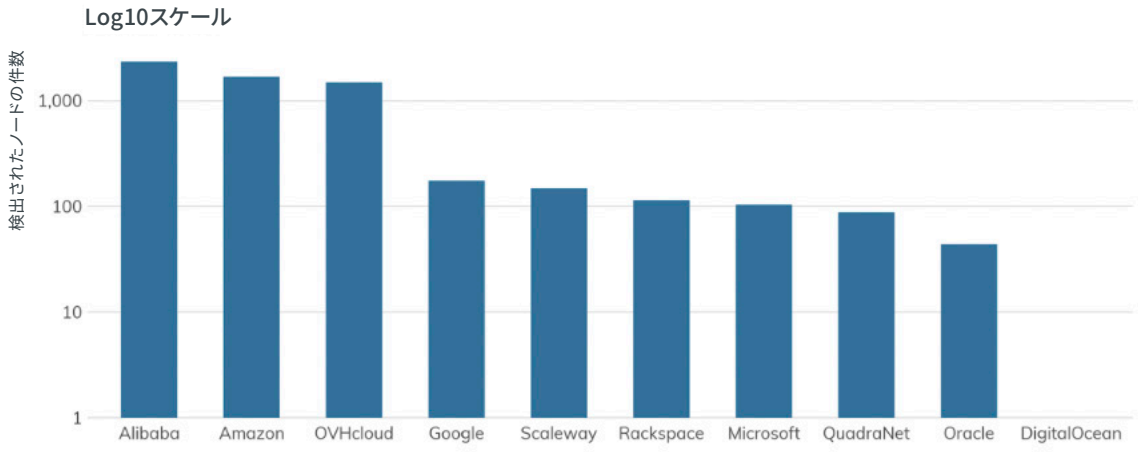


Log10スケール



クラウドプロバイダデータベース：MEMCACHED（11,211）





Redisのセクションで述べたように、Amazonにはクラウドの「cache」サービスがあり、memcachedを直接使用したり、精巧で小さなmemcahedプロトコルをエミュレートしたりするように設定できます。また、Alibabaにはマネージドmemcachedサービスがあります。[91]そのため、これらの環境で見つかるというのは当然ですが、インスタンスがインターネットに露出されているというのは少し心配です。さらに驚いたのは、OVHがわざわざmemcachedを安全にする手助けをしているにもかかわらず[92]、1,500人近いユーザーが、そのような重要なことに気付いていないということです。

エクスポージャー情報

なぜmemcachedがそれほど騒がれているのでしょうか。2018年、[93]memcachedのUDP部分にある「ネットワークメッセージ量のコントロールが不十分」という脆弱性[94]が、史上最大の分散型DoS増幅攻撃に使われ、多くの主要なインターネットサービスに障害を引き起こしました。当時、Cloudflareがブログ[95]でその欠陥をまとめています.

「チェックが完全になされていない状態で、データが超高速でクライアントに配信されます。さらに、リクエストが小さくても、応答が大きくなることもあります（最大1MB）。」

[91] AsparaDB for memcache <https://www.alibabacloud.com/product/apsaradb-for-memcache>

[92] memcachedサービスを使用したサーバーの安全確保 <https://docs.ovh.com/gb/en/dedicated/securing-server-with-memcached-service/>

[93] memcrashedの裏側 <https://blog.rapid7.com/2018/02/27/the-flip-side-of-memcrashed/>

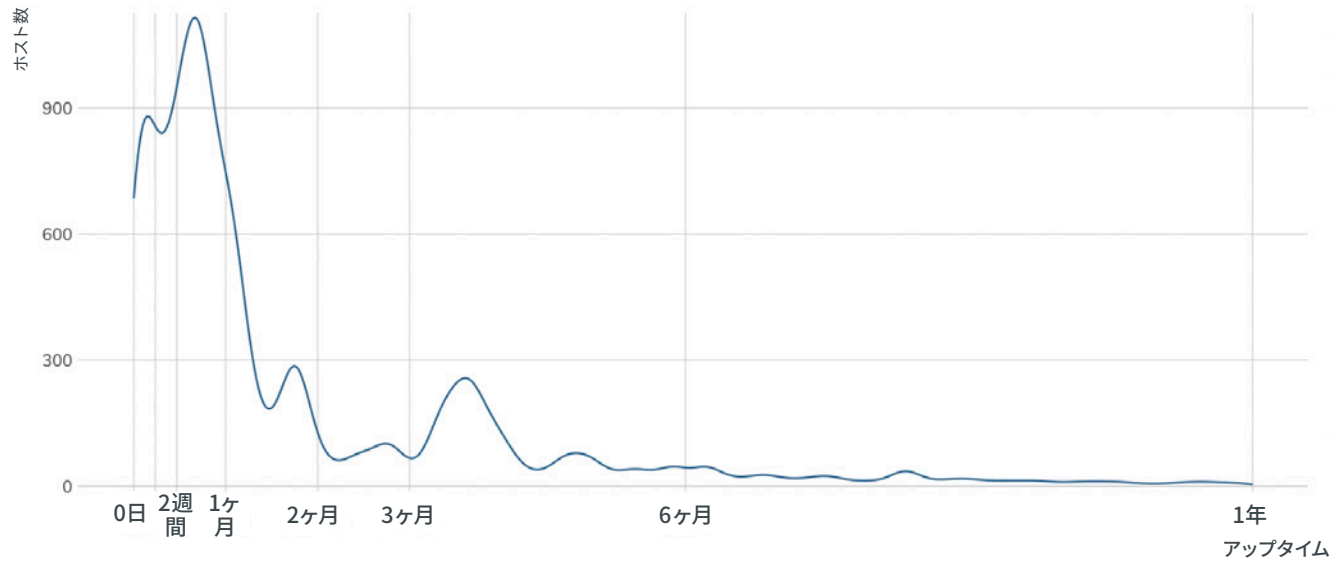
[94] CVE-2018-1000115 <https://attackerkb.com/topics/KM2uX55z24/cve-2018-1000115-major-amplections-ddos-vulnerability>

[95] Memcrashed <https://blog.cloudflare.com/memcrashed-major-ampsification-attacks-from-port-11211/>

Rapid7 Labsは、memcachedを探しながらも、何も見つからないことを期待していますが、前セクションで見た通り、その期待は破られ続けています。発見されたノード6万8,337件のうち、6万8,044件が有効なバージョン番号を返しています（つまり、300人ほどのユーザーが、自分をひどく賢いと思っているということです）。有効なバージョン番号が正しければ、そのうち47%（約32,000件）が1.5.6の固定リリースバージョン以下ということになりますが、1.5.6以上の「目的」は、デフォルトでUDPを無効にすることでした。私たちの調査では、UDPを利用して「**stats**」クエリコマンドを送り、完全な応答を受け取るため、これらのホストはすべて、他の増幅攻撃に使用される可能性があるということです。

そして、「**stats**」クエリから完全な応答を受け取るため、これらのサーバーのほとんどが少なくとも月に1度は再起動されているというのを見ることができたのは良いことです。[96]

検出されたMEMCACHEDホストのアップタイム統計



攻撃者の視点

memcachedのハニーポットはありませんが、UDP11211に接続を試行して、memcahedコマンドがあるかどうかパケットキャプチャを覗き見ていることがわかります。（使用している**統計**では多くの場合、memcachedサーバーだと考えているサーバーに接続されている誤った設定のクライアントのようなものが、しばしば見られることがあります。）ここで見られる毎日のmemcachedコマンド接続は、主にShadowserverからのものです。[97]少し恐ろしい名前ではありますが、自らを（正しく）、「インターネットを全ての人にとって安全なものにするため、陰で尽くしている非営利のセキュリティ団体」と呼んでいます。彼らはまた、毎日インターネットをスキャンして、エクスポージャーや（無料の）サポート組織を把握し、攻撃面の全体像をつかむようにしています。私たちは、Shadowserverを歓迎しています。

2020年の初めの4カ月では、11211上のデータレスUDP接続がわずか数日間に80,000件急増しましたが、この中に悪意がありそうなものは見つかりませんでした。

アドバイス

ITとITセキュリティチームは、memcachedを決してインターネットに露出せず、また、プレイブックやオートメーションを通じて、開発、テスト、およびプロダクションのmemcached環境が厳密にコントロールされていることを確認してください。

クラウドプロバイダは、引き続き安全なサービスの代替手段をセルフホストのmemcachedに提供し、プロバイダが保守するマシンイメージのパッチが最新の状態に保たれ、memcachedのデフォルト設定がインターネットに露出されていないインターフェースでのみ使えるようになっていることを確認してください。また、率直に言えば、独自のネットワーク空間にあるホストで、memcachedをインターネットに露出することを許可しないでください。

[96] Rapid7 Labsは、露出されたmemcachedインスタンスのリモートモニタリングサービスの確立を検討する必要があります。

[97] https://www.shadowserver.org/

政府のサイバーセキュリティ機関は、memcachedの危険性について定期的にリマインドを行い、安全なmemcachedの実行方法のガイダンスを提供してください。また、ISPとクラウドプロバイダに対して、memcachedのデフォルトポートへの接続をブロックするよう、強く奨励してください。

ETCD (TCP/2379)

Kubernetesの有効活用

TLDR

説明：	これも分散型キーバリューストアで、分散型システムやマシンのクラスタでアクセスする必要があるデータの安全な保存方法を提供します。
数：	2,5602, 560のノードを検出しました。 560件 (100%) にバージョンフィンガープリントがありました。
脆弱性：	2018年以降、2件の低〜中程度CVEが見つかっています。
アドバイス：	是非使用してください。ただし、インターネットに露出させないでください。
代替手段：	Redisとmemcachedはetcdとetcdとetcdと似た特性を持つ、インメモリベースのキーバリューストアです。

この、etcd key-value serviceは、Kubernetes[98]エコシステムの一部であり、システムおよびサービス設定やステート情報を保持するように設計されています。Kubernetes APIサーバーは、クラスタの監視と重要な設定変更のロールアウトにetcdのwatch APIを使用します。また、単純にクラスタのステートにおける分岐を、デベロッパーが宣言したものに戻します。これは、HTTPプロトコル上にJSON APIを露出します。

調査結果の詳細

プロジェクトSonarでは、インターネットに露出されたetcdノードを2,560件見つけました。国 (トップ10) およびプロバイダ別カウントは以下の通りです。

国	数
中国	1,036
米国	476
南アフリカ	255
ドイツ	210
香港	66
フランス	64
シンガポール	59
カナダ	56
ロシア	40
オランダ	38

プロバイダー	数
Alibaba	434
Amazon	243
Google	101
OVHcloud	89
DigitalOcean	52
Microsoft	29
Scaleway	15
Oracle	10
QuadraNet	6
Rackspace	1

[98] https://kubernetes.io/

ここでは、（Redisとmemcachedセクションで言及したため）完全性のためにetcdも含めましたが、どれがハニーポットでどれが本物かに関するデータがなく、サンプルサイズが小さすぎるため、掘り下げることはできません。

他の2つのkey-value データベース同様、etcdも決してインターネットに露出させてはいけません。他の2つのサービスと異なり、etcdはKubernetesオーケストレーション環境のためのパーパスドリブンであることが多く、それもまた直接インターネットに露出してはいけない大きな理由です。

インターネットインフラストラクチャ

道路、橋、信号、地図がなく、そして行き方を訪ねたり教えられたりする能力がなければ、ほとんどの国で路頭に迷うことでしょう。インターネットについても同じことが言えます。私たちは、インターネットが可能にしたアプリに依存して、サイトAからサイトBへと移動していますが、その多くのサービスを「見えないもの」として扱います。そのようなサービスの中で重要なものを取り上げ、どのように利用されていて、どれほど安全で、それぞれにどのような特性があるのかを見てみましょう。

ドメインネームシステム（DNS）（UDP/53）

「インターネットの弁慶の泣き所」- ティム・バーナーズ=リー

TLDR

説明：	Domain Name System（DNS）：[99]世界に配布されたインターネット上にあるサービスのアドレス帳です。
数：	471万7,65834のノードを検出しました。 9万8,439件（74.1%）に、Recogフィンガープリント（合計15件のベンダーおよびサービスグループ）がありました。
脆弱性：	全てのサービスグループを通して約200件見つかり、CVSSスコアはさまざまです。
アドバイス：	使わないという選択肢はあり得ません。
代替手段：	DNS over TLS（DoH）、DNS over HTTPS（DoH）、DNS over QUIC（DoQ）、またはNovell Netwareにダウングレード。
傾向：	使用度は昨年とほぼ同じでした。DNSは、インターネットそのものの動作に必要なので、当然と言えます。

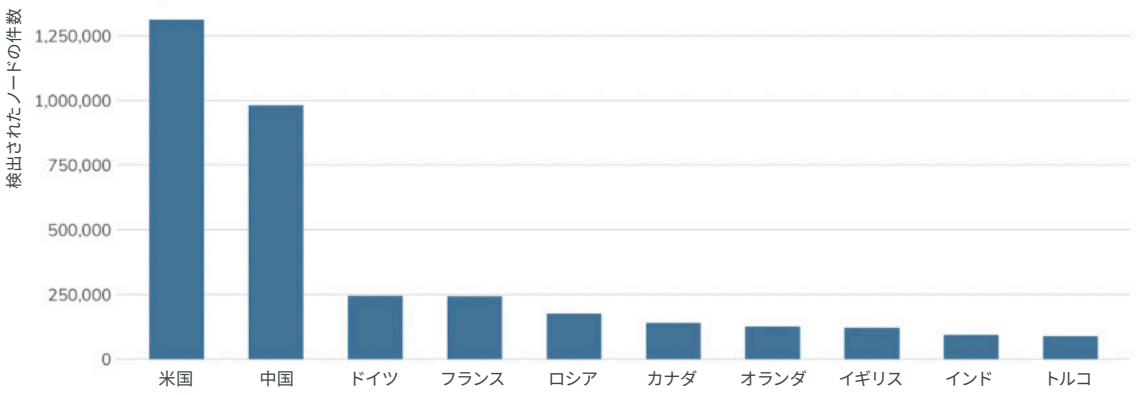
ネットワークリソースにアクセスするためにIPアドレスを暗記したいという人はいません。また、IPアドレスマッピングに膨大なスタンドアロンリストを持ちたい人もいません。しかし、例えば「example.com」というIPアドレスへのリクエストの応答を永遠に待てる人もいません。そこから生まれたのが、最も遍在的であり、ユーザーに面していながらユーザーに最も見過ごされる、インターネット上のサービスが、ドメインネームシステム（DNS）です。

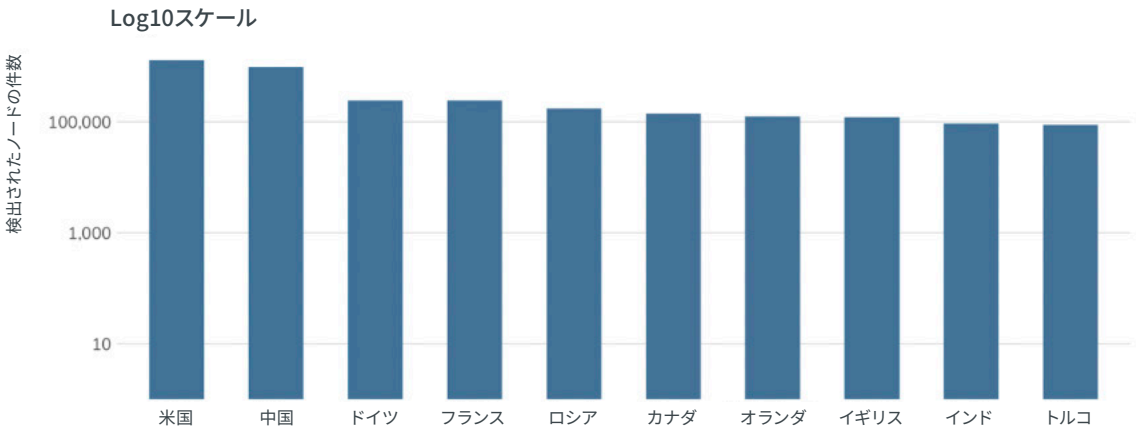
調査結果の詳細

Project Sonarは、53番ポートのUDPリクエストを通じ、約500万件のDNSサーバーを発見しました。これは、例えばWebサーバーの合計数と比べればはるかに少ない数ですが、それでもシステムの数としては相当で、それには納得できる理由があります。ISPは家庭や中小企業のユーザーにDNSサービスを提供し、企業はブランドの名前空間をコントロールするために独自のDNSをホストします。またベンダーは、アウトソーシングの一環として、またはマルウェアやその他のコンテンツタイプのフィルタリングなどの高度なサービスとして、カスタマイズされたDNSサービスを提供します。最後に、Google、Cloudflare、IBM（Quad9経由）などの大手テクノロジー企業が、多くの正当な（?）理由から、集中型のDNSサービスを提供しています。 つまり、巨大な集中型DNSプロバイダを除き、世界のDNSフットプリントは割り当てられた国のIPv4を詳しく追及するということです。ある国に割り当てられたIPが多ければ多いほど、それらすべてを追跡するDNSサーバーの数も増えます。

