安全で柔軟なネットワークアクセスを提供する「アクセス認証ソリューション」

河合 英紀　小美濃 貴行　芝原 栄男　坂本 大地　金森 一朗　園田 健太郎

要 旨

顧客情報や部品の設計情報など、機密性の高い情報を扱う部門やプロジェクトでセキュリティを徹底させて情報漏えいを防ぐためには、部門やプロジェクト単位でのネットワークのアクセス制御が不可欠です。一方、細かくアクセス制御を行えばセキュリティを向上させることはできても、運用コストが膨大になり、企業内の組織変化に迅速に追随できないという課題がありました。本稿では、SDNを利用して、人事情報を元にアクセス可能なサーバ・ネットワークを自動的に設定することで、セキュリティを向上させつつ、運用コストを削減できる「アクセス認証ソリューション」について紹介します。

KeyWords　情報セキュリティ／情報漏えい／標的型攻撃／BYOD／VLAN／SDN／OpenFlow

1. まえがき

近年、企業経営者にとって情報漏えいリスクは最も大きな脅威の1つとなっています。しかし、そのための対策であるネットワークのアクセス制御は十分とはいえません。ビジネス環境の変化に伴う企業内の組織変化に追随するためには、アクセス制御の運用コストが膨大になってしまうからです。本稿では、ネットワークをソフトウェアで動的に制御可能なSoftware-Defined Networking（SDN）を使って人事情報とアクセス制御を連動させることにより、情報のセキュリティを確保しつつ、運用コストを抑えて柔軟なアクセス制御を実現する「アクセス認証ソリューション」について紹介します。

人事情報は、社員の所属部門やプロジェクト、役職、在席地等に関する情報のことです。企業ネットワークにおいて、誰がどの情報にアクセス可能かは人事情報に基づいて決定されます。したがって、人事情報とアクセス制御が連動することで、人手によるネットワーク設定を介することなく情報への不正アクセスを防ぎ、かつ、適切な人が適切な情報にアクセスできる環境を常に保持できるようになります。また、本ソリューションをInformation Rights Management（IRM）など、ファイルのアクセス制御とあわせて適用することで、より強固なセキュリティ対策を実現できます。

2. 企業における情報漏えいとアクセス制御の課題

近年、民間企業や行政による情報漏えい事件が相次いで発生しており、個人情報や機密情報の保護に対する社会の注目・関心が高まってきています。ITが高度に発達したネットワーク社会において、事業者は情報漏えいという新たなリスクに直面しており、情報を安全に保護するための管理体制が求められています。

機密情報を保護し情報漏えいを防ぐ対策の第一歩としては、アクセス制御により機密情報の閲覧者を必要最低限にすることが挙げられます。例えば、金融・保険・証券業では金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）のガイドラインによって、部門ごとにネットワークを分離するよう推奨されています。また、銀行では、利益相反の可能性がある部門間で、システム上のアクセス制限や物理上の遮断を行うなど、情報遮断措置を講じることが法律で定められています。金融業以外でも、ネットワークの分離は重要です。例えば、標的型攻撃対策としてネットワークを分離することで、ウイルス感染の影響を局所化できます。

しかし、現実には、経営者側は情報漏えい対策に対して強い危機感を持っているにも関わらず、現場のアクセス制御

の実態は必ずしも十分ではないのが実情です。部門やプロジェクトごとに細かくネットワークを分離し、アクセス制御を行ってセキュリティを向上させようとすると、運用管理コストが膨大になってしまうからです。

例えば、人事異動によって営業部の人間が企画部に異動する場合、それに合わせてネットワークの接続を変更するための申請作業と設定作業が、ネットワークの利用者と管理者の双方に発生します。また、出張などで拠点間を移動し、外出先の拠点から自部門のネットワークに接続する場合にも、前もってネットワークの設定変更が必要です。他にも、ネットワークの設定変更が必要になるケースとしては、オフィスレイアウトの変更や部門の引っ越しなどによって接続先のLANケーブルが変わる場合や、プロジェクトのように流動的な組織に対しても、独立したネットワークを構築して機密情報を守りたい場合なども該当します。このように、ネットワークの設定変更作業はさまざまな原因とタイミングで発生するため、漏れやミスなく行っていくためには、運用管理に多大な努力と時間が必要になるのです。

アクセス認証ソリューションでは、ネットワークを細かく分離しつつ、アクセス制御を人事情報と連携させることによって、ネットワークの設定変更作業を自動化できます。そのため、変更漏れや設定ミスをなくし、安全かつ柔軟なアクセス制御を実現できます。

