2023 年 7 月 10 日

サイバー攻撃を知る-その２

対策を検討するため、相手（ハッカー）の動きを知る

技術士（情報工学部門）
きよし事務所　代表　清　孝雄（Takao Kiyoshi）　著

目次

１　サイバー攻撃とは

⑴ サイバー攻撃とは、コンピュータやネットワーク、その他の情報システムに対して、不正なアクセスやデータの窃盗、改ざん、破壊などを行う行為です。

⑵ サイバー攻撃の目的は様々ですが、①金銭的な利益が多く、②社会的・政治的な主張、③国家間の対立やスパイ活動、④愉快犯などがあります。

⑶ サイバー攻撃を行う者は、個人やグループ、組織化された犯罪集団や国家の関与がある場合もあります。「サイバー犯罪者」、「ハッカー」などと呼ばれます。

彼らは、コンピュータやシステムに存在する脆弱性（問題点や弱点）を見つけて、それを利用して自分たちの目的を達成しようとします。

それでは、サイバー攻撃の目的とはどのようなものなのでしょうか。ここでは、考えられる４つの目的をみていきましょう。

⑴ 脅迫	⑶ 抗議
⑵ 金銭の搾取	⑷ 嫌がらせ

⑴ 脅迫

企業や組織のサービスに対する脅迫を目的としている場合が考えられます。

このとき、実際に攻撃をしかけてサーバに負荷をかけ、アクセス妨害をしたのちに脅迫するパターンや、攻撃を予告したり、「ランサムウエア」による暗号化後や、盗んだ情報を公開すると脅迫して金銭を要求するパターンなどがあります。

⑵ 金銭の搾取

上述の「脅迫」にも関連する目的ですが、「ランサムウエア」や「DDoS 攻撃」をしかけてサーバへのアクセス妨害を行い、「金銭を支払えば攻撃をやめる」などといった金銭を搾取する目的の攻撃もあります。

⑶ 抗議

「DDoS 攻撃」には、企業や組織に対する抗議を目的としたものもあります。

例えば、政治への不信感や不満を形として示すために、政府機関のサーバに「DDoS

攻撃」をしかけてアクセス妨害をするといった事例も度々発生しているのです。

(4) 嫌がらせ

執拗に特定の企業を攻撃する「嫌がらせ行為」が目的の攻撃もあります。

明確な動機を推察することは難しいですが、例えばライバルの企業サイトをダウンさせたり、サイトの運営者を困らせたりといった目的で「DDoS 攻撃」や「ホームページの改ざん」が行われていることも考えられます。愉快犯や模倣犯なども存在します。

2　種類

(1) サイバー攻撃の種類には、以下のようなものがあります 。

ア　バックドア型トロイの木馬

イ　クロスサイトスクリプティング

ウ　ランサムウェア（盗難・暗号化）

エ　改ざん

オ　DDOS

カ　DNS 関連攻撃

キ　SQL インジェクション

などがあります。

ア　バックドア型トロイの木馬

被害者のシステムに隠れた脆弱性を利用して、攻撃者が遠隔からほぼ完全に制御できるようにするものです。サイバー犯罪に利用されます。

イ　XSS（クロスサイトスクリプティング）攻撃

正規のウェブサイトやアプリケーションのスクリプトに悪意のあるコードを挿入して、ユーザーの情報を取得するものです。多くの場合、JavaScript が使われますが、Microsoft VCScript, ActiveX, Adobe Flash なども利用されます。

ウ　ランサムウェア攻撃

被害者のデータやシステムを暗号化してロックし、復元するために身代金を要求するものです。支払いがない場合は、データを削除したり公開したりすると脅迫します。

エ　改ざん攻撃

ウェブサイトやデータベースなどの情報を書き換えて、内容を変更したり消去したりするものです。政治的なメッセージや不適切な画像などを掲載することもあります。

オ　DDOS（分散型サービス拒否）攻撃

被害者のシステムやネットワークに大量の不正なトラフィックを送りつけて、正常なサービスを妨害する。多数のコンピューターやデバイスから同時に攻撃することで、防御を困難にする。

カ　DNS（ドメイン名システム）関連の攻撃

インターネット上でドメイン名と IP アドレスを対応付ける DNS サービスを悪用する。例えば、DNS キャッシュポイズニングでは、DNS サーバに偽の情報を送り込んで、ユーザーをフィッシングサイトなどに誘導する。

