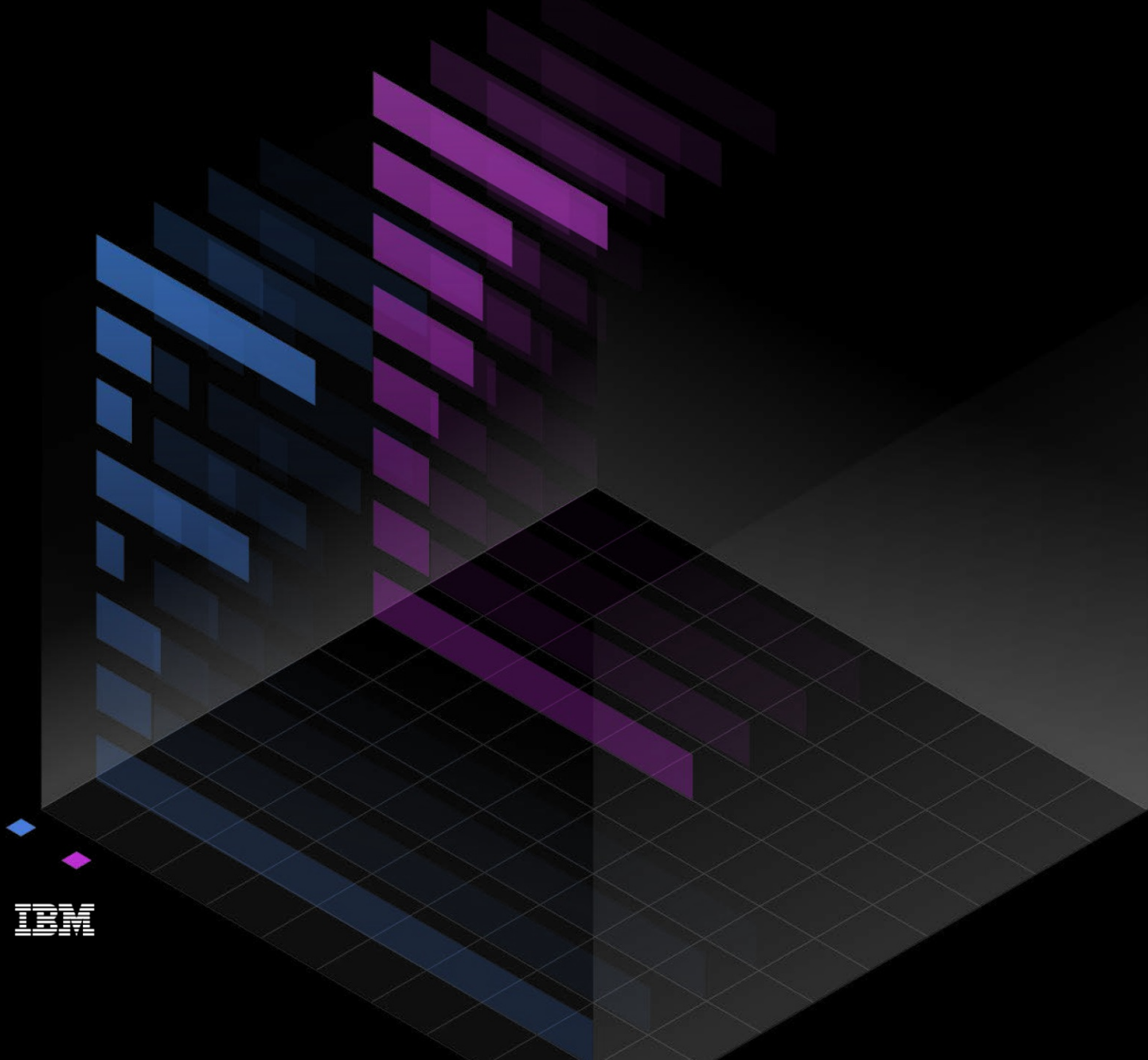
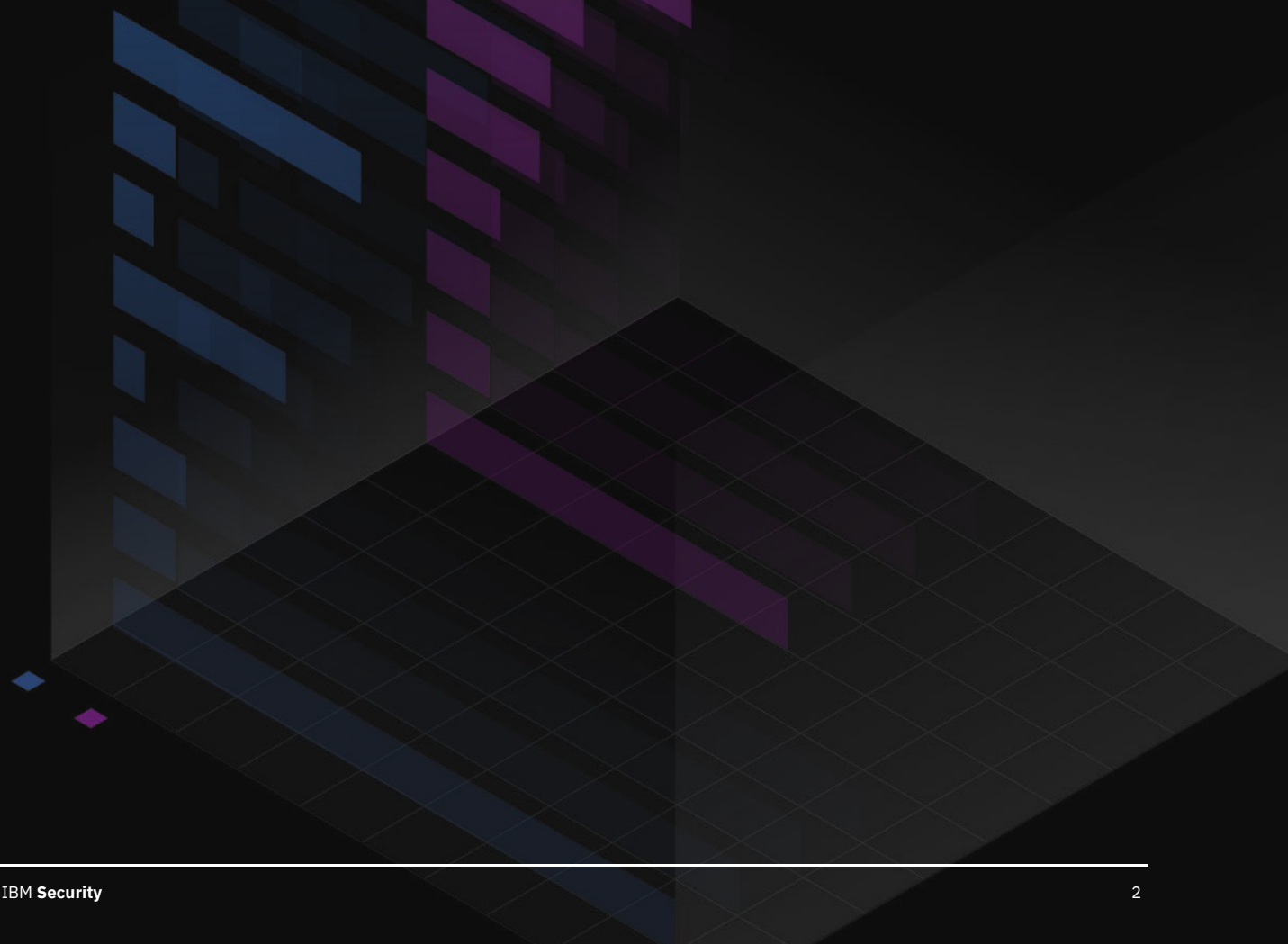
IBM Security

X-Force 脅威インテリジェンス・インデックス 2021



IBM

目次



はじめに

2020 年は間違いなく近年で最も重大な転機をもたらした年、すなわち、世界的なパンデミックや経済の混乱が何百万もの人々の生活に影響を及ぼし、社会的、政治的な不安を増大させた年であったと言えるでしょう。こうした出来事はビジネスにも大きな影響を与え、多くの企業が分散型ワークフォースへと大規模な転換を図った年でもありました。

サイバーの世界においては、2020 年のこの特殊な状況が、サイバー攻撃者に、通信ネットワークの必要性を悪用する機会を与え、さらにサプライチェーンや重要なインフラストラクチャーに豊富な攻撃機会を与えてしまうことにも繋がりました。2020 年は、迅速な対応と修復を必要とする世界的に重大な脅威が検知された一年でもありました。ほとんどの攻撃は、ネットワーク監視ソフトウェアのバックドアを利用して政府や民間団体を攻撃する国家アクターの犯行によるものであり、第三者によるリスク対策の必要性と共に、そのような攻撃を予測することの難しさを浮き彫りにしました。

こうした課題に対応できるように、IBM Security X-Force は、サイバー脅威の全貌を評価し、巧妙化する脅威とそれに関連したリスク、さらにはサイバーセキュリティーの取り組みにどのような優先順位をつけるべきかを、企業にご理解いただけるよう支援しています。お客様に提供する卓越した脅威インテリジェンスに加え、IBM Security X-Force は収集した大量のデータを分析し、脅威の全貌とその変化に関する年間の調査結果である「X-Force 脅威インテリジェンス・インデックス」をリリースしています。

追跡した傾向によると、ランサムウェアの急増が続いており、2020 年に X-Force が対応したセキュリティー・イベントの 23% を占める第 1 位の脅威タイプとなりました。ランサムウェアを使用した攻撃者は、データの暗号化と公開サイトへのデータ・リークの脅威を組み合わせることで、支払いを強要する圧力を強めました。このような策略が成功したことで、2020 年にはある犯罪組織が 1 億 2,300 万ドルを超える利益をランサムウェア攻撃を通して手に入れたと X-Force は推定しています。[1]

2020 年には、製造業に携わる複数の企業が激しいランサムウェア攻撃とその他の攻撃にさらされました。最も頻繁に攻撃対象となった業界の中で、2019 年に第 8 位であった製造業は、2020 年には金融・保険業界に次いで第 2 位になりました。X-Force は、新型コロナウイルス感染症ワクチンのサプライチェーンに関与する製造業や NGO に対して、標的を絞り込んだスピア・フィッシング・キャンペーンを使用した巧妙な技術を持つ攻撃者を検知しました。

1 このレポートでは、コストの総額はすべて米ドルで記載されています。

さらに脅威アクターは、ビジネスに不可欠なクラウド・インフラストラクチャーとデータ・ストレージをサポートするオープンソースコードの Linux を標的としたマルウェアの巧妙化を進めました。2020 年の Intezer による分析では、56 もの新種の Linux マルウェア・ファミリーが検出されており、これは、他の脅威タイプで確認された革新レベルをはるかに上回るものでした。

このような中、2021 年はより良い年になるという希望を抱ける理由があります。トレンドを予測するのは難しいことですが、唯一信頼できるもの、それは変化です。増減するサイバーセキュリティーの問題に直面した際のレジリエンスを高めるためには、アクションに繋がるインテリジェンスと、よりオープンでコネクティッドなセキュリティーの未来に向けた戦略的なビジョンが必要です。

コミュニティーによって強さを生み出すという精神に基づいて、IBM Security は「X-Force 脅威インテリジェンス・インデックス 2021」をここにご案内します。本レポートの調査結果は、セキュリティー・チーム、リスクの専門家、意思決定者、研究者、メディアなどが、過去 1 年間に発生した脅威の状況を把握し、次に起こりうるあらゆる脅威に備えるための手掛かりとなります。

エグゼクティブ・サマリー

IBM Security X-Force は、2020 年の 1 月から 12 月までの間に、IBM のお客様や公的な情報源から収集した数十億件のデータ・ポイントを用いて、攻撃タイプや感染ベクターの分析、グローバルおよび業界別の比較を行いました。以下は、「X-Force 脅威インテリジェンス・インデックス」で発表された主な調査結果です。

23%

ランサムウェアが攻撃に占める割合

ランサムウェアは 2020 年で最もよく使われた攻撃手口であり、IBM Security X-Force が対応し、修復を支援した全インシデントの 23% を占めています。

1 億 2,300 万ドル超

ランサムウェアによる推定最高被害額

X-Force は、2020 年に Sodinokibi (REvil とも呼ばれる) ランサムウェア・アクターが単独で、少なくとも最低 1 億 2,300 万ドルの利益を得て、約 21.6 テラバイトのデータを盗んだと推定しました。

25%

2020 年の第 1 四半期の攻撃に占める最大の脆弱性の割合

脅威アクターは Citrix のパス・トラバーサルの欠陥を利用し、1 - 3 月までの 3 カ月における全攻撃の 25%、および 2020 年全体における攻撃総数の 8% で、この脆弱性を悪用していました。

35%

上位の攻撃手口に占めるスキャンとエクスプロイトの割合

脆弱性のスキャンとエクスプロイトが、2019 年に第 1 位の手口であったフィッシングを上回り、 2020 年の攻撃手口の第 1 位に跳ね上がりました。

第 2 位

最も頻繁に攻撃を受けた業界での製造業の順位

製造業は 2019 年の第 8 位から順位を上げ、2020 年には金融サービスに次いで 2 番目に多く攻撃された業界でした。

5 時間

脅威グループのサーバー上の攻撃用トレーニング動画の長さ
イランの国家アクターの操作ミスによって、X-Force の研究者は誤って設定されたサーバー上にあった約 5 時間の動画を発見し、犯罪者の手のうちを明らかにすることに成功しました。

100 人超

精度が高いフィッシング・キャンペーンの攻撃対象となった経営幹部の人数
X-Force は 2020 年の中頃に、新型コロナウイルス対策において個人用防護具（PPE）を確保するタスク・フォースで管理と調達の役割を担う、100 人を超える上級経営幹部に接触したグローバル・フィッシング・キャンペーンを検知しました。

49%

ICS 関連の脆弱性の増加率、2019-2020
2020 年に検知された産業用制御システム（ICS）関連の脆弱性は、2019 年に比べて 49% 増加しました。

56

新種の Linux マルウェア・ファミリーの数
2020 年に検知された新種の Linux 関連のマルウェア・ファミリーの数は、過去最多の 56 件でした。これは 2019 年から 2020 年に比べて 40% の増加となります。

31%

攻撃に占めるヨーロッパの割合
2020 年に最も頻繁に攻撃対象となったのはヨーロッパで、X-Force が観測した攻撃の 31% が同地域で発生しました。その後に、北アメリカ（27%）とアジア（25%）が続きます。

2020 年に観測された主要な攻撃

2020 年の攻撃の状況を理解することは、セキュリティー・チームによるリソースの優先順位付け、最も発生可能性の高いシナリオの演習、攻撃手法の変化の特定に役立ちます。

以下のセクションで、2020 年に X-Force が観測した主要な攻撃の傾向に関する洞察を紹介します。ランサムウェアは紛れもなく最も頻繁に使われた攻撃手法であり、その次に続く攻撃手法としてかなりの差をつけてデータ窃盗とサーバー・アクセス攻撃が続いています。攻撃手口では、スキャンとエクスプロイトが 2020 年の首位になり、その後にフィッシングと認証情報の窃盗が続きます。[2]

攻撃手法の上位 3 位

1. ランサムウェア (攻撃の 23% を確認)
2. データ窃盗 (2019 年から攻撃が 160% 増加)
3. サーバー・アクセス攻撃 (2019 年から攻撃が 233% 増加)

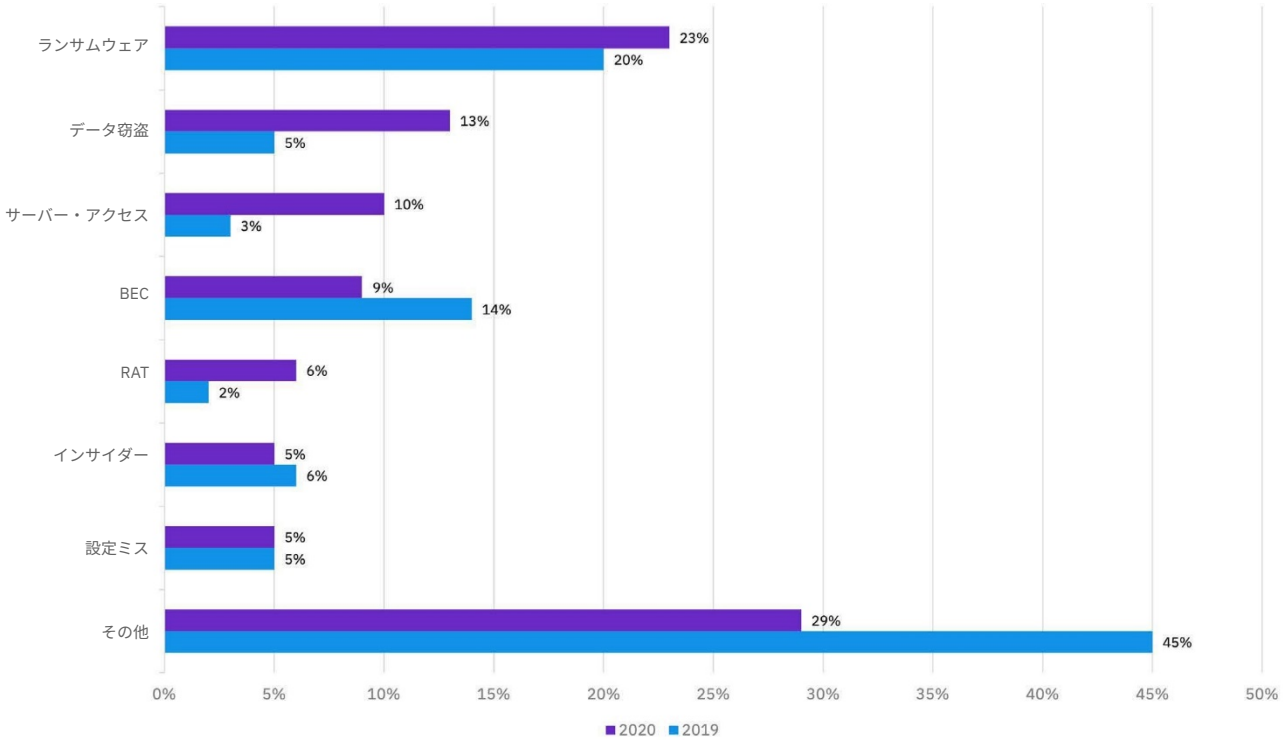
攻撃手口の上位 3 位

1. スキャンとエクスプロイト (攻撃の 35% に関連。2019 年は 30%)
2. フィッシング (攻撃の 33% に関連。2019 年は 31%)
3. 認証情報の窃盗 (攻撃の 18% に関連、2019 年は 29%)

図 1

主要な攻撃手法 (2020 年と 2019 年の比較)

2020 年と 2019 年の攻撃手法の内訳 (観測された全攻撃における比率で表示) (出典: IBM Security X-Force)



2 このレポートでは、「攻撃」と「インシデント」はほとんど同じ意味で使用されています。インシデントとは、攻撃や疑わしい攻撃の調査/修復につながった、X-Force インシデント対応チームへの企業からのホットライン・コールを意味します。

ランサムウェアを悪用したビジネスの急増

ランサムウェア攻撃は、2020 年に X-Force の活動で確認された全インシデントの 23% を占めました。前年の 20% から増加しており、これは、より多くのサイバー犯罪者がランサムウェアは収益性が高いと認識しつつあることを示しています。

脅威アクターは、主にリモート・デスクトップ・プロトコル、認証情報の窃盗、あるいはフィッシングといった攻撃手口を介して被害者の環境へのアクセスを得ることで、ランサムウェア攻撃を実行しました。こうした攻撃手口は、過去にもランサムウェアをインストールするために同じように悪用されていました。

