\Orchestrating a brighter world NEC

サイバー攻撃自動防御ソリューション 導入事例

国立研究開発法人 国立国際医療研究センター 様

SDNとセキュリティ製品の連携で サイバー攻撃全般への対応強化を実現

国立研究開発法人 国立国際医療研究センター
理事長特任補佐・
センター病院医療情報管理部門長
美代 賢吾 氏

国立研究開発法人 国立国際医療研究センター
バイオバンク 臨床情報DB管理室
上級研究員・情報管理室職員
小南 亮太 氏

国立研究開発法人 国立国際医療研究センター
企画経営部 情報管理室
NW監視センター
中川 陽介 氏

NCGM National Center for Global Health and Medicine

社　　名：国立研究開発法人 国立国際医療研究センター
所 在 地：東京都新宿区戸山1-21-1
代 表 者：理事長　春日 雅人
　　センター病院 院長　大西 真
沿　　革：1868年に山下門内に設置された兵隊假病院を起源とし、幾度かの組織変更を経て、2015年4月に国立研究開発法人となる。
事業概要：国立高度専門医療センターとして、主に感染症・免疫疾患および糖尿病・代謝性疾患に関する基礎研究、臨床研究から技術開発、診療、人材育成まで高度総合医療を推進。また、海外への保健医療支援（技術・人材）をはじめとしたグローバルな医療活動にも力を入れている。研究所、センター病院、国府台病院、臨床研究センター、国際医療協力局、国立看護大学校など多様な組織で構成されている。
U　R　L：http://www.ncgm.go.jp/

事例のポイント

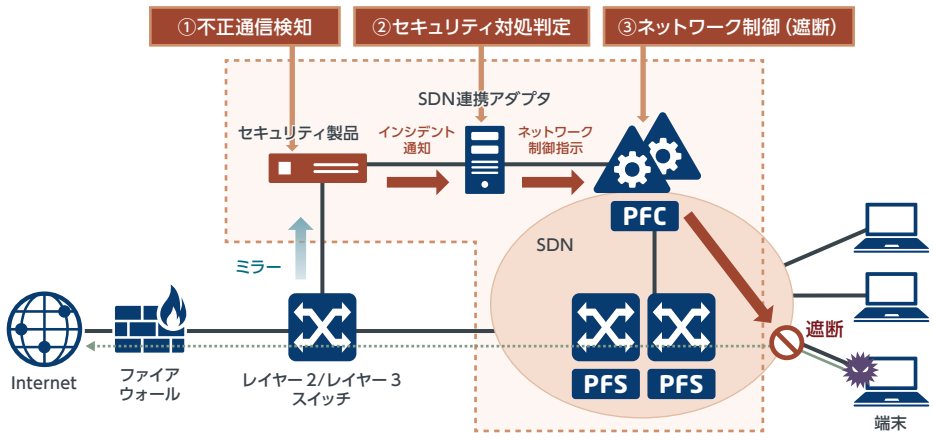
課題背景

- インターネット接続に利用する業務系ネットワークのセキュリティ強化
- 業務系ネットワークにおけるセキュリティ運用の改善
- 業務系ネットワークの運用効率向上

成　果

- **標的型メールをはじめとするサイバー攻撃への対策を強化**
  未知の脅威の検知に定評のあるセキュリティ製品とSDNの連携により、検知精度の向上、対応の自動化・迅速化を実現
- **緊急度の高いインシデント発生時の自動対処を実現**
  自動検出および自動対処（遮断・隔離）によって、人的には不可能な24時間365日のインシデント対応を実現し、被害の未然防止につなげられた
- **ネットワークの運用管理が容易に**
  SDNを採用したことでネットワークの設定や運用状況の見える化を実現。障害時の迅速な切り分けに加え、設定変更や拡張も容易かつ柔軟に行えるようになった

導入ソリューション



※PFC (ProgrammableFlow Controller) / PFS (ProgrammableFlow Switch)：NECのSDN対応製品
SDN連携アダプタ：セキュリティ製品のインシデントログから、適切なセキュリティ対処を判定し、SDNコントローラに指示を出すソフトウェア

国立研究開発法人 国立国際医療研究センター 様

導入前の背景や課題

業務系ネットワークの更新に際し セキュリティ強化を重要テーマに

国立研究開発法人 国立国際医療研究センター様は、国が定める6つの「国立高度専門医療研究センター」の1つとして、感染症・免疫疾患および糖尿病・代謝性疾患に関して国内の医学研究・開発医療の中核的役目を果たしています。また、35超の診療科を有するセンター病院（東京都新宿区）と国府台病院（千葉県市川市）で、高度な総合診療機能を提供していることも大きな特徴です。

