

# DaouOffice System Admin Guide



# DaouOffice System Admin Guide

Daou Japan



# 目次

目次	v
1. はじめに	1
1.1 Web管理者画面とは	1
1.2 Web管理者画面へ接続	2
Web管理者画面接続に必要な仕様	2
Web管理者画面へログイン/ログアウト	2
管理者情報変更	3
2. サマリー	5
3. システム	7
3.1 概要	7
3.2 サーバ管理	7
サーバの追加	8
サーバの変更	9
サーバの削除	9
3.3 ライセンス	9
3.4 アップデート	10
S/Wアップデート	11
アップデートファイル登録	11
アップデート	11
リリースノート	12
Proxyサーバ設定	12
3.5 サービス	13
メール	13
送受信環境	13
基本環境	13
送受信ドメイン書き換え	14
受信者アドレス書き換え	15
メール送信オプション	15

リレー許可ポリシー	16
送受信キューポリシー	17
予約メール	17
プロセス	18
受信サーバ	18
送信サーバ	18
配信サーバ	19
POPサーバ	19
IMAPサーバ	20
メール検索	21
性能チューニング	21
リターンメール(NDR)	22
メール添付管理	22
TMA連動	23
<b>4. ドメイン/サイト管理</b>	<b>25</b>
4.1 ドメインリスト	25
ドメイン追加	25
ドメイン変更	26
ドメイン削除	26
ドメイン検索	26
4.2 サイト一覧	27
サイトの追加	27
サイトの変更	29
サイトの削除	29
サイトの検索	29
サイト管理者画面に移動	30
4.3 サイトグループリスト	30
サイトグループ追加	30
サイトグループ変更	31
サイトグループ削除	32
サイトグループ検索	32
<b>5. セキュリティ</b>	<b>33</b>
5.1 共通	33
アンチウイルス	33
証明証	35
基本証明書	35
自己証明書	35
認証局証明書	36
APIアクセス	37

海外ログイン遮断許可設定	37
5.2 メール	38
アンチスパム	38
コンテンツフィルタ	38
許可/遮断ルールの追加	39
許可/遮断ルール変更	40
許可/遮断ルールの削除	41
許可/遮断ルールの設定	41
フィルタ検査	41
ライブアップデート	41
接続段階遮断	43
IP遮断	43
IPフィルタ	44
同時接続数制限	45
RBL	46
接続段階許可	47
SMTP段階遮断	47
DNS検査	48
SPF検査	48
送信者遮断	49
送信者フィルタ	50
受信者遮断	51
受信者フィルタ	51
同報メール応答遅延	52
SMTP段階許可	53
グループポリシー	54
グループポリシー追加	54
グループポリシー変更	55
グループポリシー削除	55
グループポリシーの適用設定	55
グループポリシー適用順位	55
グループポリシー検索	56
フィルタ情報ポリシー	56
フィルタ情報管理サーバ	56
ローカルサーバの許可	57
ローカル学習型フィルタ	57
フィルタ検索	57
情報漏洩防止	58
情報漏洩モニタリング	58

情報保護フィルタ	59
保護対象設定	62
遮断メール通知設定	63
情報漏洩防止機能のフォルダ管理	63
メール保存ポリシー	64
SSL/TLS設定	64
SMTP	64
POP	65
IMAP	66
5.3 WAS	66
アクセス制限	66
セッション検証	67
HTTPS設定	68
<b>6. 統計</b>	<b>69</b>
6.1 概要	69
統計情報の検索	70
統計情報のダウンロード	70
統計情報の印刷	71
6.2 メール	71
要約	71
正常メール	71
スパムメール	72
全段階	72
接続段階	72
SMTP段階	73
コンテンツ段階	74
フィッシングメール	74
ウイルスメール	75
POP	75
IMAP	76
6.3 システム	76
CPU	76
メモリ	76
ディスク	77
6.4 統計レポート	77
統計レポートの追加	77
統計レポート変更	78
統計レポートの削除	78
統計レポート設定	78



<b>7. モニタリング</b>	<b>79</b>
7.1 概要	79
7.2 送受信メールステータス	79
7.3 ログ	80
メールログ	80
メールログの検索	80
スパムメール/正常メール登録	81
メールログ更新	82
ログ設定	83
7.4 システムステータス	83
プロセスステータス	84
リソースステータス	84
メール処理ステータス	85
MTAスレッドステータス	85
遮断中のIPアドレス検索	86
キューモニタリング	87
キュー検索	87
キュー削除	88
キュー転送	89
7.5 お問い合わせ/警告メール	89
お問い合わせ	89
警告メール設定	89
<b>8. モバイル</b>	<b>91</b>
8.1 モバイルアプリのバージョン管理	91
モバイルアプリのバージョン追加	91
モバイルアプリのバージョン追加	92
モバイルアプリのバージョン削除	92
モバイルアプリバージョンフィルタリング	92
<b>9. その他</b>	<b>93</b>
9.1 IPグループ設定	93
IPグループ追加	93
IPグループ更新	94
IPグループ削除	94
9.2 初期化	94
9.3 保存期間設定	95
9.4 パスワード探し設定	95
<b>10. 管理者</b>	<b>97</b>
10.1 管理者リスト	97

管理者の追加	97
管理者の変更	98
管理者の削除	98
管理者検索	99
10.2 管理者ログ	99
管理者ログのリスト	99
管理履歴の検索	100
図目次	101

# 1. はじめに

---

## 1.1 Web管理者画面とは

管理者は、システムの環境設定、サイト（ドメイン）の登録など、システムを管理、運用するための一連作業が可能な権限を持つユーザです。管理者には、運用効率の向上のため、Webベースの管理コンソールを提供します。サーバ運用の経験がない管理者もWeb管理者画面を利用することで、簡単に運用することができます。

### Web管理者画面の主要機能

- 便利なWebベースの管理コンソール
- 60種類の統計情報の提供
- リアルタイムでのシステムモニタリング、スパム遮断ルールが簡単に設定可能
- リアルタイムでログモニタリング、検索機能をサポート
- 各種環境設定ファイルのバックアップ及び復元が可能
- サイト（ドメイン）別、グループ別、ユーザ別の環境設定及びメールサービスの設定が可能
- Webコンソールの有用性により、管理者の運用負担を最小化
- 管理者別の権限設定

### 管理者の種類

管理者(管理画面)は2つ種類があります。

- システム管理者- DaouOffice のモニタリング、セキュリティなどのシステムやサービス全体に関連する項目を設定することができます。  
システム管理にアクセス可能なユーザをシステム管理者とします。システム管理者は、管理者画面のすべてのサイトにアクセスできる権限があります。
- サイト管理者 - DaouOffice に登録されたそれぞれのサイト（ドメイン）を管理します。サイト管理にアクセスできるユーザをサイト管理者とします。各サイト（ドメイン）ごとに管理者を指定することが

できます。

サイト管理では、特定のサイト（ドメイン）に必要な環境とサービスを設定します。

## 1.2 Web管理者画面へ接続

### Web管理者画面接続に必要な仕様

Web管理者画面へ接続するためにはネットワークに繋がっているPC及びWebブラウザが必要です。 Web管理者画面へ接続可能なOS及びWebブラウザの種類とバージョンは次の通りです。

- Windows Vista , Windows7, Windows8
- Internet Explorer 9, 10 ,11
- ただし、IE 以外はサポートしません。

### Web管理者画面へログイン/ログアウト

DaouOffice Web管理者画面へ接続するためにはネットワークに繋がっているPC及びWebブラウザが必要です。

#### ログイン

Web管理者画面へログインする方法は次の通りです。

1. Webブラウザのアドレスバーに '**http://hostname:8000**' を入力します。 hostnameはDNSに登録されているWeb管理者画面のhostnameになります。
2. ログイン画面にて**アカウント**と**パスワード**を入力します。
  - アカウント - 管理者サーバへ接続するためのユーザアカウントです。システム管理者のデフォルトアカウントは'**mailadm@ドメイン**' です。
  - パスワード - 当該アカウントに対するパスワードを入力します。システム管理者のデフォルトパスワードは**tims**です。
3. アカウントとパスワードの入力後、Loginをクリックします。



セキュリティのためmailadmで最初ログインする際にはパスワード変更画面に移動します。



システム管理やサイト管理のログイン方法は全て同じです。ただし、管理者権限に応じて表示されるページ（システム管理又はサイト管理）に違いがあります。



ログインする際、画面上段で言語(日本語、韓国語)を設定することができます。

## ログアウト

ログアウトして管理者サーバのセッションを終了します。ログインしたWeb管理画面の右上にある**ログアウト**をクリックします。

## 管理者情報変更

画面右上にあるユーザ名をクリックすると、管理者情報を修正できる画面に移動します。

確認及び変更可能な項目は次のとおりです。

- 名前 - ログインしている管理者の名前が表示されます。
- 言語 - システム管理者画面で使用する言語を選択します。
- 1ページに表示するリスト数 - モニタリングなど1つの画面に表示されるリスト数です。
- 統計出力グラフ種類 - 統計画面に表示するグラフの種類を選択します。折れ線グラフと棒グラフから選択します。
  - 折れ線グラフ - 各項目の変化の推移を確認したいときに選択します。
  - 棒グラフ - 項目別の比較をしたいときに選択します。
- セッション維持時間 - 管理者がログイン後、指定した時間の間に入力等の動作をしない場合、自動的にログアウトする時間を選択、または入力します。



## 2. サマリー

---

サマリーではWeb管理者画面のメール統計及びシステムステータスを確認することができます。

### 通知

最近更新された現状、ストレージ使用率、プロセスの状態が表示されます。

### システム情報

DaouOffice がインストールされた日付、サーバのライセンス、バージョン情報が表示されます。



ライセンスの更新は、[システム > ライセンス]で行うことができます。

### モニタリング

送受信されたメールの統計とシステム状態情報が表示されます。

### メールトラフィック

- メール種類 - 正常メール、スパムメール、フィッシングメール、ウイルスメール
- 時間/期間 - 最近1日、最近1ヵ月



各メールの種類別の詳細な統計情報は、[統計]を参照してください。

### システムステータス情報

- メールプロセス - メールを送受信するデーモンの動作状態を表示します。
- Webサービス - ユーザのWebサービスの動作状態を表示します。
- 負荷率 - システム負荷率を表示します。
- CPU 使用率 - CPUの使用状況を表示します。
- Memory - メモリの使用状況を表示します。

- Disk - 各パーティション別ディスク使用状況を表示します。



システムの状態に関するより詳しい情報は、[モニタリング > システムステータス]を参照してください。



## 3. システム

---

### 3.1 概要

DaouOffice サーバが正常に動作するためには、各環境を優先的に設定する必要があります。**システム管理**では DaouOffice サーバのそれぞれの環境を設定することができます。

システムメニューで実行できる機能は次の通りです。

- DaouOffice が設置されたシステム情報を登録
- DaouOffice ライセンス管理
- DaouOffice バージョンアップデート
- DaouOffice 内部重要ファイルのバックアップ及び復旧
- DaouOffice サービスの環境設定

### 3.2 サーバ管理

サーバ管理では、DaouOffice が設置されたサーバ情報の確認、設定及び管理します。DaouOffice は複数台のサーバ (multi-host) でサービスを提供することができます。DaouOffice が複数台のサーバで構成された場合、各サーバ情報を全て登録することで、管理者画面を通じて一元管理することができます。

サーバ管理画面のリスト構成は次の通りです。

- サーバ名 - DaouOffice が設置されたサーバ名をFQDNで表示します。
- IPアドレス - DaouOffice が設置されたサーバの IPアドレスを表示します。

## サーバの追加

DaouOffice が設置されているサーバを追加します。DaouOffice が設置されていないサーバを追加することはできません。

1. Web管理者画面の[システム > サーバ管理] メニューをクリックします。
2. サーバリストで**追加**をクリックします。
3. サーバ追加画面で各項目を入力します。
  - サーバ名 - サーバ名を入力します。サーバのFQDNを入力します。 (例) tms.daou.co.jp
  - HOST ID - HOST IDを入力します。HOST IDはDaouOffice を設置する際に必要です。詳細については、購入先にお問い合わせください。
  - IPアドレス - IPアドレスを入力します。
  - 仮想IPアドレス - DaouOffice をFront End(Proxy機能) とBack End(メールサーバ機能)を分けて複数台のサーバで運用する場合、Back Endサーバはユーザのメールフォルダを保存するストレージに直接アクセスします。Back Endの複数サーバに対し、L4 Switchなどでロードバランシングを行うケースで設定します。Front Endは、L4 Switchにメールを転送しますが、このL4 SwitchのIPアドレスが、Back Endサーバの仮想IPアドレスになります。
  - メールストレージ - ユーザのメールフォルダとメールを保存するためのストレージサーバとして使用するかどうかを設定します。
    - 使用可否 - ストレージサーバとしての使用可否を選択します。DaouOffice が複数台のサーバで構成されている場合、ストレージを持つサーバ(Back End)と持たないサーバ(Front End)などに分けることが可能です。
    - Index FS - Index FSはユーザメールフォルダが作成されるディレクトリです。メールフォルダにアクセスしない、Front Endサーバとして運用するサーバには入力する必要はありません。Index FSは同時に複数の場所を指定することができます。
    - Data FS - Data FSはユーザメールが保存されるディレクトリです。Index FSと同様に、メールフォルダを運用しないサーバでは、入力する必要はありません。Data FSは同時に複数の場所を指定することができます。
  - WASのストレージ - カレンダー、掲示板、コミュニティ、アドレス帳の設定と、これらの機能で添付するファイル(Webメールの大容量添付は除く)を保存するためのストレージサーバとして使用するかどうかを設定します。
    - 使用可否 - ストレージサーバとしての使用可否を選択します。カレンダー、掲示板、コミュニティ、アドレス帳の設定と、これらの機能で添付するファイル(Webメールの大容量添付は除く)を保存するためのストレージですので、この機能を利用しない場合は、使用しないに設定してください。
    - Was FS - WAS FSは同時に複数の場所を指定することができます。
4. 設定完了後、**追加**をクリックします。

## サーバの変更

サーバ管理リストでサーバ情報を変更します。

1. Web管理者画面の[システム > サーバ管理] メニューをクリックします。
2. サーバリストで変更するサーバのサーバ名をクリックします。
3. サーバ変更画面で各項目を変更します。
4. 変更完了後、**変更**をクリックします。



HOST IDは変更できません。

## サーバの削除

サーバ管理リストでサーバ情報を削除します。

1. Web管理者画面の[システム > サーバ管理]メニューをクリックします。
2. サーバリストで削除するサーバにチェックを入れて、リストの上にある**削除**をクリックします。

## 3.3 ライセンス

DaouOffice は基本的にメール、アドレス帳、Webフォルダ、カレンダー、組織の機能を提供します。正規パッケージのほか、掲示板、コミュニティ、添付ファイルのプレビューなどの付加機能を使用するためには、別途ライセンスを購入後、登録する必要があります。

ライセンスは次の通りになります。

### 基本ライセンス

- ユーザライセンス: DaouOffice を利用するユーザ数を定義します。

### サービスライセンス

次のライセンスをそれぞれ登録することができます。ライセンスを登録するたびに、該当機能が有効になります。例えば、Socialライセンスを登録すると、掲示板、コミュニティ、予約/貸出、アンケート機能が有効になります。

- Social : 掲示板、コミュニティ、予約、アンケート
- Mobile : モバイルWeb、モバイルアプリ、同期化、PCメッセージャー

- Collaboration : レポート、業務、ToDo+

### 期間ライセンス

期間ライセンスは次の通りにSpamとVirusがあり、ライセンス期限が終了すると、新しいフィルタルールを更新することができません。

- Spam: スパムルールをアップデートするためのライセンスです。
- Virus: ウイルスのフィルタルールをアップデートするためのライセンスです。

### 付加機能ライセンス

- セキュアメール: メールを送信する時、パスワードを設定して送る機能です。受信者はメールを確認する際、パスワードを入力しないと、該当メールを確認することはできません。
- OTP(One-Time Password): ユーザが DaouOffice にログインする度にIDとパスワード以外、認証サーバを通じて得られたOPTパスワードをもう一度入力してログインする機能です。
- プレビュー: メール、掲示板、コミュニティ、レポート、アンケートにあるファイルをダウンロードせずに確認する機能です。

ライセンスのアップデート方法は次の通りです。

1. ライセンスファイルを購入先から入手してください。
2. システム管理者画面の[システム > ライセンス] メニューをクリックします。
3. 参照をクリックして、PCにあるライセンスファイルを選択してアップロードします。
4. 全てのライセンスファイルをアップロード後、登録をクリックします。



DaouOffice が複数設置されている場合は各サーバ別にライセンスをアップロードします。



ライセンスのアップデート（登録）後、[モニタリング>お問い合わせ/警告メール>警告メール]で使用可否を使用するに設定することを推奨します。ライセンスの満了期限が近付くと、メールでお知らせします。

## 3.4 アップデート

DaouOffice を最新のバージョンにアップデートしたり、アップデートする際に利用するProxyサーバを設定することができます。

## S/Wアップデート

特定のURLから更新ファイルをダウンロードしアップデートするか、取得した更新ファイルをアップロードしてオフラインでアップデートを行うことができます。



DaouOffice が複数台設置されている場合にはサーバ別にバージョンの情報を確認してアップデートを行ってください。

DaouOffice で提供する製品バージョン情報は次の通りです。

- 現在バージョン - 現在設置されているDaouOffice のバージョン
- アップデートファイルのバージョン - アップデートするためにアップロードしたDaouOffice パッケージ

## アップデートファイル登録

バージョンをアップデートするためにDaouOffice パッケージを登録します。

1. [システム > アップデート]のメニューをクリックします。
2. アップデートファイル登録のファイルを選択をクリックしてパッケージを選択した後、**確認**をクリックします。またダウンロードURL入力にパッケージのダウンロードサイトを入力後、**確認**をクリックします。



毎日0~1時の間にエージングデーモンが起動されて、アップデートとは関係なく指定された時刻にアップロードされたパッケージを削除しますので、ご注意ください。

## アップデート

DaouOffice の最新バージョンにアップデートします。アップデートするためにはDaouOffice パッケージをアップロードしないとけません。

1. システム管理者画面で[システム > アップデート] のメニューをクリックします。
2. アップデートファイルのバージョンを確認した後、**アップデート開始**ボタンをクリックします。
3. アップデート確認メッセージが表示されます。**確認**ボタンをクリックします



アップデートには数分~数十分がかかる可能性があります。



アップデート時に、必要に応じてDaouOffice サーバの再起動が必要な場合があります。サーバを再起動する必要がある場合には、再起動のメッセージが表示されます。

サーバを再起動すると、DaouOffice サービスが数分ほど中断されるので、ご注意ください。



DaouOffice のバージョンは**プラットフォーム. メジャー. マイナー**で行われます。たとえば、バージョンが8.4.0であれば8は、このプラットフォームのバージョン、4はメジャーバージョン、0はマイナーバージョンです。

メジャー以降のバージョンが更新された場合は、ライセンスを再登録する必要があります。ライセンス登録の方法は、ライセンスを参照してください。[3.3 ライセンス](#)を参照してください。



パッケージのアップロード後には、アップデート画面が表示されます。新しいパッケージをアップロードするためには**戻る**ボタンをクリックします。

## リリースノート

オフラインアップデート後には、該当バージョンのリリースノートが確認できます。



オフラインアップデートを実行した場合にのみ、リリースノートが表示されます。

1. システム管理者画面の **【システム > アップデート】** をクリックします。
2. 現在バージョンの横にある **リリースノート** をクリックします。

## Proxyサーバ設定

アップデートproxyサーバ設定はスパム及びウイルスフィルタとアップデート情報をインターネットを通じてアップデートを行う時、ウェブProxyサーバを経由する場合設定します。

Proxyサーバを使用する際、ID/パスワードの認証が必要な場合にはBasic Authのみサポートします。



Proxy認証を使用する時、パスワードに **「#」** 文字は使用できません。

Proxyサーバを設定する方法は次の通りです。

1. **【システム > アップデート】** のメニューをクリックします。

## 2. Proxyサーバ設定で次の項目を設定します。

- Proxyサーバ使用 - 使用可否を選択します。（デフォルト値：使用しない）
- Proxy認証 - Proxyサーバの認証の使用可否を選択します。認証方式はBASICです。（デフォルト値：使用しない）
- Proxy認証設定 - Proxyサーバ認証を使用する場合、表示されます。IDとパスワードを入力します。
- Proxyサーバ情報 - ProxyサーバのIPアドレスとポートを入力します。

## 3. テストボタンをクリックしてサーバとの接続状態を確認します。

## 4. 設定が完了されると、確認ボタンをクリックします。

# 3.5 サービス

## メール

メールを送受信する際に適用する基本ポリシーと、検索などの設定を行います。

## 送受信環境

### 基本環境

DaouOffice がメールを送受信する際に適用する基本ポリシーを設定します。

## 1. [システム > サービス > メール > 送受信環境 > 基本環境]をクリックします。

## 2. 基本環境の項目を設定します。

- 最大メールサイズ - 送受信できる最大メールサイズを入力します。設定したメールの最大サイズより大きいメールが送受信された場合、送受信を拒否します
- スпам検査最大メールサイズ - スпамを検索する最大メールサイズを指定します。設定した最大メールサイズより大きいメールは、スパム検査しません。（勸奨値は512KB以下です）
- 最大受信者数 - 一度のSMTP接続で受けつけることのできる最大同報受信者数を設定します。最大2000まで指定できます。
- 最大ホップ数 - 受信メールで許可できる最大ホップ数です。具体的にはメールヘッダーの‘Received’の最大許可数で、制限値を超えるとスパムメール及び正常ではないメールの可能性が高いため、フィルタルールによって処理されます。
- 最大セッション数 - 一度のSMTP接続で許可するメール最大件数を設定します。通常、スパム送信は一度の接続で大量のメールを送信するために、適切な値で設定することを推奨します。推奨値は20です。
- グリーティングメッセージ - 送信サーバへ応答するSMTP接続に対するメッセージです。使用者がメッセージ内容を定義できますが、デフォルトメッセージを使用することを推奨します。

