修論審査

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

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

2022.02.12

後藤研　杉本久美

研究概要

近年の企業ネットワークの課題

リモートワークの普及による
セキュリティ課題

ネットワークの構築・運用上の課題
（複雑化したネットワーク構成や
運用コストの増加）

SDNが有効
しかしSDNはセキュリティ課題を有する

対策①：
SDPによる企業ネットワーク
内外からのアクセス制御

対策②：**コントローラDAC**によるNW管理システム
からSDNコントローラへのアクセス制御
対策③：**SDP**によるSDNコントローラからSDN
スイッチへのアクセス制御
対策④：SDNコントローラの**Packet Inメッセージの**
受信頻度の閾値によるDoS対策

SDNのデータ層、コントローラ層でそれぞれ組み合わせて使えることを示す

SDNとは

Software Defined Networking

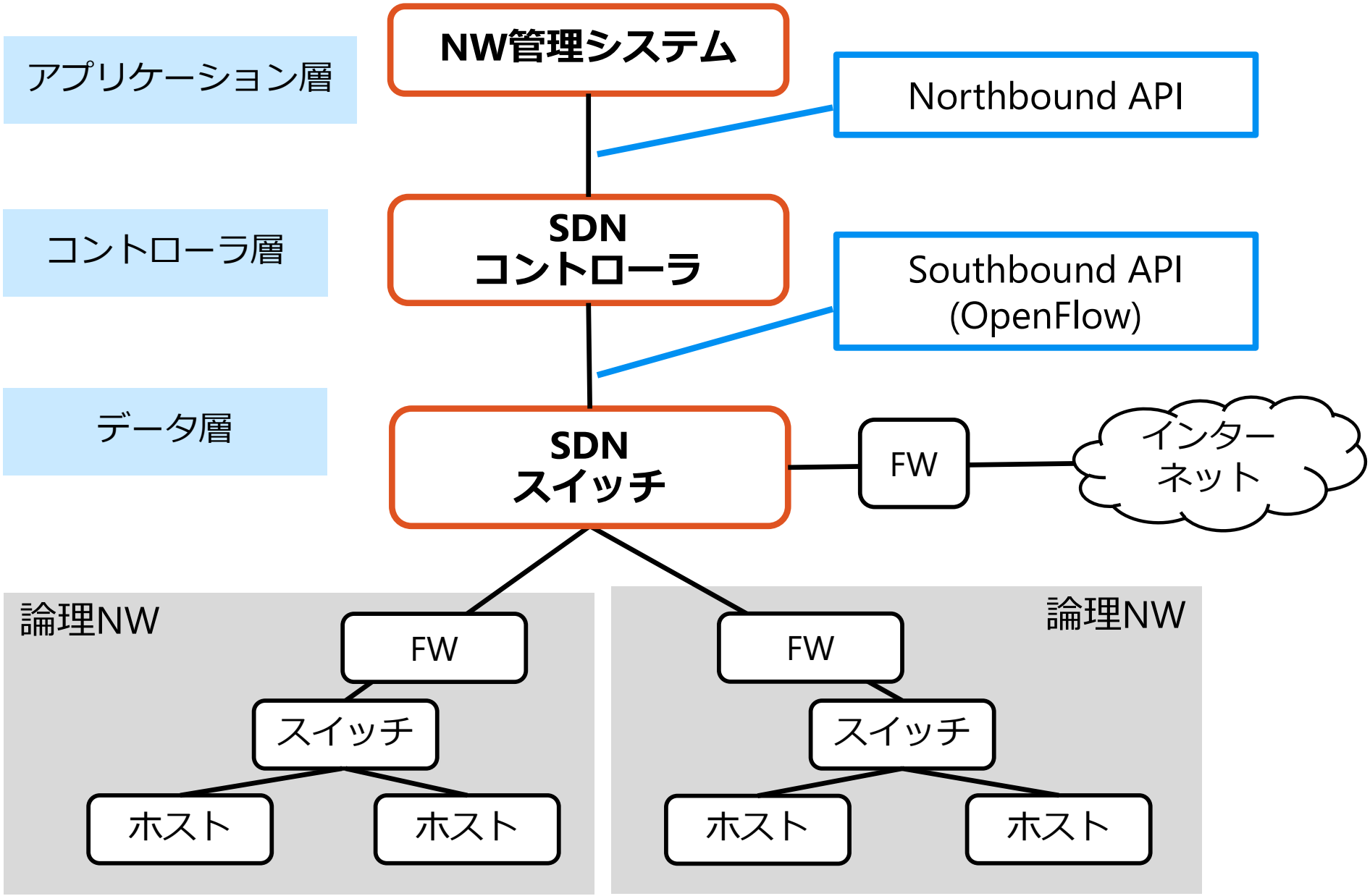
ソフトウェアによって動的にネットワークを構成

- 機器のデータ転送機能と制御機能を分離
- 制御機能をSDNコントローラで集中管理
  （全体像の把握、設定を一括で変更）

従来のネットワーク

- 1つの機器がデータ転送機能と制御機能を持つ
- 機器同士で情報を交換
- 個々に設定を行う

SDNとは


アプリケーション層
NW管理システム
Northbound API
コントローラ層
SDN
コントローラ
Southbound API
(OpenFlow)
データ層
SDN
スイッチ
FW
インター
ネット
論理NW
FW
スイッチ
ホスト
ホスト
論理NW
FW
スイッチ
ホスト
ホスト

SDNによる対策

企業ネットワークの構築・運用上の課題	SDNの特徴
① 複雑化したネットワーク構成 ② 分離されたネットワーク間の相互アクセス	ネットワークの仮想化
③ ネットワーク構成の柔軟性・構築の迅速性	ソフトウェアでネットワークを制御
④ 運用コストの削減 ⑤ 運用の簡素化 ⑥ ネットワークキャパシティの強化	SDNコントローラでネットワーク機器を一括管理

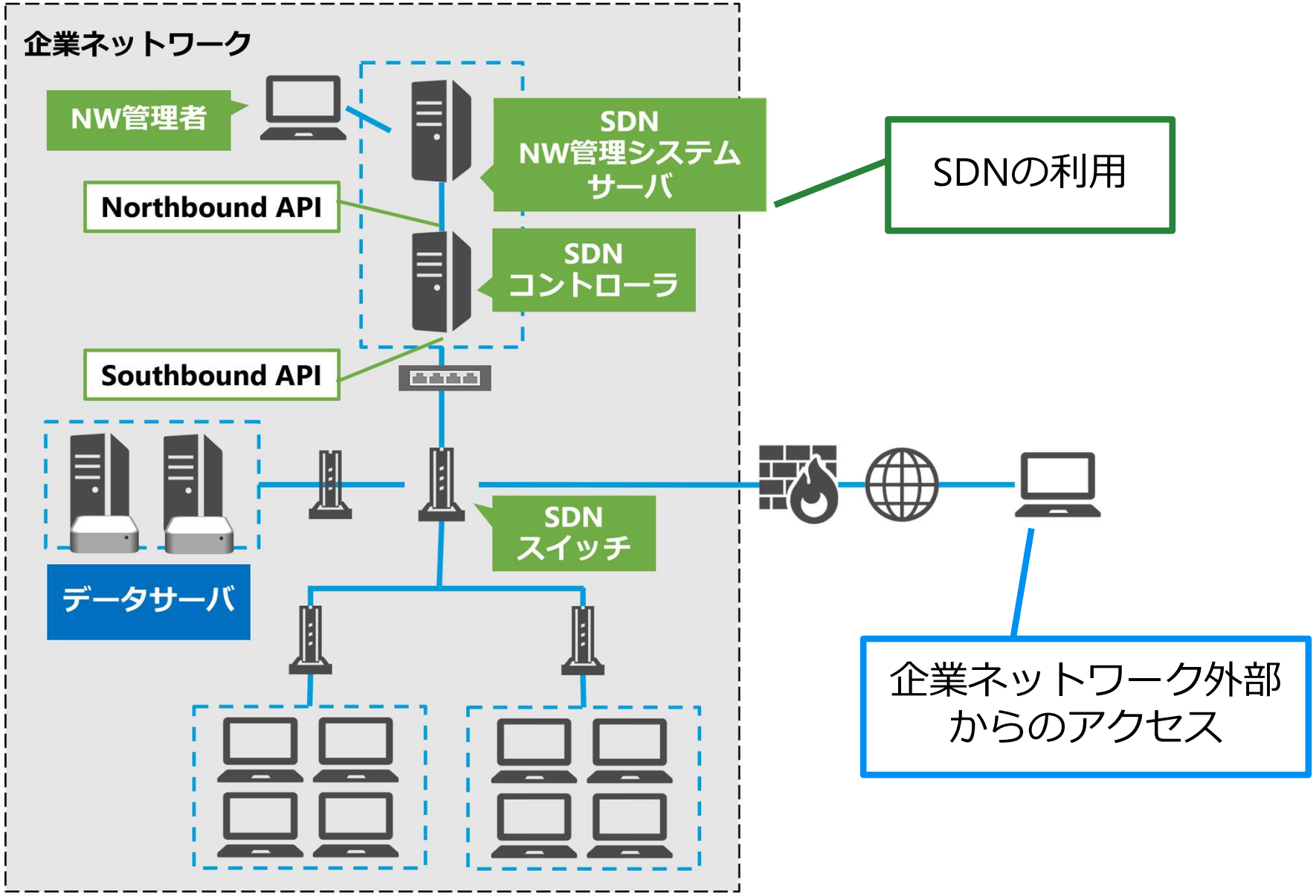
SDNの導入事例

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

	オフィスA	オフィスB	オフィスC	オフィスD	大規模オフィス	工場A	工場B	工場C	データセンタ（自社）	データセンタ（プロバイダ）
複雑化したNW構成	●				●					
NW間の相互アクセス				●		●	●	●		
柔軟性・迅速性		●	●	●	●			●		●
運用コスト削減					●				●	●
運用の簡素化	●	●		●		●	●	●	●	
NWキャパシティの強化									●	●