3. アクセス認証ソリューション

アクセス認証ソリューションの概要を図1に示します。本ソリューションは、「機密性の高い情報を扱っている部門やプロジェクトでのセキュリティを徹底させたい」場合に有効です。機密性の高い情報の例としては、顧客データ、企業の経営データ、新製品企画情報、部品の設計情報、製造プロセス情報などが挙げられます。

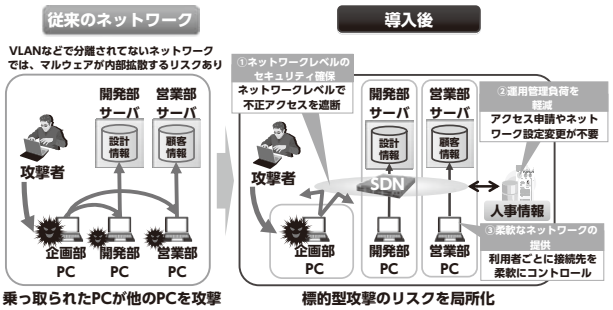


図1　アクセス認証ソリューションの概要

本ソリューションのポイントは、

(1) ネットワークレベルでのアクセス制御
(2) クライアントPC間のアクセスの制限
(3) 人事情報と連動した設定の自動化

以上の3点です。

(1) ネットワークレベルでのアクセス制御を行うことで、誰がいつどこからアクセスしているかをログに残すことができます。また、サーバレベルでのアクセス制御だけでは、すべてのサーバが攻撃対象となってしまいますが、ネットワークを分離することで、攻撃範囲を部門単位に限定することができます。

(2) クライアントPC間のアクセスの制限は、SDNがネットワークに接続しているノードの種類に応じてトラヒックをコントロールすることにより可能になります。これにより、標的型攻撃により内部に入り込んだマルウェアがクライアントPCの脆弱性を突いて蔓延することを阻止することができ、影響を局所化できます。

(3) 人事情報と連動した設定の自動化は、人事情報データベースとOpenFlow[*1]スイッチの設定を連動させることにより実現されます。これにより、人事異動や拠点間の移動時に必要だったネットワークの設定変更作業を、漏れなくミスなく自動化できます。

以上のポイントにより、これまで難しかったネットワークのセキュリティ向上と、運用コスト削減の両立を実現することができます。

3.1 システム構成

アクセス認証ソリューションのシステム構成例を図2に示します。本ソリューションでは、各拠点の既存のネットワークに、OpenFlowスイッチと管理サーバを追加し、人事情報と連携させます。

OpenFlowスイッチには、基本的にソフトウェアスイッチとして、汎用サーバの上でOpen vSwitchを使用します。また、OpenFlowスイッチをUNIVERGE PFシリーズのハードウェ

*1 「OpenFlow」はネットワーク制御機能をスイッチから分離し、コントローラに集約することで、ネットワークを集中制御できる方式でSDNを実現する技術の1つ。NECはOpenFlowの非営利標準化団体であるOpen Networking Foundation（ONF）の設立メンバー

