

The logo graphic consists of two overlapping shapes: a light gray shape on the left and a dark gray/black shape on the right. The light gray shape is a rounded rectangle with a pointed top-right corner. The dark gray shape is a triangle pointing downwards, overlapping the bottom-right corner of the light gray shape.

AntiVirus

追補マニュアル

メールアーカイブ設定

目次

1 概要	5
2 更新状況	6
3 保存状況	8
4 共通設定	10
5 メール設定	11
5.1 保守状況	11
5.2 基本設定	11
5.3 アカウント	13
5.4 グループ	15
5.5 アクセス制限	17
6 アーカイブ検索	18
6.1 ログイン	18
6.2 簡易検索	19
6.3 詳細検索	20
6.4 WEBからのユーザ登録	22



1 概要

メールアーカイブの概要を説明します。

メールのアーカイブ

- ・メールのウイルスチェック、スパムチェックを行い、マウントされているストレージボリューム(論理パーティション)へメールを保存します。
- ・メールの他に、そのメールに関連する属性情報(暗号化の有無、添付ファイルの有無など)を記述されたファイルも保存します。
- ・オプションにより、メール内容を暗号化します。

検索用のインデックスの作成

- ・本日のメールデータのインデックスをサーバ内部に作成し、一定時間おきに自動更新します。
- ・本日のメールデータ以外のインデックスは各ボリューム上に作成し、1日に1回自動更新します。

主ホスト登録

- ・メールをアーカイブするには、メールホスト名の登録が必須です。

アカウント登録

- ・メールの検索を行うには、アカウントの登録が必須です。
- ・アカウントをグループ化することもできます。

検索

検索はブラウザ上よりおこないます。

- ・登録したアカウントでログインが可能です。
- ・メールが持つサーチIDと、アカウントが持つサーチIDが一致したメールを検索します。
- ・メールが持つサーチIDと、アカウントが属しているグループのサーチIDが一致したメールを検索します。
- ・管理者はすべてのメールを検索できます。

アーカイブ導入手順

- (1)メールデータおよびインデックスを保存するストレージをサーバと接続します。
- (2)上記ストレージを認識したことを確認後、マウントします。
- (3)アーカイブを開始します。

アーカイブハードウェア構成

- ・メールデータおよびインデックスを保存するストレージは別途ご用意ください。
USB HDD、iSCSIにも対応しています。
- ・サーバの管理画面からストレージの認識(iSCSIの場合)、ストレージをマウントします。

2 更新状況

アーカイブ設定画面の「更新状況」タブをクリックすると以下の画面が表示されます。

- ・メールデータは、使用中のボリュームに書き込みます。
- ・当日のインデックスについては、サーバ内部のHDDに作成します。
- ・自動更新(初期設定では3時間毎)でインデックスを追加します。
インデックスを追加したメールは検索の対象になります。
- ・当日のインデックスは、使用中のボリュームに昨日までのインデックスに追加するかたちで一日に一度自動更新されます。

●インデックス作成ログ

メールアーカイブのインデックス作成状況を表示します。

更新時刻	: インデックスを追加した時刻
種別	: 当日のメールインデックスの場合は、"mail"を表示します。 当日分のインデックスを昨日迄のインデックスに追加する場合は、"mail-merge"を表示します。
件数	: インデックス化された件数を表示します。
成否	: インデックス作成の成否(成功"Success"、失敗"Fail")を表示します。
対象ディレクトリ	: メールデータを書き込むディレクトリを表示します。 メールがない場合は表示されません。
ボリューム	: 当日のインデックスはサーバ内部のHDDのパーティション(/dev/sda1)が使われます。外部のメールアーカイブしているボリュームがSCSIインタフェースの場合、/dev/sdb1 などと表示されます。実際にマウントしたデバイス名を表示します。
空容量	: 上記ボリュームの空き容量(MByte)を表示します。

[手動作成] ボタンをクリックすると、当日のまだインデックス化していないメールデータを、追加でインデックス作成します。このことで、手動更新した時刻までのメールが検索の対象になります。

