最適なネットワークセキュリティ環境を実現する仮想化ソリューション

Solution for Virtualization to Ensure Optimal Network Security Environment

● 小平荘治　● 三橋健治　● 八尋秀治　● 池田信一

あらまし

インターネットに関する技術標準であるRFC(Request For Comments)においてIP(Internet Protocol)が定義されたことで,インターネットは広く普及したが,セキュリティ対策の議論は不十分なままであった。そのため，正常な通信を装った攻撃によって比較的容易にインターネットサービスが妨害されてしまう。また，攻撃手法は日々進化するため，現状のセキュリティ対策が今後も有効であることは保証されない。そのような状況下において，セキュリティ対策は一過性のものではなく，All-IPネットワークに必須な技術要素へと変化し，費用に対する考え方にもネガティブなイメージのある支出から事業継続に不可欠な投資へとパラダイムシフトが生じている。富士通は，この変化に応えるためにネットワークセキュリティ技術の開発，およびソリューション提供に取り組んでいる。

本稿では，まずネットワークにおけるセキュリティ対策の課題について整理し，それらの課題解決に向けた技術要素を紹介する。そして，通信サービスの仮想化で注目されているSDN/NFV(Software Defined Networking/Network Functions Virtualisation)の技術を取り入れた富士通製品の特長を紹介する。

Abstract

The Internet became widely diffused once the Internet Protocol (IP) was defined in an Internet technical standard, Request for Comments (RFC). Meanwhile, security measures were left insufficiently discussed. Given this situation, intruders disguised as normal communication can relatively easily penetrate and disrupt Internet services. Their methods of attacks are becoming more sophisticated on a daily basis, meaning that present-day security measures cannot be guaranteed to work in the future. Against this background, security measures are becoming an indispensable technological component for an all-IP network, as opposed to a one-off program. In addition, a paradigm-shift is occurring with respect to the way the cost of such measures is perceived, from burdensome expenses to investments indispensable for business continuity. In responding to this shift, Fujitsu undertakes the development of network security technology and offers network security solutions. This paper reviews issues with the current security measures, and outlines some technological factors to address them. It then describes specific features of the Fujitsu products that have introduced Software-Defined Networking (SDN) and/or Network Functions Virtualisation (NFV)—key technologies for virtualizing network and communication services.

ま え が き

2000年代から音声・データ通信のIP（Internet Protocol）ネットワーク化が進み，2010年代にはLTEやWi-Fiのような通信方式のグローバル標準化，Android OSを搭載した通信端末などによりコモディティ化が進展してきている。一方で，標準化によりオープンソースソフトウェアが広く活用されるようになった結果，ソースコードに潜在する脆弱性までもが共通化された。第3世代移動通信システム（3G）までは，通信方式の差異がある程度セキュリティ上の防御壁の役割を果たしていた。しかし，今後はグローバルに流通している攻撃ツールや攻撃手法が国内通信キャリア（電気通信事業者）に向けられる可能性が出てきた。

また，IPが広く普及する要因となったインターネットに関する技術標準であるRFC（Request For Comments）は，セキュリティ対策の議論が不十分なまま広く普及した。そのため，正常な通信を装った攻撃によって比較的容易にインターネットサービスを妨害されてしまう。

2013年以降,国内ISP（Internet Services Provider）に多大な影響を与えている通称「水責め」と呼ばれるDNS（Domain Name System）サーバに対するDDoS（Distributed Denial Of Service）攻撃はその一例である（**図-1**）。[(1)] DNSで使用されるUDP（User Datagram Protocol）は，ユーザーからのデータがコネクションを確立せずにサーバのアプリケーションレイヤーまで到達する。そのため，攻撃者にとってはアプリケーションサービスを妨害することに都合が良いプロトコルである。同じく，UDPを使用しているNTP（Network Time Protocol）を悪用した攻撃によって，400 GbpsのDDoS攻撃も観測されており，より一層の警戒と対策が求められる。

そこで富士通は，ネットワークセキュリティ技術の開発，およびソリューションの提供に取り組んでいる。

本稿では，まずネットワークにおけるセキュリティ対策の課題を整理し，課題解決に向けた技術要素を紹介する。そして，ネットワークセキュリティで注目されているSDN/NFV（Software Defined Networking/Network Functions Virtualisation）の技術を取り入れた富士通製品を紹介する。

