CYBER
THREAT
ANALYSIS

NORTH KOREA

Recorded Future®

By Insikt Group®

July 18, 2024

制裁下にもかかわらず北朝鮮国民は国外の技術の使用を継続しています

制裁下にもかかわらず、北朝鮮国民は2024年にリリースされたばかりの外国製のデバイスを使用し続けており、
他地域の市場の消費者とほぼ同時期に最新モデルのデバイスを入手している様子が伺えます。

Insikt Groupは、北朝鮮のIP空間と検閲回避のためのプロキシサービスをNetwork Intelligenceで観察しました。これらのプロキシサービスは、一部の北朝鮮人が地元の検閲を回避しようとしている可能性が高いことを示しています。

Insikt GroupはNetwork Intelligenceから、在外北朝鮮人が北朝鮮内の出来事や政策の最新情報を入手するために政権の公式ニュースウェブサイトを訪れる可能性が非常に高いことを観察しました。

エグゼクティブサマリー

北朝鮮の人々は、個人的・業務的使用でインターネットにアクセスするために国外の技術を使用し続けていますが、検閲を回避するための難読化サービスを採用するユーザーが増えているようです。これらの調査結果は、Insikt GroupがRecorded Future Network Intelligenceを通して収集した北朝鮮に関連する最近の分析に基づいており、2017年から2020年にかけての情報に基づく分析からアップデートされた状況を明らかにしています。これらの結果は、北朝鮮が世界の他地域から決して孤立してはおらず、一部のユーザーはソーシャルメディアの閲覧、コンテンツのストリーミング、ビデオゲームのプレイに積極的であることを示しています。最新の分析では、コロナ禍に際し北朝鮮が外国人に対し国境を閉鎖したため、こうした活動が北朝鮮内の個人に関連している可能性が高く、国内でインターネットにアクセスできる外国人訪問者に関連していない可能性が高いことを示す点で特徴的です。

Recorded Futureの調査結果は、北朝鮮の人々がApple、Samsung、Windows、Huaweiのデバイスなど、国外の技術を使用し続けていることを示しています。インターネットにアクセスできる個人は、ソーシャルメディアやビデオゲームを継続的に利用しており、アメリカ、中国、韓国のソーシャルメディアとチャットアプリが混在していることも観察されます。北朝鮮の人々が引き続きVPN（仮想プライベートネットワーク）やプロキシサービスを利用していることを観測しましたが、国内の監視や検閲を避けるために難読化サービスを利用していることが観察されたのは今回が初めてで、政権が認めていないオンライン活動の運用上のセキュリティに対する意識が高まっていることを示しています。VPNやプロキシサービスに加えて、外国製のアンチウイルスと思われる製品も使用されていることが確認されました。また、Insikt Groupは、オンラインでアクセス可能な北朝鮮の国外向けウェブサイトに関連するNetwork Intelligenceのデータを分析し、在外北朝鮮人が定期的に公式ニュースサイトにアクセスしている痕跡を発見し、これらのニュースは外国人だけでなく、在外同国民も対象としていることを示しました。

Recorded Futureの調査結果は、厳しい制裁下にもかかわらず、北朝鮮が国外の技術とソフトウェアを取得し続けていることを示しています。インターネットにアクセスできる一部の北朝鮮人は、世界の他の地域の人々と同様の生活を送っており、最新の携帯電話やゲーム機を使用してソーシャルメディアを閲覧したり、友人と

チャットしたりしています。インターネットを通じた外国の技術やサービスへの継続的なアクセスが、北朝鮮が制裁を回避し、政権として追加収入を得る能力に貢献している可能性が高いと見られます。北朝鮮とのやり取りの接点としては、自社製品が北朝鮮の人々の手に渡っていることを組織が発見したり、インターネットにアクセスできる北朝鮮の人々がオンラインサービスを使用したり、北朝鮮のIT労働者によって開発されたりすることが考えられ、物理的にも仮想的にも接点が存在します。

自社の製品が北朝鮮の人々の手に渡る可能性があると疑われる組織は、購入者およびユーザー、第三者が政権と関係のある制裁対象団体、特にロシアと中国に製品を再販する可能性のある地域の購入者とユーザーに対して適切なデューデリジェンスを実施する必要があります。北朝鮮と関係のある制裁対象企業に製品またはサービスが譲渡された場合、企業は政府機関から罰金などを科せられる可能性もあります。さらに、北朝鮮の手に渡ったデバイスは、脆弱性を分析されてサイバー攻撃に使用されたり、コピーされて国内バージョンの作成に利用されたりする場合があります。北朝鮮で、コロナ禍収束後の国境再開後に中国との貿易関係が再開され、ロシアがウクライナ侵攻を続ける中で武器供給を行う先のロシアとの貿易関係が急拡大していることから、外国の技術の輸入を続ける可能性は非常に高く、これは特に注目すべきと言えるでしょう。北朝鮮が外国の技術を輸入し続けることで、長期的に、北朝鮮の政権に課せられた制裁の効果を低下させる可能性が高くなります。

主な調査結果

- Insikt Groupは、北朝鮮の人々がアメリカのソーシャルメディアサービスやゲーム、中国と日本のメッセンジャーアプリ、アメリカ、ロシア、中国の検索エンジンを使用している痕跡を確認しました。
- Insikt Groupによる以前の調査と同様に、北朝鮮のインターネットユーザーは、韓国標準時（KST）の月曜日から金曜日の午前9:00から午前1:00の間に最も活発的に活動します。
- 制裁下にもかかわらず、北朝鮮のインターネットユーザーは、Apple、Samsung、Huawei、Xiaomi製品などの外国製のデバイスを使用し続けています。
- 最も人気のあるデスクトップOSはWindowsで、観測されたOSの約43%はWindows 8以前であり、一部ではWindows XPも使用されていました。

- Insikt Groupは、北朝鮮のIP空間と検閲を回避するように設計されたサービスを含む35のユニークなVPNまたはプロキシサービス間のイベントをNetwork Intelligenceで観測しました。これは、一部の北朝鮮人が地元の検閲を回避しようとしている可能性が高いことを示しています。
- 在外北朝鮮人は、国内の時事問題や政権の政策的立場について最新情報を入手するために、公式ニュースサイトを訪れる可能性が非常に高いです。
- 北朝鮮が中国やロシアとの貿易関係を継続しているため、制裁下であるにもかかわらず、北朝鮮は外国の技術を取得し続ける可能性が高く、国外からのアクションが将来的に有効である可能性は限定的です。

