

GUARDIANSUITE

検査サーバー 利用の手引き

～GUARDIANWALL V8.0 編（メール）～

* Excel、Hotmail、Internet Explorer、Outlook、PowerPoint、Visio、Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

Copyright©2015 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 I T 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/>

2015-Mar-01 GUARDIANSUITE V5.0
GUARDIANWALL V8.0

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 ～ GUARDIANWALL V8.0 編（メール）～』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 のメール部分（GUARDIANWALL）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）

GUARDIANWALL の機能、動作の仕組みの概要について説明します。

2 運用（22 ページ）

GUARDIANWALL を用いた電子メール運用ポリシーの設定、保留メールの管理、運用方法について説明します。

3 グループ管理（40 ページ）

グループ管理機能について説明します。

4 システム設定・保守（50 ページ）

各種機能について、直接設定ファイルを編集して設定する方法、ログファイル、保存メールデータについて説明します。

5 仕様（64 ページ）

各設定ファイルの詳細仕様、日本語検査機能に関する詳細仕様について説明します。

6 サポートツール（178 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。

7 トラブルシューティング（182 ページ）

GUARDIANWALL 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 ABCabc123	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ることを示しています。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。	・『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：

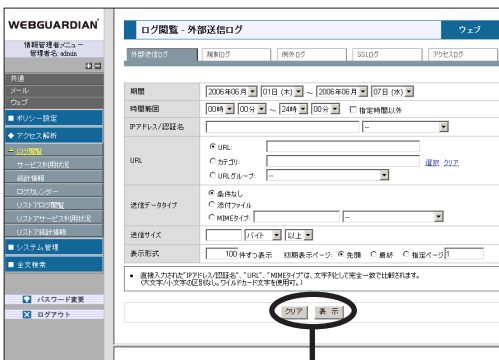
ウェブブラウザより本システムにアクセスすると、この画面が表示されます。この画面から、各利用者別にログインします。

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。

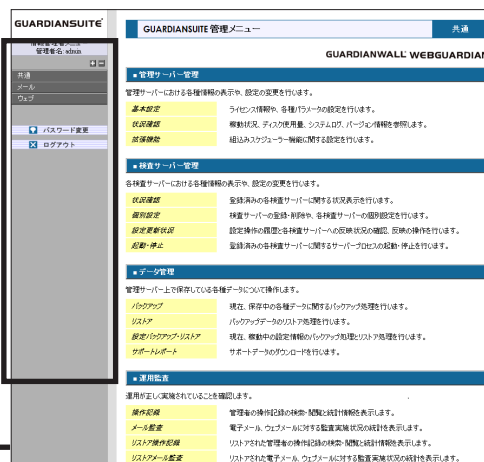
利用者別トップページ：

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	機能	10
1-2	導入モデル	10
1-3	電子メールの処理方法	11
1-4	検査の対象となる電子メール	12
1-5	検査・配送制御機能	13
1-6	情報検査機能	14
1-7	メール保存機能	14
1-8	タイムスタンプ機能	15
1-9	個人情報検査機能	18
1-10	標的型攻撃メール検知機能	20
2	運用	22
2-1	電子メール運用ポリシー	22
2-2	メール発信の防止方法	23
2-3	保留メールの管理	24
2-4	情報管理者と部門情報管理者	26
2-5	一時保留メールの管理	27
2-6	運用例	34
2-7	設定例	36
3	グループ管理	40
3-1	グループ管理機能概要	40
3-2	グループの登録	43
3-3	グループ管理	44
3-4	検索条件グループ	46
3-5	検査・配送ルール	47
4	システム設定・保守	50
4-1	設定ファイル	50
4-2	システムの設定更新と再起動	52
4-3	設定変更	53
4-4	グループ管理	54
4-5	ログファイル管理	59
4-6	保存メール管理	60
4-7	MSP (Mail Submission Program) の設定変更	61

5 仕様.....	64
5-1 日本語検査仕様.....	64
5-2 サーバー設定ファイル.....	70
5-3 検査・配送ルール設定ファイル.....	100
5-4 MIME タイプ検査条件設定ファイル.....	145
5-5 キーワード条件式設定ファイル.....	147
5-6 動作一覧定義ファイル.....	149
5-7 通知メール.....	150
5-8 送信先外部サーバーの切り替え.....	171
5-9 添付ファイル暗号化機能仕様.....	173
5-10 標的型攻撃メール検知機能仕様.....	175
6 サポートツール.....	178
6-1 rescue.pl.....	178
6-2 watch.pl.....	180
7 トラブルシューティング.....	182

1 概要

本章では、GUARDIANWALL の機能、仕組みについて説明します。

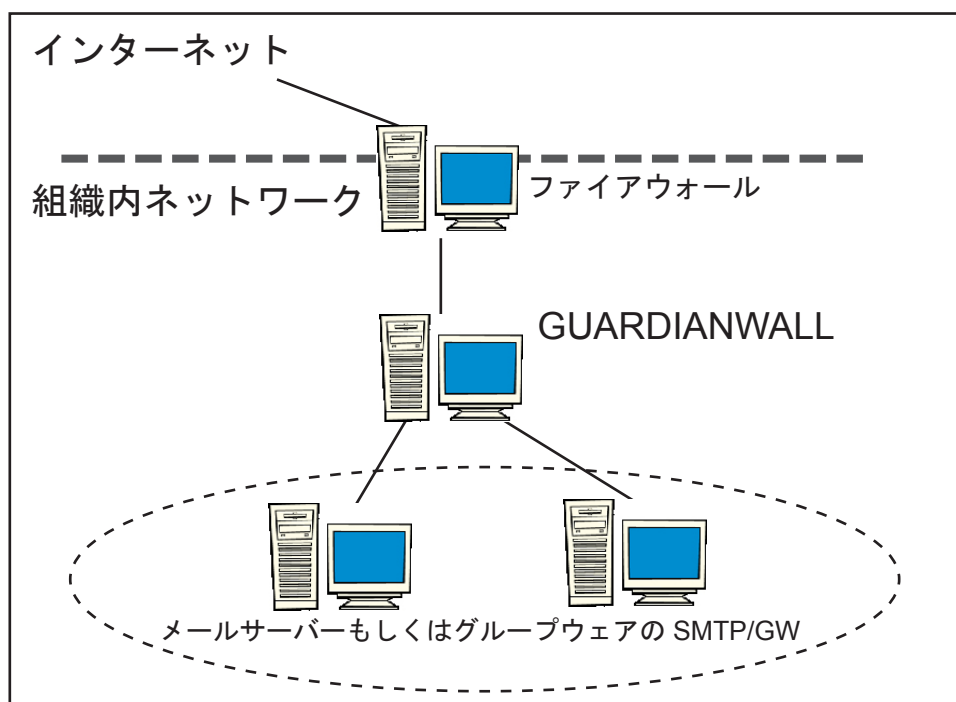
1-1 機能

GUARDIANWALL は、LAN（Local Area Network）などの組織内ネットワークからインターネットへ送出される電子メールの内容を検査し、あらかじめ設定されたポリシーに従わない情報の外部発信を防止します。さらに、電子メールの本文（添付ファイルを含む）を保存することができます。

1-2 導入モデル

GUARDIANWALL は、ファイアウォールの内側のネットワークにすでに設置されている SMTP ゲートウェイへのインストールを推奨します。既存の SMTP ゲートウェイではなく、新規ハードウェアにインストールする場合は、事前に、SMTP ゲートウェイとして SMTP トラフィックを正しく中継、送信できるようにネットワーク設定、send-mail 等 MTA（Mail Transfer Agent）ソフトウェアの設定を行う必要があります。

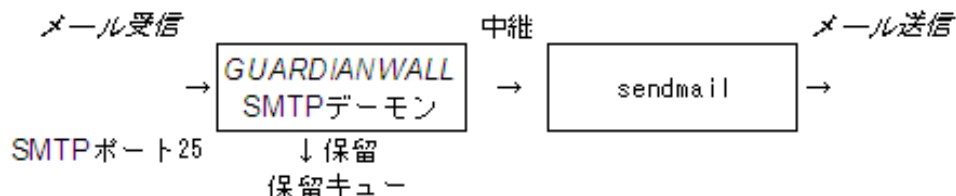
● SMTP ネットワーク構成例



1-3 電子メールの処理方法

GUARDIANWALL の SMTP サーバー（デーモン）がポート 25（初期値）の電子メールを受信し、配送ルールの適用、MIME タイプ検査、キーワード検査を行います。実際のメールの中継・送信処理は sendmail に渡され、配送が行われます。

● 電子メールの処理の流れ



実際のメールの送信処理は、`/usr/lib/sendmail` を MSP（Mail Submission Program）として使用します。事前に SMTP トラフィックを正しく中継し、メール送信が正しく行われるよう各種ネットワーク設定、MSP の設定が完了している必要があります。

本システムは、SMTP トラフィックを処理するようなアプリケーション（グループウェアの SMTP ゲートウェイ、ウィルス検査ソフト等）がすでにインストールされている環境での動作は保証していません。また、本システムをインストールするサーバーホストで利用できる MTA ソフトウェアは `sendmail`、もしくは `sendmail` 互換インタフェースを持つ `qmail`、`Postfix` だけになります。

本システムは、必ずファイアウォールの内部側ネットワークに設置してください。インターネットと直接つながれたネットワークセグメントや DMZ（DeMilitarized Zone）には、そこに設置しなければならない積極的な理由がない限り、無用なサーバーは設置すべきではありません。そのような場所には、SMTP トラフィックの中継だけを行う SMTP ゲートウェイを設置してください。本システムは、通常のメールサーバーより詳細なログ情報を保存し、メールのメッセージデータを保存します（保留機能、メール保存機能使用時）。したがって、DMZ やインターネットと直接つながれたネットワークセグメントへの設置は推奨しません。内部側ネットワークへの設置を強く推奨します。

※ `sendmail 8.12` より MSP として `sendmail` が起動された場合の動作が `8.11` 以前とは変更されています。`submit.cf` ファイルを特に設定することなくデフォルトのままインストールした場合は、`sendmail 8.12` 以降を MSP として起動すると `localhost` の SMTP ポートに接続します。`GUARDIANWALL` と共に使用すると、そのままではメールがループすることになり、メールの中継、送信が正しくできません。`sendmail 8.12` 以降をご使用になる場合は、「4-7 MSP の設定変更」（61 ページ）をご参照ください。

1-4 検査の対象となる電子メール

本システムは、組織内ネットワークからインターネットへ送出される電子メールだけを検査対象とします。デフォルトの設定では外部から送信されたメールの検査は行わず、そのまま中継します。

組織内部から発信されたメールであるか、外部から送信されたメールであるかの判定は、本システムを導入した際に設定する「**内部ドメイン名**」に基づき判定されます。デフォルトではメールのヘッダーの差出人アドレス（ヘッダーの**From:** アドレス）が内部ドメイン名に属する場合に内部から発信されたメールとみなします。

設定により、外部から送信されたメールも検査対象とすることができますが、外部から送信されたメールに対しては、いかなる場合でも、その差出人へ通知メールを送信しません。

「**内部ドメイン名**」は、インストール時に設定しますが、インストール後でも設定を変更することができます。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「**3-3-5-1 基本設定**」（228 ページ）をご参照ください。

※エンベロープ FROM が空（**MAIL FROM:** <>）のメールについては、デフォルトの設定では検査対象にしないで中継します。通常、MTA が自動的に送信する配送上のエラーなどの通知メールのエンベロープ FROM が空になります（RFC1123 参照）。一般的には、こういったメールを保留や削除する必要はありません。なんらかの事情により、削除、保留を行いたいメールのエンベロープ FROM が仮に空であっても、ただちにエンベロープ FROM が空であるという条件だけをもって検査等を行うことはお勧めいたしません。

1-5 検査・配送制御機能

検査・配送制御機能とは、電子メールの特定ヘッダーの内容、メールのサイズなどを条件としてメールの処理方法を制御する機能です。電子メールの差出人アドレス、宛先アドレス、メールサイズを条件として該当するメールの配送処理もしくは後述の情報検査処理をルールとして指定できます。

目的

- ・ 特定差出人のメール送信拒否
- ・ 特定宛先へのメール送信拒否
- ・ 特定アドレスを CC に含まないメールの送信拒否
- ・ 特定アドレスを宛先に含まないメールの送信拒否
- ・ 特定差出人のメールのコピー保存
- ・ 特定宛先へのメールのコピー保存
- ・ 検査しない特権的利用者の設定

等

検査・配送制御機能の判定結果により、以下のような動作（の組合せ）を指定できます。

送信

削除

送信保留（管理者による内容確認）

管理者へ通知

差出人へ通知

メール保存（コピーの保存）

指定アドレスへの転送

情報検査（後述）

1-6 情報検査機能

情報検査機能とは、電子メールのサブジェクト、本文、添付ファイルの日本語内容検査を行い、機密情報や不適切な情報が電子メールによって外部に漏洩されていないかを検査する機能です。MIME タイプ検査機能、キーワード検査機能、個人情報検査機能があります。

MIME タイプ検査機能は添付ファイルのタイプの検査を行い、添付ファイルの MIME タイプ、ファイル名の拡張子などを指定することにより CAD データ、画像データ等指定したタイプのファイルが添付されているかどうかを検査できます。

キーワード検査機能は指定した語句の組合せを含むかどうか、またそれらキーワードを何個含むかを検査できます。

個人情報検査機能は、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。

目的

- ・ 機密情報の漏洩防止
- ・ 特定アプリケーションデータの漏洩防止
- ・ 中傷用語のスクリーニング
- ・ 猥褻、不適切な用語のスクリーニング
- ・ 個人情報を含むファイルの送付防止

等

情報検査機能の判定結果により下記の配送処理が指定できます。

送信

削除

送信保留（管理者による内容確認）

管理者へ通知

差出人へ通知

メール保存（コピー）

1-7 メール保存機能

メール保存機能とは、電子メールのメッセージ（添付ファイルなどを含む）をそのままの形式で保存する機能です。保存したメールは、権限を有する管理者がウェブブラウザから検索・閲覧することができます。

目的

- ・ 外部発信電子メールの記録保存
- ・ 特定相手先との電子メールの記録保存
- ・ 電子メール利用状況の詳細分析

等

1-8 タイムスタンプ機能

(1) 概要

メール保存データを格納するアーカイブファイルに対してタイムスタンプを取得、付与します。

タイムスタンプによって示される時刻にアーカイブデータが確かに存在していたこと、タイムスタンプが付与された時刻以降、そのアーカイブデータの内容が改ざんされていないことを第三者に証明することが可能となります。

本システムでは国際標準に準拠したデジタルタイムスタンプサービスであるアマノ株式会社の「**アマノ タイムスタンプサービス 3161**」を利用します。本サービスを利用するためには、別途タイムスタンプサービス利用契約が必要となります。利用をご希望される場合は販売会社までご連絡ください。

【タイムスタンプの定義】（タイムビジネス推進協議会ガイドラインより）

特定の電子情報と時刻情報を結合することにより、その時刻以前にその電子データが存在していたことの証明（存在証明）とその時刻までの間にその電子情報が変更・改ざんされていないことを証明（非改ざん証明）することができる手段、及びその証拠に結びつく情報。

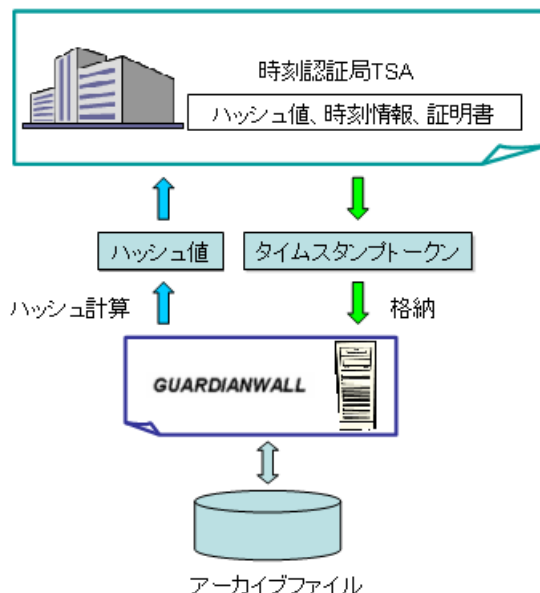
(2) メール保存アーカイブへのタイムスタンプ付与の仕組み

メールの保存とタイムスタンプの付与

メール保存機能を利用すると1日分の電子メールを1つのアーカイブファイルにまとめて格納します（保存ディレクトリの切り替えが発生した場合は、1日で複数のアーカイブファイルが作成される場合もあります）。

1日分のアーカイブファイルの作成が完了した段階で、アーカイブファイルのデータ部分のハッシュ値を計算し時刻認証局（TSA）に対してタイムスタンプの要求を行います。

TSA から発行される（信頼できる時刻情報、ハッシュ値、TSA 証明書等を含む）タイムスタンプトークンを受信してアーカイブファイルに格納します。



(3) メール保存アーカイブのタイムスタンプ検証の仕組み

タイムスタンプトークン内のハッシュ値とアーカイブファイルのデータ部分から計算されるハッシュ値を比較して検証を行います。

情報管理者がウェブ管理画面でアーカイブファイルの検証を行うと、データ部分の改ざんなどが無ければ「VALID」、改ざんもしくはデータの破損などがあれば「INVALID」と表示されます。

取得、付与されたタイムスタンプトークンの別途管理が必要な場合はウェブ管理画面よりダウンロードすることができます。

(4) 仕様

タイムスタンプ仕様

タイムスタンプは1時間に1回取得し、アーカイブファイル中に電子メールメッセージと共に格納していきます。本システム上では、1時間に1回取得するタイムスタンプを中間タイムスタンプと呼びます。

1日分の電子メールを全てアーカイブファイルに格納完了した後にさらにタイムスタンプを取得し、アーカイブファイルに格納します。最後に付与したタイムスタンプを最終タイムスタンプと呼びます。

最終タイムスタンプを付与したアーカイブを「終端済」と呼び、これ以上このアーカイブファイルに追記は行えません。アーカイブファイルの検証はこの最終タイムスタンプを基に行います。

中間タイムスタンプによりアーカイブ中の個々の電子メールメッセージを概ね1時間単位で分割した部分的な検証を行うことに用いることができますが、現在は特に使用しません。

最終タイムスタンプの付与時刻

1 日分のアーカイブファイルに対する最終タイムスタンプは、1 日分のメール処理の完了が確認された段階で付与しますので、翌日に日付が変わってから付与されます。1 日の途中で保存ディレクトリの切り替えが発生した際は、切り替え前の保存ディレクトリ側にあるアーカイブファイルに対しては当日中に付与される場合もあります。

タイムスタンプ付与時の通信

タイムスタンプの取得のために AMANO タイムスタンプサービス局（TSA）と HTTP 通信が発生します。

この通信では、アーカイブデータから計算されたハッシュ値が TSA に送られます。データ内容は TSA へは送信されません。

障害時の処理

何らかの障害によりタイムスタンプの付与ができない場合は、あらかじめ設定された回数リトライを行います。

通信回復後にタイムスタンプが付与される場合、回復後の時刻でタイムスタンプが取得されます。

長期間通信不可であった場合、通信回復後でも指定日数を越えた古いアーカイブファイルには最終スタンプを付与しない場合があります。

旧バージョンで作成されたアーカイブとの互換性

旧バージョンで作成されたアーカイブファイルにはタイムスタンプを付与しません。また、検証も行えません（旧バージョンで作成されたアーカイブでも検索・閲覧は正常に行えます）。

旧バージョンで当日のアーカイブファイルを作成している時にバージョンアップを行っても、当日中は旧バージョンフォーマットでアーカイブを作成継続しますので、タイムスタンプ機能は当日には使用できません。

翌日以降に新しいアーカイブファイルが作成される時からタイムスタンプの付与が始まります。

利用タイムスタンプサービス仕様

アマノタイムスタンプサービス 3161

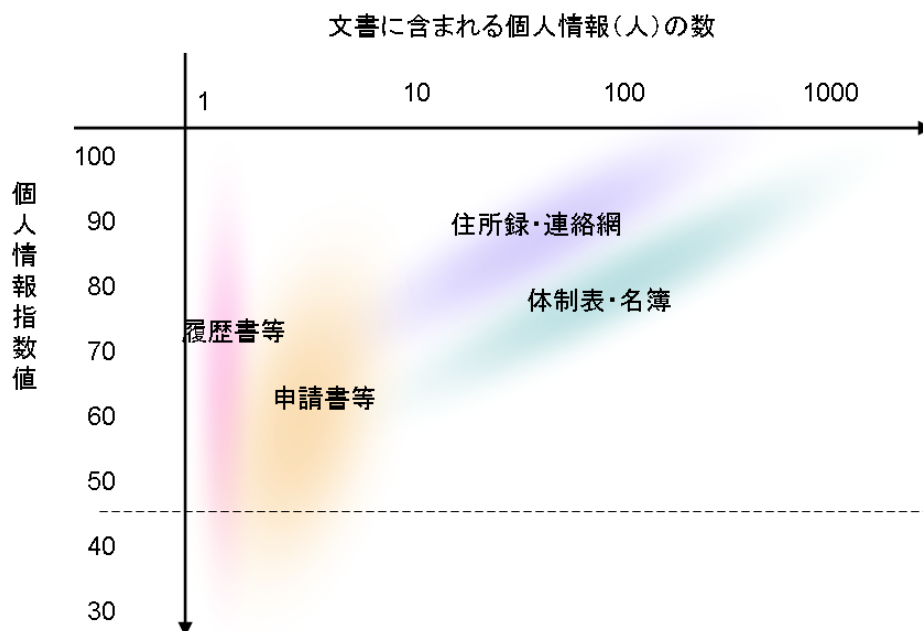
- ・（財）日本データ通信協会による「タイムビジネス信頼・安心認定制度」の認定第 1 号（SD0001）
- ・ JISX5063-1、ISO-18014、RFC-3161 に準拠
- ・ セコムトラストネット株式会社の WebTrust 規準のルート認証局から発行される時刻認証局用証明書
- ・ 証明書有効期限：11 年 1 カ月

有効期間が 11 年 1 カ月間の TSA 証明書を 1 年ごとに更新しているため、本サービスでは最低 10 年間から最高 11 年間の有効期間のタイムスタンプをご利用いただけます。

1-9 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。総合的な指数だけでなくより詳細な検査を行いたい場合は、個人情報件数や項目数、各項目の個別の検出件数に関して条件を設定して検査することもできます。



- ・本機能は個人情報の漏洩を防止することを完全に保障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。
- ・郵便番号は総合指数として評価されますが、個人情報件数には含まれません。
- ・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。
- ・特許取得済み。

1-10 標的型攻撃メール検知機能

(1) 概要

電子メールのアドレス情報や添付ファイルから標的型攻撃メールの疑いがあるメールを検知します。

対象メールが標的型攻撃メールと判定された場合、標題に警告メッセージを付与します。また、設定により管理者へ通知メールを送信することもできます。

(2) 仕組み

電子メールの差出人アドレスと宛先アドレスから、差出人アドレスを詐称し、メーリングリスト等を利用して不特定多数の宛先へ送信された疑いのあるメールを標的型攻撃メールとして検出します。また、ファイル名に偽装の疑いがある実行ファイルや、スクリプトが埋め込まれている疑いのあるリンクファイル(ショートカットファイル)が添付されているような電子メールについても標的型攻撃メールとして検出します。

MEMO

2 運用

本章では、GUARDIANWALL の運用方法について説明します。

2-1 電子メール運用ポリシー

電子メールの運用ポリシーは、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、以下に基本的なポリシーの例を紹介します。

(1) 社外送信できるユーザーを限定する

イントラネットとして利用しているグループウェアなどのメールシステムを SMTP ゲートウェイを通してインターネットと接続する際に、外部へ送信できるユーザー、部署を差出人アドレス、ドメイン名で限定することができます。

(2) 送信先を限定する

電子メールを送信できる相手先アドレスやドメインなどを限定することができます。さらに、上記 (1) の設定と組み合わせれば、送信ユーザー、部署ごとにそれぞれ送信先のアドレス、ドメインを限定することもできます。

(3) 社外へ送信する場合は、必ず上司に写し(CC)を送る

社外へ発信されるメールが同時に特定のアドレス（例：上司や管理者のアドレス）に送られているか検査し、送られていない場合、メールの社外送信を防止できます。もしくは、社外へ送信されるメールのコピーを特定のアドレス（例：上司や管理者）に自動的に転送することもできます。

(4) 「社外秘」などの語句を含むメールの送信防止

電子メールや電子文書などに、機密扱いであることを明示するキーワードを設定する文書管理規定を設定し、その特定キーワードを含むメールの社外発信を防止できます。悪意を持った意図的な情報漏洩を防止することはできませんが、送信される範囲が分からないメーリングリストや、不注意な転送による予期しない社外への流出を防止することができます。

(5) 添付ファイルの送信防止

特定のアプリケーションデータがメールに添付されていた場合、そのメールの外部への発信を防止することができます。また、電子メールを業務利用に限定している場合、社外への発信を業務で利用している特定のアプリケーションデータのみに限定することもできます。

(6) 外部へ発信されるメールのコピーを保存する

社外へ発信される全てのメール、あるいは特定の差出人から発信されたものや、特定の宛先アドレス、ドメインに発信しているメールのコピーをファイルに保存することができます。

さらに特定の添付ファイルを含むものや、特定のキーワードを含むメールのみを保存することもできます。

2-2 メール発信の防止方法

GUARDIANWALL がメールの送信を防止する場合、「削除」と「保留」の2種類の防止方法があります。

「削除」の場合は、メールの送信を行わず、設定により差出人や管理者に通知のメールを送信します。

「保留」の場合は、メールの送信を一時保留し、設定により差出人や管理者に通知のメールを送信し、管理者が保留理由、メール内容を閲覧したうえで、外部へ「中継」するか「削除」するか処置します。

	メールの送信	事後の処置
削除	送信しません。ただちに削除します。	できません。
保留	送信しません。メールは削除せず一時的に保留します。	管理者が、送信許可（中継）、送信不可（削除）を選択します。

2-3 保留メールの管理

(1) 保留メールの管理方法

本システムが用意する保留メールの管理方法のインタフェースを2種類用意しています。それぞれ、「一覧処理方式」「個別処理方式」と呼びます。

① 一覧処理方式

本システムに現在保留あるいは一時保留されている全てのメールの一覧を表示し、処置したいメールを選択して、必要な操作（保留理由閲覧、内容閲覧、送信許可、送信不許可）を行います。

GUARDIANWALL

情報管理者メニュー
管理名: admin

共通

メール

■ポリシー設定

▲保留メール管理

■保存メール管理

■ログ閲覧

■システム管理

ウェブ

パスワード変更

ログアウト

保留メール管理

メール

保留メールの一覧です。現在、16通のメールが保留されています。

発信者

宛先

保留タイプ

クリア

表示

保留(8)

送出(6)

削除(2)

選択:すべて

解除

保留

一時保留

既読のみ

未読のみ

監査済のみ

未監査のみ

チェックしたメールを - 動作を選択 -

Prev

1

Next

	MSGID	年月日時刻	発信者 標題	サイズ 添付	保留タイプ	状態
<input type="checkbox"/>	SAA23211	2014/11/26 16:29:40	sato@canon-its.co.jp 添付ファイルあり	37.14KB [添付]	保留	閲覧済み(自) 監査済み(自)
<input type="checkbox"/>	SAA23270	2014/11/26 16:30:20	sato@canon-its.co.jp 添付ファイルあり	37.14KB [添付]	保留	閲覧済み(自)
<input type="checkbox"/>	SAA23382	2014/11/26 16:33:17	user@test.co.jp 添付ファイルあり	37.74KB [添付]	一時保留	閲覧済み(自)
<input type="checkbox"/>	TAA25295	2014/11/26 17:23:31	yamada@example.com 一時保留メール	460B -	一時保留	-
<input type="checkbox"/>	TAA25321	2014/11/26 17:24:12	user01@example.com ABC	460B -	保留	閲覧済み(他) 監査済み(他)
<input type="checkbox"/>	TAA25352	2014/11/26 17:24:37	user01@example.com 01_複数ファイルの添付	22.37MB [添付]	保留	-
<input type="checkbox"/>	TAA25367	2014/11/26 17:25:48	yamamoto@its.co.jp 06_ネットワーク共有ファイルへのリンク	2.69KB [添付]	保留	-
<input type="checkbox"/>	TAA25571	2014/11/26 17:28:33	user001@example.com お知らせ	486B -	一時保留	-

Prev

1

Next

② 個別処理方式

本システムのデフォルトの設定では、メールを保留した際に、メールを識別する「MSGID」とパスワードに相当する「問合せコード」を設定し、メールの差出人に通知します。

個別処理方式は、この MSGID と問合せコードの組合せを指定して、必要な操作（保留理由閲覧、内容閲覧、送信許可、送信不許可）を行います。

本方式で保留メールを管理する場合は、差出人が通知された MSGID と問合せコードを管理者に伝え、保留メールの処置を依頼する必要があります。

機能	一覧処理方式	個別処理方式
保留メールの選択	一覧リストから選択	MSGID、問合せコード入力
内容閲覧 / 添付ファイルのダウンロード	○	○
理由閲覧	○	○
送信許可（中継）	○	○
送信不許可（削除）	○	○
転送	○ ※内容閲覧権限が無い場合は使用できません	○

設定を変更することにより、一覧処理方式、個別処理方式それぞれの各機能の使用許可、不許可を設定できます。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「6-2-1-4 情報管理者の権限リスト」（412 ページ）、「6-2-1-5 部門情報管理者の権限リスト」（424 ページ）、「6-2-1-3 アカountの編集・削除」（411 ページ）をご参照ください。

2-4 情報管理者と部門情報管理者

本システムでは、「情報管理者」と主に保留メールの管理を行う「部門情報管理者」の2種類に分けて設定できます。

メールを保留する運用を行わない場合や、保留メールの管理を一人の管理者が行う場合は、部門情報管理者を設定する必要はありません。

本システムによるメールの保留と管理者の内容閲覧による組織的なメール内容検査を運用する場合は、メールの内容閲覧が可能な権限を持つ（例：各部門の上司など）部門情報管理者を複数設定することができます。

デフォルトの設定では、情報管理者、部門情報管理者に対してそれぞれ以下の保留メールの処理方式を設定しています。

情報管理者	・・・	一覧処理方式
部門情報管理者	・・・	個別処理方式

また、デフォルトでは一覧処理方式のメール内容閲覧操作を禁止しています。

	情報管理者	部門情報管理者
システム管理	<ul style="list-style-type: none"> ・ 検査・配送ルールの設定 ・ MIME タイプ検査条件の設定 ・ キーワード検査条件の設定 ・ 通知文の設定 ・ システム設定 	権限無し
保留メール管理	(デフォルト設定) <ul style="list-style-type: none"> ・ 一覧処理方式 内容閲覧は不可	(デフォルト設定) <ul style="list-style-type: none"> ・ 個別処理方式
保存メール管理	(デフォルト設定) <ul style="list-style-type: none"> ・ 一覧照会（ヘッダのみ） ・ バックアップ操作 ・ アーカイブ検証 	(デフォルト設定) <ul style="list-style-type: none"> ・ ログ閲覧不可 ・ 内容閲覧不可

設定を変更することにより、情報管理者に個別処理方式を使用させることや、部門情報管理者に一覧処理方式を使用させることもできます。さらに、一覧処理方式でも内容閲覧ができるように設定変更できます。また、同じ情報管理者でも、あるアカウントでは一覧処理方式で内容閲覧を許可して、別の情報管理者のアカウントでは個別処理方式を使用させるなど、アカウント単位で権限が個別に設定できます。

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「6-2-1-4 情報管理者の権限リスト」（412 ページ）、「6-2-1-5 部門情報管理者の権限リスト」（424 ページ）、「6-2-1-3 アカウントの編集・削除」（411 ページ）をご参照ください。