→企業ネットワークの構築・運用上の課題はSDNでの解決が期待

SDNを導入した企業ネットワーク



SDNを導入した企業ネットワークのセキュリティ課題①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

企業ネットワークにおける境界型防御の限界

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情報資産へのアクセス
- 私物PCの利用が増加

境界型防御では一度企業ネットワーク内に侵入されると
攻撃を防ぐことが困難

ゼロトラスト：境界の内外に関係なくすべてを信用しない

SDP：ゼロトラスト実現手段の1つ
SDPによりリモートワークのセキュリティに対応できる

SDNを導入した企業ネットワークのセキュリティ課題②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

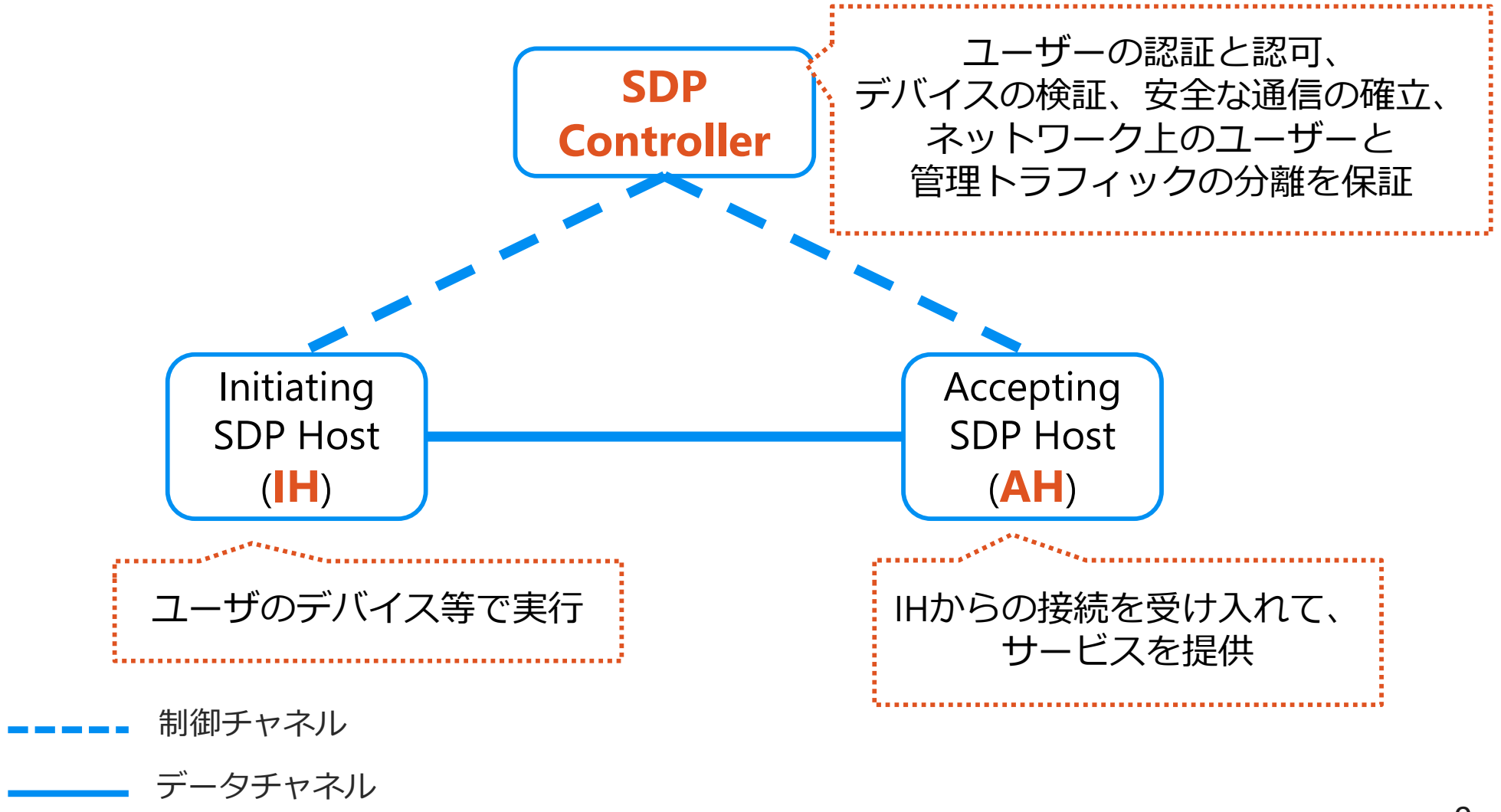
SDNの構造上のセキュリティ課題

アプリケーション層	● 権限のない人によるSDNアプリケーションの操作 ● 不正なSDNアプリケーション
コントローラ層	● SDNコントローラの乗っ取り ● SDNスイッチへの不正なフローエントリの挿入
データ層	● ホストからSDNスイッチへの不正な通信 ● フローエントリの改ざん ● フローテーブルのリソースの限界

- 先行研究でもSDNのセキュリティは取り上げられている
- STRIDE分析を行い、より重大なリスクを引き起こす脅威について対策を考察する

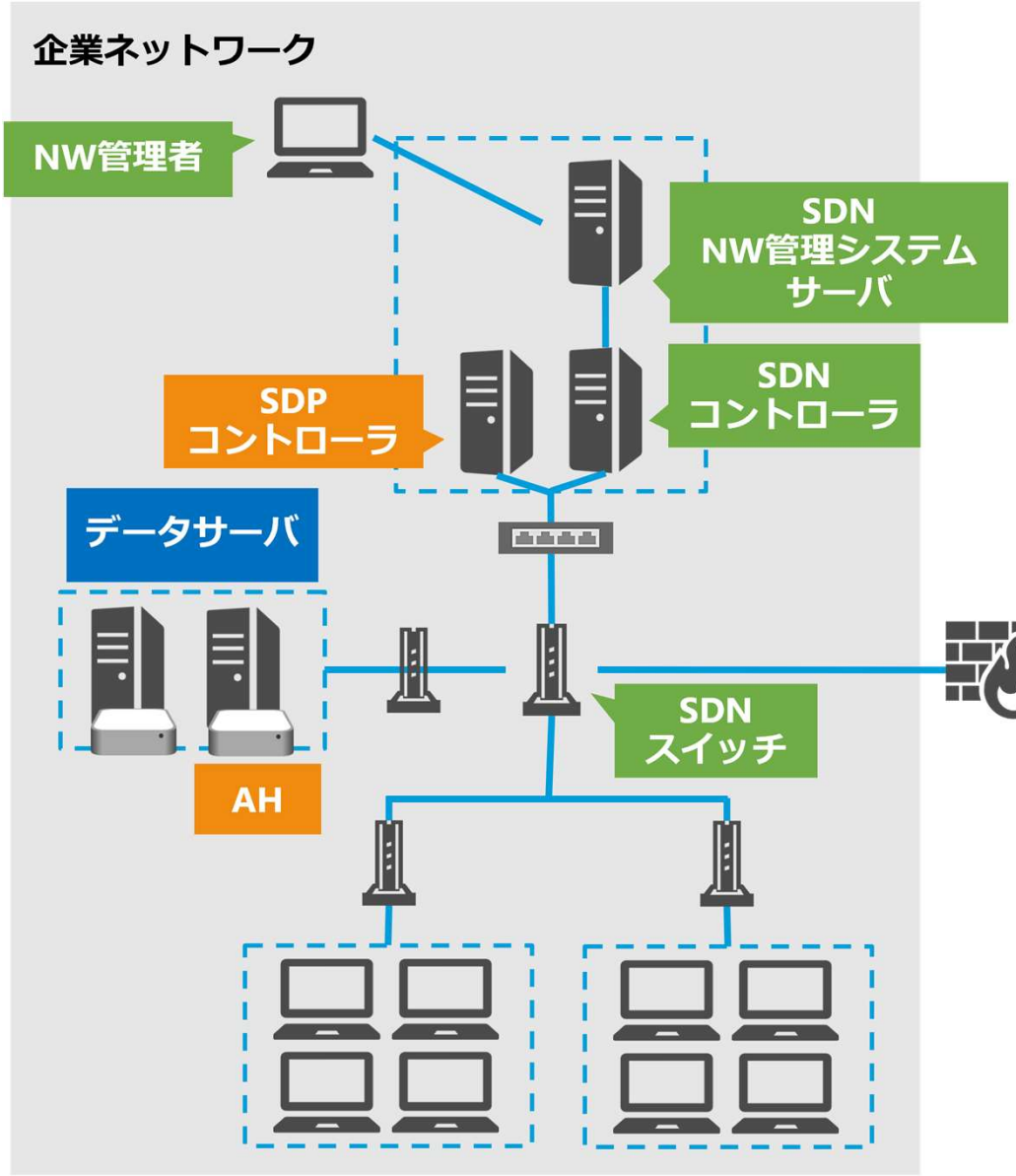
SDPの構成

境界をソフトウェア上で構築し、SDPコントローラでアクセスを制御



SDPを用いたセキュリティ強化の研究

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



On the Security of SDN:
A Completed Secure and Scalable Framework Using the Software-Defined Perimeter

