NET&COM 2004

セキュアネットワークフォーラム

「営業担当者のための欲張りLinuxセキュリティ講座」

株式会社NTTデータ

技術開発本部

原田季栄

haradats@nttdata.co.jp

はじめに

本講演について

- 最近「セキュアOS」や「セキュリティ強化 Linux」という言葉を耳にする機会が増えました。おおいに興味はある、あるいは業務上必要になったが忙しくて調べる時間がないという方のために、40分間で Linux のセキュリティ上の課題とそれに対する対策の現状のポイントを解説します。

- 話題のSELinux（Security-Enhanced Linux）についてもとりあげますが、個別の技術内容の詳細ではなく、セキュリティ強化OSの背景にある考え方や全体像、またセキュリティ強化OSの限界や実際の運用上の課題等あまり知られていない部分についてスポットを当て、極力専門用語を排除し、本講演用に作成されたマルチメディア素材を使いながらわかりやすく解説します。

講演の狙い

- SELinuxを含め、Linuxのセキュリティ強化は「技術」という観点からは非常に難しいものですが、それに至る考え方や「概念」は実はシンプルです。

- そこで、個々の仕様や専門的な用語ではなく、その裏にある本質的な概念を営業担当者の方を含めこの分野のバックグラウンドを持たない方でも理解できるようにしようというのが本講演の狙いです。通常であれば何100時間もかけて調べなければわからないこと、あるいは個別のツールの評価からは見えにくい全体像を40分という短い時間に、しかも楽しく理解していただこうということで「欲張り」という言葉をタイトルに添えました。

講演で使用する素材について

- 技術系でない方々にもわかりやすくするため HTML, FLASH 等により インタラクティブ、ビジュアルな素材を作成しました。

- 本講演では FLASH により説明する予定です。

- 本資料は当日配布資料の事務局提出締切である１月２３日時点の内容であり、本講演で用いる資料では一部変更があるかもしれません（きっとあるでしょう）。

本講演の聞き方

- 講演を聞かれた方々が後日実際に個別の技術や情報を調べられるようにするため選択形式の「問題集」を当日資料として用意しました。

- それぞれの問題に対する回答は、講演の進行に伴い講師より説明がありますので、筆記用具をご用意の上、該当する箇所に丸印をつける等メモを残されますと講演終了後には、講演内容のサマリーとなります（そのままお持ち帰りください）。