2-5 一時保留メールの管理

一時保留メールは、情報管理者や部門情報管理者による管理とメールの差出人自身による管理が可能です。設定された一時保留期間内であれば、情報管理者や部門管理者、あるいは差出人自身が一時保留メールに対する各種操作（保留理由閲覧、内容閲覧、送信許可、送信不許可）を行うことができます。本章では、それぞれの管理方法について説明します。一時保留時間の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「3-3-5-2 情報検査機能設定」（234 ページ）をご参照ください。

(1) 情報管理者・部門情報管理者による一時保留メールの管理

保留メール管理と同様の方法で、処置したい一時保留メールに対して必要な操作（保留理由閲覧、内容閲覧、送信許可、送信不許可）を行います。「**一覧処理方式**」の場合、本システムに現在保留あるいは一時保留されている全てのメールの一覧が表示されるため、保留メールと一時保留メールを同時に管理することができます。保留メール管理についての詳細は、「2-3 保留メールの管理」をご参照ください。

(2) 差出人による一時保留メールの管理

差出人によるログイン機能を「**オン**」に設定している場合のみ、下記 URL へアクセスすることで差出人による一時保留メールの管理が可能になります。

`http:// <管理サーバー IP アドレス> :8800/mail/step1.php`

差出人による一時保留メールの管理については、管理方法のインタフェースとして「**個別処理方式**」のみを用意しています。しかし、認証方式に LDAP 認証を設定することで、「**個別処理方式**」によるメール問合せの前に LDAP サーバーによるユーザー認証を行うこともできます。差出人によるログイン機能や認証方式の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「3-3-5-2 情報検査機能設定」（234 ページ）をご参照ください。

(a) LDAP サーバーを利用したユーザー認証

認証方式として LDAP 認証を指定している場合、上記 URL へのアクセスにより、以下のようなログイン画面が表示されます。ここでは、差出人は、LDAP サーバーを認証データベースとしたユーザー認証を行います。認証後、問合せ画面へ遷移し、一時保留メールへの問合せが可能となります。本画面による認証が必要となるのは初回アクセス時のみです。認証後は、ログアウトを行うか、ブラウザを閉じるまで認証を行う必要がありません。

一時保留メール - ログイン		メール
アカウントとパスワードを入力し、ログインしてください。		
アカウント	<input type="text" value="user03"/>	
パスワード	<input type="password" value="....."/>	
		<input type="button" value="表示"/>

(b) 個別処理方式による問合せ

認証方式を「オフ」に設定している場合、あるいはログイン画面ですでに認証済みである場合、上記 URL へのアクセスにより、以下のような問合せ画面が表示されます。差出人は、メールが一時保留時された際に通知される「MSGID」と「問合せコード」の組合せを指定し、一時保留メールへ必要な操作（内容閲覧、送信許可、送信不許可）を行います。ただし、差出人による保留メールへの操作は許可されていません。そのため、保留メールの「MSGID」と「問合せコード」を指定した場合は無効となります。

一時保留メール - 問い合わせ		メール
保留されたメールに問い合わせを行います。 MSGIDと問い合わせコードを指定して[表示]ボタンを押してください。		
MSGID	<input type="text" value="LAA17775"/>	
問い合わせコード	<input type="text" value="CJGR2MEA"/>	
		<input type="button" value="表示"/>

(c) 一時保留メールの操作

問合せ画面にて、正しいMSGIDと問合せコードが指定された場合、以下のような内容閲覧画面が表示されます。差出人に許可されているメール操作は、内容閲覧、送信許可、送信不許可です。保留理由は閲覧できません。本画面下部の、[メール送出] ボタンをクリックすると、メールが送信されます（送信許可）。[メール削除] ボタンをクリックすると、メールは削除されます（送信不許可）。また、ログアウトする場合は、画面最下部にある [ログアウト] ボタンをクリックします。この [ログアウト] ボタンは、認証方式が「オフ」に設定されている場合は表示されません。

【メール】 - 「システム管理」 - 「情報検査機能設定」 - 「拡張」 - 「保留メール送出時の確認」において、「一時保留メール詳細」の「宛先チェック」が「オン」に設定されている場合は、宛先アドレスの横にチェックボックスが表示されます。全ての宛先アドレスにチェックをすると、一時保留メールを送出することができます。また、「一時保留メール詳細」の「添付ファイルチェック」が「オン」に設定されている場合は、ダウンロード後ファイル名の前に [↓] マークが表示されます。全ての添付ファイルをダウンロードすると、一時保留メールを送出することができます。

一時保留メール - 本文閲覧		メール
MSGID: RAA31553 保留日時: 2014/12/11 15:11:50 送出予定日時: 2014/12/11 16:11:50		
発信者	user03@example.co.jp	
受信者	sato@example.co.jp, tanaka@example2.co.jp	
日付	Thu, 11 Dec 2014 15:10:53 +0900	
標題	飲み会の件	
サイズ	14.31KB	
ヘッダー	Received: from unknown [10.70.141.89] by vmcent55.slab.example.co.jp ESMTP id RAA31553; Thu, 11 Dec 2014 15:11:50 +0900 Date: Thu, 11 Dec 2014 15:10:53 +0900 From: =?ISO-2022-JP?B?GyRCPi5APhsoQIAbJEJDTjtSGyhC?= <user03@example.co.jp> To: sato@example.co.jp, tanaka@example2.co.jp Subject: =?ISO-2022-JP?B?GyRCHMskXzJxJE43bxsoQg=?= Message-Id: <20141211151053.DE0E.4C546807@example.co.jp> MIME-Version: 1.0 Content-Type: multipart/mixed; boundary="----- _5475762300000000DC73_MULTIPART_MIXED_" Content-Transfer-Encoding: 7bit X-Mailer: Becky! ver. 2.68 [ja]	
保留宛先 	<input type="checkbox"/> <sato@example.co.jp> <input type="checkbox"/> <tanaka@example2.co.jp> <input type="checkbox"/> <user@example1.co.jp>	
エンベロープ	MAIL FROM: <user03@example.co.jp> RCPT TO: <sato@example.co.jp> <tanaka@example2.co.jp> <user@example1.co.jp>	
添付	 メンバー.xlsx (9.65KB) [application/octet-stream]  案内.docx (0B) [application/octet-stream]	
本文	本日はいかがですか？	
この保留メールを処理してください。  		
		

一時保留メールに対して操作（内容閲覧、送信許可、送信不許可）を行った際、保留メール操作ログ、操作ログに操作内容が記録されます。その際、操作実施者を識別するため、保留メール操作ログの場合はアカウント欄、操作ログの場合は補足欄に、LDAP 認証時に入力されたアカウントが記録されます。ただし、認証方式が「オフ」の場合、アカウント情報がないため、「-」（ハイフン）が記録されます。

保留メール操作ログ

年月日 時刻 MSGID	発信者 標頭 日付 発信者 同報者	操作 アカウント	サイズ
2010/09/14 16:52 SAA21219	nakaichi.shusai@canon-its.co.jp delay9 Tue, 14 Sep 2010 16:52:21 +0900 nakaichi.shusai@canon-its.co.jp -	内容閲覧 nakaichi	506B -
2010/09/14 16:53 SAA21219	nakaichi.shusai@canon-its.co.jp delay9 Tue, 14 Sep 2010 16:52:21 +0900 nakaichi.shusai@canon-its.co.jp -	送出 nakaichi	506B -
2010/09/14 16:53 SAA21231	nakaichi.shusai@canon-its.co.jp delay10 Tue, 14 Sep 2010 16:52:36 +0900 nakaichi.shusai@canon-its.co.jp -	削除 nakaichi	507B -

操作ログ

日時	利用者 管理クラス IP	区分1 区分2 区分3	区分4 区分5 区分6	操作	ターゲット 補足
2010-09-14 16:39:34	- 10.70.141.91	検査サーバー メール 共通	運用 保留メール 削除	実行	4C8F2689-SAA20486-460A6D8D 送信者/nakaichi
2010-09-14 16:39:27	- 10.70.141.91	検査サーバー メール 共通	運用 保留メール 送付	実行	4C8F2683-SAA20476-460A6D8D 送信者/nakaichi
2010-09-14 16:39:14	- 10.70.141.91	検査サーバー メール 共通	運用 保留メール -	参照	4C8F2683-SAA20476-460A6D8D 送信者/nakaichi



認証方式が「オフ」の場合、「/opt/Guardian/Admin/etc/admin/admin.conf」の [CGI] セクションへ以下の設定を行うことで、「-」ではなく、差出人のヘッダー from アドレスが保留メール操作ログのアカウント欄、操作ログの補足欄へ記録されます。

```
SenderAccountManagerLog = 1
```



メールが一時保留された際に送信される通知メールに以下のような URL を設定すると、一時保留メールの操作時、問合せ画面での「MSGID」と「問合せコード」の入力を省略することができます。認証方式が「LDAP 認証」である場合、ログイン画面での認証後、内容閲覧画面へ遷移します。認証方式が「オフ」の場合はログイン画面を表示されません。

```
http://<管理サーバー IP アドレス>:8800/mail/tempqueue/p_client.  
php?msgid=$MSGID&code=$PCODE
```

※ SSL でサーバーへアクセスする場合は、「https://<管理サーバー IP アドレス>:4443/mail/tempqueue/p_client.php?msgid=\$MSGID&code=\$PCODE」となります。

(3) 一時保留メール管理サーバー

差出人によるログイン機能が「オン」である場合、差出人による一時保留メール操作を受け付ける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。このサーバーは WEBGUARDIAN のプロキシ独自認証機能で使用するパスワード変更サーバーと共通です。WEBGUARDIAN プロキシ独自認証機能の詳細については、『検査サーバー 利用の手引き ~ WEBGUARDIAN V4.0 編 (ウェブ) ~』の「2-1 プロキシ独自認証機能」(16 ページ)をご参照ください。

(a) サーバーの起動・停止方法

【メール】-「システム管理」-「情報検査機能設定」-「拡張」画面で、「一時保留メール管理画面へのログイン」の「ログイン機能」を「オン」に設定した場合に自動で起動されます。「オフ」の設定を行った場合は停止されます。

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) サーバーの起動状況確認

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。この場合、専用サーバーは「Process “`/opt/Guardian/Admin/public/bin/httpd`”」と表示されます。

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、WEBGUARDIAN 共通～』の「3-2-1-2 状況確認」(51 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、WEBGUARDIAN 共通～』の「3-2-1-3 拡張機能」(55 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。

(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。

① 専用サーバーを停止します。

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

- ② 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>
```

- ③ 専用サーバーを起動します。

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

[2] SSL でサーバーへアクセスする場合

SSL で専用サーバー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。

- ① 専用サーバーを停止させます。

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

- ② `/opt/Guardian/Admin` ディレクトリへ移動します。

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

- ③ SSL ファイルを作成します。

```
#touch SSL
```

- ④ 専用サーバーを起動させます。

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

[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)

- ① 専用サーバーを停止します。

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


- ② 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>
```

- ③ 専用サーバーを起動します。

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

2-6 運用例

以下に基本的な運用例を紹介します。

(1) 部門情報管理者を置かず、一人の情報管理者が保留メールの管理を行う

情報管理者が保留メールを検閲する権限を有する場合、本システムの保留メール内容閲覧権限を変更し、内容閲覧を許可することができます。

(2) メール保留を発生させない

検査結果によるメールの保留、管理者による内容閲覧の後、処置を行うといった運用が特に必要がなければ、メールの削除（差出人への通知）、管理者への通知、メールの保存などで運用を行うことができます。

差出人への警告だけでよい場合は、差出人への削除通知文を編集し、運用ポリシーに従っていないという内容の警告メールを送信するという運用ができます。

(3) 差出人へ通知しない

差出人へ通知メールを送信しなければ、差出人にメールを保留もしくは削除したことを知られることはありません。

差出人に知られること無く管理者が保留メールの内容閲覧や送出、削除の処置を行います。

(4) 差出人が管理者に処置を依頼する

GUARDIANWALL のデフォルトの設定では、メールを保留した際に、個別処理方式に必要な MSGID と問合せコードを差出人のみに通知します。したがって、差出人から管理者に MSGID と問合せコードを伝え、処置を依頼しない限り、保留メールの内容が管理者によって読まれることはありません。

保留メールは指定期間（デフォルト 30 日）を過ぎると自動的にサーバー上から削除されます。

本運用方式は差出人のプライバシーに最大限配慮した運用方法です。

あるユーザーが、電子メール運用ポリシーに従わないメールを発信してしまう。



GUARDIANWALL が、検査の結果メールの発信を保留します。



GUARDIANWALL が、「メールが外部へ送信されず保留されているので上司に処置を依頼してください。」という文面と共に MSGID、問合せコードを差出人にメールで通知します。



GUARDIANWALL が同内容の通知メール（問合せコードはなし、保留理由が表示されている）を管理者に送信します。



通知メールを受けたユーザーが、自分の上司である部門情報管理者へ MSGID、問合せコードを伝え保留メールの処置を依頼します。



依頼を受けた部門情報管理者が、GUARDIANWALL システムに自分のユーザーアカウント、パスワードを入力しログインします。



部門情報管理者が依頼された MSGID、問合せコードを入力し該当保留メールの内容閲覧、そして適切な処置（送出もしくは削除）をします。



GUARDIANWALL が差出人と管理者に保留メールの処置通知メールを送信します。

差出人が管理者に処置を依頼する場合の処理の流れ

2-7 設定例

以下に基本的な設定例を紹介します。

(1) 検査・配送ルール

検査・配送ルールの差出人アドレス、宛先アドレスと動作の設定に関して説明します。設定方法については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「3-3-1-1 検査・配送ルール」(130 ページ)をご参照ください。設定内容の詳細仕様については、「5-3 検査・配送ルール設定ファイル」(100 ページ)をご参照ください。

差出人、宛先アドレスの設定欄にアドレスのみ設定した場合はそれぞれデフォルトで、ヘッダー FROM、エンベロープ TO アドレスが評価対象になります。デフォルト以外の評価対象アドレスを指定するためには下記に示した指定方法で記述してください。

指定項目	指定方法	評価対象アドレス
差出人	デフォルト (アドレスのみ)	ヘッダー FROM アドレス
	FROM = address	ヘッダー FROM アドレス
	EFROM = address	エンベロープ FROM アドレス
宛先	デフォルト (アドレスのみ)	エンベロープ TO アドレス
	ERCPT = address	エンベロープ TO アドレス
	TO = address	ヘッダー TO アドレス
	CC = address	ヘッダー CC アドレス
	RCPT = address	ヘッダー TO, CC アドレス

設定例)

- ・ 特定特権者以外の社外発信メールは検査

```
100 : FROM={priv1} : * : 0 : 中継
101 : FROM={priv2} : * : 0 : 中継
102 : * : * : 0 : 検査
```

- ・ 特定アドレスへの CC 指定無き社外発信メール保留、CC 指定有れば中継

```
100 : * : CC=address : 0 : 中継
101 : * : * : 0 : 保留
```

- ・ 特定アドレスへの CC もしくは TO 指定無き社外発信メール保留、有れば中継

```
100 : * : RCPT=address : 0 : 中継
101 : * : * : 0 : 保留
```

(2) MIME タイプ検査条件

MIME タイプ検査条件の設定例に関して説明します。設定方法については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』の「3-3-1-2 MIME タイプ」（149 ページ）をご参照ください。設定内容の詳細仕様については、「5-4 MIME タイプ検査条件設定ファイル」（145 ページ）をご参照ください。

設定例)

- ・指定添付ファイルを含むメール送信保留する（指定 MIME タイプを本番で登録する）。Word, Excel 添付メールの送信保留、それ以外の添付ファイルは送信可。

```
100: 本番: application/*: doc
120: 本番: application/*: xls
```

- ・指定添付ファイルを含むメールの量的統計情報のみ採取する。メールは、中継する（本番 / 試行 状態を全て試行で登録する）。

```
100: 試行中: application/*: doc
120: 試行中: application/*: xls
130: 試行中: application/*: ppt
140: 試行中: application/*: jxw
```

- ・指定添付ファイルのみ送信許可。その他添付ファイルは送信保留する（指定 MIME タイプのみ試行中で登録し、最下行のルールにコンテンツタイプ: application/*、拡張子: * の条件を本番で登録する）。Word, Excel のデータのみ送信許可、それ以外の添付ファイルは送信保留。

```
100: 試行中: application/*: doc
120: 試行中: application/*: xls
999: 本番: application/*: *
```

(3) キーワード検査条件

キーワード検査条件の設定例に関して説明します。設定方法については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』の「3-3-1-3 キーワード」（157 ページ）をご参照ください。設定内容の詳細仕様については、「5-5 キーワード条件式設定ファイル」（147 ページ）をご参照ください。

設定例)

- ・指定キーワードの組合せを含むメールを送信保留する（キーワード条件式を本番で登録する）。社外秘もしくは部外秘という文字列を含むメールの送信保留。

```
100: 本番: 社外秘 | 部外秘
```

- ・ 指定キーワードの組合せを含むメールの量的統計情報のみ採取する。メールは中継する（本番 / 試行 状態を全て試行で登録する）。

100:	試行中:	社外秘
120:	試行中:	部外秘
130:	試行中:	転送禁止
140:	試行中:	confidential

MEMO

3 グループ管理

3-1 グループ管理機能概要

グループ管理機能は、情報管理者、部門情報管理者が特定の利用者のメールだけを限定的に管理する機能です。

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、保留メール管理画面で保留メール一覧処理を行うと、そのグループに属する利用者のアドレスが発信者に含まれる保留メールの一覧だけが表示されます（設定により、受信者にアドレスが含まれるメール、発信者、受信者いずれかにアドレスが含まれるメールの表示も可）。

同様に、各種メールのログ表示機能を利用した時に、グループ管理機能は、管理者が特定の利用者グループのメールだけを限定的に閲覧することができる機能です。

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が発信者であるメールの一覧だけが表示されます（設定により、受信者にアドレスが含まれるメール、発信者、受信者いずれかにアドレスが含まれるメールの表示も可）。

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メールだけを管理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

管理対象に指定されたグループのアドレスを発信者、宛先、もしくは、その両方に含むメールだけ、保留メール一覧管理画面に表示します。

同様に、各種ログ閲覧画面においても、グループのアドレスを発信者、宛先、もしくは、その両方に含むメール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)。

管理対象グループを発信者(設定により受信者、両方)に含む保留メールだけ一覧表示します。

MSGID	年月日 時刻	発信者 宛先	サイズ 送信
UAA22760	2006/04/24 18:57:26	yamada@example.co.jp R60リスト	24.98KB 有
JAA23017	2006/05/12 09:32:50	yamada@example.co.jp 最終通告	23.29KB 有
LAA21191	2006/05/12 18:53:16	kato@example.co.jp 町会後報	1.95KB 有
FAA10020	2006/06/09 13:53:54	hio@example.co.jp Re: 調査依頼	74.95KB 有
TAA16341	2006/06/09 17:38:58	yamada@example.co.jp Re: 献血のお知らせ	74.95KB 有

管理対象グループを発信者(設定により受信者、両方)に含む保存メールのログだけを一覧表示します。

年月日 時刻	発信者 宛先	サイズ	閲覧
2006/06/13 18:33	Taro_Yamada@tokyo.example.co.jp2 明日の件確認	464B	未

利用例) 部門情報管理者「manager1」(グループ「osaka」を管理) の場合の表示

管理対象に指定されたグループのアドレスを発信者、宛先、もしくは、その両方に含むメールだけ、保留メール一覧管理画面に表示します。

管理対象グループを発信者（設定により受信者、両方）に含む保留メールだけ一覧表示します。

保留メール管理

保留メールの一覧です。現在、5通のメールが保留されています。

保留(5) 送出(0) 削除(0)

選択: すべて 解除 既読のみ 未読のみ チェックしたメールを [動作を選択]

	MSGID	年月日 時刻	発信者 宛先	サイズ 添付
<input type="checkbox"/>	UA22760	2006/04/24 18:52:26	yamada@example.co.jp 別のアドレス	24.98KB 無
<input type="checkbox"/>	JAA23017	2006/05/12 08:32:03	yamada@example.co.jp 最終通告	23.29KB 有
<input type="checkbox"/>	LA27191	2006/05/12 10:53:16	kato@example.co.jp 原価情報	1.25KB 無
<input type="checkbox"/>	PA010820	2006/06/09 13:53:54	llo@example.co.jp Re: 調査依頼	74.95KB 無
<input type="checkbox"/>	TAA16341	2006/06/09 17:38:58	yamada@example.co.jp Re: 献血のお誘い	74.95KB 有

同様に、各種ログ閲覧画面においても、グループのアドレスを発信者、宛先、もしくは、その両方に含むメール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）。

管理対象グループを発信者（設定により受信者、両方）に含む保存メールのログだけを一覧表示します。

メール閲覧

検索条件

任意期間: 2006年06月 01日 (木) ~ 2006年06月 14日 (木)

期間: 月間 2006年06月

検索: 2006年 ※ 待機待ちのタイムアウトする場合があります。

時間範囲: 00時 ~ 24時 指定時間以外

発信者アドレス: [検索]

受信者・同報者アドレス: [検索]

メール種類: [検索]

サイズ: [検索] 以上

検索条件: すべて満たす

動作: [検索]

閲覧: [検索] 監査: [検索]

表示形式: ☐ すべてのメールを表示 ☒ 20件ずつ表示

初期表示ページ: ☒ 先頭 ☐ 最終 ☐ 指定ページ [1]

☐ エンベロープアドレスを表示する

[クリア] [表示]

検索(00件)

保存メール 検索結果: 2006年06月01日 ~ 2006年06月14日

詳細情報を表示 ☒ 既読(他ユーザ) ☒ 既読 ☒ 監査済み

6/1 ~ 09/9/00件

年月日 時刻	発信者 宛先	サイズ	監査
2006/06/13 10:33	Taro Yamada@yamada.tokyo.example.co.jp 明日の件確認	464B	未



保留メール管理で「一覧処理方式」を利用している時だけ、グループに属する利用者のメールの一覧が表示されます。「個別処理方式」を利用している場合は、グループの設定に関係なく、入力したMSGID、問合せコードに一致するメールの管理を行います。

3-2 グループの登録

グループの作成、削除、変更はブラウザーで設定できます。(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「3-3-1-5 グループ」(169 ページ)をご参照ください。

グループ - 新規作成

新しいグループを作成します。

グループ名※

コメント

メールアドレス

アドレスリスト※

※印がある項目は必須です。
 ・グループ名に使用できるのは英数字と「_」(アンダースコア)だけです。(全角文字は不可)
 ・グループ名は英字の大文字と小文字は区別します。
 ・アドレスリストにはワイルドカードが指定できます。

グループに属するメールアドレスを1つずつ追加します。登録されたメールアドレスの大文字、小文字は同一視して判定します。長さ0以上の任意の文字列に一致する、ワイルドカード文字「*」を使用することもできます。

たとえば、あるドメイン(とそのサブドメイン)に属するメールアドレスを全て登録する場合は、以下のように2行記述します。

*@tokyo.example.co.jp

*.tokyo.example.co.jp



1つのグループに登録できるアドレス数は最大8000件です。

グループ名に使用できるのは半角の英数字と「_」(アンダースコア)だけです。英大文字小文字は区別します。

メールアドレスに使用できるのは半角の英数字とスペース、「_」「.」「-」「*」「@」「「」「¥」です。

3-3 グループ管理

(1) 管理対象グループ

管理対象に指定されたグループのアドレスを発信者、宛先、もしくは、その両方に含むメールだけ、保留メール一覧管理画面に表示します。同様に、各種ログ閲覧画面においても、グループのアドレスを発信者、宛先、もしくは、その両方に含むメール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、WEBGUARDIAN 共通 ～**』の「6-2-1-4 情報管理者の権限リスト」（412 ページ）、「6-2-1-5 部門情報管理者の権限リスト」（424 ページ）、「6-2-1-3 アカウントの編集・削除」（411 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アドレスを発信者、受信者（後述のグループ対象範囲条件で指定可能）に含むメールだけを表示するようにします。

グループ対象範囲条件

指定したグループに属するアドレスを発信者、もしくは、受信者に含むメールだけ表示したい場合は、「**送受信メール**」を選択します。発信者に含むメールだけ表示したい場合は、「**送信メールのみ**」を選択します。受信者に含むメールだけ表示したい場合は、「**受信メールのみ**」を選択します。

デフォルトの設定では以下のアドレスを使用して判定します。

ログ一覧表示画面

発信者： ヘッダー From アドレス

受信者： ヘッダー To, CC とエンベロープ TO アドレス

保留メール一覧表示画面

発信者： ヘッダー From アドレス

受信者： ヘッダー To, CC とエンベロープ TO アドレス

(2) 優先除外対象グループ

少数のアドレスを除いて、それ以外のアドレス全てを管理対象にしたいような場合には、少数のアドレスをグループとし、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。

優先除外対象に指定されたグループのアドレスを発信者、宛先、もしくは、その両方に含むメールを、保留メール一覧管理画面に表示しません。同様に、各種ログ閲覧画面においても、グループのアドレスを発信者、宛先、もしくは、その両方に含むメールを表示しません（優先除外対象と判定されたメールは、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）。

特定のユーザーのメールを保留メール一覧や、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。



管理対象グループ（もしくは、優先除外対象グループ）は、複数のグループを指定することができます。ただし、管理対象グループ（もしくは、優先除外対象グループ）に指定したグループ数に関わらず、定義したアドレス（もしくは、ワイルドカードを含むアドレスパターン）を合計して最大で 8000 件しか管理対象にできません。それを超えるアドレスについては無視されます。

たとえば、A グループに 5000 件、B グループに 4000 件のアドレス（もしくは、ワイルドカードを含むアドレスパターン）を登録している場合、管理対象グループ（もしくは、優先除外対象グループ）に A:B のように、A グループと B グループを同時に指定しても、合計が 8000 件を超えているため、8000 件を超えたアドレスは無視します。必ず、合計 8000 件以内で定義してください。

3-4 検索条件グループ

保存メール検索・閲覧画面などの各種ログ検索・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アドレスをメールの発信者（もしくは受信者）に含むメールを検索します。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、WEBGUARDIAN 共通～』の「3-3-3-1 メール閲覧」（188 ページ）をご参照ください。

発信者アドレス	<input type="text"/>	--
受信者・同報者アドレス	<input type="text"/>	--
メール標題	<input type="text"/>	開発部 営業部 人事部

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（リストボックス内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、WEBGUARDIAN 共通～』の「6-2-1-4 情報管理者の権限リスト」（412 ページ）、「6-2-1-5 部門情報管理者の権限リスト」（424 ページ）、「6-2-1-3 アカウントの編集・削除」（411 ページ）をご参照ください。

GUARDIANSUITE 利用者管理メニュー 管理者名: unadm 共通 ◆ 利用者管理 情報管理者 部門情報管理者 システム管理者 ■ セキュリティ メール ウェブ パスワード変更 ログアウト	グループ管理	開発 + 更新
	システム各種設定	開発 + 更新
	優先除外対象グループ	<input type="radio"/> なし(全メールが対象) <input type="radio"/> グループ <input type="text"/> を管理対象外にする 選択
	管理対象グループ	<input type="radio"/> なし(全メールが対象) <input type="radio"/> グループ <input type="text"/> だけを管理対象にする 選択
	グループ対象範囲条件	送信メールのみ
	検索条件グループ指定	<input type="radio"/> なし(グループ条件指定なし) <input type="radio"/> 登録済み全グループを選択可能にする <input type="radio"/> グループ <input type="text"/> だけを選択可能にする 選択
	■ ウェブオペレーション権限リスト	
	規制ルール管理	開発 + 更新
	例外ルール管理	開発 + 更新
	ユーザー定義管理	開発 + 更新

検索条件グループ指定

保存メール検索・閲覧画面などで発信者、受信者・同報者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、登録済のグループ名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。

特定のグループ名だけをリストアップしたい場合は、グループ名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。

3-5 検査・配送ルール

検査・配送ルールの発信者、宛先条件の指定に、グループを用いることができます。検査・配送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、WEBGUARDIAN 共通～』の「3-3-1-1 検査・配送ルール」(130 ページ)をご参照ください。

GUARDIANWALL
 情報管理メニュー
 管理者名: admin
 共通
 メール
 ◆ポリシー設定
 ◆検査・配送ルール
 MIMEタイプ
 キーワード
 通知文
 グループ
 保留メール管理
 ■保存メール管理
 ■ログ閲覧
 ■システム管理
 ウェブ
 パスワード変更
 ログアウト

検査・配送ルール - 編集

メール

定義されているルールを表示しています。
ルール編集完了後、【登録】画面でルールを更新して下さい。

行	ID	説明
2	102	"stop"は保留

差出人条件: *

宛先条件: ercpt=bp-*@example.co.jp

数値条件: keyword(set=stop,weight,max)>=1

動作: カスタム

☐ IDは必須項目です。
☐ 受信者通知の設定は、受信者通知機能がONの場合に有効です。
☐ メール保存の設定は、保存対象が「検査配送ルール」に指定されたメールのみ保存の場合のみ有効です。
☐ 検査条件の有効ID範囲の指定は、検査条件分割機能がONの場合に有効です。

IDをクリックすると【編集】画面になります。

行	ID	差出人条件	宛先条件	数値条件	動作
1	101	admin@example.co.jp	*	0	中継
2	102	*	ercpt=bp-*@example.co.jp	keyword(set=stop,weight,max)>=1	カスタム "stop"は保留
3	103	*@osk.example.co.jp	*	0	カスタム "保留通知を部長へ"
4	104	*	*	Address(RCPT)>=10	保留

差出人、宛先及び条件は、下表に示す記法を用いて、ヘッダー情報やエンベロープ情報に対して条件指定ができます。本表記法の詳細については、「5-3 検査・配送ルール設定ファイル」(100 ページ)をご参照ください。

指定項目	指定方法	評価対象アドレス
差出人	FROM = {group}	ヘッダー FROM アドレス
	EFROM = {group}	エンベロープ FROM アドレス
宛先	ERCPT = {group}	エンベロープ TO アドレス
	TO = {group}	ヘッダー TO アドレス
	CC = {group}	ヘッダー CC アドレス
	RCPT = {group}	ヘッダー TO, CC アドレス
備考 ・ 演算子「=」は評価対象アドレス（の少なくとも1つ）が指定グループ（group）に属していれば真 ・ 宛先で演算子「==」を使用すると、評価対象アドレス（複数）全てが指定グループ（group）に属していれば真 ・ 演算子の前に「!」をつけると真偽値が逆になります。		



検査・配送ルール の条件に用いたグループ定義内容は、GUARDIANWALL サーバー起動時に定義内容を読み込みます。グループの定義内容を変更した場合は、同サーバーの再起動を行ってください。再起動方法については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通 ～**』の「**3-2-2-4 起動・停止**」(99 ページ) をご参照ください。

検査・配送ルール の条件に使用しているグループを削除したい場合は、先に検査・配送ルール の該当グループを使用しているルール行を変更または削除してください。

MEMO

4 システム設定・保守

本章では、GUARDIANWALL システムの各種設定方法、保守方法について説明します。

4-1 設定ファイル

ブラウザを利用して、GUARDIANWALL の基本的な項目は設定できますが、設定ファイルを直接編集して変更する方法について説明します。

GUARDIANWALL の設定ファイルは、管理サーバーと検査サーバーの 2 箇所にあります。

管理サーバー側をマスターとして管理していますので変更する場合は、こちらを編集することになります。

設定ファイルとしては下表に示す 6 種類があります。

■ 管理サーバー側

設定ファイル	パス名
サーバー設定ファイル ^(※1)	/opt/Guardian/Admin/etc/wall/mss.conf (共通)
	/opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf (個別)
	/opt/Guardian/Admin/etc/wall/zp.conf (共通)
検査・配送ルール設定ファイル	/opt/Guardian/Admin/etc/wall/mss.acl
MIME タイプ検査条件設定ファイル	/opt/Guardian/Admin/etc/wall/mss.mtype
	/opt/Guardian/Admin/etc/wall/mss.mtype.d/*.mtype
キーワード検査条件設定ファイル	/opt/Guardian/Admin/etc/wall/mss.keywd
	/opt/Guardian/Admin/etc/wall/mss.keywd.d/*.keywd
通知文設定ファイル	/opt/Guardian/Admin/etc/wall/mss.notice
	/opt/Guardian/Admin/etc/wall/template/*
	/opt/Guardian/Admin/etc/wall/zp.notice
動作一覧定義ファイル	/opt/Guardian/Admin/etc/wall/action
(※1) 管理サーバー側で管理しているサーバー設定ファイルは、全ての検査サーバー（メール）に共通で利用可能な設定を行う mss.conf、zp.conf と、検査サーバーごとに個別で利用するための設定を行う server.conf の 3 つの設定ファイルを持ちます。 検査サーバー側のサーバー設定ファイルを更新する場合は、これら 3 つの設定ファイルを併合したものを使用します。 なお、これらのサーバー設定ファイルの内容は、server.conf で記述しているものを優先して利用します。	