- 添付ファイル名の長さ - 受信メールに添付されるファイル名の長さを制限します。
- 最大添付ファイル数 - 受信メールに添付されるファイル数を設定します。
- 送信IPアドレスをヘッダーに追加 - 送信元のIPアドレスをX-headerに追加する機能の使用可否を選択します。
- メールアドレス RFC検査 - メールアドレスがRFC標準に遵守しているかを検査します。RFC標準に遵守していない場合、受信拒否します。  
DaouOffice の独自仕様でIDに連続する二つのドット(.)は許可しますが、「%」と「&」は許可しません。この仕様はWebメール限定で適用されますが、MS OutlookまたはOutlook ExpressなどのPCクライアントでは適用されません。
- SMTP認証 - SMTP認証機能の使用可否を選択します。  
CRAM-MD5暗号化の方式をサポートします。ただし、CRAM-MD5を使用するためにはドメインのパスワード暗号化がClear TextまたはTWOFISHに設定されていなければなりません。
- 送信者存在可否検査 - メールを送信者がローカルドメインのユーザの場合、SMTPプロトコル上のMail Fromのメールアドレスが存在するか検索します。送信者が存在する場合のみメールが送信されます。
- 認証IDと異なるMail From拒否 - SMTP Authで利用したアカウント (ID) とMail Fromのアカウント (ID) が異なる場合、受信を拒否します。
- 受信者の存在を隠す - 受信者認証で受信者が存在しない場合、通常No Such Userというエラーメッセージを返します。使用するに設定した場合は、エラーメッセージを返さずに、当該メールを受信後削除します。これによって、存在しないメールアドレスを相手側に隠すことが可能です。無作為でメールを送信し、メールアドレスを収集するようなスパマー対策に有効です。ただし、正常な送信先からメールアドレスを間違えて送った際には、存在しないメールアドレスに対してリターンメール (NDR) を送信しないので、使用にはご注意ください。
- 受信者アドレスの重複削除 - エイリアスユーザと仮想メールアドレスを含めて、受信者に同一なメールアドレスがある場合、受信者が一通のメールのみ受信するかの可否を設定します。  
但し、1通のメールでエイリアスアカウント (Alias) が複数ある場合は、重複して受信するケースがあります。例えば、hr@example.comというエイリアスアカウントにjinji@example.comとrecruit@example.comが登録されている、そして、recruit@example.comもエイリアスアカウントにjinji@example.comが登録されている場合、hr@example.comとrecruit@example.com宛に来たメールに対しては、jinji@example.comは2通のメールを受信します。
- ユーザ別送信メールサイズ制限 - ユーザ別に送信できるメールサイズ制限の使用可否を選択します。  
ユーザ別送信メールサイズはSMTP認証を実施するメールクライアントプログラム (例: MS Outlook、MS Outlook Express、MS LiveMail、Eudora、Thunderbirdなど) を使用する場合のみ適用されません。Webメールは適用されません。

3. 設定が完了したら、**保存**をクリックします。

## 送受信ドメイン書き換え

SMTPの“Mail From”と“Rcpt To”コマンドにあるメールアドレスのドメイン部分を書き換えします。

1. [システム > サービス > メール > 送受信環境 > 送受信ドメイン書き換え] メニューをクリックします。
2. 送受信ドメイン書き換えを使用するかを選択します。
3. 使用するを選択した場合、受信変更前のドメインと変更後のドメインをテキストボックスに入力します。



。(例) `exampledomain.net exampledomain.com`

4. **追加**ボタンをクリックします。
5. 削除 - 書き換えリストから削除するには、ドメインを選択した後、**削除**ボタンをクリックします。
6. 設定完了後、**保存**ボタンをクリックします。

## 受信者アドレス書き換え

メール受信時のSMTPの“Rcpt To” コマンドにある受信者のメールアドレスを書き換えします。


1. [システム > サービス > メール > 送受信環境 > 受信者アドレス書き換え] メニューをクリックします。
2. 受信者アドレス書き換えを使用するかを選択します。
3. 使用するを選択した場合、書き換え前のアドレスと書き換え後のアドレスをテキストフォルダに入力します。(例) `before@exampledomain.net after@exampledomain.com`
4. **追加**ボタンをクリックします。
5. 削除 - 書き換えリストから削除するには、リストからメールアドレスを選択した後、**削除**ボタンをクリックします。
6. 設定完了後、**保存**ボタンをクリックします。

## メール送信オプション

メール送信オプションではメール送信時の分割受信者数（受信サーバに1回の接続で送信する受信者数）設定と、送信するメールを任意のサーバ（送信ゲートウェイサーバ）に指定することができます。また、特定のドメイン宛のメールを特定のサーバに送信することも可能です。

- 分割受信者数 - メールを送信する際の受信者数です。  
(例) 分割受信者数を30名に設定し、300通のメールを同時送信する場合、30通ずつ10回に分けて送信します。
- 送信ゲートウェイサーバ - DNSのMXレコードを参照せず、登録されているサーバにメールを送信します。メールを転送するメールサーバの情報を入力します。最大5件まで登録できます。  
(例) 分割受信者数を30名に設定し、300通のメールを同時送信する場合、30通ずつ10回に分けて送信します。複数の送信ゲートウェイサーバが登録されている場合、送信の順番は任意で決まります。
- 指定ドメインの送信サーバ - 外部ドメインにメールを送信する時、特定ドメインに対して送信サーバを指定できます。ドメイン別に最大10個まで設定できます。  
(例) 外部の特定ドメイン(`daou.co.jp`)に対して送信サーバを(`192.168.0.1`)を指定すると、宛先が該当のドメインと一致した場合、指定したサーバにメールを送信します。

メールの送信オプションを設定する方法は次の通りです。

1. [システム > サービス > メール > 送受信環境 > メール送信オプション] メニューをクリックします。
2. 各項目を設定します。
  - 分割受信者数 - メールを送信する際の、1回でメールサーバに送信する受信者数を入力します。
  - 送信ゲートウェイサーバ - 送信ゲートウェイサーバのIPアドレスとポートを入力して追加アイコンを()をクリックします。削除するには、リストでサーバを選択した後、削除アイコンをクリックします。

- 指定ドメインの送信サーバ - 送信サーバを指定するドメインと送信サーバのIPアドレスを入力して**追加**ボタンをクリックします。

3. 設定完了後、**保存**ボタンをクリックします。

## リレー許可ポリシー

メールのリレー許可ポリシーを設定します。受信者が外部ドメインの場合は、外部メールサーバにメールを送信します。外部にメールを送信できるユーザは認証が必要です。送信認証ができない場合、送信できるIPアドレスやメールアドレスを事前に設定することで、外部へのメール送信を許可することが可能です。

1. [システム > サービス > メール > 送受信環境 > リレー許可ポリシー]をクリックします。
2. 基本ポリシーで許可方法を選択します。リレー許可の基本ポリシーは次のような4つをサポートします。
  - 全てのリレーを許可する - 条件なしで、全てのリレーを許可します。この設定は全てのリレーを許可しますので、推奨しません。
  - 全てのリレーを許可しない - SMTP Authで許可されたユーザのみリレーを許可します。
  - 部分的にリレーを許可する - 基本的にリレーを拒否しますが、許可するIPアドレス、許可する送信者ドメイン、許可する受信者ドメインからのリレーを許可します。このポリシーの設定を推奨します。
  - 部分的にリレーを許可しない - 基本的にはリレーを許可しますが、許可しないIPアドレス、許可しない送信者ドメインからのリレーは拒否します。
3. 各リレーのポリシーによって詳細項目を設定します。
  - 詳細設定 - **部分的にリレーを許可する**を選択時に表示される項目です。
  - 許可するIP アドレス - **部分的にリレーを許可する**を選択時に表示される項目です。
    - リレーを許可するIPアドレスを登録します。許可するIPアドレスに登録されたIPアドレスから送信したメールは、認証なしで外部に送信されます。
    - 許可するIPアドレスに登録されたIPアドレスを削除または検索することができます。
  - 許可しないIPアドレス - **部分的にリレーを許可する**を選択時に表示される項目です。
    - 許可するIPアドレスに登録されているIPアドレスの場合でも、許可しないIPアドレスに登録するとリレーを拒否します。
    - 許可しないIPアドレスに登録されたIPアドレスを削除、または検索することができます。
  - 許可する送信者ドメイン - **部分的にリレーを許可する**を選択時に表示される項目です。
    - リレーを許可する送信者 (Mail From) ドメインを登録します。
    - 許可する送信者 (Mail From) ドメインに登録されたドメインを削除または検索することができます。
  - 許可する受信者ドメイン - **部分的にリレーを許可する**を選択時に表示される項目です。
    - リレーを許可する受信者 (Rcpt To) ドメインを登録します。
    - 許可する受信者 (Rcpt To) ドメインに登録されたドメインを削除または検索することができます。
  - 許可しないIPアドレス - **部分的にリレーを許可しない**を選択時に表示される項目です。
    - 許可しないIPアドレスを登録します。
    - 許可しないIPアドレスに登録されたIPアドレスを削除または検索することができます。
  - 許可しない送信者ドメイン - **部分的にリレーを許可しない**を選択時に表示される項目です。

- 許可しない送信者（Mail From）ドメインを登録します。
- 許可しない送信者ドメインに登録されたドメインを削除または検索することができます。

4. 設定完了後、**保存**ボタンをクリックします。

## 送受信キューポリシー

マルチサーバで運用する際にメールフォルダ側のサーバ障害、または外部のメールサーバの障害によって送信に失敗した場合、メールは一次的にキューに保存されます。送受信キューポリシーで送受信メールキューに溜まっているメールを処理する方法を設定します。



システム負荷が高い場合、リトライインターバルの間隔が遅れるか、リトライできない場合があります。処理できなかったキューに対しては、そのままキューのディレクトリに残ります。

送受信キューポリシーを設定する方法は次の通りです。

1. 送信または、受信のキューポリシーを設定します。
  - リトライインターバル - 再送信を試行する処理間隔を入力します。
  - 最大保存期間 - 送信または受信キューに保存される期間を入力します。最大値は7日で、推奨値は3日です。
2. 設定完了後、**保存**ボタンをクリックします。



最大保存期間を推奨値(3日)より長く設定するとシステムに障害を招く恐れがありますので推奨値の設定を推奨します。

## 予約メール

予約メールの予約可能期間や送信インターバルなどの設定を行います。

1. [システム > サービス > メール > 送受信環境 > 予約メール]をクリックします。
2. 予約メールを設定します。各項目の説明は次の通りです。
  - 最大予約可能期間 - 予約メールキューに保存する最大期間を指定します。ディスク容量などを考慮した上で、期間を設定してください。
  - 送信インターバル - 定期的に予約メールキューをチェックし、予約した時間にメールを送信します。実際の予約時間より、この送信インターバル時間分、遅れて送信されます。
  - 予約メールDB保存ディレクトリ - 予約メールの送信情報DBを保存するディレクトリを指定します。
  - 送信サーバ名 - 予約メールを送信する際に使用する送信サーバのホスト名またはIPアドレスを入力します。
  - 送信SMTPポート - 送信サーバのポートを指定します。
  - コネクションタイムアウト - 送信サーバとのタイムアウトを指定します。
3. 設定完了後、**保存**ボタンをクリックします。

## プロセス

各メールサーバシステムに関連するパラメータを設定します。

### 受信サーバ

受信サーバでは、メールを受信してユーザメールフォルダに転送するか、受信キューに保存します。

1. [システム > サービス > メール > プロセス > 受信サーバ]をクリックします。
2. 受信サーバのデフォルト環境を設定します。各項目の説明は次の通りです。
  - 最大スレッド数 - 同時に処理できる最大メールの数です。メールのトラフィックが多くなると、最大スレッド数まで同時に処理します。最大スレッド数を超えるトラフィックがある場合、外部からのSMTP接続ができなくなります。メールのトラフィックが少なくなると、スレッド数も減少します。
  - 開始スレッド数 - 受信サーバを起動する際のスレッド数です。
  - スレッド当り処理件数 - 1つのスレッドで処理するメール件数です。スレッドは、指定数までのメールを処理してから、使用リソースを返還し、プロセスを終了します。
  - 内部コネクションタイムアウト - TCP接続後、設定時間内にプロトコルの通信がない場合は接続を解除します。
  - 内部I/Oタイムアウト - TCP接続後、設定時間内にデータの入出力がない場合は接続を解除します。
  - Busyメッセージ応答時間 - SMTP接続要求に対し、Busyメッセージの応答遅延時間を入力します。
  - ルーティングプロトコル - メールフォルダを管理しているサーバ側の配信サーバ（1台の場合は同筐体の配信サーバ）への送信プロトコルです。TMTPは、DaouOffice の独自のプロトコルでSMTPより速く処理します。
  - ルーティングポート - 配信サーバのポート番号です。TMTPの場合、7777がデフォルトポートです。
  - MTA timeout - SMTPのプロトコル毎にタイムアウトを指定することができます。タイムアウト指定は**MTA timeout**タブで設定します。各プロトコルの段階は次の通りです。
    - connection, greeting, helo, mailfrom, rcptto, receiving\_data, endofsession, rset, handshaking, rcptauth
3. 設定完了後、**保存**ボタンをクリックします。

### 送信サーバ

メールを外部に送信する場合は、メールキューを送信キューに一時保存します。送信サーバは送信キューに保存されたメールを処理します。

1. [システム > サービス > メール > プロセス > 送信サーバ]をクリックします。
2. 送信サーバを設定します。各項目の説明は次の通りです。
  - 最大スレッド数 - 最大スレッド数を指定します。
  - 開始スレッド数 - 送信サーバ起動時のスレッド数を指定します。
  - 外部 I/Oタイムアウト - 外部サーバとのTCP接続後、設定された時間内にファイルの入出力がない場合は接続を解除します。
  - 外部コネクションタイムアウト - 外部サーバとのTCP接続後、設定された時間内にプロトコルの入

出力がない場合は接続を解除します。

3. 設定完了後、**保存**ボタンをクリックします。

## 配信サーバ

配信サーバは、ユーザのメールフォルダまでメールを配信する役割を担っています。同報で受信されるメールや512KB 以上のメールも処理します。

1. [システム > サービス > メール > プロセス > 配信サーバ]をクリックします。
2. 配信サーバを設定します。各項目の説明は次の通りです。
  - 最大ルーティングスレッド数 - 最大ルーティングスレッド数は、ユーザのメールフォルダへのメールの配信またはリターンメールを処理するスレッド数です。
    - 最大ルーティングスレッド数を指定します。
    - メールフォルダにメールを保存するRoutedスレッドは、受信サーバと配信サーバからメールを受信して処理しますので、最大ルーティングスレッド数は、最大Routedスレッド数の25%程度に設定することを推奨します。
  - 最大Routed スレッド数 - 受信キューに溜まったメールをユーザメールフォルダに保存するスレッド数です。
  - バックアップ スレッド数 - バックアップスレッドはRoutedスレッドが処理できずに残したメールキューを処理します。
    - バックアップスレッドの数を入力します。
  - スレッド当り処理件数 - 1つのスレッドで処理するメール件数です。スレッドは、指定数までメールを処理してから、使用リソースを解放し、プロセスを終了します。
  - ルーティング コネクション タイムアウト - TCP接続後に、指定された時間内にプロトコルの通信がない場合は、接続を解除します。
  - ルーティング I/O タイムアウト - TCP接続後に、指定された時間内に、データの入出力がない場合は、接続を解除します。
  - リトライインターバル - 受信キューに保存されたメールを処理するインターバルです。
3. 設定完了後、**保存**ボタンをクリックします。

## POPサーバ

POPサーバのプロセスパラメータを設定します。 POPサーバを設定する方法は次の通りです。

1. [システム > サービス > メール > プロセス > POPサーバ]をクリックします。
2. POP サーバを設定します。各項目の説明は次の通りです。
  - 最大スレッド数 - POPサーバの最大スレッド数を指定します。
  - 開始スレッド数 - POPサーバの起動時のスレッド数を指定します。
  - I/O タイムアウト - TCP接続後、設定された時間内にファイルの入出力がない場合は、接続を解除します。
  - ポート - POPのサービスポートです。デフォルト値は110です。マルチサーバで構成された場合、メールフォルダを直接アクセスするサーバのPOPサービスポートです。
  - プロキシポート - マルチサーバで構成された場合、POPプロキシサーバのサービスポートです。1台でサービスする場合、このポートは使用しません。

- 最大POP コマンド数 - 1つのPOP接続でクライアントから受けつける最大コマンド数です。指定値を超えた場合、接続を解除します。
- 認識できない最大コマンド数 - クライアントからのUnkownコマンド数です。指定値を超えた場合、接続を解除します。
- 管理者パスワード設定 - POPサーバに接続できるパスワードを入力します。POPプロトコルを利用してユーザのメールフォルダに接続する際、管理者パスワードを入力すると、当該ユーザのメールフォルダにログインできます。
- POPプロキシのIPアドレス - マルチサーバで構成された場合、POPプロキシサーバ以外のIPアドレスからは、POPサービスを提供しません。POPプロキシサーバのIPアドレスを入力します。

3. 設定完了後、**保存**ボタンをクリックします。



管理者パスワードを設定すると、全てのユーザアカウントに対してPOPログインが可能です。パスワードの設定には特に注意が必要です。

## IMAPサーバ

IMAPサーバのプロセスパラメータを設定します。IMAPサーバを設定する方法は次の通りです。

1. [システム > サービス > メール > プロセス > IMAPサーバ]をクリックします。
2. IMAPサーバを設定します。各項目の説明は次の通りです。
  - 最大スレッド数 - IMAPサーバの最大スレッド数を指定します。
  - 開始スレッド数 - IMAPサーバの起動時のスレッド数を指定します。
  - I/O タイムアウト - TCP接続後、設定された時間内にファイルの入出力がない場合は、接続を解除します。
  - ポート - IMAPのサービスポートです。デフォルト値は143です。マルチサーバで構成された場合、メールフォルダを直接アクセスするサーバのIMAPサービスポートです。
  - プロキシポート - マルチサーバで構成された場合、IMAPプロキシサーバのサービスポートです。1台でサービスする場合、このポートは使用しません。
  - 最大IMAPコマンド数 - 1つのIMAP接続でクライアントから受けつける最大コマンド数です。指定値を超えた場合、接続を解除します。
  - 最大認識不可能なコマンド数 - クライアントからのUnkownコマンド数です。指定値を超えた場合、接続を解除します。
  - 管理者パスワード設定 - IMAPサーバに接続できるパスワードを入力します。IMAPプロトコルを利用してユーザのメールフォルダに接続する際、管理者パスワードを入力すると、当該ユーザのメールフォルダにログインできます。
  - IMAPプロキシのIPアドレス - マルチサーバで構成された場合、IMAPプロキシサーバ以外のIPアドレスからは、IMAPサービスを提供しません。IMAPプロキシサーバのIPアドレスを入力します。
3. 設定完了後、**保存**ボタンをクリックします。



管理者パスワードを設定すると、全てのユーザアカウントに対してIMAPログインが可能です。パスワードの設定には特に注意が必要です。



## メール検索

Webメールでメールの検索時、検索可能なメールの検索範囲、メールのサイズ、添付ファイルの拡張子を設定することができます。

1. [システム > サービス > メール > メール検索]をクリックします。
2. 検索エンジンの項目を設定します。
  - 検索範囲 - メール検索時、メール本文と添付ファイルの検索可否を選択できます。
    - 本文の内容まで - 添付ファイルの内容は検索しません。
    - 添付ファイルの内容まで - 添付ファイルの内容まで検索します。
  - 検索可能な最大メールサイズ - 検索可能なメールのサイズを指定します。サイズを大きく設定した場合、システムの負荷が高くなる恐れがあります。デフォルト値は10MBです。
  - 検索可能なファイルの拡張子 - 添付ファイルの内容まで検索時、添付ファイルの内容が検索可能な添付ファイルの拡張子を選択します。

現在サポートする添付ファイルの拡張子は次の通りです。

  - \*.chm, \*.doc, \*.docx, \*.dwg, \*.htm, \*.hwd, \*.hwp, \*.html, \*.jtd, \*.mdi, \*.mht, \*.msg, \*.pdf, \*.ppt, \*.pptx, \*.rtf, \*.sql, \*.sxc, \*.sxi, \*.txt, \*.wpd, \*.xls, \*.xlsx, \*.xml
  - 追加 - リストでファイルの拡張子の選択後、追加(➤)をクリックします。
  - 削除 - 追加されたリストで削除するファイルの拡張子の選択後、削除(➤)をクリックします。
3. メール検索の設定完了後、**保存**ボタンをクリックします。



検索範囲を本文または添付ファイル内容に選択した後、キーワードを英語に入力した場合には中間文字列の検索ができません。空白文字(space)に区別されて初文字列を入力しないと検索できません。(例) testという文字列を検索するためにはtesまたはtestを入力します。estを入力すると検索できません。



本文または添付ファイルの内容まで検索を設定した以降に受信されたメールから検索できます。設定した以前に受信したメールは検索できません。

## 性能チューニング

DaouOffice の管理者がパフォーマンスと関連したオプションを直接設定できます。パフォーマンスと関連されたオプションは次の通りです。

- 使用者のインデックス作成周期 - 使用者のインデックスが作成される周期を指定します。設定されている数のメールが受信される場合インデックスを作成します。
- 複数宛メールを1件のみ保存 - 同報メールの場合、元ファイルのみディスクに保存して他のメールは元ファイルのハードリンクを作成して使用します。



性能チューニングのオプションはシステムに及ぼす影響が大きいためパフォーマンスチューニングをしたい場合、製品サポートセンターにお問い合わせください。

性能チューニングを設定する方法は次の通りです。

1. [システム > サービス > メール > 性能チューニング]をクリックします。
2. 使用者のインデックス作成周期を入力します。
3. 複数宛メールを1件のみ保存の使用可否を選択します。
4. 設定完了後、保存ボタンをクリックします。

## リターンメール(NDR)

DaouOffice では何らかの理由で送受信できなかったメールは、リターンメール (NDR) として返送されます。返送される理由は、存在しない受信者、メール容量の超過、メールサーバの障害などがあります。リターンメール (NDR) は外部に送信したメールの場合のみ適用されます。

リターンメールで既定義された変数は次の通りです。

- \$subject: リターンされる元メールの件名
- \$reportmta: 返送メールを送信するMTAホスト名
- \$recipient: 元メール受信者
- \$status: SMTP状態コード (例) 4.2.1 <domain> Service not available 、 closing transmission channel
- \$diagnostic: 返送の理由 (例) 550 Don't send spam.

