

GUARDIANSUITE

検査サーバー 利用の手引き

～ WEBGUARDIAN V3.6 編(ウェブ) ～

- * *GUARDIANSUITE* は、キヤノン IT ソリューションズ株式会社の登録商標です。
- * *GUARDIANWALL* は、キヤノン IT ソリューションズ株式会社の登録商標です。
- * *WEBGUARDIAN* は、キヤノン IT ソリューションズ株式会社の登録商標です。
- * Sun, Sun Microsystems は、Sun Microsystems, Inc. の商標または登録商標です。
- * SunOS, Solaris は、Sun Microsystems, Inc. の登録商標です。
- * SPARC は、SPARC International, Inc. の登録商標です。
- * Linux は、Linus Torvalds の登録商標です。
- * Netscape, Netscape Navigator, N ロゴ及び操舵輪のロゴは、米国及びその他の諸国の Netscape Communications Corporation 社の登録商標です。
- * Microsoft, the Microsoft Internet Explorer ロゴは、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
- * Internet Explorer は、米国 Microsoft Corporation の商品名称です。
- * Microsoft Office, Microsoft Word, Microsoft Excel は、米国及びその他の国における米国 Microsoft Corporation の商品名称です。
- * Microsoft PowerPoint は、米国及びその他の国における米国 Microsoft Corporation の登録商標です。
- * Adobe, Adobe Acrobat は、Adobe Systems Incorporated (アドビシステムズ社) の商標です。
- * 一太郎は、株式会社ジャストシステムの登録商標です。
- * Sendmail は、米国 Sendmail, Inc. の登録商標です。
- * その他本マニュアル中に記載されている社名、商品名は、各社の商標または登録商標です。

Copyright © 2011 Canon IT Solutions Inc.

本マニュアルの一部あるいは全部について、キヤノン IT ソリューションズ株式会社の事前の承認なく、複製、転載することを禁止します。

<http://www.canon-its.co.jp/>

2011-May-25 *GUARDIANSUITE* V4.5

GUARDIANWALL V7.4

WEBGUARDIAN V3.6

MEMO

はじめに

この度は、GUARDIANSUITEをご導入いただき誠にありがとうございます。

本章では本マニュアル『検査サーバー 利用の手引き ～ WEBGUARDIAN V3.6 編（ウェブ）～』の使い方について説明します。

また、本システムの導入方法については、『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』を、詳細な操作方法については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』をご覧ください。

(1) 本マニュアルの使い方

本マニュアルは、GUARDIANSUITEのウェブ部分（WEBGUARDIAN）の概要と詳細内容について説明します。情報管理者は、必ずこのマニュアルをお読みいただいたうえで、本システムの運用、設定を行ってください。

以下に、各章の概要を説明します。

1 概要（10ページ）

WEBGUARDIANの機能、システムイメージ、概要について説明します。

2 運用（16ページ）

WEBGUARDIANの運用方法について説明します。

3 ポリシー管理機能（34ページ）

ポリシー管理機能について説明します。

4 グループ管理（56ページ）

グループ管理機能について説明します。

5 プロキシ設定（64ページ）

プロキシ設定について説明します。

6 仕様（80ページ）

各設定ファイルの詳細仕様について説明します。

7 サポートツール（104ページ）

本システムが提供するサポートツールの使用方法について説明します。

8 トラブルシューティング（112ページ）

WEBGUARDIANのトラブルへの対処方法を説明します。

(2) 表記ルールについて

本マニュアルで使用している表記ルールについて説明します。



書体について

画面やファイル中のテキストは枠で囲い、以下のような書体で記述します。

書体	意味	使用例
あいうABCabc123	画面上のコンピュータ出力	GUARDIANSUITE インストーラ Linux版
あいうABCabc123	ユーザーが入力する文字	# mv /usr/sbin/sendmail /usr/sbin/sendmail.OFF
あ いうABC abc 123	コマンド行の可変部分	# rm filename # rm <ファイル>
あいうABCabc123	ファイルやシステム中のテキスト	Top 5 合計メール数順 (total: 64)

マークについて

本システムを安全にご使用いただくため、守っていただきたい事項に次のマークを使用しています。必ずお読みください。

マーク	意味
	注意： システムの停止やデータの消去など、重大なトラブルを発生させる可能性があります。十分注意してください。
	情報： 操作や運用に関連した情報です。参考にお読みください。

記号について

本マニュアルでは以下のような記号を使用しています。

記号	意味	使用例
『』	参照するマニュアル名を表します。 ※ただし、同じマニュアル内では省略します。	<ul style="list-style-type: none"> ・『利用の手引き』の「1-1 機能」(22ページ)をご参照ください。 ・「新規インストール」を選択します。 ・MTA (Mail Transfer Agent)
「」	参照する章、節の番号と名称、または、システム内のメニュー、項目、値、強調する語等を表します。	
()	ページ番号、または、補足内容を表します。	
[]	システム中のボタン名、リンク名等を表します。	・ [設定] ボタンをクリックします。
[]	システム内のトップレベルメニュー、タブメニュー名を表します。	・ 「状況確認」 - 【稼動状況】
\	画面例などで、テキストがページ行幅を超える場合に、継続を示します。	・ Enter your domain name \ [your.domain]: example.co.jp

設定例について

本マニュアルに記載されているIPアドレスやドメイン名、URLアドレスなどの設定例は、説明のためのものです。実際はそれぞれの環境に合わせた設定を行ってください。

(3) 管理画面名称

本システムは、ウェブブラウザ経由で操作できます。ウェブブラウザより本システムにアクセスした際、表示される画面を管理画面と総称します。

本節では各管理画面の名称について説明します。



ログイン画面：

ウェブブラウザより本システムにアクセスすると、この画面が表示されます。この画面から、各利用者別にログインします。

メニューフレーム:

各利用者が行うことのできる操作が表示されます。

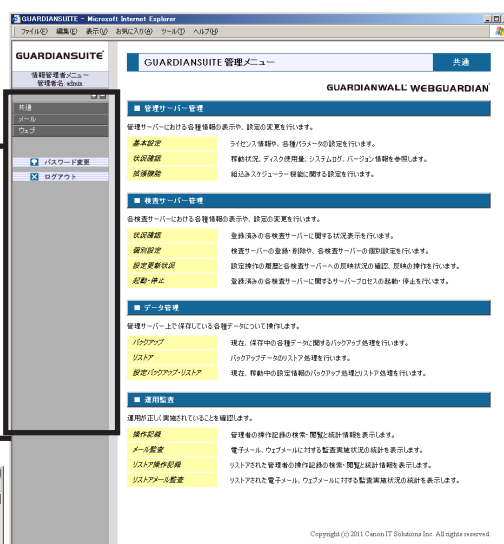
利用者別トップページ:

ログインすると、各利用者別のトップページが表示されます。



表示（設定） / クリアボタン：

操作を実行、もしくはクリアするボタンは主に
操作画面下中央に配置しています。



操作画面：

各操作を行います。

MEMO

目次

1 概要	10
1-1 目的	10
1-2 機能概要	11
1-3 個人情報検査機能	13
2 運用	16
2-1 プロキシ独自認証機能	16
2-2 シングルサインオン(NTLM認証)機能	23
2-3 ポリシー例	27
2-4 運用例	28
2-5 URLDB更新時期メール通知設定	29
3 ポリシー管理機能	34
3-1 ポリシー管理概要	34
3-2 アクセス制御処理の流れ	35
3-3 規制ルール	36
3-4 例外ルール	43
3-5 グループ	45
3-6 時間・曜日	46
3-7 URLグループ	46
3-8 MIMEタイプ	49
3-9 キーワード	49
3-10 ファイルタイプ	50
3-11 ブロック画面	52
3-12 オーバーライドコード	53
4 グループ管理	56
4-1 グループ管理機能概要	56
4-2 グループの登録	57
4-3 グループ管理	58
4-4 検索条件グループ	60
4-5 規制ルール/例外ルール	61
4-6 システム設定	62

5 プロキシ設定	64
5-1 基本設定	64
5-2 検査機能設定	69
5-3 ユーザー認証設定	71
5-4 メール通知設定	74
5-5 キャッシュ設定	76
5-6 プロキシ多段構成時の設定	78
6 仕様	80
6-1 日本語検査機能仕様	80
6-2 プロキシ設定ファイル	89
6-3 ポリシー設定ファイル	99
6-4 外部送信データのアーカイブ処理	103
7 サポートツール	104
7-1 rescue.pl	104
7-2 sanity_chk.pl	106
7-3 watch.pl	107
7-4 queue_mgr.php	109
8 トラブルシューティング	112

1 概要

本章では、WEBGUARDIANが提供するサービスと機能についての概要を説明します。

1-1 目的

WEBGUARDIANは、組織ネットワーク管理に関する次のようなご要望にお応えすることができます。

- ・組織内のユーザーが許可されていない情報をウェブ経由で組織外へ送信するのを防ぎたい。
- ・ユーザーがアクセス可能なURLに制限を掛けたい。
- ・利用者をグループ化して、グループ単位でアクセス制限を適用したい。
- ・ワープロデータや表データなどファイルタイプによって送信を制限したい。
- ・送信されるデータに好ましくないキーワードが入っていないか検査したい。
- ・個人情報を含むファイルの送出を防止したい。
- ・GUARDIANWALLで検査できないウェブメールに対してGUARDIANWALLと同等のアクセス制限を掛けたい。

WEBGUARDIANは、ユーザーが組織外へ送信するウェブリクエストに対して柔軟できめ細かなアクセス制限を適用することができます。

- ・ユーザーのウェブアクセスに関する記録を全て保存しておきたい。
- ・好ましくないウェブアクセスが発生していないかどうか、アクセス記録からトレースしたい。
- ・組織内のユーザーのウェブ利用に関する統計データを確認したい。

WEBGUARDIANは、ウェブアクセスに関する詳細なデータを全てのトランザクションに対して記録することができます。WEBGUARDIANが記録するログデータを分析すれば、単純なアクセスログではトレース不可能な内容まで把握することができます。

1-2 機能概要

以下に *WEBGUARDIAN* の主な機能の概要を示します。

(1) プロキシ機能

http、https、ftp (ftp over http) 対応のプロキシサーバーとして動作します。

(2) ユーザー認証機能

ユーザー認証機能に LDAP 認証、*WEBGUARDIAN* 独自認証、シングルサインオン (NTLM 認証) を使用することができます。

これによりユーザー単位のアクセス記録やアクセス制御が行えます。

詳細については、「5-3 ユーザー認証設定」(71 ページ) をご参照ください。

(3) アクセス制御機能

認証名、IP アドレス、URL、ユーザーエージェント名、送信メッセージボディに関する条件の組合せに対してアクセス制御を実施することが可能です。

詳細については、「3-2 アクセス制御処理の流れ」(35 ページ) をご参照ください。

(4) キーワード検索

検索エンジンに入力キーなどになる URL パラメータ値やウェブメールの送信内容や添付ファイルにあたるメッセージボディに対してキーワード検索が可能です。また、単なるテキストデータ以外のワープロファイルなどのアプリケーションデータにも対応しています。

詳細については、「3-9 キーワード」(49 ページ) をご参照ください。

(5) 個人情報検査

氏名、住所、電話番号など個人を特定する情報の組合せを含んでいるかどうかを検査することができます。

詳細については、「1-3 個人情報検査機能」(13 ページ) をご参照ください。

(6) 多段階の利用制限機能

規制条件に該当したアクセスに対して、記録、禁止、他 URL へのリダイレクトなど複数のアクションを適用することが可能です。

詳細については、「3-3 規制ルール」(36 ページ) をご参照ください。

(7) 管理者へのメール通知機能

規制条件に該当したアクセスに対して、ユーザーへの応答以外にも同時に規制対象アクセスがあったことを管理者へ電子メールで知らせることも可能です。

詳細については、「5-4 メール通知設定」(74 ページ) をご参照ください。

(8) 不正アクセストレース機能

WEBGUARDIAN経由でアクセスした内容は、時刻やリクエストURLなどのヘッダー情報に加えてメッセージボディの内容も完全に記録されます。

これらのアクセス記録から不正と判断されるアクセスを事後的にトレースすることが可能になります。

(9) ウェブメール閲覧機能

組み込み定義されたウェブメールサイトへのメール送信記録を閲覧することができます。メッセージ本文やサブジェクト、また添付ファイル内容も確認することが可能です。

(10) 検索エンジン入力キー閲覧機能

組み込み定義された検索エンジンサイトへの入力キーワードを閲覧することができます。またユーザーの認証名やIPアドレスで閲覧対象を絞り込みすることも可能です。

(11) インスタントメッセージ閲覧機能

組み込み定義されたインスタントメッセージングサービスへのメッセージ送信記録を閲覧することができます。送信されたメッセージを確認することも可能です。

(12) ソーシャルウェブ閲覧機能

組み込み定義されたソーシャルウェブサービスへの送信記録を閲覧することができます。送信された内容、また添付ファイル内容も確認することが可能です。

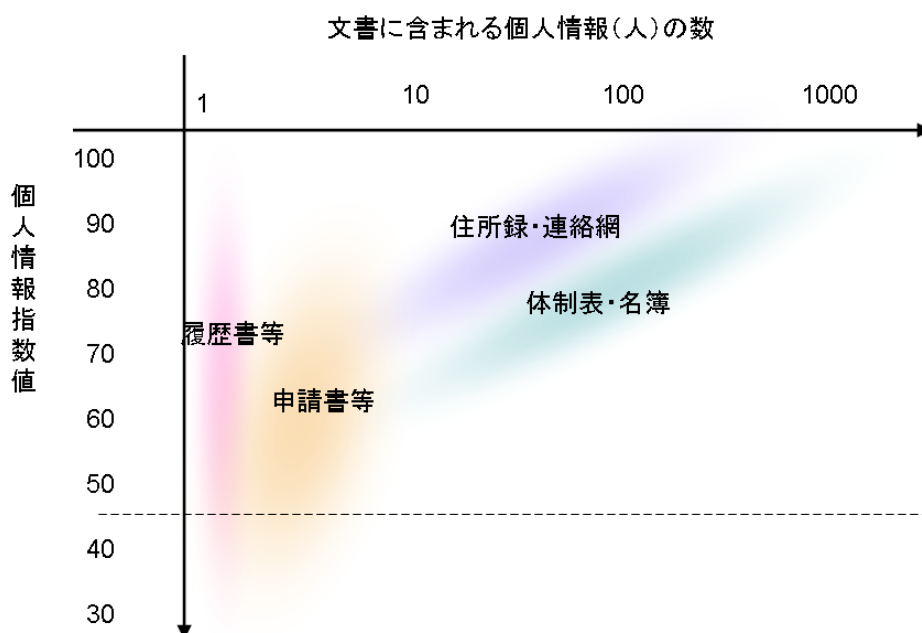
(13) 複数台構成対応

ウェブアクセス数が非常に多い組織などでは、WEBGUARDIANを複数台で構成することが可能です。このような場合でも1つの管理サーバーから一括して分散構成されたWEBGUARDIANを管理することができます。

1-3 個人情報検査機能

(1) 概要

キーワード検査対象となる添付ファイル中に個人情報を含むかどうかを判定します。住所録や名簿のような個人情報を多数含む文書と履歴書や申請書のような個人を特定するための属性情報を多数含む文書をどちらも単一の指標で判定するので簡単な条件設定で個人情報を含む文書ファイルの判定が可能です。



(2) 仕組み

個人情報の基本項目となる氏名、住所、組織名情報はあらかじめ登録された辞書と比較することにより検出します。また、電話番号、メールアドレス、クレジットカード番号などはパターンマッチにより検出します。これらの検出位置の、相互の近さなどから氏名とその他の情報の組合せとして、個人情報を判断します。検出した個人情報の件数、検出した属性情報の項目数などから統計的な処理を行い総合指数として数値化します。

(3) 仕様

以下の項目を、個人を特定するための属性情報として検査対象とします。

- ・氏名（漢字、ひらがな、カタカナ）
- ・住所 / 郵便番号
- ・電話番号
- ・メールアドレス
- ・生年月日 / 年齢
- ・組織名
- ・クレジットカード番号

氏名、住所、組織名を約7万件辞書に登録しています。総合指数は0から100までの値を示し、より多くの個人情報を含んでいる文書や個人を特定するための属性情報がより揃っている文書がより高い数値を示します。



- ・本機能は個人情報の漏洩を防止することを完全に保証するものではありません。
 - ・検査対象のファイル形式、バージョンによっては検査できないものがあります。
 - ・辞書に登録されていない氏名、住所、組織名は検出できません。検査結果の個人情報件数については実際の件数とは異なる場合があります。
 - ・未公開あるいは公開可能な個人情報であるかは判定できません。
 - ・事業者ごとに保護対象とする個人情報の定義は異なります。本指標値を個人情報保護のための目安としてご利用ください。
 - ・特許出願中。
-

2 運用

本章では、WEBGUARDIANの運用方法について説明します。

2-1 プロキシ独自認証機能

WEBGUARDIANではプロキシ認証によって、認証名からリクエストを行っているユーザーを特定することができます。

LDAP認証ではLDAPサーバー、独自認証ではWEBGUARDIANが作成する独自のデータベースを認証データベースとして使用します。

独自認証ご利用時、パスワード有効期限、初期パスワード変更機能を有効にすると、定期的にユーザーにパスワードの変更を促すことができます。本章ではこれらの機能を有効にした場合の動作仕様について説明します。

(1) 注意事項

- ・管理サーバーをアクティブ/スタンバイ構成で運用されている場合、スタンバイ機をアクティブ機に切り替える際、ウェブ検査サーバーを再起動してください。
- ・管理サーバーをアクティブ/スタンバイ構成で運用されている場合、スタンバイ機をアクティブ機に切り替えた後、パスワード変更サーバーを起動する必要があります。パスワード変更サーバーの起動方法については、「(3) パスワード変更サーバー」-「(a) サーバーの起動・停止」をご参照ください。また、パスワード変更サーバーをSSL対応にさせるためには、「/opt/Guardian/Admin/SSL」という空ファイルを作成する必要があります。パスワード変更サーバーのSSL対応については、「(3) パスワード変更サーバー」-「(d) サーバー設定の変更方法」をご参照ください。

(2) ユーザーによるパスワード変更

パスワード有効期限を設定している場合、あるいは初期パスワード変更機能が「オン」に設定されている場合、ユーザーはパスワードを変更する必要があります。

(a) パスワード変更通知

プロキシ認証時にユーザーが入力したパスワードが有効期限切れであった場合、以下の画面を表示しユーザーにパスワード変更を促します。通知画面の表示は、パスワード変更後より指定された日数が経過した翌日のアクセス時になります。

パスワード変更通知

パスワードの有効期限が切れています。
以下のボタンより、新しいパスワードに変更してください。

[パスワードの変更](#)

Copyright (c) 2011 Canon IT Solutions Inc. All rights reserved.

また、プロキシ認証時にユーザーが入力したパスワードが管理者により登録された初期値であった場合、以下の画面を表示しユーザーにパスワード変更を促します。

パスワード変更通知

パスワードは初期設定値です。
以下のボタンより、新しいパスワードに変更してください。

[パスワードの変更](#)

Copyright (c) 2011 Canon IT Solutions Inc. All rights reserved.

(b) パスワード変更

パスワード変更通知画面の[パスワードの変更]ボタンをクリックすると以下のパスワード変更画面が表示されます。各設定項目を入力後[更新]ボタンをクリックします。

パスワード変更	ウェブ
<small>認証ユーザー test のパスワードを変更します。 以下のフォームに、古いパスワードと新しいパスワードを入力してください。</small>	
旧パスワード	<input type="password" value="....."/>
新規パスワード	<input type="password" value="....."/>
新規パスワード(再入力)	<input type="password" value="....."/>
クリア 更新	

Copyright (c) 2011 Canon IT Solutions Inc. All rights reserved.



