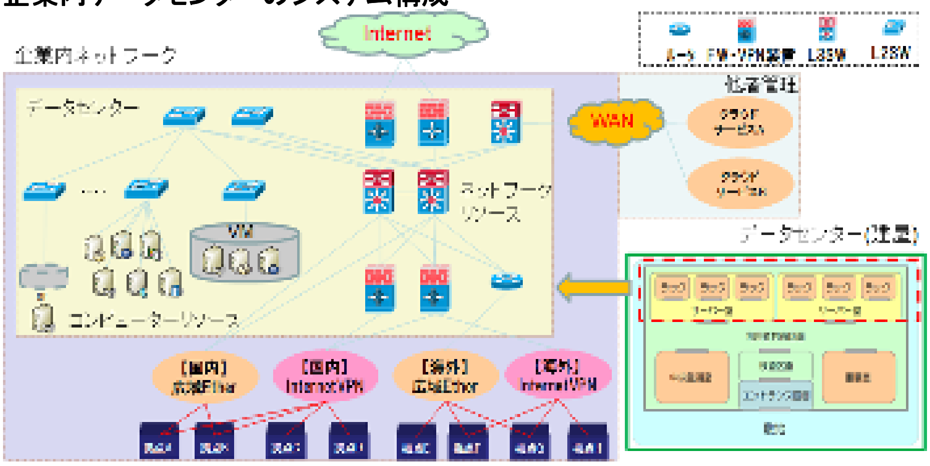
企業内データセンターのセキュリティ課題 ～SDNによる解決手法の提案、及び評価～
Enterprize datacenter security solution by software defined networking

飯塚哲史・ネットワーク分科会・情報セキュリティ大学院大学

In the data center (DC) to support the corporate network, ever more computer resources are aggregated to, with respect to demand that you want to consolidate companies in the system and application services at a lower cost, computer resources in the data center, it is effectively the network resources With leverage, and that collateral security, it has been asked to provide systems and services to various users.
Moreover, while the obtained flexible network, regarding the demand for security, it has become severer than ever。 Access right management, external attacks, such as a patch management, it has become necessary to take measures against various threats.
In this paper, we clarified the problems that are currently faced with DC, it is proposed whether can be solved by using the technology of the SDN.
Then, it is assumed to be performed issues (system, operational) of the security aspects of one possible resolution in the proposed method for verifying the evaluation

企業内データセンターのシステム構成



背景:企業内ネットワークを支えるデータセンター(DC)では,DC内のコンピュータリソース,ネットワークリソースを柔軟に分割し，かつセキュリティを担保した状態で,様々なユーザにシステム,サービスを提供することが求められている。そこで，DC内で柔軟なネットワークの構築,かつセキュリティを担保した状態を実現する候補として，Software Defined Networking(SDN)の技術が注目されている。

目的:DC内で利用されるコンピュータリソース,ネットワークリソースに対して，SDNの技術を利用することで，DC内にて発生している既存のセキュリティ課題(システム上の課題,運用上の課題)が解決することを目指す。

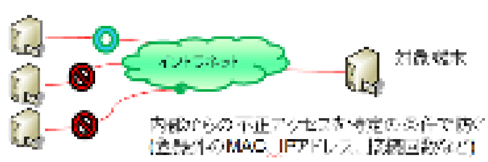
セキュリティ課題

リスク	分析結果	具体例
機密性	情報漏えい	企業内ネットワークの各拠点から、不正な端末を接続し、サーバからデータを漏洩
	なりすまし	クラウドサービス上のサービスから、不正アカウントでサーバに接続し、情報を入手する。
完全性	データ改ざん	各拠点のPC端末、データセンター内のサーバ等より、コンピュータリソースにアクセスし、データを改ざん
	誤動作	コンピューターリソース、ネットワークリソースの設定を操作し、誤動作を起こさせる。(故障、過失)
可用性	不正アクセス	各拠点にマルウェアに感染したPCにより、不正にアクセスされる
	DoS攻撃	Internet上から企業内ネットワークに対して、DoS攻撃を受け、サービスが利用不可状態となる。

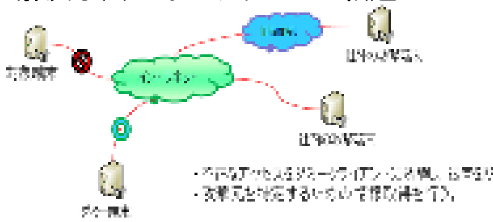
SDNと情報セキュリティとの関係

リスク		機能		
		仮想化	SW制御	集中管理
機密性	情報漏えい		○	○
	なりすまし	○	○	
完全性	データ改ざん		○	○
	誤動作		○	○
可用性	不正アクセス	○	○	
	DoS攻撃	○	○	

解決手法1:不正アクセスの遮断



解決手法2:不正アクセスの転送



まとめ:
DC内でのセキュリティ課題(システム上,運用上)を取り上げ，それが期待されるSDNの機能,特徴を活用することで，解決することができるかを提案した。
また、提案を行った解決手法のうち、不正なソフトウェアに侵入される可能性について、実現が可能かの検証を行い、特定の端末まで誘導するところまでは確認できた。

課題:
・正常な端末、不正な端末を交互に接続した際に問題なく動作するか
・不正な端末からのアクセスを特定の端末を経由させ、目標とする端末まで転送した後、通信を解析できるか
・データセンターの実環境に適用した場合に、問題なく動作をするのか。