ランサムウェア・アクターは、攻撃チェーンを拡大することで、攻撃をさらに成功させています。2020 年に X-Force が観測したランサムウェア・グループの中で最も成功しているのは、Ransomware as a Service (RaaS) カルテル立ち上げでした。また、攻撃の様々な側面に特化したサイバー犯罪者に、操作の重要な側面をアウトソーシングすることに焦点を当てていました。

X-Force Incident Response のデータによると、ランサムウェア攻撃の 59% で二重の恐喝を用いた戦術が確認できました。企業はバックアップからの復旧を実施することで、身代金の支払いを拒否することもできるため、攻撃者はデータを暗号化してアクセスできない状態にするだけの戦術から新たな戦術にシフトする動きを見せています。攻撃者はデータを盗み、身代金を支払わない場合は機密データを漏えいすると脅迫するようになりました。一部のランサムウェア・プロバイダーは、被害を受けた企業から盗んだ機密情報を販売するためのオークションを、ダーク Web 上で開催したこともありました。

実際、X-Force は、Sodinokibi (REvil とも呼ばれる) ランサムウェア・プロバイダーが、こうした恐喝戦術を用いて 2020 年に少なくとも 1 億 2,300 万ドルの利益を得たと推定しています。
ランサムウェアの開発者は、支払いを強要する手段としてデータ漏えいの脅威を利用することにより、バックアップからの復旧で対処する企業の裏をかく方法を見つけ出しました。

機密データの漏えいによって企業評価が失墜するという脅威は、企業とその顧客に大きな損失をもたらす可能性があり、長時間に及ぶ復旧にかかるコストに加え、訴訟や規制違反による高額の罰金につながる恐れもあります。ランサムウェアを使用した攻撃者がリーク・サイトに機密データを公開した場合、このような漏えいはメディアに取り上げられることが多く、こうした攻撃に関連したさらなる風評被害を招くことになります。公表された漏えいデータを X-Force が分析したところ、2020 年に公表されたデータ漏えいのうち、ランサムウェア関連のデータ漏えいが 36% を占めていました。

最も一般的なランサムウェア・タイプである Sodinokibi

2020 年に X-Force が頻繁に観測したランサムウェア・タイプの上位 2 位は、Sodinokibi (ランサムウェア・インシデントの 22%) と Nefilim (11%) でした。これらは両方とも、データ窃盗とランサムウェア攻撃を組み合わせて使われるものです。

X-Force によって頻繁に観測されたその他のランサムウェア・タイプには、RagnarLocker (7%)、Netwalker (7%)、Maze (7%)、Ryuk (7%)、EKANS (4%) があります。ランサムウェア攻撃の残りの 42% には、Egregor、CLOP、Medusa など、その他の少数のタイプが含まれます。

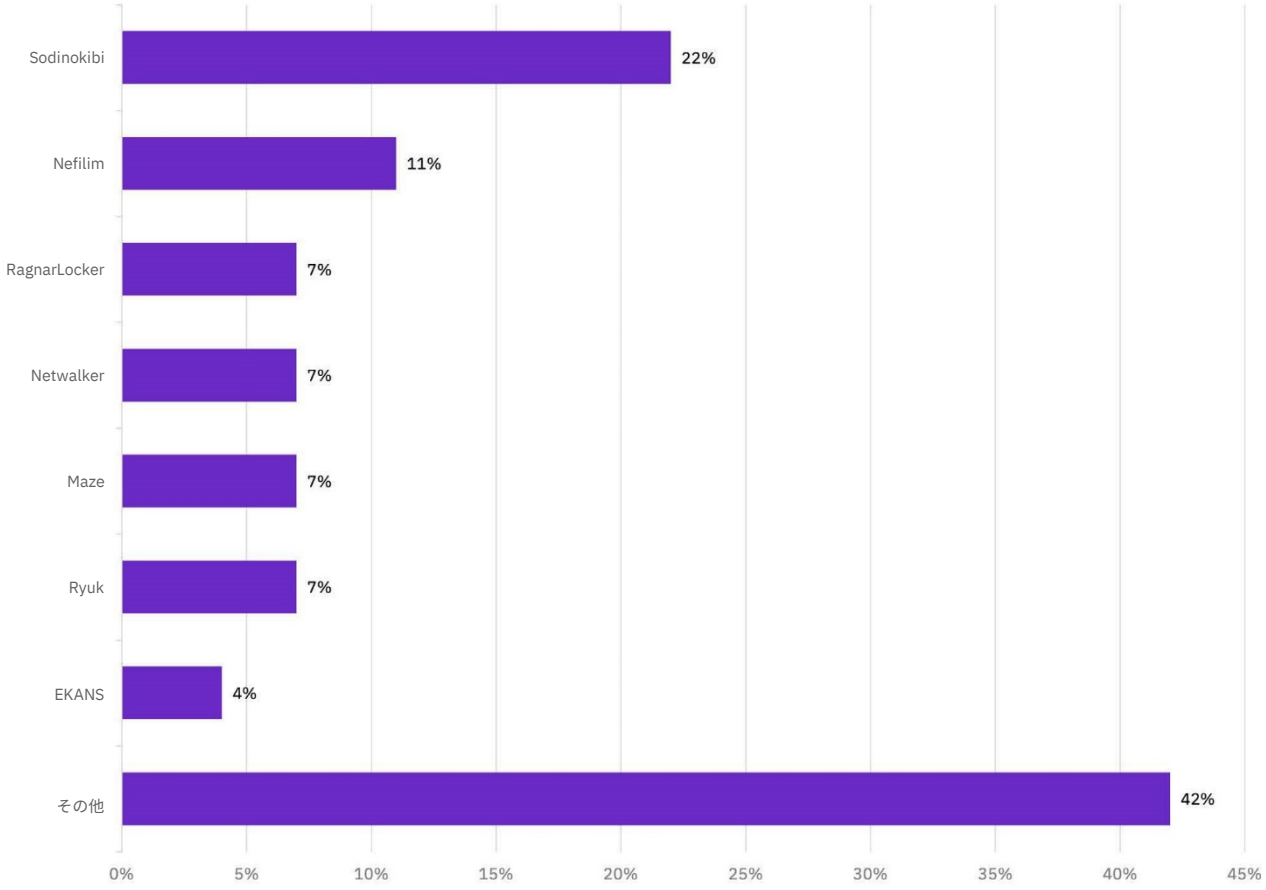
59%
ランサムウェア攻撃が二重の恐喝の戦術を使用した割合

1 億 2,300 万ドル超
Sodinokib を使用した犯罪者が 2020 年に得た利益

図 2

主要なランサムウェア・タイプ

2020 年に観測されたランサムウェア・タイプの比率の内訳（出展: IBM Security X-Force）



X-Force が 2020 年に最も頻繁に観測したランサムウェア・タイプは Sodinokibi であったため、X-Force はその攻撃に関する大量のデータと洞察を収集し、それらを詳しく追跡しました。その中には、IBM のお客様に対する Sodinokibi 攻撃だけでなく、Sodinokibi グループが実行したと主張した攻撃のすべてが含まれます。

この調査によって以下のパターンが明らかになりました。

— Sodinokibi ランサムウェア攻撃は、2020 年の 6 月または 7 月にピークを迎え、8 月と 9 月に中断した後に再度増加しています。これは、脅威アクターの稼働性、休暇、代替要員の従事している期間に関係している可能性があります。

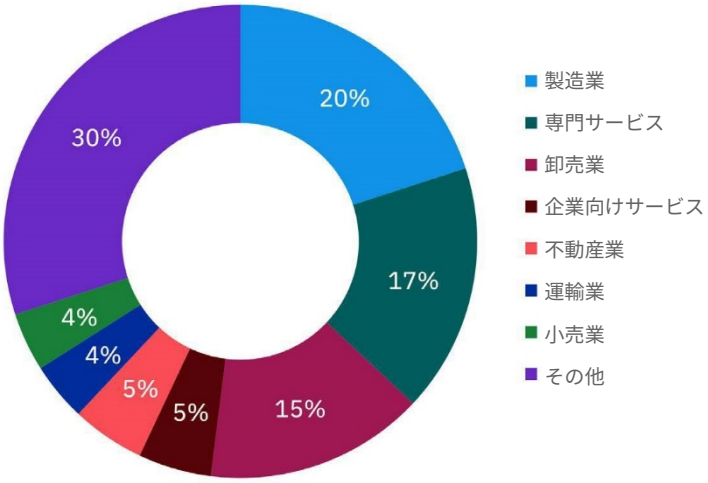
— 製造業、専門サービス、卸売業は、最も頻繁に Sodinokibi の攻撃対象となった業界です。この理由としては、Sodinokibi アクターがこれらの業界の企業は、特にパンデミックの期間中はダウンタイムへの耐性が低かったり、あるいは特別な機密データを保有していると評価した可能性が考えられます（*図 3 を参照*）。

— Sodinokibi からの身代金の要求額は、被害を受けた企業の年間総収益のおよそ 1% から 5% になる傾向にあり、あるケースでは 4,200 万ドルにもなりました。

図 3

Sodinokibi ランサムウェア攻撃の業界別比率

2020 年に観測された Sodinokibi ランサムウェア攻撃の業界別比率の内訳（出展: IBM Security X-Force）



数字で見る Sodinokibi ランサムウェア

最も頻繁に攻撃対象となった地域

1. 米国（58%）
2. 英国（8%）
3. オーストラリア（5%）
4. カナダ（3%）

推定損害額
2020 年総額: 1 億 2,300 万ドル超
2020 年 8 月のみ: 5,500 万ドル

窃盗データの推定合計:
21.6 テラバイト

X-Force の推定では、2020 年に Sodinokibi による被害を受けた企業のうち**約 2/3** が身代金を支払い、およそ 43% がデータ漏えいの被害に遭いました。

推奨されるランサムウェア攻撃対処法

攻撃への備えが重要: ランサムウェア攻撃（ランサムウェアとデータ窃盗を組み合わせて恐喝する手法を含む）への対応計画を導入、実践します。

データのバックアップをオフラインで安全に保管する: バックアップがあれば、組織は迅速に自力でランサムウェア攻撃から回復することができます。

高度な多層防御策を実装する: 多面的なアプローチを採用します。例えば、ネットワーク内のすべてのアクセス・ポイントに多要素認証を導入し、エンドポイントを可視化する、積極的な脅威ハンティングを行い、定期的なペネトレーション ・テストの実施を通してネットワークの弱点を特定し、速やかにパッチを適用して既知の脆弱性を軽減するなどが推奨されます。

ランサムウェア完全攻略ガイド

登録してホワイト・ペーパーをダウンロードする>

データ窃盗

データ窃盗、つまり被害者の機密データを奪う攻撃者は、2020 年に X-Force が対処した攻撃の 13% を占め、2019 年の 5% から大幅に増加しました。

2020 年 の 9 月 と 10 月に相次いだ Emotet マルウェアを利用した攻撃は、急増したデータ窃盗を利用した攻撃のかなりの部分を占めていました。2020 年に X-Force が対処したデータ窃盗を利用した攻撃のうち、46% がこれらの Emotet 攻撃であり、主にアジアで実行されました。

2020 年にデータ窃盗を利用した攻撃を受けた製造業者は、全データ窃盗インシデントの 33% に上りました。エネルギー業が 21%、3 位の金融・保険業が 17% を占めました。

サーバー・アクセス攻撃

サーバー・アクセスは 2020 年に 3 番目に多かった攻撃タイプで、同年に X-Force Incident Response が対処した全攻撃の 10% を占めていました。サーバー・アクセス攻撃には、盗んだサーバーの認証情報を悪用したり、脆弱性を突く、またはその他の方法で、脅威アクターが被害者のサーバーに不正にアクセスするという脅威活動が含まれます。

2020 年に X-Force Incident Response が観測したサーバー・アクセス攻撃のうち、約 36% が金融・保険業を標的にしていました。また、企業向けサービス (14%)、製造業 (7%)、ヘルスケア (7%) も大きな被害を受けました。

脅威アクターが Citrix のパス・トラバーサル脆弱性である CVE-2019-19781 の悪用に成功したことで、サーバー・アクセス攻撃の勢いが増大しました。

Citrix の脆弱性 CVE-2019-19781

X-Force のデータによると、2020 年前半に発生したインシデントのうち、15% が Citrix の脆弱性である CVE-2019-19781 に直接関係していました。これは他のどの脆弱性よりも 15 倍以上も多いことがわかりました。2019 年 12 月に公表されたこの脆弱性は、Citrix Application Delivery Controller (ADC)、Citrix Gateway、NetScaler Gateway に影響を及ぼしています。攻撃者は CVE-2019-19781 を利用して、脆弱な Citrix サーバーで任意のコードを実行できます。

数字で見る CVE-2019-19781 の悪用

- 2020 年 1 月: 全インシデントの 59%
- 2020 年第 1 四半期: 全インシデントの 25%
- 2020 年前半: 全インシデントの 15%
- 2020 年に X-Force が対処した全インシデントの 8%
- 脆弱性が判明している Citrix サーバー: 25,000 台以上

複数のグループが Citrix の脆弱性を悪用

2020 年、X-Force は CVE-2019-19781 を悪用している複数の脅威アクター・グループを観測しました。これには金銭目的のサイバー犯罪者だけでなく、国家支援のグループも含まれていました。確認されたグループは次のとおりです。

— HHive0088 (別名 APT41、中国の関与が疑われる)

— ITG07 (別名 Chafer、イランの関与が疑われる)

— Sodinokibi (別名 REvil) ランサムウェア・アクター

— Maze ランサムウェア・アクター

それぞれのケースにおいて、攻撃者はこの脆弱性を利用してシステムにアクセスし、Adwind などのリモートアクセス型トロイの木馬 (RAT) をインストールし、媒介となるマルウェアとして Trickbot や Cobalt Strike をデプロイし、Sodinokibi や Maze などのランサムウェアまでデプロイしていました。一部の攻撃者は、この脆弱性を利用してネットワークにもアクセスし、ランサムウェア攻撃を仕掛けていました。

2020 年に最も頻繁に悪用された上位 10 の脆弱性

以下のリストは、2020 年に悪用された脆弱性の上位 10 件を示しています。注目すべきは、リストの中で 2020 年に公表された脆弱性が 2 つしかない点です。これは即ち、古い脆弱性による脅威が今も続いていることを証明しています。2020 年を通して、脅威アクターは 2019 年以前から存在する脆弱性をより多用する可能性が高くなっていました。これはおそらく、2020 年に明らかになった脆弱性の多くは悪用しにくいことと、古い脆弱性へのパッチ適用は困難であると、多くの組織が直面していることに基づいているものと考えられます。

1. **CVE-2019-19871:** Citrix Application Delivery Controller
2. **CVE-2018-20062:** NoneCMS ThinkPHP のリモート・コード実行
3. **CVE-2006-1547:** Apache Software Foundation (SAF) Struts の ActionForm
4. **CVE-2012-0391:** Apache Struts の ExceptionDelegator コンポーネント
5. **CVE-2014-6271:** GNU Bash のコマンド・インジェクション
6. **CVE-2019-0708:** 「Bluekeep」、Microsoft リモート・デスクトップ・サービスのリモート・コード実行
7. **CVE-2020-8515:** Draytek Vigor のコマンド・インジェクション
8. **CVE-2018-13382** および **CVE-2018-13379:** Fortinet FortiOS の不適切な認証とパス・トラバーサル
9. **CVE-2018-11776:** Apache Struts のリモート・コード実行
10. **CVE-2020-5722: HTTP:** Grandstream UCM6200 の SQL インジェクション

頻繁に用いられる攻撃手口

CVE-2019-19781 が頻繁に悪用された結果、脆弱性のスキャンとエクスプロイトは、脅威アクターがよく使用する攻撃手口の最上位に躍り出ました。その割合は、X-Force が対処した既知の攻撃手口による全インシデントの 35% に上っています。[3] 一方、スキャンとエクスプロイトは、前年には、全攻撃の 30% に過ぎませんでした。

通常、スキャンとエクスプロイト攻撃はリソースをほとんど必要とせず、自動化や拡張によって多様な被害者を標的にすることができます。2020 年にこの攻撃手口が急増した原因もそこにあると考えられます。2020 年のスキャンとエクスプロイト攻撃では、Citrix のパス・トラバーサルの脆弱性に加えて、Heartbleed の脆弱性や、脆弱性あるいは設定ミスのある管理プロトコルが標的になり、暗号の脆弱性である CVE-2017-9248 も悪用されました。

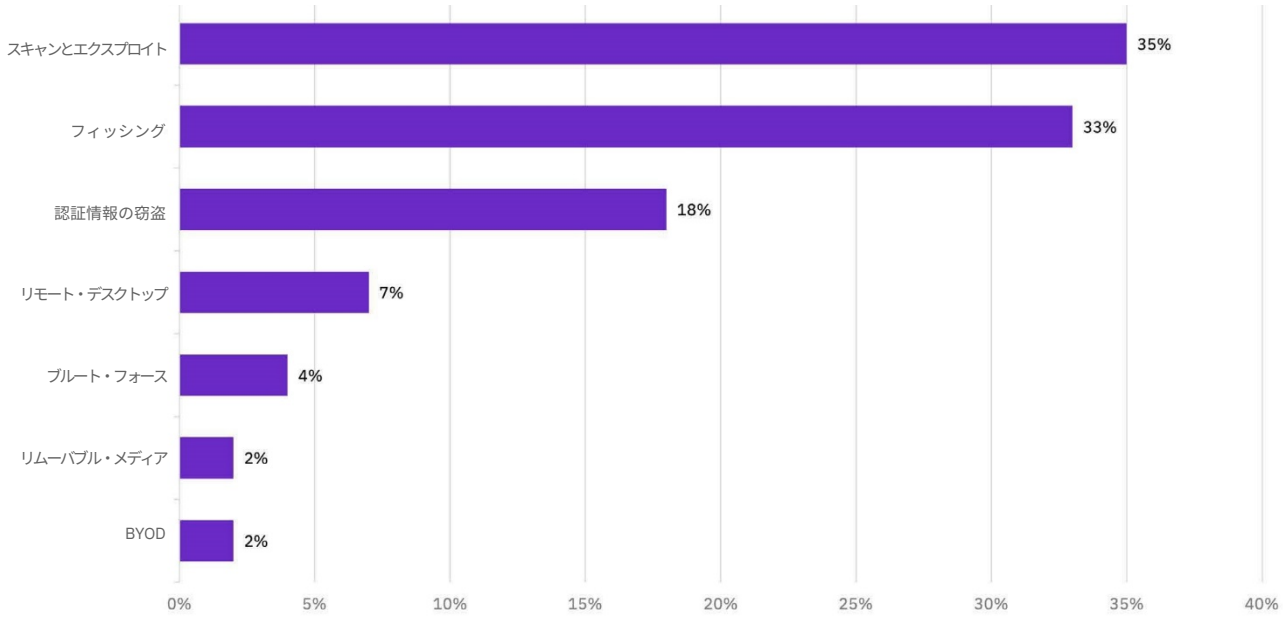
フィッシングは 2 番目に多かった攻撃手口で、昨年の 31% からわずかに増加して 33% の攻撃で使用されました。これは、変化する攻撃者の手法と、フィッシングに対する防御のメカニズムが互いに拮抗していることを示唆しています。

認証情報の窃盗は攻撃全体の 18% を占め、昨年の 29% から大きく減少しました。これは、2020 年に実行した多くの侵害行為において、脅威アクターが認証情報の窃盗に代わり、スキャンとエクスプロイト攻撃による成功率の高まりを悪用した可能性を意味しています。

図 4

頻繁に用いられた攻撃手口

2020 年に IBM Security X-Force Incident Response によって観測された 7 つの攻撃手口の比率の内訳
(出展: IBM Security X-Force)



