製品に用意された機能だけで行う不正アクセスの検出

奥天 陽司
GTSC Security Response Team
Microsoft Asia Limited,.

Agenda

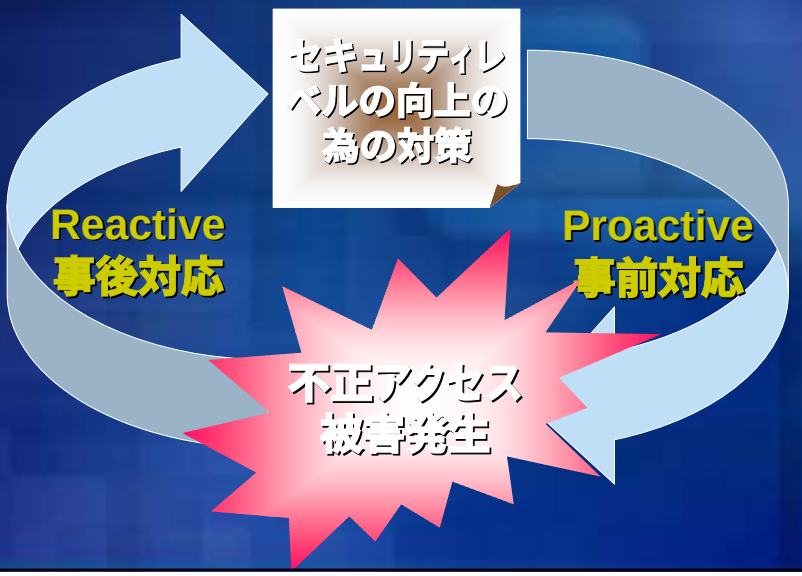
- 不正アクセスへの対応
- 記録（ログ）の収集
  - Windows 2000
  - Internet Information Server 5.0
  - SQL Server 2000
- ログの調査
  - イベントログ
  - IIS ログ
- その他のソリューション