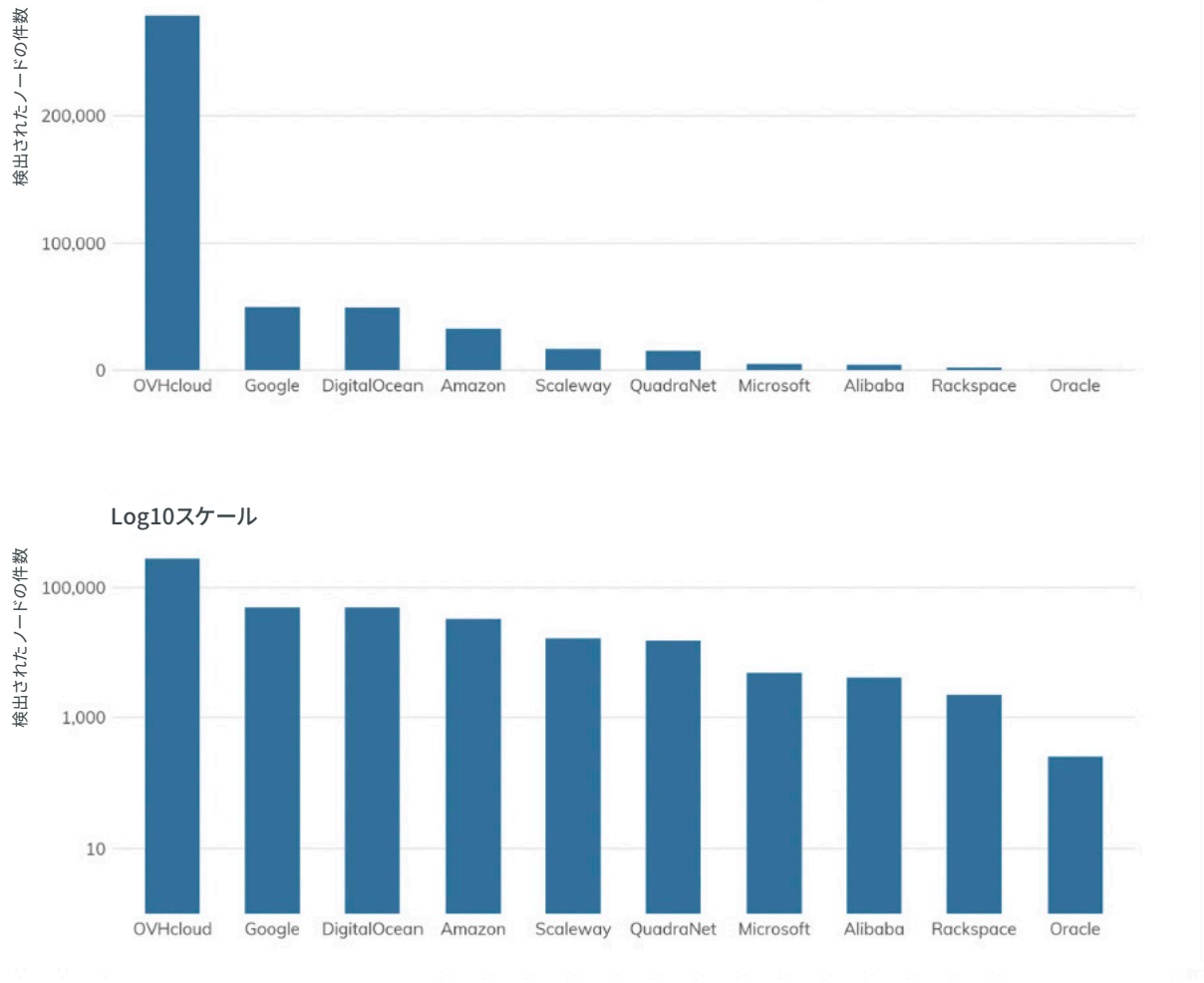
[99] RFC 1034 <https://tools.ietf.org/html/rfc1034>

インフラの上位10か国：DNS（UDP/53）





クラウドプロバイダインフラ：DNS（UDP/53）



一方、貴重（かつコストの高い）クラウドリソースを、DNSのホスティングに費やすというのは、理にかなっていません。しかしながら、OVHユーザーには、使用できるサイクル（および資金）が多くあるようです。つまり、これらは単なるOVHのDNSサーバーではありません。DNSベンダーのソフトウェアが持つ多様性とバージョンの分布から、そのような結論に達しました。現在、OVHは世界最大のデータセンターを持っており、[100]もはや単なるクラウドサービスプロバイダではありません。そのため、同社がトップの座にあり、そうあるべきだというのは納得できます。

最も小規模な組織がISPの外部DNSを（直接または再帰的なDNSを通して）使用していること、また、ホームユーザーのほとんどがいまだにISPのDNSを使用していることから、自律システムのDNSサーバーの分布には大きなロングテールがあることが想像できます。

[100]（今でもこの通りだと思っています）<https://www.itworldcanada.com/article/why-ovh-opened-the-worlds-largest-datacentre-in-the-great-white-north/387358>

エクスポージャー情報

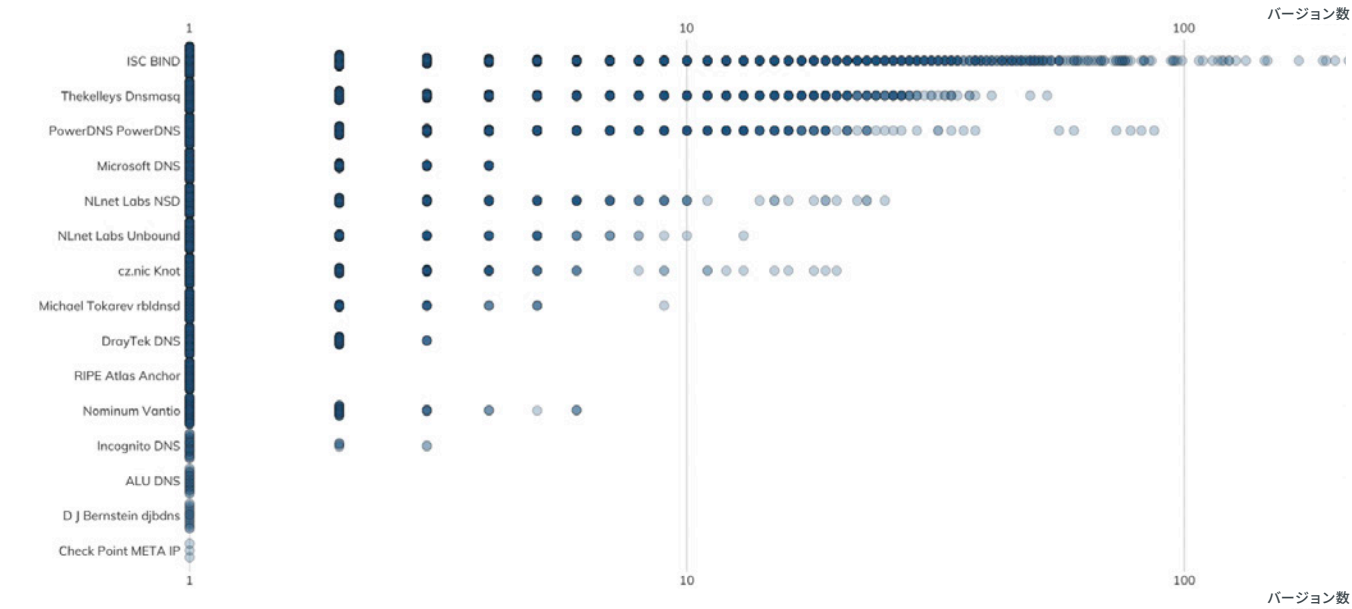
DNSには、これまで多くの課題がありました。DNSはリサーチャーと攻撃者の両者から、大きく注目されるバイナリプロトコルです。これと、UDPサービスの性質から、約60バイトになるバイナリDNSリクエストを作成することが可能です。このリクエストはDNSレスポンスを求め、レスポンスは4,000バイト近く（約1対7の増幅）になる可能性がるため、低〜中程度の増幅型DDoS攻撃に非常に有用となります。[101]また、年々難しくなってはいますが、特別に作成したバイナリメッセージを通じてDNSサーバーに侵入することも可能です。

国	数	割合
ISC BIND	2,007,593	57.39%
Thekelleys Dnsmasq	556,228	15.90%
NLnet Labs NSD	520,785	14.89%
PowerDNS PowerDNS	342,143	9.78%
Microsoft DNS	43,185	1.23%
NLnet Labs Unbound	14,158	0.40%
Nominum Vantio	7,596	0.22%
DrayTek DNS	2,674	0.08%

国	数	割合
cz.nic Knot	1,897	0.05%
Michael Tokarev rbldnsd	898	0.03%
RIPE Atlas Anchor	614	0.02%
ALU DNS	539	0.02%
Incognito DNS	78	0.00%
D J Bernstein djbdns	45	0.00%
Check Point META IP	6	0.00%

BIND（現在はISC BIND）は最初のDNSサーバーで、現在でも最も普及しており（Recogフィンガープリントが見つかったものの中で）、おそらくそのために、119件のCVE（ほとんどがDoS関連）があったと考えられます。 しかし、現実はこれほど明確ではありません。ISC BINDだけでも、550件の異なるバージョンストリング（ほとんどが正当）が見つかりました。状況がどれほど混乱しているかを把握するために、DNSサーバーを持つ自律システム全体で、ベンダーごとにバージョンの多様性を見ることができます。

ASNとベンダー別で見るDNSソフトウェアバージョンディストリビューション



[101] <https://www.us-cert.gov/ncas/alerts/TA13-088A>

これが真面目な調査レポートではなくてソーシャルメディアサービスだったとしたら、今頃「それでも使っているの？」というmeme gifに「パッチ」という単語を入れて投稿しているでしょう。 つまり、私たちは使っているときにDNSのことを忘れるだけでなく、それを実行するときですら忘れてしまうということです。Denial-of-Serviceの欠陥は、これらのサーバーで毎年見られますが、DNSが実行されていたら、それは実行されているのだから、そのまま実行させておく必要があるのです。

攻撃者の視点

私たちはDDoS保護サービス市場にいるわけではなく、またDDoS攻撃の発生を検知できるよう、主要ロケーションにDDoSプローブを置いているわけでもありません。Heisenbergでは、TCPおよびUDPベースのDNSトラフィックが見られますが、そのほとんどはインベントリスキャンや設定ミスです。

これは、攻撃者がDNSのことを気にしなくなったということではありません。全てのDDoSミティゲーションベンダーはサービスレポートで年に数回、このことを必ず私たちにリマインドしています。2019年には、VerizonがDoS全般の大幅な増加[102]を指摘しました（これにはDNSが関連していました）。また、常に新しく巧妙な攻撃ベクトルがリサーチおよび開発されています。[103]

しかし、DNSへの攻撃はDoSだけではありません。私たちが家から何でも購入できるようにするには、組織は、パブリックのトップレベルドメイン名を登録し、さまざまな種類の記録を設定する必要があります。[104]これが、攻撃に2つの手段を与えます。まずはレジストラレベルで、これが多要素認証（この場合SMSではなくアプリベースが理想）でドメイン登録アカウントを保護することが**必須な**理由です。そして次に、外部のDNSプロバイダでも同じことをしてください（外部のDNSを利用している場合）。2020年5月に、Internet Systems Consortiumはまさにこのトピックについて、背景をより詳しく知るのに役立つウェビナー[105]を開催しました。また、SpamHausは、GoDaddyでは毎日約100件のドメインが新たにハイジャックされていると推定[106]しています。

DNSをコントロールする者が、インターネット上でのあなたの身分を決めるのです。

アドバイス

ITとITセキュリティチームは、レジストラと外部のDNSプロバイダアカウントを多要素認証で保護し、内部および外部のDNSシステムのパッチ処理を完全にして、DNSの乱用や設定の変更のサインを徹底的に監視してください。また、DNSを壁の後ろに隠した配管のようにではなく、第一線のアプリケーションとして扱うようにしてください。

DNS登録とホスティングサービスを提供する**クラウドプロバイダは、**多要素認証を義務付け、また、潜在的な悪意のある活動（乗っ取りの試みなど）を検知するためのプロセスを確立してください。デフォルトでインストールされたDNSサービスに付属する全てのマシンイメージは、新しいDNSサーバーのバージョンがリリースされたら直ちに更新し、アップグレードの必要性を全ての既存ユーザーに通知してください。

政府のサイバーセキュリティ機関は、あらゆる種類のDNS攻撃に関してタイムリーな通知を行い、DNSインフラの安全性を確保する方法を文書化するリソースを持つようにしてください。

[102] 2020 DBIR <https://threatpost.com/verizon-data-breach-report-dos-skyrockets-espionage-dips/155843/>

[103] NXNSAttack（2020年5月19日開示）<https://attackerkb.com/search?q=NXNSAttack>

[104] 言ってみれば、今はそれがインターネットの目的ですよね。

[105] ドメイン名ハイジャックのスライド/レコーディング <https://www.isc.org/presentations/>

[106] <https://www.spamhaus.org/news/article/797/the-current-state-of-domain-hijacking-and-a-specific-look-at-the-ongoing-issues-at-godaddy>

DNS-OVER-TLS（DoT）（TCP/853）

DNSの暗号化は非常に有効です。悪者が暗号化する場合を除いて。

TLDR

説明：	DNS over TLS[107]は、その名の通り、TLS接続に埋め込まれたDNSプロトコルで、表面上DNSリクエストの機密性を高めるものです。
数：	3,237件のノードを検出しました。 ベンダーが混ざってしまっていて、バージョン情報については見分けがついたものの、より詳細については調査が必要です。
脆弱性：	DNSの中にあってサービスをサポートしていたり、TLSを示すコードにあるもの（多くの場合、ただのWebサーバー）だったりします。
アドバイス：	In an open relationship It's complicated Separated （読み進めて理由を見つけてください）
代替手段：	分かりやすく、シンプルで単純かつ機密性が低いUDP DNS、DNS over HTTPS（DoH）、[108]DNS over QUIC（DoQ）、[109]鳥類キャリアによるDNS（DoAC）。[110]
傾向：	急上昇中。2019年4月と比べて2倍近くに増加しています。

表向きの数値上は、DNS over TLS（以下DoTと呼ぶ）は、レガシークリアテキストプロトコル向けの機密性ソリューションであり、その他多くの機密性（および整合性）に対する介入の試みに耐えてきています。DNSが盗難や中間者攻撃を受けにくくするための、数少ない現代の取り組みの1つです。

調査結果の詳細

Webブラウザがインターネットの新たなオペレーティングシステムになったことから、DoTを調査することにしました。DoTとその仲間はすべてブラウザ（またはどのようなアプリも）がユーザーの家庭、ISP、組織が選んだDNS解決方法とレゾリューションプロバイダをバイパスできるようにします。TLS上に示されることから、攻撃者にとってはDNSをコマンド&コントロールチャネルおよび脱出チャネルと利用し続けられる、優れた手段にもなります。

DoHではなくDoTの調査を選んだ理由は、DoHに比べてDoTエンドポイントを数える方がはるかに簡単だからです。[111]クエリの標準的な方法に関して、何らかの合意があるようで、DoHを数えるのも簡単になってきています。そのため、将来的にはレポートの対象となると思われますが、今はとりあえず、Project SonarがどのようなDoTを見つけたのかに注目しましょう。

