

IIS をガードする ISAPI フィルタ
guard3 1.26 説明書

2002 年 6 月 5 日

長谷川 武 has@ccs.co.jp

TRUSNET® セキュリティサービス (www.trusnet.com)
CCS セントラル・コンピュータ・サービス株式会社

目 次

1. guard3 1.26 とは	4
1.1 guard3	4
1.2 guard3 1.26	4
2. guard3 1.26 ご使用上の注意	5
2.1 著作権	5
2.2 動作の安定性	5
2.3 免責	6
3. guard3 1.26 の新しい点	7
3.1 脆弱性対策 [1.24(脆弱) 1.25(対策済)].....	7
3.2 不当なエンコーディングの排除 [1.20 新機能].....	7
3.2.1 生データの検査と排除	7
3.2.2 %xx デコード後文字列の検査と排除	7
3.3 パターンマッチ機能 [1.20 新機能][1.24 新機能].....	8
3.4 フィルタ対象ゾーンの指定機能 [1.20 新機能].....	8
3.5 長さ制限機能の強化 [1.20 新機能].....	8
3.6 リクエスト拒絶時のカスタムエラー表示 [1.24 新機能].....	8
3.7 バグ修正	9
4. guard3 1.26 のインストール	10
4.1 新規インストール (Windows 2000).....	10
4.2 既存 guard3 の入れ替え (Windows 2000).....	13

5. guard3 1.26 のパラメタ記述例	14
6. guard3 1.26 のパラメタ記述仕様	16
6.1 共通設定と個別設定	16
6.2 共通設定	16
6.2.1 共通設定のレジストリキー	16
6.2.2 共通設定のパラメタ項目	16
6.2.2.1 UriSizeLimit URL 長の上限	17
6.2.2.2 PathSizeLimit URL 中のパス名長の上限	17
6.2.2.3 QueryStringSizeLimit URL 中のクエリストリング長の上限	17
6.2.2.4 EncodeErrorPage エンコードエラー時に表示する HTML ファイル	18
6.2.2.5 SizeErrorPage サイズエラー時に表示する HTML ファイル	19
6.2.2.6 ErrorPageBase エラーページの基準ディレクトリ	19
6.2.2.7 WriteLogFile ログ出力をするか否か	20
6.2.3 互換性のための項目	20
6.3 個別設定	21
6.3.1 ゾーン名	21
6.3.2 個別設定のレジストリキー	21
6.3.3 個別設定のパラメタ項目	22
6.3.3.1 UriSizeLimit URL 長の上限	22
6.3.3.2 PathSizeLimit URL 中のパス名長の上限	23
6.3.3.3 QueryStringSizeLimit URL 中のクエリストリング長の上限	23
6.3.3.4 Rule<NN>_xxx パターンマッチルールのための項目群	23
6.3.3.5 Translations 文字の置換	24
6.3.3.6 EncodeErrorPage エンコードエラー時に表示する HTML ファイル	24
6.3.3.7 SizeErrorPage サイズエラー時に表示する HTML ファイル	25
6.3.3.8 ErrorPageBase エラーページの基準ディレクトリ	25
6.4 パターンマッチルール	26
6.4.1 動作とマッチパターン	26
6.4.2 パターンマッチルールの評価順序	27
6.4.3 パターンマッチルールのレジストリ記述	27
6.4.3.1 Rule<ルール番号>_Action ルールの動作	27
6.4.3.2 Rule<ルール番号>_Method HTTP メソッドのパターン	28
6.4.3.3 Rule<ルール番号>_Path パス名のパターン	28
6.4.3.4 Rule<ルール番号>_Qs クエリストリングのパターン	28
6.4.3.5 Rule<ルール番号>_QsItem<項目パターン番号> 「名前 = 値」対のパターン	28
6.4.4 マッチパターン	29
7. パラメタ変更の反映	30
7.1 Windows 2000 の IIS 5.0 の場合	30
7.2 Windows NT 4.0 の IIS 4.0 の場合	30

1. guard3 1.26 とは

1.1 guard3

ISAPI フィルタ

guard3 は、Microsoft 社の標準的な WWW サーバソフトである Internet Information Services (IIS) に組み込んで使用する「ISAPI フィルタ」といわれる種類のアドインモジュールです。

guard3 は、長すぎる URL を送りつけたり入力データにメタキャラクタを混入して Web アプリケーション運営者が意図しない悪用・妨害を試みる行為に対し、HTTP リクエストを遮断したり害のある文字を別のものに置換したりするフィルタソフトウェアです。

フリーソフトウェアと入手先

guard3 は長谷川武が作成し、セントラル・コンピュータ・サービス株式会社が配布するフリーソフトウェアです。一般的なバージョンは次のところから入手できます。

<http://www.trusnet.com/tools/guard3/index.html>

これまで (2002 年 5 月まで) 一般的なバージョンは 1.03 でした。

ここで「一般的なバージョン」と断っているのは、公開されていない場所で guard3 の機能強化や改良が行われていて、実際にはより多くのバージョンが存在するためです。

1.2 guard3 1.26

新バージョン

guard3 1.26 は、guard3 の新バージョンです。

次のところから入手できます。

http://www.trusnet.com/tools/guard3/guard3_126.lzh プログラム

http://www.trusnet.com/tools/guard3/guard3_126.pdf ドキュメント (本書)

2. guard3 1.26 ご使用上の注意

guard3 バージョン 1.26 をお使いになる場合には次の点にご注意ください。

2.1 著作権

guard3 の著作権は作者 長谷川武 (has@ccs.co.jp) および配布者 セントラル・コンピュータ・サービス株式会社 (東京都江東区亀戸 6-41-10) が有します。

フリーソフトウェア

- ・ guard3 バージョン 1.26 は 1.03 にひきつづき、フリーソフトウェアです。セキュリティ対策のために IIS に組み込むという目的であればあなたでもご自由にお使いいただけます。
- ・ guard3 そのものを転売すること(他者にコピーを譲渡しその際に対価を受け取ること)はお断りいたします。

ソースコード

- ・ guard3 のダウンロードアーカイブにはソースコードが添付されています。guard3 に脆弱性 / バックドア / バグが疑わしい場合は (手間はかかりますが) 誰でも検証できるようにしています。
- ・ また、必ずしも優れたコードではありませんが、guard3 のソースコードをご自身が ISAPI フィルタを C++ で記述する際の参考にしてくださってけっこうです。
- ・ ただし、guard3 のソースコードの大部分をそのまま再利用し、少しだけ改造したものを guard3 とは全く無関係な新しいソフトウェアと称して配布することはお断りいたします。
- ・ guard3 のソースコードを改変してご使用になれる場合は、ソースコードやドキュメントに関する原作者の著作権表示 (本節「2.1 著作権」冒頭の表記) を維持するように願います。

