FORTINET

導入事例

NICHIDAI

新たな「セキュアネットワーク」を実現!
重要情報が保存されるサーバーセグメントをFortiGateで堅牢に保護

自動車部品用精密鍛造金型などを生産する株式会社ニチダイでは、事業継続に欠かせないシステムの安定稼働に向け情報セキュリティ対策を強化。外部からの攻撃を防御する次世代ファイアウォール（NGFW）「FortiGate 300D」に加え、内部のサーバーセグメントを保護するため「FortiGate 300D」を追加導入した。同一機種にそろえることにより、外部用ファイアウォールの障害時に内部用ファイアウォールを代替機として利用でき、統一的な運用管理が可能だ。また、「FortiAnalyzer」を活用しサーバーセグメントに対するトラフィックを可視化し、現状の把握・整理を効率的に行い、内部ファイアウォールのセキュリティポリシー設定に役立てたことでセキュアな社内ネットワークを実現した。

導入・構築のポイント

(1)事業継続の観点から内部ネットワークのセキュリティ対策を強化

(2)既存NGFWの代替機として利用できるよう外部用と内部用をFortiGate 300Dに統一

(3)FortiAnalyzerで通信状況を可視化してFortiGateのポリシーを設定

株式会社ニチダイ

本　　社 京都府京田辺市薪北町田13
創　　業 1959年5月
設　　立 1967年5月
資 本 金 14億2992万円
従業員数 367名（単独）664名（連結）
（2016年9月30日現在）

顧客満足度・株主満足度・社員満足度のすべてを最大限に実現し、永続的に向上させていくことにより、新たな価値を創造し、社会に貢献できる企業を目指している。http://www.nichidai.jp/

株式会社ニチダイ
システム部
次長
宮原 洋二氏

株式会社ニチダイ
システム部システム課
課長
齊藤 文昭氏

株式会社ニチダイ
システム部システム課
係長
友田 祐樹氏

各種システムを一括管理し設計開発などの情報保護に注力

ニチダイは「他社ではできない製品と、他社の追随を許さない高い技術力」を追求するオンリーワン企業を目指すとともに、3E（エクセレント・エキサイティング・エクスパンド）カンパニーの実現に向け、3つの事業を展開している。「ネットシェイプ事業」は、主に自動車部品生産に利用される精密鍛造金型の設計・製造を担う金型部門と、部品の量産を担う精密鍛造部門で構成。「2部門のトータルエンジニアリング力を生かして国内外の自動車部品メーカーのニーズに応じたサービスの提案・提供を行っています」とニチダイのシステム部次長の宮原洋二氏は述べる。

「アッセンブリ事業」はディーゼルエンジン車、ガソリンエンジン車用ターボチャージャー部品を国内及びタイ工場で組み立て顧客企業の現地調達ニーズに対応する。そして「フィルタ事業」は、独自の拡散接合技術を使って産業用フィルタを製造。石油、化学、ガス、繊維、食品、航空宇宙産業など様々な分野で利用されている。

同社は自動車部品用金型の設計開発など多数の技術情報を保有しており、従来から情報保護に注力。例えば、IT統制として定期的なリスク評価をはじめ、セキュリティインシデントを発見･予防する仕組みの整備、ネットワークを介した情報への不正アクセスの監視、アクセス記録の保存などを行ってきた。

株式会社ニチダイ
システム部システム課
磯野 拓真氏

株式会社ニチダイ
システム部システム課
桐原 里加氏

「基幹系システムや技術系システムをはじめ、業務で使用するあらゆるシステムを京都府宇治田原工場内で一括管理しています。本社や営業所は通信事業者の閉域網を介して宇治田原工場のサーバーにアクセスする仕組みです」とシステム課課長の齊藤文昭氏は説明する。

ニチダイでは、他拠点から宇治田原工場に集約されるインターネット通信に対するセキュリティ対策として外部用ファイアウォールを2016年1月に更新。フォーティネットのNGFW「FortiGate 300D」を導入し、ファイアウォール、IPS、アンチスパム、Webフィルタリングなどのセキュリティ機能を利用している。このFortiGateでさらにWebプロキシの機能も有効化することで、保守期限の迫った既存のプロキシサーバー機能の集約も検討しているという。

外部用と同一機種のFortiGateを内部ネットワーク用に導入

こうした外部向けセキュリティ対策の一方、企業内部の機密情報を狙ったサイバー攻撃の脅威は後を絶たない。システム課係長の友田祐樹氏は「今年に入ってから、ランサムウェアの被害に遭い、サーバー内の情報が暗号化されて使えなくなったというニュースを多く見かけるようになりました。サイバー攻撃の手口も巧妙化しており、内部ネットワークのサーバーを保護するセキュリティ対策が急務になっていました」。

そして、齊藤氏は「当社はまだセキュリティインシデントの実害がないとはいえ、システムは業務遂行の生命線です。業務停止を回避し、事業継続の観点からも内部ネットワークのセキュリティ強化が経営課題となっていたのです」と話す。

システム部では内部用ファイアウォール導入に向けて検討を開始。数社の製品を検討した結果、外部用と同じ「FortiGate 300D」の導入を決定した。その決め手の

一つが「使いやすさです。ポリシー管理などもGUIで分かりやすく行えます。何のポリシーなのか日本語でコメントを書けるので、システム課のだれが見ても内容を理解できます」（友田氏）。

また、外部用に導入したFortiGateはシングル構成だったため、内部用に同じ機種を採用することで万一の障害時に代替する狙いもある。ファイアウォールに障害が起きると外部に公開しているEDIシステムやメールシステムも使えず、業務に支障を来すことになるため冗長化が課題になっていたという。

