攻撃者の視点で“真の脆弱性”を可視化する

ペネトレーションテストサービス

JISC
Japan Information Service Co, Ltd.



そのセキュリティ対策、“本当に有効”だと証明できますか？



システムを直接攻撃

脆弱性の「疑い」ではなく
脆弱性「そのもの」を明示

信じる根拠がある診断

国際認証取得ツール**NodeZero**と
元米国CISOホワイトハッカー監修で
精度も安全性も保証

NodeZero
BY HORIZON3.ai

Government-Grade Security Assurance

- **Authorized** at the **FedRAMP High** Impact Level
- **SOC 2 Type II** Examination Completed
- Designed to **Support GDPR** Requirements



証拠を提示

脆弱性攻撃成功に至るメソッドと
その対策案を詳細にレポート

高速・自律型ペネトレーションテスト

ペネトレーションテストサービスは、Horizon3.ai社の自律型テストツール「NodeZero」を活用して実施します。
一般的な自動診断ツールのように決められた手順を繰り返すのではなく、実際の攻撃者の行動を再現しながら検証を進めるため、人による手動テストと同等以上の検証を、より短時間で実現します。

NodeZero BY HORIZON3.ai

・Authorized at the FedRAMP High Impact Level
・SOC 2 Type II Examination Completed
・Designed to Support GDPR Requirements

最新の攻撃手法を踏まえた実践的かつ信頼性の高い評価を行い、監査対応はもちろん経営層や取引先への説明にも活用できる説得力のある診断結果をご提供します。

私たちは Horizon3.ai 社の日本におけるファースト・パートナー企業です
※パートナーは各国・地域ごとに数社限定で認定されています

複数の異なるAI技術を統合して設計されたNodeZero

なぜ、NodeZeroが攻撃者の行動を再現できるのか、人と同等以上の検証が自律的に実現できるのか、説得力のある診断結果を提供できるのか。
その理由は、攻撃シミュレーションに特化した3種類のAIを組み合わせ、統合システムとして設計されているからです。

NodeZeroは、**グラフ推論**によって攻撃の道筋を組み立て、状況に応じて次に取るべき行動を判断します。実際の攻撃実行は確実なロジックで行い、**機械学習**で結果を整理・評価します。

NodeZero BY HORIZON3.ai

さらに**独自の生成AI**を活用して状況の解釈や次の攻撃方針の検討を補助し、説明の生成だけでなく攻撃プロセス全体を支援します。これにより、実証に基づいた納得感のある診断結果を提供します。

- グラフ推論 Graph-based reasoning
  攻撃計画や経路発見のための論理的推論に使われるAI技術
- 機械学習 ML／Classical ML
  データ分類や行動パターンの識別など探索／評価の補助に活用
- 限定的な生成AI Scoped GenAI
  レポート作成や難易度の高い次の攻撃ステップ提案に用いる

攻撃者の視点でリスクを可視化する

多くの企業が、脆弱性診断や設定見直しなどのセキュリティ対策を行っています。しかし――
それが「実際の攻撃」に耐えられるかどうかは、まったく別の話です。

ペネトレーションテストの流れ

攻撃者の視点から、事前に合意した範囲内で安全に疑似攻撃を実施し、システムに脆弱性が存在するかを検証します。
さらに、その脆弱性が実際に悪用可能か（不正侵入や権限取得が成立するか）まで確認します。
これにより、本当に優先して対処すべきリスクを明確にします。この流れは人であってもツールであっても同じです。



段階	内容
① 偵察 Reconnaissance	対象システムで公開・稼働しているサービスを確認し、攻撃の入り口となり得る箇所を洗い出します。
② 情報収集 Information Gathering	システムやソフトウェアの設定状況を確認し、既知の脆弱性や設定不備がないかを調査します。
③ 初期侵入 Initial Access	発見した脆弱性を利用し、疑似攻撃を実施します。 実際に侵入が可能かを検証し、リモートコード実行の可否を確認します。
④ 権限昇格の検証 Lateral Movement	一般利用者の権限から、管理者レベルの操作が可能になる危険性がないかを検証します。
⑤ 被害リスク評価 Privilege Escalation	侵入後、他のサービスやサーバへアクセス可能かを検証し、被害拡大の可能性を評価します。

セキュリティ対策の“証明”が求められる時代に

セキュリティ対策は **“やっていること”** ではなく **“守れていること”** が問われる時代です。
サイバー攻撃の高度化、法規制や顧客からの要求強化により、企業は **”脆弱性がないこと”** だけでなく **”脆弱性が突破されないこと”** を証拠をもって説明する責任が求められています。

■ISO27001やISMAPのペネトレーションテスト推奨
■大企業・金融機関からSOC2 Type2と同レベルの評価要求
■JNSAレポートでは“実効性ある脆弱性管理”が求められる

当社のペネトレーションテストは単なる脆弱性の洗い出しではなく
攻撃者視点で **“本当に突破できるか”** を検証し、次の **“3つを可視化”** します。

現場が迷わず対策できる
リスクの優先順位

課題を明らかにする
防御範囲と理由

ビジネスリスクを抑える
安全性の証明

私たちは、セキュリティの **“実効性を証明するパートナー”** として、ITシステムの脆弱性管理を実現します。

ペネトレーションテストの利用シーン

当社のペネトレーションテストサービスは、以下のような課題を解決します。

防御策が本当に機能していることを検証することができない



導入済みのセキュリティ対策が本当に効果を発揮するか、現実の攻撃を直接行って評価します。

新規・更新するシステムの安全性をリリース前に確認したい



クラウドサービスやWebアプリの公開前に脆弱性を評価することで堅牢なシステムをリリース可能です。

スキャナ診断の結果が大量でどこから対策すべきか分からない



攻撃に成功したルートだけを明示するため、誤検知・過検知もなく優先度も明確に提示可能です。

監査や取引先から対策の有効性を説明するよう求められている



攻撃ログ・成功可否を含むレポートで、説明責任に柔軟に応えることが可能です。

セキュリティは適切な管理を維持し続けることが重要

近年、サイバー攻撃の手法は高度化・巧妙化を続けており、その進化は止まることがありません。攻撃者は常に新たな脆弱性や手口を研究し、従来の対策をすり抜ける方法を生み出しています。その結果、企業や組織が受ける被害は年々拡大傾向にあり、情報漏えいや業務停止、信用失墜など、経営に重大な影響を及ぼす事例も増えています。
セキュリティ対策は一度実施すれば終わりではありません。
実効性を確保するためには、ペネトレーションテストを定期的に実施し、現時点での脆弱性や対策の有効性を継続的に検証することが不可欠です。

弊社のペネトレーションテストサービスは、お客様の様々なニーズにお応えします。

ご要望に応じて定期的に実施することが可能です　実施頻度は自由に選択いただけます

閉鎖環境や特殊な環境下においても、ホワイトハッカーによる手動での検証が可能です

脆弱性に関するお悩みやご質問がございましたら、お気軽にご相談ください



モノと人をスマートに結ぶ

サービスについてのお問合せ

ジスクソフト株式会社
システムソリューション事業部

contact@jisc.co.jp