■ 検査サーバー側

設定ファイル	パス名
サーバー設定ファイル	/opt/Guardian/WALL/etc/mss.conf /opt/Guardian/WALL/zencry/etc/zp.conf
検査・配送ルール設定ファイル	/opt/Guardian/WALL/etc/mss.acl
MIME タイプ検査条件設定ファイル	/opt/Guardian/WALL/etc/mss.mtype /opt/Guardian/WALL/etc/mss.mtype.d/*.*mtype
キーワード検査条件設定ファイル	/opt/Guardian/WALL/etc/mss.keywd /opt/Guardian/WALL/etc/mss.keywd.d/*.*keywd
通知文設定ファイル	/opt/Guardian/WALL/etc/mss.notice /opt/Guardian/WALL/template/* /opt/Guardian/WALL/zencry/etc/zp.notice /opt/Guardian/WALL/zencry/template/*
動作一覧定義ファイル	なし



GUARDIANWALL Ver6.0 から、設定ファイルの管理は管理サーバーで行います。

もし、検査サーバー側の設定ファイルを直接編集し利用していた場合、管理サーバーで何らかの設定変更が行われた時にその編集内容は上書きされ、以前の設定は無効になってしまいます。

設定ファイルを直接編集する場合は、必ず管理サーバー上のものを編集するようにしてください。

4-2 システムの設定更新と再起動

管理サーバー上の設定ファイルを直接変更した場合は、GUARDIANWALL 上のその設定ファイルを更新し、稼動中の SMTP サーバー、STORE サーバーにその設定変更を反映させるための再起動を行う必要があります。下表のスクリプトを利用してください。

■ 設定ファイルの更新（管理サーバー側）

項目	起動スクリプト 引数
サーバー設定ファイル編集時	/opt/Guardian/Admin/support/pushMailWall [-s <server_id>] conf
検査・配送ルール設定 ファイル編集時	/opt/Guardian/Admin/support/pushMailWall acl
MIME タイプ検査条件設定 ファイル編集時	/opt/Guardian/Admin/support/pushMailWall mtype
キーワード検査条件設定 ファイル編集時	/opt/Guardian/Admin/support/pushMailWall keyword
通知文設定ファイル編集時	/opt/Guardian/Admin/support/pushMailWall notice

■ GUARDIANWALL の再起動（検査サーバー側）

項目	起動スクリプト 引数
GUARDIANWALL 再起動	/etc/init.d/Guardian.mail restart

ウェブブラウザを利用して設定変更した場合は、これらのスクリプトを必要に応じて CGI プログラムの中で実行していますので、GUARDIANWALL の再起動を行う必要はありません。

4-3 設定変更

内部ドメイン名の設定変更を例に、設定変更の手順を説明します。

内部ドメイン名は、GUARDIANWALL を導入した内部ネットワークのドメイン名を設定します。設定されたドメイン名に従って、GUARDIANWALL が処理するメールがネットワーク内部から送信されたものか、外部から送信されたものか判定します。外部から送信されたメールに対しては、いかなる場合でも、その差出人へ通知メールは送信しません。デフォルト設定では外部から送信されたメールの検査は行わず、そのまま中継します。

その他の設定項目については、「5-2 サーバー設定ファイル」(70 ページ) をご参照ください。

サーバー設定ファイルをエディタ等で編集します。

- 全ての GUARDIANWALL に共通で利用する場合

```
# vi /opt/Guardian/Admin/etc/wall/mss.conf
```

- 複数管理している GUARDIANWALL の内 1 台だけで利用する場合

```
# vi /opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf
```

以下の要領で内部ドメイン名を記述してください。

内部ネットワークで使用しているドメイン名が複数ある場合は、「&」で区切り続けて記述してください（「&」の前後に空白文字は入れないようにしてください）。

未設定の場合はデフォルトでインストールしたサーバーホストのドメイン名の「XXX.YY.jp」が内部ドメインとして設定されます（サーバーホストのドメインが取得できない場合はエラーとなり SMTP サーバーは起動できません）。

```
[Mail]
InternalDomains = domain1.co.jp&domain2.co.jp
```

GUARDIANWALL の設定ファイルを更新します。

```
# /opt/Guardian/Admin/support/pushMailWall [-s <server_id>] conf
```

※特定の GUARDIANWALL のみ行う場合は、-s オプションで検査サーバー ID を指定して実行してください。

各検査サーバー上で、GUARDIANWALL を再起動します。

```
# /etc/init.d/Guardian.mail restart
```

4-4 グループ管理

(1) グループの定義

グループの作成、削除、変更は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「3-3-1-5 グループ」(169 ページ)をご参照ください。設定ファイルを直接編集して変更する場合は、下記ファイルを直接編集します。

サーバーの種類	管理サーバー
登録ディレクトリ	/opt/Guardian/Admin/etc/wall/group/
ファイル名	<グループ名>.addr

登録ディレクトリに「グループ名.addr」という名前のファイルを作成します。各ファイルには、そのグループに属する利用者のメールアドレスを1行ごとに記述します。登録されたメールアドレスの大文字、小文字は同一視します。長さ0以上の任意の文字列に一致する、ワイルドカード文字「*」を使用することもできます。たとえば、あるサブドメインだけに属するアドレスを全て登録したい場合は、以下のように記述することができます。

*@sub.example.co.jp

記述例)

グループ名 : tokyo

ファイル名 : tokyo.addr

```
*@tokyo.example.co.jp
*.tokyo.example.co.jp
admin@example.co.jp
user1@example.co.jp
```

グループ名 : osaka

ファイル名 : osaka.addr

```
*@osaka.example.co.jp
*.osaka.example.co.jp
admin@example.co.jp
```



グループ名に使用できるのは半角の英数字と「_」(アンダースコア)だけです。英大文字小文字は区別します。

メールアドレスに使用できるのは半角の英数字とスペース、「_」「.」「-」「*」「@」「「」「¥」です。

管理サーバー上のグループ別設定ファイルを直接編集した後、以下のスクリプトを利用して、GUARDIANWALL の同設定ファイルを更新してください。

グループファイル

```
# /opt/Guardian/Admin/support/pushMailWall -f<グループ名>group
```

また、グループを削除する場合は、以下のスクリプトを利用して、管理サーバーの設定ファイルと GUARDIANWALL の同設定ファイルを削除してください。

```
# /opt/Guardian/Admin/support/pushMailWall -d -f<グループ名>group
# rm /opt/Guardian/Admin/etc/wall/group/<グループ名>.addr
# rm /opt/Guardian/Admin/etc/wall/group/<グループ名>.ldap
```



GUARDIANWALL の検査・配送ルール内で、ここで編集したグループを利用している場合、検査サーバー上で GUARDIANWALL の再起動が必要です。「<グループ名>.ldap」は LDAP インポート機能を利用し、検索方法の「保存する」をチェックした場合に、作成されるファイルです。

(2) 管理対象グループの設定

情報管理者、部門情報管理者の個別設定ファイルを編集し、設定する方法を説明します。グループ管理機能の詳細については、「3 グループ管理」(40 ページ)をご参照ください。

なお、個別設定ファイルの編集は、管理サーバー上で行います。

管理対象に指定されたグループのアドレスを発信者、宛先、もしくは、その両方に含むメールだけ、保留メール一覧管理画面に表示します。同様に、各種ログ閲覧画面においても、グループのアドレスを発信者、宛先、もしくは、その両方に含むメールだけを一覧表示します。

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
```

```
[Admin]
HoldList=true          # 一覧処理方式を利用する
HoldMessage=true       # 本文内容閲覧許可
Group=tokyo            # 管理グループ
Group=tokyo:osaka      # 複数設定する場合は「:」で区切る
FromFilter=true        # 発信アドレスがグループに属するメールを管理する
RcptFilter=true        # 宛先アドレスにグループに属するものが含まれて
                        # いるメールを管理する。
```

- ・ 部門情報管理者、アカウント「manager1」の場合
/opt/Guardian/Admin/etc/admin/manager/manager1.conf

```
[Manager]
HoldList=true
HoldMessage=true
Group=osaka          # グループ osaka を管理する
FromFilter=true
RcptFilter=true
```



グループ指定に関する制限事項

管理対象グループに複数のグループを指定することができますが、指定グループ数に関わらず、全て合計して最大で 8000 件のアドレスしか管理対象にできません。それを超えるアドレスについては無視されます。

少数のアドレスを除いて、それ以外の（8000 件を超えるアドレス）全てを管理対象にしたいような場合には、後述の優先除外対象グループを使用してください。

管理サーバー上のアカウント別設定ファイルを直接編集した後、以下のスクリプトを利用して、GUARDIANWALL の同設定ファイルを更新してください。

情報管理者

```
# /opt/Guardian/Admin/support/pushMailWall -f <account> admin
```

部門情報管理者

```
# /opt/Guardian/Admin/support/pushMailWall -f <account> manager
```


(3) 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	管理するグループ名を列挙する。未指定時は、全てのメールが管理対象（閲覧対象）	文字列（グループ名） 複数の場合は、「:」で区切る
ExcludeGroup	未指定	優先除外するグループ名を列挙する。未指定時は除外を行わない。（全てのメールを管理する）	文字列（グループ名） 複数の場合は、「:」で区切る
QueueGrouping	True	保留メール管理でグループ管理機能を使用し、グループに属するメールを表示する場合は True、全ての保留メールを表示する場合は False を指定する。	True/False
LogGrouping	True	ログ一覧表示でグループ管理機能を使用し、グループに属するメール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、グループに属するメール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
FromFilter	True	差出人アドレスがグループに含まれるメールをグループ管理対象とする場合は、True を指定する。False を指定した場合は差出人アドレスがグループに含まれていても管理対象とならない。FromFilter と RcptFilter の少なくとも一方が True でなければならない。	True/False
FromFilterSelect_Queue	header	保留メール管理画面でグループ管理対象とするメールの差出人アドレスとして何を使用するか指定する。 ヘッダー / エンベロープ / 両方から選択する。	header/envelope/both
FromFilterSelect_Log	header	ログ一覧表示、統計情報表示画面でグループ管理対象とするメールの差出人アドレスとして何を使用するか指定する。 ヘッダー / エンベロープ / 両方から選択する。	header/envelope/both
RcptFilter	False	宛先アドレス（の一部または全部）がグループに含まれるメールをグループ管理対象とする場合は、True を指定する。False を指定した場合は宛先アドレス（の一部または全部）がグループに含まれていても管理対象とならない。 FromFilter と RcptFilter の少なくとも一方が True でなければならない。	True/False

キー	初期値	意味	設定範囲
RcptFilterSelect_Queue	envelope	保留メール管理画面でグループ管理対象とするメールの宛先アドレスとして何を使用するか指定する。 ヘッダー / エンベロープ / 両方から選択する。	header/envelope/both
RcptFilterSelect_Log	both	ログ一覧表示、統計情報表示画面でグループ管理対象とするメールの宛先アドレスとして何を使用するか指定する。ヘッダー / エンベロープ / 両方から選択する。	header/envelope/both
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名を列举する。 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（グループ名） 複数の場合は、「:」で区切る
FromFilterSelect_Search	header	発信者の検索条件にグループを選択した場合、差出人アドレスとして何を検索対象にするか指定する。 ヘッダー / エンベロープ / 両方から選択する。	header/envelope/both
RcptFilterSelect_Search	header	受信者・同報者の検索条件にグループを選択した場合、宛先アドレスとして何を検索対象にするか指定する。 ヘッダー / エンベロープ / 両方から選択する。	header/envelope/both



統計情報表示をグループ管理対象とする場合

統計情報の元となる配送ログは宛先としてエンベロープ情報のみ記録しています。RcptFilter の値を TRUE とした場合は、宛先側条件指定である RcptFilterSelect_Log の設定に関わらず常にエンベロープ TO を用います。
他のログの表示件数と異なる場合がありますのでご了承ください。

4-5 ログファイル管理

(1) ログファイルの種類

GUARDIANWALL が記録するログファイルは下表に示す 6 種類あります。

ログ保存ディレクトリの初期値は「/opt/Guardian/WALL/logs/」に設定しています。

ログファイル	パス名	備考
システムログ	(LOG_DIR)/log.YYYYMMDD	システムのログ
配送ログ	(LOG_DIR)/deliver/YYYY/MM/DD	メール処理記録 統計情報表示に利用
情報検査ログ	(LOG_DIR)/screening/YYYY/MM/DD	MIME タイプ、キーワード 情報検査結果記録
保留メール操作ログ	(LOG_DIR)/manager/YYYY/MM/DD	保留メール操作の記録
保存メール検索用ログ	(LOG_DIR)/archive/YYYY/MM/DD	保存メール内容の参照に利用
保存メール閲覧ログ	(LOG_DIR)/viewer/YYYY/MM/DD	保存メール内容の閲覧記録
(LOG_DIR) : ログ保存ディレクトリ YYYY MM DD : 年月日		

(2) ログファイルの削除

本システムを連続で稼動していれば、指定期間を超えた古いログファイルは自動的に削除されます。

手で削除したい場合は、上表より削除したいファイルを削除してください。ログファイルを削除しても、本システムを再起動する必要はありません。

(3) ログファイルの形式について

ログファイルを直接使用したい場合は、管理サーバーの各種ログ閲覧画面の「ダウンロード」の機能をご利用ください。ログファイルを CSV 形式に変換したファイルをダウンロードしてご利用いただけます。ログファイル中に記録されている項目に関しては、CSV ファイル中に記述しておりますので、ご参照ください。

上記システム上にあるログファイルの記録形式に関する情報は公開しておりません。製品の改良などにもない予告無く変更する場合がありますので、ご了承ください。

4-6 保存メール管理

(1) ファイルの種類

GUARDIANWALL でメール保存機能を利用している場合、保存ディレクトリ以下に下表に示すファイルを作成します。

メール保存ディレクトリは初期値では、未設定です。

ファイル	パス名	備考
メールアーカイブ	(ARC_DIR)/YYYYMMDD-HOSTID-DEVID.mar	メッセージデータのアーカイブファイル
インデックス	(ARC_DIR)/YYYYMMDD-HOSTID-DEVID.index	アーカイブファイルのインデックス情報ファイル
インデックスリスト	(ARC_DIR)/index.list	アーカイブ、インデックスファイルのリスト
削除用インデックスリスト	(ARC_DIR)/index.list.old	古いアーカイブ、インデックス削除時に使用するリスト
(ARC_DIR) : メール保存ディレクトリ HOSTID : ホスト ID DEVID : ファイルシステムのデバイス ID YYYY MM DD : 年月日		

(2) ファイルの削除に関して

本システムを連続で稼動している場合は、保存ディレクトリに指定された各ディレクトリの領域を 100% まで利用し、保存ディレクトリを順次切り替えながら使用します。古いアーカイブデータ、インデックスデータは順次消しながら使用しますので、手動で削除する必要はありません。手動で上記ファイルの削除や編集をすると、保存先のディレクトリが変わったり、以前の古いアーカイブ、インデックスファイルが削除されなくなったりすることがあります。上記ファイルを手動で削除したり、編集したりしないでください。



保存ディレクトリは、メール保存専用の領域を指定してください。ログ保存領域や、OS や他のプログラムなどで使用する領域とは共有しないでください。必ず、1 つのメール保存ディレクトリは、1 つのパーティション、ファイルシステムから構成してください。

4-7 MSP（Mail Submission Program）の設定変更

(1) sendmail（Ver8.11 以前）

以下の手順で、sendmail.cf の変更を行ってください。

・ GUARDIANWALL の停止

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

・ sendmail の停止

```
# /etc/init.d/sendmail stop
```

・ sendmail.cf の変更、確認

sendmail -bt 等で必ず変更後の内容が正しいことを確認してください。

また、sendmail 単独で起動し、メールの中継、（場合によっては当サーバーでの）受信が正しく行われること、さらに、sendmail を MSP としてメールの送信が行えることを確認してください。

・ GUARDIANWALL の起動、確認

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

sendmail -q30m の起動も行われます。

ブラウザで情報管理者の管理画面にログインし、【共通】-「**検査サーバー管理**」-「**状況確認**」-【**稼動状況**】で稼動中となっていることを確認してください。



GUARDIANWALL をインストールしている環境では、書籍などで紹介されている、通常のメールサーバー管理等の sendmail の設定、起動手順をそのまま実行することはできません。

GUARDIANWALL 稼動状態で起動されている sendmail は SMTP 受信デーモンではありません。SMTP の受信は GUARDIANWALL が行います。sendmail は（メールがスプールされていれば）キューの再送処理を行うだけのデーモン（/usr/lib/sendmail -q30m）として起動しています。

(2) sendmail Ver8.12 以降

sendmail Ver8.12 以降を使用する場合は、以下の点に注意して設定を確認してください。

sendmail Ver8.12 より sendmail を MSP (Mail Submission Program) として起動してメール送信する場合の動作が変更されています。sendmail を MSP として起動した場合は、submit.cf を参照します。特に設定することなくデフォルトのままインストールされた submit.cf の設定は localhost の smtp ポートに接続し、メールを送信する設定になっています。sendmail Ver8.12 以降だけがインストールされた環境では問題になりませんが、GUARDIANWALL をインストールした環境ではメールがループすることになり、正常にメールの送信ができません。必ず、以下の設定を行ってください。

GUARDIANWALL からメール送信のために sendmail を起動する際に、submit.cf を使用しない sendmail 起動オプションを追加する必要があります。

- ・ 管理サーバー側の GUARDIANWALL のサーバー個別設定ファイル (/opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf) に以下内容を追記して、GUARDIANWALL の設定ファイルの更新と、再起動を行ってください。

```
[SMTP]
SendmailOption = -Am
```



sendmail Ver8.12 以降をご使用の場合のみ上記オプションを設定してください。また、設定値には上記値以外のものは設定しないでください。

sendmail Ver8.11 以前のバージョンは上記オプション値を指定するとエラーとなって sendmail が起動できなくなり、GUARDIANWALL からメールの送信ができません。



sendmail の設定変更手順については、前述の「(1) sendmail (Ver8.11 以前)」と同様になります。

(3) qmail, Postfix

qmail、Postfix を使用する場合は、以下の点に注意して設定を確認してください。

前提条件

qmail、Postfix の sendmail 互換インタフェースを使用しますので、インストールしてください。

qmail,Postfix の設定変更

qmail、Postfix の SMTP サーバーの代わりに GUARDIANWALL が SMTP サーバーとして動作することになります。そのために qmail、Postfix の SMTP サーバーを止め、起動しないように設定を変更する必要があります。

- ・ 管理サーバー側の GUARDIANWALL のサーバー個別設定ファイル（/opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf）に以下内容を追記して、GUARDIANWALL の設定ファイルの更新と、再起動を行ってください。

qmail の場合

```
[SMTP]
MailSubmissionProgram = qmail
QmailProgram = <sendmail 互換プログラムパス名>
                (デフォルト /usr/lib/sendmail)
QmailQueueDirectory = <キューディレクトリ>
                (デフォルト /var/qmail/queue)
QmailQueueListProgram = <キューリスト表示プログラムパス名> <引数>
                (デフォルト /var/qmail/bin/qmail-qstat)
```

Postfix の場合

```
[SMTP]
MailSubmissionProgram = postfix
PostfixProgram = <sendmail 互換プログラムパス名>
                (デフォルト /usr/lib/sendmail)
PostfixQueueDirectory = <キューディレクトリ>
                (デフォルト /var/spool/postfix)
PostfixQueueListProgram = <キューリスト表示プログラムパス名> <引数>
                (デフォルト /usr/sbin/postqueue -p)
```



QmailProgram, PostfixProgram はオリジナル sendmail ではなく、それぞれ qmail、Postfix の sendmail 互換インタフェース用 sendmail プログラムを指定してください。



qmail、Postfix の起動 / 停止スクリプトは、ご使用の環境に合わせて準備してください。GUARDIANWALL の起動 / 停止スクリプト（/etc/rc2.d/Guardian.mail 等）では qmail、Postfix の起動 / 停止は行いません。

5 仕様

本章では、日本語検査機能、各設定ファイルに関する詳細仕様について説明します。

5-1 日本語検査仕様

(1) メッセージ検査範囲

プレーンテキストのみのメッセージ（MIME マルチパートでないもの）

メッセージヘッダー部、メッセージボディ部別々に検査します。

```
Received: #####  
Return-Path:  
Mime-Version: 1.0  
Subject: =?ISO-2022-JP?B?#####3=?=  
From: #####@example.co.jp (=?ISO-2022-  
JP?B?#####=?=)  
Date: 27 May 1997 11:04:59 +0900  
To: xxxxxxxx@yyyyyyyyy.co.jp  
Cc: yyyyyyyyyy@example.co.jp  
Lines: 116  
Message-Id: <338A414B.64532.002@example.co.jp>  
Content-Type: text/plain; charset=ISO-2022-JP
```

```
This is a simple message.  
PLAINTEXT MESSAGE  
---
```

Message Header 部
base64 デコード実施

Message Body 部

キーワード条件式が「キーワード1 & キーワード2」の場合、ヘッダー部に「キーワード1」、ボディ部に「キーワード2」が含まれたメッセージは、上記キーワード条件式を満たしません。

MIME マルチパート形式メッセージ

パートごとに検査します（キーワードの論理式の適用範囲はパート内のみです）。

```
Received: #####
Return-Path:
Mime-Version: 1.0
Subject: =?ISO-2022-JP?B?#####3=?=
From: #####@example.co.jp (=?ISO-2022-
JP?B?#####=?=)
Date: 27 May 1997 11:04:59 +0900
To: xxxxxxxx@yyyyyyyyyy.co.jp
Cc: yyyyyyyy@example.co.jp
Lines: 116
Message-Id: <338A414B.64532.002@example.co.jp>
Content-Type: multipart/mixed; boundary=" BOUNDARY"
```

```
This is preamble message.
This is a multipart message in MIME format.
```

```
--BOUNDARY
Content-Type: text/plain; charset=ISO-2022-JP
```

```
PART1 PLAINTEXT PART
TEXT TEXT TEXT TEXT
```

```
--BOUNDARY
Content-Type: application/octet-stream; size=524288
Content-Transfer-Encoding: base64
Content-Description: perfmon.doc
```

```
JdAtbGg1LbR8AwCksAsAETi4liABDFBFukYwNTI
CpUBRbFQoigMncyZ0x1rpCQEFAIkACqVpC5SSJJ
QaVrWitWYq6rVaOdrnmq2b5tpURX79999+730z
nvc9/n739Pv8Avd22jkbbeZRXIqEUyICEIxIeXY
```