サーバーが高負荷な状態にあり、2分間経過してもパスワード変更が完了しない場合はタイムアウトが発生します。「/opt/Guardian/Admin/etc/admin/admin.conf」の[CGI]セクションに以下の設定を記述することで、タイムアウト時間を変更することができます。

例) タイムアウト時間を 60 秒に変更する場合

```
WebAuthChgPwTimeOut = 60
```

数値は 0 以上 7200 以下の整数を指定することができます。

(c) 操作ログの確認

ユーザーがパスワードを変更すると、操作ログがデータベースに記録されます。これらのログは操作ログ閲覧画面で、以下の検索条件を指定することで確認することができます。操作ログの検索、閲覧方法の詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUADIAN 共通 ~』の「3-2-4-1 操作記録」をご参照ください。

・ 検索条件 1

区分 1	検査サーバー
区分 2	ウェブ
区分 3	共通
区分 4	運用
区分 5	ユーザアカウント
区分 6	パスワード変更

・ 検索条件 2

ターゲットへ「認証名」を指定する。

(3) パスワード変更サーバー

プロキシ独自認証が有効時、ユーザーによるパスワード変更を受け付けるための専用サーバーを管理サーバーと同一の筐体で起動させます。

(a) サーバーの起動・停止方法

ユーザー認証設定画面で以下の設定を行った場合に自動で起動されます。それ以外
の設定を行った場合は停止されます。ユーザー認証設定の詳細については、『管理
サーバー 利用の手引き ~ GUARDIANWALL、WEBGUADIAN 共通 ~』の「3-4-
3-2 ユーザー認証設定」(319 ページ)をご参照ください。

[基本設定]	
プロキシ認証	オン
認証方式	独自認証
[独自認証設定]	
パスワード有効期限	1 日以上
あるいは	
初期パスワード変更機能	オン

また、手動で行う場合の方法を以下に示します。

・起動する場合

```
#/etc/init.d/Guardian.pub start
```

・停止させる場合

```
#/etc/init.d/Guardian.pub stop
```

(b) サーバーの稼働状況確認

管理画面より専用サーバーの稼働状況を確認することができます。起動している場合は、プロセス欄に「httpd -f/opt/Guardian/Admin/public/conf/httpd.conf」と表示されているプロセスを確認することができます。また、スケジューラーにて「稼働状況レポート」を設定することで、サービスから送信されるレポートからも確認することができます。

稼働状況確認の画面詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUADIAN 共通 ~』の「3-2-1-2 状況確認」(50 ページ)を、スケジューラーに関する詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUADIAN 共通 ~』の「3-2-1-3 拡張機能」(54 ページ)をご参照ください。

(c) サーバーが使用するポート番号

専用サーバーが使用するポートはデフォルトで「8800」(SSL利用時は「4443」)です。これらのポートは変更可能です。設定方法については、後述の「(d) サーバーの設定変更」をご参照ください。



WEBGUARDIANをプロキシとしてサーバーへアクセスする場合、WEBGUARDIANによる検査対象外となるため、各種ログは出力されません。

(d) サーバー設定の変更方法**[1] ポート番号を変更する場合**

ポート番号「8800」は変更可能です。変更する場合は、管理サーバー内で以下の手順で設定を行ってください。

専用サーバーを停止します。

```
#/etc/init.d/Guardian.pub stop
```

専用サーバー設定ファイル「/opt/Guardian/Admin/public/conf/httpd.conf」を編集します。

(下記は「8888」へ変更する場合の例)

```
Port 8888

<IfDefine SSL>
Listen 8888
Listen 4443
</IfDefine>
```

専用サーバーを起動します。

```
#/etc/init.d/Guardian.pub start
```

検査サーバー設定ファイル「/opt/Guardian/Admin/etc/wg/httpd.conf」に以下設定を追記します。

```
WGAAuthAdminPort 8888
```

検査サーバーと設定ファイルを同期させます。

```
#/opt/Guardian/Admin/support/pushWebWG -r httpd
```

[2] SSLでサーバーへアクセスする場合

SSLでパスワード変更画面へアクセスすることが可能です。SSLを使用する場合は、以下の手順で設定を行ってください。

検査サーバーのSSL 接続許可ポートへポート番号「4443」を設定する。

設定方法の詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「3-2-2-2 個別設定」(73ページ)をご参照ください。

専用サーバーを停止させます。

```
#/etc/init.d/Guardian.pub stop
```

/opt/Guardian/Admin ディレクトリへ移動します。

```
#cd /opt/Guardian/Admin
```

SSL ファイルを作成します。

```
#touch SSL
```

専用サーバーを起動させます。

```
#/etc/init.d/Guardian.pub start
```

検査サーバー設定ファイル「/opt/Guardian/Admin/etc/wg/httpd.conf」に以下の設定を記述します。

```
WGAAuthChangePasswdSSL On
```

検査サーバーと設定ファイルを同期させます。

```
#/opt/Guardian/Admin/support/pushWebWG -r httpd
```

[3] SSL通信時に使用するポート番号を変更する場合

SSLでパスワード変更画面へアクセスする際に使用するポート番号を変更することができます。

ポート番号を変更する場合は、以下の手順で設定を行ってください。

(下記は「4444」へ変更する場合の例)

検査サーバーのSSL接続許可ポートへポート番号「4444」を設定する。

設定方法の詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「3-2-2-2 個別設定」(73ページ)をご参照ください。
専用サーバーを停止します。

```
#/etc/init.d/Guardian.pub stop
```

専用サーバー設定ファイル「/opt/Guardian/Admin/public/conf/httpd.conf」を編集します。

```
Port 8800

<IfDefine SSL>
Listen 8800
Listen 4444
</IfDefine>
```

```
<VirtualHost _default_:4444>
```

専用サーバーを起動します。

```
#/etc/init.d/Guardian.pub start
```

検査サーバー設定ファイル「/opt/Guardian/Admin/etc/wg/httpd.conf」に以下設定を追記します。

```
WGAAuthChangePasswdSSL On
WGAAuthAdminPortSSL 4444
```

検査サーバーと設定ファイルを同期させます。

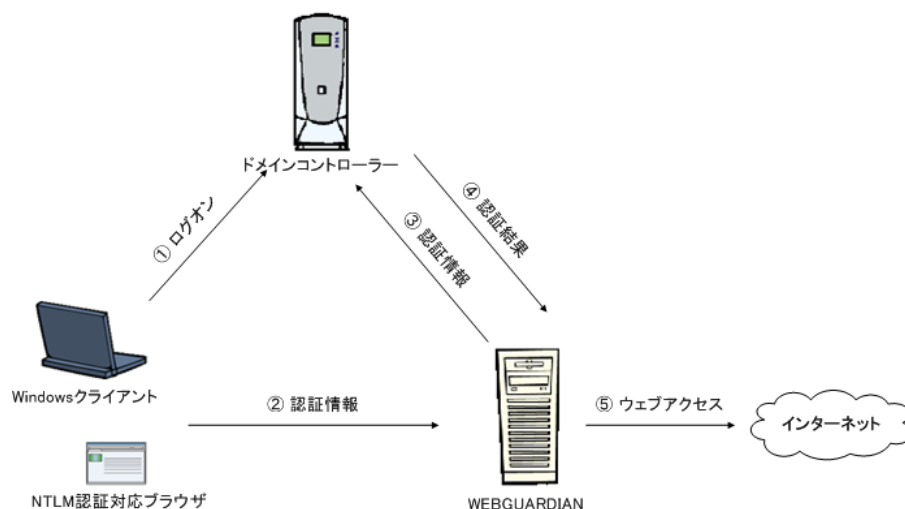
```
#/opt/Guardian/Admin/support/pushWebWG -r httpd
```

2-2 シングルサインオン(NTLM認証)機能

WEBGUARDIANではプロキシ認証にNTLM認証を使用することができます。

NTLM認証ではドメインコントローラを認証データベースとして使用します。WindowsクライアントからWEBGUARDIANに送信された認証情報をドメインコントローラに問い合わせ、認証に成功したユーザーにのみウェブアクセスを許可します。

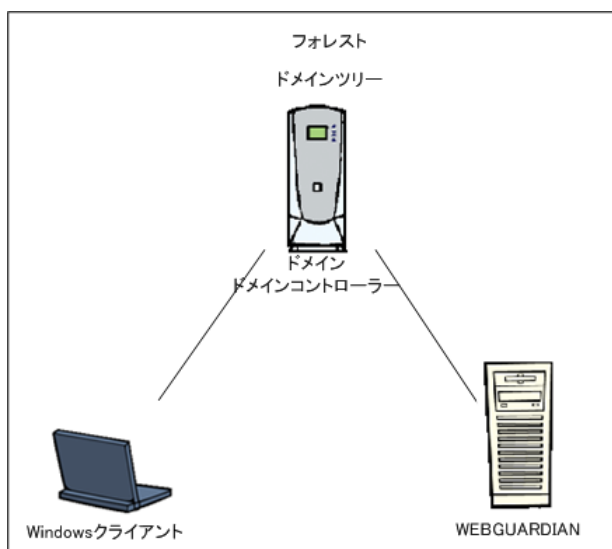
また、Windowsドメインにログオン済みのWindowsクライアントからは、ウェブブラウザがWEBGUARDIANに自動的に認証情報を送信するため、再度認証情報を入力することなくシングルサインオンによりウェブアクセスを行うことができます。



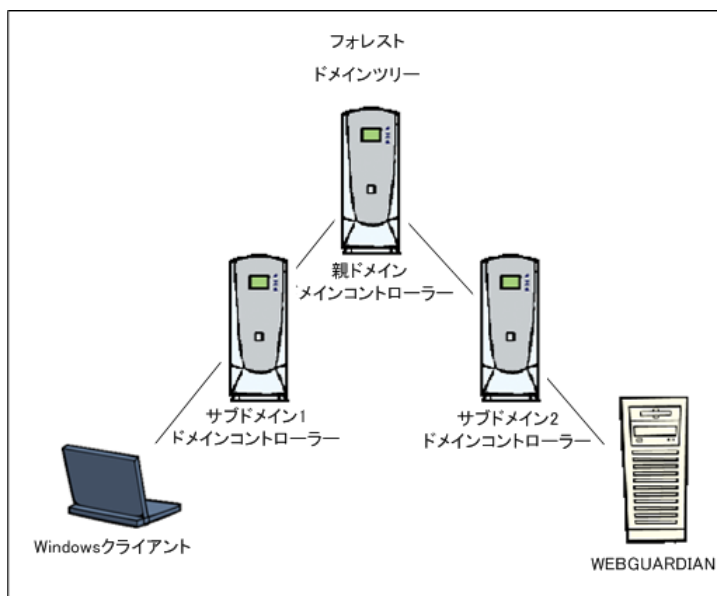
(1) NTLM認証が可能なドメイン構成

WEBGUARDIANは以下の構成でNTLM認証を行うことができます。

(a) 同じドメインにクライアントとWEBGUARDIANを配置する構成



(b) 同じドメインツリーにクライアントと WEBGUARDIANを配置する構成

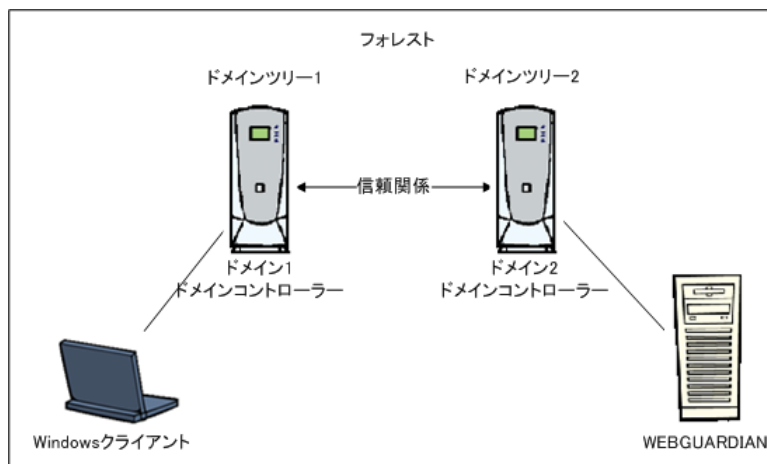


同じドメインツリーのドメインには自動的に推移的な信頼関係が作成されるため、クライアントと WEBGUARDIAN が所属するドメイン間に信頼関係を結ばなくても NTLM 認証が可能です。

ただし、クライアントと WEBGUARDIAN を配置するドメインの階層が深くなる場合は、それぞれが所属するドメイン間にショートカットの信頼関係を作成した方が認証の通信回数を減らすことができます。

図の構成では WEBGUARDIAN、サブドメイン2のドメインコントローラ、親ドメインのドメインコントローラ、サブドメイン1のドメインコントローラの順に認証の問い合わせが行われるため、サブドメイン1とサブドメイン2の間でショートカットの信頼関係を結んだ方が認証の通信回数を減らすことができます。

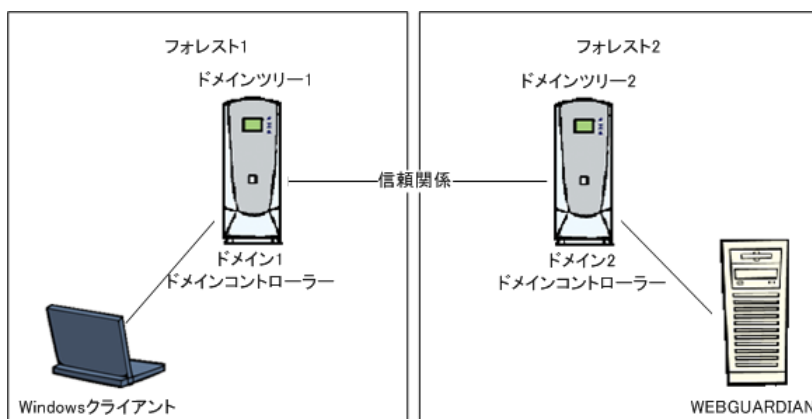
- (c) 同じフォレストの異なるドメインツリーにクライアントとWEBGUARDIANを配置する構成



同じフォレストのドメインには自動的に推移的な信頼関係が結ばれるため、クライアントとWEBGUARDIANが所属するドメイン間に信頼関係を結ばなくてもNTLM認証が可能です。

ただし、クライアントとWEBGUARDIANを配置するドメインの階層が深くなる場合は、それぞれが所属するドメイン間にショートカットの信頼関係を作成した方が認証の通信回数を減らすことができます。

- (d) 異なるフォレストにあるドメインにクライアントとWEBGUARDIANを配置する構成



異なるフォレストにあるドメインには自動的に信頼関係が結ばれません。そのため、NTLM認証を行うにはWEBGUARDIANが認証を問い合わせるドメインがクライアントの所属するドメインを信頼するように、信頼関係を作成する必要があります。

(2) 環境設定

(a) WEBGUARDIANが稼動するホストの設定

- ・WEBGUARDIANが稼動するホストで認証を問い合わせる、プライマリドメインコントローラとバックアップドメインコントローラのNetBIOSコンピュータ名に対するIPアドレスを名前解決できるように、DNSサーバーもしくはhostsファイルを設定してください。

(b) Windows クライアントの設定

- ・クライアントにはWindowsOSで稼働するNTLM認証対応ウェブブラウザを使用してください。
- ・ウェブブラウザはWEBGUARDIANに持続的接続をする必要があるため、プロキシ接続にHTTP1.1を使用するようにウェブブラウザを設定してください。
Internet Explorerでは[ツール]-[インターネットオプション]-[詳細設定]-[HTTP1.1設定]の「プロキシ接続でHTTP1.1を使用する」にチェックがあることを確認してください。
Firefoxではアドレスバーに「about:config」と入力し、「network.http.proxy.version」が1.1になっていることを確認してください。
- ・WindowsクライアントでNTLMv1を使用できるように設定してください。
Windows Vistaでは、初期設定の「LAN Manager 認証レベル」が「NTLMv2 応答のみ送信する」となっていますので、「NTLM 応答のみ送信する」に変更する必要があります。

(3) 注意事項

- ・Windows 7 上で Internet Explorer 8 を使用する場合は、シングルサインオン（NTLM 認証）は、使用できません。
- ・シングルサインオン（NTLM 認証）で利用できるユーザー名は、半角英数字、半角記号「! # \$ % & ' () - . ^ _ ` { } ~」で16文字までとなります。
ユーザー名はNetBIOS通信と互換性を持たせるため16文字までとしています。
半角記号の「/ ¥ [] : ; | = , + * ? < > @ "」は、ActiveDirectoryにユーザーを登録する際に、「_」に変換されます。
- ・WEBGUARDIANの規制ルール、例外ルールの適用は認証名（ドメインユーザーのユーザー名）のみが指定可能であるため、異なるドメインに同じユーザー名のユーザーが存在する場合でも同じユーザーとして規制ルール、例外ルールが適用されますのでご注意ください。
- ・シングルサインオン（NTLM 認証）を使用している場合でも、ログの認証名にはユーザー名のみが記録され、ドメイン名は記録されません。
- ・NTLM 認証では Windows クライアントと WEBGUARDIAN の間でチャレンジ・レスポンス方式により認証を行います。Windows クライアントと WEBGUARDIAN の接続のTCPセッションが変更される度に、新しいチャレンジを変更して新たに認証処理を行います。そのため、LDAP 認証や独自認証を選択した場合よりも認証における処理負荷が高くなることが考えられます。

2-3 ポリシー例

運用にあたって、適切なインターネットアクセス管理ポリシーを確立することは重要なことです。インターネットアクセス管理ポリシーは、業種、業務形態、セキュリティ方針などによって多種多様ですが、以下にWEBGUARDIANを利用した効果的なポリシーの例を紹介します。

(1) 特定のウェブサイトへのアクセスを記録、警告する。

あきらかに業務とは関係ないと判断されるウェブサイトへのアクセスに対して警告文を応答する、または完全に遮断する。

(2) 添付ファイルの送信を検査し、内容に望ましくないキーワードが含まれる場合はアクセスを遮断する。もしくは管理者へメールで通知する。

機密データを記録したファイルをアップロードした場合などにアクセスを中断し、即座に管理者へ通知する。

(3) ウェブメールの利用を制限する。

GUARDIANWALLによるSMTP通信におけるメッセージ制御ポリシーと同じポリシーをウェブメールへも適用する。

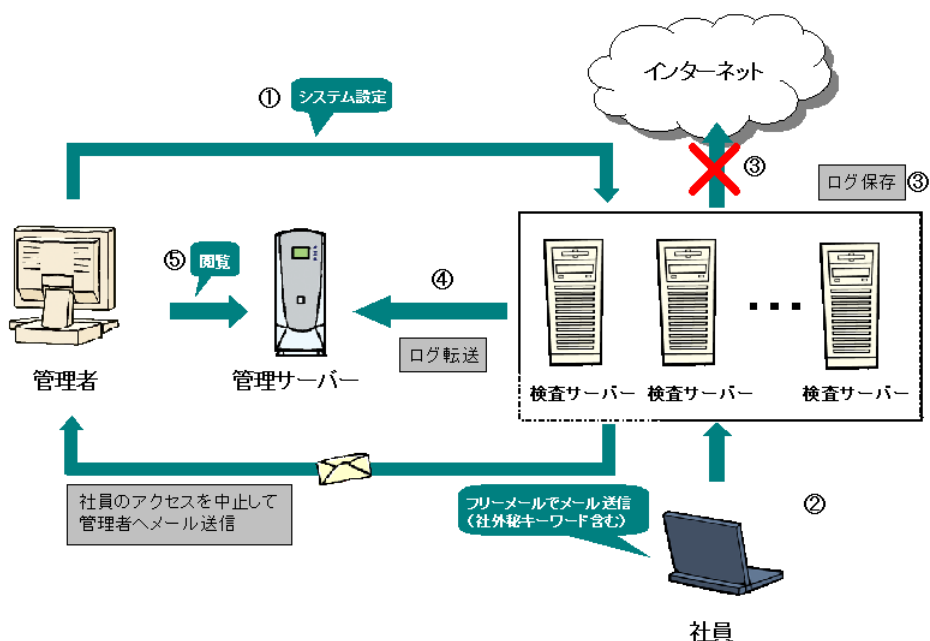
通信手段に依存しない統一的なポリシー運用を実現します。

(4) HTTPSサイトへのアクセスを監視する。

HTTPSサイトへのアクセスだけを監視することができます。HTTPSサイトへのアクセスは暗号化されているため送信内容を確認することはできませんが、秘蔵性が高いと思われる通信を行っているユーザーやサイトを特定することが可能です。

2-4 運用例

WEBGUARDIANの標準的な運用例、処理の流れは以下のとおりです。



管理者

キーワード検索条件として「社外秘」「名簿」「給与」を設定します（随時登録、変更、削除可能）。

社員

フリーメールを利用して本文に「社外秘」が含まれるメールを社外に送信しようとしています。

検査サーバー

キーワード「社外秘」を検出し以下の動作を行います。

- ・メール送信を中断
- ・管理者へキーワード検索結果通知メールを送信
- ・ログ保存

検査サーバー

管理サーバーへログの転送を行います。

管理者

管理サーバーにアクセスして、ログの閲覧を行います。

2-5 URLDB更新時期メール通知設定

URLDBのライセンス更新時期(ライセンス終了日)の指定日()前からURLDBのライセンス更新が実施されるまで、ユーザーへ電子メールで通知する機能の設定です。

ただし、評価版ライセンスの場合は対象外となります。

()メール通知日を指し、ライセンス終了日より遡った日を設定ファイルで指定します。

(1) メール通知日の設定方法

指定値には、0以上の数値指定が可能です(0はライセンス終了日当日)。

指定値には、on、offの文字指定が可能です。大文字、小文字の区別はありません。

管理サーバー上で、/opt/Guardian/Admin/etc/wg/admin.confを直接編集し、以下の設定を追加します。

日単位でメール通知したい場合の指定

複数の日を指定する場合は、カンマ「,」で区切って指定してください。

数値の指定順序に制限はありません。

例は、ライセンス終了日の1日前、15日前、30日前、60日前に通知(デフォルト設定)します。

設定例)

```
[URLDB]
NotifyUrldbTerm = 1,15,30,60
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG admin
```

