Microsoft

インターネット Web サーバー 構築ガイドライン 【ドラフト版】

～ 第 9 章： ログやトレースを活用しよう

※本ガイドラインは各章の先行ドラフト版公開を行い、全章の公開後、正式版文書としてまとめを行い、再度公開します。

第 1 版 2010/05/07

マイクロソフト株式会社

第 9 章 ログやトレースを活用しよう

Web サーバーのログは、問題発生時のトラブルシュートに使用されるにのみならず、処理と作業の恒常性を測ったり、マーケティング的な分析などにも使用されます。また、コンプライアンスの絡んだ調査などでは、証拠として使用される場合もあります。

そのため、いつ・誰が・どのような処理を行ったか、を記録するログの機能は非常に重要です。

実際のところ、サーバーが過去に行った処理内容を調査するには、ログを確認する以外に方法はありません。

IIS 7 にはログや、トレースを取得するためのさまざま機能が搭載されており、用途に合わせてそれらを組み合わせることで、処理の詳細な記録はもちろん、膨大なログの中から必要な情報を、必要な分だけ簡単に取り出すことができます。

IIS が出力する様々な情報

Windows OS は、既定の状態で、システム中に発生する様々な例外(エラー)や警告をイベント ログとして記録する機能を提供しています。また、Windows の **監査** 機能を有効にすると、ファイルやデバイスなどのリソースへのアクセス、および変更作業を監視し、その処理内容はイベント ログとして記録することができます。

Windows の提供する監査機能は、システムとリソースの状態監視という面からは非常に強力ではありますが、サービス (※) 独自の挙動に関してまでは監視を行いません。

(※) この**サービス**は、**UNIX** でいうところの**デーモン**を指してします。

IIS 7 は、Windows OS が提供している監査機能により監視されているとともに、IIS 7 自らのサービスの状態と挙動を監視するための以下の機能を提供しています。

- アクセス ログ
- 失敗した要求のトレース
- ワーカー プロセスの監視

以降では、IIS 7 の提供する各機能について紹介します。

アクセス ログ

IIS 7 では、Web サイトが動作を開始すると同時に、Web サーバーへのリクエストとレスポンスに関するログの記録が開始されます。

ログには、リクエストの日時、クライアントの IP アドレスと使用ポート、User-Agent やリクエストの内容など、一般的に Web サイトの調査に必要となる項目が既定で含まれ、テキスト形式のファ

イルとして、IIS が指定する以下の既定のアクセス ログ ファイル用フォルダーに保存されていきます。

```
C:¥inetpub¥logs¥LogFiles
```

アクセス ログ ファイル用フォルダーの内部はさらに、Web、FTP サイトごとにフォルダーが分割されており、その中に日付別に名前がつけられたアクセス ログ ファイルが保存されます。
アクセス ログ ファイル用フォルダーの命名規則は以下の通りです。

Web サイト :“W3SVC” + サイト ID (数字)
FTP サイト :“FTPSVC” + サイト ID (数字)

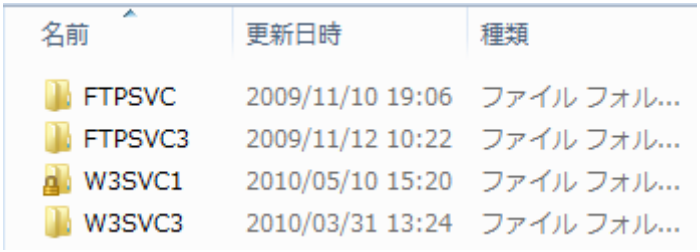


図 : アクセス ログ フォルダーの例

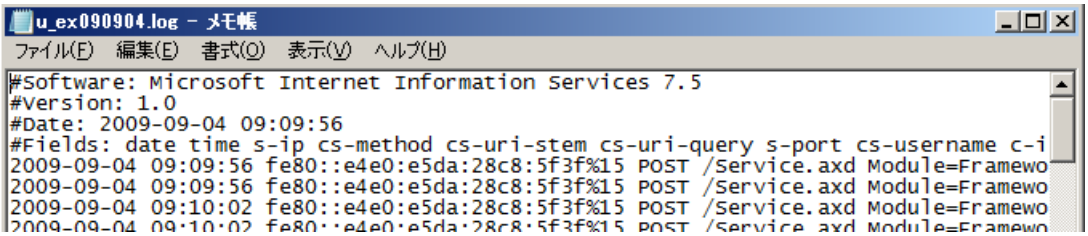
アクセス ログ ファイルの命名規則は以下のとおりです。

“u_ex” + (2 桁表記の UTC 年月日) + “.log”

図 : アクセス ログ ファイルの例

アクセス ログの内容

アクセス ログは HTTP.sys によって出力されます。ファイルの形式は ASCII 形式なので、一般的なテキスト エディターで内容を確認することができます。



図：アクセス ログ ファイルをメモ帳で開いたところ

ログのフィールドはスペース (空白) で区切られており、既定で使用されている時刻形式は UTC (Universal Time Coordinated : 協定世界時) です。

既定で出力されるアクセスログ ファイルのフィールドは以下の通りです。

フィールド	意味
date time	リクエストを受信した日時 (UTC 形式)
s-ip	サーバーの IP アドレス
cs-method	使用された HTTP メソッド
cs-uri-stem	操作のターゲット
cs-uri-query	ターゲットのクエリー情報
s-port	サーバーの ポート
cs-username	ユーザー名
c-ip	クライアントの IP アドレス
cs(User-Agent)	ユーザーエージェント (リクエストに使用されたクライアントの情報)
sc-status	HTTP 状態コード
sc-substatus	HTTP の副状態コード
sc-win32-status	Windows 状態コード
time-taken	リクエストの処理に要した時間

表：既定のアクセスログ ファイルのフィールド

アクセス ログ ファイルは、スペース区切りのテキスト形式のファイルであるため、その分析を行うために Microsoft Excel も使用することができます。また、一般的に知られているクエリー構文でログの内容を分析するための Log Parser というツールも用意されています。

Microsoft TechNet - 『Log Parser 2.2 日本語版』
http://technet.microsoft.com/ja-jp/scriptcenter/dd919274.aspx

アクセス ログ ファイルは、自動的に削除はされませんので、ディスク容量の兼ね合いを見て手動で削除する必要があります。

たとえば、一日のアクセス ログ ファイルのサイズ増分が微々たるものであったとしても、Web サイトが動作しているかぎり、その容量は増加していきます。数年後にディスクの空き容量を使いきってしまい、異常が発生するということも考えられますので注意が必要です。

アクセス ログの種類

IIS 7 は既定で複数のログ ファイルの形式をサポートしており、任意の形式のものを選択して使用することができます。また、カスタムの設定を使用して独自形式のログを取得することも可能です。
IIS 7 で指定可能なアクセス ログの形式は以下のとおりです。

形式	説明
IIS	Microsoft IIS ログ ファイル形式
NSCA	NCSA (National Center for Supercomputing Applications) 共通ログ ファイル形式
W3C	W3C ログ ファイル形式
カスタム	カスタム ログ モジュール用のカスタム形式

表 : アクセスログの形式

各ログ ファイルの形式の詳細につきましては、以下のドキュメント中の解説をご参照ください。

Microsoft TechNet - 『IIS 7.0: サーバー レベルでサーバーごとにログ記録オプションを構成する』
http://technet.microsoft.com/ja-jp/library/cc732910(WS.10).aspx

IIS 7 でアクセス ログの形式を変更するには、以下の手順を実行します。

1. IIS マネージャーを起動し、[接続] ウィンドウのツリービューを展開し、”Default Web Site” か、目的の Web サイトを選択します。
2. [機能] ビューで [ログ記録] アイコンをダブルクリックします。

図 : ログ記録アイコン

3. [ログ記録] の設定画面が表示されるので、[形式] ドロップダウン リスト ボックスから、任意の形式を選択します。

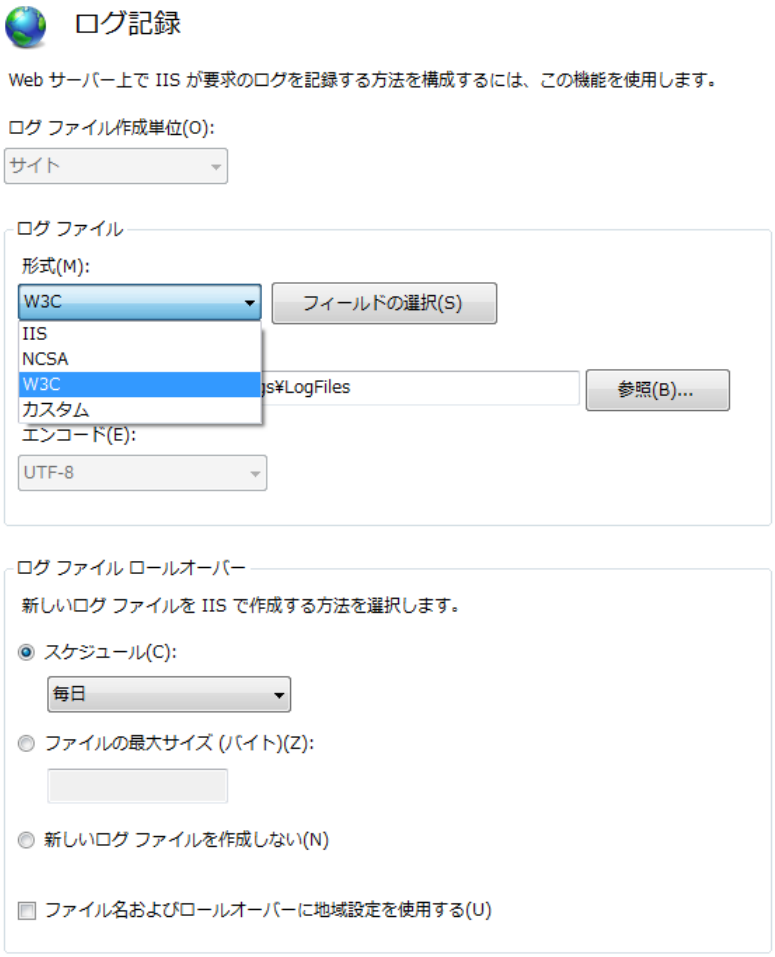


図 ： ログ記録 設定画面

4. 画面右の、[操作] ウィンドウの [適用] リンクをクリックします。

以上で変更内容が適用され、指定した形式でアクセスログが取得されます。

アクセス ログの記録項目を変えるには

アクセス ログ ファイルの形式に “W3C” を指定した場合に限り、ログ ファイルが記録する項目 (フィールド) を変更することができます。

これにより調査に必要な項目を追加したり、逆に不要な項目を記録しないようにしてログ ファイルの容量を抑えたりすることができます。

アクセス ログの記録項目を変えるには以下のようにします。

1. IIS マネージャーを起動し、[接続] ウィンドウのツリー ビューを展開し、”Default Web Site” か、目的の Web サイトを選択します。
2. [機能] ビューで [ログ記録] アイコンをダブル クリックします。

図 ： ログ記録アイコン

3. [ログ記録] の設定画面が表示されるので、[形式] ドロップダウン リスト ボックスから、”W3C” を選択します。(※既定の値です)
4. 同ドロップダウン リスト ボックス右横の [フィールドの選択] ボタンをクリックします。