[107]RFC 7858 <https://tools.ietf.org/html/rfc7858>

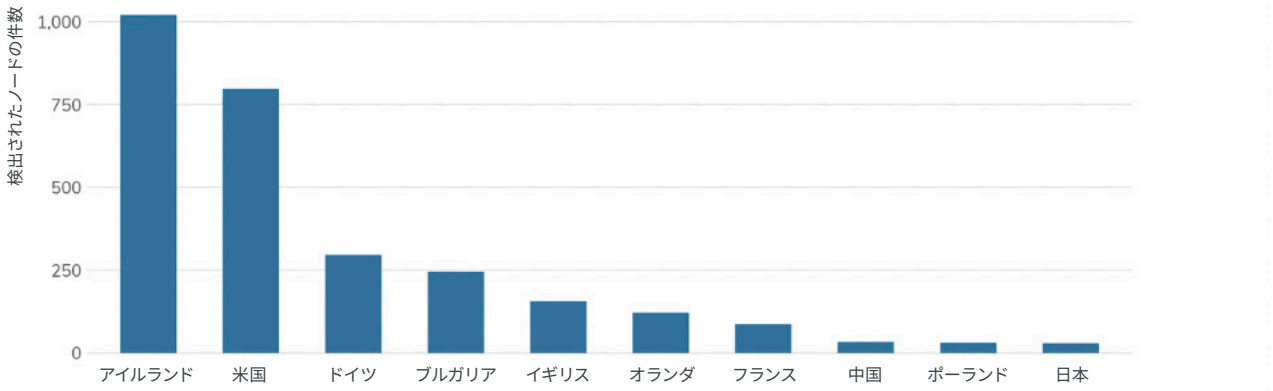
[108]RFC 8484 <https://tools.ietf.org/html/rfc8484>

[109]専用QUIC接続を介したDNSの仕様 <https://tools.ietf.org/id/draft-huitema-quic-dnsoquic-06.html>

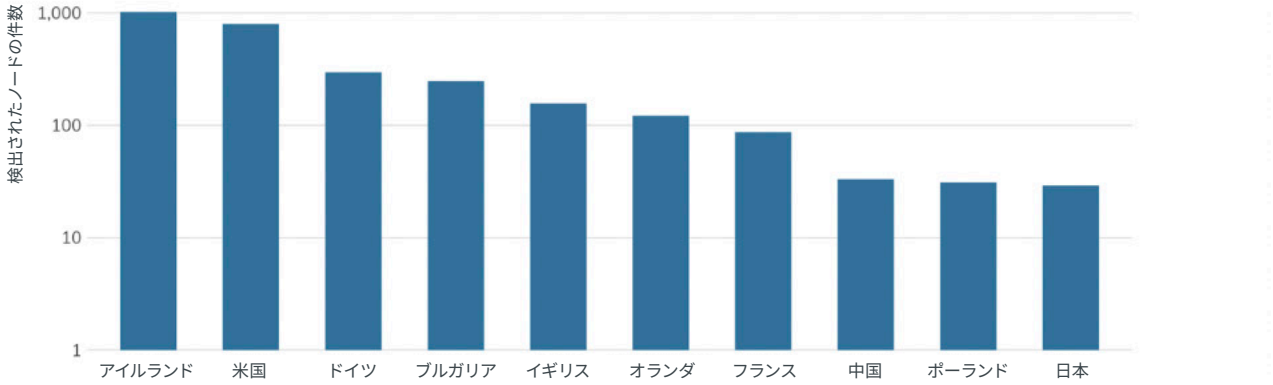
[110]完全に作り上げたものですが、RFC 2549を考えると理論的には可能です <https://tools.ietf.org/html/rfc2549 >

[111]正直なポイント？

インフラ上位10か国：DoT（853）



Log10スケール



表の読み方は合っています。DoTサービスを実行しているノード数で1位となったのはアイルランドで、これは、「サプライズなしで安全にWebをブラウズできる方法を提供する、DNSベースのコンテンツフィルタリングサービス」であるCleanBrowsing[113]を共同経営している、Daniel Cid[112]という方のおかげです。Danielの名前はアイルランドに*割り当てられている*AS205157[114]にありますが、CleanBrowsingサービス自体はカリフォルニアが営業拠点です。[115]CleanBrowsingは実に、DoTコーパスの約50%近く（1,612ノード）を占めており、563ノードが米国に、また少数のサーバーがその他十数国のネットワークスペースに帰属しています。

米国とドイツ両国には、DoTサービスを示す豊富なサーバーの種類や自律システムがあります（CleanBrowsing以外に目立つものはありません）。

ブルガリアがトップ10にランクインするのは珍しいので、何があるのか詳しく見たところ、ISP向けの「メタ」サービスプロバイダーともいえるFiber Optics Bulgaria OOD[116]に多く（相対的にという意味で242件）のDoTサーバーが見つかりました。IPv4アドレスが相対的に不足していることから、242件をDoT専用にするというのは、大きな投資です。

数字は低いものの、日本がランクインするというのは興味深い結果です。日本のDoPは、ほぼすべてが1社のISPであるInternet Initiative Japanによるものです。[117]

[112] <https://en.wikipedia.org/wiki/Daniel_B._Cid>

[113] <https://cleanbrowsing.org/>

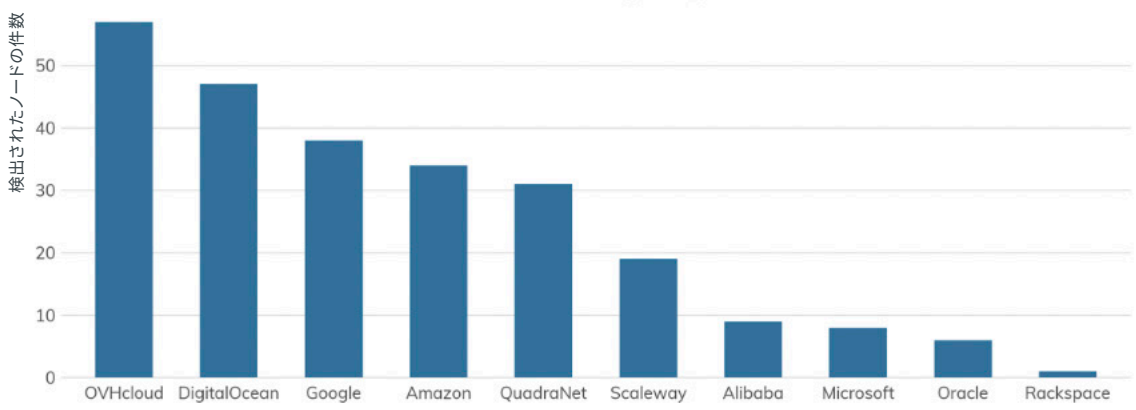
[114] <https://bgpview.io/asn/205157>

[115] はい、IPアドレス属性の全体的な状況は、実にひどく、大規模な修繕をするか、IPアドレスの属性を止めるかのどちらかです。

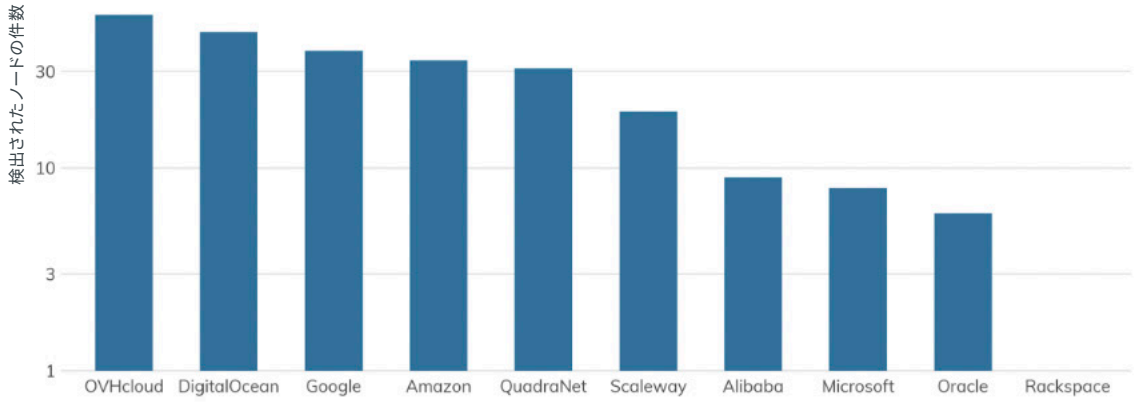
[116] http://www.fobul.net/>

[117] <https://www.iij.ad/jp/ja/>

クラウドプロバイダインフラ：DoT（853）



Log10スケール



ご存知ない人のために一応説明すると、GoogleはDoTの分野で大手[118]ですが、一握りのわずかなIPアドレスにDNSエクスポージャーを集中させる傾向があります（つまり、そのバーはGoogleプロパーではないということです）。CleanBrowsing（本当にどこにでも存在するのです）を除外した場合、Googleの主なエクスポージャーは、Pi-hole[119]のインスタンスを実行している数十件のサーバー（正確にはdnsmasq-pi-hole-2.80）が残ります。この調査結果をOVとDigitalOceanに当てはめてみると、予想通り、同じPi-holeのセットアップがこれらのクラウドでも上位に入っています。

独自のDoTサーバーをホストするのに、わざわざPi-holeセットアップを実行する必要はありません。nginx[120]インスタンスを起動し、基本的な設定[121]を作成して、その背後に独自のDNS[122]をセットアップすれば、ISPがDNSのクエリを詮索することを阻止できます。

[118] <https://developerers.google.com/speed/public-dns/docs/dns-over-tls>

[119] <https://pi-hole.net/>

[120] Nginxはコーパスにある非CleanBrowsingサイトの50%のDoTをプロキシにしました。

[121] <https://www.nginx.com/blog/ussion-nginx-as-doh-gateway/>

[122] GetDNSは賢い今どきのチョイス <https://getdnsapi.net/>

エクスポージャー情報

通常はここでバージョンやCVEの話をしますが、いくつかの要素がDoTの状況を複雑にしています。まず、この分野では独自のソリューションを使用している大企業がいるため、「CleanBrowsing v1.6a」といったバージョンフィンガープリント情報は、あまり役に立ちません。次に、私たちが注目するべきなのは、Webサーバーとバックエンド DNSサーバーのどちらのバージョンでしょうか（それとも両方か）。後者は、nginx DoTセットアップを設定して第三者にプロキシでき、それが応答でピックアップされるため、役に立たないかも知れません。最後に、PowerDNS[123]などの二流「大手」に注目したところで、結局は以下のような状況になります。

PowerDNS
PowerDNS Authoritative Server 4.0.9 (built Jul 31 2019 00:17:38 by buildbot@4842127c3c6c)
PowerDNS Authoritative Server 4.1.1
PowerDNS Authoritative Server 4.1.10 (built Jun 20 2019 23:00:19 by root@e0846b1bda55)
PowerDNS Authoritative Server 4.1.11
PowerDNS Authoritative Server 4.1.3 (built May 24 2018 12:54:13 by root@cebf8df1a8ce)
PowerDNS Authoritative Server 4.1.4 (built Aug 29 2018 14:08:38 by root@7d1469b19fba)
PowerDNS Authoritative Server 4.1.6
PowerDNS Authoritative Server 4.1.6 (built Feb 6 2019 14:44:29 by root@FreeBSD-Core-default-job-03)
PowerDNS Authoritative Server 4.2.0 (built Jan 5 2020 00:41:27 by nobody@pkg.ssnet.ca)
PowerDNS Authoritative Server 4.2.0 (built Jan 27 2020 11:34:42 by root@113amd64-quarterly-job-13)
PowerDNS Authoritative Server 4.2.1
PowerDNS Authoritative Server 4.2.1 (built Nov 29 2019 11:55:12 by root@2ccf7cb0fe12)
PowerDNS Authoritative Server 4.2.1 (built Nov 29 2019 13:34:28 by root@f06a46cf444e)
PowerDNS Authoritative Server 4.3.0-beta2 (built Feb 19 2020 01:48:39 by root@eacdc4c975a9)
PowerDNS Authoritative Server 4.3.0-rc2 (built Mar 18 2020 20:04:33 by root@freebsd_12x64-system-job-01)
PowerDNS Authoritative Server 4.4.0-alpha0.189.master.gdbcbb6820 (built Mar 27 2020 18:40:56 by root@4bf58b8d80f0)
PowerDNS Recursor
PowerDNS Recursor 3.7.3 (jenkins@autotest.powerdns.com built 20151009082750 suresh@)
PowerDNS Recursor 4.0.4
PowerDNS Recursor 4.1.1
PowerDNS Recursor 4.1.11
PowerDNS Recursor 4.1.14
PowerDNS Recursor 4.1.15 (built Dec 3 2019 12:30:06 by root@626a1e888795)
PowerDNS Recursor 4.1.8
PowerDNS Recursor 4.1.8 (built Nov 26 2018 14:00:19 by buildbot@73da2fe09a4f)
PowerDNS Recursor 4.2.0 (built Jul 15 2019 09:36:44 by root@d44ad1e36fdb)
PowerDNS Recursor 4.2.1 (built Dec 6 2019 15:21:13 by root@b55bffd5a41e)
PowerDNS Recursor 4.2.1 (built Dec 6 2019 16:06:22 by root@acea22bef73d)
PowerDNS Recursor 4.2.1 (built Dec 6 2019 17:14:08 by root@77f29736172f)
PowerDNS Recursor 4.2.1 (built Dec 6 2019 17:42:47 by root@5cbd65d75070)
PowerDNS Recursor 4.3.0 (built Mar 2 2020 14:27:59 by root@031b640c6ba8)
PowerDNS Recursor 4.3.0 (built Mar 28 2020 20:36:40 by balor@optimus-G750JZ)
PowerDNS Recursor 4.3.0-beta1.203.master.ge8a76b3be (built Feb 6 2020 10:46:29 by root@68ea2e4b7b0c)
PowerDNS Recursor 4.3.0-beta1.25.master.g732b1dbd0 (built Dec 31 2019 12:13:41 by root@2bbbfe93b2b7)

[123] <https://www.powerdns.com/>

少し見ただけで、PowerDNSの世界でも完全なカオスであることが分かります。しかし、DNSとカオスというのは密接に連携するものでもあります。

攻撃者の視点

HeisenbergにはDoTハニーポットがありませんが、DoTというのは従来のDNSバイナリ型クエリの単なるTLSラッパに過ぎません。それをTCP/853のフルパケットキャプチャで探すと、私たち自身（!）と他のいくつかのリサーチャーが見つかったのです。あまり嬉しいことではありませんが、DoTの目的がプライバシーの保護であることを考えると、ランダムなDoTリクエストはあってはならないのです。

攻撃者はおそらく、独自のDoTサーバーを立ち上げるか、他のDoTサーバーを再設定して、フィッシング攻撃に成功して足がかりを得たら、それらのDNSバックエンドをCovert Channelとして利用するでしょう。これが、私たちがDoTを数えて整理する主な理由で、家庭用ISPおよび従来のホスティングプロバイダのIPスペースで見られるDoTは増えてきています。毎月調査を行う中で、DoTを試している人が増えているように見えます。

アドバイス

ITとITセキュリティチームは、TCP/853をブロックしてDoTとDoHのブラウザ設定をできるだけ封鎖し、組織のITポリシーをバイパスできないようにしてください。また内部（および外部）でのDoTとDoHサービスを使おうとするすべての試みを監視してください。つまり、自分自身がそれを設定している場合を除き、不正な内部DoTを禁じることが、最も安全な方法だということです。

クラウドプロバイダは、自立したいというユーザーに対して、マネージドDoTソリューションで、パッチされた安全なディスクイメージの提供を検討してください。（これは、組織とクラウドに関するアドバイスがほぼ反対という数少ないケースの1つです。）

政府のサイバーセキュリティ機関は、悪意のあるDoTの使用を監視し、最新情報の発表を適宜行ってください。このような機関は、DoT、DoH、DoQなどに関する公正で専門的な情報源でもあるべきです。

NTP（123）

ザ・スミスの不朽の名言、「How Soon is Now（今はいつ来るの？）」です。

TLDR

説明：	時刻同期させるサービスが、Network Time Protocolです。[124]
数：	163万8,577のノードを検出しました。 163万8,495件（99.9%）に、バージョンや/その他のフィンガープリント可能な情報があり、それよりも（かなり）小さなサブセットから、オペレーティングシステム情報を得られました。
脆弱性：	若干数あります。主にDenial-of-Serviceと情報漏洩ですが、時々リモートコード実行も見られます。
アドバイス：	是非使用してください。ただし、インターネット上では使用しないでください。そして、正しく設定してください。パッチ処理もお忘れなく。
代替手段：	なし。これは、時刻同期のデファクトスタンダードです。
傾向：	まるで時間が止まっているかのようです。2019年から変化が一切ありませんでした。