リターンメール作成方法は次の通りです。

1. 各項目を入力します。
  - 件名 - 返送メールの件名を入力します。あらかじめ設定されている件名の使用を推奨します。
  - 送信者 - 送信者のメールアドレスを入力します。デフォルトでは postmaster@デフォルトドメインでメールが送信されます。
  - 本文 - リターンメールの本文を作成します。
  - メールの原文を含む - メール原文を含む可否を選択します。使用するを選択すると、元メールが添付ファイル型式で送信されます。
2. 設定完了後、保存ボタンをクリックします。

## メール添付管理

メールの添付ファイルに関連する設定を行います。

1. システム管理者画面の[システム > サービス > メール > メール添付管理]をクリックします。
2. 添付ファイル関連項目と自動ログアウト時間を設定します。



○ 添付ファイル - メールへの添付ファイルに対するオプションを設定します。

- 大容量添付ダウンロード期間 - 添付ファイルをメールに添付せずに、そのリンクのみ送る（大容量添付）ことが可能です。大容量添付ファイルをダウンロードできる期間を入力します。この期間が過ぎると、メール受信者も該当添付ファイルのダウンロードができません。
- 大容量添付ダウンロード回数 - 大容量添付ファイルをダウンロードできる回数を制限します。
- 通常添付最大サイズ - アップロード可能な通常添付ファイル（大容量添付を利用しない場合）のサイズを入力します。ファイルサイズ単位はMBです。最大値は100MBで、推奨値は20MBです。
- 大容量添付最大サイズ - アップロード可能な大容量添付ファイルの最大サイズを入力します。ファイルサイズ単位はMBです。最大値は1024MBで、推奨値は500MB以下です。
- 添付ファイルアップロード時Ez Uploadの使用可否 - メール、Webフォルダ、掲示板などで、ファイルアップロード時、ドラッグ&ドロップでファイルを添付する機能の使用可否を選択します。

3. 設定が完了しましたら、**保存**ボタンをクリックします。



大容量添付ファイルの最大サイズの最大値を設定するとWebメールのサービスに大きな障害が発生する可能性がありますので推奨値をご利用ください。

## TMA連動

メールアーカイブ（Archiving）製品であるTerrace Mail Archiveとの連動設定を行います。Terrace Mail Archive製品以外のアーカイブ製品とは連動できません。

Terrace Mail Archiveサーバの連動設定方法は次の通りです。

1. [システム > サービス > メール > TMA連動]をクリックします。
2. TMA連動の各項目を設定します。

○ 基本環境

- 使用可否 - Terrace Mail Archiveサーバと連動可否を選択します。
- 保存詳細オプション - スпамメールとウイルスメールのアーカイブ可否オプションを設定します。
- アーカイブサーバ情報 - アーカイブサーバに使用されるTerrace Mail Archiveサーバを登録します。サーバ名 - ホスト名またはIPアドレスを入力します。ポート - ポートを入力します。
- サーバ情報の入力後、**テスト**ボタンをクリックしテストを行います。テストの成功後、**追加**ボタンをクリックします。

○ シングルサインオン（SSO）

- 使用可否 - アーカイブセンタ（TMAの一般ユーザ画面）ログイン時にSSO（Single Sign On）方式の使用可否を選択します。
- DES暗号化キー - アーカイブセンタ接続時の暗号化キーを設定します。

TMAの[環境設定>認証設定]のSingle Sign On（SSO）で設定したDES暗号化キーを設定してくだ

さい。

■ SSL使用可否 - SSO接続時に、SSLの使用可否を設定します。

3. 設定完了後、**保存**ボタンをクリックします。

## 4. ドメイン/サイト管理

---

### 4.1 ドメインリスト

パッケージを設置する際、ドメインを入力します。該当ドメインはデフォルトドメインといいます。基本的にドメインリストにはデフォルトドメインが表示されます。

サイトを追加するには先にサイトで使用するドメインを作成しなければなりません。ドメインリストでデフォルトドメイン以外追加したドメインを変更または削除することができます。

### ドメイン追加

ドメインを追加する方法は次の通りです。

1. システム管理者画面の [ドメイン/サイト管理 > ドメインリスト] をクリックします。
2. ドメインリスト上段にある **追加** ボタンをクリックします。ドメイン追加画面に移動します。
3. ドメイン追加画面で各項目の情報を入力します。
  - ドメイン名 - ドメイン名を FQDN で入力します。（例） daou.co.jp
  - ログイン方法 - ログインする際、ユーザを区別するため、入力しなければならない情報を選択します。
  - 仮想ドメイン - 該当ドメインに所有する仮想ドメインアドレスを入力後、**追加** ボタンをクリックします。

仮想ドメインとは上記で入力したドメインが使用する全ての情報を同じく使用できるドメインのことです。例えば、daou.co.jp というドメインを daou.com の仮想ドメインに設定すると、daou.co.jp と daou.com というドメインを同じドメインで取り扱い処理します。
  - ユーザ別仮想ドメイン - 上記で指定したドメインはこのドメインの全てのユーザに同じく適応されます。ユーザ別に違う仮想ドメインを設定する場合は **ユーザ別仮想ドメイン** に該当ドメインを入力します。

サイト管理者はユーザの仮想ドメインをここで入力されたドメイン中選択して設定することができます。

4. 入力が完了しましたら、**追加**ボタンをクリックします。



ドメイン名、ドメインWebアドレス、ログイン方法は必須入力項目です。

## ドメイン変更

ドメインリストでドメイン情報を変更します。ただし、サイトで使用中のドメインは変更することはできません。

1. システム管理者画面の【ドメイン/ サイト管理>ドメインリスト】をクリックします。
2. ドメインリストで変更するドメイン名をクリックします。
3. ドメイン変更画面で各項目情報を変更します。
4. 情報の変更が完了しましたら、**保存**をクリックします。



ドメイン名を変更する際、変更までのドメイン情報の統計及びログ情報は初期化されます。

## ドメイン削除

追加したドメイン中使用しないドメインを削除します。デフォルトドメインと使用中のドメインは削除することはできません。

1. システム管理者画面の【ドメイン/サイト管理 > ドメインリスト】をクリックします。
2. ドメインリストで削除するドメインを選択後、**削除**ボタンをクリックします。



パッケージを設置する際、入力したドメインがデフォルトドメインです。デフォルトドメインは色がついて、ドメインリストで簡単に探すことができます。

## ドメイン検索

登録されたドメインを検索することができます。登録されたドメインが多い場合は検索機能を利用してドメインを検索することで簡単に探すことができます。

1. システム管理者画面の [ドメイン/サイト管理 > ドメインリスト] をクリックします。
2. ドメインリストの上段にある検索ウィンドウで検索キーワードを入力します。検索キーワードにはドメインを入力します。  
(例) daou, daou.co.jp
3. Enterキーまたは**検索**ボタンをクリックします。

## 4.2 サイト一覧

サイト現況を確認して管理します。またはサイト管理者画面に移動して各サイトの掲示板、Webフォルダ、アドレス帳、組織図等を管理することができます。

### サイトの追加

サイト（ドメイン）を追加します。

1. サイト管理者画面の [ドメイン/サイト管理 > サイト一覧] をクリックします。
2. サイト一覧の上段にある**追加**をクリックします。サイト追加画面に移動します。
3. サイト追加画面で各項目の情報を入力します。
  - サイト機能情報
    - ドメイン名 - サイトで使用するドメインを選択します。ドメインは [ドメイン/サイト管理 > ドメインリスト] で確認または追加することができます。  
サイトの追加が完了しましたら、ドメイン情報は変更することができません。
    - サイト名 - サイトの機関や会社名を入力します。
    - 接続URL - サイトを接続URLを入力します。
    - サイト Indexfs / Datafs - メールホストを選択すると該当ホストのIndexfs リストと Datafs が表示されます。Indexfsと Datafsを選択後、**追加**ボタンをクリックします。  
Indexfsはユーザメールフォルダが作成されるディレクトリで、Datafsはユーザのメールが保存されるディレクトリです。Indexfsと Datafsは同時に複数の場所を指定することができます。
    - 最大ユーザ数 - サイトで利用できる最大ユーザ数を入力します。サイトの最大ユーザ数は[システム > ライセンス]で登録したアカウントライセンス数を超過して入力することはできません。
    - パスワード暗号化 - サイトのユーザパスワードの暗号化方式を選択します。
    - トータルアカウント容量 - サイトで利用できるメールの容量とWebフォルダの合計容量を入力します。本サイトで、すべてのアカウントが利用できるメール容量とWebフォルダの容量を合計した値です。  
最小 2GBを入力しなければなりません。

- 共有容量 - パブリックフォルダ、掲示板、コミュニティ内の掲示板、レポート、タススで添付ファイルを保存できる容量を入力します。共有容量を超えると、パブリックフォルダ、掲示板、コミュニティ内の掲示板、レポート、タススで添付ファイルを添付できないように設定することができます。

共有容量は掲示板、レポート、タスク、Webフォルダの使用量で、該当機能を使用しなくても容量に含まれます。

- 共有容量超過警告送信 - **共有容量**が設定されると表示されるメニューです。共有容量を超えた場合、容量超過に対し警告メールを送信する可否を選択します。警告メールはシステム管理者とサイト管理者に一日一回送信されます。
- 共有容量超過警告比率 - **共有容量**設定されると表示されるメニューです。共有容量超過警告メールを送信する比率を入力します。例えば、**共有容量超過警告比率**に90を入力すると、設定された共有容量の90%が使用された場合、警告メールが送信されます。
- 有容量超過時の措置 - **共有容量**設定されると表示されるメニューです。共有容量を超過すると、自動的にパブリックフォルダ、掲示板、コミュニティ内の掲示板、レポート、タスクなどでファイルをアップロードできなようにすることができます。容量超過際にファイルをアップロードできないようにするには**共有容量超過時の措置**を使用するに設定します。

最小10GB以上を入力しなければなりません。

#### ○ 提供サービス

- メールサービス - 該当サイトで使用するメールサービスを選択します。
- 各メニューの使用可否を選択します。**使用しない**を選択すると、サイト管理及びWebサービスに接続する際、該当メニューは表示されません。
- 海外ログイン遮断 - 海外からの接続を許可するかどうか選択します。  
海外ログインを遮断しても **[セキュリティ > 海外ログイン遮断許可設定]**でIPを登録すると、特定IPのアクセスは許可することができます。

#### ○ サイト追加情報

- 担当者 - サイトの運用担当者名を入力します。
- 電話番号 - サイト所有機関の運用担当者の直通電話番号を入力します。

#### 4. 入力完了しましたら、**保存**をクリックします。



ドメイン名、サイト名、ドメインIndexFS/Datafs、最大ユーザー数は、必須入力項目です。



一つのドメインに複数のサイトを追加することは可能ですが、一つのサイトに複数のドメインを使用することはできません。一つのドメインに複数のサイトを追加する場合はサイト別の統計はサポートしません。



アカウントを追加する度にトータルアカウント容量が超過されていないことを確認します。トータルアカウント容量が超過した瞬間からはアカウントを追加することはできません。  
パブリックフォルダ、掲示板、コミュニティ内の掲示板、レポート、タススで使用する量を計算して、共有容量が超過していないことを一日一回確認します。指定された共有容量を超過した場合はシステム管管理者とサイト管理者に警告メールが送信されます。



提供されるサービスは登録されたライセンスに依存します。例えばSocialサービスライセンスが登録されていない場合は掲示板、コミュニティ、予約、アンケートのメニューは表示されません。ライセンスに対する詳細の説明は[3.3 ライセンス](#)を参照してください。



海外からのログインを遮断するため、一日一回自動的にIP情報を更新します。手動で更新することはできません。

## サイトの変更

サイト（ドメイン）の情報を変更します。

1. システム管理者画面の **[ドメイン/サイト管理 > サイト一覧]** をクリックします。
2. サイト一覧で変更するサイト名をクリックします。
3. サイト変更の画面で各項目の情報を変更します。ただし、ドメインは修正することはできません。
4. 情報の変更が完了しましたら、**変更** ボタンをクリックします。

## サイトの削除

登録されているサイト（ドメイン）を削除します。



サイトを削除すると、サイトに関連するデータ（メール、掲示板、コミュニティ、Webフォルダなど）がすべて削除されます。

1. システム管理者 **[ドメイン/サイト管理 > サイト一覧]** をクリックします。
2. サイト一覧で削除するサイトを選択後、**削除** ボタンをクリックします。

## サイトの検索

ドメインやサイト名で検索します。登録されたサイトが多い場合は、検索を利用してサイトを簡単に探すことができます。

1. システム管理者画面の **[ドメイン/サイト管理 > サイト一覧]** をクリックします。
2. サイト一覧の右上にある検索ウィンドウに検索キーワードを入力します。検索キーワードにはドメイン又はサイト名を入力します。

(例) daou, daou.co.jp, ダウジャパン

3. Enterキーを押すか、**検索**をクリックします。

## サイト管理者画面に移動

サイト管理者画面に移動すると、各サイトのメール、掲示板、Webフォルダ、コミュニティ、組織図などの対して設定を確認または変更することができます。

サイト管理者画面に移動する方法は次のとおりです。

1. システム管理者画面の [ドメイン/サイト管理 > サイト一覧] をクリックします。
2. サービスを管理するサイトの **サイトへ移動** をクリックします。



サイト管理者はサイト管理画面のみアクセス可能です。システム管理者はシステム管理画面とサイト管理画面、両方アクセス可能です。

## 4.3 サイトグループリスト

一つのシステムに2個以上のサイトを作成して、該当サイトをグループ会社の組織に構成することができます。グループ会社の組織図を共有することができ、兼職処理を介して、柔軟に二つのサイトに移動することができます。

### サイトグループ追加

二つ以上のサイトグループを生成することができ、サイトグループを追加する方法は次の通りです。

1. システム管理者画面の [ドメイン/サイト管理 > サイトグループリスト] をクリックします。
2. サイトグループリスト上段にある **追加** をクリックします。サイトグループ追加画面に移動します。
3. サイト追加画面で各項目の情報を入力します。
  - サイトグループ基本情報
    - サイトグループ名 - サイトを一つに統合する **グループ名** を入力します。
    - サイトマッチング - **グループに含まれるサイト** を選択後、**矢印アイコン** をクリックして、追加します。
  - 兼職者リスト



- 兼職者追加 - 一人多数のサイトに所属されている場合、兼職者で設定することができます。  
追加をクリックして、各サイトで兼職に登録されているユーザを選択後、矢印アイコンをクリックして追加します。確認をクリックします。
- 兼職者削除 - 兼職者リストで削除する対象をチェックした後、削除をクリックします。

○ 兼職者以外組織図共有

- 組織図共有者 - グループサイトの組織図を照会できる共有対象者を選択します。
  - ・ 選択しない - 兼職者のみ組織図を共有します。
  - ・ 指定ユーザ - ユーザ、部署、職位、職級、役職、ユーザグループ別で組織図共有者を設定することができます。
  - ・ 全ユーザ - グループに所属したサイトのすべてのユーザが組織図を共有します。
- 共有範囲 - 組織図共有対象者には2つの方法で組織図を共有します。
  - ・ 組織図と検索提供 - グループ会社の全部署情報を公開します。
  - ・ 検索のみ提供 - 部署情報のツリー構成は公開しません。検索のみで部署及びユーザを確認することができます。



兼職者は所属されているサイトの組織図を確認することができます。ただし、所属されているサイトで組織図の接続を拒否する設定になっている場合は組織図を確認することができません。



兼職者はサービスにログイン後、左上段のロゴをクリックして、自身に所属したサイトを自由に移動することができます。



兼職者と組織図共有者はサービスにログイン後、左下の組織図を通じて、グループサイトの組織図を確認することができ、モバイル及びPCメッセージャーで他のサイトのユーザとチャットすることが可能です。

## サイトグループ変更

サイトグループリストでサイトグループ情報を変更します。

1. サイト管理者画面の[ドメイン/サイト管理 > サイトグループリスト]をクリックします。
2. サイトグループリストで変更しようとするグループの名前のクリックします。
3. サイトグループ変更画面で各項目の情報を変更します。
4. 情報変更が完了しましたら、変更をクリックします。

## サイトグループ削除

登録したサイトグループを削除します。

1. システム管理者画面の[ドメイン/サイト管理 > サイトグループリスト]をクリックします。
2. サイトグループリストで削除しようとするサイトグループを選択後、**削除**をクリックします。

## サイトグループ検索

サイトグループ名で検索します。登録されているグループが多い場合、検索を利用して、サイトを簡単に探すことができます。

1. サイト管理者画面の[ドメイン/サイト管理 > サイトグループリスト]をクリックします。
2. サイトグループリストの上段にある検索欄に検索キーワードを入力します。検索キーワードにはグループ名を入力します。
3. Enterを或いは**検索**をクリックします。

## 5. セキュリティ

---

### 5.1 共通

#### アンチウイルス

受信又は送信されるメールに、ウイルスが含まれているか否かを検査して遮断します。検査するメールの最大サイズを設定して当該サイズ以下のメールのみ検査し、サイズ以上のメールは通過させます。ウイルス感染は各ユーザに甚大な悪影響を及ぼす可能性もあるので、必ずウイルスメール検査を行うようにしてください。



添付ファイルに暗号化されたパスワードがある場合は開封できず、ウイルス検査の対象とはなりませんのでご注意ください。

ウイルスフィルタの使用方法は次の通りです。

- メールウイルス検査 - 送受信メールにウイルスが含まれるかどうか検査します。
- ウイルスお知らせメール - ウイルスお知らせメールはウイルス送受信に対する警告メールなので、処理方法に関係なく設定した受信対象メールアドレスにお知らせメールが送信されます。
- 添付ファイル検査 - メールに添付したファイルにウイルスが含まれるかどうか検査します。
- ウイルスフィルタ - ウイルスフィルタの更新状況を確認して、更新周期の設定、或いは手動で更新することができます。

アンチウイルスを使用するための設定方法は次の通りです。

1. システム管理者画面の【セキュリティ > 共通 > アンチウイルス】をクリックします。
2. 設定方法は次の通りです。
  - 使用可否(推奨: 使用する) - ウイルス検査の使用可否を選択します。

- 最大検査メールサイズ(推奨: 5MB) - ウイルスを検査するメールの最大サイズを入力します。  
入力したサイズと同じか小さい場合のみウイルス検査を実行します。
  - 検査失敗時の処理ポリシー - ウイルス検査に失敗した時の処理ポリシーを選択します。
    - 送信 - ウイルス検査に失敗したメールを送信
    - タグ - メール件名の前にタグを追加して送信
  - ウイルス検査に失敗するケースは下記の通りです。
    - ウイルスサーバ (エンジン) に接続できない場合
    - パスワードがかかったファイルの場合
3. ウイルスお知らせメールの送信設定は次の通りです。
- 使用可否(推奨: 使用する) - ウイルスお知らせメールの受信可否を選択します。
  - お知らせメールの受信対象 - お知らせメールの受信対象(送信者, 受信者, 送信者+受信者)を選択します。
  - 送信者メールアドレス - ウイルスお知らせメールを送信する送信者のメールアドレスを入力します。
4. 添付ファイル検査の設定方法は次の通りです。
- 添付ファイル検査の使用可否 - 添付ファイル検査の使用可否を選択します。ここに記載している添付ファイルはメールに添付されているファイルだけではなく、掲示板、コミュニティに添付するファイルがすべて含まれております。
  - 検査時期(推奨: アップロード際検査使用、ダウンロード際検査使用しない) - 添付ファイルをメール、掲示板、コミュニティ、Webフォルダにアップロード、またはダウンロードする際にウイルス検査を実行するかをチェックします。  
添付ファイルをダウンロードする際、ウイルス検査をすると、添付ファイルをアップロードした後に追加されたウイルスパターンも検索できる利点がありますが、ファイルをダウンロードする度にウイルス検査をしますので、システムに負荷が高くなる可能性があります。
  - 最大検査サイズ - ウイルスを検査する添付ファイルの最大サイズを入力します。  
入力したサイズと同じか小さい場合のみウイルス検査を実行します。
5. 設定が完了しましたら**保存**ボタンをクリックします。



DaouOffice のパッケージにウイルスエンジンが含まれていない場合があります。ウイルスエンジンがパッケージに含まれていない場合は、ルールの上アップデート可否を確認した時間情報を取得できないため、ウイルスエンジンのアップデートの時間が表示されません。



ウイルスメールに対処するため、アップデート周期を**1時間毎**に設定するのが推奨します。



**最近アップデート時間**は直近のウイルスフィルタをアップデートした日付と時間となりますので、アップデートされていない場合は**最近アップデート時間**は変更されません。

## 証明証

SSL (Secure Socket Layer) プロトコルはWeb上のセキュリティ通信のためSSLで暗号化された情報をやり取りするプロトコルです。管理コンソール及びWebメールの接続にHTTPS通信を行い、データを保護します。

SSLプロトコルの暗号化に使用する証明書の種類は次の通りです。

- 基本証明書
- 自己証明書
- 認証局証明書

次はそれぞれの証明書を設定する方法に対して説明します。



証明書のファイルの拡張子は `.cer` のみサポートします。



DaouOffice がマルチサーバで構成する場合、各サーバ毎に証明書を登録する必要があります。

## 基本証明書

DaouOffice で提供する基本証明書です。有効期間は10年です。

1. システム管理者画面の **[セキュリティ > 共通 > 証明書]** をクリックします。
2. サーバを選択します。
3. **証明書種類** を **基本証明書** に選択します。
4. **保存** をクリックします。
5. 証明書を適用するためWebサーバの再起動可否メッセージが表示されます。**確認** ボタンをクリックします。

## 自己証明書

公認認証機関の証明書ではなく、独自に発行された証明書です。自己証明書の有効期間は管理者が指定することができます。

公認認証機関の証明書ではないため、SMTPで認証局証明書を要求するサーバからは拒否される場合もあります。Outlook等のメールクライアントアプリケーションでは警告メッセージが表示されることもあります。