3 攻撃手口が分かっていない複数のインシデントは、このデータには含まれません。

高度な脅威アクター

2020 年に X-Force が観測した脅威グループの中には、操作を誤ったためにうっかり手の内を明かしてしまい、X-Force の研究者に貴重な洞察を提供するグループもありました。さらに別のケースでは、高度な脅威アクターを追跡することで、脅威アクターがワクチンの配布を標的にする方法や、感染拡大につけ込んで継続的にフィッシングの罠を仕掛ける方法など、新型コロナウイルス関連の脅威について有益な洞察が得られました。

現場を押さえられたイランの脅威グループ

2020 年 9 月、X-Force のアナリストはフィッシング詐欺の Hive0082 と関係のあるインフラストラクチャーを発見しました。Hive0082 は Silent Librarian、COBALT DICKENS、または TA407 とも呼ばれ、その活動が何度も公表されているにもかかわらず、遅くとも 2013 年から世界の学術機関を活発に攻撃しています。

2020 年 9 月の活動は、それまでの攻撃と大した違いはありませんでした。ただしその実行者は、標的とする学術リソースの有効なログイン・ページをスプーフィングするためにツールを使用し、そのメタデータを残していきました。具体例を挙げると、X-Force の研究者は、このキャンペーンで Chrome の拡張機能である「Single File」が連続的に使用されていることに気付きました。この機能を使用すると、Web サイトをコピーしているマシンのタイムスタンプを取得することができます。このキャンペーンで使用されたなりすまし Web サイトの一部に、「イラン夏時間」のタイムスタンプが含まれていました。これは Hive0082 の実行者が犯しそうなミスです（*図 5 を参照*）。

図 5

Hive0082 フィッシング詐欺

イラン夏時間のタイムスタンプが表示された Hive0082 なりすまし Web ページのメタデータ（出展: IBM Security X-Force）

```
</script>
<!--
Page saved with SingleFile
url: [redacted]
saved date: Mon Apr 08 2019 13:20:57 GMT+0430 (Iran Daylight Time)
-->
```

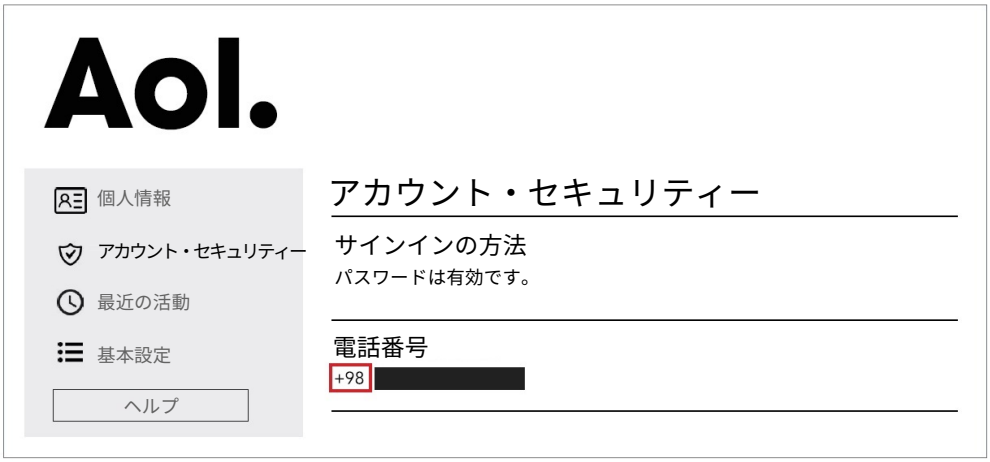
別の事例では、X-Force が ITG18 と呼んで追跡している、イランの支援を受けたもう 1 つの脅威グループのミスによって、彼らの活動について前例のない洞察が得られました。このグループは、過去の操作でセキュリティー上のミスを犯したことがあります。例えば、基本的なサーバーの設定を間違ったために、標的が発覚したケースや、グループが運用しているあるサーバーに仕掛けられたランサムウェアが暴露されたケースがありました。

2020 年 5 月、X-Force は ITG18 が所有する、サーバーの設定ミスをさらにもう 1 つ発見しました。このサーバーには 40 ギガバイトを超える動画とデータ・ファイルが保存されていました。動画には、ITG18 が侵害したアカウントを偵察するために使用する手順や技術が収められていました。さらには ITG18 の活動に関するメタデータも含まれており、ITG18 の VPN インフラストラクチャー、脅威アクターの電話番号、米国政府を標的とする複数のフィッシング行為の失敗などが露呈しました。

図 6

ITG18 の訓練用 AOL アカウント

ITG18 のサーバーの設定ミスにより発覚した、訓練で使用される AOL アカウントに関連付けられた脅威アクターの電話番号
(出典: IBM Security X-Force)



両グループの操作ミスから得られた洞察によって、X-Force 脅威インテリジェンスのアナリストは、進行中の攻撃についてその標的に警告を発し、訓練の方法やパスワード窃盗の手法に関する見識を高め、悪意ある活動に使われているインフラストラクチャーをリアルタイムに特定することができました。X-Force はこのようにして得られた洞察を利用して防御を強化し、被害を受ける可能性のある様々な組織に警告を発することができました。

新型コロナウイルス・フィッシング・キャンペーン

X-Force は新型コロナウイルスに関連したサイバー活動の調査を進める中で、高度な脅威アクターによる、新型コロナウイルス関連のサプライチェーンに対する様々なフィッシング・キャンペーンを探知しました。

ワクチンのコールド・チェーンに対する攻撃

2020 年 10 月、X-Force 脅威インテリジェンスは、新型コロナウイルス・ワクチンを安全に配布する技術に関心がありそうな個人、団体、超国家的機関を標的にした、大量のフィッシング・メールを確認しました。今回明らかになった活動は、国連児童基金 (UNICEF) と Gavi Vaccine Alliance による、ワクチンを世界中に配布するための Cold Chain Equipment Optimization Platform (CCEOP) を模したものです。今のところ関係性は明らかではありませんが、これらの攻撃の背後には国家支援の攻撃者がいた可能性があります。

このフィッシング・キャンペーンは、敵対者によって非常に緻密に設計されていました。敵対者は認証情報を収集して、新型コロナウイルス感染症のワクチンの輸送と配布プロセスに関する有益な洞察を入手しようとしていたと考えられます。標的には欧州委員会の税制・関税同盟総局のほか、エネルギー、製造業、Web サイト制作、ソフトウェアおよびインターネット・セキュリティー・ソリューション分野の組織が含まれていました。これらはいずれもドイツ、イタリア、韓国、チェコ共和国、広域欧州圏、台湾などに本社を置く国際的な組織です。

図 7

新型コロナウイルス・ワクチンに関するフィッシング

新型コロナウイルス・ワクチンのコールド・チェーンに対する攻撃で使用されたフィッシング・メールの例
(出典: IBM Security X-Force)

PPE サプライチェーン攻撃

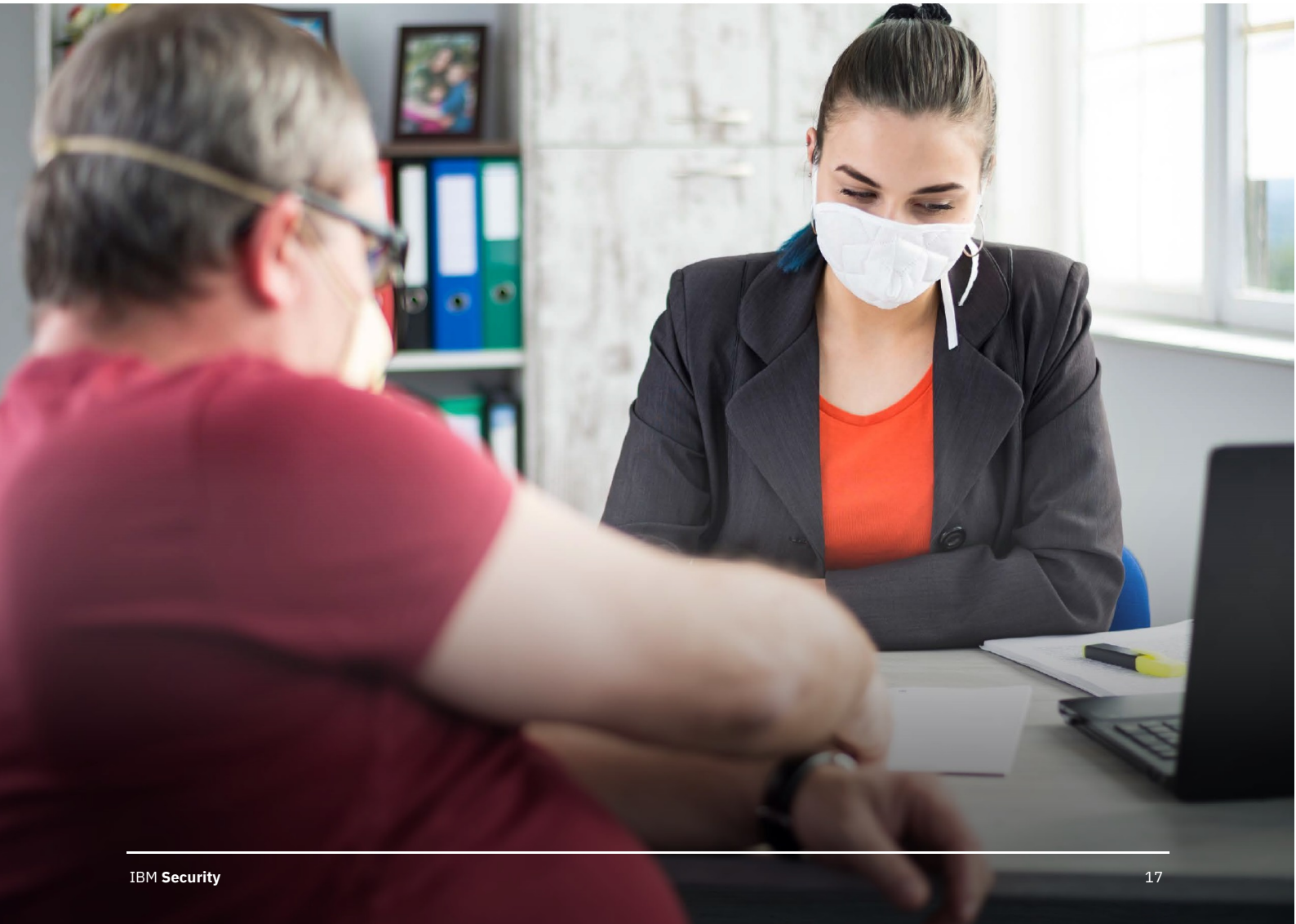
2020 年 5 月、X-Force の調査により、PPE を調達するドイツの官民協同委員会と関係のある、ドイツの多国籍企業が標的になっていることが判明しました。これは、絶対に必要な PPE の確保に奔走している状況を悪用して、標的を正確に狙い定めたキャンペーンでした。

このキャンペーンの背後にいる脅威アクターは、この組織で管理と調達を担当する 100 人以上の上級役員と、サード・パーティーのエコシステムを標的にしていました。X-Force は、このキャンペーン全体で約 40 の組織が狙われていたことを確認しました。このサプライチェーンの標的が広範囲に及んでいることを考えると、他の委員会メンバーもこの悪意あるキャンペーンの攻撃対象になっていた可能性があり、警戒の強化が求められます。

ウクライナを狙ったキャンペーン

2020 年の 3 月中旬から 4 月中旬にかけて、X-Force は悪意のある .docx ファイルを発見しました。これはおそらく、現在も継続中の不審な Hive0051 (別名 Gamaredon) 攻撃によるものです。この新しい活動は、ウクライナ国内の組織を集中的に標的とする、Hive0051 の従来の攻撃パターンと一致していると思われます。

X-Force が発見した悪意ある文書ファイルのコンテンツは、新型コロナウイルス感染症と地政学的なテーマの罠を組み合わせて使われ、ウクライナの政府機関と NGO になりすましていました。このグループが、地域の発展に大きな関心を持つウクライナの国民や組織をだまして利益を得るために、進行中の地政学的発展と新型コロナウイルスの感染拡大にまつわる不安を利用したということは十分に考えられます。



OT と ICS への脅威

オペレーショナル・テクノロジー（OT）に向けての脅威は、現実の世界に影響を及ぼす可能性があります。化学物質の流出、機械の誤作動、あるいは車の衝突事故さえ起こりかねません。こうした理由から、X-Force では OT に関する調査と分析を優先して対処しています。X-Force は独自のデータ・ソースに基づき、OT ネットワークを利用している組織に対する脅威について、独自の洞察を提供しています。

X-Force のアナリストは、2020 年の OT に対する攻撃パターンを調査するために、OT ネットワークに影響を与え得る製造、石油・ガス、運輸、公益事業、建設、および鉱業の関連組織で発生したインシデントを追跡調査しました。

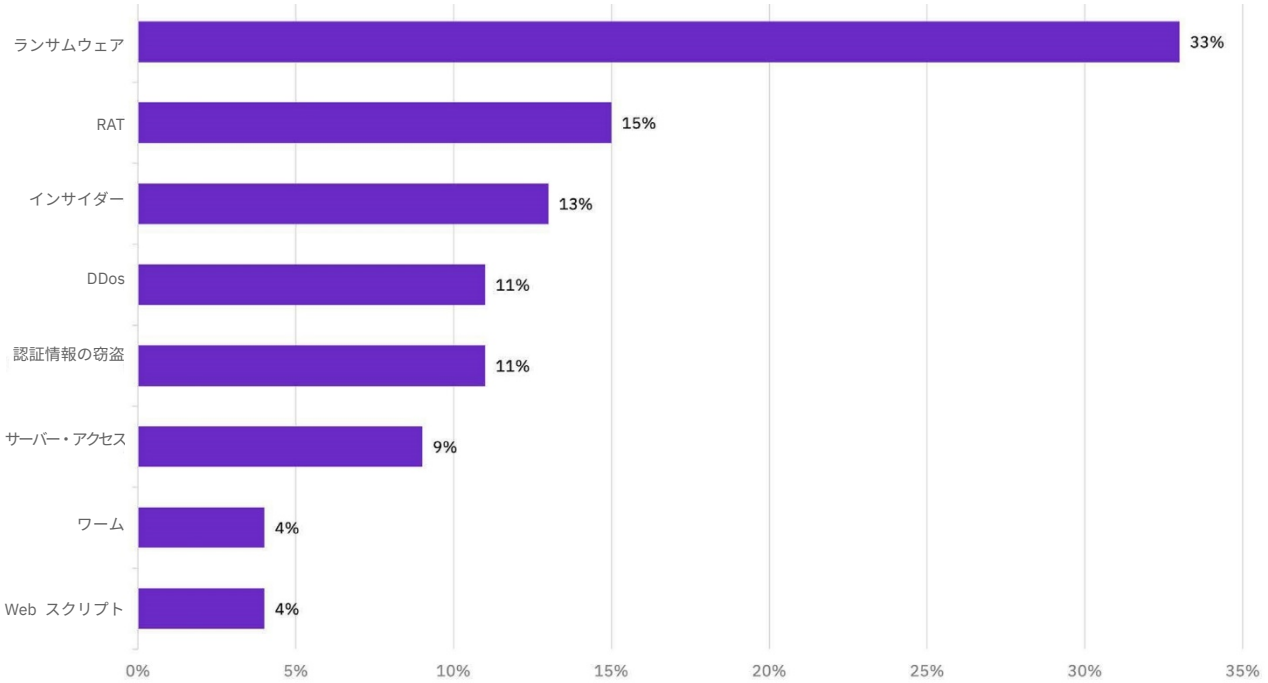
ランサムウェア

X-Force Incident Response のデータによると、最も頻繁に発生した OT への脅威はランサムウェア攻撃であり、これは X-Force が 2020 年に観測した全体的な攻撃傾向とも一致しています。2020 年の OT に対する全攻撃のうち、33% をランサムウェア攻撃が占めていました。この傾向は、脅威アクターがランサムウェア攻撃を行ううえで、OT ネットワークを備えた組織が特に魅力的であると考えていることを示唆しています。2020 年に X-Force が観測した OT 組織へのランサムウェア攻撃では、EKANS、Nefilim、Medusa、PJX、Egregor のランサムウェアの種類などが上位に入っています。

図 8

OT への攻撃タイプ

2020 年に観測された OT を備えた組織に対する攻撃タイプの比率の内訳（出展: IBM Security X-Force）



リモートアクセス型トロイの木馬

リモートアクセス型トロイの木馬（RAT）は、2020 年に 2 番目に多かった OT への攻撃タイプで、X-Force Incident Response のデータによると全攻撃の 15% を占めていました。脅威アクターは RAT を使用してデバイスにアクセスし、そのデバイス上で秘密監視ができます。2020 年に X-Force Incident Response が OT 接続ネットワークで観測した RAT には、Trickbot、Adwind、jRAT などがあります。

インサイダー脅威

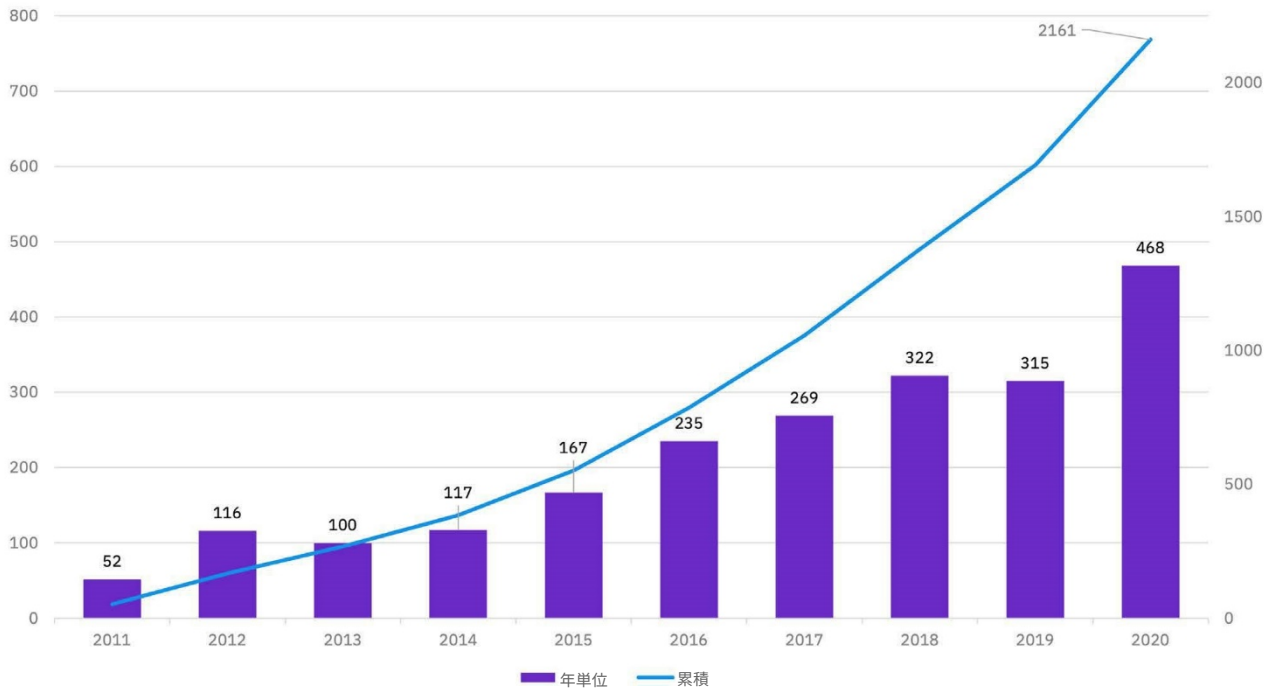
X-Force のデータによると、インサイダー脅威は 2020 年の OT 関連インシデント全体の 13% を占め、そのうちの約 60% に悪意あるインサイダーが関与しており、約 40% は過失によるものでした。X-Force が観測した悪意あるインサイダー・インシデントには、マルウェアと関係がある不審な Web サイトに接続している従業員や、第三者の Web サイトで自社の機密情報を売却している可能性のある従業員などが含まれていました。

