2020-2021

サイバーエスピオナージ報告書

エグゼクティブインサイト

verizon

サイバーエスピオナージ報告書（CER）は、ベライゾン初の高度なサイバー攻撃に関するデータを駆使した報告書です。本書は、7年分のデータ漏洩/侵害調査報告書（DBIR）とVTRAC（Verizon Threat Research Advisory Center）のサイバーエスピオナージ（スパイ活動）によるデータ漏洩/侵害対応に関する14年以上にわたって蓄積された専門知識に基づいています。このCERは、サイバースパイ攻撃に対するサイバー防衛体制やインシデント対応（IR）機能を会社のために支えているサイバーセキュリティの専門家のためのガイドです。

サイバースパイ活動の攻撃者は、サイバー防御およびインシデント対応の担当者に個別の挑戦を仕掛けてきます。高度な技術を使ったり、特定のポイントに焦点を当てたりする攻撃者たちは、強固に保護された環境に迅速かつ密かにアクセスしようとします。攻撃者の目的にもよりますが、彼らはネットワーク内を自由に動き回り、ターゲットのアクセス権やデータを取得し、検知されることなく出ていきます。あるいは少し離れたところに居座り続けます。

スパイ活動を行う攻撃者は、国家関連組織（または州関連組織）、競合他社、あるいは犯罪組織の可能性もあります。彼らのターゲットは公共部門（政府）と民間部門（企業）の両方です。国家機密、知的財産、機密情報は国家安全保障や政治的な立場、経済的な優位性などにつながるため、このような情報を求めています。

サイバースパイ活動を実施する攻撃者の手口は、不正侵入すること、目立たないように紛れ込むこと（または完全に姿を隠すこと）、および機密性の高い資産やデータに不正アクセスすることなどです。技術の発達によりスパイ活動はこれまでよりスピーディ、効率的、回避的になり、その原因究明は難しくなっています。簡単に言うと、攻撃者にとってサイバースパイ活動は、比較的検知されるリスクが低く、リソースという観点からはコストも低く、報酬面では潜在機会の高い大きなチャンスなのです。

このCERでは、サイバースパイ活動の攻撃者とその被害者に関する要素を特定するだけでなく、こうしたサイバー攻撃を防止、低減、検知、およびそれに対する対応力を上げるためのフレームワークやツールについても特定します。フレームワークやツールとは、VERIS（Vocabulary for Event Recording and Incident Sharing：イベント記録とインシデント共有のための言語）フレームワーク、VIPR（Verizon Incident Preparedness and Response：インシデントへの準備と対応）についての報告書、NIST（National Institute of Standards and Technology：アメリカ国立標準技術研究所）のサイバーセキュリティフレームワーク、CIS（Center for Internet Security：インターネットセキュリティセンター）のCSC（Critical Security Controls：クリティカルセキュリティコントロール）、およびNAICS（North American Industry Classification System：北米産業分類システム）などです。

veriscommunity.net/

enterprise.verizon.com/resources/reports/vipr/

www.nist.gov/cyberframework

www.cisecurity.org/controls/cis-controls-list/

www.naics.com/

データ漏洩/侵害パターン

2014年度から2020年度DBIRの対象期間において全体的に多かったデータ漏洩/侵害のタイプに関しては、サイバースパイ活動は6位（10%）でしたが、4位の特権の悪用（11%）や減少している5位のPOSへの侵入（11%）に迫っています。

サイバースパイ活動は検知が難しいため、実際の数字はもっと高い可能性があります。またサイバースパイ活動によるデータ漏洩/侵害において盗まれるデータの種類（例：秘匿情報、内部情報、機密情報など）は、複数の法律や規制要件に基づく報告義務に該当しない場合があります。

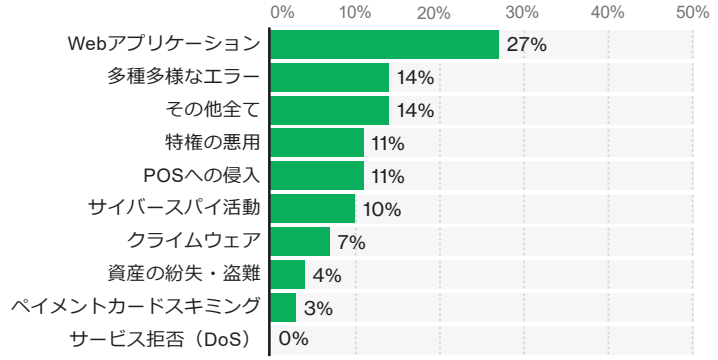

図1：データ漏洩/侵害のパターン（2014年度～2020年度DBIR、n=16,090）

発見までの時間

2014年度から2020年度のDBIRによると、サイバースパイ活動の攻撃者が不正アクセスするまでにかかる時間はわずか数秒から数日間、脱出するまでの時間は数分から数週間でした。これに対しサイバー防御担当者がサイバースパイ活動によるデータ漏洩/侵害を発見するまでの時間は数カ月から数年、また封じ込めまでの時間は数時間から数週間という結果でした。