不正アクセスへの対応

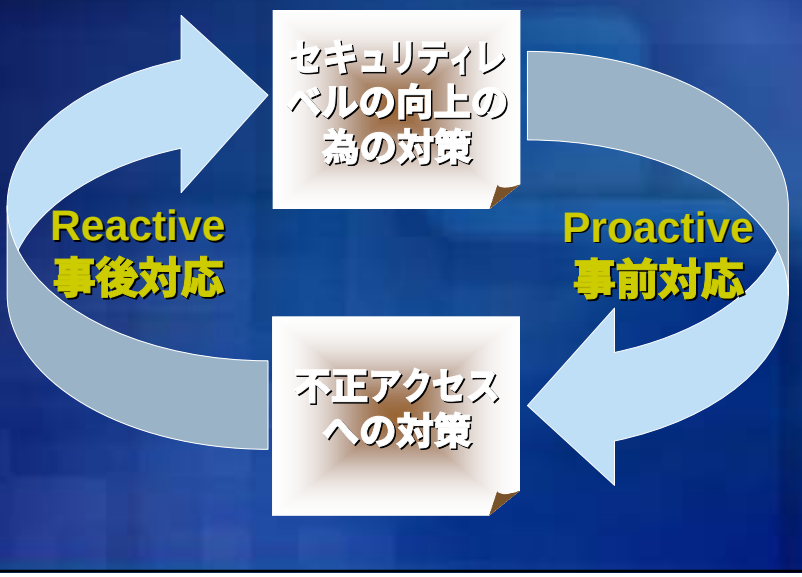
不正アクセスへの対応

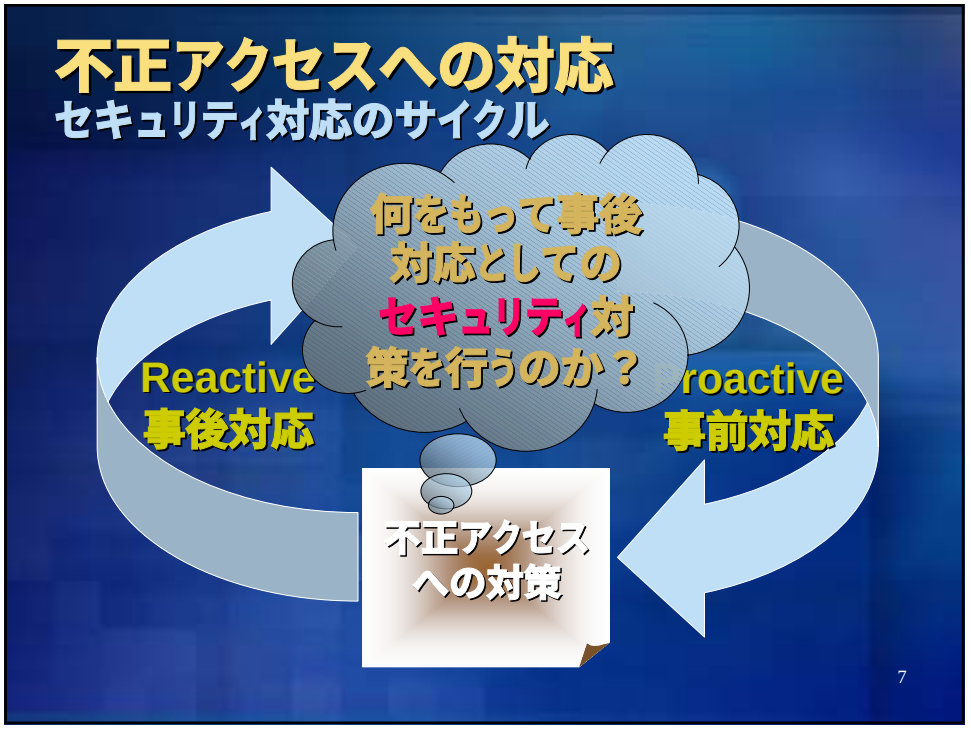
- 不正アクセスとは
  - 意図しないユーザーから
  - 意図しないリソースへ
  - 意図しない方法を使用してアクセス
- 不正アクセス防止法案の制定
  - パスワードの悪用
  - セキュリティホールの悪用
  - 刑事処罰の対象

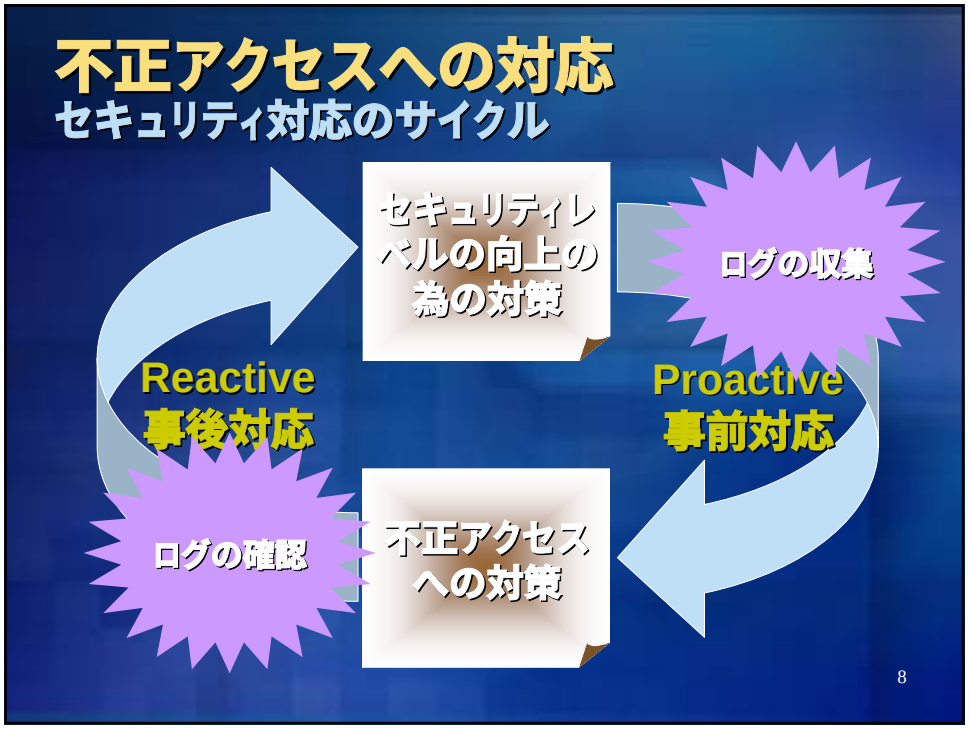
不正アクセスへの対応
セキュリティ対応のサイクル



不正アクセスへの対応
セキュリティ対応のサイクル




不正アクセスへの対応
セキュリティ対応のサイクル
何をもって事後対応としてのセキュリティ対策を行うのか？
Reactive
事後対応
roactive
事前対応
不正アクセスへの対策
7


