Linuxセキュリティ強化エッセンシャル

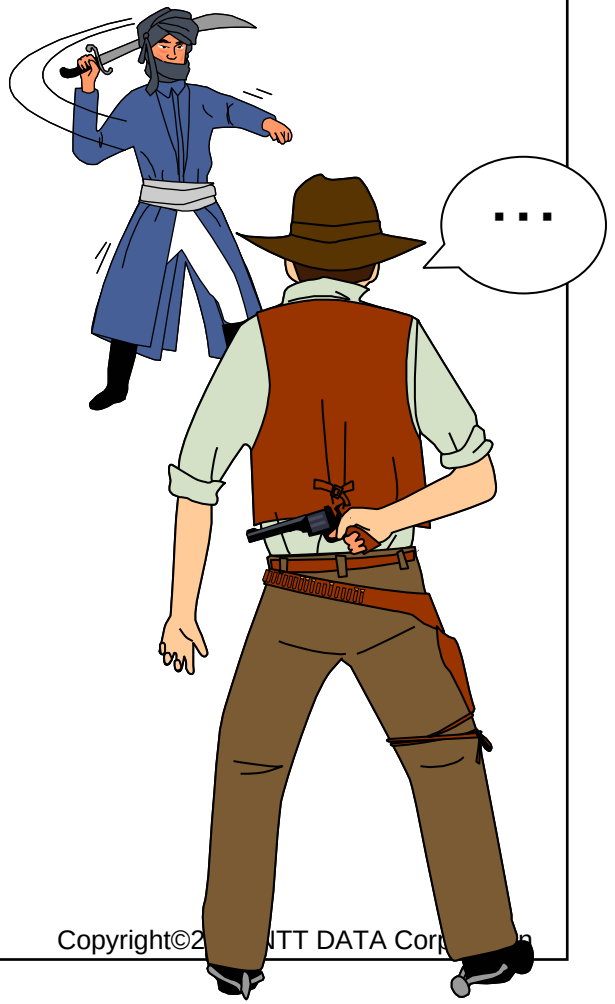
株式会社NTTデータ オープンソース開発センタ
シニアスペシャリスト 原田季栄 <haradats@nttdata.co.jp>

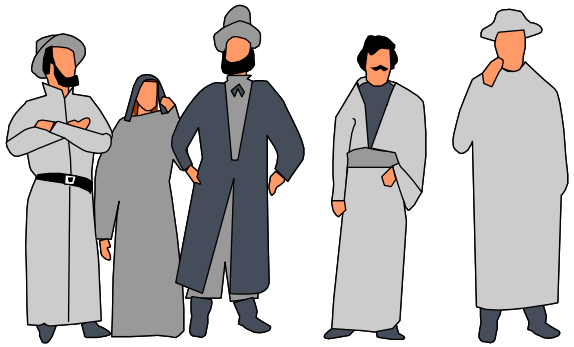
- 1時間で理解する「Linuxセキュリティ強化」のエッセンス
  - 既存OSが直面しているセキュリティ上の脅威とは
  - 既存のツールでは守れないのか
  - OSのセキュリティ強化が必要な理由
  - Linuxの「セキュリティ」は十分か？
  - セキュリティ強化OS、高信頼OS、「基準」
  - 「強制アクセス制御」とは
  - SELinuxについて
  - 残された課題
  - NTTデータの取り組み

考えられる脅威

KEYWORDS:

- 「セキュリティ強化」とは考えられる脅威への対策、予防策です。
- 脅威について正しく理解することが必要です。
- 「これで完璧」はありません。





ファイアウォールとIDS

KEYWORDS:

- 2000年頃から国内でもファイアウォールやIDS(侵入検知システム)の導入が定着しはじめました。
- ファイアウォールとIDSが装備されているシステムに対して攻撃が行われた場合について考えてみましょう。

ファイアウォールとIDS

KEYWORDS:

