金沢大学
KANAZAWA UNIVERSITY

次世代ファイアウォールからメールセキュリティ、サンドボックスまでフォーティネット製品を連携しキャンパスネットワークのセキュリティの統合管理と抜本的強化

大学・研究機関を狙った標的型攻撃などの脅威が増すなか、金沢大学ではキャンパスネットワークの更新に合わせてセキュリティ対策を強化。フォーティネットの「FortiGate」をはじめ、「FortiSandbox」、「FortiMail」などを導入。キャンパスのセキュリティ対策をフォーティネット製品に統一し、各製品を連携することにより、学外からの攻撃のみならず、学内から学外への脅威の拡散をブロックするほか、統一的なオペレーションによる運用管理の効率化を実現している。

導入・構築のポイント

（1）包括的にセキュリティ機能をFortiGateで統合

（2）ハイエンド機種FortiGate 3700Dによる数年後の利用環境を意識した導入

（3）FortiGate、FortiMail、FortiSandboxを同一ネットワーク上で連携させることで、最新の脅威への対応と運用管理工数の削減を同時に実現

ハードとソフトの両面からセキュリティの強化を推進

金沢大学は2014年度にスーパーグローバル大学創成支援事業「徹底した国際化による、グローバル社会をけん引する人材育成と金沢大学ブランドの確立」が採択され、大学改革と教育の国際化を推進している。そして、金沢大学が育成する人材像を具体的に示した「金沢大学グローバルスタンダード」を設定。知識基盤社会における中核的リーダーとして求められる能力・体力・人間力を明示し、それに準拠したカリキュラムを導入・実践している。

また、国際社会に積極的に貢献できるよう、英語によるコミュニケーション力の向上を図るほか、語学力と国際感覚を兼ね備えたグローバル人材を育成するため、日本人学生の留学支援や海外から留学生の受け入れを広げている。

さらに、高校生に最先端科学と最新科学技術を学ぶ機会を提供するグローバルサイエンスキャンパスのプログラムを実施。「高校生に大学の提供する授業や実験に参加させており、学生・教職員と同様に大学のネットワークにアクセスできる環境を整えています。様々なユーザーが安全に学内ネットワークを利用できるよう情報セキュリティに注力しています」と金沢大学総合メディア基盤センター長の森本章治氏は述べる。

大学・研究機関を狙ったサイバー攻撃が増大するなか、金沢大学では政府の指針に合わせてハードとソフトの両面からセキュリティ対策の強化に取り組んできた。ソフト面では「総合メディア基盤センターを中心にCSIRTのようなインシデント対応組織づくりを行うほか、2017年度中にISMS認証を取得する準備を進めています」と教育研究システム係長の山上尚幸氏は説明する。

キャンパスネットワークの更新に合わせてセキュリティ対策を抜本的に強化

ハード面の取り組みでは、キャンパスネットワーク（KAINS：Kanazawa University Academic Integrated Network System）の更新に合わせ、学術情報ネットワーク（SINET）や学内の各部局に接続するセキュリティ機器を整備してきた。

KAINSは学生・教職員を含め、約15,000人のユーザーにサービスを提供するための重要なインフラである。これらには学内有線LANはもちろんのこと、全キャンパスで展開するWi-Fiアクセスや、シングルサインオンによる学内ポータルをはじめ、時間割管理・履修登録・シラバス・電子教材などの

金沢大学 角間キャンパス

金沢大学

所在地　石川県金沢市角間町

1949年、新制大学として発足。源流は現在の金沢大学（医学類）となる種痘所を1862（文久2）年、加賀藩が設置。2008年、8学部を3学域（人間社会学域、理工学域、医薬保健学域）、16学類に改組して新たなスタートを切り、2012年に創基150年を迎えた。

「地域と世界に開かれた教育重視の研究大学」を大学憲章に掲げ、「東アジアの知の拠点」を目指し、グローバル社会で活躍できる人材の育成に取り組む。

https://www.kanazawa-u.ac.jp/

学習支援、電子職員録、教材データベース、履修者管理、教育・業務支援システムなどの様々なサービスが含まれる。そして、学生・教職員が安心してネットワークとサービスを利用できるようセキュリティ対策の整備に取り組んできた。2011年に更新したKAINS11以前のネットワークは、外部のWebサーバーとの通信にプロキシサーバーを経由する構成となっており、「プロキシサーバーでダウンロードファイルのウイルスをチェックしていました。以前の基幹ネットワークの帯域は1Gbpsでしたが、実効速度ではプロキシサーバーが大きなボトルネックになっていたのです」と理工研究域技術専門職員の浜貴幸氏は当時の状況を説明する。また、対外接続のためのファイアウォールは全学用と部局用に複数台あり、コストと運用の両面で改善が求められていたという。