期間単位でメール通知したい場合の指定

期間を指定する場合は、ハイフン「-」を指定してください。

例は、ライセンス終了日の1日前から30日前までの期間で通知します。

設定例)

```
[URLDB]
NotifyUrldbTerm = 1-30
```

と同様に検査サーバーに設定を反映する必要があります。

混合(日と期間)でメール通知したい場合の指定

例は、ライセンス終了日の1日前から30日前までの期間、40日前、60日前に通知します。

設定例)

```
[URLDB]
NotifyUrldbTerm = 1-30,40,60
```

と同様に検査サーバーに設定を反映する必要があります。

メール通知を止めたい場合の指定

offを指定すると、メールを通知しません。

設定例)

```
[URLDB]
NotifyUrldbTerm = Off
```

と同様に検査サーバーに設定を反映する必要があります。



- ・ NotifyUrldbTerm パラメータの指定がない場合、または on を指定した場合は、デフォルト設定(ライセンス終了日の1日前、15日前、30日前、60日前)でメールを通知します。
- ・ NotifyUrldbTerm パラメータに数値指定(日と期間)と on / off が、同時に指定された場合は、メールを通知しません。上記の混合は不可となります。

(2) ライセンス終了日を過ぎたメール通知の設定方法

指定値には、on、offの文字指定が可能です。大文字、小文字の区別はありません。管理サーバー上で、/opt/Guardian/Admin/etc/wg/admin.confを直接編集し、以下の設定を追加します。

ライセンス終了日を過ぎたメール通知を止めたい場合の指定

offを指定すると、メールを通知しません(デフォルト設定)。

設定例)

```
[URLDB]
NotifyUrldbTermLater = Off
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG admin
```

ライセンス終了日を過ぎたメール通知を続行したい場合の指定

on を指定すると、ライセンス終了日以降も毎日メールを通知し続けます。

設定例)

```
[URLDB]
NotifyUrldbTermLater = On
```

と同様に検査サーバーに設定を反映する必要があります。



NotifyUrldbTermLater パラメータの指定がない場合は、デフォルト設定 (off 指定) となりメールを通知しません。

(3) 送信先メールアドレスの設定方法

管理サーバー上で、/opt/Guardian/Admin/etc/wg/admin.conf を直接編集し、以下の設定を追加します。

複数のアドレスを指定したい場合は、コロン「:」で区切って指定してください。

設定例)

```
[URLDB]
NotifyUrldbTermMail = test@example.co.jp
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG admin
```



NotifyUrldbTermMail パラメータの指定がない場合は、以下で設定した全てのメールアドレスをデフォルト送信先メールアドレスとします。

- ・『管理サーバー利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「3-4-3-3 メール通知設定」- 「管理者メールアドレス」(320 ページ)
- ・『管理サーバー利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「3-2-2-2 個別設定」- 「URLDB」- 「完了通知メール」(88 ページ)

(4) メール通知文の設定方法

通知内容をカスタマイズすることができます。

ただし、メール標題(1)、差出人アドレス(2)は、カスタマイズできません。
管理サーバー上で、/opt/Guardian/Admin/etc/wg/urldb.tpl を直接編集してください。

(1) WEBGUARDIAN: URLDB ライセンス更新依頼通知

(2) root

設定例)

ホスト名: \$WG_HOST
URLDB 利用期間: \$DB_SPAN

URLDB のご利用期間が終了しようとしています。
ただちに URLDB のライセンス更新を実施してください。

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG udbtemplate
```



本文では、ライセンス期間と検査サーバーの情報を埋め込むために以下の変数を記述することができます。

(a) \$DB_SPAN : ライセンス終了日

(b) \$WG_HOST : 検査サーバーのホスト名

この内容は複数台構成一括設定対象です。

MEMO

3 ポリシー管理機能

3-1 ポリシー管理概要

WEBGUARDIANは、組織内のクライアントから外部へのHTTPアクセスに関してその利用者やその宛先（URL）、または送出されようとしているデータの中身（形式やサイズ、キーワード）を検査して、そのアクセスが組織のウェブ利用ポリシーに適合するものであるかどうかを判断することができます。

また検査結果の種類に応じて、利用者に対して応答するアクションを設定することが可能です。

たとえば、業務外利用と判断されるサイト（URL）へのアクセスや機密情報と判断されるデータを送信しようとした場合に、警告または禁止画面を応答し宛先のサーバーへのデータ送信を遮断することができます。

また同時に特定の業務外利用ケースに関してはリアルタイムに管理者へ通知する機能も備えています。

検査結果アクションは以下のものを利用することができます。

<アクション・リスト>

- (a) 中継
- (b) 試行
- (c) 警告
- (d) オーバーライド
- (e) 禁止
- (f) リダイレクト

また、アクションに付随する副作用を定義することも可能です。

Ver3.0では、利用可能な副作用はメール通知機能のみです。

<副作用・リスト>

- (a) メール通知

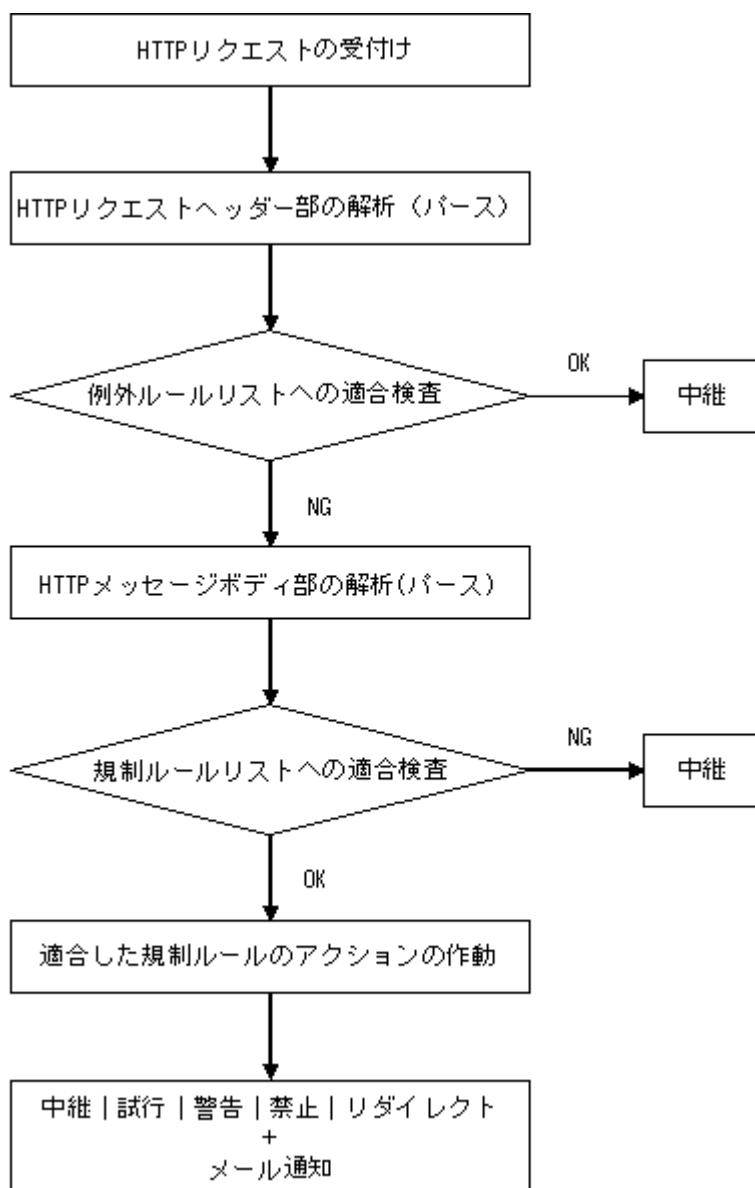


ポリシー設定は、複数台構成一括設定対象です。

つまり、検査サーバーが複数台設置されている場合、ポリシーに関する設定は全ての検査サーバーで同じものが適用されます。

3-2 アクセス制御処理の流れ

プロキシサーバー内のアクセス制御部では、以下の流れでHTTPリクエストデータを検査しています。



3-3 規制ルール

HTTP リクエストの内容の条件と、条件が適合した場合の結果の組合せを規制ルールとして定義します。

規制ルールは複数定義することができます。

検査処理は規制ルールの並び順に実施され、適合する規制ルールが見つかるかまたは全ての規制ルールに適合しなかった場合に終了します。

適合する規制ルールが見つかった場合は、定義されているアクションが作動し、通信内容が規制ログに記録されます。全ての規制ルールに適合しなかった場合、通信は中継されます。

(1) アクション

(a) 中継

通信を中継します。

中継アクションでは、リクエストを中継した結果取得されるデータに対して、サイズ制限値とデータサイズが制限値以上となった場合のアクションを設定することができます。アクションは「試行」「警告」「オーバーライド」「禁止」「リダイレクト」から選択します。アクションを適用する結果、ダウンロードがブロックされる場合、WEBGUARDIAN と上位サーバーとの通信は中断されます。



- ・ダウンロードサイズ制限は、レスポンスヘッダーに含まれる受信データの長さ情報 (Content-Length) の値を対象とします。
 - ・ダウンロードサイズ検査が行われる通信は、すでに当該ルールの条件を満たして中継動作が適用されているため、ダウンロードサイズ検査の結果にかかわらず、以降のルール行の評価は行われません。
-

(b) 試行

通信を中継します。中継アクションと同じですが、試験的に設定する規制ルールを区別する場合に使用します。

(c) 警告

通信を中継せずに、警告メッセージをユーザーに応答します。

一定時間内の再アクセスは警告メッセージを応答せずに、通信を中継します。

一定時間を経過した後に再アクセスがあると、再度警告メッセージをユーザーに応答します。



(d) オーバーライド

通信を中継せずに、禁止メッセージをユーザーに応答しますが、ユーザーがメッセージ画面の入力欄にオーバーライドコードを入力して解除操作を行うことで、一定期間リクエストが中継されるようになります。解除時間はオーバーライドコードごとに指定できます。

解除時間内の再アクセスは禁止メッセージを応答せずに、通信を中継します。

解除時間を経過した後に再アクセスがあると、再度禁止メッセージをユーザーに応答します。



(e) 禁止

通信を中継せずに、禁止メッセージをユーザーに応答します。

**(f) リダイレクト**

通信を中継せずに、設定された URL へのリダイレクト命令を応答します。

(2) メール通知機能

各規制ルール定義のアクション設定で「詳細」を開くとメール通知の設定を行うことができます。

規制ルールに適合した場合に、管理者または代替管理者へ規制ルールに適合するリクエストが発生したことを知らせる電子メールが送信されます。



アクション項目で「中継」を選択し、ダウンロードサイズ制限を設定した場合、通知メールはダウンロードサイズ制限が適用された場合のみ送信されます。

(3) 適合条件

適合条件は、以下の要素条件の組合せとして定義されます。

適合の成否は、定義されている要素条件成否の論理積の値です。

(a) グループ

認証名、クライアントマシン、User-Agent を特定する条件です。

規制ルール設定画面では、すでに登録してあるグループ定義のID(グループ名)を選択します。

詳細は後述の「3-5 グループ」(45 ページ)で説明します。

(b) 時間・曜日

リクエスト時刻を特定する条件です。

規制ルール設定画面では、すでに登録してある時間・曜日定義のID(説明)を選択します。

詳細は後述の「3-6 時間・曜日」(46 ページ)で説明します。

(c) URL

アクセス先のURLを特定する条件です。特定のURLやカテゴリを制限する場合や、IP アドレス指定のURLを制限する場合に利用します。

規制ルール設定画面では、すでに登録してあるURLグループ定義のID(グループ名)を選択します。

詳細は後述の「3-7 URL グループ」(46 ページ)で説明します。

(d) メソッド

HTTP リクエストのメソッドを特定する条件です。

リクエストの種類(データ取得系、データ送信系、データ更新系など)で特定する場合に利用します。

複数指定することが可能です。複数登録されている場合は、どれかに適合した場合結果が適合になります。

(e) MIMEタイプ

HTTP リクエストにメッセージボディが含まれる時に、メッセージボディのMIMEタイプによりリクエストを特定する場合に利用します。

規制ルール設定画面では、すでに登録してあるMIMEタイプ定義のID(セット名)を選択します。

詳細は後述の「3-8 MIME タイプ」(49 ページ)で説明します。

(f) キーワード

HTTPリクエストにメッセージボディ、またはURLのクエリー部に含まれるキーワードによってリクエストを特定する場合に利用します。

対象データはMIMEタイプ情報などによる適切に復号化された値に対して文字列比較されます。

規制ルール設定画面では、すでに登録してあるキーワード定義のID(セット名)を選択します。

詳細は後述の「3-9 キーワード」(49ページ)で説明します。

(g) 個人情報

HTTPリクエストにメッセージボディが含まれる時に、添付ファイルの個人情報総合指数値によってリクエストを特定する場合に利用します。

総合指数は0～100の値になります。複数の検査対象ファイルが含まれる場合、各ファイルの総合指数の中で最大の値が検査結果となります。

設定する総合指数値に対して、検査結果の総合指数値が「以上」「以下」のいずれかの条件を指定することができます。

(h) ファイルタイプ

HTTPリクエストにメッセージボディが含まれる時に、添付ファイルのファイルタイプによってリクエストを特定する場合に利用します。

また、添付ファイルの拡張子が、ファイルタイプの判定結果と「一致する」「一致しない」のいずれかの条件を指定することができます。

詳細は後述の「3-10 ファイルタイプ」(50ページ)で説明します。

(i) 送信データサイズ

HTTPリクエストにメッセージボディが含まれる場合に、メッセージボディのサイズからリクエストを限定する場合に利用します。

設定するバイト数に対して、メッセージボディのサイズが「超(より大きい)」「以上」「以下」「未滿(より小さい)」のどれかの条件を指定することができます。

(j) データタイプ

HTTPリクエストにメッセージボディが含まれる場合に、インスタントメッセージングによるリクエストを特定する場合に使用します。

指定できるサービスは以下のとおりです。

- ・ Windows Live メッセンジャー
- ・ AOL インスタント・メッセンジャー及びICQ



- ・対応クライアントは、Windows Live メッセンジャー 2009、AOL インスタント・メッセンジャー Ver5.1.3036、ICQ Ver6.5, 7.4（ただし、Windows7/IE8 上で動作しているものは対象外）です（2011 年 3 月現在）。
- ・インスタントメッセンジャーのプロキシ設定で、HTTPS プロトコルを使用する設定がされている場合、本条件の対象外です。
- ・インスタントメッセンジャーによるリクエストをブロックした場合、ブロック画面は表示されません。また、オーバーライド及びリダイレクトは禁止と同じ動作となります。
- ・AOL インスタント・メッセンジャーで、チャットメッセージの送信をブロックした場合、当該のチャットセッションは利用できなくなります。ご了承ください。

(k) パスワード

HTTP リクエストにメッセージボディが含まれる時に、添付ファイルのパスワード設定の有無によってリクエストを特定する場合に利用します。「パスワード設定あり」「パスワード設定なし」「パスワード設定なし / 判定不可」のいずれかの条件を指定することができます。

- | | |
|------------------|---|
| パスワード設定あり | : パスワード設定された添付ファイルが含まれる |
| パスワード設定なし | : パスワードの有無の識別が可能なファイルで、パスワード設定されていない添付ファイルが含まれる |
| パスワード設定なし / 判定不可 | : パスワード設定のない添付ファイル、またはパスワード設定の判定ができないファイルが含まれる |



- ・パスワード設定があることを判定できるのは、Excel、Word、PowerPoint、PDF、一太郎だけです。ソフトウェアの種類・実装によっては、パスワード設定の有無の判定が行えない場合があります。
- ・パスワード付きで「ブックの保護」が指定された Excel ファイルはパスワード設定されたファイルと判定されます。
- ・PowerPoint 2003 の書き込みパスワードが設定されたファイルはパスワード設定されたファイルと判定されます。

Excel、Word、PowerPointのパスワード設定の判定一覧

Excel、Word、PowerPoint ファイルのパスワード設定の判定は下表のとおりとなります。

ファイル形式	ファイルの種類 ※1	パスワード設定の判定 ※2
Excel	セキュリティ設定無し	×
	読み取りパスワード有り	○
	書き込みパスワード有り	×
	IRM設定有り	○
	「ブックの保護」パスワード有り	○
	「ブックの保護」パスワード無し	×
	「共有ブックの保護」パスワード有り	○
	「共有ブックの保護」パスワード無し	×
	「シートの保護」パスワード有り	×
	「シートの保護」パスワード無し	×
Word	セキュリティ設定無し	×
	読み取りパスワード有り	○
	書き込みパスワード有り	×
	IRM設定有り	○
PowerPoint	セキュリティ設定無し	×
	読み取りパスワード有り	○
	書き込みパスワード有り	× ※3
	IRM設定有り	○

1 古いバージョンの Excel、Word、PowerPoint では、該当の種類のファイルを作成する機能（セキュリティ設定機能）が搭載されていない場合があります。

2 パスワード設定の判定：・・・パスワード設定有りと判定されます。

×・・・パスワード設定無しと判定されます。

なお、一つのファイルに複数のセキュリティ設定が施されている場合、に該当するセキュリティ設定が一つでもあれば、同時に×に該当する設定がされていても、（パスワード設定有り）と判定されます。

3 PowerPoint2003 に関してのみ、（パスワード設定有り）と判定されます。

(4) 留意事項

規制ルールの適合判定処理では、最初のルールの適合検査をはじめる前にリクエストの全てのデータが解析されます。

解析処理は、リクエストデータの全体をシステム内部に読み込んでから開始されるため、規制ルール判定処理が終了するまで、送信データが一時的にプロキシサーバー上でせき止められます（リクエストのバッファリング）。

このため、通信にHTTPを使うストリーミング系のアプリケーションでは利用に支障をきたすことが予測できます。このようなケースを回避するには、後述の「3-4 例外ルール」（43ページ）を利用してリクエストのバッファリングを回避する設定を行ってください。

3-4 例外ルール

特定のリクエストに対して、規制ルールの適合判定処理を行わないように指示するためのルールです。

たとえば、プログラムで自動的に行われる HTTP アクセスや、動画データや音楽データなどの HTTP を使ってリアルタイムで配信・受信するプログラムのアクセスなどを、検査対象から除外する場合に利用します。

この検査は、規制ルール判定処理のメッセージボディの解析処理フェーズより先だって行われるため、メッセージボディの解析に大きな負荷がかかることが予想される場合や、また音楽データなどの解析を実施しても意味がないデータしか扱わないことが事前に予測できる場合に利用すると、プロキシー処理の転送スループットに良い効果が期待できます。

インストール後の初期状態では、「ストリーミング系ソフト」「Windows Update」が登録されています。



「ストリーミング系ソフト」「Windows Update」の設定はサンプルであり、全てのストリーミング系ソフト及び Windows Update の通信に対応するものではありません。必要に応じて、設定を修正してご利用ください。

(1) 適合条件

例外ルールの条件指定は、リクエストのヘッダー情報から判別できるものに限定されます。

適合条件は、以下の要素条件の組合せとして定義されます。

適合の成否は、定義されている要素条件成否の論理積の値です。

(a) グループ

認証名、クライアントマシン、User-Agent を特定する条件です。

例外ルール設定画面では、すでに登録してあるグループ定義の ID (グループ名) を選択します。

詳細は後述の「3-5 グループ」(45 ページ) で説明します。

(b) 時間・曜日

リクエスト時刻を特定する条件です。

例外ルール設定画面では、すでに登録してある時間・曜日定義の ID (説明) を選択します。

詳細は後述の「3-6 時間・曜日」(46 ページ) で説明します。

(c) URL

アクセス先の URL を特定する条件です。特定の URL やカテゴリを制限する場合や、IP アドレス指定の URL を制限する場合に利用します。

例外ルール設定画面では、すでに登録してある URL グループ定義の ID (グループ名) を選択します。

詳細は後述の「3-7 URL グループ」(46 ページ) で説明します。

(d) メソッド

HTTP リクエストのメソッドを特定する条件です。

リクエストの種類 (データ取得系、データ送信系、データ更新系など) で特定する場合に利用します。

複数指定することが可能です。複数登録されている場合は、どれかに適合した場合結果が適合になります。

(e) 送信データサイズ

HTTP リクエストにメッセージボディが含まれる場合に、メッセージボディのサイズからリクエストを限定する場合に利用します。

設定するバイト数に対して、メッセージボディのサイズが「超 (より大きい)」、「以上」、「以下」、「未満 (より小さい)」のどれかの条件を指定することができます。

(2) メール通知

例外ルールに適合した場合に、管理者または代替管理者へ例外ルールに適合するリクエストが発生したことを知らせる電子メールが送信されます。

3-5 グループ

以下の3つの要素条件から、リクエストの属するグループを特定します。
適合の成否は、定義されている要素条件成否の論理積の値です。

(a) 認証名

ユーザー認証機能を有効にしている場合に、リクエスト送信者の認証名(ユーザーID)からリクエストを限定する場合に利用します。
複数指定することが可能です。複数登録されている場合は、どれかに適合した場合結果が適合になります。

(b) IPアドレス

ユーザーが利用しているクライアントノードのIPアドレスを特定する場合に利用します。

IPアドレスまたはネットワークアドレスを指定します。IPアドレスの各オクテットでは、カンマ「,」区切りによる数値の複数指定形式と、数値2個をハイフン「-」でつないだ範囲指定形式をサポートしています。

ユーザーエージェントと *WEBGUARDIAN* のプロキシサーバーの間に別のプロキシサーバー(下位プロキシ)を介在している場合は、下位プロキシサーバーホストのIPアドレスが対象となります。



下位プロキシが X-Forwarded-For ヘッダーでクライアントノードのIPアドレスを *WEBGUARDIAN* に送信することで、下位プロキシが介在している場合にも *WEBGUARDIAN* でクライアントIPアドレスを対象とすることが可能です。詳細については、「5-6 プロキシ多段構成時の設定」 - 「(1) *WEBGUARDIAN* の下位にプロキシサーバーが存在する場合」(78ページ)をご参照ください。

複数指定することが可能です。複数登録されている場合は、どれかに適合した場合結果が適合になります。

(c) User-Agent

ユーザーが利用しているユーザーエージェントソフトを特定する場合に利用します。
設定した文字列が、HTTPリクエストのUser-Agentヘッダーの値に含まれる場合に適合すると判断されます。設定文字列では大文字小文字の違いは無視されます。
複数指定することが可能です。複数登録されている場合は、どれかに適合した場合結果が適合になります。

3-6 時間・曜日

リクエスト時刻を特定するための条件です。

リクエスト時刻が、指定された時間範囲内であれば適合となります。

3-7 URLグループ

以下の3つの要素条件から、リクエストの属するURLグループを特定します。

複数の条件が指定されている場合は、どれかに適合すれば全体の結果が適合となります。

(a) URLリスト

URLの条件を表す文字列(URLパターン)を登録します。

複数登録可能です。

URLパターンが複数登録されている場合は、どれかに適合すれば結果が適合となります。

URLパターンは、以下の4つのパートから構成されています。

パスの後の「?」文字に続くクエリー文字列は対象となりません。

ワイルドカード文字は各パート内のみで展開されます。

スキーム名

「http」「https」「ftp」のうち1つを選択してください。

ホスト名

WWWサーバー、FTPサーバーマシンのホスト名またはIPアドレスを指定します。

日本語ドメイン名を使用可能です。ASCII文字の大文字と小文字は区別されません。

指定文字列中に長さ0以上の任意の文字列と一致する「*」を使用することができます。ただし、ホスト名のラベル(「.」で区切られる要素)内で全角文字と「*」を同時に指定することはできません。

ポート番号

WWWサーバー、FTPサーバーマシンのポート番号を指定します。

省略された場合は、全てのポート番号に適合します。

特定のポート番号に限定したい場合は、明示的にポート番号を指定してください。

ポート番号にはワイルドカード文字(「*」)を使うことはできません。

パス

WWWサーバー、FTPサーバーマシン上のファイルやプログラム名などを表すパスを指定します。

パスに使うことができる文字は、印字可能な ASCII 文字のみです。

日本語などのマルチバイト文字には対応していません。

ワイルドカード文字（「*」）を使うことができます。



スキームが「https」の時は、パス部を指定することはできません。

暗号化通信になるために接続先のホスト名とポート番号しか特定することができないためです。

< 設定例 >

http://www.example.co.jp/

スキーム : http
ホスト : www.example.co.jp
ポート番号 : 任意
パス : / (トップのみ)

http://*.example.co.jp/security/*

スキーム : http
ホスト : example.co.jp ドメインのホスト
ポート番号 : 任意
パス : 「/security/」で始まるもの全て

http://*.example.co.jp/*

スキーム : http
ホスト : example.co.jp ドメインのホスト
ポート番号 : 任意
パス : 任意

http://*.EXAMPLE.co.jp:80/*

スキーム : http
ホスト : example.co.jp ドメインのホスト
ポート番号 : 80 番のみ
パス : 任意

ftp://*/*

スキーム : ftp
ホスト : 任意
ポート番号 : 任意
パス : 任意



ワイルドカード文字は各パート内のみで展開されるため、「ftp://*」では「*」はホスト名部に適用され、パス部には適用されません（パス部は「/」のみが対象となります）。ホスト名、パスの両方とも任意の場合は「ftp://*/*」のように指定してください。

https://*

スキーム : https
ホスト : 任意
ポート番号 : 任意
パス : 指定不可

(b) カテゴリ

URL が属するカテゴリの条件を登録します。

カテゴリ条件に拡張子条件が同時に指定されている場合、指定されたカテゴリに属し、かつ URL のファイル名部分の拡張子が指定された拡張子に一致する URL が適合します。拡張子が複数登録されている場合は、どれかに適合すれば結果は適合となります。拡張子条件に指定できる文字は、印字可能な ASCII 文字のみです。大文字と小文字は区別されません。

複数登録可能です。カテゴリが複数登録されている場合は、どれかに適合すれば結果は適合となります。

(c) IPアドレスURL

URL のホスト名部が IP アドレスであるリクエストを特定する場合に使用します。

ホスト名部が IP アドレスである全ての URL が適合します。適合する IP アドレスの範囲をプライベートアドレスに限定することもできます。プライベートアドレスとは、「10.0.0.0/8」「172.16.0.0/12」「192.168.0.0/16」「169.254.0.0/16」です。

3-8 MIMEタイプ

リクエストにメッセージボディが含まれる時に、メッセージボディのMIMEタイプによりリクエストを特定するための条件です。

たとえば、MS-WORD や MS-EXCEL のファイルのアップロードを条件にしたい場合などに定義します。

複数登録可能です。複数登録されている場合は、どれかに適合すれば全体の結果が適合となります。

(1) 検査対象

各メッセージの Content-Type ヘッダーの値と照合します。

Content-Type ヘッダーの値が実際のメッセージボディのMIMEタイプと異なる場合は検査は間違ふことになります。

(2) マルチパートの場合

各パートを再帰的に検査しますので、パートのMIMEタイプも対象にすることができます。

(3) 添付ファイル名の検査

メッセージボディのMIMEタイプが添付形式 (multipart/form-data) の場合は、パートヘッダーのContent-Dispositionヘッダー中のfilename属性をもとに添付ファイルのファイル名を条件に付加することができます。

添付ファイル名指定文字には、ワイルドカード文字を使うことができます。

添付ファイル名指定文字が「*」だけの場合は、添付ファイルが存在するという指定になります。この「添付ファイルが存在する」とは、Content-Dispositionヘッダーが存在し、filename属性があるという意味になります。

3-9 キーワード

HTTPリクエストにメッセージボディ、またはURLのクエリー部に含まれるキーワードによってリクエストを特定する場合に利用します。

対象データはMIMEタイプ情報などによる適切に復号化された値に対して文字列比較されます。

3-10 ファイルタイプ

リクエストにメッセージボディが含まれる時に、添付ファイルのファイルタイプによりリクエストを特定するための条件です。「添付ファイル」の定義は、filenameパラメータがあるパートです。

ファイルタイプは、タイプ文字列で指定します。

複数のタイプ文字列を指定する場合は、「type1+type2」のように記述します。タイプ文字列の英大小文字は同一視します。

(1) 対応形式

対応するファイルタイプと指定するタイプ文字列を以下の表に示します。

	タイプ文字列	ファイルタイプ	拡張子(拡張子検査で使用)
1	ZIP	ZIPアーカイブ	zip
2	LHA	LHAアーカイブ	lzh
3	RAR	RARアーカイブ	rar
4	CAB	CABアーカイブ	cab
5	GZIP	GZIP圧縮ファイル	gz tgz
6	BZIP2	BZIP2圧縮ファイル	bz2
7	Z	UNIX Compress圧縮ファイル	z
8	TAR	TARアーカイブ	tar
9	TEXT	テキストファイル	txt
10	PDF	PDFファイル	pdf
11	EXCEL	Microsoft Excelファイル	
12	WORD	Microsoft Wordファイル	doc docx docm dotx dotm
13	PPT	Microsoft PpowerPointファイル	ppt pps pptx pptm potx potm ppsx ppsm
14	JTD	ジャストシステムー太郎ファイル	jaw jbw juw jfw jvw jtd jtt
15	HTML	HTMLファイル	html htm
16	XML	XMLファイル	xml
17	RTF	Microsoft RTFファイル	rtf
18	VISIO	Microsoft Visioファイル	vsd
19	EXE	DOS/Windows 実行形式ファイル	exe



- ・ファイルタイプ判定はファイルのヘッダー、トレイラー等のいくつかの特徴情報に基づき判定します。作成したアプリケーションの種類・実装・バージョンによっては判定できない場合があります。添付ファイルがあるファイルタイプに判定されても実際に対応するアプリケーションでファイルを開くことができるかどうかは保証できません。表以外のアプリケーションファイルでも同一のファイルフォーマットを用いている場合は、表にあるファイルタイプに判定されることがあります。
- ・ZIP,LHA,RAR,CAB のSFX 形式ファイルはEXE ファイルと判定されます。
- ・Excel2007の読み取りパスワードが設定されたファイル、パスワード付きで「ブックの保護」が設定されたファイル、パスワードで保護された共有ブックは判定できません。
- ・PowerPoint2007の読み取りパスワードが設定されたファイルは判定できません。

(2) 拡張子検査

拡張子検査で、各ファイルタイプに一致すると判定される拡張子は、表の「拡張子」のとおりです。拡張子の英大小文字は同一視します。条件として、拡張子がファイルタイプに「一致する」「一致しない」のいずれかを指定します。

- 一致する : 全ての添付ファイルについて、ファイルタイプと拡張子が一致する
- 一致しない : 少なくとも1つの添付ファイルについて、ファイルタイプと拡張子が一致しない



「/opt/Guardian/Admin/etc/wg/httpd.conf」に設定を記述することで、ファイルタイプと拡張子の対応を変更できます。

ファイルタイプの有効な拡張子は、指定する拡張子リストで上書きされるため、当該ファイルタイプの有効な拡張子を全て指定してください。

例) LHA アーカイブの拡張子に lha を追加する

