プロセスの依存関係に基づく分散システムのセキュリティ機構

光来健一*　千葉滋**　益田隆司*

*東京大学
**筑波大学・さきがけ研究21

インターネットからの攻撃

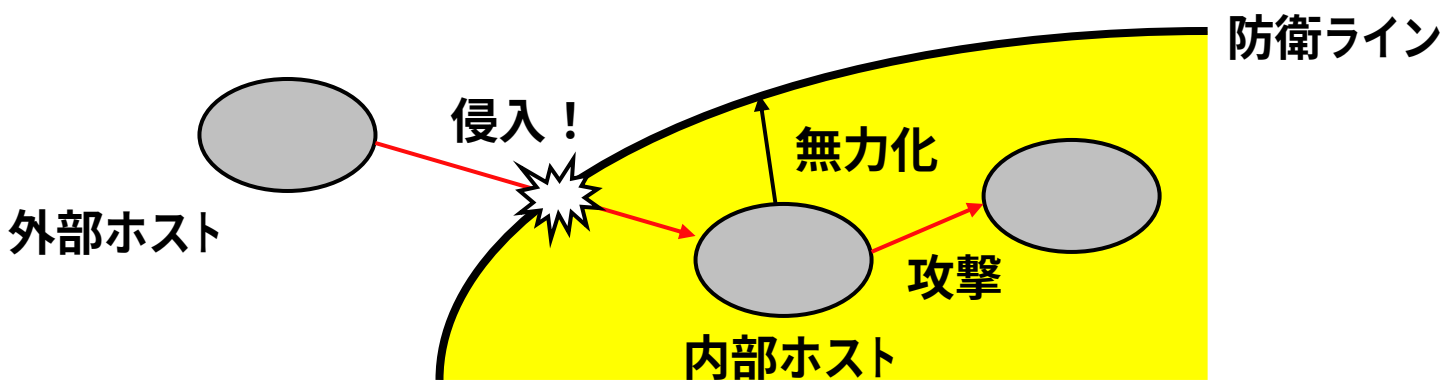
- サービスを外部に提供しているホストは常に攻撃の危険にさらされている
  - セキュリティホールを利用した攻撃
    - 注意深くコーディングされていないプログラムを悪用する
      - バッファをオーバフローさせ任意のコードを実行させる
      - PATH環境変数をうまく設定して、相対パスで指定されたsystem関数に任意のプログラムを実行させる
  - ユーザになりすまして侵入
    - ネットワークを流れるパスワードを盗聴する
    - パスワードを類推する

防衛ラインモデルによる対策

- 信頼できるホストと信頼できないホストの境界でアクセス制限するセキュリティモデル
  - ファイアウォールの構築
    - ☞外部からのパケットを制限して攻撃を未然に防ぐ
  - StackGuard[Cowan et al. 98]
    - ☞バッファオーバフローを検出できるように関数呼び出しの際にスタックに印をつける
  - 通信路の暗号化･ワンタイムパスワード
    - ☞ネットワーク上を素のパスワードが流れないようにしてパスワードの盗聴を防ぐ

