SDNを導入した企業ネットワークのセキュリティ課題と対策の考察

Security Challenges and Measures on SDN Enterprise Networks

杉本久美・ネットワーク分科会・情報セキュリティ大学院大学

SDN is an effective solution to the problems of network construction and operation, which are the issues of today's enterprise networks. Therefore, I clarified security challenges and considered measures on SDN enterprise networks. I showed that access control such as SDP is effective.

研究背景と目的

- 近年の企業ネットワークの課題
  - ネットワークの構築・運用上の課題
    （構成変更を重ねることによりネットワークが複雑化、ネットワークの運用コストの増加など）
  - リモートワークの普及によるセキュリティ課題

  → **SDN** (Software Defined Network)が有効
  しかしSDNはセキュリティ上の課題を有する
- SDNを導入した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、対策を考察する

SDNの概要

- データ転送機能を切り離して制御機能を集約しており
- 主にSDNアプリケーション、SDNコントローラ、SDNスイッチで構成される
- SDNアプリケーションとSDNコントローラ間はNorthbound APIによって、SDNコントローラとSDNスイッチ間はSouthbound APIによって通信する

SDNを導入した企業ネットワークのセキュリティ課題と対策

課題 1：境界型防御では十分にセキュリティを確保できない

課題 2：SDNのNorthbound APIにおける攻撃者にSDNコントローラを操作される脅威

課題 3：SDNのSouthbound APIにおけるSDNコントローラからSDNスイッチへのOpenFlowメッセージの改ざんの脅威

課題 4：SDNのSouthbound APIにおけるSDNスイッチからSDNコントローラへのPacket Inメッセージによる DoS攻撃の脅威

対策 1：ゼロトラスト実現手段の１つである**SDP**を導入することで、接続前にデバイスの検証を行う

対策 2：**コントローラDAC**によってNW管理システムからSDNコントローラへの通信を検証し、正常な通信のみSDNコントローラへ送信する

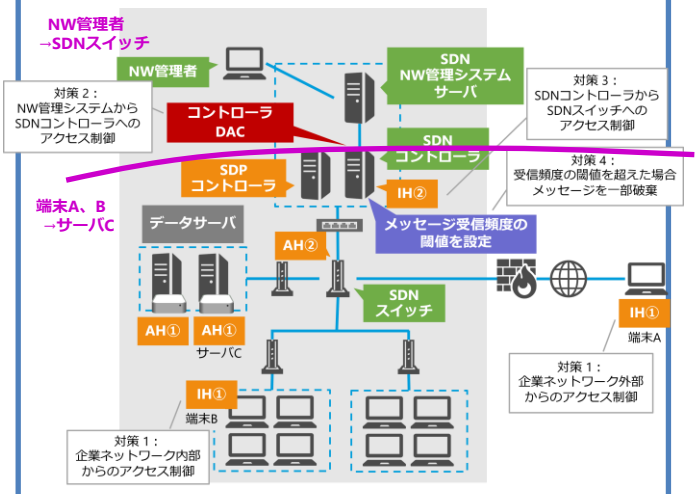
対策 3：SDNコントローラからSDNスイッチへのアクセスを**SDP**によって制御することで、正常なSDNコントローラのみ通信を許可する

対策 4：SDNコントローラのPacket Inメッセージの受信頻度が事前に決めた**閾値**を超えた場合、一部のPacket Inメッセージを破棄する

対策の統合

対策1～4について、SDNを導入した企業ネットワークに図のように統合する。

端末Aや端末Bからサーバ Cへのアクセスは、対策1と対策4によってセキュリティが確保できることを示す。
また、NW管理者がSDNスイッチに指示するときは対策2と対策3によってセキュリティが確保できることを示す。



すべての通信をSDPコントローラで認証することでSDPコントローラに負荷がかかることや、端末からサーバへのアクセスまでに遅延が発生する可能性があることは今後の課題である。