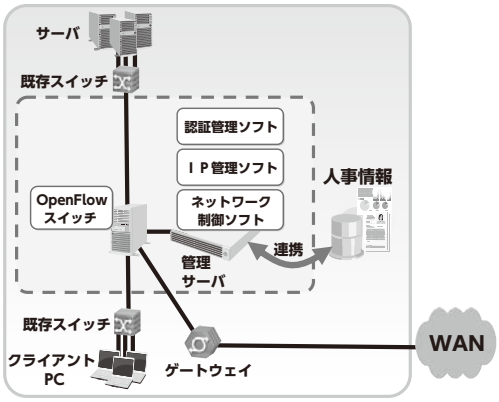


図2　アクセス認証ソリューションのシステム構成例

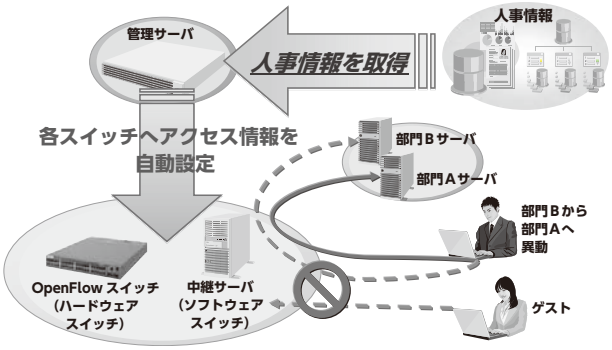


図3　ネットワークレベルのセキュリティ

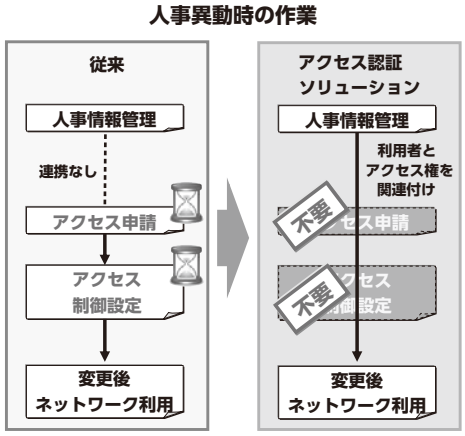


図4　運用コストの削減

アスイッチとして提供することも可能です。

管理サーバ上で動作するネットワーク制御ソフトは自主開発のOpenFlowコントローラです。また、IPアドレスを払い出すIP管理ソフトとしてDHCP、認証管理ソフトとしてOpenLDAPを使用します。適用規模・性能は限定的になりますが、ソフトウェアのOpenFlowスイッチを管理サーバの上で動作させることにより、1台のサーバを追加するだけの形態での提供も可能です。サポートされる認証方式は、端末認証、802.1X認証（RADIUSサーバ別売）、Web認証の3種類で、これらを組み合わせた運用も可能です。

複数の拠点に導入する場合は、それぞれの拠点の既存ネットワークに図2と同様にOpenFlowスイッチと管理サーバを追加します。人事情報と連動したネットワーク設定情報が管理サーバ間で共有されるため、2拠点目以降は人事情報との連携は不要です。既存ネットワークを活用したスモールスタートが可能なので、特に機密性の高い情報を扱い、ネットワーク分離の必要性が高い部門から優先して導入し、その後、必要に応じて複数拠点に段階的に同一構成を展開し、スケールアウトさせることが可能です。

3.2 アクセス認証ソリューションの特長

ここでは、アクセス認証ソリューションの3つの特長として（1）ネットワークレベルのセキュリティ、（2）運用コストの削減、（3）柔軟なネットワーク、について説明します。

（1）ネットワークレベルのセキュリティ

アクセス認証ソリューションでは、管理サーバが人事情報を取得し、それにあわせてOpenFlowスイッチに利用者ごとのアクセス情報を自動的に設定します（図3）。

そのため、人事異動時のアクセス権の変更漏れや設定ミスを防止し、ネットワークレベルで不正アクセスを遮断することができます。また、クライアントPC間の通信も簡単に制限できるため、標的型攻撃や情報漏えいなどイントラネット内部からのセキュリティリスクに対応することができます。

（2）運用コストの削減

従来のネットワークでは、人事情報とネットワークのアクセス制御は連動していませんでした。そのため、人事異動などの組織の変更があった場合、ネットワーク利用者がアクセス変更申請を行い、それに応じてネットワーク管理者がアクセス制御の設定変更を行う必要がありました（図4）。一方、アクセス認証ソリューションでは、人事情報に連動して自動的にアクセス制御設定が行われるため、人手による変更作業は不要になります。組織の変化に伴うアクセス申請とアクセス制御の設定作業は1人につき10～20分程度の短い時間です

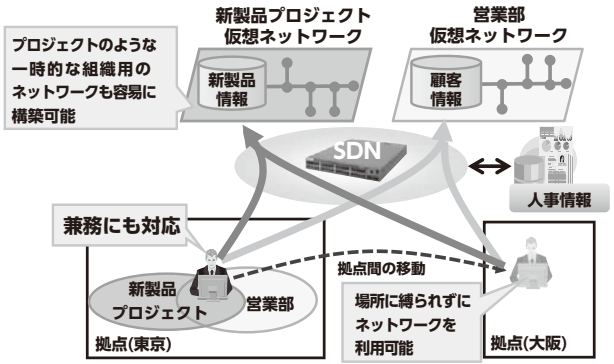


図5　柔軟なネットワーク

が、年間に発生する組織の変化（人事異動、拠点間の移動、オフィスレイアウトの変更、プロジェクト用ネットワークの構築など）と、それに付随するアクセス申請とアクセス制御の設定作業のコストを積み上げると、かなりの額になります。3,000人規模の企業を想定した試算では、5年間で約60%の運用管理コスト削減効果を見込んでいます。導入コストを考慮すると、トータルコストでは約30%の削減を見込むことができます。