再配布

- ・ guard3 を、CD-ROM、Web サイトなどを使って再配布することをご希望の方は、作者までご連絡いただき作者の了解を得た上で行ってください。

2.2 動作の安定性

guard3 バージョン 1.26 は、他のバージョンの guard3 と同じく、Web サーバおよび Web アプリケーションの安全に寄与する目的で作られているソフトウェアです。このドキュメント執筆時点で既知のバグはひととおり修正済みですが、潜在する不完全性・不備により、悪意ある HTTP リクエストの排除に失敗したり、Web サーバのプロセス動作そのものに悪影響を及ぼすおそれがないとは言いきれません。

guard3 バージョン 1.26 をお使いになるときは次のような安全対策を施しつつご使用ください。

- 1) WWW コンテンツのバックアップを定期的にとる。
- 2) IIS のサービスプロセス (inetinfo.exe) が異常終了していないか定期的に確認する。
- 3) 動作が怪しいときにはログを記録するモードで guard3 1.26 を動作させる。ただし、ログファイルでディスクが一杯にならないようご注意ください。

デバッグ情報

guard3 1.26は、万が一の場合に備えてデバッグ情報を含めた状態でビルドしてあります。IISが稼動するサーバにデバッガがインストールされていれば^注、異常発生箇所のスタックトレースなどの情報が取得できます。

注 セキュリティ対策の観点からは、本番稼動用サーバにデバッガソフトをインストールしておくことはお奨めできません。

2.3 免責

guard3 ソフトウェアをご使用の際に生じるいかなる損害についても、開発者 長谷川武ならびに配布者 セントラル・コンピュータ・サービス株式会社は一切の賠償責任を負いません。このソフトウェアはご使用者の自己責任においてお使いください。

ただし、障害の情報はお寄せいただくと幸いです。可能な範囲でできるだけのフォローはさせていただきます。

3. guard3 1.26 の新しい点

guard3 1.26 には 1.03 に対して次の新機能および改善が加わりました。下記の新機能の中にはバージョン 1.1 ~ および 1.25beta で実装されたものも含まれています。

3.1 脆弱性対策 [1.24(脆弱) 1.25(対策済)]

1.24 およびそれより古いバージョンの guard3 には、ある特定の工夫をした HTTP リクエストを送り付けることで guard3 が本来はたらかせるはずのフィルタ機構を迂回できる脆弱性がありました。1.25 にてこの問題に対策を施しました。

3.2 不当なエンコーディングの排除 [1.20 新機能]

不当あるいは不都合と考えられる一定の文字パターンが HTTP リクエストの URL のパス部分(? の手前) に含まれていると、HTTP ステータスコード 400 のエラーとして排除します。

3.2.1 生データの検査と排除

クライアントから送られてきたままの HTTP リクエストの URL のパス部分に次に該当するものがあれば、その HTTP リクエストをステータスコード 400 で排除します。

不当あるいは不都合な %xx エンコーディング

- 1) xx の 2 桁に正しい十六進数を伴わない %xx 形式のエンコーディング
- 2) ナルキャラクタを表すエンコーディング %00
- 3) % そのものを表すエンコーディング %25

3.2.2 %xx デコード後文字列の検査と排除

HTTP リクエストの URL のパス部分の %xx エンコーディングをデコードした後の結果に次のものが含まれていれば、その HTTP リクエストをステータスコード 400 で排除します。

冗長な UTF-8 エンコーディングとその派生形

- 1) 冗長な 2 バイト UTF-8

ビットパターン 1100000x 10xxxxxx
1 バイト目 0xC0 ~ 0xC1 2 バイト目 0x80 ~ 0xBF

- 2) その派生形

ビットパターン 1100000x yyxxxxxx
1 バイト目 0xC0 ~ 0xC1 2 バイト目 0x01 ~ 0xFF

- 3) 冗長な 3 バイト UTF-8

ビットパターン 11100000 1000000x 10xxxxxx
1 バイト目 0xE0 2 バイト目 0x80 ~ 0x81 3 バイト目 0x80 ~ 0xBF

4) その派生形

ビットパターン 11100000 yy00000x yyxxxxxx

1 バイト目 0xE0 2 バイト目 0x01, 0x40, 0x41, 0x80, 0x81, 0xC0, 0xC1

3 バイト目 0x01 ~ 0xFF

ここに,

x xxxxxx は ASCII コードに該当するビットパターン

yy は任意のビットパターン

不都合なディレクトリ区切記号

5) 文字 ¥

ただし, シフト JIS 漢字コードの 2 バイト目に該当する 0x5C (¥) は排除しない。

不都合な相対ディレクトリ表現

6) 次の文字列のいずれか // /./ /..

3.3 パターンマッチ機能 [1.20 新機能][1.24 新機能]

URL を構成する一部分が特定の文字列のパターンにマッチしたときに HTTP リクエストを排除する機能。指定の仕方によっては特定のパターンのみ受容するようにも指定できます。

- 1) パターンマッチは HTTP メソッド, URL のプログラムパス部分, クエリストリング部分全体, クエリストリングに含まれる個々の「名前 = 対」の 4 種類に対して指定できる。
- 2) 複数のパターンマッチルールを設定し, 組み合わせて複雑な排除 / 受容の条件を設定することができる。

3.4 フィルタ対象ゾーンの指定機能 [1.20 新機能]

フィルタパラメータを特定の IP アドレスおよび特定のディレクトリパスに限定して設定できるようになりました。

3.5 長さ制限機能の強化 [1.20 新機能]

URL の長さだけでなく, URL のプログラムパス部分およびクエリストリング部分についても個別に長さ制限を指定できるようになりました。

3.6 リクエスト拒絶時のカスタムエラー表示 [1.24 新機能]

guard3 が HTTP リクエストを拒絶したとき WWW クライアントへ送り返すエラーメッセージの内容として, WWW サーバ管理者が自分で用意した HTML ファイルを使うよう指定できるようになりました。

3.7 バグ修正

- ・パターンマッチのパターンをレジストリから読み込む際のバグを修正しました。[1.24]
- ・パターンマッチのパターンの大文字アルファベットが正しく機能しない問題を修正しました。
[1.23]
- ・そのほか、いくつかのバグを修正しました。