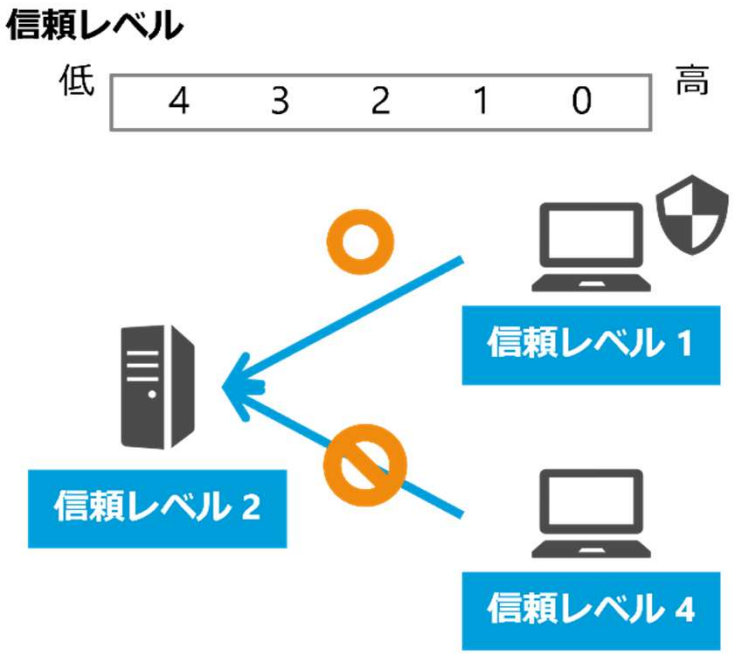
A. Sallam, A. Refaey and A. Shami, in IEEE Access (2019)

企業ネットワーク外部からのアクセスをSDPで制御

Beyond Corpのアクセス制御

- Googleが実装したゼロトラストモデル
- 企業のリソースへのアクセスはデバイスの状態とユーザの認証情報によって制御される

- ✓ 高い信頼レベルを保つには最新のバージョンにアップデートする必要があるなど、デバイスの状況に応じてアクセス制御が可能
- ✓ デバイスが信用できなくなった場合、デバイスが修復されるまで検疫ネットワークに割り当てる



