

Windowsサーバシステムのログ管理

インターネット セキュリティ システムズ株式会社
テクニカル・ソリューション課 マネージャ
エグゼクティブ セキュリティ エンジニア
小倉 秀敏

対象アプリケーション

- **Internet Information Server**
- **SQL Server**

ログ管理の目的

- **目的**
 - 定常状態を知る
 - セキュリティ問題が発生している兆候を知る
- **不正侵入・不正利用の防止は不可能**
 - 事後の発見のみ
 - 防御には防御ソリューションが必要
 - サーバに対する「悪意を持った全ての操作」が記録できるわけではない
- **フォレンジックスを目的にしない方がよい**
 - フォレンジックスには専門のトレーニングが必要
 - Explorerでログファイルを参照するだけで証拠能力は消滅

ログ管理を容易にするために・・・ カスタムMMCの構成

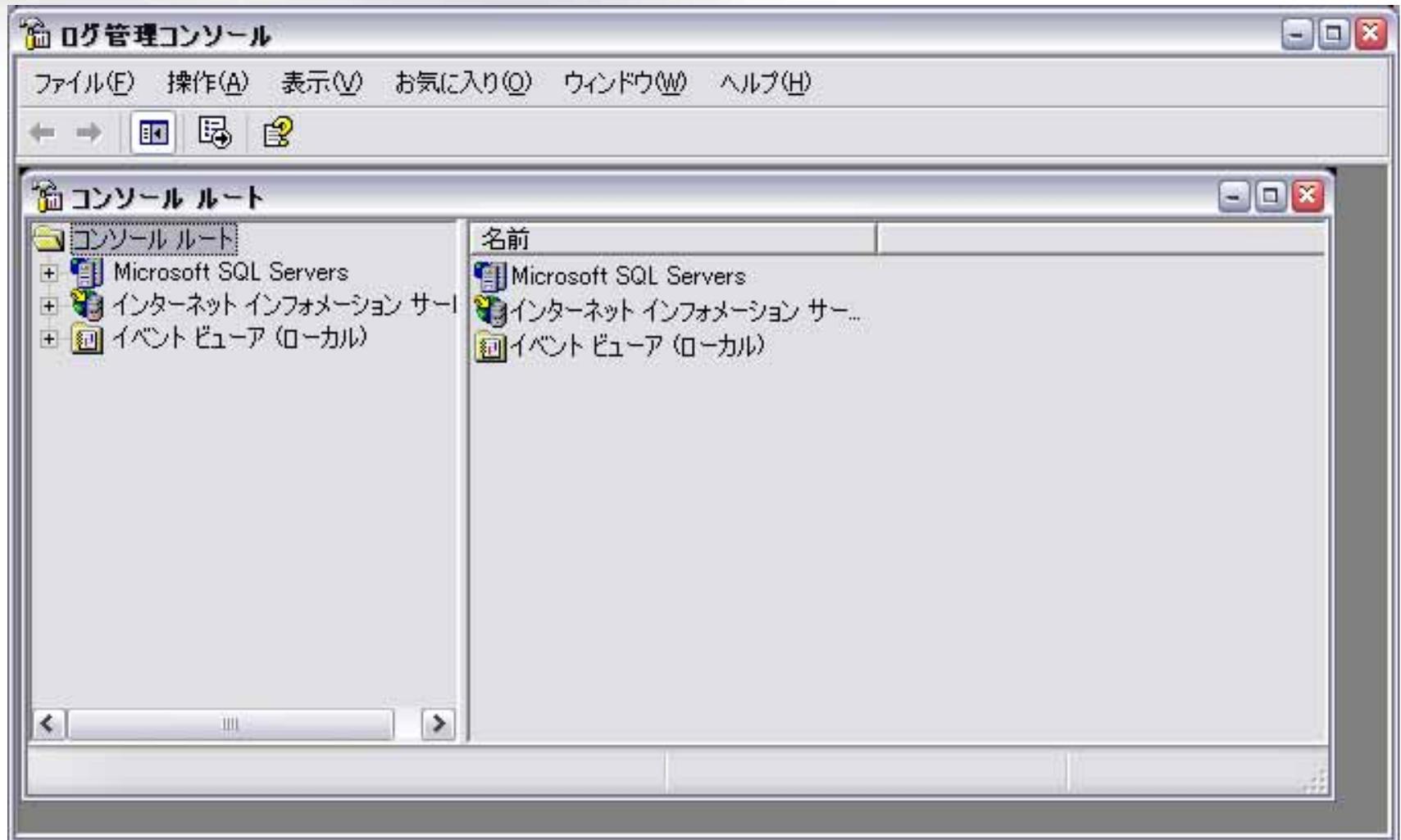
- 専用のMMCコンソールファイルの作成
 - mmc /aコマンドによるカスタムコンソールファイルの作成
 - SQL Enterprise Manager、IISコンソール、イベントビューア等をひとまとめに