4. guard3 1.26 のインストール

guard3 1.26の新規インストールは、IISへのISAPIフィルタの追加手順を実施することで行えます。

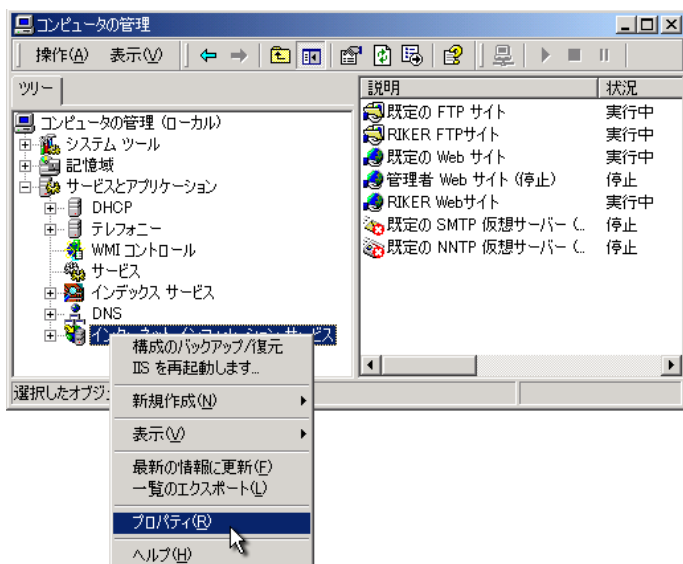
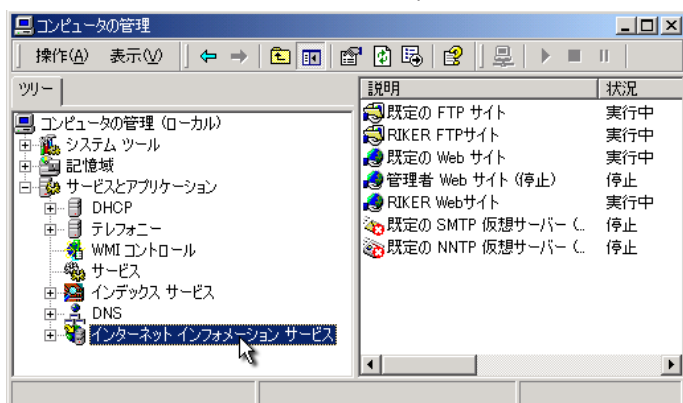
Windows 2000のIIS 5.0場合は次のようになります。他のWindowsプラットフォーム(Windows NT Server 4.0, Windows XP)についてもこれに準じた手順を行ってください。

Windows NT Server 4.0にguard3を新規インストール/入れ替えを行った際はIIS Adminサービスの再起動が必要になります。

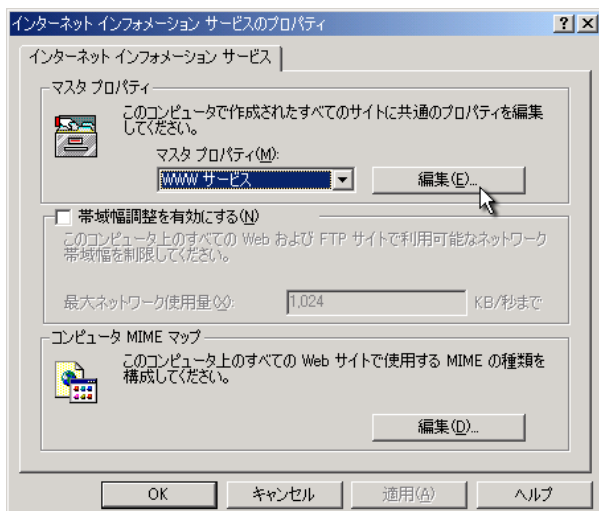
4.1 新規インストール (Windows 2000)

管理者権限のあるアカウントで次の操作を行ってください。

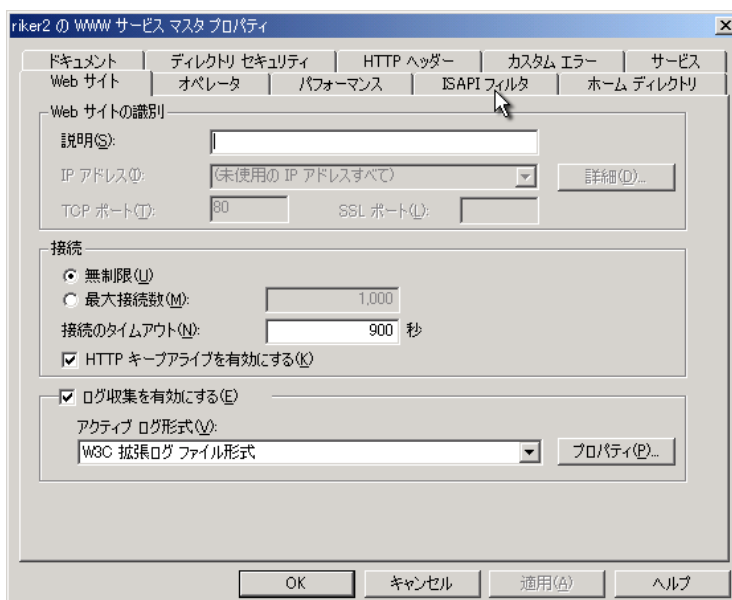
- (1) 「スタート」メニューの「プログラム」の「管理ツール」から「コンピュータの管理」を開きます。
- (2) 「コンピュータの管理」の中の「サービスとアプリケーション」の中の「インターネットインフォメーションサービス」を選び、「プロパティ」を開きます。



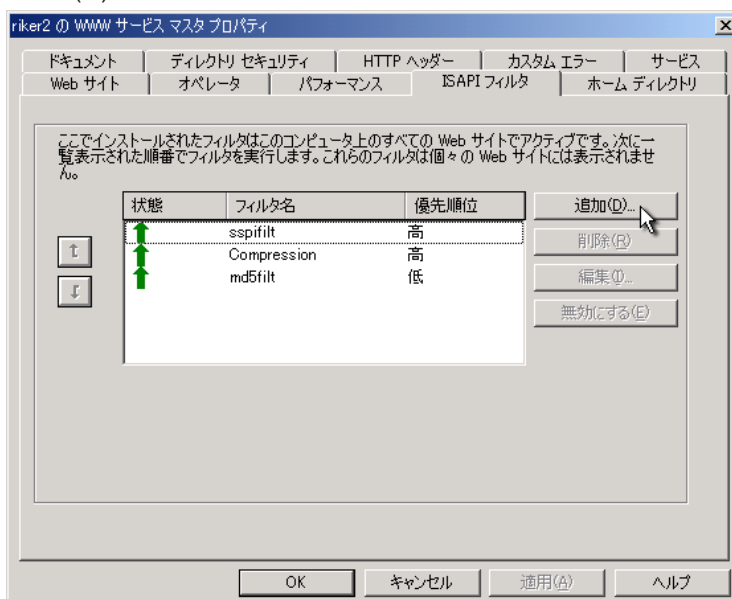
(3) 「マスタプロパティ」の「WWW サービス」の「編集(E)...」を選びます。