KAINS11ではFortiGate 1240Bを導入し、ファイアウォールや不正侵入検知／防御、アンチウイルス、アプリケーション制御などの各種セキュリティ機能を利用してきた。例えば、アプリケーション制御機能を用いてP2Pファイル共有サービスなど、学内では不要と判断されるアプリケーションを制限してきた経緯がある。

将来の脅威への対応まで考慮しての高い性能と機能を備えた次世代ファイアウォール（NGFW）

KAINS11に更新した2011年から5年の間に大学を取り巻くセキュリティの脅威も大きく変化している。特定の組織を狙った標的型攻撃などの被害も深刻化。「標的型攻撃の被害に遭う大学・研究機関などの事例も多数報告されています。そこで、2016年に更新したKAINS16ではシステムの仮想基盤についてもセキュリティを強化するなど、サイバー攻撃の被害抑制を最優先課題として様々な施策に取り組んでいます」と森本氏は話す。

そして、KAINS16では、FortiGateについても更新している。その要件は脅威の変化に対応できる十分なパフォーマンスと機能を備えていることだ。予算の都合上、新たに導入するセキュリティ機器は最低でも5年間は使い続ける必要がある。前回更新のKAINS11からKAINS16までの5年間を見てもサイバー攻撃の手口は巧妙化しており、次期更新までの今後5年間の脅威を予測することは困難である。そのため、NGFWで利用する機能は脅威の変化に応じて追加していけることが機種選定の前提となる。

FortiGate 1240Bの導入時にも十分なサイジングを行ったが、大学を取り巻く脅威の拡大とともにFortiGateが備える様々なセキュリティ機能を追加してきた経緯がある。その結果、「ハードウェアのリソースに限界があり、パフォーマンスが課題になっていました。そこで、KAINS16ではより高いパフォーマンスを備えるアプライアンスを選定しています」と浜氏は説明する。

そして、各メーカーのNGFWを比較・検討した結果、「FortiGate 3700D」を採用した。総合メディア基盤センターでは技術職員の人数が限られていることもあり、様々なセキュリティ機能が1台のハードウェアに包括的に集約され、脅威の変化に応じてファームウェアのバージョンアップにより機能を追加・拡張できること、GUIで操作しやすいこと、限られた予算の中で可能な限りパフォーマンスの高い上位機種を導入するといった方針の下で選定した。

最新のFortiOSと専用のSPU(Security Processing Unit)を搭載したFortiGate 3700Dにより、パフォーマンスを低下させることなく、今後のネットワークセキュリティに求められる高い可用性と拡張性が確保できると判断。「FortiGate 3700Dはセキュリティ機能、パフォーマンス、コストのいずれも十分に本学の要件を満たすものでした」と山上氏は述べる。

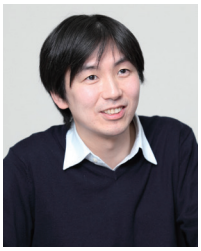
FortiGate、FortiMail、FortiSandboxの自動連携により巧妙化する脅威へも対応

金沢大学ではFortiGate 3700Dのほかに、「FortiSandbox 3000D」、「FortiMail-VM」、「FortiAnalyzer 3000E」を導入している。FortiSandboxは、大学や研究機関などへの標的型攻撃が深刻化するなか、導入が急務となっていた。だが、予算の制約もあり、導入・運用コストは可能な限り抑える必要がある。FortiSandboxはFortiGate及びFortiMailと自動連携することにより、運用管理工数を削減できるので予算内での導入が可能になる。

浜氏は「一般的に脅威の検知と解析を主眼にするサンドボックス製品が多いのに対し、FortiSandboxは検知と防御、つまり脅威を食い止めることを主眼にしています。機能もシンプルで扱いやすく、他のサンドボックス製品とは一線を画しています」と評価する。

