2020 年 9 月 2 日
フォーティネットジャパン株式会社

# フォーティネットの FortiGate、攻めの IIoT を推進するアズビルのネットワークインフラで採用

## 複数のセキュリティ機能と Web プロキシを 1 台のアプライアンスに統合した効率化と SSL インスペクション性能の高さが評価される

幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）サイバーセキュリティソリューションの世界的リーダーであるフォーティネット（Fortinet®）は本日、アズビル株式会社（以下、アズビル）がフォーティネットのハイエンド次世代ファイアウォール FortiGate 2000E を導入し、IT 環境の変化に柔軟に対応し、運用負担を軽減するネットワークインフラを構築したことを発表しました。

計測・制御の技術を追求し、プロセスオートメーションやファクトリーオートメーション、ビルディングオートメーションシステムを通じてものづくりやビル、社会インフラを支えてきたアズビルは、近年、クラウドや AI をはじめとする先端的な IT 技術を駆使し、異常の予兆を検知するなどスマートで自律的な IIoT（インダストリアル IoT）ソリューション提供に取り組んでいます。アズビルでは、こうした「攻め」の施策を安心して推進するための「守り」にも力を入れており、ファイアウォール（Web フィルタリング）や IPS、Web プロキシといった複数のセキュリティ機器を導入し、対策に努めてきました。

**クラウド浸透、IT 環境の変化にともなって浮上した新たな課題**

攻めと守りを両立させるアズビルでは、長年運用してきたオンプレミス環境を活かしながら新しいテクノロジーも積極的に採用し、「クラウドファースト」の考え方を取り入れて IT 環境を整備してきましたが、Web ベースのサービス利用が増えたことにより新たな課題が浮上していました。特に最近のリッチな Web サービスによってセッション数やトラフィック量が増加し、プロキシサーバのパフォーマンスに影響を与え始め、ユーザーから苦情が出るレベルではなくともインフラを監視する側ではタイムアウトが発生する問題を認識しており、NAT 処理の設定を手作業で最適化して対応することもありました。 さらに、SSL 通信の増加に伴い、Web フィルタリングでコントロールできる範囲が狭くなってきたことで、SSL インスペクションの実施も課題となっていました。

**FortiGate でセキュリティ機能と Web プロキシを 1 台に統合**

ファイアウォールの更改に合わせてアズビルが検討した複数の提案のうち、高い評価を受けて採用されたのが FortiGate 2000E でした。ファイアウォールや SSL インスペクションの性能、さらに将来的に IPS やアプリケーションコントロールといったさまざまなセキュリティ機能を拡張し強化できることが決め手となりました。FortiGate であれば 1 台で次世代ファイアウォールと Web プロキシサーバの機能を実現するシンプルな構成で、導入に要する時間と費用を抑えて運用の負担も軽くできるため、コストパフォーマンスの高さも評価されました。

アズビルは約 20 年近く同一ベンダーのファイアウォール製品を運用してきました。そのため、アクセスコントロールポリシーは継ぎ足しで肥大化しており、それらのルールをきちんと FortiGate に移行できるかが導入時の懸念となっていました。FortiGate の導入に伴い、ポリシーの見直しや不要なポリシーの廃止といった決断をフォーティネットおよびパートナー企業の支援を得て行うことで、スムーズに移行することができました。

**Active Directory 認証の導入でセキュリティ強化**
FortiGate 2000E の導入と同時に、アズビルは Active Directory 認証を導入しセキュリティレベルを高めました。これまでは内部セグメントからは誰でもインターネットにアクセス可能でしたが、ドメイン認証を経てユーザー情報をベースにしたアクセスコントロールを実現しました。Active Directory 認証により監査の効率化という利点ももたらされました。以前の監査では、プロキシサーバのログに記録された IP アドレスを元に、DHCP サーバのログと付き合わせて確認する必要がありましたが、FortiGate の採用でその作業を大幅に簡素化することができました。

**複数の機器を 1 台のアプライアンスに集約することで、運用、メンテナンスの負荷低減**
複数台あったセキュリティ機器を FortiGate に集約したことによる運用やメンテナンスの負荷低減というメリットも出ています。以前の運用ではセキュリティ機器の OS アップデートなどは外部ベンダーに依頼していたため、見積もりを取って作業日をスケジュールするという手間と時間がかかっていました。今では社内リソースで FortiGate の GUI から簡単にできるようになったため、作業の効率化と費用軽減の効果がありました。

