SQAT® Security Report

2024-2025年 秋冬号

サイバーセキュリティにおけるOSINTアタックサーフェスの重要性

知る・守る
続ける

BBSecは内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

ごあいさつ

株式会社ブロードバンドセキュリティ
セキュリティサービス本部 本部長　山崎 義雄

2024年も半ばを過ぎ、この半年間で情報セキュリティやサイバーセキュリティに関するさまざまなニュースが取り上げられました。中でも、ランサムウェアに関連するニュースが多く取り沙汰されました。特に、大手出版グループへの攻撃では、情報漏洩やサービス停止、物流機能や経理機能の停止など、さまざまな被害が発生しました。その結果、2024年4月～6月期の連結決算では、特別損失として20億円が計上されるなど、被害の深刻さが注目を集めました。また、ランサムウェアによるサイバー攻撃のニュースには、サプライチェーンに関連する事例が多く見られる点も注目に値します。たとえば、自治体や企業から印刷業務を請け負っている企業がランサムウェアの被害を受け、複数の委託元組織の情報が漏洩したケースや、大手保険会社の委託先である税理士法人がランサムウェアに感染し、情報漏洩が発生したケースなどが代表的です。IPAが発表した「情報セキュリティ10大脅威　2024」においては、組織に対する脅威としてランサムウェアが1位、サプライチェーンの脆弱性を悪用した攻撃が2位に挙げられていますが、これらが社会全体にとって大きな脅威となっている現状が浮き彫りになっています。こうした状況に対抗するためには、ランサムウェア対策だけでなく、サプライチェーンに関連するサイバーセキュリティの強化も重要です。しかし、そのためには、脅威の中に潜む別の脅威を見抜く力が求められます。そうした知識と洞察力を身につける一助として、「SQAT® Security Report」をご活用いただければ幸いです。

本レポートは、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における2024年上半期（1月～6月）の診断結果からデータを抽出し、集約したものを弊社のエンジニアらの感性も交えてアウトプットしたものです。今号は巻頭企画として、アタックサーフェスとOSINTに焦点を当てた記事や、弊社ともかかわりの深い秋田県立大学の廣田准教授によるプログラミング教育・セキュリティ教育を取り上げた寄稿記事などが掲載されております。

本レポートが読者の皆様のセキュリティ対策における有益な情報としてご活用していただけることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げるBBSecの使命であると考えております。

CONTENTS

※本レポートは、弊社セキュリティサービス本部のホームページ
「SQAT®.jp（URL：https://www.sqat.jp/）」
https://www.sqat.jp/sqat-securityreport/からダウンロード可能です。

SQAT.jp

巻頭企画

サイバーセキュリティにおけるOSINT
アタックサーフェスの重要性

軍事の諜報活動の一部だったOSINTという手法は、現在では日常的に用いられ、サイバーセキュリティ分野でも活用されるようになった。組織としては公開を意図していなかった情報でも、攻撃者がOSINTを用いて攻撃対象となりうる組織のIT資産の情報などを入手してしまう可能性もある。今号ではOSINTについて様々な角度から迫り、紐解いていく。

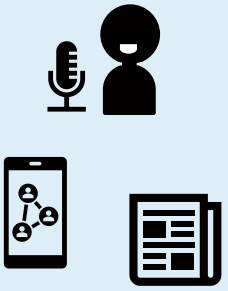
SQAT® Security Report 編集部

OSINTとは

OSINT（オシント）とは「Open Source Intelligence（オープンソース・インテリジェンス）」の略称である。その名のとおり、インターネットやニュース記事、SNSなど一般的に入手可能である公開情報を収集・分析することで情報を得る手法のことである。

もともとは軍事の諜報活動の一部で、SIGINT（Signal Intelligence：通信傍受による諜報）やHUMINT（Human Intelligence：人的情報による諜報）とともに用いられ、国家の安全保障や軍事的な戦略策定に利用されていた。現在では日常的に用いられ、サイバーセキュリティ分野にも活用されている。