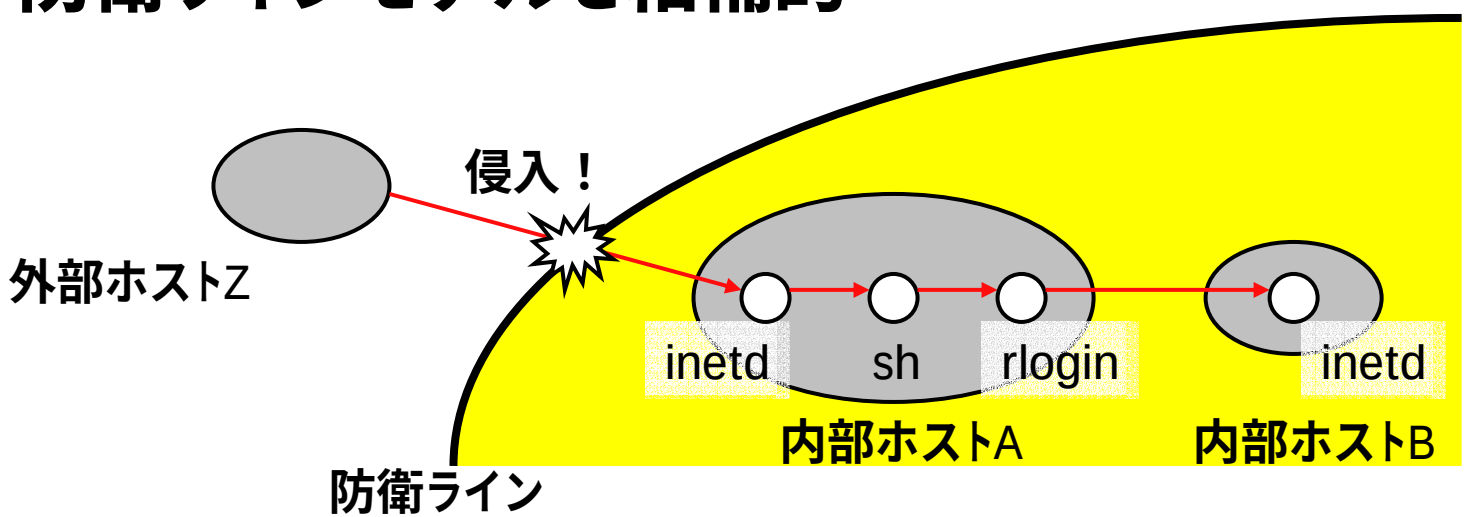
防衛ラインモデルの欠点

- 防衛ラインを一旦突破されると、それ以降の攻撃に対して無力になる
  - ファイアウォールマシンに侵入された時
    - ☞ファイアウォールの設定を変更されると無意味になる
  - パスワードを知られた時
    - ☞正規ユーザと区別できなくなる



行動追跡モデル

- 防衛ラインを突破されても侵入者の行動を追跡してアクセス制限するセキュリティモデル
  - 侵入者が行った通信を追跡
  - 侵入者が起動したプロセスを追跡
- 防衛ラインモデルと相補的