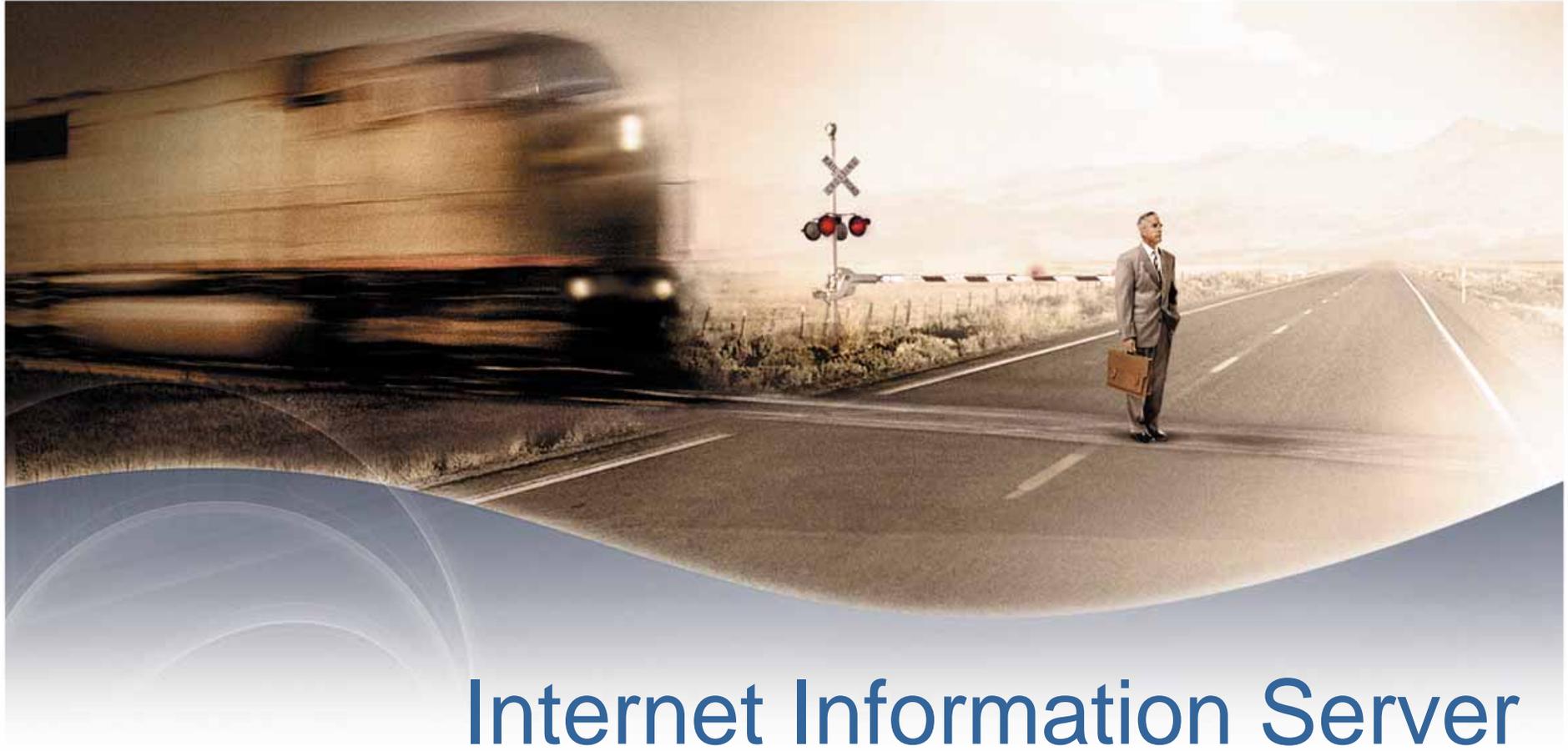


MMCへのスナップインの追加



カスタマイズが終了したMMC





Internet Information Server

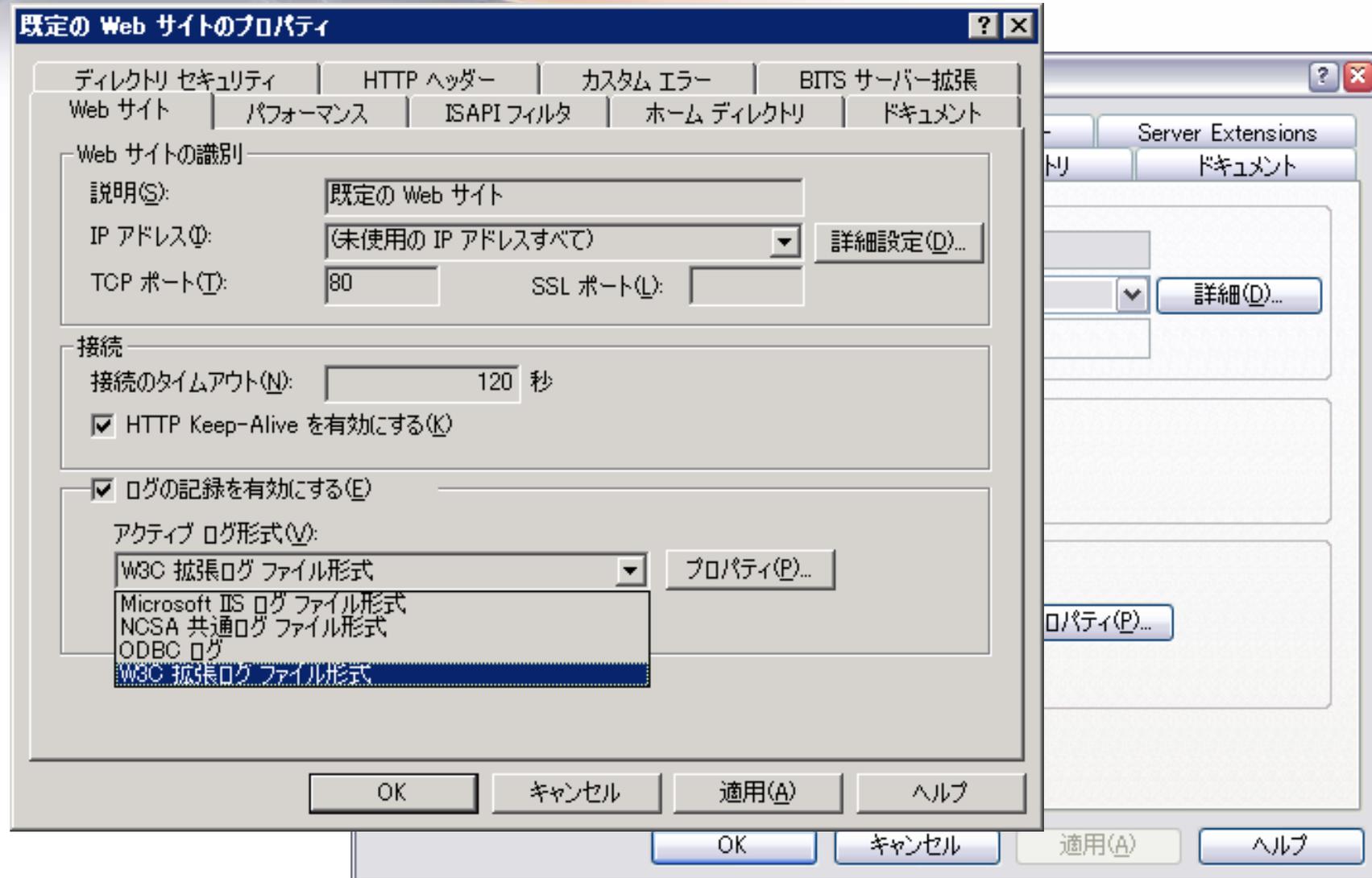
■ 対象ログ

- %SystemRoot%\system32\Logfilesディレクトリに保存されるログ

■ 解析する内容とは

- IISに対するアクセスログ
- 制限的であることを理解する必要あり
 - バッファオーバーフローにより動作させられたプログラム等をログすることはできない
 - Webアプリケーションの構成によりログに保存できるレベルが影響を受ける

IISログ形式の設定



■ データベースへのログ保管

- Windows 2003 ServerのIIS 6.0から利用可能
- ログ保管先にデータベースを利用
- データベースに保管された他システムとのログの突き合わせには有効
 - IPアドレスなどを利用した複数ログの結合クエリ
- IIS自体のパフォーマンスに影響を与えるため積極的には使用されない
ClientHost, Username, LogTime, Service, Machine, ServerIP,
ProcessingTime, BytesRecvd, BytesSent, ServiceStatus, Win32Status,
Operation, Target, Parameters

IISで記録可能な項目

拡張設定項目	説明
クライアント IP アドレス	クライアントのIPアドレス
ユーザ名	サーバにアクセスしたユーザの名前
サービス名	クライアントで実行されているインターネット サービス
サーバー名	サーバの名前
サーバー IP	サーバのIPアドレス
サーバー ポート	クライアントが接続したポート番号
メソッド	クライアントが実行を試みたアクション
URI Stem	HTML ページ、CGI プログラム、スクリプトなどの、アクセスされたリソース
URI クエリ	クライアントが実行しようとしたクエリ文字列
プロトコルの状態	HTTP 関連の処理の状態
Win32の状態	Windows 関連の処理の状態
送信バイト数	サーバが送信したバイト数
受信バイト数	サーバが受信したバイト数
所要時間	処理にかかった時間
プロトコルバージョン	クライアントが使用したプロトコルバージョン
ホスト	コンピュータ名
ユーザエージェント	クライアントが使用したブラウザ
Cookie	送受信された Cookie の内容
参照者	ユーザを現在のサイトに導いたサイト
プロトコルの副状態	HTTP 関連の処理のその他の状態

■ URIクエリを追加しない場合

- #Fields: time c-ip cs-method cs-uri-stem sc-status
- 00:57:12 xx.xx.xx.xx POST /iishelp/iis/misc/Query.asp 200

■ URIクエリを追加した場合

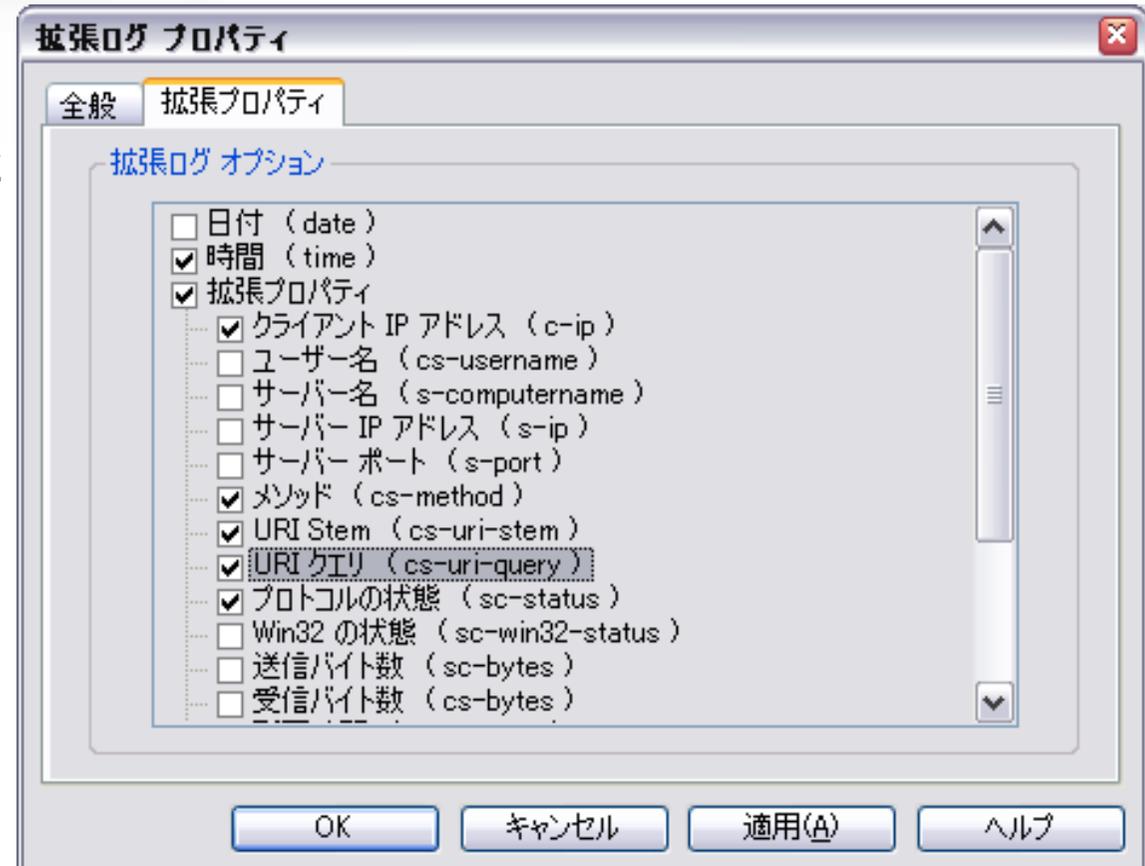
- #Fields: time c-ip cs-method cs-uri-stem cs-uri-query sc-status
- 00:58:45 xx.xx.xx.xx POST /iishelp/iis/misc/Query.asp
SearchType=0 200

■ ユーザーエージェントはあまり意味がない

- 01:14:55 xx.xx.xx.xx POST /iishelp/iis/misc/Query.asp SearchType=3 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)