自動更新	: 選択した時間間隔で自動更新を行います。
3日以上未更新	: チェックすると、メールデータがアーカイブされているにも関わらず、3日以上インデックスが作成されない場合、警告のメールが送信されます。
スタート時刻	: 当日インデックスを作成開始する時刻を指定します。 この時刻以降は、自動更新の時間間隔毎にインデックスを作成します。

手動更新、自動更新を行っている最中はデータ検索ができません。

インデックス作成に要する時間は件数の増分に比例します。

●モジュール更新ログ

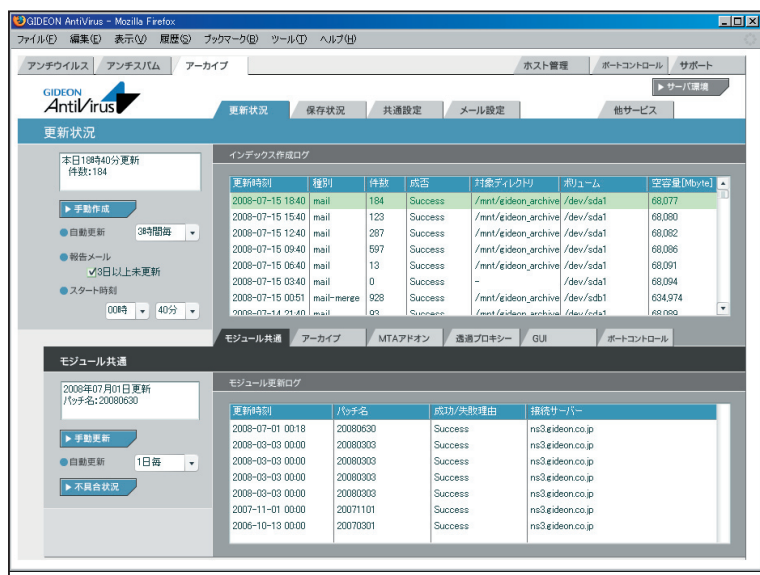
各モジュールの更新状況を表示します。モジュールとは、アーカイブが動作するために必要な実行ファイルやスクリプト、またはそれらが参照するファイルを指します。

初期設定では1日1回の自動更新に設定されています。緊急対策が必要な場合は[手動更新]ボタンをクリックし、最新のモジュールを取得してください。

既に更新済みの場合は、新たに更新されません。

[不具合状況]ボタンをクリックすると、モジュールの不具合などに関する情報サイトを表示します。
 各タブ(AntiSpam、透過プロキシ、GUI)をクリックすることでモジュールそれぞれの更新状況が表示されます。

※各モジュール内の [強制更新]ボタンは通常はクリックしないでください。



3 保存状況

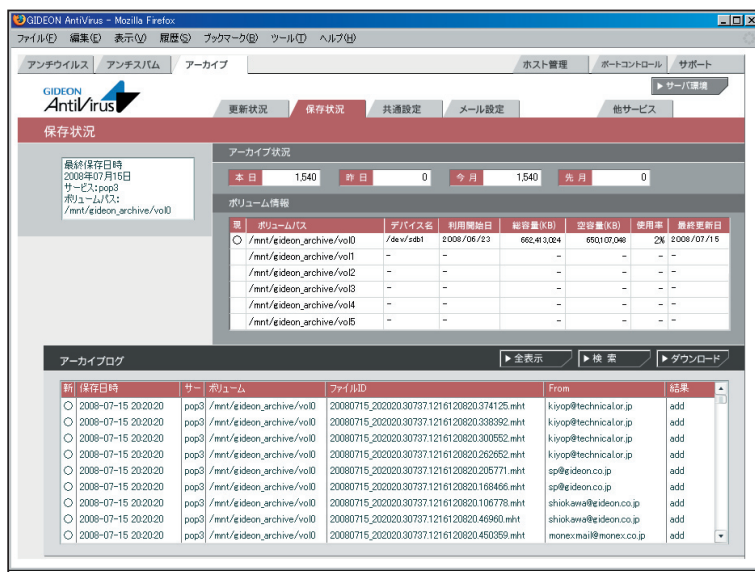
アーカイブ設定画面の「保存状況」タブをクリックすると以下の画面が表示されます。
メールをアーカイブした履歴や統計情報などを閲覧できます。