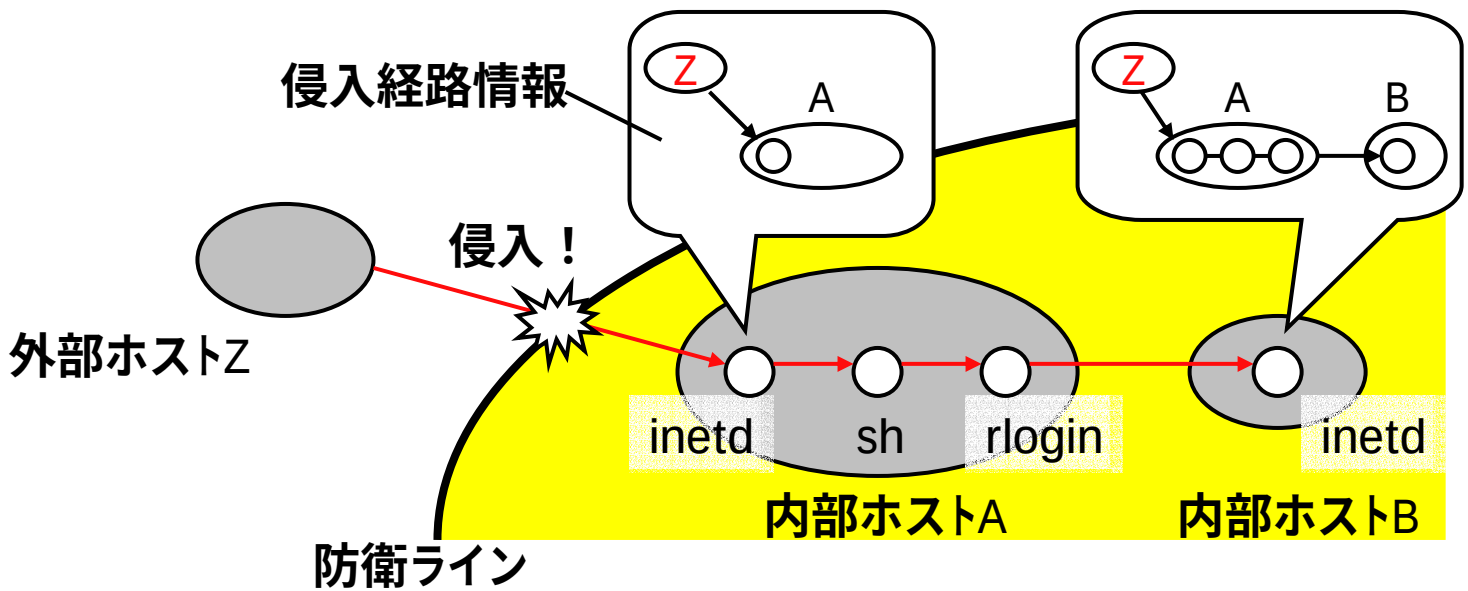


Compactoシステム

- 行動追跡モデルを実現するシステム
  - 各プロセスが侵入経路に関する情報を保持する
    - ☞侵入経路は一般的にグラフになる
      - プロセス間の通信
      - プロセスの親子関係
  - プロセス間で侵入経路情報を伝播させる
    - ☞伝播先のプロセスの侵入経路情報とマージされる
  - 侵入経路情報を基にアクセス制限を行う
    - ☞高速にアクセス権限を検査できる
    - ☞ネットワーク接続が切れても問題ない
      - cf. ログに基づく追跡

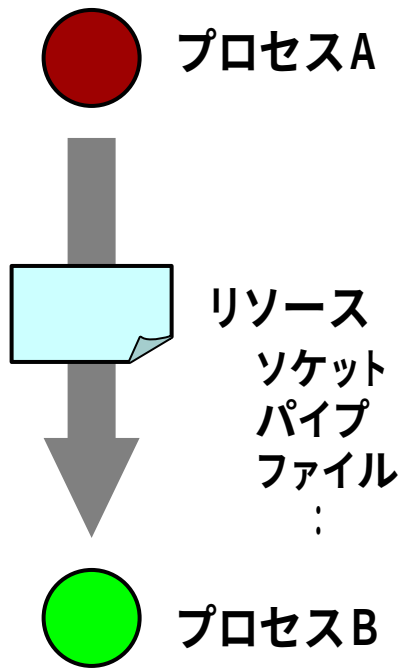
侵入経路情報を用いたアクセス制限の例

- 踏み台攻撃の防御
  - ホストBのinetdはrloginによるログインを拒否できる
    - ☞侵入経路情報により外部ホストZから侵入してきていることがわかるため



侵入経路情報の伝播

- 通信したプロセス間での伝播
  - OSリソースを介して伝播させる
    - ☞リソースにも侵入経路情報を記録する
  - プロセスからリソースへ
    - ☞データを書き込んだ時
  - リソースからプロセスへ
    - ☞データを読み込んだ時
- プロセスの親子間での伝播
  - 親プロセスから子プロセスへ
    - ☞子プロセスを生成した時



侵入経路情報を扱う上での問題

- 侵入経路情報は非常に大きくなる可能性がある
  - プロセス間で侵入経路情報を伝播させるオーバヘッドが大きくなる
    - ☞特に多数のホストと通信するサーバが侵入経路に含まれる場合
  - 侵入経路情報を検査するオーバヘッドが大きくなる
    - ☞侵入経路に含まれるホストを一つ一つ調べなければならない