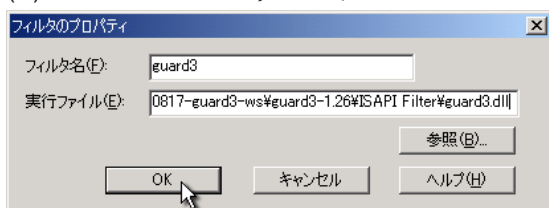
(4) 「ISAPI フィルタ」タブを選びます。



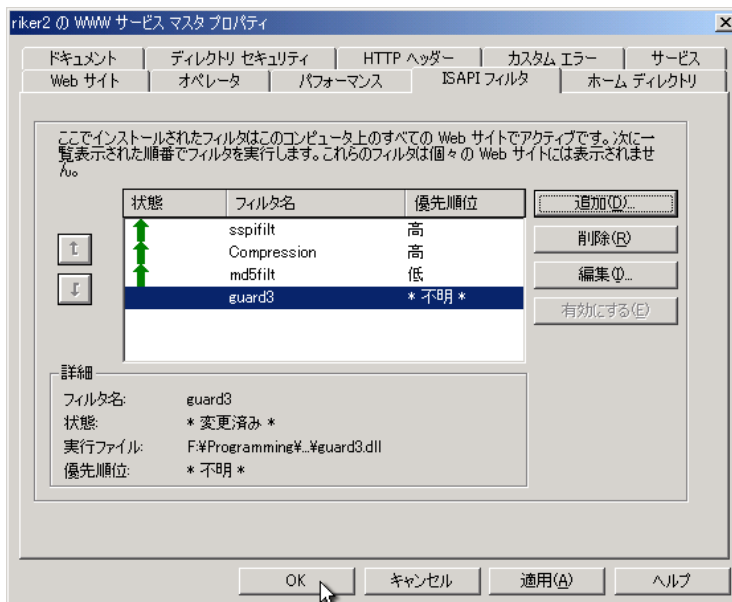
(5) 「追加(D)...」を選びます。



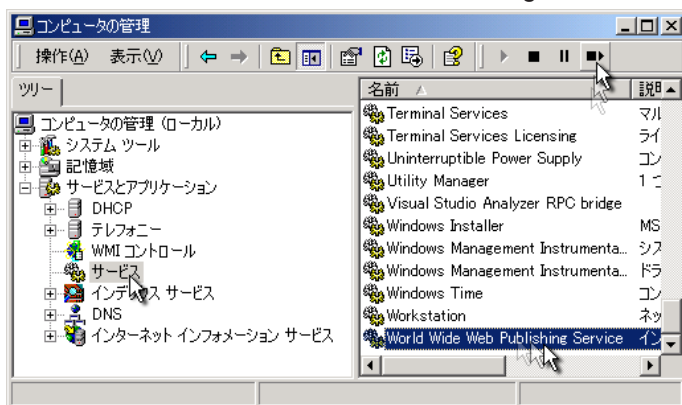
- (6) 「フィルタ名」欄に「guard3」, 「実行ファイル」欄に guard3.dll のパスを入力 (または「参照 (R)...」を使って指定) して, 「OK」ボタンをクリックします。



- (7) guard3 がフィルター一覧に現れたことを確認し, 「OK」ボタンをクリックします。



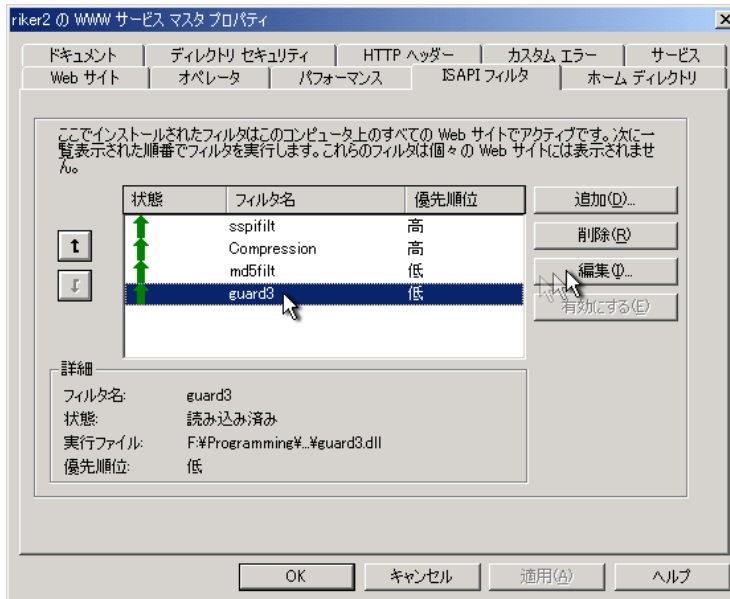
- (8) 「サービス」の「World Wide Web Publishing Service」を再起動します。



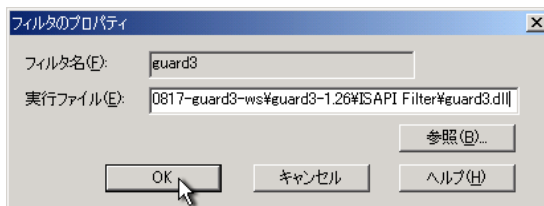
4.2 既存 guard3 の入れ替え (Windows 2000)

すでに古いバージョンのguard3をお使いの場合、管理者権限のあるアカウントで次の手順を行い、IIS がロードする guard3.dll ファイルを入れ替えてください。

- (0) 既存の guard3.dll とは異なるパスに新しい guard3.dll を置きます。
- (1)(2)(3)(4) 上記「新規インストール (Windows 2000)」の手順と同じ操作
- (5) 現在インストールされている ISAPI フィルタのリストの中から「guard3」を選び「編集(I)...」をクリックします。



- (6) 「実行ファイル」欄に新しい guard3.dll のパスを入力 (または「参照(B)...」を使って指定) して、「OK」ボタンをクリックします。(フィルタ名欄の変更はここではできません。)



- (7)(8) 上記「新規インストール (Windows 2000)」の手順と同じ操作

5. guard3 1.26 のパラメタ記述例

guard3 1.26のフィルタリング・パラメタはこれまでのバージョンと同様にレジストリに記述します。ただし、記述項目がいくつか増えています。

以下に guard3 1.26 のパラメタをレジストリに記述した例を示します。(以下の例の記述で []内は項目のタイプ、<key> はその項目がレジストリキーであることを示します。)

例

```
1 HKLM\SOFTWARE\CCS\guard3\ <key>
2 HKLM\SOFTWARE\CCS\guard3\WriteLogFile = 1 [DWORD]
3 HKLM\SOFTWARE\CCS\guard3\images\ <key>
4 HKLM\SOFTWARE\CCS\guard3\images\Rule01_Action = "Accept" [SZ]
5 HKLM\SOFTWARE\CCS\guard3\images\Rule01_Path = "*.gif" [SZ]
6 HKLM\SOFTWARE\CCS\guard3\images\Rule02_Action = "Accept" [SZ]
7 HKLM\SOFTWARE\CCS\guard3\images\Rule02_Path = "*.jpg" [SZ]
8 HKLM\SOFTWARE\CCS\guard3\images\Rule03_Action = "Reject" [SZ]
9 HKLM\SOFTWARE\CCS\guard3\images\Rule03_Path = "*" [SZ]
10 HKLM\SOFTWARE\CCS\guard3\//192.168.7.59\ <key>
11 HKLM\SOFTWARE\CCS\guard3\//192.168.7.59\UrlSizeLimit = 701 [DWORD]
12 HKLM\SOFTWARE\CCS\guard3\//192.168.7.59\PathSizeLimit = 500 [DWORD]
13 HKLM\SOFTWARE\CCS\guard3\//192.168.7.59\QueryStringSizeLimit = 200 [DWORD]
14 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\ <key>
15 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\UrlSizeLimit = 201 [DWORD]
16 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\PathSizeLimit = 100 [DWORD]
17 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\QueryStringSizeLimit = 100 [DWORD]
18 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule01_Action = "Reject" [SZ]
19 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule01_Path = "*gif*" [SZ]
20 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule02_Action = "reject" [SZ]
21 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule02_QsItem01 = "=eno" [SZ]
22 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule02_QsItem03 = "=0100" [SZ]
23 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule03_Action = "reJect" [SZ]
24 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Rule03_Qs = "*clear*" [SZ]
25 HKLM\SOFTWARE\CCS\guard3\//192.168.7.60/photo-db\Translations = "|_<00>;<00><00>"
    [MULTI_SZ]
```

