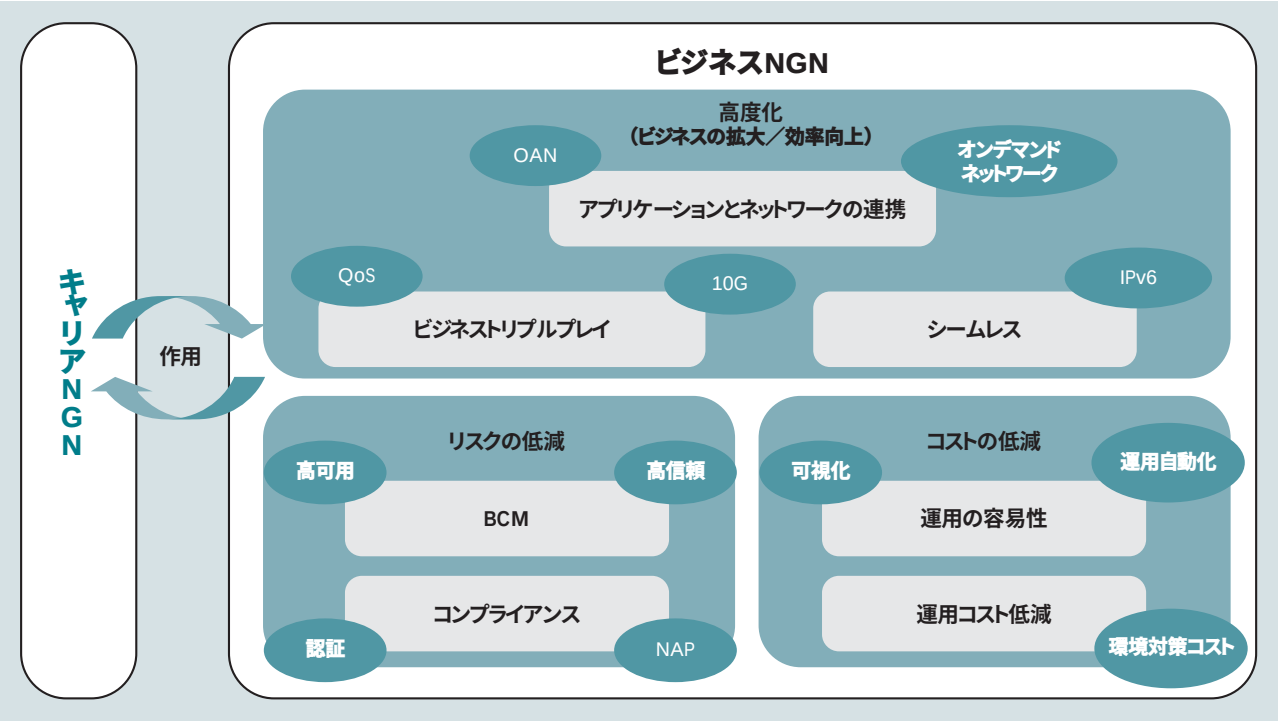
「ビジネスNGN」を実現するスイッチ製品「AXシリーズ」

Activities of Switch Products for “Business NGN,” Next Generation Network Infrastructure of Enterprises

池田 尚哉 Naoya Ikeda
宮島 賢悟 Kengo Miyajima
樋口 秀光 Hidemitsu Higuchi
渡辺 義則 Yoshinori Watanabe



注:略語説明 NGN(Next Generation Network)，OAN(Open Autonomic Networking)，QoS(Quality of Service)，IPv6(Internet Protocol Version 6)，BCM(Business Continuity Management)，NAP(Network Access Protection)

図1 アラクサラネットワークス株式会社の考える「ビジネスNGN」
「ビジネスNGN」とはキャリアNGNを有効に利用し「B(Business)toBtoB時代」において成功するためのビジネスプラットフォームである。各要件に対してそれを実現するためのネットワークインフラに求められる機能要件をだ円内の白文字で示す。