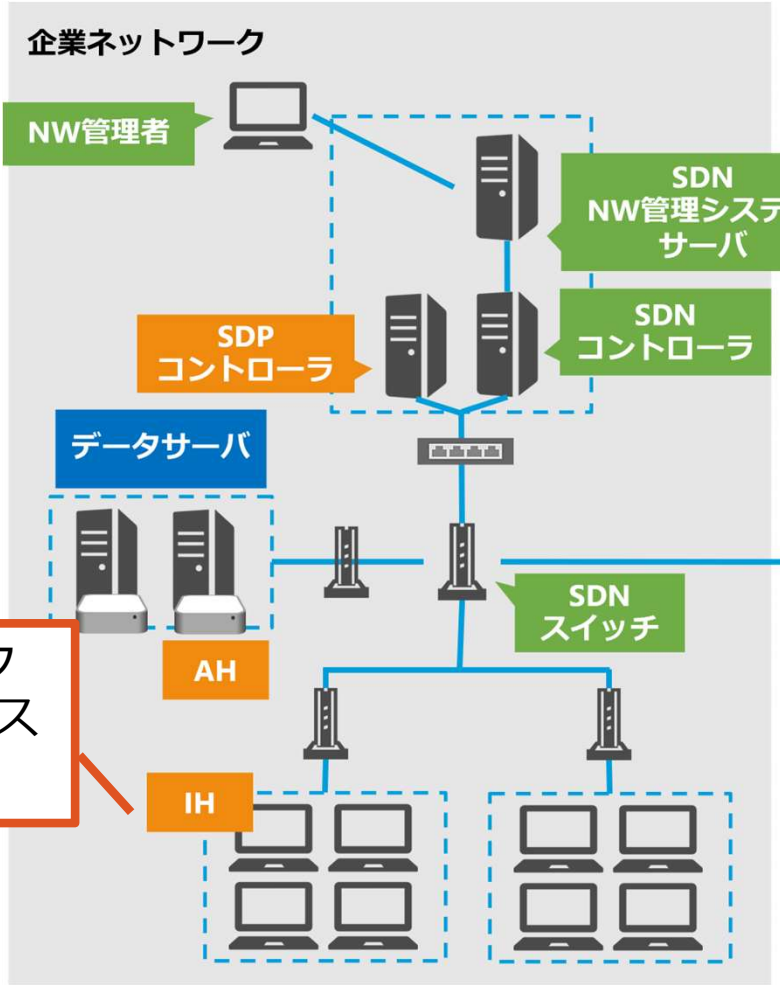
境界型防御の課題の対策　まとめ

リモートワークの普及による課題

- エンドポイントのセキュリティが重要
- 企業ネットワーク内部からのアクセスも信用できない

対策

SDPを用いて企業ネットワーク内外からのアクセスから資源を守る



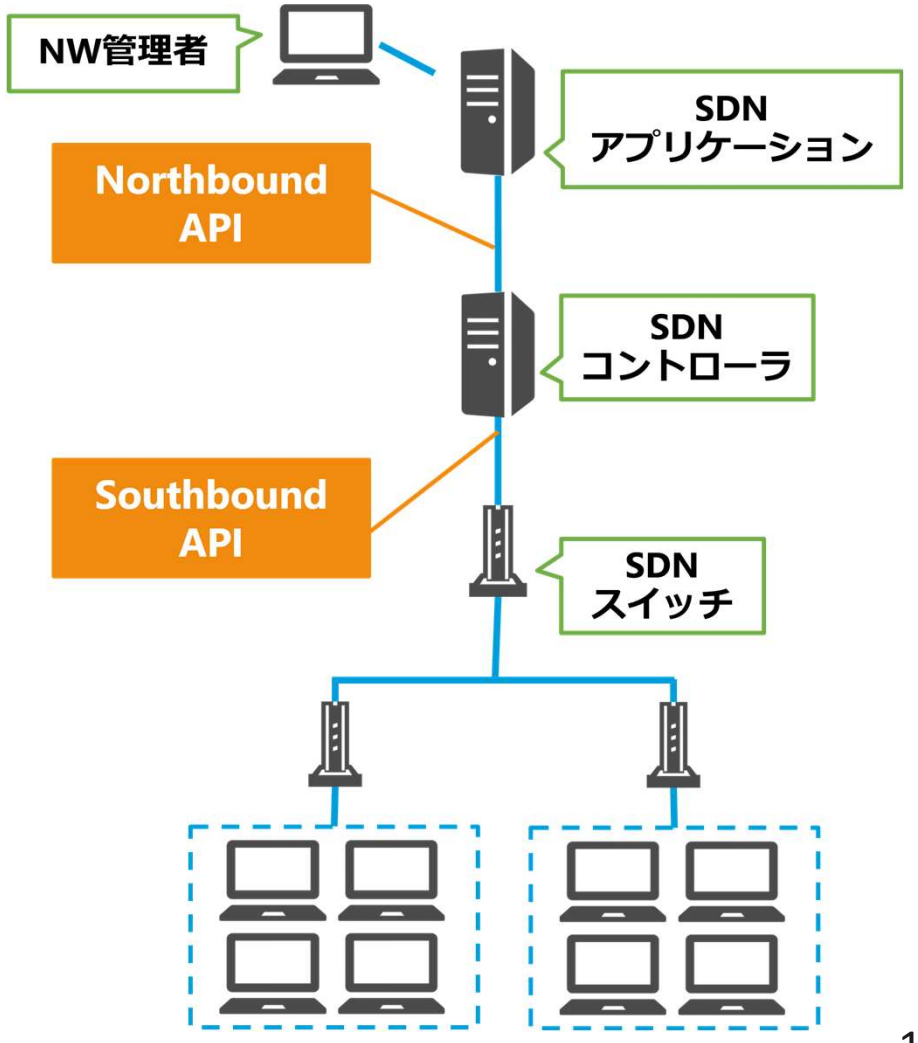
ユーザの認証やデバイスの検証によるエンドポイントのセキュリティ強化

企業ネットワーク内部からのアクセスを検証

SDNの構造上のセキュリティ課題

Northbound API、Southbound APIへの**STRIDE分析**から
想定される被害を明らかにし、対策を検討

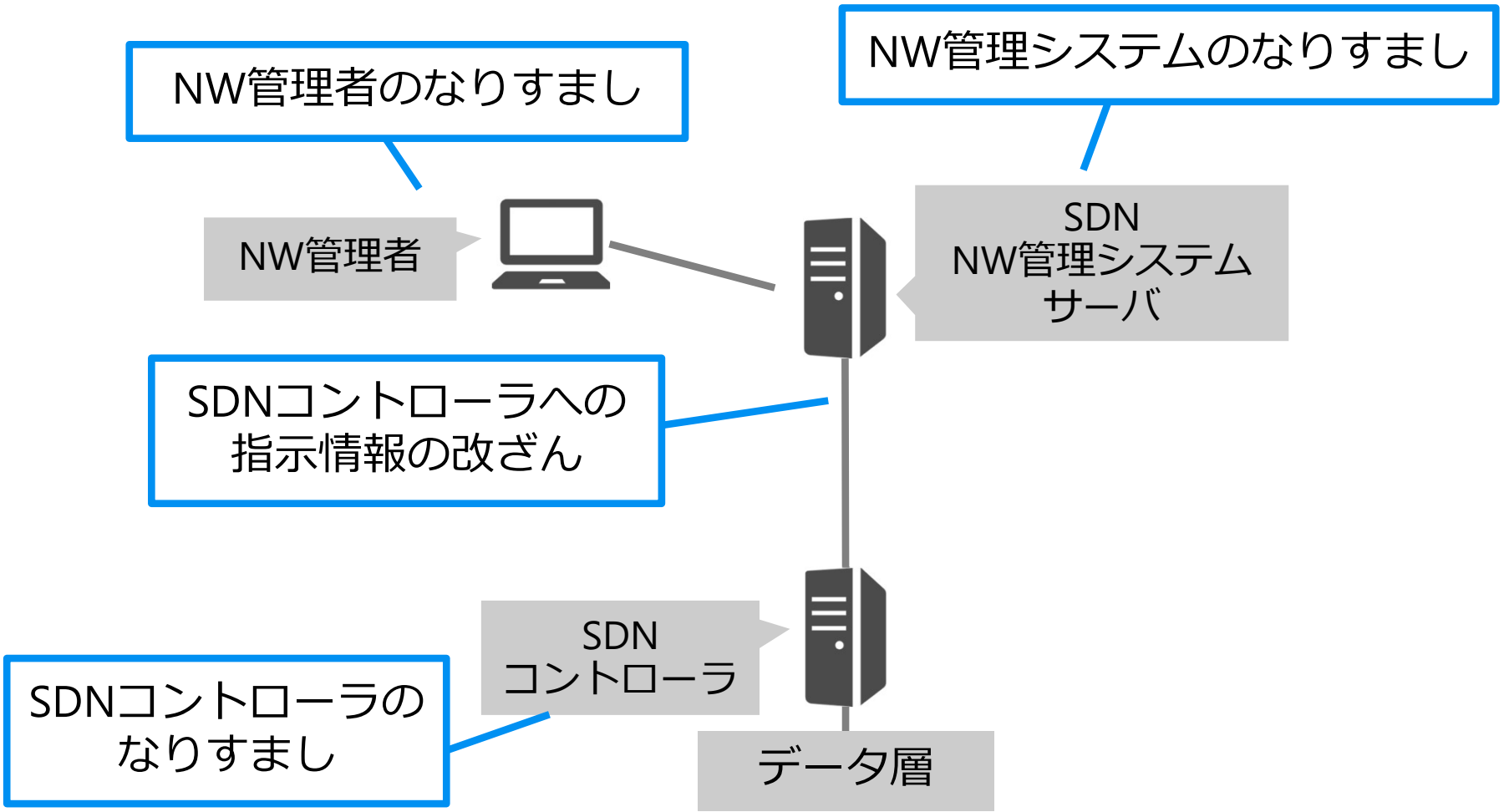
STRIDE分析
- **S**poofing (なりすまし)
- **T**ampering (改ざん)
- **R**epudiation (否認)
- **I**nformation Disclosure (情報漏洩)
- **D**enial of Service (サービス妨害)
- **E**levation of Privilege (権限昇格)



Northbound APIのセキュリティ対策

攻撃者によるSDNコントローラの操作

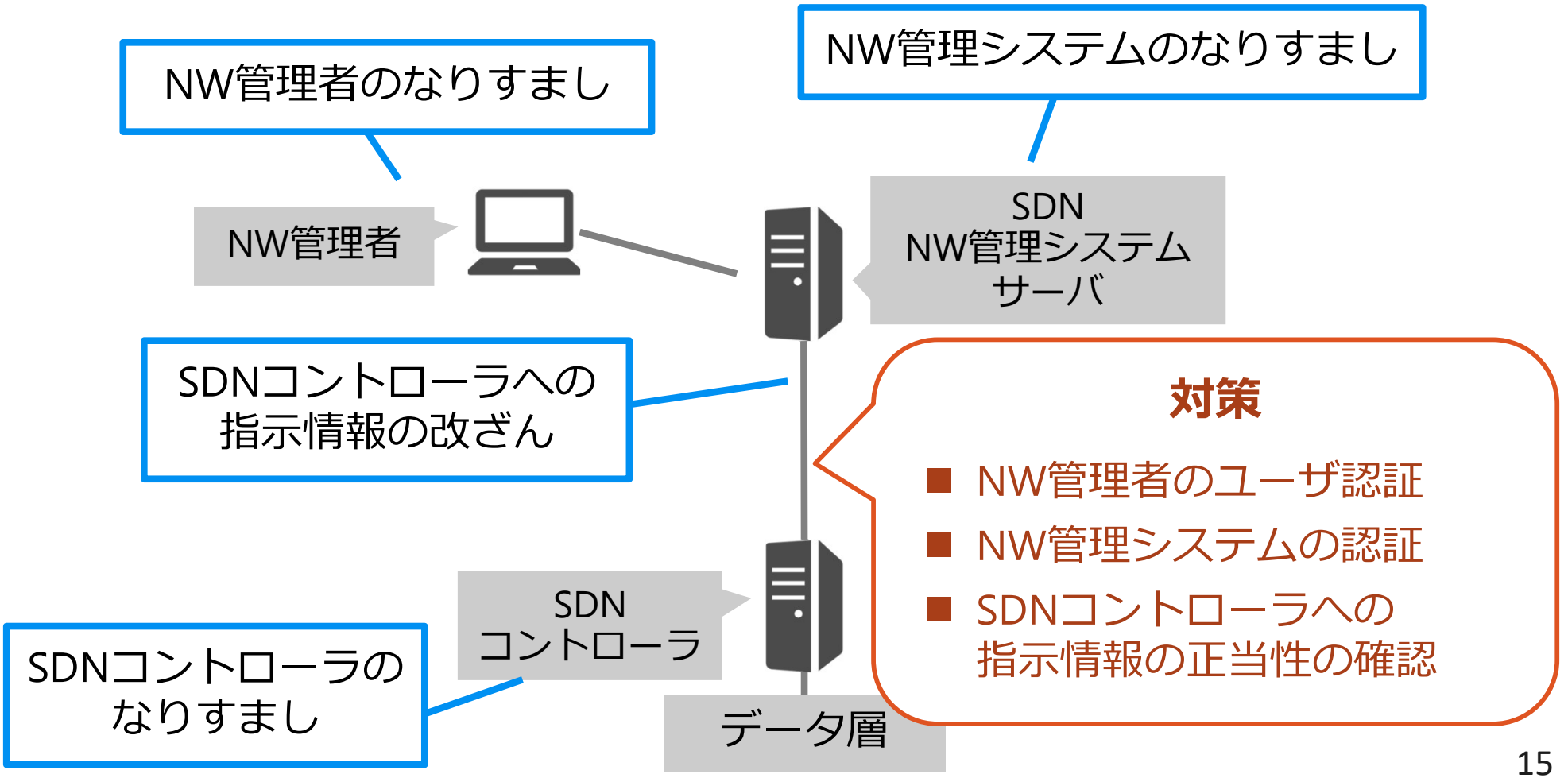
→任意のフロールールをSDNスイッチに送信できるため、
企業ネットワーク全体が脅かされる