アズビル株式会社 業務システム部 インフラ・セキュリティグループ グループマネージャー 田熊 賢一氏は次のように述べています。「ガスや電力、スマートビルなどさまざまな業界でセキュリティガイドラインの策定が進んでおり、セキュリティの確保が重要視されてきています。お客様が安心して利用できる商品を提供するために、開発プロセスや出荷後の運用管理などあらゆる分野において、セキュリティを確保するための取り組みを進めています。FortiGate は、従来型のインフラを確実に保護しつつ、クラウドをはじめとする先端テクノロジーを活用するためのハイブリッドクラウドへの移行後も保護機能が提供されるので安心しています。今後は、各拠点からの接続をアプリケーションに応じて動的に制御するポリシールーティング、いわゆる SD-WAN の検討も視野に入れて、さらに柔軟で強固な IT 環境を整えていきます」

フォーティネットジャパン株式会社 社長執行役員 久保田 則夫は次のように述べています。「高い技術力でインダストリアル IoT 分野を牽引するアズビル様に FortiGate をご採用いただいたことを非常に嬉しく思います。ネットワークとセキュリティの機能を統合したフォーティネットの FortiGate であれば、既存のインフラを強固に守りつつ、セキュア SD-WAN や業務用システムを守る OT セキュリティでもいち早く活用することが可能です。アズビル様が攻めと守りを両立し、事業のさらなる成長に少しでもお役に立てるよう、今後もお手伝いさせていただく所存です」

**関連リンク**
導入事例：アズビル株式会社
FortiGate: 次世代ファイアウォール (NGFW)

FortiGate セキュア SD-WAN

**フォーティネットについて (www.fortinet.com)**

フォーティネット（NASDAQ: FTNT）は、世界中の大手企業、サービスプロバイダ、そして政府機関を守っています。フォーティネットは、拡大するアタックサーフェス（攻撃対象領域）に対するシームレスな保護とインテリジェンスを提供し、外部との明確な境界が消滅したネットワークでの、増え続けるパフォーマンスの条件に応じるパワーで、現在もまた将来も、お客様に貢献します。ネットワーク上でも、アプリケーションやクラウド、またはモバイル環境であっても、妥協することなく、極めて重大なセキュリティ上の問題に対応するセキュリティを提供できるのはフォーティネットのセキュリティ ファブリックのアーキテクチャだけです。フォーティネットは世界で最も多くのセキュリティアプライアンスを出荷し、世界 465,000 以上のお客様がビジネスを守るためにフォーティネット に信頼を寄せています。フォーティネットのネットワークセキュリティエキスパート(NSE)インスティチュートは、テクノロジーカンパニーとしても、ラーニングカンパニーとしても業界で最も大きく広範なサイバーセキュリティのトレーニングプログラムを有しています。フォーティネットジャパンについては、www.fortinet.com/jp をご覧ください。

Copyright© 2020 Fortinet, Inc. All rights reserved. 「®」および「™」マークはいずれも、Fortinet, Inc.とその子会社および関連会社の米国における登録商標および未登録商標であることを示します。フォーティネットの商標には、Fortinet、FortiGate、FortiGuard、FortiCare、FortiManager、FortiAnalyzer、FortiOS、FortiADC、FortiAP、FortiAppMonitor、FortiASIC、FortiAuthenticator、FortiBridge、FortiCache、FortiCamera、FortiCASB、FortiClient、FortiCloud、FortiConnect、FortiController、FortiConverter、FortiDB、FortiDDoS、FortiExplorer、FortiExtender、FortiFone、FortiCarrier、FortiHypervisor、FortiIsolator、FortiMail、FortiMonitor、FortiNAC、FortiPlanner、FortiPortal、FortiPresence、FortiProxy、FortiRecorder、FortiSandbox、FortiSIEM、FortiSwitch、FortiTester、FortiToken、FortiVoice、FortiWAN、FortiWeb、FortiWiFi、FortiWLC、FortiWLCOS、FortiWLM などが含まれますが、これらに限定されるものではありません。その他の製品名およびサービス名等は、各社の商標である場合があります。フォーティネットは、本プレスリリース内の第三者に帰する声明、認可またはテストについては、検証を行っておらず、また、このような第三者に帰する声明を承認するものではありません。本プレスリリースは、保証または債務保証、または契約として一切拘束を受けるものではなく、記載された製品仕様または製品性能は、ある特定の環境や条件のもとで計測されていることがあります。また、本プレスリリースには、将来の見通しに関して不確実性および仮説を伴う記述が含まれている場合がありますが、本不確実性が現実になったり、あるいは本仮説が正しくないことが判明したりする場合、明文的あるいは暗黙的に記述された内容と異なる結果が生じることがあります。これには、サイバー犯罪活動の動向予測に関する記述などが含まれますが、これに限定されるものではありません。このような動向は予測することが困難であり、また、このような動向に関する公開予測や期待事項は結果として正しくないことがあります。フォーティネットは、このような将来見通しを改正する義務を一切負うものではなく、また改正を発行することもありません。