NINS
National Institutes of Natural Sciences

自然科学研究機構(NINS)様
http://www.nins.jp

平成16年4月の法人化により新たに発足した大学共同利用機関法人。国立天文台、核融合科学研究所、基礎生物学研究所、生理学研究所、分子科学研究所の5つの研究所から成り、自然科学に関する研究を推進している。

住　所：〒105-0001
東京都港区虎ノ門4-3-13
ヒューリック神谷町ビル2階
設　立：2004年

マイクロセグメンテーションの効率的な導入・運用で仮想化環境のセキュリティ強化を実現

「基礎生物学研究所」「生理学研究所」「分子科学研究所」の3つの研究機関が立地する自然科学研究機構 岡崎3機関では、構内ネットワーク更新のタイミングで分散セキュリティシステム「vArmour DSS」を導入。先進的かつ利便性に優れるマイクロセグメンテーション技術を取り入れることで、仮想化環境のより一層強固なセキュリティ対策への第一歩を踏み出しました。

構内サーバ間トラフィックの可視化・制御で内部セキュリティ強化を

自然科学研究機構は、全国の大学の研究者が共同利用できる研究施設を運営する「大学共同利用機関法人」として、「国立天文台」「核融合科学研究所」「基礎生物学研究所」「生理学研究所」「分子科学研究所」の5つの研究機関を擁しています。愛知県岡崎市には、このうち3つの研究所が集まる「岡崎3機関」が立地しており、国内外の研究者が集まりさまざまな研究プロジェクトが行われています。近年では、かつて基礎生物学研究所に長年在籍した大隅良典名誉教授が2016年のノーベル生理学・医学賞を受賞するなど、その研究レベルの高さがあらためて国内外から脚光を浴びています。

岡崎3機関は広大な敷地内に3つの研究所と統合事務センターの施設が立ち並び、その間は構内ネットワークで結ばれています。各研究所内のネットワークの管理は各研究所の運用担当者が担っていますが、それぞれのネットワークを集約するコアスイッチをはじめ、上位ネットワークの管理は「岡崎情報ネットワーク管理室」と呼ばれる専門チームが担当しています。

岡崎3機関では2017年3月、構内ネットワーク施設の更新を行いました。同機関は5年ごとにネットワークの見直しを行っていますが、自然科学研究機構 岡崎情報ネットワーク管理室 大野人侍氏によれば、今回の更新ではデータセンター内部のネットワークセキュリティ対策に力を入れたといいます。

岡崎情報
ネットワーク管理室
大野 人侍氏

「サーバはほぼすべてVMware vSphere環境上で仮想化して運用しており、各仮想サーバのセキュリティ状況を簡単に可視化し、効率的に制御できる方法はないかと模索していました。構内ネットワークとインターネットとの境界上にはファイアウォールを設置していますが、構内ネットワーク内のサーバ同士のEast - West通信に関してはほとんど監視・制御する製品や方法がなかったため、新たに制御する仕組みを導入する必要があるとも考えていました。実際に誤って、あるいは意図的に、構内ネットワークに持ち込まれた個人のBYOD端末やUSBメモリ等から脅威の拡散が始まっていたとしても、何が起こっているかすら調べるすべがないのが現状です」

「vArmour DSS」によるマイクロセグメンテーション実装を選択

岡崎情報
ネットワーク管理室
技術職員
内藤 茂樹氏

大野氏らは、仮想サーバごとにネットワークトラフィックを可視化・制御し、セキュリティ対策を強化するためのさまざまな方策を比較検討しました。Linux OSのiptablesを手動で設定したり、あるいはエージェント型のセキュリティ製品を導入することで各仮想サーバを制御するなど、技術・製品を検討しましたが、どれも手間が掛かったり、あるいはコストがかさんだりと、一長一短だったといいます。自然科学研究機構 岡崎情報ネットワーク管理室 技術職員 内藤茂樹氏は、当時の様子を次のように振り返ります。

「既にVMware vSphereの仮想化環境を利用していたので、VMware NSXのマイクロセグメンテーション技術にも着目しましたが、弊機構はL2ベースでネットワークを構築・運用しており、VXLANのようなL3ベースでないと真価を発揮できないVMware NSXとは相性が良くないと判断しました。またハードウエア型ファイアウォール製品の仮想アプライアンス版を各サーバに導入する方式も考えましたが、マイクロセグメンテーション化する機能はなく、既に同様のファイアウォール機器を導入していたこともあり、割高で二重投資は避けたいと考えました」

そんなとき、市場調査から浮上したのが「vArmour DSS」でした。vArmour DSSはVMware NSXと同様に、各仮想マシンを更に分割・セグメント化し、セグメント化された仮想マシンごとにファイアウォール機能を実装、同時に、仮想マシン同士の通信セキュリティを制御するマイクロセグメンテーション機能を提供します。しかもvArmour DSSには、VMware NSXをはじめとするほかの製品にはないさまざまなメリットがあったと大野氏は述べます。

「L2の仮想スイッチにVLANを設定するだけで利用できるため、既存のL2ベースのネットワーク構成を大きく変える必要がありませんでした。また、トラフィックのルートマップやアプリケーションマップなど可視化する機能に極めて優れる点を高く評価しました。アプリケーション層の情報までログに記録されるとともに、迅速で、かつ、豊富なログ・アラートの管理・検索機能も提供されているため、既存システムと連携したログ・アラートを活用し、包括的なセキュリティ管理能力が高まると確信しました」