IISログ設定

- URIクエリをログに残す
 - URIを残すことで、クエリとして渡された文字列を確認することが可能



どんなログを残すか

■ 利用状況を把握した上での設定

- 利用しているメソッドに応じた設定
- GETメソッドのみであればURI、POSTメソッドを使っているのであればCookie等その他の情報

```
#Fields: time c-ip cs-method cs-uri-stem cs-uri-query sc-status cs(Cookie) cs(Referer)
02:35:53 xx.xx.xx.xx GET /iishelp/iis/misc/search.asp Searchset=3&SearchString=オブジェクト 200 ASPSESSIONIDGGQGGVFC=IFFFPKHBBLNMNEIFJJBPHOMB
http://localhost/iishelp/iis/misc/default.asp
02:35:55 xx.xx.xx.xx POST /iishelp/iis/misc/Query.asp SearchType=3 200
ASPSESSIONIDGGQGGVFC=IFFFPKHBBLNMNEIFJJBPHOMB
http://localhost/iishelp/iis/misc/search.asp?Searchset=3&SearchString=オブジェクト
```

■ 取得する情報の選択

- Webアプリケーションで利用しているものを確認して項目を設定
- GETメソッドが利用される場合URIが重要
- POSTメソッドを使用している場合は渡される内容を直接取得は不可能
- 受信バイト数、送信バイト数
 - XSS攻撃の際、リクエスト、レスポンスが大きくなる可能性があるため送信バイト数や受信バイト数が利用できる可能性あり

攻撃とログの例

- ディレクトリ・トラバーサル
- IDS検知回避
- バッファ・オーバーフロー

ディレクトリ・トラバーサル

■ /cgi-binディレクトリ配下からディレクトリ・トラバーサルを利用

```
2005-01-25 04:44:31 192.168.35.52 GET /cgi-bin/main.cgi  
board=FREE_BOARD&command=down_load&filename=../../../../ 80 -  
192.168.35.217 - 404 0 3 1800 150
```

```
2005-01-25 04:44:31 192.168.35.52 GET /cgi-bin/main.cgi  
board=FREE_BOARD&command=down_load&filename=../../../../../../../../  
./etc/passwd 80 - 192.168.35.217 - 404 0 3 1800 178
```

```
2005-01-25 04:44:31 192.168.35.52 GET /cgi-bin/main_menu.pl - 80 -  
192.168.35.217 - 404 0 3 1800 97
```

```
2005-01-25 04:44:31 192.168.35.52 GET /cgi-bin/majordomo.pl - 80 -  
192.168.35.217 - 404 0 3 1800 97
```

```
2005-01-25 04:44:31 192.168.35.52 GET /cgi-  
bin/makechanges/easysteps/easysteps.pl - 80 - 192.168.35.217 - 404 0 3  
1800 119
```

```
2005-01-25 04:44:31 192.168.35.52 GET /cgi-bin/man.sh - 80 -  
192.168.35.217 - 404 0 3 1800 91
```

ディレクトリ・トラバーサル

■ IntelInfoディレクトリからのトラバーサル

2005-01-25 05:12:46 192.168.35.52 GET /..%2f..%2f..%2f..%2fwinnt/system32/cmd.exe /c+dir+c: 80 - 192.168.35.217 - 404 0 3 1800 137

2005-01-25 05:12:46 192.168.35.52 GET /..%5c..%5c..%5c..%5c..%5c../winnt/system32/cmd.exe /c+dir+c:¥ 80 - 192.168.35.217 - 404 0 3 1800 148

2005-01-25 05:12:46 192.168.35.52 GET /..%5c..%5c..%5c..%5cwin2000/system32/cmd.exe /c+dir 80 - 192.168.35.217 - 404 0 3 1800 136

2005-01-25 05:12:46 192.168.35.52 GET /..%5c..%5c..%5c..%5cwindows/system32/cmd.exe /c+dir 80 - 192.168.35.217 - 404 0 3 1800 136

2005-01-25 05:12:46 192.168.35.52 GET /..%5c..%5c..%5c..%5cwinnt/system32/cmd.exe /c+dir 80 - 192.168.35.217 - 404 0 3 1800 134

2005-01-25 05:12:46 192.168.35.52 GET /..%5c..%5cwinnt/system32/cmd.exe /c+dir+c: 80 - 192.168.35.217 - 404 0 3 1800 123

Nimdaが残すディレクトリ・トラバーサル

■ Nimdaワームが残す典型的なログ (URIのみ)

```
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /msadc/..%5c../..%5c../..%5c/..%5c1%5c1c../..%5c1%5c1c../..%5c1%5c1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c1%5c1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c0../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c0%5c%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c1%5c9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c3c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c3c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

IDS等の検知回避系

■ IDSの検知回避もしくはディレクトリ・トラバーサルを目的

- Nimda等の攻撃にも含まれる
- URIに含まれる文字列をエンコード
- 現在この手法で回避されるIDSはない

2005-01-25 04:44:58 192.168.35.52 GET /.%2e/.%2e/.%2e/winnt/boot.ini - 80 - 192.168.35.217 - 404 0 3 1800 112

2005-01-25 04:44:58 192.168.35.52 GET /.%2e/.%2e/.%2e/winnt/repair/sam._ - 80 - 192.168.35.217 - 404 0 3 1800 116

2005-01-25 04:44:58 192.168.35.52 GET
/..%2f..%2f..%2f..%2f..%2f../windows/repair/sam - 80 - 192.168.35.217 - 404 0 3 1800 133

2005-01-25 04:44:58 192.168.35.52 GET
/..%2f..%2f..%2f..%2f..%2f../winnt/repair/sam - 80 - 192.168.35.217 - 404 0 3 1800 131

2005-01-25 04:44:58 192.168.35.52 GET
/..%2f..%2f..%2f..%2f..%2f../winnt/repair/sam._ - 80 - 192.168.35.217 - 404 0 3 1800 133

バッファオーバーフロー系

■ IIS idq.dll ISAPI extension buffer overflow

2005-01-25 05:24:22 192.168.35.52 GET /null.ida

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
=x 80 - 192.168.35.217 - 404 0 2 1800 286
```

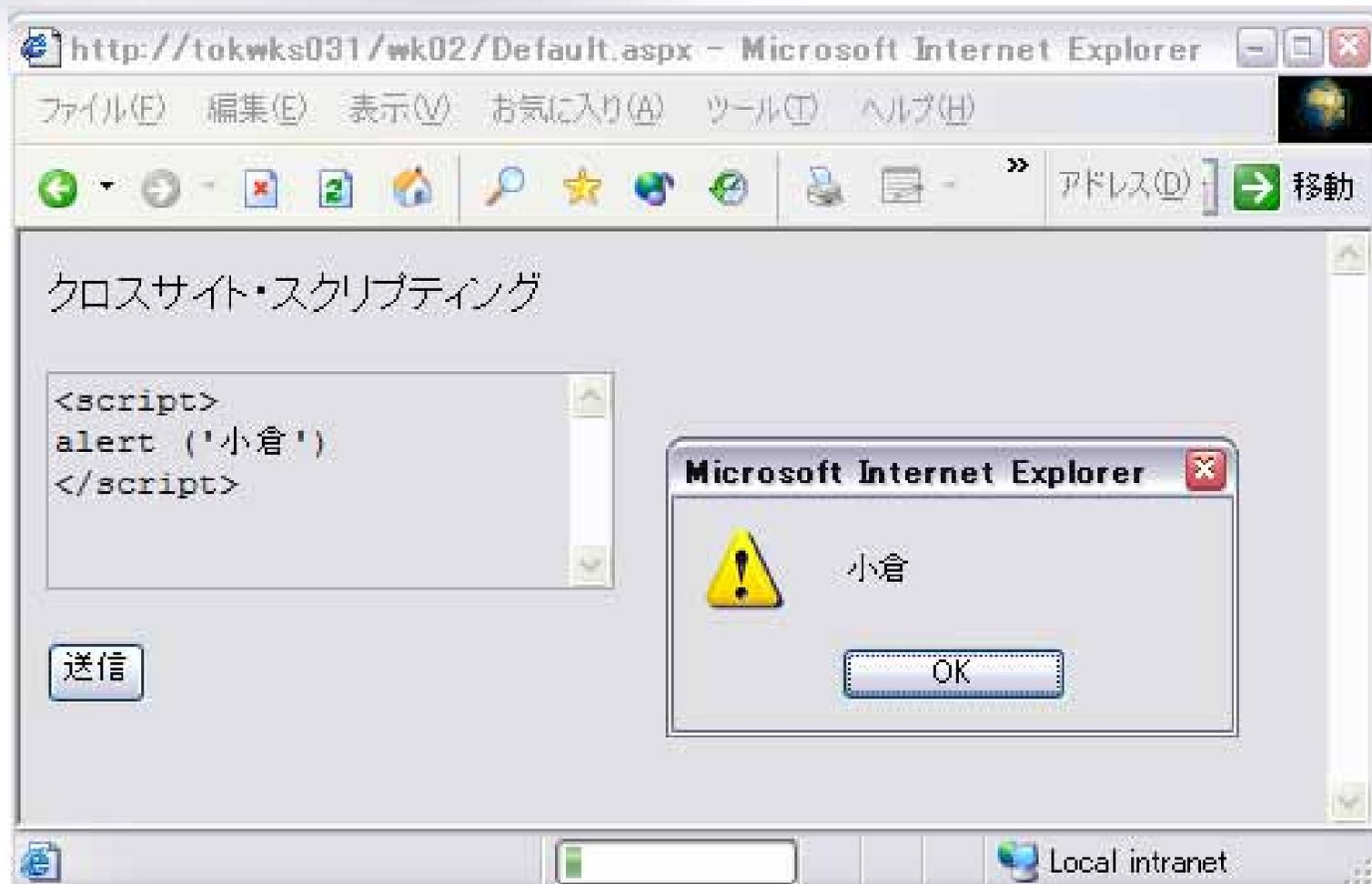
2005-01-25 05:24:22 192.168.35.52 GET /null.ida