```
WGFileNameExtension LHA lzh lha
```

設定後は、以下のスクリプトを実行して、検査サーバー(ウェブ)上の設定ファイルを更新してください。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

3-11 ブロック画面

規制ルール適合検査の結果、「警告」「オーバーライド」「禁止」のいずれかのアクションが適用された場合に、WEBGUARDIANから直接ユーザーエージェントへ応答されるメッセージ画面をブロック画面と呼びます。

ブロック画面は、「警告」「オーバーライド」「禁止」それぞれのアクション用のものを用意することができます。また、固有のブロック画面を作成することにより同じアクションの時でも規制ルール単位に異なる応答画面を設定することができます。

ブロック画面の中では、リクエストの内容に基づいた以下の情報を含めることができます。

- ・適合した規制ルールのルール名
 - ・適合した規制ルールのルール ID
 - ・適合した規制ルールにキーワード条件があった時見つかったキーワード文字列
 - ・リクエストした URL
 - ・リクエストした URL のカテゴリ
 - ・ユーザー認証名
 - ・クライアントの IP アドレス
 - ・MIMEタイプ / 個人情報 / ファイルタイプ / パスワードのいずれかの条件に適合した添付ファイル名
 - ・個人情報総合指数 (1)
 - ・個人情報件数 (1)
 - ・個人情報項目数 (0 ~ 7 の値) (1)
 - ・個人情報密度 (0 ~ 100 の値、単位は %) (1)
 - ・ダウンロードサイズ制限に適合したダウンロードデータのファイル名
 - ・ダウンロードサイズ制限に適合したダウンロードデータの Content-Type
 - ・ダウンロードサイズ制限に適合したダウンロードデータのサイズ
- (1) 適合した規制ルールに個人情報条件があった時。



- ・個人情報検査対象パートが複数ある場合、総合指数が最大のパート (複数存在する場合はその内最初に出現するパート) の総合指数 / 個人情報件数 / 個人情報項目数 / 個人情報密度の値が使用されます。
 - ・ダウンロードデータのファイル名は、Content-Disposition レスポンスヘッダーの filename パラメータが取得可能な場合はその値となり、そうでない場合は URL のファイル名部の値となります。いずれも存在しない場合、ファイル名は空となります。
-

3-12 オーバライドコード

規制ルール適合検査の結果、「オーバーライド」アクションが適用された場合は、WEBGUARDIAN から直接ユーザーエージェントへ応答されるメッセージ画面にオーバーライドコードの入力欄が表示されます。ユーザーがオーバーライドコードを入力し解除操作を行うことで、WEBGUARDIANが行うリクエストのブロックを一定期間解除させることができます。

複数のオーバーライドコードを登録することができますので、用途に応じてオーバーライドコードを使い分けることができます。



オーバーライドコード

半角英数字20文字までの解除用コードを指定します。他のオーバーライドコードエントリーで使用されているコードを使用することはできません。

解除時間

メッセージ画面でユーザーが解除操作を行ってから、再度メッセージ画面を応答するまでの時間を指定します。

有効期間

オーバーライドコードが有効となる期間を指定します。



- ・クライアントにインスタントメッセージのようなオーバーライドコードの入力ができないアプリケーションを使用する場合は、オーバーライドブロックを解除できません。

ただし、ウェブブラウザのような解除操作が可能なアプリケーションでオーバーライドブロックを解除済の状態であれば、インスタントメッセージ等のアプリケーションを使用することが可能です。

- ・オーバーライド解除中であるかのステータス情報は *WEBGUARDIAN* のメモリ内に保持されるため、*WEBGUARDIAN* を再起動した場合は、解除時間内であっても再度オーバーライドブロック画面が表示されます。

MEMO

4 グループ管理

4-1 グループ管理機能概要

グループ管理機能は、情報管理者、部門情報管理者が各種ログ表示機能を利用した時に、特定の利用者グループのログだけを限定的に閲覧することができる機能です。利用者は、あるグループに属し（複数のグループに属することも可）、管理者はあるグループ（複数のグループを管理することも可）を管理します。あるグループを管理できるように定義された管理者は、ログ検索画面で一覧処理を行うと、そのグループに属する利用者のログだけが一覧表示されます。

この機能を利用すると、たとえば、部門情報管理者である各上司が各部門に属する利用者のログだけを閲覧するというような使い方ができます。

利用例）情報管理者「admin1」（グループ「tokyo」を管理）の場合の表示

各種ログ閲覧画面において、グループに属するユーザー（認証名、IPアドレス、ネットワークアドレス、User-Agent）のログだけを一覧表示します（検索条件を指定することなく、限定された範囲のログだけを表示します）。

管理対象グループに属するユーザーのログだけ一覧表示します。

年月日	IPアドレス	URL	MD5ハッシュ	サイズ
2005/12/01	192.168.14.171	http://www.google.co.jp/dtsp/this-jack-dm-vdngp		9K

4-2 グループの登録

グループの作成、削除、変更はウェブブラウザで設定できます。(グループ管理権限のある)情報管理者アカウント、もしくは、利用者管理アカウントでログインし、グループ管理機能を使用します。操作方法の詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「3-4-1-3 グループ」(243 ページ)をご参照ください。

WEBGUARDIAN

グループ

新しいグループを作成します。
グループは、IPアドレス、認証名ユーザー認証機能が有効な場合、User-Agent の組合せ条件として定義します。

ID 名: 300

グループ名: 新規グループ300

認証名リスト

IPアドレス

ネットワークアドレス

User-Agent

※印のある項目は必須です。

- ・「グループ名」(承認値: 半角文字で100字、全角文字で50字)
- ・IPアドレスの最大登録数は 32 個までです。
- ・IPアドレスの各オクテットでは、斜線(/)で区切りで連続指定ができます。
- ・IPアドレスの各オクテットでは、斜線(/)値を0xFFで区切ることで範囲指定ができます。
- ・認証名の最大登録数は 255 個までです。
- ・認証名に使用する文字はASCII文字(印字可能)のみです。
- ・認証名(制限値: 40文字以内)
- ・User-Agent(リストのUser-Agentヘッダーに含まれる部分文字列を指定してください。大文字/小文字は区別されません)

登録 キャンセル

Copyright (c) 2011 Canon IT Solutions Inc. All rights reserved.

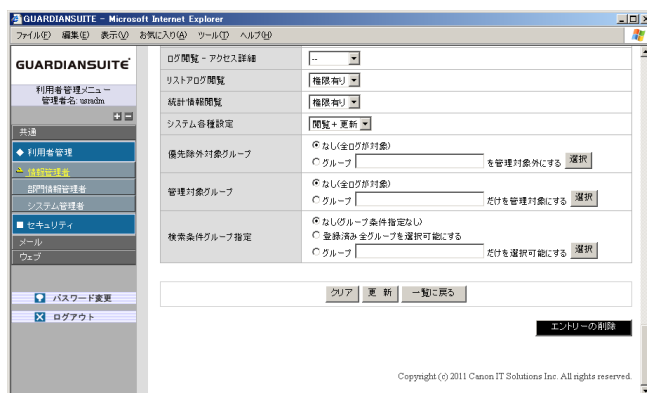
グループ定義の詳細については、「3-5 グループ」(45 ページ)をご参照ください。

4-3 グループ管理

(1) 管理対象グループ

各種ログ閲覧画面において、管理対象に指定されたグループに属するユーザー（認証名、IP アドレス、ネットワークアドレス、User-Agent）のログだけを一覧表示します。検索条件を指定してログの検索を行った場合は、グループ管理機能で限定された範囲内のログから指定条件を満たすログを検索することになります。

情報管理者、部門情報管理者の管理対象グループは、ウェブブラウザで設定できます。利用者管理アカウントで利用者管理画面にログインし、アカウント管理機能を使用します。権限設定変更、操作方法の詳細については、『管理サーバー 利用の手引き～GUARDIANWALL、WEBGUADIAN共通～』の「6-2-1-4 情報管理者の権限リスト」（398 ページ）、「6-2-1-5 部門情報管理者の権限リスト」（400 ページ）、「6-2-1-3 アカウントの編集・削除」（387 ページ）をご参照ください。



管理対象グループ

指定したグループに属するユーザー（認証名、IP アドレス、ネットワークアドレス、User-Agent）のログだけを表示するようにします。

(2) 優先除外対象グループ

少数のユーザーを除いて、それ以外のユーザー全てを管理対象にしたいような場合には、少数のユーザーをグループとし、そのグループを優先除外対象グループとして指定すればグループ定義を簡略化できます。

各種ログ閲覧画面において、優先除外対象に指定されたグループに属するユーザー(認証名、IP アドレス、ネットワークアドレス、User-Agent)のログを表示しません(優先除外対象と判定されたログは、前述の管理対象グループに属するものでも表示しません)。特定のユーザーのログを、ログ一覧に表示させたくないような場合に使用してください。



優先除外対象グループ、管理対象グループを指定した場合、指定するグループ数に比例してログの検索速度は低下します。ご了承ください。

4-4 検索条件グループ

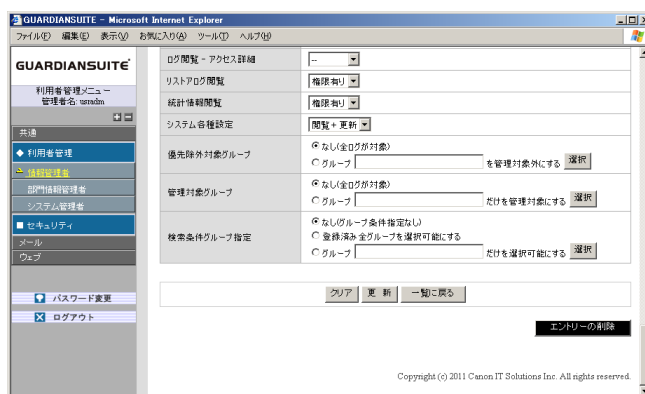
各種ログ検索・閲覧画面で検索条件として選択できる(リストボックス内にリストアップされる)グループをアカウントごとに指定できます。ログ検索・閲覧画面では選択されたグループに属するユーザー(認証名、IPアドレス、ネットワークアドレス、User-Agent)のログを検索します。ログ検索・閲覧操作方法の詳細については、『管理サーバー利用の手引き ~ GUARDIANWALL、WEBGUADIAN 共通 ~』の「3-4-2-1 ログ閲覧」(276 ページ)をご参照ください。

IPアドレス/認証名	<input type="text"/>	--
URL	<input checked="" type="radio"/> URL:	<input type="text"/>
	<input type="radio"/> カテゴリ:	<input type="text"/>
	<input type="radio"/> URLグループ:	--

1: 社員
 2: 開発部
 3: 役員
 4: 人事部

[選択](#) [クリア](#)

情報管理者、部門情報管理者アカウントごとに、検索条件のグループ指定部に選択できる(リストボックスにリストアップされる)グループを設定できます。利用者管理アカウントで利用者管理画面にログインし、アカウント管理機能を使用します。権限設定変更、操作方法の詳細については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUADIAN 共通 ~』の「6-2-1-4 情報管理者の権限リスト」(398 ページ)、 「6-2-1-5 部門情報管理者の権限リスト」(400 ページ)、 「6-2-1-3 アカウントの編集・削除」(387 ページ)をご参照ください。



検索条件グループ指定

各種ログ検索・閲覧画面の「IPアドレス / 認証名」の検索条件指定で、グループ指定部に選択できるグループを指定します。

「なし」を選択した場合は検索条件のグループ指定部にグループを選択できません。「登録済み全グループを選択可能にする」を選択した場合は、登録済みのグループ全てを検索条件のグループ指定部にリストアップします。

特定のグループだけをリストアップしたい場合は、グループIDを指定してください。[選択] ボタンをクリックすると、グループの選択画面が表示されます。

4-5 規制ルール/例外ルール

規制ルール/例外ルールの条件として、グループを用いることができます。規制ルール/例外ルール設定画面の操作方法の詳細については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUADIAN共通～』の「3-4-1-1 規制ルール」(229ページ)及び「3-4-1-2 例外ルール」(241ページ)をご参照ください。

規制ルール

定義されているルールエントリを表示しています。
合符条件を編集し、[更新]ボタンを押してください。

ID: 1

ルール名 ※: ウェブメール禁止

グループ: --

時間・曜日: --

URL: 1. ウェブメール

メソッド: すべて

MIMEタイプ: --

キーワード: --

送信データ: 個人情報 総合指数: [] 以上 [] フェイルテスト

サイズ: [] Kバイト [] 以上 []

アクション ※:

☐ 中継

☐ 試行

☐ 警告

☒ 禁止

☐ リダイレクト URL: []

※印がある項目は必須です。

- 「ルール名」(制約値: 半角文字で120字、全角文字で60字)
- 「メソッド」が「カスタム」の場合、対象とするメソッドを半角スペース区切りで指定してください。
- 「送信データ」はPOSTやPUTメソッド時にクエリに含まれるボディデータを意味しています。
- 「送信データのヘッダー」では、ホッダー名に加えてURLに含まれるContent-Lengthの値を対象とします。
- 個人情報総合指数100の値で、より多くの個人情報を含む文書がより高い値を示します。
- 「送信データのサイズ」(クエリヘッダーに含まれる送信データの長さ情報Content-Lengthの値)を対象とします。
- 「送信データのサイズ」は1バイト1024バイト、1Mバイト1024Kバイトです。
- 「代替管理者」に複数のメールアドレスを設定する場合はセミコロン区切りで入力してください。最大25まで登録可能です。

削除 更新 キャンセル

Copyright (c) 2011 Canon IT Solutions Inc. All rights reserved.

例外ルール

定義されている例外ルールを表示しています。
合符条件を編集し、[更新]ボタンを押してください。

ID: 1

例外ルール名 ※: ストリーミング系ソフト

グループ: 1. ストリーミング系ソフト

時間・曜日: --

URL: --

メソッド: すべて

送信データサイズ: [] Kバイト [] 以上 []

メール通知: ☐ 管理者 代替管理者: []

※印がある項目は必須です。

- 「例外ルール名」(制約値: 半角文字で120字、全角文字で60字)
- 「メソッド」が「カスタム」の場合、対象とするメソッドを半角スペース区切りで指定してください。
- 「送信データサイズ」(クエリヘッダーに含まれる送信データの長さ情報Content-Lengthの値)を対象とします。
- 「送信データサイズ」は1バイト1024バイト、1Mバイト1024Kバイトです。
- 「代替管理者」に複数のメールアドレスを設定する場合はセミコロン区切りで入力してください。最大25まで登録可能です。

削除 更新 キャンセル

Copyright (c) 2011 Canon IT Solutions Inc. All rights reserved.

4-6 システム設定

情報管理者、部門情報管理者の個別設定ファイルを直接編集し、グループ管理機能を設定することができます。

情報管理者、部門情報管理者の個別設定ファイルの詳細については『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「7-1 情報管理者アカウント管理」(410 ページ) 及び「7-2 部門情報管理者アカウント管理」(415 ページ) をご参照ください。

(1) グループ管理設定

管理サーバー上で情報管理者、部門情報管理者の個別設定ファイルの編集を行います。

記述例)

- ・ 情報管理者、アカウント「admin1」の場合

/opt/Guardian/Admin/etc/admin/admin/admin1.conf

