トピックス

サイバー攻撃への備えを確認せよ
―Red Teamを利用したサイバーレジリエンスの強化―

サイバー攻撃はますます巧妙さを増しており、企業においては既存のセキュリティに加え、これまでとは異なる対策が求められている。その1つとして、Red Teamという概念を用いたセキュリティ評価手法に注目が集まっている。本稿では、この評価手法について、その概要とどのように活用すべきかを考察する。

NRIセキュアテクノロジーズ サイバーセキュリティ事業本部
サイバーセキュリティサービス二部 セキュリティコンサルタント
佐藤 裕作（さとう ゆうさく）
専門はペネトレーションテスト、Red Team演習、Webアプリケーションセキュリティなど

変化し、巧妙化するサイバー攻撃

システムに対して疑似的な攻撃を行うことで、そのセキュリティ対策状況を評価する手法は、脆弱性検査やセキュリティ診断と呼ばれ、こうした手法を用いて保有するシステムのセキュリティを評価・改善することは、すでに一般的になっている。一方で、サイバー攻撃は巧妙さと執拗さを増しており、企業には、セキュリティ向上のためのさらなる努力が求められている。

こうしたなか、より高度なセキュリティ評価手法として、「Red Team演習」や「脅威ベースペネトレーションテスト（TLPT）」といったキーワードが注目されている。2018年5月に金融庁から「諸外国の『脅威ベースのペネトレーションテスト（TLPT）』に関する報告書」が公表されたこともあり、国内でも関心が高まっている。

評価手法の種類とその違い

脆弱性検査、ペネトレーションテスト、Red Team演習とは、どのような評価手法なのか。筆者が考える各評価方法の平均的な内容を整理する（表1参照）。

（1）脆弱性検査／セキュリティ診断

評価対象を事前にサーバーやアプリケーションの単位で定義し（スコープベース）、ギャップ分析のアプローチで脆弱性を網羅的に洗い出すことを目的とした手法。一般的にこの方式では、システム侵害に直結するような深刻な脆弱性のみならず、セキュリティ上望ましくないとされる軽微なものも含め、改善点を挙げることが期待される。ただし、脆弱性を発見・修正することが最大の関心事であり、検出された脆弱性に対して実際に攻撃を加え、その影響は調査しない場合が多い。

調査の実施に際しては、2つの工程を併用する場合が多い。スキャナーと呼ばれる自動化されたツールを用いて、対象システム上の問題点を検出する工程と、人の手による手動テストの工程である。後者は主に、ツールの誤検知の排除や、ツールでは技術的に検出が困難な領域をカバーするために実施される。

(2) ペネトレーションテスト

前述の脆弱性検査は、脆弱性の洗い出しを重視した取り組みである。一方、ペネトレーションテストでは、シナリオベースの実施方式がとられる。このシナリオは、実際に発生しているサイバー攻撃や、対象となる組織のIT環境を踏まえた内容となっており、攻撃者の目標とその実現へ至るまでの攻撃のシナリオを事前に設計した上で、シナリオに沿ってテストを実施する。この場合、攻撃者の目標が達成可能な道筋が存在するかどうかを調査することが主眼であり、脆弱性がどこにあるのかを列挙することは重視されない。調査の過程で、テスト実施者は、実際の攻撃者と同様に、システム上で検出された脆弱性を利用し、その結果を攻撃ステップに利用したり、複数の脆弱性を組み合わせたりして、目標の達成を試みる。

表1　セキュリティ評価手法の比較

	脆弱性検査/ セキュリティ診断	ペネトレーション テスト	Red Team演習
実施方式	スコープベース	シナリオベース	シナリオベース
評価方式	ギャップ分析的 脆弱性の洗い出し	リスク分析的 攻撃目標の達成可否	リスク分析的 攻撃目標の達成可否
手法	自動ツール ＋手動テスト	現実の攻撃の再現 （＝手動テスト中心）	現実の攻撃の再現 （＝手動テスト中心）
深さ	脆弱性の存在の確認	脆弱性を悪用して 影響範囲を分析	脆弱性を悪用して 影響範囲を分析
評価対象	システム個別	システム全体	システム＋人＋プロセス 組織としての サイバーレジリエンス

(3) Red Team演習

Red Team演習は、ペネトレーションテストの概念を拡張したものである。先に述べた金融庁の報告書で定義されている「脅威ベースのペネトレーションテスト（TLPT）」も、これと同じ種類のものである。Red Team演習においても、ペネトレーションテストと同様に、攻撃者の視点によるシナリオベースのアプローチが用いられる。ペネトレーションテストはサイバー攻撃に対するシステムの耐性の評価が目的だが、Red Team演習ではさらに進めて、システムだけではなく、それを監視・運用する人や、そのプロセスまで含め、総合的なセキュリティ耐性の評価を行う点が大きく異なる。また実際に発生しているサイバー攻撃の脅威を再現することにより重きを置いている点も特徴である。

侵入を前提に被害を最小化する

「侵入させないための対策」だけでなく、「侵入を前提に被害を最小化する対策」を含めたサイバー攻撃への耐性は、サイバーレジリエンス（Cyber Resilience）と呼ばれ、近年注目されている。

Red Team演習は組織のサイバーレジリエンスを確認する上で有効である。Red Team演習では、実際のサイバー攻撃を再現するRed Teamと、それに対抗して組織を攻撃から守るBlue Teamの攻防という構図でテストを行う。Red Teamはハッキング技術に精通した外部のセキュリティプロフェッショナルにより構成され、Blue Teamは組織内のSOC（Security Operation Center）や、CSIRT（Computer Security Incident Response Team）といったセキュリティチームで構成される。