また、FortiMailは第三者機関で実証された高精度のウイルス対策とスパム対

金沢大学
電子情報学系 教授
総合メディア基盤センター長
森本 章治氏



金沢大学
理工研究域
（総合メディア基盤センター）
技術専門職員
浜 貴幸氏

金沢大学
情報化推進室
教育研究システム係 係長
（総合メディア基盤センター）
山上 尚幸氏

金沢大学
人間社会系事務部
（総合メディア基盤センター）
主任技術職員
松能 誠仁氏

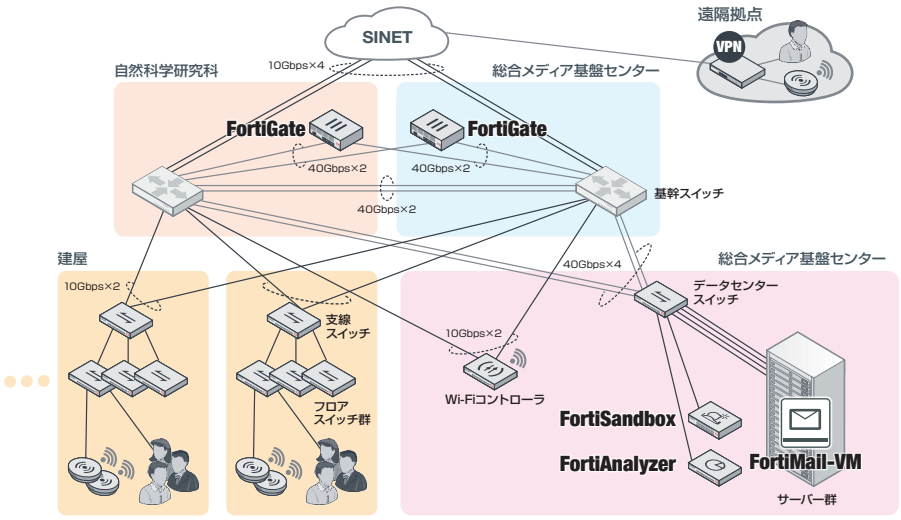
策のスキャンを入口・出口の双方向で行い、メールシステムを防御する。ユーザー数無制限のライセンスで提供し、「予算も限られる中で初期導入費用だけで済み、利用者の多い大学にとってライセンスフリーはありがたいですね」と人間社会系事務部主任技術職員の松能誠仁氏は話す。

そして、各種セキュリティ機器をフォーティネット製品に統一し、連携させることでシンプルなネットワークセキュリティ構成が可能になり、効果的かつ効率的な脅威防御が可能になる。FortiGateやFortiMailを通過するファイルの中に不審なものがあればFortiSandboxに送り、挙動を分析。そして、不審なコードを検出した場合、マルウエア対策用のシグネチャーを作成、脅威データベースを更新してFortiGateやFortiMailに反映し、脅威をブロックする仕組みだ。

標的型攻撃など日々、進化するサイバー攻撃の脅威の検出と防御はフォーティネットのセキュリティ研究部門である「FortiGuard Labs」が担う。世界の脅威の動向を絶えずモニタリングし、マルウエアやボットネットの監視、マルウエアのリバースエンジニアリング、シグネチャーの作成、ゼロディ攻撃の分析など広範な分野をカバーする。

世界中で稼働しているFortiGateは、FortiGuard Labsにとって脅威情報を得るためのセンサーの一つとなる。FortiGateからの脅威情報に基づいてシグネチャーを作成し、24時間365日体制でタイムリーにセキュリティ対策をアップデートすることにより、常に最新の脅威からユーザーを保護する。また、FortiGuardインテリジェンスに基づくフォーティネットのネットワークセキュリティプラットフォーム（FortiOS）は世界有数の第三者機関やユーザーによって検証されているため使う側として安心して利用することができる。

統合メディア基盤センターに設置されたFortiGate 3700D、FortiSandbox 3000D、FortiAnalyzer 3000E



セキュリティ機能の包括的統合とVDOMの活用で運用を効率化

KAINSは金沢大学の教育・研究・業務全般にわたる広範なサービスを支える重要なインフラとなり、「万一、ネットワークが何らかの原因で停止するような事態になれば学内の教育・研究や業務に大きな影響が及ぶことになりかねません。そこで、KAINS16ではネットワークの信頼性、可用性を高めるための様々な工夫をしています」と森本氏は語る。

その工夫の一つが、ネットワークの冗長化と広帯域化、機能の集約を図っていることだ。40Gbpsのインタフェースを備えるFortiGateと基幹スイッチを1組にして、角間キャンパス中地区にある総合メディア基盤センターと南地区にある自然科学研究科の建屋にそれぞれ配置して冗長化と負荷分散を実施。万一、片側が障害を起こして停止した場合にも、もう片側で稼働を継続することにより、学生・教職員に安定したサービス提供を可能にしている。

FortiGateと基幹スイッチは40Gbpsのリンクアグリゲーションにより学内のネットワークと学外のSINETを接続し、広帯域のキャンパスネットワークを構成する。そして、セキュリティ機能はFortiGateに集約。ファイアウォール、不正侵入検知／防御、DoS検知／防御、アンチウイルス、Webフィルタリング、アプリケーション制御、キャプティブポータル、VPNなどの各種セキュリティ機能を活用している。