```
--BOUNDARY--
This is epilogue message
```

第 1 パート
プレーンテキスト
ヘッダー

base64 デコード実施

第 2 パート
プレーンテキスト

MIME preamble 部
(無い場合もあります)

第 3 パート
プレーンテキスト
パートヘッダーは無視し
ます

第 4 パート
MS WORD ドキュメント
デコード、テキスト抽出
実施
パートヘッダーは無視し
ます

第 5 パート
プレーンテキスト
MIME epilogue 部
(無い場合もあります)

キーワード条件式が「キーワード 1 & キーワード 2」の場合、同一パートに「キーワード 1」、「キーワード 2」が含まれたメッセージのみ上記キーワード条件式を満たします。第 1 パートに「キーワード 1」のみ含まれ、第 2 パートに「キーワード 2」のみ含まれる場合は、本メッセージは上記キーワード条件式を満たしません。

※添付ファイル名は、ファイル名 1 つで検査対象の 1 つのパートとして扱います。

添付ファイル名中キーワードと他のパート（テキスト本文など）の間でキーワードの「&」条件は満たすことができません。

(2) キーワード検出範囲

① 下記のように単語が複数行にまたがっていても検出できます。

例) 「社外秘」のキーワードを検出できます。

あいうえおかきくけこさしすせそ社外
秘たちつてとなにぬねの

② 単語が複数行にまたがっていても、行頭に空白文字列が入っている場合や、引用された場合は検出できません。

例) 「社外秘」のキーワードを検出できません。

本日は晴天なり、社外
秘
> あいうえおかきくけこさしすせそ社外
> 秘たちつてとなにぬねの

③ メッセージのヘッダー部分では継続行を表す行頭の空白は無視します。

例) 「社外秘」のキーワードを検出できます。

Subject: このメールは社外
秘につき...

※キーワードが次行にまたがっている場合にキーワード検出を行わないように設定を変更することもできます。LookAheadNextLine オプション (85 ページ) をご参照ください。

(3) アプリケーションデータ

キーワード検査時に MIME 形式で添付された下記アプリケーションファイルに対しては、テキスト情報を抽出してキーワード検査を行います。検査時にファイル内容の識別を行っており、ファイル名が指定されていない場合や、拡張子が通常のものとは異なっても、キーワード検査を実行します。

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, 2010, 2013

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, 2010, 2013

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。

バイナリブック形式の検査はできません。

Excel アドイン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, 2010, 2013

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。

PowerPoint アドイン形式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, 2008, 2009, 2010, 2011, 2012

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は、多重に検出したり、検出できなかっ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、挿入される場合があります、キーワードを誤検出したり、検出できなかっ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。

(4) 圧縮ファイルの展開

対応形式

以下の表の圧縮 / アーカイブファイルを展開することが可能です。

	タイプ名	ファイルタイプ
1	ZIP	ZIP アーカイブ
2	LHA	LHA アーカイブ (拡張子は一般に .lzh)
3	RAR	RAR アーカイブ
4	CAB	CAB アーカイブ
5	GZIP	GZIP 圧縮ファイル
6	BZIP2	BZIP2 圧縮ファイル
7	Z	UNIX Compress 圧縮ファイル
8	TAR	TAR アーカイブ
9	7ZIP	7ZIP アーカイブ
10	ARJ	ARJ アーカイブ
11	RPM	RPM パッケージ
12	DEB	Debian パッケージ
13	ISO	ISO9660 イメージファイル
14	MSI	Microsoft インストールパッケージ
15	HQX	BinHex エンコードファイル
16	AS	AppleSingle ファイル
17	TNEF	Microsoft Outlook リッチテキストファイル
18	SZDD	DOS Compress 圧縮ファイル
19	PACK	UNIX PACK 圧縮ファイル

パスワード設定され暗号化された圧縮 / アーカイブ形式ファイルは展開できません。ファイル名に設定された拡張子に関係なく、ファイルの内容を識別して展開を試みます。

展開されたファイルの MIME のコンテンツタイプは便宜的に application/octet-stream が指定されたものとして扱い MIME タイプ検査を適用します。

※制限事項

- ・初期状態では、圧縮ファイルの展開を行わないように設定されています。設定の変更方法については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEB-GUARDIAN 共通～』の「3-3-5-2 情報検査機能設定」(234 ページ)をご参照ください。
- ・標準設定で展開する形式は、表の 1 ～ 8 の ZIP, LHA, RAR, CAB, GZIP, BZIP2, Z, TAR 形式です。表の他の形式も展開する場合は、拡張展開機能 **ExtractArchive_Full オプション** (86 ページ)をご参照ください。
- ・9 重まで多段に圧縮されたファイルを展開します。多重圧縮の展開制限数の設定

- を変更する場合は、**MaxExtractNesting オプション** (86 ページ) をご参照ください。
- 圧縮ファイルのサイズが 10 MB を超える場合は、展開を行いません (展開後のファイル合計サイズではなく、展開前の 1 つの圧縮ファイルサイズになります)。制限サイズの設定を変更する場合は、**MaxExtractSize オプション** (87 ページ) をご参照ください。
 - 展開後の 1 つのファイルサイズが 100 MB を超える場合、展開処理を行いません。制限サイズの設定を変更する場合は、**MaxExtractFileSize オプション** (87 ページ) をご参照ください。
 - 圧縮に使用したソフトウェアの種類・実装によっては、必ずしも検査時に元のファイル名が得られなかったり、展開が正常に行えなかったりする場合があります。また、圧縮に使用した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。
 - ZIP, LHA, RAR, CAB の DOS/Windows 実行形式による自己展開ファイル (SFX 形式圧縮ファイル) を展開する場合は、**ExtractArchive_SFX オプション** (86 ページ) をご参照ください。その他の SFX 形式ファイルは展開できません。
 - 日本語または ASCII 文字以外の TNEF 形式ファイルは展開できません。

(5) 個人情報検査

検査動作適用時に行う個人情報検査は、text/html パートを除く添付ファイルだけ対象とします。

検査可能なアプリケーションデータの種類、展開可能な圧縮ファイルについては前述の仕様と同じです。

5-2 サーバー設定ファイル

サーバー設定ファイルは、SMTP サーバー、STORE サーバーの詳細動作を設定します。

ファイルパス名

検査サーバー : /opt/Guardian/WALL/etc/mss.conf

(/etc/MGWall.conf は上記ファイルへのシンボリックリンクです)

管理サーバー : /opt/Guardian/Admin/etc/wall/mss.conf

表記法

[SectionName]

KeyName = Value

KeyName2 = Value2

SectionName, KeyName の英大小文字を区別しない。

Value に True/False を指定する場合は英大小文字を区別しない。

[LICENSE] セクション

LicenseKey : 文字列

ライセンスキー。

初期値 : 指定なし

[SMTP] セクション

SMTPPort : 整数 (1 ~ 65535)

SMTP サーバーホストの受信ポート番号。

初期値 : 25

MaxConnections : 整数 (0 ~ 999)

最大同時コネクション数。

初期値 : 0 (「0」指定時は無制限。システム制限値まで)

MaxMessageSize : サイズ表記もしくは整数 (最大指定 2 GB)

最大メッセージサイズ。

初期値 : 0 (「0」指定時は無制限。システム制限ファイル最大値まで)

サイズ表記 : ?G?M?K?B のような数字+単位の表記 (単位省略時は KB)

例)

1G : 1 GB

2M512K : 2.5 MB

1K : 1 KB

1024B : 1 KB

MaxRecipients : 整数 (0 ~ 99999)

1 通のメールに指定できる受信者アドレスの総数。

初期値 : 1000 (「0」指定時は無制限)

※この値を超えて受信者が指定されたメールを受け取ることはできません。100 以上指定されたメールを受信しても、送信時は宛先を 100 以下に分割して送信します。

ConnectionTimeout : 整数 (60 ~ 9000)

受信コネクションタイムアウト (秒数)。

初期値 : 1800 秒

AddReceivedField : TRUE/FALSE

メッセージヘッダーへの Received フィールドの付加。

初期値 : TRUE

SendmailProgram : パス名

sendmail プログラムパス名。

初期値 : /usr/lib/sendmail

CheckSendmailMqueue : TRUE/FALSE

sendmail に送信データを渡す前にキューの空き容量を調べる。

初期値 : TRUE

SendmailQueueDirectory : パス名

sendmail のキューディレクトリ。

初期値 : /var/spool/mqueue

※ MSP に qmail、Postfix が指定されている場合は、それぞれ QmailQueueDirectory、PostfixQueueDirectory に指定されているディレクトリの空き容量を検査します。

MailSubmissionProgram : sendmail/qmail/postfix

メール送信に利用する MSP のソフトを指定する。

初期値 : sendmail

SendmailOption : 文字列

メール送信時に sendmail を起動する時に付加するオプション。

初期値 : 指定なし

QmailProgram : パス名（絶対パス指定）
qmail を MSP として使用する時に、sendmail 互換インタフェースプログラムの絶対パスを指定する。
初期値 : /usr/lib/sendmail

QmailQueueDirectory : パス名
qmail を MSP として使用する時に、qmail のキューディレクトリを指定する。
初期値 : /var/qmail/queue

QmailQueueListProgram : パス名
qmail を MSP として使用する時に、qmail のキューのリストを表示するプログラムを指定する。
初期値 : /var/qmail/bin/qmail-qstat

PostfixProgram : パス名（絶対パス指定）
Postfix を MSP として使用する時に、sendmail 互換インタフェースプログラムの絶対パスを指定する。
初期値 : /usr/lib/sendmail

PostfixQueueDirectory : パス名
Postfix を MSP として使用する時に、Postfix のキューディレクトリを指定する。
初期値 : /var/spool/postfix

PostfixQueueListProgram : パス名（引数付与可）
Postfix を MSP として使用する時に、Postfix のキューのリストを表示するプログラムを指定する。
初期値 : /usr/sbin/postqueue -p

[Mail] セクション

InternalDomains : ドメイン名
内部ドメイン名リスト。
サーバーホストのドメイン名「XXX.co.jp」、「XXX.com」など。「&」で連結して複数ドメイン指定可能（ワイルドカード表記不可）。
初期値 : サーバーホストの FQDN ホスト名からドメイン名を取得

IgnoreExternalMail : TRUE/FALSE
外部から送信されたメール（上記内部ドメイン名リスト以外のアドレス）は検査対象とせずそのまま中継。
初期値 : TRUE

IgnoreErrorMail : TRUE/FALSE

エンベロープ FROM が空 (MAIL FROM: <>) のメールは検査対象とせずそのまま中継。
初期値 : TRUE

ExcludeGroup : 文字列

検査・配送ルールの適用対象外 (検査せずに中継) にしたいグループを指定する。「:」で区切り複数指定可能。

メールがグループに属するかどうかの判定条件の調整は、以下の **FromFilter**、**RcptFilter**、**FromFilterSelect**、**RcptFilterSelect** を使用する。

初期値 : 未指定

※グループの定義内容を変更した場合は、**GUARDIANWALL** の再起動が必要です。

FromFilter : TRUE/FALSE

差出人アドレスがグループに属するメールを検査・配送ルールの適用対象外にする。

初期値 : TRUE

RcptFilter : TRUE/FALSE

宛先アドレスの 1 つがグループに属するメールを検査・配送ルールの適用対象外にする。

初期値 : FALSE

FromFilterSelect : header/envelope/both

差出人アドレスとして何を調べるかを指定する。

header : ヘッダーの FROM アドレス

envelope : エンベロープの FROM アドレス

both : ヘッダーとエンベロープのいずれかに含む

初期値 : header

RcptFilterSelect : header/envelope/both

宛先アドレスとして何を調べるかを指定する。

header : ヘッダーの TO と CC に含まれるアドレス

envelope : エンベロープの RCPT アドレス

both : ヘッダーとエンベロープのいずれかに含む

初期値 : both

ExcludeFROM : header/envelope/both

検査・配送ルールの宛先条件指定に、発信者アドレスを除外する P_CC などを使用した場合、除外すべき発信者アドレスとして何を使用するか指定する。

header : 指定宛先からヘッダーの FROM アドレス（がもし含まれていれば）を除外する

envelope : エンベロープの FROM アドレス

both : ヘッダーとエンベロープの両方

初期値 : header

※判定において除外するだけでヘッダー等のアドレス記述を削除するものではありません。発信者アドレスを除外して宛先アドレスを検査するルールの記述については、「5-3 検査・配送ルール設定ファイル」（100 ページ）をご参照ください。

GroupMaxAddresses : 整数

検査配送ルールやユーザー個別定義ファイルの管理対象グループ等 1 つのグループ設定箇所において、1 つもしくは複数のグループ指定から読み込むアドレス定義の最大数。1 つのグループ定義箇所においてこの制限値を超えたアドレス定義は無視します。

初期値 : 8000

※管理サーバーの設定ファイル（/opt/Guardian/Admin/etc/admin/admin.conf）と同じ値にする必要があります。

[NoticeMessage] セクション

Signature : 文字列

通知メールの差出人名。

初期値 : “GUARDIANWALL”

※日本語（2 バイトコード）設定不可。

※空白を含む場合は、全体を “” で囲む必要があります。

MailAddress : メールアドレス

通知メッセージの発信者アドレス（ヘッダー From:）指定。

初期値 : root@ サーバーホスト名

※ MSP の設定によっては、書き換えられる可能性があります。

Reply-To : メールアドレス

通知メッセージの代替返信アドレス指定。

初期値 : 設定無し

NotifySender : TRUE/FALSE

差出人への通知機能を使用する。

初期値 : TRUE

※「FALSE」指定時は、他の設定に関係なく差出人へは通知を送信しない。

NotifyAdmin : TRUE/FALSE

管理者への通知機能を使用する。

初期値 : TRUE

※「FALSE」指定時は、他の設定に関係なく管理者へは通知を送信しない。

NotifyRecipients : TRUE/FALSE

受信者への通知機能を使用する。

初期値 : FALSE

※「FALSE」指定時は、他の設定に関係なく受信者へは通知を送信しない。

NotifyHeaderToSender : TRUE/FALSE

保留／削除時の差出人への通知メールに保留／削除対象メールのヘッダー情報サマリを表示する。

初期値 : TRUE

NotifyReasonToSender : TRUE/FALSE

保留／削除時の差出人への通知メールに保留／削除理由を表示する。

初期値 : FALSE

NotifyRcptToSender : TRUE/FALSE

保留／削除時の差出人への通知メールに保留／削除した宛先を表示する。

初期値 : TRUE

NotifyHeaderToAdmin : TRUE/FALSE

保留／削除時の管理者への通知メールに保留／削除対象メールのヘッダー情報サマリを表示する。

初期値 : TRUE

NotifyReasonToAdmin : TRUE/FALSE

保留／削除時の管理者への通知メールに保留／削除理由を表示する。

初期値 : TRUE

NotifyRcptToAdmin : TRUE/FALSE

保留／削除時の管理者への通知メールに保留／削除した宛先を表示する。

初期値 : TRUE

NotifyHeaderToRecipients : TRUE/FALSE

保留／削除時の受信者への通知メールに保留／削除対象メールのヘッダー情報サマリを表示する。

初期値 : TRUE

NotifyReasonToRecipients : TRUE/FALSE

保留／削除時の受信者への通知メールに保留／削除理由を表示する。

初期値 : FALSE

NotifyRcptToRecipients : TRUE/FALSE

保留／削除時の受信者への通知メールに保留／削除した宛先を表示する。

初期値 : FALSE

MaxNotifyRecipients : 整数 (0 ~ 9999)

受信者に通知メールを送る時の最大送信数。1つのメールで同時に複数の受信者への通知が発生した時にこの指定値を超えて受信者に通知メールを送ることを防ぐ。

初期値 : 10 (「0」を指定時は全ての受信者に通知)

MimeFormatForward : TRUE/FALSE

メールの転送、並びに通知文に元メールを添付する際に、MIME カプセル化 (MIME マルチパートの message/rfc822 パート) して送る。

初期値 : TRUE

※一部古いメーラーでは、message/rfc822 パートを読めないものがあります。

ForwardEnvelopeInfo : TRUE/FALSE

転送メールに元メールのエンベロープ情報を表示する。

初期値 : FALSE

ForwardHeaderInfo : TRUE/FALSE

転送メールに元メールのヘッダー情報のサマリを表示する。

初期値 : FALSE

ForwardReason : TRUE/FALSE

転送メールに保留理由を表示する。動作定義の転送オプションの場合はルール適用の結果、保留もしくは削除の場合に限りその情報を表示する。

初期値 : FALSE

NotifySender_Approve : yes/no/cont/nega

差出人に対する保留後送出通知の送信条件を指定する。

- yes : 保留時の通知有無に関係なく、送出通知を送信する
- no : 保留時の通知有無に関係なく、送出通知を送信しない
- cont : 保留時に通知した場合だけ、送出通知を送信する
- nega : 保留時に通知していない場合だけ、送出通知を送信する

初期値 : cont

NotifyAdmin_Approve : yes/no/cont/nega

管理者に対する保留後送出通知の送信条件を指定する。

- yes : 保留時の通知有無に関係なく、送出通知を送信する
- no : 保留時の通知有無に関係なく、送出通知を送信しない
- cont : 保留時に通知した場合だけ、送出通知を送信する
- nega : 保留時に通知していない場合だけ、送出通知を送信する

初期値 : cont

※「nega」を指定すると、保留時に、管理者には通知せず代替管理者に保留通知を送信した場合、保留後送出時に代替管理者に通知を送信しませんが、管理者には通知を送信します。

NotifyRecipients_Approve : yes/no/cont

受信者に対する保留後送出通知の送信条件を指定する。

- yes : 保留時の通知有無に関係なく、送出通知を送信する
- no : 保留時の通知有無に関係なく、送出通知を送信しない
- cont : 保留時に通知した場合だけ、送出通知を送信する

初期値 : no

NotifySender_Cancel : yes/no/cont/nega

差出人に対する保留後削除通知の送信条件を指定する。

- yes : 保留時の通知有無に関係なく、削除通知を送信する
- no : 保留時の通知有無に関係なく、削除通知を送信しない
- cont : 保留時に通知した場合だけ、削除通知を送信する
- nega : 保留時に通知していない場合だけ、削除通知を送信する

初期値 : cont

NotifyAdmin_Cancel : yes/no/cont/nega

管理者に対する保留後削除通知の送信条件を指定する。

- yes** : 保留時の通知有無に関係なく、削除通知を送信する
- no** : 保留時の通知有無に関係なく、削除通知を送信しない
- cont** : 保留時に通知した場合だけ、削除通知を送信する
- nega** : 保留時に通知していない場合だけ、削除通知を送信する

初期値 : cont

※「nega」を指定すると、保留時に、管理者には通知せず代替管理者に保留通知を送信した場合、保留後削除時に代替管理者に通知を送信しませんが、管理者には通知を送信します。

NotifyRecipients_Cancel : yes/no/cont

受信者に対する保留後削除通知の送信条件を指定する。

- yes** : 保留時の通知有無に関係なく、削除通知を送信する
- no** : 保留時の通知有無に関係なく、削除通知を送信しない
- cont** : 保留時に通知した場合だけ、削除通知を送信する

初期値 : no

NotifySender_Delay : yes/no/cont/nega

差出人に対する自動送出通知の送信条件を指定する。

- yes** : 一時保留時の通知有無に関係なく、自動送出通知を送信する
- no** : 一時保留時の通知有無に関係なく、自動送出通知を送信しない
- cont** : 一時保留時に通知した場合だけ、自動送出通知を送信する
- nega** : 一時保留時に通知していない場合だけ、自動送出通知を送信する

初期値 : no

NotifyAdmin_Delay : yes/no/cont/nega

管理者に対する自動送出通知の送信条件を指定する。

- yes** : 一時保留時の通知有無に関係なく、自動送出通知を送信する
- no** : 一時保留時の通知有無に関係なく、自動送出通知を送信しない
- cont** : 一時保留時に通知した場合だけ、自動送出通知を送信する
- nega** : 一時保留時に通知していない場合だけ、自動送出通知を送信する

初期値 : no

※「nega」を指定すると、保留時に、管理者には通知せず代替管理者に保留通知を送信した場合、代替管理者に再通知を送信しませんが、管理者には再通知を送信します。

NotifyRecipients_Delay : yes/no/cont

受信者に対する自動送出通知の送信条件を指定する。

- yes** : 一時保留時の通知有無に関係なく、自動送出通知を送信する
- no** : 一時保留時の通知有無に関係なく、自動送出通知を送信しない
- cont** : 一時保留時に通知した場合だけ、自動送出通知を送信する

初期値 : no

NotifySender_Again : yes/no/cont/nega

差出人に対する保留再通知の送信条件を指定する。

- yes** : 保留時の通知有無に関係なく、保留再通知を送信する
- no** : 保留時の通知有無に関係なく、保留再通知を送信しない
- cont** : 保留時に通知した場合だけ、保留再通知を送信する
- nega** : 保留時に通知していない場合だけ、保留再通知を送信する

初期値 : cont

NotifyAdmin_Again : yes/no/cont/nega

管理者に対する保留再通知の送信条件を指定する。

- yes** : 保留時の通知有無に関係なく、保留再通知を送信する
- no** : 保留時の通知有無に関係なく、保留再通知を送信しない
- cont** : 保留時に通知した場合だけ、保留再通知を送信する
- nega** : 保留時に通知していない場合だけ、保留再通知を送信する

初期値 : cont

※「nega」を指定すると、保留時に、管理者には通知せず代替管理者に保留通知を送信した場合、代替管理者に再通知を送信しませんが、管理者には再通知を送信します。

NotifyRecipients_Again : yes/no/cont

受信者に対する保留再通知の送信条件を指定する。

- yes** : 保留時の通知有無に関係なく、保留再通知を送信する
- no** : 保留時の通知有無に関係なく、保留再通知を送信しない
- cont** : 保留時に通知した場合だけ、保留再通知を送信する

初期値 : no

CheckSender : header/envelope

差出人に対する通知メールの宛先アドレスを指定する。

- header** : 宛先アドレスをヘッダーの FROM アドレスにする。
- envelope** : 宛先アドレスをエンベロープの FROM アドレスにする。

初期値 : header

[Admin] セクション

AdminMailAddress : 管理者メールアドレス

管理者宛通知メールの送信先メールアドレス。

初期値 : root

HoldList : TRUE/FALSE

情報管理者の保留メール処理方式で一覧処理方式を利用する。

TRUE : 一覧処理方式、FALSE : 個別処理方式

初期値 : TRUE

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) と同じ値にする必要があります。

HoldMessage : TRUE/FALSE

情報管理者の保留メール処理でメール本文閲覧を許可する。

TRUE : 閲覧許可、FALSE : 閲覧不可

初期値 : FALSE

HoldReason : TRUE/FALSE

情報管理者の保留メール処理で保留理由閲覧を許可する。

TRUE : 閲覧許可、FALSE : 閲覧不可

初期値 : TRUE

HoldForward : TRUE/FALSE

情報管理者の保留メール処理で転送処理を許可する。

TRUE : 転送操作許可、FALSE : 転送操作不可

初期値 : TRUE

HoldApprove : TRUE/FALSE

情報管理者の保留メール処理で送出処理を許可する。

TRUE : 操作許可、FALSE : 操作不可

初期値 : TRUE

HoldCancel : TRUE/FALSE

情報管理者の保留メール処理で削除処理を許可する。

TRUE : 操作許可、FALSE : 操作不可

初期値 : TRUE

[Manager] セクション**HoldList** : TRUE/FALSE

部門情報管理者の保留メール処理方式で一覧処理方式を利用する。

TRUE : 一覧処理方式、FALSE : 個別処理方式

初期値 : FALSE

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) と同じ値にする必要があります。

HoldMessage : TRUE/FALSE

部門情報管理者の保留メール処理でメール本文閲覧を許可する。

TRUE : 閲覧許可、FALSE : 閲覧不可

初期値 : TRUE

HoldReason : TRUE/FALSE

部門情報管理者の保留メール処理で保留理由閲覧を許可する。

TRUE : 閲覧許可、FALSE : 閲覧不可

初期値 : TRUE

HoldForward : TRUE/FALSE

部門情報管理者の保留メール処理で転送処理を許可する。

TRUE : 転送操作許可、FALSE : 転送操作不可

初期値 : TRUE

HoldApprove : TRUE/FALSE

部門情報管理者の保留メール処理で送出処理を許可する。

TRUE : 操作許可、FALSE : 操作不可

初期値 : TRUE

HoldCancel : TRUE/FALSE

部門情報管理者の保留メール処理で削除処理を許可する。

TRUE : 操作許可、FALSE : 操作不可

初期値 : TRUE

Group : グループ名 [: グループ名 ...]

グループ管理機能を利用する場合に管理対象とするグループ名を指定する。

「:」で区切り複数指定可能。指定が無い場合は全てのメールが管理対象になる。

初期値 : 未指定

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) と同じ値にする必要があります。

QueueGrouping : TRUE/FALSE

保留メール管理でグループ管理機能を使用する。

初期値 : TRUE

※「FALSE」指定時はグループ管理を行わず、全てのメールが管理対象になる。

FromFilter : TRUE/FALSE

差出人アドレスがグループに属するメールを管理対象にする。

初期値 : TRUE

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) と同じ値にする必要があります。

RcptFilter : TRUE/FALSE

宛先アドレスの1つがグループに属するメールを管理対象にする。

初期値 : FALSE

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) と同じ値にする必要があります。

FromFilterSelect_Queue : header/envelope/both

グループ管理機能利用時に、保留メール管理で選択表示するメールの差出人アドレスとして何を調べるかを指定する。

header : ヘッダーの FROM アドレス

envelope : エンベロープの FROM アドレス

both : ヘッダーとエンベロープのいずれかに含む

初期値 : header

RcptFilterSelect_Queue : header/envelope/both

グループ管理機能利用時に、保留メール管理で選択表示するメールの宛先アドレスとして何を調べるかを指定する。

header : ヘッダーの TO と CC に含まれるアドレス

envelope : エンベロープの RCPT アドレス

both : ヘッダーとエンベロープのいずれかに含む

初期値 : envelope

ExcludeGroup : グループ名 [: グループ名 ...]

グループ管理機能を利用する場合に優先除外対象とするグループ名を指定する。

「:」で区切り複数指定可能。指定が無い場合は除外を行わない。

初期値 : 未指定

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) と同じ値にする必要があります。

[Directories] セクション**LogDirectory** : パス名

ログファイル格納ディレクトリ。

初期値 : /opt/Guardian/WALL/logs

MessageQueue : パス名

メッセージ処理一時キューディレクトリ。

初期値 : /opt/Guardian/WALL/mqueue

QuarantineQueue : パス名

保留メッセージ保管ディレクトリ。

初期値 : /opt/Guardian/WALL/pqueue

※ MessageQueue と同一パーティションのディレクトリに指定すること。この値を変更した場合は、保留メールのソートに使用するファイルを再作成するコマンド (/opt/Guardian/WALL/bin/mw_qmgr -c) を実行する必要があります。

ArchiveQueue : パス名

メール保存処理用一時キューディレクトリ。

初期値 : /opt/Guardian/WALL/queue

※ MessageQueue と同一パーティションのディレクトリに指定すること。ディレクトリ指定が無い場合は、動作で保存オプションを指定してもメール保存を行いません。

[Archive] セクション**ArchiveMode** : none/all/out/in/rule

保存するメールの対象を指定する。

none : 保存しない

all : 全メール保存

out : 外部へ送信するメールのみ保存

in : 外部から受信したメールのみ保存

rule : 検査・配送ルールで指定したメールのみ保存

初期値 : none

ArchiveDirectories : パス名 [: パス名 ...]

メールを保存するディレクトリを指定する。「:」で区切り複数指定可能。

初期値 : 指定なし

NotifyDiskSwitch : TRUE/FALSE

メール保存ディレクトリの切り替え時に管理者宛に通知メールを送信する。

初期値 : FALSE

ArchiveInterval : 整数 (60 ~ 9999)

保存処理起動間隔 (秒数)。

初期値 : 60 秒

MaxMessageSize : サイズ表記 (単位省略時は KB)

保存処理を行うメールの最大制限サイズ。

指定サイズを超えるメールの保存処理は行いません。

初期値 : 50 MB

※サイズ表記については、**MaxMessageSize** (70 ページ) をご参照ください。

RefuseLoadAverage : 整数

ロードアベレージを指定します。

システムが指定値を超える負荷の場合、保存処理を一時中断します。

保存処理待ちメールのコピーはメール保存処理用一時キューディレクトリに保管され、システム負荷が下がった時に保存処理を再開します。

初期値 : 10

※ご注意

STORE サーバーがアーカイブ処理をするかどうかを決定する設定になります。

SMTP サーバーのメールの検査や配送には直接的には影響はありません。

ただし、本設定値を超える状況が長く続くような環境であれば、メール保存処理用一時キューの空き容量が不足するような状況になる可能性があります。同一パーティション上にメール配送用のメッセージ処理一時キューもある場合は、メール配送が行えなくなる場合もあります (接続元 MTA に一時エラーを応答する)。

また、メール保存処理用一時キューのデフォルトの保存期間が 10 日のため、本設定値を超える状況が 10 日を越えると保存処理待ちメールのコピーが削除され、そのメールは保存処理が行われなくなります。このような環境では一時的な対処として、メール保存処理用一時キューの保存期間を変更してください。

メール保存処理用一時キューの保存期間については、**[Expire]** セクションの **ArchiveQueue** (83 ページ) をご参照ください。

QueueLimitSize : サイズ表記 (単位省略時は MB)

メール保存処理用一時キューの使用制限サイズ。

保存処理待ちのメールのコピーは、指定されたサイズを超えない範囲で、同キューに一時保存される。指定制限値を越えている場合は、新たにキューにデータを保存しません。そのコピーされなかったメールに関してはアーカイブに保存処理が行われません。

初期値 : 0 (「0」指定時は無制限)

※サイズ表記については、**MaxMessageSize** (70 ページ) をご参照ください。

[Screening] セクション**MaxMimeNesting** : 整数 (0, 1 ~ 999)

MIME パートのネスティングの最大数。これを超えてネストされた MIME メッセージはデコード失敗とする。

初期値 : 16 (「0」指定時は無制限)

CaseSensitive : TRUE/FALSE

キーワード検査処理時、英大文字、小文字を区別する。

初期値 : FALSE

※この値を変更した場合はキーワードを再登録する必要があります。

IgnoreScreeningFail : TRUE/FALSE

検査動作でキーワード検査処理失敗時、無視してメッセージを中継する。

初期値 : TRUE

※「FALSE」指定時は不正フォーマットを理由に検査結果 NG となります。

IgnorePasswordLock : TRUE/FALSE

検査動作でアプリケーションデータがパスワードロックされている時無視する。

初期値 : TRUE

※「FALSE」指定時は、キーワード検査実行時にパスワードロックを理由に検査 NG となります。

※ Word、Excel、PowerPoint、PDF、一太郎の読取りパスワード

※ ZIP 圧縮ファイルのパスワードについては、IgnoreExtractPasswordLock (88 ページ) をご参照ください。

LookAheadNextLine : TRUE/FALSE

キーワード検査処理時、次行にまたがるキーワードも検出する。

初期値 : TRUE

MIMELogLevel : none/weak/strong もしくは整数 (0 ~ 9)

MIME タイプ検査で情報検査ログに記録する条件の状態を指定する。

none : 指定条件を満たしても、ログに記録しません

weak : 「本番」条件を満たすメールだけ記録します

strong : 「試行」と「本番」条件を満たすメールを記録します

条件指定モードが「10 段階」の場合は、数値 (0-9)、もしくは「none」の値を使用します (「weak」は「1」、「strong」は「0」と同等)。

初期値 : none

KEYWORDLogLevel : none/weak/strong もしくは整数 (0 ~ 9)

キーワード検索で情報検査ログに記録する条件の状態を指定する。

none : 指定条件を満たしても、ログに記録しません

weak : 「本番」条件を満たすメールだけ記録します

strong : 「試行」と「本番」条件を満たすメールを記録します

条件指定モードが「10 段階」の場合は、数値 (0-9)、もしくは「none」の値を使用します (「weak」は「1」、「strong」は「0」と同等)。

初期値 : none

DPINFOLogLevel : none もしくは整数 (0 ~ 100,999)

個人情報検査で情報検査ログに記録する総合指数値の条件を指定する。

none, 9999 : ログに記録しません。

0 ~ 100 : 総合指数値が指定した値以上の場合記録します。

初期値 : none

ExtractArchive : TRUE/FALSE

圧縮ファイルを展開する。

初期値 : FALSE

※「TRUE」指定時は圧縮ファイルの展開を行う。

ExtractArchive_Full : TRUE/FALSE

拡張展開機能を有効にする。

ZIP, LHA, RAR, CAB, GZIP, BZIP2, Z, TAR 形式に加え、7ZIP, ARJ, RPM, DEB, ISO, MSI, HQX, AppleSingle, TNEF, SZDD, PACK の展開を行う。

初期値 : FALSE

※管理サーバーの設定ファイル (/opt/Guardian/Admin/etc/admin/admin.conf) にも同じ設定をする必要があります。

ExtractArchive_SFX : TRUE/FALSE

DOS/Windows 実行形式による自己展開ファイル (SFX 形式圧縮ファイル) を展開する。

初期値 : FALSE

※ ZIP, LHA, RAR, CAB の SFX 形式のみ展開する。

MaxExtractNesting : 整数 (0, 1 ~ 999)

多重圧縮ファイルの最大展開数。この値を超えて多重に圧縮されたファイルの展開は、本指定回数以上の展開を行わない。

初期値 : 9 (「0」指定時は無制限に展開)

※本設定値を超えた場合、デフォルトでは検査結果は OK となります。設定変更については、IgnoreExtractMax (88 ページ) をご参照ください。

MaxExtractSize : サイズ表記（単位省略時は KB）

展開処理を行う圧縮ファイルの最大制限サイズ。

指定サイズを超える圧縮ファイルの展開処理は行いません。

初期値：10 MB

※サイズ表記については、MaxMessageSize（70 ページ）をご参照ください。

MaxExtractFileSize : サイズ表記（単位省略時は KB）

展開ファイルの最大制限サイズ。

圧縮ファイルの展開時に指定サイズを超えるファイルを展開しようとした場合に展開処理を中止し、展開処理を行いません。

初期値：100 MB

※サイズ表記については、MaxMessageSize（70 ページ）をご参照ください。

AppGetText : TRUE/FALSE

添付ファイルのアプリケーションデータのテキストを抽出し検査する。

初期値：TRUE

※「FALSE」指定時はテキスト抽出、検査を行いません。

※ Word、Excel、PowerPoint、PDF、一太郎のみ。

※「FALSE」指定時は、上記アプリケーションファイルの、パスワードロックの有無の判別も行えなくなります。

AppGetTextRefuseLA : 整数

平均負荷（ロードアベレージ）が指定値を超えている場合は、添付ファイルのアプリケーションデータからテキストデータを抽出しない。

初期値：0（「0」指定時は無制限）

※「0」指定時は、平均負荷の値に関わらずテキスト抽出を行います。

AppGetTextMaxRun : 整数

同時コネクション数が指定値を超えている場合は、添付ファイルのアプリケーションデータからテキストデータを抽出しない。

初期値：0（「0」指定時は無制限）

※「0」指定時は、同時コネクション数に関わらずテキスト抽出を行います。

AppGetProperty : TRUE/FALSE

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：FALSE

Property_keyword : 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指定文字列を挿入する。

初期値：未指定（挿入文字列無し）

IDRangeCheck : TRUE/FALSE

MIME タイプ検査条件、キーワード検査条件の ID 値による条件の分割機能を使用する。

初期値 : FALSE

SubjectScreening : TRUE/FALSE

メール標題だけを単独パートとして取り出しキーワード検査対象にする。

初期値 : FALSE

※本オプションが「FALSE」でも通常、標題部分はヘッダーと共に検査対象になっています。

FileNameScreening : TRUE/FALSE

添付ファイル名部分を単独パートとして取り出しキーワード検査対象にする。

初期値 : TRUE

※本オプションが「FALSE」にすると、添付ファイル名部分は検査対象になりません。

SubjectSignature : 文字列

メール標題を単独パートとしてキーワード検査する場合に指定文字列を挿入して検査する。

初期値 : 未指定 (挿入文字列無し)

FileNameSignature : 文字列

添付ファイル名部分をキーワード検査する場合に指定文字列を挿入して検査する。

初期値 : 未指定 (挿入文字列無し)

IgnoreExtractMax : TRUE/FALSE

多重圧縮ファイルの最大展開数 (**MaxExtractNesting** オプション) で指定された値を超えて多重に圧縮されたファイルの検査結果を OK とする。「FALSE」指定時は検査結果 NG とする。

初期値 : TRUE

※ ZIP ファイルを作成したソフトによっては、展開できない場合があります。

IgnoreExtractPasswordLock : TRUE/FALSE

ZIP 形式圧縮ファイルがパスワードロックされている時、該当 ZIP ファイルの検査結果を OK とする。「FALSE」指定時はパスワードロックを理由に検査 NG とする。

初期値 : TRUE

※ ZIP ファイルを作成したソフトによっては、パスワードロック状態を検出できない場合があります。

※ Word、Excel、PowerPoint、PDF、一太郎の読取りパスワードについては、**IgnorePasswordLock** (85 ページ) をご参照ください。

DPIInfo_BufSize : サイズ表記（単位省略時は MB）

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。

初期値：100 MB

DPIInfo_IdxOverflow : 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

ResultFormat : 整数（16 進表記）

保留通知メールや保留メール詳細画面に記載される保留理由の内容を設定する。

0xPPAAMMKK（P, A, M, K は 0 ～ 7 の整数）の形式で設定し、各桁によって設定対象が異なる。

複数の設定を行う場合は、OR 演算で必要な値を組み合わせる。

初期値：0x00000000

※個人情報検査結果に関する記載内容を設定する場合は、PP（上位 1,2 桁）へ以下を設定する。

00：初期値。検出されたファイルのファイル名、MIME タイプ、総合指数を記載する。

01：総合指数を記載しない。

04：検出されたファイルが圧縮ファイルに含まれていた場合、その圧縮ファイル名を記載する。

10：検出されたファイルのファイル名と MIME タイプを記載しない。

※適用されたルールに関する記載内容を設定する場合は、AA（上位 3,4 桁）へ以下を設定する。

00：初期値。保留動作が適用された場合のみルールを記載する。

01：検査動作が適用された後に保留された場合でもルールを記載する。

02：適用されたルールの説明を記載する。

10：適用されたルールの ID のみを記載する。

※MIME タイプ検査結果に関する記載内容を設定する場合は、MM（上位 5,6 桁）へ以下を設定する。

00：初期値。検出されたファイルのファイル名と MIME タイプを記載する。

01：マッチした MIME タイプが含まれる条件セット名を記載する。

02：マッチした MIME タイプの ID を記載する。

04：マッチした MIME タイプが含まれる条件セットのコメントを記載する。

10：検出されたファイルのファイル名と MIME タイプを記載しない。

40：検出されたファイルが圧縮ファイルに含まれていた場合、その圧縮ファイル名を記載する。

※キーワード検索結果に関する記載内容を設定する場合は、KK（上位7,8桁）へ以下を設定する。

- 00：初期値。キーワードが検出されたパート、マッチしたキーワードを記載する。
- 01：マッチしたキーワードが含まれる条件セット名を記載する。
- 02：マッチしたキーワードのIDを記載する。
- 04：マッチしたキーワードが含まれる条件セットのコメントを記載する。
- 10：マッチしたキーワードを記載しない。
- 20：キーワードがマッチした回数を記載する。
- 40：検出されたファイルが圧縮ファイルに含まれていた場合、その圧縮ファイル名を記載する。

DMC.Timeout : 整数（10 ～ 9999）

添付ファイル1個あたりのテキスト抽出処理のタイムアウト値（秒数）。

初期値：120 秒

Screening.Timeout : 整数（30 ～ 9999）

メール1通あたりの検査処理のタイムアウト値（秒数）。

初期値：480 秒

HoldAddressCheck : TRUE/FALSE

保留メール詳細画面で、宛先チェック機能を使用する。

初期値：FALSE

HoldAttachCheck : TRUE/FALSE

保留メール詳細画面で、添付ファイルチェック機能を使用する。

初期値：FALSE

DelayAddressCheck : TRUE/FALSE

一時保留メール詳細画面で、宛先チェック機能を使用する。

初期値：FALSE

DelayAttachCheck : TRUE/FALSE

一時保留メール詳細画面で、添付ファイルチェック機能を使用する。

初期値：FALSE

[Expire] セクション

SweepInterval : 秒数（0, 600 ～ 86400（24 時間））

各種不要ファイル、古いログ、古い保留メッセージを処理する間隔。

初期値：3600（「0」指定時は処理しない）

HoldMessages : 日数 (0 ~ 9999)

保留メッセージの最大保存期間。

初期値 : 30 日 (「0」指定時は無制限)

※制限期間を超えた保留メッセージは削除されます (削除通知はありません)。

ArchiveQueue : 日数 (0 ~ 9999)

メール保存処理用一時キューの最大保存期間。

初期値 : 10 日 (「0」指定時は無制限)

※制限期間を超えた保存処理待ちメールのコピーは削除されます。

DeliverLog : 日数 (0 ~ 9999)

配送ログの最大保存期間。

初期値 : 180 日 (「0」指定時は無制限)

※制限期間を超えたログファイルは削除されます。

ScreeningLog : 日数 (0 ~ 9999)

情報検査ログの最大保存期間。

初期値 : 180 日 (「0」指定時は無制限)

※制限期間を超えたログファイルは削除されます。

ArchiveLog : 日数 (0 ~ 9999)

保存メールログの最大保存期間。

初期値 : 180 日 (「0」指定時は無制限)

※制限期間を超えたログファイルは削除されます。

ViewerLog : 日数 (0 ~ 9999)

保存メール閲覧ログの最大保存期間。

初期値 : 180 日 (「0」指定時は無制限)

※制限期間を超えたログファイルは削除されます。

ManagerLog : 日数 (0 ~ 9999)

保留メール操作ログの最大保存期間。

初期値 : 180 日 (「0」指定時は無制限)

※制限期間を超えたログファイルは削除されます。

SystemLog : 日数 (0 ~ 9999)

システムログの最大保存期間。

初期値 : 7 日 (「0」指定時は無制限)

※制限期間を超えたログファイルは削除されます。

MaxDeliverLogSize : サイズ表記（単位省略時は MB）（*1）
配送ログの最大保存容量。
初期値：0（「0」指定時は容量制限無し）
※ログ容量が指定制限サイズを超えた場合、古いログファイルから削除されます。

MaxScreeningLogSize : サイズ表記（単位省略時は MB）（*1）
情報検査ログの最大保存容量。
初期値：0（「0」指定時は容量制限無し）
※ログ容量が指定制限サイズを超えた場合、古いログファイルから削除されます。

MaxArchiveLogSize : サイズ表記（単位省略時は MB）（*1）
保存メールログの最大保存容量。
初期値：0（「0」指定時は容量制限無し）
※ログ容量が指定制限サイズを超えた場合、古いログファイルから削除されます。

MaxManagerLogSize : サイズ表記（単位省略時は MB）（*1）
保留メール操作ログの最大保存容量。
初期値：0（「0」指定時は容量制限無し）
※ログ容量が指定制限サイズを超えた場合、古いログファイルから削除されます。

MaxViewerLogSize : サイズ表記（単位省略時は MB）（*1）
保存メール閲覧ログの最大保存容量。
初期値：0（「0」指定時は容量制限無し）
※ログ容量が指定制限サイズを超えた場合、古いログファイルから削除されます。
（*1）サイズ表記については、**MaxMessageSize**（70 ページ）をご参照ください。

DelayMessages : 分数（5 ～ 9999）
一時保留メッセージの保留期間。
初期値：60

DelaySendInterval : 秒数（60 ～ 3600）
一時保留メッセージを自動送出するプロセスの起動間隔。
自動送出プロセスはここで設定された間隔で起動され、保留期間を過ぎた一時保留メッセージを順番に送出していきます。
初期値：60

DelaySendMaxProcess : 整数（1 ～ 99）
一時保留メッセージの自動送出プロセスが同時に起動できる最大プロセス数。
初期値：30

DelaySendTimeout : 秒数 (0 ~ 3600)

一時保留メッセージ自動送出プロセスのタイムアウト値。

メッセージ送出中にタイムアウトが発生した場合はメッセージ送出後にプロセスが終了します。

初期値 : 60

※「0」を設定した場合は、無制限となります。

DelaySendRefuseLoadAverage : 整数 (0 ~ 99)

ロードアベレージを指定します。

システムが指定値を超える負荷の場合、一時保留メッセージの自動送出処理を一時中断します。保留期間が過ぎたメッセージについては、システム負荷が下がった時に送出されます。

初期値 : 10

DelaySendSleep : 整数 (1 ~ 100)

自動送出を行うメッセージ数を指定します。

一時保留メッセージの自動送出プロセスは、システム負荷を軽減するため、複数サイクルに分けて送出処理を行います。ここでは、1 サイクルで処理するメッセージ数を指定します。

初期値 : 10

DelaySendMaxMessages : 整数 (1 ~ 1000)

一時保留メッセージの自動送出プロセスが処理する最大メッセージ数を設定します。

初期値 : 300

ReNotifyHoldMessages : 分数 (0 あるいは 30 ~ 14398560)

未処理の保留メッセージに対して再通知を行う間隔。

初期値 : 0 (「0」指定時は再通知を行わない)

ReNotifyInterval : 秒数 (60 ~ 3600)

未処理の保留メッセージへの再通知処理プロセスの起動間隔。

初期値 : 60

ReNotifyRefuseLoadAverage : 整数 (0 ~ 99)

ロードアベレージを指定します。

システムが指定値を超える負荷の場合、未処理保留メッセージに対する再通知処理を一時中断します。再通知対象のメッセージについては、システム負荷が下がった時に再通知が行われます。

初期値 : 10

ReNotifySleep : 整数 (1 ~ 100)

再通知を行うメッセージ数を指定します。

未処理保留メッセージへの再通知処理プロセスは、システム負荷を軽減するため、複数サイクルに分けて再通知処理を行います。ここでは、1 サイクルで処理するメッセージ数を指定します。

初期値 : 10

ReNotifyMaxMessages : 整数 (1 ~ 1000)

未処理の保留メッセージへの再通知処理プロセスが処理する最大メッセージ数を設定します。

初期値 : 500

[Encrypt] セクション

Encryption : 整数 (0,1,2)

添付ファイル暗号化機能を設定する。

0 : 暗号化しない

1 : 全て暗号化

2 : 検査・配送ルールで指定されたメールのみ暗号化

初期値 : 0

EncryptType : AES/ZIP

暗号化方式を指定する。

AES : 暗号化 ZIP+ パスワード

ZIP : ZIP 圧縮 + パスワード

初期値 : ZIP

PasswdLength : 数値 (8 ~ 64)

暗号化する際に設定するパスワードの長さを指定する。

初期値 : 8

ExcludeEncryptGroup : 文字列

暗号化除外グループを指定する。

初期値 : 設定なし

PasswdSend : 整数 (0,1)

パスワード通知メールの送信先を指定する。

0 : 送信者

1 : 送信者、エンベロープ TO アドレス

初期値 : 0 (送信者へ通知)

NotifyMailMode : TRUE/FALSE

パスワード通知メールの通知文を指定する。

TRUE : 管理画面で登録した通知文を使用する。

FALSE : デフォルト通知文を使用する。

初期値 : FALSE

[Queue] セクション

DirectoryLimitSize : サイズ表記（単位省略時は MB）

保留メールキューの使用制限サイズ。メールの保留時は、指定されたサイズを超えない範囲で、保留メールキューにメールを保留させる。

初期値 : 0（「0」指定時は無制限）

※サイズ表記は、**MaxMessageSize**（70 ページ）をご参照ください。

ErrorAction : 整数

メールの保留時に保留メールキューに指定された使用制限サイズを超える、もしくは、保留メールキューに指定されたファイルシステムの容量が足りないため、メールを保留できない場合の動作を指定する。

0 : SMTP リザルトコードで一時エラーを送信元 MTA に返す

1 : 中継

2 : 削除

初期値 : 0

[Check_MAIL] セクション

LocalIP : IP アドレス

指定した IP アドレス（もしくはネットワーク部）からの接続を内部接続とみなし、接続を許可します。

初期値 : 設定なし

※ IP アドレスをネットワークアドレスとして指定する場合は、IP アドレスのオクテット境界まで指定してください。例えば「192.168.1.0」のホスト全て指定する場合は、「192.168.1.」まで指定してください。複数の IP アドレスを指定する場合は、「:」で区切ってください。

※ IP アドレスだけでなく、エンベロープ FROM アドレスと合わせて制限を行う場合は、後述の **ClientIP** と **ClientFROM** をご利用ください。

ClientIP : IP アドレス

指定した IP アドレス（もしくはネットワーク部）からの接続を内部接続とみなし、後述の **ClientFROM** のチェックを実施します。指定した IP アドレスからの接続でない場合は、内部接続とはみなされず、**ClientFROM** のチェックも行いません。

初期値 : 設定なし

※ IP アドレスをネットワークアドレスとして指定する場合は、IP アドレスのオクテット境界まで指定してください。例えば「192.168.1.0」のホスト全て指定する場合は、「192.168.1.」まで指定してください。複数の IP アドレスを指定する場合は、「:」で区切ってください。

ClientFROM : メールアドレス

指定したエンベロープ FROM アドレスからの接続を内部接続とみなし、接続を許可します。指定した FROM アドレスからの接続でない場合、接続を拒否します。この設定は前述の ClientIP が設定されており、かつ ClientIP で指定した IP アドレスからの接続であった場合にのみ有効です。

初期値 : 設定なし

※アドレス部に「*」（ワイルドカード）を指定することができます。また、複数アドレスを指定する場合は「:」で区切ってください。

DenyIP : IP アドレス

指定した IP アドレス（もしくはネットワーク部）からの接続を拒否します。

初期値 : 設定なし

※ IP アドレスをネットワークアドレスとして指定する場合は、IP アドレスのオクテット境界まで指定してください。例えば「192.168.1.0」のホスト全て指定する場合は、「192.168.1.」まで指定してください。複数の IP アドレスを指定する場合は、「:」で区切ってください。

AllowIP : IP アドレス

指定した IP アドレス（もしくはネットワーク部）以外からの接続を拒否します。

初期値 : 設定なし

※ IP アドレスをネットワークアドレスとして指定する場合は、IP アドレスのオクテット境界まで指定してください。例えば「192.168.1.0」のホスト全て指定する場合は、「192.168.1.」まで指定してください。複数の IP アドレスを指定する場合は、「:」で区切ってください。

DenyFromAddress : メールアドレス

指定したエンベロープ FROM アドレスからの接続を拒否します。

初期値 : 設定なし

※アドレス部に「*」（ワイルドカード）を指定することができます。また、複数アドレスを指定する場合は「:」で区切ってください。

OnlyLogging : TRUE/FALSE

[Check_MAIL] セクションでの設定により接続を拒否する場合、実際には接続を拒否せずログのみを採取します。

初期値 : FALSE

[Check_RCPT] セクション**RefuseRouteAddress** : TRUE/FALSE

エンベローブ TO アドレスがソースルーティングアドレスであった場合、接続を拒否します。

初期値 : FALSE

LocalDomain : ドメイン名

エンベローブ TO アドレスのドメインが指定されたドメイン名であった場合、接続を許可します。指定されたドメインでなかった場合、接続を拒否します。

初期値 : 設定なし

※内部ネットワーク側にあるメールサーバーで受理すべきアドレスのドメイン名を指定してください。

※複数のドメイン名を指定する場合は、「:」で区切ってください。

AllowRcptAddress : メールアドレス

エンベローブ TO アドレスが指定されたアドレスであった場合、接続を許可します。

初期値 : 設定なし

※内部ネットワーク側にあるメールサーバーで受信すべきメールアドレスを指定してください。

※アドレス部に「*」（ワイルドカード）を指定することができます。また、複数アドレスを指定する場合は「:」で区切ってください。

DenyRcptAddress : メールアドレス

エンベローブ TO アドレスが指定されたアドレスであった場合、接続を拒否します。

初期値 : 設定なし

※アドレス部に「*」（ワイルドカード）を指定することができます。また、複数アドレスを指定する場合は「:」で区切ってください。

AllowFromAddress : メールアドレス

エンベローブ FROM アドレスが指定されたアドレスであった場合、接続を許可する。

初期値 : 設定なし

※アドレス部に「*」（ワイルドカード）を指定することができます。また、複数アドレスを指定する場合は「:」で区切ってください。

OnlyLogging : TRUE/FALSE

[Check_RCPT] セクションでの設定により接続を拒否する場合、実際には接続を拒否せずログのみを採取します。

初期値 : FALSE

ReplyMessage : 文字列

接続を拒否する場合の接続元への応答コード、メッセージを設定します。

初期値 : 550 We do not relay

RefuseMultiRcptOnNullFrom : TRUE/FALSE

エンベロープ FROM アドレスが <> の時、エンベロープ TO アドレスの複数指定を拒否します。

初期値 : FALSE

QuickAbort : TRUE/FALSE

接続を拒否する場合、接続元への応答後、セッションを切断します。

初期値 : FALSE

[APT] セクション

DetectAptMail : TRUE/FALSE

標的型攻撃メール検知機能を有効にするかどうかを設定します。

TRUE : 有効

FALSE : 無効

初期値 : FALSE

NotifyAdmin : TRUE/FALSE

標的型攻撃メール検知時に管理者へ通知メールを送信するかどうかを設定します。

TRUE : 送信する

FALSE : 送信しない

初期値 : FALSE

NoticeMailAttach : TRUE/FALSE

管理者への通知メールに元メールを添付するかどうかを設定します。

元メールは message/rfc822 形式で添付されます。

TRUE : 添付する

FALSE : 添付しない

初期値 : FALSE

SubjectMessage : 文字列（最大 120 バイト）

標的型攻撃メールと判定されたメールの標題に付与される文字列を設定します。

EUC コードを URI エンコードした文字列を設定します。

初期値：%A1%DA%C9%B8%C5%AA%B7%BF%B9%B6%B7%E2%A5%E1%A1%BC%A5%EB%A4%CE%B6%B2%A4%EC%A4%A2%A4%EA%A1%DB（【標的型攻撃メールの恐れあり】）

PublicAddressGroup : 文字列（最大 640 バイト）

公開されたメーリングリストなど不特定多数に送信するために利用されるアドレスグループを設定します。

初期値：なし

※グループは「:」（コロン）区切りで複数指定ができます。

PublicAddressNum : 整数（0 ～ 100）

不特定多数の宛先へ送信された疑いありと判断するためのアドレス数を設定します。

PublicAddressGroup に含まれる BCC アドレスがここで設定された個数以上ある場合、不特定多数の宛先に送信された疑いありと判定します。

初期値：2

※設定値が「0」の場合、差出人詐称の疑いがあるメールは全て標的型攻撃メールと判断されます。

※ BCC アドレス、差出人詐称については、「5-10 標的型攻撃メール検知機能仕様」をご参照ください。

5-3 検査・配送ルール設定ファイル

検査・配送ルールは1行に、ルールID、条件、動作からなる1つのルールを記述します。先頭行から順に評価し、最初に3つの条件論理式を全て満たすルールが見つければ、そのルール行の動作が実行されます。

ファイルパス名

検査サーバー : /opt/Guardian/WALL/etc/mss.acl

管理サーバー : /opt/Guardian/Admin/etc/wall/mss.acl

書式