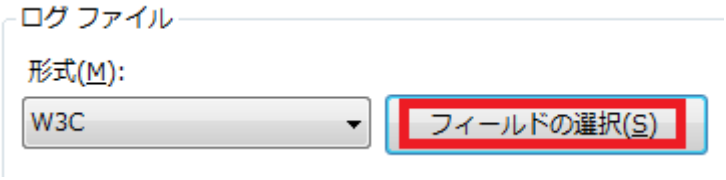


図 ： ログ記録 設定画面の ログ ファイル セクション

5. [W3C ログ記録フィールド] ダイアログ ボックスが表示されるので、ログ ファイルに記録したいフィールドのチェック ボックスにチェックを入れるか、記録したくないフィールドのチェックを外すかして [OK] ボタンをクリック

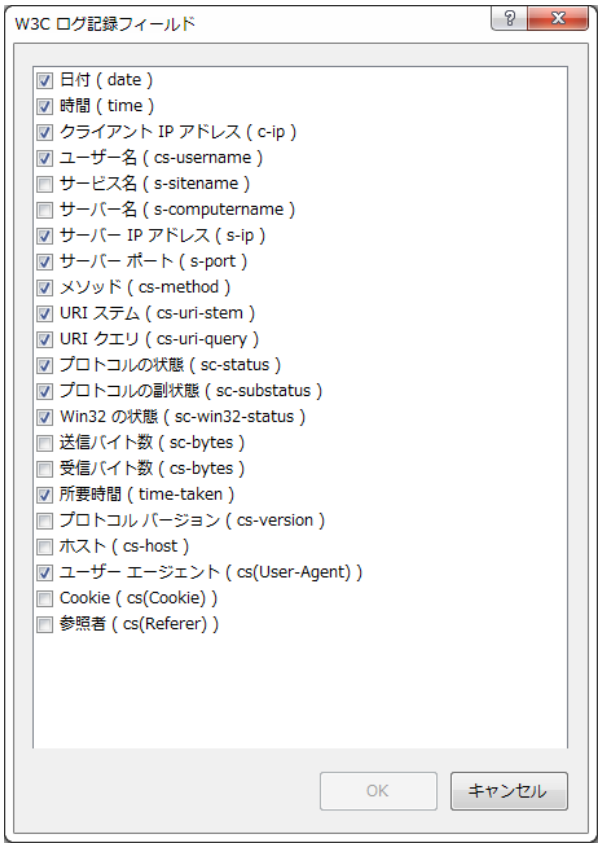


図 ： W3C ログ記録フィールド ダイアログ ボックス

5. 画面右の、[操作] ウィンドウの [適用] リンクをクリックします。

以上で変更内容が適用され、指定した項目の情報がアクセス ログで取得されるようになります。

アクセス ログ ファイルの分け方

IIS 7 のアクセス ログ ファイルは、既定の設定で一日単位 (UTF) でファイルが作成されていますが、そのほかにも時間、週、月単位、サイズ単位で分けて記録するよう指定することができます。

また逆に、まったく分割しないで 1 つのファイルに記録めさせる続けることも可能です。

アクセス ログ ファイルの分割ルールを指定する方法は以下のとおりです。

1. IIS マネージャーを起動し、[接続] ウィンドウのツリー ビューを展開し、”Default Web Site” か、目的の Web サイトを選択します。
2. [機能] ビューで [ログ記録] アイコンをダブル クリックします。

図 : ログ記録アイコン

3. [ログ記録] の設定画面が表示されるので、[ログ ファイル ロールオーバー] セクションの [スケジュール] オプション ボタンにチェックをつけ、同下のドロップダウン リスト ボックスから、1 のログ ファイルに記録する期間を選択します。

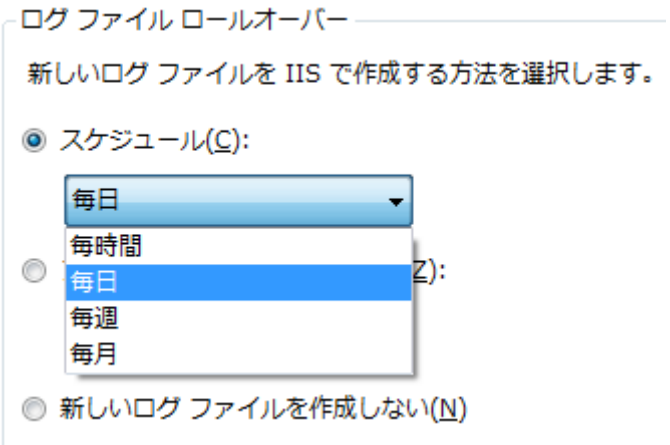


図 : 1 つのログ ファイルに記録する期間の指定

また、期間ではなく、ログ ファイルのサイズで指定を行いたい場合は、[ファイルの最大バイト数] オプション ボタンにチェックをつけ、テキスト ボックスにファイル サイズをバイト単位で指定します。

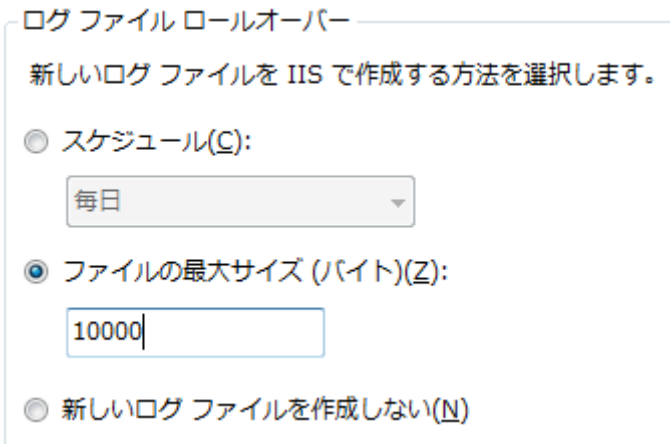


図 ： ログ ファイルをファイル サイズにより分割するように指定

さらに、ログ ファイルを分割せずに 1 つのファイルに記録し続けたい場合は、[新しいログ ファイルを作成しない] オプション ボタンにチェックをつけます。

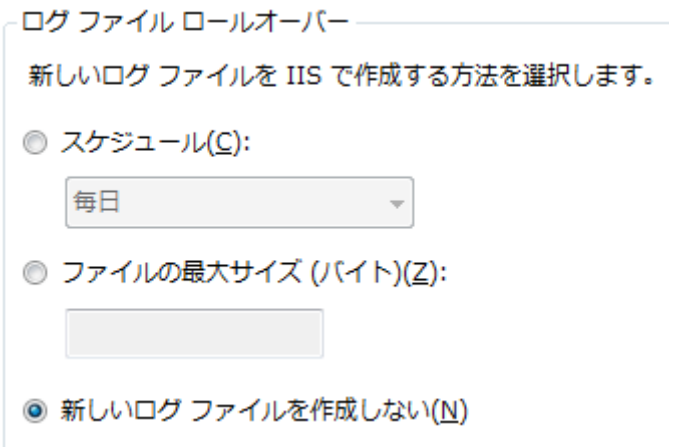


図 ： ログを 1 つのファイルに保存し続けるように指定

6. 画面右の、[操作] ウィンドウの [適用] リンクをクリックします。

以上で変更内容が適用され、指定した期間、あるいはファイル サイズ単位でアクセス ログ ファイルが作成されるようになります。

ログについての詳細な設定方法につきましては、以下のドキュメントをご参照ください。

Microsoft TechNet – 『IIS 7.0 でログ記録を構成する』
http://technet.microsoft.com/ja-jp/library/cc732079(WS.10).aspx

失敗した要求のトレース とは?

IIS 7 には、リクエストに対して行われる Web サーバー上で処理の処理について、ファイルの種類や、処理時間、Web サーバーが返す HTTP のステータスを条件として、トレース ログを取得する機能が提供されています。

たとえば、ASP.NET アプリケーションでエラーが発生する場合、拡張子が "aspx"、HTTP ステータスが "500" という条件でトレースを取得し、そのトレース ログを分析することで、VisualStudio のデバッガが使用できない状況でも、ある程度の原因究明が行えます。

取得されるトレース ログは XML 形式のファイルとして保存されますが、同時にそれらログ ファイルの表示を見やすく成形するための XLS ファイルも同時に生成されます。そのため生成された xml (トレース ログ ファイル) を Web ブラウザーでオープンすると以下のように視覚的に見やすい状態で表示が行われます。