産業用制御システムの脆弱性

図 9

ICS の脆弱性（2011 年から 2020 年まで）

ICS を標的とする公表された脆弱性の数（2011 年から 2020 年までの年単位と累積）(出展: IBM Security X-Force)



X-Force の追跡調査によると、ICS プラットフォームの脆弱性は増大し続けており、昨年に若干減少したものの、2020 年は過去最高に達しました。具体的には、2020 年の ICS 脆弱性は前年比で 49% 増加したことを X-Force が確認しています。ICS の脆弱性は OT システムにとってのリスクを高め、有害で物理的な影響を及ぼす可能性があるため、憂慮すべき問題です。

なりすまし被害が多かったブランド

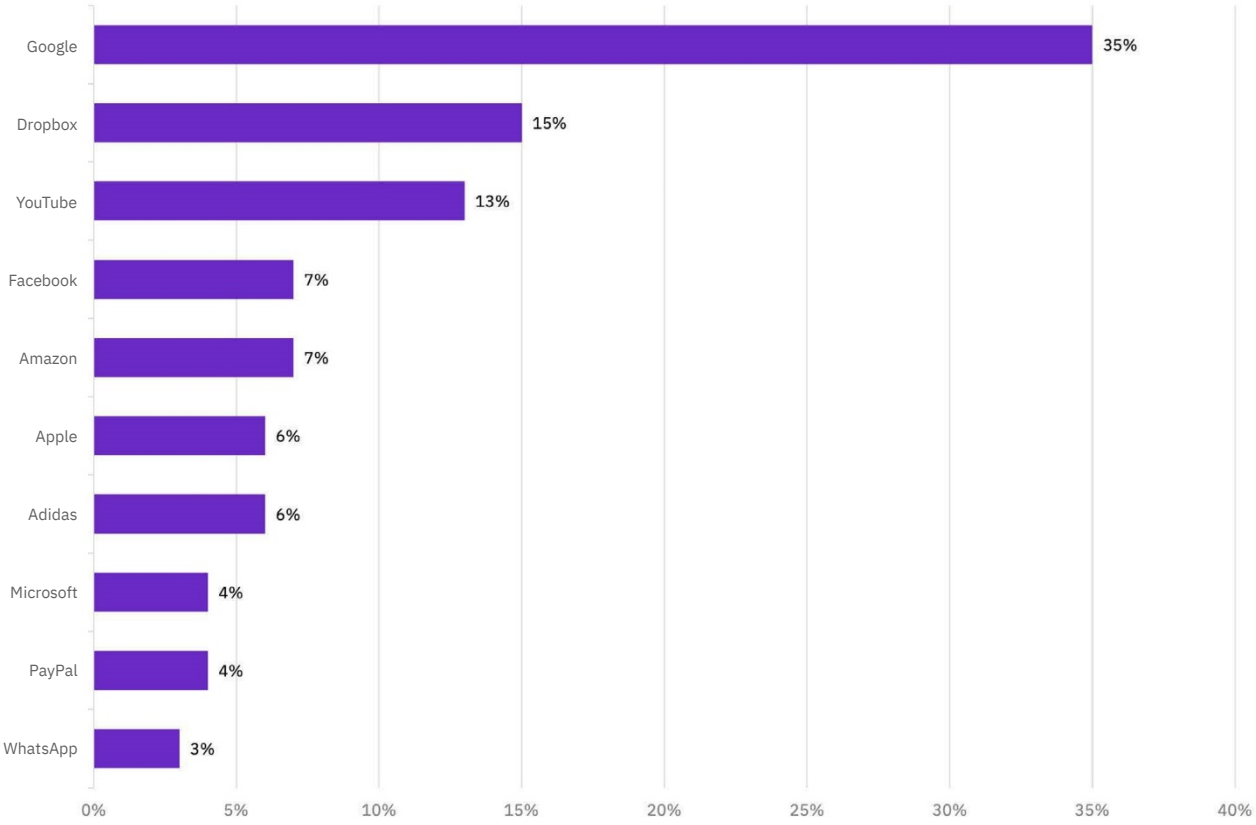
Quad9 は、悪意あるドメインを追跡してユーザーに警告し、それらのドメインに関係している脅威アクターの活動からユーザーを保護しています。Quad9 は、毎日平均 1,000 万件の悪意あるドメイン・ネーム・システム (DNS) 要求を遮断しています。IBM は、他の脅威インテリジェンス・プロバイダーよりも平均で 8 日早く、悪意あるドメインを識別しています。X-Force は Quad9 パートナーであり、組織が信頼できる DNS を介して安全にインターネット通信ができるよう支援しています。

X-Force と Quad9 は、2019 年と同様に 2020 年も、悪意あるドメインで頻繁に使用されているなりすましブランドの追跡を続けました。脅威アクターはこれらのブランドになりすまそうとします。ブランドの人気やユーザーからの信頼を利用して被害者をだまして電子メールを開かせ、リンクをクリックさせ、機密情報を入力させるなどして入手した機密情報を攻撃に利用しようとしています。

図 10

なりすまし被害が多かった上位 10 ブランド

2020 年にスパムによるなりすまし被害が多かった上位 10 ブランドの内訳 (10 ブランドを比率で表示) (出展: Quad9)



テクノロジー企業やソーシャル・メディア企業は、なりすまし被害に遭ったブランドとして引き続き上位を占めており、2020 年にスプーフィングされたブランドの中では Google、Dropbox、YouTube が大きな比率を占めています。Google は、2019 年に続いてなりすましブランドの最上位となっています。昨年からの上位なりすましブランドである Amazon、Apple、Microsoft、Facebook と共に、Adidas と PayPal も 2020 年にトップ 10 入りしています。Adidas のスプーフィング活動の大半は 1 月に行われていることから、コロナウイルスの感染拡大とは無関係であり、Superstar や Yeezy などのスニーカーが関係していると考えられます。PayPal のトップ 10 入りについては、認証情報や資金の盗用をもくろむ金銭目的のサイバー犯罪者の関与が強く疑われています。

脅威アクターは、テクノロジーとソーシャル・メディア企業の人気や、その資産にデジタル方式でアクセスできるというユーザーの期待を踏まえて、これらの企業のスプーフィングに強い関心を持っていると思われます。さらに、X-Force Incident Response のデータから判断すると、Google Gmail や Microsoft O365 などの電子メールと電子メールと連動するプラットフォームのスプーフィングは、脅威アクターの代表的な手法になっています。さらに、脅威アクターにとって、これらのブランドは簡単に収益化できる標的でもあります。こうした人気の高いプラットフォームで使われるアカウントを不正に入手し、それをダーク Web で売って簡単に利益を得ることができるからです。

新しいマルウェアの脅威

脅威アクターがマルウェアの調整、強化、改良を続ける中、データから複数のマルウェア開発の傾向が明らかになってきました。2020 年の最も顕著な傾向は、Linux を標的にしたマルウェアの急増であり、その次が Go プログラミング言語で記述されたマルウェアの増加です。2020 年秋の Emotet マルウェアの激増は、この種の脅威が再浮上してきたことを示しています。どちらの傾向にも、より効果的に検知能力を回避するという、脅威アクターの究極の目標が表れています。

Linux の脅威の 1 年

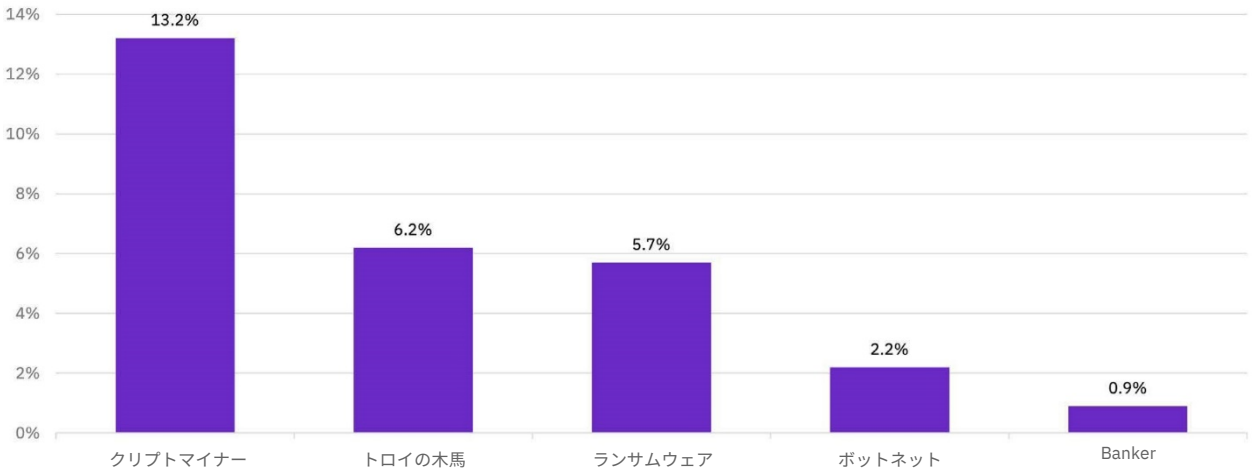
Intezer 社は、IBM Security と提携しているマルウェア・コードの分析企業です。同社の研究者は、攻撃者によるクリプトマイナーとトロイの木馬の利用が増加していることを確認しました。おそらくこれは、クラウドなどの最新のインフラストラクチャーに適応しようとする試みによるものです。クラウドでは、すでにワークロードの 90% が Linux 上で稼働しており、新型コロナウイルス感染症の影響でその導入はますます加速しています。

2020 年、攻撃者は Linux クリプトマイナーとランサムウェアの開発に力を入れていました。その理由は、自社サーバーをクラウドに移行する組織の増加と、クラウド環境の拡張可能な処理能力にあると思われます。Intezer 社のこのグラフは、2020 年に様々な種類の Linux マルウェア開発に使用された新しいコードの平均比率を示しています。

図 11

Linux マルウェアにおける新しいコードの革新レベル

Linux マルウェア開発に使用された新しいコードの平均比率（マルウェア・タイプ別、2020 年）(出展: Intezer)

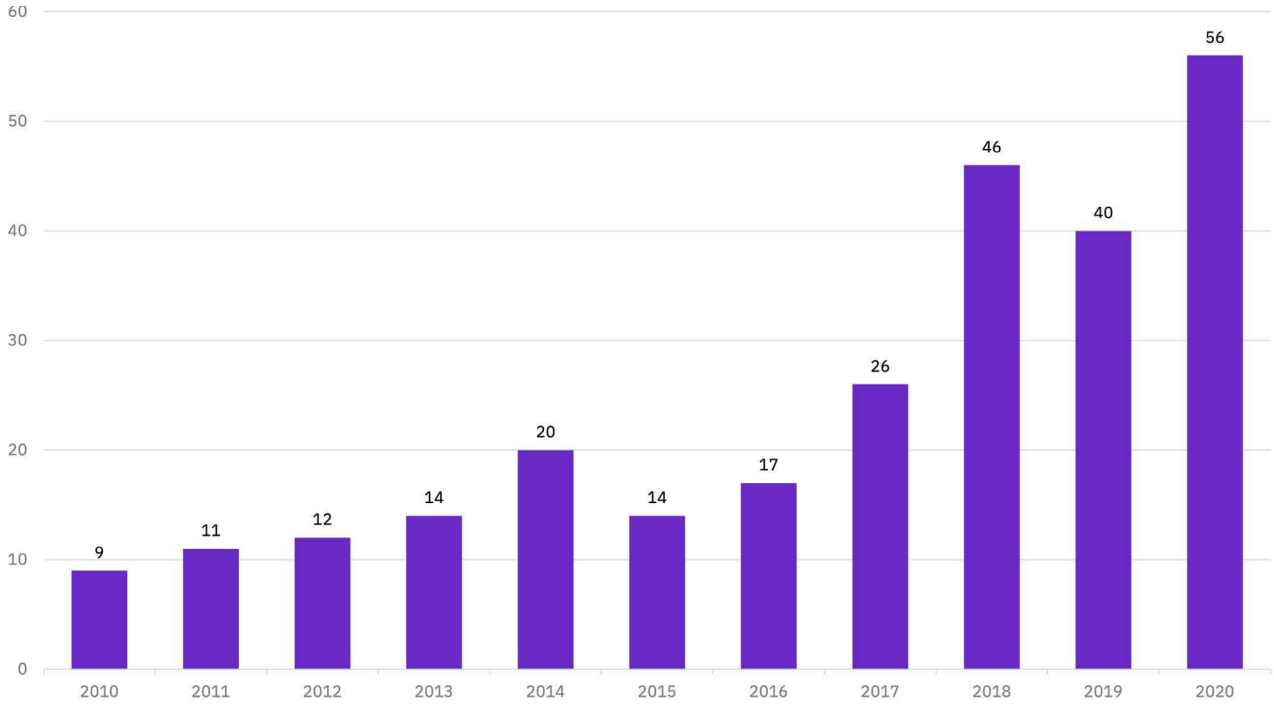


2010 年以降、Intezer 社は新しい Linux マルウェア・ファミリーの増加を観測しており、2020 年にはこれまで報告された中で最も多い 56 個のマルウェア・ファミリーを発見しました。これは 2019 年と比較すると 40% の増加です。この傾向は、Linux の脅威に分類されるマルウェア・ファミリーが増加していることを明確に示しています。

図 12

新しい Linux マルウェア・ファミリー (2010 年から 2020 年まで)

各年の新しい Linux マルウェア・ファミリーの数 (出展: Intezer)



X-Force のマルウェア・リバース・エンジニアも、IBM Security X-Force が対処したインシデントを通して、2020 年に Linux マルウェアが増加したことを確認しました。2020 年の冒頭には、パス・トラバーサル・フロー (CVE-2019-19871) を悪用する複数の脅威アクターによって、脆弱な NetScaler デバイスを標的にしたマルウェア (NotRobin マルウェアなど) も開発されました。2020 年の後半にかけて、マルウェア・エンジニアは、これまで Windows マルウェアを重視していた脅威アクターが、現在は Linux マルウェアを強化している徴候を複数確認しています。

例えば、IBM Security X-Force Incident Response は、Linux ランサムウェアの亜種を観測しています。以前は Windows システムを狙ったマルウェアしか確認されていませんでした。観測された亜種としては、Defray911/RansomEXX ランサムウェアや SFile ランサムウェアの Linux 版などがあります。

新しい「Go-to」言語

2020 年の 1 年間で、X-Force のマルウェア・リバース・エンジニアは脅威アクターが新しいマルウェアを作成する際に Go (Golang の省略形) プログラミング言語を使用していることにますます注目してきました。Go プログラミング言語は C に似たオープンソース言語で、プログラミングの生産性を高めるために設計され、2012 年に発表されました。

Go で記述されたマルウェアは、2020 年全体を見ると 1 月からピークの 6 月までに 500% 増加し、年末にかけても頻繁に使用されました。脅威アクターの間でこのプログラミング言語の人気が高まっていることがよくわかります。一方 2019 年には、Go で書かれたマルウェアのサンプルはほとんど見られませんでした。2020 年には、Go がランサムウェアで頻繁に使用されているのが観測されました。Go は様々な標的を狙う複数の脅威アクターに使用されているほか、OT ネットワークを標的にする脅威アクターにも人気があるようです。

攻撃者が Go を使用する理由は、複数のシステムにデプロイしやすいからです。Go では Linux、Windows、OS X 用に別々のマルウェアを記述するのではなく、マルウェアを一度記述するだけで、それと同じソースコードを様々なプラットフォーム用にコンパイルできます。その結果、様々な種類のオペレーティング・システムでマルウェアの実行が可能になります。

単一の「パッケージ」を作成すれば、Go バイナリーは検知の回避にも役立ちます。他の言語で書かれたマルウェアとは異なり、Go ベースのマルウェアはコード内のすべてのライブラリーを静的にリンクできます。これはつまり、Go マルウェアは独立して動作でき、ドロッパーやサイドローディングを追加する必要がないため、ウィルス検知を簡単に回避できることを意味します。ただし、この機能によりバイナリーが非常に大きくなるため、Go マルウェアはフィッシング目的の添付ファイルとして使用されることはあまりないかもしれません。

Intezer 社は、Windows と Linux の両方のシステムを標的にした、クロスプラットフォーム・マルウェアの開発に最適なプログラミング言語として、複数の APT 攻撃者が Go を導入していることも確認しました。

— APT28 (ITG05): ロシアの国家的グループ。2020 年 12 月、このグループは新型コロナウイルス感染症をフィッシングの罠として利用し、Zebrocy マルウェアの Go バージョンを配信しました。

— APT29 (ITG11): ロシアの別の国家的グループ。Intezer Analyze は WellMail の Linux 版を特定することができました。このマルウェアが UK レポートで IOC とコードを共有しているからです。

— Carbanak (ITG14 または FIN7): 大規模なサイバー犯罪グループ。ある Linux サンプルは、2019 年の Carbanak Windows サンプルとコードを共有していたため、それが糸口となって Intezer 社に特定されました。

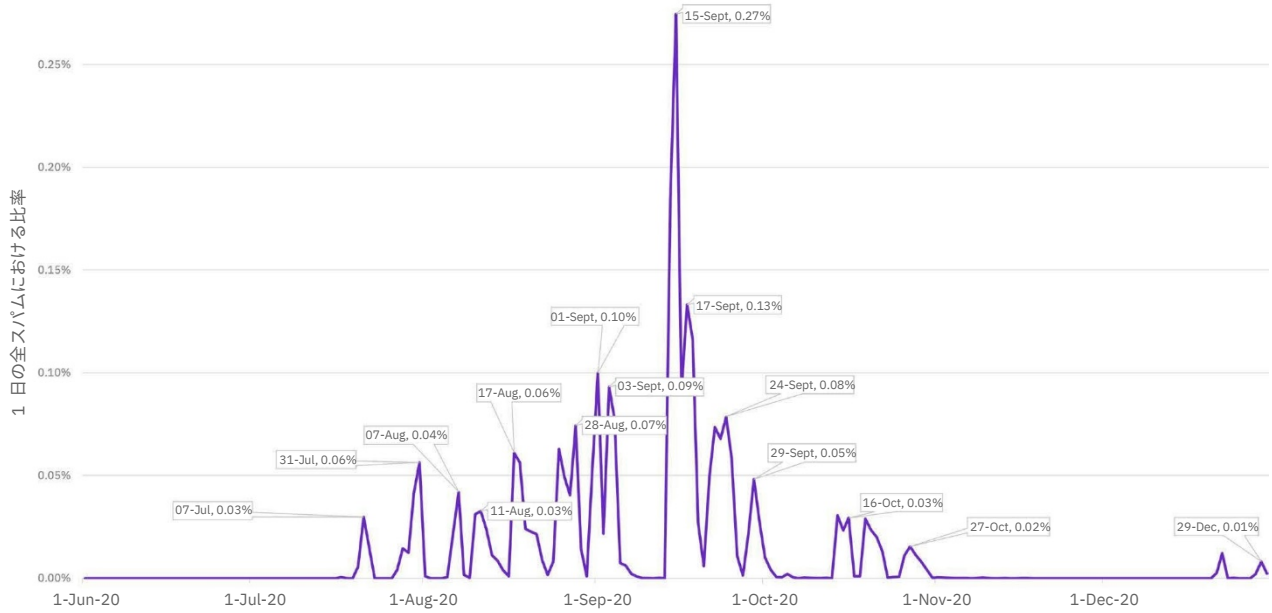
Emotet の再流行

IBM は 2020 年にスパムとフィッシングのトラップを実施し、Emotet を詳しく追跡しました。その結果、このマルウェアは、春から初夏にかけて、なりを潜めていたものの、7 月に再び活動化し、9 月から 10 月にかけて、特に日本で猛威を振るっていたことが分かりました。X-Force の Emotet に対する新しいアンチ解析（解析回避）能力について観測の結果、犯罪者たちが一旦活動の手を休めて、マルウェアの検出回避能力を改良していたため、一旦活動が小康状態になったものだと考えています。