IP技術をベースとした次世代通信網であるNGN（次世代ネットワーク）が商用サービス段階に入った。キャリアのNGNサービスを有効に活用するために企業ネットワークも次世代のビジネスプラットフォームへの進化が必要と考え，アラクサラネットワークス株式会社では「ビジネスNGN」というコンセプトを提唱している。「ビジネスNGN」は「高度化」，「リスクの低減」，「コストの低減」という三つの構成要素から成り，それらを実現するためのスイッチ製品の開発に取り組んでいる。

具体的には，セキュリティの確保のための認証・検疫，省エネルギー運用も含む運用自動化といった機能をスイッチ製品で提供することにより，「ビジネスNGN」の実現を支援する。

1. はじめに

ICT（Information and Communication Technology）の利活用が企業活動の生命線となる中，大規模・高機能化が進化するとともに，システム障害や情報漏洩（えい）などのリスク回避が以前にも増して重要な課題となっている。今後は，これらのリスク回避と安心・安全な高度ICT基盤構築の成否がビジネスの成功と継続性（BCM：Business Continuity Management）に直結することになっていくと考える。さらにネットワークシステムの大容量化に伴う環境対策コストの低減も新たな課題として重要視されてきている。

アラクサラネットワークス株式会社（以下，アラクサラと言う。）は，ルータ，スイッチの専業メーカーとしてネットワークの創造に努めており，次世代の企業ICT基盤として「ビジネスNGN（Next Generation Network：次世代ネットワーク）」を提唱している（図1参照）。

ここでは，「ビジネスNGN」を実現する具体的な要件として，アラクサラのスイッチ製品における認証・検疫機能，運用自動化機能と，トラフィック状況の自動的な把握をめざす研究への取り組みについて述べる。

2. ネットワークの認証・検疫機能

2.1 ICTシステムにおけるセキュリティの確保

従来のネットワークセキュリティは，組織の外部からの攻撃や進入に対して防御を行うファイアウォールやIDS（Intrusion Detection System），IPS（Intrusion Prevention System）などの仕組みにより確保されてきた。しかし，昨今増えつつある情報漏洩やウィルスなどによる被害は，組織の内部において，ウィルスに感染したPCや組織のセキュリティポリシーを満たさないPCをシステムに接続することなどによってもたらされている。

こうした状況を踏まえ，アラクサラでは，組織内部からセキュリティを確保するため，ネットワーク認証機能を重点化している。さらにネットワーク認証機能をベースに検疫システムと連携し，よりセキュアなシステムの実現を図っている。

2.2 トリプル認証機能によるネットワーク認証

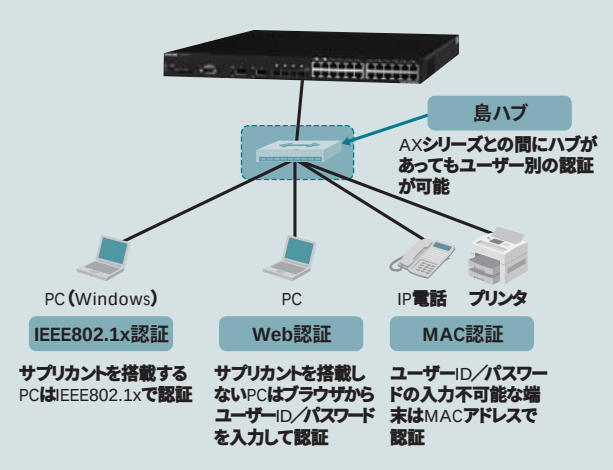
ネットワーク認証は，端末やユーザーがシステムに接続する最初の段階で，認証スイッチと認証サーバが連携して接続可否のチェックを行い,システムへの接続を許可する機能である。主な認証方式として，Web画面上でのユーザー入力を用いるWeb認証，端末のハードウェアアドレスを用いるMAC（Media Access Control）認証，さらに国際標準規格のIEEE802.1x方式による認証の3方式がすでに利用されている。これらの導入に際して課題となるのは，システム内に異なるOS（Operating System）を持つPCやサーバ，ネットワークプリンタなど，さまざまな端末が存在し，各端末で使用できる認証方式が異なること，また，各端末は各スイッチやハブ内で混在して設置されていることなどである。