セキュリティ対策の形態

現在，広く用いられているネットワークセキュリティ対策は以下の三つである。

（1）センサーによる攻撃検知・遮断

ネットワークを流れるトラフィックのデータパターンや通信の振舞いを解析し，主に既知の脅威を検知・遮断する。解析に用いられるシステムは，通信レイヤーや方式の違いにより，NGFW（Next Generation Firewall），IPS（Intrusion

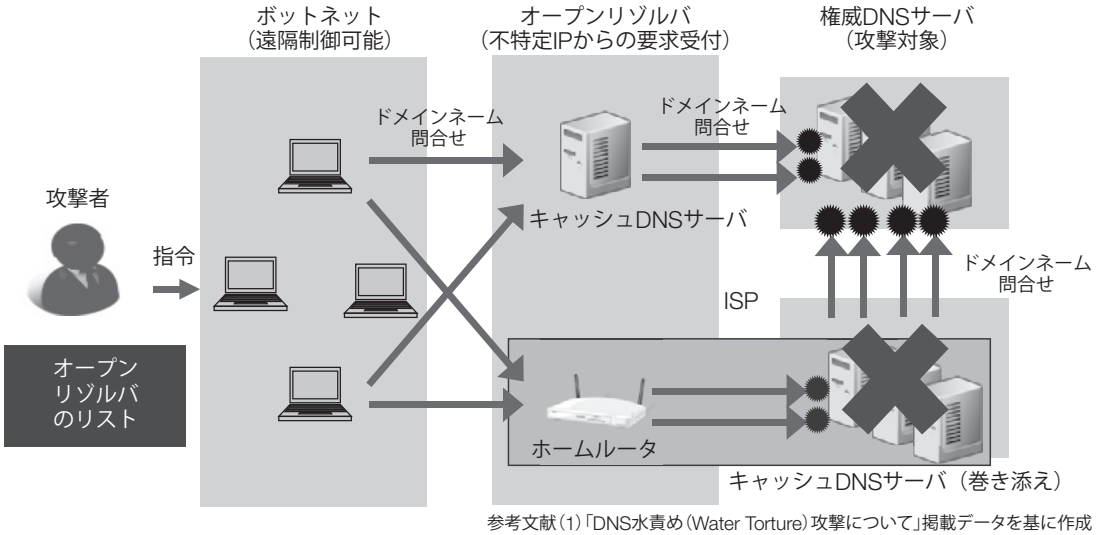

図-1　DNS攻撃「水責め」のメカニズム

Prevention System），WAF（Web Application Firewall）などに分類される。攻撃元が分散したり，長い時間をかけて攻撃を受けたりすると，脅威が認識できない場合がある。そのような特性を持つ脅威や未知の脅威を，どのように検知するかが課題である。

（2）セキュリティログ分析

限られた時間の情報だけでは検知できない脅威に対し，ログを継続的に収集し分析する。また，特定の通信レイヤーでは検知できない脅威に対し，複数センサーのログの相関分析を行うことで検知精度を高める役割を持つ。なお，セキュリティの検知ログが膨大なデータ量になるため，処理の効率化が課題である。

（3）分析結果に基づく対策検討・指示

攻撃が発覚した場合に防御策や軽減策を検討し，上述のセンサーによる攻撃検知・遮断で対応する。しかし，攻撃パターンが変化するため，対策を一律で規定することが難しい。また，攻撃から対策までのリードタイム短縮が重要であり，いかに自動化を図って対応するかが課題である。

多くの通信キャリアは脅威全般を防いでくれることを期待してセキュリティ製品を導入するが，実際はその一部しか防ぐことができない。攻撃パターンが絶えず変化するため，その都度，セキュリティ設計変更が要求されることを認識しておく必要がある。**図-2**は，セキュリティ運用・監視における継続的なメンテナンスを怠った場合のログの検知精度，および分析精度の低下を示したものである。この二つの精度低下を引き起こす原因と結果を挙げてみる。

