

National Exposure Index 2017

日本

2016年に、Rapid7 LabsはNational Exposure Indexを公開しました。National Exposure Indexは、測定から得られた定量的な指標を提供します。これによって、次のような基本的な疑問に答えることができます。最新の暗号化を利用して保護されていないサービスや、あるいは攻撃が増加しているなかで提供するのが適切でないサービスがありますが、インターネット上のリスクの状態はどのようになっているのでしょうか。また、リスクのあるサービスが提供されている国や地域はどこなのでしょう。

Rapid7は、今年も調査を実施しました。インターネットでのパッシブな傍受やアクティブな攻撃によるリスクを明らかにし、リスクのあるサービスに関する年ごとの変化について詳細な情報を提供します。今年は、ランキングを決定するためのアルゴリズムを調整して、国ごとの全体的なリスクをより正確に反映するようにしました。また、スキャンと位置の特定の方法を改善しました。一部のリスクについては、緩和されていることの証拠を示しました。

調査結果の要点

- 最もリスクの高い地域は、ジンバブエ、香港¹、サモア、コンゴ共和国、タジキスタン、ルーマニア、アイルランド、リトアニア、オーストラリア、エストニアでした。国家のリスクについて語るうえでは、サイバー空間における3つの超大国、アメリカ、中国、ロシアについて触れる必要があります。ロシアと中国はリスクの高い国家の上位50か国に含まれていますが、アメリカは、膨大な量のIPv4アドレス空間を所有しているにもかかわらず、比較的リスクが低くなっています。
- 2016年の調査では、最もリスクが高い国家はベルギーでした。IPアドレスで指定可能であり、サービスを公開しているサーバーが多数存在していたことがその一因でしたが、この1年で、そのようなサーバーは25万台減少しました。その結果、ベルギーはリスクの高い国家の上位50か国から外れました。
- 100万以上のエンドポイントで、Microsoft製品とのファイル共有サービス（SMB、TCPポート445）が公開されていました。そのうち800,000エンドポイントはWindowsシステムであることが確認されており²、製品とバージョンは多岐にわたっていました。これらのエンドポイントは、SMBの脆弱性を悪用して拡散する、2017年5月に公開されたランサムウェア、WannaCryの攻撃対象となりました。同じ脆弱性を悪用しようとするアクティビティが大量に発生したため、2017年5月には、SMBのポート・スキャンが17%増加（470万ノードから550万ノード）しました。ポート445をブロックすることで、同様の脅威を緩和できます。
- telnet（ポート23）のポート・スキャンでは、2016年は1,480万ノードが応答しましたが、2017年に応答したノードは1,000万ノードを下回りました。外部から接続できるtelnetサービスが33%減少した主な要因として、次の2つが考えられます。1つは、Miraiボットネットへの対応などのために、インターネット・サービス・プロバイダがポート23を閉じたことです。2つ目は、MiraiやBrickerBotなどのボットネットによって、ノードがオフラインにされたことです。

¹ 香港（中華人民共和国香港特別行政区）は独立国家ではありませんが、IMFの一員です。国家の選択基準については、『National Exposure Index 2017 - 14 June 2017』の「Appendix C: Selected Countries」で詳しく説明しています。

² Rapid7のオープン・ソース・ツール“Recog”を使用：<https://github.com/rapid7/recog>

調査結果は、National Exposure Index 2017 で Rapid7 が考察した 2 つの全体的なテーマに沿ったものでした。まず、インターネットでのリスクの高まりによって、犯罪者などの悪意を持った人々にとって魅力的な環境が整ったほか、意図的ではないデータ侵害の可能性も高まっています。また、ベルギーの例のように、国家的な関与を通じてインターネットでのリスクを減らし、ネットワークの強化とユーザーの保護を行うことができます。国家の安全と商取引に責任を負う各国のインターネット・サービス・プロバイダや政策担当者は、現実のデータに基づく意思決定を行いリスクを低減させるために、今回の調査結果を役立てることができ

日本についての調査結果

日本についての統計情報

国	日本
ランク	155
割り当てられた IPv4 のアドレス空間	203,276,288
使用率 (サーバー)	1.6%
Web の暗号化率	35.5%
シェルの暗号化率	67.8%
クライアントでのメールの暗号化率	44.4%
公開されている SMB の割合	0.1%
公開されているデータベースの割合	0.2%

日本についての調査結果の概要

日本は 2 億以上の IPv4 アドレスを割り当てられています。これは、アメリカと中国に次いで、世界で 3 番目の数字です。Rapid7 の研究者がスキャンを実施したところ、320 万台以上のサーバーが応答しました。National Exposure Index における日本の 155 位という順位は、日本におけるインターネットの優先事項がネットワーク環境の保護につながっていることを反映しています。

日本では、IPv4 空間の大半は、サーバー以外によって使用されています。スキャンの対象となるポートが応答を示すアドレスは、膨大な割り当てのうち 1.6% に過ぎませんでした。これは、攻撃対象領域が非常に小さいことを意味します。この要因として考えられるのは、IPv4 空間を周到に管理していることと、IPv6 の導入に早期から取り組んでいることです。IPv6 は、従来の方法ではスキャンすることがほぼ不可能です。

しかし、実数としては、それでも **25 万台**以上のサーバーが telnet のポート・スキャンに応答しており、**数十万台**のサーバーが SMB と Samba で使用されるポート 445 のスキャンに応答しました。日本の IT 管理者とインターネット・サービス・プロバイダは、特に National Exposure Index 2017 のレポートで概要を説明した最近の出来事に留意して、インターネット上で許可されることと予測されることについて確認するとよいでしょう。

レポートの全文は、<https://www.rapid7.com/national-exposure> からご確認ください。

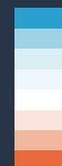


日本は 2 億以上の IPv4 アドレスを割り当てられています。これは、アメリカと中国に次いで、世界で 3 番目の数字です。



Exposure Index の色分類

リスクが最も低い



リスクが最も高い

お問い合わせ

E メール : research@rapid7.com