Northbound APIのセキュリティ対策

攻撃者によるSDNコントローラの操作

→任意のフロールールをSDNスイッチに送信できるため、
企業ネットワーク全体が脅かされる

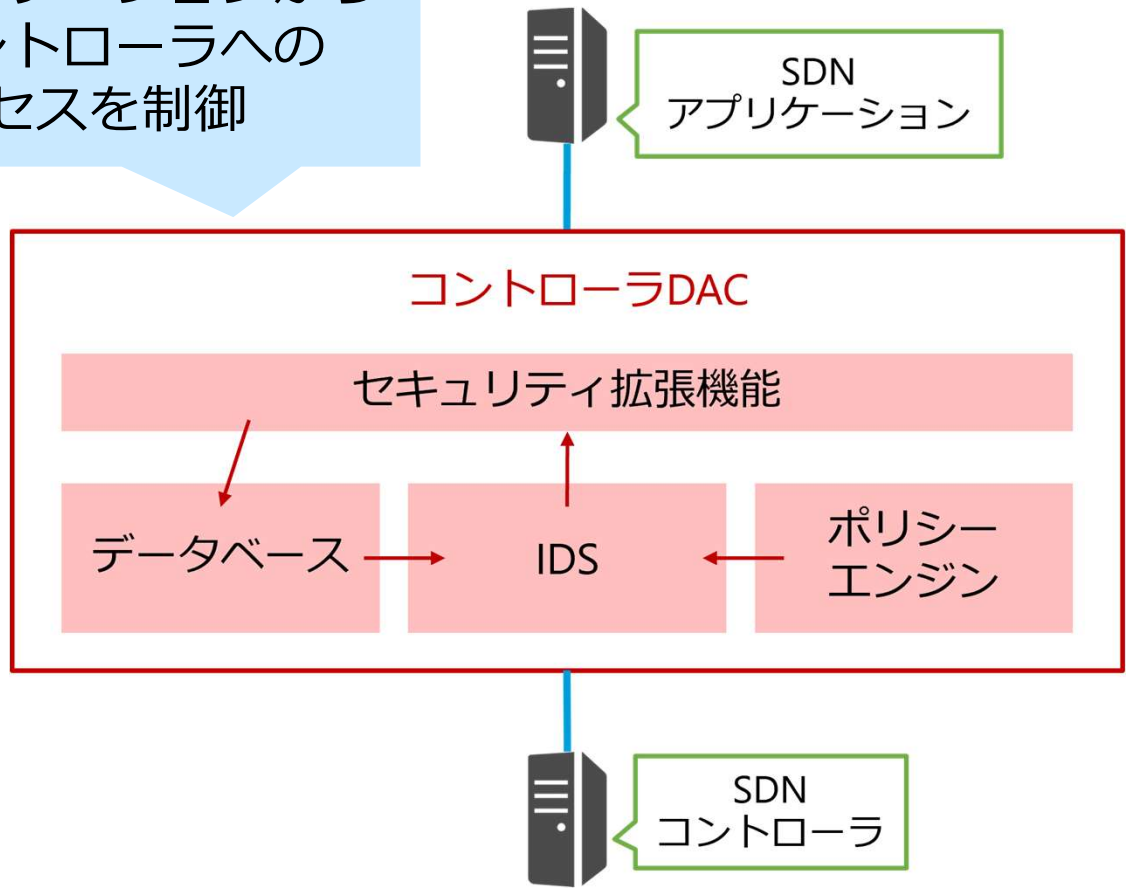


Northbound APIのアクセス制御

Controller DAC: Securing SDN controller with dynamic access control

Tseng, Y., Pattaranantakul, M., He, R., et al, in IEEE Access (2017)

SDNアプリケーションから
SDNコントローラへの
アクセスを制御



Northbound APIの対策　まとめ

課題
攻撃者によるSDNコントローラの操作

対策
コントローラDACの導入

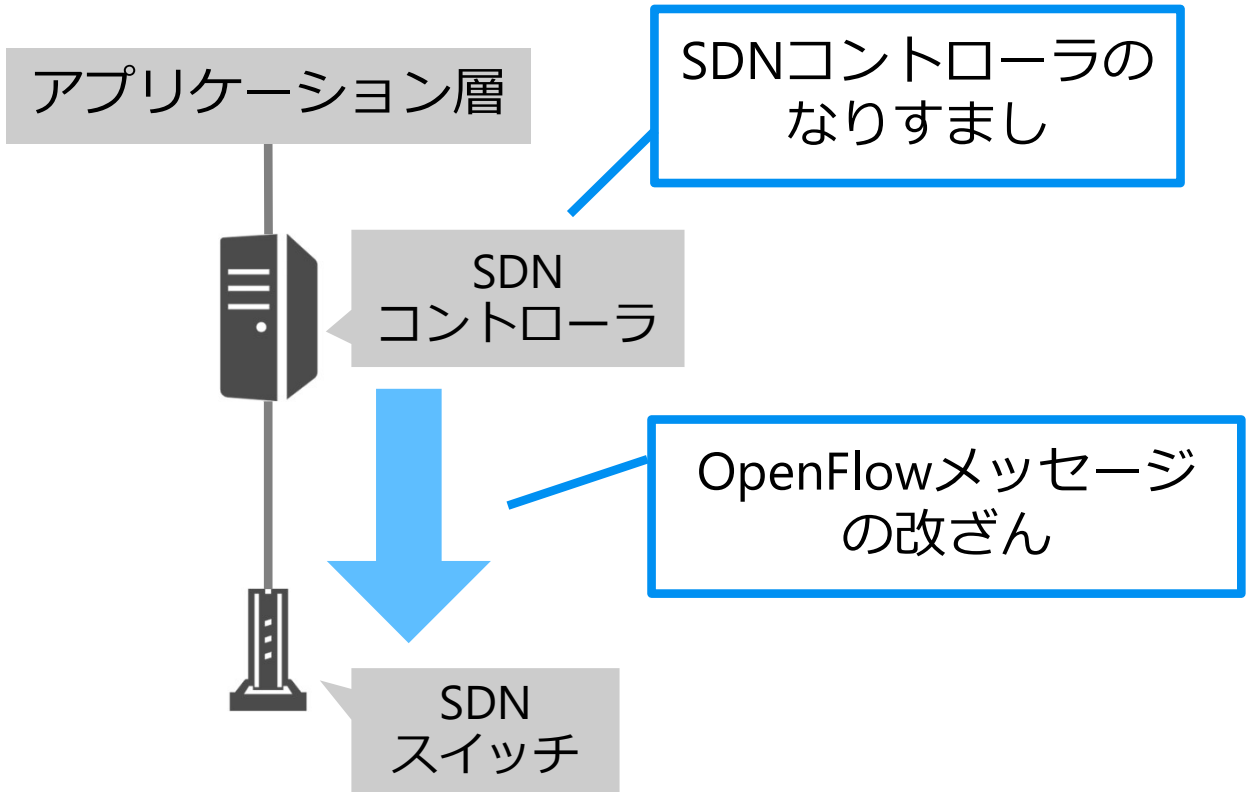
脅威	コントローラDACによる対策
NW管理システムのなりすまし	NW管理システムの認証
SDNコントローラへの指示情報の改ざん	不正な通信の検知
NW管理者のなりすまし	NW管理者の認証はNW管理システムによって行われる
SDNコントローラのなりすまし	×（コントローラDACが保護するの対象外）