● アーカイブ状況

アーカイブ状況では、メールをアーカイブした件数を表示します。
「本日」、「昨日」、「今月」、「先月」のメールアーカイブ数を表示します。

● ボリューム情報

- 現 : 現在使用しているボリュームに○印を付けます。
- ボリュームパス : マウントしているボリューム名を表示します。
- デバイス : 論理デバイス名を表示します。
- 利用開始日 : ボリュームを利用開始した日付を表示します。
- 総容量 : 論理デバイスの総容量(KByte)を表示します。
- 空容量 : 論理デバイスの空容量(KByte)つまりメールアーカイブに使用可能な容量を表示します。
- 使用率 : データおよびインデックスで使用した容量が総容量の何%かを表示します。



● アーカイブログ

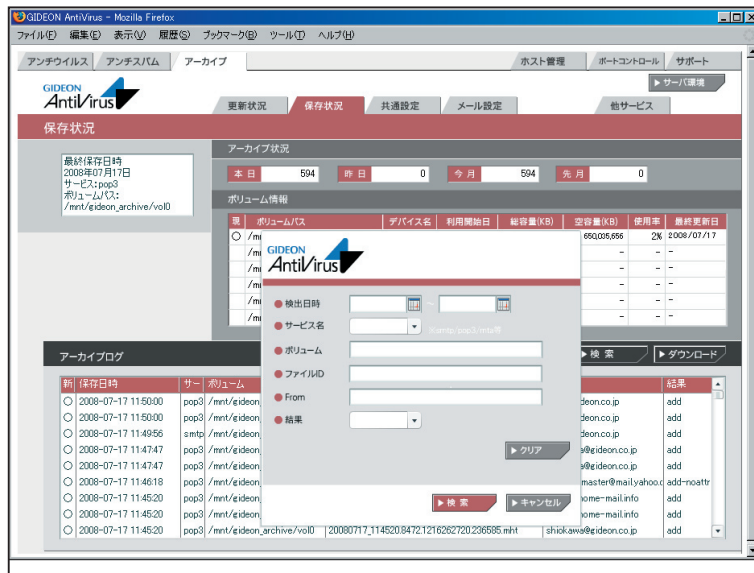
保存状況画面の下部「アーカイブログ」欄では、アーカイブしたメールの情報リストを閲覧できます。選択行をクリックすると詳細情報を表示します。各タイトル項目をクリックするとソートします。

- 新 : 初めて表示するリストの場合は○印を表示します。
- 保存日時 : メールデータをアーカイブした日時を表示します。
- サービス : mta と表示します。
- ボリューム : アーカイブの対象ボリュームを表示します。
- ファイルID : アーカイブ時につけたID でユニークになります。
- From : From のメールアドレスを表示します。
- 結果 : メールデータおよびインデックスが作成された場合,"add"
メールデータは作成したが、インデックスは作成されない場合,"add-noattr"
メールデータが作成できない場合,"fail" を表示します。