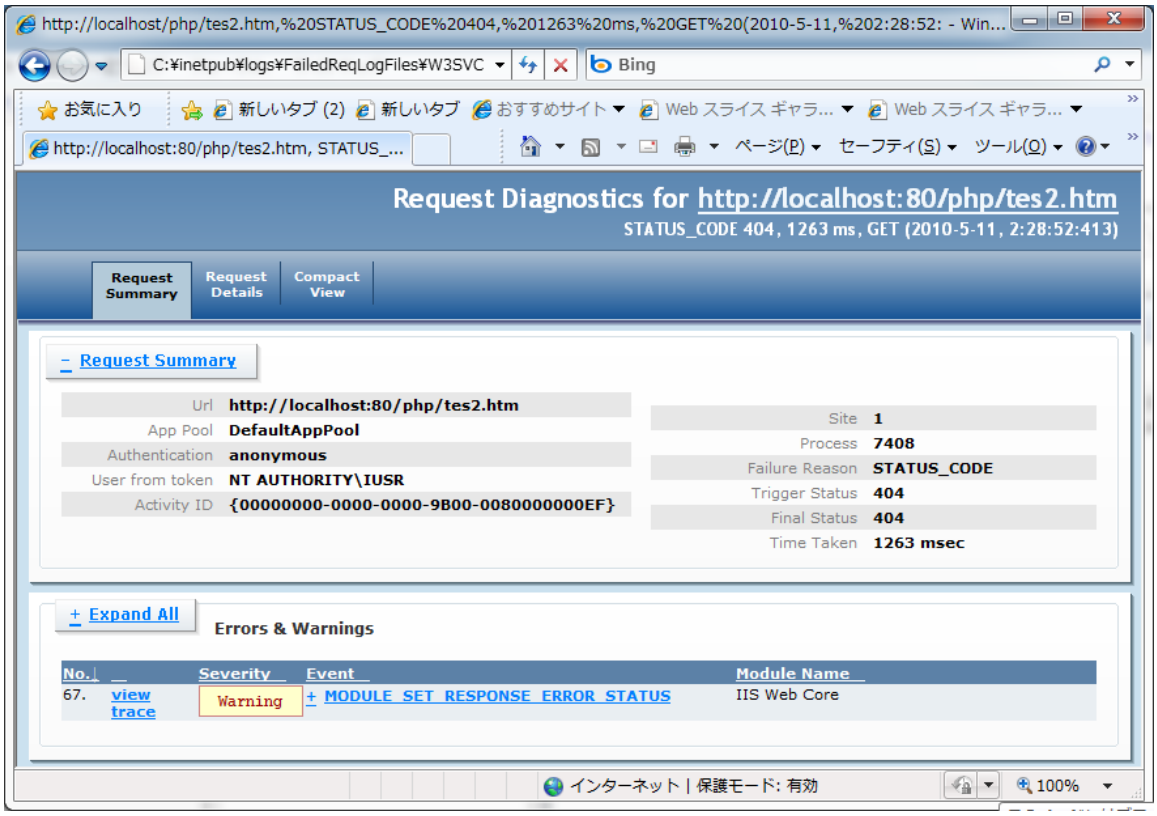


図 : 失敗した要求のトレース のログ ファイルの表示

インストール方法

失敗した要求トレース 機能を使用するには、IIS のセットアップ画面で [トレース] を選択する必要があります。

失敗した要求トレース機能のインストール方法は、Windows Server 2008 R2 と Windows 7 では手順に違いがあります。

以下に Windows Server 2008 R2 と Windows 7 でのインストール手順を示します。

Windows Server 2008 R2 の場合

1. [スタート] をクリックし、[管理ツール] をポイントして、[サーバー マネージャー] をクリックします。

図:サーバー マネージャー

2. [Web サーバー (IIS)] を展開し [役割サービスの追加] をクリックします。

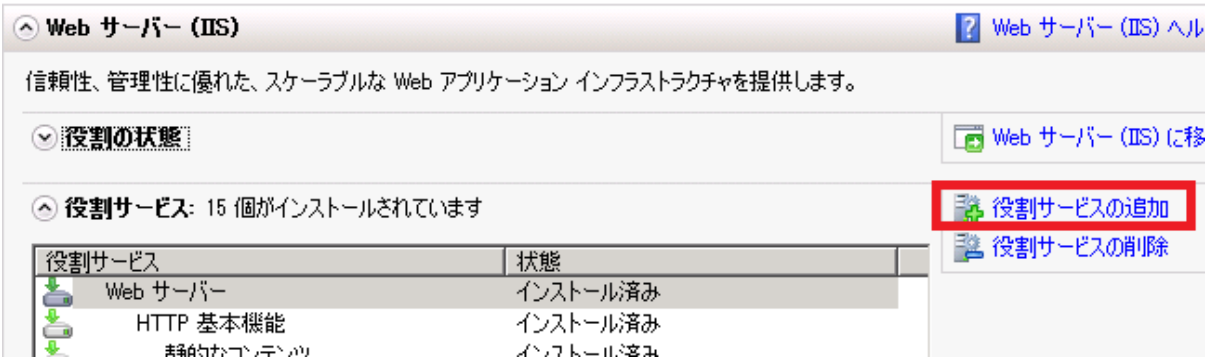


図:役割サービスの追加 メニュー

3. [役割の追加] ウィザードが起動し、[役割サービスの選択]画面が表示されるので、[トレース] を選択し、[次へ] ボタンをクリックします。

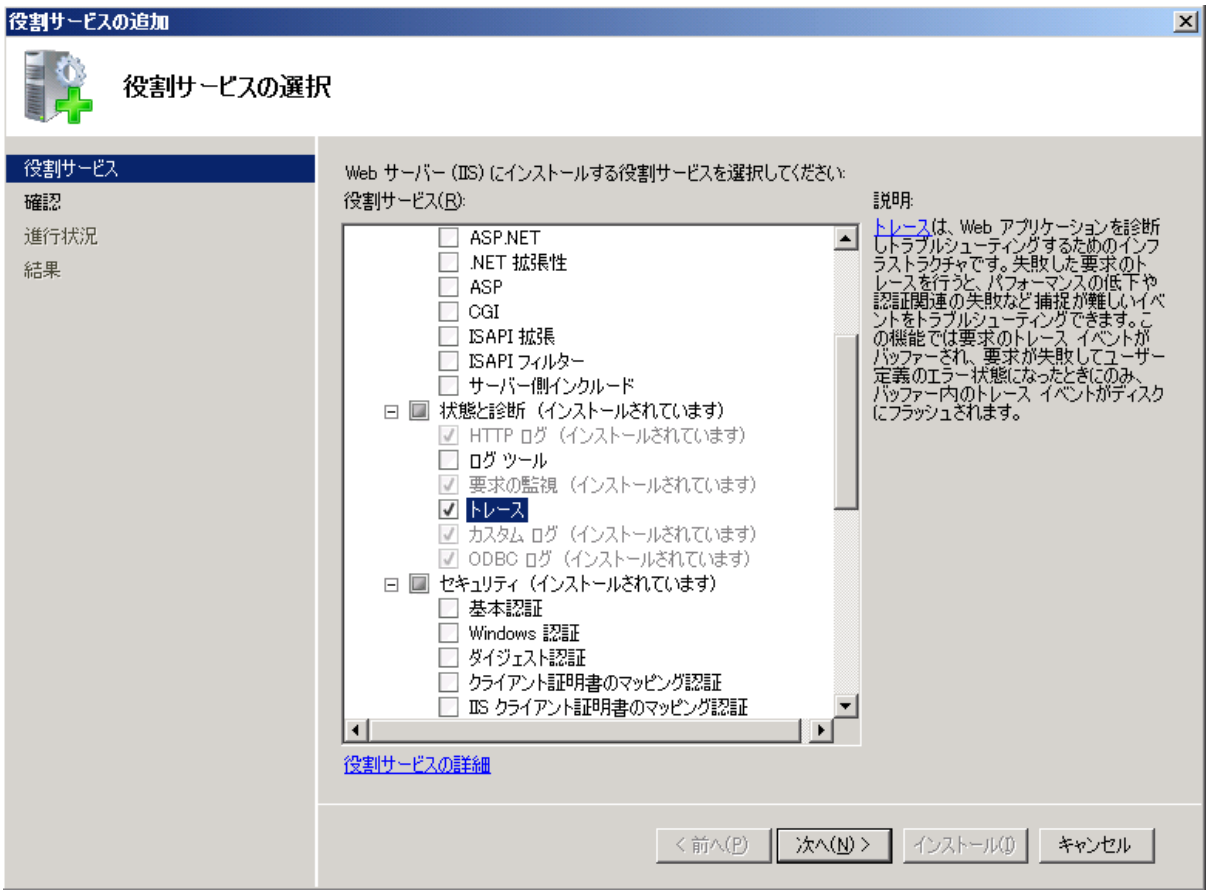


図 : [役割サービスの選択] ダイアログ ボックス

4. [インストール オプションの確認] 画面が標示されるので [インストール] ボタンをクリックしてインストールを実行します。
5. [インストールの結果] ページで、Web サーバー (IIS) の役割と必要な役割サービスのインストールが正常に完了したことを確認してから [閉じる] ボタンをクリックします。

Windows 7 の場合

1. [スタート] ボタンをクリックし、[コントロール パネル] をクリックします。
2. [コントロール パネル] 内の [プログラム] リンクをクリックします。

図:コントロール パネルの [プログラム] リンク

3. [Windows の機能の有効化または無効化] リンクをクリックします。

図: [Windows の機能の有効化または無効化] リンク

4. [Windows の機能] ダイアログ ボックスで、[インターネット インフォメーション サービス] のツリーより [追跡] を選択します。

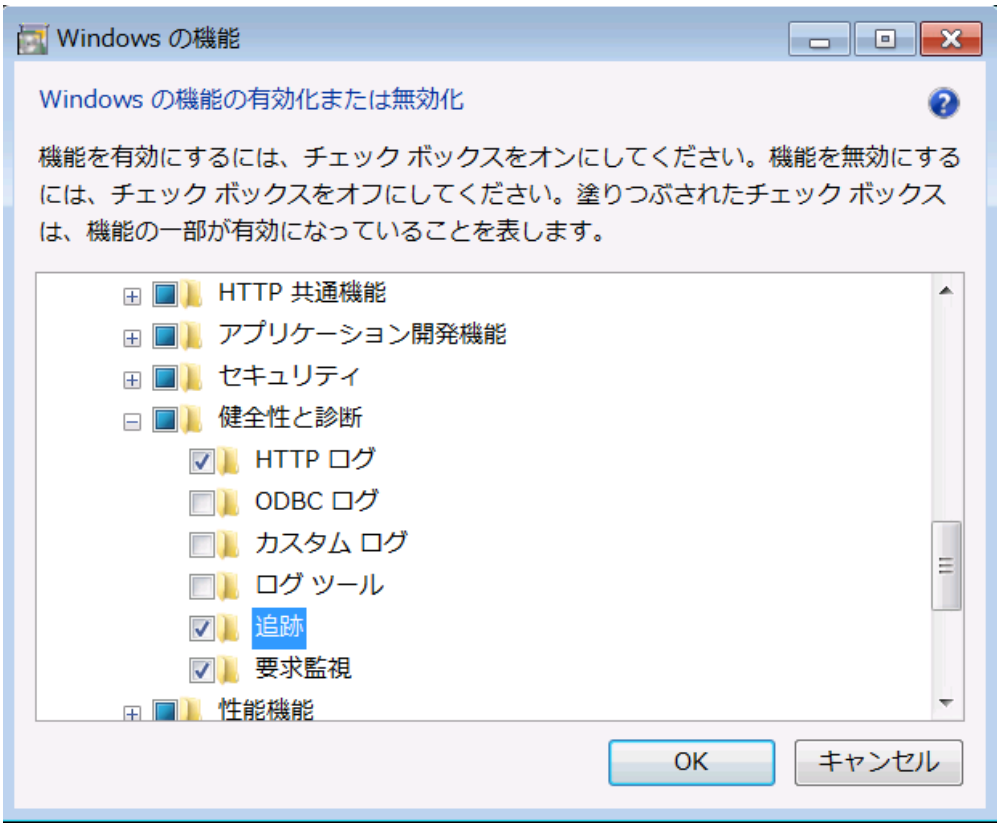


図: [Windows の機能] 選択ダイアログ ボックス

5. [OK] をクリックするとインストールが行われます。

使い方の例

失敗した要求トレース の機能を使用してトレース ログを取得し、取得されたトレース ログの内容を確認するまでの具体的方法をご紹介します。

なお、作業を簡単にするために、トレース ログ取得の条件は、**HTTP 404 File Not Found.** が発生した際とします。

失敗した要求トレースの有効化

失敗した要求のトレースの取得条件は、仮想ディレクトリ単位で設定できますが、トレース機能の有効化/無効化は Web サイト単位で設定する必要があります。

IIS 既定の Web サイトである "Default Web Site" で [失敗した要求トレース] 機能を有効にするには、以下の手順を実行します。

1. IIS マネージャーを起動します。
2. 画面左の [接続] ウィンドウのツリー ビューを展開し、[Default Web Site] を選択します。
3. 画面右の [操作] ウィンドウで [失敗した要求トレース] リンクをクリックします。

図 : [失敗した要求トレース] メニュー

4. [Web サイトの失敗した要求トレースの編集] ダイアログ ボックスが表示されるので [有効にする] チェック ボックスにチェックをつけて [OK] ボタンをクリックします。

