

# Windows NTシステムにおける セキュリティ管理とそのポイント

塩月 誠人 <shio@ccs.co.jp>

セントラル・コンピュータ・サービス株式会社  
インターネットビジネス部

## はじめに

### －コンピュータセキュリティとは？

- 機密性 ... 保護すべき情報が守られる
- 保全性 ... 改竄やなりすましを防げる
- 可用性 ... 安定・継続して利用できる

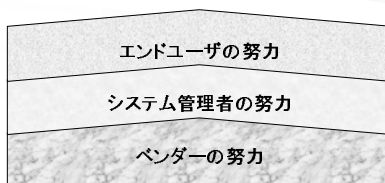
98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

2

## はじめに

### －セキュリティ向上のための努力



98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

3

## はじめに

### －セミナーの目的、スコープ

- NTシステム管理者を対象
- ネットワークOSとしてのNTセキュリティ
- OSが潜在的に保有するセキュリティ
- セキュアなコンフィギュレーション、運用方法
- 各種セキュリティ関連ツール、情報源の紹介

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

4

## はじめに

### －注意事項

#### • レジストリの編集について

- －「警告：レジストリ エディタの間違った使用は、修正のため Windows NT を再インストールしなければならないような、深刻なシステム障害を引き起こします。マイクロソフトではレジストリ エディタの使用の結果生じたあらゆる問題に関しては保証しておりません。ご了承の上ご使用ください。」(MSKBより)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

5

## はじめに

### －注意事項(つづき)

#### • 紹介する設定やツールについて

- －ここで紹介する各種の設定変更やさまざまなツール類については、事前にできる限り確認作業をしておりますが、場合によっては思わぬ結果を引き起こす可能性もあります。各々の情報源をご確認の上、ご自身のリスクで行なって下さいませよう、お願いいたします。

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

6

はじめに

– 注意事項(つづき)

• MSKB(ナレッジベース)の参照方法

- 文書中のQ?????は、MS KnowledgeBaseの記事ID
- <http://support.microsoft.com/support/kb/articles/q?????/???a.sp> で参照
- 文書中のJ?????は、日本語版KBの記事ID
- <http://www.microsoft.com/mscorp/worldwide/japan/support/kb/articles/j?????/???a.htm> で参照

Microsoft、MS-DOS、Windows、Windows NT は米国 Microsoft Corporation の登録商標です。文書中に記載されている会社名、製品名、サービス名は、各社の登録商標または商標です。

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

7

## 目次

- I. トータルセキュリティ実現のために
- II. NT4.0の標準セキュリティ機能
- III. NTにおけるセキュリティ上の問題点
- IV. セキュリティ対策のポイント
- V. 問題点ごとの対策
- VI. IISおよびIEに関するセキュリティ

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

8

## トータルセキュリティ実現のために

1. セキュリティポリシーとは
2. ネットワークレベルのセキュリティ
3. ホストレベルのセキュリティ
4. アプリケーションレベルのセキュリティ

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

9

トータルセキュリティ実現のために

### 1. セキュリティポリシーとは

– セキュリティポリシー(方針)とは何か

- サイトのセキュリティに関するルールの公式な表明
  - 明文化されている
  - 実現可能である
  - 組織内のすべての階層において受容・支持
- セキュリティ目標
  - 各人(管理者、ユーザ、...)が目指すべき到達点
  - トレードオフのものさし

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

10

トータルセキュリティ実現のために

– セキュリティポリシーはなぜ必要か

- 組織内全員のセキュリティに関する共通認識
- 組織外に対する明確な意思表示
- 行動のガイドラインの基礎
- 責任の所在の明確化
- セキュリティインシデントへの迅速な対処

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

11

トータルセキュリティ実現のために

– セキュリティポリシーの構築

- リスク分析(資産と脅威)
  - なにを守るのか?
    - » ハードウェア、ソフトウェア
    - » データ、利用者
    - » 社会的信用、...
  - なにから守るのか?
    - » 盗難、漏洩、損失、改竄、使用不能
    - » 外部からの攻撃、内部からの攻撃
    - » 不正アクセス、ウイルス、動的コンテンツ、...

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

12

トータルセキュリティ実現のために

– セキュリティポリシーの構築(つづき)

- サービス提供 対 セキュリティ
  - ユーザにどのようなサービスを提供するか
- ユーザビリティ 対 セキュリティ
  - 操作性の良し悪し
- 対策・復旧コスト 対 損失
  - セキュリティ対策のハード・ソフト
  - 性能のコスト(暗号化等)
  - 運用のコスト

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 13

トータルセキュリティ実現のために

– よいセキュリティポリシーとは

- 実現可能である
- 実行可能である
- 柔軟である
- 明解である
- ハードウェア・ソフトウェアとは切り離されている
- 担当および責任の所在が明らかである

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 14

トータルセキュリティ実現のために

– セキュリティポリシーの内容

- ハードウェア・ソフトウェアの調達ガイドライン
- プライバシー・ポリシー
- アクセス・ポリシー
- 責任ポリシー
- 認証ポリシー
- 可用性ポリシー
- 保守ポリシー
- 違反の報告に関するポリシー
- サポート情報

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 15

トータルセキュリティ実現のために

– セキュリティポリシーの閉じたループ

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 16

トータルセキュリティ実現のために

2. ネットワークレベルのセキュリティ

– セキュリティ対策の三つのアプローチ

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 17

トータルセキュリティ実現のために

– ファイアウォールの定義

- 「ファイアウォールとは、2つのネットワークの間におけるアクセス・コントロール・ポリシーを実現するようなシステム、あるいはシステムの集まりのことである。」(Internet Firewalls Frequently Asked Questionsより)
- アクセスコントロール
- ログの記録・管理
- 異常の検知、通知
- 認証、暗号化

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 18

トータルセキュリティ実現のために

#### – ファイアウォールの有効性

- 限定された個所でネットワーク全体を管理
  - ポリシの実装および検証が比較的容易
  - OSセキュリティフィックスのリスクを回避
  - 「すべての卵を一つの籠に入れ、それを監視せよ」
- LAN単位でのセキュリティポリシーを実現
  - 公開用ホスト群を設置するLAN
  - プライベートなLAN、等
- コンテンツセキュリティの実現
  - Viruses, Java, ActiveX, ...
  - アクセス制御を要するようなWebサイト、Webページ

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

19

トータルセキュリティ実現のために

### 3. ホストレベルのセキュリティ

#### – ホストセキュリティとは

- アクセスコントロール
  - 誰が、何に、いつ、をコントロール
- アカウンタビリティ
  - 識別、認証、利用記録
- オウディッタビリティ
  - システム内部の各種イベントログ
- ノーティフィケーション
  - イベント発生時の通知
- リカバリ
  - データリカバリ、システムリカバリ

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

20

トータルセキュリティ実現のために

#### – ホストセキュリティの有効性

- ホスト間のセキュリティ確保
  - 信頼できるホスト、信頼できないホスト
  - LAN上のパケット盗聴
- 物理セキュリティの補助
  - 信頼できるユーザ、信頼できないユーザ
- ダイアルアップ等により直接インターネットへ接続
- 公開サーバ(Web、E-Mail、DNS、...)
  - サービス提供のため、アクセスを許可
  - 要塞化が求められる
- Firewallマシン

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

21

トータルセキュリティ実現のために

### 4. アプリケーションレベルのセキュリティ

#### – サービスごとのセキュリティ

- SMTPサービス
- POPサービス
- DNSサービス
- WWWサービス
- ダイアルアップサービス
- ...

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

22

トータルセキュリティ実現のために

#### – アプリケーションセキュリティの特徴

- OSに統合されたセキュリティ
  - OSの認証、アクセス制御、ログ機能を利用
  - IIS、Exchange等
- OSに依存しないセキュリティ
  - 独自の認証機能等を持つ
- 業界標準、相互運用性が重要
  - SSL、S/MIME、APOP、CHAP、RADIUS、...