[全表示]ボタンをクリックすると、検出ログの最新リストを再表示します。

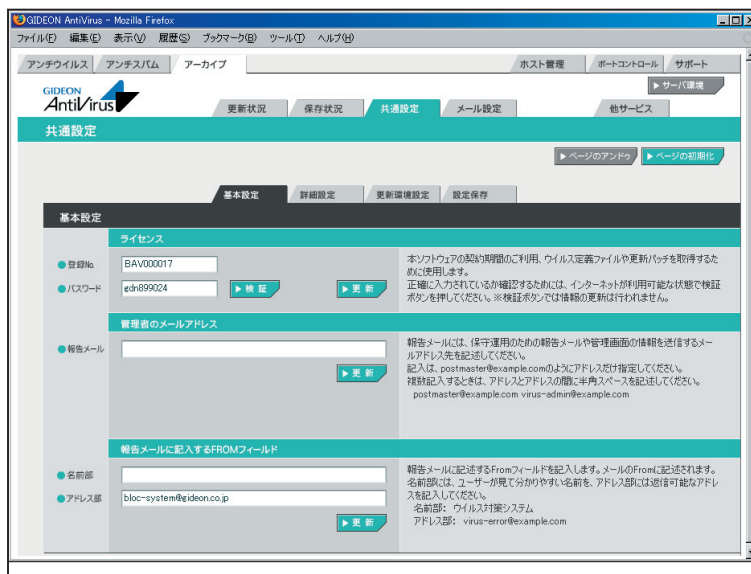
[検索]ボタンをクリックすると、項目での絞り込み検索ができます。

また、検出ログは [ダウンロード]ボタンをクリックすることで、CSV ファイルとしてクライアントPC に保存することができます。



4 共通設定

本項は、アンチウイルスでの設定と共通です。詳細は、「3.6 共通設定」の項を参照してください。



5 メール設定

5.1 保守状況

本項は、アンチウイルスでの設定と共通です。詳細は「3.7.1 保守・状況」の項を参照してください。

5.2 基本設定

メールアーカイブするための基本的な設定を行います。

●サーバリスト

ホスト別名リストに登録することで、複数の別名を同時に検索対象とすることができます。

(例)

メールサーバ名にns.domain.co.jpやmail.domain.co.jp を使っている場合、またpopサーバ(192.168.1.4または210.154.23.226)を使っている場合、test@ns.domain.co.jp はtest@domain.co.jpとして検索します。