- 回答を聞き逃した場合には、説明の終了後時間があれば各問題の回答の振り返りを行う予定ですが、それがない場合には後述する連絡先にお問い合わせください。

質問、サポート

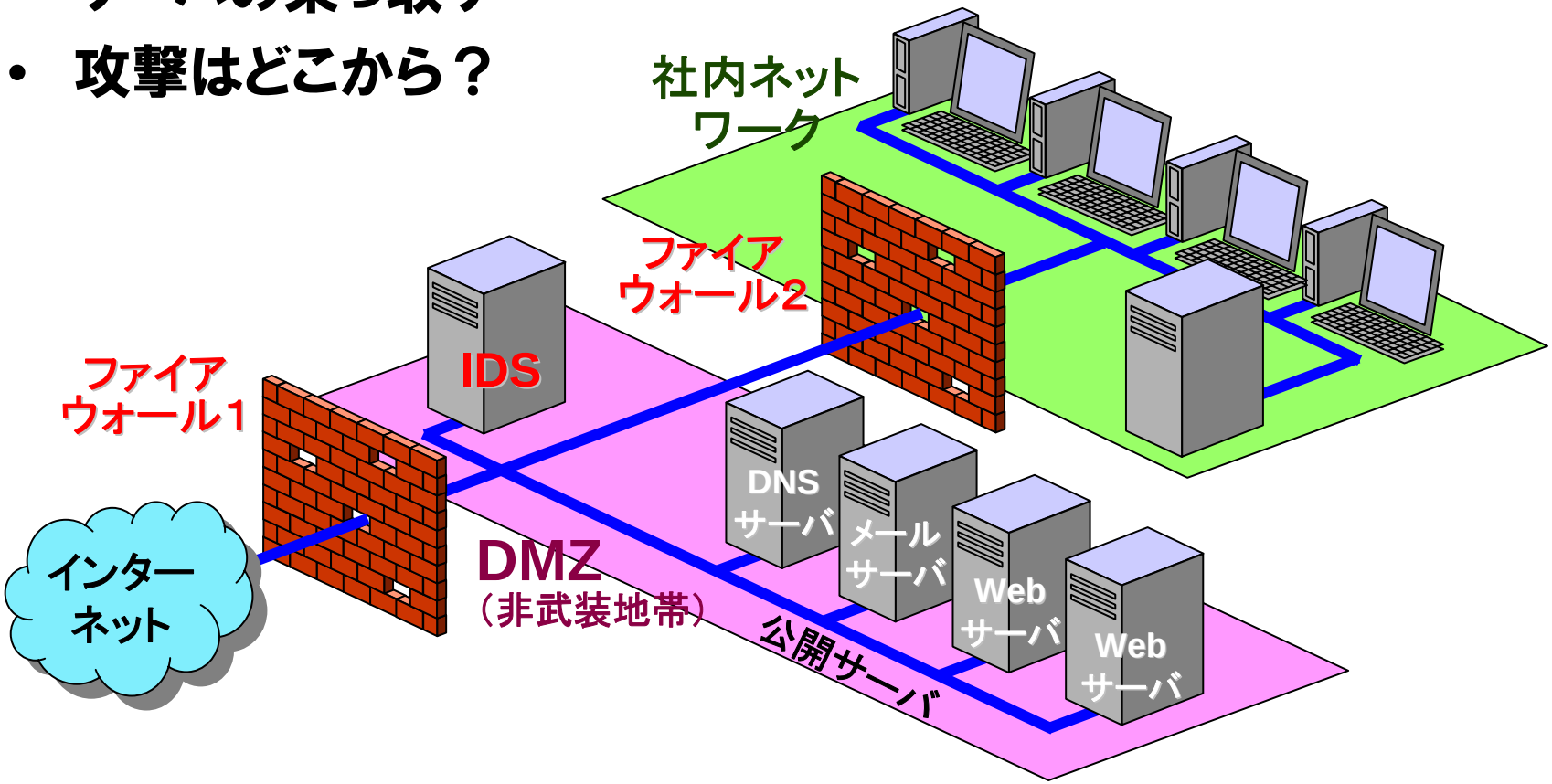
- **本講演のサポート用のメールアカウントを作成しています。**
  ご質問、ご意見、ご感想があればお気軽にメールください。

nc2004-ml@rd.nttdata.co.jp

本編はじまり

想定される被害

- ホームページの改ざん
- サーバの乗っ取り
- 攻撃はどこから？



攻撃の手順

- 「守る」ためには、「攻撃」の内容と手順の理解が必要。
- 典型的な流れ
  - web, ftp等のサービスを公開しているサーバにアクセス
  - サーバ上のプログラムの脆弱性(特にバッファオーバーフロー)を突いてそのプログラムを乗っ取る
  - サーバのシステム管理者権限を奪う
  - 色々悪いことをする
- そんなことが本当にできるの？
  - できます
  - 時間があればデモします