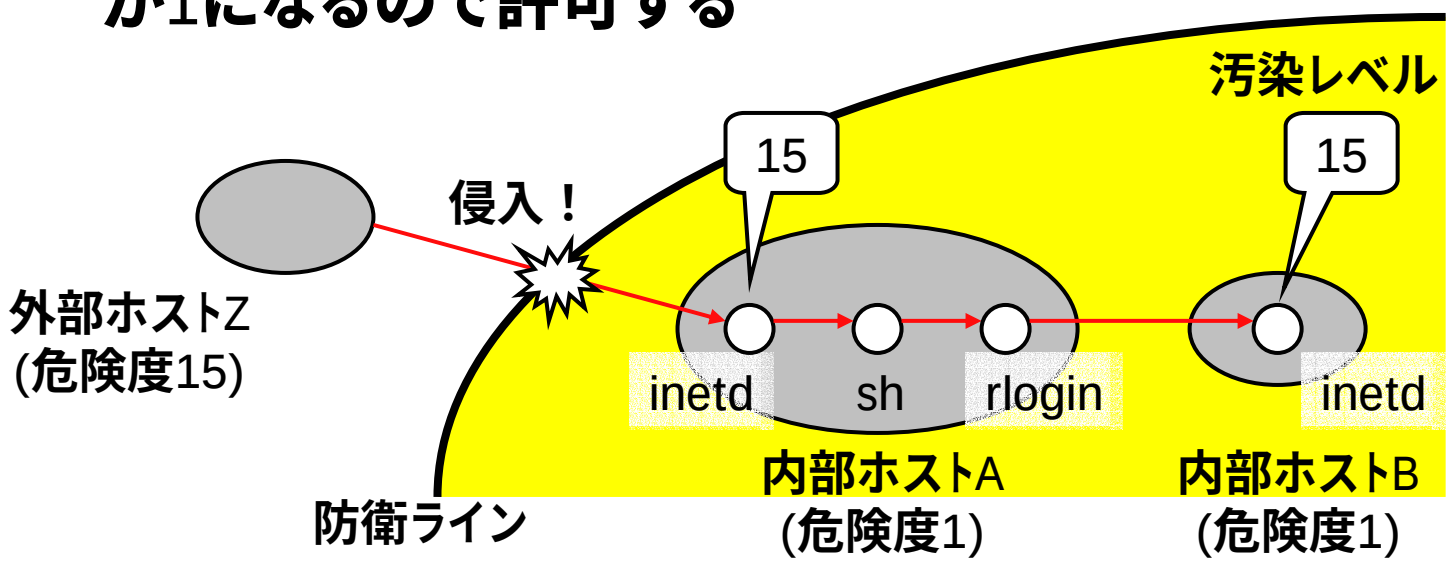
侵入経路情報を圧縮する必要がある

侵入経路情報の圧縮

- 汚染レベル
  - 侵入経路情報に含まれるホストの危険度の最大値
    - ☞セキュリティ上は最も危険度の高いホストを考えることが重要になる
  - 補助情報として危険度最大のホストのグループIDも併用する
  - 現在の実装では合計16ビット
- 圧縮された侵入経路情報はプロセスがどのくらい攻撃を受けているかを表していると考えられる
  - 汚染レベルの高いプロセスほど危険

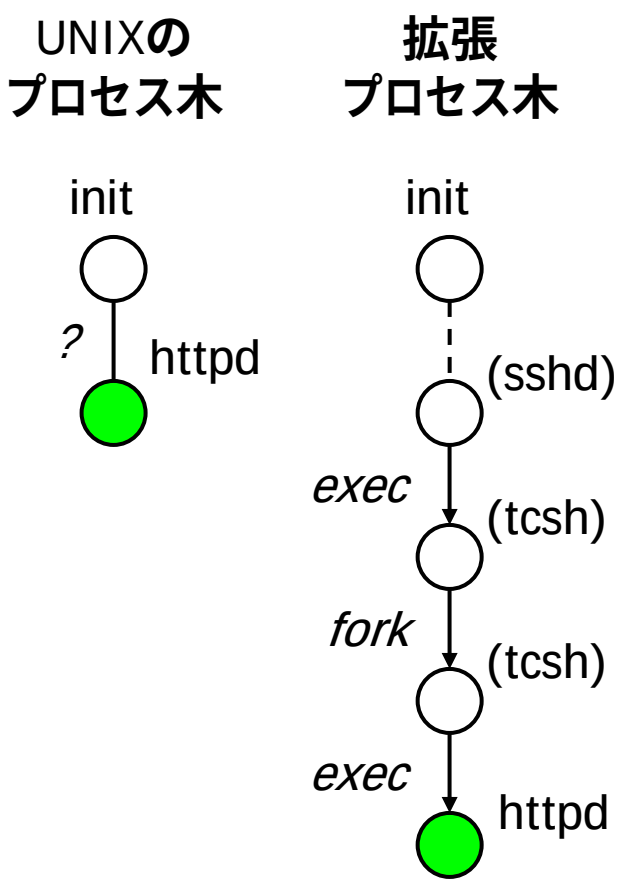
汚染を用いたアクセス制限の例

- ホストBのinetdは汚染レベルによりアクセス制限
  - 汚染レベルが15の時は外部から侵入されてrloginを実行されているので拒否する
  - 内部ホストAから直接rloginしてきた時は汚染レベルが1になるので許可する



プロセス木を用いた追跡

- 各ホストではプロセス木を使って細かい粒度で追跡を行う
  - 正確な親子関係が必要
- 拡張プロセス木を保持する
  - 子プロセスを持つプロセスは終了しても情報を残す
  - execする前のプロセスの情報も残す