図 13

Emotet スパムの傾向（2020 年 6 月から 12 月まで）

1 日の Emotet スパムの量（1 日の全スパムにおける比率、2020 年 6 月から 12 月まで）
(出展: IBM Security X-Force)



Emotet はスパム・キャンペーンによって広く拡散します。IBM のスパム・トラップは、2020 年に発生したすべての Emotet マルウェアが、Office Word の悪意のあるマクロを含んだ電子メールの添付ファイルを介して拡散したことを観測しました。このマルウェアは、一般的なカジノ・スパムやセクストーションのキャンペーンといった他のスパム・キャンペーンの波に乗り、こうしたメールを転送して悪意のあるペイロードを仕掛けたと考えられています。さらに、Emotet マルウェアは、正規のメールのやりとりを読み込んで、正しい返信を装い、感染した添付ファイル付きのメールを送ることもあります。IBM の分析によって、Emotet スパムの大部分は平日に送信されるということも判明しました。

X-Force インテリジェンス・アナリストにより、Emotet マルウェアのサンプルでアンチ解析（解析回避）能力などの新機能が明らかになりました。こうした機能をアップデートするということは、脅威アクターが Emotet に継続的に投資しており、このマルウェア・ファミリーが引き続き世界中の組織にとっての脅威となる可能性があるということを示しています。

金融サイバー犯罪

脅威アクターはより巧妙な手口を使い、新たな脅威を生み出しているため、金融マルウェアは、サイバー犯罪の中で、常に金融機関やその他の企業にとっての脅威となっています。2020 年に IBM Trusteer は、サイバー犯罪グループが高度に自動化されたプロセスを使ってモバイル・バンキング詐欺を介して、銀行口座から預金をすべて引き出していたことを検知しました。2020 年には、特にヨーロッパでリモート・オーバーレイ攻撃が多く見られました。

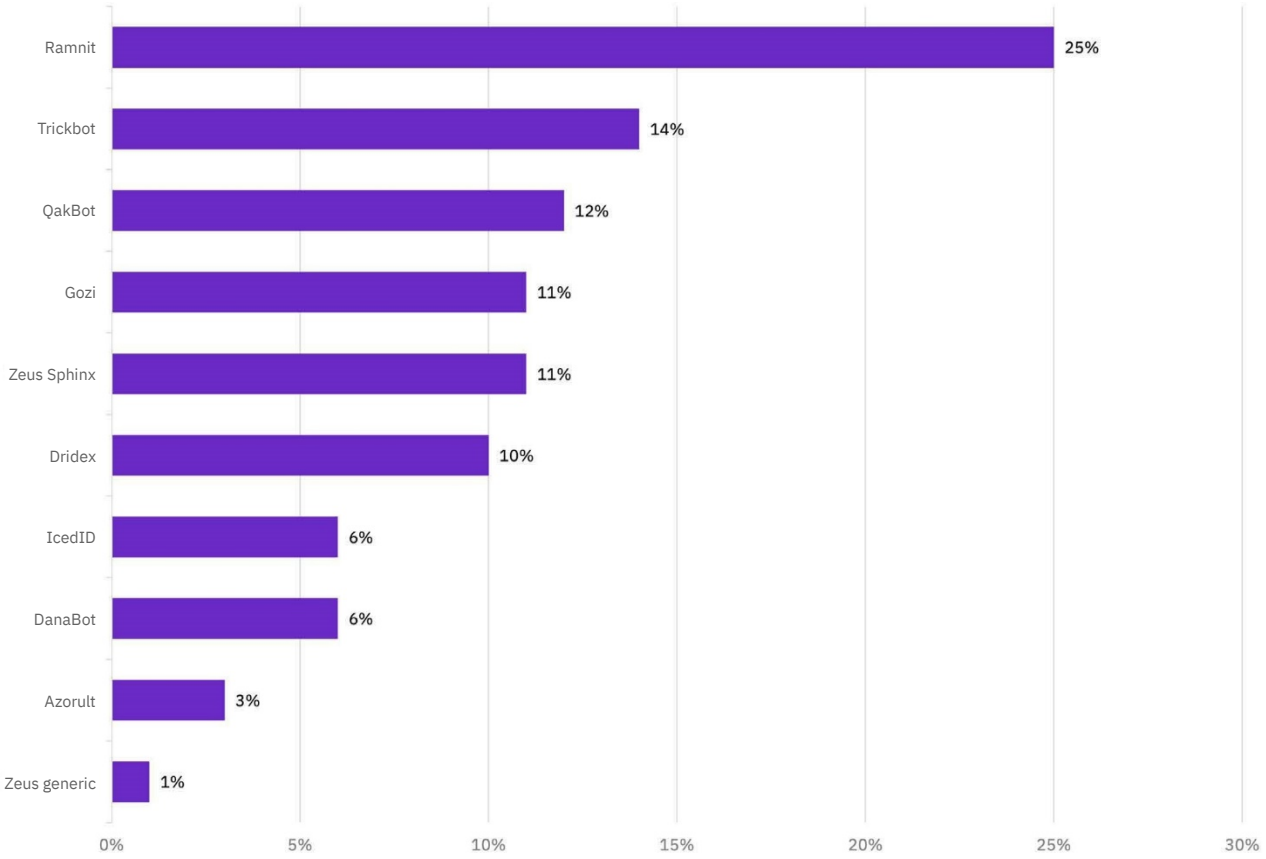
主となるバンキング型トロイの木馬

2020 年に頻繁に検出された金融マルウェア・ファミリーに大きな変化はありませんでした。特に驚くべきこともなく、新種も現れませんでした。だからといって、従来の金融サイバー犯罪グループが、この 1 年間にクライムウェアをアップデートせず、新たな攻撃や収益化の手法を生み出さなかったというわけではありません。

図 14

上位 10 のバンキング型トロイの木馬ファミリー

2020 年の主となるバンキング型トロイの木馬の内訳（上位 10 位を比率で表示）(出展: IBM Trusteer)

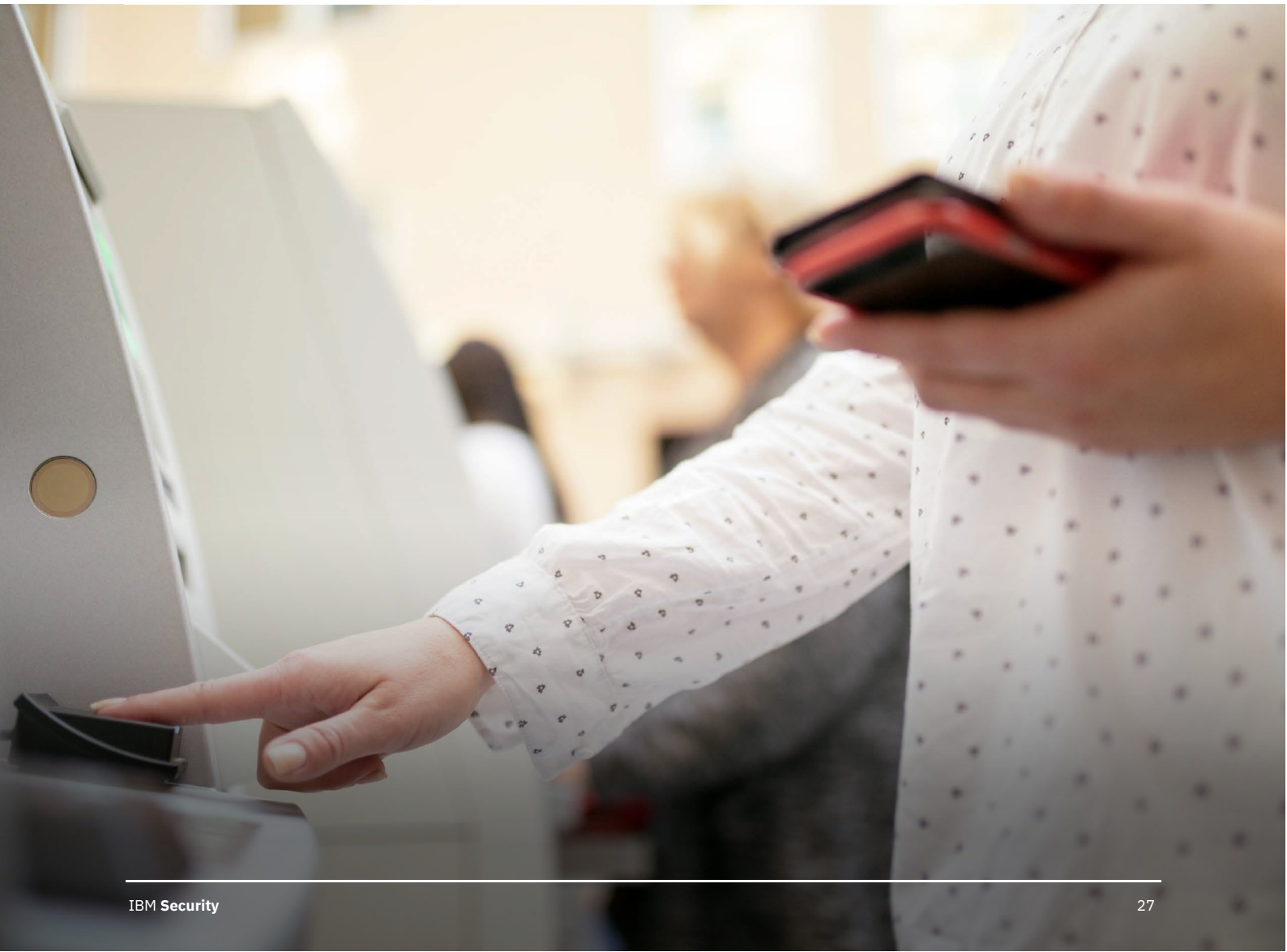


バンキング型トロイの木馬のハイライト

1. **Ramnit**: 昨年の 2 位から 1 位になりました。このマルウェアは、閉鎖的で組織的なサイバー犯罪グループによって引き続き操作されており、収益化モデルを多様化させ、標的とする様々な地域に適応しています。攻撃は依然として、個人と企業の両方の口座に集中しています。

2. **Trickbot**: このランサムウェアを使用した場合、Ryuk ランサムウェア攻撃へと発展するケースが多く見られました。このマルウェアは、1 位から 2 位に転落しました。これは、2020 年 10 月の一時的に無害化し根絶する取り組みの結果によるものと考えられます。このマルウェアは東ヨーロッパを発祥とするもので、ビジネス組織、ビジネス・バンキング、大企業を標的にしています。

3. **Qakbot**: 第 3 位に入ったこのマルウェアは、Emotet ボットネットによって企業ネットワークに拡散されます。2020 年には、それを足掛かりとして、ProLock ランサムウェアにより攻撃し、収益化を図る戦略に転じています。このマルウェアも東ヨーロッパを発祥としており、企業、ビジネス・バンキング、大企業を標的にしています。



地理的な傾向と業界の傾向

どの地域も業界も、それぞれ固有の攻撃を受けています。これは、地域や業界毎に、様々な脅威アクター、動機、資産、地政学的な事象を要因とした攻撃が行われていることに起因します。このセクションでは、本レポートで取り上げている攻撃の全体的な傾向の内訳を示すと共に、それらの傾向が各地域や業界に与える影響をについて詳しく説明します。

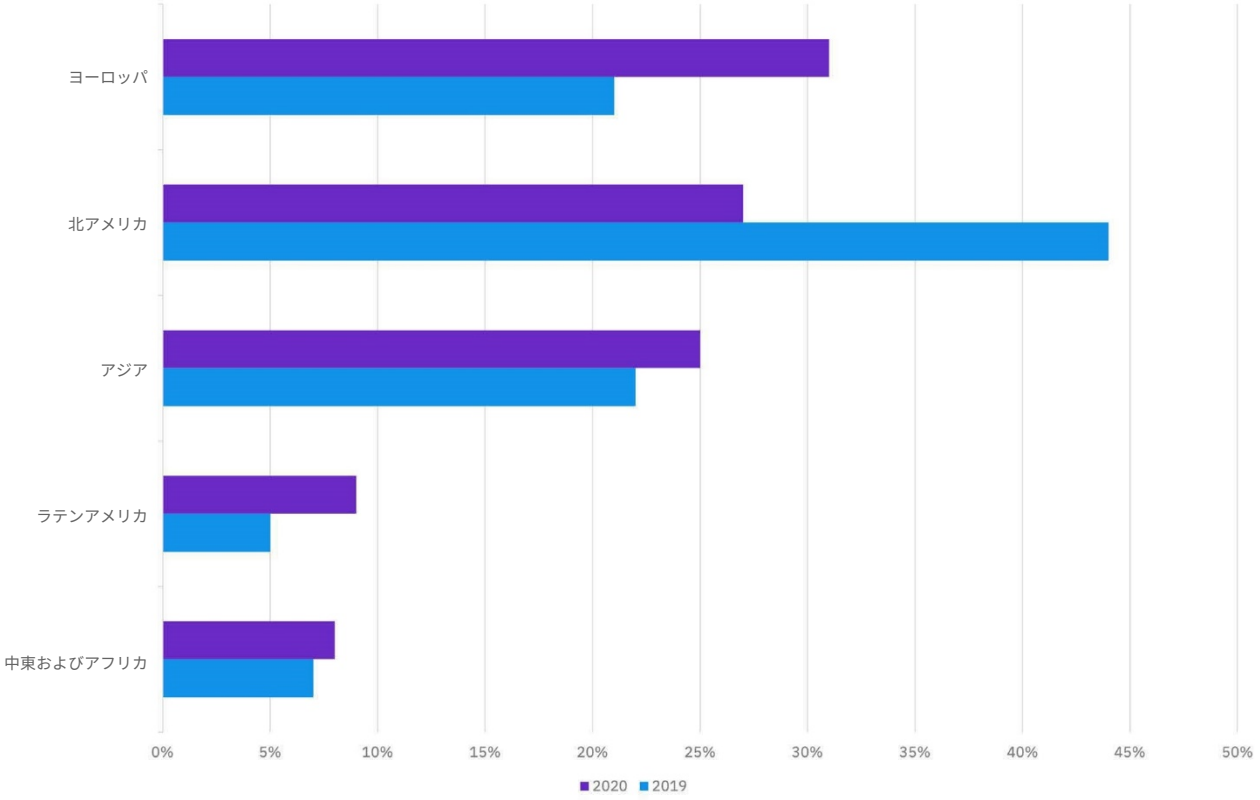
地理的な影響

2020 年、脅威アクターの活動が集中し、攻撃の大部分を受けたのはヨーロッパ、北アメリカ、アジアでした。その理由として、これらの大陸が占める富の割合が高い（世界の GDP の 89% を超える）ことが考えられます。この 3 つの地域のうち、ヨーロッパの企業への攻撃が最も顕著に増加しています。これには、ランサムウェア攻撃、インサイダー攻撃、サーバー・アクセス攻撃が大きく影響しています。

図 15

攻撃の地理的内訳（2020 年と 2019 年の比較）

X-Force Incident Response が観測した全攻撃の地理的な分布（2020 年と 2019 年の比較）(出展: IBM Security X-Force)



ヨーロッパ

— **攻撃量**: IBM Security X-Force は、2020 年の攻撃の 31% がヨーロッパ地域で発生したことを確認しました。2019 年の 21% から大幅に増加しており、ヨーロッパは 2020 年に世界で最も頻繁に攻撃対象となった地域になりました。

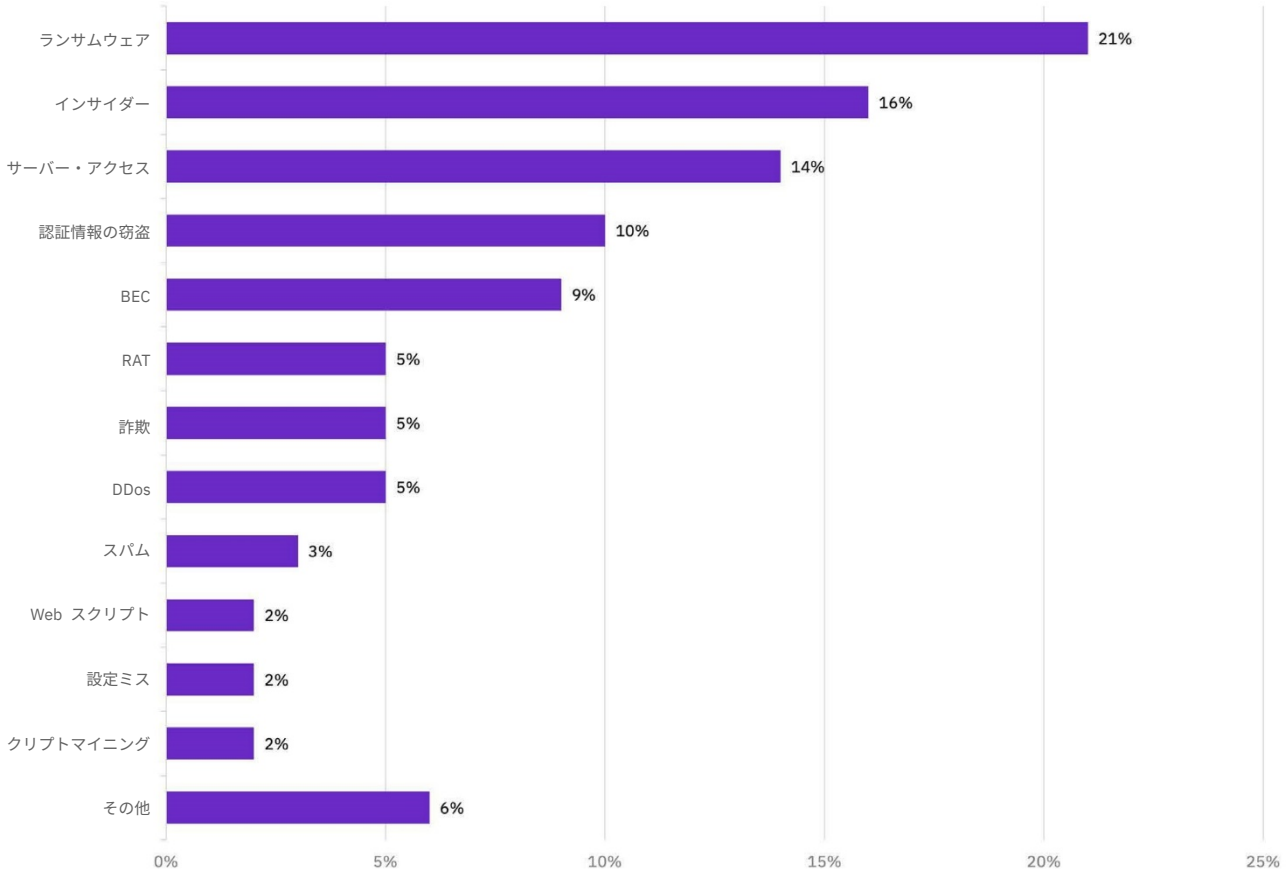
— **攻撃タイプ**: ランサムウェアは 2020 年に発生した全攻撃の 21% を占め、ヨーロッパで最もよく使われた攻撃手口となりました。この割合は高いものの、北アメリカにおけるランサムウェアの攻撃率よりは低くなっています。2020 年に、ヨーロッパは最も多くのインサイダー攻撃を受けました。これは、北アメリカとアジアで発生した攻撃の 2 倍の件数になります。ヨーロッパはさらに、大量のサーバー・アクセス攻撃も受けました。これは、2020 年の同大陸での全攻撃の 14% を占めています。認証情報の盗難、ビジネス・メール詐欺 (BEC)、リモートアクセス型トロイの木馬 (RAT)、不正行為や DDoS も、割合は低いものの、2020 年にヨーロッパの企業に影響を及ぼしました。2020 年には全世界で CVE-2019-19781 を悪用した攻撃が観測されましたが、そのうちの 33% はヨーロッパで発生したものでした。これは、他のどの地域よりも高い数値です。