自己証明書を設定する方法は次の通りです。

1. システム管理者画面の **[セキュリティ > 共通 > 証明書]** をクリックします。
2. サーバを選択します。

3. **証明書種類**を**自己証明書**に選択します。
4. 自己証明書を作るための必要な情報を入力します。
  - Common name - 該当メールサーバのドメインを入力します。
  - Country - 国を選択します。
  - その他情報をを入力します。
5. **保存**ボタンをクリックします。
6. 証明書を適用するためWebサーバの再起動可否メッセージが表示されます。**確認**ボタンをクリックします。

## 認証局証明書



公認証明機関（Thawte、 Verisign 等）で発行された証明書です。公認証明機関の証明書を作成するためには、Private keyとCSR（Certificate signing request）が必要です。

認証局証明書を使用する方法は次の通りです。

1. システム管理者画面の[セキュリティ > 共通 > 証明書]をクリックします。
2. サーバを選択します。
3. **証明書種類**を**認証局証明書**を選択します。
4. 認証局証明書を作るための必要な情報です。
  - Common name - 該当メールサーバのドメインを入力します。
  - Country - 国を選択します。
  - その他情報を入力します。
  - 暗号化キーの長さ（Bit） - 暗号化時に使用するキーの長さを選択します。1024bits/2048bits
5. **Private KeyとCSVをダウンロードする**をクリックします。
6. 公認証明機関で証明書を取得するため、ダウンロードしたCSRを公認証明機関に提出します。
7. 公認証明機関で発行した証明書を登録するため、**証明書登録**ボタンをクリックします。
  - Private Key - **参照**ボタンをクリックして、5番でダウンロードしたprivate keyを登録します。
  - 認証局証明書 - **参照**ボタンをクリックして、公認証明機関で発行した証明書を登録します。
  - ルート証明書 - ルート証明書が必要な場合、ルート証明書にチェックして証明書を登録します。
  - チェーン証明書 - チェーン証明書が必要な場合、チェーン証明書にチェックして証明書を登録します。チェーン証明書はRoot証明機関より認証を受けた中間証明機関で発行する証明書で、証明書を認証局証明書として認識するために必要となります。追加ボタンをクリックして、チェーン証明書を順番に登録します。追加されたチェーン証明書を削除する場合は該当証明書の**削除**ボタンをクリックします。
8. **保存**ボタンをクリックします。
9. 証明書を適用するためWebサーバの再起動可否メッセージが表示されます。**確認**ボタンをクリックします。

## APIアクセス

ユーザ登録APIなどDaouOffice で提供するAPI(Application Programming Interface)へアクセスできるIPアドレスを設定します。

1. システム管理者画面[セキュリティ > 共通 > APIアクセス]をクリックします。
2. **APIアクセス**の使用可否を選択します。
  - 使用しない - DaouOffice の APIにアクセスすることができません。
  - すべて許可 - すべての IPから APIにアクセスすることができます。
  - 部分許可 - 許可された一部の IPのみ APIにアクセスすることができます。
3. 使用可否を**部分許可**に選択した場合、許可する IP アドレスを登録します。
  - 追加 - IP アドレスを入力後、追加アイコン()をクリックして IP アドレスリストに追加します。
  - 削除 - IP アドレスリストで削除するアドレスを選択して、削除アイコン()をクリックします。
4. 設定が完了しましたら**保存**ボタンをクリックします。


## 海外ログイン遮断許可設定

海外から DaouOffice に接続すると、接続を遮断します。 海外からのログインを遮断しても、許可するIPアドレスを登録して、特定のIPからのアクセスは許可することができます。



海外ログイン遮断の使用可否は [ サイト > ドメイン/サイト一覧 > サイトの変更 > 提供サービス ] で設定します。

海外ログインを遮断した場合、特定IPを登録して接続を許可する方法は次の通りです。

1. システム管理者画面の[セキュリティ > 共通 > 海外ログイン遮断許可]をクリックします。
2. 海外ログイン遮断許可設定の使用可否を選択します。
  - 使用- 海外ログインを遮断する際、特定IPアドレスからの接続は許可します。
    - **海外ログイン遮断許可設定を使用する**に選択した場合、許可IPアドレスを登録します。IPアドレス入力欄にアドレスを入力して、**追加アイコン**()をクリックします。
  - 使用しない
3. 設定が完了しましたら、**保存**をクリックします。

## 5.2 メール

### アンチスパム

受信されたメールは、3段階（接続段階、SMTP段階、コンテンツフィルタ）で処理されます。各段階別の規則によってスパムメール、スパム疑惑メール、ウイルスメール、正常メール、管理者定義スパムメールに分類され、分類されたメールは、分類別の処理方法に従います。この時の処理方法は、メールアドレスとドメインに設定されているグループポリシーによって異なる処理をすることができます。

処理の段階別のフィルタによってメールは次のように分類されます。

表 5-1 処理段階別のメール分類

項 目	説 明
スパムメール	処理段階別フィルタによってスパムと分類されたメールです。
スパム疑惑メール	スパム疑惑メールの判断ルールに合致、もしくは学習型フィルタのスパム疑惑メール範囲内に該当したメールです。
ウイルスメール	ウイルスフィルタによってウイルスとして分類されたメールです。
正常メール	許可ルールによって問題なく通過される、スパム、ウイルスメールではないメールです。
管理者定義スパムメール	管理者が定義したルールに合致したメールです。

メールの処理段階別に応じたフィルタの種類は次の通りです。

### コンテンツフィルタ

受信メールの本文内容（Contents）に特定キーワードや文字列を含む場合に、当該メールをフィルタするための許可及び遮断ルールを設定できます。一般文字列のみではなく正規表現を利用して様々な遮断条件を作成できます。

スパム検査可能な最大メールサイズは512KBです。

### 許可/遮断ルールリストの構成

許可/遮断ルールリスト項目の構成は次の通りです。

- フィルタ名 - 許可/遮断ルール名です。
- 詳細内容 - 許可/遮断ルールの詳細内容です。
- メール分類 - 該当フィルタで処理されたメール分類です。
- 使用可否 - 設定したフィルタの使用可否を表示します。





フィルタによって処理されたメール分類の説明は表 5-1 処理段階別のメール分類を参考してください。

## 許可/遮断ルールの追加

本文内容（Contents）に特定キーワードや文字列を含む場合に、遮断又は許可します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > コンテンツフィルタ]をクリックします。
2. **遮断ルール**又は**許可ルール**を選択します。
3. ルールリスト画面で**追加**ボタンをクリックします。
4. ルール追加画面が表示されます。各ルールの項目を設定します。

- フィルタ名 - ルールのフィルタ名を入力します。アルファベットの大小文字、数字、‘-’、‘\_’のみ入力できます。最大64byteまで入力可能です。必須入力項目です。
- 使用可否 - 当該遮断ルールの使用可否を選択します。
- 動作方法
  - 1つの条件でも一致する場合（OR） - 受信されたメールが設定したルールに1つでも一致する場合、**メール分類**で選択した通りに処理
  - 全ての条件と一致する場合（AND） - 受信されたメールが設定したルールに全て一致する場合、**メール分類**で選択した通りに処理
- 条件 - 許可/遮断ルールでフィルタする項目と比較する方法を設定します。スパム検査最大サイズは512KBです。

フィルタリング項目は次の通りです。

- 件名 - メールヘッダーのSubjectを検査します。
  - 本文内のURL - メール本文やHTMLに含まれているURLリンク（http://で始まるアドレス）を検査します。
  - 送信者（ENV） - SMTPプロトコル段階でのMail Fromを検査します。
  - 受信者（ENV） - SMTPプロトコル段階でのRcpt Toを検査します。
  - 送信者（Header） - メールヘッダーの送信者（（From））を検査します。
  - 受信者（Header） - メールヘッダーの受信者（（To））を検査します。
  - 同報受信者（Cc-Header） - メールヘッダーを参照して受信者（（Cc））を検査します。
  - ヘッダー全体 - メールヘッダーの全てを検査します。
  - ヘッダー値 - 特定ヘッダーのフィールドを指定して入力値を検査します。
- （例）Message-id: xxxx Header Message-Idに ‘xxxx’ を含むとフィルタする
- Content-Type - メールヘッダーのContent-typeを検査します。
  - 本文 - メールの本文に特定内容を含むかを検査します。
  - メールサイズ - 添付ファイルを含むメールの全体サイズを検査します。
  - IPアドレス - メールのIPアドレスを検査します。IPアドレスの入力方法は次の通りです。

（例）

1つのIPアドレスで入力：192.168.0.1

IPアドレス範囲で入力：192.168.0.1-192.168.0.35

サブネットマスクで入力: 192.168.0.1/24

- 添付ファイル名 - メールに添付されたファイル名を検査します。
- 添付ファイル本文 - 添付ファイルの本文の内容を検査します。サポートするファイルの形式は次の通りです。

zip, txt, rtf, htm, html, xml, pdf, mht, hwd, doc, ppt, xls, hwp, chm, dwg, sxw, sxc, sxi, mdi, msg, eml, xlsx, pptx, docx, jtd

条件方法は次の通りです。

- 含むと/含まないと - 条件の文字列が、対象のメール項目と比較して、「含むと/含まないと」でフィルタします。
- 一致すると/一致しないと - 条件の文字列が、対象のメール項目と比較して、「一致すると/一致しないと」でフィルタします。但し、IPアドレスが比較対象の場合には一致する場合のみフィルタします。
- 始まると/始まらないと - 対象のメール項目において、条件の文字列から、「始まると/始まらないと」でフィルタします。
- 終わると/終わらないと - 対象のメール項目において、条件の文字列で、「終わると/終わらないと」でフィルタします。
- 合うと/合わない (正規表現) - 条件項目の文字列を正規表現に変換して、対象のメール項目と比較し、「合うと/合わない」でフィルタします (正規表現文字として入力する必要はありません)。  
この比較方法は 大・小文字を区別しません。
- 合うと/合わない (正規表現、大・小区別) - 条件項目の文字列を正規表現式に変換して、対象のメール項目と比較し、「合うと/合わない」でフィルタします。  
この比較方法は 大・小文字を区別します。
- 存在しないと - 条件項目が対象のメール項目として「存在しないと」でフィルタします。

5. ルールの設定が完了したら、追加ボタンをクリックしてルールを保存します。



**添付ファイルの本文**を使用する場合、フィルタリング性能が低下する可能性があります。また、システムメモリ使用量が増加する可能性がありますので、使用する場合には十分にモニタリングしなければなりません。メモリ使用量が増加し、高負荷になる場合は、使用を中止してください。



本文内のURL, 受信者 (ENV, Header), 送信者 (ENV, Header) のフィルタ時に大小文字を区別しません。

## 許可/遮断ルール変更

許可/遮断ルールリストにあるルールを変更します。変更する方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > コンテンツフィルタ] をクリックします。
2. 遮断ルール又は許可ルールを選択します。
3. ルールリストで変更するルールのフィルタ名をクリックします。

4. ルール変更画面が表示されます。各ルール項目を変更します。
5. 修正が完了しましたら、**修正**ボタンをクリックします。



## 許可/遮断ルールの削除

許可/遮断ルールリストにあるルールを削除します。削除する方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > コンテンツフィルタ]をクリックします。
2. **遮断ルール**又は**許可ルール**を選択します。
3. ルールリストで削除するルールを選択後、**削除**ボタンをクリックします。

## 許可/遮断ルールの設定

フィルタに使用するルールを作動させます。又は使用に設定されているルールを中止します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > コンテンツフィルタ]をクリックします。
2. **遮断ルール**又は**許可ルール**を選択します。
3. ルールリストで使用するルールを選択した後、**使用**をクリックします。  
使用に設定されているルールを中止する場合は**使用しない**をクリックします。
4. ルール使用可否変更完了のメッセージが表示されます。**確認**ボタンをクリックします。
5. ルールリストの**使用可否**項目が使用() または使用しない()に変更されていることを確認します。

## フィルタ検査

当該ルールが属している段階別フィルタを検索して、どのパターンがどのルールに属しているかを検索することができます。



フィルタ検索に関して詳細な説明は[フィルタ検索](#)を参照してください。

許可/遮断ルールリストでフィルタを検索する方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > コンテンツフィルタ]をクリックします。
2. **遮断ルール**又は**許可ルール**を選択します。
3. ルールリストで**検索**ボタンをクリックします。
4. 検索画面で検索範囲又は検索条件を選択します。
5. **検索**ボタンをクリックすると検索結果リストが表示されます。

## ライブアップデート

パターンフィルタは、製品サポートセンターからライブアップデートで遮断ルールを提供します。

- パターンフィルタ - コンテンツ遮断ルールの一覧です。当該ルールに合致する内容 (Contents) がメールに含まれている場合、スパムメールとして処理されます。
- スパムフィンガープリント - イメージスパムやスパムURL情報をHash情報化して保存し、メールのHash情報と比較してスパム処理するようにします。
- 学習型フィルタ - メールの内容を自動的に分析、学習してキーワード別にスパム指数を付与します。スパム指数範囲によって、正常メール、スパム疑惑メール、スパムメールに分類され、処理されます。

学習型フィルタがメールを分類する基準値 (スパム指数) を設定できます。次のアイコン (🔍) を調整して基準値を設定します。推奨値は50です。

推奨値よりスパム指数を小さく設定するとスパムを遮断する確率は高くなりますが、正常メールが誤遮断される可能性もあります。正常メールが誤遮断された場合はスパム指数を調節してください。 (例) スパム疑惑メールの設定範囲が30~90の場合に、学習型フィルタが分析した受信メールのスパム指数が30より小さい場合は、正常メールとなります。スパム指数が30~90の場合はスパム疑惑メールとなり、90より大きい場合はスパムメールに分類されます。

- スパム指数 30 以下 - 正常メール
- スパム指数 30~80 - スパム疑惑メール
- スパム指数 80以上 - スパムメール

## パターンフィルタ使用の設定

製品サポートセンターから提供されるパターンフィルタの使用可否を選択します。

1. システム管理者画面の [セキュリティ > メール > アンチスパム > コンテンツフィルタ > ライブアップデート] をクリックします。
2. 各パターンフィルタの使用可否を選択します。
3. スパム指数基準値を次のアイコン (🔍) をマウスで調整して設定します。
4. パターンフィルタの設定を保存するには保存ボタンをクリックします。

## パターンフィルタのアップデート周期設定

各フィルタールのアップデート時間及びアップデート周期を設定することができます。

1. システム管理者画面の [セキュリティ > メール > アンチスパム > コンテンツフィルタ > ライブアップデート] をクリックします。
2. アップデート周期設定で各フィルタ毎に **アップデート周期** を選択します。
3. 設定が完了しましたら **保存** ボタンをクリックします。



スパムメール、ウイルスメール、スパイウェアなどに対処するため、アップデート周期を**1時間毎**に設定することを推奨します。



**最近アップデート時間**は直近の各パターンをアップデートした日付と時刻となりますので、アップデートされていない場合は**最近アップデート時間**は変更されません。

## 手動アップデート

各パターン別に手動でアップデートすることができます。

1. システム管理者画面の【セキュリティ > メール > アンチスパム > コンテンツフィルタ > ライブアップデート】をクリックします。
2. 手動でアップデートするために、各パターンの**アップデート開始**ボタンをクリックします。



ウイルスフィルタのアップデート時刻を確認したり、手動でアップデートするには[アンチウイルス](#)部分を参考してください。

## 接続段階遮断

DaouOffice に接続しようとするIPアドレスを制限して、スパムメールを防止できます。



接続段階の遮断フィルタの種類は次の通りです。

- IPアドレス遮断 - 登録されているIPのSMTP接続遮断
- IPフィルタ - 単位時間の間に1つのIPアドレスからのSMTP接続回数を制限
- 同時接続数制限 - 1つのIPからの同時接続回数を制限
- RBL - RBL (Realtime Spam Black List) サーバが提供するIPを遮断

各フィルタを設定する方法は次の通りです。

### IP遮断

DaouOffice に接続しようとする特定のIPアドレスを遮断するため、IPアドレスを登録します。

1. システム管理者画面の【セキュリティ > メール > アンチスパム > 接続段階遮断 > IP遮断】をクリックします。
2. IP遮断の**使用可否**を選択します。
3. 遮断IPに入力するIPアドレスの形式を選択します。
4. IPアドレスを入力後、追加アイコン()をクリックしてリストに追加します。
  - IP 削除 - IPアドレスリストで削除するIPアドレスを選択した後、削除アイコン()ボタンをクリックします。
  - IP 検索 - IPアドレスリストでIPアドレスを検索する場合、リスト下位にIPアドレスを入力した後、**検索**ボタンをクリックします。
  - IP リストファイルインポート - **インポート**ボタンをクリックしてIPアドレスリストを一度に追加

します。

- IP リストファイルエクスポート - IPアドレスリストで**エクスポート**ボタンをクリックして、IPアドレスリストをtextファイル (.txt) としてエクスポート可能です。

5. 拒否メッセージのコード及びメッセージを作成します。下記は、推奨値です。

- コード - 550
- メッセージ - Your IP is blocked.

6. 設定が完了しましたら**保存**ボタンをクリックします。



IP グループはシステム管理者画面の[その他 > IPグループ]で設定したグループです。

## IPフィルタ

設定時間中に基準値以上のメールを送るIPアドレスを遮断するルールについて設定します。

(例),

- 単位時間:30秒、接続数:10、受信メール数:100、受信者認証失敗数:10、遮断時間:1時間 に設定した場合、30秒間に、特定IPアドレスの接続数が10回を越えている、もしくは特定IPアドレスから送信されたメールの受信者数が100名を超えている、もしくは受信者の認証が10回を越えて失敗すると、当該IPアドレスの接続を1時間遮断し、拒否メッセージを送信者に送信します。

IPフィルタは基本設定と詳細設定があります。

- 基本設定 - IPフィルタの基本設定です。
- 詳細設定 - 設定時間中、特定IPアドレスに対して上位の遮断ルール（接続数、受信メール数、受信者認証失敗数）と遮断時間を、別々に適用したい際に設定する機能です。別々に適用したい条件を入力した後、アドバンスド設定を適用する対象（（IPアドレス））を入力します。

IPフィルタの設定方法は次の通りです。

## 基本設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > 接続段階遮断 > IPフィルタ]をクリックします。
2. IPフィルタの**使用可否**を選択します。
3. 単位時間を設定します。推奨値は1分です。
4. 遮断ルールを設定します。
  - 接続件数（推奨値：30件）
  - 受信メール数（推奨値：30件）
  - 受信者認証失敗回数（推奨値：10回）
5. 遮断時間を設定します。
6. 拒否メッセージのコード及び、メッセージを作成します。下記は推奨値です。
  - コード - 421

○ メッセージ - Your IP is filtered by IP Rate Control.

7. 設定が完了しましたら、**保存**ボタンをクリックします。

## 詳細設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > 接続段階遮断 > IPフィルタ]をクリックします。
2. **詳細設定**メニューをクリックします。
3. **追加**ボタンをクリックします。
4. IPフィルタの**使用可否**を選択します。
5. 単位時間を設定します。推奨値は1分です。
6. 遮断ルールを設定します。
  - 接続件数（推奨値：30件）
  - 受信メール数（推奨値：30件）
  - 受信者認証失敗回数（推奨値：10回）
7. 遮断時間を設定します。
8. 特定IPアドレスを登録します。IPアドレスの入力形式を選択します。
9. IPアドレスを入力後、追加アイコン(➤)をクリックしてリストに追加します。
  - IP削除 - IPリストで削除するIPを選択した後、削除アイコン(⬅)をクリックします。
  - IP検索 - IPアドレスを入力後、**検索**ボタンをクリックします。
  - IPリストファイルインポート - **インポート**ボタンをクリックして、IPアドレスを一度に追加することができます。
  - IPリストファイルエクスポート - IPリストで**エクスポート**ボタンをクリックして、IPアドレスリストをtextファイル(.txt)にエクスポートします。
10. 設定が完了しましたら、**追加**ボタンをクリックします。



IP グループはシステム管理者画面の[その他 > IPグループ]で設定したグループです。

## 同時接続数制限

同時接続によるメールサーバの負荷を防止するため、同じIPアドレスからの同時接続数を制限します。信頼できるIPアドレスから大量のメールを送信する場合には、当該するIPアドレスを接続段階で許可IPに登録します。

同時接続数制限は基本設定と詳細設定があります。



- 基本設定 - 同時接続数制限の基本設定です。
- 詳細設定 - 特定IPアドレスに対して同時接続数制限を別々に適用したい際に設定する機能です。別々に適用する同時接続数を入力して、設定を適用する対象（IPアドレス）を入力します。

基本設定は次の通りです。



1. システム管理者画面の[セキュリティ > メール > アンチスパム > 接続段階遮断 > 同時接続数制限]をクリックします。
2. 同時接続数制限**使用可否**を選択します。
3. IPアドレス当たり、同時に接続できる**最大制限接続数**を入力します。推奨値は10です。
4. 拒否メッセージのコード及び、メッセージを作成します。下記は推奨値です。
  - コード - 421
  - メッセージ - You made too many connections.
5. 設定が完了しましたら、**保存**ボタンをクリックします。

## 詳細設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > 接続段階遮断 > 同時接続数制限]をクリックします。
2. **詳細設定**メニューをクリックします。
3. **追加**ボタンをクリックします。
4. 同時接続数制限の**使用可否**を選択します。
5. IPアドレス当たり、同時に接続できる**最大制限接続数**を入力します。推奨値は10です。
6. IPアドレスを入力した後、追加アイコン()をクリックしてリストに追加します。
  - IP削除 - 削除するIPアドレスを選択した後、削除アイコン()をクリックします。
  - IP検索 - IPアドレスを入力した後、**検索**をクリックします。
  - IPリストファイルインポート - **インポート**をクリックしてIPアドレスリストを一度に追加することができます。
  - IPリストファイルエクスポート - IPリストで**エクスポート**をクリックして、IPアドレスリストをtextファイル(.txt)でエクスポートします。
7. 設定が完了しましたら、**追加**ボタンをクリックします。