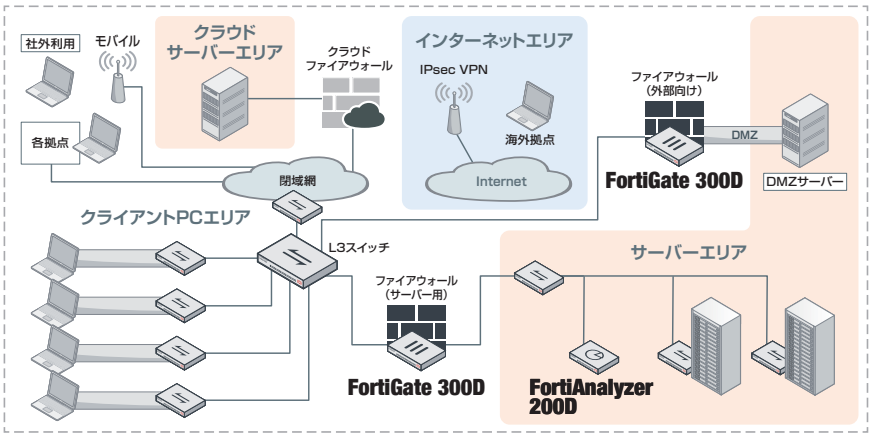
システムを設置している宇治田原工場は京都市内から離れた場所にあるためシステム事業者が代替機を持って交換するにも数時間はかかる。「外部用ファイアウォールをアクティブ−スタンバイ構成で冗長化するよりも、1台は内部用ファイアウォールとして使い、外部用の障害時に代替機として利用すれば一石二鳥です」（友田氏）。内部用FortiGate導入時に外部用への切り替えをテストしたところ、コンフィグの投入や配線ケーブルの差し替えなどわずか10分ほどで切り替えられたという。

FortiAnalyzerで通信状況を可視化しFortiGateにポリシーを適用

内部用もファイアウォールのほか、IPS、アンチウイルス、アプリケーション制御などの機能を使用し、サーバーセグメントへのセキュリティを保護している。そして、内部ファイアウォールはサーバーから情報を盗み取ったり、ウイルス／マルウエアを拡散したりする脅威から内部ネットワークを保護する役割がある。

ニチダイではActive Directoryを使ってユーザーの部署や権限に応じたアクセス制御を実施してきたが、内部のクライアント／サーバー間の実際の通信状況を詳細に把握することは困難だった。内部ネットワークのセキュリティを強化するにはユーザー権限に基づくセキュリティポリシーを精査し過不足のない形で適用する必要がある。

そこで、FortiAnalyzerを活用しクライアント／サーバー間の通信状況を可視化。「当初は制限をかけずにどのクライアントからどのサーバーにアクセスしているのかモニタリングし、FortiAnalyzerを使ってトラフィックデータを蓄積しました。そして、サーバーへのより細かなアクセス可否について内部用FortiGateのポリシーを設定しています」と友田氏は説明する。



システム部では基幹業務システムや技術系システムなど数十台に及ぶサーバーを運用管理しているが、クライアントからアクセスする必要がないサーバーやポートへの通信を拒否するようにポリシーを設定するなど、モニタリング開始から二週間で内部用FortiGateの稼働を開始できたという。

トラフィックデータの抽出作業などを担当したシステム課の磯野拓真氏は「サーバー間の通信が見える化され、内部ネットワークの状況を容易に把握できるようになりました」とFortiGateとFortiAnalyzerの組み合わせによる運用業務の効率化を導入効果に挙げる。複数のネットワーク機器の大量のsyslogを取得し分析するよりも、FortiAnalyzerに集約され、データとして整理された情報をFortiViewで視覚的に判断し、詳細分析はcsvでエクスポートして実施した方が容易でコストもかからないのでは、と評価は高い。

サーバートラフィックに影響なく高いパフォーマンスを発揮

ニチダイでは内部用FortiGateをサーバーセグメントに配置し、技術系サーバーは大容量データが流れることから、当初は負荷が懸念されたという。だが、「FortiGate 300Dはコンテンツとネットワークのプロセッサを分けているためか、サーバーへのトラフィックの影響はほとんどありません」。友田氏がこう話すように、FortiGateは独自のSPU（セキュリティプロセッシングユニット）を搭載。コンテンツプロセッサとネットワークプロセッサがそれぞれ独立して動作することにより、創業当初から掲げている「セキュリティ機器がボトルネックになってはならない」を実現、よりその効果が体感できる内部（LAN）ネットワークで実力を発揮させた。

メールを悪用した標的型攻撃などの脅威が広がる中、ニチダイでは日ごろから怪しいメールは開かないといった従業員のセキュリティ教育を徹底。従業員の意識も高く「不審なメールが届いた場合、社員の皆さんはシステム部に対応を問い合わせてきます」とシステム課の桐原里加氏は話す。スパムメール対策としてFortiGateのアンチスパム機能とスパム対策専用機を組み合わせて検知しているが、さらに高精度の検知・防御が行えるようサンドボックスの導入も今後の検討課題になるという。

FortiGateとFortiAnalyzerの統合運用性を体感し、“フォーティネット・セキュリティ・ファブリック”を自社のネットワークで実践するニチダイは、セキュリティネットワークの強化に向け、フォーティネットにさらなる期待を寄せる。「セキュリティに関する様々な情報を集め、適切に対策を講じていく必要があります。最新情報の提供や製品・サービスの提案をお願いしたいですね」と宮原氏。外部・内部のセキュリティを強化し、独自の技術と製品を世界のユーザーに提供するニチダイの取り組みが注目される。

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