バッファオーバーフロー？

- Buffer
  - バッファー、緩衝材
- Overflow
  - 限度を超えて（over）流れる
  - 氾濫する。あふれる。

イメージを見てみましょう。

ファイアウォールとIDSの効果は？

どうすれば防げたか？

- 公開しない
- サービスを停止する
- anonymous（匿名）接続をさせない
- バッファオーバーフローを起こさせない

- 「リスクはゼロにはできない」

Linuxのセキュリティ

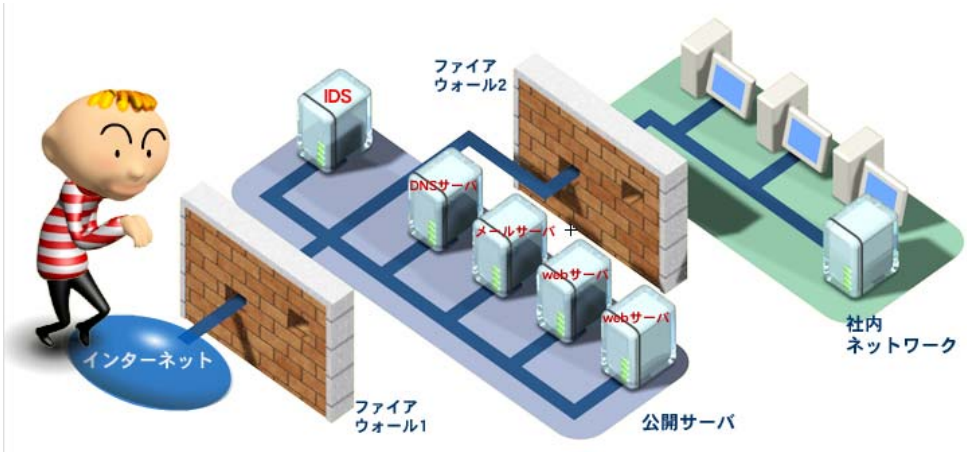
- ファイルやディレクトリの所有者がアクセス権を設定できる
  - 分類（アクセス権を設定できる単位）
    - 自分、グループ、その他の3種
    - グループに対するアクセス設定は1つしか登録できない（このグループには見せるが、このグループには見せない、という登録はできない）
  - 設定内容
    - 読める/読めない、書ける/書けない、実行できる/実行できない
    - 設定は粗いレベル
- root と呼ばれるシステム管理者権限を持つユーザは、設定の内容に関わらずアクセスできてしまう

何が困るかというと

- ネットワークから接続されてサーバのシステム管理者権限を奪われてしまうと、何でもできてしまう（サーバ室に入室して、管理者としてログインしたのと同じ状態になってしまう）

• これは困りませんか？

- サービスを提供している以上管理者権限を奪われる可能性はゼロにはできないので、権限を奪われたとしても完全に自由にはさせないようにしようというのがOSセキュリティ強化の基本。



強制アクセス制御

- 「強制アクセス制御」という手法を適用することによりセキュリティを強化できることがわかっています。
- 要するに、ファイルやディレクトリを含めたリソースに対するアクセスを厳密に監視して、判断し、問題ない場合だけ許すというものです。
- 判断をするには基準が必要で、それを「アクセスポリシー」と呼びます。
- いわゆる「全社セキュリティポリシー」等とはちょっとレベルが違うので注意しましょう。

Linuxの構造

- おさらい
  - Linuxのセキュリティにはちょっと問題がある
  - 「強制アクセス制御」というのを適用すれば良くなるらしい
- どうやって適用するかを知るには、少しだけ Linux の構造を知る必要があります。
  - カーネル（Linuxの全機能を実現する特別なプログラム）
    - 車におけるエンジンのようなものです
  - システムコール（カーネルの機能を呼び出す関数群）
  - カーネルを取り替えることによりできることや機能が変わります。
  - つまり、「強制アクセス制御」を組み込んだカーネルを標準のカーネルと取り替えれば良いわけです。

ちょっと待って！

- そんなことをしたら普通のLinuxのプログラムが実行できなくならないの？（そんなものをLinuxと呼んでいいの？）

- **大丈夫です。**
- 置き換えるカーネルの「見た目」を普通のカーネルと同じにしておけば、プログラム達からは違いがわからず今までどおりに仕事をしてくれます。
- コンピュータの世界的には「インタフェースの互換性が保たれている」と言います。

SELinux

- SELinux（Security－Enhanced　Linux）とは米国家安全保障局（NSA）が実際にLinuxに強制アクセス制御を適用したLinuxです。
- 導入の手順は、
  - 普通のLinuxをインストールする
  - 強制アクセス制御対応のカーネルを作る（コンパイルする）
  - 普通のカーネルと置き換える
  - 最近はRPMでも導入できるようになりました
- カーネルの見た目は同じなので、それまで使っていたプログラムやLinux用のプログラムは今まで通りに使えます。
- 実装された強制アクセス制御はFLASKというプロジェクトで１０年近く研究開発された成果です。

SELinuxを使うということ

- プログラムの互換性が保たれているから、今まで通り？
- それだけではないんです。
  - アクセスを制限する内容（アクセスポリシー）を適切に運用するということが重要です。
  - デフォルトとして配布されているポリシーはテキストファイルで数万行あります。本当はこれを自分のシステムなり用途に合わせて作り直して使うべきですが・・・。
  - カーネルは、見た目は同じでも実際の処理は大幅に増えていますからパフォーマンスの低下は避けられません。
- SELinuxや強制アクセス制御はそれ自体がセキュアな環境を約束してくれるわけではなく、手段にすぎないことに注意しましょう。

