状況認識のための セキュリティアプライアンス

笠原（九大）* 武蔵（熊大）
須永（富士通SSL） *リーダー

SS研セキュリティマネジメントWG
セキュリティアプライアンスグループ

目次

- セキュリティアプライアンスの必要性
- 技術的紹介
  - ファイアウォール
  - IDS/IPS（侵入検知システム・侵入防止システム）
  - WAF（Web Application Firewall）
  - 利用例としてのP2P対策
- 導入・管理・運用
- まとめ
- 付録：セキュリティアンケートについて

セキュリティアプライアンスの必要性

セキュリティアプライアンスの必要性

- 組織内のインシデントについて知る必要がある
- インシデントへの対応が必要になる

- その技術的解＝セキュリティアプライアンス
  - パケット・トラフィックに対する
    - 監視カメラ
    - 防火壁
    - 検問
  - …のようなもの

状況認識（Situation Awareness）

- 状況を認識しなければ適切に対処できない
  - SNMPによる流量記録ではおおざっぱすぎる
  - tcpdumpによる生パケットでは細かすぎる
- 機器の導入により見えてくる物がある
  - ポート番号ではわからない利用傾向
  - ウィルスの活動・踏み台の発見
  - 機器の設定ミス等々
- リスク分析が可能になり、次の一手への資料になる

インシデント予防と対応

- インシデント予防策としてのアプライアンス
  - ファイアウォールによる可能性の絞り込み
  - IDSによる傾向分析・早期発見
  - IPSによるリアルタイム遮断等
  - 「監視されている」事による利用者への抑止力
- インシデント発生時の対応
  - ファイアウォールによる緊急回避
  - IDSによる類似トラフィックの発見
  - WAFによるパッチ等
- 「アリバイ」証明
  - ログによって、組織外の事件に対する潔白を証明する
- 機器がないと、手も足も出ない場合がある

技術的紹介

ファイアウォール

ファイアウォール

- 通信を特定の基準（ポリシー）に基づき選別する仕組み
- ネットワーク型
  - ネットワーク上に設置、「内」と「外」を区別する
- ホスト型
  - ホストに導入、ネットワークからの攻撃等を防ぐ

ネットワーク型ファイアウォール

- 扱うプロトコル階層による区別
  - パケット単位
    - IPアドレス・ポート番号などヘッダ情報による選別
    - 静的フィルタ・動的フィルタ
    - ステートフル（状態保持型）
      - 主にTCPの状態遷移を認識し正当なセッションを識別
  - セッション・アプリケーション単位
    - セッションを再構築し高次プロトコルを認識して制御
      - ポート番号に依存しないアプリケーション制御
    - 例
      - ポートが固定されていないP2P通信を帯域制限
      - 特定のURLへのHTTPアクセスを遮断

NATとファイアウォール

- ここで言うNATはNAPT（Network Address Port Translation）のこと
  - 内側のプライベートアドレス空間を外側の少数のグローバルアドレスに変換し通信可能とする技術
  - 同じアドレスを使う異なる通信を区別するため、ポート番号を変換し変換表を維持する
- 変換表にない通信を遮断するため、自動的にステートフルフィルタとなる
  - 簡易的な一方通行のファイアウォール
- 高機能なファイアウォールの置き換えになるものではない

プロキシ（proxy）

- サーバとクライアントの間にあって通信を代理・仲介する仕組み
  - 通常クライアント側に置かれ、クライアントがサーバの代わりとして接続する
    - サーバからはクライアントに、クライアントからはサーバに見える
  - プロキシの両側のネットワークを不連続にできる

プロキシの種類

- トランスポート層ゲートウェイ
  - アプリケーションによらず通信を代理で仲介
    - SOCKSが代表的実装
      - プロトコルに依存しないプロキシ動作
      - クライアント側の対応が必要
- アプリケーション層ゲートウェイ
  - 特定のプロトコルに特化
    - ウェブプロキシが代表的
  - 代理だけでなく、通信内容の検査も可能
    - WAF（後述）