攻撃者のプロセスは進みが遅く、整然としており、長いため、サイバースパイ攻撃は持続的かつ複雑です。つまり攻撃者は、ターゲットの環境やサイバーセキュリティ体制を理解し、その情報を利用して見つからないまま目的を達成することに細心の注意を払っているのです。

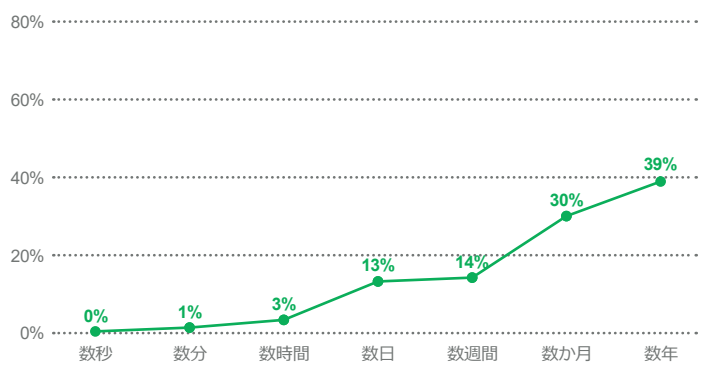

図2：サイバースパイ活動によるデータ漏洩/侵害を発見するまでの時間（2014年度～2020年度DBIR、n＝125）

ターゲットにされた犠牲者

被害にあった業種

DBIRのデータに基づき、過去7年間（2014年度から2020年度DBIRの対象期間）でサイバースパイ活動によるデータ漏洩/侵害の影響を最も強く受けた業種を以下の通り特定しました：教育業（NAICS 61）、金融業（NAICS 52）、情報産業（NAICS 51）、製造業（NAICS 31–33）、鉱業および公益事業（NAICS 21+22）、専門業（NAICS 54）、公務（NAICS 92）。

サイバースパイ活動によるデータ漏洩/侵害の被害を受けた7つの業種のうち、他よりも被害の大きかったトップ3の業種は以下の通りです：公務（31%）、製造業（22%）、専門業（11%）。

あなたの会社の業種がこの報告書で注目されていないとしても、危険がないわけではありません。サイバースパイの攻撃者は、あなたの会社の資産とデータを今も狙っている可能性があります。またはすでに攻撃されているのに把握できていないだけかもしれません。

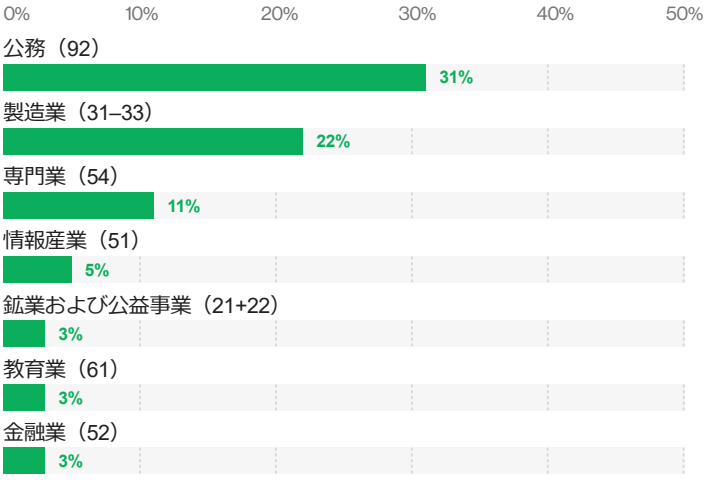

図3：業種別サイバースパイ活動によるデータ漏洩/侵害（2014年度～2020年度DBIR、n=1,580）

属性の種類

サイバースパイ活動によるデータ漏洩/侵害によく見られる属性の種類は以下の通りです：ソフトウェアのインストール（完全性）（91%）、行動の変化（完全性）（84%）、秘匿情報（機密性）（73%）、内部情報（機密性）（29%）、認証情報（機密性）（21%）、システム情報（機密性）（19%）。

