



# NEWS RELEASE

2020年7月15日

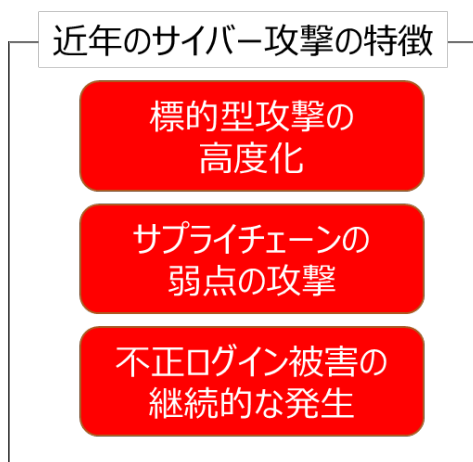
株式会社ブロードバンドセキュリティ

## 「SQAT®ペネトレーションテスト」の提供を開始 ～多様なシナリオによる疑似攻撃でシステムを包括的に診断し、被害を最小化～

株式会社ブロードバンドセキュリティ（本社：東京都新宿区、代表取締役社長：持塚 朗、以下 BBSec）は、このたび脆弱性診断サービスのラインナップを拡充し、新たに「SQAT®ペネトレーションテスト」の提供を開始いたします。これは、従来オプションサービスとして提供していたペネトレーションテストを刷新し、標準サービスとしてリリースするものです。既に、地方銀行様での採用が決定しており、金融業界をはじめとする、高度なセキュリティ対策を推進されているお客様のご利用を想定しています。

### サービス提供の背景

経済産業省による最新の調査報告『昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について』（2020年6月12日）<sup>1</sup>では、近年のサイバー攻撃の特徴として、「標的型攻撃の高度化」「サプライチェーンの弱点の攻撃」「不正ログイン被害の継続的な発生」の3つが挙げられています。今日の企業・組織には、「関連し合うシステムの弱い部分を狙った継続的で高度な攻撃」への備えがこれまで以上に求められているといえます。



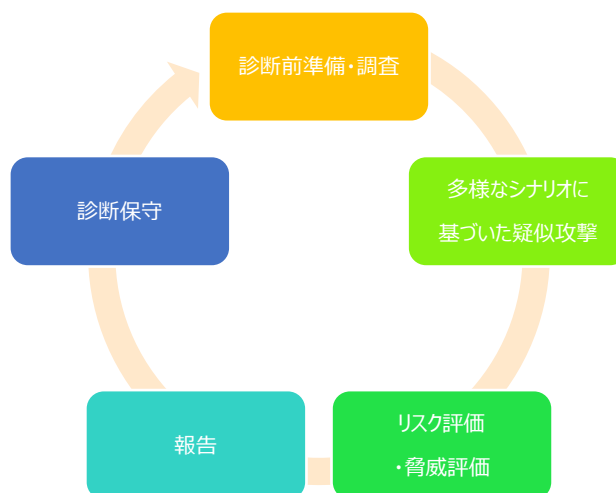
（経済産業省『昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について』より弊社作成）

<sup>1</sup> <https://www.meti.go.jp/press/2020/06/20200612004/20200612004-1.pdf>

「ペネトレーションテスト」とは、事前の綿密な調査により特定した「システムのより弱い（脆弱な）個所」を起点としてシナリオベースの疑似攻撃を仕掛け、システムの堅牢性を確認する検査です。実際の攻撃を体験することにより、効果的な防御方法（システム・運用方法）の構築が可能となり、万一攻撃者にシステムへ侵入された場合の被害の最小化につながることが期待されます。BBSec では従来より、PCI DSS 等の厳格なセキュリティ規制を課される金融業界のお客様を中心に、オプションメニューとして同サービスを提供し、多数の実績を積んでまいりました。そうした中、前述のようなサイバー攻撃の現状、お客様からのご要望の増加を受け、このたび標準サービスとして提供を開始いたします。

### サービスの概要

「SQAT<sup>®</sup>ペネトレーションテスト」では、まず診断対象の詳細な分析を実施後、システムの弱点を特定した上で疑似攻撃を仕掛けます。この疑似攻撃では、一般的なペネトレーションテストでターゲットとする Web アプリケーションやネットワークインフラだけではなく、無線 LAN からの侵入や疑似マルウェアへの感染などの現実的かつ多様な攻撃起点・ゴールを設定したシナリオを用います。疑似攻撃終了後、対象システムの特性を踏まえたリスク評価のほか、BCP に対するリスク評価、トレンドに基づく脅威評価などを実施し、その結果をご報告します。これに加えて本サービスでは、問題部位が解消されたことを確認するための再診断を無償（診断後 3 カ月以内）でご提供したうえで、継続的なサポートを提供する各種診断保守メニュー（一部有償）をご用意している点に大きな特徴があります。