IP グループはシステム管理者画面の[その他 > IPグループ]で設定したグループです。

## RBL

RBL (Real-time Spam Black Lists) はスパムメール送信IPアドレスをブラックリストで管理します。ブラックリストにあるIPアドレスからの接続を遮断することで、スパムメールを遮断できます。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > 接続段階遮断 > RBL]をクリックします。
2. RBLの**使用可否**を選択します。
3. 処理方法を選択します。
  - 送信 - 当該メールをユーザに送信します。
  - 受信拒否 - 当該メールを送信せず、受信拒否します。
  - 削除 - 当該メールを送信せずにすぐ削除します。
  - タグ - 当該メールの件名の前にタグを追加したり、メールヘッダーにX-headerを追加してメール



を送信します。**タグ設定**にてX-header及びタグを設定します。

4. RBL DNS 設定を選択します。
  - **基本 RBL** - 環境設定で設定したDNSサーバを利用してクエリーするようになります。最大5個まで登録できますが、性能面を考慮して、2個以上登録しないことを推奨します。
  - **ユーザ指定 RBL** - ユーザ指定RBL設定は、ユーザが設置したRBL DNSサーバを指定することができます。
5. 拒否メッセージを登録します。処理方法を受信拒否にする場合に使用されるメッセージです。永久に遮断するためには500番台エラーを入力することをお勧めします。
6. 設定が完了しましたら、**保存**ボタンをクリックします。

## 接続段階許可

メールを送信する特定IPアドレスが接続段階で遮断されるのを防止できます。

1. システム管理者画面の[**セキュリティ > メール > アンチスパム > 接続段階許可**]をクリックします。
2. 接続段階許可の**使用可否**を選択します。
3. 許可するIPアドレスの入力形式を選択します。
4. IPアドレスを入力した後、追加アイコン(➤)をクリックしてリストに追加します。
  - IP削除 - 削除するIPアドレスを選択した後、削除アイコン(◀)をクリックします。
  - IP検索 - IPアドレスを入力した後、**検索**ボタンをクリックします。
  - IPリストファイルインポート - **インポート**をクリックして、IPアドレスリストを一度に追加することができます。
  - IPリストファイルエクスポート - IPリストで**エクスポート**をクリックして、IPアドレスリストをtextファイル(.txt)でエクスポートします。
5. 設定が完了しましたら、**保存**ボタンをクリックします。



IP グループはシステム管理者画面の[**その他 > IPグループ**]で設定したグループです

## SMTP段階遮断

SMTP段階(EHLOからRCPTまで)で、スパムメールを遮断します。各フィルタ種類が次の通りです。

- DNS検査 - EHLOコマンド後ろのドメイン、送信者のドメイン、受信者のドメインを検査後、これに違反時に遮断
- SPF検査 - 送信者ドメインをSPFで不正ドメイン検査後、遮断
- 送信者遮断 - 送信者遮断リストにある送信者から送られたメールを遮断
- 送信者フィルタ - 単位時間の基準値以上のメールを送信した送信者を設定した時間に遮断
- 受信者遮断 - 受信者遮断リストにある受信者から送られたメールを遮断
- 受信者フィルタ - 単位時間の基準値以上のメールを受信した受信者を設定した時間に遮断
- 同報メール応答遅延 - 設定された数以上のメールを同報送信する場合、受信速度を調整して、受信メールの数を制限

各フィルタの設定方法は次の通りです。

## DNS検査

SMTPプロトコル上のドメインのDNS検査可否を設定します。但し、DNS検査は外部のDNSに検査を行いますので、処理に時間がかかる場合があります。

DNSを検査する対象は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > DNS検査]をクリックします。
2. 各検査対象を選択します。
  - EHL0 DNS検査
    - 使用可否 - EHL0 DNS検査の使用可否を選択します。
    - 検査方式 - 検索方式を選択します。
    - Soft Fail時の処理 - Soft FailはDNSサーバの応答がない場合などで失敗する場合です。その場合の処理として正常処理、受信拒否、いずれかを選択します。
  - 送信者DNS検査
    - 使用可否 - 送信者DNS検査の使用可否を選択します。
    - Soft Fail時の処理 - Soft FailはDNSサーバの応答がない場合などで失敗する場合です。その場合の処理として正常処理、受信拒否、いずれかを選択します。
  - 受信者DNS検査
    - 使用可否 - 受信者DNS検査の使用可否を選択します。
3. 設定が完了しましたら、**保存**ボタンをクリックします。



IPアドレスとEHL0ドメインIPアドレスの一致可否はC クラスアドレスまでのみ検査します。即ち、IPアドレスとEHL0ドメインIPアドレスのCクラスアドレスが一致すると許可します。 CクラスとはIPアドレスの4byteの中で前の3byte(ネットワークID)が同じネットワークを示します。(例) 192.168.10.x



Outlook又はOutlook ExpressなどのPC用メールクライアントから送信されるメールでは、EHL0のドメインが正しくない場合があります。従って、EHL0 DNS検査機能を使用する場合にはPC用メールクライアントから送信されるメールが遮断される場合もあります。

## SPF検査

SMTPプロトコルの中で送信者のドメインをSPF (Sender Policy Framework) 検査を行い、不正ドメインから送信されるメールを遮断します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > SPF検査]をクリックします。
2. SPF検査の**使用可否**を選択します。

3. **検索方式**を選択します。
4. **処理方法**を選択します。
  - 基本ポリシーに従う - 推奨値です。基本ポリシーの処理方法は次の通りです。
    - Softfail, Invalid, Neutral, None, Temperror, Permerror - タグ
    - Pass - 使用しない
    - Fail - 拒否
  - 個別ポリシー指定(アドバンスド機能) - SPF結果値によって個別ポリシーを指定できます。
5. 設定が完了しましたら**保存**ボタンをクリックします。

## 個別ポリシー指定及び処理方法

- SPF結果
  - Pass - DNSの照会に成功しSPFレコードを見つけ、レコードで送信システムのドメイン認証が確認できました。
  - Fail - DNSの照会結果、SPFレコードは見つきましたが、SMTPクライアントのドメイン使用権限がレコードで明確に拒否されました。
  - Softfail - DNSの照会結果、一致するSPFレコードを見つけました。レコードでSMTPクライアントのドメイン使用認証が拒否されましたが、拒否が明確でないため、失敗とは確認できませんでした。
  - Invalid - SPFレコードに間違った形式の値が登録され、クエリ時に間違った値が入っています。
  - Neutral - SPFレコードでSMTPクライアントのドメイン認証を要求しません。メッセージは受け取りますが、仕様によってNoneのように処理します。
  - None - 一致するSPFレコードが見つからなかったため、SPF処理が実行できませんでした。
  - Temperror - SPFレコードでSMTPレコードが見つからなかったため、SPF処理が実行できませんでした。
  - Permerror - SPF処理中にSPFレコードにエラーがあるなど、一時的なエラーではない場合に発生します。
- 処理方法
  - タグ - メールヘッダまたはメールの件名に設定されたタグが挿入されてユーザに送信されます。
  - 拒否 - メールをユーザのメールフォルダに送信せずに拒否します。
  - 通過 - メールをユーザのメールフォルダに送信します。
  - 使用しない - 当該のカテゴリを使用しません。



タグは既に定義されていて管理者がタグを別途指定することはできません。

## 送信者遮断

特定ユーザが送信したメールをSMTPプロトコル段階で遮断するように設定します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 送信者遮断]をクリックします。
2. 送信者遮断の**使用可否**を選択します。
3. 遮断する送信者のメールアドレス又はドメインを入力した後、追加アイコン(➤)をクリックしてリス

トに追加します。

(例) メールアドレス: test@xxx.com ドメイン: @xxx.com, @yyy.co.jp

4. 設定が完了しましたら、**保存**ボタンをクリックします。

## 送信者フィルタ

特定の送信者が設定時間中、デフォルト値以上のメールを送信する送信者を設定時間、遮断します。

(例)

- 設定時間が30秒、設定時間中の送信メール数:10、遮断時間:1時間 に設定された場合、特定送信者が30秒間に、10件以上のメールを送信すると、当該送信者からのメールを1時間遮断します。

送信者フィルタは基本設定と詳細設定があります。

- 基本設定 - 送信者フィルタの基本設定です。
- 詳細設定 - 特定IPアドレスに対して、設定時間中に送信者メール数制限と遮断時間を基本設定とは別に適用したい時に設定する機能です。入力は一上記と同じで、アドバンスド設定を適用する対象 (IPアドレス) を入力します。



送信者フィルタの設定方法は次の通りです。

### 基本設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 送信者フィルタ]をクリックします。
2. 送信者フィルタの**使用可否**を選択します。
3. **設定時間**を入力します。推奨値は1分です。
4. **送信メール数**を入力します。推奨値は30です。
5. **遮断時間**を設定します。
6. 拒否メッセージのコード及びメッセージを作成します。下記は、推奨値です。
  - コード - 421
  - メッセージ - Your sent too many messages.
7. 設定が完了しましたら、**保存**ボタンをクリックします。


### 詳細設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 送信者フィルタ]をクリックします。
2. **詳細設定**メニューをクリックします。
3. **追加**ボタンをクリックします。
4. 送信者フィルタの**使用可否**を選択します。
5. **設定時間**を入力します。推奨値は1分です。
6. **送信メール数**を入力します。推奨値は30です。

7. **遮断時間**を入力します。
8. IPアドレスを入力した後、追加アイコン()をクリックしてリストに追加します。
  - IP削除 - 削除するIPアドレスを選択した後、削除アイコン()をクリックします。
  - IP検索 - IPアドレスを入力した後、**検索**ボタンをクリックします。
  - IPリストファイルインポート - **インポート**をクリックしてIPアドレスリストを一度に追加することができます。
  - IPリストファイルエクスポート - IPリストで**エクスポート**をクリックして、IPアドレスリストをファイルにエクスポートします。
9. 設定が完了しましたら、**追加**ボタンをクリックします。

## 受信者遮断

特定の受信者に受信されるメールをSMTPプロトコル段階で遮断するように設定します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 受信者遮断]をクリックします。
2. 受信者遮断の**使用可否**を選択します。
3. 遮断する受信者のメールアドレス又は、ドメインを入力した後、追加アイコン()をクリックしてリストに追加します。  
(例) メールアドレス: test@xxx.com ドメイン: @xxx.com, @yyy.co.jp
4. 設定が完了しましたら、**保存**ボタンをクリックします。

## 受信者フィルタ

デフォルト値以上のメールを受信する受信者を、設定時間遮断します。

(例)

- 設定時間が30秒、受信メール数:10、遮断時間:1時間 に設定された場合、特定の受信者が30秒間に、受信するメールが10件を超えると、当該受信者宛のメールを1時間遮断します。

受信者フィルタは基本設定と詳細設定があります。



- 基本設定 - 受信者フィルタの基本設定です。
- 詳細設定 - 特定IPアドレスに対して設定時間中、受信メール数制限と遮断時間を別々に適用したい際に設定する機能です。

## 基本設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 受信者フィルタ]をクリックします。
2. 基本設定のメニューで受信者フィルタの**使用可否**を選択します。
3. **設定時間**を入力します。推奨値は1分です。
4. **受信メール数**を入力します。推奨値は30です。

5. **遮断時間**を入力します。
6. 拒否メッセージのコード及び、メッセージを作成します。次は推奨値です。
  - コード - 421
  - メッセージ - You sent too many messages to specific receiver
7. 設定が完了しましたら、**保存**ボタンをクリックします。

## 詳細設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 受信者フィルタ]をクリックします。
2. **詳細設定**メニューをクリックします。
3. 受信者フィルタの**使用可否**を選択します。
4. **設定時間**を入力します。推奨値は1分です。
5. **遮断時間**を入力します。
6. IPアドレスを入力した後、追加アイコン()をクリックしてリストに追加します。
  - IP削除 - 削除するIPを選択した後、削除アイコン()をクリックします。
  - IP検索 - IPアドレスの入力後、**検索**をクリックします。
  - IPリストファイルインポート - **インポート**をクリックして、IPアドレスリストを一回で追加することができます。
  - IPリストファイルエクスポート - IPリストでエクスポートをクリックして、IPアドレスリストのファイルをエクスポートします。
7. 設定が完了しましたら、**追加**ボタンをクリックします。

## 同報メール応答遅延

設定された数以上の同報メールを送信する場合、応答遅延を利用し、当該接続に対し、メールの受信速度を調節します。

同報メール応答遅延は基本設定と詳細設定があります。



- 基本設定 - 同報メール応答遅延の基本設定です。
- 詳細設定 - 特定IPアドレスに対して、同報メール応答遅延を別々に適用したい際に設定する機能です。入力上記と同じで、アドバンスド設定を適用する対象（IPアドレス）を入力します。

## 基本設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 同報メール応答遅延]をクリックします
2. 同報メール応答遅延の**使用可否**を選択します。
3. **受信者タイプ**を選択します。
  - 全受信者
  - 類似ID受信者：IDパターンが類似している受信者（例）aaa、aa1、aa2、…
4. **制限受信者数**を入力します。推奨値は10名です。




- 制限受信者数 - 同報メールを送れる最大受信者数です。
- 5. **遅延時間**を入力します。推奨値は2秒です。
  - 遅延時間 - SMTPプロトコル応答を遅延させる時間です。
- 6. 設定が完了しましたら、**保存**ボタンをクリックします。

## 詳細設定

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階遮断 > 同報メール応答遅延]をクリックします。
2. **追加**ボタンをクリックします。
3. **使用可否**を選択します。
4. **受信者タイプ**を選択します。
  - 全受信者
  - 類似ID受信者 : IDパターンが類似な受信者 (例) aa、a1、a2、…
5. 制限受信者数を入力します。推奨値は10名です
  - 制限受信者数- 同報メールを送れる最大受信者数です。
6. **遅延時間**を入力します。推奨値は2秒です。
  - 遅延時間 - SMTPプロトコル応答を遅延させる時間です。
7. IPアドレスを入力後、追加アイコン()をクリックしてリストに追加します。
  - IP削除 - 削除するIPアドレスを選択した後、削除アイコン()をクリックします。
  - IP検索 - IPアドレスを入力した後、**検索**をクリックします。
  - IPリストファイルインポート - **インポート**をクリックして、IPアドレスリストを一度に追加することができます。
  - IPリストファイルエクスポート - IPリストで**エクスポート**をクリックして、IPアドレスリストをファイルでエクスポートします。
8. 設定が完了しましたら、**追加**ボタンをクリックします。

## SMTP段階許可

メールを送信する特定IPアドレス又は特定メールアドレス、ドメインがSMTP段階で遮断されるのを防止できます。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > SMTP段階許可]をクリックします。
2. SMTP段階許可の**使用可否**を選択します。
3. 許可するメールアドレス又はドメインを入力します。メールアドレス/ドメインを入力した後、追加アイコン()をクリックしてリストに追加します。
4. 許可IPアドレスを入力した後、追加アイコン()をクリックしてリストに追加します。
  - IP削除 - 削除するIPアドレスを選択した後、削除アイコン()をクリックします。
  - IP検索 - IPアドレスを入力した後、**検索**をクリックします。
  - IPリストファイルインポート - **インポート**をクリックして、IPアドレスリストを一回で追加することができます。



- IPリストファイルエクスポート - IPリストで**エクスポート**をクリックして、IPアドレスリストをファイルにエクスポートします。

5. 設定が完了しましたら**保存**ボタンをクリックします。

## グループポリシー

メールの受信者をグループに分け、メールの各カテゴリに対してグループごとに別々の処理方法(ポリシー)を設定することが出来ます。

- スпамメール
- スпам疑惑メール
- ウイルスメール
- 管理者定義メール

DaouOffice の初期設定では、基本的に3つのポリシーがデフォルトで設定されています。

- DEFAULT - 特定グループポリシーに含まれていない受信者に提供するデフォルトグループポリシーです。デフォルトポリシーは処理方法のみ変更が可能です。
- OUTBOUND - 内部ローカルドメインを除外した全ての外部ドメインで送受信されるメールに対する処理方法です。
- SYSTEM - システム負荷を最小限にするため、大容量メールを処理する場合に使用できるポリシーです。接続段階又はSMTP段階でスパム、ウイルスメールを大量送信されるのを受信拒否(reject)することができます。Systemポリシーを使用する際は、全ての送受信メールに対して、最優先に適用されるようになります。この場合にはユーザが受信を許可した送信者も遮断され場合があるので、必ず事前に確認した上で使用してください。

## グループポリシー追加

グループポリシーを追加します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > グループポリシー]をクリックします。
2. グループポリシー画面で**追加**をクリックします。
3. ポリシー追加画面にて各項目を設定します。
  - ポリシー名 - ポリシー名を入力します。最大64byteまで入力可能です。
  - 使用可否 - ポリシーの**使用可否**を選択します。
  - メールアドレス/ドメイン - 当該ポリシーを適用するメールアドレス及びドメインを追加します。
  - 処理方法 - 各メールのカテゴリ別に処理方法を設定します。
    - 送信 - 遮断せずにメールを受信者に配信します。
    - 遮断レベル - 遮断レベルを選択します。
    - タグ - 適用するタグの入力方式を選択します。
    - 駆除後に送信- ウイルスを駆除後に送信します。
    - 削除 - メールを受信して削除します。**system**ポリシーのみ選択できます。
    - 受信拒否 - メールをユーザのメールフォルダに転送せずに、送信者に返送します。受信拒否



処理は**system**ポリシーでのみ選択が可能です。

- グループポリシーによる - 接続段階またはSMTP段階で特定遮断ルールによってメールが分類される時、当該メールの受信者のポリシーによって処理します。**system**ポリシーのみ選択が可能です。

4. グループポリシーの項目設定が完了しましたら、**追加**ボタンをクリックします。

## グループポリシー変更

グループポリシーを変更します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > グループポリシー]をクリックします。
2. グループポリシーのリストで変更するグループポリシー名をクリックします。
3. グループポリシーの情報を変更します。
4. グループポリシーの項目の変更が完了しましたら、**変更**ボタンをクリックします。

## グループポリシー削除

グループポリシーを削除します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > グループポリシー]をクリックします。
2. グループポリシーで削除するグループポリシーを選択後、**削除**をクリックします。

## グループポリシーの適用設定

グループポリシーの使用可否を設定します。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > グループポリシー]をクリックします。
2. グループポリシーで使用に設定するグループポリシーを選択後、**使用**をクリックします。  
又は、グループポリシーで使用しないに設定するグループポリシーを選択後、**使用しない**をクリックします。
3. 設定変更の完了メッセージが表示されます。**確認**ボタンをクリックします。
4. グループポリシーのリストの使用可否項目で使用 (○) 又は使用しない (⊗) に変更されいていることを確認します。

## グループポリシー適用順位

多数のポリシーに属する各グループ（メールアドレス、ドメイン）のメール処理方法は、優先順位が一番高く設定されたポリシーが適用されます。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > グループポリシー]をクリックします。
2. グループポリシーリストから、適用順位を変更するグループポリシーを選択します。
3. 上に又は下をクリックして、ポリシーの順位を設定します。

## グループポリシー検索

グループポリシーに含まれているメールアドレス又はドメインを検索することができます。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > グループポリシー]をクリックします。
2. グループポリシーのリストの上段にある**検索**をクリックします。

## フィルタ情報ポリシー

フィルタ情報ポリシーの設定をします。フィルタ情報ポリシーの設定は次の通りです。

- フィルタ情報管理サーバ - フィルタリングされたIPアドレスの情報を収集・共有するかを設定します。
- ローカルサーバ許可 - ローカルドメインが使用するIPアドレスまたはローカルホストのIPアドレスから送信したメールはスパムフィルタルールにより、遮断されずに受信するように設定します。
- ローカル学習型フィルタ - ユーザが申告したメールを管理者が学習させ、メールを遮断するかを設定します。

## フィルタ情報管理サーバ

複数のサーバでDaouOffice を運用する場合、フィルタリングするIPアドレスの情報を収集・共有できるサーバをフィルタ情報管理サーバとして指定することができます。フィルタ情報管理サーバで収集されたIPアドレスを利用し、IPフィルタを適用することができ、フィルタ情報管理サーバを指定しない場合は、ローカルの情報でIPフィルタを適用します。



DaouOffice を1台で運用する場合は、フィルタ情報管理サーバを指定する必要はありません。

フィルタ情報管理サーバの設定方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > フィルタ情報ポリシー]をクリックします。
2. フィルタ情報ポリシーの**使用可否**を選択します。
  - 個々の管理 - サーバ毎にIPアドレスの情報を収集し適用します。他のサーバと情報を共有しません。
  - 単一管理 - 特定のサーバをフィルタ情報管理サーバに指定し、情報を共有してIPフィルタを適用します。
3. **タイムアウト**を設定します
  - 設定したタイムアウト時間で、フィルタ情報管理サーバと接続ができない場合は、フィルタせずにメールを受信します。
  - 秒単位でタイムアウトを設定します。(推奨値: 5秒)
4. 設定が完了しましたら、**保存**ボタンをクリックします。



フィルタ情報管理サーバの管理方式を単一管理時、各サーバのフィルタルールとシステム時間が一致している必要があります。この条件を満たさないとフィルタ情報管理サーバが誤動作する可能性があります。

## ローカルサーバの許可

ローカルドメインが使用するIPアドレスまたはローカルホストのIPアドレスから送信したメールはスパムフィルタルールにより、遮断されずに受信するように設定できます。ローカルドメインが使用するIPアドレスは次の通りです。

- [環境設定 > システム > サーバ管理]に登録されたIPアドレス
- [環境設定 > その他 > IPグループ]に登録されたIPアドレス

ローカルドメインの内部メールサーバの許可ポリシーを設定する方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > フィルタ情報ポリシー]をクリックします。
2. ローカルサーバの許可の使用可否を選択します。
3. 保存をクリックします。

## ローカル学習型フィルタ

管理者が学習させた学習型フィルタをローカル学習型フィルタといいます。ライブアップデートで提供される学習型ルールとは別に、ユーザが申告したメールを管理者が学習させます。ローカル学習型フィルタは、アップデートで提供される学習型フィルタに統合され、スパムメールを判断します。ローカルシステムで学習させることが可能になり、より正確にスパムメールを遮断することができます。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > フィルタ情報ポリシー]をクリックします。
2. ローカル学習型フィルタの使用可否を選択します。
3. 保存をクリックします。

