



内部セグメンテーションファイアウォール(ISFW)で実現する「セキュアネットワーク」

外部からの脅威に対抗するだけでなく、内部ネットワークに潜む脅威からビジネスを守る内部セグメンテーションファイアウォール (ISFW) に着目する企業が増えている。半導体製造装置や精密測定機器の製造・販売でグローバルなビジネスを展開する株式会社 東京精密では、内部ネットワークのセキュリティ強化に向けてフォーティネットの次世代ファイアウォール「FortiGate 3200D」を導入し、サーバーセグメントを保護するISFWを構成。従来の「ネットワーク・セキュリティ」からセキュリティを重視した「セキュアネットワーク」への移行を進めている。

株式会社 東京精密

本 社 東京都八王子市石川町2968-2
 設 立 1949年3月
 資 本 金 104億6200万円
 売 上 高 777億9200万円 (連結)
 従業員数 1784名 (連結)
 事 業 所 八王子工場、土浦工場
 国内17営業所、海外拠点66カ所、
 国内グループ会社5社など
 (2017年3月31日現在)

半導体製造装置、精密測定機器を柱として、アジアを中心に欧米などグローバルな事業を展開。世界中の優れた技術・知恵・情報を融合して世界No.1の製品を創り出し、成長し続けることを目指している。
<http://www.accretech.jp/>



株式会社 東京精密
 業務会社
 情報システム室 IT戦略チーム
 チームリーダー 上級職
宇野澤 宏夫氏



株式会社 東京精密
 業務会社
 情報システム室 IT戦略チーム
 主任
宮野 寿幸氏



株式会社 トーセシステムズ
 開発部
 ITサービス チーム
 情報セキュリティスペシャリスト
戸塚 陽介氏

導入・構築のポイント

- (1) ネットワーク・セキュリティからセキュアネットワークへ
- (2) ISFWのコアに高性能のFortiGate 3200Dを配置
- (3) FortiAnalyzerで社内ネットワークを可視化

経営の最重要課題になる情報セキュリティ対策

東京精密は、透明性の高い経営システムの構築・運営に努め、持続的な成長と中長期的な企業価値の向上を目指すことをコーポレート・ガバナンスに掲げる。そして、事業の柱である半導体製造装置と精密計測機器の顧客には大手電機メーカーや自動車メーカーなど、セキュリティにセンシティブな企業が多いという。

東京精密 情報システム室 IT戦略チームチームリーダーの宇野澤宏夫氏は「お客様とのビジネスにおいて、信頼関係が重要です。これまでも情報の取り扱いには十分留意してきましたが、様々な情報がネットワークを介してやり取りされる現在、情報セキュリティ対策が経営の最重要課題になっています」と述べる。

東京精密では、社内にはコンプライアンス委員会やリスク管理委員会、情報セキュリティ委員会などを設け、コーポレート・ガバナンスとコンプライアンス、セキュリティの強化に取り組んできた。情報セキュリティについては、2004年に情報セキュリティ委員会を設置し、知的財産権取得・管理、営業機密管理、技術情報流出防止などに取り組む。そして、情報セキュリティ委員会の下に、IT関係のセキュリティ全般を企画推進するITセキュリティ部会、オフィス内のセキュリティ全般を担当するオフィスセキュリティ部会、セキュリティ教育及び監査を担う監査・教育部会を設け、活動してきた。

そして、ITセキュリティ部会の構成メンバーでもある情報システム室が中心となって社内の情報セキュリティ対策を推進。FortiMail

をはじめ、FortiSandbox、FortiAnalyzerを導入し、サイバー攻撃が疑われる不審なメールの挙動をチェックしたり、社内ネットワークの見える化やログの収集・分析を行ったりするなど、統合的な情報セキュリティ対策を段階的に進めてきた。

ネットワーク・セキュリティからセキュアネットワークへ

東京精密では本社・工場・国内営業拠点の通信は、インターネット接続やメールの送受信を含め、東京・八王子の本社を經由してやり取りされる。本社ネットワークについては、外部向けのファイアウォールのほか、L3コアシッチを配置してLANのトラフィックを制御してきた。

社内ネットワークの運用を担う東京精密 情報システム室 IT戦略チーム主任の宮野 寿幸氏は「これまでの内部ネットワークは安定的につながることを重視して構築・運用してきました。しかし、昨今はサイバー攻撃の脅威もあり、外部だけでなく、内部ネットワークのセキュリティ対策が重要になっています。そこでリプレースを契機にコアシッチに替え、内部セグメンテーションファイアウォールとしてFortiGateを導入したのです」。

宮野氏がこう話すように、これまでの内部ネットワークはコアシッチを配置してクライアントPCとサーバーなどをつなげてきた。そして、セキュリティを担保するため、ネットワークにセキュリティを付加した「ネットワーク・セキュリティ」を構成してきたと言える。

だが、サイバー攻撃が深刻化する中、内部ネットワークに潜む脅威から保護するセキュリティの仕組みが必要になる。ファイアウォールを配置して正しい通信のみ許可するといったセキュリティ主体のネットワーク「セキュアネットワーク」の構築がポイントになる。

例えば、データを暗号化して身代金を要求するランサムウェアの被害がニュースなどでも取り上げられているが、「重要データを取り扱うサーバーセグメントを保護するため、FortiGate 3200DによるISFWの導入に踏み切りました」(宇野澤氏)。