キ　SQL インジェクション

データベースと連動した Web アプリケーションなどに対する攻撃手法の一つで、検索文字列など外部から指定するパラメータの一部に SQL 文の断片などを混入させ不正な操作を行うものです。例えば、SQL 文の中に「;」を入れることで、本来実行されるべきでない SQL 文が実行されることがあります。

☕コーヒーブレイク　ちょっと一休み☕

【「DoS 攻撃」と「DDoS」攻撃の違い 】

DoS 攻撃は、攻撃者が 1 台の機器から対象の機器に過剰な攻撃をしかけるサイバー攻撃です。

DDoS 攻撃と DoS 攻撃の違いは、攻撃元となる機器の台数と、「踏み台」を利用するか否かの部分だといえます。

３　サイバー攻撃の実例

サイバー攻撃は世界中で頻発しており、多大な被害や影響をもたらしています。ここでは、最近起きたいくつかの事例を紹介します。

サイバー攻撃の実例としては、以下のようなものがあります。

ア　バックドア型トロイの木馬

パソコン遠隔操作事件

2012 年、国内の複数パソコンから掲示板への犯罪予告の書き込みが行われ、4 人もの人間の誤認逮捕に繋がるという事件があった。真犯人は、少なくとも 5 人にトロイの木馬を感染させ、端末にバックドアを設置。そこから端末を遠隔操作することで、無実の人間に罪を着せ、警察の失態を招いた事案でした。

イ　XSS（クロスサイトスクリプティング）攻撃

2010 年に YouTube のコメントシステムの脆弱性を狙った XSS 攻撃があり、YouTube のコメントが閲覧できなくなったり、デマ情報を記載したポップアップ画面の表示、悪趣味なサイトにリダイレクトされるなどの事象に見舞われました。また、金融サービスサイトに関係するフィッシング被害の要因の一つが XSS 攻撃であることが知られています。

ウ　ランサムウェア攻撃

取り扱う貨物量が全国一の名古屋港で、システム障害が発生し、コンテナの積み下ろしができなくなっていました。名古屋港管理組合によると、コンテナターミナルでシステム障害が発生し、システムデータは暗号化され、協会内のプリンターの一部から「ランサムウエア」に感染したことを通告する英語の文書が印刷された。トレーラーへのコンテナの積み下ろしのほか、搬入や搬出の作業が止まっているという。

名古屋港をめぐっては、2022 年 9 月にも、管理組合のサイトでアクセス障害があり、親ロシア派のハッカー集団が「サイバー攻撃をした」と、犯行声明を出していた。

暗号化だけでなく、ダークウエブと言われる闇サイトに盗まれた情報も公開され、「**二重の脅迫**」を受けることが知られています。

ランサムウェア攻撃における脅迫として「データの暗号化」「情報の暴露」「サービス妨害（DoS）」「被害者の顧客や利害関係者への連絡」の 4 つがあると解説。攻撃者はこの 4 つを組み合わせ、「二重脅迫」や「四重脅迫」などを行うという。

2019 年 6 月に発生した、南房総市の公立小中学校計 12 校で、攻撃者と見られるサイバー犯罪集団「Lockbit」は暗号化したデータと引き換えに金銭を要求したほか、要求に応じない場合はデータを公開するなど、二重脅迫行為に及んでいるとのこと。攻撃

はネットワークの管理を受託する事業者からの報告により判明したもので AD サーバやバックアップサーバも暗号化され、南房総市は 2022 年 7 月に事実を公表し謝罪しています。南房総市教育委員会は攻撃者の要求には応じず、自力での解決を目指す姿勢です。

エ　改ざん攻撃

ホームページの改ざん（書き換え）は、インターネットにおいて頻繁に発生する事件のひとつです。

2000 年には、官庁のホームページが狙われて、相次いで改ざんされました。その後も現在に至るまで、同じような手口で、自治体や大手企業、学校などのホームページが改ざんされています。

ホームページの改ざんは、ある目的を持って特定の団体や企業を攻撃する場合と、無差別に情報セキュリティ対策の甘いホームページを改ざんする場合に分類することができます。

爆破予告が模倣犯のように流行することがあります。

オ　DDOS（分散型サービス拒否）攻撃

2017 年 9 月。この攻撃では Google サービスが標的となり、2.54 Tbps の規模に達しました。Google Cloud は 2020 年 10 月に攻撃を受けました。

攻撃者は、なりすましパケットを 18 万件の Web サーバに送信し、そうしたサーバが Google に応答を送信しました。この攻撃は単発的な事件ではなく、攻撃者は、過去 6 か月間に Google のインフラストラクチャで複数の DDoS 攻撃を実行していました。