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
x=x 80 - 192.168.35.217 - 404 0 2 1800 287
```

2005-01-25 05:24:22 192.168.35.52 GET /null.ida

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX=x 80 -  
192.168.35.217 - 404 0 2 1800 338
```


クロスサイト・スクリプティング



- **<script>・・・</script>がPOSTで渡されていることが分らない**
 - #Software: Microsoft Internet Information Services 6.0
 - #Version: 1.0
 - #Date: 2005-01-24 20:20:43
 - #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
cs(Cookie) sc-status sc-substatus sc-win32-status sc-bytes cs-bytes
 - 2005-01-24 20:20:43 192.168.35.52 GET /wk02/Default.aspx - 80 - 192.168.35.217
CookieLoginAttempts=4 200 0 0 994 405
 - 2005-01-24 20:21:08 192.168.35.52 POST /wk02/Default.aspx - 80 - 192.168.35.217
CookieLoginAttempts=4 200 0 0 1132 820
- **Webアプリケーションの構成により、攻撃自体がログに残らない**
- **注意: W3C形式でログを保存した場合、時刻はGMT**
 - Microsoftサポートオンライン: 拡張ログファイル形式では時刻が常にGMTで記録される
 - <http://support.microsoft.com/default.aspx?scid=kb;ja;194699>

IPSであれば・・・

- POSTメソッドによるクロスサイト・スクリプティングを検知可能
 - IISのログでは確認できない内容を補うことが可能

The screenshot shows a window titled "Event Details 1/14" with two main sections: a table of event details and a list of event attribute value pairs.

Event Details Name	Event Details Value
Date/Time	2005-01-25 05:21:09 JST
Tag Name	HTTP_POST_Script
Alert Name	HTTP_POST_Script
Severity	Medium
Observance Type	Intrusion Detection
Combined Event Count	1
Cleared Flag	<input type="checkbox"/>
Target IP Address	192.168.35.52
Target Object Name	80
Target Object Type	Target Port
Target Service	http
Source IP Address	192.168.35.217
SourcePort Name	2961
Sensor IP Address	192.168.35.52
Sensor Name	server_sensor_1

Attribute Name	Attribute Value
algorithm-id	2000635
AttackSuccessful	2
DestinationEthernetAddress	00:50:56:C0:00:08
field	TextBox1
IANAProtocolId	6
protocol	http
server	tokwks031
SystemAgent	TOKWKS031
URL	/wk02/Default.aspx
value	<script> .alert+('.</script>

The "value" attribute is highlighted with a red dashed box.

On the right side of the window, there is a text area containing the following information:

HTTP POST contains malicious script (HTTP_POST_Scri

About this signature or vulnerability

RealSecure Server Sensor, BlackICE Agent for Server, RealSecure Desktop Protector, BlackICE Server Protection, BlackICE PC Protection, RealSecure Sentry, RealSecure Guard, M Series, RealSecure Network Sensor:

This signature detects if an HTTP POST command contains a <script> tag

At the bottom of the window, there are buttons for "OK", "Cancel", "Information...", "Copy...", "Export...", and "Go". The "Event Number" is set to 1.

IPSでの検知時の情報

- Date/Time : 2005-01-25 05:21:09 JST
- Tag Name : HTTP_POST_Script
- Alert Name : HTTP_POST_Script
- Severity : Medium
- Tag Brief Description :
- Observance Type : Intrusion Detection
- Combined Event Count : 1
- Cleared Flag : No
- Target DNS Name :
- Target IP Address : 192.168.35.52
- Target Object Name : 80
- Target Object Type : Target Port
- Target Service : http
- Source DNS Name :
- Source IP Address : 192.168.35.217
- SourcePort Name : 2961
- Sensor DNS Name :
- Sensor IP Address : 192.168.35.52
- Sensor Name : server_sensor_1
- Attribute Value Pairs for Event Number : 1
- Attribute Name : algorithm-id
- Attribute Value : 2000635
- Attribute Name : AttackSuccessful
- Attribute Value : 2
- Attribute Name : DestinationEthernetAddress
- Attribute Value : 00:50:56:C0:00:08
- Attribute Name : field
- Attribute Value : TextBox1
- Attribute Name : IANAProtocolId
- Attribute Value : 6
- Attribute Name : protocol
- Attribute Value : http
- Attribute Name : server
- Attribute Value : tokwks031
- Attribute Name : SystemAgent
- Attribute Value : TOKWKS031
- Attribute Name : URL
- Attribute Value : /wk02/Default.aspx
- Attribute Name : value
- Attribute Value : <script>..alert+('..</script>

SQLインジェクション

■ サンプルWebサイトに対してSQLインジェクションによるログイン認証回避

- ユーザ認証を以下のようなSQLで実現している場合

```
SELECT UserID FROM UserTbl
```

```
WHERE UserName = txtUserName AND Passwrđ = txtPassword
```

- ユーザ名として' OR 1=1 を与えると…

```
SELECT UserID FROM UserTbl
```

```
WHERE UserName = txtUserName AND Passwrđ = txtPassword OR 1=1
```

- 常に認証に成功

- 正規のユーザ名とパスワードを知っている必要がない

SQLインジェクションの際のログ

- 不正なSQL文が渡されていることが分からない

#Software: Microsoft Internet Information Services 6.0

#Version: 1.0

#Date: 2005-01-24 21:00:37

#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username
c-ip cs(Cookie) sc-status sc-substatus sc-win32-status sc-bytes cs-bytes

2005-01-24 21:01:11 192.168.35.52 POST /hacmebank/Login.aspx - 80 -
192.168.35.217

CookieLoginAttempts=5;+ASP.NET_SessionId=4nhskaykui2jor45oqjzpm5
5 302 0 0 539 753

2005-01-24 21:01:11 192.168.35.52 GET /hacmebank/welcome.aspx - 80 -
192.168.35.217

CookieLoginAttempts=4;+ASP.NET_SessionId=4nhskaykui2jor45oqjzpm5
5 200 0 0 6657 529

IPSであれば...

- POSTメソッドにより渡されている文字列を正確に把握可能

Event Details Name	Event Details Value
Date/Time	2005-01-25 06:01:07 JST
Tag Name	HTTP_Post_Field
Alert Name	HTTP_Post_Field
Severity	Low
Observance Type	Intrusion Detection
Combined Event Count	1
Cleared Flag	<input type="checkbox"/>
Target IP Address	192.168.35.52
Target Object Name	80
Target Object Type	Target Port
Target Service	http
Source IP Address	192.168.35.217
SourcePort Name	3363
Sensor IP Address	192.168.35.52
Sensor Name	server_sensor_1

Attribute Name	Attribute Value
algorithm-id	3000006
AttackSuccessful	2
DestinationEthernetAddress	00:50:56:C0:00:08
field	txtUserName
IANAProtocolId	6
server	tokwks031
SystemAgent	TOKWKS031
URL	/hacmebank/Login.aspx
value	+OR+1=1--

RealSecure Guard, BlackICE Agent for Server, RealSecure Desktop Protector, RealSecure Server Sensor, M Series, RealSecure Network Sensor:

This signature detects HTTP POST requests and lists any information disclosed as a result of this command.

This security event is categorized as an audit event. It is not necessarily indicative of an attack or threat to your network.

This signature detects the POST data passed.

Default risk level

Event Number: 4

OK Cancel Information... Copy... Export...

