SecuAvail
NEWS RELEASE

関係各位

令和 8 年 11 月 17 日
株式会社セキュアヴェイル
東証スタンダード 3042/札証本則 証券コード 3042
代表取締役社長　米今政臣

セキュアヴェイルの次世代 SOC サービス『AI-SOC』が SonicWall TZ シリーズに対応

IT セキュリティの専業企業、株式会社セキュアヴェイル（本社：大阪市北区、代表取締役社長：米今政臣、証券コード：3042、以下セキュアヴェイル）は、創業より 25 年にわたって提供する SOC サービス（セキュリティ運用サービス）の運用経験とグループ会社である株式会社 LogStare が開発した AI ログ分析機能を活用した『AI-SOC』サービスを提供しております。

昨今の増大する不正アクセスへの対策や現状調査の一助になれるよう『AI-SOC』サービスのラインナップを拡張し、この度 SonicWall TZ シリーズに対応した『AI-SOC for SonicWall』を提供開始します。

セキュアヴェイルの SonicWall UTM の運用実績と LogStare が開発した AI ログ分析機能を有効的に活用した SOC エージェント機能によって、月額￥9,800 という低価格での提供を実現します。

『AI-SOC for SonicWall』は、SonicWall UTM を通過する全ての通信のログを分析し、外部からの不正アクセスや内部からの不正通信による情報漏えいの可能性などを検知してアラートします。「状況サマリー」「詳細分析」「詳細調査・対応」などのレポートを AI がアラートと共にメールでお知らせします。

また、月次レポートとして SOC エージェントによる 1 か月間の通信を分析した全体傾向や総括コメント、前月レポートとの比較など、100 ページ以上の報告書を提出します。セキュリティ担当者が不在の会社でもセキュリティの問題に関する速やかな対応が可能です。レポートは SCS 評価制度をはじめとした各種ガイドラインのエビデンスとしても利用できます。

この『AI-SOC for SonicWall』はセキュアヴェイルの長年の SOC 基盤や体制を活用することにより以下のメリットを提供します。

1）低価格でのサービス提供（月額 9800 円～）
2）24 時間 365 日の SonicWall UTM ログ監視サービスの提供
3）インターネット利用によるログ収集・保管
4）AI ログ分析機能によるセキュリティアラート通知
5）月次ログ分析レポートの提供
6）ログ調査ポータルの提供（オプション）
7）長期ログ保管（オプション）

サービス提供対象は、TZ シリーズ（200/300）とし、エンドユーザーへの直接の販売に加え、ソリ

ューションパートナーの募集も開始いたします。



【レポートイメージ】



015_IPS(アクション別)	
期間	2026-10-31 00:00:00 - 2026-10-31 23:59:59
デバイス名	Kensho-Env-SW01
利用監視・収集項目	Kensho-Env-SW01
レポート作成条件	メッセージID '609' or '608'

【レポート概要】

本レポートは、SonicWALLによって検知されたIPSイベントを対象に、
アクション別の観点から検知状況を集計したものです。

どのような対応（検知・遮断等）がどの程度発生しているかを確認することで、
IPSがどのように動作しているか、その全体的な傾向を可視化します。

IPSの検知状況と制御方針のバランスを把握し、
IPSの検知や対応内容が適切に動作しているかを確認することを目的としています。

【ログ分析結果】

1. 状況サマリー

IPSイベントは合計1,533件です。内訳はIPS Blockが1,245件（約81.2%）、IPS Alertが288件（約18.8%）です。
集計上は、遮断アクションが検知アクションを上回っています。

2. 分析ポイント

IPS BlockはIPS Alertの約4.3倍です。IPSが検知したイベントの多くで遮断アクションが記録されています。

IPS Alertも288件発生していますが、この集計だけでは対象イベントの内容や通信が許可されたかどうかを判定できません。

3. 詳細分析

アクション別の件数は、IPS Blockが1,245件、IPS Alertが288件です。レポートには発生日時、検知シグネチャ、送信元・宛先IPアドレスが含まれていないため、イベントの集中状況や対象通信の特定はできません。

4. 推奨調査・対応

IPS Alertのイベント明細を抽出し、発生日時、検知シグネチャ、送信元・宛先、適用アクションを確認してください。通信が遮断されていない場合は、該当するシグネチャとポリシーの設定を照合し、許可が意図した動作かを判断してください。

5. まとめ

IPSイベントの約81.2%でIPS Blockが記録され、約18.8%でIPS Alertが記録されています。アクションの全体傾向は把握できますが、個々のイベントの脅威性や通信への影響は、この集計データだけでは判断できません。

【前回レポートとの比較】

前回のレポートデータがありません

	セキュリティアクション	ログ件数
1	IPS Block	1,245
2	IPS Alert	288
合計		1,533

株式会社セキュアヴェイル概要

2001 年設立。創業以来ネットワークセキュリティに特化して企業や組織の情報システムの運用をサポートする国内では数少ない IT セキュリティ専業企業。企業のシステムセキュリティを確保し、事業運営を安心して継続させるために「安全」で「役立つ」サービスを提供します。

創業期から 25 年以上提供し続ける統合セキュリティ運用サービス「NetStare」は SOC（Security Operation Center）と NOC（Network Operation Center）双方を提供する業界でも数少ない統合セキュリティ運用サービスです。クライアント企業のネットワーク機器を常時 1.1 万台以上監視し、1 日 25 億件の膨大なログを収集し、機器故障、通信障害、サイバー攻撃などを 24 時間 365 日体制でいち早く発見します。

※記載されている会社名および商品名は、各社の登録商標または商標です。
※本プレスリリースに関するお問い合わせは下記までお願いします。
株式会社セキュアヴェイル　カスタマーサポートセンター
TEL: 03-4405-6128　Email: contact@gr.secuavail.com

SonicWall
SonicWall（ソニックウォール）は、SonicWall 社（アメリカ）が提供している、企業等のネットワークをサイバー攻撃から守るための UTM（統合脅威管理）および次世代ファイアウォール（NGFW）の製品・ブランド名。日本の IT セキュリティ市場において、SonicWall は長年の実績を持つ外資系セキュリティベンダーの代表格の一つ。社員数数名の小規模オフィス（SOHO）から、100～150 名程度の中小企業までを幅広くカバーするラインナップを展開している。『TZ シリーズ』は、中堅・中小企業（SMB）や分散型企業の拠点向けに開発されたデスクトップ型の次世代ファイアウォール（UTM）。

UTM
複数の異なる以下のセキュリティ機能を 1 台のハードウェア（またはクラウド）に集約し、ネットワーク管理、つまり統合脅威管理（Unified Threat Management）を行う。
- ファイアウォール：外部からの不正なアクセスや通信を防御。
- IDS / IPS：ネットワークへの侵入や不審な攻撃を検知・遮断。
- アンチウイルス：通過するデータに含まれるウィルスやマルウェアを検知・除去。
- Web フィルタリング：業務に関係ないサイトや、危険性のある Web サイトへのアクセスを制限。
- アンチスパム：迷惑メールの侵入を防ぐ。

IDS（Intrusion Detection System）
ネットワーク内の不正な通信のデータ中身を検知して管理者へ通知する。

IPS（Intrusion Prevention System）
ネットワーク内の不正な通信の中身を検知し、自動で遮断・防御する。