## フィルタ検索

スパムコンテンツフィルタ、スパムアドバンスドフィルタで登録したフィルタルールを検索する機能です。

- 検索範囲 - メールが処理される各段階別に選択して検索することができます。検索する検索範囲を選択します。
- 検索種類 - 遮断ルール又は許可ルールを選択します。
- キーワード - 検索するキーワードを入力します。入力形態はルールの追加/変更で入力できるパターンとIPアドレス、メールアドレス又は一般文字列（URL、ヘッダー内容）が入力可能です。
  - フィルタ名含む - コンテンツ段階又は情報漏洩防止機能で設定したフィルタ名を検索する場合にチェックします。

- IPアドレス範囲含む - キーワードに入力したIPアドレスが特定範囲に含まれているかどうかを検索します。その場合、キーワードはIPアドレス形式で入力します。

フィルタを検索する方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > アンチスパム > フィルタ検索]をクリックします。
2. **検索範囲**と**フィルタ種類**を選択して、キーワードを入力します。
3. **検索**をクリックします。



検索した結果から詳細内容をクリックすると、**キーワード**が含まれたルールなどに移動して、詳細内容の確認ができます。

## 情報漏洩防止

### 情報漏洩モニタリング

情報漏洩防止機能は、電子メールによる情報漏洩を防ぐための機能です。送受信されるメールに、重要な情報を含むメールに対してルールを設定しフィルタすることができます。フィルタされたメールをモニタリングすることで、情報漏洩を防止できます。但し、メールモニタリングは個人のプライバシー保護のため必ずユーザの同意が必要ですのでご注意ください。

情報保護フィルタによって検出されたメールは、管理者が指定したフォルダに保存することができます。特定フォルダに保存されたメールをモニタリングして、情報漏洩の内容と漏洩者を特定できます。但し、フォルダ保存期間以後は消去されますのでご注意ください。



情報漏洩モニタリングのフォルダ期間設定は**情報漏洩モニタリング**リストで**設定**をクリックすると[セキュリティ > メール > 情報漏洩防止 > フォルダ管理]に移動します。

### 情報漏洩防止モニタリング内容の検索

検索には基本検索と詳細検索があります。最新1000件のメールから確認したい情報を検索できます。

最新1000件のメールを指定して検索条件のメールを検索します

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報漏洩モニタリング]をクリックします。
2. 情報漏洩モニタリングで検索範囲を選択します。
3. 検索条件を選択して、キーワードを入力します。
4. **検索**をクリックします。

詳細検索項目を利用すると、最新1000件のメール以外の情報も検索できます。但し、表示は最新1000件までとなります。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報漏洩モニタリング]をクリックします。
2. 情報漏洩モニタリング画面の上段の**詳細検索**をチェックします。
3. 詳細検索条件の設定画面が表示されましたら、各項目を選択又は入力します。
4. **検索**をクリックします。

## 情報漏洩モニタリング内容の削除/全体削除

フォルダに保存されているメールの情報を削除できます。削除されたメールは二度と復元できません。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報漏洩モニタリング]をクリックします。
2. 保存フォルダ名で該当フォルダを選択します。
3. リストで削除するメールを選択後、**削除**をクリックします。

## 情報漏洩モニタリング内容の送信

フォルダに保存されているメールの送信が可能です。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報漏洩モニタリング]をクリックします。
2. **保存フォルダ名**で該当フォルダを選択します。
3. リストで送信するメールを選択後、**送信**をクリックします。

## 情報保護フィルタ

本文（Contents）に特定の文字列やキーワードを含む送受信メールをフィルタするためのルールを設定することができます。一般文字列のみではなく正規表現を利用して様々な条件を作成することができます。

フィルタルールを構成する内容は次の通りです。

- 特定フォルダに保存/送信 - [セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]で設定した特定フォルダにフィルタされたメールを保存した後、本来のメール受信者に送信します。保存期間が過ぎたメールは削除されます。
- 特定メールアドレスに転送/送信 - 指定した特定メールアドレスにメールを転送した後、本来のメール受信者に送信します。
- 特定フォルダに保存 - [セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]で設定した特定フォルダにフィルタされたメールを受信者に送信せず、保存のみ行います。
- 特定メールアドレスに転送 - 受信者にメールを送信しないで、指定した特定メールアドレスにメールを転送します。

情報保護フィルタを設定する方法は次の通りです

## 情報保護フィルタ追加

情報保護フィルタを追加します。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]をクリックします。
2. 情報保護フィルタ画面で**追加**をクリックします。
3. 情報保護フィルタの追加画面で各項目を入力します。
  - フィルタ名 - 他のフィルタ名と区分できるフィルタ名を入力します。
  - 使用可否 - フィルタの使用可否を選択します。
  - 動作方法 - 動作方法を選択します。
    - 1つの条件でも一致する場合 - 該当フィルタに設定されている複数の条件中、1つの条件でも一致する場合、メールをフィルタリングします。
    - 全ての条件と一致する場合 - 該当フィルタに設定されている全ての条件と一致する場合、メールをフィルタリングします。
  - 処理方法 - 条件に該当するメールの処理方法を選択します。
    - 特定フォルダに保存/送信 - [セキュリティ > メール > 情報漏洩防止 > フォルダ管理]で設定した特定フォルダにフィルタリングされたメールを保存して、メールの元の受信者に送信します。メールは保存期間によって削除されます。
    - 特定メールアドレスに転送/送信 - 指定した特定メールアドレスにメールを転送して、メールは元の受信者に送信します。
    - 特定フォルダ保管 - [セキュリティ > メール > 情報漏洩防止 > フォルダ管理]で設定した特定フォルダにフィルタリングされたメールが保存されます。元の受信者にはメールを送信しません。メールの保存期間によって削除されます。
    - 特定メールアドレスに転送 - 受信者にメールを送信せず、指定した特定メールアドレスに転送されます。
  - 条件 - 条件を設定します。
    - 件名 - メール Headerの Subjectを比較します。
    - 本文内の URL - メール本文内やHTMLに含まれているURLリンク (http://で始まるアドレス)を比較します。
    - 送信者(ENV) - SMTP プロトコル段階の Mail Fromを比較します。
    - 受信者(ENV) - SMTP プロトコル段階の Rcpt Toを比較します。
    - 送信者(Header) - メール Header ▪ 送信者(From)を比較します。
    - 受信者(Header) - メール Headerの 受信者(To)を比較します。
    - 同報受信者(Cc-Header) - メール Headerの受信者(Cc)を比較します。
    - ヘッダー全体 - メール Headerの全てを比較します。
    - ヘッダー値 - 特定 Headerのフィルタを指定して入力した値を比較します。  
(例) Message-id : xxxx Headerの Message-Idに ‘xxxx’ を含む場合フィルタリング
    - Content-Type - メール Headerの Content-typeを比較します。
    - 本文 - メール本文に特定内容が含まれているか比較します。
    - メールサイズ - 添付ファイルを含んだメールの全体サイズを比較します。

- IP - メールの発送 IPを比較します。
- 添付ファイル名 - メールの添付されたファイル名を比較します。
- 添付ファイルの本文 - 添付ファイルの本文の内容を比較します。サポートするファイルの拡張子は次の通りです。  
(zip, txt, rtf, htm, html, xml, pdf, mht, hwd, doc, ppt, xls, hwp, chm, dwg, sxw, sxc, sxi, mdi, msg, eml, xlsx, pptx, docx, jtd)
- 個人情報 - カード番号や口座番号等の個人情報が含まれているか確認します。  
フィルタリング対象を個人情報で選択する場合はメール本文に含まれている個人情報の数を1から1000まで指定することができます。ただし、個人情報を複数追加する場合は個人情報の数を指定することはできません。

条件をフィルタリングする方法を選択します。

- 含むと/含まないと - 条件項目の文字列をメール項目に含むと/含まない場合にフィルタリングします。
- 一致すると/一致しないと - 条件項目の文字列をメール項目と比較して正確に一致すると/一致しない場合フィルタリングします。ただし、IPが比較対象の場合は一致する場合のみ比較します。
- 始まると/始まらないと - 条件項目の文字列でメール項目が始まると/始まらない場合にフィルタリングします。
- 終わると/終わらないと - 条件項目の文字列でメールの項目が終わると/終わらない場合フィルタリングします。
- 合うと/合わない(正規表現式) - 条件項目の文字列を正式表現に変換してメール項目と比較した際、合うと/合わない場合フィルタリングします。正規表現式の文字は別途入力する必要があります。該当比較は大小比較をしません。
- 合うと/合わない(正規表現式、大小区別) - 条件項目の文字列を正式表現式に変換してメール項目と比較際、合うと/合わない場合フィルタリングします。該当比較は大小区分をします。
- 存在しないと - 条件項目がメール項目に存在しない場合フィルタリングします。
- より大きいと/より小さいと - 条件項目で設定したメールサイズがより大きいと/より小さいとフィルタリングします。

4. フィルタ追加設定が完了しましたら、**追加**ボタンをクリックします。



**添付ファイルの本文** の条件を使用する場合はパフォーマンスが低下するし、システムメモリも増えることがあります。したがって、本条件を使用する場合は十分に監視する必要がありますので、メモリ使用量や負荷が高くなる場合は使用を中止してください。

## 情報保護フィルタの変更

情報保護フィルタのリストにあるフィルタを変更します。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]をクリックします。
2. 情報保護フィルタ画面で修正するフィルタ名をクリックします。



3. 情報保護フィルタ修正画面でフィルタ情報を変更します。
4. フィルタの修正が完了しましたら、**変更**をクリックします。



## 情報保護フィルタの削除

リストにあるフィルタを削除します。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]をクリックします。
2. 情報保護フィルタ画面にて削除するフィルタを選択した後、**削除**をクリックします。

## 情報保護フィルタの使用可否

情報保護フィルタの使用可否を選択します。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]をクリックします。
2. フィルタリストで使用に設定するフィルタを選択後、**使用**又は**使用しない**をクリックします。
3. 設定変更の完了メッセージが表示されます。**確認**ボタンをクリックします。
4. フィルタリストの使用可否項目で使用()又は使用しない()に変更されていることを確認します。

## 情報保護フィルタ検索

フィルタを検索します。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 情報保護フィルタ]をクリックします。
2. フィルタリストで**検索**をクリックします。
3. [セキュリティ > メール > アンチスパム > フィルタ検索]に移動します。

## 保護対象設定

フィルタを適用させる対象を設定します。設定方法は次の通りです。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > 保護対象]をクリックします。
2. 詳細設定画面で次の項目を設定します。
  - 保存対象設定 - 保存メールの対象を選択します。
    - 全体保存 - フィルタの条件とは関係なく、全てのメールを保存及び送信します。
    - 特定フィルタに適用されたメールのみ保存(推奨) - 情報保護フィルタにマッチするメールのみ保存します。
  - 保存(詳細)オプション - 保存(詳細)オプションを選択します。(すべて選択を推奨)
    - スпамメールを保存しない - スпамとして判断されるメールを保護対象から除外し、保存しません。
    - ウイルスメールを保存しない - ウイルスとして判断されるメールを保護対象から除外し、保



存しません。

- 送受信区分 - 送信メール又は受信メールを適用するかどうかを選択します。
- 圧縮設定 - 圧縮設定を選択します。

■ 情報漏洩防止機能で保存されたメールを確認するために圧縮されたメールを復元するとサーバの負荷があがります。サーバ負荷を減らすためには、圧縮をしないことを推奨します。

- 個人情報オプション設定 - プライバシーオプション - メールに個人情報が含まれていることを確認するために、検出条件を設定します。個人情報オプション設定は、韓国の住民登録番号のような特定情報のみ保護します。日本での利用は、推奨できません。

3. 設定が完了しましたら、**保存**をクリックします。

## 遮断メール通知設定

ユーザが送信したメールが情報保護フィルタによって遮断されたことを送信者に通知する機能です。



情報保護フィルタの処理方法が**特定フォルダに保存/送信**または**特定メールアドレスに転送/送信**の場合、メールが情報保護フィルタに該当してもメールは受信者に転送するため、通知メールが送信されません。

1. システム管理者画面の [**セキュリティ > メール > 情報漏洩防止 > 遮断メール通知設定**]をクリックします。
2. 使用可否を選択します。
  - 使用 - 情報保護フィルタがメールを遮断すると送信者に通知メールを送信します。
  - 使用しない
3. 通知メールの**件名**と**送信者メールアドレス**を入力します。
4. 遮断メール通知の変数を確認します。該当変数は通知メールに基本的に含まれる項目で管理者が変更することができます。
  - \$subject - 情報保護フィルタによって遮断されたメールの件名
5. 通知メールの内容を確認して、必要な場合内容を修正します。
6. 遮断されたメールの原本を通知メールに含まれるか、選択します。
7. 設定が完了しましたら、**保存**をクリックします。

## 情報漏洩防止機能のフォルダ管理

情報漏洩防止で使用するフォルダを追加・削除します。フォルダは最大5個まで作成可能です。保存期間は、ディスクの使用量を考慮し設定してください。

### 情報漏洩防止機能のフォルダ管理

1. システム管理者画面の [**セキュリティ > メール > 情報漏洩防止 > フォルダ管理**]をクリックします。
2. **追加**をクリックします。
3. 新しいフォルダの入力欄にフォルダ情報を入力します。

- フォルダ名 - フォルダ名を入力します。英字、数字のみ入力可能です。
  - 保存期間 - 保存期間を入力します。最大メール保存期間は365です。
4. フィルダの追加が完了しましたら、**保存**をクリックします。

## 情報保護フォルダの削除

フォルダを削除する場合、当該フォルダにメールを保存として指定したフォルダを削除します。

1. システム管理者画面の[セキュリティ > メール > 情報漏洩防止 > フォルダ管理]をクリックします。
2. フォルダリストで削除するフィルダの**削除**をクリックします。
  - 使用中のフィルダを削除するには、先に情報保護フィルタで、当該ルールを先に削除してください。
3. フィルダの削除が完了しましたら、**保存**をクリックします。

## メール保存ポリシー

メールセキュリティと関連してメールを圧縮及び暗号化、整合性を設定します。

1. システム管理者画面の[セキュリティ > メール > 保存ポリシー]をクリックします。
2. それぞれのセキュリティの使用可否を設定します。
  - メール圧縮 - ディスクの効率性を高めるために、受信メールを圧縮して保存します。
  - メール暗号化 - 受信メールを暗号化して保存します。
  - 改ざん確認 - 受信メールの偽造及び変更可否を確認して、メールの整合性を確認します。**改ざん確認**を使用すると、Webメールのメール確認画面に改ざんを確認するボタンが表示されます。**改ざんを確認**ボタンをクリックしてメールの整合性を確認します。
3. 設定が完了しましたら、**保存**をクリックします。



メール圧縮及びメール暗号化を使用すると、システム負荷が高くなり、メールの処理に影響を与える可能性があります。ハードウェアのリソースを確認した上、使用可否を設定してください。

## SSL/TLS設定

### SMTP

SMTPプロトコルに利用されるTLS, SSL, Submissionについて設定します。

1. システム管理者画面の[セキュリティ > メール > TLS設定 > SMTP]をクリックします。
2. 受信メールと送信メールでそれぞれのTLSを設定します。
  - 使用しない - 暗号化せずに通信をします。

- TLS サポート - 相手側が暗号化をサポートする場合は、暗号化通信を行います。暗号化をサポートしない場合は、暗号化せずに普通のSMTP通信を行います。
- 3. SSLの使用可否とポート番号を設定します。
  - SSLポート設定 - SMTPプロトコルで暗号化された情報でやり取りをするか設定します。
  - SSLポート番号 - SSLポートを使用する場合はポート番号を入力します。基本ポート番号は465です。
- 4. Submissionポート使用可否とポート番号を設定します。
  - Submission port設定 - Submission portは送信専用で使用するポートです。Submission portの使用可否を選択します。
  - Submission port番号 - 基本的にSubmission portで使用するポート番号は587に指定されて表示します。
- 5. 設定が完了しましたら、**保存**ボタンをクリックします。



受信メールを使用しない、送信メールをTLSサポートに設定した場合、MS Outlook 2007で[ツール>アカウント設定>電子メールアカウントの変更>インターネット電子メールの設定の詳細設定>詳細設定]メニューで送信サーバ (SMTP) の使用する暗号化接続の種類を自動に設定してください。使用する暗号化接続の種類を自動に設定することで、Ms Outlook 2007が自動的にTLSをサポートします。

## POP

POPSは、POPの通信を暗号化します。POPとPOPSのサービスを提供するIPアドレスを設定します。

POPSのサービスポートと、POP/POPSにアクセス可能なIPアドレスを設定します。

1. システム管理者画面の[セキュリティ > メール > TLS設定 > POP]をクリックします。
2. POPSサーバポート及びPOPにアクセス可能なIPを設定します。各項目の説明は次の通りです。
  - POPSサーバポート - POPSプロトコルで使用するポートを指定します。基本ポートは995です。
  - POPアクセス可能なIPアドレス - 外部からPOPプロトコルで接続可能なIPを設定します。
  - POPSアクセス可能なIPアドレス - 外部からPOPSプロトコルで接続可能なIPを設定します。
3. 設定が完了しましたら、**保存**をクリックします。



POPサービスのみ提供したい場合は、POPアクセス可能なIPアドレスには、0.0.0.0-255.255.255.255を設定し、POPSアクセス可能なIPアドレスには空白（何も登録しない）で設定します。POPとPOPS両方ともサービスを提供する場合はPOP及びPOPSのアクセス可能なIPアドレスを全部0.0.0.0-255.255.255.255に設定します。POPSサービスのみ提供したい場合は、POPアクセス可能なIPアドレスには、空白（何も登録しない）を設定し、POPSアクセス可能なIPアドレスには、0.0.0.0-255.255.255.255を設定します。



POPサーバに対する設定は[システム > サービス > メール > プロセス > POPサーバ]で行います。

## IMAP

IMAPSは、IMAP通信を暗号化します。IMAPとIMAPSのサービスを提供するIPアドレスを設定します。

1. システム管理者画面の[セキュリティ > メール > TLS設定 > IMAP]をクリックします。
2. IMAPSサーバポート及びIMAP/IMAPSアクセス可能なIPを設定します。各項目の説明は次の通りです。
  - IMAPSサーバポート - IMAPSプロトコルで使用するポートを指定します。基本値は993です。
  - IMAPアクセス可能なIPアドレス - 外部からIMAPプロトコルに接続可能なIPを設定します。
  - IMAPSアクセス可能なIPアドレス - 外部からIMAPSプロトコルに接続可能なIPを設定します。
3. 設定が完了しましたら、**保存**をクリックします。



IMAPサービスのみ提供したい場合、IMAPアクセス可能なIPアドレスには、0.0.0.0-255.255.255.255を設定し、IMAPSアクセス可能なIPアドレスには、空白（何も登録しない）を設定します。IMAPとIMAPS両方ともサービスを提供する場合はIMAP及びIMAPSのアクセス可能なIPアドレスを全部0.0.0.0-255.255.255.255に設定します。IMAPSサービスのみ提供したい場合、IMAPアクセス可能なIPアドレスには、空白（何も登録しない）を設定し、IMAPSアクセス可能なIPアドレスには、0.0.0.0 - 255.255.255.255を設定します。



IMAPサーバに対する設定は[システム > サービス > メール > プロセス > IMAPサーバ]で行います。

## 5.3 WAS



### アクセス制限

DaouOffice サービスにアクセスするIPアドレスを設定します。

1. システム管理者画面の [セキュリティ > WAS > アクセス]をクリックします。
2. アクセス制限の使用可否を選択します。
  - 全て許可 - サービスにアクセスするIPを全て許可します。つまり、IPと関係なくサービスにアクセスすることができます。
  - 部分許可 - 許可したIPからのアクセスのみ許可します。許可しないIPからサービスにアクセスす

るとページが正常に表示されません。

3. 使用可否を**部分許可**に設定した場合、許可IPアドレスを登録後、リンク許可可否を設定します。


- 追加 - IPアドレスを入力後、**追加アイコン**()をクリックして、IPアドレスリストに追加します。許可されたIPアドレス以外DaouOffice サービスにアクセスするとページが正常に表示されません。
- 削除 - IPアドレスリストで削除するIPを選択後、**削除アイコン**()をクリックします。
- 大容量添付ファイルリンク許可 - アクセス制限の使用可否が**部分許可**で、メール受信者が許可されたIPからアクセスしない場合や、DaouOffice ユーザではない場合は、大容量添付ファイルを確認することができません。IPと関係なく大容量添付ファイルリンクを許可する場合は**大容量添付ファイルリンク許可**にチェックします。
- 開封確認リンク許可 - アクセス制限の使用可否が**部分許可**で、メール受信者が許可されたIPからアクセスしない場合や、DaouOffice ユーザではない場合は、開封確認をすることはできません。IPと関係なく開封確認を許可する場合は**開封確認リンク許可**にチェックします。
- セキュアメールリンク許可 - アクセス制限の使用可否が**部分許可**で、メール受信者が許可されたIPからアクセスしない場合や、DaouOffice ユーザではない場合は、セキュアメールを確認することはできません。IPと関係なくセキュアメールを許可する場合は**セキュアメールリンク許可**にチェックします。


4. 設定が完了しましたら、**保存**をクリックします。

1. システム管理者画面の[**セキュリティ > WAS > アクセス**]をクリックします。

2. アクセス制限の**使用可否**を選択します。

- 使用可否を**部分許可**に設定した場合、許可IPアドレスを登録します。

- 追加 - IPアドレスを入力後、**追加アイコン**()をクリックしてIPアドレスリストに追加します。許可されたIPアドレス以外は掲示板、コミュニティ、Webフォルダにアクセスすることができません。

- 削除 - IPアドレスリストで削除するIPアドレスを選択後、**削除アイコン**()をクリックします。

3. 設定が完了しましたら、**保存**をクリックします。

## セッション検証

ユーザがログインすると、ユーザのアクセスIPアドレスとセッションIDをログアウトするまで、一時的に保存します。ユーザがログアウトしていない状態のときに別のIPアドレスからの同じセッションIDでアクセスしようとする、そのIPアドレスをブロックします。ユーザがログアウトすると、アクセスIPアドレスとセッションID情報は削除されます。