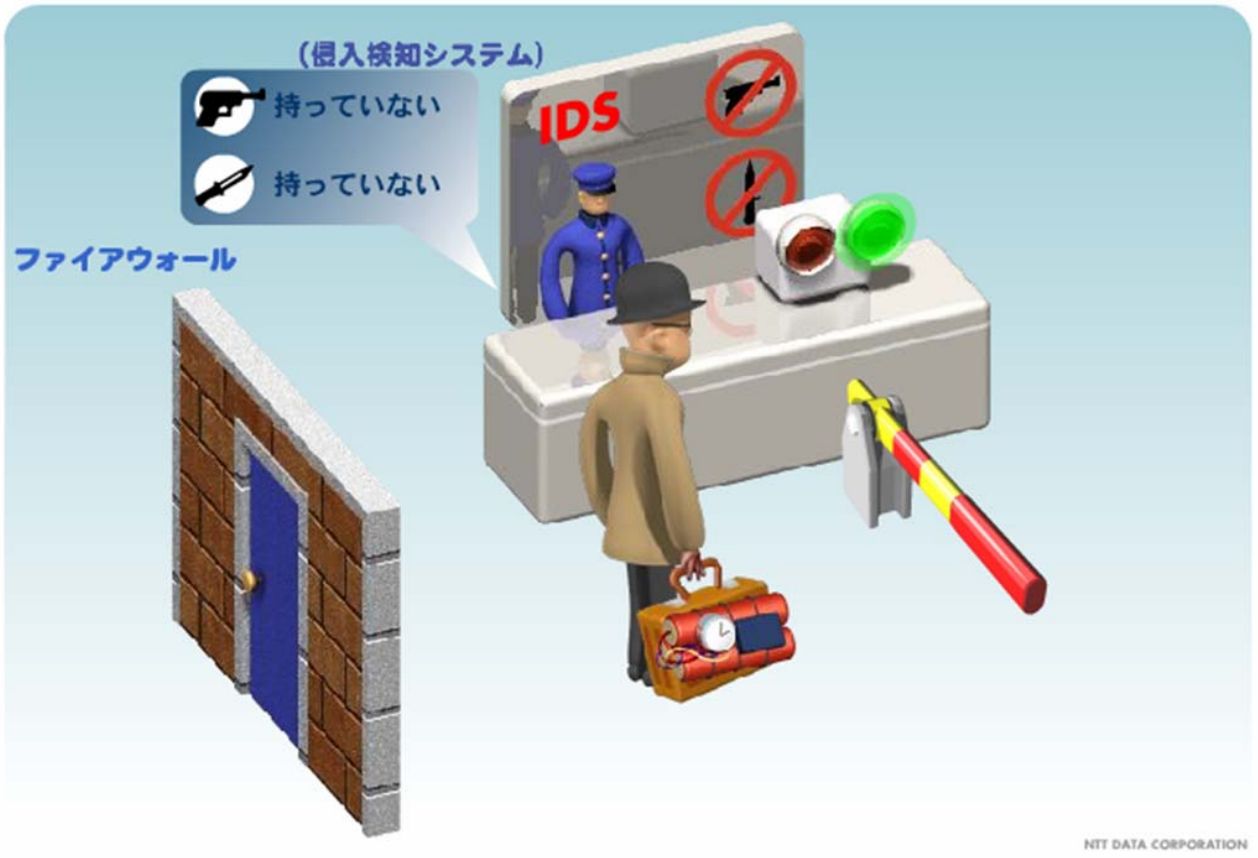
ファイアウォールとIDS

KEYWORDS:

- ファイアウォールやIDSは有効ではありますが、効果は限定的であり、それだけでは安心できません。

ファイアウォールとIDS

KEYWORDS:



バッファオーバーフローとは

KEYWORDS: バッファオーバーフロー

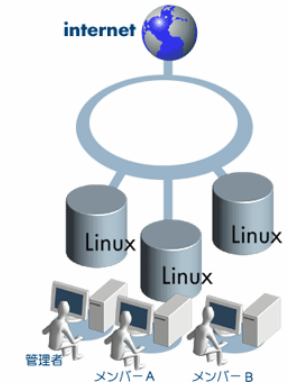
- システムの不正侵入に使われる典型的な手法が「バッファオーバーフロー」です。
- 意味
  - Buffer = バッファ、緩衝材
  - Overflow = 限度を超えて流れる。氾濫する。
- バッファオーバーフローには色々な対策が考案、実装されていますが、バッファオーバーフローはプログラムの欠陥なので、これを根絶することは不可能です。

バッファオーバーフローとは

KEYWORDS: **バッファオーバーフロー**

不正侵入のデモ

KEYWORDS: **バッファオーバーフロー**



- **実際に脆弱性を抱えるftpサーバに対して攻撃を行います。**
- **Linux上のftpサーバに対して、WindowsXPからプログラムを起動して攻撃します。**
- **ftpサーバからはftpクライアントに見えます。**
- **攻撃が成功した段階で、侵入者はそのサーバの管理者になってしまいます。**

OSセキュリティ強化の必要性

KEYWORDS: **バッファオーバーフロー**

- **ファイアウォールやIDSで防げる脅威はネットワークに関連するものに限定されており、サーバ内の脅威には対処できません。**
- **従って、内外からの脅威に備えるためにはサーバ自身のセキュリティを高めることが重要です。**