きめ細かな制御とアプリケーションレイヤーまで可視化できる点を評価

岡崎情報
ネットワーク管理室
技術職員
澤 昌孝氏

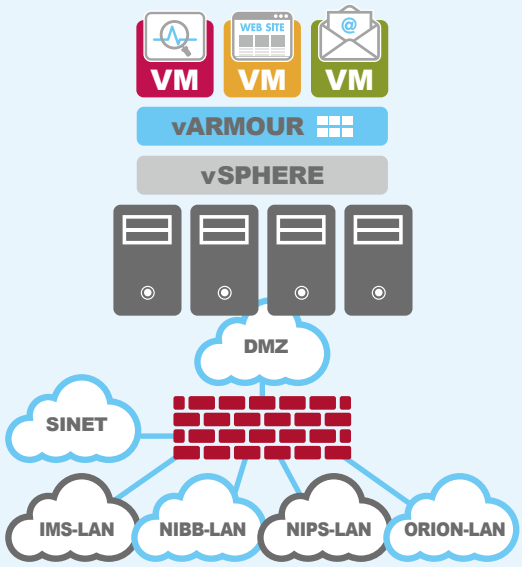
岡崎情報ネットワーク管理室では早速vArmour DSSの評価版を手に入れ、その機能や使い勝手の検証作業を行いました。実際にこの作業にあたった自然科学研究機構 岡崎情報ネットワーク管理室 技術職員 澤昌孝氏によれば、評価の段階からvArmour DSS特有のマイクロセグメンテーション機能の機能と使い勝手の高さは非常に印象的だったといいます。

「エージェントレスによりパフォーマンスが高くスループットが高速で、仮想スイッチに直接接続されているため非常にきめ細かくトラフィックを可視化・制御できると感じました。またTCP／UDPポートレベルだけでなく、アプリケーション層の識別まで可視化できるため、より実践的なセキュリティ制御につながるのではとの期待がありました」

こうした評価結果を受け、岡崎3機関では次期ネットワーク更新においてvArmour DSSを正式に導入することを決定しました。vArmour DSSの評価や、その後の導入プロセスにおいては、vArmour社の技術者が直接岡崎3機関に出向き、現場で澤氏らとともにvArmour DSSのインストールや設定作業にあたりました。初めてのインストールにもかかわらず導入作業は予定通り無事スムーズに終えることができました。澤氏によれば、「導入時の最新バージョン（v3.1.0）で新たにオートマイクロセグメンテーションという機能が追加され、マイクロセグメンテーションの導入・設定をほぼ自動で行えるようになったことで、導入・展開作業が大幅に楽になりました」という。

こうして2017年4月より、岡崎3機関の新ネットワークインフラ「ORIONネットワーク2017」を構成する1製品として、vArmour DSSの本格稼働が開始しました。岡崎情報ネットワーク管理室で管理する約50の仮想サーバのうち、まずは特定の部分に対してマイクロセグメンテーションの設定を施し、トラフィックのモニタリングを継続的に行っています。

■ネットワーク導入イメージ



今後はすべてのサーバのトラフィック可視化とポリシー制御を

vArmour DSSの導入により、これまでは決して見ることができなかった「仮想サーバごとのアプリケーション・トラフィック状況」が初めて把握できるようになりました。内藤氏によれば、これによって仮想化基盤全体のセキュリティ強化に向けた第一歩が踏み出せるようになったといいます。

「まずは仮想サーバ間の現状を把握できないことには、これからどんな対策を施せばいいかも分かりません。これから徐々にvArmour DSSの適用範囲を広げていき、まずはすべての仮想サーバ間の通信を完全に可視化することを目指します。そしてそのトラフィック分析を基に、仮想サーバ間通信の適切な制御やルール作りに取り掛かる予定です」

また大野氏は、こうした制御を管理コンソール上で集中処理できるようになった点が、何よりも大きな導入効果だと評価します。

「vArmour DSSは、複数のサーバに展開されている各仮想マシンのセキュリティ制御を1箇所から集中管理できるため、個々のLinuxサーバのiptablesを手動で設定・更新するのに比べれば作業効率は雲泥の差です。また単に作業が楽になるだけでなく、セキュリティの管轄を管理する上でもメリットがあります。私たちの役割はインフラ管理であり、その上で稼働する仮想サーバは各利用部門の管轄下にあります。そのため場合によっては、私たちは仮想サーバにログインできる権限すら与えられていません。しかしvArmour DSSなら、たとえ仮想サーバのOS管理者の権限がなくとも、すべてのサーバのセキュリティ状況を集中管理できます」

今回の導入効果を受け、大野氏らは今後vArmour DSSによるトラフィック可視化・制御の適用範囲を順次広げていくとともに、「将来的にセキュリティ脅威を積極的に検知・排除できるハニーポットの仕組みを実装する際には、vArmourのマイクロセグメンテーション上で追加可能な独自のハニーポット技術である『Deceptionテクノロジー（偽装サーバ）』も候補として検討してみたい」としています。

vARMOUR
〒100-0004 東京都千代田区大手町1-5-1
大手町ファーストスクエア イーストタワー4階
TEL:03-5219-1480
https://www.varmour.com