背景と方法論

北朝鮮のインターネットシステムは世界の他のどのシステムとも異なっています。1990年に設立された北朝鮮のインターネット（イントラネット）は、世界の他の地域が毎日使用している広範なインターネットから完全に分離されています。イントラネットはKwangmyong（광명망）と呼ばれ、完全にプライベートなIPv4ネットワークを使用しています。北朝鮮のネットユーザーはより広範なインターネットにはアクセスできず、より広範なインターネットの側もKwangmyongネットワークにはアクセスできません。

北朝鮮イントラネットの国内人気はますます高まっています。2015年にはイントラネット上に最初のオンラインショッピングモールがオープンし、2021年までに22のショッピングモールのウェブサイトが存在しています。2020年、北朝鮮中央銀行（중앙은행）は電子決済システムを開始しましたが、2021年現在、ユーザーがオンラインショッピングをできるかどうかは不明です。2018年には、北朝鮮人の18〜20%がKwangmyongにアクセスできる携帯電話を持っていたと推測され、2020年には20歳から50歳までの主要都市の北朝鮮人の70%が携帯電話の加入者であると推定されました。Kwangmyongのユーザー数は増加し続けていますが、より広範なインターネットにアクセスできる個人の数は依然非常に少ないままです。

2022年の報告によると、北朝鮮のインターネット普及率は約0.1%と世界で最も低く、2万人のユーザーがいることになります。比較すると、世界の平均インターネット普及率は約65.6%で、隣の韓国のインターネット普及率は97%です。インターネットにアクセスできる選ばれた少数の北朝鮮人でさえ、1時間のインターネット使用の承認取得のプロセスには数日かかります。インターネットでは、英語と中国語のウェブサイトのみを利用できます。金正恩に近い数十の家族だけが無制限のインターネットアクセスが可能と考えられており、国内の外国人は国内のユーザーと分離されています。

Insikt Groupは、2017年、2018年、2020年に北朝鮮のインターネットトラフィックを調査しています。これらの報告は、北朝鮮のインターネットユーザーが、ソーシャルメディアの閲覧、ゲームのプレイ、ビデオのストリーミング、暗号資産の業界に関連する活動など、世界の他の地域の人々がインターネット上で行っているのと同様のことをしている証拠を提供しました。長年にわたり、VPNなどの難読化サービスの使用が増加して

きましたが、これはおそらくユーザー操作のセキュリティ意識の高まりに対応していると考えられます。また、インターネットのトラフィックパターンに基づいて、北朝鮮の個人を受け入れている可能性が高い複数の国も観測されました。

Insikt Groupは、Network Intelligenceデータセットを使用し、北朝鮮のインターネットユーザーの行動に関する最新の分析を実施しました。Recorded Future Network Intelligence分析は、ネットワークを通過するデータの監視と分析から導き出されます。このデータは、攻撃者がサイバー攻撃を構築、ステージング、開始する際に、攻撃者と被害者との間のトラフィックを観察するために使用されます。北朝鮮の場合、このデータのサブセットを使用して、北朝鮮の主要なIP範囲*175.45.176[.]0/24*から発散するイベントを観測することができました。このNetwork Intelligenceは、IP範囲全体のすべての活動の小さなサンプルにすぎませんが、以下で詳細に検討するいくつかの結論を引き出すのに十分なデータがあったと考えています。

この分析を行った理由は2つあります。まず、前回の分析から4年が経過したため、過去4年間での変化、国外での北朝鮮ユーザーの証拠、北朝鮮から発せられる悪意のある活動の兆候など、北朝鮮のインターネット行動に関する最新の理解を求めていたこと。第二に、コロナ禍により、純粋に北朝鮮の人々のインターネットトラフィックを観察するユニークな機会が得られたことです。2020年のコロナ禍後、外国人は出国させられ、2023年後半まで北朝鮮に戻ることが許されず、最初の外国人ツアーグループは2024年2月に到着しました。北朝鮮のインターネット行動に関するこれまでの分析には外国人が含まれていた可能性が非常に高いですが、2023年1月から2024年3月までのNetwork Intelligenceの分析では、北朝鮮に外国人がほとんどまたはまったく存在しない時間枠に焦点を当てています。

技術的分析

活動の傾向

これまでの分析と同様に、北朝鮮の人々のインターネット上の行動は、国外ユーザーの行動を反映したものです。北朝鮮人は、ソーシャルメディアサービスであるFacebook、X（旧Twitter）、Instagram、メッセンジ

ャーアプリのWeChat、LINE、QQ、検索エンジンのYahoo、Baidu、Yandex、Sogouを使用していることが確認されています。北朝鮮の人々がサイバーオペレーション中の偵察のためにこれらのソーシャルネットワークサービスを使用することがあることが判明しています。また、今回の調査結果では、北朝鮮の人々がXboxなどのコンソールゲーム機をプレイしたり、電子商取引サイトを閲覧したり、ポルノを見たりする可能性が非常に高いことも示されています。また、McAfeeのアンチウイルス製品を利用している痕跡も見られ、一部の北朝鮮人がサイバーセキュリティに懸念を抱いていることを示しています。

生活パターン

Insikt Groupは、2023年6月にNetwork Intelligenceを利用してさらに詳しく調査しました。この月を選んだのは、データが比較的一貫していることと、外国人観光客が再び入国できるようになる前だったためで、北朝鮮人のインターネット利用を代表する可能性が高いものです。北朝鮮におけるインターネット活動に関する前回の分析において、2017年には週末に活動がピークに達しましたが、2018年には平日に活動がシフトしました。これは、北朝鮮のインターネットにアクセスできる人々によるインターネットの業務利用が増加した結果と思われます。2023年6月にRecorded FutureのNetwork Intelligenceを使用してまとめられたデータは、2018年に報告された内容と一致しています。2023年6月の活動のピークは月曜日から金曜日で、土曜日と日曜日に活動が著しく減少しました。2018年の活動は、8:00から21:00 （韓国標準時）の間にピークに達しました。同様のパターンが続いていますが、2023年6月のピークは12:00から1:00まで長く続き、2:00に減少し、9:00に再び回復するものでした。このデータは、夜間の活動増加の理由を特定するのに十分となる決定的なものではありませんでしたが、特に政権の収益を生み出す北朝鮮のIT労働者の数が増加しているため、北朝鮮とは別のタイムゾーンに対応するために深夜まで働いている可能性があるものと考えられます。