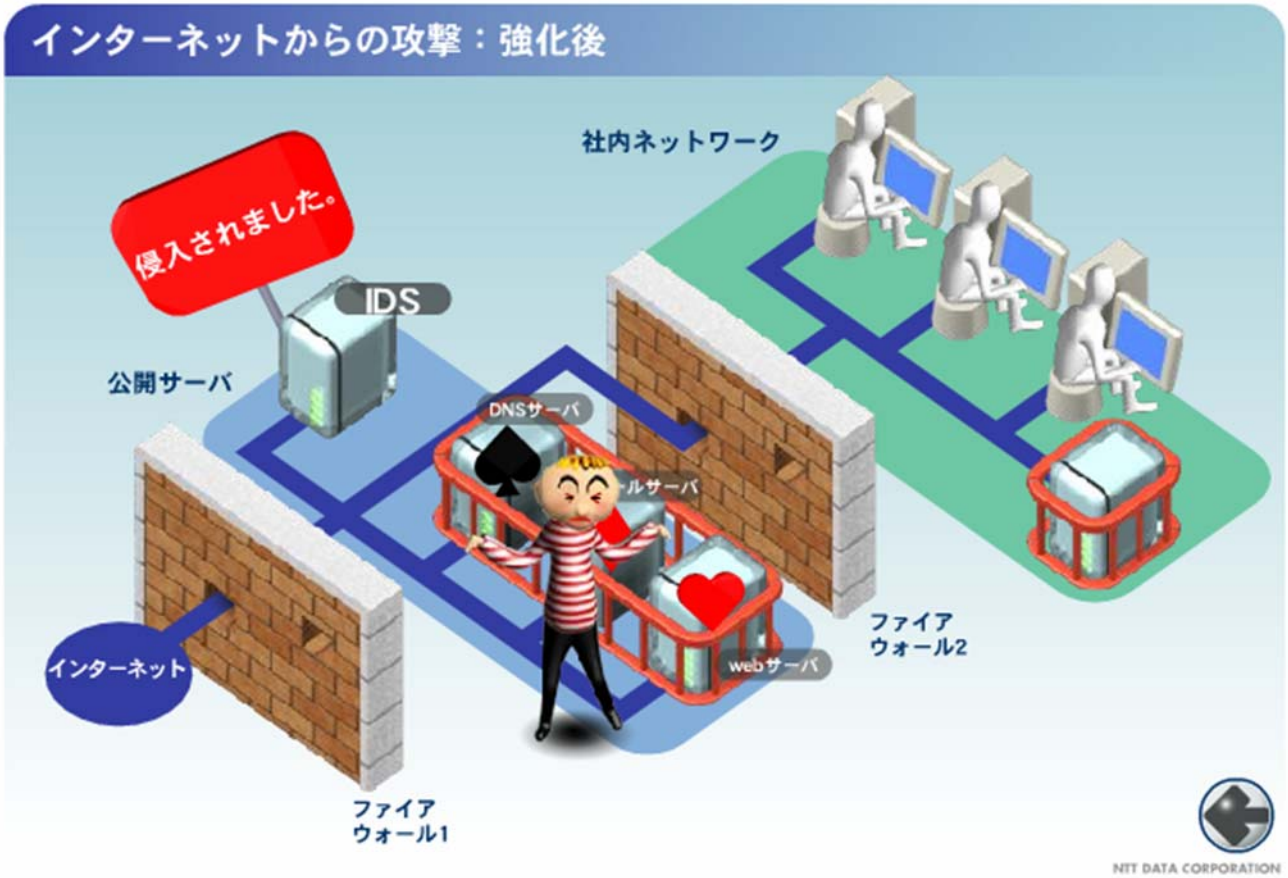
脅威を防ぐためには

KEYWORDS: **バッファオーバーフロー**

- **パッチを当ててOSを最新に保つことにより被害を受ける可能性を軽減することができます。**
- **しかし、パッチが適用されるまでの間や、新規の脆弱性に対しては無防備になってしまうことは避けられません。**
- **セキュリティを強化したOSを利用することにより、脅威に対するリスクを軽減することが可能となります。**

脅威を防ぐためには

KEYWORDS: **バッファオーバーフロー**



Linuxのセキュリティ

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)

- **Linuxが標準で備えているアクセス制御機構は、「任意アクセス制御（DAC）」と呼ばれます。**
- **ファイルやディレクトリの所有者は、自分自身、グループ、それ以外に対するアクセス権限を設定できます。**
- **システム管理者は、全てのファイルやディレクトリに対するアクセス権限の設定内容を変更や無視できます。**

Linuxのセキュリティ

KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)

Linuxのセキュリティ

KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)

- **システム管理者は、設定の内容に関わらず任意のファイルやディレクトリにアクセスできてしまいます。**

Linuxのセキュリティ

KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)

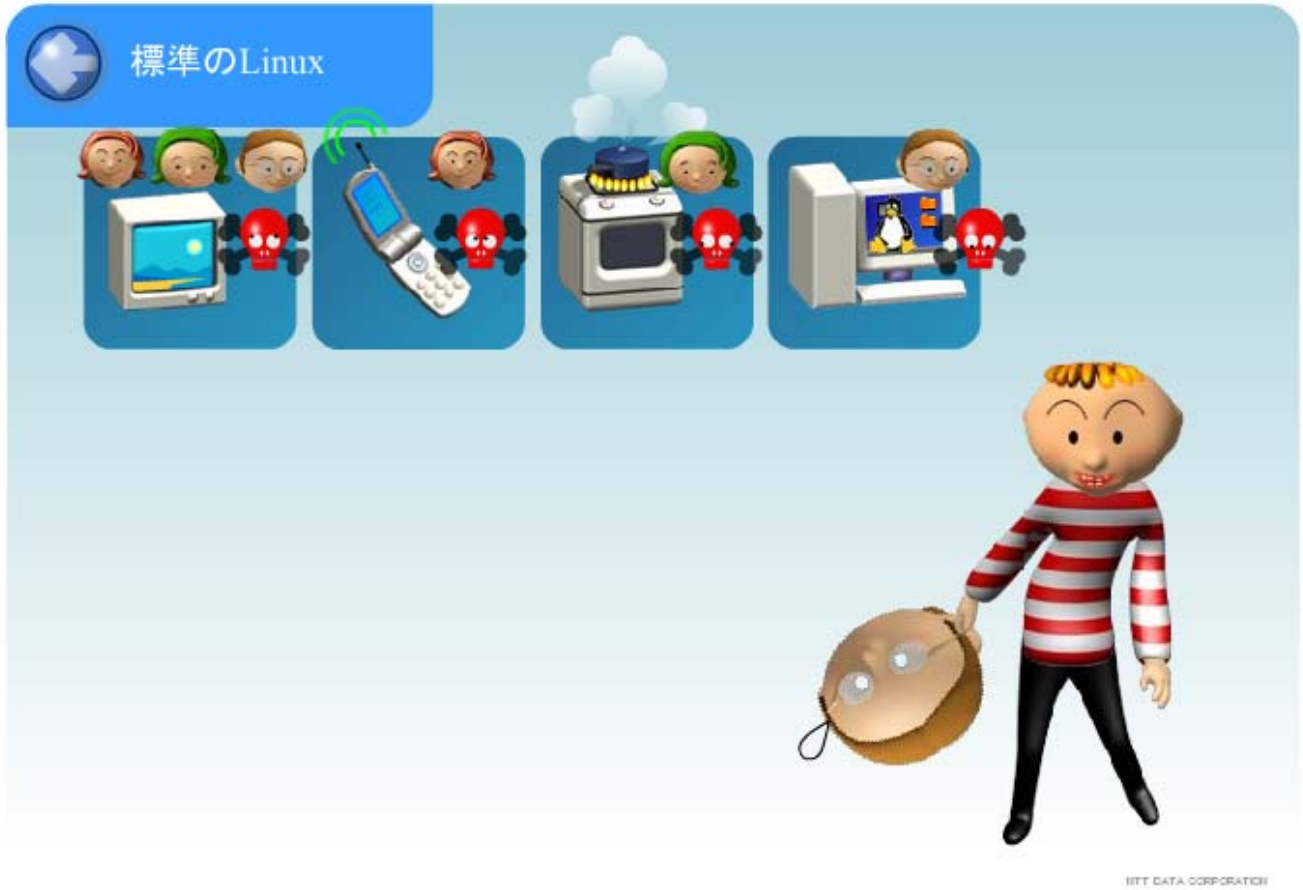
Linuxのセキュリティ

KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)

- **システム管理者が、設定の内容に関わらず任意のファイルやディレクトリにアクセスできてしまうということは・・・**
- **不正にシステム管理者権限を奪われると致命的な被害は免れられません。**
  - **ホームページ改ざん、ユーザの追加・削除、データの破壊、ホスト名やネットワーク設定の変更等**
  - **ログだって改ざん、削除できてしまいます**