他の実装はないの？

- 他のLinuxへの強制アクセス制御の実装として、
  - LIDS（Linux Intrusion Detection System）
  - RSBAC（Rule Set Based Access Control）
  - SubDomain

  等があります。
- SELinuxは、これらの中でももっとも細かなアクセス制御を行うことが可能であり（逆に言えば管理の負担も大きいということです）、NSAが開発、公開していることからも大きく注目されています。

「高信頼OS」って？

- 標準のOSに対して何らかのセキュリティ強化をしたものを「セキュリティ強化OS」、あるいは「高信頼OS（Trusted OS）」と呼びます。
  - 例えばプリンタの印刷待ち書類一覧も権限があるものしか見えなかったりとか、顧客毎にカスタマイズされて出荷されるOSもあるようです。
  - 主な用途は軍事、金融関係が中心と思われます。
- 「高信頼OS」と呼ばれるための明確な定義はありませんが、公的機関による認証を受けていることが違いであり、全て商用の製品となります。（位置付け的にオープンソースで高信頼OSが開発されることは考えにくい）
- 具体例としては
  - TrustedSolaris, Pitbull, VirtualVault 等

セキュリティ強化の基準

- 高信頼OSとして認定されるための基準、「セキュリティ強化」の基準は？
- TCSEC（Trusted Computer System Evaluation Criteria）
  - 1985年に DoD が発行
  - コンピュータシステムに求められるセキュリティの機能要件を定義（前述の「強制アクセス制御」もここで記述されている）
  - 認定自体は1999年に終了しているが、普遍的な内容により現在も参照され続けている。（「TCSECにおけるB1レベル相当・・・」のように）
- ISO 15408
  - 現在の国際的な規格だが、「機能要件」というよりは試験、証明、ドキュメントに関する内容。PP（Protection Profile）が機能要件に近い）。