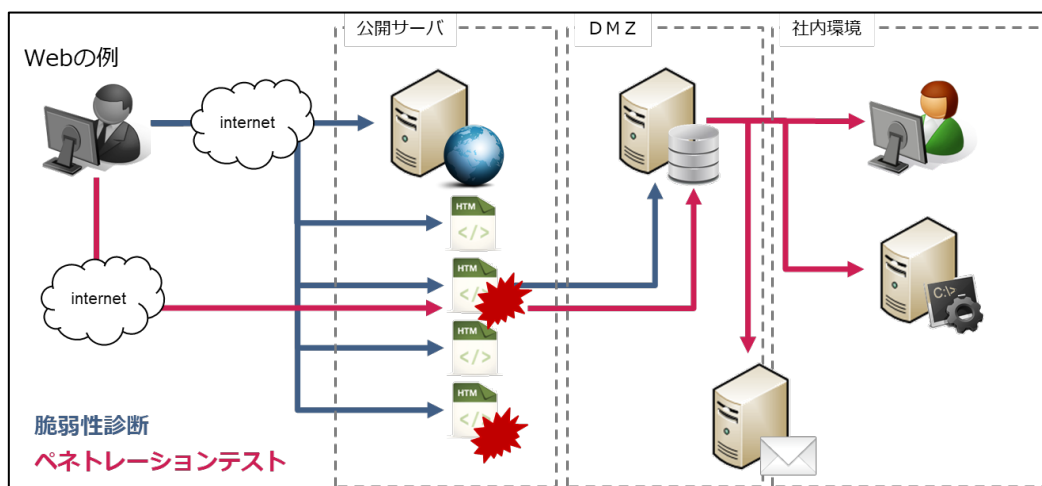


また、本サービスでは、長年の診断経験を活かし、次の 3 つの要素を核に、お客様のご要望に応じたきめ細かなサービスを提供いたします。

サービス	お客様とのコミュニケーション	サポート
<ul style="list-style-type: none"> <li>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技術者による検査・テスト</li> <li>OWASP Top10、ASVS、NIST SP800シリーズなど各種国際的標準を踏まえた診断項目</li> <li>詳細な検出状況を網羅した報告書</li> </ul>	<ul style="list-style-type: none"> <li>技術担当者同席での診断前のご相談</li> <li>診断・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</li> <li>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（診断実施前後）</li> </ul>	<ul style="list-style-type: none"> <li>診断後3カ月以内の再診断（無償）</li> <li>継続保守を目的とした自動診断・改ざん検知・ソースコード検査メニューの提供（有償）</li> </ul>

参考：脆弱性診断とペネトレーションテストの違い

	脆弱性診断	ペネトレーションテスト
対象	ネットワークやインフラ、Webアプリケーション	ネットワークやインフラ、Webアプリケーションに加えて、物理侵入テストを含むことも
目的	脆弱性の検知・検出	不正アクセス、侵害行為が成立するかどうかの確認
範囲	広く網羅的に診断	侵入する、侵害行為が成立するためのポイントを探すことが目的となるため、必ずしも範囲は広くない
期間	対象範囲及び仕様により決まるが、ペネトレーションテストよりは短期間	脆弱性診断よりも長い期間を要する場合もある



## サービス提供価格

テストのシナリオ、実施規模により異なります。詳細はお問い合わせください。

## BBSecについて

株式会社ブロードバンドセキュリティは、ITセキュリティの診断・運用・保守・デジタルフォレンジックを手掛けるトータルセキュリティ・サービスプロバイダーです。「日本のITネットワークを世界一堅牢にする」をコンセプトに、2000年11月の設立以来、高い技術力と豊富な経験、幅広い情報収集力を生かし、大手企業、通信事業者からITベンチャーに至るまで、様々な企業のITサービスをセキュリティ面でサポートしています。

URL : <https://www.bbsec.co.jp/>

## SQAT®について

「SQAT®」(Software Quality Analysis Team)は、株式会社ブロードバンドセキュリティが提供する脆弱性診断サービスです。高い専門スキルを備えた有資格者を多数擁するチームが、さまざまな側面から総合的な診断を実施し、組織の情報システムの強化を支援します。金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで、幅広い業界のお客様にご利用いただいています。

**SQAT** Software Quality Analysis Team

URL : <https://www.sqat.jp/>

以上

### 【本リリースに関するお問合せ】

株式会社ブロードバンドセキュリティ 経営企画室

TEL : 03-5338-7430 E-mail : [press@bbsec.co.jp](mailto:press@bbsec.co.jp)

### 【本サービスに関するお問合せ】

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

TEL : 03-5338-7417 E-mail : [sales@bbsec.co.jp](mailto:sales@bbsec.co.jp)