SQAT® Security Report

2023-2024年 秋冬号

ペネトレーションテストとは？
企業が認識すべき
セキュリティリスクの可視化

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　齊藤 義人

2023年も半分以上が経過しましたが、サイバー攻撃に関する注目すべき話題が後を絶ちません。政府も事態を重く見ておりサイバーセキュリティに関する政策や各種取り組み、情報配信等にさらに力を入れています。重要インフラ事業者等のサイバーセキュリティ強化やサービス障害に備えた体制整備もその一環です。近年では、DDoS攻撃やランサムウェア攻撃が大きな影響を与えており、警察庁とNISCから、昨年9月に発生した国内の政府関連や重要インフラ事業者に対する一連のサイバー攻撃に関する分析レポート「DDoS攻撃への対策について」が、5月に公開されました。ランサムウェア攻撃の事例では、名古屋港へのランサムウェア攻撃が挙げられます。一時的に名古屋港全ターミナルの作業を停止させたことについて、影響範囲の広さもさることながら、復旧に掛かったコストや労力といった事態の深刻さについても計り知れないものだったと推測されます。ほかにも気象庁への脆弱性をついた攻撃が観測され、情報流出の可能性があるとの発表があり、政府組織へ向けたものだった点で注目させられました。サイバー攻撃の脅威に対して認識を深め、適切な対策を講じる必要性や重要性は益々高まってきていると言えるでしょう。

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2023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、リスク分析の重要性からシステムのサイバー攻撃耐性を検証するペネトレーションテスト等を解説する企画や、長崎県立大学　情報システム学部の加藤雅彦教授からの、セキュリティ人材の育成と採用に関する寄稿記事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。

一般社団法人 日本ハッカー協会主催
「Hack Fes. 2023」の様子（2023年7月開催）

専門知識を学んだり、スキルを磨いたりするためのセキュリティエンジニア対象のイベント「Hack Fes. 2023」に弊社は協賛企業として参加しました。

※写真は弊社撮影。撮影および掲載許可を得ています。

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

ペネトレーションテストとは

企業が認識すべきセキュリティリスクの可視化

経済産業省が公開している「サイバーセキュリティ経営ガイドライン」。
そこでは、セキュリティリスクの把握・分析・対応について、
経営者が確実に実施しなければならない項目とされている。
ではどのように対応するのか。
本企画ではより専門的な領域のセキュリティリスク分析の中で、
プロセスに組み込むべき要素の一つである
ペネトレーションテストについて解説する。

SQAT® Security Report 編集部

リスク分析は経営者のリーダーシップのもとで行わなければならない

2023年3月、サイバー攻撃の多様化・巧妙化に伴って経済産業省は「サイバーセキュリティ経営ガイドライン　Ver3.0」を公開した。「サイバーセキュリティ経営ガイドライン」とはサイバー攻撃から企業を守る観点で経営者が認識する必要がある事項などをまとめたもので、「経営者が認識すべき3原則」や「サイバーセキュリティ経営の重要10項目」などが掲載されている。

この「経営者が認識すべき3原則」の中で、「経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要」と触れられており、ガイドライン内でもセキュリティリスクについて広く言及されている。つまり、セキュリティリスクの把握・分析・対応といった活動は、経営者が率先して取り組み、推進しなければならない重要なものである。

とはいえ、それらに精通した経営者はどれだけいるだろうか。特にリスクの分析は、一般的に発見されたリスクに対して発生確率や発生したときの損害などを考慮し、状況を把握することを指し、専門的な知識がなければ実施が難しい領域である。

セキュリティリスクの把握・分析に役立つ手法と言えば様々あるが、リスクアセスメントや脆弱性診断、アタックサーフェス調査、ペネトレーションテストなどを思い浮かべる方も多いだろう。今回は中でも、リスク分析において被害範囲などを判断するといった、リスクの“可視化”に有効なペネトレーションテストについて紹介する。

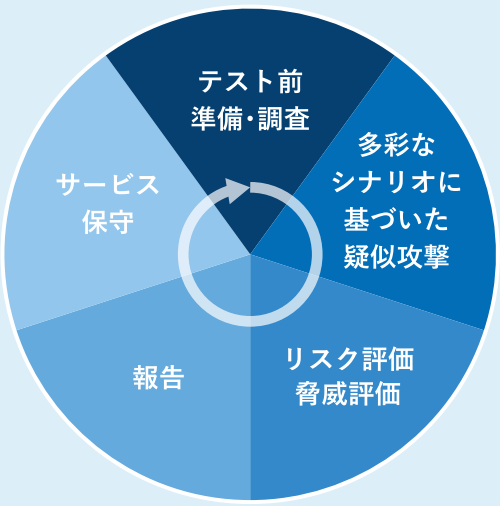
弊社サービスの場合　SQAT® ペネトレーションテスト

ペネトレーションテストに際しては、入念なヒアリングがカギとなります。

弊社「SQAT® ペネトレーションテスト」ではテスト前の準備・調査をしっかりと行うことで、具体的かつ多様なシナリオを用いた疑似攻撃が可能であり、かつ不要なところに影響を与えない疑似攻撃が可能なため、効果的な結果が得られます。

