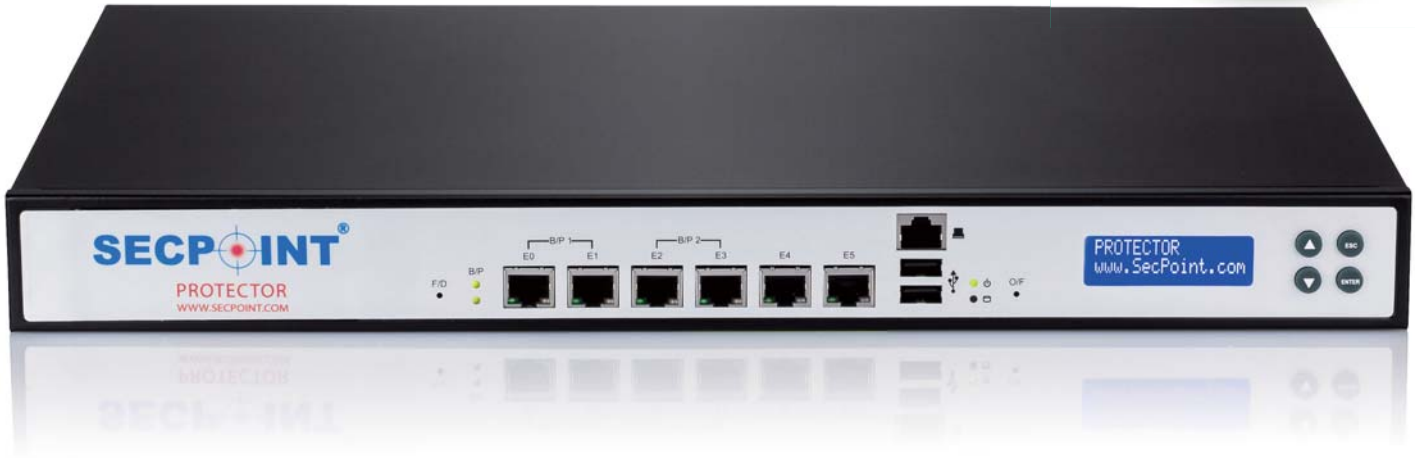
# 欧州各国政府機関やインフラ企業での採用実績が豊富な非破壊型脆弱性検査ツール

SECPOINT® Penetrator

Wi-Fi 脆弱性診断も可能

1年間使い放題
64,000円～
圧倒的低価格




## 6万件の脆弱性リスト。毎月500件強追加

SQLインジェクションやXSS、SSLの脆弱性は即座に発見可能です。脆弱性を抱えるCMSも簡単に問題点を発見できます。NAS、Wi-Fiルータ、ネットワークカメラの脆弱性も含んでいます。米国HIPAA法に基づく健康情報に関するプライバシールール及びセキュリティルール、PCI DSS に基づくクレジットカード情報および取り引き情報を保護するためのグローバルセキュリティ基準、OWASP Top10、Google ハックデータベースなど豊富な情報セキュリティ監査に準拠して活用いただけます。Microsoft Windowsの脆弱性はもちろん、Bugtraq ID / Mitre CVE / Ubuntu USN / OSBDBも含んでいます。

## 脆弱性検査ツールを自社利用

脆弱性診断はBackTrack Linux, Kali Linuxなどのペネトレーションツールを用いて行うことが一般的でした。このため、企業における専門知識を持たない品質検査部門において活用することは困難でした。そこで、一般の人でもプルダウン操作で簡単に脆弱性診断を行いやすくしたのが、脆弱性検査ツール「Penetrator」です。
1999年にデンマークで脆弱性診断ツール専門ベンダーとして誕生以来、15年以上の歴史をもつ世界的権威のSecPoint社が開発・提供しているこの脆弱性診断ツールはIoT時代を見据え、様々なデバイスやソフトウェアを膨大な脆弱性情報をもとに診断します。自社運用することで、新発売の商品だけでなく、発売済の商品の脆弱性診断を定期的に行うことで、商品の品質担保を行うことが可能となり、他社製品との差別化が行えます。

また、700以上の実際のエクスプロイト攻撃をシミュレーションし、外部ネットワークセグメント上のWindows、Unix、ルータやファイアウォール等から社内ネットワークへ侵入をする検査を実施することが可能です。

## バックドアフリーのデンマーク製

企業や市民の権利よりも国家権力が勝る米国、ロシアおよび中国とその傀儡国家の製品ではなく、市民の権利が強いデンマーク製です。バックドアがないことを開発元が宣言しており、欧州政府機関やインフラ企業でも採用実績があり、安心して利用できます。