主ホスト名:domain.co.jp

ホスト別名:ns.domain.co.jp mail.domain.co.jp 192.168.1.4 210.154.23.226

ホスト別名を複数登録する場合、上記のように半角スペースを挿入して区切ってください。

複数のメールサーバが使われている場合や、新たにメールサーバを追加したり、メールサーバ名を変更した場合、「ホスト別名」に登録するだけで、同様に検索できます。

後述の「From/To」などを検索対象とする場合、このホスト別名を追加した時点から検索するためのインデックスが自動で作成されます。

[追加]ボタンをクリックすると、新規のリストを作成し追加することができます。

既存リストの変更の場合、リストをダブルクリックすることで、項目の変更ができます。

●アーカイブポリシー

「挙動」では、アーカイブをおこなう条件を以下の3種類から選択します。

- 1.すべてのメールをアーカイブする
- 2.ウイルスチェック後のメールをアーカイブする
- 3.スパムチェック後のメールをアーカイブする

3.の場合は、ウイルスチェックの後にスパムチェックを行います。したがってウイルスチェックおよびスパムチェック後のメールをアーカイブします。

[更新]ボタンをクリックすると「挙動」を変更した場合、有効になります。

「暗号化を行う」にチェックマークを付けた場合、メールデータを簡易な暗号化を行った後でアーカイブします。

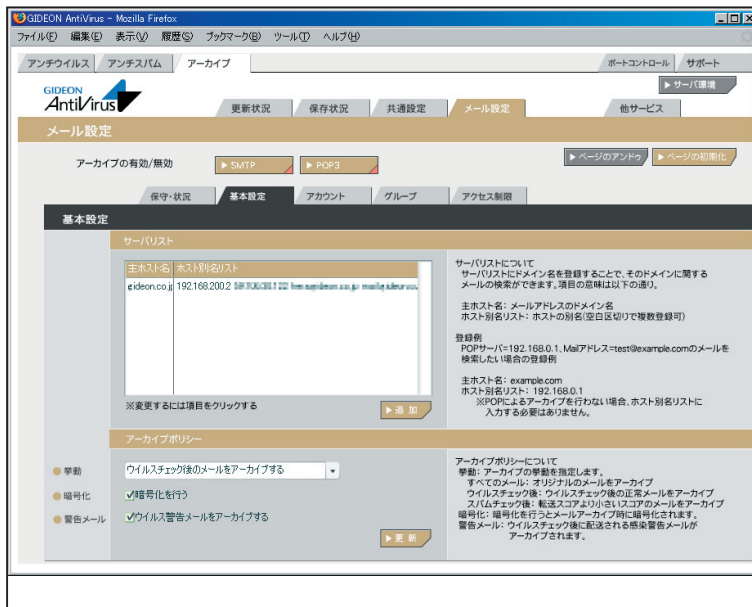
[更新]ボタンをクリックすると「暗号化を行う」有無の変更が有効になります。

注意

暗号化は、暗号強度よりも検索スピードを重視しているため、暗号強度を求める場合には、ハード的に暗号化するHDD の選択を推奨します。

「ウイルス警告メールをアーカイブする」にチェックマークを付けた場合、ウイルス検知した場合、その警告メールもアーカイブします。

[更新]ボタンをクリックすると「ウイルス警告メールをアーカイブする」有無の変更が有効になります。



5.3 アカウント

● アカウントリスト

アカウントリストに登録することで、アーカイブされたメールを検索することができます。

属性 : "有効"、"無効"、"管理者"の3種類から選択します。

"有効"を選択すると、各々のアカウントで登録したサーチIDのメールを検索することができます。

"無効"を指定すると一切検索できなくなります。

"管理者"を指定するとすべてのメールを検索できます。

"管理者"の場合はサーチIDリストに登録する必要はありません。

注意

一般のユーザは、"管理者"では登録しないでください。

アカウント : 通常はメールアカウントを使用します。test@domain.co.jp などのメールアドレスを使います。

サーチID リスト : メールアカウントを登録します。

(例)

test@domain.co.jp が、別名としてtest1@domain.co.jp とtest2@domain.co.jp を使用している場合

以下のように登録すると複数の別名を同時に検索できます。

アカウント :test@domain.co.jp

サーチID リスト :test@domain.co.jp test1@domain.co.jp test2@domain.co.jp

この例で、更に「5.2 基本設定」の項で説明した「サーバリスト」に次のように登録されている場合

主ホスト名 :domain.co.jp

ホスト別名 :ns.domain.co.jp

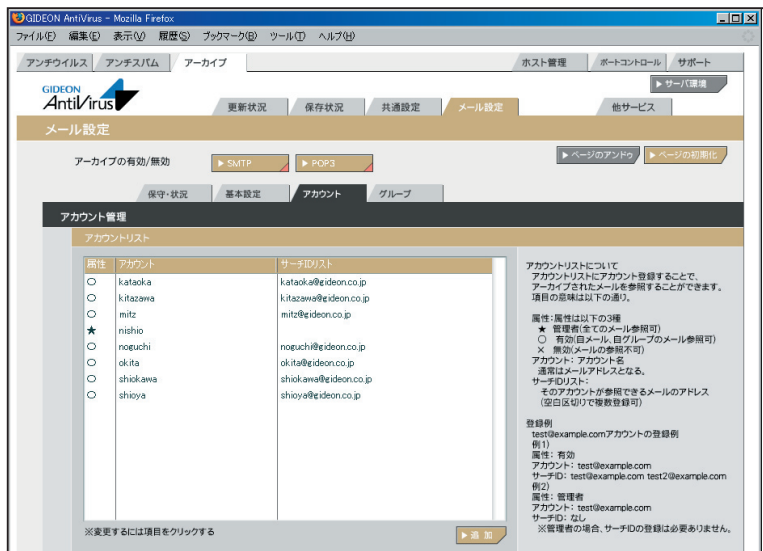
以下のアカウントも同時に検索します。

test@ns.domain.co.jp、test1@ns.domain.co.jp、test2@ns.domain.co.jp

[追加] ボタンをクリックすると、新規のリストを作成し追加することができます。

既存リストの変更の場合、リストをダブルクリックすることで、項目の変更ができます。

メールアーカイブ設定



5.4 グループ

● グループリスト

グループリストに登録することで、アカウントをグループ化することができます。

(例)