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

23

### NT4.0の標準セキュリティ機能

1. ユーザ認証
2. アカウントの原則
3. ユーザ権利の原則
4. NTFSファイルシステム
5. レジストリ
6. システム監査(イベントログ)
7. ドメインセキュリティモデル
8. その他の標準セキュリティ機能
9. TCSEC C2セキュリティ

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

24

NT4.0の標準セキュリティ機能

1. ユーザ認証

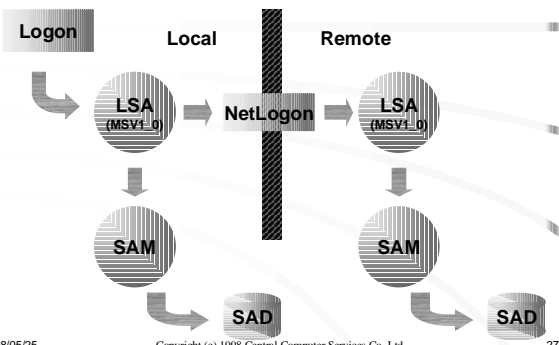
- ユーザおよびグループ
  - ユーザ単位の識別・認証
  - ユーザ、グループでアクセス制御を実行
- セキュリティID(SID)
  - ユーザ、グループ、マシンアカウントの識別子
  - コンピュータ名、システム時刻、スレッド時間からハッシュ生成

NT4.0の標準セキュリティ機能

- パスワード保護のメカニズム
  - One-Way-Function (OWF) ... ハッシュ化
  - さらに暗号化してレジストリに格納
- ネットワークログオン
  - チャレンジ・レスポンスによるネットワーク認証

NT4.0の標準セキュリティ機能

ユーザ認証のしくみ



NT4.0の標準セキュリティ機能

2. アカウントの原則

- パスワードの有効期間・変更禁止期間
- パスワードの長さ・一意性
- アカウントのロックアウト
- パスワード変更
- アカウントの無効

NT4.0の標準セキュリティ機能

3. ユーザ権利の原則

- ローカルログオン
- ネットワーク経由でコンピュータにアクセス
- オペレーティングシステムの一部として機能
- サービス・バッチジョブとしてログオン
- システムのシャットダウン
- その他

NT4.0の標準セキュリティ機能

4. NTFSファイルシステム

- ユーザ・グループによるアクセス制御
- NTFSパーミッションとシェアパーミッション
- ファイルオブジェクトの再利用禁止
- NTFSセキュリティ監査

### 5. レジストリ

- 多くのセキュリティ情報を一括管理
- ユーザ・グループによるアクセス制御
- レジストリセキュリティ監査

### 6. システム監査(イベントログ)

- ログオンとログオフ
- ファイルとオブジェクトへのアクセス
- ユーザ権利の使用
- ユーザとグループの管理
- セキュリティ原則の変更
- 再起動、シャットダウン、およびシステム
- プロセスの追跡

### 7. ドメインセキュリティモデル

- シングルログオン
- ユーザ・リソースの集中管理
- ドメインコントローラ
- ドメイン間の信頼関係
- ユーザプロファイルとホームディレクトリ
- ログオン制約(場所、時間)
- アカウントタイプと有効期限

### 8. その他の標準セキュリティ機能

- プロトコルフィルタ
- データバックアップ
- ディスク冗長構成
- パフォーマンスモニタ
- サーバマネージャ

### 9. TCSEC C2セキュリティ

- Windows NT 3.5 SP3で認定
- 任意アクセス制御
- オブジェクトの再使用
- 識別と認証
- 監査
- C2 Configuration Manager(リソースキット)

## NTにおけるセキュリティ上の 問題点

1. ユーザ認証
2. NTFSファイルシステム
3. レジストリ
4. TCP/IP
5. システム監査

NTにおけるセキュリティ上の問題点

### 1. ユーザ認証

#### 1.1 アカウント標準設定

– 管理ユーザ「administrator」

- デフォルトで名称が固定
- 標準ではロックアウトされない
- SIDの中のRID(Relative ID)値が固定 ... 500
  - S-1-5-21-796086221-1724263446-1256410061-500

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 37

NTにおけるセキュリティ上の問題点

– アカウントの原則およびユーザ権利の原則

- アカウントの原則はデフォルトでは未設定
- ネットワークアクセスのユーザ権利
- ローカルログオンのユーザ権利
- シャットダウンのユーザ権利
  - ↓

デフォルトでは不特定のユーザに許可されている

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 38

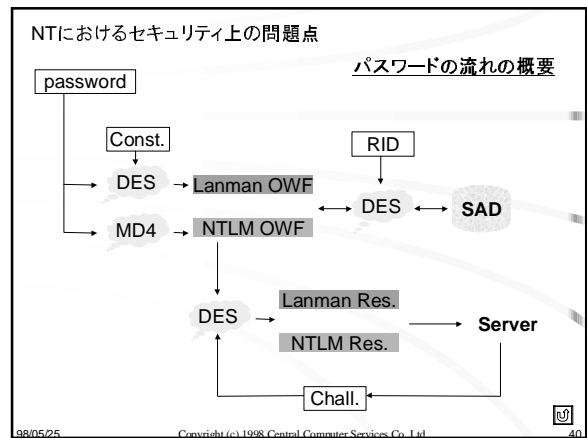
NTにおけるセキュリティ上の問題点

### 1.2 パスワードの脆弱性

– PWDumpによるパスワードハッシュのダンプ

- PWDump ... Jeremy Allison氏により開発
- sambaとのパスワード同期が目的
- OWF(One Way Function)へ復号することが可能
- NTCrack, L0phtCrack等によりパスワードクラック
- 基本的にAdministrator権限が必要だが、SAMファイルにアクセスできれば通常ユーザでも利用可
- Resource KitのNLTEST.EXEにも同様の機能

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 39



NTにおけるセキュリティ上の問題点

– 物理アクセスによる強制的パスワード変更

- Chnptw ... Petter N Hagen氏により開発
- LinuxをFDからブートして使用
- 任意のユーザのパスワードを変更可能

NTFSのマウント  
↓  
SAM読み込み  
↓  
ファイルシステム中のパスワード部分を直接変更

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 41

NTにおけるセキュリティ上の問題点

– Getadminによる管理者権限取得

- Getadmin ... Konstantin Sobolev氏により開発
- 低レベルカーネルルーチンのバグを利用
- 任意のユーザを管理者グループに入れることが可能

SYSTEM権限の実行プログラムにアタッチ  
↓  
SYSTEM権限でスレッドを起動  
↓  
任意のユーザを管理者グループに編入

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 42

NTにおけるセキュリティ上の問題点

– Lanman認証パスワードの脆弱性

- Lanman認証パスワード ... ネットワーク認証の下位互換性のため(NTLM0.12以前)
- すべて大文字で表現
- 14バイト長固定
- 7バイトずつで処理  
→ 比較的クラックされやすい

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 43

NTにおけるセキュリティ上の問題点

**Lanmanパスワード**

MyPassword 平文パスワード

↓ 大文字, 14バイトまで空白追加

M Y P A S S W O R D

Const. → DES      Const. → DES

7バイトずつ暗号化

74 AC 99 CA 40 DE D4 20 DC 1A 73 E6 CE A6 7E C5

Lanman OWF

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 44

NTにおけるセキュリティ上の問題点

**NTLMパスワード**

MyPassword 平文パスワード

↓ ASCII → UNICODE変換

M y P a s s w o r d

MD4

MD4でハッシュ

F1 2C 41 80 83 C0 5E 3A 7D E7 85 82 E6 1F 65 2D

NTLM OWF

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 45

NTにおけるセキュリティ上の問題点

– Notification Packagesによるパスワード取得

- Notification Packagesとは...ユーザ登録時やパスワード変更時に自動的にクリアテキストのパスワードを操作するための機能
- HKLM¥SYSTEM¥CurrentControlSet¥Control¥Lsa¥Notification PackagesにDLL名を記述
- 標準でレジストリにFPNWCLNTが登録  
→ トロイの木馬を仕掛けられる可能性

(注: FPNWCLNT.DLLとはNetWareとの間でパスワード同期を行なうためのモジュール。NT Serverでは標準でSystem32ディレクトリにインストールされているが、Workstationには存在しない。)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 46

NTにおけるセキュリティ上の問題点

– サービス・アカウント・パスワードの表示

- サービス・アカウント・パスワード ... Serviceが動作するアカウントのパスワード
- HKLM¥security¥policy¥secretsの下に暗号化されて保持
- 管理者権限があれば通常のAPIを使用して復号することが可能
- RASのパスワードも同様(パスワードを保存しない設定にしても!!)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 47

NTにおけるセキュリティ上の問題点

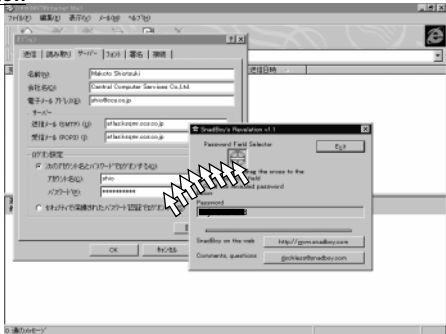
– Revelationによる各種パスワードの表示

- Revelation ... SnadBoy Software社が開発
- 95, NT上で、\*\*\*\*\*表示になっているパスワードを平文で表示する
- 解読可能か否かはアプリケーションに依存
  - Internet Mail / News, Outlook Express
  - ダイアルアップ接続
  - IE
  - MS Word 7.0
  - .....