可用性と負荷分散

- パケット単位の静的フィルタではきめ細やかで十分な制御ができない
- 動的・ステートフルフィルタ、アプリケーション層での制御は高層になるほど負荷が高い
- 状態をもつと、障害発生時に切り替えが困難
- 負荷分散も難しい
  - セッション単位で振り分ける仕組みが必要になる

ファイアウォールの限界

- 境界線の曖昧さ
  - 可搬型PCによる物理的乗り越え
  - VPN技術による論理的乗り越え
- 許可している通信による攻撃
  - メールやウェブによるウィルス侵入等
- 記述できない制限
  - パケットフィルタではポート固定でないプロトコルを制限する記述ができない、など
- 他の防御機構と組み合わせる必要がある

アプリケーションとの相性

- ファイアウォール導入により影響を受けるアプリケーションがある
  - H.323 などのマルチメディア系
  - e-Learning 系
  - グリッド系
- 一般的でないポートを利用するもの
  - 利用者はファイアウォールで何が制限されているかわからない
  - 個別対応が必要な場合がある

ホスト型ファイアウォール

- ホストに導入し、ネットワークインターフェイスから出入りするパケットを選別
  - ホスト内部の情報を利用した細かい制御が可能
    - 接続ネットワークによるフィルタ設定の切り替え
    - プロセスの動作状況を反映したフィルタ設定
    - 実行ファイル単位でのネットワーク利用許可・不許可
  - パケットの正規化
    - プロトコル違反パケットの破棄・修正
    - プロトコル実装の差違を吸収しOS推定を妨害

主要OSでの搭載状況

- Windows
  - XP/Vista には標準搭載
    - XPはホストから出るパケットを制御できない
    - Vistaではより細かい設定が可能となった
  - 2000には機能はあるがGUIはない
- MacOS X
  - 標準搭載
- Linux
  - iptables など標準で利用可能
- 適切に設定されているかどうかという問題
  - デフォルト設定が良くないと、機能を切られたりする

IDS: Intrusion Detection System
IPS: Intrusion Prevention System
（侵入検知システム・侵入防止システム）

侵入検知システム・侵入防止システム

- ネットワーク型
  - 悪意のあると思われる通信を検出し、警報を発したり、遮断したりする仕組み
    - 誤用検知
    - 異常検知
- ホスト型
  - ホスト上で悪意のあると思われる活動を検出し、警報を発したりする仕組み
    - ファイル改ざん検出
    - ログ監視
    - プロセス挙動監視

ネットワーク型

- ネットワーク上の通信（流量・内容等）を監視し、侵入等を検知
- 誤用（abuse）検知
  - シグニチャ型とも呼ぶ
  - パケット内容を高速に走査
  - 既知のパターン（シグニチャ）に合致すると警報
  - 誤検出の多さが課題
  - 暗号化通信に無力
  - 未知の攻撃に弱い
- 異常（anomaly）検知
  - 平常の通信状態を学習
  - 平常状態からの外れ値を検知し警報
  - 平常状態の学習が難しい
  - 異常値の原因がわかりにくいことがある

IDS（侵入検知）とIPS（侵入防止）

- IDSは横で通信を見ているだけ
  - 監視カメラに相当する
  - それ自身に侵入を防御する機能はない
    - 偽のRSTパケットを送信・ファイアウォールのフィルタルールを変更するといった実装はある
- IPSは通信経路上で動作
  - ファイアウォールに類似
  - 必要に応じて通信を遮断する

実装

- Snort
  - http://www.snort.org/
  - オープンソースのIDS/IPS
  - 検知ルールの購読に有料版と無料版がある
  - Snortベースの商用アプライアンスもある

ホスト型

- ホストに導入し、システムの状態を監視・監査
  - ファイルの改ざん検出
    - 実行ファイルの置き換え
    - ログの改ざん
  - 攻撃らしい通信パケットの検知・遮断
  - ログから特定の文字列を検出
  - システムコール呼出傾向からの異常検知
  - 等々