営業関連グループにsalesA、salesB、salesCの3名が所属している場合、次のように登録します。

グループID : sales

アカウントリスト : salesA@domain.co.jp salesB@domain.co.jp salesC@domain.co.jp

サーチID リスト : sales@domain.co.jp

名称を"sales" とすると、

「グループID」 は"sales"とし、「アカウントリスト」には、利用アカウントを

salesA@domain.co.jp salesB@domain.co.jp salesC@domain.co.jp のように登録します。「サーチ

IDリスト」はsales@domain.co.jp とすることで、"sales" グループは

salesA、salesB、salesC の登録アカウントすべてで検索できます。

同様に、部課単位に定義すると課別のアカウントをまとめて部の検索も可能になります。

個々の組織内部統制ルールに従って、メール検索範囲をグループ化することで可能になります。

直前のサーバのIPアドレスをチェックしてスパム判定を行います。

※「アカウントリスト」に登録するに先立ち、前項の「5.3 アカウント」でアカウントの登録をしてください

[追加]ボタンをクリックすると新規のリストを作成し追加することができます。

既存リストの変更の場合、リストをダブルクリックすることで、項目の変更ができます。

重要

グループ登録には慎重な判断の上で、登録できる範囲と権限に留意ください。

情報の機密保持に関しては当社製品の責任範囲ではありませんのでご了承ください。

メールアーカイブ設定

The screenshot shows the 'メール設定' (Mail Settings) page in the GIDEON AntiVirus web interface. The 'グループ管理' (Group Management) section is active, displaying a table of groups. The table has three columns: 'グループID' (Group ID), 'アカウントリスト' (Account List), and 'サーチIDリスト' (Search ID List). The table contains 15 rows of data. To the right of the table, there is a sidebar with instructions on how to register groups and accounts.

グループID	アカウントリスト	サーチIDリスト
admin	mitz nishio shiokawa	admin@eideon.co.jp
all	kataoka kitazawa mitz nishio noguchi okita shiokawa	all@eideon.co.jp
spambox	shiokawa	spambox@eideon.co.jp
tech	mitz nishio shiokawa	tech@eideon.co.jp
announce	kataoka kitazawa mitz nishio noguchi okita shiokawa	announce@eideon.co.jp
info	kataoka kitazawa nishio noguchi okita shiokawa	info@eideon.co.jp
jobs	kataoka nishio	jobs@eideon.co.jp
meeting	kataoka kitazawa mitz nishio noguchi okita shiokawa	meeting@eideon.co.jp
office	kataoka nishio noguchi shiyoa	office@eideon.co.jp
query	kataoka kitazawa nishio noguchi shiyoa	query@eideon.co.jp
sales	kataoka kitazawa nishio noguchi okita shiyoa	sales@eideon.co.jp
sp	kataoka kitazawa nishio noguchi okita shiokawa	sp@eideon.co.jp

※変更するには項目をクリックする

グループ管理

グループリスト

グループID: test-groupの登録例

グループID: test-group
アカウントリスト: test@example.com, test2@example.com
※アカウントとして登録されていないデータは登録されません。
サーチID: test-group@example.com

※この登録によりtest@example.com, test2@example.comのアカウントがtest-group@example.comのメールを参照することができます。