1. [**セキュリティ > WAS > セッション検証**]をクリックします。

2. アクセスIPアドレスとセッションIDの一致を確認する機能(アクセス制限)の使用可否を選択します。

3. **保存**をクリックします。

## HTTPS設定

httpsプロトコルの使用可否を設定します。httpsを使用しないに設定した場合はユーザがhttpsで接続して、サービスにログインすると、ログイン成功後はhttpに戻されます。httpsを使用するに設定した場合はユーザがhttpで接続してもユーザ情報を保護するため、自動的にhttpsで接続され、ログイン成功後もhttpsの接続を維持します。ただしログイン後もhttpsの接続を維持するためには証明局証明証を事前に登録する必要があります。

1. システム管理者画面の **【セキュリティ > WAS > HTTPS設定】** をクリックします。
2. ログイン後、httpsの接続を維持する可否を選択します。  
○ 使用、使用しない(基本値)
3. **保存を** をクリックします。

## 6. 統計

---

### 6.1 概要

統計ではメールの処理方法と処理プロセスを分析した統計情報を確認することができます。統計情報を通して、送受信メールの推移や過度なトラフィックを発生させる主要原因を確認することによって、DaouOfficeの運用・管理に活用できます。

#### 統計の種類

統計情報は、種類によって推移分析と順位分析で確認できます。

- 推移分析 - 選択した期間のメールの推移を分析
- 順位分析 - 選択した期間の順位項目別のトラフィック分析

DaouOffice で提供する統計の種類は次のようになります。

- 概要 - 正常、スパム、フィッシング、ウイルスメール処理に関する統計情報の概要をメール種類別に表示します。
- 通常のメール - 許可ルールによって受信されたメールとスパム/ウイルスメールではない正常メールの統計を表示します。
- スパムメール - 管理者（又はユーザ）の遮断ルール又はスパムフィルタ（パターンフィルタ、学習型フィルタ、フィンガープリントフィルタ、ローカル学習型フィルタ）によって遮断されたメールと何らかの理由でスパムメールとして処理されたメールの統計を処理段階別に表示します。
- フィッシングメール - フィッシングメールに関する統計を表示します。
- ウイルスメール - ウイルスエンジンによってフィルタリングされたメールの統計を表示します。
- POP - POPの使用量統計情報です。
- IMAP - IMAPの使用量の統計情報です。
- CPU - 各サーバーのCPU使用量の推移を表示します。
- メモリ - 各サーバーのメモリ使用量の推移を表示します。

- ディスク - 各サーバー機器のディスク使用量の推移

## 統計情報の検索

統計情報を確認する方法は次の通りです。

1. システム管理者画面の **[統計]**メニューをクリックします。
2. 左画面の統計種類メニューで確認したい統計情報をクリックします。
3. 統計条件を選択します。
  - ドメイン選択 - ドメインを選択するかまたは、ドメイン情報を直接入力します。
  - グラフ種類 - 折れ線グラフ、棒グラフの中で選択
  - 期間 - 検索期間を選択します。
4. 統計条件の入力後、**検索**ボタンをクリックします。

## 統計情報のダウンロード

検索した統計結果をCSV、HTML、EXCELファイル形式でダウンロードすることができます。

1. システム管理者画面の **[統計]**メニューをクリックします。
2. 左画面の統計種類メニューで確認したい統計情報をクリックします。
3. 確認したい条件を入力して統計を検索します。
4. 統計情報の下段の表からダウンロードするファイル形式を選択します。
  - CSV、HTML、EXCEL
5. **保存**ボタンをクリックしてファイルを開く又は保存します。



統計情報をEXCELファイルで確認する時にはMS Excelでマクロのセキュリティを「低」に設定しなければなりません。

マクロのセキュリティを設定する方法は次の通りです。

MS Excel 2003では[ツール> オプション > セキュリティ] タブでマクロセキュリティボタンをクリックしてセキュリティレベルを低に指定します。

MS Excel 2007では[Microsoft Officeボタン > Excelオプション > セキュリティセンター]をクリックします。

MS Excel 2010では[ファイル > オプション > セキュリティセンター]をクリックします。

**セキュリティセンター設定**ボタンをクリックして**マクロ設定**をすべてのマクロを有効にするに指定します。



## 統計情報の印刷

参照した統計情報を印刷することが可能です。

1. システム管理者画面の[統計]メニューをクリックします。
2. 左画面の統計種類メニューで確認したい統計情報をクリックします。
3. 確認したい条件を入力して統計を検索します。
4. 画面の右上にある印刷ボタンをクリックすると印刷ブラウザが表示されます。
5. 印刷ボタンをクリックして統計結果を印刷します。



統計情報にデータがある場合には種類別に色で区分して印刷されます。正常に色の区別ができない場合、Internet Explorerの [ツール > インターネットオプション > 詳細設定 > 印刷]にて背景の色とイメージを印刷するを選択して印刷すると正常に出力されます。

## 6.2 メール

メールの統計では、メールの処理形態と処理の全過程を分析し、統計結果を確認することができます。

### 要約

正常メール、スパムメール、フィッシングメール、ウイルスメール処理に関する統計概要の期間別の推移を確認することができます。受信メールと送信メールに分類して統計情報を確認することができます。

### 正常メール

正常メールでは、許可ルールによって受信したメール又はスパム・ウイルスメールではないメールの統計を確認することができます。

#### 推移分析

- 正常メール - スパム/ウイルスメールではないメール
- 許可ルールによって処理されたメール

## 順位分析

- [許可メール] フィルタ名 - 期間別順位
- [正常メール] IPアドレス - 送信IPアドレスの期間別順位
- [正常メール] 送信者メールアドレス - 送信者メールアドレスの期間別順位
- [正常メール] 受信者メールアドレス - 受信者メールアドレスの期間別順位
- [正常メール] 送信者ドメイン - 送信者ドメインの期間別順位

## スパムメール

管理者（又はユーザ）の遮断ルール又はパターンフィルタ、学習型フィルタ、フィンガープリントフィルタ、ローカル学習型フィルタによって遮断されたり、スパムメールとして処理されたメールの統計をメールの処理段階別に表示します。

スパムメールは次のような段階で処理され、全段階及び、各段階別の統計を確認することが可能です。

1. 接続段階
2. SMTP段階
3. コンテンツ段階

## 全段階

スパムメール処理の全段階に対する統計を期間別推移で確認することが可能です。

- 接続段階
- SMTP段階
- コンテンツ段階

## 接続段階

### 推移分析

スパム処理段階の中で、接続段階のルールによって遮断された接続回数の統計が、下記項目別に確認できます。

- IPアドレス遮断
- IPアドレスフィルタ
- RBL
- 同時接続数制限

## 順位分析

各接続段階のルールによって遮断された上位100個のIPアドレスリストを、下記項目別に確認できます

- [IP遮断] IPアドレス - 登録されたIPアドレスのSMTP接続を遮断
- [IPフィルタ] IPアドレス - 設定時間あたりの1つのIPアドレスからのSMTP接続回数
- [同時接続数制限] IPアドレス - 1つのIPアドレスからの同時接続数
- [RBL] IPアドレス - RBL (Realtime Spam BlackList) サーバが提供するIPによって遮断されたIPアドレスの順位

## SMTP段階

### 推移分析

SMTPプロトコル段階の各ルールによって遮断されたSMTPセッション数を、下記項目別に確認できます。

- DNS検査 - EHLOドメイン、送信者ドメイン、受信者ドメイン
- SPF検査
- 送信者 - 送信者遮断、送信者フィルタ
- 受信者 - 受信者遮断、受信者フィルタ
- 同報メール応答遅延
- 送受信環境 - 最大メールサイズ、最大ホップ数、最大受信者数、最大許可セッション数、外部送信リレーIPアドレス
- メールサーバ拒否

### 順位分析

SMTPプロトコル段階のルールによって遮断されたドメイン、送信者、受信者の上位100件の確認できます。

- [EHLO DNS検査] とは- EHLOコマンドの後のドメイン有効性を検索した後、違反した際に遮断。
  - IPアドレス
  - 送信者ドメイン
- [SPF検査] - SPF検査に違反するメールを遮断
  - IPアドレス
  - 送信者ドメイン
  - 送信者メールアドレス
- [送信者ドメインDNS検査] 送信者メールアドレス - 送信者のドメインをDNS検査して有効ではない場合に遮断
- [受信者ドメインDNS検査] 受信者メールアドレス - 受信者のドメインをDNS検査して有効ではない場合に遮断
- [送信者遮断] 送信者メールアドレス - 送信者遮断リストに登録された送信者が送信したメールを遮断
- [受信者遮断] 受信者メールアドレス - 受信者遮断リストに登録された受信者が送信したメールを遮断
- [送信者フィルタ] 送信者メールアドレス - 設定時間中、デフォルト値以上のメールを送信した送信者

を設定した期間遮断

- [受信者フィルタ] 受信者メールアドレス - 設定時間中、デフォルト値以上のメールを受信した受信者を設定した期間遮断

## コンテンツ段階

### コンテンツ段階

コンテンツ段階のフィルタ項目（件名、本文、ヘッダーなど）の各ルールによってスパムメールに振り分けられた、下記項目別にメール件数の期間別推移を確認できます。

- スパムメール
- スパム疑惑メール
- 管理者定義メール

### 順位分析

コンテンツ段階の各ルールによって振り分けされたスパムメールの項目別上位100個リストを、下記項目別に確認できます。

- IPアドレス
- 送信者メールアドレス
- 処理方法 - グループポリシーの設定時、処理方法（送信、削除、隔離保存、タグ）
- 受信者メールアドレス
- フィルタ種類



処理方法はシステム管理者画面の [セキュリティ > メール > アンチスパム] にての処理方法になります。詳細な説明は[グループポリシー](#)を参照してください。

## フィッシングメール

フィッシングメールとは、個人情報などを不正に取得しようとする攻撃型スパムメールを言います。このメニューでは、フィッシング遮断ルールによって処理されたメールに関する統計を確認できます。

### 推移分析

フィッシングメールの期間別統計を確認できます。

## 順位分析

IPアドレス、送信者メールアドレス、受信者メールアドレスの順位分析を表示します。

## ウイルスメール

ウイルスフィルタ（エンジン）によって処理されたウイルスメールの統計結果を確認できます。

## 推移分析

遮断されたウイルスメールの期間別統計を確認できます。

## 順位分析

ウイルスフィルタによって遮断されたウイルスメールを上位100個まで表示します。

- IPアドレス
- 送信者メールアドレス
- 受信者メールアドレス
- ウイルス名

## POP

POP使用量に関する推移を指定した期間で確認できます。

## 推移分析

POPにログインした数とメールを閲覧した数の推移を確認できます。

- POPログイン - POPにログインした数
- POPメールダウンロード- POPを通じてメールを閲覧した数

## 順位分析

POP 使用に関する項目別順位100件のリストを確認できます。

- [ログイン] アドレス別順位
- [ログイン] IPアドレス別順位
- [メールダウンロード] アドレス別順位
- [メールダウンロード] IPアドレス別順位

## IMAP

IMAP使用量に関する推移を指定した期間で確認できます。

### 推移分析

IMAPでログインした数を期間別で確認できます。

### 順位分析

IMAP使用に関する項目別順位100件のリストを確認できます。

- [ログイン] メールアドレス別順位
- メール件数

## 6.3 システム

DaouOffice の機器のCPU、メモリ、ディスクのデータを期間別に確認することができます。システム統計は推移分析のみを提供します。

## CPU

導入サーバー別CPU使用量の推移を指定した期間で確認できます。

- System
- User
- I/O Wait
- Idle

## メモリ

メモリ使用量に関する推移を指定した期間で確認できます。

- 物理 (Physical) メモリ
- スワップ (Swap) メモリ



メモリ使用量が80%以上続く場合には適切な対応を行ってください。

## ディスク

ドメイン毎のディスク使用量に関する推移を指定した期間で確認できます。特に隔離使用率が80%以上の場合には、メールの保存期間を調節してディスクの使用率を下げることを推奨します。

## 6.4 統計レポート

管理者はシステム管理者画面にログインしなくても統計レポートを通じて送受信メールの流量及びシステム（CPU、メモリ、ディスク）の使用量などの情報を確認することができます。特定メールアドレスに統計レポートを定期的に送信することにより、DaouOffice のステータスを把握できます。追加できる統計レポートの最大件数は100個です。

次は統計レポートの設定を追加、変更、削除する方法に対する説明です。

### 統計レポートの追加

統計レポートを追加する方法は次の通りです。

1. システム管理者画面の[統計 > レポート]メニューをクリックします。
2. 統計レポートリストで追加ボタンをクリックします。
  - 種類 - 統計レポートの種類を選択します。[統計]メニューから確認できる項目として統計レポートの種類を選択します。
  - 期間 - 統計レポートを受信する統計期間を選択します。
  - 送信時間 - 統計レポートを送信する時間を設定します。
  - 言語 - 統計レポートの表示言語を設定します。
  - 統計レポート受信者 - 統計レポートを受信する受信者のメールアドレスを入力します。
3. 設定完了後、追加ボタンをクリックします。

## 統計レポート変更

統計レポートリストで統計レポート設定を変更します。

1. システム管理者画面の **[環境 > レポート]** メニューをクリックします。
2. 統計レポートリストで変更する統計レポートを選択後、変更ボタンをクリックします。
3. 各項目を変更します。
4. 変更完了後、**追加** ボタンをクリックします。

## 統計レポートの削除

統計レポートリストで統計レポートを削除します。

1. システム管理者画面の **[統計 > レポート]** メニューをクリックします。
2. 統計レポートリストで削除する統計レポートを選択後、**削除** ボタンをクリックします。

## 統計レポート設定

統計レポートの送信者を設定することができます。

1. システム管理者画面の **[統計 > レポート]** メニューをクリックします。
2. 統計レポートリストで **設定** ボタンをクリックします。
3. 統計レポート送信者画面が表示されます。送信者名とメールアドレスを入力します。
4. 入力の完了後、**確認** ボタンをクリックします。



## 7. モニタリング

---

### 7.1 概要

モニタリングでは、より円滑なサービスを提供する為に、Web訪問者数、送受信メールの処理、システムの現状と処理の履歴を確認できる機能を提供します。

モニタリングが可能な項目は次の通りです。

- 送受信メールの処理状況を把握
- 送受信メールのトラフィックを監視
- 処理メールの追跡
- システム現状把握
- 送受信の障害の検知

### 7.2 送受信メールステータス

リアルタイムステータスでは、Webメールのメール受信ステータスをリアルタイムに監視し、正常メールとスパムメール、フィッシングメール、ウィルスメールと遮断メールの割合と受信状況を確認することができます。

- メールステータス[24時間] - 24時間前までのメール送受信量を3時間単位で表示します
- メールステータス[30日間] - 30日前までのメール送受信量を日単位で表示します。

## 7.3 ログ

### メールログ

メールログでは、DaouOffice で送受信メールを処理しているステータスをリアルタイムでモニタリングすることができます。メールログの分析を通してリアルタイムトラフィックを確認して、メールの送受信を阻害するメールを瞬時にスパムメールに登録することができます。

ただし、DaouOffice の負荷を軽減するため、リアルタイムログモニタリングは最新の1000個のログに制限します。

メールの分類に応じたモニタリングの項目は次のとおりです。

- 全体メール - 送受信されるすべてのメールをモニタリングします。
- 正常メール - 送受信されるメールの中の正常メールをモニタリングします。
- スパムメール - 送受信されるメールの中のスパムメールをモニタリングします。
- フィッシングメール - 送受信されたスパムメールからフィッシングメールのみをモニタリングします。
- ウイルスメール - 送受信されたメールの中のウイルスメールのみを監視します。
- エラーメール - 送受信されるメールからエラーが発生したメールのみをモニタリングします。確認できるエラー表記は以下のとおりで、次の3つのエラーの場合に表示されます。
  - connection-reset - 接続が切断された場合
  - connection-refused - 接続が拒否された場合
  - ime-out - サーバ間の応答がない場合
- Webメール - ユーザーがWebメールでメールを使用したログ示します。当該示される内容はログイン、メール確認、移動、コピー、削除、転送、受信フォルダの作成、変更、削除します。ただし、メール確認、メール送信以外には、メールの件名を表示することはできません。
- IMAP - MAPがメールを処理したログを示しています。
  - メールのコピー、移動、削除、予約
  - メールフォルダ作成、変更、削除
- POP - POPがメールを処理したログを示しています。
  - ログイン、メールのダウンロード、メールの削除

### メールログの検索

メールログを検索することができます。電子メールログの検索結果が1000件を超える場合は、最新の1000個まで表示されます。



検索結果は、システムの負荷を軽減するために、最近の1000個だけ出力して保管期間が過ぎたメールは自動的に削除されます。



メールログの検索対象は、ログの保存期間を設定した期間の送受信ログです。メールログの保存を確認または変更するには、画面のトップに**設定**をクリックします。

## 基本検索

基本検索の方法は次の通りです。

1. システム管理者画面の[**モニタリング** > **ログ** > **メールログ**]メニューをクリックします。
2. モニタリングする下位メニューをクリックします。
3. メールログのリストの右上の検索対象を選択します。
4. 検索条件を選択します。
  - 完全一致 - 検索対象と検索語が同じメールのログを検索します。
  - 一部一致 - 検索対象のキーワードが含まれたメールのログをすべて検索します。
5. キーワードを入力します。
6. **検索ボタン**をクリックします。

## 詳細検索

詳細検索では、期間と条件を詳細に設定して、メールログを検索します。

1. システム管理者画面[**モニタリング** > **ログ** > **メールログ**]をクリックします。
2. モニタリングする下位メニューをクリックします。
3. メールログリストの右上の**詳細検索**をチェックします。
4. 詳細検索条件の設定画面が表示されたら、当該検索条件を入力します。
5. **詳細検索**をクリックします。



検索項目は、メールログのサブメニューに応じて異なります。

## スパムメール/正常メール登録

メールログのモニタリングリストで正常(またはスパム)として処理されたメールをスパム(または正常)メールとして登録し直すことができます。

追加したルールはシステム管理者画面の[**セキュリティ** > **メール** > **アンチスパム** > **コンテンツフィルタ** > **遮断ルール**]または[**セキュリティ** > **メール** > **アンチスパム** > **コンテンツフィルタ** > **許可ルール**]で確認することができます。

スパムメール又正常メール登録は、次の下位メニューで実行可能です。

- 送受信メール(全体) - スパムメールや正常メール登録
- 正常メール - スパムメール登録

- スпамメール、フィッシングメール - 正常メール登録

## スパムメールとして登録

正常メールとして処理されたメールをスパムメールとして登録します。

1. システム管理者画面の[**モニタリング** > **ログ** > **メールログ**]メニューをクリックします。
2. モニタリングする下位メニューをクリックします。
  - 送受信メール(全体)、正常メール、フィッシングメール、ウィルスメール、エラーメール
3. メールログのリストの**正常/スパム**の申告項目で**スパムメール申告**ボタンをクリックします。
4. **スパムメール登録**画面が表示されます。
5. 当該の項目を選択します。
  - ダウ技術管理者に報告 - ダウ技術のスパムメールの管理者に申告します。管理者は、そのメールを確認した後、ブロックルールを作成および配置します。
  - 遮断ルールを追加 - 送信者、件名の遮断ルールを入力した後、メールの処理方法を選択します。
6. スпамメールの設定が完了後、**確認**ボタンをクリックします。



メール処理方法については、処理ステップメールの分類を参照してください。

## 正常メール登録

スパムメールとして処理されたメールを正常に登録します。

1. システム管理者画面[**モニタリング** > **ログ** > **メールログ**]メニューをクリックします。
2. モニタリングする下位メニューをクリックします。
  - 送受信メール(全体)は、正常メール、フィッシングメール、ウィルスメール、エラーメール
3. メールログのリストの**正常/スパム申告**項目で**正常申告**をクリックします。
4. **正常メールで登録**画面がポップアップされます。
5. 項目を選択します。
  - ダウ技術管理者に報告 - ダウ技術のスパムメールの管理者に申告します。管理者は、そのメールを確認した後、ブロックルールを作成および配置します。
  - 許可ルールを追加 - 追加するルールを選択し、送信者、件名の許可ルールを入力します。
6. スпамメールの設定の完了後、**確認**ボタンをクリックします。

## メールログ更新

設定されている時間の隔離でログ情報が更新されます。**更新**をクリックするとログデータがすぐに更新されます。



メールログの更新の時間設定を確認または変更するには、画面の上段に**設定**をクリックします

## ログ設定

DaouOffice メールログ環境を設定することができます。

1. システム管理者画面の[**モニタリング** > **ログ** > **ログ設定**]メニューをクリックします。
2. ログ設定の各項目を設定します。
  - メールログ
    - 保存期間 - メールを送受信に関するログを保存する期間を設定します。ログは最大365日まで保存することができます。ログのアーカイブが長期間になると、ディスク容量を多く占め検索時にシステムに負荷が発生します。推奨値は30日です。
    - 件名表示可否 - 件名表示可否の設定は、個人情報の保護のために使用する機能です。メールログのタイトル部分の表示可否を設定します。メールログの件名表示確認は、システム管理者画面の[**モニタリング** > **ログ** > **メールログ**]で確認することができます。
    - Debug ログオプション - システムに異常があると判断される場合には、専門的なサポートの必要性によって確認するログです。
  - リアルタイムログモニタリング
    - 使用可否 - システム管理者画面の[**モニタリング** > **ログ** > **メールログ**]リアルタイムログを表示する可否を決定します。
    - ログ自動更新インターバル - [**モニタリング** > **ログ** > **メールログ**]でメールログのリストを自動的に更新する時間を設定します。時間間隔が短いと、CPUに負荷を与えます。推奨値は30秒です。
    - 本文表示機能 - ログの本文を表示に設定します。
3. 設定完了後、**保存**をクリックします。

## 7.4 システムステータス

DaouOffice がインストールされたサーバのステータスをチェックし、サーバ毎のプロセスとシステムのステータスをモニタリングすることができます。

## プロセスステータス

サーバ別にプロセスのステータスをモニタリングすることが可能です。確認可能なプロセスは tpopd、t4imapd、webmail、tmtad、tremoted、tmss-routed、search、notifierです。

1. システム管理者画面[モニタリング > システムステータス > プロセス]をクリックします。
2. サーバプロセスのステータスを確認することができます。主要機能と使用方法是次の通りです。
  - 起動(Start)/停止(Stop) - 選択したプロセスを起動又は、停止させます。
  - 再起動(Restart) - 選択したプロセスを再起動します。（但し、Webメール、searcher、notifierは、を除外）
3. 再設定(Reconfiguration) - 選択したプロセスを中止させずに、新たな設定を適用します。（但し、Webメール、searcher、notifierは、を除外）