アラクサラでは，このような多様な環境において既存システムの資産を生かすため，複数のネットワーク認証の混在を可能にする「トリプル認証」を「AXシリーズ」で製品化している。トリプル認証を利用すると，例えば，ユーザー認証が必要な場合にはWeb認証，プリンタなどの汎用OSを持たない端末にはMAC認証，より強固なセキュリティを確保したい場合にはIEEE802.1x認証と，三つの認証方式を1台のスイッチで運用可能である。

AXシリーズでは，トリプル認証をさらに発展させ，例えば，オフィスなどで数台の机ごとに配置される集線用のハブ（島ハブ）の配下に異なる認証方式が必要な端末が複数混在しているような場合でも，端末ごとに認証可能なシステムを提供できる特徴を持っている（**図2**参照）。

2.3 検疫ネットワーク

検疫システムは複数のベンダーが提供しており，それぞれ必要な認証方式が異なるが，AXシリーズではトリプル認証により，さまざまな検疫システムとの連携が可能である。



注：略語説明　ID（Identification），MAC（Media Access Control）

図2　トリプル認証機能を用いたネットワーク構成例
トリプル認証は同時に3方式の認証が可能なため，認証方式の異なる端末が混在する既存システムの資産を生かしながらネットワーク認証の導入が可能である。

例えば，Microsoft※1）社のサーバOSであるWindows Server※1）2008が提供するNAP（Network Access Protection）との連携も可能である。アラクサラはMicrosoft社のNAPパートナーとしてNAPの開発段階からシステム評価・開発を行っており，高い接続性を確保している。

また，日立製作所が提供する統合システム運用管理「JP1」とも連携可能であり，顧客の既存システムでの導入を容易にしている。

3. ネットワーク運用の自動化

3.1 OANの必要性

従来のICTシステムでは，業務の変化に際して，個々の装置に対して別々の手段でICTインフラを制御していたため，ICTシステムの変更が容易ではなく，かつ時間もかかるという課題があった。これを改善するために最近ではWeb技術を利用したICTインフラを制御する技術の開発が進み，サーバ，ストレージ，周辺機器の管理のためのデータモデルの標準化が進んでいる。

一方，ネットワーク機器においても，最近ではサーバなどと同様にWebベースの制御技術を用いることによってICT全体の運用負荷を軽減しようという動きがあり，インターネット技術の国際標準化団体であるIETF（The Internet Engineering Task Force）で標準化が検討される方向にある。

この動きに先駆け，アラクサラでは次世代企業ネットワークを支える新しい運用技術として，「オープン・オートノミック・ネットワーキング（OAN）」コンセプトを2006年2月に発表した。OANは企業ネットワークの運用自動化，およびそれによる運用コスト低減への寄与が期待されている。

3.2 OAN技術の標準化活動

IETFにおけるネットワーク運用管理の標準化を議論するエリア（Operations and Management Area）には，17のワーキンググループがある。アラクサラが主に参加しているのは，通信装置のコンフィギュレーションに関する標準化技術の推進活動を行っているNETCONFワーキンググループである。

アラクサラでは，2006年11月のIETF会合におけるNETCONFワーキンググループにて，次世代のネットワーク機器制御プロトコルであるNETCONF/SOAP（Simple Object Access Protocol）ベースのネットワーク管理API（Application Program Interface）についてのドラフトを提案した。このドラフトは，RFC（Request for Comments）4743（NETCONF over SOAP）に対して，実装方式を提案するものである。この提案技術は，AXシリーズ（AX1200S/AX2400S/AX3600S/AX6300S/AX6700S）において製品化済みであり，現在，IETFでRFC化を推進中である。

アラクサラではさらに，NETCONF上で扱うACL（Access Control List）のデータモデル，VLAN（Virtual Local Area Network）のデータモデルに関するドラフト提案を行うなど継続した標準化活動を行っている。

3.3 OAN技術を用いた省電力

ICTシステムの各装置は，「常時通電」であるため，業務時間外でも電力を消費している。サーバなどでは，スケジューラなどを使って，夜間や休日にサーバを止めたりする制御を自動化することが考えられるが，同じようにOAN技術を使って，スケジューラに装置給電の制御を行うことを指示させて，リモート機器の電力供給を制御することが可能である。