- コントローラDACを導入してアクセス制御や通信内容の正当性の確保が可能になる
- ただしコントローラDACのポリシーエンジンの設定が重要

Southbound APIのセキュリティ対策①

SDNスイッチが持つフローテーブルの改ざん

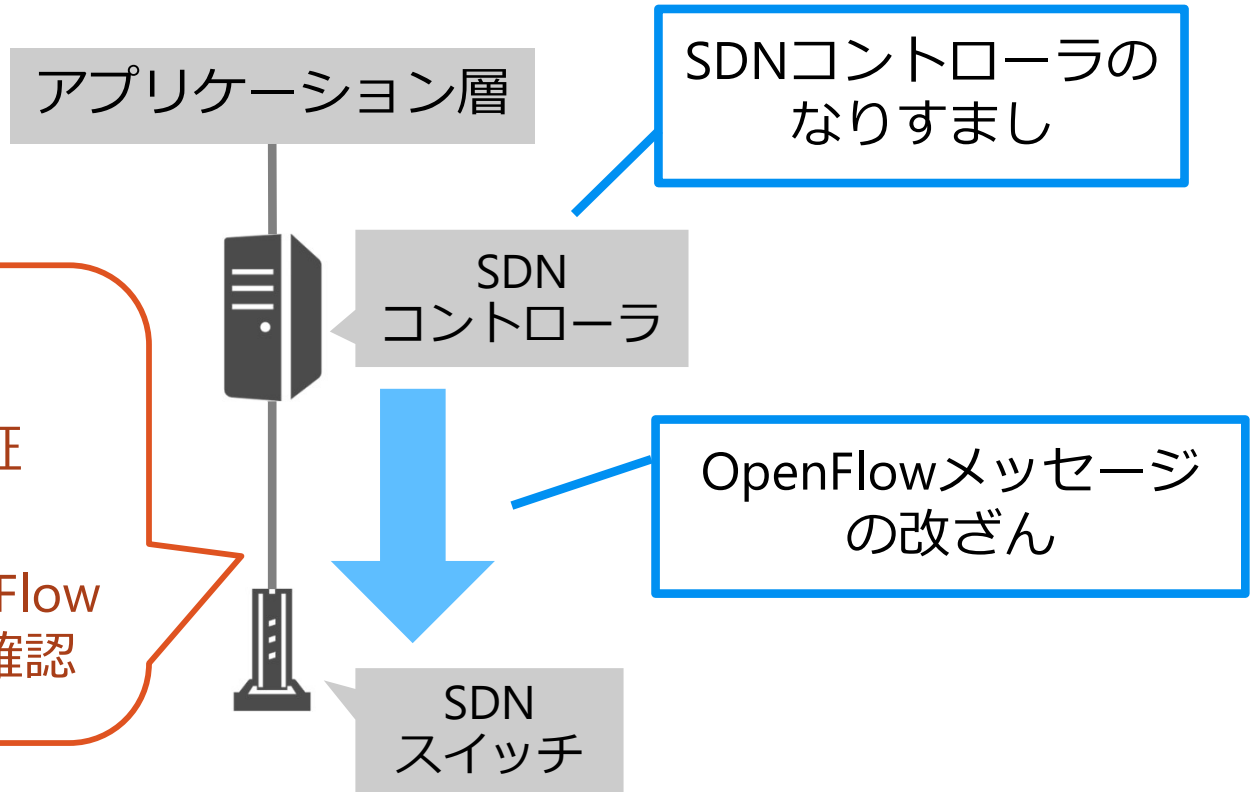
→パケットが正常に処理されないため、
ネットワークの混乱や情報漏洩が起こる



Southbound APIのセキュリティ対策①

SDNスイッチが持つフローテーブルの改ざん

→パケットが正常に処理されないため、
ネットワークの混乱や情報漏洩が起こる



対策

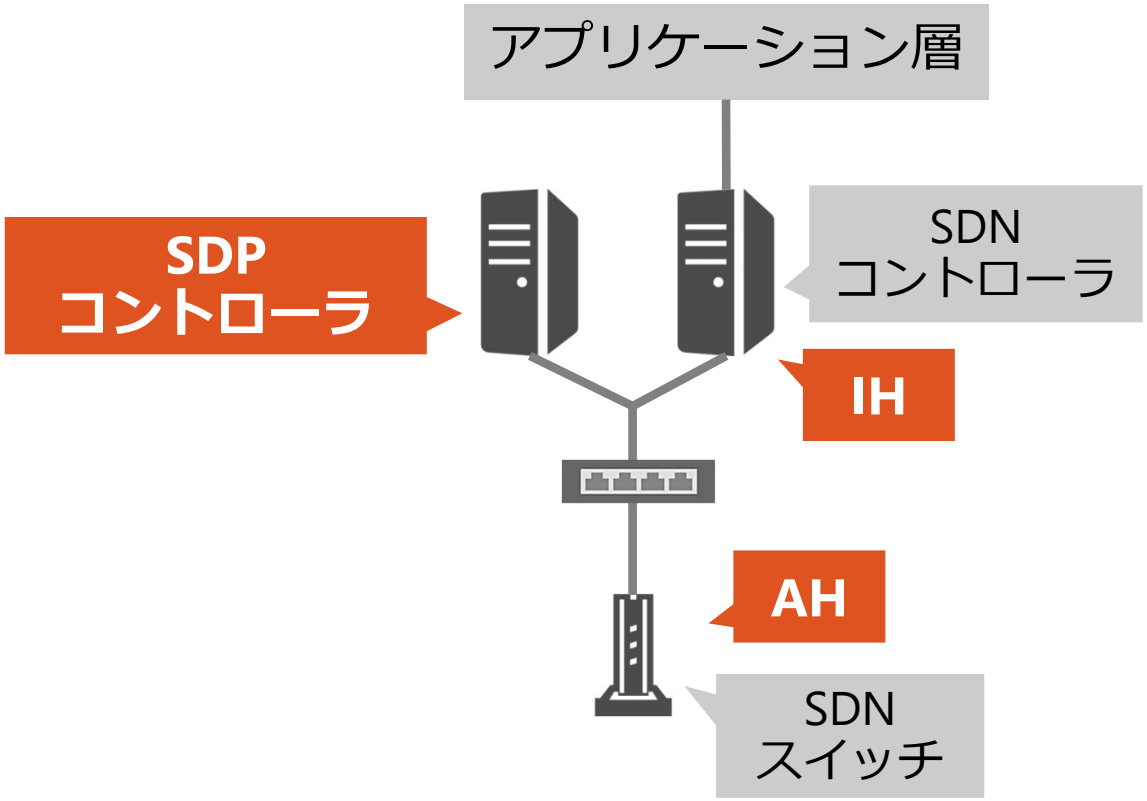
- SDNコントローラの認証
- SDNコントローラからSDNスイッチへのOpenFlowメッセージの正当性の確認

SDNコントローラからスイッチへのアクセス制御

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

SDPによるSDNスイッチの保護

SDPにより**SDNコントローラを認証してからSDNスイッチに**
アクセスすることで、不正なSDNコントローラからのアクセスを防ぐ

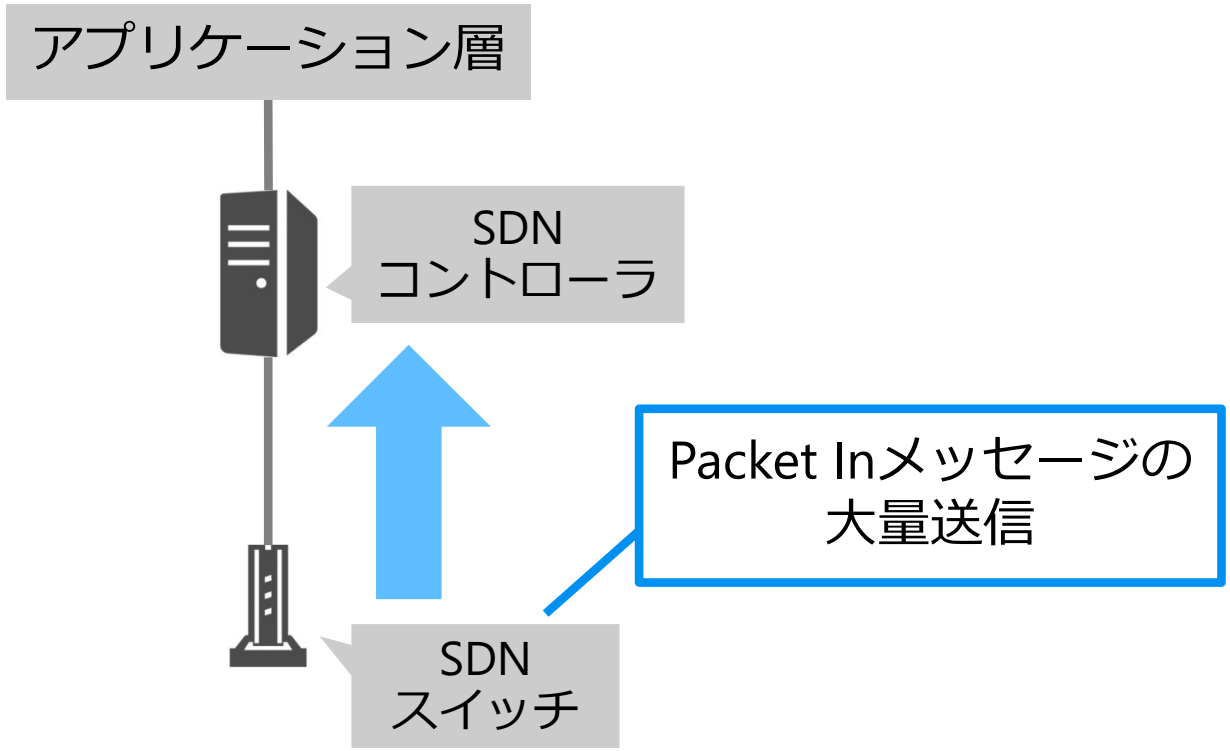


Southbound APIのセキュリティ対策②

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

- ✓ Packet Inメッセージ…SDNスイッチがフローテーブルの条件に合致しないパケットを受け取った時に**SDNコントローラに問い合わせを行う**OpenFlowメッセージ
- ✓ ユーザデバイスはそのようなパケットをSDNスイッチに送ることで攻撃できる

→これによりSDNコントローラは機能停止



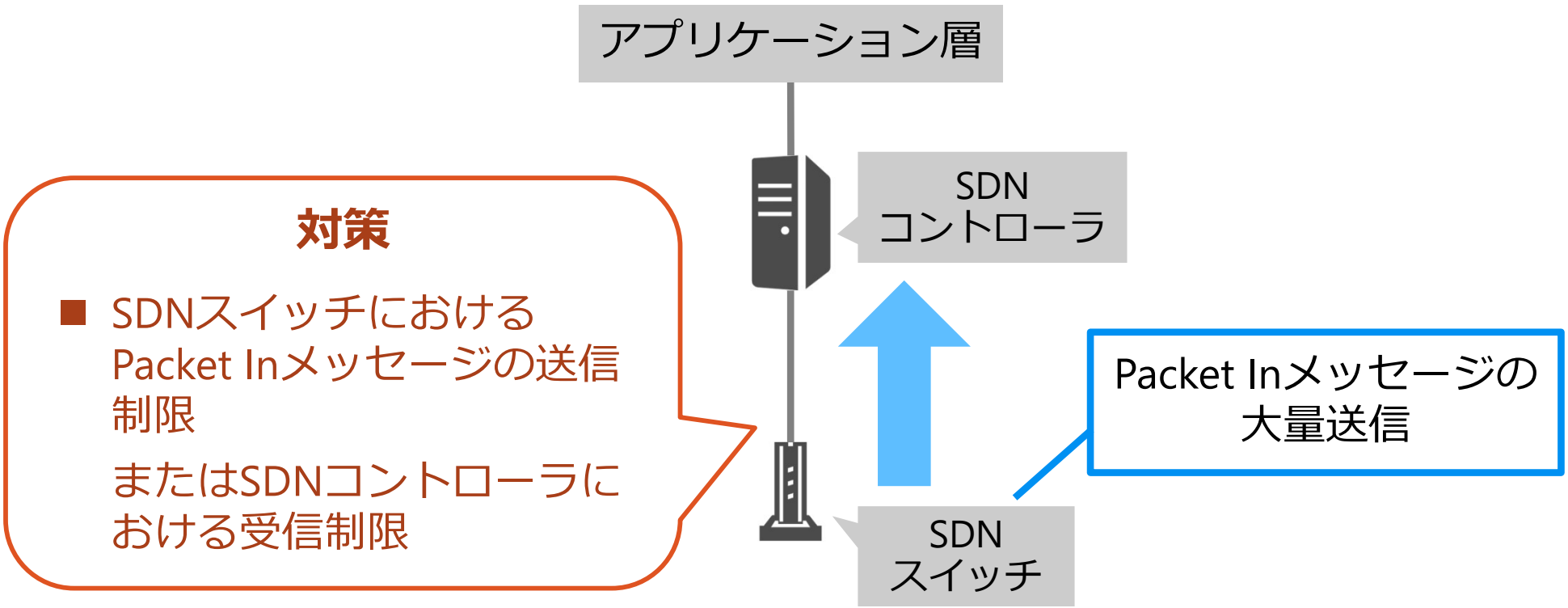
Southbound APIのセキュリティ対策②

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

Packet Inメッセージ…SDNスイッチがフローテーブルの条件に合致しないパケットを受け取った時にSDNコントローラに問い合わせを行うOpenFlowメッセージ