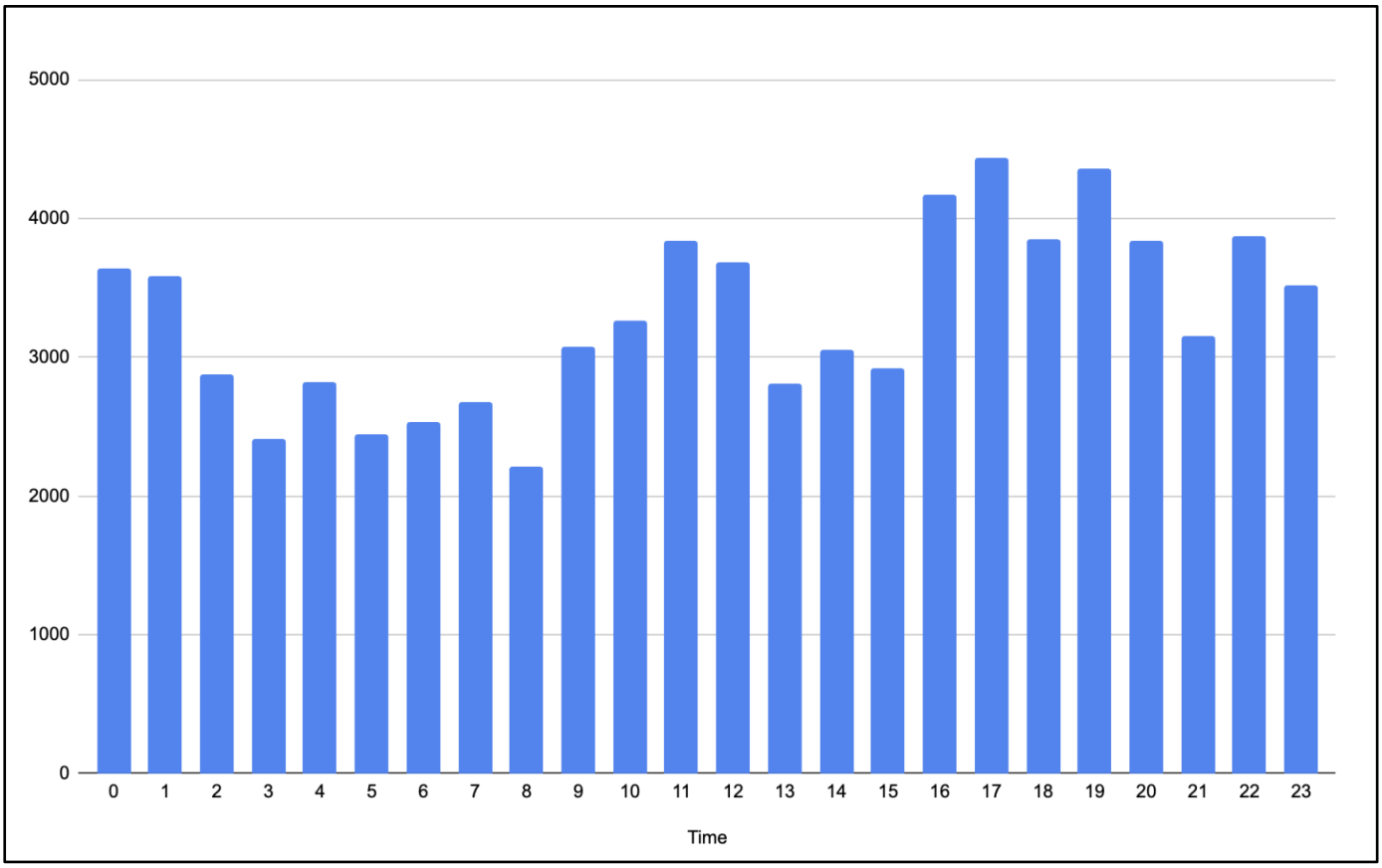

図1：*2023年6月（韓国標準時）の時間別の北朝鮮のインターネット活動の観測結果、Y軸はRecorded Future Network Intelligenceの観測値（出典：Recorded Future）*