```
aclruleset  =      aclrule /  
                aclruleset aclrule  
aclrule      =      id “.” fromexp “.” rcptexp “.” sclexp “.” action LF
```

	<i>id</i>	: ルール ID 番号	
	<i>fromexp</i>	: 差出人アドレス条件論理式	
	<i>rcptexp</i>	: 宛先アドレス条件論理式	
	<i>sclexp</i>	: 数値条件論理式	
	<i>action</i>	: 動作	

(1) ルール ID 番号

id = 1*DIGIT;1 ~ 99999999、複数行で ID の重複はできません。

(2) 差出人アドレス条件論理式

```

fromexp    =    fromatom /
                fromexp "&" fromexp / ; 論理積
                fromexp "|" fromexp   ; 論理和
fromatom    =    fromselector f_operator pattern /
                "(" fromexp ")" /
                "!" fromatom          ; 否定
fromselector =    "FROM" / "EFROM" / "IPADDR"
f_operator   =    "=" / "!="
pattern      =    addrpattern /          ; アドレスパターン
                "{" groups "}"          ; グループ名 (単数または複数)
groups       =    groupname /           ; グループ名
                groups "+" groupname    ; グループ名 (複数)

```

```

┌ fromselector
├ FROM      : ヘッダー FROM
├ EFROM     : エンベロープ FROM
├ IPADDR    : 接続元 IP アドレスヘッダー
├ f_operator
├ =         : 左辺指定アドレスが右辺値にマッチする
├ !=        : 左辺アドレスが右辺値にマッチしない
├ ※右辺がグループの場合は、グループ定義のどれか 1 つにマッチすればグ
├ ループに属する (マッチする) とみなします。
└

```

例)

FROM = *@example.com

ヘッダー FROM アドレスが指定パターンに一致すれば真

EFROM != {GROUP}

エンベロープ FROM アドレスが指定グループに属しなければ真

FROM = *@example.com | FROM = *@example.co.jp

ヘッダー FROM アドレス「*@example.com」、または、「*@example.co.jp」に一致すれば真

IPADDR = 192.168.0.2

接続元 IP アドレスが指定値ならば真

```
EFROM = *@example.com & IPADDR != 10.90.*
```

エンベロープ FROM アドレスが「*@example.com」に一致し、かつ、接続元 IP アドレスが「10.90.*」に一致しなければ真

```
FROM = {group1+group2}
```

ヘッダー FROM アドレスが group1 と group2 のいずれかに属していれば真

アドレスパターンには長さ 0 以上の任意の文字列にマッチするワイルドカード文字「*」が使用できます。ワイルドカード文字は、アドレスパターン文字列中の任意の位置に任意個使用できます。



旧バージョン（Ver5.0 以前）との互換性のため下記表記法も使用できます。

FROMGROUP	= groupname	ヘッダー FROM
EFROMGROUP	= groupname	エンベロープ FROM
IPADDRGROUP	= groupname	IP アドレス

単にアドレスパターンを 1 つだけ記述した場合は、

```
FROM = addr
```

と同一とみなされます。

※論理式形式で条件を記述する場合は、「FROM =」を省略することはできません。



検査・配送ルール の条件に用いたグループは、サーバー起動時に定義内容を読み込みます。グループの定義内容を変更した場合は、システムの再起動を行ってください。



1 つの fromselector に指定したグループ数に関わらず、グループ定義のアドレスを合計して最大 8000 件まで判定します。「{grp3+grp2+grp1}」のように複数のグループを指定した場合は、グループ名のアルファベット辞書順（“grp1”，“grp2”，“grp3”，... の順）にグループ定義内容を読み込み、8000 件を超えたアドレス定義内容は無視します。必ず、合計 8000 件以内で定義してください。

(3) 宛先アドレス条件論理式

```

rcptexp      =      rcptatom /
                    rcptexp "&" rcptexp /      ; 論理積
                    rcptexp "|" rcptexp      ; 論理和
rcptatom     =      rcptselector r_operator pattern /
                    "(" rcptexp ")" /
                    "!" rcptatom      ; 否定
rcptselector =      "ERCPT" / "TO" / "CC" / "RCPT" /
                    "P_ERCPT" / "P_TO" / "P_CC" / "P_RCPT"
r_operator   =      "=" / "!=" / "==" / "!=="
pattern      =      addrpattern /      ; アドレスパターン
                    "{" groups "}"      ; グループ名（単数または複数）
groups       =      groupname /      ; グループ名
                    groups "+" groupname ; グループ名（複数）

```

```

| rcptselector
| ERCPT      : エンベロープ TO
| TO         : ヘッダー TO
| CC         : ヘッダー CC
| RCPT       : ヘッダー TO とヘッダー CC
| P_ERCPT    : エンベロープ TO 発信、ただし、発信者アドレスを除く
| P_TO       : ヘッダー TO、ただし、"
| P_CC       : ヘッダー CC、ただし、"
| P_RCPT     : ヘッダー TO とヘッダー CC、ただし、"
| ※発信者アドレス：デフォルトはヘッダー FROM に指定されているアドレ
|   スを指定宛先から（もし、含まれていれば）除外して判定します。判定
|   において除外するだけでヘッダー等のアドレス記述を削除するものでは
|   ありません。設定変更については、ExcludeFROM オプション（72 ページ）
|   をご参照ください。
| r_operator
| =          : 左辺指定アドレスの一部もしくは全部が右辺値にマッチ
|             する場合真
| !=         : 左辺指定アドレス全てが右辺値にマッチしない場合真
| ==         : 左辺指定アドレス全てが右辺値にマッチする場合真
| !=         : 左辺指定アドレスの一部もしくは全部が右辺値にマッチ
|             しない場合真
| ※右辺がグループの場合は、グループ定義のどれか 1 つにマッチすればグ
|   ループに属する（マッチする）とみなします。

```

例)

```
ERCPT = *@example.com
```

エンベロープ TO に「*@example.com」に一致するアドレスが1つでも含まれていれば真

```
T0 == *@example.com
```

ヘッダー TO に指定されているアドレスの全てが「*@example.com」に一致すれば真

```
ERCPT = {GROUP}
```

エンベロープ TO アドレス（の一部もしくは全部）がグループ GROUP に属すれば真

```
T0 = *@example.com | T0 = *@example.co.jp
```

ヘッダー TO アドレス（の一部もしくは全部）が「*@example.com」、または、「*@example.co.jp」に一致すれば真

```
P_CC = *@example.com
```

ヘッダー CC アドレスから発信者アドレスを除き（一部もしくは全部）が「*@example.com」に一致すれば真

```
T0 = *@example.com & CC != *@example.co.jp
```

ヘッダー TO アドレス（の一部もしくは全部）が「*@example.com」に一致し、ヘッダー CC に「*@example.co.jp」に一致するアドレスが1つも含まれていなければ真

```
CC == {group1+group2}
```

ヘッダー CC に指定されているそれぞれのアドレスが、グループ 1 またはグループ 2 のいずれかに属していれば真

アドレスパターンには長さ 0 以上の任意の文字列にマッチするワイルドカード文字「*」が使用できます。ワイルドカード文字は、アドレスパターン文字列中の任意の位置に任意個使用できます。



旧バージョン（Ver5.0 以前）との互換性のため下記表記法も使用できます。

ERCPTGROUP	=	groupname
TOGROUP	=	groupname
CCGROUP	=	groupname
RCPTGROUP	=	groupname

単にアドレスパターンを 1 つだけ記述した場合は、

ERCPT = addr

と同一とみなされます。

※論理式形式で条件を記述する場合は、「ERCPT =」を省略することはできません。



検査・配送ルールの条件に用いたグループは、サーバー起動時に定義内容を読み込みます。グループの定義内容を変更した場合は、システムの再起動を行ってください。



1 つのパラメータに指定したグループ数に関わらず、グループ定義のアドレスを合計して最大 8000 件まで判定します。「{grp3+grp2+grp1}」のように複数のグループを指定した場合は、グループ名のアルファベット辞書順（“grp1”，“grp2”，“grp3”，... の順）にグループ定義内容を読み込み、8000 件を超えたアドレス定義内容は無視します。必ず、合計 8000 件以内で定義してください。

(4) 数値条件論理式

sclexp	=	sclatom / sclexp "&" sclexp / ; 論理積 sclexp " " sclexp ; 論理和
sclatom	=	s_exp s_operator s_exp / "(" sclexp ")" / "!" sclatom ; 否定
s_operator	=	">" / ">=" / "<" / "<=" / "=" / "!="
s_exp	=	function / const / size / ; 関数、定数、サイズ定数 s_exp s_op s_exp / "(" s_exp ")"
s_op	=	"*" / "/" / "+" / "-" / "%" ; 四則演算（積、商、和、差、剰余）
function	=	funcname ["(" [parameters] ")"] ; 詳細は各関数参照
parameters	=	param / parameters "," param
const	=	1 * DIGIT ; 定数値
size	=	1 * (1 * DIGIT unit) ; 単位付きサイズ定数値
unit	=	"G" / "M" / "K" / "B" ; GB、MB、KB、バイト

s_operator	
>	: 左辺値が右辺値を超える場合真
>=	: 左辺値が右辺値以上の場合真
<	: 右辺値が左辺値を超える場合真
<=	: 右辺値が左辺値以上の場合真
=	: 左辺値と右辺値が等しい場合真
!=	: 右辺値と左辺値が等しくない場合真



数値式「s_exp」の評価時に、0 値による割り算（/, %）が発生した場合は、便宜的に該当式の値を 0 として扱います。

数値条件論理式は左から順に評価され、式が真または偽になった場合、そこから右方の評価は行いません。たとえば、

SIZE() > 2MB | ATTACHMENT() > 6

という式では、「SIZE() > 2MB」を先に評価し真になった場合、右の式を評価しなくても条件式全体が真になるため「ATTACHMENT() > 6」の評価を省略します。

同様に、

SIZE() > 2MB & ATTACHMENT() > 6

という式では、「SIZE() > 2MB」を評価し偽になった場合、右の式の評価を省略します。

SIZE 関数

メッセージのサイズ、添付ファイルのサイズを検査し、その値を関数値とします。

書式

```
function    =    "SIZE" [ "(" [ parameters ] ")" ]
parameters=    param /
                parameters "," param
param       =    "filename" "=" (wildcard-string / quoted-string) /
                "filename" "!=" (wildcard-string / quoted-string) /
                "type" "=" (wildcard-string / quoted-string) /
                "type" "!=" (wildcard-string / quoted-string) /
                "filetype" "=" type-string /
                "filetype" "!=" type-string /
                ("passwordlock" / "passwordlock" "=" ("part" / "all")) /
                ("nopasswordlock" / "nopasswordlock" "=" ("part" / "all")) /
                ("nopasswordlock+" / "nopasswordlock+" "=" ("part" / "all")) /
                ("max" / "min" / "sum") /
                "all"
```

```
| ----- |
| filename = filename |
|   指定添付ファイル名だけ対象とします。複数指定することはできません。 |
| filename != filename |
|   指定添付ファイル名以外を対象とします。複数指定することはできません。 |
| type = type |
|   指定 MIME タイプのパートだけ対象とします。複数指定することはできません。 |
| type != type |
|   指定 MIME タイプのパート以外を対象とします。複数指定することはできません。 |
| filetype = "type" |
|   添付ファイルのファイルタイプを判定し、指定したファイルタイプだけを |
|   集計の対象とします。指定するタイプ文字列と対応するファイルタイプは |
|   以下の表に示します。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。関数内 |
|   に filetype パラメータを複数指定することはできません。 |
| ----- |
```

	タイプ文字列	ファイルタイプ
1	ZIP	ZIP アーカイブ
2	LHA	LHA アーカイブ (拡張子は一般に .lzh)
3	RAR	RAR アーカイブ
4	CAB	CAB アーカイブ
5	GZIP	GZIP 圧縮ファイル
6	BZIP2	BZIP2 圧縮ファイル
7	Z	UNIX Compress 圧縮ファイル
8	TAR	TAR アーカイブ
9	TEXT	テキストファイル
10	PDF	PDF ファイル
11	EXCEL	Microsoft Excel ファイル
12	WORD	Microsoft Word ファイル
13	PPT	Microsoft PowerPoint ファイル
14	JTD	ジャストシステムー太郎ファイル
15	HTML	HTML ファイル
16	XML	XML ファイル
17	RTF	Microsoft RTF ファイル
18	VISIO	Microsoft Visio ファイル
19	EXE	DOS/Windows 実行形式ファイル
20	7ZIP	7ZIP アーカイブ
21	ARJ	ARJ アーカイブ
22	RPM	RPM パッケージ
23	DEB	Debian パッケージ
24	ISO	ISO9660 イメージファイル
25	MSI	Microsoft インストールパッケージ
26	HQX	BinHex エンコードファイル
27	AS	AppleSingle ファイル
28	TNEF	Microsoft Outlook リッチテキストファイル
29	SZDD	DOS Compress 圧縮ファイル
30	PACK	UNIX PACK 圧縮ファイル

```

| filetype != "type"
|   指定したファイルタイプ以外を対象とします。
| passwordlock / passwordlock = (part / all)
| nopasswordlock / nopasswordlock = (part / all)
| nopasswordlock+ / nopasswordlock+ = (part / all)
|   passwordlock      : パスワードが設定された添付ファイルだけを対象
|   nopasswordlock    : パスワード設定の無い添付ファイル、パスワード 設
|                       定の判定ができないファイルを対象
|   nopasswordlock+   : 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だけを対象
|   同じものを複数指定したり、これらを 1 つの関数内で複数同時に指定したり
|   することはできません。省略時にはパスワードの有無によるファイルの
|   限定は行わず、全ての添付ファイルが対象となります。
|   また、タイプを指定することで zip ファイルに対するパスワード有無判定
|   の動作を変更することができます。
|   part : アーカイブされているファイルのうち 1 つでも暗号化されている
|           ものがあれば「パスワード設定あり」と判定する (デフォルト)
|   all  : アーカイブされている全てのファイルが暗号化されている場合に
|           のみ「パスワード設定あり」と判定する
|   zip 以外の圧縮ファイル (rar,arj,7zip) については指定されたタイプに関わ
|   らず part タイプ (デフォルト) として動作します。
|   passwordlock/nopasswordlock/nopasswordlock+ それぞれ単独で指定した場合
|   には part タイプ (デフォルト) として動作します。
| min / max / sum
|   各パートのサイズの最小 / 最大値 / 合計値を関数値とする。
|   同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりする
|   ことはできません。省略時のデフォルトは「sum」(合計値) です。
| all
|   圧縮ファイルも展開して検査する。

```

パラメータを省略し、「SIZE」もしくは「SIZE ()」と表記した場合は、メッセージのサイズが関数値となります。

「filename」、「type」、「filetype」パラメータを指定した場合は、それぞれの条件にマッチする添付ファイルだけを対象とします。これらパラメータを同時に指定した場合は、指定した条件に同時にマッチする添付ファイルだけを対象とします。

例)

```
SIZE >= 2M512K
```

メッセージのサイズが 2.5 MB 以上ならば真

```
SIZE(filename= "*.doc", max) > 10MB
```

ファイル名が「*.doc」にマッチする添付ファイルの（複数ある場合はそれらの最大値）サイズが 10 MB を超えれば真

```
SIZE(filename= "*.xls", passwordlock) > 10MB
```

ファイル名が「*.xls」にマッチする添付ファイルで、かつ、パスワードロックされているもの（複数ある場合はそれらの合計値）が 10 M を超えれば真

```
SIZE filetype=" PDF+EXCEL", sum) > 2M
```

PDF ファイルと EXCEL ファイルの全ての合計サイズが 2 M を超えていれば真