不正アクセスへの対応
セキュリティ対応のサイクル
セキュリティレベルの向上の為の対策
ログの収集
Reactive
事後対応
Proactive
事前対応
ログの確認
不正アクセスへの対策
8

不正アクセスへの対応
不正アクセスを知る

- ネットワーク経由での不正アクセスの流れ
  - そのシステムのシステム構成を把握
    - ドメインの選定
    - 攻撃対象（ホスト）の決定
    - Port Scan
    - 公開リソースへのアクセス
    - パスワードアタック（権限の取得）
    - 追跡の無効化（ログ機能の停止）
    - 脆弱性の悪用
    - 非公開リソースへのアクセス
    - データの取得、書き換え、破壊
    - 行動の隠蔽（ログの破棄）
- 不正アクセスの殆どは、再試行を行っている
- 一度で成功した攻撃は、内部犯行の可能性もしくはソーシャルエンジニアリング

不正アクセスへの対応
動作記録（ログ）の収集の必要性

- 何に使用するのか
  - 事象（インシデント）の発見
  - インシデントの内容の検証
  - 告訴に向けた証拠の保持
- ログ収集の内容
  - ユーザー認証の有無、結果、失敗
  - オブジェクトへのアクセス有無、結果、失敗
  - プログラム実行の有無、結果、失敗
  - リクエストの受信記録

不正アクセスへの対応
ログ収集に関する注意点

- システムへの影響
  - パフォーマンスダウン
  - システムリソースの消費
  - 記憶領域リソースの消費
- 管理への影響
  - 取得した内容の確認作業に掛かる人件費
  - 突然の事態に対応した体制、ポリシー
- ログの取得の目的を見極める
  - ゴールは、不正アクセスの発見
  - 不正アクセスが成功した場合、記録は困難
    不正アクセスを失敗させることが重要

ログの収集

収集できる情報の種類

- イベントログ (共有機能)
  監査を有効にする必要がある
  - システムログ
  - セキュリティログ
  - アプリケーションログ
- パフォーマンスモニタ (共有機能)
  - システムの動作状況
- アプリケーションの各種ログ (個別機能)
  - アクセスログ

イベントログ

- OS に備わったログ機能
  - システム (主に OS, ドライバの状態)
  - アプリケーション (プログラム全体に開放)
  - セキュリティ (監査イベントの記録)
- システムの監査を行った場合、セキュリティイベントログへ記録
- イベントの記録が不可能となった時点で、コンピュータの停止が可能
  セキュリティオプションにて設定

イベントログ
取得例

イベントログの設定を行う

GPO の監査を有効にする

各フォルダの監査を有効にする

レジストリの監査を有効にする

イベントビューアのプロパティ設定
1. ログ格納先の確認
2. 最大ログサイズの設定確認

イベントログ
取得例

イベントログの設定を行う

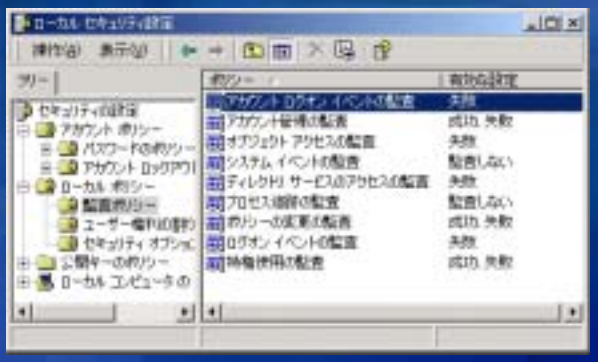
GPO の監査を有効にする

各フォルダの監査を有効にする

レジストリの監査を有効にする

監査ポリシーの設定

アカウント ログオン イベントの監査	失敗のみ
アカウント管理の監査	成功と失敗
オブジェクトアクセスの監査	失敗のみ
ディレクトリサービスのアクセスの監査	失敗のみ
ポリシーの変更の監査	成功と失敗
ログオンイベントの監査	失敗のみ
特権使用の監査	失敗のみ