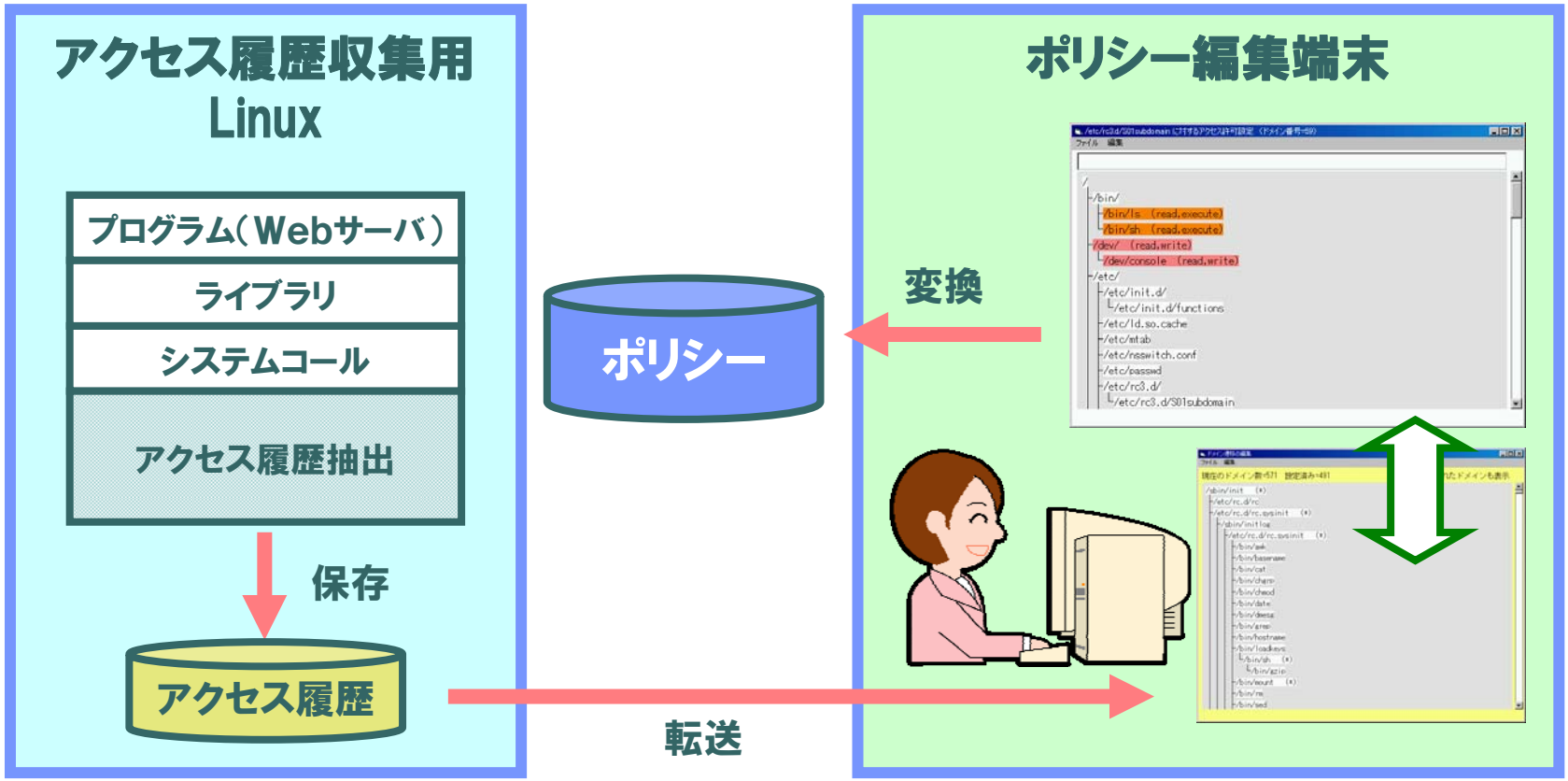
残されている課題は？

- セキュリティ強化OSや高信頼OSを正しく管理運用すること＝アクセスポリシーを適切に設定すること
- 用途にあったOSを選択すること
  - 「値段が高ければ良い」は間違い
  - 求められるレベル、考えられるリスクに適したものを
- コントロールを失わないこと
  - 高信頼OSを導入して、設定の変更もアウトソーシングしないといけなくなるとしたら・・・
  - セキュリティ強化OSを導入したとして、その運用は正しいかの検証が必要
- 限界を知る
  - 高信頼OSやセキュリティ強化OSにもバグは存在する
  - 最終的には物理的な保護が必要ではないか？