```
SIZE filetype!=" HTML", sum) > 3M
```

HTML 以外の添付ファイルの合計サイズが 3 M を超えていれば真



- ・拡張展開機能が有効な場合だけ、表の 7ZIP ～ PACK 形式を判定します。拡張展開機能が有効でない場合に、これらのタイプ名を指定することはできません。
- ・添付ファイルのサイズはデコード後のファイルサイズです。
- ・パスワード設定が有ることを判定できるのは、Excel、Word、PowerPoint、PDF、一太郎、ZIP、RAR、7ZIP、ARJ 圧縮ファイルだけです。圧縮に使用した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。
- ・PowerPoint2003 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。
- ・アプリケーションファイルのテキスト検査機能を無効にしている場合は、Excel、Word、PowerPoint、PDF、一太郎のパスワード設定の判別ができません。アプリケーションファイルのテキスト検査機能の設定変更方法については、AppGetText オプション（85 ページ）をご参照ください。
- ・filename パラメータの引数に ASCII 文字以外（全角文字、漢字など）を指定することはできません。
- ・情報検査機能設定で圧縮ファイルの展開をしないよう設定されている場合は、all パラメータを指定しても圧縮ファイルの展開を行いません。圧縮ファイルの展開設定変更の方法については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「3-3-5-2 情報検査機能設定」の「圧縮ファイル」（225 ページ）をご参照ください。

-
- 圧縮ファイルを展開した場合の、便宜的な type の扱いは application になります。
 - ファイルタイプ判定はファイルのヘッダー、トレー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障できません。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。
 - 圧縮ファイルの展開を行わない場合でも、ZIP,RAR ファイルのパスワード設定の有無は判定できます。
 - 拡張展開機能が有効でない場合は、ARJ,7ZIP ファイルのパスワード設定の有無は判定できません。
 - 拡張展開機能を有効にした場合は、圧縮ファイルの展開を行わない場合でも ARJ ファイルのパスワード設定の有無を判定できます。
 - 拡張展開機能が有効でも圧縮ファイル展開しない設定の場合は 7ZIP ファイルのパスワード設定の有無は判定できません。拡張展開機能を有効にし、かつ、圧縮ファイルを展開する設定の場合は 7ZIP ファイルのパスワード設定の有無を判定できます。
 - ZIP, LHA, RAR, CAB の SFX 形式ファイルは、SFX 形式圧縮ファイルを展開する設定時には EXE ではなくそれぞれの圧縮ファイルと判定します。SFX 形式ファイルを展開しない設定時には 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ファイルタイプの判定ができません。
 - Excel2010,Excel2013 の読み取りパスワードが設定されたファイルはファイルタイプの判定ができません。
 - Word2007 (SP2 以降) ,Word2010,Word2013 の読み取りパスワードが設定されたファイルはファイルタイプの判定ができません。
 - PowerPoint2007,PowerPoint2010,PowerPoint2013 の読み取りパスワードが設定されたファイルはファイルタイプの判定ができません。
-

※ 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	○ (Excel2007 以前) × (Excel2010/2013) ^(※3)
	「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	○ (Excel2007 以前) × (Excel2010/2013)
	「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	○ ^(※4)
	書き込みパスワード有り	× ^(※5)
	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) Excel2010/2013 をパスワード有りのブック保護したあと、Excel2003 形式で保存し、再度、Excel2010/2013 形式で保存した場合、○（パスワード設定あり）と判定されます。

(※4) PowerPoint2013 で作成した PowerPoint2003 ファイルについては ×（パスワード設定無し）と判定されます。

(※5) PowerPoint2003 に関してのみ、○（パスワード設定有り）と判定されます。ただし、PowerPoint2007 (SP2 以降)、PowerPoint2013 で作成した PowerPoint2003 ファイルについては ×（パスワード設定無し）と判定されます。

ATTACHMENT 関数

添付ファイル数を検査し、その値を関数値とします。

書式

```
function    =    "ATTACHMENT" [ "(" [ parameters ] ")" ]
parameters=    param /
               parameters "," param
param       =    "filename" "=" (wildcard-string / quoted-string) /
               "filename" "!=" (wildcard-string / quoted-string) /
               "type" "=" (wildcard-string / quoted-string) /
               "type" "!=" (wildcard-string / quoted-string) /
               "filetype" "=" type-string /
               "filetype" "!=" type-string /
               ("passwordlock" / "passwordlock" "=" ("part" / "all")) /
               ("nopasswordlock" / "nopasswordlock" "=" ("part" / "all")) /
               ("nopasswordlock+" / "nopasswordlock+" "=" ("part" / "all")) /
               "all"
```

```
| filename = filename
|   指定添付ファイル名だけ対象とします。複数指定することはできません。
| filename != filename
|   指定添付ファイル名以外を対象とします。複数指定することはできません。
| type = type
|   指定 MIME タイプのパートだけ対象とします。複数指定することはできません。
| type != type
|   指定 MIME タイプのパート以外を対象とします。複数指定することはできません。
| filetype = "type"
|   添付ファイルのファイルタイプを判定し、指定したファイルタイプだけを
|   集計の対象とします。指定できるタイプ文字列と対応するファイル
|   タイプは SIZE 関数と同じです。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。関数内に filetype パラメータを複数指定することはできません。
| filetype != "type"
|   指定したファイルタイプ以外を対象とします。
```

```

passwordlock / passwordlock = (part / all)
nopasswordlock / nopasswordlock = (part / all)
nopasswordlock+ / nopasswordlock+ = (part / all)
passwordlock      : パスワードが設定された添付ファイルだけを対象
nopasswordlock    : パスワード設定の無い添付ファイル、パスワード設
                    定の判定ができないファイルを対象
nopasswordlock+   : 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だけを対象
同じものを複数指定したり、これらを1つの関数内で複数同時に指定したり
することはできません。省略時にはパスワードの有無によるファイルの
限定は行わず、全ての添付ファイルが対象となります。
また、タイプを指定することでzipファイルに対するパスワード有無判定
の動作を変更することができます。
part : アーカイブされているファイルのうち1つでも暗号化されている
      ものがあれば「パスワード設定あり」と判定する（デフォルト）
all  : アーカイブされている全てのファイルが暗号化されている場合に
      のみ「パスワード設定あり」と判定する
zip 以外の圧縮ファイル（rar,arj,7zip）については指定されたタイプに関わ
らず part タイプ（デフォルト）として動作します。
passwordlock/nopasswordlock/nopasswordlock+ それぞれ単独で指定した場合
には part タイプ（デフォルト）として動作します。
all
  圧縮ファイルも展開して検査する。

```

パラメータを省略して表記した場合は、添付ファイルの数が関数値となります。本システムにおける「添付ファイル」の定義は、以下のパートを除く全てのパートを添付ファイルとみなします。

- multipart パートなど構造をあらわすパート
- filename パラメータの無い text/plain パート（「本文」とみなす）

「filename」、「type」、「filetype」パラメータを指定した場合は、それぞれの条件にマッチする添付ファイルだけを対象とします。これらパラメータを同時に指定した場合は、指定した条件に同時にマッチする添付ファイルだけを対象とします。

例)

```
ATTACHMENT >= 10
```

「添付ファイル」の数が 10 以上ならば真

```
ATTACHMENT (filename= "*.doc" ) > 10
```

ファイル名が「*.doc」にマッチする添付ファイルの数が 10 を超えれば真

```
ATTACHMENT (type= "image" ) > 10
```

MIME タイプが「image」にマッチするパートの添付ファイルの数が 10 を超えれば真

```
ATTACHMENT (filename= "*.xls" , all) <= 20
```

圧縮ファイルがある場合は展開し、それも含めてファイル名が「*.xls」にマッチ

```
ATTACHMENT (filetype=" PDF+EXCEL" ) > 2
```

添付されている PDF ファイルと EXCEL ファイルの合計数が 2 を超えていれば真

```
ATTACHMENT (filetype!=" HTML" ) > 3
```

HTML 以外の添付ファイル数が 3 を超えていれば真



- ・パスワード設定が有ることを判定できるのは、Excel、Word、PowerPoint、PDF、一太郎、ZIP、RAR、7ZIP、ARJ 圧縮ファイルだけです。圧縮に使用した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。
 - ・Excel、Word、PowerPoint のパスワード設定の判定に関する制限事項は SIZE 関数と同様です。
 - ・アプリケーションファイルのテキスト検査機能を無効にしている場合は、Excel、Word、PowerPoint、PDF、一太郎のパスワード設定の判別ができません。アプリケーションファイルのテキスト検査機能の設定変更方法については、AppGetText オプション (85 ページ) をご参照ください。
 - ・filename パラメータの引数に ASCII 文字以外 (全角文字、漢字など) を指定することはできません。
 - ・情報検査機能設定で圧縮ファイルの展開をしないよう設定されている場合は、all パラメータを指定しても圧縮ファイルの展開を行いません。圧縮ファイルの展開設定変更の方法については、『管理サーバー 利用の手引き ~ GUARDIANWALL、WEBGUARDIAN 共通~』の「3-3-5-2 情報検査機能設定」の「圧縮ファイル」(225 ページ) をご参照ください。
 - ・圧縮ファイルを展開した場合の、便宜的な type の扱いは application になります。
 - ・ファイルタイプ判定に関する制限事項は SIZE 関数と同様です。
 - ・圧縮ファイルの展開を行わない場合でも、ZIP、RAR ファイルのパスワード設定の有無は判定できます。
 - ・拡張展開機能が有効でない場合は、ARJ、7ZIP ファイルのパスワード設定の有無は判定できません。
 - ・拡張展開機能を有効にした場合は、圧縮ファイルの展開を行わない場合でも ARJ ファイルのパスワード設定の有無を判定できます。
 - ・拡張展開機能が有効でも圧縮ファイル展開しない設定の場合は 7ZIP ファイルのパスワード設定の有無は判定できません。拡張展開機能を有効にし、かつ、圧縮ファイルを展開する設定の場合は 7ZIP ファイルのパスワード設定の有無を判定できます。
-

ADDRESS 関数

メッセージの宛先アドレスの数を検査し、その値を関数値とします。

書式

```
function    =    "ADDRESS" "(" parameter ")"
parameter  =    rcpt [ "!=" "{ groups }" ]
groups      =    groupname /
                  groups " + " groupname
rcpt        =    "TO" / "CC" / "RCPT" / "ERCPT"
```

※パラメータの省略はできません。

```

| TO      : ヘッダーの TO に指定されているアドレス数を検査する。
| CC      : ヘッダーの CC に指定されているアドレス数を検査する。
| RCPT    : ヘッダーの TO と CC に指定されているアドレス数を検査する。
| ERCPT   : エンベロープ TO に指定されているアドレス数を検査する。
|         特定グループに属するアドレスを対象外としたい場合は、
|         「!= {group}」を記述する。
|
|-----|
```

例)

```
ADDRESS(RCPT) >= 10
```

ヘッダー TO、CC に指定されているアドレスが 10 以上ならば真

```
ADDRESS(CC!= {GROUP}) > 10
```

ヘッダー CC に指定されているアドレスから、グループ「GROUP」に属するものを除いて数え、その数が 10 を超えれば真



- ・検査対象メールのヘッダーの書式が不正な場合は、アドレスの数を正確に数えられない場合があります。
- ・同一のアドレスが複数指定されている場合、重複も含めて数えます。
- ・1つのパラメータに指定したグループ数に関わらず、グループ定義のアドレスを合計して最大 8000 件まで判定します。「{grp3+grp2+grp1}」のように複数のグループを指定した場合は、グループ名のアルファベット辞書順（“grp1”，“grp2”，“grp3”，... の順）にグループ定義内容を読み込み、8000 件を超えたアドレス定義内容は無視します。必ず、合計 8000 件以内で定義してください。

DOMAIN 関数

メッセージの宛先アドレスからドメイン部分の数を検査し、その値を関数値とします。

書式

```
function    =    "DOMAIN" "(" parameter ")"
parameter  =    rcpt [ "!=" "{ groups" "]"
groups      =    groupname /
                  groups "+" groupname
rcpt         =    "TO" / "CC" / "RCPT" / "ERCPT"
```

※パラメータの省略はできません。

```

| TO      : ヘッダーの TO に指定されているドメイン数を検査する。
| CC      : ヘッダーの CC に指定されているドメイン数を検査する。
| RCPT    : ヘッダーの TO と CC に指定されているドメイン数を検査する。
| ERCPT   : エンベロープ TO に指定されているドメイン数を検査する。
|          特定グループに属するアドレスを対象外としたい場合は、
|          「!= {group}」を記述する。
|
|-----|

```

例)

```
DOMAIN(RCPT) >= 10
```

ヘッダー TO、CC に指定されているドメインが 10 以上ならば真

```
DOMAIN(CC!= {GROUP}) > 10
```

ヘッダー CC に指定されているアドレスから、グループ「GROUP」に属するものを除いて数え、そのドメイン数が 10 を超えれば真



- ここで使う「ドメイン部」とは、アドレスの「@」より後方部分の文字列全てです。
- 検査対象メールのヘッダーの書式が不正な場合は、ヘッダーのドメインの数を正確に数えられない場合があります。
- 英大小文字を同一視して同一のドメインかどうかの判定を行い、同一のドメインが複数指定されている場合、重複を排除して異なるものだけを数えます。
- パラメータにグループを指定した時のアドレス数に関する制限事項は、ADDRESS 関数のものと同様です。

DISCLOSED_ADDRESS

メールヘッダーの宛先に指定されるアドレス数を検査し、メールを実際に受け取る (エンベロープアドレスで指定される) 受信者ごとにそのアドレスとは異なるアドレスがヘッダーに表示されている数を集計して関数値とします。

書式

```
function    =    "DISCLOSED_ADDRESS" (" parameter ")
parameters=    param /
                parameters " , " param
param       =    "exclude" "=" "{" groups "}" ][ " , " ("max" / "min" / "sum" ) ]
groups      =    groupname /
                groups "+" groupname
```

```
┌-----┐
│ exclude = {groups} │
│   指定されたグループに属するアドレスを集計から除外します。1つの関数 │
│   内で複数指定することはできません。 │
│ max/min/sum │
│   メールを実際に受け取る (エンベロープアドレスで指定される) 受信者が │
│   複数ある場合に、それぞれの値の集計方法を指定します。 │
│   「max」(最大値) を指定した場合は、受信者ごとに検出した値の中で最大 │
│   の値に関数値とします。「min」(最小値) を指定した場合は、受信者ごと │
│   に検出した値の中で最小の値に関数値とします。「sum」(合計値) を指定 │
│   した場合は、各受信者の検査結果値を合計した値に関数値とします。 │
│   省略時のデフォルトは「max」です。同じものを複数指定したり、2つ以上 │
│   組み合わせて同時に指定したりすることはできません。 │
└-----┘
```

(例)

エンベロープアドレス

RCPT TO: taro@example.jp, bob@example.com

ヘッダーアドレス

TO: taro@example.jp, bob@example.com

CC: cab@abc.co.jp

```
DISCLOSED_ADDRESS() >= 1
```

実際に受信する受信者ごとに自分のアドレスと異なるアドレスがヘッダーの宛先に表示されている数が1以上であれば真。

本例では「taro@example.jp」「bob@example.com」それぞれが受け取るメールのヘッダーには3つのアドレスが表示されており、自分以外のアドレスは2つあるため (その最大値である) 関数値は「2」となります。

`DISCLOSED_ADDRESS(exclude={CSOL}) >= 1`

ヘッダーの宛先からグループ「CSOL」に属するアドレスを除外し、実際に受信する受信者ごとに自分のアドレスと異なるアドレスがヘッダーの宛先に表示されている数が1以上であれば真。



- ・ 検査対象メールのヘッダーの書式が不正な場合は、アドレス数を正確に数えられない場合があります。
 - ・ 同一のアドレスが複数指定されている場合、重複も含めて数えます。
 - ・ パラメータにグループを指定した時のアドレス数に関する制限事項は、ADDRESS 関数のものと同様です。
-

DISCLOSED_DOMAIN

メールヘッダーの宛先に指定されるドメイン部分の数を検査し、メールを実際に受け取る（エンベロープアドレスで指定される）受信者ごとにそのアドレスのドメインとは異なるドメインがヘッダーに表示されている数を集計して関数値とします。

書式

```
function    =    "DISCLOSED_DOMAIN" "(" parameter ")"
parameters=    param /
                parameters "," param
param       =    "exclude" "=" "{" groups "}" "[" ( "max" / "min" / "sum" ) "]"
groups      =    groupname /
                groups "+" groupname
```

```

| ----- |
| exclude = {groups} |
|   指定されたグループに属するアドレスを集計から除外します。1つの関数 |
|   内で複数指定することはできません。 |
| ----- |
| max/min/sum |
|   メールを実際に受け取る（エンベロープアドレスで指定される）受信者が |
|   複数ある場合に、それぞれの値の集計方法を指定します。 |
|   「max」（最大値）を指定した場合は、受信者ごとに検出した値の中で最大 |
|   の値を関数値とします。「min」（最小値）を指定した場合は、受信者ごと |
|   に検出した値の中で最小の値を関数値とします。「sum」（合計値）を指定 |
|   した場合は、各受信者の検査結果値を合計した値を関数値とします。省略 |
|   時のデフォルトは「max」です。同じものを複数指定したり、2つ以上組み |
|   合わせて同時に指定したりすることはできません。 |
| ----- |

```

(例)

エンベロープアドレス

RCPT TO: taro@example.jp, jiro@example.jp, bob@example.com

ヘッダーアドレス

TO: taro@example.jp, jiro@example.jp, bob@example.com

CC: cab@abc.co.jp

```
DISCLOSED_DOMAIN() >= 1
```

実際に受信する受信者ごとに自分のドメインと異なるドメインがヘッダーの宛先に表示されている数が1以上であれば真。

本例では「taro@example.jp」「jiro@example.jp」「bob@example.com」それぞれが受け取るメールのヘッダーには3つの異なるドメインが表示されており、自分以外のドメインは2つであるため（その最大値である）関数値は「2」となります。

`DISCLOSED_DOMAIN(exclude={CSOL}) >= 1`

ヘッダーの宛先からグループ「CSOL」に属するアドレスを除外し、実際に受信する受信者ごとに自分のドメインと異なるドメインがヘッダーの宛先に表示されている数が1以上であれば真。



- ここで使う「ドメイン」とは、アドレスの「@」より後方部分の文字列全てです。
 - 検査対象メールのヘッダーの書式が不正な場合は、ドメイン数を正確に数えられない場合があります。
 - 英大小文字を同一視して同一のドメインかどうかの判定を行い、同一のドメインが複数指定されている場合、重複を排除して異なるものだけを数えます。
 - パラメータにグループを指定した時のアドレス数に関する制限事項は、ADDRESS 関数のものと同様です。
-

MIMETYPE 関数

MIME タイプ検査を行い、その検査結果を関数値とします。通常検査動作部分で MIME タイプ検査を行います。本関数を用いることにより、動作適用前の条件部分で MIME タイプ検査を条件として、その結果により、適用動作を変えるようなルール記述ができます。

書式

```
function    =    "MIMETYPE" [ "(" [ parameters ] ")" ]
parameters=    param /
                parameters "," param
param       =    "set" "=" setname /
                "id" "=" (const / const "/" const) /
                ("weight" / "count" / "score") /
                ("max" / "min" / "sum") /
                "logmode" "=" ("new" / "add") /
                "loglevel" "=" const
```

set = setname

指定条件セットを使用して検査を行います。本パラメータ省略時はデフォルト条件セットを使用します。複数指定することはできません。

id = id

id = id / id

条件セット中の指定 ID 番号の条件だけを使用します。「id1/id2」と指定した場合は、それぞれ使用 ID 値の下限、上限となり「id1」以上、「id2」以下の範囲の ID だけを使用します。省略時は全 ID を使用します。複数指定することはできません。

weight / count / score

検査条件の重み、マッチした条件数、重みとマッチした条件数を掛けた値のいずれを検査結果値とするかを指定します。同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりすることはできません。省略時のデフォルトは「weight」（重み）。

試行 / 本番の 2 段階指定方式の場合は、試行条件は「0」、本番条件は「1」の値を持ちます。

max / min / sum

パートごとに検出した検査結果値の最大値 / 最小値 / 合計値を関数値とします。省略時のデフォルトは「max」（最大値）。

「min」（最小値）を指定した場合は、各パートで検出した検査結果値の中で最小の値を関数値とします。「sum」（合計値）を指定した場合は、各パートの検査結果値を合計した値を関数値とします。同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりすることはできません。

logmode = new**logmode = add**

情報検査ログに検査の結果検出した添付ファイル名を記録したい場合に指定します。「new」は、検査を行う前の情報検査ログ添付ファイル欄の検査結果を破棄して本関数の検査結果を記録します。「add」は本関数の検査を行う前の検査結果に追記します。

同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりすることはできません。省略時は検査結果を記録しません。

loglevel = *number*

上記「logmode」を指定した時、関数値が「number」以上の場合だけログに記録します。複数指定することはできません。省略時のデフォルトは「1」。

「min」指定の場合はログには記録しません。「max」指定の場合は「number」以上の検査結果値であった添付ファイル名を記録します。「sum」指定の場合は、1 以上の検査結果値を持つ添付ファイル名を記録します。複数指定することはできません。



- ・条件に一致する条件IDが検出されなかった場合は、関数値は0となります。
- ・MIME 検査条件は、条件セットの上位行の条件から順に判定され、最初に一致した条件が1つだけ検出されます。したがって、「count」指定の場合は、1つのパートの検査結果値の最大値はたかだか1となり、「score」指定時と「weight」指定時の検査結果値の違いはありません。たとえば、拡張子が「xls」であるファイルが1つと拡張子が「doc」であるファイルが2つ添付されている場合、下記条件セットを用いると weight 指定時の関数値は、パートごとに、2、4、4 となります。関数パラメータの「min」「max」「sum」指定で、それぞれの最小値、最大値、合計値を集計しますので関数値は、それぞれ、2、4、10 となります。

ID	重み	条件	
100	2	*/*	xls
200	4	*/*	doc

- ・MIME タイプ検査関数において、圧縮ファイルの展開を行うかどうかは、検査動作と同様に圧縮ファイルの展開設定に従います。圧縮ファイルの展開設定変更の方法については、『管理サーバー 利用の手引き ～ GUARD-
IANWALL、WEBGUARDIAN 共通～』の「3-3-5-2 情報検査機能設定」の「圧縮ファイル」（225 ページ）をご参照ください。

例)

```
MIMETYPE(set=main) >= 5
```

条件セット「main」を用いて MIME タイプ検査を行い、満たした条件の重み（の最大値）が 5 以上ならば真

```
MIMETYPE(set=set1, sum) > 10
```

条件セット「set1」を用いて MIME タイプ検査を行い、パートごとに満たした条件の重みの合計値が 10 を超えれば真

```
MIMETYPE(logmode=new, loglevel=5) > 8
```

デフォルト条件セットを用いて MIME タイプ検査を行い、満たした条件の重み（の最大値）が 8 を超えれば真。これまでの、情報検査ログに記録すべきパートの情報は破棄して、本検査において満たした条件の重みが 5 以上のパートを情報検査ログに記録する。

KEYWORD 関数

キーワード検査を行い、その検査結果を関数値とします。通常検査動作部分でキーワード検査を行います。本関数を用いることにより、動作適用前の条件部分でキーワード検査を条件として、その結果により、適用動作を変えるようなルール記述ができます。

書式

```
function    =    "KEYWORD" [ "(" [ parameters ] ")" ]
parameters=    param /
               parameters " , " param
param       =    "target" "=" ( "subject" / "filename" / "header" / "text" /
               "attachment" ) /
               "filename" "=" (wildcard-string / quoted-string) /
               "filename" "!=" (wildcard-string / quoted-string) /
               "filetype" "=" type-string /
               "filetype" "!=" type-string /
               "set" "=" setname /
               "id" "=" (const / const "/" const) /
               ( "weight" / "count" / "score" / "row" / "row+" ) /
               ( "max" / "min" / "sum" ) /
               "subtotal" "=" ( "max" / "min" / "sum" ) /
               "logmode" "=" ( "new" / "add" ) /
               "loglevel" "=" const
```

```

| target = subject
| target = filename
| target = header
| target = text
| target = attachment

```

キーワード検査対象部分を限定したい場合に指定します。「subject」指定時はサブジェクトだけが検査対象となります。「filename」指定時は、添付ファイルのファイル名パラメータ部だけが検査対象となります。「header」指定時は、ヘッダーだけが検査対象となります。「text」指定時はメール本文だけが検査対象となります。「attachment」指定時は添付ファイルだけが検査対象となります。デフォルトではヘッダー、本文、ファイル名、添付ファイルが検査対象となります。複数指定することはできません。本システムにおける「添付ファイル」の定義は、以下のパートを除く全てのパートを添付ファイルとみなします。

- multipart パートなど構造をあらわすパート
- filename パラメータの無い text/plain パート (「本文」とみなす)

filename = filename

指定添付ファイル名だけ対象とします。複数指定することはできません。

filename != filename

指定添付ファイル名以外を対象とします。複数指定することはできません。

filetype = "type"

添付ファイルのファイルタイプを判定し、指定したファイルタイプだけを集計の対象とします。指定できるタイプ文字列と対応するファイルタイプは SIZE 関数と同じです。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。関数内に filetype パラメータを複数指定することはできません。

filetype != "type"

指定したファイルタイプ以外を対象とします。

set = setname

指定条件セットを使用して検査を行います。本パラメータ省略時はデフォルト条件セットを使用します。複数指定することはできません。

id = id

id = id / id

条件セット中の指定 ID 番号の条件だけを使用します。「id1/id2」と指定した場合は、それぞれ使用 ID 値の下限、上限となり「id1」以上、「id2」以下の範囲の ID だけを使用します。省略時は全 ID を使用します。複数指定することはできません。

weight/count/score/row/row+

検査条件の重み (weight)、キーワード検出数 (count)、重みとキーワード検出数を掛けた値 (score)、キーワード検出 ID 種数 (row, row+) のいずれを検査結果値とするか指定します。row 指定時は条件セット中の検出したキーワード式の ID 番号の (重複を省いた) 数を値としますので後述の subtotal の指定はできません。row+ 指定字は検査対象パート全てで検出したキーワードの ID 番号の (重複を省いた) 数を値としますので、後述の subtotal と max/min/sum の指定はできません。

max / min / sum

検査対象パートごとに検出した検査結果値の最大値 / 最小値 / 合計値を関数値とします。省略時のデフォルトは「max」(最大値)。

各検査対象パート内の検査結果の集計方法は後述の subtotal で指定します。

```
| subtotal = max / min / sum
| 1つの検査パート内で検査結果値の最大値 / 最小値 / 合計値を各パートの
| 検査結果値とします。複数の各パート間の検査結果値の集計方法は前述の
| max/min/sum で指定します。同じものを複数指定したり、同時に2つ以上
| 組み合わせて指定したりすることはできません。省略時のデフォルトは検
| 査対象パートごとの集計方法と同じ指定となります。
| logmode = new
| logmode = add
| 情報検査ログに検査の結果検出したキーワードを記録したい場合に指定し
| ます。「new」は、検査を行う前の情報検査ログキーワード欄の検査結果を
| 破棄して本関数の検査結果を記録します。「add」は本関数の検査を行う前
| の検査結果に追記します。
| 同じものを複数指定したり、2つ以上組み合わせて同時に指定したりする
| ことはできません。省略時は検査結果を記録しません。
| loglevel = number
| 上記「logmode」を指定した時、関数値が「number」以上の場合だけログ
| に記録します。省略時のデフォルトは「1」です。
| subtotalにminを指定している場合と検査対象パートごとの集計方法に
| 「min」を指定している場合はログには記録しません。
| 検査対象パートごとの集計方法に「max」を指定している場合は、1つの検
| 査対象パートの検査結果値が「number」以上（subtotal=max または省略時）
| もしくは1以上（subtotal=sum）となる検出キーワードを記録します。検査
| 対象パートごとの集計方法が「sum」指定の場合は、1つの検査対象パート
| 検査結果値が1以上となる検出キーワードを記録します。複数指定するこ
| とはできません。
```




- ・キーワード検索条件で、キーワードを AND 条件で記述している場合、検出語数の定義は以下のようになります。
下記条件セットを用いて検査を行い、1つの検査パート中に「機密」を2語、「文書」を3語検出した場合、該当条件の検出語数は5となります。同様に、「機密」を0語、「文書」を3語の場合は、本キーワード条件を満たしませんので0となります。

ID	重み	条件
100	2	機密 & 文書
200	4	社外秘 部外秘

- ・同様に上記条件セットを用いて、検査を行いキーワード検索条件で、キーワードを OR 条件で記述している場合、検出語数の定義は以下のようになります。1つの検査パート中に「社外秘」を2語、「部外秘」を3語検出した場合、該当条件の検出語数は5となります。同様に、「社外秘」を0語、「部外秘」を3語の場合は、該当条件の検出語数は3となります。
- ・アプリケーションファイルのテキスト検査機能を無効にしている場合は、Excel、Word、PowerPoint、PDF、一太郎、各ファイルのキーワード検査ができません。アプリケーションファイルのテキスト検査機能の設定変更方法については、AppGetText オプション (85 ページ) をご参照ください。
- ・キーワード検索関数において、圧縮ファイルの展開も行うかどうかは、検査動作と同じく、圧縮ファイルの展開設定に従います。圧縮ファイルの展開設定変更の方法については、『管理サーバー 利用の手引き ~ GUARD-
IANWALL、WEBGUARDIAN 共通~』の「3-3-5-2 情報検査機能設定」の「圧縮ファイル」(225 ページ) をご参照ください。
- ・ファイルタイプ判定に関する制限事項は SIZE 関数と同様です。
- ・PowerPoint2013 で作成した読み取りパスワード有りあるいは書き込みパスワード有り PowerPoint2003 ファイルについてはキーワード検査ができません。

例)

```
KEYWORD(set=main) >= 5
```

条件セット「main」を用いてキーワード検査を行い、検出したキーワード条件の重み (の最大値) が 5 以上ならば真

```
KEYWORD(set=set1, score, sum) > 10
```

条件セット「set1」を用いてキーワード検査を行い、パートごとに検出したキーワードの検出語数と重みを掛けた値の合計値が 10 を超えれば真

```
KEYWORD(set=set1, id=100, count, sum) > 20
```

条件セット「set1」の ID 番号 100 の条件だけ用いてキーワード検査を行い、パートごとに検出した ID 番号 100 のキーワード検出語数の合計値が 20 を超えれば真

```
KEYWORD(target=subject, logmode=new, loglevel=5) > 8
```

デフォルト条件セットを用いてメールのサブジェクト部だけキーワード検査を行う。満たした条件の重み（の最大値）が 8 を超えれば真。これまでの、本メールの情報検査ログに記録すべき情報は破棄して、本検査における満たした条件の重みが 5 以上のパートを情報検査ログに記録する。

REGEX 関数

正規表現パターンによるキーワード検査を行い、その検査結果を関数値とします。指定正規表現のパターン検査を検査対象パートごとに行単位で行い、指定パターンがマッチする行数を集計し、関数値とします。

書式

```
function    =    "REGEX" [ "(" [ parameters ] ")" ]
parameters=    param /
                parameters " , " param
param       =    "target" "=" ( "subject" / "filename" / "header" / "text" /
                "attachment" ) /
                "filename" "=" ( wildcard-string / quoted-string ) /
                "filename" "!=" ( wildcard-string / quoted-string ) /
                "filetype" "=" type-string /
                "filetype" "!=" type-string /
                "pattern" "=" regular-expression /
                ( "max" / "min" / "sum" ) /
                "logmode" "=" ( "new" / "add" ) /
                "loglevel" "=" const
```

```
| target = subject
| target = filename
| target = header
| target = text
| target = attachment
```

正規表現検査対象パートを限定したい場合に指定します。「subject」指定時はサブジェクトだけが検査対象となります。「filename」指定時は、添付ファイルのファイル名パラメータ部だけが検査対象となります。「header」指定時は、ヘッダーだけが検査対象となります。「text」指定時はメール本文だけが検査対象となります。「attachment」指定時は添付ファイルだけが検査対象となります。デフォルトではヘッダー、本文、ファイル名、添付ファイルが検査対象となります。複数指定することはできません。本システムにおける「添付ファイル」の定義は、以下のパートを除く全てのパートを添付ファイルとみなします。

- ・ multipart パートなど構造をあらわすパート
- ・ filename パラメータの無い text/plain パート（「本文」とみなす）