実装

- Tripwire
  - http://sourceforge.net/projects/tripwire/
  - 主にファイルの改ざんを監視
- OSSEC
  - http://www.ossec.net/
  - ログ解析・システムの完全性チェック・レジストリ監視・rootkit検知等
- デスクトップOS用セキュリティ製品でウィルス検査・ファイアウォールとともに統合されてきている

UTM: Unified Threat Management

- 「統合脅威管理」
  - ファイアウォール・アンチウィルス・IPS・コンテンツフィルタ等のネットワークセキュリティ機能を統一管理すること、また統合された機器
- 利点
  - 低い導入・管理コスト
- 欠点
  - 低い自由度・耐故障性

WAF
（Web Application Firewall）

Web Application Firewall

- ウェブ通信に特化したファイアウォール
  - ウェブサーバの手前に設置
  - クライアントからの要求やサーバからの応答内容を検査
  - ポリシーに合致しない通信を遮断
  - 危険な要求や応答内容を安全なものに変換
- レガシーなアプリケーションを修正せずに防御
- 「リバースプロキシ」の一種
  - 通常のプロキシはクライアントの代理
  - リバースプロキシはサーバの代理

WAFの機能

- ウェブサーバ・サービスへの様々な攻撃を検出し、防止する
  - SQLインジェクション
  - クロスサイトスクリプティング
  - OSコマンドインジェクション
  - クッキー改ざん
  - 入力フォームのhidden属性改ざん
  - クレジットカード番号漏洩
  - バッファオーバーフロー
  - 不正なページ遷移
  - ディレクトリトラバーサル
  - エラーページ・HTTPヘッダからの情報漏洩
  - 表示ファイルタイプの規制
  - 文字コード変換によるフィルタ回避
  - 等々

利用例としてのP2P対策

P2Pとは

- Peer to Peer モデル
  - 計算機ネットワークの形態の一つ
  - クライアント・サーバモデルの対義語
  - ネットワークに参加するホストが明確なクライアントやサーバという区別をもたず、クライアントとサーバの両方の機能を兼ね備えた同等もしくは類似した役割を担う
- P2Pモデルを応用したソフトウェアを指すこともある

具体的な応用例

- ファイル共有
- 情報共有
- メッセンジャー
- 音声通信
- CDN（Contents Delivery Network）

何が問題か

- P2P自体は単なる通信技術
- 応用としてのファイル交換ネットワーク
- 使われ方で問題が発生している
- ポートの固定されたサーバ・クライアントモデルより通信状況を把握しにくい
- 状況把握・利用制限のためにはセキュリティアプライアンスの導入が必要な場合も

違法ファイル共有

- CDやDVDを吸い出したファイルの違法流通
  - 音楽・映画・ゲーム等々
- 効率化のための機能による問題
  - キャッシュ機能・ダウンロード中ファイルの他ホストへの公開など
    - 利用者が意識せずとも違法ファイル流通に荷担
  - 権利者から組織等に警告、法律問題に発展の危険性もある

情報漏洩

- P2Pを利用した情報漏洩ウィルスの存在
  - マイドキュメント等を固めてP2P網に放流
  - P2P網には一般にファイルを削除する手段が提供されていない
    - いったん放流されると回復が困難
- P2Pが悪いと言うより、利用者の管理が問題
  - P2Pで流通するファイルは感染危険度が高い
  - ウィルス感染の危険性が高い環境で秘密情報を扱うのが問題
- 家族の共用PCに知らないうちに入っていた、といった事例も

制限するか否か

- P2Pソフトウェアの利用自身は違法ではない
- 利用の仕方によるリスクをはらんでいる
  - 現実問題としての事件・事故
    - ウイルス感染
    - 情報漏洩
    - 権利団体からのクレーム
  - トラフィックの増大
- 最終的には組織ごとの判断になる
  - 問題が起きてから慌てないように準備
  - なぜ制限しているのかの説明根拠も必要