NTPがなければ、インターネットは今のように機能しません。これほどの力を持つNTPは、すべてBPOC[125]で、うぬぼれた偉そうなものだと思うかもしれません。しかし、 時間に関して全てのコンピュータを同期させる という仕事は見事にこなします。Denial-of-Service攻撃に利用されるときを除いては。1985年に誕生したNTPは、唯一のネットワークベースの時刻同期プロトコルという訳ではありませんが、事実上の標準となっています。

[124] RFC 5905 <https://tools.ietf.org/html/rfc5905>

[125] キャンパスの大きなプロトコル

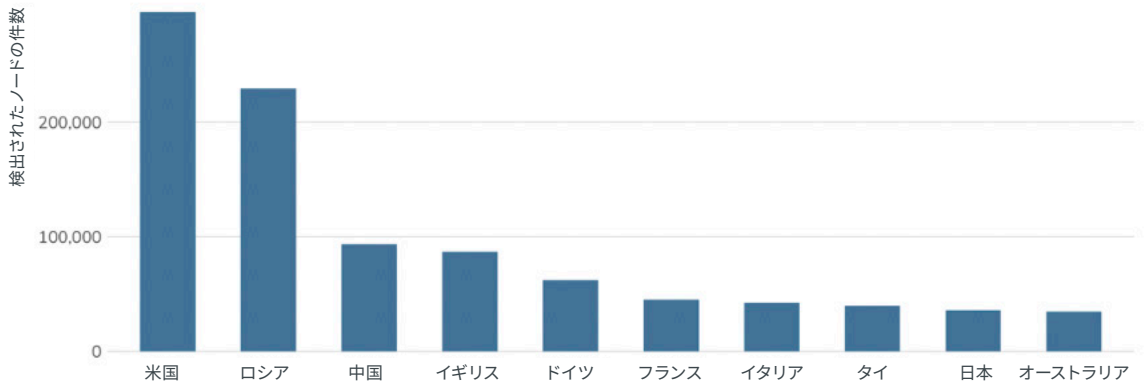
NTPサーバーは、stratumと呼ばれる最大15レベルまである階層で動作します。私たちが毎日使用する、権威ある可用性の高いNTPサーバーがあります（多くの場合オペレーティングシステムベンダーが提供し、またtime.apple.comやtime.windows.comなど分かりやすい名前のホストで動作しています）。

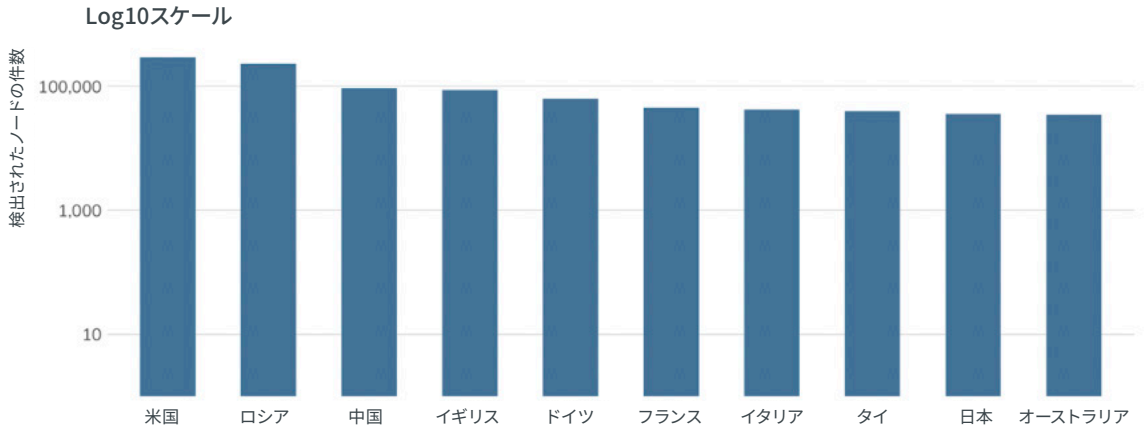
事実上、ルーターや電話、またRaspeberryPiなど、つまりGPS信号をタイムソースと認識する専用機器なら、なんでもNTPサーバーになります。ただ、何かがタイムサーバーになれるからというだけで、そうなるべきだとは限りません。

調査結果の詳細

Project Sonarでは、パブリックインターネット上に163万8,577件のNTPサーバーが見つかったので、時間に関する問題は多いと言えるでしょう。[126] 編集者はそう思わないみたいなので、国やクラウド別の状況を見てみましょう。

インフラ上位10か国：NTP（123）

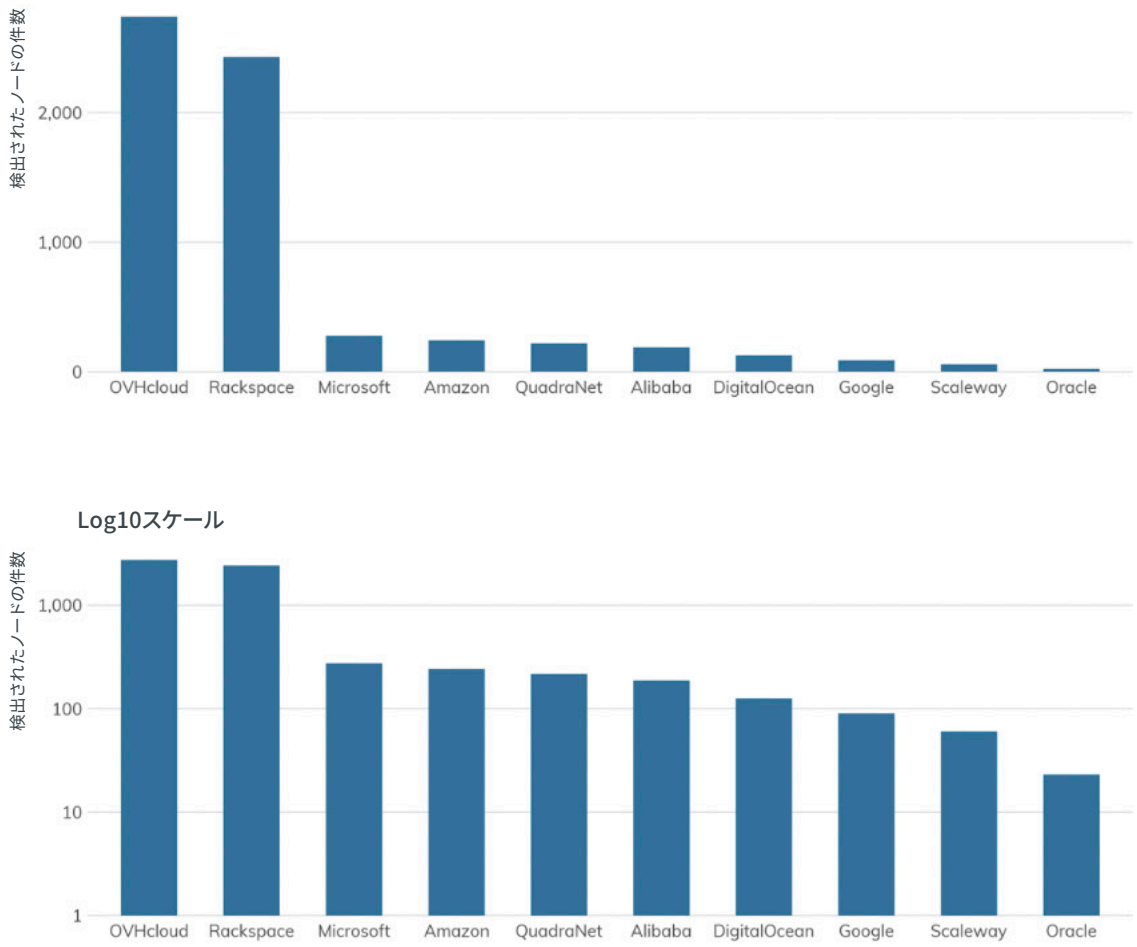




米国には、多くのIPv4ブロック、多くのコンピュータ、そして物事をコントロールしたがる、多くのSP大手やIT企業があります。また、正当な理由なしにNTPを運営する企業も多くあります。米国がトップの座にあるのは、このような理由からです。ここで遂にロシアが2位に上がっています。理由は米国と似ていますが、ロシアの場合、大手ISP2社がエクスポージャーの40%強を占めています。 莫大なIPv4スペースと人口を持つ 中国が3位であるというのは、企業やISPが、むやみにNTPを露出すると、必要以上に問題を引き起こすということに気付いたことを意味します。

[126] 本当に、このセクションでダジャレをいうチャンスを逃すと思いましたか。

クラウドプロバイダインフラ：NTP（123）



Rapid7 Labsとしては、クラウド環境（プロバイダと顧客の両方）が、NTPを実行することの危険性を真摯に受け止め、多くのユーザーにエクスポージャーがほとんどないというのは喜ばしく思います。

エクスポージャー情報

プロトコル自体に対するメインのサポートサイトのページトップに、NTPの危険性に関する大規模で深刻な警告があるということは、NTPに危険が潜んでいるのだということはお分かりになったでしょう。[127]最大の危険が発生するのは、増幅型DDoSに利用された場合です（UDPベースのプロトコルであるため）。NTPは現在でも使われていますが、そのような目的にはmemcachedのように、はるかに優れたサービスがあります。

NTPサーバーも、他のソフトウェア同様、脆弱性を持ったソフトウェアの集まりに過ぎません。何かをインターネットに載せると、悪者がそれをコントロールしようとします。組織が 何かしらの理由で NTPサーバーを独自に実行する場合、それをパブリックインターネットに載せる必要は何もありません。また、例えそうしなければならない理由があったとしても、すべてのサブネットからのリクエストに応答するように設定する必要はありません。

なぜこのようなあら探しをしているのでしょうか。パッチ処理をしないというのも、もう1つの問題です。さらに、ネットワークセットアップについて攻撃者に情報を与えているかも知れないという問題もあります。NTPコーパスでは、内部ネットワークインターフェース上のプライベートIPアドレススキームが25万5,602件（15.5%）で見つかりました。

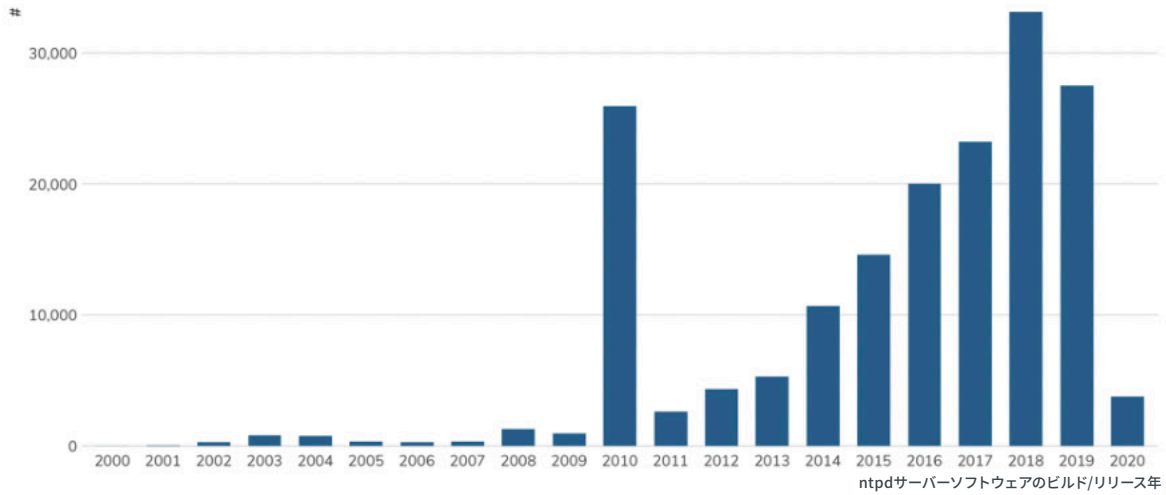
[127] <http://support.ntp.org/bin/view/Main/WebHome>

150万件以上のNTPサーバーが、オペレーティングシステムやバージョンに関するヒントを公開しているのです。

OS	数	割合
UNIX (ジェネリック)	1,089,876	69.61%
Ciscoデバイス	294,330	18.80%
Linux+カーネルバージョン	99,032	6.32%
BSD+カーネルバージョン	38,798	2.48%
Juniperデバイス+バージョン	32,469	2.07%
VMware+バージョン	8,597	0.55%
SunOS	948	0.06%
その他	657	0.04%
vxWorks	505	0.03%
Sidendinder+バージョン	332	0.02%
QNX+バージョン	186	0.01%
macOS+バージョン	66	0.00%

合計で、18万410件 (11%) がNTPの正確なバージョンとビルド情報を公開しており、約4,000件が正確なリリース日も提供しています。

不適切に設定されたNTPDサーバーのビルド年



NTPデバイスのミックスには、[不]健全なリモートコード実行、情報漏洩、ローカルサービスDoS、増幅型DDoSのミックスが広がっています。

もし本セクションの初めに、「ただのNTPサーバじゃないか」と思っていたのであれば、そうではないということを少しでも説得できたのなら幸いです。

攻撃者の視点

「エクスポージャー情報」セクションでは、NTPシステムにおける潜在的（および測定された）弱点に関する多くの情報を提供しました。攻撃者は、ユーザーの攻撃面がどのように設定されているかを見て、標的としての可能性を判断します（そしてサイバー保険の掛け金も上がるでしょう）。NTPは、設定の亀裂やパッチ管理プロセスをすべて公開し、またエントリの手段まで提供することができます。

そして、増幅攻撃にNTPが利用されれば、存在すら知らなかった、または本当に必要だと考えたNTPサーバーが、他のサイトの攻撃にも使われるのです。

アドバイス

ITとITセキュリティチームは、ファイアウォールの背後でNTPを使用し、適切なパッチ管理を行ってください。外部でNTPを実行する必要がある場合は、対話できるホストやネットワークを制限してください。

クラウドプロバイダは、露出するNTPを引き続き必要最低限に抑え、（インターネットの外での）NTPの安全な実行方法についてユーザーにガイダンスを提供してください。

政府のサイバーセキュリティ機関は、NTPの新たな脆弱性や、NTPに対する活発なDoS作戦が発見された場合、速やかに通知してください。 NTPをインターネットに露出することの危険性や、さまざまなNTPサービスの安全な設定方法に関する教材を配布できるようにしてください。

Webサーバー

昨年（2019年）は、World Wide Webの誕生から30周年を迎えました。何十万ものブロガー、ニュースアウトレット、ベンダーがそれについて話、Webとは何か、そして今後どこに向かうのかについて、ひっきりなしに意見を述べたので、ここではそれは省きます。「Webサーバー」は、そのコアが、Hypertext Transfer Protocol（HTTP）プロトコルリクエストを受け取って応答するソフトウェアのかけらであることを考えると、非常に意味の深い単語です。現在では、騒がしいブログ投稿や猫の写真を配信する、従来のサーバー環境内にあるコンポーネントから、冷蔵庫、ネットワークルータ、インターホン、自動車またはドローンに内蔵されているマイクロチップに合致するAPIリクエストのコンデュイットまで、ほとんどすべてのもののフロントエンドです。かなり小さく、笑えるほど簡単にインタラクトできるため、「どこにでも」存在します。

本セクションでは、暗号化（HTTP 443）と、インターネットに接続された暗号化された（HTTP 80）Webサーバーに注目します。このうちの一部は、リモートアクセスのセクションでCitrixサーバーを説明する際に少し言及しました。（Citrixクライアントからの）初期接続と応答は、Webサーバーから来るためです。[1]軽量のHTTPプローブからのエクスポージャーについて、あまり多くは語ることがないので、モリアのドワーフのように、このセクションについてあまり深く掘り下げることはしません。[129]

[128] いった通りでしょう。どこにでもあるのです。

[129] さらに、私たちは高度にカスタマイズされたHTTP[S]インターネット全体のスキャンを専門とするNetcraft（<https://news.netcraft.com/archives/category/web-server-survey/>）やGoogleではありません。

HTTP (TCP/80) とHTTPS (TCP/443)

