1ZD-03

企業ネットワークにおける SDN 利用のセキュリティ課題と対策の評価

杉本久美† 後藤厚宏†
情報セキュリティ大学院大学†

1. はじめに

近年の企業ネットワークは，構成変更を重ねてきたネットワークが複雑化していること，大規模なネットワークではポリシー変更の運用コストが高いこと，ネットワークの構築に時間がかかることなどのネットワークの構築・運用上の課題を抱えている．加えて昨今のリモートワークの普及により，企業ネットワーク外部からの接続においても，内部と同等のセキュリティを確保したいという新たな業務形態の導入に伴うセキュリティ上の課題が生まれている．

これらの課題の対策として，ネットワークの構築・運用上の課題には Software Defined Network (SDN)[1]が，新たな勤務形態におけるセキュリティ上の課題にはゼロトラストの考え方を用いることが有効であると考える．

SDN は，ネットワークの仮想化ができること，ソフトウェアでネットワークを制御していること，SDN コントローラで一括管理しやすい特徴を持つ．このような特徴を活用して企業ネットワークの構築・運用上の課題を解決するため，実際に SDN の導入が進んでいる．しかし，上記のような SDN の特徴は，SDN の構造上のセキュリティ課題となる．

本稿では，SDN を導入して構築・運用上の課題を解決しようとする企業ネットワークにおけるセキュリティ課題を明らかにし，その対策を考察する．

2. SDN を導入した企業ネットワークのセキュリティ課題

本稿では図 1 のような企業ネットワークにおいて解決すべきセキュリティ課題を考える．

課題①：企業ネットワークにおける境界型防御の課題

リモートワークの普及に伴い，従来の境界型防御では十分にセキュリティが確保できなくなってきている．そこで，境界の内外に関係なくすべてを信用しないというゼロトラストが注目されている．

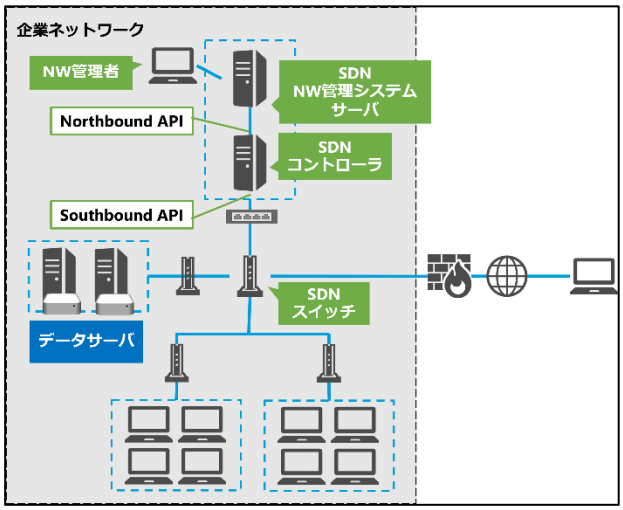

図 1 SDN を導入した企業ネットワーク

課題②：SDN の構造上のセキュリティ課題

SDN にはアプリケーションである NW 管理システムがコントローラを制御するための Northbound API と，SDN コントローラが SDN スイッチのフローテーブルを操作するための Southbound API があり，それぞれにセキュリティ課題がある．Northbound API では，SDN コントローラでネットワーク機器を一括管理していること，Southbound API では SDN スイッチがフローテーブルに従ってデータを送信していることがボトルネックになり得ると考える．

3. 企業ネットワークの境界型防御の課題の対策

新たな業務形態におけるセキュリティ課題に対して，ゼロトラストの手段の 1 つである Software Defined Perimeter (SDP)が有効だと考える．

SDP[2]とは境界をソフトウェア上で構築し，SDP コントローラによってアクセス制御する．SDP は，接続を開始するクライアントの Initiating Host (IH)，接続を受け入れるサーバの Accepting Host (AH)，認証を行う SDP コントローラによって構成される．クライアントがサーバに接続する前に SDP コントローラによって認証することでセキュリティを確保している．

Security Challenges of Using SDN in Enterprise Networks and Evaluation of the Measures Taken
† Kumi Sugimoto, Atsuhiro Goto
† Institute of Information Security

Sallam ら[3]は SDN を導入したサービスプロバイダの企業ネットワークにおいて，SDP を用いることで企業ネットワークの外部からのアクセス制御を強化できることを示した．また BeyondCorp[4][5]は，エンドポイントのセキュリティ状態を確認し，信頼レベルを用いてアクセス制御を可能としている．

そこで図 1 の企業ネットワークに両先行事例を導入し，外部からの通信と同様に内部からの通信についても SDP でアクセス制御することで，データサーバなどのリソースを保護することを考える．ただし，SDP コントローラによる IH の認証に，デバイスの状態のようなエンドポイントの状態を確認できるよう適切な認証情報を用いる必要がある．