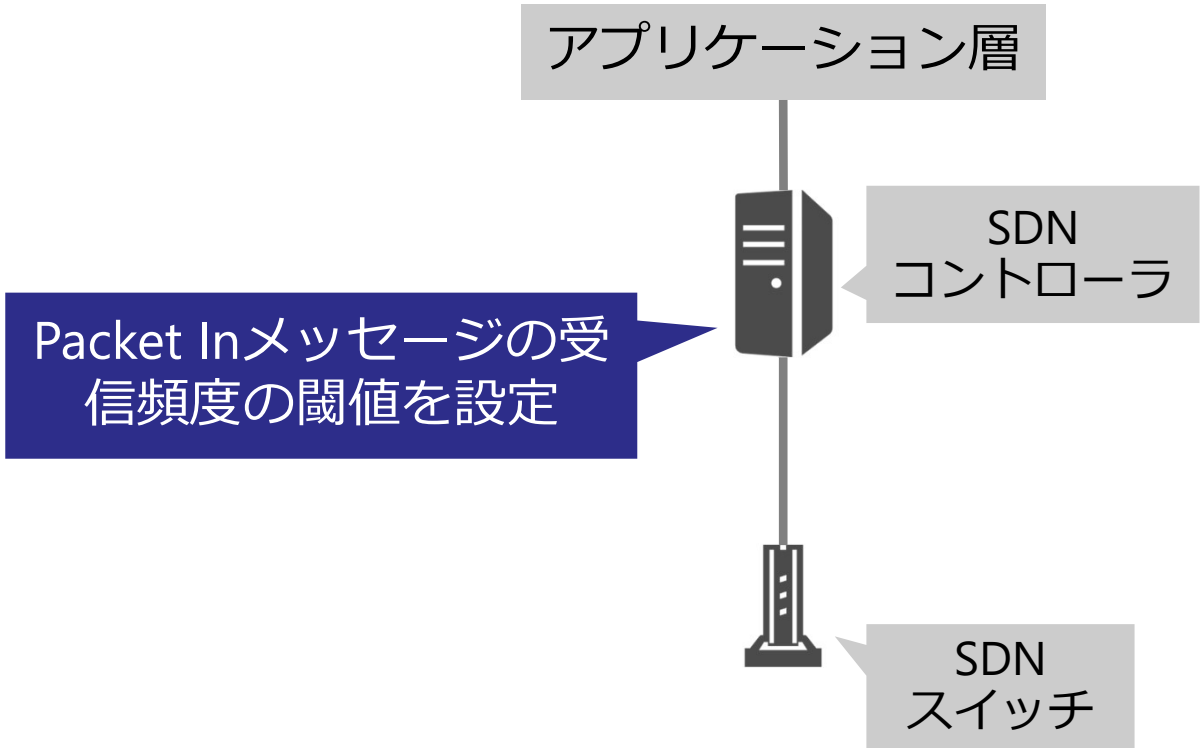
ユーザデバイスはそのようなパケットをSDNスイッチに送ることで攻撃する

→これによりSDNコントローラは機能を一部停止



SDNコントローラからスイッチへのアクセス制御

SDNコントローラにおいてPacket Inメッセージの受信頻度の閾値を設定
閾値を超えたらPacket Inメッセージの一部を破棄



Southbound APIの対策　まとめ

課題

- フローテーブルの改ざん
- SDNコントローラへのDoS攻撃

対策

- SDPを用いたSDNコントローラからSDNスイッチへのアクセス制御
- Packet Inメッセージの受信頻度の閾値制御

脅威	SDP、Packet Inメッセージの受信頻度の閾値の設定による対策
SDNコントローラのなりすまし	SDPによるSDNコントローラの認証
OpenFlowメッセージの改ざん	×、ただし暗号化など従来の対策が有効
Packet Inメッセージの大量送信	SDNコントローラにおけるPacket Inメッセージの受信頻度の閾値の設定

SDNスイッチのフローテーブル、SDNコントローラの保護が可能

セキュリティ課題への対策案

SDNを導入した企業ネットワークにおける課題への対策案

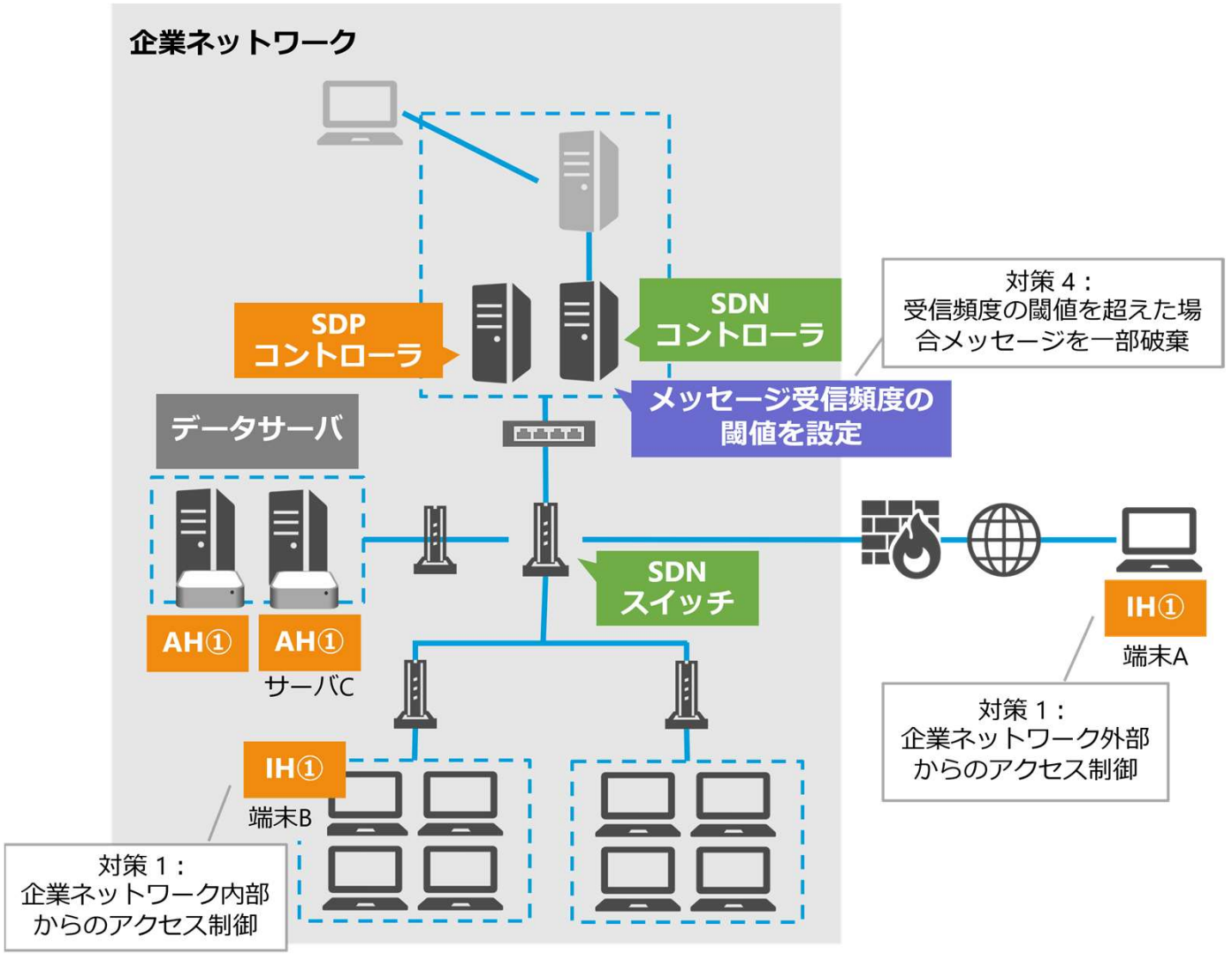
	セキュリティ課題	対策
1	境界型防御の限界	**SDP**によるユーザからのアクセス制御
2	（Northbound API） 攻撃者のSDNコントローラの操作	**コントローラDAC**によるNW管理 システムからSDNコントローラへの通信の検証
3	（Southbound API） フローテーブルの改ざん	**SDP**によるSDNコントローラからSDNスイッチへの通信の検証
4	（Southbound API） SDNコントローラへのDoS攻撃	SDNコントローラにおいて**Packet In メッセージの受信頻度**の閾値の設定

