6E-04

企業における SD-WAN を活用した ネットワークセキュリティ対策の提案

野島　主成†　　後藤　厚宏†
情報セキュリティ大学院大学†

概要

企業の情報通信ネットワークでは、クラウドサービス利用の増加、ビジネス展開のスピードアップに伴う事業統合・分離への対応、IoT（Internet of Things）などネットワーク接続機器のマルチデバイス化など、取り巻く環境にも変革が起きている。また、ネットワークの利用上の問題もあり、これらへの解決策として SD-WAN（Software Defined WAN）が注目されている。本研究では、SD-WAN を導入する企業におけるセキュリティ対策を検討し、提案することを目標とする。

1. 企業の情報通信ネットワークの現状と課題

企業の IT インフラ基盤を支える情報通信ネットワークの重要度が増している。最近ではクラウドサービス利用の増加、事業統合・分離の増加、IoT 機器の接続など情報通信ネットワークを取り巻く環境に変革が起きている。またネットワーク利用上の問題点として、ウイルス感染への不安、運用・管理人材の不足、運用・管理費用の増大、セキュリティ対策の確立が困難といった点が挙げられている[1]。

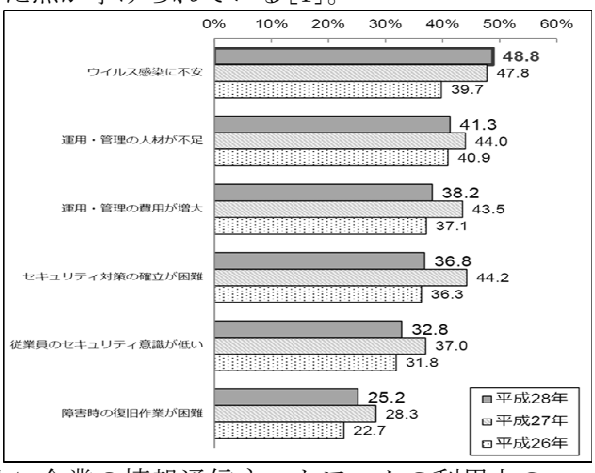

図 1 企業の情報通信ネットワークの利用上の問題[1]

これら課題への解決策として SD-WAN が注目されている。本稿では SD-WAN を導入する企業におけるセキュリティ対策を検討し、確実かつ迅速な運用が可能なネットワークを提案する。

2. 企業における SD-WAN

SD-WAN は、専用線、ブロードバンド回線等の従来の物理回線をアンダーレイ回線として用いながら、回線種別に依存せずにオーバーレイによる仮想の WAN 構成を実現する。

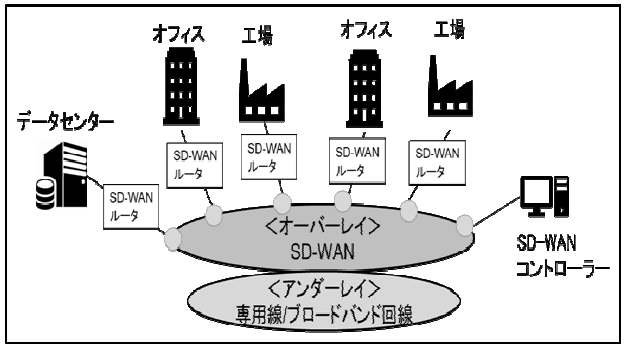

図 2 企業の SD-WAN 構成

これにより、複数の通信会社による回線・モバイルなど多種多様な物理回線から、自由にメイン回線およびバックアップ回線を選択して、企業 WAN を構成することが可能となる。また、同一の仮想的なオーバーレイネットワークを一元管理できるようになるため、WAN の運用・管理における負荷の削減が見込める。

3. SD-WAN の機能

SD-WAN では従来の WAN では実現できていなかった機能が実装される。企業の情報通信ネットワークに効果のある機能が実装され、これらを有効に活用することで大きな効果が得られると想定している。主な機能と想定効果について以下に示す。

The proposal for organizational measurement of network security utilizing SD-WAN
†Kazunari NOJIMA, Atsuhiro GOTO
†Institute of Information Security

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.