解説

guard3のパラメタはレジストリキーHK_LOCAL_MACHINE¥SOFTWARE¥CCS¥guard3¥の下に配置します。上記の例ではHK_LOCAL_MACHINEをHKLMと略記しています。

2行目は従来からあるパラメタで、guard3にログファイルを記録させる指定です。

ディレクトリを対象範囲に

3行目から9行目では、仮想ディレクトリ/imageの下のコンテンツに対してのみ有効なフィルタリング・パラメタを指定しています。ここでは、3つのパターンマッチルールを列記して、.gifファイルと.jpgファイルへのアクセスのみを許し他を禁止しています。

この/imageへの指定は、対象とするIISが複数の仮想サイトを稼働させている場合には全ての仮想サイトに適用されます。

仮想サイトを対象範囲に

10行目から13行目では、IPアドレス192.168.7.59でHTTPを受け付けている仮想サイトに対してのみ有効なフィルタリングパラメタを指定しています。ここではURLの全長、プログラム・パス部分の長さ、クエリストリング部分の長さのそれぞれについて上限のバイト数を指定しています。

複合した指定

14行目から25行目までは、IPアドレスとディレクトリ・パスの両方を記述して、ある仮想サイトの中の特定のディレクトリ下のコンテンツに対してのみ有効なフィルタリングルールを指定しています。

ここでは、各種長さ制限を指定するとともに、次のようなパターンに該当するHTTPリクエストを禁止しています。

Rule 01 ファイルのパスに“ gif ”という文字列を含む場合、HTTPリクエストを拒絶。

Rule 02 クエリストリングの「名前=値」対の中に“ eno ”という値をもつものと“ 0100 ”という値をもつものの両方が同時に含まれている場合、HTTPリクエストを拒絶。

Rule 03 クエリストリングに“ clear ”という文字列が含まれている場合、HTTPリクエストを拒絶。

最後の25行目では、メタキャラクタとして意味を持つおそれのある縦棒(|)とセミコロン(;)を両方ともアンダースコア(_)に置き換えるよう指定しています。このTranslationsパラメタは従来からあったものを、個別のゾーンに指定できるようにしたものです。

6. guard3 1.26 のパラメタ記述仕様

guard3 1.26 のパラメタをレジストリに記述する際の詳細について説明します。

6.1 共通設定と個別設定

対象となるIISが管理するWWWコンテンツへのアクセス全体に影響が及ぶ設定を「共通設定」、特定の仮想サイト IP アドレスや仮想ディレクトリパスに対してのみ効力を発揮する設定を「個別設定」と呼びます。

共通設定は一つのサーバマシンにつき一組だけ定義できます。個別設定は必要に応じて複数個を定義可能です。

6.2 共通設定

共通設定パラメタは次の要領で記述します。

6.2.1 共通設定のレジストリキー

共通設定は次のレジストリキーの直下のレジストリ項目として記述します。

HKLM¥SOFTWARE¥CCS¥guard3¥

6.2.2 共通設定のパラメタ項目

共通設定のパラメタ項目には次のものがあります。

サイズ制限

UrlSizeLimit	URL 長の上限
PathSizeLimit	URL 中のパス名長の上限
QueryStringSizeLimit	URL 中のクエリストリング長の上限

カスタムエラーページ

EncodeErrorPage	エンコードエラー検出時に表示する HTML ファイルのパス名
SizeErrorPage	サイズエラー検出時に表示する HTML ファイルのパス名
ErrorPageBase	エラーページ (HTML ファイル) の基準ディレクトリ

ログ出力のコントロール

WriteLogFile	ログ出力をするか否か
--------------	------------

6.2.2.1 UrlSizeLimit URL 長の上限

データタイプ REG_DWORD

説明

許容するURLの最大長。バイト数。このサイズを超えるURLをもつHTTPリクエストは排除される。

ここで数えるURL長には、ドメインに関する部分（http://foo.bar/dir1/dir2/file?paramのhttp://foo.barの部分）の文字数は含まない。

後述の個別設定でも同名のパラメタでURL長の上限を指定できるが、共通設定のこのパラメタは個別設定の省略時解釈値として使われる。

指定可能範囲 0 ~ 4095

省略時解釈値 4095

例 UrlSizeLimit=1001

6.2.2.2 PathSizeLimit URL 中のパス名長の上限

データタイプ REG_DWORD

説明

許容する、URL中のパス名の長さの上限。バイト数。このサイズを超えるパス名をもつHTTPリクエストは排除される。

後述の個別設定でも同名のパラメタでURL中のパス名の長さの上限を指定できるが、共通設定のこのパラメタは個別設定の省略時解釈値として使われる。

指定可能範囲 0 ~ 4095

省略時解釈値 4095

例 PathSizeLimit=500

6.2.2.3 QueryStringSizeLimit URL 中のクエリストリング長の上限

データタイプ REG_DWORD

説明

許容する、URL中のクエリストリングの長さの上限。バイト数。このサイズを超えるパス名をもつHTTPリクエストは排除される。

クエリストリングのための区切り文字「?」はここで数えるバイト数には含まれない。

後述の個別設定でも同名のパラメタでURL中のクエリストリングの長さの上限を指定できるが、共通設定のこのパラメタは個別設定の省略時解釈値として使われる。

指定可能範囲 0 ~ 4095

省略時解釈値 4095

例 QueryStringSizeLimit=500

6.2.2.4 EncodeErrorPage エンコードエラー時に表示する HTML ファイル

データタイプ REG_SZ

説明

不正なエンコードを理由に HTTP リクエストを排除する際に表示させるカスタムエラーメッセージページ (HTML) の物理パス名。

このパラメタにパス名全体 (絶対パス名) を指定することも可能だが、別の ErrorPageBase パラメタで特定のディレクトリを指定しておき、そこからの相対パスを指定する方法もある。その場合、エンコードエラーに対するエラーページのファイルのパス名には、

ErrorPageBase パラメタのディレクトリパス と

EncodeErrorPage パラメタの相対パス

を連結したものが使われる。

後述の個別設定でも同名のパラメタでエンコードエラー検出時のエラーページ HTML ファイルのパス名を指定できるが、共通設定のこのパラメタは個別設定の省略時解釈値として使われる。

