令和５年３月 22 日

各　位

株式会社ビヨンドブルー
代表取締役　木村光秀
横浜市鶴見区鶴見中央４－36－1

いつもの脆弱性診断やプラットフォーム診断からステップアップ！ 新サービス「ファスト ペネトレーションテスト」を 60 万円から

レイ・イージス社と連携し予算で断念していた方、難しそうで敬遠していた未経験者向けに提供開始

サイバーセキュリティ対策ソリューションや DX 支援・デジタルアドバイザリー事業を手がける株式会社ビヨンドブルー(本社:神奈川県横浜市、代表取締役:木村　光秀　以下ビヨンドブルー)はペネトレーションテストサービスを展開するグローバル企業のレイ・イージス・ジャパン株式会社(本社:東京都新宿区、代表取締役　青木登)と連携し、これまで関心はあっても、高額でペネトレーションテスト(侵入試験)を断念していた金融機関や、インターネットサービスを展開する企業様に気軽に試していただける簡易ペネトレーションテストを開発し攻撃面として最も容易なインターネット面に限定し弊社独自ツールで一定程度の自動化を図ることで、コスト面でペネトレーションテストを実施できなかったお客様や、これから初めてペネトレーションテストを行うお客様にも導入いただきやすいパッケージに仕上げました。

1. 背景

ペネトレーションテストは、一般的に数百万円や数千万円と高額になりやすいことから、コスト面においてどうしても手が出しづらいとのお声を数多くいただいておりました。
この度お客様のご要望にお応えするため、独自開発ツールによる自動化により、インターネット面に面したネットワーク機器に限定することで、初めてのお客様にもお求めになりやすい低価格でのペネトレーションテストパッケージの提供を開始しました。

通常、プラットフォーム診断、ペネトレーションテスト、レッドチーム、TLPT と順に高度で難易度の高い試験になっていくが、本サービスは、プラットフォーム診断とペネトレーションテストの中間に位置するサービスで、インターネットに面したシステム（ファイヤーウォール、VPN 接続機器、外部 DNS, メールサーバー、コーポレートサイト等）に対して、プラットフォーム診断に加えて、一般的によく見られる攻撃手法により簡易ペネトレーションテストを実施する基本的なパッケージサービスとなっており、これまでハードルの高かったペネトレー

ションテストを実施してみたい企業様に待望のソリューションに仕上がっております。

■こんなお客様にオススメです。

・これまでにペネトレーションテストの実施経験がないお客様
・ペネトレーションテストの実施をコスト面から見送られていたお客様
・コスト面からペネトレーションテストを 2.3 年ごとなど、期間を空けてしか実施できなかったお客様
・プラットフォーム診断だけでなく、侵入につながる悪用可能性を検証したいお客様

すでに、複数の金融機関様での採用も決まっており、今後、監督官庁の セキュリティ対策における監査要求が上がっていく中、限られた予算の中で優先するリスク管理の中で、これまでより深いレベルでの試験を手軽に実施することが可能となります。サービス名称通り、ヒアリングシートを受領し契約締結後、診断開始から５IP までのデバイスであれば最速（ファスト）5 日間で診断作業は完了します。これには、ブルートフォース攻撃や DoS 攻撃の耐性確認、ユーザアカウント情報の列挙などが行われます。診断後は標準で 5 営業日以内に診断報告書が提出され無償で診断報告会も含まれております。

このテストを通じて、段階的に自社システムをブロック単位でより深い診断にレベルアップして診断をしてもらい、一度に実施すると数千万と高額になるペネトレーションテストを細分化することで、より身近なサービスに感じてもらうことを狙いとしています。

１．サービス概要

対象機器	ファイアウォール、VPN接続機器、外部DNS、メールサーバー、コーポレートサイト（ホームページ）等 （原則としてインターネットからアクセスできる機器・IPアドレスが対象です）
標準診断期間	5営業日(（追加：＋1営業日/2IPアドレス毎）)
ご報告書作成	診断完了後5営業日
アフターサポート	修正箇所に対する再診断（ご報告書提出から3か月以内で1回） メールによるお問い合わせ（ご報告書提出から3か月以内・回数制限無し）

診断項目	**診断内容**
プラットフォーム診断	対象機器へのプラットフォーム診断の実施
脆弱性の悪用	プラットフォーム診断で発見された脆弱性の悪用可否確認
露出情報の収集	インターネットに露出している、または脆弱性を悪用することで取得できる対象システム関連情報の収集
ユーザー・アカウント情報の列挙	認証用ユーザー情報等、ユーザー・アカウント情報の収集に対する対策有無の確認
ブルートフォース攻撃	対象機器に対してよく利用されるログイン情報をもとにブルートフォース攻撃を実施し、耐性を確認
DoS攻撃耐性の確認	DoSにつながりうる挙動が発生するかを疑似的に確認 （実際のサービス停止を直接的に引き起こす攻撃は実施いたしません）

２．株式会社レイ・イージス・ジャパンについて

RayAegis Information Security（本社、台湾、新北市新店区、Founder 江 格、以下「RayAegis」）とアリス社の合弁で設立された経験豊富で技術力の高いホワイトハッカーを 300 名以上擁するプロフェッショナル集団です。AI を利用した独自開発ツールを活用し、高度な Web アプリケーション脆弱性診断やペネトレーションテスト、TLPT、DDoS 演習などのセキュリティサービスで急成長した台湾トップ企業で政府、軍、金融機関にとりわけ強く、世界のグローバル企業においても多数採用されています。2022 年 4 月に（株）ビヨンドブルー社と提携し、国内金融機関を中心に採用企業を伸ばしております。

以　上

＜本件に関するお問い合わせ＞
【報道関係の方】
株式会社ビヨンドブルー　管理部　　広報担当まで
TEL：045-502－7068　　MAIL： toiawase@beyondblue.tokyo
https://beyondblue.tokyo