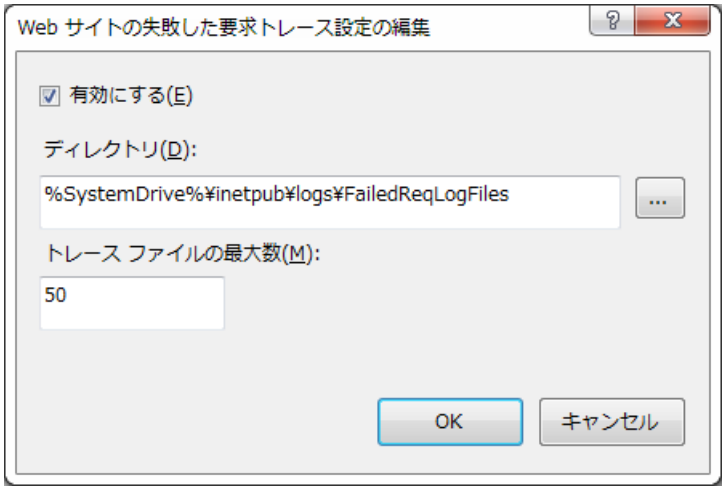


図 ：[Web サイトの失敗した要求トレースの編集] ダイアログ ボックス

以上で、失敗した要求トレースの機能が有効になりました。

次に、[失敗した要求トレースの規則] を設定し、トレース ログを取得する際の条件を設定します。

失敗した要求トレースの規則の設定

トレース ログを取得するリクエストの条件設定を行うと、IIS はその条件に従いトレース ログを取得します。トレース ログを取得するリクエストの条件設定は、IIS マネージャーの [失敗した要求トレースの規則] で行います。

[失敗した要求トレースの規則] は、仮想ディレクトリごとに個別で設定することが可能ですが、ここでは手順を簡単にするために **Default Web Site** での設定とし、トレース ログの取得条件を **HTTP 404 File Not Found.** が発生した際とします。

具体的な設定の手順は以下の通りです。

1. IIS マネージャーを起動します。
2. [接続] ウィンドウのツリーを展開し、[Default web Site] を選択します。
3. 画面中央の [機能 ビュー] から [失敗した要求トレースの規則] アイコンをダブルクリックします。

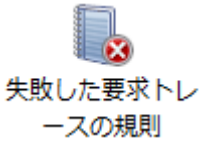


図 ： 失敗した要求トレースの規則 アイコン

4. [失敗した要求トレースの規則] 画面が表示されるので、画面右の [操作] ウィンドウより [追加] リンクをクリックします。

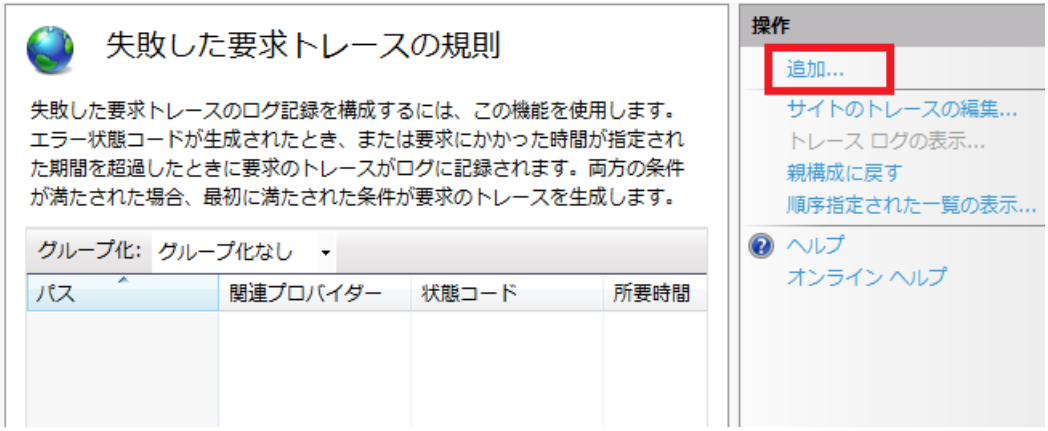


図 ：[失敗した要求トレースの規則] の [追加] メニュー

5. [失敗した要求トレースの規則] ウィザードが起動し、[トレースするコンテンツの指定] 画面が表示されるので、同画面中の [すべてのコンテンツ] オプション ボタンにチェックをつけて [次へ] ボタンをクリックします。

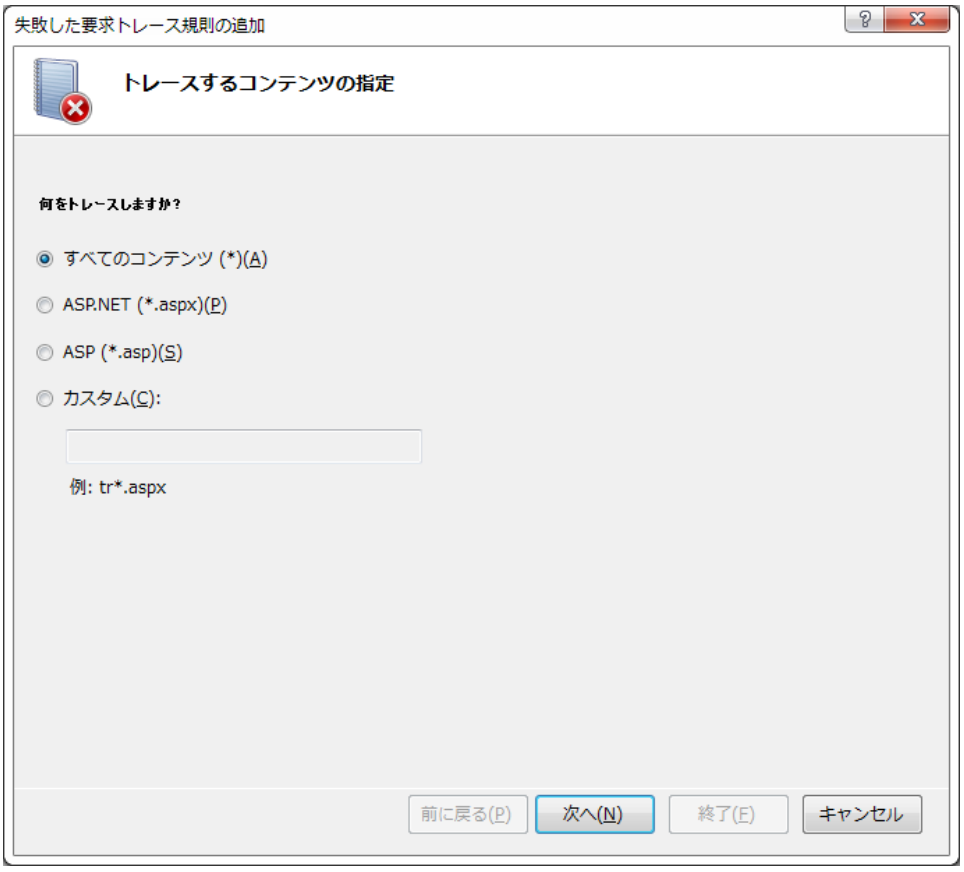


図 ：[トレースするコンテンツの指定] 画面

6. [トレース定義の条件] 画面が表示されるので、[状態コード] チェック ボックスにチェックをつけ、同テキスト ボックスに “404” と入力し、[次へ] ボタンをクリックします。

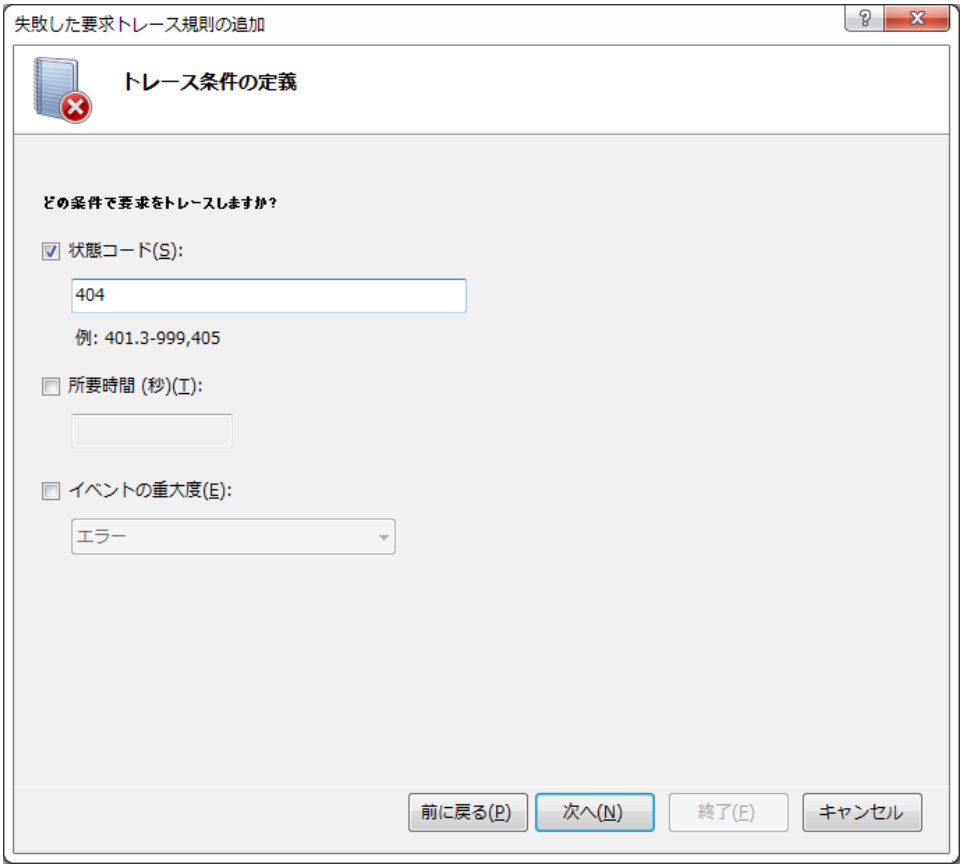


図 ：[トレース定義の条件] 画面

7. [トレース プロバイダーの選択] 画面表示されるので [プロバイダー] チェック ボックスリストで [WWW Server] のみにチェックが着いた状態とし、[詳細] ドロップダウン リスト ボックスで [詳細] を選択して [終了] ボタンをクリックします。

