RayAegis® Japan

Keep the Lights, Keep the Fights, for Security Future

Ray Aeigs Japan ペネトレーションテスト

PCI DSS V4対応

PCI DSS v4.0準拠要件に対応するペネトレーションテストを提供します。
総勢350名以上*のホワイトハッカーを擁するレイ・イージス・グループが
世界中でペネトレーションテスト、レッドチームオペレーションの実績と
経験を通じて最高品質のテストを提供します。

*: 2024年12月時点での数字です。

株式会社レイ・イージス・ジャパン

ペネトレーション（侵入）テストの効果とは？

「もし泥棒があなたの会社に侵入しようとしたら…」

実は、サイバー攻撃も同じです。ペネトレーションテストは、セキュリティの専門家があなたの会社のシステムに「善意の侵入テスト」を行うサービスです。

実際の攻撃が起きる前に、システムの弱点を見つけ出し、対策を立てることができます。例えば、悪用されがちな脆弱性の有無や簡単に破られてしまうパスワードなどを発見し、改善案を提示します。
世界では毎日約30万件のマルウェアが作られ、多くの企業が攻撃の標的となっています。事前の対策で、大切な情報や会社の信頼を守りましょう。
このテストは、経験豊富な専門家が安全に実施するため、業務を妨げることなく、確実にセキュリティを強化できます。

ペネトレーションテストの種類と費用

	ペネトレーション 検査項目数：105項目	**ASVS L1 準拠版** 検査項目数：142項目以上	**備考**
小規模	128万円	192万円	
中規模	148万円	222万円	一般的なWebサーバはペネトレーションの中規模になります。
大規模	168万円	252万円	

上記サービスの価格詳細については（株）レイ・イージス・ジャパンまでお問合せください。
なお、上記価格情報については予告なく変更される場合がありますのでご了承ください。

ペネトレーションテスト期間（ご参考）

STEP	1日目	2-3日目	4-5日目	6-7日目	2-4週目	5-7週目	（後日調整）
お申込み	1日						
ヒアリング		2日					
御見積			2日				
ご発注				1日			
診断日程調整				1日			
診断実施					3-4週間		
結果報告・対策のご提案						15営業日	
報告会							1日（通常１H程度）
再診断							1年以内に実施

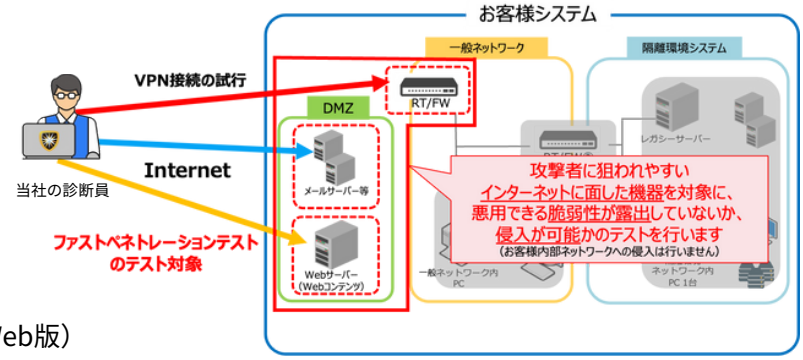
株式会社レイ・イージス・ジャパン

シナリオ別のペネトレーションテストの例

『**ファストペネトレーションテスト**』プラットフォーム診断の結果と組み合わせ、基本的な対策が取れているか確認するサービスとなっており、以下のような診断を行います。

- 一般的なプラットフォーム診断21項目
- 発見された脆弱性が実際に悪用できるかをレイ・イージス独自開発のツールにより確認
- よく利用されるログインID・パスワード等でのログイン試行（約3000件）
- アカウント情報などを列挙できるか確認し、可能な場合は収集・提示
- Webアプリケーションに対する基本的な脆弱性診断

診断項目：最大35項目（標準） / 57項目（Web版）

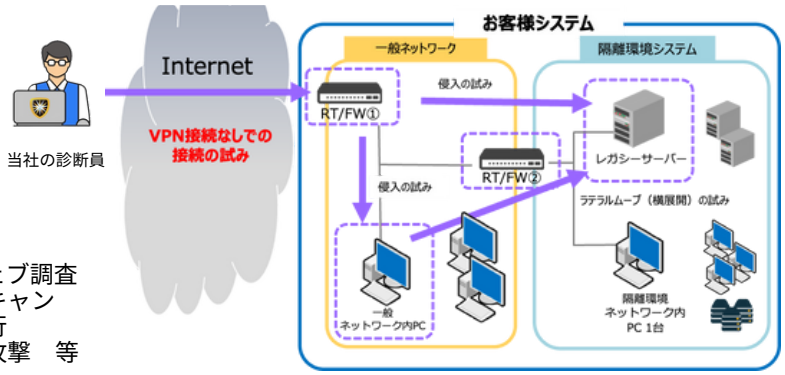


『**外部ペネトレーションテスト**』AIエンジンによる検出ロジックを追加した脆弱性診断・疑似攻撃ツールなどを駆使し、経験豊富なレイ・イージスのホワイトハッカーがシステムへの侵入を試みます。