— **攻撃を受けた国**: 2020 年にヨーロッパで最も頻繁に攻撃対象となった国は、英国、スイス、フランス、イタリアでした。

図 16

ヨーロッパへの攻撃タイプ

ヨーロッパへの全攻撃の攻撃タイプ別内訳 (X-Force Incident Response のデータ、2020 年) (出展: IBM Security X-Force)



北アメリカ

— **攻撃量**: 2020 年に X-Force が対処した全攻撃の 27% が北アメリカにおけるものでした。前年度より順位を下げ、世界で 2 番目に攻撃が多かった地域となりました。これは、この地域が全攻撃の 44% を占めていた 2019 年とは全く対照的です。ヨーロッパとアジアにおける攻撃率の増加が、この変動の最も大きな要因です。

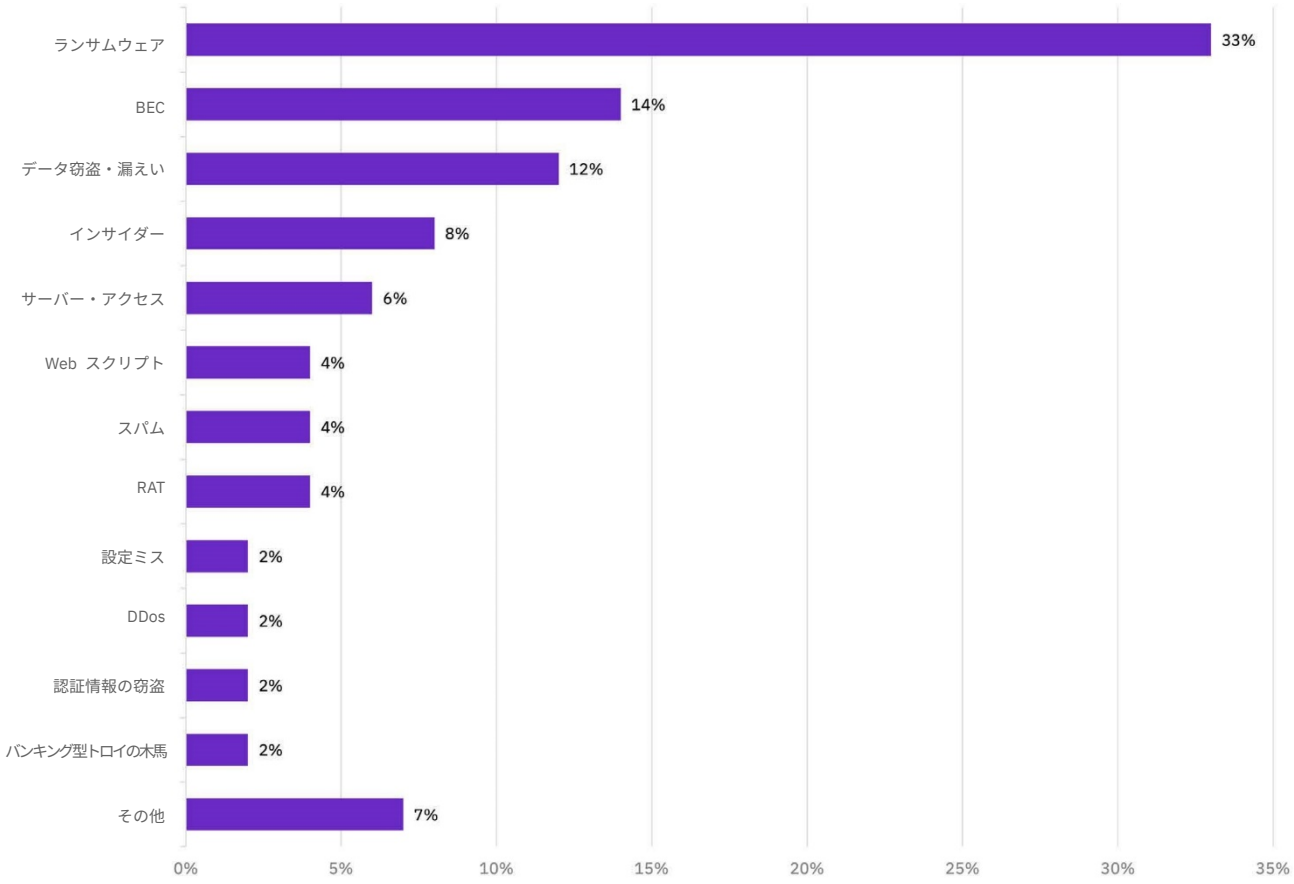
— **攻撃タイプ**: 北アメリカは、攻撃件数で見ると、他のどの地域よりも多くのランサムウェア攻撃を受けました。これは、2020 年の北アメリカに対する全攻撃の 33% を占めます。2020 年に、北アメリカの企業は、BEC、データ窃盗、データ漏えいや RAT などの大量の攻撃を受けました。また、CVE-2019-19781 を悪用した全攻撃の 29% が北アメリカで観測されました。これは、ヨーロッパに次いで 2 番目の多さです。

— **攻撃を受けた国**: 2020 年に北アメリカで最も頻繁に攻撃対象となった国は米国で、次いでカナダとなりました。

図 17

北アメリカへの攻撃タイプ

北アメリカへの全攻撃の攻撃タイプ別内訳 (X-Force Incident Response のデータ、2020 年) (出展: IBM Security X-Force)



アジア太平洋

— **攻撃量**: アジア太平洋地域への攻撃は、2020 年に IBM Security X-Force によって観測された全攻撃の 25% を占めました。2019 年の 22% から増加しています。

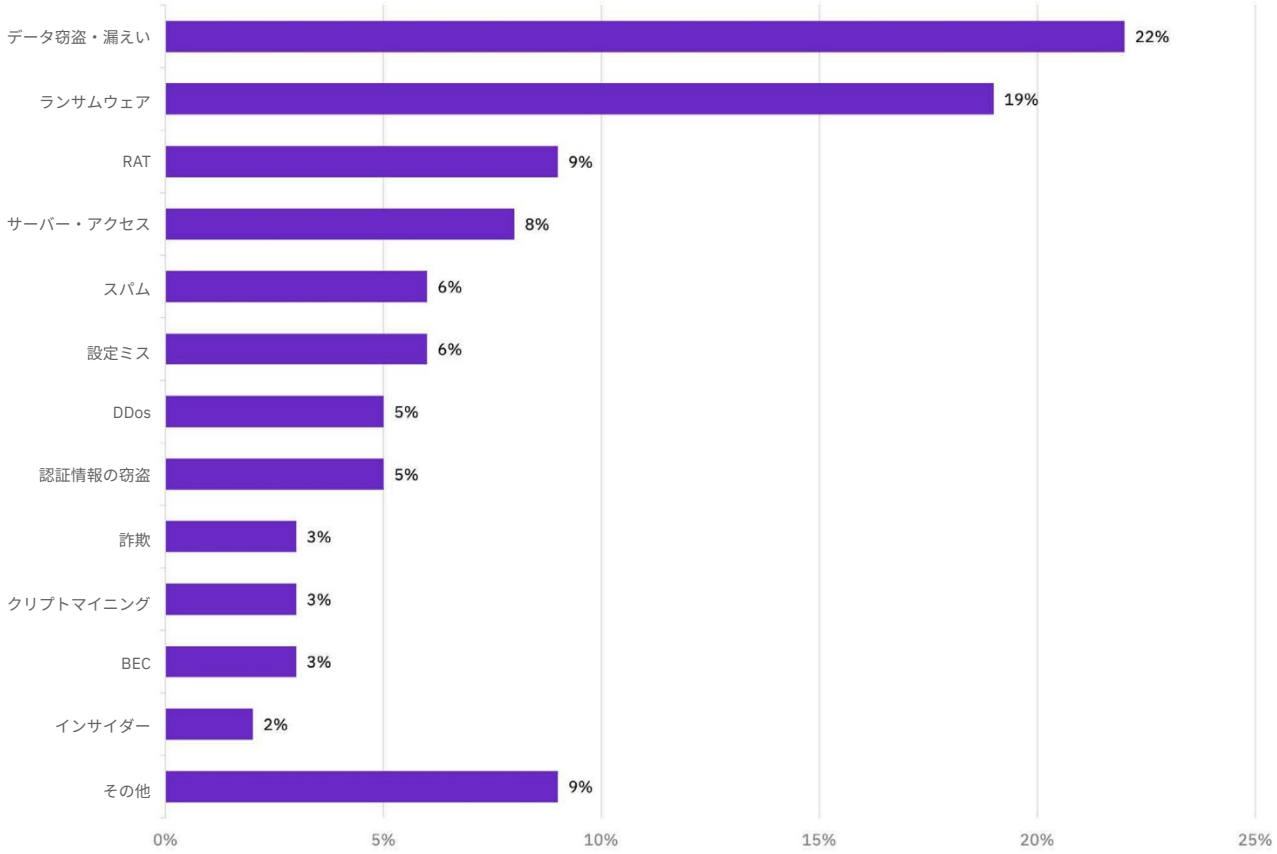
— **攻撃タイプ**: 2020 年にアジアで最もよく見られた攻撃手口は、ランサムウェアを抑え、データ窃盗でした。これには、2020 年秋に活発化した Emotet データ窃盗攻撃が大きく影響しており、この地域における全攻撃の 22% を占めました。ランサムウェア攻撃は、アジアにおける 2020 年の全攻撃の 19% を占めており、PJX や Locky などのランサムウェアが含まれていました。アジア太平洋は、RAT に関係する攻撃を世界で一番多く受けました。リモートアクセス型トロイの木馬は、2020 年のこの地域における全攻撃の 9% を占めました。アジアもまた 2020 年に、CVE-2019-19781 を悪用した攻撃を受けており、その割合は全体の 21% でした。2020 年のアジアにおける BEC 攻撃は、他の地域に比べるとそれほど多くありませんでした。その理由として、多要素認証を実装したことが影響している可能性が挙げられます。アジア太平洋地域で最も頻繁に攻撃対象となった業界の上位 2 位は、製造業、金融・保険業でした。

— **攻撃を受けた国**: 2020 年にアジアで最も頻繁に攻撃対象となった国は日本で、これを大きく下回って、インド、オーストラリアと続きます。

図 18

アジアへの攻撃タイプ

アジアへの全攻撃の攻撃タイプ別内訳 (X-Force Incident Response のデータ、2020 年) (出展: IBM Security X-Force)



中央アメリカおよび南アメリカ

— **攻撃量**: 中央アメリカと南アメリカの企業への攻撃は、2020 年に IBM Security X-Force が観測した全攻撃の 9% でした。これは、2019 年の 5% から増加しています。

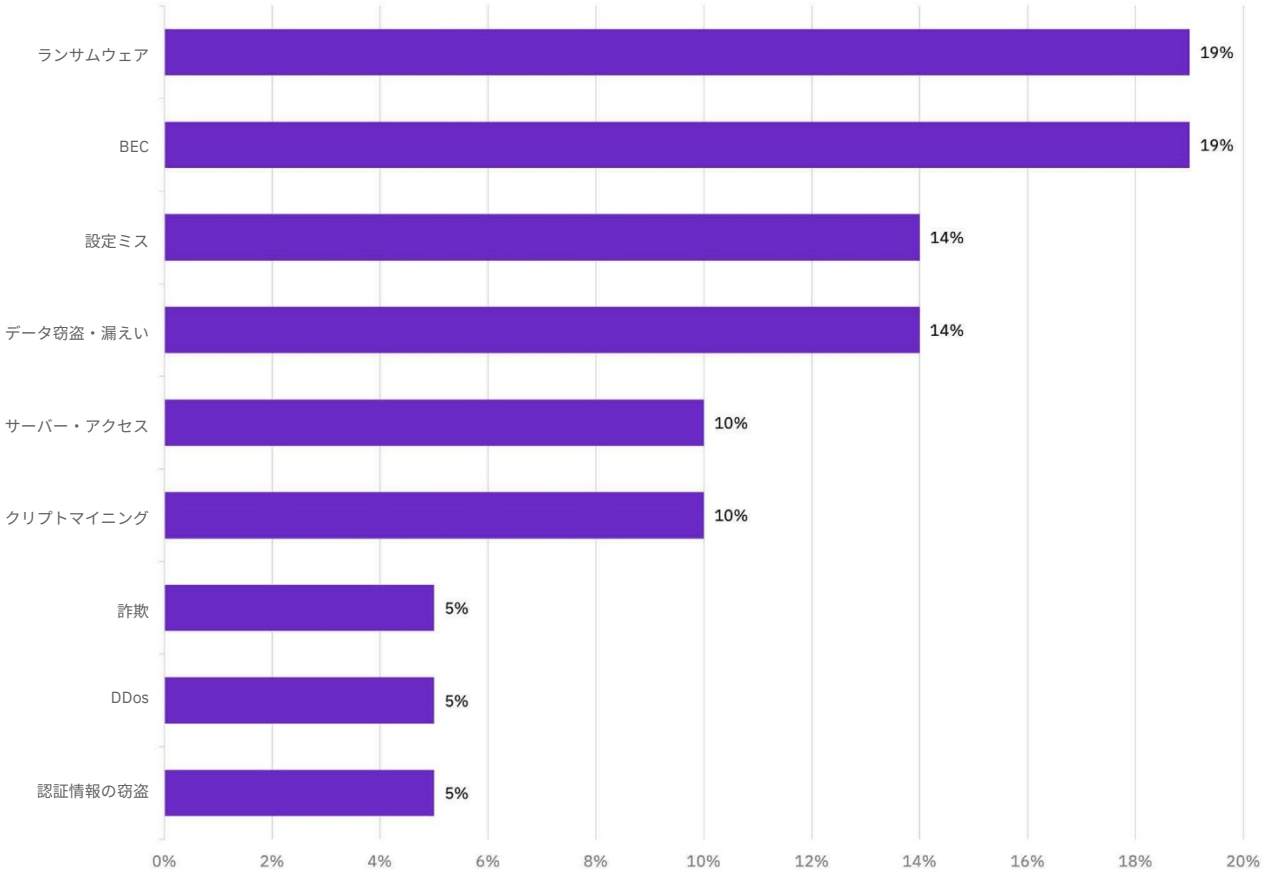
— **攻撃タイプ**: 中央アメリカと南アメリカでは、ランサムウェアと BEC が同率で最上位の攻撃手口になりました。いずれもこの地域における攻撃の 19% を占めています。次いで、設定ミス、データ窃盗、データ漏えいが僅差で続きました。中央アメリカと南アメリカでは特に、設定ミスによるインシデントが北アメリカやヨーロッパよりも多く見られました。一方、サーバー・アクセス攻撃については、他の地域ほど大きな影響を受けませんでした。

— **攻撃を受けた国**: 2020 年に中央アメリカと南アメリカで最も頻繁に攻撃対象となった国はブラジルでした。

図 19

中央アメリカおよび南アメリカへの攻撃タイプ

中央アメリカおよび南アメリカへの全攻撃の攻撃タイプ別内訳（X-Force Incident Response のデータ、2020 年）
(出展: IBM Security X-Force)



中東およびアフリカ

— **攻撃量**: 2020 年の X-Force のデータによると、中東とアフリカの企業への攻撃は、全攻撃の 8% でした。前年の 7% からわずかに増加しています。

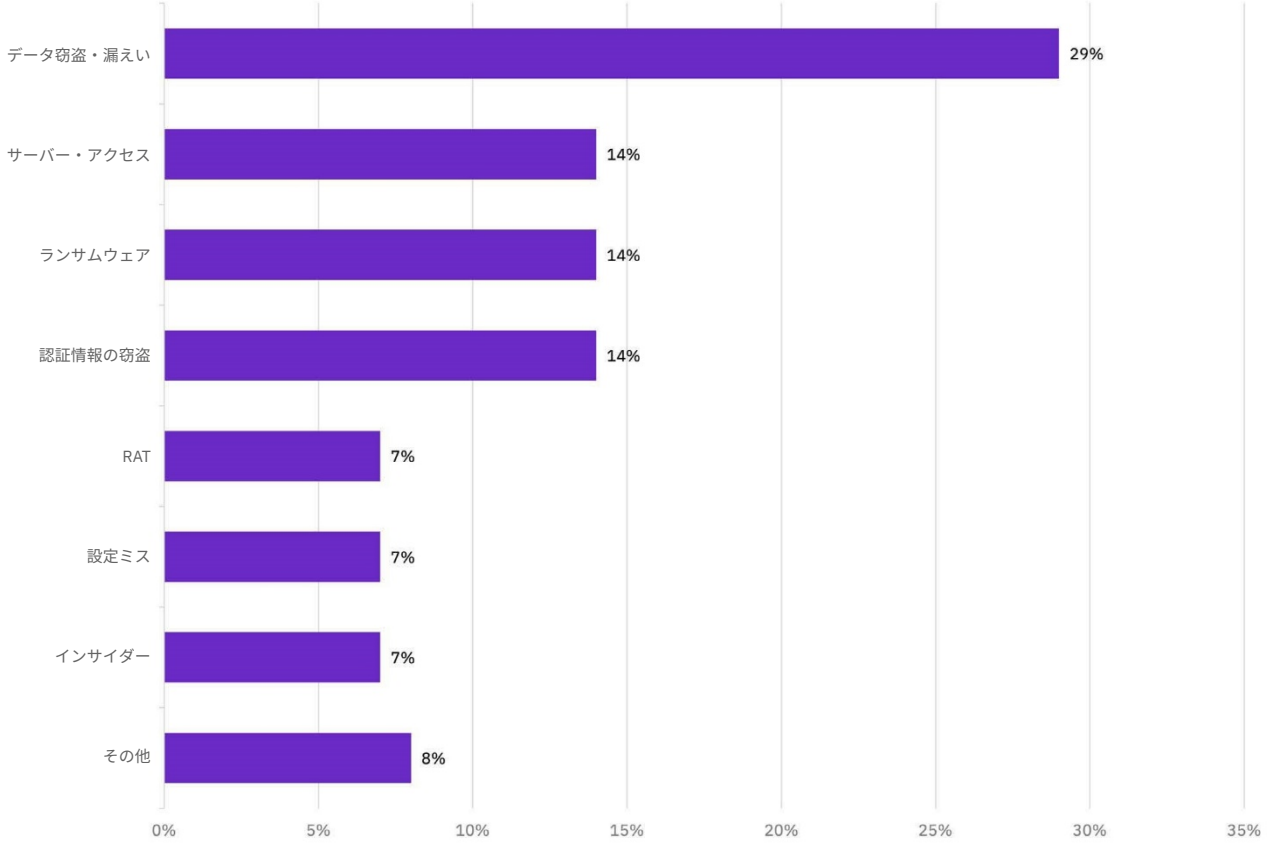
— **攻撃タイプ**: 2020 年に中東とアフリカで群を抜いて多かった攻撃手口は、データ窃盗とデータ漏えいです。全攻撃の 29% で、この地域においてかなりの比率を占めました。サーバー・アクセス、ランサムウェア、認証情報の窃盗が同率で 2 位となり、それぞれが攻撃の 14% を占めました。2020 年は、RAT、設定ミス、インサイダー脅威も、中東とアフリカの企業に影響を及ぼしました。

— **攻撃を受けた国**: 2020 年に中東とアフリカで最も頻繁に攻撃対象となった国は、サウジアラビア、アラブ首長国連邦、南アフリカ、トルコでした。

図 20

中東およびアフリカへの攻撃タイプ

中東およびアフリカへの全攻撃の攻撃タイプ別内訳 (X-Force Incident Response のデータ、2020 年)
(出展: IBM Security X-Force)