これに対して全体の漏洩/侵害では、属性の種類は以下のようになります：ソフトウェアのインストール（完全性）（43%）、行動の変化（完全性（32%）、認証情報（機密性）（29%）、個人情報（機密性）（28%）、決済情報（機密性）（22%）。

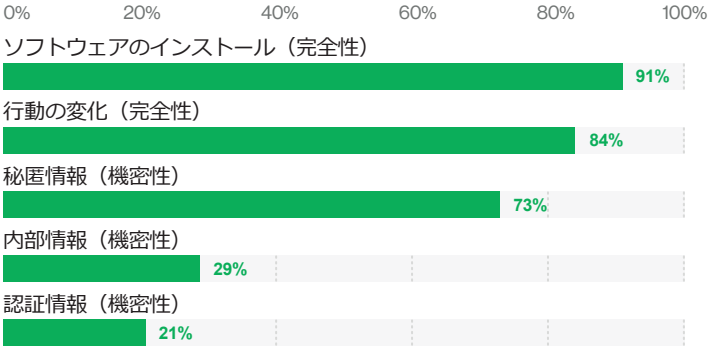

図4：サイバースパイ活動によるデータ漏洩/侵害によく見られる属性の種類（2014年度～2020年度DBIR、n=1,571）

資産の種類

サイバースパイ活動によるデータ漏洩/侵害によく見られる資産の種類（2020年度DBIR）は以下の通りでした：デスクトップまたはノートPC（88%）、携帯電話（14%）、Webアプリケーション（10%）。

これに対し漏洩/侵害全体では（2020年度DBIR）、よく見られる資産の種類はWebアプリケーション（43%）、デスクトップまたはノートPC（31%）、メール（21%）でした。

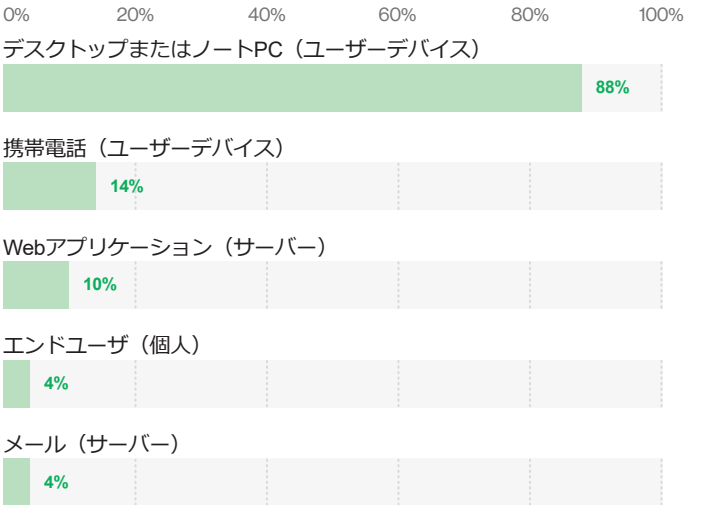

図5：サイバースパイ活動によるデータ漏洩/侵害によく見られる資産の種類（2020年度DBIR、n=113）

データの種類

サイバースパイ活動によるデータ漏洩/侵害によく見られるデータの種類（2020年度DBIR）は以下の通りでした：認証情報（56%）、秘匿情報（49%）、内部情報（12%）、機密情報（7%）。

漏洩/侵害全体においてよく見られるデータの種類は、個人情報（58%）、認証情報（41%）、内部情報（17%）、医療情報（16%）でした。

攻撃者

攻撃者の種類

サイバースパイ活動によるデータ漏洩/侵害（2014年度～2020年度DBIRの対象期間）によく見られる攻撃者の種類は以下の通りでした：州関連組織（85%）、国家関連組織（8%）、組織犯罪グループ（4%）、元従業員（2%）。州関連組織や国家関連組織はスパイ活動という動機に関連しているため、これは当然の結果とも言えます。

攻撃者の動機

2020年度DBIRおよび2014年度～2020年度DBIRの両方の対象期間に収集した全ての漏洩/侵害データに基づき、攻撃者の動機の圧倒的1位は「金銭目的」（2020年度：86%、2014～2020年度：76%）、第2位は「スパイ活動」（2020年度：10%、2014～2020年度：18%）であることが分かりました。