表 3 SD-WAN の主な機能と想定効果

#	機能	内容	想定効果
1	セグメンテーション/マルチテナント	物理WAN上に複数の論理的なWANを構築して制御する	・セキュリティ対策 ・アジリティ改善 ・コスト削減
2	インターネットブレークアウト	特定のアプリケーショントラフィックを拠点のインターネット回線を利用して直接通信させることで回線利用効率を最適化する	・回線利用効率向上 ・コスト削減
3	ハイブリッドWAN	業務システムへのアクセスは専用回線を通し、メール・ファイルサーバ等へのアクセスはブロードバンド回線を通すことでトラフィック分散を最適化する	・回線利用効率向上 ・コスト削減
4	NFV（Network Functions Virtualization）	ネットワーク機能を仮想化し、汎用的なハードウェア、あるいはクラウド上で実現する。	・セキュリティ対策 ・コスト削減
5	ゼロタッチプロビジョニング	通信システムや情報システムの設定を自動的に行う。	・運用効率化 ・アジリティ改善

4. SD-WAN におけるセキュリティ対策の検討

ネットワーク利用上の各問題に対して施策を適用することで対策が可能か検討する。

(1)ネットワーク経由のウイルス感染拡大防止

ネットワークを経由したウイルス感染拡大防止策として、ウイルスが感染に利用する通信をネットワーク機器で遮断する方法がある。従来の WAN ではネットワーク担当者がネットワーク機器毎にログインし、ネットワークアクセス制御設定を実施する必要がある。本提案では、SD-WAN コントローラーからネットワークアクセス制御設定を一括配布することで設定反映までの時間短縮を図る。

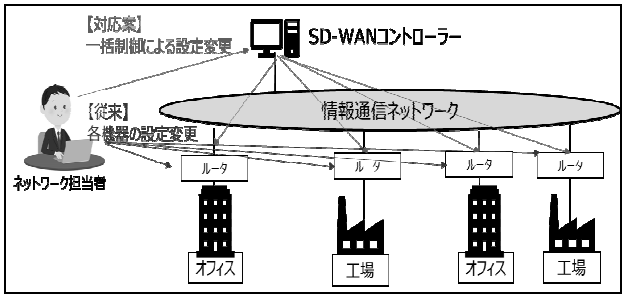

図 4-1 SD-WAN コントローラーによる設定

(2)インターネット利用時の Web アクセスセキュリティ強化

SD-WAN では、オフィス、工場等に設置した SD-WAN ルータから直接インターネットにアクセス可能となる。専用回線とインターネット回線を併用するネットワーク構成で、インターネットブレークアウト機能を用いることでネットワーク帯域を効率的に利用可能となるが、URL フィルタリング、Web ウイルスチェック等のセキュリティ機能は集中管理することで運用管理工数を下げる必要がある。

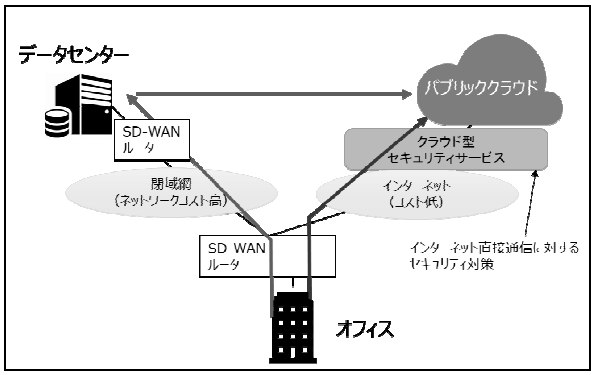

図 4-2 インターネット接続セキュリティ強化

5. SD-WAN の課題

SD-WAN は新しい技術であり、以下のような課題も出てきている。

(1)障害対応が複雑化

ネットワーク障害が発生した場合、従来ネットワークのアンダーレイ部分に加えて、オーバーレイ部分の調査も必要となり、障害対応が複雑化する。オーバーレイ部分は基本的にコントローラーの情報に基づく調査となるため、十分な情報が得られない場合は障害対応が長期化する可能性がある。

(2)メンテナンスによるネットワーク停止の増加

コントローラーのメンテナンスに伴いネットワーク停止、一部機能制限等が発生する。また、ソフトウェアアップデートを頻繁に実施する環境においては、ネットワーク停止頻度が増加する。

6. まとめと今後の予定

本稿では、SD-WAN を導入する企業のセキュリティ対策として、SD-WAN コントローラーからの設定一括配布によるネットワークアクセス制御設定の迅速化、及びクラウド型セキュリティサービスを利用した Web アクセスセキュリティ強化の可能性を示した。

今後は本提案について、検証環境を用いて有用性・実効性の検証を実施し、SD-WAN における最適なセキュリティ対策を提案する。

参考文献

[1] 総務省 平成 28 年通信利用動向調査
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html
[2] Open Networking User Group (ONUG)
http://opennetworkingusergroup.com/
[3] 総務省 情報通信白書(平成 29 年度版)

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.