イベントログ
取得例

イベントログの設定を行う

GPO の監査を有効にする

各フォルダの監査を有効にする

レジストリの監査を有効にする

監査ポリシーの設定

アカウント ログオン イベントの監査
ドメインログオンの失敗を監査し、パスワードに対する Brute Force 攻撃を検出

アカウント管理の監査
アカウントの削除、もしくは不正使用用途のアカウント作成を検出

オブジェクトアクセスの監査
ファイルなどに対してのアクセスを検出、フォルダへの不正ファイルの書き込みも発見可能

ディレクトリサービスのアクセスの監査
ディレクトリのデータの改ざんの検出が可能

ポリシーの変更の監査
監査を無効とする事前攻撃を検出

ログオンイベントの監査
アカウントのコンピュータへのログオンの失敗を監査し、Brute Force 攻撃を検出

特権使用の監査
監査の結果が非常に多くなるため失敗のみ記録し、プロセスが特権の取得に失敗した事を検出可能

イベントログ
取得例

イベントログの設定を行う

GPO の監査を有効にする

各フォルダの監査を有効にする

レジストリの監査を有効にする

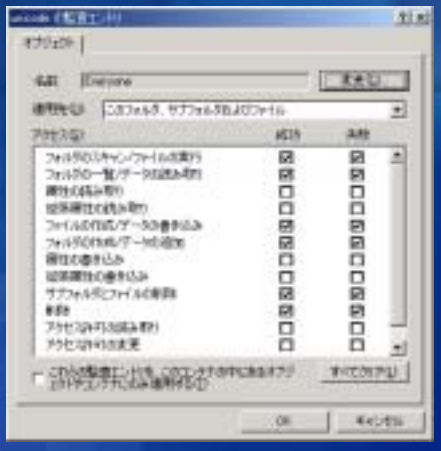
フォルダの監査設定

システムフォルダの監視

アプリケーションフォルダの監視

ドライブルートの監視

重要データの監視



イベントログ
取得例

- イベントログの設定を行う
- GPO の監査を有効にする
- 各フォルダの監査を有効にする
- レジストリの監査を有効にする

フォルダの監査設定

システムフォルダの監視
システムフォルダに保存されたアプリケーション (コマンドプロンプトなど) を実行されたり書き換えられた際の経過を記録

アプリケーションフォルダの監視
使用しているアプリケーションや、そのデータが保存されているフォルダへのアクセスを記録
アプリケーションのログも対象

ドライブルートの監視
ドライブのルートディレクトリ (特に C ドライブ) への書き込みの有無について記録

重要データの監視
その他、コンピュータ上で重要と考えられる情報へのアクセスの失敗を記録

イベントログ
取得例

- イベントログの設定を行う
- GPO の監査を有効にする
- 各フォルダの監査を有効にする
- レジストリの監査を有効にする

レジストリ監査設定

監視が必要なレジストリのみ、アクセスの追跡を行う
データ量が過大となるため、常時の取得は危険
Windows 2000 では regedt32.exe を使用

イベントログ
IIS と SQL Server のセキュリティイベント

- IIS
  - Windows の SAM を使用した認証を使用した場合に記録される
- SQL
  - セキュリティイベントには記録されず、アプリケーションイベントへ記録

パフォーマンスモニタ

- 効果的なイベントのデータを累積的に取得することが可能
- 複数のソースのデータを一元管理可能
- データのサンプリングタイムをカスタマイズ可能
- 時系列でのデータ取得が可能で、傾向を調べる事が可能
- 閾値を超えたデータが発見された場合に、外部アプリケーションの呼び出しが可能
- 詳細が取得できないため、一時調査もしくは監視に向く