攻撃

2014年度～2020年度DBIRの対象期間における攻撃の上位3つは、サイバースパイ活動によるデータ漏洩/侵害、全てのデータ漏洩/侵害共に同じでしたが順位は異なりました。サイバースパイ活動によるデータ漏洩/侵害の場合は、マルウェア（90%）、ソーシャル（83%）、ハッキング（80%）でした。全ての漏洩/侵害の場合は、ハッキング（56%）、マルウェア（39%）、ソーシャル（29%）の順でした。

つまりサイバースパイ活動の攻撃者は、あらゆる侵害を行う攻撃者よりもマルウェアおよびソーシャル攻撃に依存しているということです。

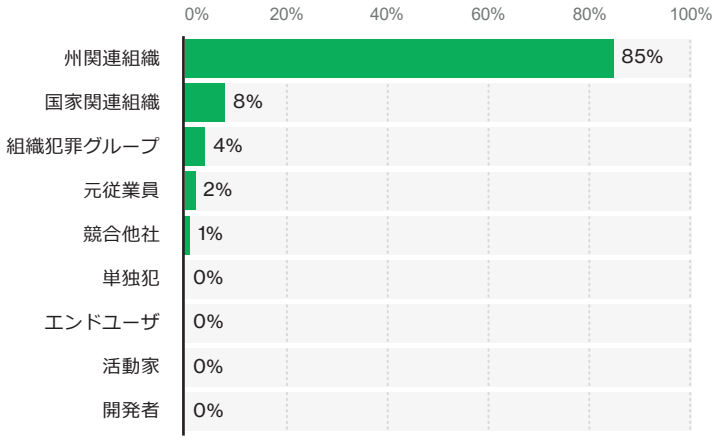

図6：サイバースパイ活動によるデータ漏洩/侵害における攻撃者の種類(2014年度～2020年度DBIR、n=1,435)

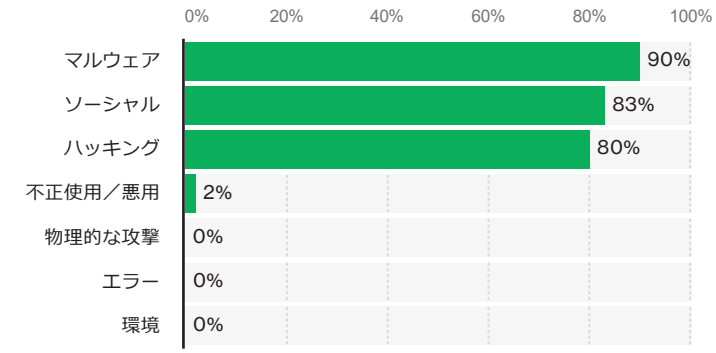

図7：サイバースパイ活動によるデータ漏洩/侵害における攻撃の種類（2014年度～2020年度DBIR、n=1,580）

サイバースパイ活動によるデータ漏洩／侵害とデータ漏洩／侵害全体における攻撃の種類と経路の比較（2014年度～2020年度DBIRの対象期間）

VERISカテゴリ	サイバースパイ活動	全体
ソーシャルの種類	フィッシング（97%） なりすまし（2%） 贈収賄（1%）	フィッシング（87%） なりすまし（9%） 贈収賄（3%）
ハッキングの種類	バックドアまたはC2の使用（86%） 窃取した認証情報の使用（30%） ブルートフォース（12%）	窃取した認証情報の使用（63%） バックドアまたはC2の使用（39%） ブルートフォース（18%）
マルウェアの種類	バックドア（78%） C2（77%） ダウンローダー（40%） 保存データの窃取（40%） スパイウェア/キーロガー（33%） データのエクスポート（32%）	C2（48%） データのエクスポート（42%） スパイウェア/キーロガー（40%） RAMスクレーパー（35%） バックドア（25%）
マルウェアの経路	メール添付（67%） メールのリンク（17%） Webドライブバイ（11%） マルウェアによるダウンロード（11%）	メール添付（43%） 直接インストール（39%） メールのリンク（9%）

まとめ

業種

サイバースパイ活動によるデータ漏洩/侵害を最も多く受けたトップ3の業種は公務（31%）、製造業（22%）、専門業（11%）でした。漏洩/侵害の割合別では製造業（35%）、鉱業および公益事業（23%）、公務（23%）でした。