## リソースステータス

サーバリソースのステータスをモニタリングすることが可能です。リソースとはサーバで利用可能な資源を意味し、システム負荷率及びディスク使用量を表示します。

### システム負荷率

システム負荷率を数値及び信号で表示します。

- 数値 - 基本的にシステム負荷率が10%以下の場合、現在のシステムは安定的に運用されていることになります。
- 信号表示 - システムのステータスを表示します。
  - 正常 - グリーン
  - 注意 - 黄色
  - 緊急 - 赤

### ディスクリソース

ディスクの使用量はシステム全体のディスク容量を表示します。各パーティション毎の使用量/全体容量（%）で表示します。現在の各使用量は、信号表示でステータスを確認することができます。

### レポート作成

ログ保存期間内のシステムのステータスレポートをダウンロードすることが可能です。

## メール処理ステータス

受信メールサーバから現在まで処理したメール及びフィルタリングされたIPの数など、メールサーバのステータスを項目別に確認することができます。

確認するメールサーバを選択すると、当該メールサーバのメール処理ステータスの情報が表示されます。表示する項目は次の通りです。

**表 7-1** メール処理ステータス項目

項目	説明
MTA起動時間	受信メールサーバの起動から停止するまでの総実行時間です。
実行中スレッド	受信メールサーバで実行するスレッドの数です。
処理済み	受信メールサーバの起動から現在までに送受信したメールの数です。
処理中	受信キューに保存されているメールの数です
受信済み	受信メールサーバがメールを受信した後、転送メールサーバにメールを転送した数です。
IPフィルタ	接続レベル、SMTPレベル、ウイルスフィルタのフィルタルールによってフィルタリングされたIPアドレスの数です。 IPフィルタリング、ウイルスフィルタリング
IP遮断	フィルタリングルールによって、遮断されたIPアドレスの数です。
ウイルス遮断	ウイルスメールの処理数です。
スパム	フィルタ管理でスパムコンテンツフィルタによって処理された送受信メール（全体）数と各々処理されたメール数です。 ▪ 削除、保存、警告、ログ、返信、送信、タグ

## MTAスレッドステータス

受信メールサーバであるMTAスレッドのステータスを確認することができます。

### スレッド状態表示

確認するメールサーバを選択すると、当該メールサーバのMTAスレッドのステータスが表示されます。

**表 7-2** MTAスレッドの項目

項目	説明
待機中	スレッドが実行されない状態
接続中	メールを送信するため、TCP通信段階で接続を試行している状態
SMTP Greeting状態	接続後、EHL0又はHEL0プロトコルを受信する前の状態
Mail From状態	Mail Fromプロトコルを受信した状態
Rcpt To 状態	Rcpt to プロトコルを受信した状態

項目	説明
Data状態	Dataプロトコルを受信又は、コンテンツを受信している状態
Quit状態	Quitプロトコルを受信する状態
New Session状態	Quitプロトコルの代わりにrsetプロトコルを受信し新しいセッションになっている状態
接続終了	Quitプロトコルを受信した後、TCP通信段階で接続終了する状態
認証前の状態	受信者認証を行う前の状態 受信者の存在可否をチェックする状態
認証後の状態	受信者認証を行った後の状態 受信者が存在していれば次の段階に移動、存在していなければメールを返送
IPフィルタ処理中	受信メールがIPフィルタルールによって当該IPアドレスを遮断している状態
IP遮断処理中	接続したIPアドレスを検査して遮断する状態
RBL検査中	メール接続時、当該メールのIPアドレスを利用してRBLをLookupする状態
送信者DNS検査中	送信者メールのドメインをDNS Lookupする状態
受信者DNS検査中	受信者メールのドメインをDNS Lookupする状態
送信者IPフィルタ処理中	受信メールの送信者アドレスがIPフィルタによって当該IPアドレスを遮断する状態
同時接続数制限処理中	メール送信時、同時に複数のスレッドに接続してメールを送信するソースIPアドレスを遮断する状態

## スレッドID別の状態確認

各スレッドID別に開始時間、現在ステータス、接続IPアドレスを確認することができます。

- スレッドID - tmtadプロセスのスレッドIDです。スレッドIDは固有のIDを持ちます。
- 時間 - スレッドが最初に作成された時刻です。
- 現在ステータス - スレッドの現在の状態を表示します。（例） 待機中、接続中など
- 接続IP - 各スレッドに接続したIPアドレスです。

## 遮断中のIPアドレス検索

接続段階、SMTP段階、ウイルスフィルタによって遮断されたIPアドレスリストを確認して、遮断されたIPアドレスを解除することができます。

1. システム管理者画面の[モニタリング > システムステータス > 遮断中のIPアドレス検索]メニューをクリックします。
2. 検索するサーバを選択します。
3. フィルタIPに検索するIPアドレスを入力します。
4. 検索ボタンをクリックします。





遮断された理由を確認した後、当該IPアドレス遮断を解除する場合には**解除**ボタンをクリックします。

## キューモニタリング

送受信されるメールがメールサーバの異常により、すぐに送受信ができない場合は、キューに一時的に保存されることになります。管理者はキューモニタリングでキューに保存されているメールリストを確認し、再送信及び削除することができます。

キューモニタリングは次の通り分類されます。

- 受信メールキュー - 受信メールキューに保存されるケースは次の通りです。
  - メールのサイズが大きい (512KB以上)
  - 同報メール - 受信メールキューに保存した後に処理
- 内部のメールサーバに異常がある場合、メール転送ができず、受信メールキューに一時的に保存
- 送信メールキュー - 送信メールキューに保存されるケースは次の通りです。
  - 外部に送信するメール
  - 外部メールサーバに異常がある場合、メールの転送ができず送信メールキューに一時的に保存

### キューモニタリングリストの構成

正常に処理できなかったメールのリストを確認することができます。キューモニタリングリストの上端に当該キューの合計メール件数が表示されます。

キューモニタリングリストの項目は次の通りです。

- 時間/送信IP - メール処理時間 (YYYY/MM/DD HH:mm) とメールを送信したIPアドレスです。
- 送信者 - SMTPプロトコル (mail from) 上の送信者です。
- 受信者 - SMTPプロトコル (rcpt to) 上の受信者です。
- 件名 - メール本文です。件名をクリックするとメールの本文が確認できます。
- 説明 (処理理由) - メールが正常に処理できなかった理由が表示されます。

## キュー検索

基本検索、詳細検索でキューを検索することができます。

### 基本検索

検索条件と範囲を選択してキューを検索します。最新1000件のキューから確認したいログを検索できます。

1. システム管理者画面の[モニタリング > システムステータス > キューモニタリング] メニューをクリッ

クします。

2. **受信メールキュー**又は**送信メールキュー**をクリックします。
3. キューリストの右上で検索範囲を選択します。
  - 件名 - メール本文の件名
  - 送信IP - メール送信IPです。
  - 送信者 - SMTPプロトコル (mail from) 上の送信者
  - 受信者 - SMTPプロトコル (rcpt to) 上の受信者
4. 検索条件を選択し、検索キーワードを入力します。
5. **検索ボタン**をクリックします。

## 詳細検索

期間とその他の検索条件を利用してキューを検索します。詳細検索は最新1000件だけではなく、全てのキューに対して検索します。但し、システムの負荷を減らすため、検索結果は1,000件のみ表示します。

1. システム管理者画面の[**モニタリング** > **システムステータス** > **キューモニタリング**]メニューをクリックします。
2. **受信メールキュー**又は**送信メールキュー**をクリックします。
3. キューリストの右上で**詳細検索**をチェックします。
4. 詳細検索条件の項目を選択して、検索条件に当該するキーワードを入力します。
  - 開始日/終了日 - メールが処理された日付の範囲を選択します。
  - 検索方式 - 検索条件（完全一致、部分一致）を選択します。
  - 送信者 - SMTPプロトコル (mail from) 上の送信者です。
  - 受信者 - SMTPプロトコル (rcpt to) 上の受信者です。
  - 件名 - メール件名です。
  - IPアドレス - メールの送信IPアドレスです。
5. **検索ボタン**をクリックします。

## キュー削除

キューに保存されているメール情報を削除することが可能です。削除されたメールは復元することができません。キューに保存されたメールを削除する方法は次の通りです。

1. システム管理者画面の[**モニタリング** > **システムステータス** > **キューモニタリング**]メニューをクリックします。
2. **受信メールキュー**又は**送信メールキュー**をクリックします。
3. メールリストで削除するメールを選択します。
4. リスト右上で**削除ボタン**をクリックします。

## キュー転送

キューに保存されているメールを転送することが可能です。メールを送信する方法は次の通りです。

1. システム管理者画面の[モニタリング > システムステータス > キューモニタリング] メニューをクリックします。
2. 受信メールキュー又は送信メールキューをクリックします。
3. メールリストで転送するメールを選択します。
4. リスト上段の転送ボタンをクリックします。

## 7.5 お問い合わせ/警告メール

### お問い合わせ

システム運用中に生じた問題点等は購入先のサポート宛にメール送信し、お問い合わせください。速やかにメールまたは電話にて回答いたします。

お問い合わせ方法は次の通りです。

1. システム管理者画面の[モニタリング > お問い合わせ/警告メール > お問い合わせ]メニューをクリックします。
2. お問い合わせの内容を入力します。
  - 件名 - お問い合わせの件名を入力します。
  - 質問者のメールアドレス - 質問者のメールアドレスを入力します。お問い合わせへの回答を得るために正確に入力します。
  - 返信先メールアドレス - 返信先メールアドレスを入力します。
  - 本文 - お問い合わせの内容を作成します。
3. 作成完了後、確認ボタンをクリックします。

### 警告メール設定

DaouOffice の異常が発生した場合、警告メールを指定した受信者へ自動的に送信します。

#### 警告メールが送信されるケース

警告メールが送信されるケースは、次の通りです

- 受信キューにメールが2000以上保存されている場合

- 送信キューにメールが2000以上保存されている場合
- ディスクの使用率が80%以上の場合（ディスク及び Inode 使用率）
- パターンフィルタが3日間アップデートできなかった場合
- 学習型フィルタが3日間アップデートできなかった場合
- フィンガープリントフィルタが3日間アップデートできなかった場合
- 起動されてないプロセスがある場合
- 複数台のサーバでサービスする際に、応答のないサーバがある場合
- スпамライセンス、ウイルスライセンスの終了日が残り30日を切った場合
- 統計ファイルが1日以上溜まった場合
- ログモニタリングが正常に実行されていない場合
- ウイルスエンジンが正常に実行されていない場合
- Webメールエンジンで使用するheapメモリの領域が足りない場合



警告メールのチェック周期は1時間（60分）です。但し、ディスクの使用率は、12時間ごとに確認します。

警告メールを設定する方法は次の通りです。

1. システム管理者画面の【**モニタリング** > **お問合せ/警告メール** > **警告メール**】メニューをクリックします。
2. 警告メールの**使用可否**を選択します。
3. 警告メールを受信する受信者の**メールアドレス**を入力します。
4. 警告メールの送信者名と送信者のメールアドレスを入力します。
5. 設定完了後、**保存**ボタンをクリックします。

## 8. モバイル

---

### 8.1 モバイルアプリのバージョン管理

モバイル機器別（PC、iPhone、Android携帯など）に最新のパッケージをアップロードして、ユーザーがアクセスしたときDaouOffice の更新ステータスをお知らせます。



システム管理者画面の[ドメイン/サイト管理]でサイト件名をクリックします。サイト変更画面の**提供サービスのモバイルが使用**である場合にのみ、PCのメッセージャーとモバイルwebまたはモバイルアプリを使用することができます。そのため、モバイルを使用していない場合には、モバイルに関連する情報を設定する必要はありません。

### モバイルアプリのバージョン追加

バージョンを追加する方法は次の通りです。

1. システム管理者画面の[モバイル > Appバージョン管理]をクリックします。
2. 機器のバージョンリストのトップの追加をクリックします。追加画面に移動します。
3. 各項目を入力または設定します。
  - デバイス - 機器の種類を選択します。
    - PC - 新しいバージョンのPCメッセージャーを配布する時に選択します。
    - iPhone - iOS用のアプリを配布する時に選択します。
    - Android - アンドロイドアプリを配布する時に選択します。

アンドロイドアプリを配布する時は **In-house**と **Market**を選択することができます。**In-house**はアプリのパッケージを内部サーバにアップして、ユーザがURLでサーバにあるパッケージをダウンロードする方式です。 **Market**はアンドロイドマーケット等、外部サーバにアプリのパ

パッケージをアップして、ユーザがマーケットで直接ダウンロードする方式です。

- 重要度 - アップロードするパッケージの重要度を選択します。ユーザーが更新内容を確認し、すぐに更新する場合は上を選択します。
- バージョン - アップロードパッケージのバージョンを入力します。
- アップデートメッセージ - 更新するときにユーザーに公開されているメッセージを作成します。多言語でサービスをする場合は、項目の追加をクリックして、各言語に更新メッセージを作成します。
- パッケージのアップロード - **ファイルを選択**をクリックして、アップロードするパッケージをコンピュータから選択します。
- アップデート内容 - 更新された項目を記述します。各言語でサービスをする場合は、項目の追加をクリック、各言語での更新項目を作成します。
- 備考 - 他の管理者の立場から必要な情報が把握できるように、当該内容を記録します。

4. 設定完了後、**保存**をクリックします。

## モバイルアプリのバージョン追加

追加したバージョンを変更する方法は次の通りです。

1. システム管理者画面の[モバイル > Appバージョン管理]をクリックします。
2. デバイスのバージョンのリストから変更する項目をクリックします。
3. 各項目を変更します。
4. 修正が完了後、**保存**をクリックします。

## モバイルアプリのバージョン削除

提供不要なバージョンのアプリや、無効なパッケージをアップロードした場合は、モバイルアプリのバージョンを削除することができます。

1. システム管理者画面の[モバイル > Appバージョン管理]をクリックします。
2. 機器のバージョンのリストから削除する項目を選択して、リストのトップの**削除**をクリックします。

## モバイルアプリバージョンフィルタリング

モバイルアプリバージョンを機器別にフィルタリングすることができます。

1. システム管理者画面の[モバイル > Appバージョン管理]をクリックします。
2. 機器バージョンのリストトップの**全体分類**ドロップダウンボックスをクリックします。
  - PC、iPhone、Android

## 9. その他



---

### 9.1 IPグループ設定

内部的に使用する複数のIPアドレスをグループ登録することで、セキュリティ設定などのメニューでIPアドレスを簡単に登録することができます。

#### IPグループ追加

IPグループ追加する方法は次の通りです。

1. システム管理者画面の[その他 > IPグループ] メニューをクリックします。
2. **追加**をクリックします。
  - グループ名を入力します。グループ名は2bytes以上32bytes以下で入力します。
  - IPアドレスの入力種類を選択します。
    - IPアドレスで入力 - IPアドレス形式に合うように入力をします。
    - IP範囲で入力 - 0.0.0.0 - 255.255.255.255内のIPアドレス範囲を入力します。
    - サブネットマスクで入力 - サブネットマスク形式でIPアドレスを入力します。
  - IPアドレスを入力した後、追加ボタン (  ) をクリックしてIPアドレスリストに追加します。
  - IPアドレス削除 - IPアドレスリストでIPアドレスを削除するには、IPアドレスを選択した後、削除ボタン (  ) をクリックします。
  - IPアドレス検索 - IPアドレスリストでIPアドレスを**検索**するには、リストの下位にIPアドレスを入力した後、検索ボタンをクリックします。
  - IPアドレスリストのファイルをインポート- **ファイルをインポート**ボタンをクリックして、IPアドレスリストを一度に追加します。
  - IPアドレスリストのファイルをエクスポート- **ファイルでエクスポート**ボタンをクリックして、IPアドレスリストをファイルでエクスポートします。

3. IPグループ設定完了後、**追加**ボタンをクリックします。

## IPグループ更新

IPグループリストでIPアドレスを変更します。

1. システム管理者画面の[**その他** > **IPグループ**] をクリックします。
2. IPグループリストで変更する IPグループ名をクリックします。
3. IPグループの情報を変更します。
4. IPグループの変更後、**変更**ボタンをクリックします。

## IPグループ削除

IPグループリストでIPグループを削除します。

1. システム管理者画面の[**その他** > **IPグループ**] クリックします。
2. IPグループリストで削除するIPグループを選択後、**削除**ボタンをクリックします。

## 9.2 初期化

DaouOffice がインストールされた後、内部DBに格納されている各種データを、初期化することができます。



初期化を実行すると、登録されたデータは削除されますので、初期化には十分ご注意ください。

初期化できるデータは次の通りです。

- 統計 - 統計に関連する全てのデータを初期化します。
- モニタリング - メールログ、送受信キュー、管理者作業ログの情報を初期化します。
- セキュリティ - 全段階フィルタとグループポリシーを初期化します
- 情報漏洩防止 - 情報漏洩モニタリング、情報保護フィルタの内容を初期化します。

初期化する方法は次の通りです。

1. システム管理者画面の[**その他** > **初期化**]をクリックします。
2. 初期化するリストの**初期化**ボタンをクリックします。



## 9.3 保存期間設定

PCメッセージャー、モバイルアプリでチャットした内容及び通知の保存期間を設定します。

通知保存期間を設定する方法は次の通りです。

1. システム管理者画面の [**その他** > **保存期間設定**] をクリックします。
  - 通知保存期間 - サービスの通知を保存する期間を選択します。デフォルト値は3ヶ月です。
  - チャット内容保存期間 - PCメッセージャー、モバイルアプリでチャットした内容を保存する期間を選択します。デフォルト値は1年です。
2. 設定が完了しましたら、**保存** をクリックします。



直接入力を選択する場合は最大999まで入力することができます。

## 9.4 パスワード探し設定

パスワード探し機能の使用可否を設定します。

オプション値を〈使用する〉に設定するとユーザはパスワードを忘れた場合でも探すことができます。



## 10. 管理者

---

### 10.1 管理者リスト

複数の管理者を指定してDaouOffice を管理することができます。

#### 管理者の種類

DaouOffice の管理者は2種類があります。

- システム管理者 - DaouOffice のシステム全体を管理するシステム管理者のアクセス権を持っています。システム管理者は、各サイトのサイト管理者画面に移動して、アカウント管理、部門管理、メール、アーカイブ、カレンダーなども管理することができます。
- サイト管理者 - 特定のサイト（ドメイン）に限り、アカウント管理、部門管理、メール、アーカイブ、カレンダーなどを管理することができます。サイト管理者は、サイト管理者のみアクセスすることができます。



管理者のリストから項目名（ID、ユーザー名、ドメイン、管理者リスト）をクリックすると、順序入れ替えを変更することができます。

#### 管理者の追加

新たな管理者を追加します。

1. システム管理者画面の**[管理者]**をクリックします。
2. 管理者のリストの上段の**追加**をクリックします。
3. 管理者の追加]画面で、各項目を設定します。

- 管理者タイプ - 管理者タイプを選択します。
    - システム管理者 - システム全体に対する権限を持ち、すべてのサイトを管理することができます。
    - サイト管理者 - 特定のサイト（ドメイン）のサービス設定権限を持ちます。
  - 管理者ID - 管理者を指定します。管理者は、すでに会社で作成されたアカウントである必要があります。ユーザー検索をクリックして、ユーザー名、または名でユーザーを検索します。
  - 名前 - 管理者のユーザーIDを指定すると、該当のIDのユーザー名が自動的に表記されます。
  - 言語 - 管理者画面で使用する言語を選択します。
  - 1 ページに表示するリスト数 - モニタリング、ルールなどのリストのメニューから画面に出力するリストの数を選択します。
  - 統計出力グラフの種類 - 統計画面に表示されるグラフの種類を選択します。
    - 折れ線グラフ - 各項目の変化の推移を確認するときに選択します。
    - 棒グラフ - 項目別の比較をするときに選択します。
  - セッション維持時間 - 管理者がログイン後、指定した時間内に入力等がない場合、自動ログアウトする時間を選択または入力します。
4. 入力完了後、追加をクリックします。

## 管理者の変更

管理者リストで管理者の情報を変更します。

1. システム管理者画面の【**管理者**】メニューをクリックします。
2. 管理者リストで変更する管理者IDをクリックします。
3. 管理者変更画面に移動します。情報を変更します。
4. 変更完了後、**変更**ボタンをクリックします。



インストールですと、デフォルトドメインにmailadmというシステム管理者が自動的に登録されます。mailadmは変更できません。

## 管理者の削除

管理者リストで管理者情報を削除します。

1. システム管理者画面の【**管理者**】をクリックします。
2. 管理者リストで削除する管理者を選択した後、**削除**ボタンをクリックします。



サイトを追加すると、mailadmは、サイト管理者に自動的に登録されます。mailadmは削除できません。

## 管理者検索

管理者リストで管理者を検索します。

1. システム管理者画面の【**管理者**】をクリックします。
2. 管理者リストの右上で管理者検索範囲を選択します。  
○ ID、名前
3. キーワードを入力した後、**検索**ボタンをクリックします。

## 10.2 管理者ログ

管理者は、システム管理者とサイト管理者に分かれて管理されます。各管理者がログインした後、画面を介して操作した履歴のログを保存し、監視し、管理の混乱を防止し、各管理者の責任の所在を明らかにすることができます。

管理者ログリストの構成及び検索方法は次の通りです。

### 管理者ログのリスト

管理者が作業した内容を処理順に確認することができます。管理者ログリストのエントリは、次の通りです。

- 時間 - 管理者は、“管理リスト”を処理した時間
- 管理者ID - 当該作業を実行した管理者のID
- 接続IP - 当該作業を実行した管理者の接続IP
- 履歴 - 管理者が実行した履歴パス
- リトライ - 管理者が失敗した作業の履歴である場合の再試行

## 管理履歴の検索

管理者ID及び接続IPで管理履歴を検索することができます。

1. システム管理者画面の[**管理者**>**管理者ログ**]をクリックします。
2. 管理者のリストの右上で検索項目を選択します。  
○ 管理者ID, IPアドレス
3. キーワードを入力した後、**検索**をクリックします。

## 図目次