情報セキュリティ対策: アクセス制御とログ分析

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

1. アクセス制御: Access Controls
2. ネットワークでのアクセス制御
3. サービスのアクセス制御
4. ログ分析

アクセス制御: Access Controls

- ネットワークにおけるアクセス制御
  - Firewall
  - WAF (Web Application Firewall)
  - IDS (Intrusion Detection System) と IPS (Intrusion Prevention System)
  - 無線 AP やスイッチでの制限
- サービス毎の制御

Firewall

- TCP/IP パケットには、送信元 IP アドレス、受信先 IP アドレス、サービスポートが書いてある
  - IP アドレスは IP ヘッダ内
  - ポート番号は TCP ヘッダ内
- 不必要・危険なパケットの通過を抑制する
  - allow/deny

Firewall での ACL 例

- ACL (Access Control List) 例
  - IP アドレス指定
    - 外部から、サーバ以外への通信を遮断
    - 内部から、外部の危険なアドレスへの通信を遮断
  - ポート番号指定
    - 外部から、サーバの指定したサービス以外への通信を遮断
    - 内部から、外部への暗号化されない認証プロトコルを遮断
- 公開サーバへの攻撃を防ぐには非力
  - 例: 公開 Web サーバへの攻撃

Firewallでの ACL 具体例

- 内部から外部へ、Web サービスを許す
  - 内部から外部へ、80 番と 443 番を開ける
  - 外部の不正サイトに対して、IP アドレスを指定して閉じる
- 外部から、内部の指定した Web サーバへの通信のみを許可
  - 外部から内部へ、80 番と 443 番を閉じる
  - 外部から指定した IP アドレスへ、80 番または 443 番を開ける
- 暗号化しない POP と IMAP を閉じる
  - 送信元送信先に区別なく、109(POP2)、110(POP3)、143(IMAP) を閉じる
- 全閉鎖の後に、必要に応じて開けるのが基本的方針

WAF (Web Application Firewall)

- Web 専用の対策装置
  - URL を指定してアクセス制御
  - Web への攻撃を検知
  - 公開サーバの多くが Web
- FW で通信を許可したら、何も対策できない危険性
- Web を狙った攻撃のパターンを検知して遮断
  - ウィルス対策ソフトと同様に攻撃パターンファイルを保持

IDS: Intrusion Detection System/ IPS: Intrusion Prevention System

- サービス毎の攻撃パターンを検知
- IDS は検知のみ、IPS は遮断機能を持つ
- ウィルス対策ソフトと同様にパターンファイルを保持
- サンドボックス (sandbox) 機能を持つものもある
  - 添付ファイルなどを切り出す
  - 仮想 OS 上で動作をシミュレーション

無線 AP やスイッチ

- MAC (Media Access Control) アドレスによる制限
  - 個々の機器の MAC アドレスを許可・拒否
- 共通パスワードによる認証:WEP や WAP
- ユーザ毎の認証:802.1x
- private アドレスを使って内部を秘匿
- 例: 000Saga-u

サービスのアクセス制御

- サーバ側で、サービス毎に制御
- 接続元 IP アドレス
- ユーザ認証

例: Web サーバ

- `httpd.conf` を使った制御
  - サーバの設定を使った制御
- `.htaccess` を使った制御
  - ディレクトリでの細かな制御
- source address や user による制御
- 認証を求める制御
- FW は、サーバへのアクセスを制限できるが、URL 毎の制限はできない。

例: Apache の .htaccess ファイルを使った制限

- IP アドレスを使って、閲覧を制限
- IP アドレスや FQDN を使って、閲覧を拒否
- 閲覧時に認証を要求
  - Shibboleth 認証
  - 特定の属性に制限
- web クライアントによる制限

例: VPN 装置

- VPN (Virtual Private Network)
  - 遠隔から組織内 LAN へ接続
- 接続元 IP アドレスによる制限
- ユーザ認証

質問

例えば教務システムは、学内からアクセスする際と学外からアクセスする際の動作が異なります。どういう違いがあるか分かりますか。

ログ分析の必要性

- log：日誌、機械の運転記録
- log：an official record of events during a particular period of time, especially a journey on a ship or plane.
- 機器やサービスが正常に動作していることを記録
- 異常や攻撃の記録

例: Firewall

- 拒否した通信
- 許可した通信: 通常は取得していないこともある
- 機器の負荷

何を見るか

- 繰り返し攻撃してくるホスト
  - IP アドレスを変更して、攻撃してきていないかを確認
  - FW を通過しているならば、新規に閉鎖すべきか検討
  - 攻撃に関する情報収集により、被害の有無を確認
- 内部から大量のパケットを送信するホスト
  - ウィルス感染の恐れ
  - FW でブロックしていない場合には、外部を攻撃した可能性もある
- ルールの定期的棚卸しの必要性

例: Web サーバ

- アクセスのあった URL、時刻、送信先、クライアント名
- 誤った URL、時刻、送信先、クライアント名
- 攻撃と考えられるイベント、時刻、送信先、クライアント名
- 機器の負荷

何を見るか

- アクセス件数の統計により、情報公開の程度を評価する
- file が見つからないエラー
  - サイト内のリンクに間違いはないか
- 繰り返し攻撃しているホスト
  - アクセス制限で拒否するかを検討

課題

自身の PC に入っているウィルス対策ソフトのログを確認しなさい。