属性の種類

サイバースパイ活動によるデータ漏洩/侵害の影響を大きく受けた属性の種類は、ソフトウェアのインストール（完全性）（91%）、行動の変化（完全性）（84%）、秘匿情報（機密性）（73%）、内部情報（機密性）（29%）、認証情報（機密性）（21%）、システム情報（機密性）（19%）でした。

資産の種類

サイバースパイ活動によるデータ漏洩/侵害（2020年度DBIR）の被害を受けた資産のトップ3は、デスクトップまたはノートPC（88%）、携帯電話（14%）、Webアプリケーション（10%）でした。

データの種類

サイバースパイ活動によるデータ漏洩/侵害（2020年度DBIR）でよく見られるデータの種類は、認証情報（56%）、秘匿情報（49%）、内部情報（12%）、機密情報（7%）でした。

タイムライン

サイバースパイ活動によるデータ漏洩/侵害の場合、不正アクセスまでの時間は数秒から数日間（91%）、脱出するまでの時間は数分から数週間（88%）、発見するまでの時間は数カ月から数年（69%）、封じ込めまでの時間は数時間から数週間（79%）という結果でした。

発見

サイバースパイ活動によるデータ漏洩/侵害の発見方法のトップ3は、不審なトラフィック（48%）、ウィルス対策（23%）、緊急対応チーム（7%）でした。

攻撃者

サイバースパイ活動によるデータ漏洩/侵害によく見られる攻撃者の種類は、州関連組織（85%）、国家関連組織（8%）、組織犯罪グループ（4%）でした。

攻撃の種類

データ漏洩/侵害においてスパイ活動を目的に外部攻撃者が行った攻撃の主な種類は、フィッシング（81%）、バックドア/C2の使用（53%/60%）、保存データの窃取（27%）、ダウンローダー（27%）でした。

攻撃の経路

データ漏洩/侵害においてスパイ活動を目的に外部攻撃者が行った攻撃の主な経路は、メール（84%）、メール添付（60%）、バックドアまたはC2（60%）でした。

サイバースパイ活動によるデータ漏洩/侵害の詳細

NAICS	全体の漏洩/侵害
全体の漏洩/侵害（2014年度～2020年度）	
頻度	16,090件（2014年度～2020年度） 3,950件（2020年度）
攻撃者	外部（75%）、内部（26%）、複数の関係者（2%）、パートナー（1%）
動機	金銭目的（76%）、スパイ活動（18%）、愉快犯（3%）
サイバースパイ活動によるデータ漏洩/侵害 （2014年度～2020年度）	
頻度	1,580件（2014年度～2020年度）
攻撃者	マルウェア（90%）、ソーシャル（83%）、ハッキング（80%）
資産	個人（88%）、ユーザーデバイス（83%）、サーバー（34%）
データ	秘匿情報（75%）、内部情報（20%）、認証情報（22%）、システム情報（19%）

CISコントロール（CSC）

CSC-4：管理権限のコントロールされた使用
CSC-5：ハードウェアおよびソフトウェアのセキュアな設定
CSC-6：監査ログの保守、監視および分析
CSC-8：マルウェア対策
CSC-12：境界防御
CSC-13：データ保護
CSC-14：Need to Know（情報は知る必要のある人のみに伝え、知る必要のない人には伝えない）に基づいたアクセスコントロール
CSC-16：アカウントの監視およびコントロール
CSC-17：セキュリティ意識向上トレーニングプログラムの実施
CSC-18：アプリケーションソフトウェアセキュリティ
CSC-19：インシデントレスポンスと管理
CSC-20：ペネトレーションテストおよびレッドチームの訓練

VTRACについて

VTRAC（Verizon Threat Research Advisory Center）は、14年以上の間、世界各国の顧客のIRに対する整備状況を改善するお手伝いをしてきました。NISTのサイバーセキュリティフレームワークや弊社のVIPRフェーズなど、各業種のベストプラクティスを利用するだけでなく、ベライゾンが毎年調査を続けてきた500件を超えるインシデントから得た専門知識を使用しています。

VTRACに関する不明点やご意見などありましたら、メール（vtrac@verizon.com）またはLinkedInの弊社ページ（#cyberespionagereportまたは#vtracで検索）までご連絡ください。CERのフルバージョンは以下よりダウンロードできます。
enterprise.verizon.com/resources/reports/cyberespionagereport/

verizon