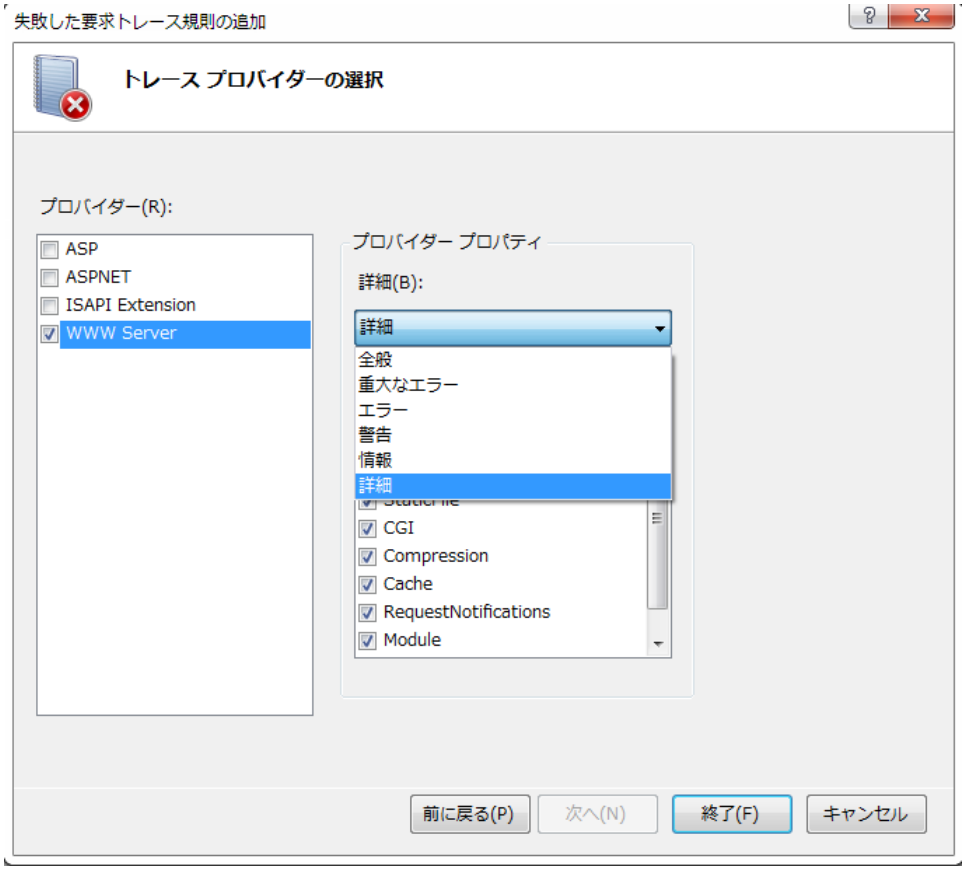


図 : [トレース プロバイダーの選択] 画面

以上で、失敗した要求トレース規則の追加作業は完了です。

Web ブラウザーを起動して、以下の URL のような存在しないファイルを指定してください。

```
http://localhost/hehehe.htm
```

ブラウザーに **HTTP エラー 404.0 - Not Found** が返されると同度にトレース ログが取得されます。

失敗した要求トレース ログの確認

エクスプローラーを起動して、トレース ログが保存されているフォルダーにアクセスします。

失敗した要求トレース ログは、既定では以下のフォルダーに保存されています。

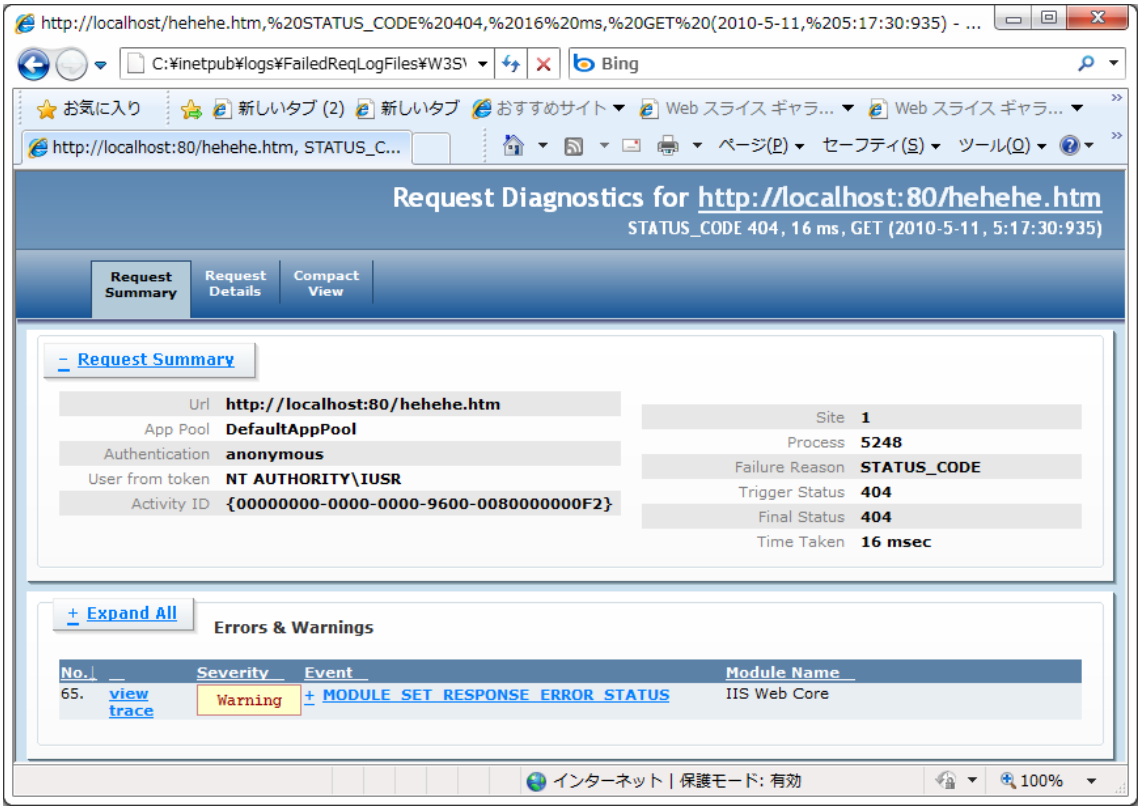
```
C:¥inetpub¥logs¥FailedReqLogFiles¥W3SVC1
```

トレース ログ ファイルは 文字列 “fr” に連番がつき、拡張子を xml としたファイル名で保存されています。

図：失敗した要求トレース ログ ファイルが保存されているフォルダー

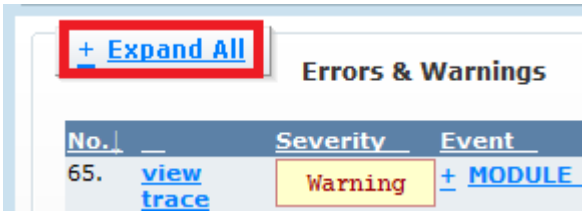
Internet Explorer を起動します。次に、トレース ログ ファイル (*.xml のファイル) を Internet Explorer のウィンドウにドラッグアンドドロップします。

トレース ログ ファイルの内容にスタイルシートが適用された状態で Internet Explorer に表示されます。

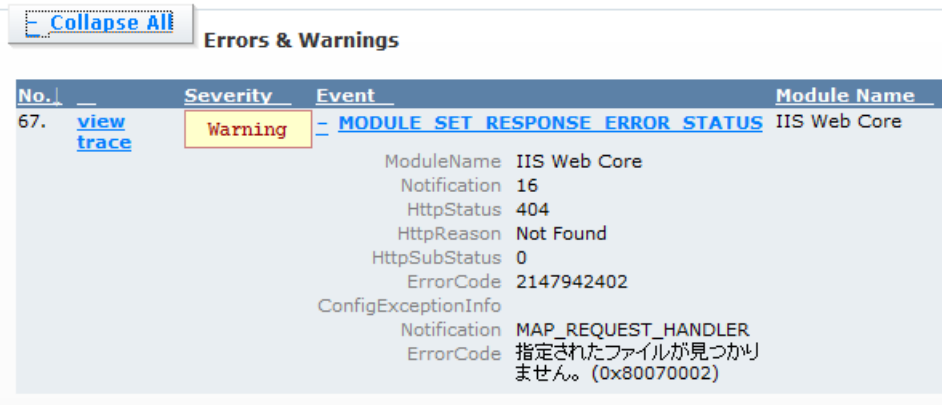


図：失敗した要求のトレース のログ ファイルの表示

トレース ログ ファイルの最初の表示は [Request Summary] タブが選択された状態となっており、トレースを取得したリクエストのあらましが表示されています。さらに、画面中の [+ Expand All] リンクをクリックすると、エラーと警告の詳細が表示されます。

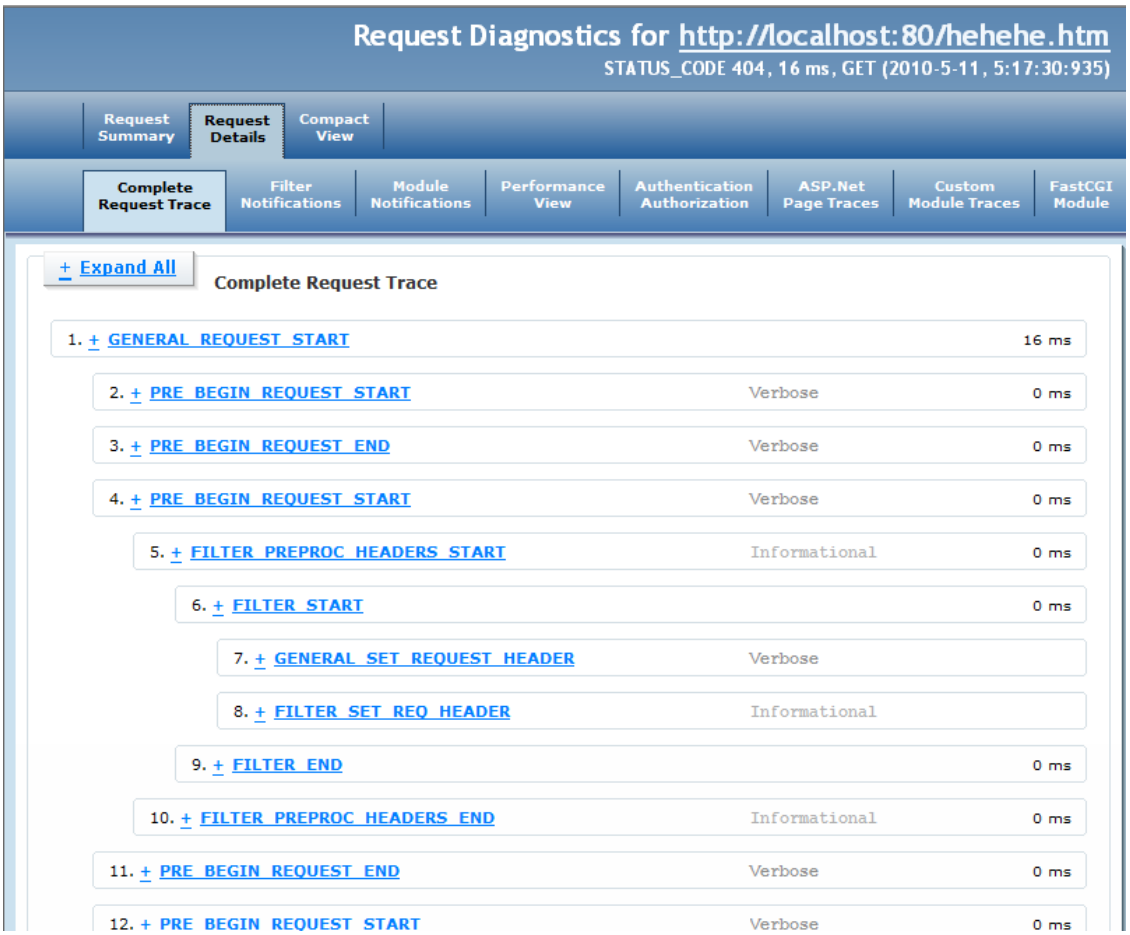


図：エラーと警告の詳細を表示するためのリンク



図：エラーと警告の詳細を表示したところ

[**Request Details**] タブを選択すると、リクエストの詳細なトレースが表示されます。同タブ内はカテゴリーごとにさらに細かいタブに分かれており、それらを選択することで、さらに細かな分析を行うことができます。