5.5 アクセス制限

アーカイブ検索iSearch のアクセスをIP アドレスで制約することができます。

記述がない場合、すべてのクライアントからアクセスが可能です。

記述がある場合、記述したクライアントからのみアクセス可能です。

記述の方法は以下の通り。

host= クライアントのIP アドレス

host= クライアントのIP アドレス/ ネットマスク

記述例：

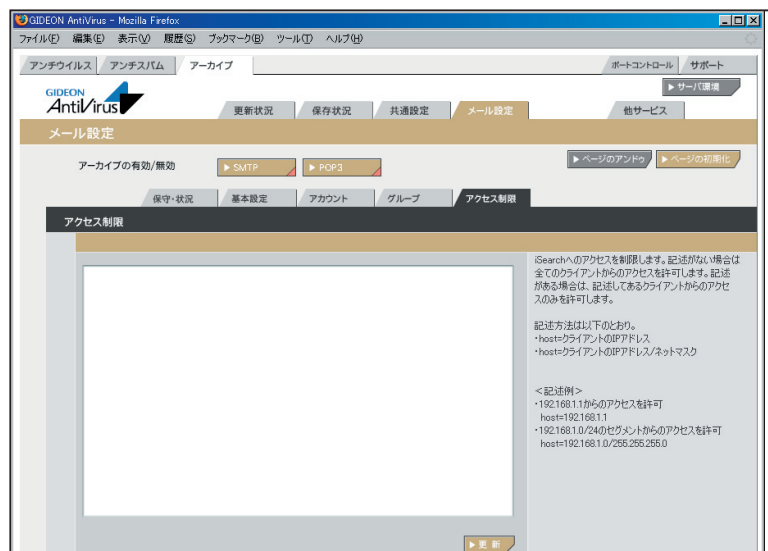
・192.168.1.1 からのアクセスを許可

host=192.168.1.1

・192.168.1.0/24 のセグメントからのアクセスを許可

host=192.168.1.0/255.255.255.0

[更新] ボタンをクリックすると、リストを更新できます。



6 アーカイブ検索

6.1 ログイン

アカウント毎のログイン画面のアクセスには、以下のURLを入力します。

http://アーカイブサーバのIP:777/isearch

例えば、アーカイブサーバのIPが"192.168.1.201"の場合、

http://192.168.1.201:777/isearch

アカウントが登録されているとそのアカウントでログインができます。

アカウント登録の際に、「属性」を"無効"と設定したアカウントはログインできません。

IDと Passwordは最大16文字まで使用可能です。



6.2 簡易検索

管理者と一般のユーザとでは検索できる範囲が異なります。

管理者は「検索文字列」のみで検索します。すべてのメールが検索対象となります。

一般のユーザは「検索文字列」か「アカウントのサーチID」もしくは「自分が所属するグループのサーチID」を対象に検索します。

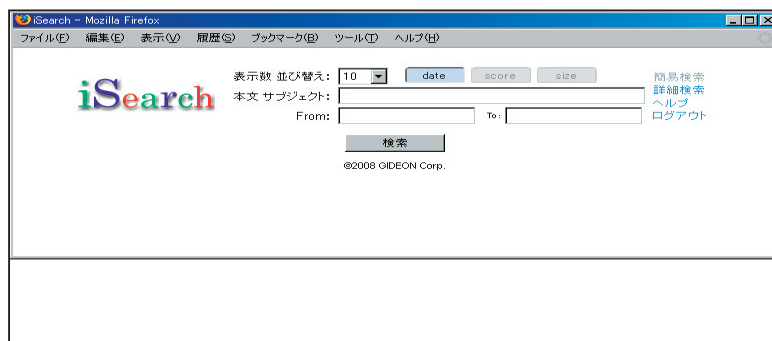
- 表示数** : 1 ページに表示される検索結果数を表します。10 ~100 まで選択可能。
- 並び替え** : 日付順(date)、スコア順(score)、サイズ順(size) にソートします。
- date** : 日付の新しい順にソートします。
- score** : スコアの多い順にソート。スコアは該当メールに含まれる「検索文字列」の出現頻度を表します。
- size** : ファイルサイズが多い順にソートします。
- 本文 サブジェクト** : 「メール本文」「メールサブジェクト」の内容を検索します。
複数キーワードをAND 条件で検索することができます。
- From** : From に含まれる文字列を検索します。複数キーワードを指定することはできません。
- To** : To に含まれる文字列を検索します。複数キーワードを指定することはできません。

転送の対象となるメールアドレス (例 : user-one@example.com) を行頭から指定し、半角スペースに続いて転送先メールアドレス (例 : spam-admin@example.com) を指定します。