SDNの構造上の課題

対策1、4はSDNデータ層での対策の統合
対策2、3はSDNコントローラ層での対策の統合 を行う

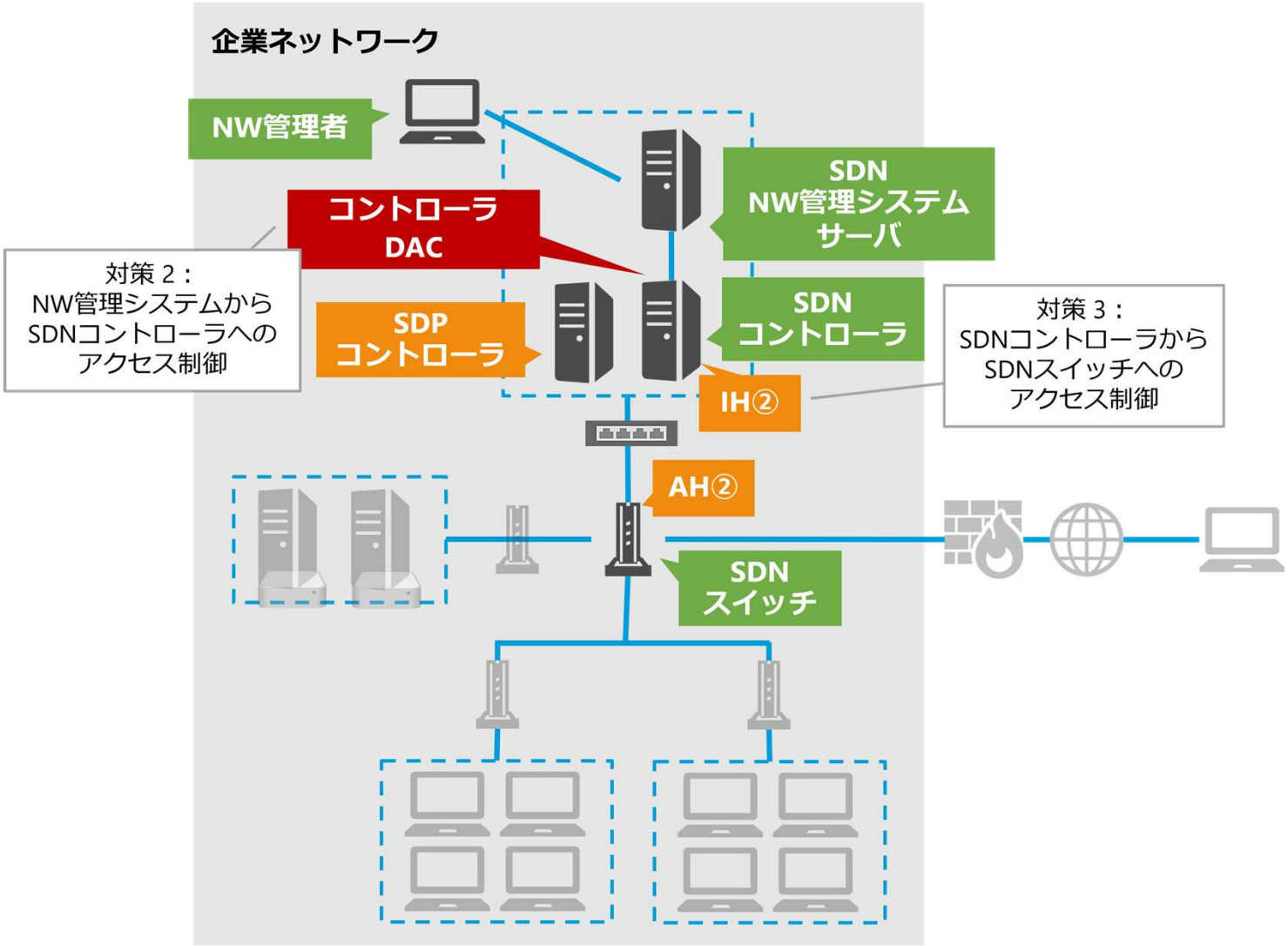
ユーザデバイスからサーバへのアクセス

データ層における対策1と4の統合した場合でも
端末AやBはサーバCに正常にアクセス可能

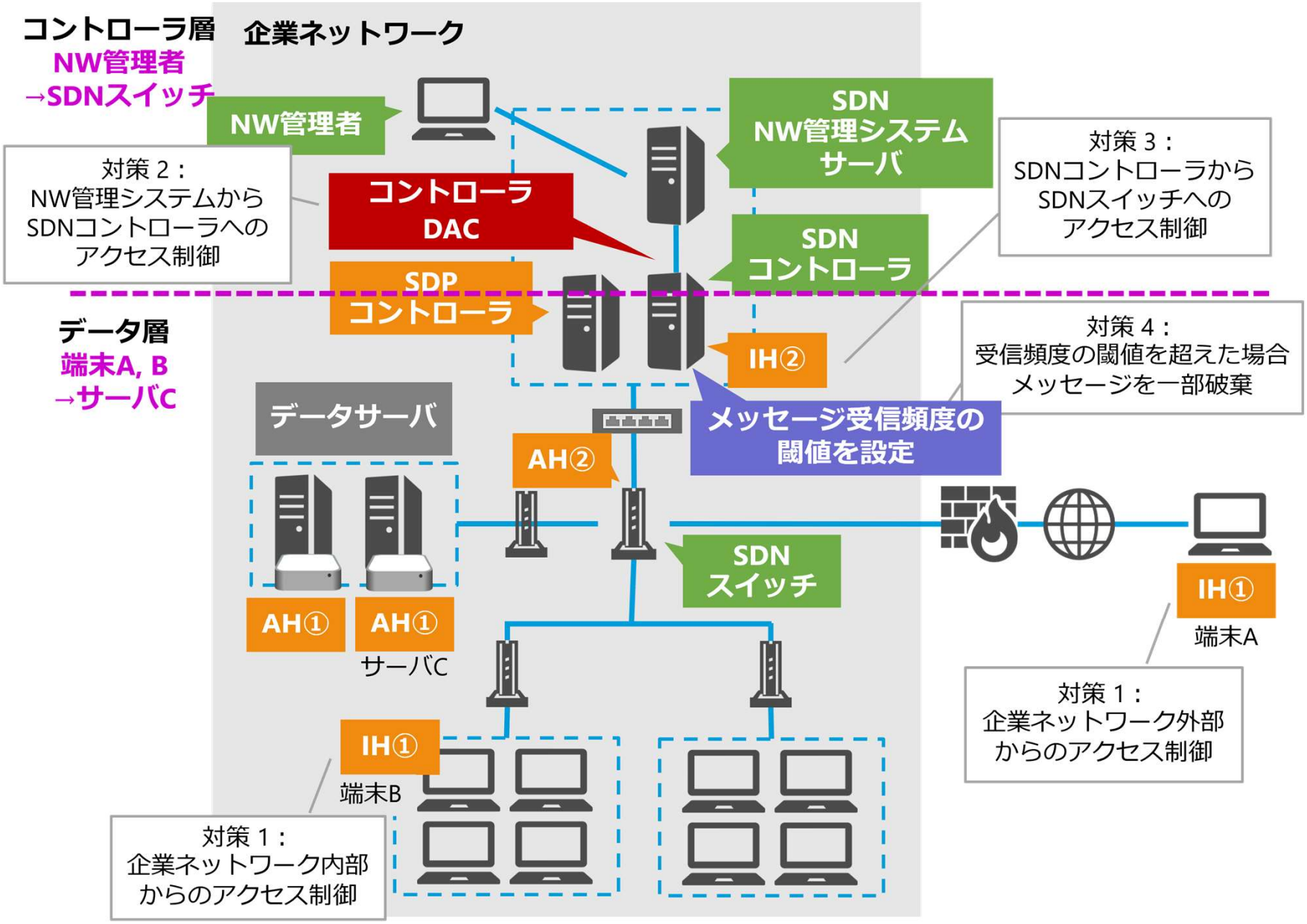


NW管理者によるネットワークの運用

コントローラ層における対策2と3の統合した場合でも
NW管理者はネットワークを正常に運用可能



セキュリティ対策のまとめ



まとめ

近年の企業ネットワークの課題

リモートワークの普及による
セキュリティ課題

ネットワークの構築・運用上の課題

SDNが有効
しかしSDNはセキュリティ課題を有する

対策①：
SDPによる企業ネットワーク内外からのアクセス制御

対策②：**コントローラDAC**によるNW管理システムからSDNコントローラへのアクセス制御
対策③：**SDP**によるSDNコントローラからSDNスイッチへのアクセス制御
対策④：SDNコントローラの**Packet Inメッセージの受信頻度の閾値**によるDoS対策

SDNのデータ層、コントローラ層でそれぞれ組み合わせて使えることを示した
残課題として

- 全ての通信を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
- ユーザデバイスがサーバにアクセスするまでにSDPの認証やSDNコントローラへのフローの問い合わせが起こることで遅延が発生する可能性
- 導入や運用にコストがかかる