```
| filename = filename
```

指定添付ファイル名だけ対象とします。複数指定することはできません。

```
| filename != filename
```

指定添付ファイル名以外を対象とします。複数指定することはできません。

filetype = "type"

添付ファイルのファイルタイプを判定し、指定したファイルタイプだけを集計の対象とします。指定できるタイプ文字列と対応するファイルタイプは SIZE 関数と同じです。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。関数内に filetype パラメータを複数指定することはできません。

filetype != "type"

指定したファイルタイプ以外を対象とします。

pattern = "regular-expression"

指定正規表現を用いて検査を行います。本パラメータの設定は必須であり省略することはできません。

正規表現の記述は、POSIX 拡張正規表現に従います。ASCII 文字だけが使用でき、英大小文字は区別します。2 バイトコード文字の指定はできません。「¥」（使用環境によってはバックスラッシュで表示されます）記号を使用する場合は 2 個重ねてください。複数指定することはできません。

max / min / sum

各検査対象パートのパターン検出行数の最大値 / 最小値 / 合計値関数値とします。同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりすることはできません。省略時のデフォルトは「max」（最大値）。

「min」（最小値）を指定した場合は、各検査パートで検出した検査結果値の中で最小の値を関数値とします。「sum」（合計値）を指定した場合は、各検査パートの検査結果値を合計した値を関数値とします。

logmode = new**logmode = add**

情報検査ログに検査の結果検出したパターンを記録したい場合に指定します。「new」は、検査を行う前の情報検査ログキーワード欄の検査結果を破棄して本関数の検査結果を記録します。「add」は本関数の検査を行う前の検査結果に追記します。

同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりすることはできません。省略時は検査結果を記録しません。

loglevel = number

上記「logmode」を指定した時、関数値が「number」以上の場合だけログに記録します。省略時のデフォルトは「1」。

「min」指定の場合はログには記録しません。「max」指定の場合は「number」以上の検査結果値であったパターンを記録します。「sum」指定の場合は、1 以上の検査結果値を持つパターンを記録します。同じものを複数指定したり、2 つ以上組み合わせて同時に指定したりすることはできません。

例)

```
REGEX(pattern= "[0-9]{4}-[0-9]{4}") >= 10
```

数字が 4 桁、ハイフン、数字が 4 桁並ぶパターンを含む行が 10 行以上検出されれば真

```
REGEX(pattern= "[0-9]{9}", logmode=new, loglevel=5) > 10
```

数字が 9 桁並ぶパターンを含む行が 10 行を超えて検出されれば真。これまでの、本メールの情報検査ログに記録すべき情報は破棄して、本検査においてパターンを 5 行以上検出したら情報検査ログに記録する。



- ・正規表現検査では、パターンを含む「行数」を検査結果値とします。同一行内に複数回パターンが出現しても、該当行で行数 1 だけをカウントします。
- ・複数の REGEX 関数を配送ルール上に記述した場合、正規表現パターンがあらわす正規集合に包含関係がある場合、一方のパターンを検出した場合、もう一方のパターンを検出できない場合があります。
- ・配送ルール全行で利用できる正規表現検査関数は最大 16 個です。
- ・アプリケーションファイルのテキスト検査機能を無効にしている場合は、Excel、Word、PowerPoint、PDF、一太郎、各ファイルの正規表現検査ができません。アプリケーションファイルのテキスト検査機能の設定変更方法については、AppGetText オプション (85 ページ) をご参照ください。
- ・正規表現検査関数において、圧縮ファイルの展開も行うかどうかは、検査動作と同じく、圧縮ファイルの展開設定に従います。圧縮ファイルの展開設定変更の方法については、『管理サーバー 利用の手引き ～ GUARD-
IANWALL、WEBGUARDIAN 共通～』の「3-3-5-2 情報検査機能設定」の「圧縮ファイル」(225 ページ) をご参照ください。
- ・ファイルタイプ判定に関する制限事項は SIZE 関数と同様です。
- ・PowerPoint2013 で作成した読み取りパスワード有りあるいは書き込みパスワード有り PowerPoint2003 ファイルについては正規表現検査ができません。

DPINFO 関数

個人情報検査を行い、その検査結果を関数値とします。通常検査動作部分で個人情報検査を行えますが、本関数を用いることにより動作適用前の条件部分で個人情報検査を行い、その結果により適用動作を変えるようなルール記述ができます。

書式

```
function    =    "DPINFO" [ "(" [ parameters ] ")" ]
parameters=    param /
                parameters " ," param
param       =    ("index" / "count" / "type") /
                "item" "=" const /
                "target" "=" ( "attachment" / "text" ) /
                "filename" "=" ( wildcard-string / quoted-string ) /
                "filename" "!=" ( wildcard-string / quoted-string ) /
                "filetype" "=" type-string /
                "filetype" "!=" type-string /
                ("max" / "min" / "sum" ) /
                "logmode" "=" ( "new" / "add" ) /
                "loglevel" "=" const
```

| target = attachment

| target = text

個人情報検査対象パートを指定します。「attachment」指定時は添付ファイルだけが検査対象となります。「text」指定時はメール本文だけが検査対象となります。複数指定することはできません。省略時のデフォルトでは、text/html パートを除く添付ファイルだけが検査対象となります。

本システムにおける「添付ファイル」の定義は、以下のパートを除く全てのパートを添付ファイルとみなします。

- ・ multipart パートなど構造をあらわすパート
- ・ filename パラメータの無い text/plain パート（「本文」とみなす）

| index / count / type

個人情報検査結果の総合指数 / 個人情報件数 / 個人情報項目数を関数値とします。省略時のデフォルトは「index」（総合指数）。

複数指定することはできません。

総合指数は 0 ～ 100 の値になります。個人情報件数は 0 以上の値になります。

個人情報項目数は 0 ～ 7 の値となります。

item = number

個人情報を作成する特定の情報項目を指定して、その検出件数を関数値とします。**number** に指定する値で指定される項目は下記のようになります。複数指定することはできません。前述の **index/count/type** と同時に指定することはできません。

- 1: 氏名（漢字、ひらがな、カタカナ）
- 2: 住所（郵便番号を含まず）
- 3: 電話番号
- 4: メールアドレス
- 5: 生年月日 / 年齢
- 6: 組織名
- 7: クレジットカード番号

filename = filename

指定添付ファイル名だけ対象とします。複数指定することはできません。

filename != filename

指定添付ファイル名以外を対象とします。複数指定することはできません。

filetype = "type"

添付ファイルのファイルタイプを判定し、指定したファイルタイプだけを集計の対象とします。指定できるタイプ文字列と対応するファイルタイプは **SIZE** 関数と同じです。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。関数内に **filetype** パラメータを複数指定することはできません。

filetype != "type"

指定したファイルタイプ以外を対象とします。

max/min/sum

複数の検査対象パートの検査結果値の最大値 / 最小値 / 合計値を関数値とします。

「**max**」（最大値）を指定した場合は、各検査パートで検出した検査結果値の中で最大の値を関数値とします。「**min**」（最小値）を指定した場合は、各検査パートで検出した検査結果値の中で最小の値を関数値とします。「**sum**」（合計値）を指定した場合は、各検査パートの検査結果値を合計した値を関数値とします。

同じものを複数指定したり、2つ以上組み合わせて同時に指定したりすることはできません。省略時のデフォルトは「**max**」（最大値）です。

```
| logmode = new
```

```
| logmode = add
```

情報検査ログに検査の結果検出した添付ファイル名を記録したい場合に指定します。「new」は、検査を行う前の情報検査ログ添付ファイル欄の検査結果を破棄して本関数の検査結果を記録します。「add」は本関数の検査を行う前の検査結果に追記します。

同じものを複数指定したり、2つ以上組み合わせて同時に指定したりすることはできません。省略時は検査結果を記録しません。

ログ記録時は、情報検査ログの添付ファイル欄に「[個人情報]」という文字列と共に添付ファイル名を記録します。メール本文を検査対象とし、記録条件を満たした場合はファイル名の変わりに「(メール本文)」という文字列が記録されます。

```
| loglevel = number
```

上記「logmode」を指定した時、関数値が「number」以上の場合だけログに記録します。省略時のデフォルトは「50」です。

「min」指定の場合はログには記録しません。「max」指定の場合は「number」以上の検査結果値であった添付ファイル名を記録します。検査対象パートごとの集計方法に「sum」を指定している場合は、1つの検査対象パートが1以上の検査結果値を持つ添付ファイル名を記録します。複数指定することはできません。



- ・個人情報検査関数において、圧縮ファイルの展開も行うかどうかは、検査動作と同じく圧縮ファイルの展開設定に従います。圧縮ファイルの展開設定変更の方法については、『**管理サーバー 利用の手引き ～ GUARDIANWALL 、WEBGUARDIAN 共通～**』の「3-3-5-2 情報検査機能設定」の「**圧縮ファイル**」(225 ページ)をご参照ください。
- ・アプリケーションファイルのテキスト検査機能を無効にしている場合は、Excel、Word、PowerPoint、PDF、一太郎、各ファイルの個人情報検査ができません。アプリケーションファイルのテキスト検査機能の設定変更方法については、**AppGetText オプション** (85 ページ)をご参照ください。
- ・ファイルタイプ判定に関する制限事項は SIZE 関数と同様です。
- ・PowerPoint2013 で作成した読み取りパスワード有りあるいは書き込みパスワード有り PowerPoint2003 ファイルについては個人情報検査ができません。

例)

```
DPINFO() >= 40
```

個人情報検査を行い、検査結果の総合指数値（の最大値）が 40 以上であれば真

```
DPINFO(count, sum) >= 20
```

個人情報検査を行い、検出した個人情報件数の合計が 20 以上であれば真

```
INFO(filename="*.xls", item=3) >= 10
```

ファイル名が「*.xls」にマッチする添付ファイルの個人情報検査を行い、検出した電話番号件数（の最大値）が 10 以上であれば真

DATE 関数

メッセージの日付（GUARDIANWALL がメールを受け付けた日付）を関数値とします。

書式

function = "DATE" "(" parameter ")"

parameter = "YEAR" / "MON" / "DAY" / "WEEK"

※パラメータを省略した場合は、「DATE (WEEK)」の値となります。

YEAR	: 年（西暦）
MON	: 月（1 ～ 12）
DAY	: 日（1 ～ 31）
WEEK	: 曜日（0：日曜 ～ 6: 土曜）

例)

DATE (DAY) = 1

メッセージの日付の日が、1 日（月初）ならば真

DATE (WEEK) >= 1 & DATE (WEEK) <= 5

メッセージの日付の曜日が、月曜日から金曜日ならば真

TIME 関数

メッセージの時刻（GUARDIANWALL がメールを受け付けた時刻）を関数値とします。

書式

function = "TIME" "(" parameter ")"

parameter = "HOUR" / "MIN" / "SEC"

※パラメータを省略した場合は、「TIME (HOUR)」の値となります。

| HOUR : 時 (0 ~ 23)

| MIN : 分 (0 ~ 59)

| SEC : 秒 (0 ~ 59)

例)

TIME(HOUR) >= 9 & TIME(HOUR) <= 17

メッセージの時刻が、9 時 ~ 17 時ならば真

TIME(HOUR) >= 18

メッセージの時刻が、18 時以降ならば真

HEADER 関数

メッセージヘッダーに指定フィールド、フィールド値があるかどうかを検査します。指定フィールドを持つ場合、関数値は「1」となります。指定フィールドがない場合、関数値は「0」となります。

書式

```
function      =      "HEADER" "(" parameters ")"
parameters    =      param /
                    parameters "," param
param          =      "field" "=" (wildcard-string / quoted-string) /
                    "value" "=" (wildcard-string / quoted-string)
```

field = *fieldname*

指定フィールド名を指定します。本パラメータの設定は必須であり省略することはできません。複数指定することはできません。英大小文字を同一視します。

value = *value*

指定フィールド値を持つかどうかを検査します。英大小文字を同一視します。

例)

```
HEADER(field=" MIME-Version" , value=" 1.0" ) > 0
```

「MIME-Version: 1.0」というフィールドが存在すれば真

```
HEADER(field=" X-Auth-Warning" )>0
```

「X-Auth-Warning:」というフィールド（フィールド値は任意）が存在すれば真

```
HEADER(field=" X-Mailer" , value=" MS*" )>0
```

「X-Mailer:」というフィールドのフィールド値が「MS」で始まる文字列であれば真



- ・フィールド値が複数行にまたがる場合、2行目以降は検査できません。
- ・エンコードされたフィールド値については、デコードした後に検査を行います。本関数はASCII文字列を検査することを前提としていますので、想定していない文字列が検出される場合があります。

CYPHER 関数

メッセージが暗号化メールであるかどうかを検査します。

判別可能な暗号メールの場合は関数値は「1」となります。判別できない場合は関数値は「0」となります。

書式

```
function    =    "CYPHER" "(" parameters ")"
parameters=    param /
                parameters "," param
param       =    "smime" / "pgp" / "ibe"
```

※パラメータを省略した場合は、暗号化メール（S/MIME、PGP、VOLTAGE IBE）かどうかを検査します。

```

| smime
|   S/MIME 暗号化メールかどうかを検査します。
| pgp
|   PGP 暗号化メールかどうかを検査します。
| ibe
|   VOLTAGE IBE 暗号化メールかどうかを検査します。

```

例)

```
CYPHER() > 0
```

暗号化メール（S/MIME、PGP、VOLTAGE IBE）であれば真

```
CYPHER(smime) > 0
```

S/MIME 暗号化メールであれば真

```
CYPHER(pgp) > 0
```

PGP 暗号化メールであれば真



S/MIME、PGP 署名のみで暗号化メールではない場合、関数値は「0」です。送信メーラーによっては暗号化メールであると判別できない場合があります。

(5) 動作

action = actname ["(" [param 0*("(" param)] ")"]

動作のパラメータ指定は、パラメータ指定位置により設定される機能が決まります。
各動作のパラメータ指定位置と指定できる内容を下記に示します。

パラメータ指定位置

```
RELAY(WarnSender, WarnAdmin, ArchiveSW,  
      \ AltAdminAddress, ForwardAddress, WarnRcpt, NotificationID,  
      \ Option, Crypt, EncNotifySender, EncNotifyRcpt, encpassword= EncPassword,  
      \ BccConvert, BccConvOption)  
DELETE (WarnSender, WarnAdmin, ArchiveSW,  
        \ AltAdminAddress, ForwardAddress, WarnRcpt, NotificationID,  
        \ Option, Crypt, EncNotifySender, EncNotifyRcpt, encpassword= EncPassword,  
        \ BccConvert, BccConvOption)  
HOLD (WarnSender, WarnAdmin, ArchiveSW,  
      \ AltAdminAddress, ForwardAddress, WarnRcpt, NotificationID,  
      \ Option, Crypt, EncNotifySender, EncNotifyRcpt, encpassword= EncPassword,  
      \ BccConvert, BccConvOption)  
DELAY (WarnSender, WarnAdmin, ArchiveSW,  
       \ AltAdminAddress, ForwardAddress, WarnRcpt, NotificationID,  
       \ Option, Crypt, EncNotifySender, EncNotifyRcpt, encpassword= EncPassword,  
       \ BccConvert, BccConvOption)  
CHECK (OK_Action, NG_Action, MimeCheckSW, KeywdCheckSW,  
       \ lb_mtype/ub_mtype, lb_keywd/ub_keywd,  
       \ set= set_mtype, set= set_keywd)
```

RELAY, DELETE, HOLD, DELAY 動作パラメータ

WarnSender : 差出人通知スイッチ
 0 : 通知しない、1 : 通知する

WarnAdmin : 管理者通知スイッチ
 0 : 通知しない、1 : 通知する

ArchiveSW : メッセージのコピー保存スイッチ
 0 : 保存しない、1 : 保存する

AltAdminAddress : 追加管理者アドレス
 (本来の管理者以外の管理者通知メール送付先)

ForwardAddress : メッセージのコピーを転送する宛先アドレス

WarnRcpt : 受信者通知スイッチ
 0 : 通知しない、1 : 通知する

NotificationID : 通知文選択 ID
 「0」指定時は各動作の基本通知文を使用する

Option : 送信オプション
 中継サーバーの ID (0 ~ 7)

Crypt	: 暗号化設定 zipenc : 添付ファイルを暗号化する 未指定時は、暗号化 / 復号を行わない。
EncNotifySender	: 差出人パスワード通知スイッチ 0 : 通知しない、 1 : 通知する
EncNotifyRcpt	: 受信者パスワード通知スイッチ 0 : 通知しない、 1 : 通知する
EncPassword	: 固定パスワード 値は半角英数と「+」「=」「/」「,」「.」「_」のみ使用可能 未指定時は、ランダムパスワードを使用する。
BccConvert	: BCC 変換スイッチ 0 : 変換しない、 1 : 変換する 未指定時は変換を行わない。
BccConvOption	: BCC 変換オプション 0 : BCC 変換後、ヘッダー From アドレスをヘッダー To アドレスに設定しない 1 : BCC 変換後、ヘッダー From アドレスをヘッダー To アドレスに設定する 未指定時は設定しない。

CHECK 動作パラメータ

OK_Action	: MIME タイプ、キーワード検査結果 OK 時の動作 Relay 、 Delete 、 Hold 、 Delay のいずれか指定
NG_Action	: MIME タイプ、キーワード検査結果 NG 時の動作 Relay 、 Delete 、 Hold 、 Delay のいずれか指定
MimeCheckSW	: MIME タイプ検査スイッチ 0 : 検査しない、 1 : 検査する
KeywdCheckSW	: キーワード検査 / 個人情報検査スイッチ 0 : 検査しない、 1 : キーワード検査だけ行う 2 : 個人情報検査だけ行う 3 : キーワード検査と個人情報検査両方行う
lb_mtype/ub_mtype	: MIME タイプ検査条件有効 ID の下界値 / 上界値 上界値に「0」を指定した場合は、下界値以上の全 ID が有効
lb_keywd/ub_keywd	: キーワード検査条件有効 ID の下界値 / 上界値 上界値に「0」を指定した場合は、下界値以上の全 ID が有効
set_mtype	: MIME タイプ検査に使用する条件セット名。 未指定時は、デフォルト条件セットを使用する。
set_keywd	: キーワード検査に使用する条件セット名。 未指定時は、デフォルト条件セットを使用する。

各動作のデフォルト設定（パラメータ省略時の設定）

Relay : Relay(0,0,0,,0,0,0,,1,0,,0,0)
Delete : Delete(1,1,0,,0,0,0,,1,0,,0,0)
Hold : Hold(1,1,0,,0,0,0,,1,0,,0,0)
Delay : Delay(1,1,0,,0,0,0,,1,0,,0,0)
Check : Check(Relay(0,0,0,,0,0,0,,1,0,,0,0)
, Hold(1,1,0,,0,0,0,,1,0,,0,0), 1,1,0/0,0/0)

共通書式

addr = 1*(ALPHA / DIGIT / “_” / “@” / “.” / “-”)
addrpattern = 1*(ALPHA / DIGIT / “_” / “@” / “.” / “-” / “*”)
groupname = 1*(ALPHA / DIGIT / “_”)
setname = 1*(ALPHA / DIGIT / “_”)
string = 1*(ALPHA / DIGIT / “_” / “.”)
regular-expression = quoted-string
quoted-string = DQUOTE *(%x20-21 / %x23-7E) DQUOTE
wildcard-string = 1*(ALPHA / DIGIT / “_” / “.” / “*”)
DIGIT = “0”-“9”
ALPHA = “A”-“Z” / “a”-“z”
LF = %x0A
DQUOTE = %x22 ; “ダブルクォート”

各種識別子、アドレスパターン文字列において、英文字の大小文字は区別せず同一視します。グループ名文字列、条件セット名文字列のみ英大小文字を区別します。

ルール設定例)

- 内部ドメイン名 : example.com

```
100 : aaa@example.com : * : 0 : Relay      発信者 aaa は中継
101 : bbb@example.com : * : 0 : Delete     発信者 bbb は削除
102 : usr@example.com : ERCPT! != *@example.com : Delete
                                         発信者 usr のメールは外部へ送信禁止
200 : * : *@abc.co.jp : 0 : Relay         abc.co.jp 宛は中継
201 : * : *@whitehouse.gov : 0 : Delete(0,1) 削除して管理者に通知
202 : * : *@kantei.go.jp : 0 : Delete(0,0,,admin@example.com)
                                         削除して admin へ通知
301 : * : * : 2M : Delete                 2M 以上のメールは削除
302 : * : * : 0 : Check                   残りは全て検査
```

- 内部ドメイン名 : example.com
- グループ : EXM = {*@example.com}

```
100 : FROM={EXM} : * : Address(RCPT!={EXM})>=10 : Delete
      EXM グループの発信者で、ヘッダー宛先にグループ外のアドレスが 10 以上
      指定されている場合は削除

101 : FROM={EXM} : * : Attachment() > 3 : Delete
      添付ファイルが 3 個を超えたら削除
```


5-4 MIME タイプ検査条件設定ファイル

MIME タイプ検査条件は、下記条件セット設定ファイルと条件セットディレクトリ下の条件ファイルから成ります。

条件セットファイルパス名

検査サーバー：/opt/Guardian/WALL/etc/mss.mtype

管理サーバー：/opt/Guardian/Admin/etc/wall/mss.mtype

条件セットディレクトリ名

検査サーバー：/opt/Guardian/WALL/etc/mss.mtype.d

管理サーバー：/opt/Guardian/Admin/etc/wall/mss.mtype.d

条件ファイルパス名

<条件セット名>.mtype

(1) 条件セットファイル書式

```
mime_set_lines    =    mime_set /
                    mime_set_lines mime_set
mime_set          =    setname ":" [ "comment" "=" comment-string ] LF
setname           =    1*(ALPHA / DIGIT / "_" )
string            =    0*( "%" HEX HEX ) / "+" / ALPHA / DIGIT )
HEX               =    DIGIT | "A" | "B" | "C" | "D" | "E" | "F"
```

MIME タイプ条件セットファイルは、各行に条件セット名、コメントを記述します。

```
[-----]
| setname      : 条件セット名                               |
| comment     : コメント (EUC コードを URI エンコードした文字列) |
|-----|
```

(2) 条件ファイル書式

```
mimeruleset=    mimerule /
                mimeruleset mimerule
mimerule   =    id ":" weight ":" content-type ":" extension LF
id          =    1*DIGIT
weight     =    "0" - "9"
content-type=    wildcard-string "/" wildcard-string
extension  =    wildcard-string / "<" wildcard-string ">"
```

MIME タイプ検査条件ファイルは、各行に ID、重み、コンテンツタイプ、拡張子を記述します。メッセージ中にコンテンツタイプ、拡張子が同時にマッチする MIME パートを含んでいれば、該当条件が HIT となり重みの値に従い条件論理式、動作などが決定されます。

id	: ルール ID 番号
表記法:	正数
	1 ~ 99999999、複数行で ID の重複はできません。
weight	: 重み (または、2 段階指定方式の場合は本番 / 試行フラグ)
表記法:	0 ~ 9 (または、2 段階指定方式の場合は 0/1)
	条件の重みを指定します。
	試行 / 本番の 2 段階指定方式の場合は、下記の意味になります。
	1: 本番 キーワード条件式を満たすと検査 NG となる。
	0: 試行 キーワード条件式を満たしても検査 NG にならない。
	ただし、統計情報の表示のため配送ログファイルには、条件セット名と ID が記録される。
content-type	: MIME コンテンツタイプ
表記法:	mediatype/subtype
	ワイルドカード表記可、大文字小文字区別しません。
extension	: ファイル拡張子、ファイル名パターン
表記法:	文字列 (拡張子、もしくは、<ファイル名パターン>)
	ワイルドカード表記可、大文字小文字区別しません。
	(2 バイトコードのファイル名は指定しないでください)

例)

試行 / 本番 2 段階の場合

100 : 0 : text/plain	: *	プレーンテキストは OK
101 : 1 : application/*	: ppt	PowerPoint データは NG
102 : 1 : application/*	: <patch.exe>	patch.exe というファイルは NG
103 : 1 : image/jpeg	: *	画像ファイルは NG
104 : 1 : video/mpeg	: *	動画ファイルは NG
105 : 1 : audio/*	: *	音声ファイルは NG
		その他全て OK

※ MIME コンテンツタイプと拡張子の両方を満たすものが、条件に一致します。ファイル名、拡張子だけで一致させたい場合は、コンテンツタイプの指定に注意してください。

5-5 キーワード条件式設定ファイル

キーワード検査条件は、下記条件セット設定ファイルと条件セットディレクトリ下の条件ファイルから成ります。

条件セットファイルパス名

検査サーバー：/opt/Guardian/WALL/etc/mss.keywd

管理サーバー：/opt/Guardian/Admin/etc/wall/mss.keywd

条件セットディレクトリ名

検査サーバー：/opt/Guardian/WALL/etc/mss.keywd.d

管理サーバー：/opt/Guardian/Admin/etc/wall/mss.keywd.d

条件ファイルパス名

<条件セット名>.keywd

(1) 条件セットファイル書式

```
keywd_set_lines    =      keywd_set /
                        keywd_set_lines keywd_set
keywd_set          =      setname ":" [ "comment" "=" comment-string ] LF
```

キーワード条件セットファイルは、各行に条件セット名、コメントを記述します。

```
[-----]
| setname      : 条件セット名                               |
| comment      : コメント (EUC コードを URI エンコードした文字列) |
|-----|
```

(2) 条件ファイル書式

```
keywdruleset      =      keywdrule /
                        keywdruleset keywdrule
keywdrule         =      id ":" weight ":" keyword-exp LF
id                =      1*DIGIT
weight           =      "0" - "9"
keyword-exp       =      keyword /
                        keyword-exp "&" keyword-exp /
                        keyword-exp "[" keyword-exp /
                        "(" keyword-exp ")"
keyword           =      1*(EUC) /
                        "" keyword SPACE keyword ""
EUC               =      (%A1 - %FE)(%A1 - %FE)
```

キーワード条件式ファイルは、各行に ID、重み、キーワード条件式を記述します。メッセージ中にキーワード条件式を満たすキーワードの組合せが含まれていれば、該当条件が HIT となり重みの値に従い条件論理式、動作などが決定されます。

id	: ルール ID 番号
表記法	: 正数
	1 ~ 32767、複数行で ID の重複はできません。
weight	: 重み（または、2 段階指定方式の場合は本番 / 試行フラグ）
表記法	: 0 ~ 9（または、2 段階指定方式の場合は 0/1）
	条件の重みを指定します。
	試行 / 本番の 2 段階指定方式の場合は、下記の意味になります。
	1 : 本番キーワード条件式を満たすと検査 NG となる。
	0 : 試行キーワード条件式を満たしても検査 NG にならない。
	ただし、統計情報の表示のため配送ログファイルには、 条件セット名と ID が記録される。
keyword-exp	: キーワード条件式
	‘(’ KEYWORDS ‘)’
	word
	word operator KEYWORDS
	operator
	& : and 条件
	: or 条件
	word
	ASCII もしくは EUC コードで記述した単語、あるいは フレーズキーワード
	※登録されたキーワードの全角半角は区別しません。
	特殊記号「(」「)」「&」「 」と単語の間には半角空白が必要です。
	特殊記号そのものを検査したい場合は、それぞれ「¥(」「¥)」 「¥&」「¥ 」 「¥”」のように「¥」を前に付けて登録してください。「&」は「 」より優先して評価されます。

例)