```
[WG]
ExcludeGroup = 1          # 優先除外対象グループ
SelectGroupList = true    # グループ選択機能を使用する
```

- ・ 部門情報管理者、アカウント「manager1」の場合

/opt/Guardian/Admin/etc/admin/manager/manager1.conf

```
[WG]
Group = 2:3               # 管理グループ。複数設定する場合は「:」で区切る。
SelectGroupList = true    # グループ選択機能を使用する
SelectGroup = 2:3         # 管理グループのみリストアップ
```



優先除外対象グループ、管理対象グループを指定した場合、指定するグループ数に比例してログの検索速度は低下します。ご了承ください。

(2) グループ管理設定用オプション一覧

情報管理者、部門情報管理者の個別設定ファイルに指定できる、グループ管理に関するオプションを下表に示します。

キー	初期値	意味	設定範囲
Group	未指定	管理するグループのIDを列挙する。未指定時は、全てのログが閲覧対象。	文字列(グループID) 複数の場合は、 「:」で区切る
ExcludeGroup	未指定	優先除外するグループのIDを列挙する。未指定時は除外を行わない(全てのログを閲覧する)。	文字列(グループID) 複数の場合は、 「:」で区切る
LogGrouping	True	ログ一覧表示でグループ管理機能を使用し、グループに属するユーザーのログのみを表示する場合はTrue、全てのログを表示する場合はFalseを指定する。	True/False
StatGrouping	False	統計情報表示でグループ管理機能を使用し、グループに属するユーザーのログから統計情報を表示する場合はTrue、全てのログから統計を表示する場合はFalseを指定する。	True/False
SelectGroupList	False	各種ログ検索画面の検索条件指定部にグループの選択機能を使用する。 True: 選択可、 False: 選択不可	True/False
SelectGroup	未指定	各種ログ検索画面の検索条件指定部にリストアップするグループのIDを列挙する。未指定時は、登録済のグループ全てがリストアップされる。	文字列(グループID) 複数の場合は、 「:」で区切る

5 プロキシ設定

5-1 基本設定

プロキシサーバーホストの動作パラメータとして以下の項目を設定することができます。

(1) ポート番号

プロキシサーバーホストがプロキシリクエストを受け付けるTCPポート番号です。初期値は「1088」です。



GUARDIANSUITE は、通信用に 8080 番ポートを使用します。

プロキシのポート番号として 8080 番を使用する場合は、GUARDIANSUITE が使用するポート番号を変更後、プロキシのポート番号設定を行ってください。

GUARDIANSUITE が使用するポート番号の変更方法については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「11 ポート番号の変更方法」(456 ページ)をご参照ください。

(2) アクセス許可ホスト

プロキシサービスの提供を許可するクライアントのアドレスを登録します。

初期値は、「all」(全て許可)です。

設定可能な形式には以下のものがあります。

(a) all

全てのクライアントを許可します。

(b) ホスト名、ドメイン名

クライアントのIPアドレスをもとにDNSを逆引きした結果のホスト名を対象に照合されます。

指定された文字列と一致する場合、または指定された文字列でホスト名が終わる場合に許可されます。

プラットフォームOSのドメイン名解決設定が適切に実施されていなければなりません。

(c) 完全なIPアドレス

クライアントのIPアドレスと一致する場合に許可されます。

(d) ネットワーク/ネットマスクの対

クライアントのIPアドレスが含まれる場合に許可されます。

(e) ネットワーク/nnn CIDR指定

クライアントのIPアドレスが含まれる場合に許可されます。

(3) 上位プロキシ**上位プロキシ**

特定の上位プロキシサーバーホストのIPアドレスとポート番号を指定します。
初期値は設定されていません。

(a) アドレス

特定のIPアドレスまたはホスト名を指定します。

(b) ポート

TCPポート番号を指定します。

上位プロキシURL

特定のリクエスト (URL) に対し、特定の上位プロキシを指定します。
初期値は設定されていません。

(a) URL

特定のURLを指定します。

URLは、英字の大文字、小文字は区別せず、同一視します。

URLには、完全一致の文字列を指定してください。

URLはワイルドカード文字「*」を使用できます。

ワイルドカード文字「*」は、長さ0以上の任意の文字列にマッチします。

(b) プロキシ

特定の上位プロキシを選択します。

で登録された上位プロキシがプルダウンに表示されます。



上位プロキシURLリストは、上位行から下位行に向かって評価され、URLがマッチする上位プロキシへ中継されます。ただし、上位プロキシが停止している場合やリクエストに問題がある場合は、その時点でリクエストが終了します。また、上位プロキシがリクエスト受付後にエラー応答を返す場合は、上位プロキシURLリスト内の次にURLがマッチした上位プロキシへ中継されます。



上位プロキシ URL 登録時の URL 指定において、スキームが「https」の場合は、https:// から始まる文字列を指定せず、接続先のホスト名とポート番号の以下形式で指定してください。

ホスト名:ポート番号

例) www.example.com:443

フォワード対象外ホストフィールド

フォワード対象外ホストフィールドには、上位プロキシサーバーホストを経由せず、直接アクセスするサーバーホストを指定します。

フォワード対象外ホストの設定可能な形式は以下です。リクエストURLのホスト名部と照合され判断されます。

(a) ホスト名

FQDN 形式のホスト名です。

ホスト名に対応するIPアドレスが直接指定されたリクエストは対象になりません。

例) www.example.co.jp

(b) ドメイン名

最初の文字が「.」で始まるドメイン名です。

例) .example.co.jp

(c) 完全なIPアドレス

数値ドット表記による IP アドレスです。

例) 192.168.123.7

(d) ネットワーク / nnn CIDR指定

例) 192.168.112.0/21

(4) 要求タイムアウト

リクエストのタイムアウト時間（秒）を指定します。

初期値は「300」秒です。

この内容は各検査サーバー個別の設定項目です。

(5) SSL接続許可ポート

SSL通信を行う場合に接続を許可するポート番号を指定します。

初期値は「443」と「563」です。

(6) 最大同時接続数

同時に受け付けることが可能なプロキシリクエスト数の最大値を指定します。
初期値は「200」です。

最大同時接続数について

プロキシサーバーの使用可能なメモリ量とCPU処理能力の両方に空きがある場合、同時接続数を増やすことでプロキシのスループットを向上させることができます。しかし、プロキシサーバーのシステムリソースの範囲を超える同時接続数を受け付けても性能は向上しません。

また、プロキシサーバーでは同時接続数と同じ数のサーバープロセスが起動しますが、サーバープロセスを生成するために必要なメモリが、サーバーで使用可能なメモリ量を超えると、システム性能は急激に低下します。

したがって、最大同時接続数はシステムリソースに応じた適切な値を設定する必要があります。

最大同時接続数は、以下の手順で見積もることができます。

システムで利用可能なメモリ量の確認**(a) Linux の場合**

free コマンドの「-/+ buffers/cache:」行で、free 値を確認します。

例)

# free						
	total	used	free	shared	buffers	cached
Mem:	4147756	3444888	702868	0	139252	2363732
-/+ buffers/cache:		941904	3205852			
Swap:	8193140	252	8192888			

使用可能なメモリは3205852 KB

(b) Solaris の場合

vmstat コマンドの free 値を確認します (1 行目は OS 起動からの平均値のため、2 行目以降の出力で確認)。

例)

# vmstat 5																			
kthr				memory								page				disk			
r	b	w		swap	free	re	mf	pi	po	fr	de	sr	dd	dd	lf	lf	in	sy	cs
0	0	0	2559712	667472	1	3	1	0	0	0	0	0	0	0	2	0	465	36	160
0	0	0	2287400	441320	0	4	0	0	0	0	0	0	0	0	0	0	464	71	184
0	0	0	2287400	441320	0	0	0	0	0	0	0	0	0	0	0	0	462	62	183
0	0	0	2287400	441320	0	0	0	0	0	0	0	0	0	0	0	0	461	62	177
...																			

使用可能なメモリは441320 KB

1つのサーバープロセスが使用するメモリ量の確認

ps コマンドで、稼働中のサーバープロセス数と、各プロセスのRSS値を確認します。
例)

```
# ps -eo rss,args | grep /opt/Guardian/WG/bin/httpd | grep -v grep | wc -l
150          150 プロセスが稼働中
# ps -eo rss,args | grep /opt/Guardian/WG/bin/httpd | grep -v grep
7908 /opt/Guardian/WG/bin/httpd -k start
7644 /opt/Guardian/WG/bin/httpd -k start
7024 /opt/Guardian/WG/bin/httpd -k start
7840 /opt/Guardian/WG/bin/httpd -k start
7868 /opt/Guardian/WG/bin/httpd -k start
7044 /opt/Guardian/WG/bin/httpd -k start
7788 /opt/Guardian/WG/bin/httpd -k start
7156 /opt/Guardian/WG/bin/httpd -k start
7812 /opt/Guardian/WG/bin/httpd -k start
...
```

1 プロセス当たり約 8000 KB

起動可能なサーバープロセス数の算出

例)

新たに起動可能なプロセス数は、 $3205852 \text{ KB} / 8000 \text{ KB} = 400$ プロセス。
すでに 150 プロセス起動しているため、 $400 + 150 = 550$ プロセス起動可能。

実環境でのピーク時のシステムリソース状況の確認

最大同時接続数の見積り値を設定後、プロキシサーバーのピーク時のシステムリソースをご確認ください。メモリ使用量がシステムリソースの上限に達している場合、最大同時接続数をより小さな値に再設定してください。メモリ量に余裕があり、/var/opt/Guardian/WG/var/error_log に以下のログメッセージが出力されている場合、最大同時接続数をより大きな値に再設定してください。