Linuxのセキュリティ

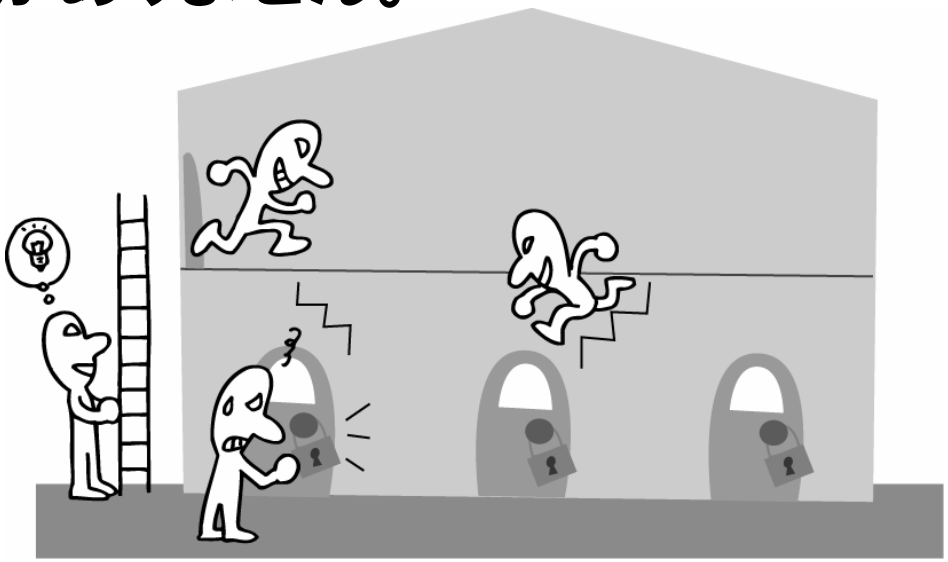
KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)



Linuxのセキュリティ

KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)

- **システム管理者以外のユーザがどんなにファイルやディレクトリへのアクセスを制限していても、システム管理者に対しては意味がありません。**



OSセキュリティ強化の原則

KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)

- 「最小権限」
  - 本当に必要な権限しか与えない
- 「区画(コンパートメント)化」
  - 実行されるプログラムに対し、OSが提供する資源へのアクセスを制限する。
    - UML (User Mode Linux), chroot, FreeBSD jail 等
- 「厳格なアクセス制御」
  - アクセス要求を無条件で処理しないで、利用要求毎にその適否を判定し、適切な場合のみ機能を提供する。
    - 「強制アクセス制御 (MAC)」

セキュリティ強化OSの効果

KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)

- セキュリティを強化したOSは一般に以下のような効果を持ちます。
  - システムが完全に乗っ取られる状態の阻止
  - プログラムやデータの改ざんの抑止
  - 詳細な履歴情報(ログ)の採取
- 標準のOSでこれらを実現することは不可能です。
  - 何故でしょうか？

セキュリティ強化OS、高信頼OS

KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS

- ネットワークからの攻撃を防ぎ、内部犯による情報漏洩を予防するためにセキュリティを強化したOSを「セキュリティ強化OS」と呼びます。
  - SELinux, LIDS, RSBAC 等
- セキュリティ強化OSの中でも特に公的機関による認定を受けたものを「高信頼OS」と呼びます。
  - Trusted Solaris, VirtualVault 等

セキュリティ強化の「基準」

KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS, TCSEC, ISO/IEC 15408

- 以下のものがよく知られています。
- TCSEC（Trusted Computer System Evaluation Criteria）
  - 1985年に米国防総省（DoD）が発行
  - 1999年に認定が終了していますが、その普遍的な内容により現在も参照され続けています。
  - http://csrc.ncsl.nist.gov/secpubs/rainbow/std001.txt
- ISO/IEC 15408
  - 「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が中心。

「強制アクセス制御」について

KEYWORDS: **バッファオーバーフロー、任意アクセス制御**(DAC)、**最小権限、強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408

- **OSセキュリティ強化の原則の中でもっとも重要なのは、「厳格なアクセス制御」です。それを実現するひとつの方式に「強制アクセス制御」があります。**
- **「強制アクセス制御」では、OSが管理する資源や機能に対するアクセス要求の許否判定を、システム管理者でも回避できないように強制的に実施します。**
- **英語では、MAC（Mandatory Access Control）と呼ばれます。**