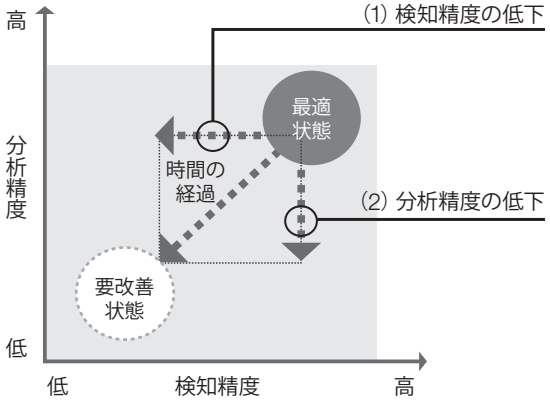

図-2　セキュリティ運用のポイント

（1）ログの検知精度の低下

新たなアプリケーションサービス開始や，データ量増大などトラフィック特性が時間とともに変化する。これにより，検知しきい値が最適値から乖離した状態となる。

（2）ログの分析精度の低下

アップデートによりシグネチャコード数が時間とともに増大する。不要なログ量も増大するため逐次フィルタリングを行わないと真の脅威が自サイトには関係ない不要ログに埋没してしまう。

実際，あるお客様の検知ログを確認したところ，不要ログは全体の80％を占め，残りの20％は脅威の可能性がある調査ログと攻撃ログであった。各検知ログにおける対策は，不要ログは検知対象から外せば良く，調査ログは切分け調査が，攻撃ログは遮断設定への変更がそれぞれ必要となる。なお，以上の三つのログとも，しきい値設定の見直しが基本的な対策方法である。

次章では，高度なセキュリティ対策を実現するための技術要素について解説する。

高度なセキュリティ対策を実現する技術要素

現在，セキュリティの強化に向けてセキュリティオペレーションセンター（SOC）の立上げを検討している通信キャリアが増えている。しかし，ネットワークオペレーションセンター（NOC）と併設して組織を運営していくと，CAPEX/OPEX（設備投資/運用コスト）の増大が避けられない。そのため，経費削減とセキュリティ強化を両立するには，NOC業務とSOC業務の共通化，および自動化を推進する必要がある。これらのセキュリティ強化のポイントとなる技術要素を紹介する。

（1）ログ解析共通基盤

現状，ベンダーから提供されているファイアーウォール（FW），IPS，WAFなどの監視システムは，各ベンダーの製品のみ監視が可能である。そのような縦割りの監視方式を改め，ログ解析用の共通基盤に一旦ログを集約する。更に，シナリオの自動実行システムを備えることで，SOC運用の人的資源を削減できる（**図-3**）。

（2）未知の脅威解析

分析システムには，セキュリティ専業ベンダー

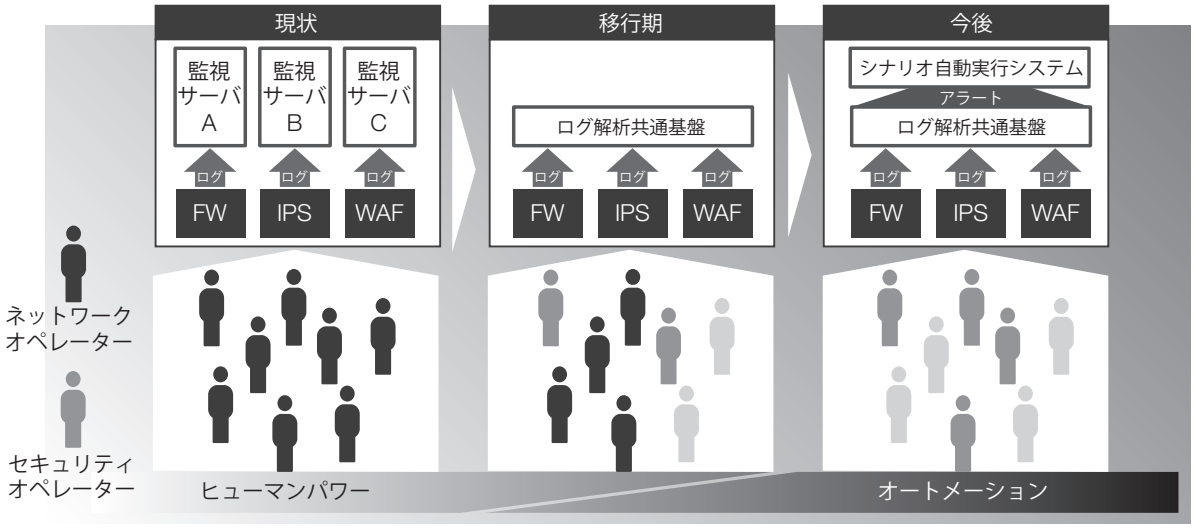

図-3　SOC運用のオートメーション化

から提供されるSIEM（Security Information and Event Management）システムを活用することが効率的である。一方で，既知の脅威パターンとの照合をメインとし，該当しなかった情報は捨てられる。トレーサビリティや，フォレンジックの観点では取りこぼしが生じることもあり，対策を別途講じる必要がある。