指定可能な値

ErrorPageBase パラメタが指定されていない場合

<ドライブ文字>:¥<ディレクトリパス>...¥<ファイル名>

ErrorPageBase パラメタが指定されている場合

<ディレクトリパス>...¥<ファイル名> または

<ファイル名>

省略時解釈値 なし

例 EncodeErrorPage=c:¥InetPub¥wwwroot¥error_messages¥common¥encode_error.htm

6.2.2.5 SizeErrorPage サイズエラー時に表示する HTML ファイル

データタイプ REG_SZ

説明

サイズオーバーを理由にHTTPリクエストを拒絶する際に表示させるカスタムエラーメッセージページ (HTML) の物理パス名。

このパラメタにパス名全体 (絶対パス名) を指定することも可能だが、別のErrorPageBaseパラメタで特定のディレクトリを指定しておき、そこからの相対パスを指定する方法もある。その場合、サイズオーバーに対するエラーページのファイルのパス名には、

ErrorPageBase パラメタの値 と この SizeErrorPage パラメタの値

を連結したものが使われる。

後述の個別設定でも同名のパラメタでエンコードエラー検出時のエラーページHTMLファイルのパス名を指定できるが、共通設定のこのパラメタは個別設定の省略時解釈値として使われる。

指定可能な値

ErrorPageBase パラメタが指定されていない場合

<ドライブ文字>:\<ディレクトリパス>...\<ファイル名>

ErrorPageBase パラメタが指定されている場合

<ディレクトリパス>...\<ファイル名> または
<ファイル名>

省略時解釈値 なし

例 SizeErrorPage=c:\inetpub\wwwroot\error_messages\common\size_error.htm

6.2.2.6 ErrorPageBase エラーページの基準ディレクトリ

データタイプ REG_SZ

説明

カスタムエラーページのパス名を指定する際の基準となるディレクトリパス。EncodeErrorPageパラメタおよびSizeErrorPageパラメタに相対パスを指定する場合に使用する。

後述の個別設定でも同名のパラメタでエンコードエラー検出時のエラーページHTMLファイルのパス名を指定できるが、共通設定のこのパラメタは個別設定の省略時解釈値として使われる。

指定可能な値

<ドライブ文字>:\<ディレクトリパス>...\<ディレクトリパス> または

<ドライブ文字>:\<ディレクトリパス>...

省略時解釈値 なし

例 ErrorPageBase=c:\inetpub\wwwroot\error_messages\common

6.2.2.7 WriteLogFile ログ出力をするか否か

データタイプ REG_DWORD

説明

guard3 が独自のログファイルを出力するか否か。0 以外 = 出力 , 0 = 出力しない。

guard3のログはディレクトリ <windows>%system32%LogFile%guard3% の下に各月ごとのファイルとして書き出される。

指定可能な値 0 および 0 以外

省略時解釈値 0

例 WriteLogFile=1

6.2.3 互換性のための項目

次の項目は旧バージョンとの互換性のために残してある項目です。説明は割愛します。

Translations [REG_MULTI_SZ]

TargetPaths [REG_MULTI_SZ]

6.3 個別設定

個別設定パラメタは次の要領で記述します。

6.3.1 ゾーン名

一組の個別設定は、特定の「ゾーン」を対象として効力を発揮します。個々のゾーンは適用範囲を示す「ゾーン名」を持ちます。ゾーン名は、仮想サイトの IP アドレスあるいは仮想ディレクトリパスを用いた次のいずれかの形式になります。

//<IPアドレス>

一つの仮想サイト全体を対象とするゾーンのゾーン名。<IP アドレス> は、たとえば 160.248.99.100 のように、十進表現のオクテットをドットで区切って 4 つ並べたもの。

/<ディレクトリパス>

一定のディレクトリパスの下を対象とするゾーンのゾーン名。WWWサーバに仮想サイトが複数あるときは各仮想サイトの同名のディレクトリパスがすべて対象となる。もともとディレクトリパスは 1 個の / から始まるパスなのであるが、ここでは / で始まることを明示するために /<ディレクトリパス> と表現している。

//<IPアドレス>/<ディレクトリパス>

一つの仮想サイトの中の特定のディレクトリパスの下を対象とするゾーンのゾーン名。上記の 2 つを組み合わせたもの。

範囲が競合する場合

複数の個別設定が行われると、複数のゾーンのゾーン名が示す領域の間に共通の部分が生じたり、包含関係が生じることがあります。その場合、次のような優先ルールにもとづいて各ゾーンの実際の範囲が決定します。

ディレクトリパスが包含関係にある場合、

ディレクトリパスがより長いほうのゾーンの範囲が先に確定します。

ディレクトリパスがより短いものは、先行して確定した他のゾーンの範囲をゾーン名が示す領域から除外した部分がそのゾーンの範囲となります。

IP アドレスが明示されているものとされていないものが混在している場合、

ディレクトリパスに包含関係があれば、そちらのルールが優先します。

IP アドレスが明示されているほうのゾーンの範囲が先に確定します。

IP アドレスが明示されていないものは、先行して確定した他のゾーンの範囲をゾーン名が示す領域から除外した部分がそのゾーンの範囲となります。

6.3.2 個別設定のレジストリキー

個別設定は次のレジストリキーの直下のレジストリ項目として記述します。

HKLM¥SOFTWARE¥CCS¥guard3¥<ゾーン名>¥

ここに、<ゾーン名> は上記の 3 形態のうちの一つ。

6.3.3 個別設定のパラメタ項目

個別設定のパラメタ項目には次のものがあります。

サイズ制限

UrlSizeLimit	URL 長の上限
PathSizeLimit	URL 中のパス名長の上限
QueryStringSizeLimig	URL 中のクエリストリング長の上限

カスタムエラーページ

EncodeErrorPage	エンコードエラー検出時に表示する HTML ファイルのパス名
SizeErrorPage	サイズエラー検出時に表示する HTML ファイルのパス名
ErrorPageBase	エラーページ (HTML ファイル) の基準ディレクトリ

パターンマッチルール

Rule<NN>_Action	受容または拒絶の指定
Rule<NN>_Method	HTTP メソッドのマッチパターン
Rule<NN>_Path	URL 中のパス名のマッチパターン
Rule<NN>_Qs	URL 中のクエリストリング全体のマッチパターン
Rule<NN>_QsItem<NN>	URL 中のクエリストリング中の「名前=値」対のマッチパターン

6.3.3.1 UrlSizeLimit URL 長の上限

データタイプ REG_DWORD

許容する URL の最大長。バイト数。このサイズを超える URL をもつ HTTP リクエストは排除される。

ここで数える URL 長には、ドメインに関する部分 (http://foo.bar/dir1/dir2/file?param の http://foo.bar の部分) の文字数は含まない。

省略時解釈値 「共通設定」の UrlSizeLimit の値

指定可能範囲 0 ~ 4095

例 UrlSizeLimit=1001

6.3.3.2 PathSizeLimit URL 中のパス名長の上限

データタイプ REG_DWORD

許容する URL の「パス部分」の最大長。バイト数。URL のパス部分とは、静的コンテンツの URL においてはページ内ジャンプ・アンカーを示す # 記号の前までの部分、動的コンテンツの URL においてはクエリストリングを示す ? 記号の前までの部分を言う。