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 48

NTにおけるセキュリティ上の問題点

Revelation



NTにおけるセキュリティ上の問題点

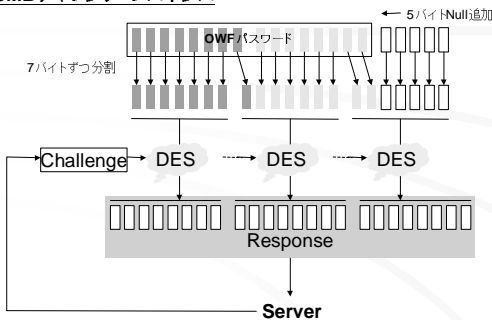
1.3 ネットワーク認証

- SMBチャレンジ・レスポンス ④

- 通信経路上でパケットをモニタすることによりチャレンジおよびレスポンスを取得
- チャレンジとレスポンスをもとに、Dictionary Attack もしくはBrute Force Attack
- 特にLanmanパスワードは脆弱
  - Dictionary Attack ... 辞書攻撃
  - Brute Force Attack ... 総当たり攻撃

NTにおけるセキュリティ上の問題点

SMBチャレンジ・レスポンス



NTにおけるセキュリティ上の問題点

- コネクションハイジャック、パケットリプレイ

- セッション認証後のサーバ・クライアント間のデータのやり取りに関する脆弱性
- 認証後のセッションをハイジャックする
- 一度流れたパケットを再度送って使用する
- 通信経路上でパケットをモニタすることが必要

NTにおけるセキュリティ上の問題点

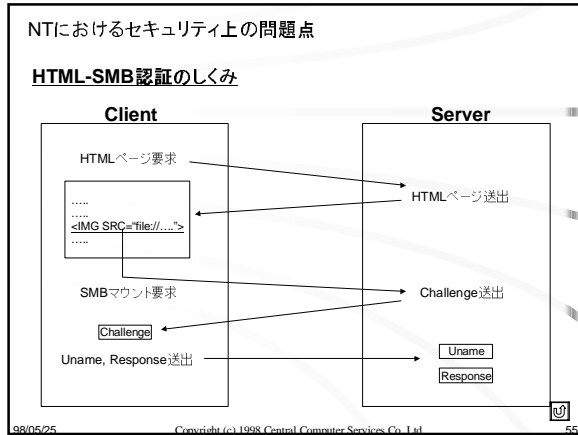
- ダウングレードアタック

- ネットワーク認証の下位互換性の問題
- 通信経路上でサーバからの応答パケットを変造することにより、クライアントに平文パスワードを要求
- C2MyAzz ... 偽のサーバレスポンスを返すツール
- 95の場合、そのまま平文パスワードを送る
- NTの場合、パスワード入力のダイアログを表示し、入力したパスワードを平文で送る

NTにおけるセキュリティ上の問題点

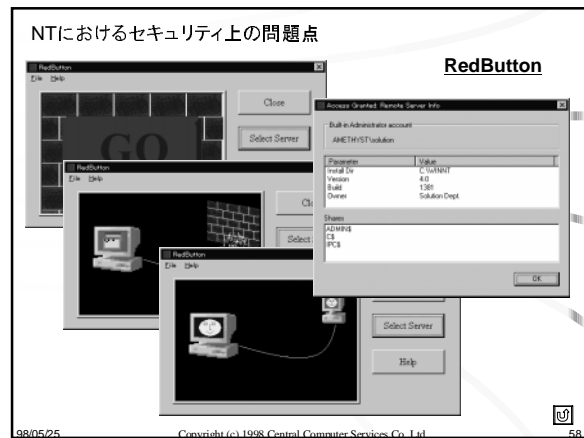
- HTMLからのSMB認証

- 不正なWebサーバをアクセスすることにより、パスワードレスポンスが奪われる
- HTML中の下記(例)のタグで、イメージ表示のために不正サーバに対してSMB認証を実行
  - <IMG SRC="file:///192.168.1.1/image/image.gif">
- Webブラウザのバージョンには依存しない



- NTにおけるセキュリティ上の問題点
- HTTP経由のMS暗号化認証
- 不正なWebサーバをアクセスすることにより、パスワードレスポンスが奪われる
  - サーバからMS暗号化認証要求に対し、IEが自動的に応答する
  - IE固有の問題
  - 対策が困難
- 98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 56

- NTにおけるセキュリティ上の問題点
- Anonymous接続 (RedButton)
- Anonymous接続とは ... 匿名 (Anonymous) ユーザによるログオンの機能
  - RedButton ... MWCにより開発
  - Anonymous接続を利用して以下の情報を表示
    - 管理者アカウント
    - OSバージョン、ビルド、所有者
    - システムディレクトリ
    - 共有一覧
  - net use ¥¥192.168.1.1¥ipc\$ "" /user:""
  - レジストリ接続、パスワードポリシーの取得、EventLog、...
- 98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 57



- NTにおけるセキュリティ上の問題点
- 2. NTFSファイルシステム**
- デフォルトアクセス権限
- Everyoneに対して以下が許可されている
    - ¥winnnt ... Full Control
    - ¥winnnt¥system32 ... Change
    - ¥winnnt¥repair ... Read
    - ¥winnnt¥cookies ... Full Control
    - ¥winnnt¥Temporary Internet Files ... Full Control
    - ¥temp ... Change
    - ¥program files ... Full Control
- 98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 59

- NTにおけるセキュリティ上の問題点
- 管理共有
- デフォルトの共有 (C\$, D\$, Admin\$等)
  - 管理者のみ共有可
  - 管理者権限があれば共有できてしまう
- 各種NTFSアクセスツール
- NTFSDOS ... DOSからNTFSに対してアクセス
  - LinuxからのNTFSアクセス
  - 物理的アクセスが必要 (FDからのブート等)
- 98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 60

## NTにおけるセキュリティ上の問題点

### – NTFS Multiple Data Streams

- NTFS上のファイルにデータを付加する機能
- Services For Macintoshでリソースフォークの保持に利用
- ファイルにアクセス権があれば複数追加可能
  - echo Hello world! > test.txt:stream1
  - more < test.txt:stream1
- 通常のコマンドからはその存在がわからない(サイズ、内容)
- streamfind ... March Information Systems

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

61

## NTにおけるセキュリティ上の問題点

### 3. レジストリ

#### – デフォルトアクセス権限

- HKLM\SOFTWARE以下 ... ほとんどEveryoneに対してread/writeを許している
- 下記レジストリにコマンドが指定された場合、ログイン時に自動的に実行してしまう
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

62

## NTにおけるセキュリティ上の問題点

### – リモートレジストリアクセス

- NT Workstation ... デフォルトでリモートレジストリアクセス可 (Anonymous userでもOK)
- NT Server ... デフォルトで管理者のみリモートアクセス可

### – .regファイル

- デフォルトのアクションがregeditの起動

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

63

## NTにおけるセキュリティ上の問題点

### 4. TCP/IP

#### – nbtstatによる情報収集

- nbtstat -A 192.168.1.1
  - <00> UNIQUE ... コンピュータ名
  - <00> GROUP ... ドメイン名
  - <03> UNIQUE ... コンピュータ名またはログオンユーザ名
  - 詳細はリソースキットのNetworking Guide参照
  - UDP port137で行なう

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

64

## NTにおけるセキュリティ上の問題点

### – OOB (Out of Band) Attack

- TCPのOut of Bandデータを受け取るによりNTが停止する(ブルースクリーン)
- TCP port139のみが対象
- さまざまなアタックツールが存在 (Winnuke)
- TCP/IPの実装の違いにより2種類のOOB Attack (BSD形式およびRFC1122形式)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

65

## NTにおけるセキュリティ上の問題点

### – Ping of Death

- 64Kバイトを超えるICMPパケットを受け取るによりNTが停止する場合がある
- ping -l 65510 192.168.1.1
- 数多くのOS、ファームウェアに同じ障害

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

66

NTにおけるセキュリティ上の問題点

– SYN Flood Attack

- 応答(ACK)を返さないSYNパケット(TCP接続要求)を多量に受けることにより、該当ポートでサービス不能になる
- netstatのstate ... SYN\_RECEIVED
- デフォルトでは約3分間、半開設状態
- TCP/IPの本質的な問題

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 67

NTにおけるセキュリティ上の問題点

– CPU Attack

- TCP port135に接続し、10文字以上入力した後にディスコネクト → CPU使用量が100%
- RPCモジュールの問題、関連してlistenしているポート(1031等)でも同じ結果
- DNS(TCP port53)にも同様の障害

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 68

NTにおけるセキュリティ上の問題点

– Simple TCP/IP Attack

- Simple TCP/IPサービス(chargen等)に対するブロードキャスト攻撃 → UDPパケットの洪水状態

– WINS Attack

- 不正なUDPパケットを受け取ることによりWINSサービスが停止

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 69

NTにおけるセキュリティ上の問題点

– スプーラサービス・メモリーーク

- SPOOLSS named pipeに接続してデータ送信することでメモリーーク
- Anonymous接続でも可
- spooleak.exe ... Ondrej Holas氏により開発

– SNMPによる情報収集

- SNMPアクセスによりユーザー一覧等の取得
  - snmputil walk 192.168.1.1 public .1.3.6.1.4.1.1.77.1.2.25

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 70

NTにおけるセキュリティ上の問題点

– Land Attack

- IPアドレスおよびポートがsource/destination共に同じであるような不正なSYNパケットを受けることにより、1分程度動作が遅くなる

– IP Fragment Overlap

- 不正にフラグメントされたIPパケットを受けることにより、ハングする
- SSPING, Teardrop, Bonk, Teardrop2, ...

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 71

NTにおけるセキュリティ上の問題点

– SP3 PPTP Attack

- PPTPの制御用TCPポート(1723)に不正なパケットを受けることにより、NTがクラッシュする

– SMB Logon Attack

- 不正なSMBログオンパケットを受け取ることにより、NTが停止する

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 72



## セキュリティ対策のポイント

### – ユーザビリティとセキュリティ

- ユーザにとって利用のしやすさとセキュリティ確保は、通常はトレードオフの関係にある
- ユーザの理解と協力が重要

利用しにくい



裏口を開ける、パスワードを貼り付ける、...