OSINT に用いられる公開情報の例

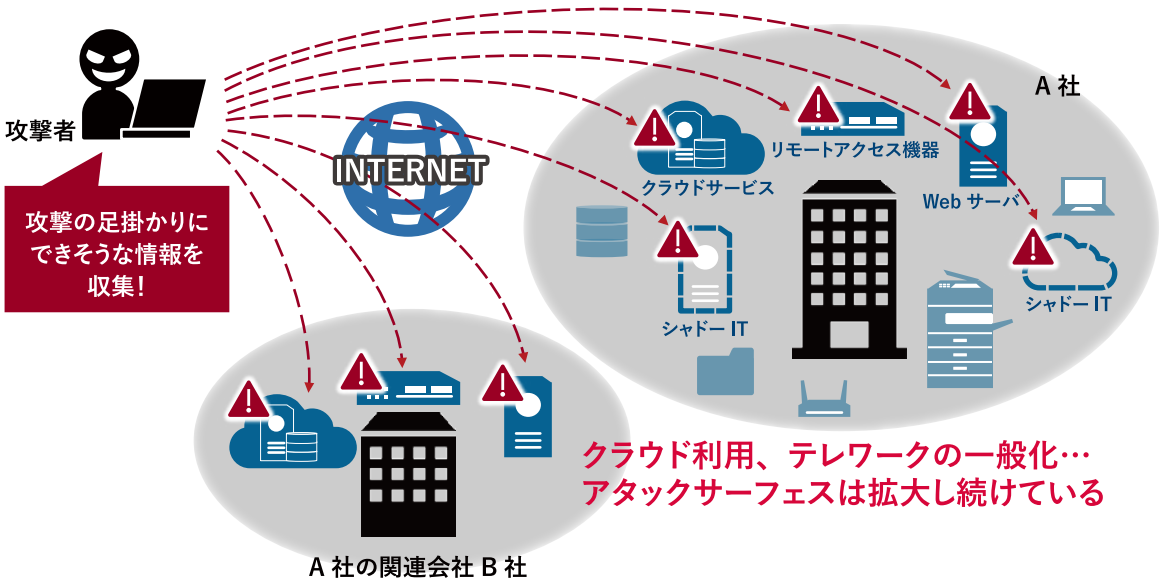


- 新聞やニュースなどの報道
- 組織のプレスリリース、インタビュー記事、Web サイト
- 組織の従業員など関係者の SNS
- セキュリティベンダの公開レポート、IoC 情報公開サイト、専門家の記事　など

サイバー攻撃に悪用される例

サイバー攻撃者がOSINTを用いることにより、アタックサーフェスと呼ばれるWebシステムやネットワーク機器などの外部との接点にある「サイバー攻撃の対象となりうるIT資産」の情報を収集する可能性がある。組織の情報を公開情報から入手することで、攻撃の予兆に気づかれず、攻撃者の身元がばれることもなく、ターゲットの弱点を知ることができる。このように攻撃者からするとメリットが多いため、攻撃前にOSINTを用いた偵察が行われる可能性がある。

アタックサーフェスと呼ばれる「**サイバー攻撃の対象となりうる IT 資産**」の情報を収集



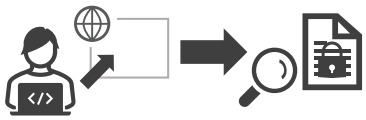
クラウド利用、テレワークの一般化…
アタックサーフェスは拡大し続けている

サイバー攻撃への悪用例

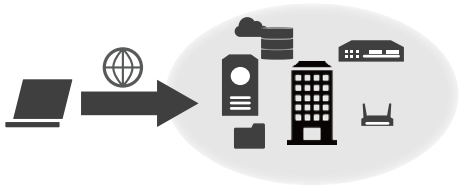
① 組織の問い合わせ用メールアドレスなどから組織のドメインを把握。さらに組織の公開情報やSNSから従業員氏名を入手。メールアドレスを予想し、マルウェアを添付して送信を試行。

② SNSなどから従業員の個人情報を得て、職位的に管理者権限を持ちうる人物を洗い出す。誕生日や趣味、家族情報などからパスワードを推測して、管理者権限アカウントへのログインを試行。

③ソースコードの保存や共有ができるサイト上で、ソースコード内にパスワードや暗号化キーが含まれているものを探す。



④ ツールを用いて開いたままになっているポートや、公開された脆弱性情報を参考にしてパッチが未適用・設定の不備が存在するなど脆弱性があるIT資産を解析する。



OSINTを用いたセキュリティ対策

ここまでOSINTをサイバー攻撃に悪用する例などを見てきたが、逆にOSINTをセキュリティ対策に活用することもできる。

組織が意図せず公開している情報や、意図的に公開している情報同士を紐づけることで得られる情報など、サイバー攻撃の材料となりうるもの、アタックサーフェスといった標的となりうるものをOSINTによって発見することができる。それらの状況を把握することで、もしサイバー攻撃の被害を受けた場合に被害範囲がどれほどになる可能性があるかを確認することが可能である。また場合によっては、外部に公開していないはずの組織の機密情報を発見するなど、すでに流出してしまった情報を見つけられる可能性がある。

OSINTを組織で行う上での注意点

OSINTを行う際に、組織として気を付けなければならないポイントがいくつかある。

まずはOSINTによって収集した情報が正確で信頼できるものか確認を怠らないことだ。インターネット上などで公開されている情報の内容が正確であるとは限らないため、偽情報や誤情報ではないか常に警戒して確認する必要がある。また入手した情報は時間とともに陳腐化する可能性があるため、定期的に再調査を実施し、情報を更新して有効性を評価し続ける必要がある。

さらにOSINTは入手する情報量が膨大になりがちなため、情報の更新や分析のためにも情報の管理・整理も必要不可欠となる。

最後に法的および倫理的な考慮を念頭に置くことだ。公開情報を収集するうえで、その行為がプライバシーの保護や関連する法律に準拠しているかどうかも気にしなければならない。プライバシーを無視した不当な監視や、コンテンツの規約で禁止されている方法での情報収集など、問題とされる可能性のある行為をすべて回避した上で情報を集めなければならない。例えばSNSなどサービスによってはツールによる自動抽出は規約違反としているものもあるなど、情報源の規約に則った情報収集方法を把握することが必要である。

先で述べたようにOSINTで集める情報は膨大だ。ツールなどを用いて効率よく情報を集めたり、収集した情報を適切に管理したり、法的および倫理的な問題を犯していないか確認したりといった部分は専門家に相談するなど、必要に応じてプロの意見を取り入れると安心できるだろう。情報社会の現代において効率よく正しい情報を得ることで、自組織の公開情報およびアタックサーフェスの状況を把握することができ、より一層高いセキュリティが見込めるはずである。