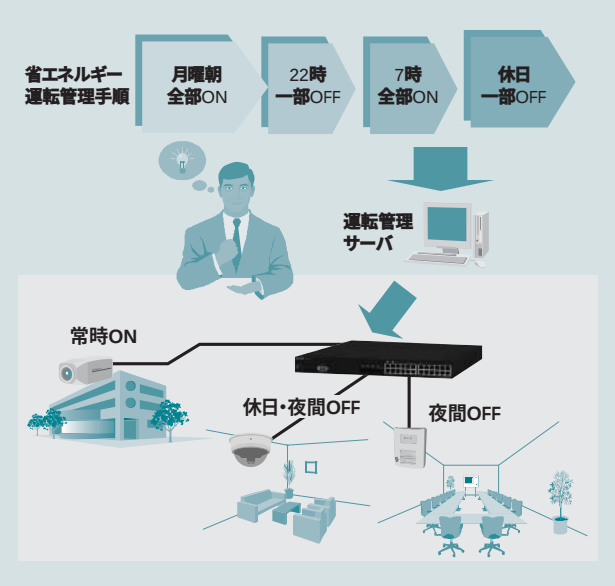


図3 OAN技術の省電力への応用
装置の設置場所の状況や運転管理手順に従って，運転管理サーバから各装置の給電制御を行い，システム全体の省エネルギーを実現する。

アラクサラのスイッチはイーサネット※2)で接続した無線LANや監視カメラなどのデバイスにPoE（Power over Ethernet）機能を用いて給電可能であり，この給電を装置の設置場所や稼働時間帯に合わせて制御（給電のON/OFF）することでネットワークシステム全体の省エネルギーを実現すると同時に，この操作を自動化することによって運用コストの低減も可能となる（**図3**参照）。

4. トラフィック状況の自動的な把握をめざす研究の取り組み

4.1 運用におけるトラフィック監視の現状とニーズ

ネットワーク上の不具合は，業務遅延や顧客サービス低下などに直結するため，トラフィック状況を常に把握し，問題発生時に迅速な解決を図ることが運用者の重要業務となっている。しかし，近年では監視対象トラフィックの増大，システムの複雑化，アプリケーションの多様化などにより，問題発生から解決までに長い時間を要する例が増えている。

エンドユーザーの申告などによって問題発生を検知すると，運用者は種々のトラフィック監視情報やサーバのログ情報などから原因の推定と切り分けを行い，さらに詳細な解析を進めるトラブルシュートを行う。近年のネットワークの高速化と複雑化は，トラブルシュートの最初の段階である状況の把握と原因の切り分けを困難にしている。

4.2 AFM技術のコンセプト

アラクサラでは，高速化・複雑化するネットワークでトラフィックの状況をリアルタイムに把握可能な新しいトラフィックモニタリング技術であるAFM（Aggregated Flow Mining）技術の研究に取り組んでいる。

AFM技術は，高速・大容量トラフィックの中から「目立つフロー」をリアルタイムに自動抽出する技術で，トラフィックの詳細を知ることよりも全体の状況をすばやく俯瞰（ふかん）することに重点を置いた技術である。

「目立つフロー」とは，パケット数の多いフロー，占有帯域の大きいフローのことである。AFM技術では，単純な1対1のコンピュータ間を流れるフローだけでなく，1対n間を流れる複数のフローを束ねたものも一つのフローと見なして抽出対象とする。このようなフローの束を集約フロー（Aggregated Flow）と呼ぶ。さらに，1対nの集約フローのnの値も同時に計測する。これを異なり数と呼ぶ。

集約フローを抽出対象とすることで，トラフィックの内訳をサーバや端末のふるまいレベルで把握することが容易になる。また，DDoS（Distributed Denial of Service）攻撃などのセキュリティ上の脅威によるフローなども把握が容易となる。さらに，