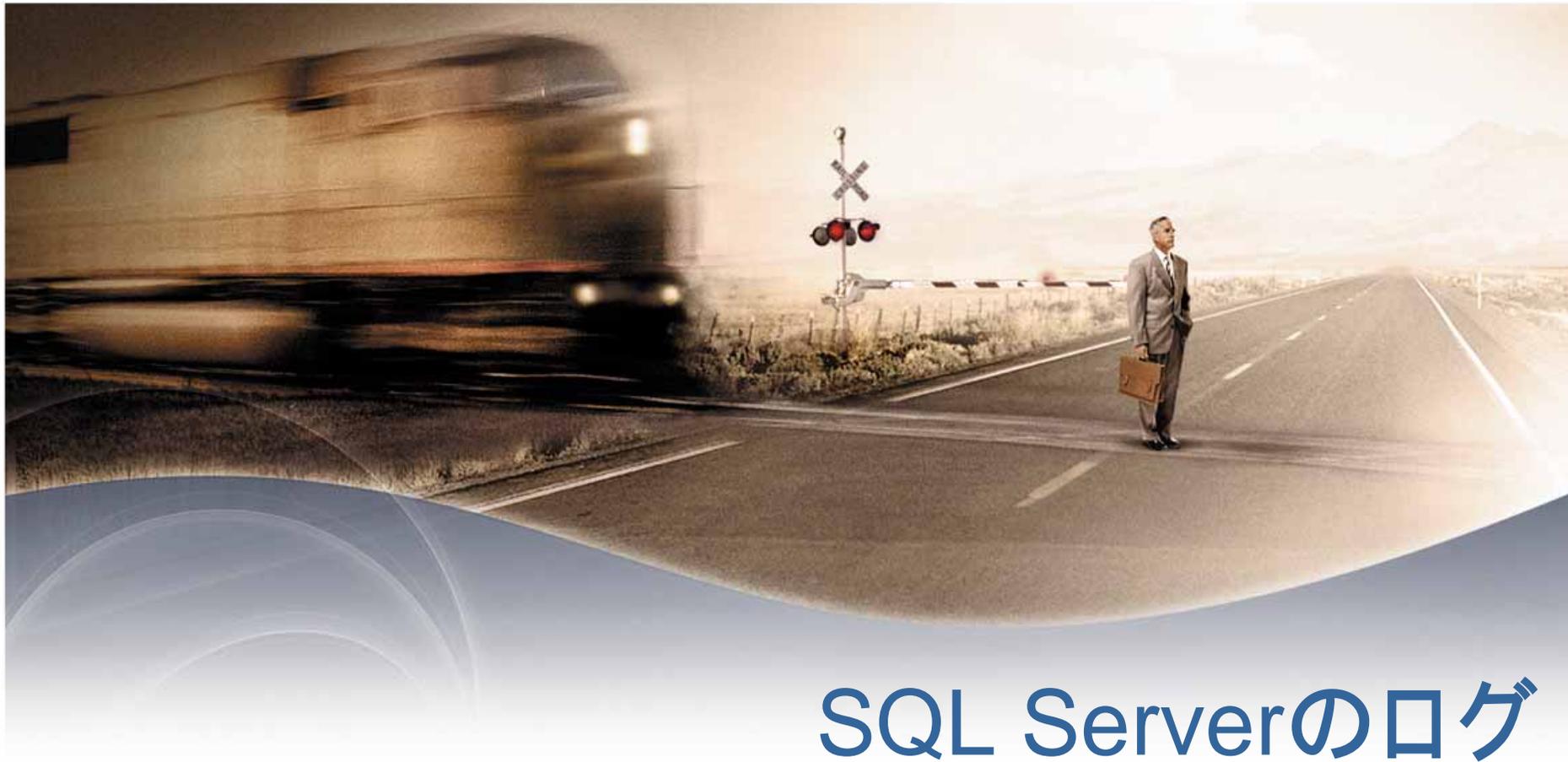
IISログはどこまで有効か

■ 有効な点

- オーバーフローを狙った長大なリクエストの記録
 - WebDAVに対する長大な要求など
 - ただし本当にバッファオーバーフローが発生したかどうかは判断不可能
- ディレクトリ・トラバーサルを悪用した攻撃
 - 主にNimdaやCodeRedなどのワーム

