情報ネットワークⅡ（情213）
【第11回】
ネットワークセキュリティ
（教科書：第7章）

担当教員：長田智和

E-Mail: nagayan@ie.u-ryukyu.ac.jp

URL: http://n-lab.info/

（講義日：2017年12月21日）

第7章：ネットワークセキュリティ

7.1 イントラネットの構成要素

- 7.1.1 ファイアウォール
  - ポリシーやフィルタリングルールに基づきパケットの通過・拒否・破棄を制御する。
  - OSI第3,4層の通信を制御する。
  - NATやVPN機能を併せ持つ製品もある。
  - IDS（Intrusion Detection System）/IPS（Intrusion Prevention System）を統合したUTM（Unified Threat Management）製品が登場。（2004年頃）
  - ステートフルパケットインスペクションによるパケットフィルタリングの高度化を実現。
- （教科書p.175の図7.1-7.2を参照）

7.1 イントラネットの構成要素

- 7.1.2 侵入検知システム・侵入防御システム
  - IDS：攻撃パターンやシグネチャDBに基づいて攻撃通信を検知するシステム。
  - IPS：IDS機能に加えて検知した攻撃を遮断するシステム。
  - シグネチャDBによるパターンマッチ方式と、アノマリー検知方式。後者は検知率100%は難しい。
  - NIDS（Network IDS）とHIDS（Host-based IDS）
    - NIDS：ネットワーク内の通信パケット全てをチェックする。
    - HIDS：当該ホストを出入りする通信パケットをチェックする。
- （教科書p.177の図7.3-7.4を参照）

7.1 イントラネットの構成要素

- 7.1.3 WAF（Web Application Firewall）
  - HTTP通信（OSI第7層）などの攻撃を検知・防御する。
  - 最近のUTM装置はWAF機能も統合されている製品が増えている。
- （教科書p.178の図7.5を参照）

7.1 イントラネットの構成要素

- 7.1.4 VPN（Virtual Private Network）
  - IPパケットをカプセル化してトンネリングし、公衆回線を専用線のように扱えるようにする技術。
  - インターネットVPNとIP-VPN
    - インターネットVPN：インターネット網を経由してIPSec等のセキュリティプロトコルを用いる。（コスト：低）
    - IP-VPN：ISPが用意する閉域網を利用する。（信頼性：高）
  - VPNで使用するプロトコル
    - SSL/VPN, SSH, IPSec, PPTP, L2TP, MPLS, etc.
- （教科書p.179の図7.6を参照）

7.1 イントラネットの構成要素

- 7.1.5 その他のサーバーおよびネットワーク機器
  - ログサーバーとモニタリング
  - 時刻同期サーバー（NTPサーバー）
  - DNS（Domain Name System）
  - メールサーバー
  - Webサーバー
  - Webプロキシサーバー
  - その他のサーバー（DBサーバー等）
  - クライアントPC

7.2 FWを用いたネットワーク構成例

- 7.2.1 公開サーバー群をFWの外に置く構成
  - FWの外側に公開サーバーを置く
  - 公開サーバーは攻撃に対する厳重な対策が必要
  - 内部ネットワークはFWにより直接通信が禁止
  - 内部ネットワークには公開サーバー経由でアクセス
  - 最もリーズナブルなFW構成
- （教科書p.183の図7.7を参照）

7.2 FWを用いたネットワーク構成例

- 7.2.2 公開サーバー群をFWの中に置く構成
  - FWの内側に公開サーバーを置く
  - サーバー・サービス毎にフィルタリングルールを作成
  - 公開サーバーの安全性は高まるが、いったん公開サーバーが侵入を許すと内部ネットワークが破たん
  - 採用されるケースは少ないFW構成
- （教科書p.183の図7.8を参照）

7.2 FWを用いたネットワーク構成例

- 7.2.3 公開サーバー群の別ポートに設置する構成
  - 公開サーバーをDMZポートに置く
  - 公開サーバー、内部ネットワークの安全性は高まる
  - FWが単一障害点となる。（FWが壊れると全体停止）
  - FWを二重化して障害対策を行うのが一般的
  - 機器が対応していれば望ましいFW構成
- （教科書p.184-185の図7.9-7.10を参照）

7.2 FWを用いたネットワーク構成例

- 7.2.4 FWによって公開サーバー群を挟む構成
  - 公開サーバーをFWとFWの間に置く
  - 公開サーバー、内部ネットワークの安全性は高まる
  - 公開サーバーFWが侵入されても内部ネットワークへの侵入は防ぐことができる。
  - FWが単一障害点となる。（FWが壊れると全体停止）
  - FWを二重化して障害対策を行うのが一般的
  - 機器が対応していれば最も望ましいFW構成
    （ただし、コストは最も高い）
- （教科書p.185の図7.11を参照）