※2） **イーサネットは，富士ゼロックス株式会社の登録商標である。**

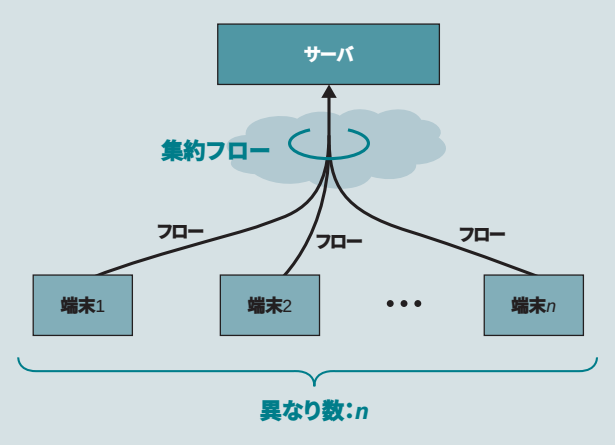


図4　集約フローの例
あて先IPアドレスとあて先ポート番号が同一のフローを束ねた集約フローは，サーバへのアクセスによるものである可能性が高いと推定される。さらに，異なり数と集約フローの帯域から，これらが通常アクセスかアタックによるものかが推定可能になる。

異なり数の情報を併用することで，抽出された集約フローの素性を推定しやすくなる(図4参照)。

4.3　AFM技術の効果

AFM技術は，集約フローの単位で帯域やパケット数の多いフローをリアルタイムで自動抽出するため，ネットワークに問題が発生したとき，ここで抽出された情報の中に問題解決の糸口となる情報が含まれている可能性が高い。また，抽出された情報はそのフローに関連するコンピュータのふるまいをある程度推定できる形の情報となっている。このため，従来の単純なインタフェース統計やsFlow※3)/NetFlow※4)などのフロー統計機能だけを利用する場合に比べ，運用者がトラフィック状況を把握するまでの手間と時間を軽減し，ターゲットを絞った詳細なトラブルシュートを始めるための有用なヒントを提供できると考える。

4.4　今後の取り組み

アラクサラは，これまでソフトウェアによる実装で論理や有効性の検証を行っている。比較的簡易なアルゴリズムであるため，ハードウェア処理により10 Gビット/sを超える超高速回線への適用も可能と考えている。現在，独立行政法人新エネルギー・産業技術総合開発機構の委託事業において，40 Gビット/s超回線におけるAFM技術の実用化をめざした技術開発を推進中である。

5. おわりに

ここでは，次世代の企業ICT基盤としてアラクサラが提唱している「ビジネスNGN」というコンセプトに関し，具体的にスイッチ製品の機能として製品化している認証・検疫技術，運用自動化の技術，および今後のネットワークの可視化のために研究開発中の新世代のトラフィック監視技術への取り組みについて述べた。

アラクサラは，この「ビジネスNGN」というコンセプトに基づき，今後も企業のICT基盤の革新を支援すべくルータ・スイッチ製品事業を推進していく所存である。

※3) sFlowは，InMon Corp.の米国およびその他の国における登録商標である。
※4) NetFlowは，Cisco Systems Inc.の米国およびその他の国における登録商標である。

参考文献など

1) T. Goddard：Using NETCONF over the Simple Object Access Protocol（SOAP），IETF（2006.12）
http://www.ietf.org/rfc/rfc4743.txt
2) T.Iijima，et al.：Experience of implementing NETCONF over SOAP，IETF（2008.2）
http://www.ietf.org/internet-drafts/draft-iijima-netconf-soap-implementation-07.txt

執筆者紹介

池田 尚哉
1981年日立製作所入社，アラクサラネットワークス株式会社
営業本部 所属
現在，スイッチ，ルータ製品のマーケティングに従事
情報処理学会会員

樋口 秀光
1985年日立製作所入社，アラクサラネットワークス株式会社
製品開発本部 所属
現在，ネットワークセキュリティ，ネットワーク運用管理のマーケティング業務に従事
情報処理学会会員

宮島 賢悟
1993年日立製作所入社，アラクサラネットワークス株式会社
営業本部 所属
現在，スイッチ，ルータ製品のマーケティングに従事

渡辺 義則
1987年日立製作所入社，アラクサラネットワークス株式会社
製品開発本部 所属
現在，スイッチ，ルータ製品向け技術の研究，調査に従事
電子情報通信学会会員