1つのプロトコルはすべてを捕えて、暗闇の中に繋ぎとめる。

TLDR

説明：	HTTP：原型であるプレーンテキストのHypertext Transfer Protocol通信です。 HTTPS：暗号化されたHTTP通信です。
数：	5,151万9,309件のHTTPノードと 3,614万1,137件のHTTPSノード を検出しました。本セクションでは、フィンガープリントを少し異なる方向から見るため、RAWデータの検出数は意味を持ちません。
脆弱性：	大変です。非常にたくさんあります。しかし、それはコアのWebサーバー自体の脆弱性でしょうか。それとも組み込まれたアドオン？利用されるWebアプリケーション？Facebookユーザーがよくいうように、「それは複雑です」。
アドバイス：	*Gopherに戻るべきです！*[130]という、冗談はさておき、今後もHTTPSを使用して是非、良いものを作り続けてください。ただ、インストールして、Webサーバーの運用をする担当者が、簡単に安全な設定を行い、パッチ状況を把握し、自信を持って迅速にアップグレードできるようにしてください。
代替手段：	QUIC、[131]、 または「Quick UDP Internet Connection」があります。これは、「UDP上の新しい多重で安全なトランスポート通信で、始めからHTTP/2セマンティック向けに設計および最適化された」ものです。HTTP[S]は今後も長く使われますが、QUICはその後継者であり、コンテンツを安全かつ効率的に提供するまったく新しい方法に導いてくれます（ただし、間違くなくこれも悪用されることになります）。

ここでは、HTTPとHTTPSを併せて（ほとんどの部分で）、調査結果、主なエクスポージャーのコア領域、また攻撃者にとっての機会を見ていきます。これまでのセクションと少し異なりますが、それは一般的にHTTPが持つ風変わりな性質の一部です。

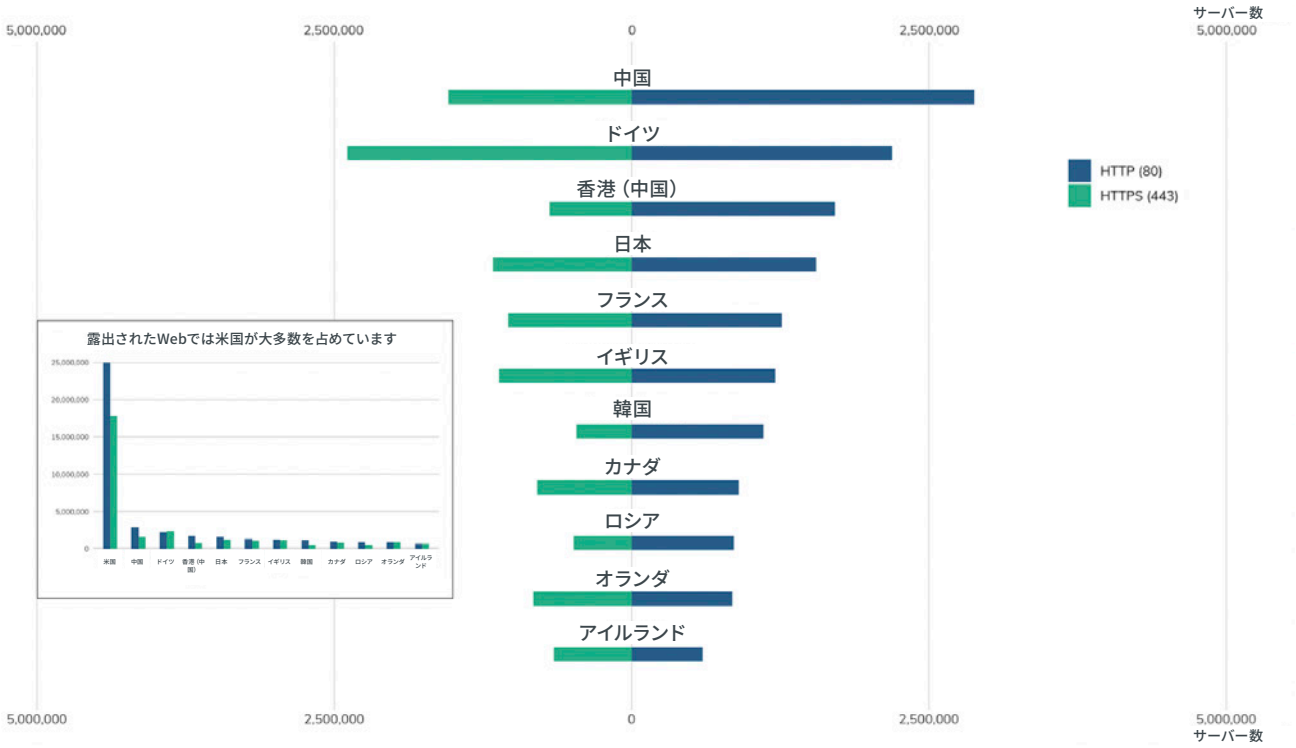
調査結果の詳細

先ほどメールのセクションで、暗号化と非暗号化サービスを比較しました。ここでも同じ比較をしますが、HTTPとHTTPSの組み合わせであるため、国別ランキングではトップ12のみを紹介します。

[130] <https://en.wikipedia.org/wiki/Gopher_(protocol)>

[131] QUIC IETFドラフト <https://tools.ietf.org/html/draft-tsvwg-quic-protocol-02>

国別で見る暗号化と非暗号化HTTPサービスの比較（上位12か国から米国を除いたもの）



インターネット上ではプレーンテキストHTTPを実行しているデバイスが、暗号化されたHTTPSWebサービスよりも30%多くあります。検出されたWebサービスという点では、米国が他を大きく引き離して1位となっています。これは、そして米国に割り当てられているIpv4スペースにあるクラウドサービス、ホスティングプロバイダ、そしてルータ、スイッチなどが多いためだと思われます。

ドイツとアイルランドはそれぞれ、HTTPSノードをHTTPよりも9%多く露出しています。また、オランダと英国も暗号化の格差を急速に狭めています。

クラウドサーバーにはWebサーバーが溢れていることは誰もが知っていますし、調査開始の日、Amazonには64万のElastic Load Balancers（バージョン2.0）があったことをここで伝える意味もないので、クラウドにおける数は省略します。

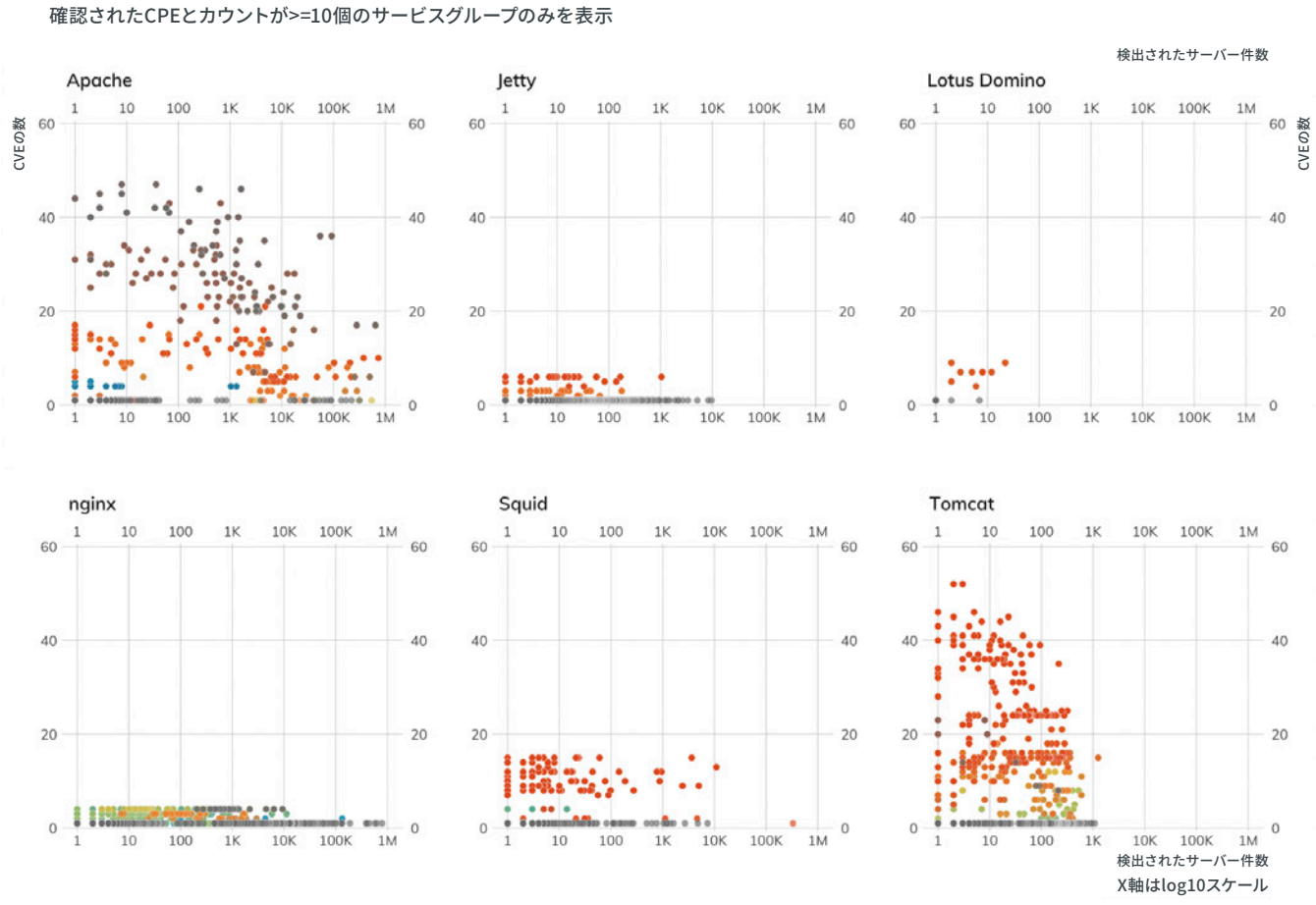
エクスポージャー情報

エクスポージャーを理解するには、これらのWebサーバーで何が実行されているかを見る必要があります。軽量のスキャンでは、それは思うほど簡単なことではありません。例えば、以下はベンダー/グループとポートのHTTPのトップ20です。

ベンダー	グループ	HTTPS (80)	HTTPの割合	HTTPS (443)	HTTPSの割合
Microsoft	IIS	5,273,393	10.24%	2,096,655	5.80%
Apache	Apache	4,873,517	9.46%	2,595,714	7.18%
nginx	nginx	3,938,031	7.64%	2,495,667	6.91%
Amazon	Elastic Load Balancing	644,862	1.25%	386,751	1.07%
Squid Cache	Squid	381,224	0.74%	8,649	0.02%
ACME Laboratories	mini_httpd	125,708	0.24%	82,427	0.23%
Oracle	GoAhead Webserver	48,505	0.09%	40,501	0.11%
Apache	Tomcat	40,702	0.08%	32,271	0.09%
Taobao	Tengine	37,626	0.07%	14,130	0.04%
Eclipse	Jetty	29,750	0.06%	50,763	0.14%
Mbedthis Software	Appweb	23,463	0.05%	19,470	0.05%
Virata	EmWeb	22,354	0.04%	7,179	0.02%
Embedthis	Appweb	17,235	0.03%	32,629	0.09%
Microsoft	Windows CE Web Server	14,012	0.03%	1,027	0.00%
TornadoWeb	Tornado	13,637	0.03%	10,151	0.03%
Tridium	Niagara	9,772	0.02%	564	0.00%
TwistedMatrix	Twisted Web	7,481	0.01%	4,984	0.01%
Caucho	Resin	5,168	0.01%	1,812	0.01%
Mort Bay	Jetty	5,079	0.01%	2,033	0.01%
SolarWinds	Serv-U	3,232	0.01%	6,421	0.02%

これは、それぞれの活発なIPアドレスの2つのポートへの「GET」リクエストで戻ったもの、そしてRecog署名から（これは優秀ですが、包括的とは全くいえません）のカウントを数えただけです。一部のサーバーでは個別のバージョンレベルまで掘り下げることができるので、そこからCommon Platform Enumeration [132]識別子を構築することになりました。この識別子を使うと、特定のインスタンスタイプと関連しているCVEの数を知ることができます。この機能を利用して、各サービスグループの各バージョンをCVEの数で比較しました。上記のリストの全てをカバーしているわけではありませんが、いくつか重要なものがあります。

HTTP（80）とHTTPS（443）を組み合わせた、程度別で見るサービスグループバージョンごとのCVE



サービスグループは、システムエクスポージャーが最低10件のものに絞り、CVSS v2のスコアのエンコードに色を使いました。

CVEで最も多く見られた脆弱性は、以下の表のとおりです。厳密にいうと、これらのCVEが別の何らかのソフトウェアコントロールによって緩和されたというのは可能ですが、脆弱性の管理者と不快な会話を避ける最も簡単な方法は、全体のパッチ処理を行うことです。

[132] CPE <https://nvd.nist.gov/products/cpe>

以下は、最も多く見られたトップ30です。

CVE	数
CVE-2017-8361	336
CVE-2013-2275	202
CVE-2012-1452	186
CVE-2016-1000107	184
CVE-2016-6440	184
CVE-2012-0038	168
CVE-2012-1835	165
CVE-2016-8827	165
CVE-2011-3868	164
CVE-2011-0607	160
CVE-2007-6740	154
CVE-2013-4564	150
CVE-2016-0948	149
CVE-2016-0956	149
CVE-2009-2047	146
CVE-2015-5670	145
CVE-2017-8577	143
CVE-2014-0134	135
CVE-2015-5355	135
CVE-2012-5932	127
CVE-2014-8089	120
CVE-2015-5685	118
CVE-2016-1000109	118
CVE-2015-5672	114
CVE-2016-5596	112
CVE-2016-5600	112
CVE-2016-4261	111
CVE-2016-4263	111
CVE-2016-4264	111
CVE-2016-4268	111

従来のWebサーバーが見られると予想していますが、その他にも、インターネットに接続されていて、Webサービスや管理インターフェースを露出するデバイスがあります（一部を以下でカウントしました）。

ベンダー	デバイス	HTTP (80)	HTTPS (443)
Cisco	ファイアウォール	123	986,766
AVM	WAP	1,942	604,890
Asus	WAP	1	177,936
Synology	NAS	61,796	50,531
チェックポイント	ファイアウォール	16,059	30,773
SonicWALL	VPN	7,413	16,061
Ubiquiti	WAP	0	11,813
HP	プリンター	16,247	9,178
MikroTik	ルーター	289,026	8,056
Tivo	DVR	6,400	6,779
Philips	電球	4,785	3,349
Polycom	VoIP	369	3,079
Ubiquiti	Webカメラ	955	922
HP	Lights Out Management	601	708
ARRIS	ケーブルモデム	350	217
Fortinet	ファイアウォール	1,221	159
Xerox	プリンター	1,575	29
Canon	多機能デバイス	124	14
Netwave	Webカメラ	6,420	7
HeiTel	DVR	2,734	2
Samsung	DVR	53,053	2
Merit LILIN	DVR	2,565	1
Fidelix	産業制御	545	0
FUHO	DVR	1,249	0
Shenzhen Reecam Tech.Ltd.	Webカメラ	1,902	0
Ubiquiti	DVR	675	0
ヤマハ	ルーター	9,675	0

例えば、Cisco ASAのファイアウォールは、100万件近く見つかりました。これらはリモートアクセスサービス（VPNなど）を提供するために設定できるので、この件数自体が「悪い」という訳ではありません。しかし、80番ポートに123件のインスタンスがあるというのは、理想的ではありません。

Ciscoと異なり、MikroTikルーターのほとんどは暗号化なしで露出されており、そのうち75%以上がデバイスの管理インターフェースを露出しています。[133]それの何がいけないのでしょうか。

Synologyネットワークに付属するストレージデバイスも5万件以上見つかりました。「**ファイル共有**」のセクションで、この種のデバイスにおける残念なエクスポージャーの状況について、詳しく説明しています。これらがインターネットにあるのは、所有者がローカルメディアの起動と、その他のファイルにアクセスできるようにするためです。