■ 無効な点

- Webアプリケーションの脆弱点に対する攻撃は記録できない
 - クロスサイト・スクリプティング
 - SQLインジェクションなど



SQL Serverのログ

SQL Serverのログ解析

■ ログの種類

■ 監査ログ

- SQL Serverユーザのログオン状況を監査
 - 失敗、成功、すべて

■ SQL Serverエラーログ

- SQL Serverのステータスを保存
 - 例: SQLServer は 192.168.35.217: 1433 で受信を待っています。等

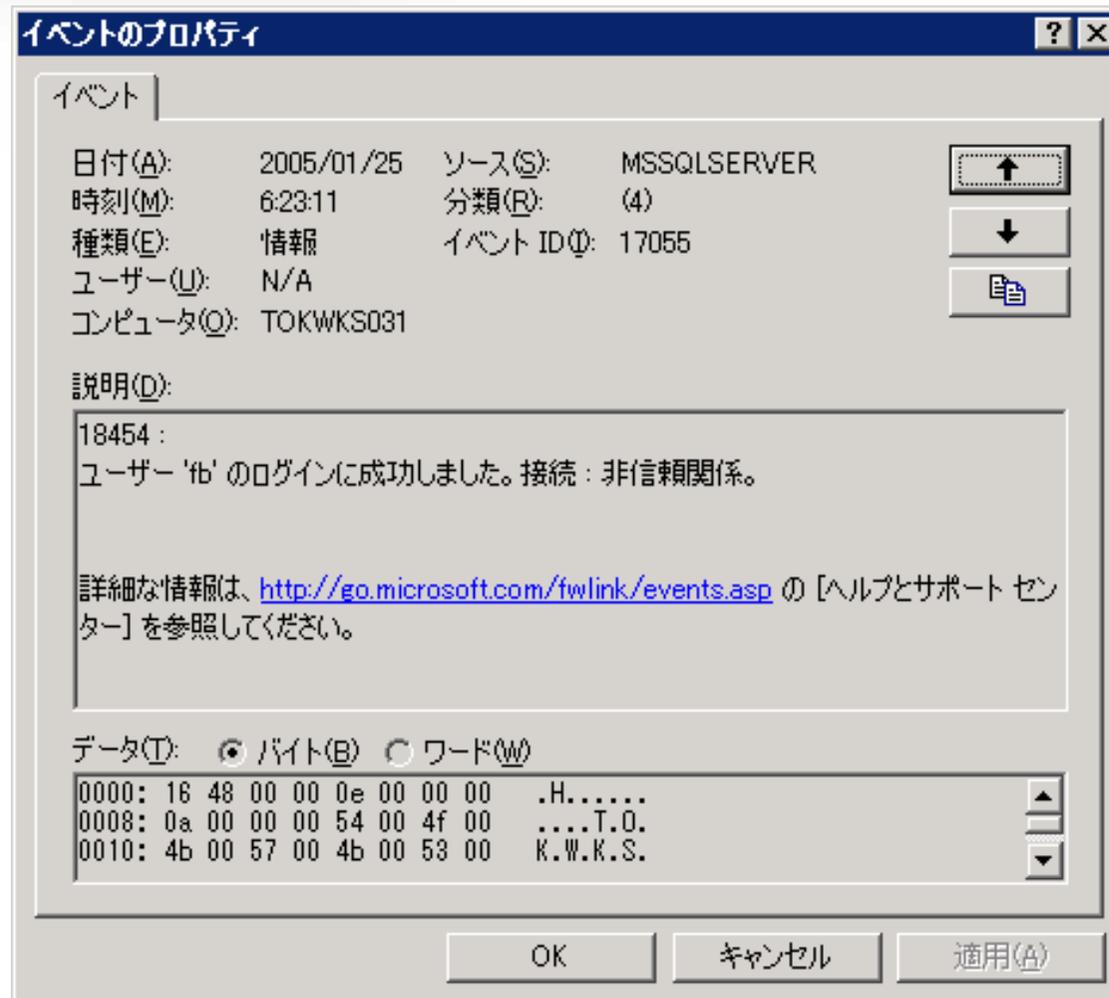
■ SQL Server Agentエラーログ

- SQL Server Agentのエラーおよび警告を記録

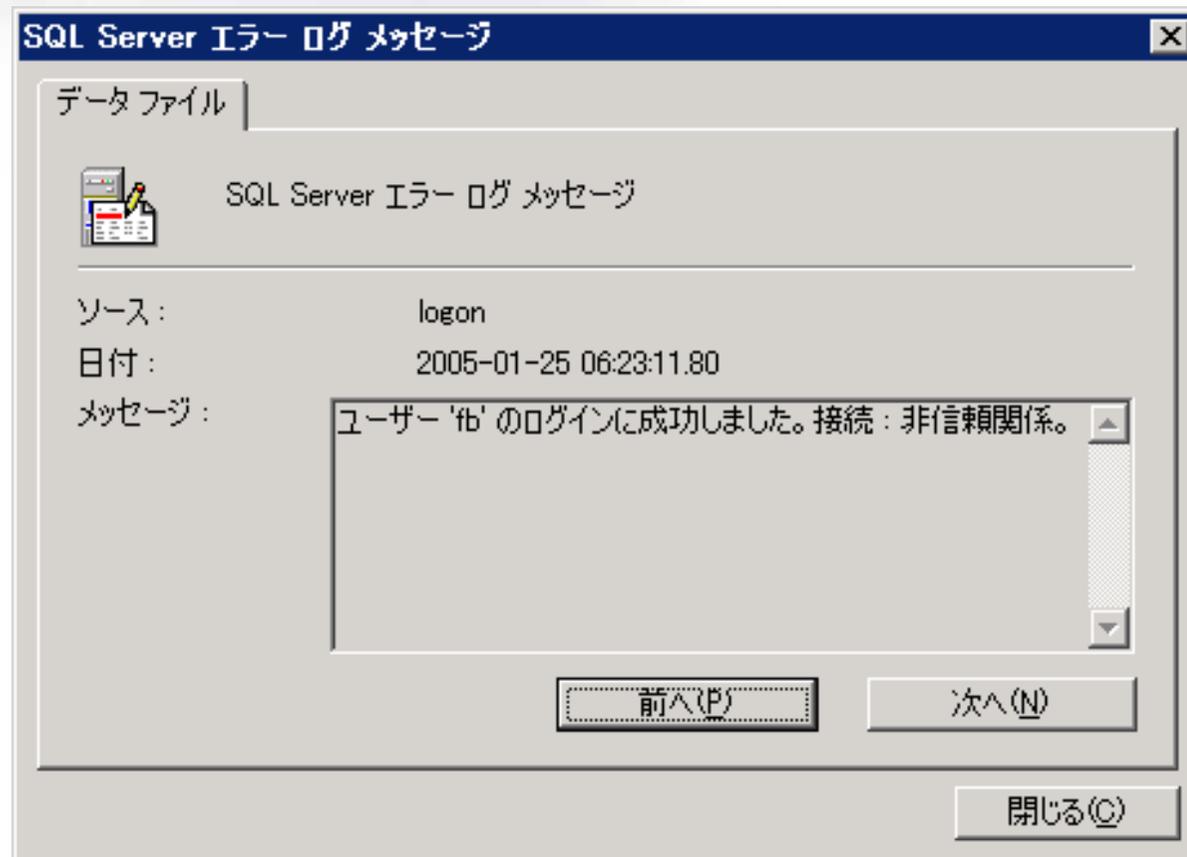
■ トレース

- SQL Serverに対するあらゆる操作を記録可能
- 別途実施する必要あり
 - SQLプロファイラ
 - システムストアプロシージャの呼び出し

SQL Server 監査ログ



SQL Serverエラーログ



SQL Server Agentエラーログ

SQL Server エージェント エラー ログ - TOKLAP031

フィルタ選択パラメータ

種類(T): フィルタ適用(A)

含まれる文字列(C):

C:\Program Files\Microsoft SQL Server\MSSQL\LOG\SQLAGENT.OUT の内容 (11 行)(Q):

種類	日付/時刻	メッセージ
	2005-01-12 17:12:29	[102] SQL Server ODBC ドライバ バージョン 3.81.9042
	2005-01-12 17:12:29	[103] ドライバが使用している Net ライブラリは DBMSSHRN.DLL です。ローカル ホスト サーバ...
	2005-01-12 17:12:29	[310] 1 個のプロセッサと 511 MB の RAM が検出されました
	2005-01-12 17:12:29	[339] ローカル コンピュータは TOKLAP031 で、Windows NT 5.1 (2600) Service Pack 1 を実
	2005-01-12 17:12:29	[364] Messenger サービスが開始されていません - NetSend 通知は送信されません
	2005-01-12 17:12:29	[129] SQLSERVERAGENT を Windows NT サービス コントロールの環境下で開始しています
	2005-01-12 17:12:29	[260] メール セッションを開始できません (理由 : メール プロファイルが定義されていません)
	2005-01-12 17:12:29	[396] CPU のアイドル状態が定義されていません - OnIdle ジョブ スケジュールは機能しません

閉じる(L) ヘルプ

SQLプロファイラ

SQL プロファイラ - [無題 - 1 (TOKLAP031)]

ファイル(F) 編集(E) 表示(V) 再生(R) ツール(T) ウィンドウ(W) ヘルプ(H)

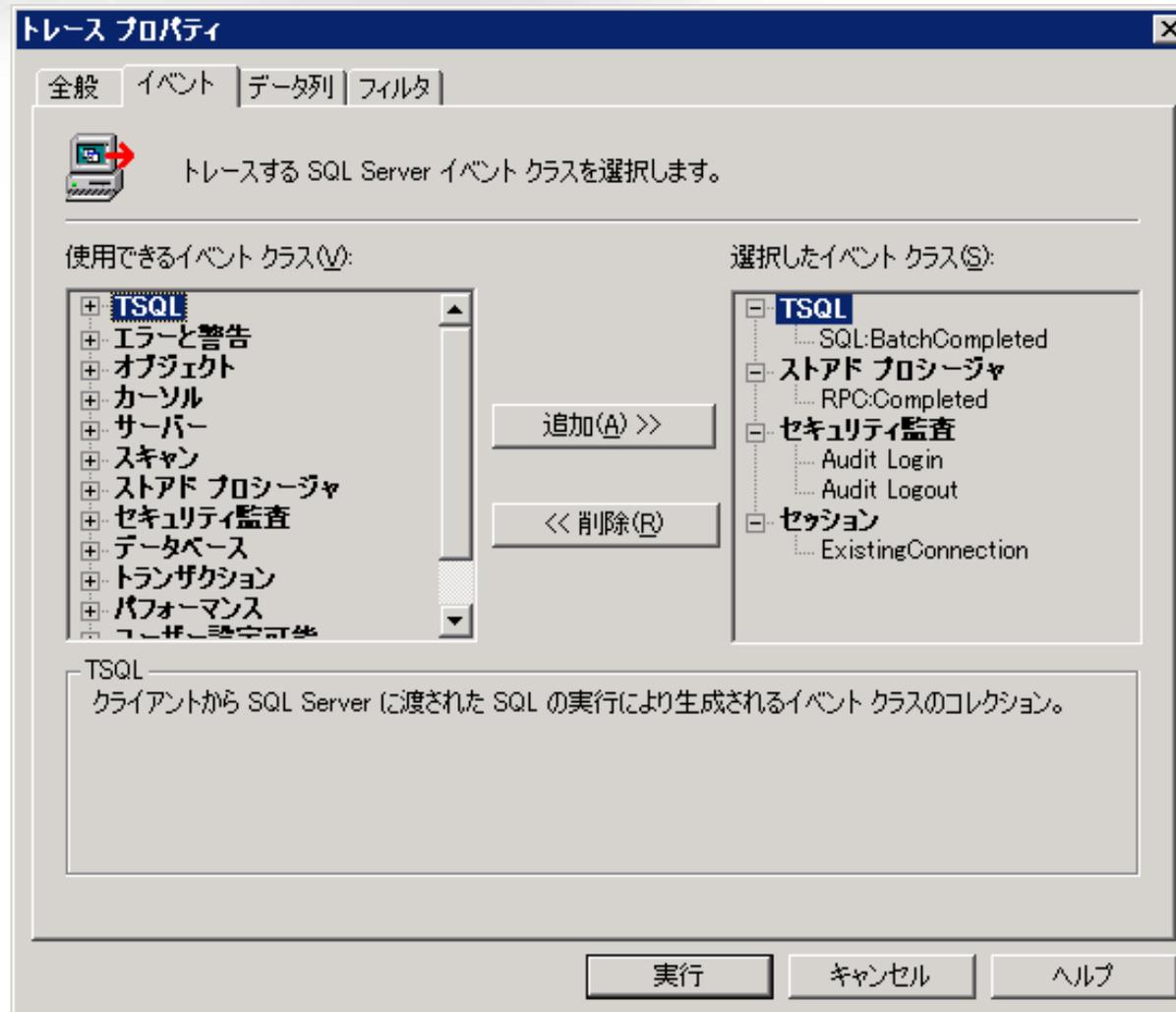
EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID
TraceStart									
ExistingConnection	-- network protocol: LPC set quote...	SQL クエリ アナラ...	hogura	ADMIN#hogura					5352
ExistingConnection	-- network protocol: LPC set quote...	MS SQLEM	hogura	ADMIN#hogura					4548
ExistingConnection	-- network protocol: TCP/IP set qu...	.Net SqlClient D...		BookStore					0
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		BookStore	0	0	0	0	0
RPC:Completed	exec spGetProducts	.Net SqlClient D...		BookStore	0	63	0	0	0
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		BookStore	0	0	0	0	0
RPC:Completed	exec spGetProducts	.Net SqlClient D...		BookStore	0	63	0	0	0
Audit Logout		.Net SqlClient D...		BookStore	0	419	0	403420	0