```
[Mon Mar 30 10:56:00 2009] [error] server reached MaxClients setting, consider raising the MaxClients setting
```

5-2 検査機能設定

通信検査機能に関する設定です。

(1) IPアドレスアクセス

ユーザーからリクエストされたURLのホスト名部がIPアドレスであった場合の動作の設定です。

以下のいずれかの動作を指定します。

(a) 「URLのIPアドレスを逆引きしない」

通常のURLと同様に、URL条件の適合検査を行います。

(b) 「URLのIPアドレスを逆引きしてルールを適用する」

DNSなどの名前解決システムを使ってIPアドレスをホスト名に変換した結果に対しても、URL条件の適合検査を行います。この場合、「逆引き不可の場合、禁止する」も同時に選択すると、逆引きの結果、IPアドレスに対応するホスト名が存在しなかった場合にアクセスを禁止します。

サーバーホストに名前解決システムの参照設定が必要です。

(2) URLDBアクセス失敗時のアクション

URLDB検索時にエラーが発生した場合の動作の設定です。

以下のいずれかの動作を指定します。

(a) 「中継」

アクセスを中継します。

(b) 「禁止」

アクセスを禁止します。

(c) 「続行」

URLがどのカテゴリにも登録されていないものとみなして処理を続行します。

(3) 警告アクション

(a) 警告解除時間

規制ルール適合検査の結果が「警告」になった場合、ユーザーに警告画面を応答する時間間隔(秒)を指定します。この時間内に再び「警告」が発生しても、警告画面は表示されません。この時間経過後に「警告」が発生した場合は、警告画面が再び表示されます。

(b) 解除中でも異なるルールにマッチした場合は警告画面を表示する

チェックした場合、(a)で設定した警告時間内であっても、異なる規制ルールの適合検査の結果が「警告」になった場合、再びユーザーに警告画面を表示します。チェックしない場合、異なる規制ルールの適合結果が「警告」であっても、(a)で設定した時間内であれば警告画面を表示せず、HTTP リクエストをそのまま中継します。

(4) オーバーライドアクション**(a) 解除中でも異なるルールにマッチした場合はオーバーライド画面を表示する**

チェックした場合、オーバーライド中であっても、異なる規制ルールの適合検査の結果が「オーバーライド」になった場合、再びユーザーにオーバーライド画面を表示します。チェックしない場合、異なる規制ルールの適合結果が「オーバーライド」であっても、オーバーライド中であればオーバーライド画面を表示せず、HTTP リクエストをそのまま中継します。

(5) 警告/オーバーライド管理用メモリサイズ

最後に警告及びオーバーライド画面を応答した時刻を管理するためのメモリサイズ(バイト)を指定します。

(6) 最大外部送信データ検査/保存サイズ

検査、保存を行う外部送信データの最大サイズ(Mバイト)を指定します。

この内容は複数台構成一括設定対象です。

5-3 ユーザー認証設定

プロキシ認証の設定です。

WEBGUARDIANではプロキシ認証によってトランザクション単位でユーザーの認証名を特定します。

使用可能な認証方式は、「LDAP 認証」「独自認証」「シングルサインオン (NTLM 認証)」です。

(1) 基本設定

プロキシ認証の基本設定を行います。

(a) プロキシ認証

プロキシ認証を使用しない場合は「オフ」を、使用の場合は「LDAP 認証」「独自認証」「シングルサインオン (NTLM 認証)」のいずれかを指定します。

(b) 領域名

認証領域 (realm) の名前を指定します。指定した名前は、ウェブブラウザの認証ダイアログに表示されます。

設定値は ASCII 文字コードにのみ対応しています。

「LDAP 認証」もしくは「独自認証」を選択した場合のみ有効になります。

(c) キャッシュ有効時間

認証結果をキャッシュする時間 (秒) を指定します。

「LDAP 認証」もしくは「独自認証」を選択した場合のみ有効になります。

(d) キャッシュサイズ

認証結果をキャッシュとして保管する共有メモリのサイズ (バイト) を指定します。

「LDAP 認証」もしくは「独自認証」を選択した場合のみ有効になります。

(e) 認証除外リクエスト

特定の条件を満たすリクエストについては認証を行わない場合、当該リクエストの条件を指定します。

(2) LDAP認証設定

プロキシ認証で「LDAP 認証」を指定した場合、以下のパラメータを設定してください。

(a) LDAPサーバー

LDAP サーバーホストの IP アドレスとポート番号を設定してください。

(b) バインドDN

ユーザーエントリー検索時のバインドDNを設定してください。

設定されていない場合は匿名バインドを行います。

設定値はASCII文字コードにのみ対応しています。

(c) バインドパスワード

ユーザーエントリー検索時のバインドパスワードを設定してください。

設定されていない場合は匿名バインドを行います。

設定値はASCII文字コードにのみ対応しています。

(d) 検索ベースDN

ユーザーエントリー検索時の起点DNを設定してください。

設定値はASCII文字コードにのみ対応しています。

(e) 検索オブジェクトクラス

ユーザーエントリーのオブジェクトクラス名を設定してください。

値が「*」の場合は、全てのオブジェクトクラスが対象となります。

設定値はASCII文字コードにのみ対応しています。

(f) 認証名属性

ユーザーエントリーの認証名として扱う属性名を設定してください。

設定値はASCII文字コードにのみ対応しています。

(3) 独自認証設定

プロキシ認証で「独自認証」を指定した場合、以下のパラメータを設定してください。

(a) パスワード有効期限

パスワードの有効期限（日）を指定します。0を指定すると無期限とみなされます。

プロキシ認証時にユーザーが入力したパスワードの有効期限が切れている場合、

ユーザーにパスワード変更を促します。

(b) 初期パスワード変更機能

初期設定されたパスワードをユーザーに変更させる機能です。

プロキシ認証時にユーザーが入力したパスワードが管理者により登録された初期値である場合、ユーザーにパスワード変更を促します。

(4) シングルサインオン(NTLM認証)設定

プロキシ認証で「シングルサインオン(NTLM認証)」を指定した場合、以下のパラメータを設定してください。

(a) ドメイン

ユーザーが所属するドメインをNetBIOSドメイン名で指定します。Windowsクライアントからユーザーが所属するドメインがWEBGUARDIANに送信されなかった場合、ここに指定した値をユーザーが所属するドメインとして使用します。

(b) プライマリドメインコントローラ

プライマリドメインコントローラをNetBIOSコンピュータ名で指定します。

(c) バックアップドメインコントローラ

プライマリドメインコントローラをNetBIOSコンピュータ名で指定します。
プライマリドメインコントローラが停止している場合、WEBGUARDIANはここに指定したドメインコントローラに認証情報を問い合わせます。



プライマリドメインコントローラと通信ができない場合にバックアップドメインコントローラに認証情報を問い合わせます。この際、プライマリドメインコントローラとの通信がTCP/IPの再送タイムアウトとなるまで、認証情報の問い合わせ先がバックアップドメインコントローラに切り替わりません。TCP/IPの再送タイムアウトは通常Solaris、Linuxとも3分以上に設定されていますので、プライマリドメインコントローラとの通信失敗時の切り替え時間を短縮したい場合は、TCP/IPパラメータの設定を変更する必要があります。

TCP/IPの再送タイムアウトに関する設定の確認方法は「8 トラブルシューティング」-「(11) TCP/IPの再送タイムアウトに関する設定の確認」(115ページ)をご参照ください。

この内容は複数台構成一括設定対象です。

5-4 メール通知設定

規制ルールや例外ルールに適合するリクエストがあった場合に、管理者または代替管理者へ電子メールで通知する機能の設定です。

(1) 管理者メールアドレス

デフォルトの送信宛先アドレスを設定してください。

複数のアドレスを指定することはできません。

(2) メール通知文

通知内容をカスタマイズすることができます。

メール標題と差出人アドレス、本文を設定できます。

本文では、リクエストに関する情報を埋め込むために以下の変数を記述することができます。

- | | |
|---------------------|---|
| (a) \$DATE | : 日時 |
| (b) \$TID | : リクエストのトランザクション ID |
| (c) \$UID | : 認証名 |
| (d) \$IP | : IP アドレス |
| (e) \$URL | : リクエスト URL |
| (f) \$QUERY | : クエリー文字列 |
| (g) \$CATEGORY | : カテゴリ |
| (h) \$RULE | : 適合した規制ルール名または例外ルール名 |
| (i) \$RULE_ID | : 適合した規制ルール ID または例外ルール ID |
| (j) \$KEYWORD | : 適合した規制ルールにキーワード条件があった時見つかったキーワード文字列 |
| (k) \$ATTACHMENT | : MIME タイプ / 個人情報 / ファイルタイプ / パスワードのいずれかの条件に適合した添付ファイル名 |
| (l) \$PI_INDEX | : 個人情報総合指数 (1) |
| (m) \$PI_COUNT | : 個人情報件数 (1) |
| (n) \$PI_TYPE_COUNT | : 個人情報項目数 (0 ~ 7 の値) (1) |
| (o) \$PI_DENSITY | : 個人情報密度 (0 ~ 100 の値、単位は %) (1) |
| (p) \$FILENAME | : ダウンロードサイズ制限に適合したダウンロードデータのファイル名 |
| (q) \$CONTENT_TYPE | : ダウンロードサイズ制限に適合したダウンロードデータの Content-Type |
| (r) \$SIZE | : ダウンロードサイズ制限に適合したダウンロードデータのサイズ |
- (1) 適合した規制ルールに個人情報条件があった時。



- ・個人情報検査対象パートが複数ある場合、総合指数が最大のパート(複数存在する場合はその内最初に出現するパート)の総合指数/個人情報件数/個人情報項目数/個人情報密度が、それぞれ \$PI_INDEX/\$PI_COUNT/\$PI_TYPE_COUNT/\$PI_DENSITY の値となります。
- ・ダウンロードデータのファイル名は、Content-Disposition レスポンスヘッダーの filename パラメータが取得可能な場合はその値となり、そうでない場合は URL のファイル名部の値となります。いずれも存在しない場合、ファイル名は空となります。

< 本文設定値例 >

以下のウェブトランザクションを検知しました。

日時	: \$DATE
トランザクション ID	: \$TID
認証名	: \$UID
IP アドレス	: \$IP
リクエスト URL	: \$URL
パラメータ	: \$QUERY
カテゴリ	: \$CATEGORY
適合ルール	: \$RULE
キーワード	: \$KEYWORD
添付ファイル	: \$ATTACHMENT
個人情報総合指数	: \$PI_INDEX
個人情報件数	: \$PI_COUNT
個人情報項目数	: \$PI_TYPE_COUNT
個人情報密度	: \$PI_DENSITY

この内容は複数台構成一括設定対象です。

5-5 キャッシュ設定

ユーザーからリクエストされたHTTPコンテンツをキャッシュさせる機能の設定です。

(1) 基本設定

キャッシュ機能

キャッシュ機能の有効化・無効化を設定します。

初期値は「オフ」に設定されています。

キャッシュ保存ディレクトリ

キャッシュの保存先ディレクトリを指定します。

初期値は設定されていません。



キャッシュ保存ディレクトリを作成する場合は、ディレクトリのオーナー「nobody」、パーミッションモード「0755」で作成してください。

(2) 動作設定

キャッシュ除外URL

キャッシュしたくない特定のURLを指定します。

URLは、英字の大文字、小文字は区別せず、同一視します。

URLには、完全一致の文字列を指定してください。

URLはワイルドカード文字「*」を使用できます。

ワイルドカード文字「*」は、長さ0以上の任意の文字列にマッチします。

初期値は設定されていません。

最大キャッシュ保存サイズ

キャッシュ保存ディレクトリにキャッシュ可能なHTTPコンテンツの最大サイズを指定します。

初期値は「1」Mバイトに設定されています。

最小キャッシュ保存サイズ

キャッシュ保存ディレクトリにキャッシュ可能なHTTPコンテンツの最小サイズを指定します。

初期値は「1」バイトに設定されています。

最大キャッシュ有効時間

キャッシュ保存ディレクトリにキャッシュされたHTTPコンテンツの最大有効時間を指定します。

初期値は「86400」秒（1日）に設定されています。



有効時間を経過したキャッシュは、キャッシュ保存ディレクトリに存在していても使用されません。

(3) キャッシュ保存ディレクトリ管理

キャッシュの削除は、htcacheclean (キャッシュ削除コマンド) が実施します。htcacheclean は、キャッシュ機能が「オン」に設定された場合のみ、デーモンとして起動します。htcacheclean の引数である「キャッシュ保存ディレクトリ制限値」と「メンテナンス間隔」を設定してください。

キャッシュ保存ディレクトリ制限値

キャッシュ保存ディレクトリのキャッシュ保存可能サイズを指定します。初期値は「1024」M バイトに設定されています。

メンテナンス間隔

キャッシュ保存ディレクトリ以下のキャッシュの削除処理を繰り返す間隔時間を指定します。初期値は「30」分に設定されています。



- ・キャッシュ機能を「オン」に設定すると、htcacheclean を起動します。また、キャッシュ機能を「オフ」に設定すると、htcacheclean を停止します。
- ・キャッシュ機能が「オン」に設定された状態で、キャッシュ保存ディレクトリ制限値やメンテナンス間隔の値を設定変更すると、htcacheclean が再起動します。
- ・キャッシュ保存ディレクトリには、キャッシュファイル以外に管理用のディレクトリが作成されるため、メンテナンス後もディスク使用量がキャッシュ保存ディレクトリ制限値以下とならない場合があります。また、メンテナンス実施後から次のメンテナンス実施までの間、キャッシュ保存ディレクトリの使用量は増加し続けます。そのため、キャッシュ保存ディレクトリ制限値にはディスク空き容量に対して十分余裕のある値を設定してください。

5-6 プロキシ多段構成時の設定

プロキシが多段で構成されている場合、X-Forwarded-Forヘッダーを使用してユーザーの利用端末のIPアドレスをプロキシサーバー間で送受することができます。

(1) WEBGUARDIANの下位にプロキシサーバーが存在する場合

下位プロキシサーバーが送信したX-Forwarded-Forヘッダーから、クライアントIPアドレスを取得することができます。

設定方法

管理サーバー上で /opt/Guardian/Admin/etc/admin/server/<ID>/httpd.conf を直接編集し、以下の設定を追加します。

設定例)

```
WGFollowXForwardedFor On
WGTrustedProxy 192.168.0.1          # 下位プロキシサーバーの IP アドレス
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

クライアントIPアドレスの読み替え対象

X-Forwarded-For ヘッダーから取得した IP アドレスは、以下の箇所で利用されます。

分類	対象
アクセス制御	グループ定義（IPアドレス/ネットワークアドレスの判定）
	警告アクション（警告を行ったクライアントの管理） ※プロキシ認証を使用しない場合のみ
ロギング	外部送信ログ、規制ログ、例外ログ、SSLログ、アクセスログに記録するIPアドレス
表示	ブロック画面に出力するクライアントIPアドレス
	メール通知文に出力するクライアントIPアドレス

注意点

下位プロキシサーバーが送信したX-Forwarded-Forヘッダーは、デフォルトではそのまま上位サーバーに送信されます。

下位プロキシサーバーが送信したX-Forwarded-Forヘッダーを上位サーバーへ送信したくない場合は、管理サーバー上で /opt/Guardian/Admin/etc/admin/server/<ID>/httpd.conf を直接編集し、以下の設定を追加します。

```
ProxyXForwardedFor Block
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

(2) WEBGUARDIANの上位にプロキシサーバーが存在する場合

WEBGUARDIANが直接通信するクライアントのIPアドレスを、X-Forwarded-Forヘッダーで上位プロキシサーバーに渡すことができます。

管理サーバー上で/opt/Guardian/Admin/etc/admin/server/<ID>/httpd.confを直接編集し、以下の設定を追加します。

```
ProxyXForwardedFor On
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

6 仕様

本章では、日本語検査機能、各設定ファイルの仕様について解説します。

6-1 日本語検査機能仕様

(1) 対応日本語文字コード

検査対象データの文字コードとしては、EUC-JP、Shift-JIS、ISO-2022-JP、UTF-8、UTF-7に対応しています。機種依存文字、ユーザー定義文字には対応していません。

送信テキストデータの文字コードを特定するヘッダー情報がないというウェブ通信の性質上、対象データを走査して機械的に文字コード判定を行っております。このため文字長が短い場合など判定が困難なケースがあり、判定を誤る場合があります。

(2) メッセージ検査範囲

HTTPのリクエストメッセージ中のキーワード検査範囲について解説します。

(a) URLのクエリー部

リクエストURLにクエリー部が含まれる場合、クエリー部だけを抜きだし、MIMEタイプが「application/x-www-form-urlencoded」のデータとしてデコードしキーワード検査を実施します。文字エンコーディングは自動判定します。

(b) メッセージボディ部

リクエストメソッドがPOSTやPUTの場合のように、リクエストにメッセージボディ部が含まれている場合に、メッセージボディ部を対象にキーワード検査を実施します。ただし、メッセージボディ部のMIMEタイプ形式によって検査方法が異なります。メッセージボディ部のMIMEタイプは、Content-Typeヘッダーの値で判断しています。

なお、添付ファイルについてはファイル内容の識別を行っており、Content-Typeヘッダーの値が以下に説明するものとは異なっても、キーワード検査を実施します。「添付ファイル」の定義は、filenameパラメータがあるパートです。

(b-1) プレインテキストの場合

Content-Typeヘッダー値が、「text/*」の形をしている場合です。

この場合、対象データがインスタントメッセージングのメッセージであるかどうかを判定し、メッセージである場合はテキストを抽出し、キーワード検査を実施します。

インスタントメッセージのキーワード検査対象範囲は以下のとおりです。

サービス	キーワード検査対象
Windows Live メッセンジャー	インスタントメッセージ
Yahoo! メッセンジャー	インスタントメッセージ チャット／カンファレンスで送信されるメッセージ
AOL インスタント・メッセンジャー	インスタントメッセージ チャットで送信されるメッセージ
ICQ	インスタントメッセージ

※対応クライアントは、Windows Messenger Ver4.7, 5.1、Yahoo! メッセンジャー Ver7.0、

AOL インスタント・メッセンジャー Ver5.1、ICQ Ver6.5です（2010年1月現在）。

※HTTPSプロトコルを使用した通信は対象外です。

※ファイル送信は対象外です。

対象データがインスタントメッセージのメッセージではない場合、対象データをそのまま文字コード判定し、対応文字コードの場合はキーワード検査を実施します。

(b-2) URLエンコード文字列の場合

Content-Type ヘッダー値が、「application/x-www-form-urlencoded」の形をしている場合です。

対象データのURLエンコーディングを復号し、結果に対して文字コード判定し、対応文字コードの場合はキーワード検査を実施します。

(b-3) アプリケーションデータ

Content-Type ヘッダー値が、以下のいずれかの値である場合です。

application/pdf

application/msword

application/vnd.openxmlformats-officedocument.wordprocessingml.document

application/vnd.openxmlformats-officedocument.wordprocessingml.template

application/vnd.ms-word.document.macroEnabled.12

application/vnd.ms-word.template.macroEnabled.12

application/vnd.ms-excel

application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

application/vnd.openxmlformats-officedocument.spreadsheetml.template

application/vnd.ms-excel.sheet.macroEnabled.12

application/vnd.ms-excel.template.macroEnabled.12

application/vnd.ms-powerpoint

application/vnd.openxmlformats-officedocument.presentationml.presentation

application/vnd.openxmlformats-officedocument.presentationml.slideshow

application/vnd.openxmlformats-officedocument.presentationml.template

application/vnd.ms-powerpoint.presentation.macroEnabled.12
application/vnd.ms-powerpoint.slideshow.macroEnabled.12
application/vnd.ms-powerpoint.template.macroEnabled.12
application/x-js-jxw
application/x-js-taro
application/octet-stream

この場合、対象データに対して以下で説明するテキスト抽出処理を実施し、取り出した文字列に対してキーワード検査を実施します。

共通

ユーザー定義文字、機種依存文字の検査はできません。

Microsoft WORD Ver. 6, 95, 97, 98, 2000, 2001 for Mac, 2002, 2003, 2007

図形、注釈参照、頭注参照、ページ番号は検査できません。

箇条書き段落番号は検査できません。

パスワード設定されたドキュメントは検査できません。

Microsoft の IRM (Information Rights Management) 機能を使用し、ドキュメントへのアクセス制限を設定したファイルの検査はできません。

Word97からWord95形式で下位保存された文書ファイルは拡張子がDOCとなりますが、実際のファイル形式はRTF (Rich Text Format) なので検査できません。

Microsoft Excel Ver. 4, 5, 95, 97, 98 for Mac 2000, 2001 for Mac, 2002, 2003, 2007

セルの内容をテキストとして検査します。図形は検査できません。

パスワード設定されたドキュメントは検査できません。

「シートの保護」を設定したファイルは検査できますが、「ブックの保護」を設定されたファイルは検査できません。

IRM機能を使用し、ドキュメントへのアクセス制限を設定したファイルの検査はできません。

Excel2007のバイナリブック形式の検査はできません。

Excel2007では、小数点以下の数値が検出できない場合があります。

Microsoft PowerPoint 95, 97, 2000, 2001 for Mac, 2002, 2003, 2007

スライドとノートのテキストが検査対象です。

図形、スライド番号は検査できません。

パスワード設定されたドキュメントは検査できません。

IRM機能を使用し、ドキュメントへのアクセス制限を設定したファイルの検査はできません。

ジャストシステム 一太郎Ver.7, 8, 9, 10, 11, 12, 13, Lite, 2004, 2005, 2006, 2007

図枠、付箋、差入枠、オブジェクト枠、レイアウト枠は検査できません。

パスワード設定されたドキュメントは検査できません。

圧縮形式で保存されたファイルは検査できません。

PDF Ver. 1.2, 1.3, 1.4, 1.5, 1.6, 1.7

「書式なしテキストのメタデータを有効にする」と指定されている場合、検査できません。

立体文字、文字の重ねで表示されている強調文字については、多重に検出したり、また検出できなかつたりする場合があります。

図形、グラフィックスは検査できません。

「文書を開くパスワード」が設定された PDF ファイルの検査はできません。

独自のセキュリティハンドラを定義して使用している場合、検査できません。

文字間の空白が無視、または挿入されることがあるため、キーワードを誤検出したり、また検出できなかつたりする場合があります。

TYPE3 フォント、ベクトルフォントの文字は検出できません。

ScanSnap で作成されたフォントが「NotDefSpecial」で、PDF 内で「Adobe-Identity-UCS」の Cmap エンコーディングを参照している PDF ファイルは検査できません。

PDF ファイル内、FlateDecode, LZWDecode, ASCII85Decode, RunLengthDecode 以外で圧縮されたデータは検査できません。



アプリケーションデータ(特にサイズが1 MB以上のPDF)の一部について、テキスト抽出処理に時間を要し、リクエストの完了に時間がかかる場合があります。ご了承ください。

(b-4) マルチパートの場合

各パートに分割し、各パートに対して上記(b-1)から(b-3)の検査を行います。キーワード検査結果はパート単位で独立です。

つまり、1番目のパートで「キーワード1」が見つかり、2番目のパートで「キーワード2」が見つかった場合、キーワード条件式「キーワード1」や「キーワード2」は条件を満たすこととなりますが、「キーワード1&キーワード2」は条件を満たさないと判断されます。

(b-5) 画像データ等その他の場合

画像、動画、音声データ、また圧縮ファイルに対してはキーワード検査を実施しません。

(3) メッセージ検査範囲外

リクエストの中の以下の箇所は、キーワード検査対象外ですのでご注意ください。

- ・ Cookie ヘッダー値
- ・ Content-Disposition ヘッダーの属性値
 - form パラメータ値 (フォームパラメータ名)
 - filename パラメータ値 (添付ファイル名)



送信データがHTML フォームデータの場合、送信内容が同じでも、MIME タイプが「application/x-www-form-urlencoded」の場合と「multipart/form-data」の場合とでは、検査結果が異なります。

「multipart/form-data」の場合は、各属性名 / 属性値の組単位でキーワード検査結果が独立です。また、パラメータ名が検査対象になりません。

「application/x-www-form-urlencoded」の場合は、属性名 / 属性値の組を全て連結したのに対してキーワード検査を実施します。また、パラメータ名も検査対象になります。

以下の各例メッセージの中で、反転している箇所がキーワード検査対象領域になります。

例1) メソッド POST URL エンコーディングのケース

```
POST http://XXXXX/search.cgi HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; U; Linux i686; ja-JP; rv:1.7.8) Gecko/20050517
Firefox/1.0.4 (Debian package 1.0.4-2)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: ja,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://XXXXX/manual/index.html
Cookie: XX_Session_Name=point; XX_Session_Value=%B5%A1%CC%A9%BE%F0%CA%F3%0A
Proxy-Authorization: Basic XXXXXXXXXXXXXXXXXXXX
Content-Type: application/x-www-form-urlencoded
Content-Length: 64

tag=search&for=html&keyword=%A5%AC%A1%BC%A5%C7%A5%A3%A5%A2%A5%F3
```

例2) メソッドGET のケース

```
GET http://XXXXX/cgi-bin/hoge.cgi?page=%C6%C3%B5%F6%C6%E2%CD%C6%0A HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; U; Linux i686; ja-JP; rv:1.7.8) Gecko/20050517
Firefox/1.0.4 (Debian package 1.0.4-2)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;
q=0.8,image/png,*/*;q=0.5
Accept-Language: ja,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
Proxy-Authorization: Basic XXXXXXXXXXXXXXXXX
```

例3) マルチパート フォームデータのケース

```
POST http://XXXXX/security/index.cgi HTTP/1.0
Host: XXXXX
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; ja-JP; rv:1.7.8) Gecko/
20050511 Firefox/1.0.4
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;
q=0.8,image/pn
g,*/*;q=0.5
Accept-Language: ja,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: EUC-JP,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Proxy-Authorization: Basic XXXXXXXXXXXXXXXXX
Content-Type: multipart/form-data; boundary=-----
24464570528145
Content-Length: 756

-----24464570528145
Content-Disposition: form-data; name="encode_hint"

あ
-----24464570528145
Content-Disposition: form-data; name="plugin"

attach
-----24464570528145
Content-Disposition: form-data; name="pcmd"

post
-----24464570528145
Content-Disposition: form-data; name="title"

セキュリティ / 説明
-----24464570528145
Content-Disposition: form-data; name="max_file_size"

6000000
-----24464570528145
Content-Disposition: form-data; name="attach_file"; filename="account1st.txt"
Content-Type: text/plain

ここに顧客情報が含まれて ...
-----24464570528145--
```

(4) プロパティ情報のキーワード検索機能

アプリケーションデータからのテキスト情報抽出では、アプリケーションデータのプロパティ情報はデフォルトでは抽出されません。プロパティ情報を抽出対象とする方法について以下で説明します。