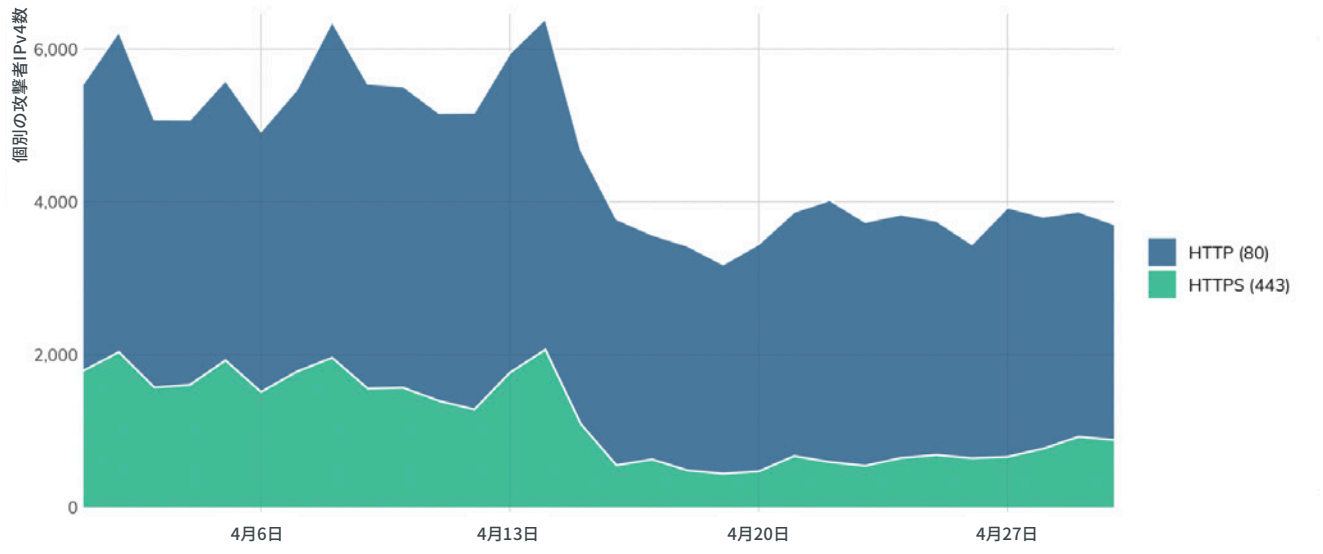
また、プリンターや電球、DVR、ホームルーターの管理インターフェース、そしてビルのコントロールシステムが丸ごと、何千件も上がっています。[134]要するに、インターネット上のWebインターフェースにはほぼ何でもあるということです。

攻撃者の視点

最近のHTTP[S]サービスには、多くの層があり、攻撃者は多くの場合、どれを最初に狙うかが分からず、足止め状態となります。組み込みシステムでHTTPサービスを攻撃することは、一般的に、最も安全な方法の1つです。一般的に所有者やネットワークオペレータによって監視されておらず、ほぼ完全に匿名で使用できるからです。

Apache Struts、WebLogicなどの 公式Webサービスも、よくエンタープライズ展開と関連付けられており、金銭的利益や機密情報へのアクセスが得られる可能性が高いため、狙われやすいターゲットです。過去18～24か月間、多くの攻撃者グループが、（「**リモートアクセス**」のセクションでも見た通り）HTTPインターフェースからファイヤーフォールとリモートアクセスシステムに主に焦点を当てています。これは、一度侵入すれば、悪用の足掛かりを内部ネットワークの中心部に置くことで、（通常は）すぐに次の足掛かりと二次的にアクセスする方法の確立が可能になるからです。

2020年4月の1日当たりに発生したHTTP（80）とHTTPS（443）の個別攻撃者



また、独自ソースのIPv4とインタラクションビューの合計から分かるように、HTTP（80）の初期プローブが（少なくとも今のところは）増加する見込みです。「80番と、特に80番から433番に動くクライアントに注意してください」とは言えません。何故なら、ほとんどのサイトが両方のポートを使用しており、優良なサイトのサービスの多くは、クライアントを自動的にHTTPSへリダイレクトするよう設定しています。それでも、80番の方をより重視しているクライアントがいたら、フラッグをつけて、深堀調査を行うことをお勧めします。また、HTTP（80）のみを使うシステムには、注意してください。

[133] そして一般的な管理者パスワードは、Google検索すれば手に入ります（そしておそらくうまくいくでしょう）。

[134] <https://www.fidelix.com/building-automation/>

アドバイス

ITとITセキュリティチームは、素晴らしいプラットフォームやサービスを構築して、HTTPS上でインターネットに載せてください。イノベーションが変化と進歩を生みます。 また、最初のHTTPリクエストが作成されてから、インターネットは悪いことよりも良いことを多くしてきました。これらの全てにパッチを当て、安全な設定とコーディングの実践を、開発および展開のライフサイクルの一部にしてください。可能な限り、管理インターフェースをインターネットの何かに置くことはせず、お使いのネットワークデバイスや「Internet of Things」デバイスが露出しているサービスを把握してください。最後に、「Server」バナーをすべて無効にし、他に漏洩されるものがないかをHTTPヘッダーで調べて、できる限りサニタイズしてください。例えばngiinxを探している攻撃者はよく、ServerヘッダーにApachegaがあると、次に移動します。この1点を変えることが、どれほど効果のあるものか、驚くはずです。

クラウドプロバイダは、安全でスケーラブルなWebテクノロジーを提供し続けてください。同時に、一般的なアプリケーションスタックが備わっているビルド済みイメージがある場合は、パッチ管理を徹底して、新しいリリースが出た場合はユーザーに通知できるようにしてください。

政府のサイバーセキュリティ機関はデジタルごみをインターネットの組み込みWebサーバーに置かないよう定期的にリマインドを行い、このような見えないサービスを狙うキャンペーンを監視してください。Microsoft IIS、Apache HTTP、nginxなどのコアテクノロジーに重大な問題がある場合は、それを一般に通知するプロセスを整え、ISP、ホスティングおよびクラウドプロバイダと連携して、被害の拡大を抑えてください。重要な通信インフラに危険なポートやサービス、特にHTTP/HTTPS上のルーター管理インターフェースの露出がないかを積極的に確認するプログラムが必要です。

結論

最初に、この世の終わりなどではないのだということを言っておきます。ここで報告したサービスはすべて乱雑な状態にあり、私たち人類が、サービスのメンテナンスと設定の安全性について、しっかり対処できていないということは確かです。しかし、それでも皆さま、そしてご家族が、日々*問題なく*Facebook、Twitter、Instagram、TikTokなどを使えていると思います。また、ここ1か月で行ったオンラインバンキングやオンライン決済も、セキュリティを心配することなく行い、直接知らなかったとしても、無数のSaaSアプリケーションを使用していたはずです。インターネット全体に、本質的な脆弱性が深く根付いているにもかかわらず、それは可能だったのです。

もちろん、悪いことも起こり得ます。DoS攻撃は1日に2万3,000件（16分に1回）[135]、脆弱性が露出されたサイトへのMagecart Javascriptの注入[136]、そしてEternalBlueベースの悪用は、WannaCryから数年たった今でもまだ流行したままです。[137]このような混乱が、（消費者やサイト訪問者、また運営側や企業の双方で）被害者にさまざまなレベルの苦痛をもたらしていることは確かです。それでも、 ほとんどのユーザーにとって 、インターネットは進化を続けていくものなのです。

現状維持が良いと言っているのではありません。まったく違います。しかし私たちは、地球温暖化の現実的な危険性を警告し続けている環境科学者や、マスクや社会的距離を求める医療専門家と同じような気持ちでいます。例えると、ビートは違っても、同じドラムを叩いているのと同じです。世界のインターネットを今まで通り扱い続ければ、遅かれ早かれシステマティックな災害にたどり着きます。現在は、理想的な状況ではないにしろ、悲惨な状況と言う訳ではありません。そしてサービスをどのように設計、開発、展開かを少し変えるだけで、インターネット全体の安定性、安全性、そしてセキュリティに非常に大きな好影響を与えることができます。

インターネット上に外部公開する場合は、以下を守ってください。

- **意図的な露出：**何かの手違いと言うのではなく、意図的に露出をすると言うことです。
- **適切な設定：**安全な設定で、必要なタスクのみを行うよう設計してください。
- **定期的なパッチ処理：**最新バージョンを維持し、特に重大な脆弱性が認識された場合は、努力を惜しまず取り組んでください。また、デフォルトのパッケージリポジトリが更新を止めた場合でも、すべてのパッチバージョンを引き出せるように努めてください。
- **注意深い監視：**自身そして組織、そしてインターネットの攻撃面を増やしたのであれば、本質的に、これらのエンティティの防御に対して貢献する責任があります。
- **攻撃されているという仮定：**サービスを探しているのはリサーチャーだけではありません。攻撃者は私たちのように倫理的および法的制限に縛られていないので、より細かく探し、意のままに攻撃します。無害なユースケースに示された方法を使っていながら、サービスは無害なインタラクションしか受けないと想定してはいけません。

イノベーションや実験をすべきではないという訳ではありません。**攻撃的が存在しているインターネットであることを想定した上で、**是非とも全く新しいプロトコルやサービスを発明し、リリースしてください。攻撃や失敗を予想し、そのようなことを補うサービスは、今後のインターネットで成功するでしょう。結局は、どのようなサービスを展開しても、賢く機知に富み、容赦のない攻撃者に支配されるかもしれないのです。ですから、それを忘れずに設計してください。

[135] <https://www.netscout.com/theatreport>

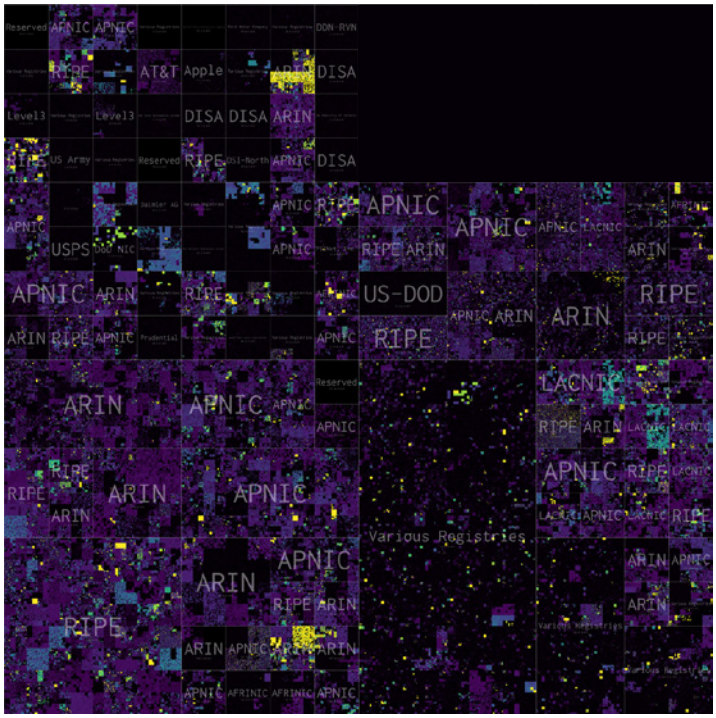
[136] <https://securityaffairs.co/wordpress/92899/cyber-crime/fbi-cisa-e-skiming-atacks.html>

[137] <https://www.darkreading.com/vulnerabilities---threats/eternalblue-longevity-underscores-patching-problem/d/d-id/1337233>

付録A：インターネットの測定

インターネットは1960代の誕生以来、無秩序に、そして爆発的に成長してきました。[138]1,000個目のノードがインターネットに接続された1987年、私は18歳でした。2020年、インターネットは50歳以上となり、インターネット上で Webサーバー、ファイル共有サイト、ストリーミングビデオサービス、ターミナルコンソール、そしてネットワークデータを送信する機能を備えたものなど、何らかのサービスを提供しているアクティブノードを3億3,008万7,843件みつけることができました。もしコンピュータサーバーの1つ1つがインターネットのサイバーマシン共和国の国民だったとしたら、世界で4番目に人口の多い国になります。

最も基本的なレベルで、インターネットは、異なるネットワークでホストされるマシンに到達するための対応およびルーティングシステムである、インターネットプロトコル、つまりIPで動作します。ということは、「インターネット」になるには、ノードやリソースは、「IPアドレス」を通したアナウンスのリンガフランカで到達可能であるべきだと納得できます。以下は、すべての4バイトのIPv4アドレスの全個体数を表したものです。それぞれのピクセルが255件の個体アドレスを示し、そのうちいくつのノードがスキャンに対応したかを、色で表しています。全部で2^32、つまり約42億件のアドレスがあると考えられます。



ご覧の通り、2^32ビットスペースにあるすべてのアドレスが、接続にオープンではありません。第1に、黒い大きな長方形は、リザーブされた非パブリックアドレスを表しています。このような、例えば10.1.1.1や192.168.0.1などのアドレスをローカルネットワーク上で見るかも知れませんが、通常はインターネット上で直接アクセスはできません。その他の暗いエリアは、個体が存在しない、プローブに応答しない、またはスキャニングを辞退したネットワークのブロックリストに載っているということになります（それに付いては、以下の「**測定方法とツール**」で詳しく説明します）。このようなスキャンができないエリアを除き、インターネットは人口の多い地域では非常に高密度になっており、それはこれまで以上に急速に変化しています。

測定方法とツール

インターネットの構成を把握するために、テレメトリを収集することは、簡単な作業ではありません。前述の通り、IPv4インターネットには42億件のアドレスがあり、そのうち37億件がパブリックインターネットに割り当てられています[139]。過去20年間、ネットワーキングの進歩とともにコンピューティング能力は高まり、以前は不可能であった、インターネットの正確な状況把握が、5分以内にできるできるようになりました[140]。クラウドコンピューティングなどのダイナミズムを取り入れた新技術も合わせることで、高速スキャニングは、広大で変化の激しいインターネットを、できるだけ正確に理解するうえで必要なだけなく、非常に重要なものとなりました。つまり、複数のサービスを持ったIpv4アドレスが、次回も同じ姿であるという保証はないのです。実際に、Rapid7の内部調査（Heisenbergハニーポットに関連した）では、IPv4アドレスのリース、わずか数秒以内にクライアントや性質が変わることもあるということが分かりました。

IPアドレススペースについて話すうえで、ここで少し時間を取って、新たに[141]拡大しているインターネットのアドレッシングとルーティングスキームであるIPv6に感謝の意を表しましょう。IPv4の2^{32}スペースとは異なり、IPv6には2^{128}のアドレスがあります。面白いので数にしてみると、まだ想像ができるIPv4の40億という数字に対し、IPv6のアドレス数は、340,282,366,938,463,463,374,607,431,768,211,456件です。桁が大きすぎて、フォーマットをきれいにするためにフォントサイズを減らさなければなりませんでした。それをまずしっかり頭に入れてください（といっても無理なことなので、あまり気にしないでください）。

[138] RFC1は大昔の1969年、UCLAのSteve Crockerが発行しました。インターネットを発明した人は誰かと聞かれたら、それはCrockerです。この知識をクイズチャレンジで生かしてください。

[139] https://ja.wikipedia.org/wiki/IPv4によると、プライベートネットワーキング、マルチキャストアドレス、その他のプライベート用途のためにリザーブされているアドレスは、5億,9,270万8,864件あるそうです。例えば、127/8ブロックにある合計約1,680万件の全てのアドレスが、ローカルループバック用です。何てもったいないのでしょう。

[140] <https://www.usenix.org/conference/woot14/workshop-program/presentation/adrian>

[141] IPv6の仕様は、25年近く前のものなので、もう「新しい」とはいえません。

しかしGoogleによると[142]、本レポート作成時点で、クライアントによるIPv6アドレスの採用率は、約31%で（これにはIpv4とIpv6両方からアドレスできる物理的なシステムもカウントされています）、ほぼすべてのIpv6が、現在Ipv4ネットワークでもアクセスできます。そのため、IPv6に注目するのは間違いなく重要ですが、IPv4でアドレス可能なインターネットが「インターネットのほぼすべて」だと仮定するのが合理的です。Sonarには見えない、完全に別のIpv6サーバーサイドインターネットがどこかに存在するとは思えません。

アクティブスキャニングの課題を説明したところで、次はパッシブなインターネットのテレメトリ収集について少しお話します。パッシブコレクションでは通常、インターネット上のコンピューターに座って、リスニングを行います。本当にそれだけです。現在、インターネット上にあるデバイスのほぼすべてがこれをしていて、nike.comを削除するというプロキシリクエスト（本当のことです）や、TCP/22のSSHに対するブルートフォース攻撃の試みなど、あらゆるナンセンスを寄せつけているのです。信じられないという方は、Webサーバーのログをチェックして見てください。パッシブ収集の専門的な形態がハニーポットです。これは、デバイスを意図的にインターネット上に設置し、誰かや何かを攻撃したりプローブしたりするように誘い、通常なら追跡できないような、深い動きをトラップするものです。その結果、悪用した後の行動を理解したり、マルウェアのサンプルを捕えて後に分析したり、また、手放したダイナミッククラウドIPがセンシティブなアプリケーションメッセージを受け取らないように削除し忘れるなど、コンピューティング基盤でよくある、悪意のないエラーを理解したりすることで、多くの情報を得ることができました。