富士通では，超高速パケットキャプチャー技術とビッグデータ分析技術[2]をセキュリティ対策に応用し，通信キャリアのような高速，広帯域ネットワークにおいても，セキュリティインシデントの事前・事後対策を可能とするソリューションの開発に取り組んでいる。

(3) セキュリティポリシー最適化

脅威解析の結果によって，センサーに対してセキュリティポリシーをチューニングし，ポリシーを最適化してセキュリティ対策を常に最新の状態に保つ必要がある。しかし，攻撃の検知からこれらの対策を完了するまでに多くの時間を要してしまうため，このリードタイムを短縮することが課題となっている。富士通では，管理者が定義した最適化ルールに基づき，ネットワークの変化に応じてその都度実施される各センサーのセキュリティポリシー最適化作業を自動実行するソリューションの開発に取り組んでいる（**図-4**）。これにより，SOC業務の負担を軽減し，最適なセキュリティレベルを保つことができると考えられる。

富士通のネットワーク仮想化ソリューション

今般，通信キャリアを取り巻く状況は，収益構造の変化，QoE（Quality of Experience）対策，新技術への追従などにより，厳しさを増している。また，多くの通信キャリアは，セキュリティ対策が費用として加わることに負担を感じている。このような課題に対応し，セキュリティサービスをビジネスとして展開していくには，通信サービス仮想化技術であるSDN/NFVが有用である（**表-1**）。富士通では，このNFV技術をセキュリティ分野へ応用し，オンデマンドでのアプリケーション配備，リソース払出し・払戻し，利用状況・稼働状況監視のソリューションとして，FUJITSU Network Virtuora OMおよびVirtuora RVを発表している。詳しくは，本特集に掲載の「NFVを活用したキャリアネットワーク変革に向けた取組み」[3]をご覧いただきたい。

以下，本ソリューションの適用例を紹介する。

(1) サービスチェーニングを利用したネットワークセキュリティサービス

ネットワークセキュリティサービスを通信キャリア側で提供する場合，サービスを契約したエンドユーザーの通信だけをセキュリティ装置に通すなどの構成変更や設定変更が必要となる。

