

報道機関各位

令和 7 年 11 月 27 日

株式会社セキュアヴェイル（東証グロース 3042）

代表取締役社長 米今政臣

---

## FortiGate の SSL-VPN 廃止を受け、セキュアヴェイルが FortiGate のセキュリティ設定最適化サービスを期間限定で提供

---

IT セキュリティの専門企業、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、東証グロース：3042、以下セキュアヴェイル）は、フォーティネット社のファイアウォール製品である FortiGate シリーズのセキュリティ設定最適化サービスを 2026 年 1 月から 3 月までの期間限定で提供します。

当サービスはセキュリティ設定の診断・見直しはもちろん、SSL-VPN から IPsec-VPN への移行作業などにも対応し、セキュリティ運用に関連する最適化作業を丸ごと委託することができます。

昨今、企業のインターネット環境において FortiGate の SSL-VPN を経由した侵入被害が増加している背景から、フォーティネット社では FortiOS 7.6.3 以降で SSL-VPN トンネルモードを廃止することを発表、IPsec-VPN への切り替えを促しています。一部の機種ではすでに SSL-VPN 機能の無効化または制限が行われており、SSL-VPN トンネルモードの継続利用が可能な最後の系統とされる FortiOS 7.4 系は 2026 年 5 月頃にサポート終了が予定されているため、安全なリモートアクセス環境を維持するためには IPsec-VPN への計画的な移行が求められます。

さらに近年、企業間取引におけるセキュリティ要求は一層高まっており、経済産業省が推進する「サプライチェーン強化に向けたセキュリティ対策評価制度」など、ネットワーク機器の管理やパッチ適用を求める基準が整備されています。VPN 装置を含むネットワーク機器もこれらの基準の対象となり、VPN 装置における脆弱性管理や設定の適正さが求められます。

こうした状況を踏まえ、セキュアヴェイルでは FortiGate を利用する企業の適切な VPN セキュリティ対策を支援するため、特別価格で以下のサービスを提供します。

- ・ SSL-VPN から IPsec-VPN への切り替えサービス
- ・ ファイアウォール設定診断サービス
- ・ 最新版 FortiOS へのバージョンアップサービス

※上記サービスのすべてまたは一部の組み合わせを選択できます

提供期間は 2026 年 1 月から 3 月、FortiGate を利用するユーザー企業はもちろん、FortiGate 取り扱いベンダーに対してもサービスを提供します。

### 【関連記事】

ファイアウォール設定診断サービス概要

[https://www.secuavail.com/event/firewall\\_audit](https://www.secuavail.com/event/firewall_audit)

-----

## 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 専門企業。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 20 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 マーケティング Gr.

TEL : 03-6264-7180 Email: [marketing@secuavail.com](mailto:marketing@secuavail.com)

本プレスリリース内容以外の IR 関係窓口

株式会社セキュアヴェイル

大阪市北区東天満 1-1-19

アーバンエース東天満ビル

経営企画本部 担当 林

TEL : 06-6136-0026

---

## 【用語説明】

### ・ FortiGate

FortiGate は、アメリカの Fortinet (フォーティネット) 社が作っているセキュリティ対策用の機器 (ファイアウォール) で、“出荷台数”で世界の 50% 超のシェアを持っていると、Fortinet 自身が公表しており、インターネットと社内ネットワークのあいだに置くセキュリティゲート (ファイアウォール) があります。

また、FortiOS (フォーティオーエス) とは、FortiGate シリーズに搭載されている専用の OS (オペレーティングシステム) です。

### ・ VPN

VPN は「Virtual Private Network (仮想専用線)」の略で、インターネット上に仮想的なトンネルを構築し、データ通信中に起こりうる情報漏洩や侵入、改ざんなどのセキュリティリスクからデータを守るための技術。企業の拠点間接続や、自宅・外出先からの社内システムへの利用され、データの暗号化により、さらにセキュリティ強化をしている。

### VPN 利用例

- 1) リモートワーク: 自宅や外出、出張先から社内サーバーやシステムに安全にアクセスする。
- 2) 企業の拠点間接続: 複数拠点のネットワークを統合し、情報共有をスムーズにする。
- 3) 公共 Wi-Fi の利用: セキュリティが低い公共の Wi-Fi を利用する際も、安全に通信できる。
- 4) IP 電話: インターネット経由の VoIP 通話も、VPN で暗号化することで盗聴リスクを低減できる。

## ・SSL-VPN トンネルモード

VPN クライアントソフトを使い、外部から社内ネットワークへ安全に接続するための仕組み。Fortinet 社は FortiGate トンネルモードのアプリを廃止し、セキュリティ上、問題のある SSL-VPN から IPsec-VPN の切り替えを促進する。世界トップシェアを公言する Fortinet 社のファイアウォール FortiGate をリモートワーク等で利用していた SSL-VPN 利用ユーザーは対応が急がれる。

## ・SSL-VPN と IPsec-VPN について

	SSL-VPN	IPsec-VPN
主な用途	Web ブラウザを利用して特定のアプリケーションにアクセスするリモートアクセス用。容易なアクセス	物理的に離れた固定 IP アドレス間の複数の拠点間の接続。強力なセキュリティで完全なネットワークアクセス。複雑で詳細な設定が必要。
暗号化	データ（個々の通信内容）を暗号化	ネットワーク全体のトラフィック（拠点間の通信全体）を暗号化
クライアント要件	Web ブラウザがあれば接続可能（個人所有端末で利用可能）	専用ソフトウェアや専用機器が必要
ファイアウォール	通信ポートが HTTPS (443 番ポート) のため、通過しやすい	利用するポートが複数あり、ファイアウォールの設定変更が可能

## ・経済産業省が進める「サプライチェーン強靱化に向けたセキュリティ対策評価制度」のポイント

### 1. サプライチェーン全体でのサイバーリスクが高まっている

特に中小企業や下請企業のセキュリティ対策が不十分な場合、攻撃者に悪用され、元請企業を含むサプライチェーン全体に被害が波及するリスクがある。

### 2. 発注企業側からは、取引先（受注企業）のセキュリティ対策のレベルを客観的に把握しづらい

企業ごとに管理方法や基準が異なるため、対策状況が見えないことが大きな課題となっている。

### 3. そのため、企業のセキュリティ対策状況を“見える化”し、共通の評価基準で確認できる仕組みを作ることが目的

取引先の選定やリスク評価の判断材料として活用できる制度とすることが狙い。

制度の正式スタートは 2026 年度 を目標に検討が進められている。