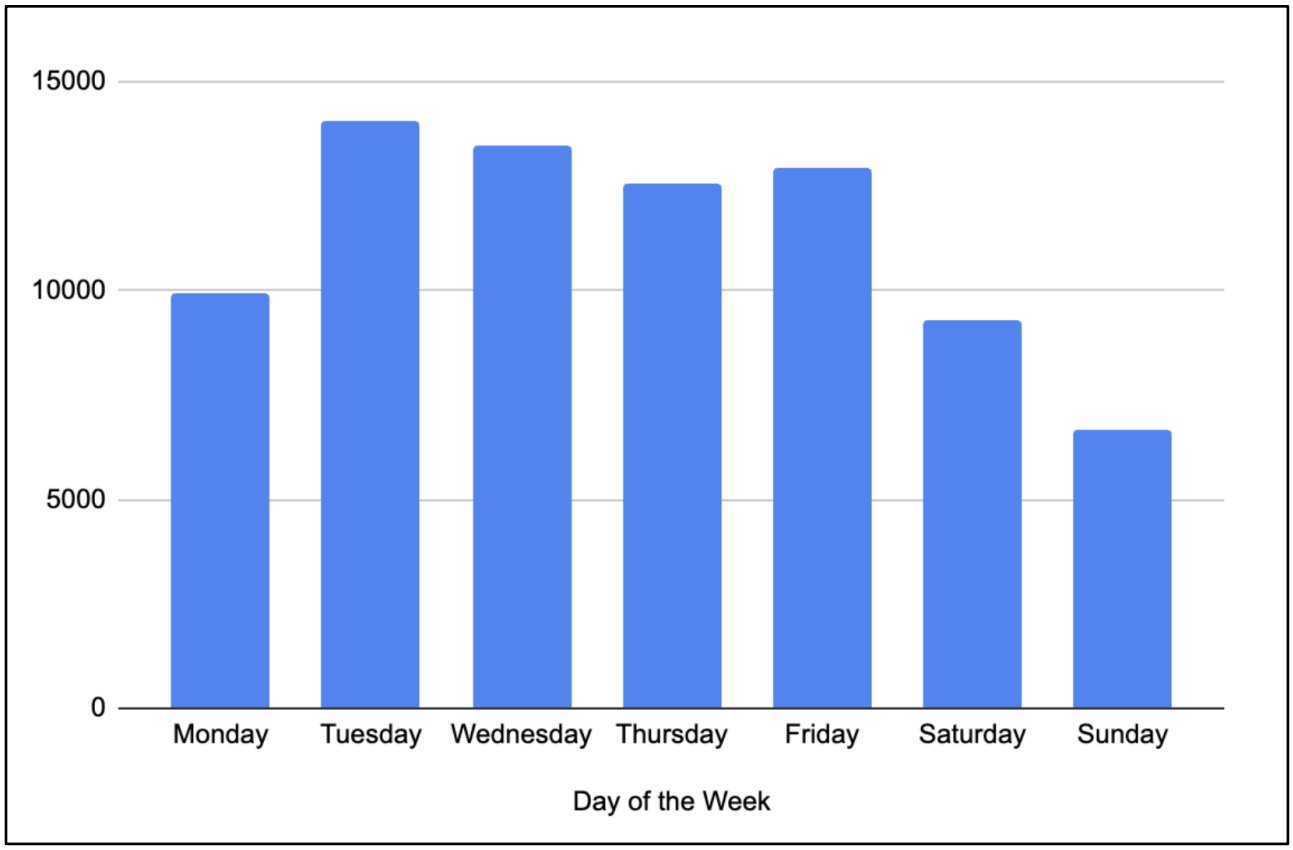

図2：*2023年6月の曜日別の北朝鮮のインターネット活動の観測結果、Y軸はRecorded Future Network Intelligenceの観測値（出典：Recorded Future）*

デバイス

北朝鮮の政権は、大幅に変更された独自のLinux OSディストリビューションRed Star OS、広範な国内モバイルネットワーク（1、2）など、独自のデバイスとソフトウェアを開発しています。しかし、この政権がDellのコンピューターや中国の携帯電話など、国外の技術を輸入していることも判明しています。Recorded Future Network Intelligenceは、デスクトップコンピューターや携帯電話など、北朝鮮国内に輸入されたデバイスの存在を確認しています。Insikt Groupは、北朝鮮ではモバイルデバイスがデスクトップやラップトップコンピューターよりもわずかに多く使用されていることを確認しました。

北朝鮮人は、アメリカの消費者と同様にApple製品を好みます。Appleデバイスは依然として北朝鮮で最も人気のブランドであり、Samsung、Xiaomi、Huaweiがその次に人気の3ブランドとなっています。ただし、すべてのAndroidデバイスブランドを考慮に入れれば、国内にはこれより多くのAndroidユーザーがいます。

2024年1月31日に発売されたSamsung Galaxy S24 Ultraのような最近の携帯電話モデルが観察されました。Recorded Futureの分析の締め切りが2024年3月であることを考慮にいれても、これは一部の北朝鮮人が他の市場の消費者とほぼ同じ速さで最新のデバイスモデルを購入していることを示しています。他のオープンソースの報告も、同政権が中国から外国製のスマートフォンを輸入し続けていることを裏付けています。

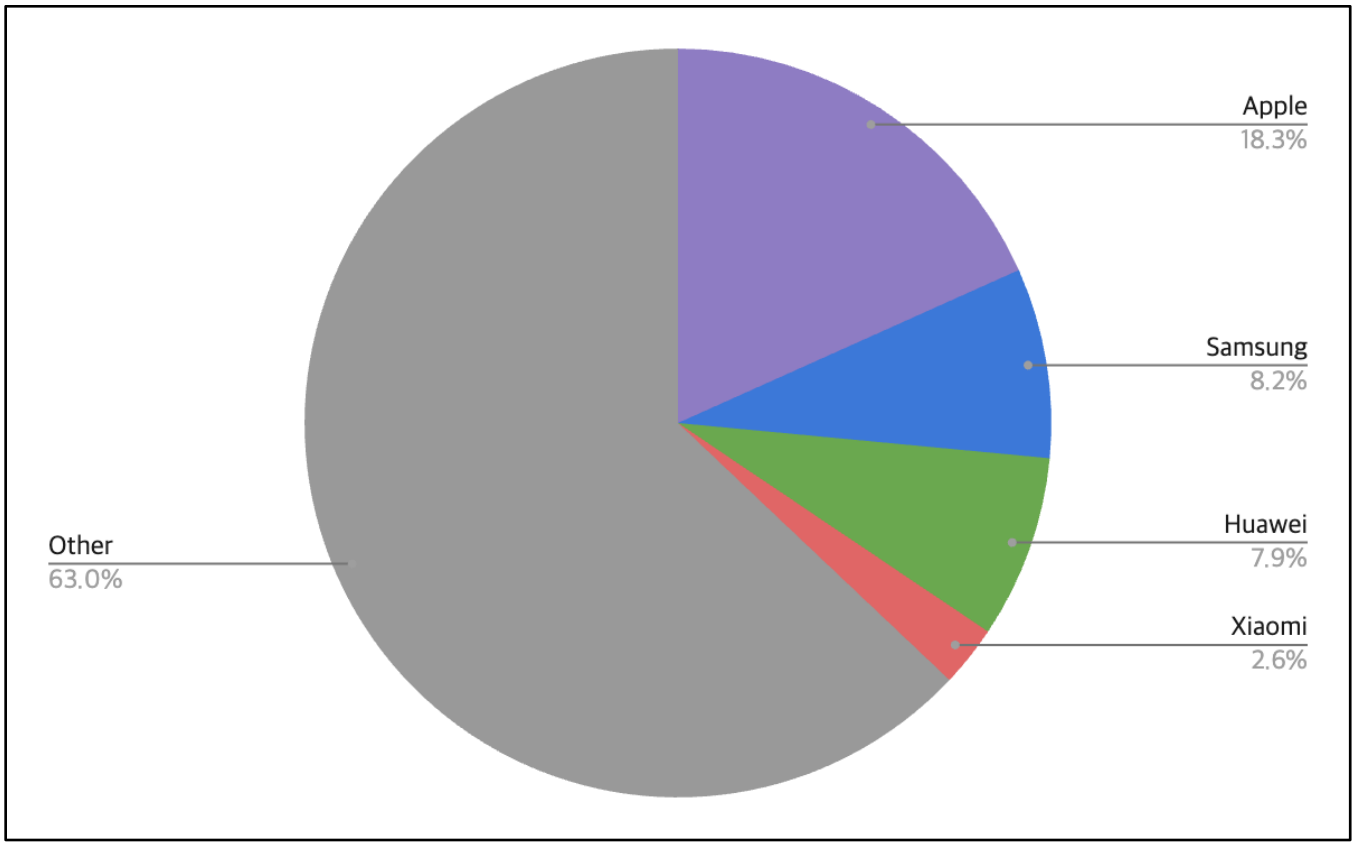

***図3：**北朝鮮で観測されたデバイスメーカーの内訳（出典：Recorded Future）*

Windowsは最も人気のあるデスクトップOSであり、多くの北朝鮮人は定期的にWindowsソフトウェアを更新しています。Windowsデバイスの約57%がWindows10または11で動作していました。ブラウザ開発者はWindowsバージョンでのユーザーエージェントの更新を停止したため、Windows11デバイスはWindows10として表示されます。Windowsデバイスの観測値の残りの43%はWindows 8以前であり、一部の北朝鮮人は未だ、Microsoftが2014年4月に更新とサポートを終了したWindows XPを使用していました。ウェブブラウザについては、ほとんどのFirefoxバージョンが最新でしたが、2017年3月にリリースされた52など、古いFirefoxバージョンのインスタンスがいくつか観察されました。同様に、ほとんどのChromeバージョンは最新でしたが、2016年4月にリリースされた49.0.2623.112など、古いChromeバージョンは比較的少数でした。