最後に、アクティブおよびパッシブな手段でテレメトリを取得した後は、インターネット全体の様相や、全般的な状況や特徴をさらに理解するために、それをさらに豊かなものにする方法が必要です。IPアドレスが、Windows ME（でないことを願いますが）など特定のOSをホストしているのが判断できるというのは、デバイスの種類や過去の傾向から想定できるリスクを理解するうえで重要なことです。[143]

Sonarについて

Rapid7は2013年から、アクティブインターネットスキャニングのProject Sonarを実施しています。Project Sonarは、IPv4アドレススペース、またフォワード（FDNS）とリバース（RDNS）DNSレコードを測定するために作成されました。[144]今日のIPスキャンアクティビティは、完全にIPv4ベースのサービスに注目していますが、採用数が増え続けていることから、今後はIPv6への対応も検討しています。

Rapid7 Labsチームが「調査」と呼ぶプロジェクトSonarスキャンは、定期的なインターバルを空けて実施されます。しかし、このインターバルの長さは、調査の種類によって異なります。例え、Rapid7は2週間ごとにさまざまなポートのHTTPスキャンを行いますが、FDNSとRDNSは毎週実施します。これは、かなり多くのデータ量となります。これまでに集めたデータすべてを併せたら、優にペタバイトの範囲に達します。最も規模の大きい調査の1つであるHTTP/80は、通常約50～60GBで、1つのzipファイルに圧縮されています。解凍された調査結果は、各行にIpv4アドレススペースのサーバーのインタラクションから受け取った、それぞれ異なる応答が含まれています。

Project SonarにモニターされるIPv4アドレスの量は、Rapid7が導入しているブロックリストによってさらに縮小されます。私たちはこのブロックリストにより、インバウンドメールから特定のIPアドレス幅をスキャンしないように要求された場合、それに従います。このブロックリストには、約2,000～3,000万件 のIPv4アドレスがあります。これは少ないですが、重要です。

Project Sonarのスキャンは、カリフォルニア州サンディエゴとロンドンのデータセンターで行います。複数の場所からスキャンすることで、インターネットのさまざまな「視点」からテレメトリを取得でき、また複数のホストでスキャンロードのバランスを取ることで、収集の効率性を高められます。Rapid7 Labsは現在、これらのデータセンターで、インターネットのさまざまな視点を定期的に分析していませんが、これは今後検討していく領域です。

ここで是非お伝えしたいのは、Project Sonarで集めた膨大なデータは、オープンデータのWebサイトに掲載されており、教育、研究、または実践（個人または企業のセキュリティに）のユースケースに合わせて、無料でご利用して頂けるということです。[145]

---

[142] <https://www.google.com/intl/en/ipv6/statistics.html>

[143] <https://www.cvedetails.com/top-50-products.php>

[144] フォワードDNSは、親しみやすい名前をIPアドレスに翻訳するシステムで、リバースDNSはその逆です。例えば、「www.rapid7.com」は、フォワードでは52.85.146.50（現時点）にリゾルブされ、一方、52.85.146.50のリバースリゾリューションは、「server-52-85-146-50.iad89.r.cloudfront.net」となります。最近では、FDNSは一般的に、IPアドレスに「誰がいるか」、そしてRDNSはそのIPアドレスが「どこ」にあるかを示します。

[145] <https://opendata.rapid7.com/>

Heisenbergについて

Project Heisenbergは、Rapid7が世界中に展開するハニーポットのネットワークで、各地域の脅威インテリジェンスを入手し、インターネットの状況を把握するためのものです。前述の通り、このハニーネットは、インターネット上で、ネットワーク内の各ハニーポットに対する不要な攻撃をリスニングします。ここで検知された攻撃は集約され、Rapid7がそれを受け取り、濃縮して分析します。Rapid7は、5大陸に120件のハニーポットを展開しています。

Heisenbergハニーネットの重要な要素の1つは、攻撃者にばれないように、ハニーポットとしての身分を隠し続けることです。そのため、その展開方法はすべて公開されておらず、本レポートからも除外されています。しかしながら、Heisenbergはブルートフォース攻撃、悪用の試み、プロキシトラフィック、に使用される認証情報や、他の隣接するインフラの設定ミスによる情報漏洩を常に捕まえています。

Recogについて

Recogが、パズルの最後のピースです。Recogは、オープンソースのフィンガープリントデータベースで[146]、インターネットスキャン中に収集された認識プロトコル情報（バナー、バージョンストリングやその他のテクニカルなヒント）を、正規化されたオペレーティングシステム、ソフトウェア、ハードウェア、およびサービスフィンガープリントに切り替えるのに使用できます。Recogは、Rapid7初期のNexpose（現在はInsightVMとして知られる）からスピンアウトしました。RecogはRapid7のInsightVMとMetasploit製品に使用されており、現在でもインターネットの構成を特定および分類するうえで重要な情報源の1つです。

Recogはさまざまなプロトコルとプロトコル応答に対応しています。例えば、HTTPの返信には、ヘッダ、クッキー、さらにHTTPボディタイトルのタグを、いくつかの種類のフィンガープリントに切り替えることができます。さらに具体的に説明します。「Server」ヘッダが`Microsoft/IIS 6.0`の値で戻ってきた場合、`IIS 6.0`が、そのHTTPサービスを実行している[147]ホストで動作しているということに加え、そのホストが古いオペレーティングシステムであるWindows 2003を実行しているということが推測できるということです。このような知識により、観察している世界のインフラに関連するリスクを予想したり、時には直接特定したりすることが可能になるのです。

[146] <https://github.com/rapid7/recog>

[147] <https://github.com/rapid7/recog/blob/master/xml/http_servers.xml#L176>

付録B：方法論

考え方は人それぞれですし、もしかしたら実際に試したことがあるかも知れませんが、インターネットを測定するというのは*難しい*ことです。まずその前に、 Rapid7 Labs のいう「インターネットの測定」とは何を意味するのでしょうか。本レポートの構成要素に関しては、「測定」とは、「日時や検出対象によって異なる、 ある特定の期間（通常は30〜240分）に、プロトコルXを使ったリクエストに積極的に応答 する、すべてのインターネットIPv4エンドポイントを、数値化すること」という定義になります。私たちはまず、すべてのIPV4スペースに対してプローブを実行し、ZMapを使用して特定のポートでリスニングしている「何か」があるかを確認します。[148]その後、最初のプローブに応答したノードに対し、プロトコルレベルのリクエストを実行します。

これがインベントリの全てだと信じたいですが、そうではありません。これは、インターネットに接続されているノードの超母集団のサンプルです。なぜこれがすべてではないのでしょうか。それは、生態系の研究で、科学者が特定の森林地域で全てのリスの数を数えようとするとき、一定のブロックエリアを調べるのと同じことです。どのようなデバイスを使っていたとしても、間違いなく全てのリスを数えることはしていません。しかし、統計的に利用できるサンプル数は獲得できます。

同様に、インターネットもある意味、自然林のようにダイナミックなものです。インターネットには定期的に落ちるポーションがあります。[149]クラウドは組織が迅速にプロビジョニングやでプロビジョニングを行えるようにします。これらの多くはインターネットで観察でき、また多くのISPは、寿命の短いIPv4のDHCP割り当てを使用し続けています。さらに、SMBなど危険が伴うサービスでは、ISPは多くの場合、それらのリソースへのアクセスをブロックするために、政府機関を連携します。最後に、Rapid7 はオプトアウト要求を受け入れるので（巨大なIpv4のヒートマップから分かるように）、そのブロック内にあるものは把握できません。

この点は、私たちのも含め、どのようなインターネットのスキャンデータでも、それを基にして決定的な結論を出すことに対する、注意喚起として書いています。レポート全体で、四捨五入や推定値が見られるのは、この理由からです。LabsチームはSonar調査の有効性を確保するため努力していますが、もしある国（やイベント）がスキャン実行中にインターネットを閉鎖すると決めたら、何もできません。

特に言及されていない限り、すべての測定は2020年の世界的なコロナウイルスパンデミック後の「ニューノーマル（今の時点で）」における測定を実施するため、2020年4月のSonar調査をベースとしています。

私たちがこのサービスを提供する理由

過去に行った「National Exposure Index（NEI）」[150]をご存じの方は、今回の調査内容が大きく違うことに気付くでしょう。なかでも最も目立つは、プロトコルのスキャンを完全に使用していることです。過去のNEI調査では、便利ではあるものの、特定のプロトコルエクスポージャーについて正確な状況が把握できない、単純なSYNスキャンを使用しました。ユーザーは、利用できるTCPとUDPポートすべてに、あらゆる種類のネットワークサービスを貼り付けることができます。フルプロトコルスキャンの結果に切り替えることで、それら特定のサービスの状況を正確に把握し、 Recogフィンガープリントを使い、またこれらのフィンガープリントを適用するのに当該サービスが十分な情報を露出した場合には、 サービスのエクスポージャーの関連性や深刻度を見積もるのに使える、豊富な情報が提供されます。

NEIシリーズは、nmapの統計的なサービスエンカウンター頻度を頼りにしています。[151]NICERでは、調査チームはエクスポージャーの状況を把握し、2020年に重要だと思われる領域をハイライトするため、中心的で重要、かつ俗に一般的なサービスで利用できる地図帳/レファレンスを作成したいと考えました。これは、Sonarが定期的に調査していることを網羅するリストでも、最も重要なサービスの全容でもありません。しかしながら、重要性とユーザビリティのバランスは取れていると私たちは考えています（つまり、レポートは既に包括的だが長く、これ以上長くすることが必ずしも改善にはつながらないということです）。

[146] <https://github.com/rapid7/recog>

[147] <https://github.com/rapid7/recog/blob/master/xml/http_servers.xml#L176>

[148] <https://github.com/zmap/zmap>

[149] <https://map.internetintel.oracle.com/>

[150] <https://www.rapid7.com/ja/info/national-exposure-index/>

[151] <https://svn.nmap.org/nmap/nmap-services>

国に注目した理由

否が応でも、国レベルの自律システムやCIDR割り当ては、一般的なIPv4エンティティ解決の中で、今でも最も正確です。一方、米国や英国などの主要産業国が、近代的インフラがそれほど整っていない国と比べ、国別IPv4の属性精度が高い（85～92%）ことから、この方法は決して完璧なものではありません。[152]私たちはすべての国および地域レベルのエンティティ解決にMaxMind[153]を使用しています。

さまざまなセクションでも述べましたが、民間のサイバーセキュリティ会社と政府機関が連携することで、インターネットの安全性が向上し、またそうあるべきだと私たちは考えます。つまり、管轄区域のエクスポージャー状況を把握することで、担当者はより良いガイダンスを作成し、完全な教育、モニタリングおよび警告プログラムを設けて、安全性を守るという使命を果たすことができるようになります。

クラウドに注目した理由

クラウド環境に移るミッションクリティカルなビジネスワークロードが増えて続けています。この理由は、すでに「クラウド」のメリットを宣伝する広告で何度も聞いているでしょうから、ここでわざわざ数値化することは省略します。AmazonやMicrosoftなどプロバイダがそれぞれ、100万件を超えるIPv4で顧客ベースを露出するサービスを持っていることから、調査チームは、調査対象のサービスのどの部分がクラウド環境から来ているのかを調べることは重要だと考えました。クラウドプロバイダは、IPv4割り当て容量、検出された使用量、そして本物の業務用途（趣味用途に対して）の観点からの関連性を基に選定しました。

可能な限り、プロバイダが提供している公式リストを使用し、プロビジョニングされた自律システムから得た既存のマッピングで補強しました。私たちは完全性を追求しましたが、クラウドスペースであっても、IPv4エンティティのマッピングは正確な科学とはなりません。

ランキング方法

ランキングというのは、ある時点で、個人や組織の考えが他のことより重要であるという人間の偏見が入るため、難しいことです。「*SMBを露出するのは、DNSを露出することよりも、はるかに危険で無責任である*」（これはNICERランキングに組み込まれた事実です）というのが良い例です。全てのエクスポージャーが平等に作られているわけではなく、前回のNEI調査では、私たちも専門的な偏見や「意見」を押し付けました。NICERランキングの主な違いは、私たちも深刻な脆弱性に関するデータを持っているということです。これはランキングされたエンティティ全ての、各サービスの数と深刻性の両方に当てはまります。

[152] これらの地域での正確性は65%かそれ以下かも知れません。

[153] <https://www.maxmind.com/ja/home>

付録C：MITRE ATT&CK サービスマッピング

レポートの各サービスセクションには、防御者に攻撃のコンテキストを提供する、「攻撃者の視点」があります。ここでは各サービスに関連するMIRE ATT&CK[154]の戦術マッピングを収集し、これらのATT&CKテクニックに関連付けられる検知方法を導入することで、コンテキストを強化し、（組織内の検知技術がATT&CKマッピングに対応しているという前提で）これらのサービスに対する攻撃者のアクションを特定するための道を提供します。

本レポートにあるサービスと戦術フェーズは、各テクニック内でグループ化され、略称で説明されています。皆さまは、説明の詳細と、MITRE ATT&CKのメインWebサイトにある、組織に合ったサービスに関連する緩和戦略を読んでください。

サービス	テクニック	説明	存在する場所 戦術フェーズ
RDP	一般的に使用されているポート（T1043）	攻撃者は、ファイヤーウォールやネットワーク検知システムをバイパスするため、よく使用されているポートを通して通信し、通常のネットワーク活動に混ることで、細かい検査を避けることがあります。 ポートに関連付けられたプロトコルや、まったく異なるプロトコルを使います。	コマンドアンドコントロール
DNS	カスタムコマンドアンドコントロールプロトコル（T1094）	攻撃者は、コマンドやデータを既存の標準アプリケーション層プロトコルでカプセル化する代わりに、カスタムコマンドアンドコントロールプロトコルを使って通信する場合があります。実装には、よく知られたプロトコルの模倣や、TIP、IPまたはその他の標準ネットワークスタックが提供する基本的なプロトコルに加え、カスタムプロトコルの開発（rawソケットを含む）があります。	コマンドアンドコントロール
DNS	データ隠蔽（T1320）	特定の種類のトラフィック（例：DNSトンネリング、ヘッダインジェクション）は、ユーザー定義が許されています。このようなフィールドは、データを隠すのに使うことができます。ネットワークプロトコル内でデータを隠すだけでなく、イメージやその他のファイル形式にデータを隠す、ステガノグラフィテクニックも使えます。特定の署名がすでに知られていなければ、検知は困難です。	
DNS	DNSポイズニング（T1382）	DNS（キャッシュ）ポイズニングは、インターネットアドレスを、他の不正なアドレスに置き換えることで、インターネットサーバーのドメインネームシステムテーブルを破損します。ウェブユーザーがそのアドレスでページを探すと、リクエストはテーブル内の不正なエントリから、別のアドレスへとリダイレクトされます。	
DNS	DNSCalc（T1324）	DNS Calcは、IPアドレスのオクテットを、最初のDNSリクエストからコマンドアンドコントロールサーバーのポートを割り出すのに使うというテクニックです。	
DNS	ダイナミックDNS（T1311）	ダイナミックDNSは、DNSシステム内の名前を、自動的に更新する仕組みです。プロバイダは、このホスト名への迅速なIP設定をサービスとして提供します。	