かえってセキュリティが緩くなる

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

79

## セキュリティ対策のポイント

### – 管理・運用のやりやすさ

- セキュリティ管理は日常業務である
- 煩雑な運用管理にならないように
- 目をつぶるべき点はある
- システム管理者間のコンセンサスが重要

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

80

## セキュリティ対策のポイント

### – ホスト、ネットワーク、アプリケーションレベル

- どのレベルで対策を施すべきかを検討
- すべてのセキュリティ対策をホストレベルで行なうのは困難
  - ファイアウォールでNetBIOS over TCP/IP (port137~139)を防ぐだけでも効果は大きい
  - サービスパックやホットフィックスを入れることができないマシンもあろう
- マシンの役割やネットワーク構成、移動アプリケーションの機能によりさまざま

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

81

## セキュリティ対策のポイント

## 2. 標準セキュリティ機能の活用

### – アカウントの原則

- パスワードの有効期間 ... 必要に応じ設定
- パスワードの変更禁止期間 ... 必要に応じ設定
- パスワードの長さ ... 8文字以上を推奨
- パスワードの履歴 ... 必要に応じ設定
- アカウントロックアウト ... 設定を推奨
- パスワード変更にログオンが必要 ... 設定を推奨
- ログオン時間超過のリモートユーザを強制的にログアウト ... 設定を推奨

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

82

## セキュリティ対策のポイント

### – ユーザ権利の原則

- 最低限必要なユーザ・グループのみに設定することを推奨する項目
  - システムのシャットダウン
  - ネットワーク経由でコンピュータにアクセス
  - ローカルログオン
- その他注意が必要な項目
  - オペレーティングシステムの一部として機能
  - サービス・バッチジョブとしてログオン

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

83

## セキュリティ対策のポイント

### – システム監査

- 監査を行なうことを推奨する項目
  - ログオンとログオフ ... 成功および失敗
  - ファイルとオブジェクトへのアクセス ... 失敗
  - ユーザ権利の使用 ... 失敗
  - ユーザとグループの管理 ... 成功および失敗
  - セキュリティ原則の変更 ... 成功および失敗
  - 再起動、シャットダウン、およびシステム ... 成功および失敗
- 大量に監査する場合はログの処理を考慮

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

84

セキュリティ対策のポイント

–ドメインセキュリティ

- ログオン時間
- ログオン先
- アカウント有効期限
- プロファイルの使用

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 85

セキュリティ対策のポイント

– NTFS

- 特に理由 (DOSとの混在等) がない限りNTFSを使用する

–データバックアップ、ディスク冗長構成

- ハード障害、ソフト障害、ミスオペレーション、改竄等からデータを保護

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 86

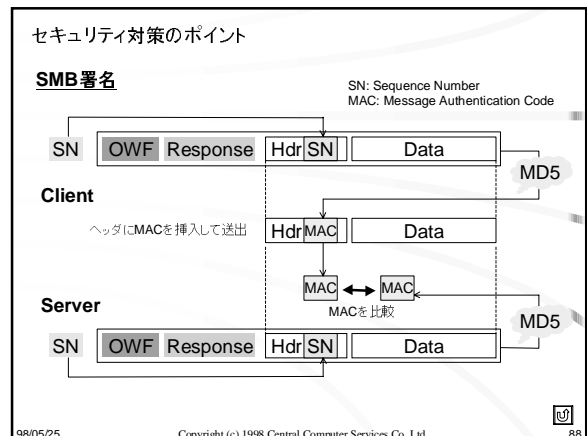
セキュリティ対策のポイント

3. 最新サービスパック・ホットフィックスの適用

– SMB署名 (SMB signing) - SP3

- ホスト間でやり取りされるSMBメッセージに署名する
- 署名 ... パスワード、チャレンジ・レスポンス、連番
  - お互いに、OWFを知っている
  - お互いに、チャレンジとレスポンスを知っている
  - 連番 (シーケンス番号) が合っている
- コネクションハイジャックを防止

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 87



セキュリティ対策のポイント

– パスワードフィルタリング (Passfilt.dll) - SP2

- パスワード登録・変更時に作用
- 次のルールが適用
  - 最低6文字なければならない
  - 最低、以下の4つのクラスのうち3つを含まなければならない
    - » A, B, C, ... Z
    - » a, b, c, ... z
    - » 0, 1, 2, ... 9
    - » 特殊記号 ( @, # 等)
  - パスワードにユーザIDやフルネームの一部を含んではいけない

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 89

セキュリティ対策のポイント

– Anonymousユーザアクセスの制限 - SP3

- SP3導入により、Anonymousユーザがリモートでレジストリにアクセスすることを禁止
- レジストリの設定により、Anonymousユーザがユーザ一覧や共有一覧を取得することを禁止
- Authenticated Usersグループが導入 ... Anonymousユーザはこのグループに含まれない
- Authenticated UsersグループでAnonymousユーザに対するNTFSやレジストリのアクセスコントロールが可能

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 90

## セキュリティ対策のポイント

### – 平文パスワードによるユーザ認証の禁止 - SP3

- SP3導入により、標準では要求があっても平文でパスワードを送らないようになる

### – SYSKEY - SP3

- パスワードをSAMデータベースに保存する際に強かに暗号化する機能
- 詳細はQ143475を参照

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

91

## セキュリティ対策のポイント

### – ホットフィックス

- サービスパック以降に修正された問題点に関するパッチモジュール
- サービスパックごとに存在 ... SP3にはSP3用のホットフィックスを適用する
- 各国語版ごとに存在 ... 基本的に、日本語版には日本語版用のホットフィックスを適用する
- すべてを適用する必要はない ... 該当ホストで実際に生じている問題を修正するために適用すべき
- 緊急に提供することが優先されているため、十分にテストされてはいない

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

92

## セキュリティ対策のポイント

### – ホットフィックス(つづき)

- 複数のホットフィックスを適用する場合は、新しいモジュールを古いもので書き換えてしまわないように順序に注意する
  - ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/postsp3.txt
- /x をつけて実行 → 各モジュールの展開のみ実行
  - 例: tearfixi.exe /x
    - » hotfix.exe
    - » hotfix.inf
    - » tcpip.sys
    - » tcpip.dgb

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

93

## セキュリティ対策のポイント

### – ホットフィックス(つづき)

- Hotfix.exeの使用方法(詳細はQ184305を参照)
  - hotfix /? ... ヘルプの表示
  - /y アンインストール (-mまたは-qと共に使用)
  - /i シャットダウン時にアプリケーションを強制終了
  - /n アンインストールディレクトリを作らない
  - /z インストール後にリポートしない
  - /q 自動モード(ユーザインターフェイスなし)
  - /m 自動モード(ユーザインターフェイスあり)
  - /l インストールされているホットフィックスの一覧表示

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

94

## セキュリティ対策のポイント

### – ホットフィックス(つづき)

- サービスパックを再インストールした場合、ホットフィックスも再び適用する
- 最低限、適用することが推奨されるもの
  - getadmin-fix
  - teardrop2-fix
  - simptcp-fix (simple TCP/IPを入れている場合)
  - srv-fix
  - pent-fix (該当するPentiumマシンの場合)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

95

## セキュリティ対策のポイント

### 4. アクセスコントロールの強化

#### – NTFSおよびレジストリ

- デフォルト設定には多くの問題点
- Everyoneは特に注意する
- ローカルおよびリモートのアクセスコントロール

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

96

セキュリティ対策のポイント

– プロトコルフィルタ

- PPTPだけを使用する場合 → PPTPフィルタリング
- TCP/IPフィルタ ... 必要なTCP/UDPポートへのアクセスのみを許可する
  - サービス(SMTP、HTTP、...)が利用するポート
  - DNSのUDPポート(port53)
- NetBIOS over TCP/IP ... TCP/UDP 137, 138, 139
- RPC ... TCP135

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

97

セキュリティ対策のポイント

5. セキュリティ設定のチェック・監査

– ネットワーク経路のセキュリティスキャン

- ISS Internet Scanner
- SNI Ballista
- Wheelgroup NetSonar
- Asmodeus, UltraScan, ...
- 大量、一括にチェックすることが可能
- きめの細かいチェックは困難

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

98

セキュリティ対策のポイント

– ホスト上でホスト自身の脆弱性を調査

- IDI Kane Security Analyst
- March Security Manager
- Axent OmniGuard/ESM
- ユーザ設定や、NTFS・レジストリのアクセス制御設定など、詳細なチェックが可能
- 一台ずつにインストールする必要がある
- リソースキットのc2config.exe

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

99

セキュリティ対策のポイント

– パスワードチェックツール

- MWC ScanNT
- L0phtCrack

– ACLチェックツール

- Somarsoft DumpAcl
- MWC FileAdmin
- Smallwonders Security Explorer

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

100

セキュリティ対策のポイント

– レジストリチェックツール

- Somarsoft DumpReg
- MWC RegAdmin

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

101

セキュリティ対策のポイント

6. 稼動状況の監視および異常通知

– 標準の監視・通知機能

- パフォーマンスモニタ
- サーバマネージャ

– イベントログ監視ツール

- Princeton Software LogCaster
- Omnitrend PageMaster/ev
- MWC EventAdmin
- Somarsoft DumpEvt