図：[**Request Details**] タブの内容

[**Compact View**] タブをクリックすると、リクエストを受信してからレスポンスを返すまでの IIS の処理の内容が表示されます。

Request Summary | Request Details | Compact View

No.		EventName	Details	Time
1.	ⓘ	GENERAL_REQUEST_START	SiteId="1", AppPoolId="DefaultAppPool", ConnId="1610612883", RawConnId="0", RequestURL="http://localhost:80/hehehe.htm", RequestVerb="GET"	05:17:30.935
2.	▯	PRE_BEGIN_REQUEST_START	ModuleName="RequestMonitorModule"	05:17:30.935
3.	▯	PRE_BEGIN_REQUEST_END	ModuleName="RequestMonitorModule", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.935
4.	▯	PRE_BEGIN_REQUEST_START	ModuleName="IsapiFilterModule"	05:17:30.935
5.	ⓘ	FILTER_PREPROC_HEADERS_START		05:17:30.935
6.	ⓘ	FILTER_START	FilterName="C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_filter.dll"	05:17:30.935
7.	▯	GENERAL_SET_REQUEST_HEADER	HeaderName="AspFilterSessionId", HeaderValue="", Replace="true"	05:17:30.935
8.	ⓘ	FILTER_SET_REQ_HEADER	HeaderName="AspFilterSessionId:", HeaderValue=""	05:17:30.935
9.	ⓘ	FILTER_END	NotificationStatus="SF_STATUS_REQ_NEXT_NOTIFICATION"	05:17:30.935
10.	ⓘ	FILTER_PREPROC_HEADERS_END		05:17:30.935
11.	▯	PRE_BEGIN_REQUEST_END	ModuleName="IsapiFilterModule", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.935
12.	▯	PRE_BEGIN_REQUEST_START	ModuleName="WebDAVModule"	05:17:30.935
13.	▯	PRE_BEGIN_REQUEST_END	ModuleName="WebDAVModule", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.935
14.	▯	PRE_BEGIN_REQUEST_START	ModuleName="FailedRequestsTracingModule"	05:17:30.935
15.	▯	PRE_BEGIN_REQUEST_END	ModuleName="FailedRequestsTracingModule", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.935
16.	ⓘ	GENERAL_ENDPOINT_INFORMATION	RemoteAddress="::1", RemotePort="37923", LocalAddress="::1", LocalPort="80"	05:17:30.935
17.	ⓘ	GENERAL_REQUEST_HEADERS	Headers="Connection: Keep-Alive Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash, */*	05:17:30.935

図 : [Compact View] タブの内容

たとえば、今回のトレースの No.65 では、× 印とともに Warning の発生場所であることを示しています。

62.	▯	NOTIFY_MODULE_END	ModuleName="HttpRedirectionModule", Notification="MAP_REQUEST_HANDLER", fIsPostNotificationEvent="false", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.951
63.	▯	NOTIFY_MODULE_START	ModuleName="WebDAVModule", Notification="MAP_REQUEST_HANDLER", fIsPostNotification="false"	05:17:30.951
64.	▯	NOTIFY_MODULE_END	ModuleName="WebDAVModule", Notification="MAP_REQUEST_HANDLER", fIsPostNotificationEvent="false", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.951
65.	✕	MODULE_SET_RESPONSE_ERROR_STATUS **Warning**	ModuleName="IIS Web Core", Notification="MAP_REQUEST_HANDLER", HttpStatus="404", HttpReason="Not Found", HttpSubStatus="0", ErrorCode="指定されたファイルが見つかりません。 (0x80070002)", ConfigExceptionInfo=""	05:17:30.951
66.	▯	NOTIFY_MODULE_START	ModuleName="CustomLoggingModule", Notification="LOG_REQUEST", fIsPostNotification="false"	05:17:30.951
67.	▯	NOTIFY_MODULE_END	ModuleName="CustomLoggingModule", Notification="LOG_REQUEST", fIsPostNotificationEvent="false", NotificationStatus="NOTIFICATION_CONTINUE"	05:17:30.951
68.	▯	NOTIFY_MODULE_START	ModuleName="WebDAVModule", Notification="SEND_RESPONSE", fIsPostNotification="false"	05:17:30.951

図 : Warning の発生個所を示すトレース ログ

以上のように、失敗した要求のトレース ログの機能を使用することで、エラーを再現しなくても処理の詳細な流れを確認し、エラーの原因を調査できるようになっています。

ワーカー プロセスの監視

IIS への各リクエストは、ワーカー プロセスと呼ばれるサーバー プロセス上のスレッドとして処理が行われます。IIS では任意の数のワーカー プロセスをホストすることが可能であり、Web サイト、

アプリケーションは、各々独自のワーカー プロセスを使用することも、また、ひとつのワーカー プロセスを共有して使用することも可能です。それらを構成には、アプリケーション プールの設定を行います。ワーカー プロセスとは、アプリケーション プールが実行された際のプロセスに他なりません。

IIS 7 では、IIS が使用している稼働中のワーカー プロセスはもちろん、各ワーカー プロセスが実行中の要求に関する情報も表示できます。この情報によって、アプリケーションのハング、メモリ リークなど、サーバー上の問題の発生場所を特定できます。

現在稼働しているワーカー プロセスの一覧を表示するには?

IIS 7 ではアプリケーション プールで実行されているワーカー プロセスについて、パフォーマンス情報を表示することができます。この情報をもとに、Web サーバーで問題を引き起こすアプリケーションを確認したり問題の修正方法を検討したりすることができます。たとえば、特定のアプリケーション プールの CPU 使用率だけが頻繁に高くなる場合、この情報をもとに、そのアプリケーション プールで実行されているアプリケーションを確認し、問題が特定のアプリケーションのみで発生しているのか、またアプリケーションを別のアプリケーション プールに移動することによって解決できるか等、さまざまな診断を行うことができます。

IIS 7 は、ワーカー プロセスとそれに関連付けられているアプリケーション プール名を一覧表示します。それぞれのワーカー プロセスについて次の情報を提供します。

項目	表示内容
アプリケーション プール名	アプリケーション プールにつけられた名前 Web ガーデンが構成されている場合、そのアプリケーション プール内で複数のワーカー プロセスが実行さるため、同じアプリケーション プール名が 複数回、リストに表示される場合がある
プロセス ID	アプリケーション プールと関連付けられているワーカー プロセス識別子 (ID)
状況	起動中、実行中、または停止中などのプロセスの状態
CPU %	最後に更新されてからワーカー プロセスが使用した CPU 時間の割合 タスク マネージャーの [CPU 使用率] に相当
プライベートバイト (KB)	ワーカー プロセスが占有しているメモリの現在のサイズ タスク マネージャーの [仮想メモリ サイズ] に相当
仮想バイト (KB)	ワーカー プロセス用の仮想アドレス空間の現在のサイズ

表 : アプリケーション プールの一覧に表示される項目

ワーカー プロセスの一覧を表示するには IIS マネージャー、もしくはコマンド ラインで Appcmd コマンドを使用します。

IIS マネージャーを使用したワーカー プロセスの一覧表示

1. IIS マネージャーを起動します。
2. 画面左の [接続ウィンドウ] のツリー ビューで、コンピューター名をクリックします。
3. [機能 ビュー] で [ワーカー プロセス] アイコンをダブルクリックします。

図 : ワーカー プロセス アイコン

4. 現在実行中のワーカー プロセスの一覧が表示されるので、リスト内の任意のワーカー プロセスを選択し、画面右の [操作] ウィンドウで [現在の要求の表示] リンクをクリックします。

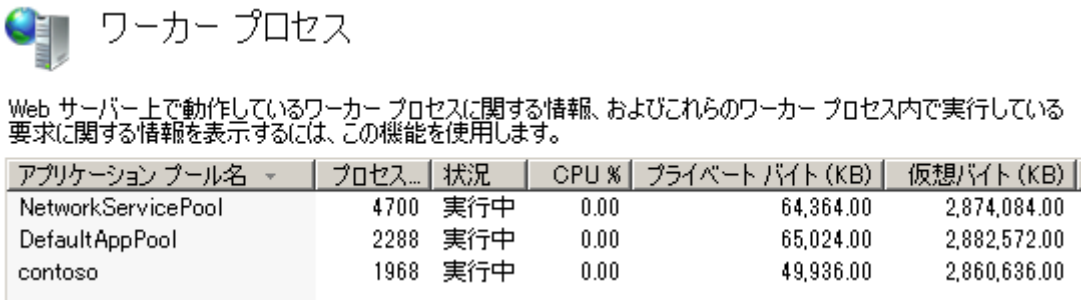


図 : 実行中のワーカー プロセスの一覧の例

ワーカー プロセスの一覧表が表示され、現在どのようなワーカー プロセスが動作し、また各々どれくらい CPU やメモリといった Web サーバーのリソースを使用しているか確認することができます。

Appcmd コマンドを使用したワーカー プロセスの一覧表示

1. コマンド プロンプトを [管理者として実行] します。
2. コマンド プロンプトに以下のコマンド ラインを入力します。

```
C:¥Windows¥system32¥inetsrv>appcmd list wps
```

以下のように、現在稼働中のアプリケーション プールの一覧が表示されます。

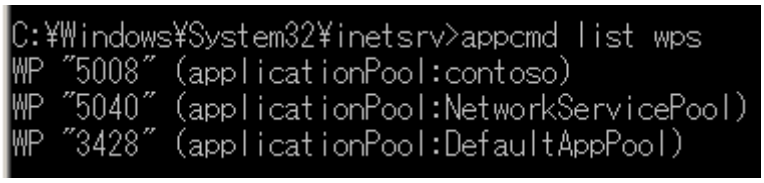


図 : コマンド プロンプトでのアプリケーション プール一覧の表示

ワーカー プロセスで現在実行中の要求を表示するには?