exec sp_reset_connection

トレースを実行しています

行 5、列 1 行 : 9 接続数 : 1

SQLプロファイラトレース対象



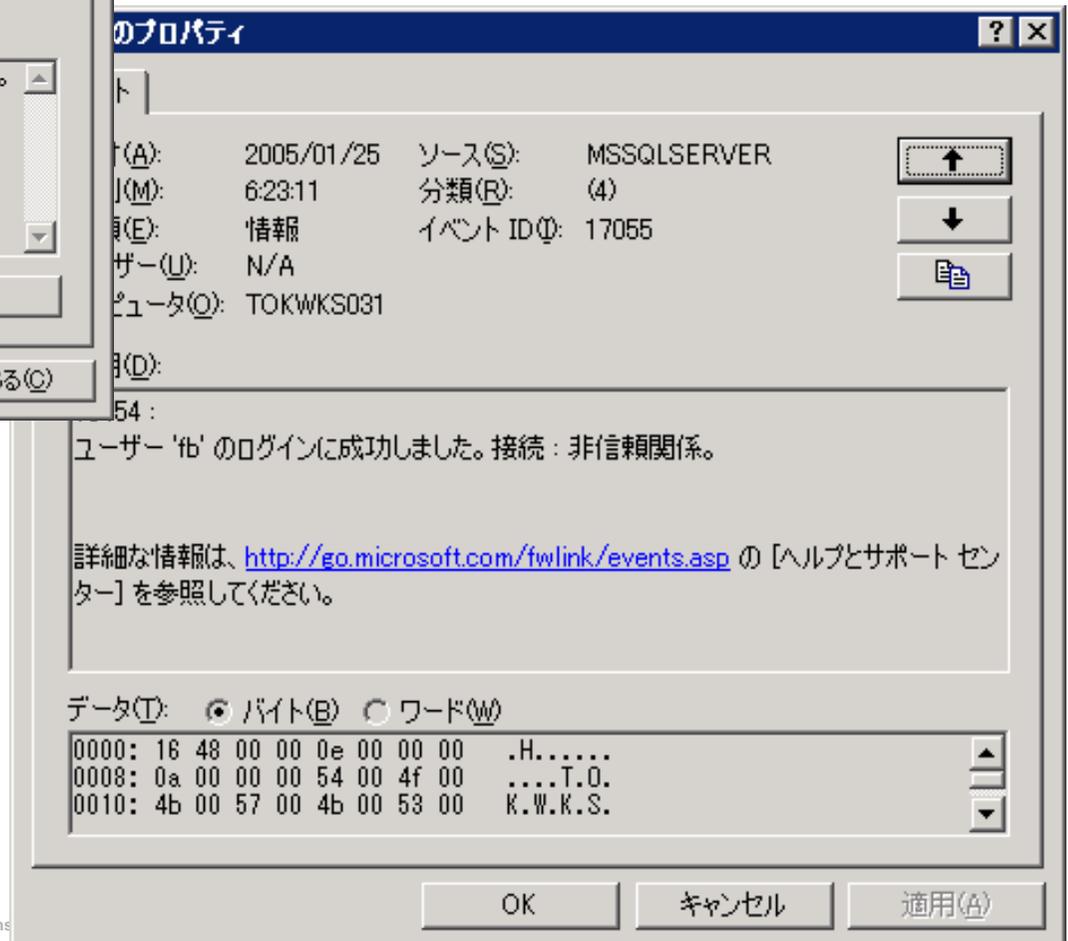
SQLプロファイラの目的

- SQL Serverのインスタンスのパフォーマンスの監視
- Transact-SQLステートメントおよびストアプロシージャのデバッグ
- 実行に時間のかかるクエリの特定
- ステートメントを1ステップずつ実行してコードが期待どおりに機能するかどうかを確認する、プロジェクトの開発段階でのSQLステートメントおよびストアプロシージャのテスト
- 稼動システムのイベントをキャプチャし、テストシステムでこれらのイベントを再生することにより、SQL Serverで行う問題のトラブルシューティング
- SQL Serverのインスタンスで発生した利用状況の監査と検討。セキュリティ管理者は、ログインの成否、ステートメントやオブジェクトへのアクセスで使った権限の成否などを含めて、すべての監査イベントを検討できます。

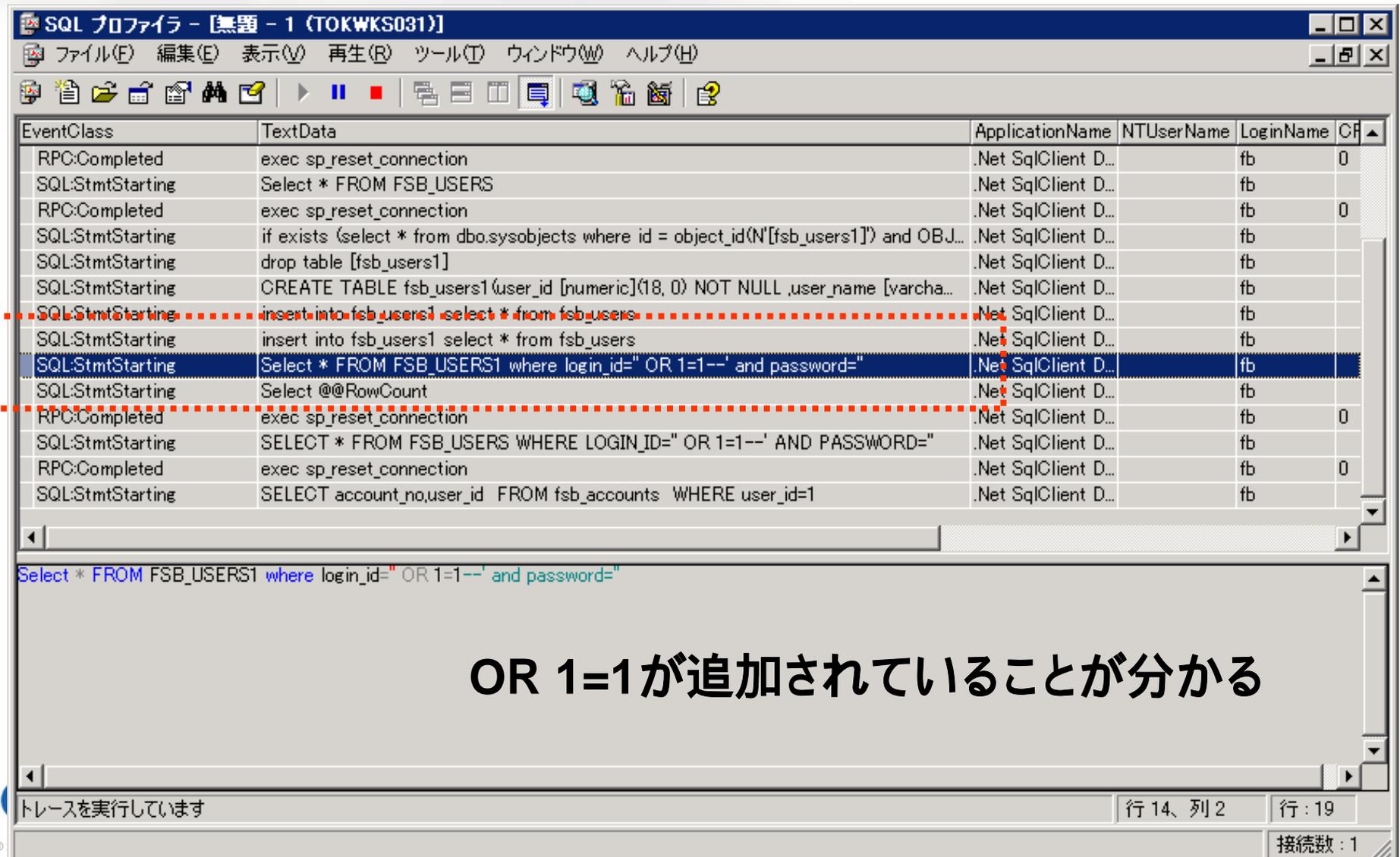
SQLインジェクションの発見

- **SQLインジェクションを実施するのは正規アカウント**
 - WebアプリケーションがSQL Serverに対してSQLインジェクションされたSQL文を発行 正規アカウントが利用される
 - イベントログやSQL Serverエラーログからは発見不可能
- **発行されるSQL文そのものの監査が必要**
 - トレースの実施

ログインしか分からない・・・



SQLプロファイラによるトレース例



EventClass	TextData	ApplicationName	NTUserName	LoginName	CF
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		fb	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		fb	
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		fb	0
SQL:StmtStarting	if exists (select * from dbo.sysobjects where id = object_id(N'[fsb_users1]') and OBJ...	.Net SqlClient D...		fb	
SQL:StmtStarting	drop table [fsb_users1]	.Net SqlClient D...		fb	
SQL:StmtStarting	CREATE TABLE fsb_users1 (user_id [numeric](18, 0) NOT NULL ,user_name [varcha...	.Net SqlClient D...		fb	
SQL:StmtStarting	insert into fsb_users1 select * from fsb_users	.Net SqlClient D...		fb	
SQL:StmtStarting	insert into fsb_users1 select * from fsb_users	.Net SqlClient D...		fb	
SQL:StmtStarting	Select * FROM FSB_USERS1 where login_id=" OR 1=1--" and password="	.Net SqlClient D...		fb	
SQL:StmtStarting	Select @@RowCount	.Net SqlClient D...		fb	
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		fb	0
SQL:StmtStarting	SELECT * FROM FSB_USERS WHERE LOGIN_ID=" OR 1=1--" AND PASSWORD="	.Net SqlClient D...		fb	
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		fb	0
SQL:StmtStarting	SELECT account_no,user_id FROM fsb_accounts WHERE user_id=1	.Net SqlClient D...		fb	

Select * FROM FSB_USERS1 where login_id=" OR 1=1--" and password="