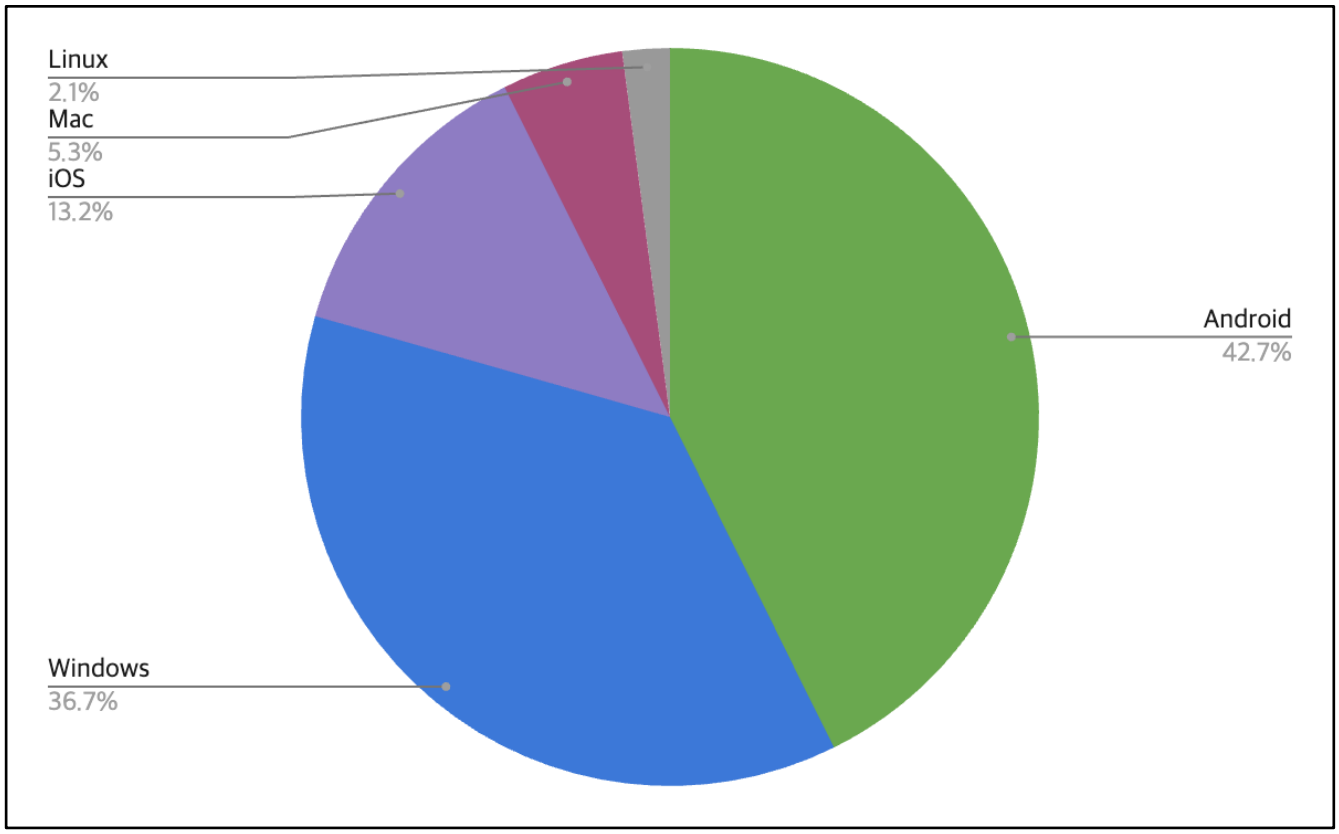

図4：*北朝鮮で観測されたオペレーティングシステムの内訳（出典：北朝鮮）*

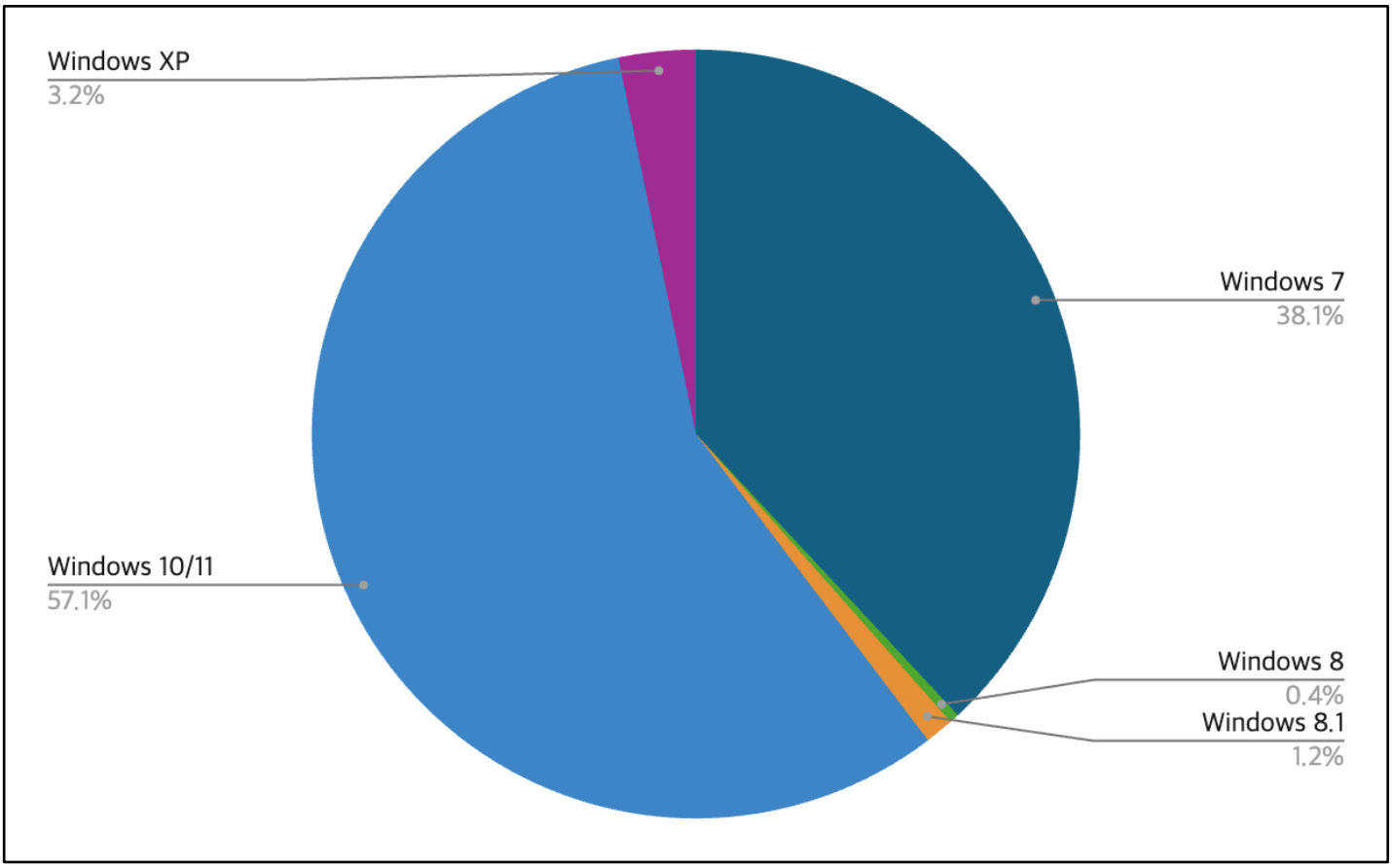

***図5：**北朝鮮で観測されたWindowsバージョンの内訳（出典：北朝鮮）*

VPNおよびプロキシサービス

Insikt Groupは、分析期間中、北朝鮮のIPアドレスとVPNエンドポイントの間で一貫した通信を確認しました。31の一意の北朝鮮のIPアドレスが35の異なるVPNまたはプロキシサービスと通信していることが判明しました。北朝鮮人は圧倒的にHotspot Shieldを使用しており、Express VPN、Private Internet Access（PIA）、Psiphon 3がそれに続きます。Hotspot、Express、PIAは世界中で使用されている一般的なVPNサービスですが、Psiphon 3はインターネットの検閲を回避するために設計されたVPNサービスです。[1]脱北者への以前のインタビューから、北朝鮮の人々はオンラインの監視と検閲を認識しており、積極的にそれを避けようとしてい