ワーカー プロセスで Web サーバーの大量のリソースが使用されている場合、または要求の処理に長い時間がかかっている場合は、ワーカー プロセスで処理されている要求の一覧を表示することができます。この情報は、サイトまたはアプリケーションのどの部分で問題が発生しているかを判断する際に役立ちます。たとえば、特定のファイルを要求するとメモリ使用量が大幅に増える場合は、コードを最適化できる開発者にサイトまたはアプリケーションに関する情報を提供できます。また、ワーカー プロセスで要求の処理に長い時間がかかる場合もあります。そのような場合は、ワーカー プロセスで現在処理されている要求を表示し、その情報を使用して、特定の要求の処理に時間がかかっている原因を調べることができます。

IIS マネージャーでは、ワーカー プロセスで現在実行中の要求に関する次の情報が返されます。

項目	表示内容
サイト ID	特定の要求のサイト識別子 (ID)
URL	要求された URL
動詞	要求で使用された HTTP 動詞 (メソッド)
クライアント IP	求を発行したクライアントの IP アドレス
状況	要求が存在する現在のパイプライン モジュールの状態
モジュール名	要求が存在する現在のモジュール
経過時間	要求の処理で経過した時間

表 : ワーカー プロセスの処理一覧に表示される項目

ワーカー プロセス内の処理の一覧を表示するには IIS マネージャー、もしくはコマンド ラインで **Appcmd** コマンドを使用します。

IIS マネージャーを使用したワーカー プロセス内の処理の一覧表示

1. IIS マネージャーを起動します。
2. 画面左の [接続ウィンドウ] のツリービューで、コンピューター名をクリックします。
3. [機能 ビュー] で [ワーカー プロセス] アイコンをダブルクリックします。
4. 現在実行中のワーカー プロセスの一覧が表示されるので、リスト内の任意のワーカー プロセスを選択し、画面右の [操作] ウィンドウで [現在の要求の表示] リンクをクリックします。

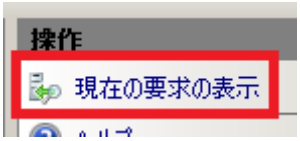


図 : [現在の要求の表示] リンク

5. 選択したワーカー プロセスで処理されているリクエストの内容が表示されます。

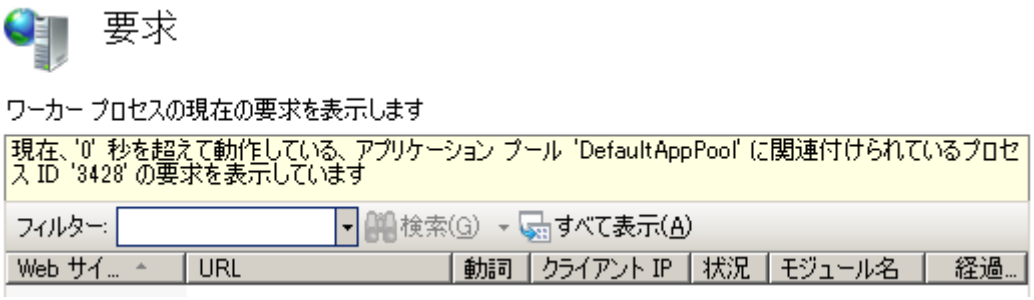


図 : ワーカー プロセスが処理を行っている要求 (リクエスト) の一覧画面

ワーカー プロセスが処理を行っている要求の一覧の項目、[経過] には、リクエストを受けてから現在までの時間が表示されるので、ハングアップや、ボトルネックとなっている処理の判断に使用することができます。

※ただし、このリストに表示される時点で、ある意味非常に時間がかかっているといえます。正常に処理が行われている一般的な要求は、非常に短い時間で処理が行われるため通常同リストには表示されません。

項目 [Web サイト] や、[URL]、[動詞] の内容は、問題の再現試験に使用することができます。

項目 [モジュール] の内容は、問題が特定のモジュールにあった場合など、切り分けに使用することができます。

これら項目を使用することで、Web サイトのパフォーマンス チューニングや、トラブルシュートを行うことができます。

Appcmd コマンドを使用したワーカー プロセス内の処理の一覧表示

1. コマンド プロンプトを [管理者として実行] します。
2. コマンド プロンプトに以下のコマン ドラインを入力します。

```
C:¥Windows¥system32¥inetsrv>appcmd list requests
```

現在処理中の要求がある場合は、各要求の処理状況がリスト表示されます。

イベント ログ

イベント ログ サービスは、OS が検知して処理を行ったエラーの情報を、イベント ログとして記録します。イベント ログが記録される状況は、大きく 2 つに分けることができます。

ひとつは、プログラム (アプリケーション、サービス) が明示的にイベント ログへ情報の出力処理を行っている場合。ふたつめは、プログラムが、その内部で発生したエラーを処理できなかった場合です。たとえば、プログラム自身がそのエラーにより異常終了してしまった場合などがこれにあたり

ます。そのため、イベント ログに記録されるエラーは、比較的重大なものが記録されることが多い傾向にあります。

　また、イベント ログは、そのエラーの最終的なログである場合が多く、トラブルシュートにおいても重要です。

イベント ログを確認するには

イベント ログは、Windows の [管理ツール] 内にある [イベントビューアー] で、その内容確認することができます。具体的な手順は以下のとおりです。

1. Windows の [スタート] ボタンをクリックし、[コントロール パネル] を選択します。
2. コントロール パネルのウィンドウが表示されるので、ウィンドウ右上にある [表示方法] ドロップダウン リスト ボックスをクリックし、[大きいアイコン] を選択します。

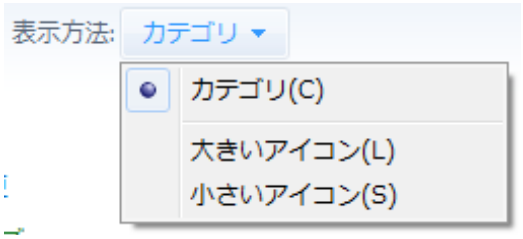


図:コントロール パネルの 表示方法 ドロップダウン リスト ボックス

3. コントロール パネルのウィンドウから [管理ツール] のアイコンをダブル クリックします。

図:管理ツール アイコン

4. [管理 ツール] のウィンドウが表示されるので、同ウィンドウ内から [イベント ビューアー] のショートカット アイコンをダブル クリックします。

図:イベントビューアーのショートカットアイコン

5. [イベント ビューアー] のウィンドウが表示されるので、画面左のツリービューを展開し、[Windows ログ] 下の [アプリケーション]、[セキュリティ]、[システム] のいずれかを選択します。

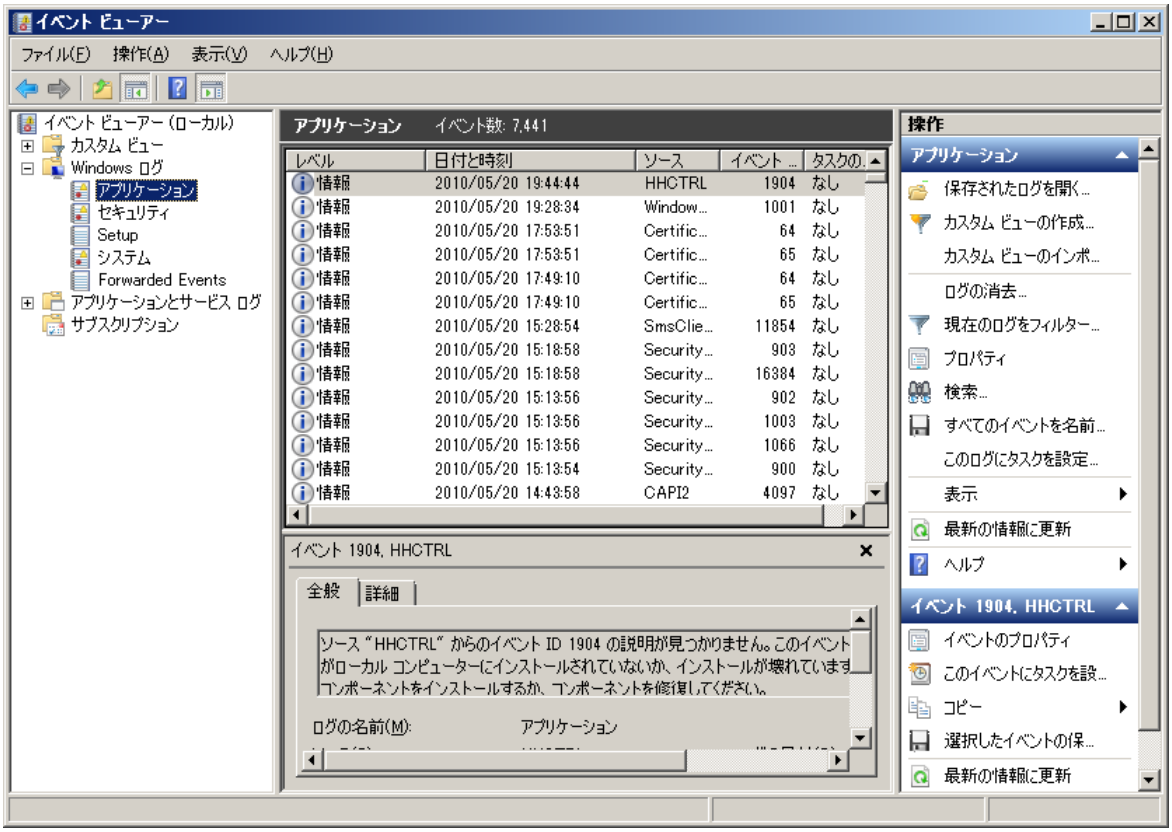


図: [イベント ビューアー] の画面

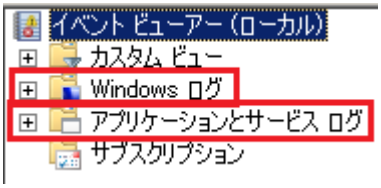
6. 画面中央にイベント ログのリストが表示されるので、任意のものをダブル クリックして、イベント ログの内容を表示します。

図 : イベント ログ

イベント ログ内には、発生時刻、メッセージ、イベントコードのほか、スタック トレース等の問題に関する詳細情報が記録されています。

イベント ログの種類

Windows Vista 以降の Windows OS のイベント ログには 2 つのカテゴリーがあります。Windows ログとアプリケーションとサービス ログです。



図：ツリービューの [Windows ログ] と [アプリケーションとサービス ログ]

Windows ログ

Windows ログのカテゴリーには、以前のバージョンの Windows でおもに使用可能していたアプリケーション ログ、セキュリティ ログ、およびシステム ログが含まれます。また、セットアップ ログと ForwardedEvents ログといった、2 つの新しいログも含まれます。Windows ログは、レガシ アプリケーションのイベントと、システム全体に当てはまるイベントを格納することを目的としています。

ログ	内容
アプリケーション ログ	アプリケーションまたはプログラムによって記録されたイベントが含まれる。たとえば、プログラムでファイル エラーが発生すると、そのイベントはアプリケーション ログに記録される。どのイベントがログに記録されるかは、プログラムの設計による。
セキュリティ ログ	ログオンに関するようなイベントと共に、リソースの使用に関連するイベント (ファイルなどのオブジェクトの作成、オープン、削除など) が含まれる。管理者は、セキュリティ ログに記録するイベントを指定することができる。たとえば、ログオンの監査を有効にすると、システムへのログオン試行がセキュリティ ログに記録される。
セットアップ ログ	アプリケーションのセットアップに関連するイベント
システム ログ	Windows のシステム コンポーネントによって記録されたイベントが記録される。たとえば、起動時にドライバーなどのシステム コンポーネントを読み込めなかった場合は、そのイベントがシステム ログに記録される。システム コンポーネントによって記録されるイベントの種類は、Windows によってあらかじめ決定されている。