「強制アクセス制御」について

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408

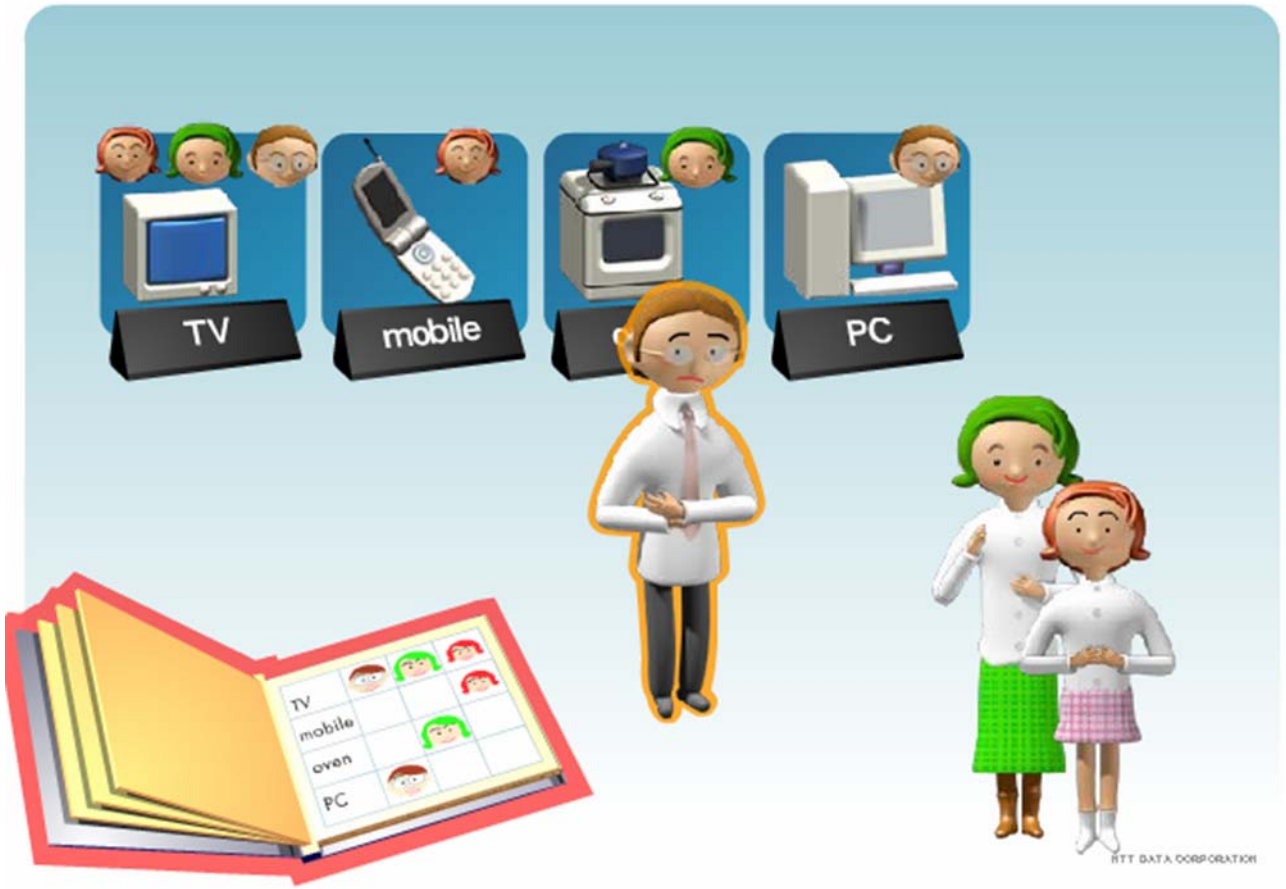
「強制アクセス制御」について

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**

- **「判断する」ためには、その基準となる「ポリシー」が必要です。**
- **「強制アクセス制御」はポリシーに従って動作するので、適切なポリシーを定義しないとセキュリティ強化を達成できません。**

「強制アクセス制御」について

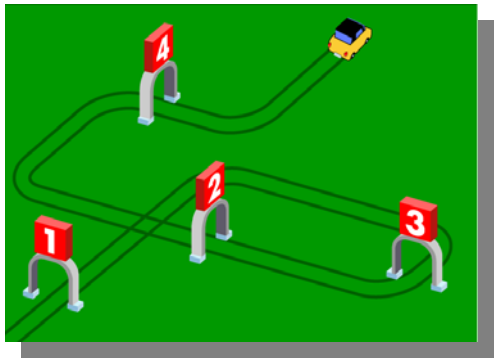
KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**

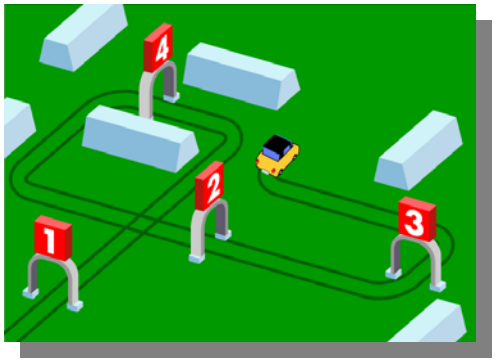


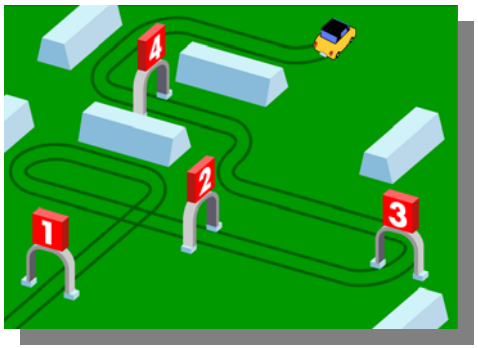
ポリシーについて

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**

- **ポリシーは細かく記述すればするほど効果が大きいですが、管理者の負担は増大します。**







SELinuxについて

KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS, TCSEC, ISO/IEC 15408、ポリシー、SELinux

- SELinux（Security-Enhanced Linux）
  - http://www.nsa.gov/selinux/
- 米国家安全保障局（NSA）が開発、公開している、強制アクセス制御を追加したLinux。
- Linuxカーネルのversion 2.6から標準で含まれており、すぐに使えます。
- プログラムの状態(ドメイン)に応じた制御（DTE）、役割に応じた制御（RBAC）等に対応しています。

SELinuxの運用

KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS, TCSEC, ISO/IEC 15408、ポリシー、SELinux

- 「ドメイン」を定義し、
- 「ドメイン」間の遷移条件を定義し、
  - ドメインの粒度は管理者まかせ。プログラムの起動時に必ずドメインを遷移させればもっとも細かくできるが、非現実的。
- 「ドメイン」毎のアクセス許可条件を記述する。
- アクセス許可の粒度は「システムコール」
- （必要に応じて）RBACを記述する。
- 上記全ては管理者が定める「ラベル」に基づいて行われる。
- ラベル付けの正しさが全ての前提となる

SELinuxの運用

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **SELinux等の実装ではポリシーは、システムコール(カーネルに対するインタフェース)単位で記述します。**