[1] *https://s3[.]amazonaws[.]com/0ubz-2q11-gi9y/en[.]html*

ることがわかっています。国内でインターネットにアクセスできる北朝鮮人は、政権による検閲を避けるためにこのサービスを使用している可能性があります。

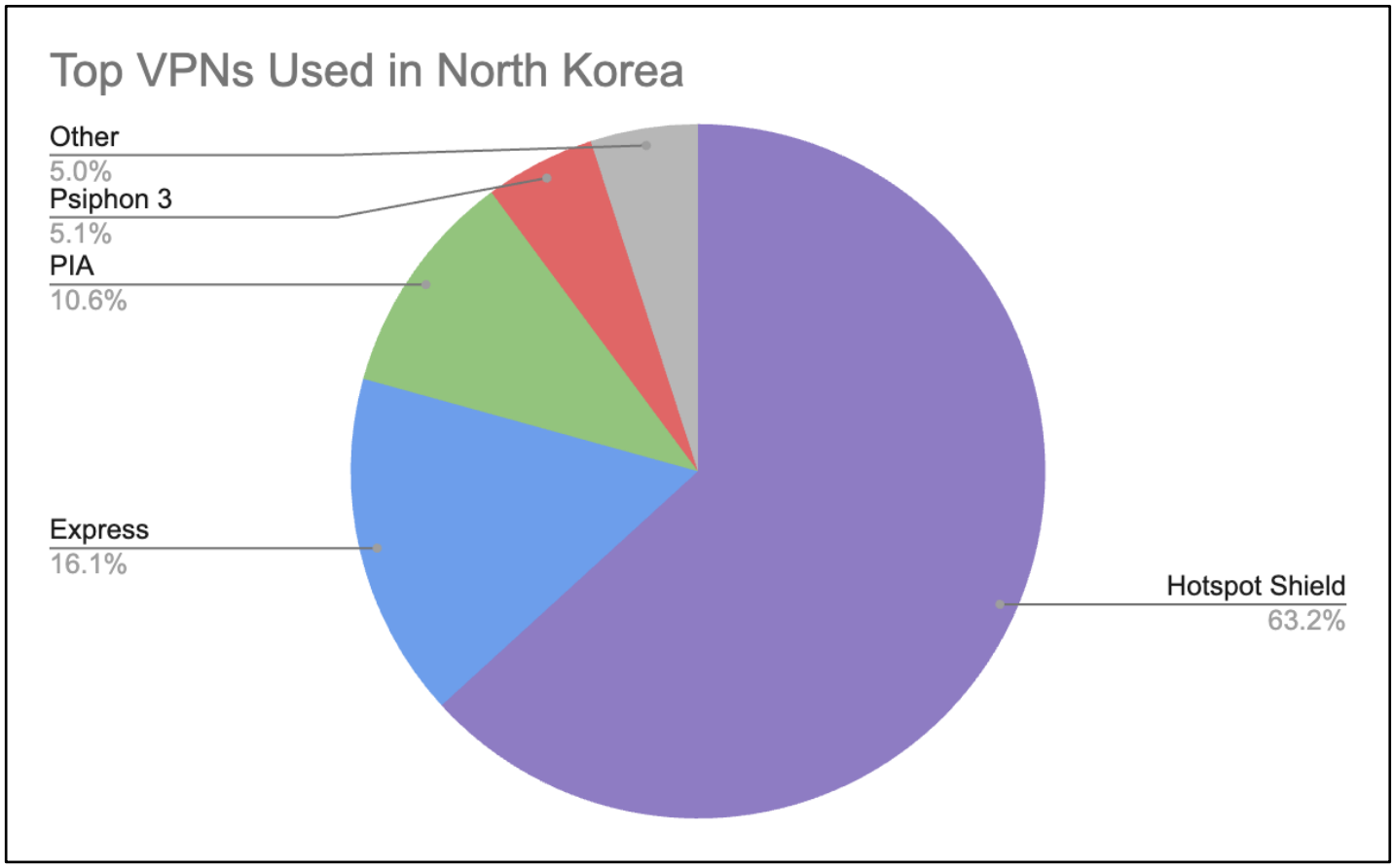

図6：北朝鮮におけるVPN使用の内訳（出典：Recorded Future）

北朝鮮のウェブサイトへの訪問者

Insikt Groupは、オンラインで公開されている北朝鮮のウェブサイトに関連するグローバルなRecorded Future Network Intelligenceも分析しました。下の**図6**に示すように、期間中のトラフィックの半分以上は労働新聞と朝鮮中央通信（KCNA）へのものでした。「Rodong Sinmun」は朝鮮労働党中央委員会の公式新聞で、国内外の視聴者・購読者に朝鮮労働党の視点を提供しています。KCNAは北朝鮮の主要国営通信社で、国内や政府の公式見解から厳しく検閲されたニュースを提供しています。当然のことながら、海外研究者と北朝鮮に関心のある人々の両方がコンテンツを閲覧し、在外北朝鮮人が国内のニュースや政策の立場をチェックしているため、これら2つのウェブサイトは観測されたNetwork Intelligenceの最大のシェアを占めています。