パフォーマンスモニタ
Windows 2000

- Server オブジェクト
  - Errors Access Permissions カウンタ
    権限がないファイルに対してアクセスが試行された回数が記録される。この回数が増加することで不正アクセスの検出が可能
  - Errors Granted Access カウンタ
    読み取りアクセスのみが許可されたコンテンツに対して書き込み操作や削除の操作を行った場合に記録される
  - Errors Logon カウンタ
    ログオンに失敗した場合に記録される。パスワードに対しての Brute Force 攻撃を受けている場合には急激に増加する
- IP オブジェクト
  - Datagrams Received Header Errors カウンタ
    正しくないチェックサム、バージョン番号の不一致、そのほかのフォーマットエラー、タイムアウト、期限切れ TTL、IP オプション処理時に検出されたエラーが記録される。機器の異常やDoS 攻撃の検出が出来る可能性がある
  - Datagrams Received Unknown Protocol カウンタ
    受信したデータのプロトコルが不正だった場合に記録される。機器の異常やDoS 攻撃の検出が出来る可能性がある

パフォーマンスモニタ
Internet Information Server 5.0

- Active Server Pages オブジェクト
  - Request Failed Total カウンタ
    エラーにより拒否された件数を確認可能。BoR などのアタックを試行している事が確認できる可能性
  - Request Queued カウンタ
    リクエストがサーバーの処理件数を超えた場合に蓄積された数。DoS などの攻撃を発見できる可能性
- Web Service オブジェクト
  - Total Copy Requests/Total Delete Requests カウンタ
    HTTP 1.1 の拡張メソッドを使用した改ざんの可能性を検出
  - Total Head Requests カウンタ
    Server のバナーを調べたりする場合に送信されることがある。
  - Logon Attempts/sec カウンタ
    1秒間に行われるユーザー認証の要求数を記録。Brute Force 攻撃によるリクエスト数の増加を検出可能

パフォーマンスモニタ
SQL Server 2000

- General Statistics オブジェクト
  - Logins/Sec カウンタ
    ログインを一秒間に試行した回数

アクセスログ

- 各アプリケーションが記録する内容
- アプリケーション毎に内容が異なる
- 参照する情報の目的が異なる
- 一般的に以下の2種類の取得が期待できる
  - リクエストの追跡
  - 重要情報の記録

アクセスログ
Internet Information Server 5.0

- W3C 拡張ログ形式にて以下のアクセスログを取得する
  - 日付 (date) ※GMT
  - 時刻 (time) ※GMT
  - クライアント IP アドレス (c-ip)
  - ユーザー名 (cs-username)
  - メソッド (cs-method)
  - URI Stem (cs-uri-stem)
  - URI クエリ (cs-uri-query)
  - プロトコルの状態 (sc-status)
  - Win32 の状態 (sc-win32-status)
  - ユーザー エージェント (cs(User-Agent))
  - サーバー IP アドレス (s-ip)
  - サーバー ポート (s-port)

Win32 Status に関しては、MSDN ライブラリを参照
http://msdn.microsoft.com/library/en-us/debug/base/system_error_codes.asp

アクセスログ (URLScan ログ)
Internet Information Server 5.0

- URLScan により破棄されたリクエストのみ記録する事が可能
  - リクエストメソッド (Verb)
  - リクエストされたリソースのファイル拡張子
  - 疑わしい URL エンコード
  - URL 中の ASCII 以外の文字の存在
  - URL 中の特定の文字シーケンスの存在
  - リクエストの中の特定のヘッダーの存在
- 注意：Web Application が正常に動作しなくなる可能性があるため、使用する場合にはテスト環境で十分な動作検証が必要

アクセスログ (URLScan ログ)

Internet Information Server 5.0

- **ログの推奨設定 (URLScan 2.5 を使用)**
  - EnableLogging = 1
    ログの取得を有効にする
  - PerProcessLogging = 1
    複数サイトをホスティングしている場合、サイト毎にログファイルを作成する
  - LoggingDirectory = L:¥logging¥URLScan
    ログの保存ディレクトリを変更する
    ログのバックアップの簡略化と保護の為
  - LogLongUrls **= 0**
    ログに記録する URL **の長さを指定。ログファイルサイズを抑えるため、既定の** 1024 **バイトで十分。明確な攻撃が確認された場合には、**128KB **まで拡張可**

プロファイラ

SQL Server 2000

- **セキュリティ監査クラスを使用し、情報を得る**
  - **ログオンの試行**
    - **Audit Logon Failed**
  - **ユーザアカウントの操作 (権限の奪取)**
    - **Audit Add DB User**
    - **Audit Add Logon to Serer Role**
    - **Audit Member to DB Role**
    - **Audit Add Role**
  - **データへの不正アクセス**
    - **Audit Object Permission**
    - **Audit Statement Permission**
    - **Audit DBCC**
    - **Audit Backup/Restore**
  - **監査の無効化**
    - **Audit Change Audit**