このサイズを超えるパス部分をもつ URL を含む HTTP リクエストは排除される。

省略時解釈値 「共通設定」の PathSizeLimit の値

指定可能範囲 0 ~ 4095

例 PathSizeLimit=256

6.3.3.3 QueryStringSizeLimit URL 中のクエリストリング長の上限

データタイプ REG_DWORD

説明

許容する URL の「クエリストリング部分」の最大長。バイト数。URL のクエリストリング部分とは、動的コンテンツの URL においてはクエリストリングを示す ? 記号よりうしろの部分、静的コンテンツの URL にはクエリストリング部分は存在しない。

このサイズを超えるパス部分をもつ URL を含む HTTP リクエストは排除される。

省略時解釈値 「共通設定」の QueryStringSizeLimit の値

指定可能範囲 0 ~ 4095

例 QueryStringSizeLimit=768

6.3.3.4 Rule<NN>_xxx パターンマッチルールのための項目群

項目群の詳細

Rule<ルール番号>_Action [REG_SZ]

Rule<ルール番号>_Method [REG_SZ]

Rule<ルール番号>_Path [REG_SZ]

Rule<ルール番号>_Qs [REG_SZ]

Rule<ルール番号>_QsItem<項目パターン番号> [REG_SZ]

説明

これら 5 種類のパラメタ項目はパターンマッチルールの記述するためのものである。パターンマッチルールについては後述する。なお、<ルール番号>と<項目パターン番号>はそれぞれ 00 ~ 99 の範囲の 2 桁の番号である。

6.3.3.5 Translations 文字の置換

データタイプ REG_MULTI_SZ

説明

文字の置き換えを指定する。マルチストリングタイプのレジストリ項目の各ストリングに、変換前文字と変換後文字の2文字をこの順に記述しさらにそれを1つ以上並べたもの。REG_MULTI_SZ。

例 Translations=|_<00>;_<00><00>

「|」と「;」をいずれも「_」へ置き換える指定。ここに、<00>はナルキャラクタを表わす。

6.3.3.6 EncodeErrorPage エンコードエラー時に表示する HTML ファイル

データタイプ REG_SZ

説明

不正なエンコードを理由にHTTPリクエストを排除する際に表示させるカスタムエラーメッセージページ (HTML) の物理パス名。

このパラメタにパス名全体 (絶対パス名) を指定することも可能だが、別のErrorPageBaseパラメタで特定のディレクトリを指定しておき、そこからの相対パスを指定する方法もある。その場合、エンコードエラーに対するエラーページのファイルのパス名には、

ErrorPageBase パラメタのディレクトリパス と
EncodeErrorPage パラメタの相対パス

を連結したものが使われる。

指定可能な値

ErrorPageBase パラメタが指定されていない場合

<ドライブ文字>:¥<ディレクトリパス>...¥<ファイル名>

ErrorPageBase パラメタが指定されている場合

<ディレクトリパス>...¥<ファイル名> または
<ファイル名>

省略時解釈値 「共通設定」のEncodeErrorPageの値

例 EncodeErrorPage=c:¥InetPub¥wwwroot¥error_messages¥site_1¥encode_error.htm

6.3.3.7 SizeErrorPage サイズエラー時に表示する HTML ファイル

データタイプ REG_SZ

説明

サイズオーバーを理由にHTTPリクエストを拒絶する際に表示させるカスタムエラーメッセージページ (HTML) の物理パス名。

このパラメタにパス名全体 (絶対パス名) を指定することも可能だが、別のErrorPageBaseパラメタで特定のディレクトリを指定しておき、そこからの相対パスを指定する方法もある。その場合、サイズオーバーに対するエラーページのファイルのパス名には、

ErrorPageBase パラメタのディレクトリパス と
SizeErrorPage パラメタの相対パス

を連結したものが使われる。

指定可能な値

ErrorPageBase パラメタが指定されていない場合

<ドライブ文字>:\<ディレクトリパス>...\<ファイル名>

ErrorPageBase パラメタが指定されている場合

<ディレクトリパス>...\<ファイル名> または
<ファイル名>

省略時解釈値 「共通設定」の SizeErrorPage の値

例 SizeErrorPage=c:\inetpub\wwwroot\error_messages\site_1\size_error.htm

6.3.3.8 ErrorPageBase エラーページの基準ディレクトリ

データタイプ REG_SZ

説明

カスタムエラーページのパス名を指定する際の基準となるディレクトリパス。EncodeErrorPageパラメタおよびSizeErrorPageパラメタに相対パスを指定する場合に使用する。

指定可能な値

<ドライブ文字>:\<ディレクトリパス>...\<ディレクトリパス> または
<ドライブ文字>:\<ディレクトリパス>...

省略時解釈値 「共通設定」の ErrorPageBase の値

例 ErrorPageBase=c:\inetpub\wwwroot\error_messages\site_1

6.4 パターンマッチルール

個別設定の中には Rule00 ~ Rule99 の最大100個のパターンマッチルールを記述することができます。

記述するパターンマッチルールのルール番号は連続した番号でなくても構いません。たとえば次のようなとびとびの値を使うことができます。

Rule03 , Rule10 , Rule97

ただし、とびとびの番号を使用すると若干余分にコンピュータのメモリを消費するので、むやみに大きな番号は使わないようお勧めします。

6.4.1 動作とマッチパターン

一つのパターンマッチルールは、次のような 1 種類の「動作」と 4 種類の「マッチパターン」から構成されます。

パターンにマッチしたときの動作

HTTPリクエストを受入れるか拒絶するか。拒絶する場合にカスタムエラーページを表示することもできる。

HTTP リクエストのメソッドに対するマッチパターン

このパターンを指定することにより、特定のメソッドをもつHTTPリクエストのみを許容したり、特定のメソッドを持つHTTPリクエストを排除することができる。

URL のパス部分に対するマッチパターン

このパターンを指定することにより、URLのパス部分に特定の文字列が含まれていたり特定のパターンにマッチするときルールの動作を有効にすることができる。

URLのパス部分に対するマッチパターンは一つのパターンマッチルールにつき一つ指定できる。

URL のクエリストリング部分全体に対するマッチパターン

このパターンを指定することにより、URLのクエリストリング部分に特定の文字列が含まれていたり特定のパターンにマッチするとき、ルールの動作を有効にすることができる。

URLのクエリストリング部分全体に対するマッチパターンは一つのパターンマッチルールにつき一つ指定できる。

URL のクエリストリングの中の「名前 = 値」対に対するマッチパターン

このパターンを指定することにより、URLのクエリストリング部分の & で区切られた「名前 = 値」対のうち少なくとも一つが特定の文字列を含んでいたり特定のパターンにマッチするとき、ルールの動作を有効にすることができる。