最も頻繁に攻撃対象となった業界

X-Force は毎年、最も頻繁に攻撃対象となった上位 10 業界を特定し、攻撃の比率に基づいてランク付けしています。最も頻繁に攻撃対象となった業界は、5 年連続で金融・保険業であり、これらの企業に脅威アクターが強い関心を持ち続けていることを示しています。

しかし、それ以外の業界のランキングは昨年から大きく変化しています。2019 年に 8 位だった製造業は、2020 年には 2 位に急上昇しました。要因としては、悪意あるアクターが OT に関連するインフラストラクチャーへの攻撃に関心を持っていることが考えられます。同様に、エネルギー業も 2019 年の 9 位から 2020 年は 3 位まで急上昇しており、攻撃者が OT 関連企業に注目していたことをさらに裏付けています。医療部門は 2019 年の最下位から 2020 年は 7 位に上昇しました。これは新型コロナウイルスに関連した攻撃と、病院への相次ぐランサムウェア攻撃に牽引されたものと思われます。運輸業は 2020 年に攻撃が減少し続け、2019 年の 3 位から 9 位に下降しました。コロナウイルスの感染が拡大する中、交通機関や輸送の利用率が低下したためと思われます。

図 21

最も頻繁に攻撃対象となった上位 10 業界 (2020 年と 2019 年の比較)

(出展: IBM Security X-Force)

業界	2020 順位	2019 順位	変動
金融・保険業	1	1	-
製造業	2	8	6
エネルギー業	3	9	6
小売業	4	2	-2
専門サービス	5	5	-
政府機関	6	6	-
医療業界	7	10	3
メディア	8	4	-4
運輸業	9	3	-6
教育業界	10	7	-3

図 22

上位 10 業界への攻撃の内訳

2020 年に最も頻繁に攻撃対象となった業界（上位 10 業界への攻撃を比率で表示）(出展: IBM Security X-Force)

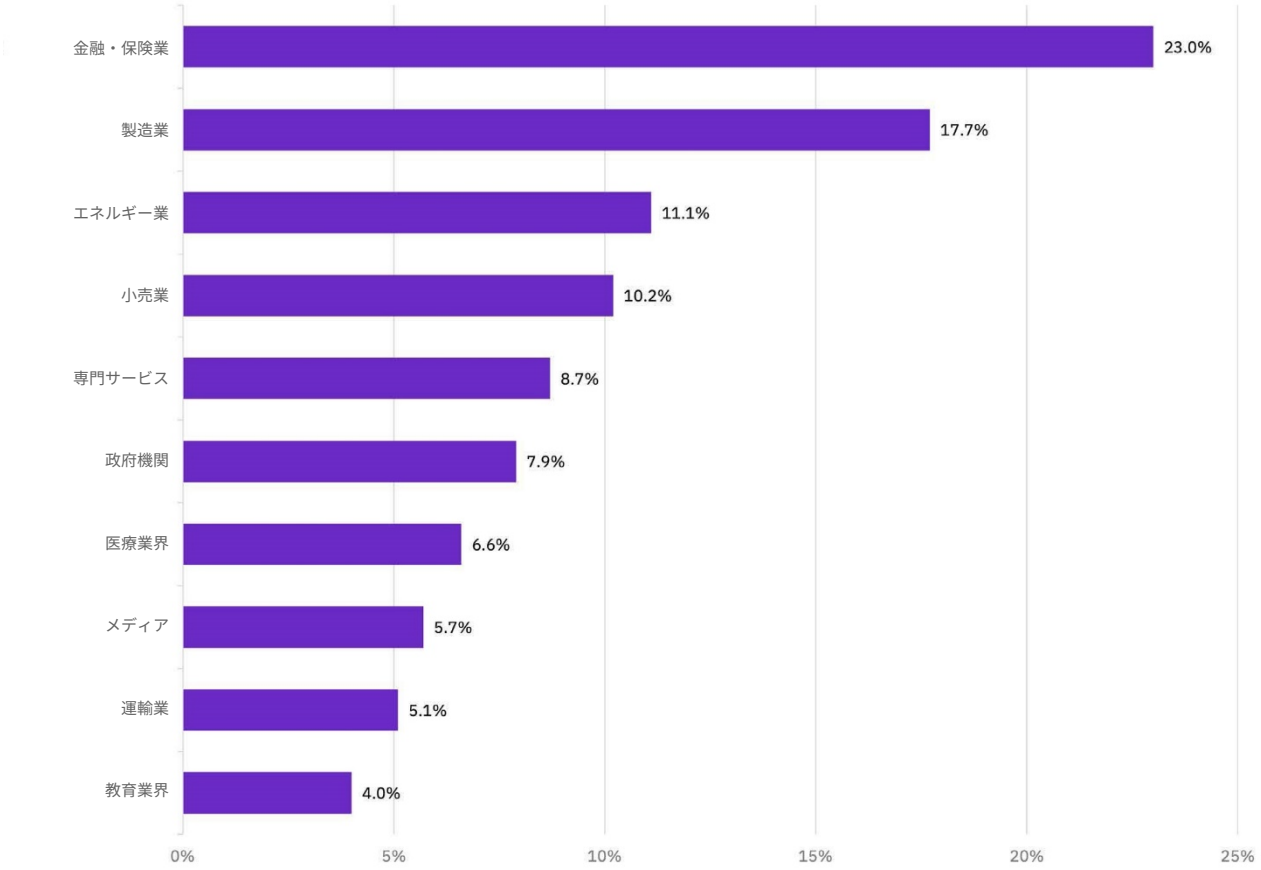


図 22 のチャートは、上位 10 の各業界に対する攻撃の比率を示しています。上位 10 業界への攻撃のうち 23% が金融・保険業に対するものでした。製造業への攻撃は 17.7% で、エネルギー (11.1%)、小売 (10.2%) と続き、残りの上位 10 業界への攻撃はそれぞれ 10% 未満でした。

図 23

業界への攻撃タイプ

業界への攻撃のタイプ別比率の内訳 (X-Force Incident Response のデータ、2020 年) (出展: IBM Security X-Force)

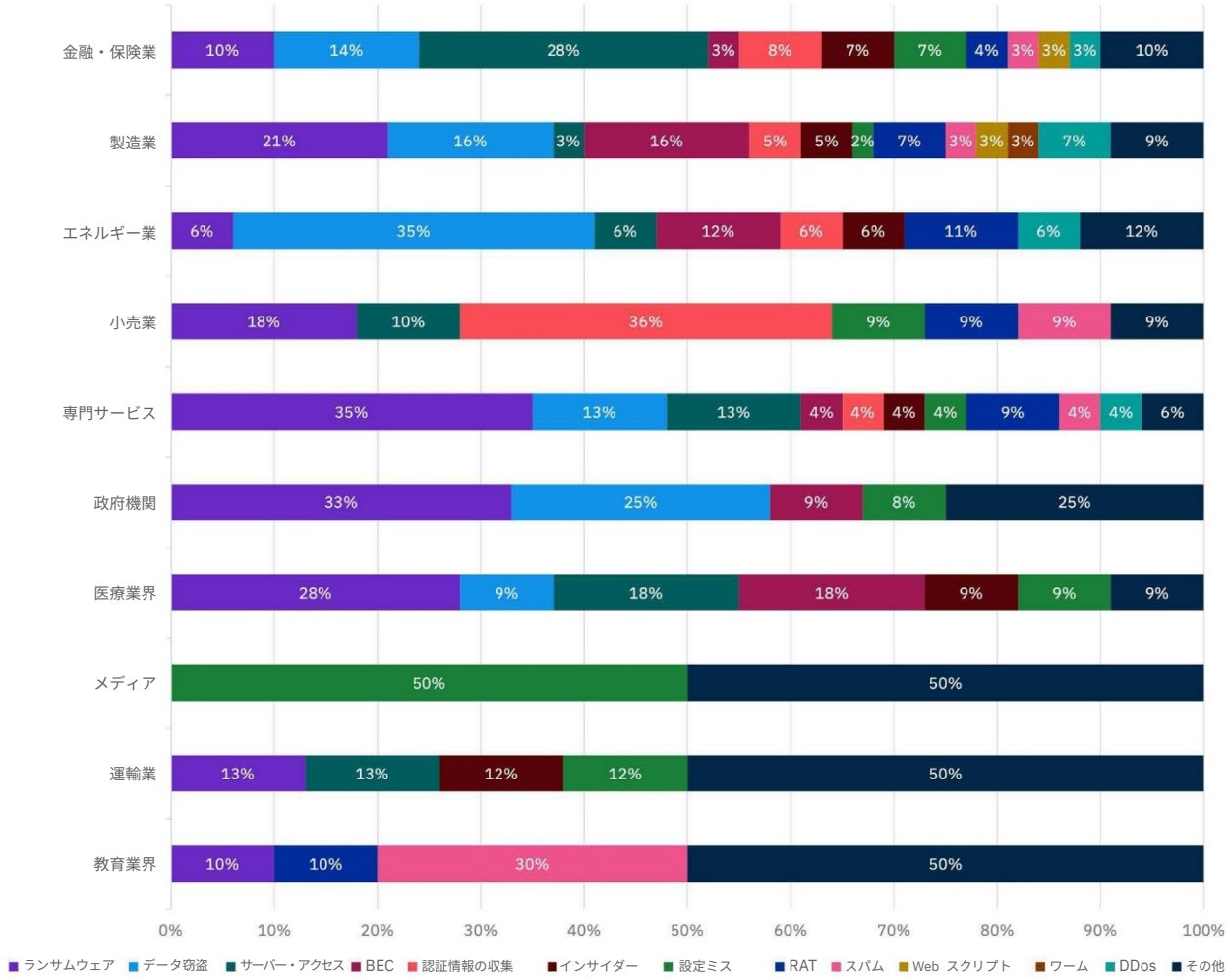


図 23 のチャートは、X-Force Incident Response のデータで、頻度の高かった各業界への攻撃を示しています。このデータとそこから得られた比率については、後続の各セクションで詳しく説明します。

金融・保険業

28%

サーバー・アクセス攻撃が 2020 年の金融・保険業への全攻撃に占める割合

10%

ランサムウェア攻撃が金融・保険業への全攻撃に占める割合

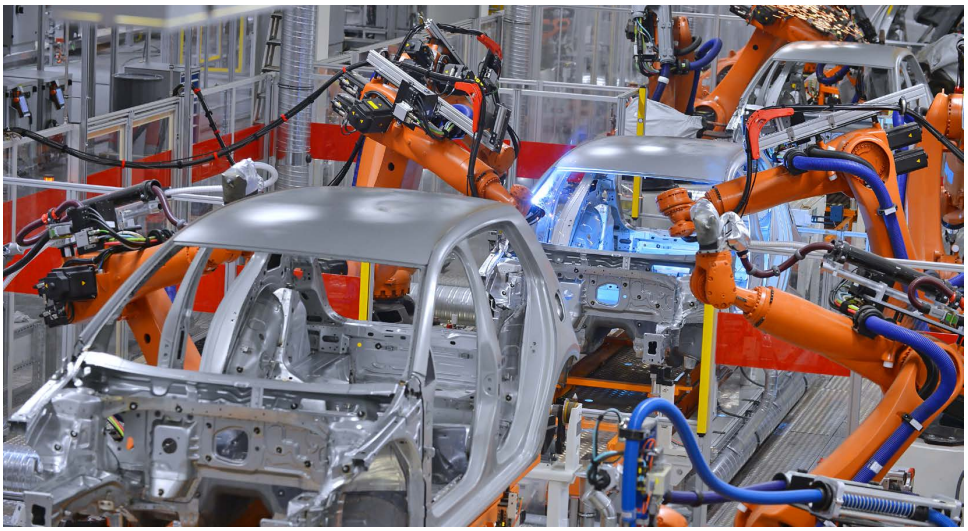
金融・保険業は、2016 年以降、最も頻繁に攻撃対象となった業界となっており、2020 年もその順位を維持しています。X-Force が 2020 年に分析した攻撃全体の 23% が金融機関に対するもので、2019 年の 17% から増加しています。

全業界の中で、最も多くのサーバー・アクセス攻撃を受けたのは、金融・保険業でした。これには主に、Citrix の脆弱性である CVE-2019-19781 が関係しています。サーバー・アクセス攻撃は、金融・保険業に対する全攻撃の 28% を占めています。CVE-2019-19781 を悪用した攻撃の比率は、金融・保険業と製造業で最も高くなり、同率で 22% を占めていました。

金融・保険業界の規制の厳しさや、サーバー・アクセス攻撃を積極的に特定して対処しようとする金融機関のアプローチが、この業界への攻撃比率の高さに影響していると考えられます。

さらに、製造業、専門サービス、政府など他の業界と比べると、金融・保険業へのランサムウェア攻撃は限定的でした。2020 年のこの業界への攻撃のうち、ランサムウェア攻撃はわずか 10% でした。ランサムウェア攻撃者は、金融機関以外の組織の方が、ランサムウェア攻撃の効果が高いと考えている可能性があります。その理由としては、金融・保険機関は強固なセキュリティー対策が施されていることから、攻撃者が、製造業や専門サービスはランサムウェア攻撃によるダウンタイムへの耐性が低いと考えていることなどが挙げられます。

製造業



21%

ランサムウェア攻撃が製造業への全攻撃に占める割合

4 倍超

製造業で発生した BEC 攻撃が他業種で発生した BEC 攻撃との比較

2020 年に最も頻繁に攻撃対象となった業界として、製造業は 2019 年の 8 位から上昇して 2 位に入りました。製造業への攻撃は上位 10 業界に対する全攻撃の 17.7% に上り、昨年の 8.1% から倍増しました。脅威アクターが再び製造業に注目している（製造業は 2015 年には 2 位、2017 年には 3 位にランクイン）のは、この業界が、特にランサムウェア、BEC、リモートアクセス型トロイの木馬攻撃の標的として魅力的であることを示しています。

2020 年の製造業に対する攻撃のうち、21% はランサムウェアによるものでした。この比率の高さは、脅威アクターが製造業をランサムウェア攻撃にとって有益な業種であると考えていることを示しています。また、攻撃件数の観点でも、製造業は他の業種よりも多数のランサム攻撃を受けています。この業界のダウンタイムに対する耐性の低さ（ダウンタイム 1 時間あたりの損失が数百万ドルに上ることもよくあります）は、脅威アクターに高い利益をもたらす要因になっていると考えられます。

ランサムウェア以外に、2020 年の製造業への攻撃では BEC が 17% を占め、その攻撃件数は他業種の 4 倍を超えています。多くの場合、製造業の企業は複数の供給業者から様々な部品を調達する必要があります。脅威アクターはこれを様々な方法で悪用し、電子メールのやり取りを偽装して、本来は供給業者に支払われるべき資金を別の口座に入金させます。製造業を狙う攻撃者の多くは、OT を標的とするのではなく、ソーシャル・エンジニアリングによって金銭を得ることを狙っているようです。

製造業でも、2020 年に受けた CVE-2019-19781 を悪用した攻撃が全体の 22% を占め、金融・保険業と同率 で 1 位になりました。

エネルギー業

35%

データ窃盗・漏えいがエネルギー業への全攻撃に占める割合

2020 年の最も頻繁に攻撃対象となった上位 10 業界への攻撃のうち、エネルギー業への攻撃は 11.1% で、昨年の 9 位から 3 位に上昇しました。エネルギー企業は 2020 年のサーバー・アクセス攻撃 (特に CVE-2019-19781 を悪用した攻撃) によって大きな被害を受け、エネルギー業界は攻撃件数で医療に次いで 4 位に入りました。

データ窃盗及びデータ漏えいは、エネルギー業界で最も多かった攻撃手口で、この業界への攻撃全体の 35% を占めました。これはデータ窃盗マルウェアやフィッシング攻撃の脅威を明確に示すものです。これらの攻撃の多くは、特に石油・ガス会社を狙ったものでした。

BEC 攻撃、デジタル通貨マイニング、ランサムウェア、リモートアクセス型トロイの木馬、サーバー・アクセス攻撃も、2020 年のエネルギー業界に影響を与えましたが、他業種ほど目立った点はありませんでした。具体的には、エネルギー業へのランサムウェア攻撃は、この業界に対する攻撃全体のわずか 6% で、頻繁に攻撃された他の多くの業界よりも大幅に低い数字でした。

小売業

36%

小売業への攻撃において認証情報の窃盗を占める割合

18%

ランサムウェア攻撃が占める割合

小売業は、2020 年に最も頻繁に攻撃対象となった業界の 4 位となり、昨年の 2 位から順位を下げました。小売業への攻撃は、上位 10 業界に対する攻撃全体の 10.2% で、昨年の 16% から減少しました。クレジット・カード決済やその他の金融取引の中心として、小売業は長い間、悪意ある脅威アクターにとって格好の標的でした。

小売業への攻撃手口では、認証情報の窃盗攻撃が最も多く、2020 年の小売業に対する攻撃の 36% を占め、このタイプの攻撃件数では小売業が他のすべての業界を上回りました。また、ランサムウェア攻撃も頻発し、小売業への攻撃全体の 18% を占めました。X-Force Incident Response のデータによると、これらのランサムウェア攻撃のほぼ全てが Sodinokibi 攻撃によるものでした。

規模は比較的小さいものの、DDoS 攻撃、詐欺、設定ミス、RAT、サーバー・アクセス攻撃も、小売業界に影響を及ぼしました。これは、小売企業を狙った金銭目当ての脅威アクターが、広範囲にわたる攻撃手口を採用していることを意味します。

専門サービス

35%

2020 年の専門サービスへのランサムウェア攻撃が占める割合 – 全業界中最多

13%

専門サービスへの攻撃におけるデータ窃盗が占める割合—さらに 13% がサーバー・アクセス

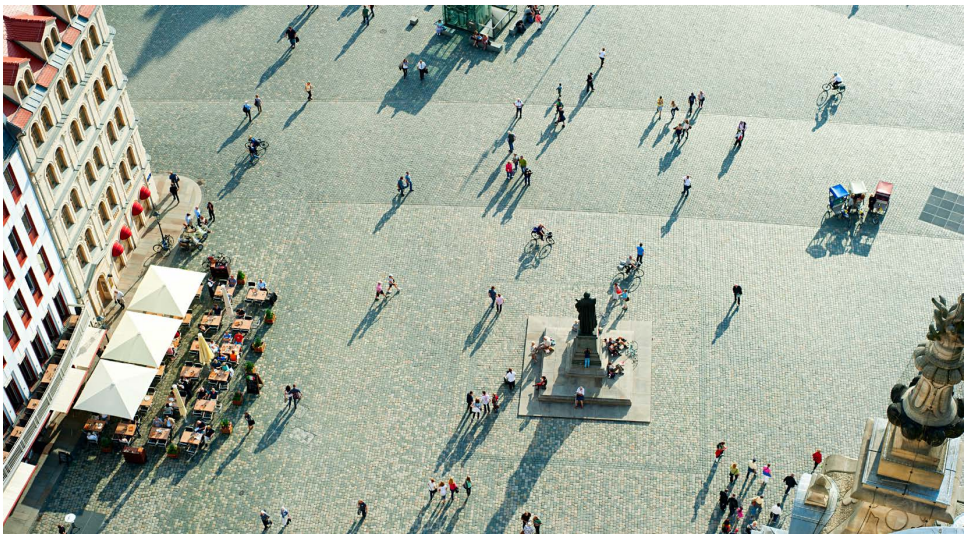
専門サービスは、2020 年に最も頻繁に攻撃対象となった業界の 5 位に入り、上位 10 業界に対する攻撃全体の 8.7% がこの業界で発生しました。2019 年においても 5 位で、この年に受けた攻撃は全体の 10% でした。専門サービスを提供する組織は、別の被害者に接近する手掛かりを得られるという点で、攻撃者にとっては特に魅力的な業界です。