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

102

セキュリティ対策のポイント

- サーバ監視ツール
  - Ipswitch WhatsUp
  - Caravelle WebWATCHER
- 侵入検出ツール
  - IDI Kane Security Monitor
  - ISS RealSecure
  - Wheelgroup NetRanger
  - Abirnet SessionWall-3

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 103

セキュリティ対策のポイント

### 7. 物理的セキュリティの確保

- 不正な物理的アクセスを排除
  - ビル、コンピュータールーム、マシン、回線、ごみ箱、...
  - バックアップメディア、修復ディスク
- ローカルログオンの制限
  - 不必要なローカルログオン権利を削除

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 104

セキュリティ対策のポイント

- リムーバブルメディア
  - 不要なリムーバブルメディア (FD, MO, CD-ROM等) ドライブはとりはずす
  - 対話的ログオンユーザのみがFDまたはCD-ROMを利用できるようにするには...
    - Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    - Name: AllocateFloppies または AllocateCDRoms
    - Type: REG\_SZ
    - Value: 1

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 105

セキュリティ対策のポイント

### 8. エンドユーザ教育

- パスワードの重要性
- 個人データのバックアップ
- コンピュータウイルス対策 (ダウンロード、E-Mail)
- ダイアルアップ接続の危険性
- モバイルコード (Java, ActiveX) の危険性

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 106

セキュリティ対策のポイント

### 9. セキュリティ情報収集

- ユーザグループ
  - 日本NTユーザ会 (JWNTUG) ㊦
- ベンダサポート
  - Microsoft Security Advisor (MS) ㊦
  - Support Online (MS) ㊦
  - Windows NTのセキュリティ (MSKK) ㊦
  - サポート技術情報 (MSKK) ㊦

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 107

セキュリティ対策のポイント

- メーリングリスト
  - JWNTUG Admin Mailing List (日本語)
  - ISS NT Security Mailing List
  - Russ Cooper's NT Bugtraq Mailing List
  - Russ Cooper's NT Security Mailing List
  - LAC Firewall Mailing List (日本語)
  - GNAC Firewalls Mailing List
  - NFR The Firewall Wizards Mailing List

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 108

セキュリティ対策のポイント

– NetNews

- comp.security.announce
- comp.security.firewalls
- comp.security.misc
- comp.security.unix
- comp.os.ms-windows.nt.admin.security
- fj.comp.security(日本語)
- fj.os.windows-nt(日本語)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 109

セキュリティ対策のポイント

– Webリソース

- Russ Cooper's NT Bugtraq ㊦
- MJE NT Security ㊦
- Bill Stout's NT Exploits II ㊦
- JWNTUG NTセキュリティ
- InfoBears NTイントラ虎の穴 ㊦
- CCS Security Related Links ㊦

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 110

問題点ごとの対策

1. ユーザ認証
2. NTFSファイルシステム
3. レジストリ
4. TCP/IP
5. システム監査
6. その他

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 111

問題点ごとの対策

1. ユーザ認証

– 管理ユーザ「Administrator」 ㊦

- 名称を変更する
- 権限の低いユーザを作成、Administratorという名称とし、そのユーザ名を監視する
- ネットワークからのログオンを制限する
- リソースキットのpassprop.exeを使用してネットワーク経由のログオン失敗によるアカウントロックアウトを有効にする
- RIDの変更は不可能

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 112

問題点ごとの対策

– アカウントの原則およびユーザ権利の原則

- サイトポリシーに基づいて設定する

– PWDumpによるパスワードハッシュのダンプ ㊦

- SAMファイルを保護する(Repairディレクトリ、ERD、バックアップテープ、...)
- SYSKEYを使用する(詳細はQ143475を参照)
- pwdump2 ... SYSKEYを使っていてもダンプ可

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 113

問題点ごとの対策

– 物理アクセスによる強制的パスワード変更

- マシンへの物理アクセスを制限する
- FD等による他OSの起動を阻止する(BIOSセットアップ)

– Getadminによる管理者権限取得 ㊦

- SP3のgetadmin-fixにより解決
- しかし、「プログラムのデバッグ」のユーザ権利を持つユーザは、依然実行可能(デフォルトではAdministratorのみ)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 114

問題点ごとの対策

– Lanman認証パスワードの脆弱性 ⑩

- パスワードポリシーの強化(8文字以上、英数字記号、...)
- パスワードフィルタの使用(SP2以降、passfilt.dll)
  - Key: HKLM\SYSTEM\CurrentControlSet\Control\LSA
  - Name: Notification Packages
  - Type: REG\_MULTI\_SZ
  - Value: PASSFILT
    - » 英数字記号混在の強制
    - » ユーザー名、フルネームを含むことを禁止、等
- 自作パスワードフィルタのインストール
- 詳細はQ151082を参照

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 115

問題点ごとの対策

– Notification Packagesによるパスワード取得 ⑩

- 以下のレジストリキーをチェック
  - Key: HKLM\SYSTEM\CurrentControlSet\Control\LSA
  - Name: Notification Packages
- FPNW(File and Print Services for NetWare)を使用しない場合は、設定されている FPNWCLNT を削除
- 不必要なDLLが設定されないようにする
- 詳細はQ99885を参照

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 116

問題点ごとの対策

– サービス・アカウント・パスワードの表示 ⑩

- SP3のIsa2-fixにより解決(英語版のみ)
- 詳細はQ184017を参照(※現時点では配布が中止されている)

– Revelationによる各種パスワードの表示 ⑩

- マシンへの物理アクセスを制限する
- パスワードを保存しない

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 117

問題点ごとの対策

– SMBチャレンジ・レスポンス ⑩

- SP3のIm-fixを入れた後、レジストリを設定
  - Lanmanレスポンスを送り出すことを制限する
  - Key: HKLM\SYSTEM\CurrentControlSet\Control\LSA
  - Name: LMCompatibilityLevel
  - Type: REG\_DWORD
  - Value: 0, 1, 2 (Default 0)
    - » 0 ... NTLMおよびLanmanパスワード両方を送る
    - » 1 ... サーバが要求したときのみLanmanパスワードを送る
    - » 2 ... Lanmanパスワードは送らない
- レベル2にした場合、95等のLanman認証を要求するマシンに対して認証できなくなる
- 詳細はQ147706(J030795)を参照(※現時点では配布が中止されている)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 118

問題点ごとの対策

– コネクションハイジャック、パケットリプレイ

- SP3のSMB署名により解決 ⑩
- SMB署名の有効化/無効化(NT Server)
  - Key: HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
  - Name: EnableSecuritySignature
  - Type: REG\_DWORD
  - Value: 0 (default), 1
    - » 0 ... disable
    - » 1 ... enable

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 119

問題点ごとの対策

– コネクションハイジャック、パケットリプレイ(つづき)

- SMB署名の要求/非要求(NT Server)
  - Key: HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
  - Name: RequireSecuritySignature
  - Type: REG\_DWORD
  - Value: 0 (default), 1
    - » 0 ... disable
    - » 1 ... enable

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 120

問題点ごとの対策

– コネクションハイジャック、パケットリプレイ(つづき)

- SMB署名の有効化/無効化 (NT Workstation)
  - Key: HKLM\SYSTEM\CurrentControlSet\Services\Rdr\Parameters
  - Name: EnableSecuritySignature
  - Type: REG\_DWORD
  - Value: 0, 1 (default)
    - » 0 ... disable
    - » 1 ... enable

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

121

問題点ごとの対策

– コネクションハイジャック、パケットリプレイ(つづき)

- SMB署名の要求/非要求 (NT Workstation)
  - Key: HKLM\SYSTEM\CurrentControlSet\Services\Rdr\Parameters
  - Name: RequireSecuritySignature
  - Type: REG\_DWORD
  - Value: 0 (default), 1
    - » 0 ... disable
    - » 1 ... enable

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

122

問題点ごとの対策

– コネクションハイジャック、パケットリプレイ(つづき)

- サーバ側が「SMB署名有効」の場合、
  - 「有効」になっているクライアントとはSMB署名を使用
  - 「無効」になっているクライアントとは通常の通信
- サーバ側が「SMB署名要求」の場合、
  - 「有効」になっているクライアントとはSMB署名を使用
  - 「無効」になっているクライアントとは通信を拒否
- 詳細はQ161372およびSP3のREADMEを参照
- IPX環境や95混在環境では使用できない
- パフォーマンスの問題

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

123

問題点ごとの対策

– ダウングレードアタック

- SP3の導入により、パスワードを平文で送出することが停止
- パスワードを平文で要求するようなSMBサーバに対してログオンできなくなるが、レジストリの追加により平文パスワード送出を制御可能(詳細はQ166730を参照)
  - Key: HKLM\SYSTEM\CurrentControlSet\Servers\rdr\parameters
  - Name: EnablePlainTextPassword
  - Type: REG\_DWORD
  - Value: 1 (plaintext password enabled), 0 (disabled)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