Virtuora OMおよびRVを利用し，ファイアーウォール機能やVPN（Virtual Private Network）

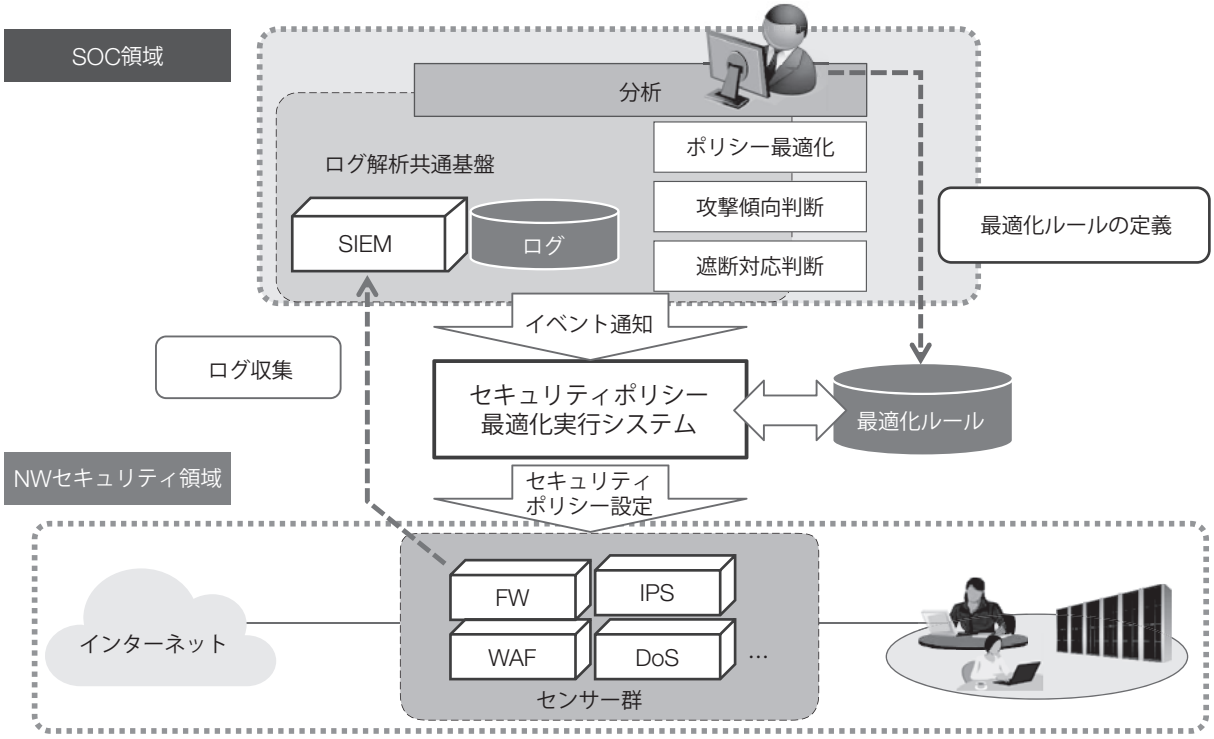

図-4　シナリオ自動実行システム

表-1　SDN/NFVによるネットワークの課題解決

ネットワーク管理者の課題	富士通のソリューション
通信インフラを短期間で構築したい	クラウド管理ソフト（OpenStack）にパッケージソフトやOSなどのインストール自動化をアドオン提供
お客様の業務や，ユーザー需要に合わせて設備増減を簡単に提供したい	
お客様に新たなサービスを短期間で提供したい	オンデマンドでのサービスチェーニング提供
新しいサービスをスモールスタート・ストップで手軽に実施したい	GUIによるサービスのライフサイクル管理実現
運用コスト（OPEX）を削減したい	
運用手順を簡素化し，作業ミスを撲滅したい	

機能などのネットワークセキュリティサービスを仮想化してサービスチェーニング（必要なときに必要なネットワーク機能の利用を可能とするためにエンドユーザーごとのパケットの転送経路を制御する技術）を適用することで，必要なサービスを最少時間で提供できるようになる（**図-5**）。

（2）イベントに応じた自動対策

例えば，悪意のあるユーザーからDNSサーバへのDDoS攻撃を検出した場合，新たな対策が必要となる。

Virtuora OMおよびRVではイベントに対する対策を定義できるため，DDoS攻撃の検出イベントに対し，ファイアーウォール機能，QoS（Quality of Service）機能を自動で適用させるなど，新たな防御手法を確立できる（**図-6**）。

む　す　び

本稿では，ネットワークのセキュリティに対する新たなソリューションを紹介した。

攻撃手法は絶えず変化する。そのため，現状のセキュリティ対策が今後も有効であることは保証されない。それよりも，いずれ見直しが必要となることを想定し，柔軟性・拡張性に優れたベースラインを確立しておくこと，また，プロアクティブな監視体制を構築し，運用する中で攻撃に備えたセキュリティ対策の知見を積み上げていくことが必要である。