「名前 = 値」対に対するマッチパターンは一つのパターンマッチルールの中で複数個(00 ~ 99 の最大 100 個) 指定することができる。

4 種類のマッチパターンは上記のうち必要なもののみを記述すれば良いようになっています。

一つのパターンマッチルールの中で上記のマッチパターンを複数指定した場合は、HTTPリクエストの該当部分の全てが指定パターンにマッチしたときにはじめてそのルールにマッチしたと見なさ

れます。

マッチパターンを何も記述しなかったとき、そのパターンマッチルールは全てのHTTPリクエストにマッチします。

6.4.2 パターンマッチルールの評価順序

パターンマッチルールは、ルール番号の小さい順にパターン照合が行われ、マッチするルールがあれば最初にマッチしたルールに書かれている動作 HTTPリクエストの許容あるいは排除 が行われます。

一つでもパターンにマッチするルールが見つかり、それ以上ルールのパターンマッチは行われません。

一つのルールの中には複数の項目からなる複合条件でマッチパターンを指定できます。その場合、そのルールに書かれている複数のパターン全てがHTTPリクエストとマッチした場合にそのルールの照合条件にマッチしたと見なされ、そのルールの動作が行われます。

6.4.3 パターンマッチルールのレジストリ記述

パターンマッチルールは次のようなレジストリ項目で記述します。

パターンにマッチしたときの動作

Rule<ルール番号>_Action ルールの動作

照合パターンの指定（必要なもののみを指定する。複数指定可）

Rule<ルール番号>_Method HTTPメソッドのパターン

Rule<ルール番号>_Path パス名のパターン

Rule<ルール番号>_Qs クエリストリングのパターン

Rule<ルール番号>_QsItem<項目パターン番号> 「名前=値」対のパターン

6.4.3.1 Rule<ルール番号>_Action ルールの動作

データタイプ REG_SZ

説明

パターンマッチルールにマッチしたときにそのHTTPリクエストを許容するか排除するかの指定。次のいずれか。「accept」と「reject」の綴りでは大文字小文字は区別されない。

- “accept” （許容）
- “reject” （排除、デフォルト動作）
- カスタムエラーページの物理パス（排除、カスタムエラーページ表示）

例 Rule03_Action=reject

Rule03_Action=c:\inetpub\wwwroot\error_messages\site_1\error1.htm

6.4.3.2 Rule< ルール番号 >_Method HTTP メソッドのパターン

データタイプ REG_SZ

説明

HTTPリクエストのメソッドに対するマッチパターンの指定。HTTPリクエストのメソッドは本来大文字であるが、このパラメタで小文字の綴りを指定してもマッチする。

例 Rule03_Method=put

メソッドが「PUT」のHTTPリクエストであるという条件。

6.4.3.3 Rule< ルール番号 >_Path パス名のパターン

データタイプ REG_SZ

説明

URLのパス部分に対するマッチパターンの指定。

例 Rule03_Path=*.gif

パス部分が .gif .GIF .gif 等で終わるという条件。

6.4.3.4 Rule< ルール番号 >_Qs クエリストリングのパターン

データタイプ REG_SZ

説明

URLのクエリストリング部分全体に対するマッチパターンの指定。

例 Rule03_Qs=*clear*

クエリストリング部分に clear という文字列を含むという条件。

6.4.3.5 Rule< ルール番号 >_QsItem< 項目パターン番号 > 「名前 = 値」対のパターン

データタイプ REG_SZ

説明

URLのクエリストリングの中の & で区切られた「名前=値」対のどれか一つに対するマッチパターンの指定。

例 Rule03_QsItem07=Debug=Yes

“ Debug=Yes ” という「名前 = 値」対が一つでも含まれているという条件

6.4.4 マッチパターン

マッチパターンは次のような文字の組み合わせで記述します。

*

ワイルドカード。照合対象の0文字以上の任意の文字列にマッチさせたい箇所に使う。たとえば、「gif という文字列を含む」という意味のパターンは「*gif*」のように書く。

アルファベット (A-Z a-z)

アルファベットの綴りにマッチさせたい箇所に使う。パターンに記述したアルファベットは照合対象の綴りが同じアルファベットであるなら大文字でも小文字でもマッチする。たとえば、パターン「gif」は、gifにも、GIFにも、gIfにも、またそれ以外の大文字小文字の組み合わせ全て対してもマッチする。

%nn (nn は 00 以外の十六進数)

特定の文字コードにマッチさせたい箇所に使う。たとえば、パターン「%2a」は文字 * にマッチする。なお、パターン「%41」は文字 A にマッチするが文字 a にはマッチしない。

上記以外の文字

その文字そのものにマッチする。

補足

マッチパターンの実装にあたっては、照合対象文字列に指定したパターンが「含まれる」のではなく、照合対象文字列全体が指定したパターン「そのものにマッチする」という記述のスタイルを選択しています。それは、前者だと対象文字列全体にマッチするパターンを、

^パターン\$

のように「先頭にマッチ」「末尾にマッチ」というメタキャラクタを導入して記述しなければならないのに対し、後者では、

パターン

と書くだけでそれが実現できるからです。その代わり「特定の文字列を含む」というパターンは、

文字列

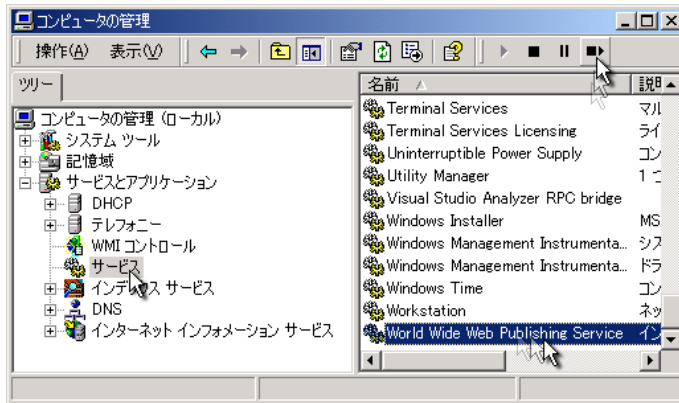
と書く必要が生じています。

7. パラメタ変更の反映

レジストリに記述したパラメタの変更を guard3 1.26 に反映させるためには、従来のバージョンと同様、WWWあるいはIIS全体のサービスプロセスを一旦停止させた上で再開する必要があります。

7.1 Windows 2000 の IIS 5.0 の場合

「コンピュータの管理」の「サービス」の「World Wide Web Publishing Service」を再起動させてください。



7.2 Windows NT 4.0 の IIS 4.0 の場合

まず、コントロールパネルの「サービス」の中で「IIS Admin Service」を停止させます。このとき、IIS Admin Service の下位の「World Wide Web Publishing Service」なども一緒に停止させるかと聞いてくるので OK と答えます。

続いて、同じくコントロールパネル「サービス」の「World Wide Web Publishing Service」を起動します。このとき IIS Admin Service も自動で起動されます。

FTPなど、IISの中のサービスでWWW以外に稼働させていたものがあればそのサービスも起動してください。

以上