どう規制するか

- 規則・広報など人的な手段による努力目標
- トラフィックの監視
  - セキュリティアプライアンスによる監視
    - 流量制限等可能な製品もある
  - 商用監視サービスの利用
- フィルタ・流量制限
  - セキュリティアプライアンスによる対応
  - 主要なポートのフィルタ
    - ポート番号を変更されると抜けられる

利用者への対応

- 技術は悪くない→使う人間が悪い
  - 広報・教育に頼らざるを得ない部分
- 外国人対応
  - 国によって著作権に対する感覚が異なる
  - 単純に言葉の問題で規則が周知されない
- 規制の際に、留学生や外国人研究者によるP2Pの利用に少し注意が必要

導入・管理・運用

管理的側面について

- コストの問題
  - 初期導入コスト
  - 維持管理コスト
- 運用ポリシー
  - 「盗聴」と同等のことが可能になる
  - 内容を見ての遮断は検閲になりかねない
  - 機器そのもの、ならびに機器の生成するログへのアクセス権限が重要な問題となる

どこにどう入れるか？

- 安い物ではないため、予算とのトレードオフ
  - 導入コストと並んで維持コストが高い物が多い
- 一般的な選択肢
  - 対外ルータの近傍
    - インターネットからの防御
  - 主要なスイッチに付随
    - 内部から内部への攻撃なども監視・防御
  - 主要なサーバの近傍
  - 機密度の高いネットワークへの入り口（中への防御）
    - 事務系ネットワーク・病院系等
  - 信頼度の低いネットワークへの入り口（外への防御）
    - 学生寮・教育システム・共用ネットワークなど

ネットワーク設計との関係

- 監視しやすいネットワーク設計が必要？
  - 主要トラフィックの流れを想定し効率的なフィルタ・監視ポイントを設定
  - IDSの場合ポートミラーやスプリッタの設置を考える必要がある
    - 10GbE のミラーリングや分岐は容易でない
  - UTM等それ自体がボトルネックになりかねない
- ネットワークの更新時にまとめて設計できるといいのではないか
  - 導入後の状況把握により、新たな機器が必要とされる場合もある

更新計画

- 機器の更新を視野に入れた計画が必要
- 陳腐化
  - トラフィックの増加
  - ネットワークの更新による速度向上・インターフェイスの変化
  - 保守切れ
    - データベースの更新されないアプライアンスは無用の長物
- 互換性
  - 新種のサービス・プロトコルへの対応
    - 例: IPv6
  - 特定サービスとの非互換性
    - 例: H.323（遠隔会議の主要プロトコル）など

ログ管理

- これらの機器は通常大量のログを生成する
- 管理ポリシーが必要
  - どこに保存するか
    - syslogサーバ・外付けストレージ等
  - どれくらいの期間保存するか
    - インシデント発生時は過去にさかのぼる必要がある
    - 持っていると官憲に出さないといけなくなる可能性はある
  - 閲覧権限の規定
    - インシデント発生時のみ詳細閲覧可
    - CISOの許可等
  - 統計解析問題
    - 物量があるので人手も時間もかかる
    - アウトソースも視野に入れて検討が必要

導入前の準備（理想論？）

- 運用ポリシーを決める
  - ポリシーが決まらないとコスト計算ができない
- コストを計算する
  - これに従って導入規模等を決める
- 構成員の同意を得る
  - セキュリティポリシーに入れる
  - 雇用契約時に宣誓書で遵守させる
  - etc…
- 実際は機器を入れてから考える場合が多い

まとめ

- セキュリティアプライアンスは、組織内ネットワークの状況把握に重要な役割
- 初期コスト＋維持コストがかかる
  - お金
  - 人手
  - 手間
- 有用だが、導入には覚悟が必要
  - ただ漫然と入れると、高価な宝の持ち腐れ

付録: セキュリティアンケートについて

- セキュリティアプライアンスに関する事例調査
  - 機器の傾向
  - 導入の動機
  - 運用/管理の実情
- P2P対策の現状
- 十分な情報を得るため、一部の機関に協力をお願いした