7.3 ネットワークスキャン

- 7.3.1 ドメイン情報の取得
  - whois DBを利用して攻撃対象組織の情報を収集
  - 攻撃対象ネットワークのIPアドレス等の情報を収集
  - DNSサーバーの望ましい運用
    - 不要な情報をDNSに保管しない
    - ゾーン転送を制限する
    - ドメイン名・サーバー名に必要以上の情報を与えない
    - 社外DNSは社内DNSに問い合わせに行かない
    - 外部へのDNS問い合わせは社外DNS経由で行う
- （教科書p.187-188の図7.12-7.13を参照）

7.3 ネットワークスキャン

- 7.3.2 ホストへのスキャン
  - DNSなどから得られるIP情報等をもとに組織のネットワーク構成を把握しようとする行為。
  - スキャンによって得られた情報をもとに攻撃に移る。
  - 攻撃者はオニオンルーティング技術を使って自身の接続経路を秘匿するケースもある。
  - ICMP等を使ったスキャンを行い、次に、そこで知り得たホストに対してポートスキャンを行う。
  - OSやネットワークサーバーの種類やバージョン情報を取得し、攻撃可能な脆弱性に対して攻撃を行う。
  - FWを適切に設定していれば、FWで遮断できる。

7.3 ネットワークスキャン

- 7.3.2 ホストへのスキャン
  - ICMPを用いたスキャン
    - ping：ICMPのtype0（エコー応答）、type8（エコー要求）、type11（時間経過）を利用してネットワーク到達性を確認
    - traceroute：IPのTTL（Time To Live）、ICMPのtype11を利用してネットワーク経路を調べる
    - ping, tracerouteコマンドをFWで遮断するのが効果的対策
  - ポートスキャン
    - TCPスキャニング、ステルススキャニングにより、攻撃対象ホストで稼働しているサービスを特定する
- （教科書p.189-190図7.14-7.15を参照）

7.3 ネットワークスキャン

- 7.3.2 ホストへのスキャン
  - ポートスキャン対策
    - 不要なサービスは稼働しない（FWで不要ポートへのアクセスをブロックする）
    - 各サービスはセキュリティパッチ適用された最新版を利用する等

7.3 ネットワークスキャン

- 7.3.3 パスワードの奪取
  - ブルートフォース攻撃
    - 利用者ID又はパスワードを固定して、もう片方を無作為に総当たりで試す方法
  - アカウント管理ファイルの奪取
    - OSの外部からパスワード管理ファイルを奪うこと
  - ネットワーク上のパスワードの奪取
    - 遠隔ログインを試みる利用者からパスワードを奪うこと
- （教科書p.193図7.16を参照）

7.4 セッションハイジャック

- ARP Poisoning攻撃
  - ARPテーブルを書き換えて、2者間の通信を取得
  - ダムHUBだけではなく、スイッチングHUBでも可能
  - イントラネット（組織内LAN）への侵入が入口
    - スイッチングHUBの物理ポートに接続される
    - イントラネット内のホストに侵入されて踏み台にされる
  - （動作の流れは教科書で説明）
- （教科書p.195図7.17-7.18を参照）

7.4 セッションハイジャック

- DoS攻撃
  - SYN Flood
    - TCPの3ウェイハンドシェイクを悪用した攻撃
    - SYNパケットをサーバーに送信し、サーバーからのSYN/ACKパケットに応答しない（これを無数に繰り返す）
    - SYN cookiesで対策可能（IP偽装されていない場合のみ）
  - Ping of Death
    - ICMPエコー要求（type8）パケットにサーバー側OSが処理不能なサイズのデータを付けて送りつける攻撃
    - 最近のOSでは対策済み

7.5 マルウェア対策

- 7.5.1 コンピュータウィルスとワーム
  - コンピュータウィルス
    - 特徴：宿主となるプログラムが必要
    - 自己伝染機能：自己を複製し他に感染を広げる機能
    - 潜伏機能：特定の条件になるまで、活動を待機する機能
    - 発病機能：破壊などの活動を行う機能
  - ワーム
    - 特徴：メモリ上で単体で活動
    - 単独で侵入し、感染し、活動を行うプログラム
    - 攻撃対象のセキュリティホールを利用して侵入
    - 宿主となるプログラムが必要なものはワームウイルスという