SELinuxがあればOK？

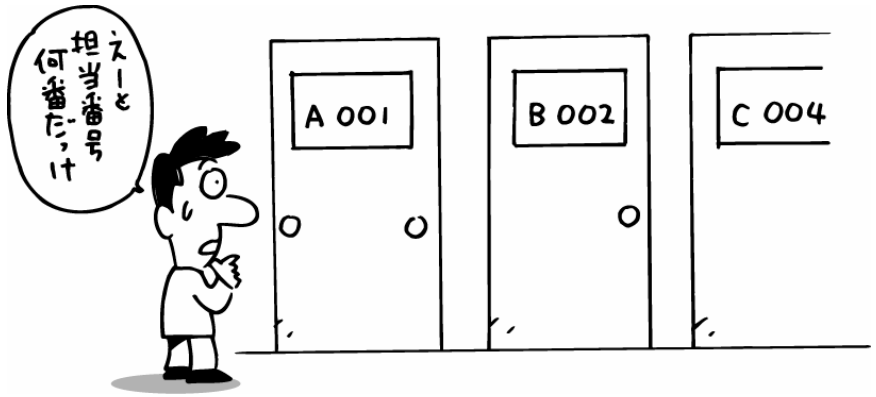
KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS, TCSEC, ISO/IEC 15408、ポリシー、SELinux

- 問題は「適切なポリシー」の管理運用
  - 「とりあえず動く」ようにするだけなら簡単＝ポリシー違反をかたっぱしからポリシーに変換して追加してやれば良い
  - それで良いの？（動けば良いならセキュアOSはいらない）

SELinuxがあればOK？

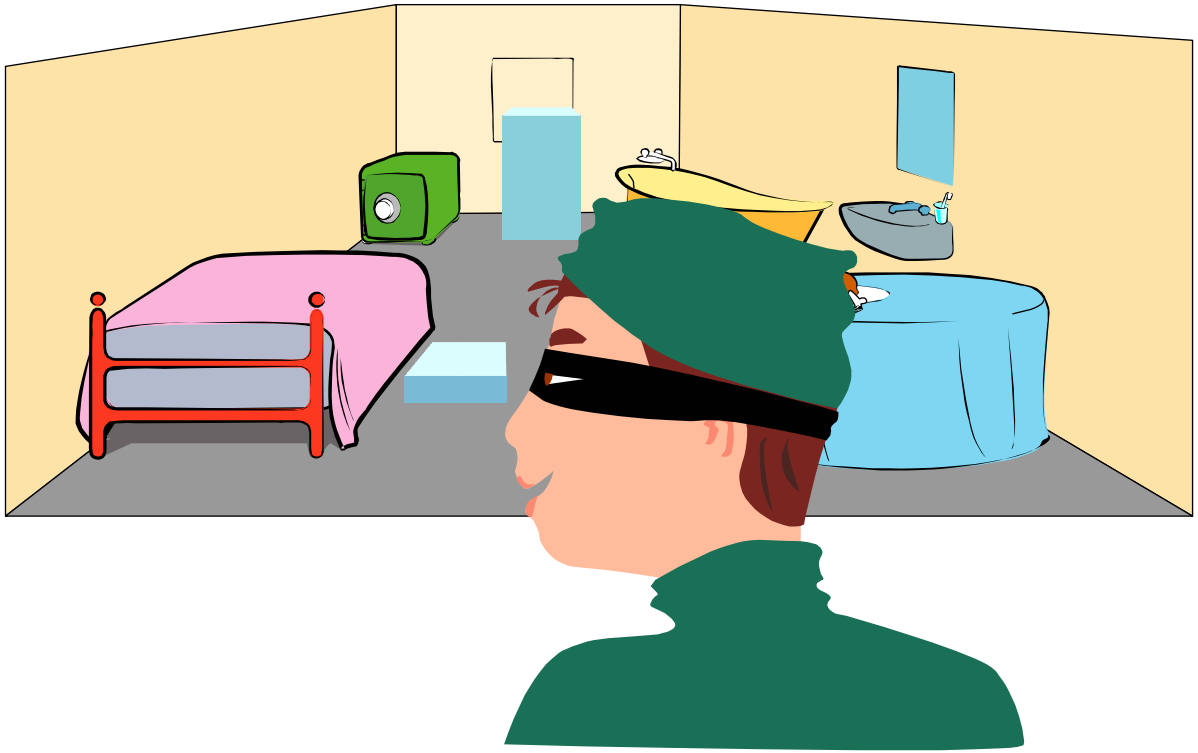
KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **問題は「適切なポリシー」の管理運用**
  - **詳細なポリシーを書き下ろすのは非常に困難**
  - **ファイル名、ディレクトリ名を直接使えないのはわかりにくい・・・**