残りのトラフィックは、より広範なインターネットからアクセス可能な他の北朝鮮のウェブサイトへのものでした。

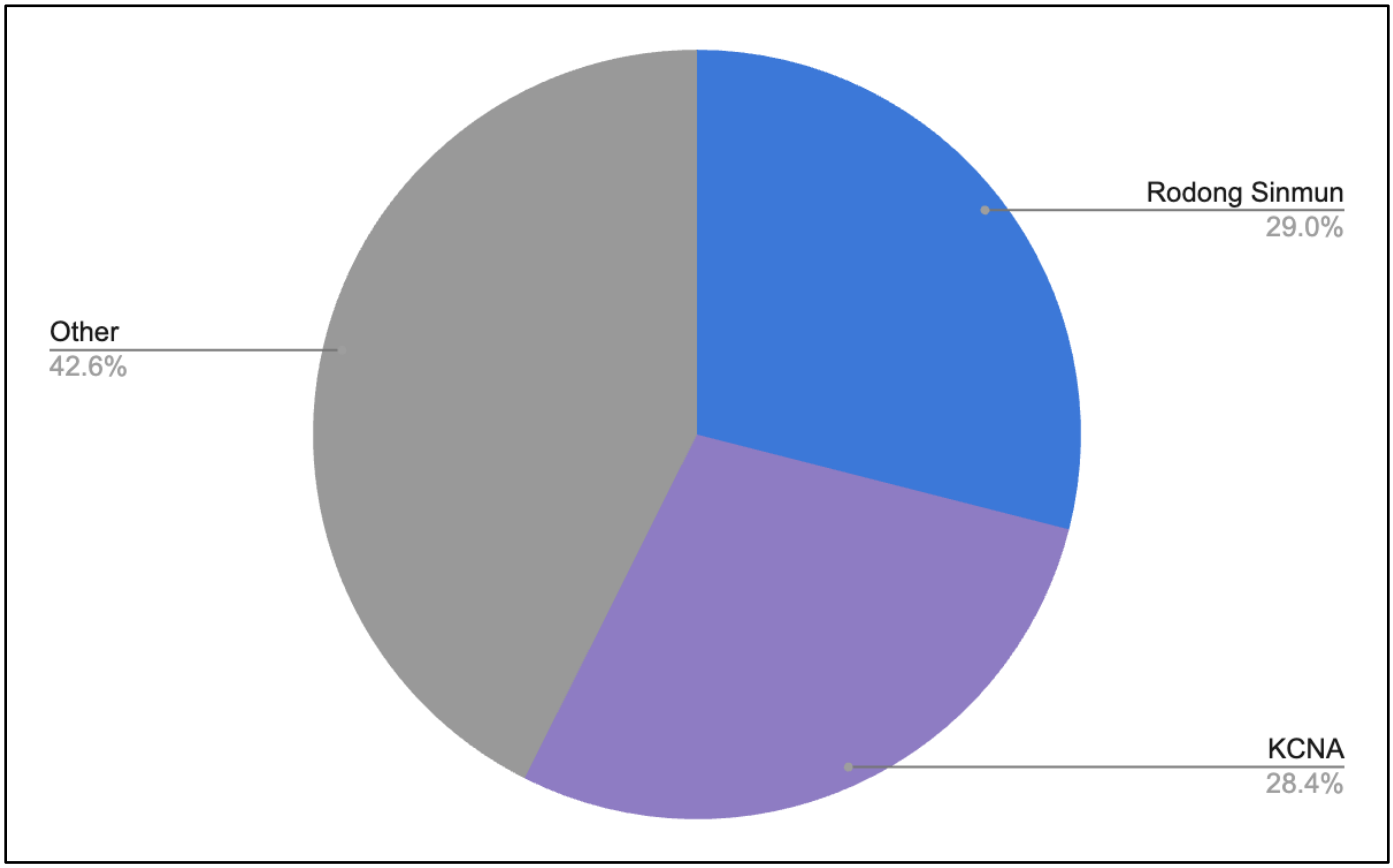

図7：*北朝鮮のウェブサイトへのNetwork Intelligenceの内訳（出典：Recorded Future）*

在外北朝鮮人

上述のように、Network Intelligenceで観測されたのトラフィック一部は、海外の北朝鮮人が政権の最新の公式ニュースや声明にキャッチアップしていることに関連しているとRecorded Futureは評価しています。分析期間中、Network Intelligenceでアフリカ大陸から北朝鮮のウェブサイトへの一貫したトラフィックが観測されました。Insikt Groupは以前、この地域における北朝鮮政権の活動と長年の関係について報告しています。しかし、2023年後半、北朝鮮政府はアフリカ地域の大使館の閉鎖を開始しています。この閉鎖は財政難やアフリカ諸国との関係悪化によるものと推測する人もいます。アフリカから北朝鮮のウェブサイトへのトラフィックに関連するRecorded Future Network Intelligenceは、大使館の閉鎖と相関し、大使館の閉鎖前後にトラ