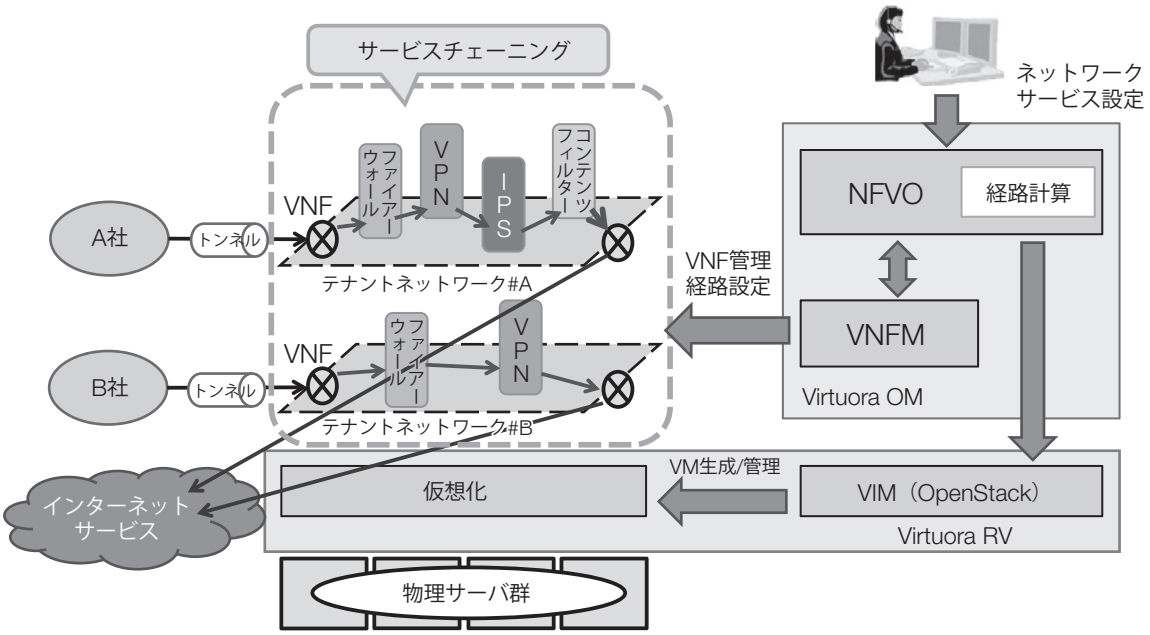

図-5　ネットワークセキュリティのサービスチェーニング

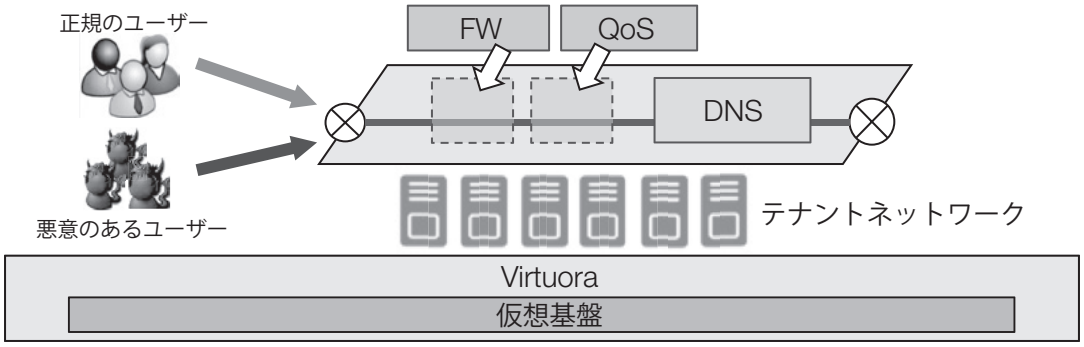

図-6　NFVを活用したDDoS対策

また，セキュリティは一過性の災い対策ではなく，All-IPネットワークに必須な技術要素へと変化し，費用に対する考え方にもネガティブな支出から事業継続に不可欠な投資へとパラダイムシフトが生じている。今後に向けては，高度な防御機能を効率的な運用で実現し，オーバーヘッドを低減していくこと，また，法人やエンドユーザーに対するセキュリティサービスを新たな収益源へと結びつける戦略が重要である。

参考文献

(1) JPRS 森下泰宏：DNS水責め（Water Torture）攻撃について．SECCON 2014長野大会DNS Security Challenge.
http://2014.seccon.jp/dns/dns_water_torture.pdf
(2) 千葉英行ほか：IoT時代のビジネスとネットワークをつなげるフルキャプチャーシステムとビッグデータ解析技術．FUJITSU, Vol.66, No.6, p.76-80（2015）.
http://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol66-6/paper08.pdf
(3) 奥田將人ほか：NFVを活用したキャリアネットワーク変革に向けた取組み．FUJITSU，Vol.66，No.6，p.13-19（2015）.
http://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol66-6/paper03.pdf

著者紹介

小平荘治（こひら　しょうじ）
ネットワークソリューション事業本部
NFVソリューション事業部 所属
現在，通信事業者向けのネットワークセキュリティソリューションの企画・開発に従事。

八尋秀治（やひろ　しゅうじ）
ネットワークソリューション事業本部
NFVソリューション事業部 所属
現在，通信事業者向けのネットワークセキュリティソリューションの企画・開発に従事。

三橋健治（みつはし　けんじ）
ネットワークソリューション事業本部
NFVソリューション事業部 所属
現在，通信事業者向けのネットワークセキュリティソリューションの企画・開発に従事。

池田信一（いけだ　しんいち）
ネットワークソリューション事業本部
NFVソリューション事業部 所属
現在，通信事業者向けのネットワークセキュリティソリューションの企画・開発に従事。