カ　DNS（ドメイン名システム）関連の攻撃

2016 年に発生した米国「Dyn」へのランダムサブドメインによる DDoS 攻撃があります。この攻撃では、DNS サーバに対して大量のリクエストを送りつけ、処理能力を圧迫させることで、一部の Web サイトがダウンする被害が発生しました。また、DNS ハイジャック攻撃と呼ばれる手法もあります。これは、Web サイトのドメインを不正に操作する攻撃手法で、ドメイン名を書き換えることで、Web サイトに致命的な被害を与える危険なサイバー攻撃です。

※管理者 ID が乗っ取られると、多要素認証などを入れていない、利かせていない場合、DNS を書き換えられ、別のサイトに誘導される場合が良く起きています。

キ　SQL インジェクション

SQL インジェクション関連の攻撃による有名な事件としては、2017 年に発生した「Equifax」の個人情報流出事件があります。この事件では、同社の Web サイトに対して SQL インジェクション攻撃が行われ、約 1 億 4400 万人分の個人情報が流出しました。また、2019 年には、日本の大手通信会社である「ソフトバンク」が SQL インジェクション攻撃を受け、約 4 万件の個人情報が流出したことが報じられました。

4　対策

サイバー攻撃を防ぐためには、以下のような対策が必要です。

(1) セキュリティポリシー策定と徹底（研修・監査）

(2) セキュリティソフトウェアの導入と更新

(3) バックアップと復旧計画の作成

(1) セキュリティポリシーの策定と徹底（研修・監査）

組織内でセキュリティに関するルールや手順を明確にし、従業員や関係者に周知し、遵守させることです。例えば、パスワードの管理や更新、不審なメールやリンクの開かないこと、機密情報の取り扱いや保管方法などです。

(2) セキュリティソフトウェアなどの導入と更新

コンピュータやネットワークに対して、ウイルスやマルウェア、不正アクセスなどを検出し、防御するソフトウェアを導入し、常に最新の状態に保つことです。例えば、アンチウイルスソフトウェアやファイアウォール、VPN などです。

(3) バックアップと復旧計画の作成

データやシステムを定期的に別の場所にコピーし、保存することです。万が一、サイバー攻撃によってデータやシステムが破損したり消失したりした場合でも、元に戻すことができます。また、サイバー攻撃が発生した場合の対応策や連絡体制などを事前に決めておくことです。

サイバー攻撃は今後も増加する傾向にあります。技術的な進歩や社会的な変化に伴って、新たな脅威や手口が登場する可能性もあります。情報セキュリティ担当者としては、常に最新の情報を入手し、自らの知識やスキルを向上させることが重要です。また、組織内でセキュリティ意識を高めるために、教育や啓発活動も行うことが必要です。

☕コーヒーブレイク　ちょっと一休み☕

【　ランサムウエアやファイルの改ざん対策１　】

　バックアップは必須です。最近は、データ量が多いため、ネットワークストレージにバックアップを持つケースが増えています。外部メディアやネットワークを切り離したバックアップを必ず持ちましょう。
　ミラーリングをバックアップには考えてはいけません。ウイルス被害、ランサムウエアによる暗号化には、対応できません。
　必ず、スナップショットを取得して、データ本体と可能な限り、トランザクションをテク説にバックアップしましょう。

※バックアップを取っていても、戻せないケースが現実に起きています。
　バックアップから、定期的に戻す訓練を忘れずに実施してください。

【　ランサムウエアやファイルの改ざん対策２　】

　ランサムウエアによる暗号化は、攻撃者から見ると最終ステップです。
　侵入後、データを取得後に、暗号化、身代金請求するケースが多くなってきています。
　情報漏えいの兆しがあれば、早期に対策することが、最近のサイバー攻撃対策として必要とされています。

５　今後の課題

サイバー攻撃は今後も増加する傾向にあります。その理由としては、以下のようなものが挙げられます。

(1) サイバー攻撃者の技術力や組織力の向上

(2) コンピュータやシステムの複雑化や多様化

(1) サイバー攻撃者の技術力や組織力の向上

サイバー攻撃者は常に新しい手法や技術を開発し、複雑化や巧妙化しています。また、国家や組織と連携して大規模な攻撃を行うこともあります。

(2) コンピュータやシステムの複雑化や多様化

コンピュータやシステムは日々進化し、複雑化や多様化しています。その結果、脆弱性が発見される可能性が高まります。また、インターネットに接続された機器やデバイスが増えることで、攻撃対象も社会的信頼や取引先からの信用は失墜します。