(3) 柔軟なネットワーク

アクセス認証ソリューションでは、SDNによる仮想ネットワークを使ってネットワークを分離するため、流動的なプロジェクト用のネットワーク構築や、複数組織の兼務などにも容易に対応可能です。また、異なる拠点からのネットワークアクセスも、事前の申請なく利用可能となり、拠点間の移動にも柔軟に対応することが可能です。図5では、営業部に所属し、新製品プロジェクトに関わる社員が、東京の拠点から大阪の拠点に出張などで移動しても、同じ仮想ネットワークに接続できることを示しています。

4. むすび

本稿では、SDNを使って人事情報とアクセス制御を連動させることによって、安全で柔軟なネットワークアクセス制御を実現する「アクセス認証ソリューション」について紹介しました。本ソリューションは、OpenFlowによるネットワーク制御を人事情報に結び付けた認証と連携させることにより「機密性の高い情報を扱っている部門やプロジェクトでのセキュリティを徹底させたい企業様」に対し、(1) ネットワークレベルのセキュリティ、(2) 運用コストの削減、(3) 柔軟なネットワーク、を提供いたします。

* OpenFlowは、Open Networking Foundationの商標または登録商標です。

執筆者プロフィール

河合 英紀
SDN戦略本部
エキスパート

小美濃 貴行
SDN戦略本部
主任

芝原 栄男
SDN戦略本部
シニアエキスパート

坂本 大地
NECネッツエスアイ
ネットワークサービス事業本部
サービスプラットフォーム事業部
主任

金森 一朗
日本電気通信システム
ネットワークソフトウェア開発事業本部
共通基盤開発本部

園田 健太郎
クラウドシステム研究所
主任

関連URL

NECのSDNソリューション
http://jpn.nec.com/sdn/

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.66 No.2　ICTシステムを高度化するSDN特集

ICTシステムを高度化するSDN特集によせて
SDNがもたらすICTシステムの高度化とIT・ネットワーク市場の変化
NECのSDNへの取り組みとNEC SDN Solutions
SDN実用化に向けた標準化

◇ 特集論文

NEC Enterprise SDN Solutions
WANの利用、運用を効率化する拠点・データセンター接続最適化ソリューション
安全で柔軟なネットワークアクセスを提供する「アクセス認証ソリューション」

NEC Data Center SDN Solutions
仮想環境の効率化を実現するIaaS運用自動化ソリューション

NEC SDN Solutionsを支える最新技術
SDNコントローラ作成のシンプル化を実現するネットワーク抽象化モデル
Wi-Fiの利便性向上を実現するスマートデバイス通信制御技術
大規模SDNネットワークを実現するOpenFlowコントローラアーキテクチャ
ヘテロジニアス網統合制御基盤を実現するマルチレイヤ抽象化技術
運用省力化を実現するIP-VPN向けOpenFlowコントローラ

導入事例
乱立する部門LAN、移動する検査機器 医療現場のネットワークをOpenFlowで改革
事業拡大を見据えデータセンターにSDNを導入 サービスのスピード、信頼性、他社優位性を向上

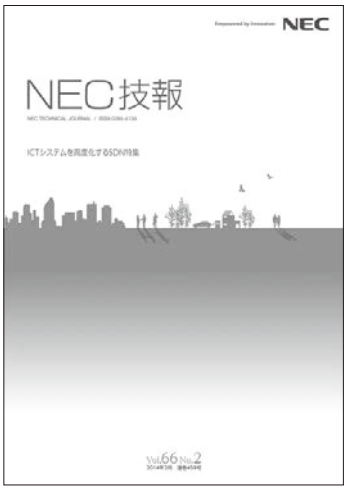
◇ 普通論文

iPASOLINK All Outdoor Radio（AOR）装置の開発
iPASOLINKシリーズ及び超多値変調技術の開発
10Gbps伝送を実現する超大容量無線伝送技術
メタマテリアルを用いた電磁ノイズ抑制技術とその実用化

◇ NEC Information

C&Cユーザーフォーラム&iEXPO2013
人と地球にやさしい情報社会へ ～インフラで、未来をささえる～
NEC講演
展示会報告

NEWS
2013年度C&C賞表彰式典開催



Vol.66 No.2
(2014年2月)

特集TOP