また、複数の仮想NGFWとしてFortiGateを利用できるVDOM（仮想ドメイン）を前回のFortiGate 1240Bの導入時から活用。学内のDMZや無線LAN、統合認証ネットワークなどのサービスに応じてVDOMを割り当て、DNSサーバー、DHCPサーバー、NAT64、DNS64などのネットワーク機能をFortiGateで実施するほか、ユーザーのサービス利用時にFortiGateを経由するようにポリシーを設定してきた。

今回のFortiGate 3700Dでもフルに VDOMを活用している。松能氏は「これらのほか、附属小・中・高校にも専用のVDOMを適用しています。それぞれの学校教育に適したWebフィルタリングを設定するなど、VDOMごとに異なるポリシーを割り当てることができるので柔軟で効率的な運用が可能です」。

インターネットなどへの接続口となる学外のSINETとの通信だけでなく、基幹スイッチの配下にある学内の通信についてもFortiGateを通過するように以前から学内ネットワークを設計している。学生・教職員の大量のトラフィックに対応するようFortiGateと基幹スイッチ間を広帯域で接続し、「FortiGate 3700Dの各種セキュリティ機能やVDOMをフルに活用してもパフォーマンスにまったく問題はなく、安定稼働しています」と浜氏は導入効果を話す。

FortiMailでセキュアなメールの送受信を推進

企業ユーザーと異なり、一般的に学生は情報セキュリティ意識が乏しい面も否めないだろう。金沢大学では全学生に個人用パソコンの利用を義務付けており、セキュリティ対策がおろそかな自宅などでウイルス感染するリスクもある。「ウイルス感染していることを知らずに学内ネットワークに接続する学生もおり、ウイルス／マルウエアを外部に出さないこともセキュリティ対策で重要です」と山上氏は指摘する。

例えば感染端末を学内の無線LANに接続した場合、FortiGateでチェック。松能氏は「FortiAnalyzerのログを見ると、感染端末がボットネットにアクセスしようとしているのを、FortiGateがブロックしていることが分かります」。そして、感染端末を所有する学生に対して注意喚起するなど、学内の端末がサイバー攻撃の踏み台とならないように防御することも総合メディア基盤センターの役割の一つになるという。

FortiMailの導入効果はどうだろうか。以前はアンチウイルスとアンチスパムの機器が別々のため、運用面や機能面で制約があったという。浜氏は「FortiMailは1台でアンチウイルスやアンチスパム、URLフィルタリング、サンドボックス連携などの豊富な機能を備えています。これらの機能をフルに活用して、メールの受信だけでなく、送信についてもURLフィルタリングやアンチスパムにより、あやしいメールは外部に送信させないようにしています。もし、フィルタリングをすり抜けても、FortiSandboxで挙動を分析し、制御する仕組みです」。また、FortiMailの導入に合わせ、実行ファイル形式の添付ファイルが含まれたメールをブロックするようにポリシーを変更するなど、セキュリティ対策を強化している。

金沢大学総合メディア基盤センター前にて、左から浜 貴幸氏、森本 章治氏、山上 尚幸氏、松能 誠仁氏。

FortiGate、FortiMail、FortiSandboxを自動連携させ運用面でも相乗効果を発揮

そして、FortiGate、FortiMail、FortiSandboxを連携することでセキュリティ強化のみならず、運用管理で大きなメリットがあるという。「FortiGateと同様のGUIでFortiMailやFortiSandboxも設定、管理できます。設計思想が統一されたフォーティネットのセキュリティソリューションに集約したことにより、機器同士の調整も取れています。FortiAnalyzerによるネットワークの可視化やログ管理についても、何が起こっているのか状況が分かりやすく、楽に運用管理できます」と松能氏はセキュリティ対策をフォーティネットに統一したことによる相乗効果を説明する。

また、脅威の巧妙化とともにセキュリティ対策が複雑になるなか、浜氏は「複数メーカーの製品を導入しそれぞれを運用するより、フォーティネット製品で統一し連携するスタイルが、その効果やコストの面でメリットが大きいと判断しました。また、フォーティネットのSEは親身になって相談に乗ってくれます。他のお客様の使われ方なども参考にしながら、いろいろ助言してくれるので助かっています。最新セキュリティ動向を含め、これからもきめ細かな対応をお願いしたいですね」とフォーティネットのサポートに期待する。

森本氏は「グローバル化の中で海外の大学と競争していくためには、教育・研究力の向上が必要です。その基盤となるキャンパスネットワークとセキュリティの強化・拡充を今後とも進めていきます」と力を込める。大学に求められるセキュリティ対策をフォーティネットに統一し、運用の効率化とセキュリティの強化を進める金沢大学の取り組みは、他の大学においても参考になるはずだ。

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