OR 1=1が追加されていることが分かる

トレースを実行しています 行 14、列 2 行 : 19 接続数 : 1

SQLインジェクションで 起こしたエラーから情報を収集

■ **HAVING 1=1--をインジェクション**

■ エラーメッセージ例

- 列 'FSB_USERS.user_id' が集計関数に含まれていない場合および GROUP BY 句がない場合は、選択リスト内では無効です。列 'FSB_USERS.user_name' が集計関数に含まれていない場合および GROUP BY 句がない場合は、選択リスト内では無効です。列 'FSB_USERS.login_id' が集計関数に含まれていない場合および GROUP BY 句がない場合は、選択リスト内では無効です。列 'FSB_USERS.password' が集計関数に含まれていない場合および GROUP BY 句がない場合は、選択リスト内では無効です。列 'FSB_USERS.creation_date' が集計関数に含まれていない場合および GROUP BY 句がない場合は、選択リスト内では無効です。

■ **FSB_USERSテーブルが存在**

■ **user_id, user_name, login_id, password, creation_date列が存在**

エラーによる情報取得の捕捉

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Durati
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	SELECT * FROM FSB_USERS WHERE LOGIN_ID=";	.Net SqlClient D...		sa				
SQL:StmtStarting	EXEC MASTER.XP_CMDSHELL DIR--' AND PASSWORD="	.Net SqlClient D...		sa				
Audit Logout		.Net SqlClient D...		sa	140	39	0	379510
Audit Login	-- network protocol: TCP/IP set quoted_identifier on set i...	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0

exec sp_reset_connection

SQL実行完了だけをトレースした場合捕捉不可能

トレースを実行しています

行 23、列 1 行 : 23

接続数 : 1

エラーによる情報取得の捕捉

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Re
TraceStart						
ExistingConnection	-- network protocol: TCP/IP set quoted_identifier off set implicit_transactions off...	MS SQLEM	hogura	ADMIN#...		
Audit Login	-- network protocol: TCP/IP set quoted_identifier on set implicit_transactions off...	.Net SqlClient D...		sa		
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0
SQL:BatchStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa		
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa		
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0
SQL:BatchStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa		
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa		
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0
SQL:BatchStarting	if exists (select * from dbo.sysobjects where id = object_id(N'[fsb_users1]') and O...	.Ne SqlClient D...		sa		
RPC:Completed	exec sp_reset_connection	.Ne SqlClient D...		sa	0	0
SQL:BatchStarting	SELECT * FROM FSB_USERS WHERE LOGIN_ID=' HAVING 1=1--' AND PASSW...	.Ne SqlClient D...		sa		

SELECT * FROM FSB_USERS WHERE LOGIN_ID=' HAVING 1=1--' AND PASSWORD='

SQL実行開始をトレースすると捕捉可能

トレースを実行しています

行 13、列 1 行 : 13

接続数 : 1

SQLインジェクションによる 任意のコマンド実行

- **master..xp_cmdshell拡張ストアードプロシージャを悪用**
 - ‘; exec master..xp_cmdshell dir--
 - ;を先頭に入れることで、1行に複数のSQL文を入れることが可能
 - xp_cmdshellを通じてdirコマンドを実行
 - 任意のコマンドを実行可能

SQLインジェクションによるdir

DisplayOutput - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

アドレス(D) http://tokwks031/hacmeba... 移動 リンク >>

ドライブ C のボリューム ラベルがありません。ボリューム シリアル番号は A036-8889 です
C:\WINDOWS\system32 のディレクトリ 2005/01/25 00:55

```
. 2005/01/25 00:55
.. 2003/03/26 21:00 20,688 $disp.sys 2003/03/26 21:00 54,700 $ias.sys 2003/03/26 21:00
4,125 $prnescp.sys 2005/01/21 17:55 289 $winnt$.inf 2005/01/22 02:11
1025 2005/01/22 02:11
1028 2005/01/22 02:11
1031 2005/01/22 02:14
1033 2005/01/22 02:11
1037 2005/01/22 02:16
1041 2005/01/22 02:11
1042 2005/01/22 02:11
1054 2003/03/26 21:00 2,151
12520437.cpx 2003/03/26 21:00 2,233
12520850.cpx 2005/01/22 02:11
2052 2005/01/22 02:11
3076 2005/01/22 02:11
3com_dmi 2003/03/26
21:00 64,512
6to4svc.dll 2003/03/26
21:00 1,460
45 2003/03/26
```

ページが表示されました

Local intranet

トレースによるxp_cmdshellの実行記録

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration
TraceStart								
ExistingConnection	-- network protocol: TCP/IP set quoted_identifier off set i...	MS SQLEM	hogura	ADMIN#...				
Audit Login	-- network protocol: TCP/IP set quoted_identifier on set i...	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	Select * FROM FSB_USERS	.Net SqlClient D...		sa				
RPC:Completed	exec sp_reset_connection	.Net SqlClient D...		sa	0	0	0	0
SQL:StmtStarting	SELECT * FROM FSB_USERS WHERE LOGIN_ID='';	.Net SqlClient D...		s				
SQL:StmtStarting	EXEC MASTER.XP_CMDSHELL DIR--' AND PASSWORD=''	.Net SqlClient D...		s				

EXEC MASTER.XP_CMDSHELL DIR--' AND PASSWORD=''

master..xp_cmdshellが起動されている

トレースを実行しています

行 13、列 1 行 : 13

接続数 : 1

SQLインジェクションによる xp_cmdshellプログラムの実行検知

Event Details 3/14

Event Details Name	Event Details Value
Date/Time	2005-01-25 15:35:36 JST
Tag Name	HTTP_POST_XP_Cmdshell
Alert Name	HTTP_POST_XP_Cmdshell
Severity	Medium
Observance Type	Intrusion Detection
Combined Event Count	1
Cleared Flag	<input type="checkbox"/>
Target IP Address	192.168.35.52
Target Object Name	80
Target Object Type	Target Port
Target Service	http
Source IP Address	192.168.35.217
SourcePort Name	3414
Sensor IP Address	192.168.35.52
Sensor Name	server_sensor_1

Attribute Name	Attribute Value
algorithm-id	2004502
AttackSuccessful	2
BLOCK	Default
DestinationEthernetAddress	00:50:56:C0:00:08
IANAProtocolId	6
protocol	http
server	tokwks031
SQL	%27%3B+EXEC+master..xp_cmdshell+dir--
SystemAgent	TOKWKS031
URL	/nacmebank/Login.aspx

HTTP POST command contains SQL command shell request (HTTP_POST_XP_Cmc

About this signature or vulnerability

RealSecure Network Sensor, M Series, BlackICE Server Protection, BlackICE PC Protection, RealSecure Sentry, RealSecure Guard, BlackICE Agent for Server, RealSecure Desktop Protector, RealSecure Server Sensor:

This signature detects attempts to execute the sqlServer xp_cmdshell program through an HTTP POST command.

parametric information:

Event Number: 3

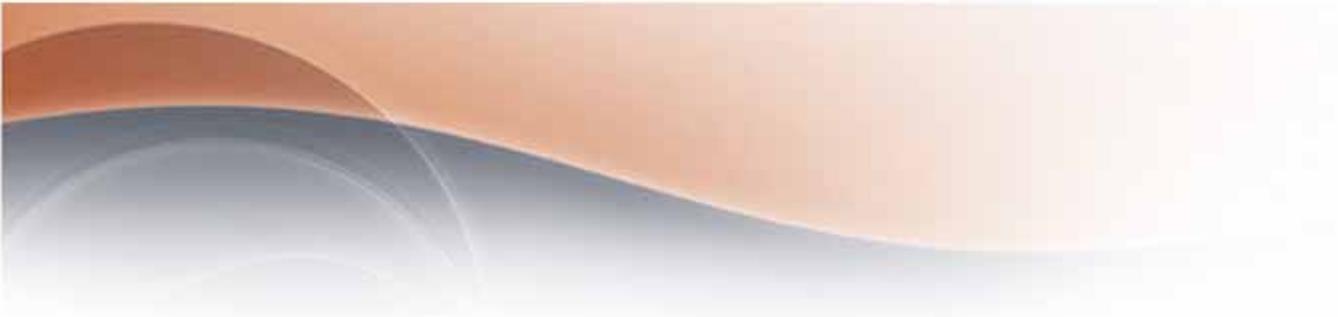
OK Cancel Information... Copy... Export... Help...

トレースの問題

- **SQLプロファイラによるトレース**
 - SQLプロファイラはSQL Serverのクライアントプログラム的一种
 - 常時接続クライアントが追加される
 - SQLプロファイラ自体はSQL Serverとは異なるホストで実行可能
 - SQL Server自体のパフォーマンス問題につながる
 - トレースの設定によっては捕捉できない状況が発生
- **システムストアプロシージャの利用**
 - SQL文を実行する前にシステムストアプロシージャにより部分的にトレースを実施
 - 部分的に実施するためSQLプロファイラを実行しておく場合よりもSQL Serverに対する影響は僅か
 - アプリケーション開発者が意図的にシステムストアプロシージャを利用しなければならない

■ Webハッキングトレーニングアプリケーション

- FoundstoneのHacme Bank™
- <http://www.foundstone.com/resources/proddesc/hacmebank.htm>
- 簡単にSQLインジェクションやクロスサイト・スクリプティングをテスト可能
- 実行後のIISやSQL Serverのログの確認に利用可能
- 環境
 - Microsoft .NET Framework 1.1
 - IIS
 - MSDE 2000もしくはSQL Server 2000
 - Microsoft ASP.NET Web Matrixがあればなお良い



 INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.