2020 年の専門サービス企業におけるインシデントでは、ランサムウェアが全業界中最多の 35% を占めました。また、ランサムウェア攻撃の件数では、専門サービス業界が製造業に次ぐ 2 位となりました。2020 年に、一部のランサムウェア (Sodinokibi など) 攻撃者は、法律会社などの専門サービス企業を重点的に狙っていました。これらの企業は顧客の機密データを保持しており、顧客が著名人の場合もあります。こうしたことから、おそらく脅威アクターはこれらの企業が機密データの漏えいを回避するために、身代金を支払う可能性が高いと判断したものと思われます。ある法律事務所のデータが 4,000 万ドルでオークションに出されたこともあり、攻撃者が専門サービス企業のデータによって高額の身代金が得られると見込んでいることがうかがえます。

2020 年はランサムウェア攻撃に加えて、データ窃盗とサーバー・アクセス攻撃も専門サービス業に大きな被害を与え、いずれもこの業界への攻撃の 13% を占めました。これらの傾向は、専門サービス企業へのインジェクション攻撃と脆弱性を突いた攻撃が頻繁に行われており、脅威アクターの狙いが機密データへのアクセスであることを示唆しています。

専門サービス企業への攻撃手口では、リモートアクセス型トロイの木馬が 3 番目に多く、この業界への攻撃全体の 9% を占めていました。

政府機関



33%

政府機関への攻撃においてランサムウェア攻撃が占める割合 – 全業界で 2 番目に高い比率

25%

データ窃盗・漏えいが占める割合

防衛、行政、公的サービスなどの公共部門は、2020 年の最も頻繁に攻撃対象となった業界の 6 位で、上位 10 業界に対する全攻撃の 7.9% を占めました。全攻撃の 8% を受けた 2019 年と比較しても、大きな変更はありませんでした。IBM Security X-Force Incident Response のデータによると、2020 年の政府機関への攻撃ではランサムウェア攻撃が最も多く、データ窃盗が僅差でこれに続いています。

2020 年に政府機関を狙った攻撃のうち、33% がランサムウェアによる攻撃でした。これは専門サービス業界に次いで 2 番目に高い結果となりました。政府機関が引き続きランサムウェア攻撃の標的となっている傾向を示していますが、X-Force Incident Response は 2020 年に政府の司法機関や運輸当局も標的になっていたことを確認しています。2020 年に X-Force が観測した、政府機関に対するランサムウェア攻撃の約 50% は Sodinokibi 脅威アクターによるものでした。このグループが 2019 年 9 月にテキサス州の 23 の自治体に連続的なランサムウェア攻撃を仕掛けて以来、この傾向は続いています。

2 番目に多かった政府機関への攻撃手口はデータ窃盗及びデータ漏えいで、政府機関に対するデータ窃盗とスパイ活動の脅威が明確に表われています。データ窃盗・漏えい攻撃は、2020 年の政府機関に対する攻撃の 25% を占めていました。外国政府、サイバー犯罪者、さらにはハクティビストまでもが政府機関からのデータ窃盗に関心を持っていることが明らかになりました。

規模は比較的小さいとはいえ、2020 年は BEC 攻撃も政府機関に影響を与え、全攻撃の 9% を占めました。これは X-Force が調査した全業界への BEC 攻撃で 4 番目に高い比率でした。多要素認証技術の実装をより一層強化することで、将来的にこの比率を低減できる可能性があります。

医療業界

28%

医療業界への攻撃においてランサムウェア攻撃の占める割合

17%

CVE-2019-19781 インシデントが医療業界で発生した割合

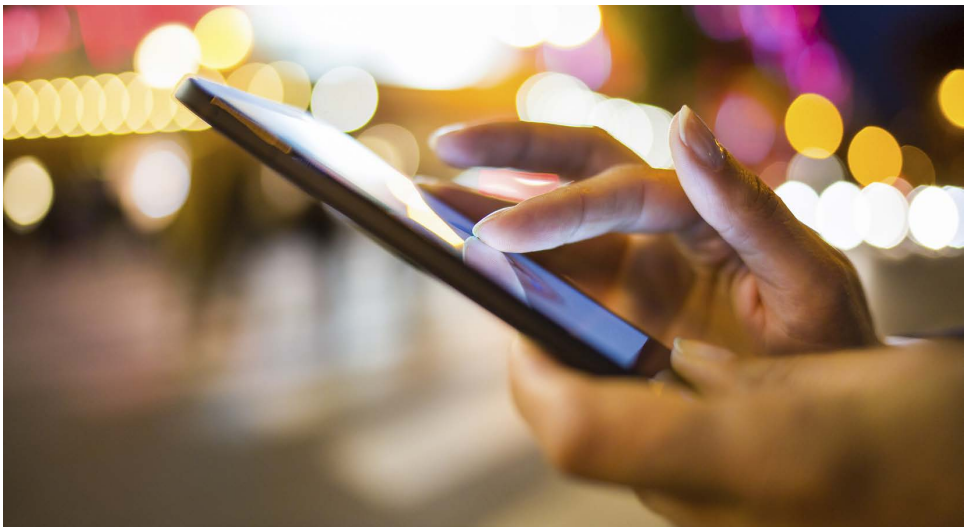
2020 年、医療業界は最も頻繁に攻撃対象となった業界の第 7 位でした。医療業界への攻撃は、上位 10 業界に対する攻撃全体の 6.6% を占め、3% で 10 位だった 2019 年から倍増しています。これはかなりの増加率であり、2020 年に新型コロナウイルス感染症が拡大する中、医療業界が、ランサムウェア攻撃や、コロナウイルス関連の研究と治療を標的にする脅威アクターから頻繁に狙われていたことを示しています。

2020 年の医療業界に対する攻撃の約 28% はランサムウェア攻撃によるものでした。医療業界へのランサムウェア攻撃は、惨事を引き起こすことがあります。2020 年 9 月、ドイツの病院を襲ったランサムウェア攻撃では、救急車が患者を 20 マイル離れた別の病院へ搬送せざるを得なくなるという深刻な事態が発生し、その後この患者は死亡しました。ドイツ当局はランサムウェア攻撃が死亡の直接的な原因ではないと断定しましたが、将来的にはこのような攻撃が患者の死亡に直接つながる可能性があります。

10 月下旬、Ryuk を使ったサイバー犯罪者が、米国の 400 を超える病院を攻撃しようとしていることをセキュリティー研究者が探知しました。米国の警察と IBM Security X-Force を含む複数のセキュリティー会社は、被害を受ける可能性のある病院に直ちに通知し、緩和策を特定しました。この対応によって、その翌週に実際に Ryuk の攻撃を受けた病院は、400 件以上のうちの 7 件になりました。

2020 年はランサムウェアに加えて、CVE-2019-19781 を悪用した医療ネットワークへのアクセスも多発しました。医療は 3 番目に多くこの CVE を悪用された業界であり、全業界に対するこの攻撃の 17% を占めていました。医療ネットワークに CVE-2019-19781 が関与した少なくとも 1 つの事案において、脅威アクターはその活動に PowerShell と Cobalt Strike を組み合わせて横展開を図り、目的を果たしました。

メディアおよび情報通信業界



90%

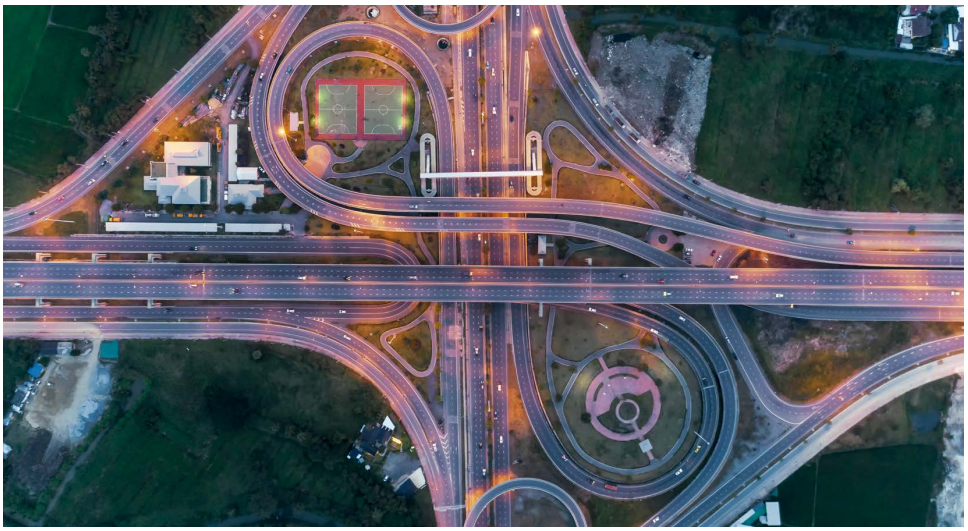
悪意ある DNS スクワッティングがメディアに向けられる割合—スプーフィングは全業界中最多

メディアおよび情報通信業界は、2020 年の最も頻繁に攻撃対象となった業界の 8 位で、上位 10 業界に対する全攻撃の 5.7% を占めました。10% の攻撃を受けた昨年の 4 位から順位は下がりました。この業界には、電気通信事業者やモバイル通信事業者のほか、メディアやソーシャル・メディア機関も含まれます。これらの企業は、特に選挙戦の年には政治の動向において、重要な役割を果たします。

X-Force の観測によると、2020 年のメディアに対する攻撃手口では、設定ミスが最多でした。これは、予期せぬデータ漏えいを防ぐためには、クラウド・インスタンスの適切な設定が重要であることを明確に示しています。

Quad9 のデータによると、悪意のあるアクターが正当なメディア発信源とよく似た URL を作成し、スプーフィングを最も多く仕掛けたのはメディア業界でした。悪意ある DNS スクワッティング（正規の Web ページとよく似た紛らわしいドメイン・ネームを使用する手口）の約 90% がメディア機関に関係していました。これは本レポートで前述した、最も頻繁に行われたブランド・スプーフィングの傾向を反映するものであり、脅威アクターがメディア企業に対する消費者の人気や信頼を利用しようとしていることを示しています。

運輸業



25%

2020 年の運輸業への攻撃において悪意あるインサイダーまたは設定ミスが占める割合

運輸業は今年の IBM Security X-Force のランキングで 9 位となり、製造業とは逆に、2019 年の 3 位、2018 年の 2 位から大幅に順位を下げました。運輸業への攻撃は 2020 年の攻撃全体の 5.1% を占めており、2019 年の 10% から減少しました。

運輸業に対する攻撃が 2020 年に減少した理由はいくつか考えられます。例えば、新型コロナウイルスの感染拡大と外出禁止令によって、2020 年は交通や輸送機関の利用が減少したため、金融情報の入手を目論むサイバー犯罪者にとっても、標的とする人物を追跡している国家にとっても、脅威アクターから見たこの業界の採算性が低下した可能性を示唆しています。さらに、運輸業におけるセキュリティー対策の強化と脅威インテリジェンスの積極的な利用が、この業界での攻撃の減少に影響している可能性があります。

悪意あるインサイダーと設定ミスのインシデントは、2020 年の運輸業に非常に大きな影響を与えました。特に他の業界と比較した場合、その影響は深刻です。これら 2 つの攻撃手口を合わせると、2020 年の運輸業に対する全攻撃の約 25% に達します。

運輸業に対するインサイダー攻撃の脅威は甚大です。最大級の損害を与えるサイバー攻撃（人命の損失につながるような攻撃）が現実化する可能性は、インサイダーが関与している場合に最も高くなるからです。

また、ランサムウェア攻撃とサーバー・アクセス攻撃は、2020 年の運輸業に対する攻撃の 26% を占めていました。

教育業界

50%

スパムまたはアドウェアが 2020 年の教育業界への全攻撃に占める割合

10%

ランサムウェア攻撃が占める割合

教育業界は、2020 年の最も頻繁に攻撃対象となった業界の 10 位で、この業界への攻撃は上位 10 業界に対する攻撃全体の 4% でした。全体の 8% の攻撃を受けた 2019 年の 7 位から順位は下がりました。

スパムとアドウェアは、2020 年の教育業界で多発した攻撃手口でした。両手口を合わせると、教育業界に対する全攻撃の 50% に達します。これらの攻撃の約半数はスパムによるものです。これは全業界中最も高い比率で、教育機関に対するフィッシング関連の脅威の高さが明確に表れています。

X-Force の観測によると、他の業界ほど大規模ではありませんが、教育業界もランサムウェア攻撃の標的として狙われていました。2020 年の教育業界に対する攻撃のうち、ランサムウェア攻撃は 10% を占めていました。 公表された漏えいデータによると、2020 年に複数の学校や大学がランサムウェア攻撃を受け、そのうちの数校が身代金を支払いました。

教育業界への攻撃にはボットネット、詐欺、RAT も使われました。2020 年は、代表的なサイバー攻撃の手法であるフィッシングと、コモディティー化されたマルウェアが、教育機関にたびたび脅威をもたらしました。

将来の展望

2021 年には、新旧の脅威が混在するため、セキュリティー・チームは同時に多数のリスクを考慮することが求められます。X-Force の分析に基づいて、2021 年に優先的に考慮すべき重要事項を以下に示します。

- **リスクの範囲は 2021 年も引き続き拡大する。**新旧両方のアプリケーションやデバイスで、数千種類の新しい脆弱性が報告されるでしょう。
- **ランサムウェアによる二重の恐喝は 2021 年も引き続き発生する。**ランサムウェアの脅威アクターは、さらに巧妙な手口を使って、リークサイトでのデータの公表をちらつかせ、高額な身代金を要求します。
- **脅威アクターは、今後も様々な攻撃手口に照準を移していく。**Linux システム、OT、IoT デバイス、クラウド環境は、引き続き攻撃対象となります。こうしたシステムやデバイスへの攻撃が高度化するにつれて、脅威アクターは手法を素早く変更すると考えられます。特に注目度の高いインシデントの後は、その傾向が顕著になります。
- **どの業界にもリスクは存在する。**各業界における攻撃状況は前年から変化しています。リスクはすべての業界にあると考え、業界の枠を超えてサイバーセキュリティー・プログラムを意味のあるものに進化、成熟させていく必要があります。

レジリエンスに関する推奨事項

このレポートで説明した IBM X-Force の知見に基づいて、脅威インテリジェンスの最新情報を把握し、強力な対応能力を備えることが、あらゆる業界と国にとって、高度化する脅威から自組織を守り、被害を軽減するための効果的な方法です。

2021 年 のサイバー脅威に備えるために組織が実行できる対策として、X-Force は以下を推奨します。

脅威に反撃するのではなく、事前に脅威を阻止する。脅威インテリジェンスを活用して、脅威アクターの動機と戦術をより深く理解し、セキュリティーのリソースを優先順位付けします。

十分な備えによってランサムウェア攻撃に対処する。ランサムウェア攻撃への対応計画（ランサムウェアとデータ窃盗を組み合わせた脅迫手法への対応など）を策定し、その計画の実施訓練を定期的に行うことによって、重大な局面での対応を格段に強化することができます。

組織のパッチ管理の構造を二重にチェックする。2020 年はスキャンとエクスプロイトが攻撃手口として最も多かったことを踏まえて、インフラストラクチャーを補強し、内部での検知機能を刷新して、自動化された悪用攻撃を迅速かつ効果的に検知し遮断します。

インサイダー脅威を防止する。データ損失防止 (DLP) ソリューション、訓練、およびモニタリングによって、悪意あるインサイダーや不注意による組織への侵害を防ぎます。

組織内でインシデント対応チームを編成し、訓練する。それが難しい場合は、インシデント対応能力を有効活用し、影響力の大きいインシデントに速やかに対応できるようにします。

組織のインシデント対応計画のストレス・テストを実施し、即時対応力を身につける。インシデント対応チームが机上演習やサイバー・レンジの実体験によって重要な経験を積むことで、データ漏えい発生時の対応時間やダウンタイムを短縮でき、最終的にコストも削減できます。

多要素認証 (MFA) を実装する。アカウントの保護レイヤーを増強することは、今後も組織にとって優先すべき最も効果的なセキュリティー対策の 1 つです。

バックアップを実行、テストし、オフラインで保管する。ランサムウェア攻撃が再び多発していることを示す 2020 年のデータを踏まえて、バックアップの存在を確認するだけでなく、実際にそれをテストしてバックアップの有効性を点検することが、組織のセキュリティーを確保するうえで非常に重要です。

IBM Security X-Force について

IBM Security X-Force は、洞察、検知、対応能力を提供し、お客様がセキュリティー体制を強化できるよう支援いたします。

IBM Security X-Force 脅威インテリジェンスは、IBM セキュリティー運用テレメトリー、調査、インシデント対応調査、商用データ、オープンソースを組み合わせることで、お客様が新たに出現した脅威を把握し、セキュリティーに関する意思決定を情報に基づいて迅速に下せるように支援します。

さらに、熟練した X-Force インシデント対応チームは、組織がセキュリティー・インシデントやデータ漏えいに対する制御を向上させる上で役立つ戦略的な修復対策を提供します。

X-Force は、IBM Security コマンド・センターのサイバー・レンジでの体験を通して、お客様に今日の脅威の実態に備えるための訓練を提供しています。

また、IBM X-Force の研究者達が、年間を通じて、進行中の調査や分析の情報をブログ、ホワイト・ペーパー、Web セミナー、ポッドキャストで提供し、新たな脅威アクター、マルウェア、攻撃手法などについての洞察を紹介しています。さらに、プレミア脅威インテリジェンス・プラットフォームのサブスクリプションをご契約いただいているお客様には、最新かつ最先端の分析結果を数多く提供しています。

次のステップ

IBM Security によるインシデント対応の活用について検討する

IBM Security について

IBM Security は、AI を活用した先進的で統合されたエンタープライズ・セキュリティー製品とサービスのポートフォリオ、ゼロトラストの原則に基づくセキュリティー戦略への最新のアプローチを活用して、お客様のビジネスを保護し、不確実な状況下でも、お客様が成功するよう支援いたします。さらに、セキュリティー戦略をお客様のビジネスに合わせ、デジタル・ユーザー、資産、データを保護するために設計されたソリューションを統合し、高まる脅威に対する防御を管理するためのテクノロジーを導入することで、今日のハイブリッドクラウド環境をサポートする、リスクの管理と制御を支援します。

IBM の新しいオープン・アプローチの IBM Cloud Pak for Security プラットフォームは、RedHat Open Shift 上に構築されており、広範なパートナー・エコシステムによってハイブリッド・マルチクラウド環境をサポートします。Cloud Pak for Security は、データとアプリケーションのセキュリティーを管理できるようにする、企業向けのコンテナ化されたソフトウェア・ソリューションです。データを移動することなく既存のセキュリティー・ツールを迅速に統合し、ハイブリッドクラウド環境全体にわたる脅威に対するより深い洞察を引き出し、セキュリティー対応のオーケストレーションと自動化を容易にします。

詳細については、http://www.ibm.com/jp-ja/security をご覧ください。また、Twitter (@IBMSecurity をフォロー) や IBM Security インテリジェンス・ブログでも、より詳しい情報をご覧いただけます。

協力者

執筆責任者:
カミーユ・シングルトン

協力者:
アリソン・ウィクオフ
アリ・エイタン (Intezer)
チャールズ・デベック
シャーロット・ハモンド
チェンタ・リー
クリス・スペリー
クリストファー・キーファー
クレア・ザボエヴァ
デビッド・マクミレン
デビッド・モールトン
ダーク・ハーツ
ジョージア・プラシノス
イアン・ガラハー (Intezer)
ジョン・ゾラベディアン
ジョシュア・チャン
ケリー・ケイン
ローレン・ジェンセン
リモール・ケッセム
マーク・アッシャー
マシュー・デフィル
ミーガン・ラドナ
メリッサ・フリードリッヒ
ミシェル・アルヴァレズ
ミッチ・メイン
ニック・ロスマン
パティ・カーヒル-イングラハム
ランダル・ロッシ
リチャード・エマーソン
サライナ・ウッケ
スコット・クレイグ
スコット・ムーア

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2021 年 3 月