ForwardedEvents ログ	リモート コンピューターから収集されたイベントを格納するために使用される。リモート コンピューターからイベントを収集するには、イベント サブスクリプションを作成する必要がある

表 : [Windows ログ] に含まれるログの種類と内容

アプリケーションとサービス ログ

アプリケーションとサービス ログは、Windows Vista から追加された新しいカテゴリーのイベントログです。これらのログは、システム全体に影響を与える可能性のあるイベントではなく、1 つのアプリケーションまたはコンポーネントのイベントを格納します。

このカテゴリーのログには、Admin (管理)、Operational (使用可能)、Analytic (分析)、および Debug (デバッグ) ログ という 4 つのサブタイプがあります。管理ログに記録されたイベントは、問題の対処方法に関する指針を示します。使用可能ログに記録されたイベントも IT 専門家に役立ちますが、情報が足りない可能性があります。

図 : アプリケーションとサービス ログの表示例

分析ログとデバッグ ログはユーザー向けではありません。分析ログには問題をトレースするイベントが格納され、多くの場合、大量のイベントが記録されます。デバッグ ログは、アプリケーションをデバッグするときに開発者が使用します。分析ログとデバッグ ログはどちらも既定では表示されず無効になっています。

ログ	内容
Admin	エンド ユーザー、管理者、およびサポート担当者を対象としたログ。管理チャネルで見つかったイベントは、問題と管理者が実行できる明確な解決方法を示す。これらのイベントは詳細に文書化されているか、またはメッセージが関連付けられているため、問題を修正するために実行する必要がある作業についての直接的な指示を得ることができます。
Operational	問題や事象の分析と診断に使用するためのログ。これらのイベントは、問題や事象に基づいてツールやタスクをトリガーするために使用できます。
Analytic	プログラムの動作の説明であり、ユーザーの操作では対処できない問題を示します。
Debug	プログラムの問題のトラブルシューティングを行う開発者を対象としたもの。

表 : [アプリケーションとサービス ログ] に含まれるログの種類と内容

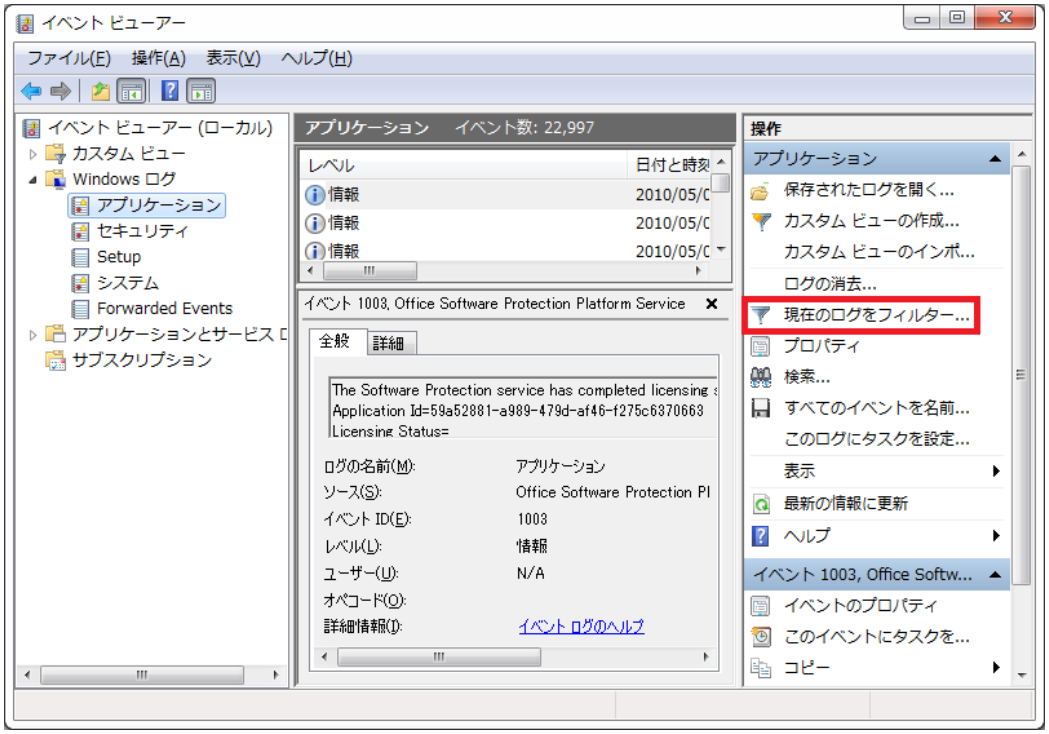
注目すべきイベントソースと ID

IIS でホストされているサービスは、さまざまなサービスが組み合わされてホストされています。そのためトラブルシュートを行う内には、複数のサービスのログの内容を確認し、総合的に原因を判断する必要があります。

たとえば、HTTP の問題のトラブルシュートを行う際には、以下のイベント ソースのイベント ログの内容をチェックします。

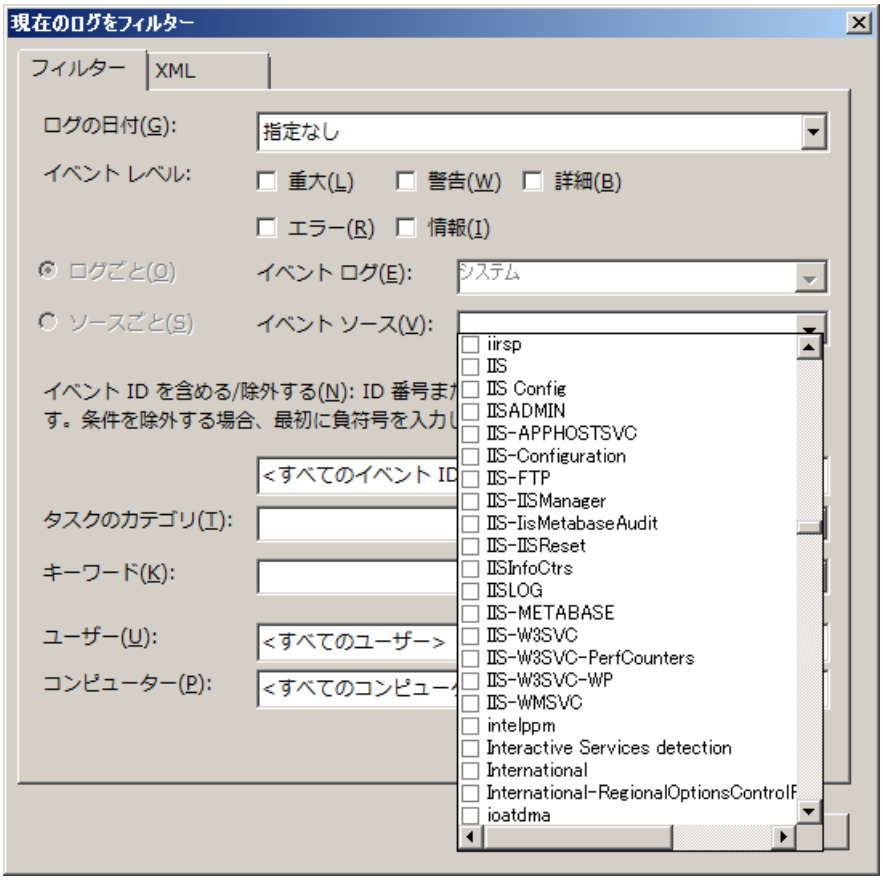
イベントソース	内容
IIS-APPHOSTSVC	Application Host Helper Service のログ。Application Host Helper Service は IIS に構成履歴やアプリケーション プール アカウントのマッピングなどの管理サービスを提供します。
IIS-W3SVC	World Wide Web Publishing Service (Web 発行サービス) のログ。Web 発行サービスは IIS マネージャーを使用した Web 接続と管理を提供します。
IIS-W3SVC-WP	ワーカー プロセス(w3wp.exe) のログ。ワーカー プロセスは、Web アプリケーションを実行し、Web サーバーを特定のアプリケーション プールを送信された要求を処理します。
IIS-WMSVC	IIS の Web 管理サービス (WMSvc) のログ。Web 管理サービスは、アプリケーション、Web サイトのリモートからの委任された管理を行えるようにします。
WAS	Windows プロセス アクティブ化サービス (WAS) のログ。WAS は、HTTP および他のプロトコルのアプリケーション プールの構成と作成ワーカー プロセスの有効期間の管理を行います。
WAS-ListenerAdapter	Web のリスナーアダプターのログ。
HttpService	Microsoft Windows HttpService のログ。HttpService は HTTP.sys をホストします。

イベント ログから特定のイベントソースを抽出するには、イベント ビューアーの画面右側の [操作] ウィンドウから [現在のログをフィルター] メニューをクリックします。



図：イベント ビューアー の画面

[現在のログをフィルター] ダイアログ ボックスが表示されるので、[イベント ソース] ドロップダウン リスト ボックスから、任意のイベント ソースのチェック ボックスをチェックして選択します。



図：[現在のログをフィルター] ダイアログ ボックス

HTTP の問題のトラブルシュートを行う際には、上記イベント ログと合わせ、**ファイヤーウォール** ログ、**Web サイト** ログ、**httperr** ログの 3 つも合わせてチェックします。

各ログの収納場所は以下の通りです。

ログ	場所
ファイヤーウォール ログ	%SyatemRoot%¥System32¥Logfiles¥Firewall
Web サイト ログ	%SyatemDrive%¥inetpub¥logs¥LogFiles¥W3SVCn (n) はサイト ID
httperr ログ	%SyatemRoot%¥System32¥Logfiles¥HTTPERR

表 : ログ ファイルの場所

なお、%SyatemRoot%¥System32¥Logfiles フォルダーを表示するには、[ファイル名を指定して実行] に、”logfiles” と入力し [Enter] キーを押下しても表示されることができます。

その他、IIS に関するプロセスとして、IIS Admin、FTP Publishing, Service などがあります。すべてのイベントの一覧につきましては、以下のドキュメントをご参照ください。

Microsoft TechNet - 『Events Reference』
http://technet.microsoft.com/ja-jp/library/cc776711(WS.10).aspx

コラム : イベント ログのサブスクリプション化

イベントビューアーで サブスクリプション を構成すると、リモート コンピューターからイベントを収集し、ローカル コンピューターのログに格納することができます。サブスクリプションがアクティブになりイベントが収集されていると、ローカルに格納されている他のイベントと同様に、転送されたイベントを表示して操作することができます。これは、複数台のサーバーを集中して管理する場合などに便利です。この機能は、Windows Vista 以降のイベント ビューアーで使用することができます。

イベント ログのサブスクリプションの具体的な構成方法などについては、以下のドキュメントのリンク先をご参照ください。

Microsoft TechNet - 『イベント サブスクリプション』
http://technet.microsoft.com/ja-jp/library/cc749183.aspx