リスク評価・脅威評価や報告に際しては、専門のアナリストチームによる入念なチェック体制があります。

サービス保守としても、テスト実施後のメニュー（一部有償）をご用意しています。



サービス	脆弱性診断、ペネトレーションテストの経験を持つ有資格技術者を中心としたチームによる検査・テスト
	OWASP Top10、ASVS、NIST SP800シリーズなど各種国際的標準を踏まえた侵入項目
	詳細な検出状況を網羅した報告書
コミュニケーション	技術担当者同席で侵入前のご相談実施
	侵入・報告書監査・ツール開発などの専門チームによるお客様への支援・対応
	専用ポータルと専用サポートデスクによる円滑なコミュニケーション
サポート	継続保守を目的とした自動診断・改竄検知・ソースコード検査メニューのご提供あり（有償）

詳しいサービス紹介はこちら

ペネトレーションテストとは

ペネトレーションテストとは「侵入テスト」とも呼ばれる、システムに対してあらゆる技術やツールを駆使してサイバー攻撃を仕掛け、侵入できるか否かを検証するテストである。事前に作成した攻撃シナリオに則って、実際にシステムに疑似攻撃・不正アクセスを行い、ゴールとして設定していた事項が達成できるかを試行するのがよく用いられる手法だ。また、ペネトレーションテストの実施が推奨されるシステムを持つ業界（下図）以外でも、脆弱性対策や侵入対策が不十分な組織がサプライチェーン上に存在すると、サプライチェーン攻撃の標的とされる可能性もあるため、気を抜かずに定期的なリスクの可視化・分析が必要である。

ペネトレーションテストの実施が推奨されるシステム

生命・生活に直接影響を与える事業に関わるシステム

例 水道・電気・ガス・道路・交通などの社会インフラ
病院、ビル管理、工場のシステム

資産に影響を与える個人情報を扱うシステム

例 銀行や証券会社、クレジットカード、仮想通貨取引所など金融・保険業
自治体や官公庁

事業継続に影響を与える機密情報を扱うシステム

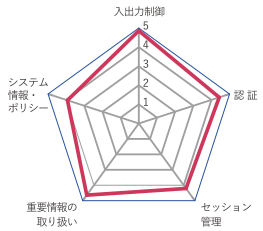
例 重要度の高い営業情報や、特許未取得の知的財産などを保持するシステム

FYI

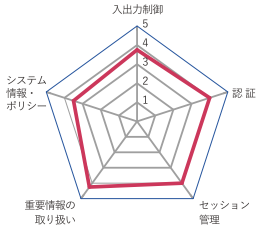
これらの業界の弊社脆弱性診断結果

インフラ、医療,福祉、金融業,保険業の業界について、弊社で実施した脆弱性診断結果の統計は下図のとおり。これらの業界は、他業界と比べても特に高いセキュリティレベルの維持が求められるため、全体的にスコアは高い。それでも例えば古いミドルウェアの脆弱性（「システム情報・ポリシー」カテゴリに該当）を突かれて侵入されてしまうケースがある。しかし、アップデートが容易でないシステムもあり、システム単体ではなく、他のソリューションと組み合わせることでセキュリティ強化を行っている場合もある。ペネトレーションテストであれば、それらを含めたリスク分析を実現できる。脆弱性診断結果から見えた、セキュリティ面で心配な部分をテストシナリオに組み込むのも良いだろう。

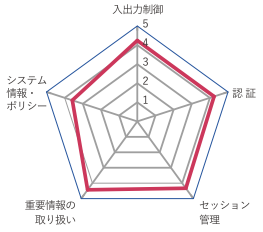
電気・ガス・熱供給・水道業



医療,福祉



金融業,保険業



その他の業界の統計情報も「業界別診断結果レーダーチャート」（P.21〜）に掲載している。また、「電気・ガス・熱供給・水道業」については、経年を踏まえて述べたパートもあるので、ご参照いただきたい。

ペネトレーションテストの効果

実際にペネトレーションテストを行うと、どのような効果があるのか。ここまでで述べた通り、ペネトレーションテストでは、攻撃者（侵入者）の目線で攻撃を試行する。そのため、実際に攻撃が成功するのか、今実施している対策は有効なのか、成功した場合にどのような被害が出るのかといったことが確認できる。

ペネトレーションテストの効果

- 検出された脆弱性を悪用して攻撃可能か確認できる
- 特定の目的（ゴール）を達成可能か試行することで、現在のセキュリティ対策の有効性を確認できる
- 攻撃された場合の影響範囲・被害レベルを確認できる
- システム特性に応じた効果的な防御方法構築に役立つ