SQL ログの活用

SQL Server 2000

クエリーの妥当性判断 (論理判断) は、非常に困難

- テーブルにトリガを仕掛け、そのテーブルの更新時にユーザーイベントを出力させることで検出

- データベースの設定をログファイルへ定期的に出力し、確認を行う (プロファイラと同処理)

```
declare @TRCID int
declare @LOGPATH nvarchar(128)

set @TRCID=0
set @LOGPATH='S:¥SQLDB¥MSSQL¥LOG¥audit_trace.log3.trc'

exec sp_trace_create @TRCID output, 2, @LOGPATH, NULL, NULL
select @TRCID
declare @ON bit
set @ON=1
-- Login fail
exec sp_trace_setevent @TRCID, 20, 1, @ON
exec sp_trace_setevent @TRCID, 20, 6, @ON
exec sp_trace_setevent @TRCID, 20, 7, @ON
exec sp_trace_setevent @TRCID, 20, 8, @ON
exec sp_trace_setevent @TRCID, 20, 11, @ON
```

```
exec sp_trace_setstatus @TRCID, 1
go

--
-- Trace Status
SELECT * FROM ::fn_trace_getinfo (default)

--
-- Trace Stop(pause)
exec sp_trace_setstatus 1, 0

--
-- Trace Stop(delete)
exec sp_trace_setstatus 1, 2
```

アタックが検出できるか

demo

ログの調査

ログの調査
サーバーの動作を追跡

- ログを確保する
  - Dump Event Log (dumpel.exe) (Free)
    イベントログの内容をテキストとして取り出す
    Windows 2000 Resource Kit の diag.cab ファイル内
    dumpel.exe –l security
  - EventconbMT (Free)
    イベントログの内容をテキストファイルとして取得
    複数のサーバーから、複雑なフィルタを行う事が可能
    http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9989D151-5C55-4BD3-A9D2-B95A15C73E92

ログの調査
ログは宝、しっかり保護を

- ログの保護
  - イベントログファイルの退避先の変更
    - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥<種別>¥File レジストリ値
    - .evt ファイルの移動が必要
  - IIS アクセスログの記録先の変更
    - インターネットサービスマネージャより変更可能
  - 痕跡を消されないための設定
    - アクセスログ格納ディレクトリのアクセス権確認 (ACL 設定)
      サービスを実行を行っているアカウントと管理者のみへアクセス許可
    - イベントログの操作権限の確認 (GPO)
    - Syslog ツールや内部ネットワークへのデータの退避 (ツール)

ログの調査
アプリケーションからの操作

- WMI の活用 (Windows Management Instrumentation)
  - マイクロソフトの独自技術ではなく、DMTF（Distributed Management Task Force）が標準化したオブジェクトモデルスキーマ CIM（Common Information Model）がベース
  - CIM は WBEM（Web-based Enterprise Management）のモデリング基盤に沿い実装されている
- 本セッションに関連する WMI Class
  - Win32 Class を使用
  - Win32_NTEventlogFile
  - Win32_SecuritySettingAuditing

```
LogFileSet = GetObject("winmgmts:{impersonationLevel=impersonate,
(Backup)}").ExecQuery("select * from Win32_NTEventLogFile where logfileName='Application'")
for each Logfile in LogFileSet
  RetVal =
  LogFile.BackupEventlog("c:¥BACKUP.LOG")
  if RetVal = 0 then WScript.Echo "Log BackedUp"
next
```

イベントログの書き出しサンプル

ログの調査
参照しないログなら意味が無い

- ログを検証する (ツール)
  - Cybersafe Log Analysis (Free)
    イベントログの内容をレポートとして出力
    Windows 2000 Resource Kit の ¥apps¥loganalyst フォルダ内
  - Log Parser 2.0 (Free)
    IIS のログファイルを SQL Query 文で分析することが可能
    癖があるので SQL Query に慣れた管理者向け
    http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8CDE4028-E247-45BE-BAB9-AC851FC166A4
  - Excel などスプレッドシート
    少ないログであれば表計算ソフトでも代用可能
  - Analog (Free)
    3rd party 製の 無料ツール。サイトの分析が可能。
    http://www.analog.cx/