設定方法

管理サーバー上で /opt/Guardian/Admin/etc/wg/httpd.conf を直接編集し、以下の設定を追加します。

設定例)

```
WGTextGetProperty      On
WGTextPropertyTitle    "[title]"
WGTextPropertyAuthor   "[author]"
WGTextPropertyKeyword   "[keyword]"
WGTextPropertySubject   "[subject]"
WGTextPropertyComment   "[comment]"
WGTextPropertyManager   "[manager]"
WGTextPropertyCompany   "[company]"
WGTextPropertyCategory  "[category]"
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

動作

WGTextGetProperty パラメータが On の場合、アプリケーションから抽出するテキスト情報の末尾に、以下の例のようにプロパティ情報が追加されます。

```
[title] 報告書
[author]
[keyword]
[subject]
[comment] 社外秘
[manager]
[company] ABC 株式会社
[category]
```

[title] 等は、WGTextPropertyTitle パラメータ等で設定される文字列

設定項目一覧

プロパティ抽出用の設定項目を以下に示します。

パラメータ	構文	デフォルト	説明
WGTextGetProperty	On Off	Off	Onの場合、プロパティ情報のテキスト抽出を行う
WGTextPropertyTitle	文字列	未定義	タイトルプロパティ値の前に付加するラベル
WGTextPropertyAuthor	文字列	未定義	作者プロパティ値の前に付加するラベル
WGTextPropertyKeyword	文字列	未定義	キーワードプロパティ値の前に付加するラベル
WGTextPropertySubject	文字列	未定義	サブジェクトプロパティ値の前に付加するラベル
WGTextPropertyComment	文字列	未定義	コメントプロパティ値の前に付加するラベル
WGTextPropertyManager	文字列	未定義	管理者プロパティ値の前に付加するラベル
WGTextPropertyCompany	文字列	未定義	会社プロパティ値の前に付加するラベル
WGTextPropertyCategory	文字列	未定義	分類プロパティ値の前に付加するラベル

プロパティ抽出仕様

プロパティ抽出の対応アプリケーションと、各アプリケーションで抽出可能なプロパティは以下のとおりです。

	2007	xls	doc	ppt	pdf	jtd
タイトル	○	○	○	○	○	○
作者	○	○	○	○	○	○
キーワード	○	○	○	○	○	○
サブジェクト	○	○	○	○	○	
コメント	○	○	○	○		○
管理者		○	○	○		
会社	○	○	○	○		
分類	○	○	○	○		

2007 : Microsoft Word 2007/Excel 2007/PowerPoint 2007

xls : Microsoft Excel Ver4/Ver5/Ver7(95)/97/98 for Mac/2000/2001 for Mac/XP/2003

doc : Microsoft Word Ver6/Ver7(95)/97/98/2000/2001 for Mac/XP/2003

ppt : Microsoft PowerPoint 95/97/2000/2001 for Mac/XP/2003

pdf : Adobe PDF 1.2/1.3/1.4/1.5/1.6

jtd : JUSTSYSTEM 一太郎 7/8/9/lite/10/11/12/13/2004/2005/2006

(5) 個人情報検査

個人情報検査は、添付ファイルを対象とします。「添付ファイル」の定義は、filenameパラメータがあるパートです。

検査可能なデータの種類の、前述のキーワード検査の仕様と同じです。

なお、管理サーバー上で/opt/Guardian/Admin/etc/wg/httpd.confに設定を記述することで、添付ファイル以外のキーワード検査対象データを個人情報検査の対象とすることができます。



プロキシ性能が低下する場合があります。

設定例)

```
WGPIInfoTarget attachment text
```

設定ファイル編集後に、管理サーバーで以下のコマンドを実行し、検査サーバーに設定を反映してください。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

WGPIInfoTargetパラメータの値の意味は以下のとおりです。

値	個人情報検査対象
attachment	添付ファイル 「添付ファイル」の定義は、filenameパラメータがあるパートです。 検査可能なデータの種類の、キーワード検査の仕様と同じです。
text	添付ファイル以外の、キーワード検査対象データ

6-2 プロキシー設定ファイル

(1) 設定ファイル配置

検査サーバー：

/opt/Guardian/WG/conf/httpd.conf

管理サーバー：

< 共通設定項目 >

/opt/Guardian/Admin/etc/wg/httpd.conf.tpl

/opt/Guardian/Admin/etc/wg/httpd.conf

< 個別設定項目 >

/opt/Guardian/Admin/etc/admin/server/<server-id>/httpd.conf

(2) 設定項目

WGAAuthEnabled :On/Off

LDAP 認証と独自認証を有効にするかを指定

On : 有効

Off : 無効

初期値: Off

WGAAuthCacheSpaceSize :数値

LDAP 認証と独自認証で使用するユーザー情報キャッシュ領域の大きさ (バイト)

初期値: 102400

WGAAuthCacheTTL :数値

LDAP 認証と独自認証で使用するユーザー情報キャッシュ時間 (秒)

初期値: 3600

WGAAuthWith :ldap/file

WGAAuthEnabled が On の場合に LDAP 認証と独自認証のどちらを使用するかを指定

ldap : LDAP サーバー

file : 独自認証

初期値: ldap

WGAAuthPasswdFile :/opt/Guardian/WG/conf/.userpasswd

独自認証機能が有効時に使用する認証データベースファイル

「/opt/Guardian/WG/conf/.userpasswd」を変更することはできません。

初期値: /opt/Guardian/WG/conf/.userpasswd

WGAAuthPasswdExpire :数値

独自認証機能が有効時のパスワードの有効期限(日)

初期値: 0

WGAAuthChangeIniPasswd :On/Off

独自認証有効時の初期パスワード変更機能の指定

On : 有効

Off : 無効

初期値: Off

WGAAuthChangePasswdSSL :On/Off

独自認証有効時にSSLでパスワード変更を行うかの指定

On : https を使用

Off : http を使用

初期値: Off

WGAAuthAdminPort :数値

独自認証機能有効時にユーザーがパスワード変更する際にアクセスするサーバーのポート番号を指定

初期値: 8800

WGAAuthAdminPortSSL :数値

独自認証機能有効時にユーザーがパスワード変更する際にSSLでアクセスするサーバーのポート番号を指定

初期値: 4443

WGAAuthLDAPHost :IPアドレス:ポート番号

LDAPサーバーホストのIPアドレスとポート番号

ポート番号の初期値: 389

初期値: なし

WGAAuthLDAPSearchBase :DN形式(ただしASCII文字列)

ユーザーエントリー検索時の起点DN

初期値: なし

WGAAuthLDAPSearchBindDN :DN形式(ただしASCII文字列)

ユーザーエントリー検索時のバインドDN

設定されていない場合は匿名バインド

初期値: なし

WGAUTHLDAPSEARCHPASSWD :ASCII文字列

ユーザーエントリー検索時のバインドパスワード
設定されていない場合は匿名バインド
初期値：なし

WGAUTHLDAPDEREF :never/always/search|find

LDAP エリアスの実体参照をどのように行うかの指定
初期値：always

WGAUTHLDAPUIDATTRIBUTE :ASCII文字列

ユーザーエントリーの認証名として扱う属性名
初期値：なし

WGAUTHLDAPOBJECTCLASS :ASCII文字列

ユーザーエントリーのオブジェクトクラス名
初期値：*

WGAUTHLDAPREFERRALS :On/Off

他のサーバーへの参照が応答に含まれていた場合の動作の指定
On の場合、参照をたどる
初期値：On

NTLMAuth :On/Off

NTLM 認証を有効にするかを指定
On : 有効
Off : 無効
初期値：Off

NTLMDomain :文字列(15文字以内の半角英数字、-(ハイフン)、_(アンダーバー))

NTLM 認証を行う場合にユーザーが所属するドメインを NetBIOS ドメイン名で指定
初期値：なし

NTLMServer :文字列(15文字以内の半角英数字、-(ハイフン)、_(アンダーバー))

NTLM 認証を行う場合に認証を問い合わせるプライマリドメインコントローラを
NetBIOS コンピュータ名で指定
初期値：なし

NTLMBackup :文字列(15文字以内の半角英数字、-(ハイフン)、_(アンダーバー))
NTLM 認証を行う場合に認証を問い合わせるバックアップドメインコントローラを
NetBIOS コンピュータ名で指定
初期値: なし

WGLicenseKey :ASCII文字列
WEBGUARDIANのライセンスキーコード
初期値: 試用版ライセンスキーコード

WGHostID :数値(8桁の16進数、00000001-FFFFFFFF)
ホスト識別情報
指定されていない場合は、現在のホストの hostid 値
初期値: なし

WGPostFilter :On/Off
ルール検査機能のフラグ
初期値: On

WGLogAllRequest :On/Off
メッセージボディを含む場合だけでなく全てのリクエストデータの保存を指定するフ
ラグ
初期値: Off

WGResolveDestIP :On/Off
URL 比較時にリクエスト URL の IP アドレスからホスト名を解決する指定
初期値: Off

WGDenyNoPTR :On/Off
WGResolveDestIP が On の場合に、IP アドレスの逆引きの結果、PTR レコードが存在し
なかった時にアクセス禁止を指示するフラグ
初期値: Off

WGPostLogDir :ASCII文字列
ポストイメージファイル保存ディレクトリパス
初期値: /opt/Guardian/WG/var/queue

WGTempDir :ASCII文字列
一時ファイル保存ディレクトリパス
初期値: /var/tmp

WGTextCmd :ASCII文字列

テキスト抽出コマンド設定

初期値: command=sbin/wgtext args="wgtext -t %t -p -x %x -o %o %i"

WGTextGetProperty :On/Off

Onの場合、アプリケーションデータからのテキスト抽出で、プロパティ情報も抽出対象とする

初期値: Off

WGTextPropertyTitle :文字列

プロパティ情報抽出時、タイトルプロパティ値の前に付加するラベル

初期値: なし

WGTextPropertyAuthor :文字列

プロパティ情報抽出時、作者プロパティ値の前に付加するラベル

初期値: なし

WGTextPropertyKeyword :文字列

プロパティ情報抽出時、キーワードプロパティ値の前に付加するラベル

初期値: なし

WGTextPropertySubject :文字列

プロパティ情報抽出時、サブジェクトプロパティ値の前に付加するラベル

初期値: なし

WGTextPropertyComment :文字列

プロパティ情報抽出時、コメントプロパティ値の前に付加するラベル

初期値: なし

WGTextPropertyManager :文字列

プロパティ情報抽出時、管理者プロパティ値の前に付加するラベル

初期値: なし

WGTextPropertyCompany :文字列

プロパティ情報抽出時、会社プロパティ値の前に付加するラベル

初期値: なし

WGTextPropertyCategory :文字列

プロパティ情報抽出時、分類プロパティ値の前に付加するラベル

初期値: なし

WGTextTrustContentType :On/Off

Offの場合、Content-Typeヘッダーの値にかかわらずテキスト抽出及びキーワード検査を試みます

プロキシ性能が低下する場合があります

初期値: On

WGSscreenDBFile :ASCII文字列

キーワード検査辞書ファイル

初期値: data/dic/keywd.dic

WGInfoTarget :attachment/text

個人情報検査の検査対象を指定する

半角スペースで区切り複数指定が可能

attachment : 添付ファイルを検査対象とする

text : 添付ファイル以外の、キーワード検査対象データを検査対象とする

プロキシ性能が低下する場合があります

初期値: attachment

WGInfoTimeout :整数(0または10~9999)

個人情報検査タイムアウト時間(秒)

0の場合、タイムアウトしない

初期値: 60秒

WGInfoCmd :ASCII文字列

個人情報検査コマンド設定

初期値: command=sbin/wg_pinfo args="wg_pinfo -x %x -o %o %i"

WGInfoBufSize :整数(1048576~1073741824)

個人情報検査時に消費できるメモリの最大値を指定する(バイト)

初期値: 104857600

WGInfoTextSize :整数(0以上)

個人情報検査を実施するテキストサイズを指定する(バイト)

0以外の数値を設定した場合、検査対象ファイルの先頭から指定バイト数のテキストについて検査を実施します

0の場合、サイズによる制限なし

初期値: 0

WGInfoIndexOverflow : 整数(0 ~ 100)

個人情報検査時、消費メモリ量が一定値を超えた場合に出力される総合指数を指定する

0 ~ 100 の数値を指定した場合、個人情報検査時に使用可能なメモリを消費した時、常に指定された値が総合指数として出力されます

設定なしの場合、最大メモリ量に達するまでに検出された個人情報によって評価された総合指数が算出されます

初期値: なし

WGFileNameExtension : ASCII文字列

ファイルタイプに対して、有効と判定する拡張子を設定する。

初期値: WGFileNameExtension ZIP zip
WGFileNameExtension LHA lzh
WGFileNameExtension RAR rar
WGFileNameExtension CAB cab
WGFileNameExtension GZIP gz tgz
WGFileNameExtension BZIP2 bz2
WGFileNameExtension Z z
WGFileNameExtension TAR tar
WGFileNameExtension TEXT txt
WGFileNameExtension PDF pdf
WGFileNameExtension EXCEL xls xlsx xlsx xlt xltm
WGFileNameExtension WORD doc docx docm dotx dotm
WGFileNameExtension PPT ppt pps pptx pptm potx potm ppsx ppsm
WGFileNameExtension JTD jaw jbw juw jfw jvw jtd jtt
WGFileNameExtension HTML html htm
WGFileNameExtension XML xml
WGFileNameExtension RTF rtf
WGFileNameExtension VISIO vsd
WGFileNameExtension EXE exe

WGSideEffect : ASCII文字列

副作用アクション定義

初期値: 1 "mail notify" command=sbin/mail_notify.php wait=0ff

WGUseURLDB : On/Off

URLDB 機能のフラグ

初期値: On

WGURLDBSidFile :ASCII文字列

URLDB の共有メモリ ID 格納ファイル

初期値: /opt/Guardian/WG/var/logs/urlldb.sid

WGURLDBTimeout :数値

URLDB 検索タイムアウト時間 (秒)

初期値: 2

WGURLDBFailedAction :ASCII文字列

URLDB アクセス失敗時の動作

allow または deny

設定されていない場合はエラーを無視して処理を続行する

初期値: なし

WGWarnInterval :数値

ユーザーに警告画面を応答する時間間隔 (秒)

初期値: 3600

WGWarnEachRule :On/Off

警告解除時間中に異なるルールによる警告アクションが発生した場合に、警告画面を表示する

初期値: Off

WGOVERRIDEEachRule :On/Off

オーバーライド中に異なるルールによるオーバーライドアクションが発生した場合に、オーバーライド画面を表示する

初期値: Off

WGWarnShmemSize :数値

最後に警告及びオーバーライド画面を応答した時刻を管理するための共有メモリサイズ (バイト)

初期値: 102400

WGFollowXForwardedFor :On/Off

X-Forwarded-For ヘッダーからユーザー端末の IP アドレスを取得して、実際に通信を行っているクライアント IP アドレスの代わりにアクセス制御やロギングで使用する

初期値: Off

WGTrustedProxy :ASCII文字列

X-Forwarded-Forヘッダーからユーザー端末のIPアドレスを取得する場合に、信頼する下位プロキシのIPアドレスまたはホスト名

半角スペースで区切り複数指定が可能

allを指定した場合、全てのプロキシを信頼する

初期値：なし(全てのプロキシを信頼しない)

WGMaxRequestBodySize :数値

検査、保存処理を行う外部送信データの最大制限サイズ(バイト)

指定サイズを超える外部送信データの検査、保存は行いません

初期値：52428800(50MB)

HostHeaderCheck :On/Off

Onの場合、HostヘッダーのないHTTP/1.1リクエストに対してエラーを返す

初期値：On

ProxyBadHeader :IsError/Ignore/StartBody

上位サーバーからの応答に不正なヘッダー行が含まれている場合の動作

IsError : リクエストを中止して502(Bad Gateway)応答を返す

Ignore : 不正なヘッダー行を受信しなかったものとして扱う

StartBody : 最初の不正なヘッダー行を受信した時、ヘッダーの読取りを終了して残りをボディとして扱う

初期値：IsError

ProxyHttpFlushBuffer :On/Off

上位サーバーからの応答の読取りがブロックする場合、応答バッファの内容をネットワークに強制的に出力する

初期値：Off

ProxyFtpEnableEPSV :On/Off

FTPサーバーとのデータコネクション開設にEPSVコマンドを使用する

初期値：On

ProxyFtpEnablePASV :On/Off

FTPサーバーとのデータコネクション開設にPASVコマンドを使用する

初期値：On

ProxyFtpDataConnectionSetup :default/robust

robustの場合、FTPサーバーとのデータコネクション開設失敗時、別のコマンドを使用してデータコネクション開設を試みる

初期値: default

ProxyXForwardedFor :On/Off/Block

X-Forwarded-For ヘッダーに対する処理を指定する

Off : X-Forwarded-For ヘッダーに対して何も処理を行わない(下位プロキシサーバーがX-Forwarded-Forヘッダーを送信した場合、上位サーバーへそのまま送信する)

On : X-Forwarded-ForヘッダーにクライアントIPアドレスを付加して上位サーバーへ送信する

Block : X-Forwarded-For ヘッダーを削除し、上位サーバーへ送信しない

初期値: Off

WGAlternateHost :半角英数字、「.」-「_」

クライアントから送信されたオーバーライドコードを処理するための代替ホスト名

初期値: webguardian.local-proxy

6-3 ポリシー設定ファイル

(1) 設定ファイル配置

検査サーバー：

/opt/Guardian/WG/conf/wg.conf

管理サーバー：

< 共通設定項目 >

/opt/Guardian/Admin/etc/wg/wg.conf

< 個別設定項目 >

なし

(2) 設定項目

WGClientSet 数値 文字列 (ip=文字列)* (uid=文字列)* (ua=文字列)*

グループエントリー

複数定義可

定義済エントリー：

WGClientSet 1 "ストリーミング系ソフト" ua="Windows-Media-Player"

ua="RMA" ua="Winamp"

WGClientSet 2 "Windows Update" ua="Windows"

ua="CRetrieveObjectByUrl::InetSchemeProvider"

ua="Industry Update Control" ua="LegitCheck" ua="Microsoft BITS"

ua="Microsoft-CryptoAPI" ua="MS Clearing House Default Agent"

ua="Progressive Download" ua="Service Pack Setup"

WGSchedule 数値 文字列 (文字列)*

時間・曜日エントリー

複数定義可

定義済エントリー:なし

**WGURSet 数値 文字列 (url=文字列)* (category=文字列[:文字列[,文字列]])*
(host=文字列)***

URL グループエントリー

複数定義可

定義済エントリー :

```
WGURSet 1 " ウェブメール " url=http://*.mail.yahoo.co.jp/ym/Compose
url=http://*.mail.yahoo.co.jp/ym/Attachments
url=http://*.hotmail.msn.com/cgi-bin/premail*
url=http://*.hotmail.msn.com/cgi-bin/doattach
url=http://*.hotmail.msn.com/cgi-bin/AttachPhoto
url=http://*.mail.goo.ne.jp/goomail/index.ghtml
url=http://mail.excite.co.jp/top
url=http://mail.excite.co.jp/wmcgi/WMBridge.exe
url=http://email.www.infoseek.co.jp/sendmessage.php
url=http://email2.www.infoseek.co.jp/api/index.php
url=http://email2.www.infoseek.co.jp/api/upload.php
url=http://*.livedoor.com/cgi-bin/lldoor/dnet/xmail.cgi
url=http://mail.google.com/a/livedoor.com/
url=http://mail.google.com/mail/
```

```
WGURSet 2 "Windows Update" url=http://*update.microsoft.com/*
url=http://*.windowsupdate.com/* url=http://c.microsoft.com/*
url=http://activex.microsoft.com/* url=http://codecs.microsoft.com/*
url=http://crl.microsoft.com/* url=http://genuine.microsoft.com/*
url=http://w2ksp4.microsoft.com/* url=http://wustat.windows.com/*
url=http://www.microsoft.com/* url=https://*update.microsoft.com
url=https://mpa.one.microsoft.com
```