フィックが著しく減少しています。これらの大使館の北朝鮮人職員は、本国の公式情報源から北朝鮮のニュースを定期的に見ていた可能性が高いと考えられます。

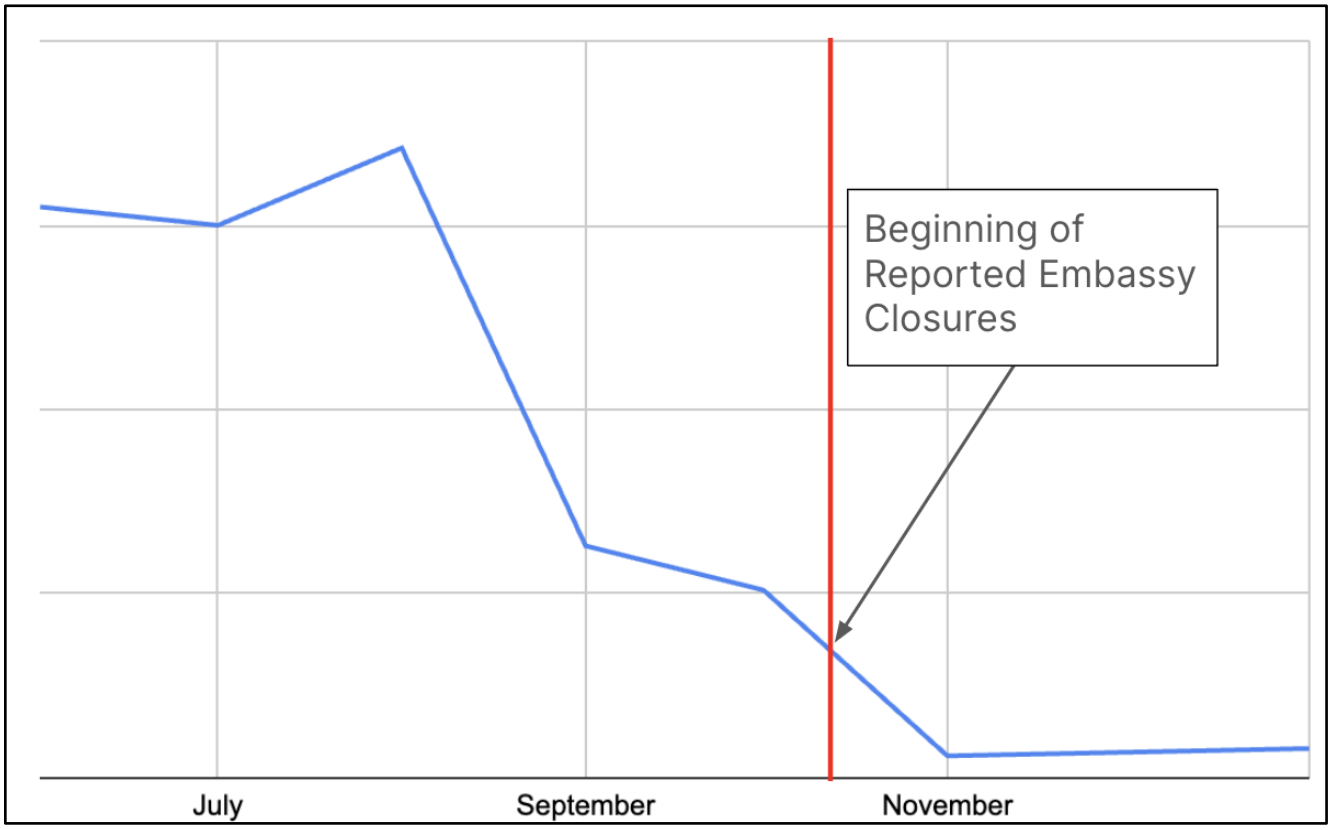

***図8：**2023年にアフリカ地域から北朝鮮のウェブサイトへ観測されたNetwork Intelligence（出典：Recorded Future）*

今後の展望

中国との貿易の継続や、ロシアによるウクライナ侵攻での北朝鮮による武器供給など、最近ではロシアとの貿易関係が急拡大していることから、北朝鮮は制裁下にもかかわらず、国外の技術を取得し、使用し続ける可能性が高いと考えられます。これは、ロシアが2024年5月に北朝鮮に対する制裁を監視する専門家パネル設置を求める国連の命令に拒否権を発動したことから、特に注目すべきでしょう。結果、北朝鮮に対して新たな国際的な制裁が課される可能性は低くなりましたが、各国は同国政権を支援していると疑われる北朝鮮の組織に対して制裁を続けています。このような制裁措置は、制裁対象企業と取引を行う第三者に誤って売却する可能性が高い地域でデューデリジェンスを実施するための財務コストを増加させる可能性があります。自社のデバイスや技術が北朝鮮に輸入されている可能性があると疑われる企業は、購入者に対して適切なデューデリジェンスを実施し、制裁に関する最新情報についてアメリカ外国資産管理局（OFAC）になど相談する必要があります。

世界のインターネットへのより広範なアクセスを持つ北朝鮮人のブラウジング行動は、引き続き他の国の傾向に同様で、平日の勤務時間中に活動がピークに達すると予想されています。さらに、北朝鮮の人々は、国内外で傍受している可能性のある人からオンライン活動を隠すために、VPNやプロキシサービスを使用し続ける可能性があります。最後に、北朝鮮の公式ニュースソースは在外国民にとって重要であり、これらのソースによって作成されたコンテンツは、外国の視聴者だけでなく、国内一般市民にも向けられていることを確認しています。

Recorded　Futureのレポートには、米国インテリジェンスコミュニティー（ICD）203：分析基準（2015年1月2日発行）と一致する可能性のある表現が含まれています。またRecorded Futureのレポートでは、米国インテリジェンスコミュニティーが採用する信頼レベル基準を使用して、分析的判断の裏付けとなる情報源の質と量を評価しています。

*Insikt Group®*について

Recorded Future の脅威研究部門である Insikt Group は、政府、法執行機関、軍、諜報機関に深い経験を持つアナリストとセキュリティ研究者で構成されています。彼らの使命は、クライアントのリスクを軽減し、具体的な成果を実現し、ビジネスの中断を防ぐインテリジェンスを生み出すことです。

*Recorded Future®*について

Recorded Futureは世界最大規模のインテリジェンス企業です。当社のインテリジェンスクラウドは、攻撃者、インフラストラクチャ、標的に関する包括的なインテリジェンスを提供します。オープンウェブ、ダークウェブ、技術ソースにわたってインターネットをインデックス化して、拡大傾向にあるアタックサーフェスと脅威状況をリアルタイムに可視化し、お客様が迅速かつ確信を持ってリスクの軽減と安全なビジネス遂行に取り組めるようにします。ボストン本社および世界各国のオフィスに従業員を擁し、75か国以上で1,800社を超える企業と政府組織と連携して、バイアスのかかっていない実用的なインテリジェンスをリアルタイムで提供しています。

詳細については、recordedfuture.comをご覧ください。