```
10 : 1 : 社外秘 | 部外秘
11 : 1 : 転送禁止
21 : 0 : AAA プロジェクト
22 : 0 : ¥( 秘 ¥)
31 : 0 : " フレーズ キーワード "
```

5-6 動作一覧定義ファイル

ウェブブラウザでの検査・配送ルール設定では、あらかじめ動作一覧定義ファイルに用意された数種類の動作の中から動作を選択します。

このファイルを編集することにより、動作内容をカスタマイズすることができます。

ファイルパス名

検査サーバー：/opt/Guardian/httpd/conf/wall/action

管理サーバー：/opt/Guardian/Admin/etc/wall/action

表記法

ラベル：動作設定

初期状態の設定

中継	: relay
中継（保存）	: relay(, , 1)
削除	: delete
削除（差出人通知なし）	: delete(0, 1)
削除（差出人通知なし保存）	: delete(0, 1, 1)
保留	: hold
保留（差出人通知なし）	: hold(0, 1)
保留（差出人通知なし保存）	: hold(0, 1, 1)
一時保留	: delay
一時保留（保存）	: delay(, , 1)
検査	: check
検査（差出人通知なし）	: check(, hold(0, 1))
検査（差出人通知なし保存）	: check(, hold(0, 1, 1))
検査返送	: check(, delete)

動作設定の詳細内容については、「5-3 検査・配送ルール設定ファイル」- 「(5) 動作」(139 ページ) をご参照ください。

5-7 通知メール

(1) 通知メール送出条件

本システムで処理したメールを保留、もしくは、削除した場合に通知メールを差出人、管理者、(元メールの)受信者に通知メールを送信することができます。差出人、管理者、受信者宛にそれぞれ通知メールを送信するには、まずサーバー設定ファイルで差出人宛、管理者宛、受信者宛の各通知機能をそれぞれ「True」に設定する必要があります。デフォルトの設定では受信者には通知メールを送信しません。

サーバー設定ファイル

宛先	条件設定	備考
差出人	[NoticeMessage] NotifySender=True	初期値 : True
管理者	[NoticeMessage] NotifyAdmin=True	初期値 : True
受信者	[NoticeMessage] NotifyRecipients=True	初期値 : False

※設定変更後は GUARDIANWALL の再起動が必要です。

各宛先の通知設定値が「True」で、かつ、検査・配送ルールによって適用された動作の通知オプションパラメータの各宛先に対応する値が「1」に指定されている場合に通知メールが送信されます。

デフォルトの設定では受信者には通知メールを送信しません。

検査・配送ルール、適用動作のパラメータ

宛先	種類	適用動作	備考
差出人	保留通知	HOLD(1)	第1パラメータ1 初期値 : 1
	削除通知	DELETE(,1)	第1パラメータ1 初期値 : 1
管理者	保留通知	HOLD(,1)	第2パラメータ1 初期値 : 1
	削除通知	DELETE(,1)	第2パラメータ1 初期値 : 1
受信者	保留通知	HOLD(,,,,,1)	第6パラメータ1 初期値 : 0
	削除通知	DELETE(,,,,,1)	第6パラメータ1 初期値 : 0

保留後送出、保留後削除通知送出条件

デフォルトの設定では、保留時に差出人に保留通知メールを送信している場合は、保留メールを送出（または、削除）すると、差出人に保留後送出通知（または、保留後削除通知）メールが送信されます。同様に、保留時に管理者に保留通知メールを送信している場合は、保留メールを送出（または、削除）すると、管理者に保留後送出通知（または、保留後削除通知）メールが送信されます。デフォルトの設定では受信者には通知メールを送信しません。以下の各設定項目を変更することにより、保留後送出通知、保留後削除通知の送信条件を変更することができます。

宛先	種類	条件設定	備考
差出人	保留後送出	[NoticeMessage] NotifySender_Approve	初期値：cont
	保留後削除	[NoticeMessage] NotifySender_Cancel	初期値：cont
管理者	保留後送出	[NoticeMessage] NotifyAdmin_Approve	初期値：cont
	保留後削除	[NoticeMessage] NotifyAdmin_Cancel	初期値：cont
受信者	保留後送出	[NoticeMessage] NotifyRecipients_ Approve	初期値：no
	保留後削除	[NoticeMessage] NotifyRecipients_ Cancel	初期値：no

条件には以下の値を設定できます。

yes/no/cont/nega

- yes : 保留時の通知有無に関係なく、通知を送信する。
- no : 保留時の通知有無に関係なく、通知を送信しない。
- cont : 保留時に通知した場合だけ、通知を送信する。
- nega : 保留時に通知していない場合だけ、通知を送信する。(*1) (*2)

(*1) 受信者の保留後送出、保留後削除通知の設定値は、「yes/no/cont」だけ指定できます（「nega」を指定しても「no」と同様、保留後送出、保留後削除時に受信者へ通知を送信しません）。

(*2) 管理者の保留後送出、保留後削除通知の設定値で「nega」を指定すると、保留時に管理者、もしくは、追加管理者のいずれかに保留通知を送信した場合、保留後送出、保留後削除時に管理者、（保留動作に指定された）追加管理者への通知を送信しません。

自動送出通知送出条件

デフォルトの設定では、一時保留メールの自動送出時、差出人、管理者、受信者へ自動送出通知メールを送信しません。以下の各設定項目を変更することにより、自動送出通知の送信条件を変更することができます。

宛先	種類	条件設定	備考
差出人	自動送出通知	[NoticeMessage] NotifySender_Delay	初期値：no
管理者	自動送出通知	[NoticeMessage] NotifyAdmin_Delay	初期値：no
受信者	自動送出通知	[NoticeMessage] NotifyRecipients_Delay	初期値：no

条件には以下の値を設定できます。

yes/no/cont/nega

- yes : 保留時の通知有無に関係なく、通知を送信する。
- no : 保留時の通知有無に関係なく、通知を送信しない。
- cont : 保留時に通知した場合だけ、通知を送信する。
- nega : 保留時に通知していない場合だけ、通知を送信する。(*1) (*2)

(*1) 受信者の自動送出通知の設定値は、「yes/no/cont」だけ指定できます（「nega」を指定しても「no」と同様、自動送出時に受信者へ通知を送信しません）。

(*2) 管理者の自動送出通知の設定値で「nega」を指定すると、保留時に管理者、もしくは、追加管理者のいずれかに保留通知を送信した場合、自動送出時に管理者、（保留動作に指定された）追加管理者への通知を送信しません。

※設定変更後は GUARDIANWALL の再起動が必要です。

保留再通知送出条件

デフォルトの設定では、保留時に差出人に保留通知メールを送信している場合は、一定時間経過後も保留メールが処理されない場合、差出人に保留再通知メールが送信されます。同様に、保留時に管理者に保留通知メールを送信している場合は、管理者に保留再通知メールが送信されます。デフォルトの設定では受信者には再通知メールを送信しません。以下の各設定項目を変更することにより、保留再通知の送信条件を変更することができます。

条件には以下の値を設定できます。

yes/no/cont/nega

- yes : 保留時の通知有無に関係なく、通知を送信する。
- no : 保留時の通知有無に関係なく、通知を送信しない。
- cont : 保留時に通知した場合だけ、通知を送信する。
- nega : 保留時に通知していない場合だけ、通知を送信する。(*1) (*2)

宛先	種類	条件設定	備考
差出人	保留再通知	[NoticeMessage] NotifySender_Again	初期値 : cont
管理者	保留再通知	[NoticeMessage] NotifyAdmin_Again	初期値 : cont
受信者	保留再通知	[NoticeMessage] NotifyRecipients_Again	初期値 : no

(*1) 受信者の保留再通知の設定値は、「yes/no/cont」だけ指定できます（「nega」を指定しても「no」と同様、再通知時に受信者へ通知を送信しません）。

(*2) 管理者の保留再通知の設定値で「nega」を指定すると、保留時に管理者、もしくは、追加管理者のいずれかに保留通知を送信した場合、保留再通知時に管理者、（保留動作に指定された）追加管理者への通知を送信しません。

※設定変更後は GUARDIANWALL の再起動が必要です。

(2) 通知メール形式

以下にデフォルトの通知文の内容を説明します。

削除通知（管理者宛）

メッセージ削除時には下記のような通知メールが管理者へ送信されます。

From: GUARDIANWALL <root@mg.example.com> To: admin@mg.example.com Subject: Returned mail: Unable to deliver 以下のメールは外部へ送信することができませんでした。 MSGID: QAA01234 ----- 送信できなかった宛先 (RCPT TO:) ----- aaa@example.co.jp ----- オリジナルメッセージヘッダー ----- From: Mr. X <sender@example.com> To: aaa@example.co.jp Subject: 秘密 Date: 1 Jan 1999 11:04:59 +0900 ----- 削除理由 ----- メール本文に下記キーワードが含まれています。 社外秘	標題 編集可
	通知文 編集可
	削除された宛先 (自動生成)
	削除メールの ヘッダー情報 (自動生成)
	削除理由 (自動生成)

標題中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$SUBJECT → 元メールの標題

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR → サーバーホストの IP アドレス

\$MSGID → メッセージ ID

削除通知（差出人宛）

メッセージ削除時には下記のような通知メールが差出人へ送信されます。
さらに、削除された元のメールが添付されます。

From: GUARDIANWALL <root@mg.example.com>
To: sender@example.com
Subject: Returned mail: Unable to deliver

以下のメールは外部へ送信することができませんでした。
MSGID: QAA01234

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

削除された宛先
(自動生成)

削除メールの
ヘッダー情報
(自動生成)

標題中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$SUBJECT → 元メールの標題

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR → サーバーホストの IP アドレス

\$MSGID → メッセージ ID

削除通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

From: GUARDIANWALL <root@mg.example.com>
To: aaa@example.co.jp
Subject: Returned mail: Unable to deliver

以下のメールは受信することができませんでした。
MSGID: QAA01234

----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

削除メールの
ヘッダー情報
(自動生成)

標題中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$SUBJECT → 元メールの標題

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR → サーバーホストの IP アドレス

\$MSGID → メッセージ ID

保留通知（管理者宛）

メッセージ保留時には下記のような通知メールが管理者へ送信されます。

From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Returned mail: Unable to deliver

以下のメールは外部へ送信することができませんでした。
メールサーバに保留されています。
MSGID: QAA01234

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

----- 保留理由 -----
メール本文に下記キーワードが含まれています。
社外秘

標題
編集可

通知文
編集可

保留された宛先
(自動生成)

保留メールの
ヘッダー情報
(自動生成)

保留理由
(自動生成)

標題中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$SUBJECT → 元メールの標題

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR → サーバーホストの IP アドレス

\$MSGID → メッセージ ID

\$PCODE → 問合せコード

保留通知（差出人宛）

メッセージ保留時には下記のような通知メールが管理者へ送信されます。
さらに、保留された元のメールが添付されます。

From: GUARDIANWALL <root@mg.example.com>
To: sender@example.com
Subject: Returned mail: Unable to deliver

以下のメールは外部へ送信することができませんでした。
メールサーバに保留されています。管理者へ問合せ処置を依頼
してください。

MSGID: QAA01234 問合せコード: ABCD1234

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

保留された宛先
(自動生成)

保留メールの
ヘッダー情報
(自動生成)

標題中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$SUBJECT → 元メールの標題

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR → サーバーホストの IP アドレス

\$MSGID → メッセージ ID

\$PCODE → 問合せコード

保留通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

From: GUARDIANWALL <root@mg.example.com>
To: aaa@example.co.jp
Subject: Returned mail: Unable to deliver

以下のメールは受信することができませんでした。
メールサーバに保留されています。管理者へ問合せ処置を依頼
してください。
MSGID: QAA01234 問合せコード: ABCD1234

----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

保留メールの
ヘッダー情報
(自動生成)

標題中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$SUBJECT → 元メールの標題

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR → サーバーホストの IP アドレス

\$MSGID → メッセージ ID

\$PCODE → 問合せコード

一時保留通知（管理者宛）

メッセージ一時保留時には下記のような通知メールが管理者へ送信されます。

From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail was temporarily reserved

以下のメールは外部へ送信することができませんでした。
メールサーバに一時的に保留されています。保留後、自動的に
送信されます。
保留時間（分）: 60 MSGID: RAA08393

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

----- 保留理由 -----

メール本文に下記キーワードが含まれています。
社外秘

通知文
編集可

一時保留された宛先
(自動生成)

一時保留メールの
ヘッダー情報
(自動生成)

一時保留理由
(自動生成)

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR	→ サーバーホストの IP アドレス
\$MSGID	→ メッセージ ID
\$PCODE	→ 問合せコード
\$DELAYTIME	→ 一時保留時間

一時保留通知（差出人宛）

メッセージ一時保留時には下記のような通知メールが差出人へ送信されます。
さらに、一時保留された元のメールが添付されます。

```
From: GUARDIANWALL <root@mg.example.com>  
To: admin@mg.example.com  
Subject: Notification: Your mail was temporarily reserved
```

以下のメールは外部へ送信することができませんでした。
メールサーバに一時的に保留されています。保留後、自動的に
送信されます。

保留時間（分）: 60 MSGID: RAA08393 問合せコード：
W4PLYHCJ

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----

```
From: Mr. X <sender@example.com>  
To: aaa@example.co.jp  
Subject: 秘密  
Date: 1 Jan 1999 11:04:59 +0900
```

通知文
編集可

一時保留された宛先
（自動生成）

一時保留メールの
ヘッダー情報
（自動生成）

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR	→ サーバーホストの IP アドレス
\$MSGID	→ メッセージ ID
\$PCODE	→ 問合せコード
\$DELAYTIME	→ 一時保留時間

一時保留通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail was temporarily reserved

以下のメールは外部へ送信することができませんでした。
メールサーバに一時的に保留されています。保留後、自動的に
送信されます。

保留時間（分）: 60 MSGID: RAA08393 問合せコード:
W4PLYHCJ

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

通知文
編集可

一時保留メールの
ヘッダー情報
（自動生成）

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR	→ サーバーホストの IP アドレス
\$MSGID	→ メッセージ ID
\$PCODE	→ 問合せコード
\$DELAYTIME	→ 一時保留時間

保留後送出通知（差出人宛、管理者宛）

保留メッセージを管理者が送出した時には、下記のような通知メールが保留時に通知メールを送信した宛先に送信されます。

From: GUARDIANWALL <root@mg.example.com>
To: sender@example.com
Subject: Notification: Your mail was approved

以下のメールは送信されました。
MSGID: QAA01234

----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

保留メールの
ヘッダー情報
(自動生成)

保留後送出通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

From: GUARDIANWALL <root@mg.example.com>
To: aaa@example.co.jp
Subject: Notification: Your mail was approved

以下のメールは受信しました。
MSGID: QAA01234

----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

保留メールの
ヘッダー情報
(自動生成)

保留後削除通知（差出人宛、管理者宛）

保留メッセージを管理者が削除した時には、下記のような通知メールが保留時に通知メールを送信した宛先に送信されます。

From: GUARDIANWALL <root@mg.example.com>
To: sender@example.com
Subject: Notification: Your mail was canceled

以下のメールは削除されました。
MSGID: QAA01234

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

保留メールの
ヘッダー情報
(自動生成)

保留後削除通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

From: GUARDIANWALL <root@mg.example.com>
To: aaa@example.co.jp
Subject: Notification: Your mail was canceled

以下のメールは削除されました。
MSGID: QAA01234

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

標題
編集可

通知文
編集可

保留メールの
ヘッダー情報
(自動生成)

自動送出通知（差出人宛、管理者宛）

一時保留メッセージが自動送出された時には、下記のような通知メールが送信されます。

※デフォルトの設定では、自動送出時に通知メールは送信しません。

```
From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail was delivered
```

以下のメールは外部へ自動送信されました。
MSGID: RAA08393

```
----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900
```

通知文
編集可

一時保留メールの
ヘッダー情報
(自動生成)

自動送出通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

```
From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail was delivered
```

以下のメールは受信しました。
MSGID: RAA08393

```
----- オリジナルメッセージヘッダー -----
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900
```

通知文
編集可

一時保留メールの
ヘッダー情報
(自動生成)

保留再通知（管理者宛）

メッセージ保留後、一定時間経過しても処理されない場合は、下記のような通知メールが管理者へ送信されます。

From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail is still held.

以下のメールはまだ処理されていません。
メールサーバに保留されています。
保留時間：0日1時間0分 MSGID: UAA29815 問合せコード：
KWWX4T

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900

----- 保留理由 -----

メール本文に下記キーワードが含まれています。
社外秘

通知文
編集可

保留された宛先
(自動生成)

保留メールの
ヘッダー情報
(自動生成)

保留理由
(自動生成)

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR	→ サーバーホストの IP アドレス
\$MSGID	→ メッセージ ID
\$PCODE	→ 問合せコード
\$HOLDTIME	→ メッセージ保留時間

保留再通知（差出人宛）

メッセージ保留後、一定時間経過しても処理されない場合は、下記のような通知メールが差出人へ送信されます。

さらに、保留された元のメールが添付されます。

```
From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail is still held.
```

以下のメールはまだ処理されていません。
メールサーバに保留されています。管理者へ問合せ処置を依頼してください。

保留時間：0 日 1 時間 0 分 MSGID: UAA29815 問合せコード：
KWWXXM4T

----- 送信できなかった宛先 (RCPT TO:) -----
aaa@example.co.jp

----- オリジナルメッセージヘッダー -----

```
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900
```

通知文
編集可

保留された宛先
(自動生成)

保留メールの
ヘッダー情報
(自動生成)

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR	→ サーバーホストの IP アドレス
\$MSGID	→ メッセージ ID
\$PCODE	→ 問合せコード
\$HOLDTIME	→ メッセージ保留時間

保留再通知（受信者宛）

※デフォルトの設定では、受信者には通知メールは送信しません。

```
From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Your mail is still held.
```

以下のメールはまだ処理されていません。
メールサーバに保留されています。管理者へ問合せ処置を依頼してください。
保留時間：0日1時間0分 MSGID: UAA29815 問合せコード：KWWWXM4T

----- オリジナルメッセージヘッダー -----

```
From: Mr. X <sender@example.com>
To: aaa@example.co.jp
Subject: 秘密
Date: 1 Jan 1999 11:04:59 +0900
```

通知文
編集可

保留メールの
ヘッダー情報
(自動生成)

通知文中の次のマクロ文字列は、右の内容にそれぞれ置き換えられます。

\$ADDR	→ サーバーホストの IP アドレス
\$MSGID	→ メッセージ ID
\$PCODE	→ 問合せコード
\$HOLDTIME	→ メッセージ保留時間

メール保存ディレクトリ切替通知

保存メールディレクトリを複数指定し、保存先のディレクトリの切り替えが行われた時に、下記のような通知メールを管理者アドレス宛に送信します。

```
From: GUARDIANWALL <root@dqg.example.com>
To: admin@mg.example.com
Subject: Notification: disk switch
```

メール保存ディレクトリが切り替わりました。
Old directory: /disk1
New directory: /disk2

※デフォルトの設定では、メール保存ディレクトリ切替通知メールは送信しません。

(3) 通知メール設定ファイル

通知メール設定ファイルには、通知メールの標題、通知文及び通知メールに処理した元メールを添付するかどうかを設定することができます。

通知文 ID、通知宛先種別ごとに 1 行使用し、上記設定を記述します。

ファイルパス名

検査サーバー : /opt/Guardian/WALL/etc/mss.notice

管理サーバー : /opt/Guardian/Admin/etc/wall/mss.notice

表記法

ID : TO : ATTACHMENT : MESSAGE_PATH : SUBJECT

ID : 通知文 ID 番号	
表記法 :	正数値もしくは文字列
	ユーザー登録通知文の ID は、1 ~ 99999999
	各動作の基本通知文は以下の文字列で指定する。
relay	: 中継通知 (デフォルト)
delete	: 削除通知 (デフォルト)
hold	: 保留通知 (デフォルト)
delay	: 一時保留通知 (デフォルト)
approve	: 保留後送出通知 (デフォルト)
cancel	: 保留後削除通知 (デフォルト)
delay_r	: 自動送出通知 (デフォルト)
again	: 保留再通知 (デフォルト)
TO : 通知宛先種別	
S :	差出人通知の設定
A :	管理者通知の設定
R :	受信 (予定) 者通知の設定
C :	コメント (SUBJECT 欄に URI エンコーディングでコメント文字列を指定)
ATTACHMENT : 元メールの添付	
0 :	元メールを添付しない
1 :	元メールを添付する
	保留後送出通知、保留後削除通知、自動送出通知には、「0」「1」いずれを指定しても元メールを添付しません。
MESSAGE_PATH : 通知文テンプレートファイル名	
	通知文内容を設定したファイルの指定
	「/opt/Guardian/WALL/template (検査サーバー)」、「/opt/Guardian/Admin/etc/wall/template (管理サーバー)」ディレクトリ以下のファイル名です。ファイルの文字コードは EUC です。

「-----」
| SUBJECT : 通知文のメール標題（サブジェクト） |
| 通知文のメール標題の指定 |
| CGI 画面から登録した場合は、Base64 エンコード済の文字列を登録します。 |
「-----」

5-8 送信先外部サーバーの切り替え

GUARDIANWALL が受信し中継する送信先サーバーをあらかじめ複数登録し、検査結果などにより送信先サーバーを選択することができます。

送信先サーバーの登録

情報管理者でログインします。【メール】-「システム管理」-「基本設定」-「拡張」-【メール送信】画面で、メール送信の設定で外部サーバーを選択し、空白で区切り複数のサーバーホストの IP アドレスを指定することができます。



登録可能なサーバーホストの IP アドレス数は最大 8 個です。

送信先サーバーの登録

外部サーバーに複数のサーバーを登録すると、【メール】-「ポリシー設定」-「検査・配送ルール」の動作詳細設定画面で「中継サーバー選択」というリストボックスが表示されます。ここから該当ルールの動作が適用された場合に使用するサーバーを選択します。

デフォルトでは外部サーバーの指定で先頭に指定されたサーバーに中継します。



中継動作実行時だけ選択したサーバーに中継します。保留動作を適用したメールが保留後送出操作時に中継されるサーバーは送出操作時に設定されているデフォルト（先頭に指定されたサーバー）となります。



動作詳細設定でサーバーを選択した場合、外部サーバー指定で登録された複数サーバーのうち何番目のサーバーを使用するのかを定義します。表示される IP アドレスそのものは、ここで設定されません。外部サーバー指定の内容や順序を変更すると、この選択内容も変更されます。



通知メールは、MSP 経由で送信されます。

5-9 添付ファイル暗号化機能仕様

(1) 暗号化パスワード生成仕様

添付ファイル暗号化機能は、GUARDIANWALL に 1 通として送信されてきたメール毎に暗号化を実施して、パスワードを生成します。そのため、1 通のメールが GUARDIANWALL に到達する前に分割された場合は、分割された数だけパスワード通知メールが送信者へ届きます。

(2) パスワード通知メール

添付ファイル暗号化機能では、添付ファイルが暗号化された際に使用したパスワードをパスワード通知メールとして送信者に通知します。

パスワード通知メールの送信先は、送信者以外ではエンベロープ TO アドレス (GUARDIANWALL に届いた時点でのエンベロープ TO アドレス) に送付することが可能です。エンベロープ TO アドレスに送付したい場合は、添付ファイル暗号化機能の設定を確認し、状況に合わせた設定を行うことで受信者へのパスワード通知メールが送信されます。

・「全メール暗号化」の場合

サーバー設定ファイル PasswdSend パラメータを 1 (送信者、受信者) とする。

宛先	設定	備考
送信者	[Encrypt] PasswdSend = 0	デフォルト設定
送信者、受信者	[Encrypt] PasswdSend = 1	受信者はエンベロープ TO アドレスのみ (ヘッダー To ではない)

・「検査・配送ルールで指定されたメールのみ暗号化」の場合

検査・配送ルールの動作詳細設定にあるパスワード通知メールの受信者にチェックする。

① 送信仕様

パスワード通知メールは以下のような宛先仕様で送信されます。

送信者通知

項目	設定値
ヘッダー From	GUARDIANWALL 管理者
エンベロープ From	GUARDIANWALL 管理者
ヘッダー To	オリジナルメールのヘッダー From
エンベロープ To	オリジナルメールのヘッダー From

受信者通知

項目	設定値
ヘッダー From	オリジナルメールのヘッダー From
エンベロープ From	オリジナルメールのヘッダー From
ヘッダー To	オリジナルメールのヘッダー To
エンベロープ To	オリジナルメールのエンベロープ To

② 通知メール形式

パスワード通知メールの通知メール切り替えにて「デフォルト通知文を使用する」を設定した場合、以下のような形式で送信されます。

パスワード通知メールの設定については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「3-3-5-4 添付ファイル暗号化設定」-【パスワード通知メール】(233 ページ) をご参照ください。

送信者通知形式

送信者へのパスワード通知メールは下記のようにになります。

```
From: GUARDIANWALL <root@mg.example.com>
To: sender@mg.example.com
Subject: 暗号化パスワード通知メール (<オリジナルメール件名>)
「<オリジナルメール件名>」の添付ファイルは暗号化されました。
暗号化された添付ファイル「<添付ファイル名>」のパスワードは「<添付パスワード>」
になります。
----- 暗号化送信された宛先 (RCPT TO) -----
aaa@example.co.jp
```

受信者通知形式

エンベロープ TO アドレスへのパスワード通知メールは下記のようにになります。

受信者通知は、暗号化送信された宛先が記載されません。

```
From: sender@mg.example.com
To: user@mg.example.com
Subject: 暗号化パスワード通知メール (<オリジナルメール件名>)
「<オリジナルメール件名>」の添付ファイルは暗号化されました。
暗号化された添付ファイル「<添付ファイル名>」のパスワードは「<添付パスワード>」
になります。
```

(3) 注意点

メーラーが使用する文字エンコード方法によっては、暗号化された添付ファイルにおいて半角カタカナを含む添付ファイル名が文字化けする場合があります。添付ファイルのデータ自体には影響はありません。ご了承ください。

また、1 通のメールに対し、添付ファイル暗号化するためには以下の制限がございます。

- ・ファイルサイズは合計 25MB まで
- ・ファイル数は 100 個まで

制限を超えるファイルサイズやファイル数の場合、添付ファイル暗号化されずにエラーとなります。

このとき、メールが配送できませんのでご注意ください。

5-10 標的型攻撃メール検知機能仕様

(1) 検査の対象となる電子メール

本機能では、組織内部へ向けて送信された電子メールだけが検査対象となります。エンベロープ TO アドレスが全て内部ドメイン名に属するような電子メールを「**組織内部へ向けて発信されたメール**」とみなします。1 個でも内部ドメイン名に属さないアドレスが含まれていると検査対象となりません。「1-4 検査の対象となる電子メール」に記載されたキーワード検査など検査・配送制御の対象となるメールとは異なりますのでご注意ください。

(2) 検査仕様

下記のような特徴をもつメールを標的型攻撃メールとして検出します。

① 差出人アドレスを詐称し、かつ不特定多数の宛先へ送信された疑いがあるメール

ヘッダーの差出人アドレス（ヘッダーの From アドレス）とエンベロープ FROM アドレスのドメインが異なる場合、差出人アドレスに詐称の疑いありと判断します。また、BCC アドレスがメーリングリストなど所定のアドレスを 2 個以上含んでいる場合、不特定多数の宛先へ送信された疑いありと判断します。



- ・ヘッダーの差出人アドレスとエンベロープ FROM アドレスのどちらか一方がもう片方のサブドメインである場合は同じドメインとみなします。
- ・メーリングリストなど不特定多数の宛先へ送信するために利用されるメールアドレスをあらかじめシステムに登録しておく必要があります。また、判定基準となる BCC アドレスの検出数も変更することができます（デフォルトは 2 個）。メールアドレスの登録や BCC アドレスの検出数の変更については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』の「3-3-5-5 標的型攻撃メール検知設定」-「公開メールアドレス」（246 ページ）をご参照ください。
- ・エンベロープ TO アドレスのうち、ヘッダーの宛先アドレス（ヘッダーの To、Cc、Resent-To、Resent-Cc アドレス）に含まれないものを BCC アドレスとします。

② 添付された実行ファイルのファイル名に偽装の疑いがあるメール

ファイル名に下記のような特徴がある場合、偽装の疑いありと判断します。本検査は GUARDIANWALL のファイルタイプ判定で DOS/Windows 実行形式ファイルと判定されたものだけが対象となります。

- ・連続する 5 個以上の空白文字がある。
- ・RLO 制御文字が使用されている。
- ・アプリケーションファイルと実行形式ファイルの二重拡張子が使用されている。



- ・全角空白、半角空白はともに 1 個の空白文字として扱います。
- ・アプリケーションファイル拡張子、実行形式ファイル拡張子はそれぞれ下記になります。

アプリケーションファイル拡張子		実行形式ファイル拡張子
PDF	pdf	exe scr pif com bat cmd
Word	doc dot docx docm dotx dotm	
Excel	xls xlt xlsx xlsx xltm xltm	
PowerPoint	ppt pps pot pptx pptm ppsx ppsm potx potm	

③ 添付されたリンクファイル（ショートカットファイル）に任意スクリプトが埋め込まれている 疑いがある

リンクファイル（ショートカットファイル）から抽出したリンク先情報をあらかじめ登録された辞書と比較することによりスクリプトを検出します。辞書にはコマンドやスクリプトの実行に関連するワードが登録されています。

(3) 通知メール

標的型攻撃メール検知設定の管理者への通知メールで、「送信する」を設定した場合、下記のような通知メールが管理者へ送信されます。さらに、「元メールを添付する」を設定した場合は、標的型攻撃メールと判定された元メールが通知メールに添付されます。

From: GUARDIANWALL <root@mg.example.com>
To: admin@mg.example.com
Subject: Notification: Detect malicious mail

標的型攻撃メールの疑いのあるメールを検知しました。
MSGID: LAA06493

----- 検知理由 -----

差出人詐称の疑いあるいは 公開メールアドレスへの送信
実行ファイルにファイル名偽装の疑い（連続する空白文字）
実行ファイルにファイル名偽装の疑い（RLO 制御文字）
実行ファイルにファイル名偽装の疑い（二重拡張子）
スクリプトが埋め込まれたリンクファイル

----- エンベロープアドレス (MAIL FROM:) -----
<sender@attacker.com>

----- エンベロープアドレス (RCPT TO:) -----
<to-info@example.com>

----- オリジナルメッセージヘッダー -----

From: Mr. X <sender@example.co.jp>
To: aaa@example.com
Date: 1 Jan 1999 11:04:59 +0900
Subject: 標的型攻撃サンプルメール

標的型攻撃メール
と判定した理由を
列挙
(自動生成)

MEMO

6 サポートツール

6-1 rescue.pl

検査サーバー（メール）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 [options]

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 <packedfile> : バックアップファイル <packedfile> からリストアする
- restorefull <packedfile> : 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 : mgwall-<バージョン番号>-<hostid>-<YYYYMMDDhhmmss>.tar.gz
mgwall-7.0.00-80fe7ea0-20051204154014.tar.gz の場合

→ バージョン番号 : GUARDIANWALL Ver7.0.00
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（メール）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/WALL/support/

(3) バックアップファイルの中身

- ① 検査・配送ルール
- ② MIME タイプ
- ③ キーワード
- ④ 通知文
- ⑤ グループ
- ⑥ 基本設定（基本、拡張、定型文含む）
- ⑦ 情報検査機能設定（基本、拡張含む）
- ⑧ メール保存機能設定（基本、タイムスタンプ含む）
- ⑨ 構成情報（スケジュール含む）
- ⑩ 各アカウント、権限ファイル
- ⑪ httpd.conf ファイル

(4) 注意点

- ・タイムスタンプ機能を使用している場合は、再度タイムスタンプライセンスファイルの登録が必要になります。
- ・設定リストア後は、検査サーバー（メール）の再起動を実施してください。
- ・リストア後のライセンスキーは、稼働中のライセンスキーに差し替えられます。
- ・旧ライセンスキーで稼働中の環境に対し、新ライセンスキーを含む設定バックアップファイルをリストアすることはできません。

6-2 watch.pl

検査サーバー（メール）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。使用する場合は、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 [options]

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 0.03
Swap free space: ok 2049 MB
Process "mw_mss" : ok alive
Process "mw_store" : ok alive
Process "Admin/httpd/bin/httpd" : ok alive
Disk free space "/opt/Guardian/WALL/mqueue" : ok 804 MB
Disk free space "/var/spool/mqueue" : ok 1134 MB
Disk free space "/opt/Guardian/Admin/logs" : ok 804 MB
Disk free space "/opt/Guardian/WALL/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/WALL/support/

(3) 監視対象

① 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。

② 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。

③ プロセス

初期値 : mw_mss
mw_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。

④ ディスク残容量

初期値 : /opt/Guardian/WALL/logs → 100 MB
/opt/Guardian/WALL/mqueue → 200 MB
/var/spool/mqueue → 200 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 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) メールが保留されない、キーワードが情報検査ログに記録されない

キーワード検査条件にキーワードを登録してキーワードを含むメールを送信したにも関わらず、期待したようにメールが保留されない場合は、以下の設定内容を確認してください。

内部ドメイン名	: デフォルトでは内部ドメイン以外から送信したものは検査対象にはなりません。
検査・配送ルール	: 適用される動作は、「 検査 」になっているか
キーワード検査条件	: 登録状態は「 本番 」になっているか

情報検査ログに記録されない、情報検査ログの記録条件（【メール】-「システム管理」-「情報検査機能設定」）もあわせてご確認ください。また、メールの条件によっては、検査・配送ルールの適用対象外になります。メールのヘッダーアドレス、エンベロープアドレスなどもあわせてご確認ください。

(2) メールが保存されない

メール保存ディレクトリを設定しているのにメールが保存されない場合は、「**保存対象**」の指定を確認してください。

「**保存対象**」の指定が「**検査・配送ルールで指定されたメールのみ保存**」の場合は、検査・配送ルールで保存と指定された動作が適用されたメールのみ保存します。「**保存対象**」の指定が「**保存しない**」の場合は、検査・配送ルールの動作設定で「**保存**」を選択しただけでは保存しません。

保存処理はデフォルトで1分間隔でアーカイブ処理を行っています。メールの配送を行った直後管理画面にアクセスしても、アーカイブ処理が完了していない場合は見ることができません。

(3) メール本文が閲覧できない

デフォルトの設定では情報管理者、部門情報管理者は保存メールの本文を閲覧する権限はありません。本文を閲覧する時は設定を変更してください。

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、WEBGUARDIAN 共通～**』の「6-2-1-4 情報管理者の権限リスト」（412 ページ）、「6-2-1-5 部門情報管理者の権限リスト」（424 ページ）、「6-2-1-3 アカウントの編集・削除」（411 ページ）をご参照ください。

(4) アップロード、ダウンロードができない

検査・配送ルール、MIME タイプ検査条件、キーワード検査条件をブラウザからアップロード、ダウンロードする機能にはブラウザの仕様により以下の制限があります。

- Microsoft Internet Explorer

マウスの左クリックではテキストファイルをダウンロードできません。ブラウザのフレーム内にテキストが表示されます。右クリック、「対象をファイルに保存」を選択してください。

- Netscape Navigator

アップロードする際は、日本語名の含まれるディレクトリ名、ファイル名を指定することはできません。

(5) GUARDIANWALL インストール後に sendmail の設定を変更する

以下の手順で、sendmail.cf の変更を行ってください。

① GUARDIANWALL の停止

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

② sendmail の停止

```
# /etc/init.d/sendmail stop
```

③ sendmail.cf の変更、確認

sendmail -bt 等で必ず変更後の内容が正しいことを確認してください。

また、sendmail 単独で起動し、メールの中継、(場合によっては当サーバーでの) 受信が正しく行われること、さらに、sendmail を MSP としてメールの送信が行えることを確認してください。

④ GUARDIANWALL の起動、確認

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

sendmail -q30m の起動も行われます。

ブラウザで情報管理者の管理画面にログインし、【共通】-「検査サーバー管理」-「状況確認」-【稼動状況】画面で稼動中となっていることを確認してください。



GUARDIANWALL をインストールしている環境では、書籍などで紹介されている、通常のメールサーバー管理等の sendmail の設定、起動手順をそのまま実行することはできません。

GUARDIANWALL 稼動状態で起動されている sendmail は SMTP 受信デーモンではありません。SMTP の受信は GUARDIANWALL が行います。sendmail は（メールがスプールされていれば）キューの再送処理を行うだけのデーモン（/usr/lib/sendmail -q30m）として起動しています。

(6) メールがループして送信できない

sendmail Ver8.12 以降を使用している場合は、「4-7 MSP の設定変更」-「(2) sendmail Ver8.12 以降」(62 ページ) をご参照ください。

(7) 障害時の復旧方法について

GUARDIANWALL 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、WEB-GUARDIAN 共通～』の「11 障害時の復旧方法」(482 ページ) をご参照ください。

MEMO