```
WGURSet 3 "ABC 株式会社 " url=http://*.abc.co.jp/*
```



日本語ドメイン名を使用したURLを指定する場合、ドメイン名部は全角文字ではなく ACE 形式 (ASCII 符号化形式) で記述します。

WGMIMESet 数値 文字列 (文字列)*

MIME タイプセットエントリー

複数定義可

定義済エントリー：

WGMIMESet 1 "URL エンコーディング" application/x-www-form-urlencoded

WGMIMESet 2 "イメージファイル" image/*

WGMIMESet 3 "マルチパート / 添付ファイル" multipart/*

WGMIMESet 4 "オフィスドキュメント" application/msword

application/vnd.ms-excel application/vnd.ms-powerpoint

WGKeywordSet 数値 文字列

キーワードセットエントリー

複数定義可

定義済エントリー：

WGKeywordSet 1 "機密"

WGDenyResponse 数値 文字列 file=文字列

禁止ブロック画面エントリー

複数定義可

定義済エントリー：

WGDenyResponse 1 "default" file=data/htdocs/DENY.html

WGOVERRIDEResponse 数値 文字列 file=文字列

オーバーライドブロック画面エントリー

複数定義可

定義済エントリー：

WGOVERRIDEResponse 1 "default" file=data/htdocs/OVERRIDE.html

WGWarnResponse 数値 文字列 file=文字列

警告ブロック画面エントリー

複数定義可

定義済エントリー：

WGWarnResponse 1 "default" file=data/htdocs/WARN.html

WGExpRule 数値 文字列 [sc=数値] [tc=数値] [dc=数値] ¥**[ml=文字列[|文字列]*] [size[>|=|<|>=|<=]数値] ¥****[effect=数値]**

例外ルールエントリー

複数定義可

定義済エントリー：

WGExpRule 1 "ストリーミング系ソフト" sc=1

WGExpRule 2 "Windows Update" sc=2 dc=2

WGACRule 数値 文字列 [sc=数値] [tc=数値] [dc=数値] ¥**[ml=文字列[|文字列]*] [mc=数値] [wc=数値] [pi_index[>|=|<|>=|<=]数値] ¥****[size[>|=|<|>=|<=]数値] [filetype=文字列[+文字列]*[:文字列]] ¥****[im=文字列[,文字列]*] [password=文字列] ¥****[action=文字列[:文字列]] [effect=数値] [size_i>=数値] ¥****[action_i=文字列[:文字列]]**

規制ルールエントリー

複数定義可

定義済エントリー：

WGACRule 1 "添付ファイル送信" mc=3 action=remark

WGACRule 2 "オフィスファイル送信" mc=4 action=remark

WGACRule 3 "機密を含むデータ送信" wc=1 action=remark effect=1

6-4 外部送信データのアーカイブ処理

(1) 概要

クライアントが送信した外部送信データは、キューディレクトリ (/opt/Guardian/WG/var/queue) に出力された後、STORE サーバー (wg_store) がログ保存ディレクトリにアーカイブします。

(2) 外部送信データの保存処理

リクエストにメッセージボディが含まれている場合、メッセージボディの内容を外部送信データとしてキューディレクトリに保存します。

ただし、以下のいずれかの条件を満たす場合、外部送信データの保存は行いません。

(a) 当該リクエストが例外ルールに適合する場合

(b) 外部送信データのサイズが、最大外部送信データ検査/保存サイズを超過する場合

最大外部送信データ検査/保存サイズの設定変更方法については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~ 』の「3-4-3-1 基本設定」の「最大外部送信データ検査 / 保存サイズ」(318 ページ) をご参照ください。

(3) STORE サーバーの動作

STORE サーバー (wg_store) は、15 秒間隔でアーカイブ処理を行います。アーカイブ処理では、キューディレクトリのファイルを順に確認し、外部送信データがあれば子プロセスを生成して、子プロセスが外部送信データをログ保存ディレクトリにアーカイブします。

子プロセスは、WEBGUARDIAN Ver3.5 以前では最大 6 個、Ver3.6 以降では最大 48 個まで同時に生成されます。

子プロセス数が最大値に達した場合、子プロセスが生成可能となるまでアーカイブ処理はスリープします。

ただし、以下のいずれかの条件を満たす場合、外部送信データはアーカイブされずにキューディレクトリに残ります。

(a) 1日分のアーカイブのサイズが、ポストイメージ制限値を超過した場合

ポストイメージ制限値の設定変更方法については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~ 』の「3-4-3-1 基本設定」の「ポストイメージ制限値」(315 ページ) をご参照ください。

(b) 外部送信データが、キューディレクトリに出力後1日以内に処理されなかった場合

詳細については、「8 トラブルシューティング」の「(10) アーカイブ処理エラー通知メールが送信される」(114 ページ) をご参照ください。

7 サポートツール

7-1 rescue.pl

検査サーバー（ウェブ）の各設定ファイルをバックアップ/リストアする Perl スクリプト

(1) 使用方法

Usage: rescue.pl [--backup | --restore <packedfile>]

オプション

- help : ヘルプメッセージを出力する
- backup : 各設定ファイルのバックアップファイルを作成する
- restore : バックアップファイル <packedfile> からリストアする
- restorefull : バックアップファイル <packedfile> から完全にリストアする

例 1) 各設定ファイルをバックアップする場合

```
# ./rescue.pl --backup
```

実行後、カレントディレクトリにバックアップファイルが作成されます。

ファイル名: <バージョン番号>-<hostid>-<YYYYMMDDhhmmss>.tar.gz

wg-3.0.03-80fe7ea0-20051204154014.tar.gz の場合

バージョン番号 : WEBGUARDIAN Ver3.0.03

hostid : 80fe7ea0

YYYYMMDDhhmmss : 作成日付 2005 年 12 月 4 日 15 時 40 分 14 秒

バックアップファイルのファイル名は変更しないでください。

例 2) 各設定ファイルをリストアする場合

```
# ./rescue.pl --restore <packedfile>
```

<packedfile> は、本スクリプトで取得したバックアップファイルを指定します。

「--restorefull」を指定した場合、構成情報がバックアップ時と違っていた場合でも構成情報を含め完全にリストアします。

たとえば、検査サーバー（ウェブ）障害時にパッケージを再インストールした直後に設定を過去（元）に戻す場合などに使用してください。

(2) スクリプト格納先

/opt/Guardian/WG/support/

(3) バックアップファイルの中身

ポリシー設定

規制ルール、例外ルール、グループ、時間・曜日、URL グループ、MIME タイプ、キーワード、ブロック画面

基本設定

ログ管理、検査機能、プロキシー設定

ユーザー認証設定

メール通知設定

管理者メールアドレス、メール通知文

サービス設定

検索エンジン、ウェブメール、ソーシャルウェブ

URLDB 設定情報

httpd.conf ファイル

urldb_manager.conf ファイル

mkdic.conf ファイル

(4) 注意点

WEBGUARDIANでは、ホストIDごとにライセンスを発行しております。よって、ホストIDの異なるマシンに設定をリストアすると、WEBGUARDIANのライセンスが無効となり、単なるプロキシーサーバーとして稼働しますので、ご注意ください。

設定リストア後は、検査サーバー（ウェブ）の再起動を実施してください。

7-2 sanity_chk.pl

検査サーバー(ウェブ)にインストールされているべき必要なパッケージの状態を検査するための Perl スクリプト (Solaris 版のみ)

(1) 使用方法

Usage: sanity_chk.pl

例) 検査サーバー(ウェブ)にインストールされている必要なパッケージの状態を検査する

<pre># ./sanity_chk.pl SANITY CHECK: OK</pre>	< 異常なしの場合 >
---	-------------

パッケージの状態に異常がある場合は「INVALID」と表示される

(2) スクリプト格納先

/opt/Guardian/WG/support/

(3) 注意点

本スクリプトは、Solaris 上でのみ動作します。Linux 上で実行した場合、有効な検査は何も行いません。

7-3 watch.pl

検査サーバー（ウェブ）の稼動監視を行う Perl スクリプト

本スクリプトはサンプルとして提供します。使用の場合は、別名にコピーしてから実行してください。

(1) 使用方法

Usage: watch.pl [オプション]

オプション

- help : ヘルプメッセージを出力する
- mail=<address> : 監視結果を <address> 宛にメールで通知する
- quiet : 問題がある場合のみ監視結果を表示あるいはメールする

「--mail」の指定がない場合は、標準出力に監視結果を出力します。

「--mail」を指定し、<address> の指定がない場合は、root 宛にメールを送ります。

例 1) 稼動監視結果を標準出力に表示する

```
# ./watch.pl
ホスト名: host1
Load average: ok 0.02
Swap free space: ok 2049 MB
Process "WG/bin/httpd": ok alive
Process "wglogger": ok alive
Process "urldb_manager": ok alive
Process "wg_store": ok alive
Process "Admin/httpd/bin/httpd": ok alive
Disk free space "/var/opt/Guardian/WG": ok 1134 MB
Disk free space "/opt/Guardian/Admin/logs": ok 804 MB
```

例 2) 稼動監視結果を user1@example.co.jp 宛にメールする

```
# ./watch.pl --mail=user1@example.co.jp
```

(2) スクリプト格納先

/opt/Guardian/WG/support/

(3) 監視対象

ロードアベレージ

初期値：12

初期値以上になると異常とみなします。

スワップ残容量

初期値：100 MB

初期値以下になると異常とみなします。

プロセス

初期値： WG/bin/httpd
 wglogger
 urldb_manager
 wg_store
 Admin/httpd/bin/httpd

初期値に指定されたプロセスが起動していないと異常とみなします。

ディスク残容量

初期値： /var/opt/Guardian/WG 300 MB
 /opt/Guardian/Admin/logs 100 MB

初期値に指定されたディレクトリについて、それぞれの値以下になると異常とみなします。

それぞれの監視対象項目の初期値を変更したい場合は、本スクリプトを別名にコピーした後、そのコピーしたスクリプトファイルを直接編集してください。

(4) 注意点

本スクリプトはサンプルとして提供します。使用する場合は、別名にコピーしてから実行してください。特に監視対象の初期値を変更する場合は、必ずコピーを編集してください。決してオリジナルの同スクリプトを書き換えないようお願いします。

7-4 queue_mgr.php

キューディレクトリ (/opt/Guardian/WG/var/queue) 内の、アーカイブ対象外となっている外部送信データを管理するための PHP スクリプト。

(1) 使用方法

Usage: queue_mgr.php [オプション]

オプション

- help : ヘルプメッセージを出力する
 - list, -l : アーカイブ対象外の外部送信データを表示する(デフォルト)
 - count, -c : アーカイブ対象外の外部送信データ数を表示する
 - move <directory> : アーカイブ対象外の外部送信データを <directory> に移動する
 - activate : アーカイブ対象外の外部送信データを再度アーカイブ対象とする
 - delete : アーカイブ対象外の外部送信データを削除する
 - F YYYY/MM/DD[:hh:mm:ss] : 指定した日時以降に送信された外部送信データを対象とする
 - T YYYY/MM/DD[:hh:mm:ss] : 指定した日時以前に送信された外部送信データを対象とする
 - u <string> : 送信先 URL に <string> を含む外部送信データを対象とする
 - v : -F, -T, -u の条件にマッチしない外部送信データを対象とする
- 「-F」「-T」「-u」のオプションを同時に指定した場合、全ての条件を満たす外部送信データが対象となります。

例 1) アーカイブ対象外の外部送信データを表示する

```
# ./queue_mgr.php
2009/04/27:17:30:31 0004688528C9D1B209-5A0AA90E-4C7E.req http://www.example.com/search.php
2009/04/27:20:34:38 00046887BB41F3A10A-5A0AA90E-4075.req http://www.example.com/search.php
2009/04/27:17:26:44 000468851B4E75E609-5A0AA90E-4C5A.req http://www.example.com/search.php
2009/04/27:17:51:46 0004688574CC84360A-5A0AA90E-4C7E.req http://www.example.com/search.php
...
```

外部送信データの送信時刻、ファイル名、送信先 URL が表示されます。

例 2) アーカイブ対象外の外部送信データの内、送信先 URL に「www.example.com」を含むものの件数を表示する

```
# ./queue_mgr.php -c -u www.example.com
525451
```

例3)アーカイブ対象外の外部送信データの内、送信先URLに「www.example.com」を含むものを削除する

```
# ./queue_mgr.php --delete -u www.example.com
delete 0004688528C9D1B209-5A0AA90E-4C7E.req
delete 00046887BB41F3A10A-5A0AA90E-4075.req
delete 000468851B4E75E609-5A0AA90E-4C5A.req
delete 0004688574CC84360A-5A0AA90E-4C7E.req
...
```

例4)アーカイブ対象外の外部送信データの内、2009/04/27に送信されたデータを再度アーカイブ対象とする

```
# ./queue_mgr.php --activate -F 2009/04/27 -T 2009/04/27
activate 00046883B131BC610C-5A0AA90E-4C7B.req
activate 000468492F6312BC05-5A0AA90E-439D.req
activate 000468492F6312BC05-5A0AA90E-439D.req
activate 00046886A99F582105-5A0AA90E-4077.req
...
```

(2) スクリプト格納先

/opt/Guardian/WG/support/

MEMO

8 トラブルシューティング

本章では、障害時の対策について解説します。

(1) ルール編集で「取り消されたアクション」と出る

WEBGUARDIANの各ルール設定で設定変更を行うと、IEの場合「取り消されたアクション」というIEのエラー画面が出ることがあります。この現象はウェブの検査サーバーを経由しながらWEBGUARDIANを再起動した場合に発生しやすいため、GUARDIANSUITEへアクセスする時はWEBGUARDIANを経由しないように注意してください。

(2) HTTPSの禁止/オーバーライド/警告/リダイレクト画面が表示されない

ウェブブラウザがIEの場合、HTTPSアクセスの禁止/オーバーライド/警告/リダイレクト画面が正しく表示されないことがあります。表示されるエラー画面はIEのバージョンにより異なります。

IE6の場合、禁止/警告/オーバーライド画面が全部表示されない場合があります。これはCONNECTリクエストに対して、プロキシでエラー応答を返した場合に1024バイトまでしか認識されないという、IE6の不具合のために発生します。このようなケースが想定される規制ルールでは、アクションを禁止、オーバーライド、警告ではなくリダイレクトにすることで対応してください。

IE7の場合、リダイレクト画面が表示されず、「ページを表示できません。」のエラー画面が表示される場合があります。これはCONNECTリクエストへの応答に対する、IEのセキュリティ上の仕様変更のために発生します。これらのケースが想定される規制ルールでは、アクションをリダイレクトではなく禁止、オーバーライド、警告にすることで対応してください。

またIE8の場合、禁止/オーバーライド/警告/リダイレクト画面が表示されず、「ページが表示されません。」のエラー画面が表示される場合があります。これについてもIE7と同様、IEのセキュリティ上の仕様変更により発生します。

IE8ご利用の場合についてはIEの仕様のため回避方法がございませんので、ご注意ください。

(3) FTPサイトで禁止/オーバーライド/警告画面が表示されない

ウェブブラウザがIE6の場合、FTPサイトアクセスの禁止/オーバーライド/警告画面が正しく表示されない場合があります。

[インターネットオプション]-[詳細設定]-[ブラウズ]-[FTPサイト用のフォルダビューを使用する]が有効になっている場合、上記画面が正しく表示されません。この場合は、前記オプションを無効にすることで対応してください。

(4) オーバーライドブロック解除後のリダイレクトあるいは警告画面表示後の再リクエストで入力データがクリアされてしまう

オーバーライドブロック解除後のリダイレクトあるいは警告画面の表示後に実行された再リクエストでは、外部送信データは送信されません。そのため、ウェブメール送信時やファイルのアップロード時など外部へのデータ送信時にオーバーライド/警告アクションが適用された場合は、アクション適用前に入力されていたデータは全てクリアされてしまいます。そのような場合は、再度データを入力し、オーバーライド解除時間内あるいは警告間隔内に再リクエストを行ってください。

(5) オーバーライドブロック解除後のリダイレクトあるいは警告画面表示後の更新ボタンで元リクエストのサイトへ正しくアクセスできない

サイトの仕組みによっては、オーバーライドブロック解除後あるいは警告画面での更新ボタン押下後に元リクエストのサイトへ正しくアクセスできないことがあります。またファイルダウンロード時に警告画面が表示され、更新ボタンにより元リクエストのサイトへ再リクエストを行った場合、ウェブブラウザの仕様によりファイルを正しくダウンロードできないことがあります。このような場合は、オーバーライド/警告アクション適用前と同じ画面操作を実施し、元リクエストのサイトへ再リクエストを行ってください。

(6) ウェブアプリケーションで禁止画面や警告画面が表示されない、またはウェブアプリケーションの動作が不定となる

ウェブアプリケーションでは、サーバーへのリクエストの結果受信したウェブページへの画面遷移を行う一般的な通信以外に、画面遷移を伴わない通信でデータの送受信を行い、Javascript等でウェブページを書き換えている場合があります。そのような画面遷移を伴わない通信をブロックした場合、禁止画面や警告画面は表示されません。また、ウェブアプリケーションの動作が不定となる場合があります。このようなケースが想定されるウェブアプリケーションに対しては、画面遷移を伴わない通信がブロックされないよう、必要に応じて規制ルールの調整を行ってください。

(7) 障害時の復旧方法について

WEBGUARDIANシステムや、稼動しているハードウェアに障害が発生した場合の復旧方法については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通 ~』の「10 障害時の復旧方法」(448 ページ)をご参照ください。

(8) Adobe Acrobatのライセンス認証が失敗する

Adobe Acrobat のライセンス認証では、Host ヘッダーを含まない HTTP/1.1 リクエストが行われます。HTTP/1.1 の仕様 (RFC2616) では、リクエストに Host ヘッダーを含むことを必須としているため、WEBGUARDIAN はデフォルトではこのようなリクエストを拒否します。同様のリクエストを行う Adobe Acrobat 以外のアプリケーションについても通信は失敗します。

以下の設定を行うことで、Host ヘッダーを含まない HTTP/1.1 リクエストを許可することができます。

管理サーバー上で /opt/Guardian/Admin/etc/wg/httpd.conf.tpl を直接編集し、以下の設定を記述します。

```
HostHeaderCheck Off
```

検査サーバーと設定ファイルを同期させます。

```
# /opt/Guardian/Admin/support/pushWebWG -r httpd
```

(9) CONNECT メソッドを使用する通信が失敗する

WEBGUARDIAN は、一般的に SSL 暗号化による HTTP 通信 (HTTPS) で使用される TCP の 443、及び 563 番ポートへの CONNECT メソッドによる接続をデフォルトで許可しており、それ以外のポート番号への CONNECT メソッドによる接続は拒否します。

アプリケーションによっては、443、及び 563 以外のポート番号への CONNECT メソッドによる接続が必要な場合があります。そのような場合、【共通】-「検査サーバー管理」-「個別設定」-【プロキシ設定】画面の「SSL 接続許可ポート」で、許可するポート番号を設定してください。

(10) アーカイブ処理エラー通知メールが送信される

クライアントが送信した外部送信データは、キューディレクトリ (/opt/Guardian/WG/var/queue) に出力された後、STORE サーバー (wg_store) がログ保存ディレクトリにアーカイブします。

システムの処理性能を超える件数の外部送信データが送信されると、アーカイブ処理に遅延が発生するため、WEBGUARDIAN はキューディレクトリに出力後 1 日以内に処理されなかった外部送信データを、アーカイブ処理の対象から外します。

検査サーバーでは毎日 00:00 に、アーカイブ対象外となった外部送信データを確認し、そのようなデータが発生している場合は管理者に以下の内容のメールを送信します。

```
From: root@dqn.example.com
To: admin@example.com
Subject: WEBGUARDIAN: アーカイブ処理 エラー通知
```

```
ホスト名: suite.dqn.example.com
キューディレクトリ: /opt/Guardian/WG/var/queue
アーカイブ対象外ファイル数: 826612
```

アーカイブ対象外となっている外部送信データがあります。
キューディレクトリを確認し、適切に処理してください。

アーカイブ対象外となった外部送信データは、処理されないままキューディレクトリに残るため、上記メールを受信した場合、「7-4 queue_mgr.php」(109 ページ)をご参照の上、キューディレクトリ内のファイルを手動で処理してください。

(11) TCP/IPの再送タイムアウトに関する設定の確認

プロキシ認証にシングルサインオン (NTLM 認証) を使用している場合などに関係する OS の TCP/IP の再送タイムアウトに関する設定の確認方法を例示します。変更する場合は、OS のドキュメント等を参照し適切な値に変更してください。

<Solaris>

```
tcp_rexmit_interval_initial    : 初期再送タイムアウト値 (ミリ秒)
tcp_rexmit_interval_max       : 最大再送タイムアウト値 (ミリ秒)
tcp_ip_abort_cinterval        : 合計タイムアウト値 (ミリ秒)
```

現在の OS の設定状態を確認するには以下のコマンドを実行してください。

```
# ndd /dev/tcp tcp_rexmit_interval_initial
3000
# ndd /dev/tcp tcp_rexmit_interval_max
60000
# ndd /dev/tcp tcp_ip_abort_cinterval
180000
```

<Linux>

```
tcp_syn_retries                : TCP 接続を行う際の SYN パケットの再送回数 (回数)
```

現在の OS の設定状態を確認するには以下のコマンドを実行してください。

```
# cat /proc/sys/net/ipv4/tcp_syn_retries
5
```

(12) ストリーミング系アプリケーションで動画を再生できない

WEBGUARDIANは、RTSP over HTTP と呼ばれるストリーミング方式による動画再生には対応していません。ご了承ください。