4. SDN の構造上のセキュリティ課題の対策

SDN の構造上のセキュリティ課題を明確にするために，STRIDE による脅威分析を行い，以下の知見を得た．

(1) SDN の Northbound API の防御

SDN は SDN コントローラでネットワークを一括管理しているため，Northbound API では SDN コントローラを攻撃者に操作されないよう保護する必要があることがわかった．これには，まずは NW 管理者アカウントの ID/PW の適切な管理や管理 PC のマルウェア対策といった従来の対策を行うことが重要である．さらに NW 管理者のユーザ認証や SDN コントローラの認証といったアクセス制御の強化が必要である．

アクセス制御の強化策としてコントローラ DAC[6]が提案されている．コントローラ DAC は NW 管理システムから SDN コントローラへのリクエスト内容を見て，認証と認可，正当性の確認し，正当な NW 管理システムからの通信しか許可しない強化策である．

(2) SDN の Southbound API の防御

SDN スイッチは自身が持つフローテーブルに従ってパケットの処理を行うため，フローテーブルが改ざんされないよう保護することが最も重要である．このため，攻撃者に企業ネットワークに侵入されないための従来の対策に加え，SDN スイッチと SDN コントローラ間の Southbound API 通信における認証を強化すべきである．

前節で述べた SDP はこのような Southbound API 防御にも有効である．具体的には，SDN コントローラに IH モジュール，SDN スイッチに AH モジュールを導入することにより，正当な SDN コントローラからの通信のみ絞ることができるにできる．

5. セキュリティ対策の統合と今後の課題

図 2 は 3 章・4 章の対策技術を SDN ネットワークに統合したものである．IH①，AH①，SDP コントローラは，ゼロトラストを考慮したセキュリティ対策としてデバイスからデータサーバへのアクセスを制御するための SDP の構成要素である．そしてコントローラ DAC は SDN の Northbound API を保護し，IH②，AH②，SDP コントローラは SDN の Southbound API を保護する．

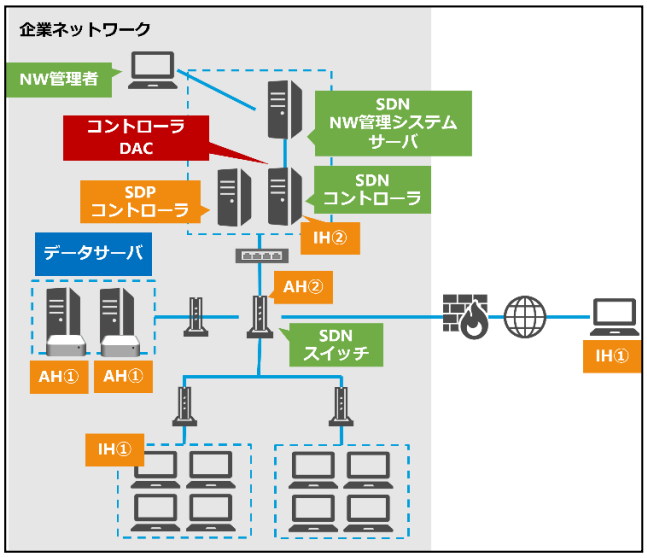

図 2　セキュリティ対策の統合

これらの対策に加え，SDN スイッチから SDN コントローラへの DoS 攻撃や SDN コントローラを複数用いたときのコントローラ同士のセキュリティ課題の解決が必要である．

参考文献

[1] ONF: Software-Defined Networking: The New Norm for Networks, https://opennetworking.org/sdn-resources/whitepapers/software-defined-networking-the-new-norm-for-networks/, (accessed 2021-05-18).
[2] cloud security alliance: SDP Architecture Guide v2, CSA, https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/ (accessed 2021-08-27).
[3] Sallam, A., Refaey, A. and Shami, A.: On the Security of SDN: A Completed Secure and Scalable Framework Using the Software-Defined Perimeter, in IEEE Access, Vol.7, pp. 146577-146587 (2019).
[4] Ward, R. and Beyer, B.: BeyondCorp: A New Approach to Enterprise Security, ;login:, Vol.39, No.6, pp.6-11 (2014).
[5] Osborn, B., Mcwilliams, J., Beyer, B., et al.: BeyondCorp: Design to Deployment at Google, ;login:, Vol.41, No.1, pp.28-34 (2016).
[6] Tseng, Y., Pattaranantakul, M., He, R., et al.: Controller DAC: Securing SDN controller with dynamic access control, *In 2017 IEEE International Conference on Communications (ICC)*, pp.1-6 (2017).