

サイバーセキュリティ PBL I

高野 祐輝

2019 年 1 月 8 日

1 目的と評価方法

- 最優 ファイアウォール技術とペネトレーションテストを組み合わせ、検疫ネットワークの設計と構築を行うことができる
- 優 ファイアウォール技術で DeMilitarized Zone のあるネットワーク設計と構築を行うことができる
- 良 ファイアウォール技術で適切なネットワークアクセスコントロールができる
- 可 各種サイバー攻撃手法と防御手法について論じることができる

2 セキュリティ哲学

2.1 サイバーセキュリティとは何か

2.2 サイバーキルチェーン

[1]

2.3 セキュリティポリシとユーザビリティ

[2]

3 TCP/IP の基礎

3.1 OSI 参照モデル

インターネットで利用されるプロトコルは、The Internet Engineering Task Force (IETF) という標準化団体により策定され、その標準は Request for Comments (RFC) という名のオープンな仕様として発行されている。例えば、我々が利用しているインターネットプロトコルであるインターネットプロトコルバージョン 4 は、1981 年に 791 番目の RFC として策定された [3]。

IETF 以外の通信に関する標準化団体としては International Telecommunication Union Telecommunication Standardization Sector (ITU-T) や、International Organization for Standardization (ISO) が存在する。実は、1977 年から 1982 年かけて、ITU-T や ISO がコンピュータネットワークの標準通信プロトコルとして、Open Systems Interconnection (OSI) の策定を行っていた。その当時は標準的な通信プロトコルは存

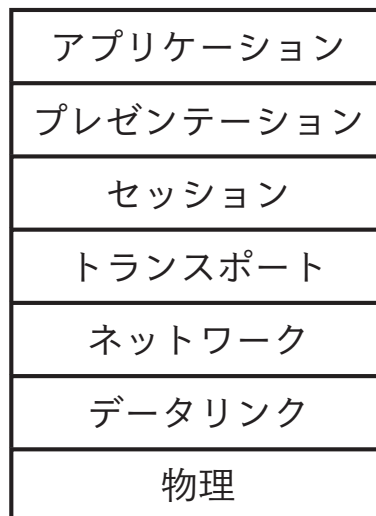


図1 OSI 参照モデル

在せず、ベンダーごとに様々なプロトコルが利用されていたため、通信プロトコルの統一化が求められていた
のである。しかしながら、最終的に OSI は主流とはならず、IETF によって策定されたインターネットプロト
コルが広く利用されるようになっていった。

OSI 自体は残らなかったが、OSI 策定の際に考案された OSI 参照モデルと呼ばれるネットワークの抽象化
手法は、今日でも広く受け入れられている。

重要ポイント

- インターネット関連のプロトコルは、IETF が発行する RFC によって標準化されている
- コンピュータネットワークはレイヤで考えることができる

3.2	データリンク層
3.3	ネットワーク層
3.4	トランスポート層
3.5	トランスポートより上の層
4	PF (Packet Filter) の基礎
5	パケットフィルタリング
6	攻撃手法と対策
7	DMZ (DeMilitarized Zone) の構築
8	検疫ネットワークの構築
9	ロードバランス
10	ロギング
付録 A Vagrant による実験環境の構築	
付録 B PF の構文	

参考文献

- [1] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, Vol. 1, p. 80, 2011.
- [2] B. Fraser. Site security handbook, September 1997. RFC2196.
- [3] J. Postel. Internet protocol, September 1981. RFC0791.