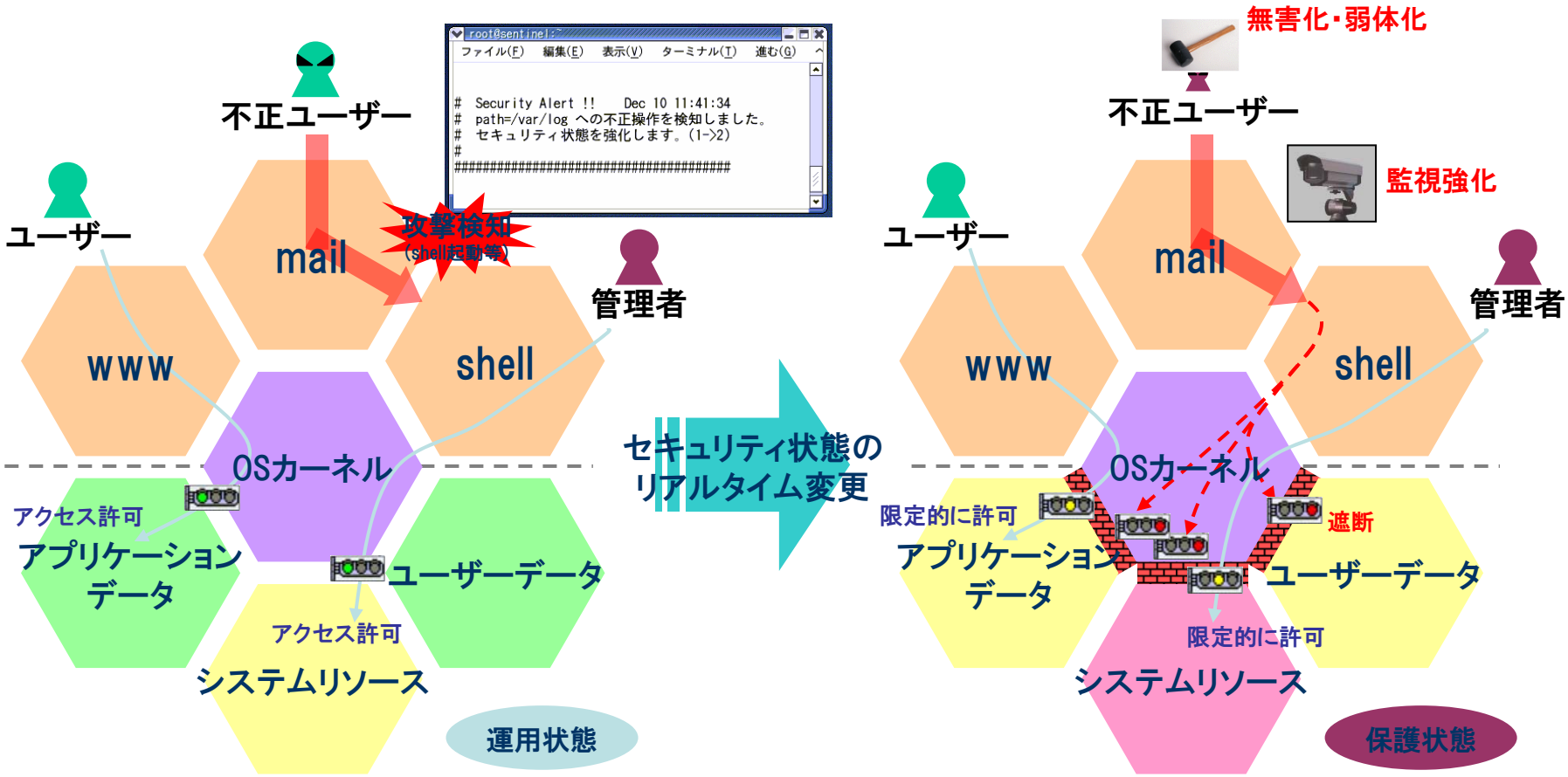
NTTデータの取り組み

- 「ポリシー自動学習機能付セキュリティ強化Linux 」・・・展示中
  - ポリシーの自動学習モードを備えた独自の強制アクセス制御カーネルを開発しました。
  - 実際にプログラムを実行させながらアクセス履歴を記録し、それをもとにポリシーを生成することができます。
- 「 Linuxカーネルベース不正侵入検知システム」・・・展示中
  - 不正なアクセスについて違反を検知したら、アクセス許可内容を自動的に制限したり、webコンテンツのメニューを限定したりできます。
  - SELinuxをベースに機能を拡張しました。
- 「書き換え不能メディアによる改ざん防止Linux」・・・展示中
  - LinuxシステムをCD－R, DVD－R, USBフラッシュ等の物理的に書き換えができないメディアに格納する全く新しい改ざん防止対策を実現しました。面倒なポリシーの運用を必要とせずに確実に改ざんを防止します。
  - Red Hatが動作するプラットフォームであれば容易に移植でき、SELinux同様プログラムの互換性は保たれています。