ログの調査
Windows 2000 のイベントログ

- 不正なユーザーがログオンを試していないか？
  - Security Event へ 監査の失敗 Event ID 529 が記録
    - Logon Type: 3 ネットワークログオン
    - Logon Type: 2 インタラクティブログオン
- 未許可オブジェクトへアクセスされていないか？
  - Security Event へオブジェクトアクセス Event ID 560 が記録
    - プロセスにより、踏み台とされたプロセスを認識
    - アクセスタイプにより不正アクセスの種類を認識
- 期待していないプロセスが起動していないか？
  - Security Event へオブジェクトアクセス Event ID 560 が記録
    - オブジェクト名により実行プログラムを認識
    - アカウント名から実行ユーザーを認識
- アカウントが追加されたり変更されていないか？
  - Security Event へアカウント管理イベントが記録
    - Event ID 624 アカウントの作成
    - Event ID 642 アカウントパスワードの変更
    - Event ID 630 アカウントの削除

ログの調査
IIS 5.0 のイベントログ

- IIS へ Brute Force 攻撃を行われていないか？
  - Security Event へ 監査の失敗 Event ID 529 が記録
    - Logon Type: 3 ネットワークログオン (NTCR)
    - Logon Type: 2 インタラクティブログオン (Basic)
- コマンドプロンプトを悪用されていないか？
  - System Event へ W3SVC Event ID 16 が記録
    'xxx=aaa' の URL '/yyy/cmd.exe' で始まるスクリプトが、構成されたタイムアウト時間内に応答しませんでした。HTTP サーバーはこのスクリプトを終了します。応答データを返さないアプリケーションを実行した場合に、CGI プロセスを終了した
- Web Application への BoR 攻撃は無いか？
  - System Event へ W3SVC Event ID 37 が記録
    処理外のアプリケーション '/LM/W3SVC/1/ROOT' を予期せず終了しました。インプロセスアプリケーションの場合に記録される

ログの調査
SQL Server 2000 のイベントログ

- SQL Server への Brute Force 攻撃
  - アプリケーションログに
    イベント ID 4 ログオンエラーが記録

ログの調査
IIS 5.0/ URLScan のアクセスログ

- アプリケーションへの BoR 攻撃
  - IIS ログに HTTP ステータス５００ が記録されている
- 未公開ファイルへのアクセス（顧客情報など）
  - 見知らぬコンテンツに対してアクセスが行われており、HTTP ステータス 200 が返信されている
- ログオンページを悪用した Brute Force 攻撃
  - 同じ IP アドレスから複数回アクセスがある
- Web の改ざん検出
  - FrontPage や WebDav に対してのアクセスが頻繁に行われている
  - CGI もしくは cmd.exe などへのアクセス

ログの調査
SQL Server 2000 のアクセスログ

- パスワードの Brute Force 攻撃がないか？
  - Logon Fail イベントが多発している
- 不正なユーザ、ロールが追加されていないか？
  - ユーザやロールの操作をログから確認
- 不正な操作が行われていないか？
  - DBCC など自由度の高いコマンドの検出
  - 強力な SP の実行を検出
  - データの置き換え、ダンプを検出
- 記録の無効化が行われていないか？
  - 監査の設定変更を検出

ログ分析ツール

demo

その他のソリューション

その他のソリューション
更に確実に不正アクセスを迎え撃つには

- ネットワークログ
  - ファイヤウオール
  - ルーター
- 侵入検出
  - IDS:侵入検知システム (ISS その他)
  - 改ざん検知システム (Tripwire その他)
  - 運用監視ソリューション (LAC その他)
- セキュリティスペシャリストの参画
  やはりプロの仕事は確実
  - 監視の外部委託
  - コンサルティング契約による定期確認
  - 脆弱性診断

まとめ

- 重要なのは、攻撃を受ける事ではなく、攻撃を受けている事を認知すること
- 将来的なトラブルに備え、証拠を確保する事は危機管理の基本
- パフォーマンスとセキュリティ対策のトレードオフを認識し、妥協点を検討
- マイクロソフト製品の提供している機能は最低限であるが、活用を検討