124

問題点ごとの対策

– HTMLからのSMB認証 ㊦

- ホストレベルでの効果的な対策は無い
- ファイアウォールで外向きのTCP port139を止める
- 信頼できないWebサーバへアクセスしない
- Lanmanレスポンス送出の停止(前出)
- パスワードの強化(前出)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

125

問題点ごとの対策

– HTTP経由のMS暗号化認証

- ホストレベルでの効果的な対策は無い
  - NTLMSecuritySupportProviderサービスを無効にすればMS暗号化認証を行わなくなる
  - しかし、他の機能に影響が出るかもしれない
- プロキシサーバ経由でWebアクセスを行なう
  - MS暗号化認証をサポートしないプロキシ
- 信頼できないWebサーバへアクセスしない
- パスワードの強化(前出)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

126

問題点ごとの対策

– Anonymous接続 [国]

- SP3の導入 → レジストリへのアクセス、バージョン情報等の取得 (winmsd) が停止
- RestrictAnonymousレジストリ設定 → 共有一覧、ユーザー一覧の取得が停止
  - Key: HKLM\SYSTEM\CurrentControlSet\Control\LSA
  - Name: RestrictAnonymous
  - Type: REG\_DWORD
  - Value: 1
- 詳細はSP3のREADMEおよびQ143474を参照

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

127

問題点ごとの対策

– Anonymous接続 (つづき)

- SP3導入後に、Anonymous接続によるレジストリアクセスを行ないたい場合 (アプリケーションによっては正常に稼動しなくなるため)
  - Key: HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
  - Name: NullSessionPipes
  - Type: REG\_MULTI\_SZ
  - Value: WINREGを追加
- 詳細はQ143138を参照

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

128

問題点ごとの対策

– Anonymous接続 (つづき)

- SP3より、Authenticated Usersというグループが導入された
- 基本的にはEveryoneグループと同様であるが、Authenticated UsersはAnonymousユーザを含まない
- ファイルやレジストリのアクセスコントロールで、EveryoneになっているものをAuthenticated Usersに変更することにより、Anonymous接続からのアクセスを制限することが可能

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

129

問題点ごとの対策

2. NTFSファイルシステム

– デフォルトアクセス権限

- 詳細はMS技術文書「Securing Windows NT Installation (Windows NTのインストールを安全に行なうために)」
- まず、¥WINNTおよびそれ以下のすべてのサブディレクトリについて、以下のように設定する
  - Administrators: Full Control
  - CREATOR OWNER: Full Control
  - Everyone: Read
  - SYSTEM: Full control

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

130

問題点ごとの対策

– デフォルトアクセス権限 (つづき)

- ¥WINNT¥REPAIR
  - Administrators: Full Control
- ¥WINNT¥SYSTEM32¥CONFIG
  - Administrators: Full Control
  - CREATOR OWNER: Full Control
  - Everyone: List
  - SYSTEM: Full control

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

131

問題点ごとの対策

– デフォルトアクセス権限 (つづき)

- ¥WINNT¥SYSTEM32¥SPOOL
  - Administrators: Full Control
  - CREATOR OWNER: Full Control
  - Everyone: Read
  - Power Users: Change
  - SYSTEM: Full control

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

132

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %WINDIR%\COOKIES
- %WINDIR%\FORMS
- %WINDIR%\HISTORY
- %WINDIR%\OCACHE
- %WINDIR%\PROFILES
- %WINDIR%\SENDTO
- %WINDIR%\Temporary Internet Files

- Administrators: Full Control
- CREATOR OWNER: Full Control
- Everyone: Special Directory Access - R/W/E, Special File Access - None
- SYSTEM: Full control

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 133

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %Boot.ini
- %Ntdetect.com
- %Ntldr

- Administrators: Full Control
- SYSTEM: Full control

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 134

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %Autoexec.bat
- %Config.sys

- Administrators: Full Control
- Everyone: Read
- SYSTEM: Full control

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 135

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %TEMP

- Administrators: Full Control
- CREATOR OWNER: Full Control
- Everyone: Special Directory Access - R/W/E, Special File Access - None
- SYSTEM: Full control

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 136

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- アプリケーションによっては、もっと緩いNTFSセキュリティ設定を要求する
- 例: MS Office97は、%windir%\system32等にread/writeの権限が必要(詳細はQ169387を参照)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 137

問題点ごとの対策

– 管理共有

- 必要でない場合、管理共有を削除する
- net share admin\$ /delete

– 各種NTFSアクセスツール

- マシンへの物理アクセスを制限する
- FD等による他OSの起動を阻止する(BIOSセットアップ)

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 138

問題点ごとの対策

– NTFS Multiple Data Streams ⑨

- NTFSの“機能”であり、制御することは不可能
- streamfind等の検出ツールを利用して検出
- 今のところ、この機能を利用したセキュリティ侵害等は報告されていない

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

133

問題点ごとの対策

3. レジストリ

– デフォルトアクセス権限

- 詳細はMS技術文書「Securing Windows NT Installation(Windows NTのインストールを安全に行なうために)」
- 以下に列挙するレジストリキーについて、Everyoneに対するアクセス権を、「値の照会」、「サブキーの列挙」、「通知」、および「読み取り制御」のみに設定する

- %Software%\Microsoft%\Windows NT%\CurrentVersion
- %Software%\Microsoft%\RPC(およびその全サブキー)
- %Software%\Microsoft%\Windows NT%\CurrentVersion

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

140

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Profile List
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\AeDebug
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Compatibility
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Drivers
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Embedding
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Fonts

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

141

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %Software%\Microsoft%\Windows NT%\CurrentVersion%\FontSubstitutes
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Font Drivers
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Font Mapper
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Font Cache
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\GRE\_Initialize

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

142

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %Software%\Microsoft%\Windows NT%\CurrentVersion%\MCI
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\MCI Extensions
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\PerfLib
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Port(およびその全サブキー)
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Type1 Installer
- %Software%\Microsoft%\Windows NT%\CurrentVersion%\WOW(およびその全サブキー)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

143

問題点ごとの対策

– デフォルトアクセス権限(つづき)

- %Software%\Microsoft%\Windows NT%\CurrentVersion%\Windows3.1MigrationStatus(およびその全サブキー)
- %System%\CurrentControlSet\Services%\LanmanServer%\Shares
- %System%\CurrentControlSet\Services%\UPS
- %Software%\Microsoft%\Windows%\CurrentVersion%\Run
- %Software%\Microsoft%\Windows%\CurrentVersion%\RunOnce
- %Software%\Microsoft%\Windows%\CurrentVersion%\Uninstall
- %HKEY\_CLASSES\_ROOT(およびその全サブキー)
- %HKEY\_USERS%\DEFAULT(およびその全サブキー)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

144

問題点ごとの対策

– リモートレジストリアクセス

- 以下のレジストリキーの設定により、レジストリに対するリモートアクセスを制限する
  - Key: HKLM\CurrentControlSet\Control\SecurePipeServers\winreg
  - 設定: winregキーに対するアクセス権を持つユーザのみがリモートでレジストリに対してアクセス可能

– .regファイル

- .regファイルに対するデフォルトのアクションを、「編集 (notepad.exeの起動)」に変更する

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

145

問題点ごとの対策

4. TCP/IP

– nbtstatによる情報収集 ㊦

- NTの基本機能であり、ホストレベルで止めるのは適さない
- ファイアウォールでUDP port137を止める

– OOB Attack

- SP3のoob-fixにより解決 (最新は、teardrop2-fix)
- 詳細はQ143478を (J030463) 参照

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

146

問題点ごとの対策

– Ping of Death

- SP2により解決(?)
- 障害がでるかどうかはケースバイケースのようである

– SYN Flood Attack

- SP2でTCP/IPのパラメータ設定レジストリが追加
- 半開状態時間やバックログ最大値を変更可能
- 詳細はQ142641を参照
- ファイアウォールでブロックする方が効果的

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

147

問題点ごとの対策

– CPU Attack

- SP2のrpc-fixおよびdns-fixにより解決
- 詳細はQ162567およびQ162927を参照

– Simple TCP/IP Attack

- SP3のsimptcp-fixにより解決
- 詳細はQ154460 (J031301) を参照

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

148

問題点ごとの対策

– WINS Attack

- SP3のwinsupd-fixにより解決
- 詳細はQ155701 (J031179) を参照

– スプーラサービス・メモリーーク

- 現時点では、fixは提供されていない

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

149

問題点ごとの対策

– SNMPによる情報収集

- 不要なSNMPサービスは削除する
- セキュリティの設定を行なう

– Land Attack

- SP3のland-fixにより解決 (最新は、teardrop2-fix)
- 詳細はQ165005 (J041381) を参照

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

150

問題点ごとの対策

- IP Fragment Overlap
  - SP3のteardrop2-fixにより解決
  - 詳細はQ179129 (J042091)を参照
- SP3 PPTP Attack
  - SP3のpptp-fixにより解決 (英語版のみ)
  - 詳細はQ179107を参照

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 151

問題点ごとの対策

- SMB Logon Attack
  - SP3のsrv-fixにより解決
  - 詳細はQ180963 (J042680)を参照
- 任意のポートでの接続受付 ㊦
  - 現時点では、fixは提供されていない