ISFWのコアに高性能の FortiGate 3200Dを配置

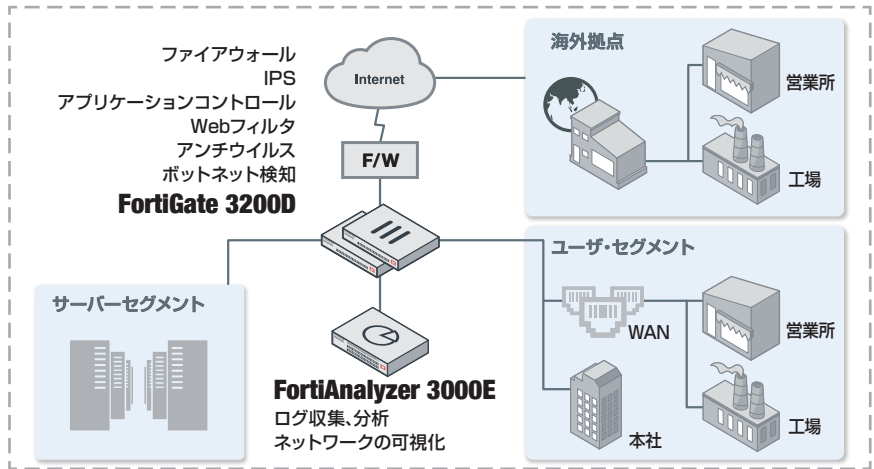
内部ネットワークのコアに配置するISFWには、高い信頼性とパフォーマンスが要求される。FortiGate 3200Dは高速処理を行う独自のSPU (Security Processing Unit) を搭載。優れたファイアウォールパフォーマンスを発揮するネットワークプロセッサ、暗号処理やコンテンツ検査を行うコンテンツプロセッサに加え、コアネットワークのセグメンテーションに要求される高速接続に対応。高密度の10GbEインタフェースを実装し、高度な「セキュアネットワーク」を実現する。

ハイエンドのFortiGate 3200Dを選定した理由について、宮野氏は「IT環境やセキュリティの要件もどんどん変化します。次のリプレースまで、長期的に使い続けられる性能と拡張性を評価しました」と述べる。そして、内部ネットワークのセキュリティ強化について、宇野澤氏は「マルウェアなどの脅威が広がるなか、複数のセキュリティ対策を組み合わせた多層防御の仕組みが必要です。その取り組みの一つが、FortiGateによるISFWの導入であり、多層的に対策を講じないと、巧妙化する脅威に対抗することは困難です」と強調する。

FortiGate 3200Dでサーバーセグメントのトラフィックを制御、可視化するほか、ファイアウォール、IDS、ウイルス対策、Webフィルタリング、アプリケーション制御などのセキュリティ機能を利用している。FortiGateなどの運用管理を担当するトーマス・システムズ ITサービスチームの戸塚陽介氏は「FortiGateは内部ネットワークのコアに配置しているため、脅威の検知を重視しています」と説明する。FortiGateで通信をブロックするとネットワークの利用を止めてしまう恐れがあるからだ。

FortiGate導入後、ある従業員からネットワークが遅いので調べてほしいといった問い合わせが情報システム室に寄せられた。戸塚氏がそのIPアドレスを調べたところ、業務の特性上、一時的に大量の帯域を消費する作業があり、ネットワークが遅くなることが判明したという。「FortiGateはポートやプロトコル、アプリケーション別などでトラフィックの状況を把握することができ、セキュリティの強化だけでなく、ネットワークの安定稼働にも効果的です」(戸塚氏)。

東京精密様セキュリティ強化：FortiGate + FortiAnalyzer



FortiAnalyzerで社内ネットワークを可視化

東京精密では、FortiGateとともに、ログの収集・分析のためFortiAnalyzerを導入している。従来、ログ用に複数台のサーバーを設置していたが、局所的な情報しか得られず、ネットワーク全体で何が起きているのか把握できなかったという。「内部統制の観点からもセキュリティ機器のログの保管が必要です。さらにネットワーク上で何が起きているのか分からなければ対応のしようもありません。そこで、FortiAnalyzerを活用してネットワークの見える化とログの収集・分析に取り組み始めたのです」と宮野氏は述べる。

FortiAnalyzerで収集したログの分析結果をITセキュリティ部会で報告している。例えば、ゲートウェイをすり抜けてマルウェアが侵入した場合、以前はいつ、どこで侵入したのかその経緯を詳細に把握することは困難だったが、FortiAnalyzerが収集したログを分析することにより、原因の特定が可能になり、必要なセキュリティ対策を講じることができるという。

最終的には、情報システム室では自動車の交通量を監視し、安全に走行を支援する高速道路の管制センターのような存在を目指しているという。全社のネットワークのトラフィックを可視化し、適切なセキュリティ対策を講じることにより、事業継続性を確保する狙いがある。

さらに東京精密では、フォーティネット製品に加え、エキスパートエンジニアによる付加価値サービス「FortiCare Advanced Service」を導入している。これは、フォーティネットの専任SEとのメールや電話による日々のタイムリーな対応、定期的なミーティングをはじめ、障害時の一次切り分け、フォーティネット製品導入の技術支援、分析サービスなどを提供する。「システムインテグレータのほかにも、フォーティネットのSEと直接コミュニケーションを取ることで、今後、導入する機器の評価・検証や技術支援などを期待しています」と宮野氏はFortiCare Advanced Service導入の理由を話す。

そして、宇野澤氏は「セキュリティにかかわる情報提供や、機器の効率的な運用管理方法を含め、フォーティネットのサポートに期待しています」と述べる。フォーティネットでは、グローバルなビジネス展開を進める東京精密のセキュリティ強化とITガバナンスの推進に向け、さらなる提案を続けていく考えだ。



FORTINET

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