JNSA
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

2007年度
セキュアOSのソリューションモデル実験に関する報告

グループリーダ　澤田　栄浩

セキュアＯＳ普及促進WG

2008 年 6 月13日

経緯と目的

I. インターネットを少しでも安全に利用できるよう社会貢献したい

II. 当該技術の普及促進をしたい

III. セキュア基盤（ＯＳ）を利用したソリューションモデルを考案したい

WG活動の概要

- 医療情報ネットワークの構築にＰＫＩ+ＶＰＮが用いられるようになった背景には、ＯＳＩの上位層での暗号化対策に脆弱性が多く含まれるという資料が公表されたことがきっかけ。
- セキュアＯＳも同様に下位層での最も基礎的な対策であるが、抵抗感が相変わらず根強い。

ＪＮＳＡのＤＭＺ設置サーバに対してセキュアＯＳを適用し、その過程も含めて広く公表していくことで多くの方にセキュアＯＳの本質を理解をしていただけるよう活動を展開することになった。

平成１９年度メンバー紹介

リーダー	澤田　栄浩（株式会社JTS）
メンバー	楠木　秀明（日本CA株式会社）
	栗原　実（株式会社富士通ソーシアルサイエンスラボラトリ）
	河本　高文（東芝ソリューションズ株式会社）
	田口 裕也（株式会社JTS）
	武田　健太郎（株式会社NTTデータ）
	冨田　高樹（みずほ情報総研株式会社）
	原田　季栄（株式会社NTTデータ）
	半田　哲夫（NTTデータ先端技術株式会社）
	三田　聖彦（インフォコム株式会社）
	やすだ　なお（JNSA／株式会社ディアイティ／サイバー大学）
協力	坂本　慶（株式会社ディアイティ）

実施すべき活動内容の検討

- セキュアOSは手軽に利用できるにもかかわらず活用されていない
- 実際に運用しているサーバにセキュリティ強化OSを導入してはどうか
- 得られた結果や知見を広く公開してはどうか

対象システム選定

- 対象システムの選定条件。
  - インターネットに接続されている情報システムであって、実証実験を通じてセキュアOSの有効性を客観的に検証可能であること
  - 実証実験の中立性・客観性の確保の観点から、使用するOSのベンダ等と密接な利害関係にあるような情報システムでないこと
  - 情報システムの運用主体において実証実験の活動の主旨についての理解が得られ、かつその協力を得られること

WGメンバーによる検討の結果、JNSA自体の事務局のwebサーバを本実験の対象システムとすることにした。

対象セキュアＯＳの選定

- **利用可能なセキュア**OS
  - OSS**では**SELinux, AppArmor, TOMOYO Linux
  - **プロプライエタリソフトウェアでは**HiZARD, PitBull, SecuveTOS, SHieldWare

- **今回の実験では、以下の理由から**TOMOYO Linux**を対象システムに導入することとした。**
  - **対象システムに搭載されている**RedHat Enterprise Linux 4 (RHEL4) **に対応しており、アプリケーションの入れ替え等の手間を省くことができる。**
  - **セキュア**OS**の導入・設定・運用という流れを、自動学習という機能を用いることでサーバ管理者自らが実施することができるので、導入時の負荷を軽減させることができる上に、導入実験としての今回の目的にも適している。**
  - **開発が日本で行われている上、開発メンバより本実験への支援が可能との回答を得ており、導入・運用における疑問点や障害の解消が容易となることが期待できる。**

実験環境の概要

- CPUはIntel i386アーキテクチャ
- ファイアウォールを経由してインターネットに接続
- 主なサービスはWebとメール
- サーバの管理作業にはSSHログインを使用
- 一般ユーザでのログインのみを認めている
- 管理者権限が必要な操作はsuコマンドで権限を取得の上で実施
- バックアッププログラムが定期的に動作

TOMOYO Linuxの導入実験

- 実現するセキュリティレベルについては、導入前に綿密に設計するのではなく、導入を進めながら、ポリシーの学習結果を見た上で検討する、という手法を取った。
- セキュリティ強化を段階的に実現していくという、「積み上げ式のセキュリティ強化」が可能であるTOMOYO Linuxの特徴を活かした導入方法とした。

サーバの運用実験

- TOMOYO Linuxの出力するログを読み、特定のログが出力されると管理者にメールで通知するスクリプトを作成。
- スクリプトは強制モード運用開始と同時にcronジョブとして登録。
- ポリシーに存在しないアクセスを要求し、そのアクセスがTOMOYO Linuxにより拒否されたことが1時間以内に管理者に通知されるようにした。

今後のセキュアOS普及にむけた知見

- 今回の実験ではWebサーバに特化したセキュリティ強化を実現した。
- Webサーバとそこから起動されるCGIの動作が通常発生する範囲内に制限されている。
- WebサーバやCGIにセキュリティホールが発見され、悪意のユーザに攻撃を仕掛けられたとしても、ポリシーに記述した範囲外の動作が行えない状態を実現。
- アクセス拒否が発生すれば必ず通知メールが送信されるように設定したことで、ポリシーに存在しない動作が要求されていないことが確認できる。

まとめ

- 今回のTOMOYO Linuxによるセキュア化を実施してみて感じたのは、「案外簡単だった」ということ。
- 予定外のプロセス実行をレポートしてくれるということが、普段の運用管理面でも思った以上に役に立つこと。

詳しくはパネルにて！！

JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

アドホック・パネル

JNSA Webサーバに“TOMOYO Linux”を導入してみました

パネルメンバー：

澤田栄浩 (JTS)
原田季栄 (NTTデータ)
やすだなお (JNSA/ディアイティ/サイバー大学)

モデレータ：

冨田高樹 (みずほ情報総研)

システム管理者の一人として

- Trusted OS、セキュアOSについての関心
- ちょっと古いWAFを使っていたが…
  - コントロールポイントが増える
  - パケットレベルしか見られない
- 管理者権限の整理
  - 程々の最小特権、権限分離
  - 外部からは十分なアクセス制御
- セキュアOSとしてのTOMOYOに注目
  - 建前的御託が少ないことに好感 ^^)

システム管理者の悩み

JNSA

- サーバのセキュリティ確保の悩み
  - 結構大変そう。色々なことを言われる…
  - 実際にセキュアなサーバを維持するのは大変
- 世の中的にも関心があるようだ…
  - 運用中のサーバを入れ替えるのは勇気が要る
  - セキュアOSの実環境での設定情報が少ない
- JNSAのサーバをサンプルにできないか…
  - これなら他でも使えそう…
  - 関係者の思惑が一致した

⇒　成果を生かそう！

WGとしての今後の活動は・・・

- 昨年度の実験内容の報告書を公開
  - 近日予定（実験上のトラブルは全て書きます）
- JNSAサーバ対応
  - 実運用の経過の観察
    - でも何も起こらない可能性大か
  - 昨年度未確認の機能についても、徐々に対応？
    - せっかくなので使ってみたい？
- TOMOYO Linux以外のセキュアOSも、もちろん研究したいと思ってます