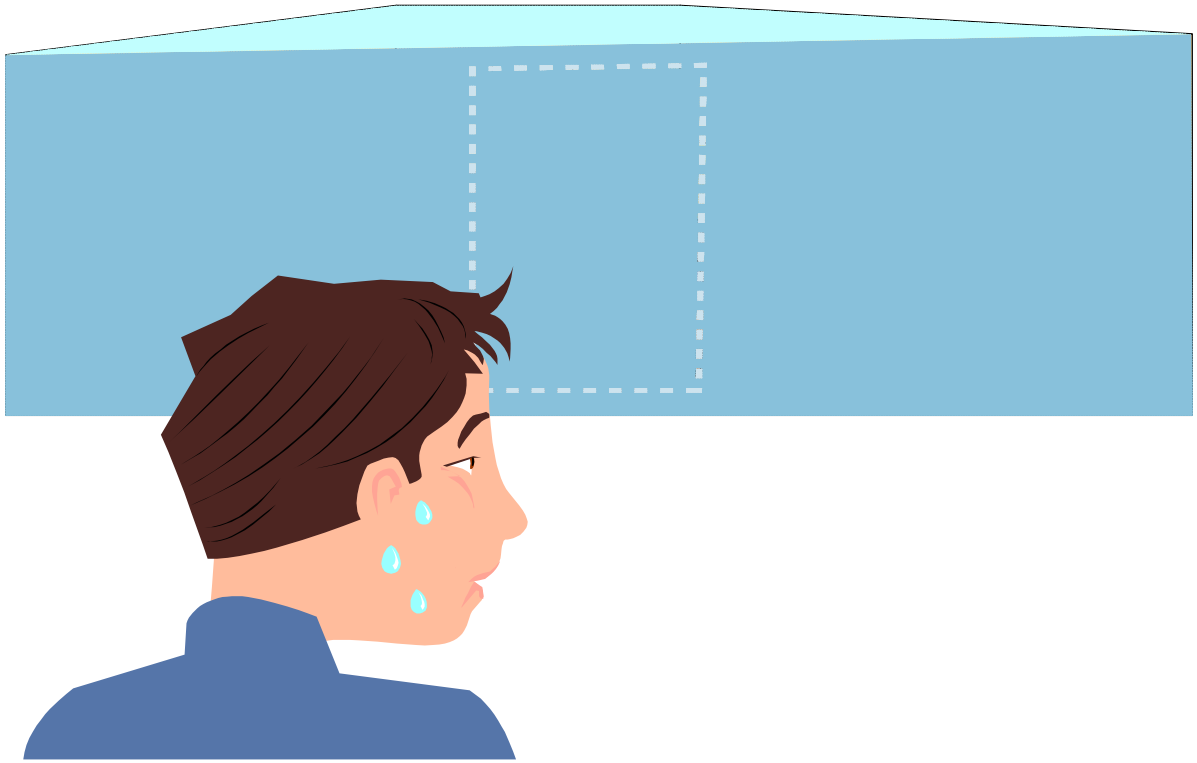
こんなセキュアOSの運用は××だ

何も保護されていない・・・。



つまらないものだけ保護している･･･。

必要なものが使えない･･･。



ログインすらできない・・・。

残された課題

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **セキュリティ強化OSの限界**
- **管理運用**

NTTデータの取り組み

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **NTTデータではセキュリティ強化OSの現状に基づき多様な取り組みを行っています。**
  - **管理運用の負担が少ない独自セキュリティ強化OSの開発**
  - **SELinuxに不足している機能の独自拡張**

改ざん防止Linux

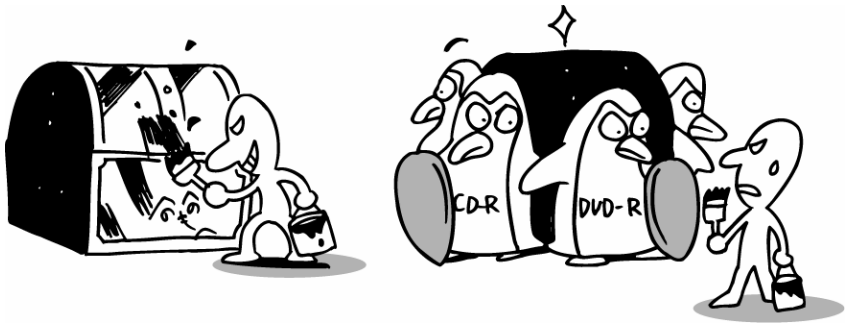
KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS, TCSEC, ISO/IEC 15408、ポリシー、SELinux

- Linuxを構成するファイルをread onlyなものとそうでないものに分類しました。
  - read onlyなもの = プログラム、ライブラリ、設定ファイルなど
  - そうでないもの = ログや一時ファイルなど
- read onlyなものは、CD-R, DVD-R, USBフラッシュメモリに格納してそこから起動するようにしました。
- ソフトウェアによらない**物理的な改ざん対策**として、Linux Conference 2003で発表しています。
  - http://lc.linux.or.jp/lc2003/30.html

改ざん防止Linux

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **セキュリティ強化OSも高信頼OSも、ソフトウェアでこれを実現している場合、それ自体の不具合を持つ可能性があります。**
- **物理的な改ざん防止は、これを破ることはできません。**



ポリシー自動学習Linux

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **セキュリティ強化OSの運用で問題となるポリシーを自動的に学習するLinuxを作ってみました。**
- **Linux Conference 2004で発表しています。**
- **「学習モード」で起動させ、プログラムの実行、必要な操作を行うとそれらを行うために必要なポリシーを自動的に学習、保存します。**