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 152

問題点ごとの対策

### 5. システム監査

- デフォルト設定の問題
  - サイトポリシーに基づいて設定する
- モニタリング・通知機能の欠如
  - サードパーティ製品の導入

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 153

問題点ごとの対策

- EventLogのGuestアクセス
  - 以下のレジストリ設定で、ゲストユーザによる ApplicationまたはSystem logに対するアクセスを停止
    - Key: HKLM\SYSTEM\CurrentControlSet\Services\EventLog\LogName] ... LogNameはApplication or System
    - Name: RestrictGuestAccess
    - Type: REG\_DWORD
    - Value: 1

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 154

問題点ごとの対策

### 6. その他

- ログオン時の警告メッセージ表示
  - 以下のレジストリを設定
    - Key: HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
    - Name: LegalNoticeCaption ... 警告ダイアログのタイトル
    - Name: LegalNoticeText ... 警告ダイアログのテキスト
    - Type: REG\_SZ
    - Value: 表示したいタイトルおよびテキスト

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 155

問題点ごとの対策

- ログオンダイアログにユーザ名を表示しない
  - 以下のレジストリを設定
    - Key: HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
    - Name: DontDisplayLastUserName
    - Type: REG\_SZ
    - Value: 1

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 156

#### 問題点ごとの対策

##### – シャットダウンにログオンを要求 (Workstation)

- 以下のレジストリを設定

- Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- Name: ShutdownWithoutLogon
- Type: REG\_SZ
- Value: 0 (Workstationのデフォルトは1 ... ログオンを要求しない)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

157

#### 問題点ごとの対策

##### – シャットダウン時にPageFile内容を消去

- 以下のレジストリを設定

- Key: HKLM\System\CurrentControlSet\Control\Session Manager\MemoryManagement
- Name: ClearPageFileAtShutdown
- Type: REG\_DWORD
- Value: 1 (デフォルトは0 ... 消去しない)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

158

#### 問題点ごとの対策

##### – ログオン資格証明のキャッシュを無効にする

- 以下のレジストリを設定

- Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- Name: CachedLogonsCount
- Type: REG\_SZ
- Value: 0

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

159

#### 問題点ごとの対策

##### – Pentiumのバグ対策

- SP3のpent-fixにより解決
- 詳細はQ163852 (J041092)を参照

##### – ROLLBACK.EXEの問題

- ROLLBACK.EXEがハードディスク内にインストールされているかどうかを確認
- もしあれば、削除する

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

160

## IISおよびIEに関するセキュリティ

1. IEのセキュリティ上の問題点
2. IISのセキュリティ上の問題点
3. CGIセキュリティ

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

161

#### IISおよびIEに関するセキュリティ

##### 1. IEのセキュリティ上の問題点

###### – IEの不具合一覧

- IE3 .url/.lnk ... 3.0aでfix
- IE3 UMD (ダブルクリック) ... 3.0bでfix
- IE3 MIT (.isp) ... 3.0bでfix
- IE Cache Exploit ... ???
- IE-NTLM Authentication ... 機能である
- IE PowerPoint Bug ... fixあり
- IE3.0, 4.0 and Java ... fixあり
- IE File Corruption Bug ... fixあり

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

162

## IISおよびIEに関するセキュリティ

### - IEの不具合一覧(つづき)

- Freiburg text-viewing Bug ... fixあり
- IE4.0 for Win95 buffer overrun ... fixあり
- IE4.0 Page Redirect ... fixあり
- IE4.0 MK Overrun ... fixあり
- IE4.0 Embed ... fixあり
- NetMeeting Speed Dial ... fixあり
- IE ghosting attack ... ???

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

163

## IISおよびIEに関するセキュリティ

### - IE使用上の注意点

- 権力、最新版を使う(fix情報に注意)
- 信頼できるWebのみアクセス
- Java、JavaScript、ActiveXは、必要となきのみON
- 最小限の権限を持つユーザコンテキストで実行(リソースキットのSU)
- 重要なホスト上ではWebアクセスを行わない
- 外向きのNBT(NetBIOS over TCP/IP)を制限

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

164

## IISおよびIEに関するセキュリティ

### 2. IISのセキュリティ上の問題点

#### - IIS4.0のセキュリティ機能

- 仮想サーバ、仮想ディレクトリごとのセキュリティ設定
  - 仮想サーバごとに特定のユーザコンテキストで動作可能
- ユーザ認証と匿名アクセス
  - 匿名アクセス ... IUSR\_コンピュータ名 または NTユーザ名
  - Basic Authentication
  - NT Challenge/Response Authentication
  - SSL Client Certificate Authentication

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

165

## IISおよびIEに関するセキュリティ

### - IIS4.0のセキュリティ機能(つづき)

- アクセス制御
  - IPアドレス・ドメイン名に基づくアクセス制御
  - ユーザ認証に基づくアクセス制御
  - Webサーバパーミッションによるアクセス制御
    - » Access Permission: Read, Write
    - » Application Permission: None, Script, Execute
  - NTFSによるアクセス制御

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

166

## IISおよびIEに関するセキュリティ

### - IIS4.0のセキュリティ機能(つづき)

- アクセスログ
  - IIS Log File Format
  - NCSA Common Log File Format
  - ODBC Logging
  - W3C Extended Log File Format
- SSL (Secure Socket Layer)
  - サーバの認証
  - ユーザの認証
  - 通信データの暗号化

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

167

## IISおよびIEに関するセキュリティ

### - セキュリティ上の問題点

- IIS自体のバグ
  - .asp. (IIS3, Q163485)
  - Long URL (IIS3, Q143484, J030428)
  - Short Filename (IIS4, Q179148, 英語版IIS4.0)
- 動的コンテンツ
  - CGI, ASP, SSI, ...
  - 該当ユーザコンテキストで許可されるすべてを実行可能
    - » %SystemRoot%へのアクセス
    - » レジストリへのアクセス
  - すべてのスクリプトについて内容をチェックすべき

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

168

IISおよびIEに関するセキュリティ

– セキュリティ上の問題点(つづき)

- 設定の誤り
  - NT自体のセキュリティ設定
  - ユーザのセキュリティ設定
  - NTFSのセキュリティ設定
  - IISのセキュリティ設定
  - 動的コンテンツのセキュリティ設定
  - 複雑かつ繁雑 → 誤りを起こしやすい、誤りを見つけにくい

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 169

IISおよびIEに関するセキュリティ

3. CGIセキュリティ

– CGIスクリプトからの情報流出

- スクリプト・ロジック
- ホストIPアドレス
- ユーザ名
- パスワード
- スクリプト専用のディレクトリ ... read不許可にする

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 170

IISおよびIEに関するセキュリティ

– 不正パラメータによる任意プログラム実行

- フォームでユーザにパラメータを入力させる場合
  - メール送信先
  - ユーザ名、パスワード
- HTMLにhiddenでパラメータを記述している場合
  - `<INPUT TYPE="hidden" NAME="address", VALUE="foo@xxx.co.jp">`

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 171

IISおよびIEに関するセキュリティ

– 不正パラメータによる任意プログラム実行(つづき)

- Perlにおける例
  - スクリプト: `system("blat $file -t $mailto");`
  - \$mailtoの入力: `xxx@yyy.co.jp & dir c:\*`
  - system以外にも、`exec()`、`open()`、`
- 入力パラメータのチェックが重要
  - `&, |, ", ...???`
  - 日本語入力の場合は???

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 172

参考資料

- トータルセキュリティ実現のために
  - コンピュータセキュリティの基礎、アスキー出版局、ISBN4-7561-0299-9
  - サイトセキュリティハンドブック [http://www.ipa.go.jp/SECURITY/ssh/ssh\\_index.htm](http://www.ipa.go.jp/SECURITY/ssh/ssh_index.htm)
  - Internet Security Policy: A Technical Guide [DRAFT] <http://csrc.nist.gov/isptg/>
  - Internet Firewalls Frequently Asked Questions <http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm>
  - ファイアウォール、ソフトバンク、ISBN4-89052-672-2
  - NCSA Firewall Policy Guide: [http://www.ncsa.com/fwpg\\_p1.html](http://www.ncsa.com/fwpg_p1.html)
  - インターネット・ファイアウォールおよびセキュリティ: <http://www.3com.com/japan/tech/papers/500619.html>

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 173

参考資料

- NT4.0の標準セキュリティ機能
  - Windows NT Server 4.0 パーフェクトガイド、翔泳社、ISBN4-88135-475-2
  - Windows NT Server 4 Security Handbook, Que Corp., ISBN0-7897-1213-X
  - DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>
  - Windows NT Platform Gets C2 Evaluation: <http://www.microsoft.com/NTWorkstation/c2.htm>
  - NT Security - Frequently Asked Questions: <http://www.it.kth.se/~rom/ntsec.html>