研究と診療――。前者は情報検索や外部データベースの利用、さらに共同研究や成果の公開などでセンターの外部とアクティブにつながっていく必要があり、一方で後者は秘匿すべき患者の個人情報を扱います。このように、セキュリティポリシーが異なる2つの業務を鑑みると、それらを同一ネットワークで構築するのは困難です。そのため、「インターネットと接続し外部の情報検索・収集やメールのやり取りなどに利用する『業務系』、主に電子カルテへのアクセスに用いるクローズドな『医療情報系』と、目的別にネットワークを物理的に分けて構築し、さらに各々の配下で部門別や用途別にポリシーの異なる多様なネットワークを整備してきました」と、センター病院医療情報管理部門長の美代賢吾氏は、センター内のネットワーク構成の概要を説明します。

同センターでは、2015年度に業務系ネットワークを更新する計画を進めていました。当初は、ネットワーク性能の強化によるユーザーの利便性向上と、物理配線によらないネットワーク構築による運用管理コストの低減を意図していました。しかし検討を重ねる過程で、重要なテーマとしてセキュリティ強化が導入目的の中心へと移っていきました。

選択のポイント

運用保守体制の課題を考慮し 攻撃への自動対処機能を要望

セキュリティ面に目を向けたきっかけは、標的型のサイバー攻撃が世間を騒がせ始めたことでした。美代氏は、「従来型のウイルスやマルウェアへの対策は以前から打っていましたが、それだけでは防ぎ切れない脅威にも対応できる仕組みが必要だと考えました」と語ります。

新しいセキュリティシステムには、未知の脅威に対する検知能力に加え、「24時間365日の運用保守体制は人員的に困難」（美代氏）であることから、不正通信を検知した際の対処（ネットワーク遮断・端末隔離）を自動化できることも求めました。これらを含め業務系ネットワーク更新の要件を提示。複数ベンダーの提案の中から最終的に目にとまったものが、NECの提案――標的型攻撃対策に優れたセキュリティ製品とSDN（Software-Defined Networking）の連携によって、標的型攻撃への自動防御を実現するソリューションでした。

「セキュリティ製品の検知率の高さや未知の脅威に関する情報収集力はもちろんのこと、それに加え、検知から端末の隔離まで、セキュリティインシデントの対処に必要な一連の業務をカバーした内容を評価しました。インシデント通知サービスの提案はいろいろといただきましたが、休日・夜間にも人を介することなく対応可能な仕組みは他にはなく、まさにセンターが求めていたものでした」。美代氏は評価のポイントをこのように説明します。

セキュリティ製品とSDNを連携させたシステムの実機による検証を経て、実際の導入開始は2015年12月。そこからわずか3カ月という短期間で構築を進め、2016年3月から運用を開始しました。

導入後の成果

瞬時の自動処置に加え アラートからの人的対応も迅速に

新たに導入したセキュリティシステムは、検知したインシデントを3段階で判定。最も危険度が高い場合には、ネットワークの遮断・端末の隔離の自動処置を実行し、他の2段階については管理者にアラート通知を行う設定にしています。

バイオバンク 臨床情報DB管理室 上級研究員・情報管理室職員の小南亮太氏は、セキュリティ管理における業務の変化を次のように説明します。「これまではユーザーからの自己申告があって初めてインシデントに気づくことが多かったのですが、新しい仕組みを導入してからは、自動処置にいたらない場合でもアラートでほぼリアルタイムに不正通信を把握でき、アラート通知にあるIPアドレスで攻撃対象となった端末・個人もすぐに分かるようになりました。もちろんケースによって異なりますが、以前はインシデントの発見から対処までに数日を要することもありましたが、今は自動検知から、自動対処であればわずか数秒、アラートを検知して現場に駆け付ける場合でも概ね10分もかからずに処置を終えることができます」。

さらに、ネットワークの運用管理業務でも、SDNの導入による明確な効果が表れています。企画経営部 情報管理室 NW監視センターの中川陽介氏は、「トラフィックの状況や経路などが管理画面で可視化されたことで、障害が発生したときの切り分けが容易になり、迅速に対応できるようになりました」と話します。また、組織変更などに伴うネットワーク設定の変更が、直感的でわかりやすいGUI画面から容易に行えることにも大きなメリットを感じています。

美代氏は、「今回導入した仕組みは、情報管理者としてまさに『望んでいたもの』でした」と述べた上で、同センターが担う役割の拡大に伴う組織の変更や拡大を視野に入れ、医療情報系ネットワークなどの他のネットワークに関しても、セキュアで柔軟かつ容易に運用管理が可能なネットワークの構築を進めていく意向を明らかにしています。

お問い合わせは、下記へ

NEC ビジネスクリエイション本部

E-mail：inquiry@sdn.jp.nec.com

URL：http://jpn.nec.com/sdn/

日本電気株式会社 〒108-8001 東京都港区芝五丁目7-1（NEC本社ビル）

2016年9月現在

Cat.No. E02-16091474J 160910001 BCC558