ポリシー自動学習Linux

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

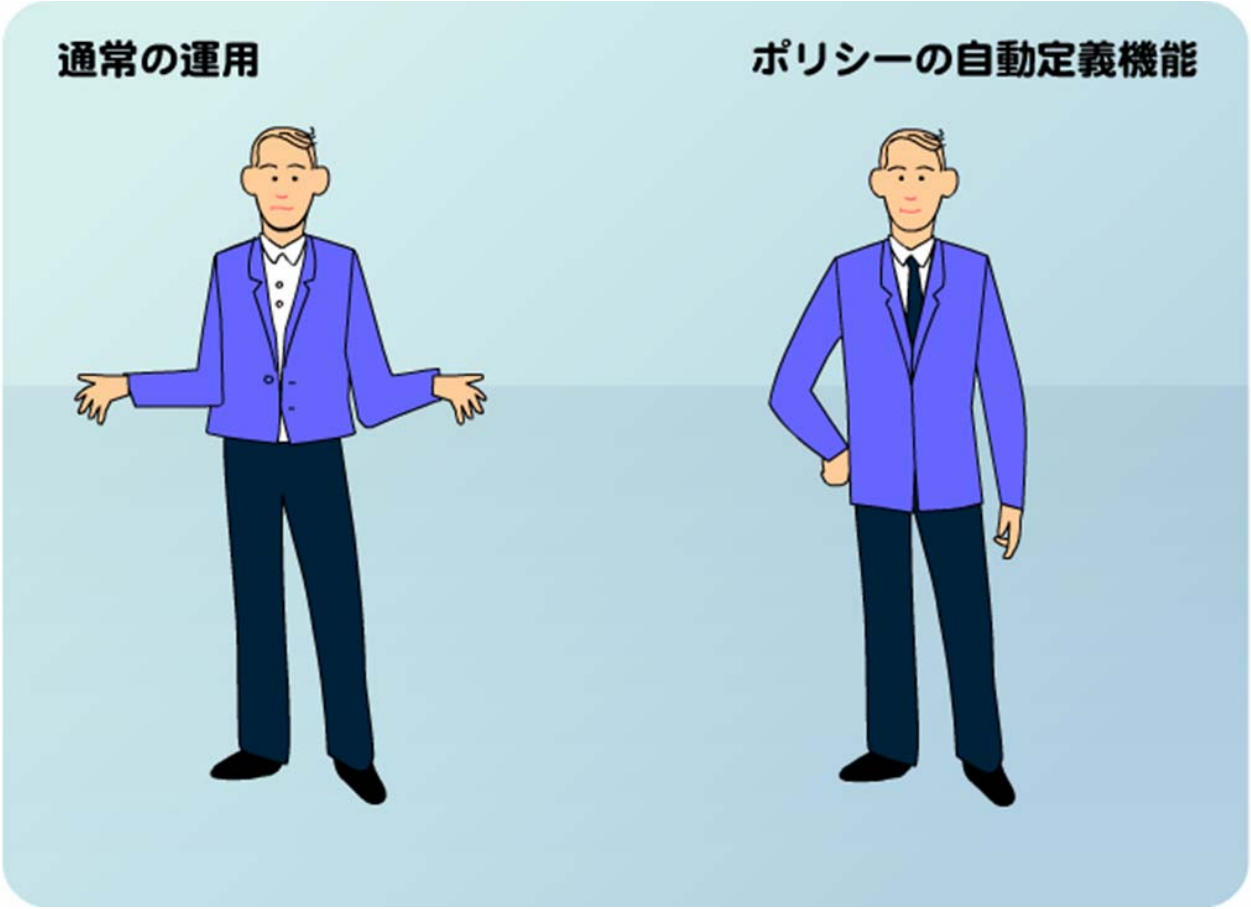
ポリシー自動学習Linux

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **SELinuxを含めて、ポリシー自動学習をできないシステムではどのように運用されているのでしょうか？**
- **デフォルトのポリシーを修正している場合がほとんどでしょう。**
- **「とにかく動くようにする」だけであれば、難しいことはありません。**
  - **エラーをポリシーに変換するツール等があります。**

ポリシー自動学習Linux

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux



ポリシー自動学習Linux

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **ポリシーは、単一のテキストファイルで構成されており、ファイル名やディレクトリ名をそのまま使えるので、確認や編集がとても簡単です。**

改ざん防止とポリシー自動学習

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **改ざん防止Linuxとポリシー自動学習Linuxを組み合わせて使うことも可能です。**
- **絶対に改ざんできないし、不要なアクセスも一切許しません。**
- **強力だけど簡単に使えます。**

キーワードのおさらい

KEYWORDS: **バッファオーバーフロー**、**任意アクセス制御**(DAC)、**最小権限**、**強制アクセス制御**(MAC)、**セキュリティ強化**OS、**高信頼**OS, TCSEC, ISO/IEC 15408、**ポリシー**、SELinux

- **バッファオーバーフロー**
  - 想定外の大きさのデータを送り込み入力用バッファをあふれさせる。乗っ取りに利用される手法。
- **任意アクセス制御**（DAC: Discretionary Access Control）
  - Windows, Linux等が標準で備えるアクセス制御
- **最小権限**（Least Privilege）
  - 人やプログラムに不必要に過大な権限を与えない
- **強制アクセス制御**（MAC: Mandatory Access Control）
  - ポリシーに基づく厳格なアクセス制御
  - OSセキュリティ強化の基本的な手法
- **セキュリティ強化OS、高信頼OS**
  - 標準のOSのセキュリティを強化したもの
  - セキュリティ強化OSの中で公的機関による認定を受けたものが高信頼OS
- TCSEC, ISO/IEC 15408
  - OSセキュリティ強化の基準。歴史的に推移している。
- **ポリシー**
  - アクセス要求の諾否を判断するための基準
- SELinux（Security-Enhanced Linux）
  - NSAが開発、公開しているセキュリティ強化Linux
  - http://www.nsa.gov/selinux/

参考資料・お問い合わせ

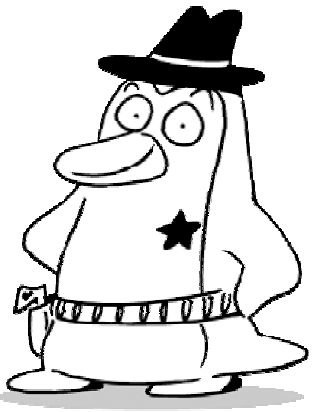
KEYWORDS: バッファオーバーフロー、任意アクセス制御(DAC)、最小権限、強制アクセス制御(MAC)、セキュリティ強化OS、高信頼OS, TCSEC, ISO/IEC 15408、ポリシー、SELinux

- 日経システム構築 2004年4月号 no.132「セキュアなシステムを作る(3つの原則に従いOSの機能を強化)」
  - 本講演の内容を含め、OSのセキュリティ強化全般に関して記述しています。
- IPA セキュリティセンター
  - http://www.ipa.go.jp/security/awareness/vendor/software.html
- SELinuxホームページ
  - http://www.nsa.gov/selinux/
- ご不明な点、ご質問はメールください。
  - haradats@nttdata.co.jp

いかがでしたか？

今日ご紹介した内容はLinuxのセキュリティ強化ですが、
その考え方は必ずしもLinuxに固有のものではありません。
セキュリティ強化OSの研究開発の起源は1980年代に
さかのぼります。その当時は、ブラウザはおろか電子メールも
ごくごく限られた人たちにしか利用されていませんでした。
勿論何百万件もの情報漏洩は起こりようもありません。
現代を生きる我々は、IT社会の便利さの裏にあるリスクと
脅威を意識して、そこから自分と資産を守ることが不可欠では
ないかと思います。限られた時間で「エッセンス」を理解
いただくためにひとつひとつの素材を心を込めて準備しました。
今日の講演が皆様のご参考になることを心より願って
やみません。どうもありがとうございました。

株式会社NTTデータ　原田季栄



presented by

NTT DATA CORPORATION