このシナリオでは、攻撃者が組織の「外殻」をどのように突破するかを模擬します。脆弱性診断では既知の脆弱性を網羅的に調査し、ペネトレーションテスト（侵入テスト）ではそれらの脆弱性を実際に利用（悪用）してシステムへの侵入を試みます。

主な対象:
- 公開Webサイト
- メールサーバー
- VPNゲートウェイ
- クラウドサービス

実施手法:
- OSINT・ダークウェブ調査
- ポート・脆弱性スキャン
- エクスプロイト試行
- ブルートフォース攻撃　等

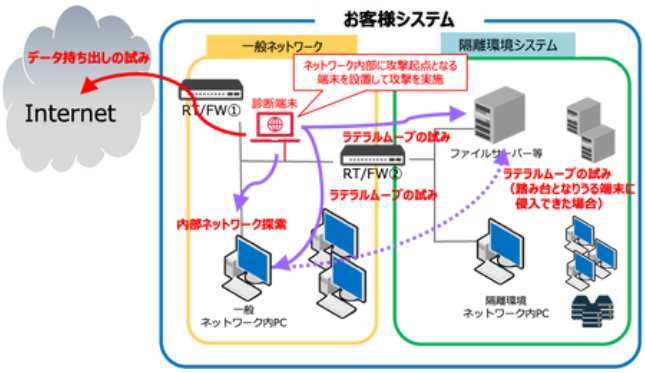


『**内部ペネトレーションテスト**』踏み台経由や内部端末からの内部侵入は、外部システムが侵害された後や、マルウェア感染後の段階を想定します。

このシナリオでは、攻撃者が組織の内部ネットワークにどのようにアクセスし、より価値の高い資産にたどり着くかを検証します。多くの場合、最初に侵害されたシステムを「踏み台」として使用し、内部ネットワークへの侵入を試みます。

主な対象:
- ADサーバー
- ファイルサーバー
- 従業員のPC
- VPN機器

実施手法:
- 権限昇格
- 内部ネットワーク探索
- 疑似マルウェア
- 中間者攻撃　等

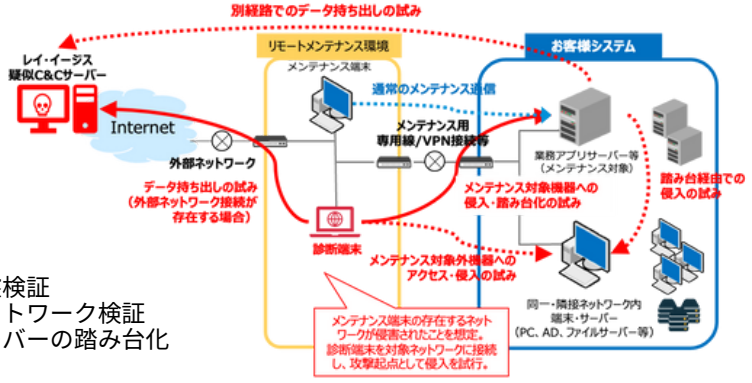


『**サプライチェーンペネトレーションテスト**※』実際の攻撃者の視点で見つける、あなたの会社の"隠れた入口"を想定します。

このシナリオでは、実際の攻撃者の視点で、システムの社外メンテナンス環境を経由し、重要な社内システムまでの侵入可能性を検証。その過程で発見された脆弱性に対して、具体的な対策を提案します。事後対応ではなく、事前の防御で大切な情報を守ります。

主な対象:
- 社内業務システム
- 認証システム
- クラウドサービス連携
- バックアップシステム

実施手法:
- サプライヤー認証基盤検証
- サプライチェーンネットワーク検証
- メンテナンス対象サーバーの踏み台化
- 情報窃取手法の検証



※リモートメンテナンス環境での実施にあたり、外部ベンダー様にもご協力をいただくシナリオです。

株式会社レイ・イージス・ジャパン

RayAegis® Japan

Keep the Lights, Keep the Fights, for Security Future

サービス提供元：株式会社レイ・イージス・ジャパン

住所：〒160-0023 東京都新宿区西新宿7-22-33 Polar西新宿 4階

メール：info@rayaegis.co.jp　電話：03-6703-6619

ホームページ

お問い合わせ

販売代理店

株式会社レイ・イージス・ジャパン