筑波大学

暗号化通信に対しても10GbpsクラスのIPS性能を実現
筑波大学計算科学研究センターのスーパーコンピュータを保護

「開かれた大学」を掲げ、多様な研究活動と人材育成に寄与してきた筑波大学の計算科学研究センターでは、世界的に見てもトップクラスの性能を誇る複数のスーパーコンピュータが稼動している。セキュリティの確保は重要課題の1つであるためログインノードへの通信にはSSHが用いられ、さらにIPSによるスキャンが実施される。そして同時に高いパフォーマンスも要求事項に挙がっていた。10Gbpsクラスの性能と高精度なセキュリティ対策の両立を求めた結果が、フォーティネットの「FortiGate 1500D」だった。

導入・構築のポイント

(1)スーパーコンピュータのログインノードにおける不正侵入防御を10Gbpsクラスのパフォーマンスで実現

(2)SSH暗号化通信についてもスループットを劣化させることなく監視

筑波大学

本部所在地　茨城県つくば市天王台1-1-1
https://www.tsukuba.ac.jp

「開かれた大学」として、最先端のスーパーコンピュータを学際共同利用に

内外に「開かれた大学」として、多様な研究活動と人材育成に寄与してきた筑波大学。その計算科学研究センターもまた、大学や組織の壁を超え、異なる分野をまたいだ研究活動を支援すべく、さまざまな学際共同研究に活用されている。

しかし、広く開かれた窓は、時に招かれざる客も呼び寄せてしまうことがある。2013年11月には、当時計算科学研究センターで運用していたスーパーコンピュータ「T2K-Tsukuba」にアクセスする際に必要な「T2K-Tsukubaログインノード」が不正アクセスを受ける事件が発生した。

スーパーコンピュータ本体が被害を受けたわけではないが、ログインに必要な認証情報が取得された恐れがあったことから、筑波大学では公開鍵を全て更新するとともにログインサーバのOSを最新のものに変更するといった対策を実施。さらに、セキュリティ監視についても万全の措置をとることを発表している。

ログインノードのセキュリティ強化とパフォーマンスの両立が課題に

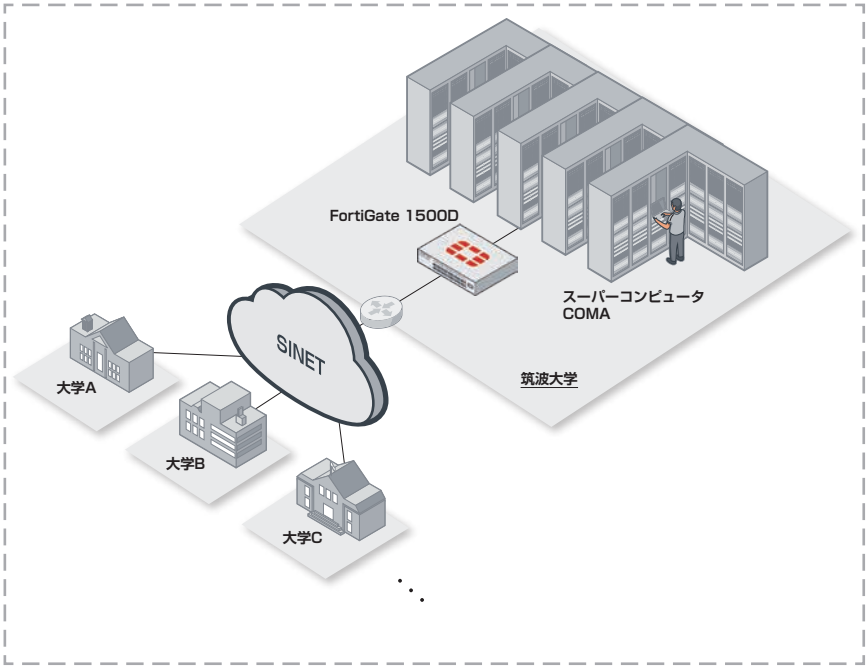
それから数年、筑波大学では引き続き、ユーザーに対するセキュリティ教育も含めたさまざまな対策を講じてきた。その1つが、PACSシリーズの第9世代スーパーコンピュータ「COMA」（Cluster Of Many-core Architecture processor）のログインノードにおける不正侵入防御システム（IPS）の導入だ。内外の研究者や学生がログインする際に必ず経由するこのノードで、不正アクセスにつながるトラフィックが含まれていないかどうかを確認してきた。

だがIPS機器を運用する中で、スループットが十分に出ないという問題が浮上してきたという。筑波大学の基幹ネットワークは10ギガビットイーサネットを前提に構築されており、IPSについても、それを妨げない性能が期待されていた。だがそれまでの機器では10Gbpsクラスのパフォーマンスが実現できず、頭を抱える事態になっていた。

特にボトルネックとなっていたのが暗号化通信だ。暗号化は通信経路上での盗聴を防ぎ、安全な通信には欠かせない技術だが、セキュリティ管理という面では課題となっている。エンドツーエンドで暗号化されたトラフィックは、たとえセキュリティ監視のためであろうと基本的に中身を見ることはできない。これを逆手に取り、近年の巧妙なサイバー攻撃の中には、制御元との通信を暗号化し、監視の目をかいくぐろうとするものが現れている。

FortiGate 1500D

そこでIPS製品側も、組織の内と外とを隔てる境界部分において暗号化通信をいったんひもとき、トラフィックを確認する機能を実装するようになってきた。だが、暗号化通信を復号した上でトラフィックの中身を確認し、再び暗号化するという一連の処理にはCPUに大きな負荷がかかる。これが、FortiGate導入以前の他社製アプライアンスでスループットがなかなか上がらない一因となっていた。



専用チップで暗号処理をオフロード、大学の求める10Gbpsの性能を実現

10Gbpsクラスの性能を実現し、SSH暗号化通信についても高速に処理できるIPS製品という条件を満たしたのが、フォーティネットの「FortiGate 1500D」だった。

FortiGateシリーズは、ネットワークを流れるパケットの再構成といった処理をCPUのみに頼るのではなく、独自開発のASICである専用SPU（Security Processing Unit）を搭載することで、高いパフォーマンスを実現することが最大の特徴だ。暗号化通信においてはCPUやFPGAを多数搭載してようやく実現する10Gbps超のIPSスループットを、少ない数のSPUで実現している。FortiGate 1500Dは、通信の復号化・暗号化やIPSによるシグネチャマッチング処理などに特化したコンテンツプロセッサ「CP8」と、パケット転送などをハードウェアで高速に処理するネットワークプロセッサ「NP6」を搭載している。負荷の高い処理に独自開発の専用プロセッサを用いることで、筑波大学が求める10Gbpsの性能を実現した。

ペタFLOPS級のスパコンに対するログインをFortiGate 1500Dで確実に監視

販売パートナーとともにPoCを実施したところ、要求する水準を問題なく達成できることが確認できた。調達は一般競争入札でなされFortiGate 1500Dが選定された。その後、2018年4月から正式運用を開始した。

導入後数カ月が経っているが、期待した通りのパフォーマンスを実現している。もちろん、セキュリティ監視という本来の目的も果たしている。時折、新たなアラートが上がったときには、筑波大学全体のセキュリティ監視を行うSOCが「具体的にどういった通信か」、「止めてしまっても問題のないトラフィックか」を確認し、対応しているという。

ペタFLOPS級の性能を誇る筑波大学計算科学研究センターのスーパーコンピュータ。その性能を生かし、しかも安全に、研究者がストレスなくさまざまな解析や予測、演算を行える環境を実現するため、フォーティネットのソリューションが果たす役割は大きい。

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