[154] MITRE ATT&CK <https://attack.mitre.org/>

サービス	テクニック	説明	存在する場所 戦術フェーズ
DNS	エンドポイントDenial of Service (T1499)	攻撃者は、ユーザーに対するサービスの可用性を悪化させる、またはブロックするために、エンドポイントDenial-of-Service (DoS) 攻撃を実行することがあります。エンドポイントDoSは、該当するサービスがホストされているシステムリソースを使い切る、またはシステムを悪用して、クラッシュ状態を持続させることで、実行されます。 エンドポイントDoSはは、サービスへのアクセスを提供するのに使用されるネットワークを飽和させることなく、サービスを使えなくします。 DoS攻撃は、インターネット全体に広がる1つまたは複数のシステムで生成されることから、一般的に分散型DoS (DDoS) と呼ばれます。 エンドポイントリソースに対するDoS攻撃を実行するには、IPアドレススプーフィングやボットネットなど、複数の方法にいくつかの要素を適用します。 攻撃者は、攻撃システム特有のIPアドレスを使うか、ソースのIPアドレスをスプーフィングして、攻撃トラフィックを攻撃システムにトレースバックするのを困難にしたり、反射を有効にしたりします。これで、ネットワーク防御デバイスのソースアドレスによるフィルタリング効果を弱めるか排除され、防御側が攻撃に対抗することがさらに困難になります。 ボットネットは、ネットワークやサービスに対するDDoS攻撃で広く使用されます。大規模なボットネットは、世界中のインターネットに広がるシステムから、かなりの量のトラフィックを生成できます。攻撃者は、独自のボットネットインフラを構築・コントロールするリソースを持っているか、または既存のボットネットをレンタルして、攻撃を行います。DDoSの最も酷いケースの中には、リクエストを生成するのに多くのシステムを使い、各システムが少量のトラフィックを送るだけで、ターゲットのリソースを使い切るのに十分な量になるというものもあります。このような状況では、正当なクライアントとDDoSトラフィックを区別することが、非常に困難になります。	インパクト
DNS FTP FTPS SMB SMTP	代替プロトコルを介した漏出 (T1048)	データ漏出が、メインのコマンドとプロトコルまたはチャネルと異なるプロトコルで実行されます。データは大体、メインコのコマンドアンドコントロールサーバーから、別のネットワークロケーションに送られます。代替プロトコルには、FTP、SMTP、HTTP/S、DNS、SMB、またはメインのコマンドアンドコントロールチャネルで使用されていないネットワークプロトコルがあります。異なるチャネルには、クラウドストレージなどのインターネットWebサービスがあります。 攻撃者は、さまざまなオペレーティングシステムユーティリティを利用し、代替プロトコルを介してデータを持ち出します。	漏出
POP3 POP3S SMTP SMTPS	コマンドアンドコントロールチャンネルを介した漏出 (T1041)	コマンドアンドコントロールチャンネルを介してデータ漏出が実行されます。データは、コマンドアンドコントロール通信と同じプロトコルを使って、通常の通信チャネルにエンコードされます。	漏出

サービス	テクニック	説明	存在する場所 戦術フェーズ
Redis	クライアント実行の悪用（T1203）	予期しない行動を引き起こす可能性のある、不安定なコーディングプラクティスが原因で、ソフトウェアに脆弱性が発生することがあります。攻撃者は、任意コードを実行するため、標的型搾取を通して特定の脆弱性を悪用できます。多くの場合、攻撃的なツールキットに最も価値のあるエクスプロイトは、リモートシステムのコード取得に利用できるものです。そこから、システムへのアクセスを獲得できるからです。ユーザーは、業務上で良く使うアプリケーションに関連するファイルを想定しているため、利便性が高いことから、エクスプロイトのリサーチと開発にとって有用なターゲットとなります。	実行
MySQL RDP	リモートサービスの悪用（T1210）	ソフトウェアの脆弱性が悪用されるのは、攻撃者がプログラム、サービスまたはオペレーティングシステムソフトウェアまたはカーネル自体のプログラミングエラーを利用して、攻撃者制御コードを実行するときです。侵入後のリモートサービス悪用に共通する目的は、リモートシステムへのアクセス可能にする、横移動です。 攻撃者は、リモートシステムが脆弱な状態にあるかどうかを判断する必要があります。これはネットワークサービススキャンや、その他、ネットワークに配置されている一般的で脆弱なソフトウェア、脆弱性を示す特定のパッチの欠如、または遠隔での悪用を検知・封鎖するためのセキュリティソフトウェアを探すディスカバリーメソッドなどを通して行われます。サーバーは、横移動の悪用にとって価値の高いターゲットです。しかし、エンドポイントシステムも、メリットや追加リソースへのアクセスを提供する場合、リスクに晒されます。	横移動
Citrix	外部リモートサービス（T1133）	VPN、Citrix、およびその他のアクセスメカニズムなどのリモートサービスでは、ユーザーは外部ロケーションから、内部エンタープライズネットワークリソースに接続できます。これらのサービスにはよく、接続と認証を管理するリモートサービスゲートウェイがあります。Windows Remote Managementなどのサービスは、外部にも使用できます。 攻撃者は最初にリモートサービスを利用してアクセスを獲得し、その後ネットワーク内に残ります。通常、正当なアカウントにアクセスしてサービスを利用することが要件ですが、認証ファーミングを通じて取得するか、またはエンタープライズネットワークに侵入してユーザーからの認証情報を入手できます。リモートサービスへのアクセスは、操作中の冗長アクセスの一部として使用されます。	初期アクセス 持続性
SMB	強制認証（T1187）	Server Message Block（SMB）プロトコルは、一般的にWindowsネットワークで、認証、またはリソースへのアクセスおよびファイル共有のためのシステム間通信に使用されます。WindowsシステムがSMBリソースに接続しようとすると、自動的に認証を試み、ユーザーの認証情報をリモートシステムに送ります。	クレデンシャルアクセス

サービス	テクニック	説明	存在する場所 戦術フェーズ
DNS memcached NTP	ネットワークDenial of Service（T1498）	攻撃者は、ユーザーに対する標的のリソースの可用性を低下またはブロックするために、ネットワークDenial-of-Service（DoS）攻撃を実行します。ネットワークDoSを実行するには、ネットワークが依存する帯域幅を使い切ります。リソースの例には、特定のWebサイト、メールサービス、DNS、NTP、およびウェブベースのアプリケーションがあります。 **リフレクション・アンプ攻撃** 攻撃者は、反射を利用して攻撃トラフィックを増幅できます。このタイプのネットワークDoSは、特定のスプーフドソースIPアドレスをホストし、それに応答するサードパーティサーバーの仲介を利用します。このサードパーティサーバーは一般的に、リフレクターと呼ばれています。攻撃者は、被害者のスプーフドアドレスを含むパケットをリフレクターに送ることで、リフレクション攻撃を実行します。ダイレクトネットワークフラッド同様、この攻撃は複数のシステムやボットネットを使用します。同様に、ターゲットにトラフィックを集中させるため、複数のリフレクターを使用します。 反射攻撃はよく、リクエストより応答が多いプロトコルを利用して、トラフィックを増幅させます。これは、一般的にリフレクション（アンプ）攻撃と呼ばれます。攻撃者は、アンプに送られたリクエスト数よりも攻撃トラフィックの量を何桁分も増やします。どれだけ増加させるかは、対象のプロトコル、使用されるテクニック、そして攻撃ボリュームで実際に増幅を生成するアンプサーバーなど、多くの変数によって変わります。リフレクション・アンプフラッドを可能にした2つの主なプロトコルは、DNSとNTPです。	インパクト
SMB	Network Share Discovery（T1135）	ネットワークにはよく、共有ネットワークドライブとフォルダがあり、ユーザーはネットワーク全体でさまざまなシステム上のファイルディレクトリにアクセスできます。 攻撃者は、コレクションの先駆者として情報収集するソースを見つけ、また横移動に有益となる可能性のあるシステムを特定するため、リモートシステムで共有されたフォルダやドライブを探します。 クラウド仮想ネットワークには、システムへのアクセスを得た攻撃者がアクセスできる、リモートネットワーク共有やファイルストアサービスがある場合があります。例えば、AWS、GCP、およびAzureは、エンドポイントまたはクラウド型システムにマッピングされた、Network File System（NFS）共有とServer Message Block（SMB）共有の作成に対応しています。	検出
SSH	プライベートキー（T1145）	プライベートの暗号キーと証明書は、認証、暗号化および解読、そしてデジタル署名に使用されます。 攻撃者は、侵入されたシステムからjプライベーをキーを集め、SSHのようなリモートサービスの認証や、メールなどの収集されたファイルの解読に使用します。	クレデンシャルアクセス
RDP	冗長アクセス（T1108）	攻撃者は複数のリモートアクセスツールを、さまざまなコマンドアンドコントロールプロトコル認証されたやリモートサービスへのアクセスで利用し、アクセスメカニズムが検知または緩和された場合でもアクセスを維持できるようにします。 1種類のツールが検知やブロック、または応答として削除された場合でも、組織が攻撃者のツールやアクセスを完全に把握していなければ、攻撃者はネットワークへのアクセスを維持できます。攻撃者はまた、外部VPNなどの外部リモートサービスを利用するために有効なアカウントへのアクセスを獲得し、ターゲットネットワーク内に設置されたリモートアクセスツールが中断されても、アクセスを維持できるようにします。	持続性 防御回避

サービス	テクニック	説明	存在する場所 戦術フェーズ
RDP VNC	リモートアクセスツール（T1219）	攻撃者は、TeamViewer、Go2Assist、LogMein、AmmyyAdminなどの、正当なデスクトップサポートやリモートソフトウェアを利用し、ターゲットシステムへの対話型のコマンドアンドコントロールチャネルをネットワーク内に確立できます。これらのサービスは一般的に、正当な技術サポートソフトウェアとして使用されており、ターゲット環境内でホワイトリストが適用される場合もあります。VNC、Ammy、TeamViewerなどのリモートアクセスツールは、攻撃者がよく使う正当なソフトウェアよりも頻繁に使用されます。	コマンドアンドコントロール
RDP VNC	リモートデスクトッププロトコル（T1076）	リモートデスクトップは、オペレーティングシステムによくある機能です。ユーザーがリモートシステムで、システムデスクトップグラフィカルユーザーインターフェースとの対話型セッションにログインできるようにするものです。Microsoftは、Remote Desktop Protocol（RDP）の実装を、Remote Desktop Services（RDS）と呼びます。RDSと同様に、リモートサービスへのグラフィカルアクセスを提供する、実装およびサードパーティツールは他にもあります。 攻撃者は、RDP/RDSを介してリモートシステムに接続し、サービスが有効化されて既知の認証情報を持つアカウントへのアクセスが許された場合、アクセスを拡大することができます。攻撃者はおそらく、RDPで使用する認証情報を取得するために、認証アクセステクニックを使用します。また、持続性を高めるために、RDPをアクセシビリティ機能のテクニックと併用することがあります。	横移動
FTP FTPS rsync SMB	Remote File Copy（T1105）	操作中、攻撃用ツールやその他のファイルを実行するため、ファイルを1つのシステムから別のシステムにコピーすることができます。コマンドアンドコントロールチャネルを通して、攻撃者がコントロールする外部システムからファイルをコピーし、FTPなど別のツールを使って代替プロトコルを通し、被害者のネットワークにツールを持ち込みます。ファイルは、MacやLinux上でも、scp、rsync、sftpなどのネイティブツールでコピーできます。	横移動 コマンドアンドコントロール
SSH Telnet VNC	リモートサービス（T1021）	攻撃者は有効なアカウントを使って、Telnet、SSH、VNCなど、リモート接続のみを受け入れるように設定されたサービスにログインできます。攻撃者は、ログオンしたユーザーとして、アクションを実行できます。	横移動

サービス	テクニック	説明	存在する場所 戦術フェーズ
MS SQL	サーバーソフトウェアコンポーネント（T1505）	攻撃者は、サーバーアプリケーションの、正当なExtensible Development機能を乱用して、システムへの継続的なアクセスを確立できます。エンタープライズサーバーアプリケーションには、アプリケーション開発者がソフトウェアの書き込みやインストールして、メインアプリケーションの機能性を拡張できるようにする機能があります。攻撃者は、悪意のあるソフトウェアコンポーネントをインストールして、サーバーアプリケーションを乱用します。 SQLに保存されたプロシージャは、頻繁に使用されるSQLクエリをユーザーが書き直すという手間を省けるよう、保存および再利用できるコードになっています。保存されたプロシージャは、プロシージャ名を使うか、特定のイベント（例：SQLサーバーのアプリケーションが起動または再起動されたときなど）を通して、呼び出すことができます。攻撃者は、SQLデータベースサーバーに持続的なメカニズムを提供できる、悪意のあるストアドプロシージャを作成することができます。SQL構文からオペレーティングシステムコマンドを実行するには、攻撃者は追加機能を有効化する必要があります。 Microsoft SQL Serverは、共通言語ランタイム（CLR）統合を有効にできます。CLR統合が有効になっている場合、アプリケーション開発者は任意のNETフレームワーク言語（VB、NET、Cなど）を使用して、ストアドプロシージャを書き込むことができます。攻撃者は、ストアドプロシージャにリンクされているCLRアセンブリを作成または変更できます。これらのCLRアセンブリは、任意のコマンドを実行するために作成できます。	持続性
DNS	シャドウDNS（T1340）	実際の所有者に気付かれることなく、悪意のあるサーバーに向けたサブドメインを密かに作成するための、ドメインアカウント認証情報を収集するプロセスです。	インフラの確立と維持
SSH	SSHハイジャック（T1184）	セキュアシェル（SSH）は、LinuxとmacOSシステムにおけるリモートアクセスの標準的な手段です。ユーザーが、一般的にパスワード、証明書、または非対称の暗号化キーペアを使用して認証する暗号化トンネルを介して、別のシステムに接続できるようにします。 侵入されたホストから横移動するため、攻撃者は、別のシステムへの既存の接続をハイジャックして、アクティブSSHセッションのパブリックキー認証で確立された信頼関係を利用します。これは、SSHエージェント自体に侵入するか、またはエージェントのソケットへのアクセスを入手して行います。攻撃者がルートアクセスを入手出来た場合、SSHセッションは簡単にハイジャックできてしまいます。 SSHハイジャックは、有効なアカウントを使って新たなセッションを作成するのではなく、既存のSSHセッションに注入するという点で、リモートサービスとは異なります。	横移動
DNS HTTPS RDP SMTP SMTPS SSH	標準アプリケーション層プロトコル（T1071）	攻撃者は、HTTP、HTTPS、SMTP、DNSなどの、一般的で標準化されたアプリケーション層プロトコルを使い、検知されないように既存のトラフィックに紛れ込んで通信します。リモートシステムへのコマンドと多くの場合これらのコマンドの結果は、クライアントとサーバー間のプロトコルトラフィックに埋め込まれます。 エンクレーブの内部で発生する接続（プロキシ、ピボットノードや他のノード間のものなど）で一般的に使われるプロトコルは、RPC、SSH、またはRDPです。	コマンドアンドコントロール 漏出

サービス	テクニック	説明	存在する場所 戦術フェーズ
etcd	システム情報ディスカバリー（T1082）	攻撃者は、バージョン、パッチ、ホットフィックス、サービスパック、アーキテクチャなどのオペレーティングシステムとハードウェアに関する詳細情報を入手しようとします。これには、攻撃者がターゲットを完全に感染させたか、または特定のアクションを試すかなどのフォローオン行動を形成するため、自動ディスカバリの際にシステム情報ディスカバリからの情報を使用します。	検出
DNS	システムネットワーク設定ディスカバリー（T1016）	攻撃者はおそらく、アクセスするシステムの設定に関する情報、またはリモートシステムの情報ディスカバリーを通して、詳細を探します。このような情報の収集に使用できるオペレーティングシステム管理ユーティリティがいくつかあります。	検出
VNC	サードパーティーソフトウェア（T1072）	サードパーティーアプリケーションやソフトウェアの展開システムは、管理目的のためにネットワーク環境で使われることがあります（SCCM、VNC、HBSS、Altirisなど）。攻撃者がこれらのシステムへのアクセスを入手した場合、コードが実行できるという可能性があります。 攻撃者は、管理、モニタリング、展開システムや、サードパーティーゲートウェイやジャンプサーバーといったエンタープライズネットワーク内にインストールされた、他のシステムを管理するためのサードパーティシステムのアクセス権と使用権を入手するかも知れません。ネットワーク全体またはエンタープライズ全体のサードパーティへのアクセスにより、攻撃者はそのようなシステムに接続されている全てのシステムへの、リモートコード実行が可能になります。アクセスは、他のシステムへの横移動、情報収集、またはすべてのエンドポイントのハードドライブを削除するなどの特定の動作に利用されます。	実行 横移動
Citrix RDP	有効なアカウント（T1078）	攻撃者は、初期アクセスを獲得するためのソーシャルエンジニアリングを通して、クレデンシャルアクセステクニックを使って特定のユーザーの認証情報を盗むか、偵察プロセスの初期に認証情報をキャプチャすることができます。	初期アクセス 持続性 権限昇格 防御回避

お問い合わせ

research@rapid7.comまでご連絡ください。

RAPID7