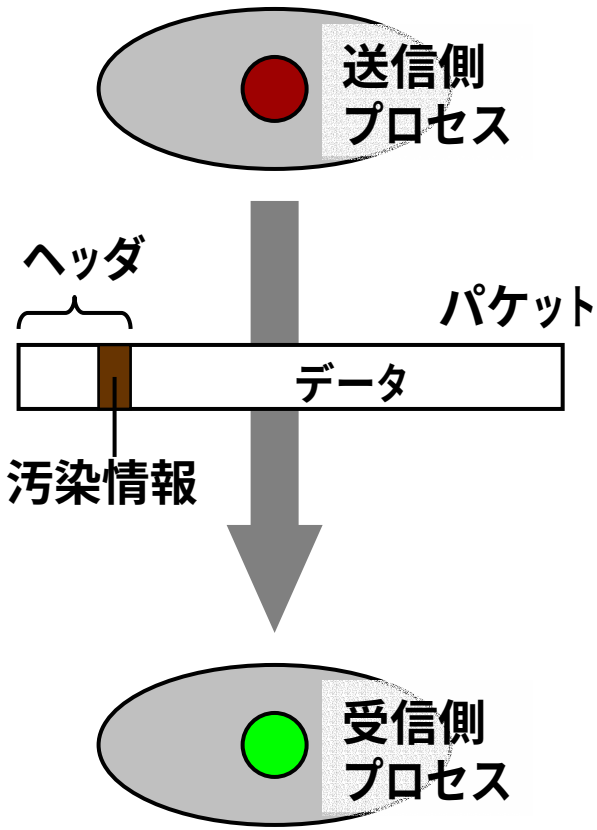


アクセス制限の記述

- システムコールレベルでアクセス制限を記述する
  - 汚染を条件として利用
    - ☞プロセスの危険度が高い時は時刻の変更を許さない
      - 🖫deny settimeofday at-plevel 2-15
  - 祖先プロセスの情報を条件として利用
    - ☞ftpで入ってきたらpasswdファイルは読ませない
      - 🖫deny read “/etc/passwd” via-prog “ftpd”
    - ☞rootであってもユーザkouraiがsuした時以外はkouraiのホームディレクトリへの移動を許さない
      - 🖫allow chdir “/home/kourai/” via-user kourai

ホスト間にまたがる汚染の伝播

- パケットのプロトコルオプションを使って汚染情報を送る
  - データ用パケットでピギーバック
  - TCPオプションで4バイトの増加
- 受信側プロセスは受け取った汚染情報を基に汚染レベルを更新する



実験

- 実験内容
  - 汚染伝播にともなうホスト間通信のオーバヘッド測定
    - ☞TCP/IPのレイテンシとスループットを測定
  - ポリシーチェックのオーバヘッド測定
    - ☞getpidシステムコールの実行時間を測定
- 実験環境
  - ＰＣ（PentiumII/400MHz、メモリ128MB）　2台
  - 100Mbpsのイーサネット
  - Compactoシステム(Linux 2.2.11ベース)

実験結果

- TCP/IPのレイテンシとスループットへの影響
  - レイテンシの増大は小さい
    - ☞3.7%(1 byte)
    - ☞1.0%(1430 bytes)
  - スループットの低下は0.6%でほとんど影響しない
- ポリシーチェックのオーバヘッド
  - ルールの有無をチェックするのに要する時間は40ns (getpidシステムコールの5.2%)
    - ☞一般的なシステムコールではこのオーバヘッドの割合はもっと小さくなる

関連研究

- Javaセキュリティ機構[Gong et al. 97]
  - メソッドの呼び出し元を追跡してアクセス権を検査する
  - プロセスの親子関係の追跡に似ている
- Deeds[Edjlali et al. 98]
  - リソースのアクセス履歴に基づきアクセス制御を行う
  - 1つのプロセスの中で行動を追跡している
- IDA[浅香97]
  - ログを基にログイン元の追跡を行いアクセス制限する
  - ログの改竄などの問題がある

Compactoの限界

- 汚染を正しく伝播できない場合がある
  - 内部ホストのカーネルが書き換えられた場合
  - パケットの送信元アドレスや汚染情報が詐称された場合
- リモート管理が難しくなる
  - リモートログインしてサーバプロセスを起ち上げるとそのプロセスが汚染されてしまう
    - ☞その結果、サーバプロセスの権限が制限される

まとめ

- 侵入経路情報の伝播によって行動追跡モデルを実現するシステムCompactoを開発した
  - 防衛ラインを突破されても侵入者の行動を追跡しアクセス制限できる
- 侵入経路情報を圧縮することによって、行動追跡モデルを効率よく実装した
  - TCPオプションを用いてホスト間で汚染情報を伝播させる

今後の課題

- TCP/IP以外のプロトコルでも汚染を伝播できるようにする
  - IPオプションを使って伝播する
- 汚染の伝播をうまく抑制できるようにする
  - 全く抑制しないと際限なく汚染が広がってしまい、実用的なシステムにならない
- パケットの送信元アドレスや汚染情報の詐称に対応できるようにする