7.5 マルウェア対策

7.5.1 コンピュータウィルスとワーム

ボット

- コンピュータに感染し、インターネットを通じて外部から操作できるようにするコンピュータウィルス
- ボットハーダー（外部から指示を行う者）からの指示に従ってスパムメール配信やDoS攻撃などを行う。

トロイの木馬

- 一見不正には見えないソフトウェアに混入
- 攻撃者のバックドアになる場合は、RAT（Remote Administration Tool）と呼ばれる。
- 一般には自己伝染機能は持たない。

スパイウェア

- 利用者の個人情報やアクセス履歴などを奪取する。

7.5 マルウェア対策

- 7.5.2 対策
  - 一般利用者の対策
    - OS、ソフトウェア等を最新バージョンに保つ。
    - セキュリティパッチを適用する。
    - ウィルス対策ソフトを導入し、最新状態に保つ。
    - 定期的に脆弱性スキャンを行う。
    - 怪しいWebサイトやスパムメールに注意する。
    - バックアップを取っておく。
  - システム管理者の対策
    - WebやMailサーバーに対策ソフトを導入する。
    - 利用者に対するセキュリティ意識の啓発活動を行う。

7.5 マルウェア対策

- 7.5.3 進化するマルウェアの実現形態
  - ポリモーフィック型マルウェア
    - プログラムコードの一部を暗号化したり圧縮して特徴パターンを変化させ、パターンマッチングを困難にする。
  - メタモーフィック型マルウェア
    - プログラムコードを分割して順序を入れ替えたり、実質的に何もしない命令（NOP命令等）を入れる等で、プログラムコードを書き換える。
  - ルートキット型マルウェア
    - 攻撃者が侵入したホストへ継続的にリモートアクセスするためのツール群。外部からFWへのアクセス手段のために正当に使われることあるが、悪用されるケースで知られる。
- （教科書p.199-200図7.19-7.20を参照）

7.5 マルウェア対策

- 7.5.4 コンピュータウィルス対策ソフトの仕組み
  - コンピュータウィルスやワーム感染を未然に防ぐことを目的としたソフトウェア。
  - PC上で運用される場合、サーバー上で運用される場合、NIDSとして運用される場合など。
  - PC上で運用される場合の2通りの検知タイミング：
    - PC外部からデータを取得するとき、当該データを検査する。
    - 定期的もしくはPCの利用者が実行を指示したとき、または新しいストレージが接続されたときに、OSが参照できるストレージを検査する。
- （教科書p.200図7.21を参照）

7.5 マルウェア対策

- 7.5.4 コンピュータウィルス対策ソフトの仕組み
  - コンペア手法
    - オリジナルファイルの情報と検査の際の差分を比較して、差異があれば感染を疑う方法。
  - パターンマッチング手法
    - コンピュータウィルスやワーム等のマルウェアの特徴情報を保持したDB（パターンファイル）を用いて対象ファイルとパターンファイルを比較する方法で、最も一般的な方法。
    - 未知のマルウェアは検知できない。未知のマルウェア又はパターンファイエル公開前のマルウェアを用いて攻撃することを「ゼロデイ攻撃」という。

7.5 マルウェア対策

- 7.5.4 コンピュータウィルス対策ソフトの仕組み
  - ヒューリスティック手法
    - 実際のOSで動作させずに検査する方法。
    - 静的ヒューリスティック手法：
      - プログラムにマルウェア固有の命令が含まれているかを検査する手法。
    - 動的ヒューリスティック手法：
      - 仮想マシン上でプログラムを実行して検証する手法。
  - ビヘイビア手法
    - 実行中のプログラムをリアルタイム監視し、不正なシステムコールやファイル操作を検出し、実際に実行される前に阻止する手法。動的ヒューリスティック手法の一種。

7.5 マルウェア対策

- 組織内のネットワークからしき起こされる脅威の例とその対策
  - 外部ネットワークからのアクセス対策（入口対策）だけではなく、内部ネットワークの対策も重要。
  - PCにウィルス対策ソフトを導入するだけではなく、内部ネットワークへの入り口にあるMailサーバーやProxyサーバー等でもマルウェア検査する。また、PCのOSや各種ソフトウェアを最新状態にする。万一、侵入された場合でも、内部から外部の通信チェック（出口対策）を行う。
  - 内部犯行への対策も必要。情報資源への適切なアクセス制御（最小権限の原則）、モニタリング、ログ収集が有効な対策。
  - クラウド環境では、Web、Mail、ストレージサービス等をHTTP経由で利用するため、WAF（Web Application Firewall）などを用いたHTTP通信の対策が必要。

【次回予告】
第12回
Webセキュリティ（1）
（第8章）

また来年！