98/05/25 Copyright (c) 1998 Central Computer Services Co., Ltd. 174

参考資料

• NTにおけるセキュリティ上の問題点

- PWDump: Windows NT Password Dump Utility  
<ftp://samba.anu.edu.au/pub/samba/pwdump/README>
- NT Crack: Windows NT Password Offline Auditing Tool  
<http://www.secnet.com/ntinfo/ntcrack.html>
- L0phtCrack: NT Password Cracker <http://www.l0pht.com/l0phtcrack/>
- The Offline Utility to Change NT Passwords  
<http://home.eunet.no/~pnordahl/ntpasswd/>
- Getadmin: <http://cmp.phys.msu.su/ntclub/pub/code.htm>
- A L0phtCrack Technical Rant  
<http://www.l0pht.com/l0phtcrack/rant.html>
- HOWTO: Password Change Filtering & Notification in Windows NT  
<http://support.microsoft.com/support/kb/articles/Q151/0/82.as>
- Security Issues Occur Due to How WinNT Handles FPNWCLNT.DLL  
<http://support.microsoft.com/support/kb/articles/q99/8/85.asp>

98/05/25

Copyright (c) 1998 Central Computer Services Co. Ltd

175

参考資料

• NTにおけるセキュリティ上の問題点 (つづき)

- NT LSA secrets  
<http://www.dhp.com/~fyodor/spl0its/NT.LSA.secrets.html>
- Administrators Can Display Contents of Service Account Passwords  
<http://support.microsoft.com/support/kb/articles/q184/0/17.asp>
- Revelation: <http://www.snadboy.com/Revelation.shtml>
- Common Internet File System (CIFS):  
<http://www.microsoft.com/intdev/cifs/>
- CIFS: Common Insecurities Fail Scrutiny:  
<http://avian.org/avian/papers/cifs.txt>
- CIFS is a load of CACA: <http://www.avian.org/avian/slides/caca.html>
- A Weakness in CIFS Authentication:  
<http://www.ntsecurity.net/security/CIFS-MiM.htm>
- Internet Explorer Exploit #4  
<http://www.ee.washington.edu/computing/iebug/>
- RedButton: <http://www.ntsecurity.com/RedButton/default.htm>

98/05/25

Copyright (c) 1998 Central Computer Services Co. Ltd

176

参考資料

• NTにおけるセキュリティ上の問題点 (つづき)

- NTFSDOS: <http://www.sysinternals.com/ntfs20.htm>
- NTFS Streams: <http://streams.march.co.uk/>
- WinNuke Testing Ground: <http://209.51.168.3/~dirk/winnuke-orig.html>
- Ping o' Death Page: <http://www.sophist.demon.co.uk/ping/>
- TCP SYN Flooding Attacks and Remedies:  
<http://www.wcmh.com/uworld/archives/95/security/004/004.txt.html>
- CAUSING 100% CPU UTILIZATION BY RPCSS:  
<http://www.ntsecurity.net/security/100CPU.htm>
- spoolse.exe: <http://oliver.efri.hr/~crv/security/bugs/NT/spoolse.html>
- Windows NT RAS PPTP exploit  
<http://oliver.efri.hr/~crv/security/bugs/NT/raspptp.html>
- Windows NT Logon Denial of Service  
<http://www.secnet.com/sni-advisories/sni-25.windows.nt.dos.advisory.html>
- netcat: <http://www.l0pht.com/~weld/netcat/>

98/05/25

Copyright (c) 1998 Central Computer Services Co. Ltd

177

参考資料

• セキュリティ対策のポイント

- Microsoft Security Advisor: <http://www.microsoft.com/security/>
- Securing Windows NT Installation  
[http://www.microsoft.com/ntserver/guide/secure\\_ntinstall.asp?A=2&B=10](http://www.microsoft.com/ntserver/guide/secure_ntinstall.asp?A=2&B=10)
- Windows NT のインストールを安全に行うために  
[http://www.microsoft.com/japan/products/ntserver/white\\_papers/](http://www.microsoft.com/japan/products/ntserver/white_papers/)
- NT 4.0 Service Pack 3 Readme File  
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3/readme.htm>
- NT 4.0 日本語版 Service Pack 3  
<http://www.microsoft.com/japan/products/ntupdate/NT4SP3/default.htm>
- サービスパックおよびホットフィックスのダウンロードサイト  
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/>
- NTBUGTRAQ NT Fixes: <http://www.ntbugtraq.com/ntfixes.asp>
- Internet Security Systems: <http://www.iss.net/>

98/05/25

Copyright (c) 1998 Central Computer Services Co. Ltd

178

参考資料

• セキュリティ対策のポイント (つづき)

- Secure Networks Inc.: <http://www.secnet.com/>
- WheelGroup: <http://www.wheelgroup.com/>
- Asmodeus (WebTrends Security Scanner): <http://www.webtrends.com/wss/>
- Intrusion Detection Inc.: <http://www.intrusion.com/>
- March Information Systems: <http://www.march.co.uk/index.html>
- AXENT Technologies, Inc.: <http://www.axent.com/>
- MWC, Inc.: <http://www.ntsecurity.com/>
- Somarsoft, Inc.: <http://www.somarsoft.com>
- Small Wonders: <http://www.smallwonders.com/>
- LogCaster: <http://www.logcaster.com/>
- PageMaster/ev: <http://www.omnitrend.com/pmev.html>
- WhatsUp: <http://www.ipswitch.com/Products/WhatsUp/whatsup.html>
- WebWATCHER: <http://www.caravelle.com>
- AbirNet: <http://www.abirnet.com/>

98/05/25

Copyright (c) 1998 Central Computer Services Co. Ltd

179

参考資料

• セキュリティ対策のポイント (つづき)

- 日本NTユーザ会 (JWNTUG): <http://www.jwntug.or.jp/index-j.html>
- MS Support Online (Knowledge Base):  
<http://support.microsoft.com/support/>
- Windows NTのセキュリティ:  
<http://www.microsoft.com/japan/products/ntserver/security/>
- サポート技術情報:  
<http://www.microsoft.com/search/worldwide/japan/support/default.asp>
- ISS NT Security Mailing List: <http://www.iss.net/vd/maillist.html>
- Russ Cooper's NT Bugtraq/NT Security Mailing List  
<http://www.ntbugtraq.com/>
- LAC Firewall Mailing List: <http://www.lac.co.jp/firewall/maillist.html>
- GNAC Firewalls Mailing List: <http://lists.gnac.net/firewalls/>
- NFR The Firewall Wizards Mailing List  
<http://www.nfr.net/forum/firewall-wizards.html>

98/05/25

Copyright (c) 1998 Central Computer Services Co. Ltd

180

#### 参考資料

##### • セキュリティ対策のポイント(つづき)

- ISS NT Security Mailing List: <http://www.iss.net/vd/maillist.html>
- Russ Cooper's NT Bugtraq/NT Security Mailing List  
<http://www.ntbugtraq.com/>
- LAC Firewall Mailing List: <http://www.lac.co.jp/firewall/maillist.html>
- GNAC Firewalls Mailing List: <http://lists.gnac.net/firewalls/>
- NFR The Firewall Wizards Mailing List  
<http://www.nfr.net/forum/firewall-wizards.html>
- MJE NT SECURITY: <http://www.ntsecurity.net>
- Bill Stout's NT Exploits II:  
<http://www.geocities.com/ResearchTriangle/3372/ntexploitsii.html>
- JWNTUG NTセキュリティ WorkingGroup:<http://www.jwntug.or.jp/index-j.html>
- InfoBears NTイントラ虎の穴: <http://www.infobears.or.jp/ntintra/>
- CCS Security Related Links:  
<http://www.you.ne.jp/younet/inet/security-links.html>

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

181

#### 参考資料

##### • 問題点ごとの対策

- The Hardening of Windows NT 4.0:  
<http://pw2.netcom.com/~honeyluv/index.html>
- Windows NT Security: Step by Step: <http://www.sans.org/ntstep.htm>
- Securing Windows NT Installation: <ftp://ftp.lucentnrg.com/ntsec/>
- Navy Secure Windows NT Installation and Configuration Guide:  
<http://infosec.navy.mil/COMPUSEC/ntsecure.html>
- Coopers & Lybrand Security Paper:  
<http://www.microsoft.com/ntserver/guide/cooperswp.asp?A=2&B=10>
- CIAC-2317 Windows NT Managers Guide:  
[http://ciac.llnl.gov/ciac/documents/CIAC-2317\\_Windows\\_NT\\_Managers\\_Guide.pdf](http://ciac.llnl.gov/ciac/documents/CIAC-2317_Windows_NT_Managers_Guide.pdf)

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.

182

#### 参考資料

##### • IISおよびIEに関するセキュリティ

- Internet Explorer Security: <http://www.microsoft.com/ie/security/>
- Unofficial Internet Explorer Security FAQ:  
<http://www.teleport.com/~hindu/iesf.html>
- The Unofficial Web Hack FAQ: <http://www.nmrc.org/faqs/www/index.html>
- The World Wide Web Security FAQ:  
<http://www.w3.org/Security/Faq/www-security-faq.html>
- CGI Security: <http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec/>
- Safe CGI Programming:  
<http://www.go2net.com/people/paulp/cgi-security/safe-cgi.txt>
- Web Security Sourcebook, Wiley Computer Publishing,  
ISBN0-471-18148-X

98/05/25

Copyright (c) 1998 Central Computer Services Co., Ltd.



183