サイバー攻撃への対応のためのBlue Teamの活動を表すフレームワークとして、NIST

Cyber Security Frameworkがある。このフレームワークでは、防御側の活動は、以下の5つで表現される。

①特定（Identify）

サービスや機器、ソフトウェアなど、攻撃から保護すべき対象を特定すること。

②防御（Protect）

セキュリティパッチの適用や設定の堅牢化、スタッフへの教育による防御策の実施。

③検知（Detect）

異常を検知し、潜在的な影響を理解するための継続的な監視活動。

④対応（Respond）

インシデントへの対応計画、対応時のコミュニケーション管理。

⑤復旧（Recover）

攻撃により汚染された環境の復旧計画と、インシデントの振り返りに基づく改善。

本フレームワークではシステムへの侵害を予防するための「特定」、「防御」といった事前の対策のみならず、システムへの侵害の発生を前提として、その後の「検知」、「対応」、「復旧」にも注目している。これは、脅威の早期発見と早期対処が、サイバー攻撃の被害を最小にとどめるという考えからである。

先に説明した脆弱性検査は、事前に設定したスコープ内での脆弱性洗い出しが目的である。そのため、これらの活動のうちの「防御」に焦点をあてた対策であるといえる。

一方でRed Team演習では、事前の攻撃シナリオの検討の段階で、「特定」の工程で考慮から漏れた対象を確認すること、また実際に脆弱性を悪用してシステムの侵害を発生させることで、「検知」以降のプロセスについての対応能力を確認できる。

攻撃者はすでに内部に侵入している

なぜ今サイバーレジリエンスに注目が集まるのか。従来の考え方では、セキュリティとは組織の内と外を隔てる境界を強固にし、侵入を防止することであった。しかし近年のサイバー攻撃では、攻撃者はすでにネットワーク内部に侵入しているのが実情である。攻撃者はゼロデイ脆弱性（ソフトウェアの脆弱性に対し、セキュリティ更新プログラムが提供される前の状態）の悪用や、数か月の期間をかけた入念なソーシャルエンジニアリングなど、あらゆる手段でネットワーク内部へ侵入する。一例を挙げると、攻撃者はメールに添付した悪性のファイルを開封させることでネットワーク内部にあるPCをマルウェアに感染させ、遠隔操作する。その後、感染PCを起点に、時間をかけてネットワーク内を探索し、目的のシステムへの侵入や情報の持ち出しを達成するといったケースがある。

Ponemon Instituteの調査（The Cost of a Data Breach in 2017）では、企業がサイバー攻撃の被害を受けた際に発生する被害額の平均は、1件あたり約4億円と非常に高額となっている。これは、攻撃者にネットワーク内部へ侵入されてしまうと、企業が攻撃者の検知に時間を要し、かつ適切な対応が取れていないことが原因と考えられる。

このような背景から、システムへの侵入を防ぐ境界線の脆弱性検査に加え、侵入後も含めて一連のシナリオを再現する、ペネトレー

ションテストやRed Team演習によるサイバーレジリエンス評価が求められている。

TTPsを持った攻撃者への対抗

近年のサイバー攻撃では、Blue Teamの監視をかいくぐるために、TTPs（Tactics, Techniques, Procedures）と呼ばれる高度な手法が用いられる。Red Team演習が実際に発生している脅威の再現に重きを置いているのは、これらの高度な手法に対抗するためである。攻撃者のTTPsのノウハウをデータベース化したフレームワークとして、米国MITRE社のATT&CK（Adversarial Tactics, Techniques & Common Knowledge）がある。このフレームワークでは、実際のサイバー攻撃で観測された具体的な攻撃テクニックが、攻撃シナリオに沿って整理されている。今後このようなフレームワークは強化され、Red Teamによって再現される攻撃シナリオの標準化が進むと考えられる。

組織のセキュリティへの取り組みに合わせた実施方式の選択

ひと口にRed Team演習と言っても、その実施方式は複数存在する。実施計画立案の際には、実施の狙いや組織の性質、またセキュリティへの取り組みの理解度に応じて適切な実施方式を選択する必要がある。

(1) 関係者への事前の連絡の有無

攻撃の現実性を高めるには、Red Team演習の告知を、対象組織内の数名の担当者のみにとどめることが望ましい。演習実施の旨を事前に関係者へ通知しないことで、Blue Teamの活動をより実践的に評価することができる。ただし、関係者からのクレームやトラブルの発生を防止するため、なぜこのような取り組みが必要であるかの認識の共有が、平時から組織内でできていることが求められる。

(2) Red Teamに与える裁量

Red Teamに許可された攻撃活動の幅が広いほど、より実践的な演習を実現できる。一方で、Red Team演習がシステムの稼働や業務に与える影響を事前に分析し、適切にコントロールすることも必要となる。攻撃活動の範囲を定義する方法としては、攻撃の対象とする機器・サービス・人間をシナリオ策定のなかで定義する方法や、攻撃手法ベースで範囲を定義する方法が考えられる。

(3) 事前情報提供の有無

Red Teamへ事前の情報提供を行わない方が、より現実のサイバー攻撃に近い条件での演習となる。一方で、限られた演習期間内で攻撃シナリオ全体にわたってBlue Teamを評価したい場合は、効率的に攻撃活動を再現するために、Red Teamにシステム構成情報を提供したり、攻撃シナリオに仮定を設けて、シナリオの途中から攻撃を再現したりすることも有効である。

Red Team演習は、現実のサイバー攻撃に対する組織の耐性を測る上で有効である。影響をコントロールしやすい実施方式から始め、Blue Teamの成熟度や、組織としてのサイバーレジリエンス強化の取り組みへの理解度に合わせ、実施形式を本格化することが望ましい。 ■