「ポリシー自動学習機能付セキュリティ強化Linux」



「Linuxカーネルベース不正侵入検知システム」

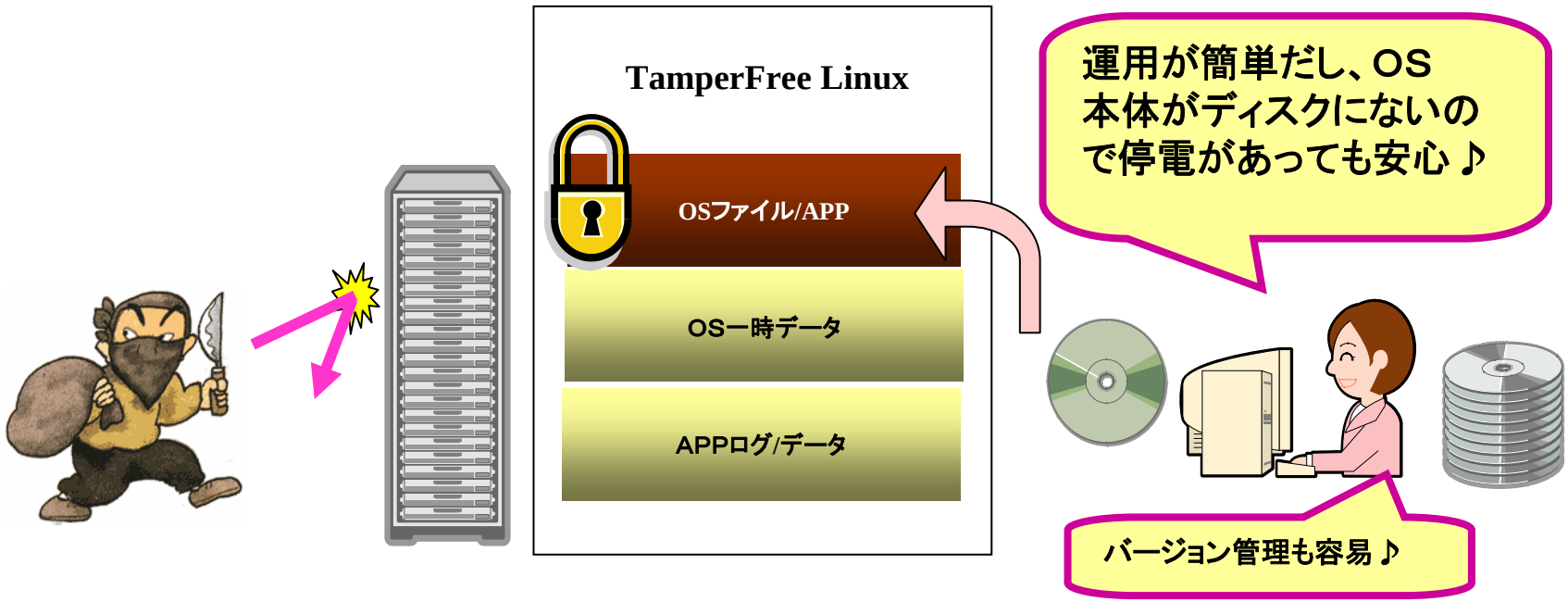


禁止アクセス行動をカーネルが検知

権限の縮小：不正アクセス防壁機構
監視強化：不正アクセス証跡の確保

「書き換え不能メディアによる改ざん防止Linux」

高価で難しい特殊OSを使わずに、web等セキュアな公開サーバを実現可能！



より詳しく知りたい方へ

- 本講演をお聞きになり、より詳しくセキュリティ強化OSやLinuxのセキュリティを学ばれたい方は、
  - SELinuxのFAQには非常によく整理された説明が掲載されています。本講演の次のステップとして、（できれば原文にて）お読みになることをお勧め致します。
    - http://www.nsa.gov/selinux/faq.html
  - SELinuxのメイン開発者の一人であるRussel氏のページに体験用サーバへのリンクや各種情報が掲載されています。
    - http://www.coker.com.au/selinux/

以上で本編は終わりです

展示について

- システム構築運用ゾーンの6830ブースにて弊社の開発した下記システムの展示を行っております。本講演の内容にも関連しますので是非お立ち寄りください。
  - 「ポリシー自動学習機能付セキュリティ強化Linux」
  - 「Linuxカーネルベース不正侵入検知システム」
  - 「書き換え不能メディアを利用した改ざん防止Linux」

講師紹介

- 氏名、所属：
  - 原田季栄 haradats@nttdata.co.jp
  - 株式会社NTTデータ　技術開発本部　オープンシステムアーキテクチャグループ

- 略歴：
  - 1985年北海道大学工学部卒。NTT横須賀電気通信研究所に入社。
  - 1991-1993年 MIT Center for Educational Computing Initiatives にてマルチメディアオーサリングシステムの日本語化に従事。その後webベースの社内ノウハウ共有システムの開発、BSデジタルデータ放送(システムおよびコンテンツ)の開発、営放システムの開発等を経て、2003年よりLinuxのセキュリティ強化に関する研究開発を行っている。