## 小規模から大規模検査まで

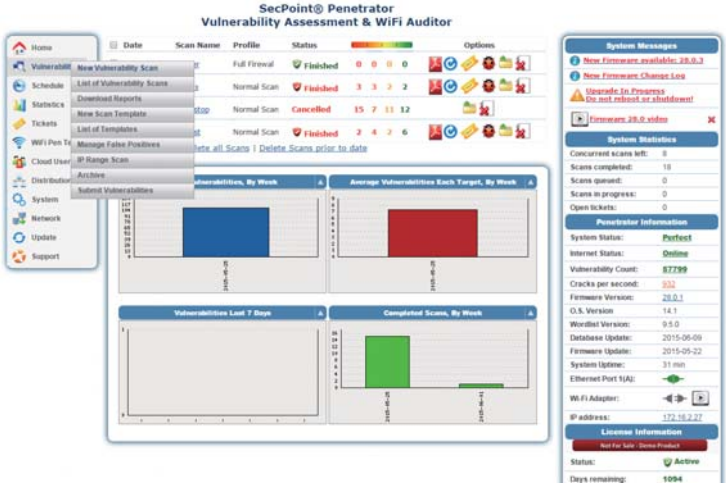
同時監査 1 IPで年間64,000円というお手頃な価格から、ノードとホスト構成で複数台のノードで大規模な検査まで、スケーラブルに対応可能です。

## Wi-Fi脆弱性検査や可搬型

・Core i7ノートパソコンへ搭載することで、優れ可搬性を発揮。診断箇所へ迅速に持ち込むことができ、検査がスムーズに行えます。
・ノード・ホスト構成も可能で、ノートパソコンを多数のノードとして一時的に配置して検査し、ホストで包括的にレポートを行うことも可能です。

## GUIによる簡単な操作

プルダウン型のGUIを搭載し、技術者でなくとも扱いやすくなっています。
スケジュールを設定して、定期的な監査を自動で実施することも可能です。




## 3つのモデルをご用意

・仮想型 Portable Penetrator
Windows/Mac/Linuxのパソコンに導入して利用する可搬型で検査箇所の汎用性に優れています。Wi-Fi脆弱性診断も可搬型であれば測定場所を選びません。
・アプライアンス型 Penetrator
アプライアンス版のPenetratorは、診断処理能力に優れ高速な検査が可能です。大規模な検査にはアプライアンス版の利用をお勧めします。
・クラウド型 Cloud Penetrator
ECサイトやCMSを運用するサービスを多数抱えている場合に、定期的な検査を行うのに便利なSaaSモデルです。機器導入などは一切必要なく利用可能です。

## お求めやすい低価格

日本の皆様へ脆弱性診断の国際的な価格で提供するため、直販にてお求めやすいプライシングを実現しています。仮想化版は、Windows/Mac/Linux/vmware/Hyper-Vに対応し、高速なアプライアンスモデルもご用意しております。

・同時スキャンを行うIPアドレス数によるわかりやすい価格体系
・1年利用とお得な 3 年利用のサブスクリプション権で販売
・年間無制限に診断可能
・保守費用なし

【年額】(消費税別)
仮想型 Portable Penetrator (同時 1 IP/ソフトウェア版) 64,000円
仮想型 Portable Penetrator (無制限/ソフトウェア版) 2,448,000円
アプライアンス型 Penetrator (同時 4 IP / Mini Case) 193,000円

## 診断可能なもの

・WEBサービスなどのDMZセグメントに配置されたサーバ
・社内利用パソコンや社内サーバ
・社内利用パソコンへの外部からの浸入
・社内のSIP電話機、プリンター、ルーター、ネットワークカメラなどのネットワーク機器
・社外からルーター、ファイアウオール、プロキシサーバー等
・パソコンのブラウザやアプリに起因する脆弱性
・Wi-Fi通信方法における脆弱性

## 診断不可能なもの

・スマートフォンのアプリケーションがもつ脆弱性
・某国諜報機関が仕掛けたルーター装置へのルート権限バックドアの発見
・全く未知の脆弱性
・TCP/IP通信を伴わないもの
・IPS等の脆弱性スキャナー防止機能及び攻撃を断続的に行うとアクセスを一時的に拒否する装置

日本地区総ディストリビューター
Bluestar CORPORATION
〒105-0003　東京都港区西新橋1丁目6-12　AIOS虎の門 4階

Penetrator ホームページ: http://penetrator.blue.co.jp/
お問い合わせ : info@blue.co.jp