転送先メールアドレスは半角スペースで区切ることで複数指定可能です。

また、転送対象のメールアドレスは、@ から始めることで、ドメインが一致するメールアドレスをすべて転送対象にすることができます。

@example.com spam-admin@example.com



6.3 詳細検索

管理者と一般のユーザとでは検索できる範囲が異なります。

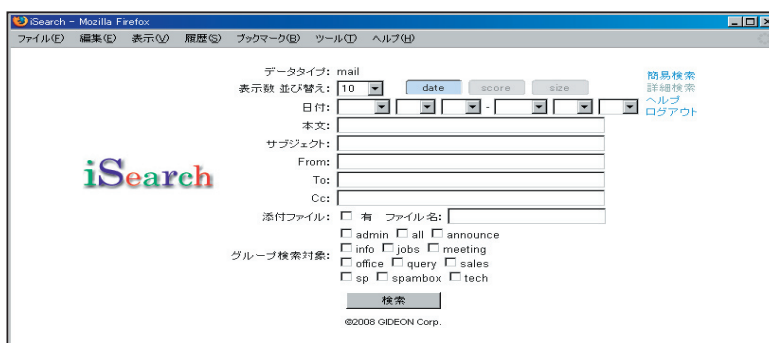
(1) 管理者

- ・グループにチェックが入っていない場合は、
検索文字列のみで検索(サーチID は関係なく、すべてのメールが検索対象)
- ・グループにチェックが入っている場合は、
「検索文字列」and「グループのサーチID」で検索

(2) 一般ユーザ

- ・グループにチェックが入っていない場合は、
「検索文字列」and「アカウントのサーチID」で検索
- ・グループにチェックが入っている場合は、
「検索文字列」and(「アカウントのサーチID」or「グループのサーチID」)で検索

- データタイプ : 将来メール以外のデータに対応したときのため。現在はmailのみ。
- 表示数 : 1 ページに表示される検索結果数を表します。10 ~100 まで選択可能。
- 並び替え : 日付順(date)、スコア順(score)、サイズ順(size) にソートします。
- date : 日付の新しい順にソートします。
- score : スコアの多い順にソート。スコアは該当メールに含まれる「検索文字列」の出現頻度を表します。
- size : ファイルサイズが多い順にソートします。
- 日付 : 左側のみ日付入力: この日付以後のメールが検索されます。
右側のみ日付入力: この日付以前のメールが検索されます。
両方の日付入力: 指定範囲内のメールが検索されます。
- 本文 : 本文の内容が検索されます。
- サブジェクト : サブジェクトが検索されます。
- From : From が検索されます。
- To CC : To Cc が検索されます。
- 添付ファイル : 添付ファイルがあるメールが検索されます。
- グループ検索対象 : (1) 管理者 全てのグループが表示されます。
(2) 一般ユーザ 自分が属しているグループのみ表示されます。



6.4 WEBからのユーザ登録

● ログインユーザ登録

ログイン画面の「ユーザ登録」リンクをクリックすることでユーザ登録およびパスワードの変更ができます。

(1) 仮パスワード送信

入力したメールアドレスに仮パスワードを送信します。

以下の条件のときに仮パスワード送信が行われます。

- ・すでにアカウントが登録されている場合、登録メールアドレスのみ仮パスワード送信します。
- ・アカウントを登録していない場合、メールアドレスのドメイン部がサーバリストに登録されている場合のみ、仮パスワード送信します。

(2) 送信されたメール例

このメールはiSearch システムのユーザ登録画面から送信されました。

1 時間以内に以下のURL にアクセスし、本パスワード登録を行ってください。

<http://192.168.0.125:777/cgi-bin/main.cgi?func=294&session=hoge>

メールアドレス :name@domaina.co.jp

仮パスワード :xxxxxx

by iSearch copyright 2008, GIDEON Corp.

(3) 仮パスワードログイン

メールに記載したURL にアクセスし、仮パスワードでログインします。

メール送信から1 時間以内にログインしないと仮パスワードは無効になります。

(4) 本パスワード登録

本パスワードを登録します。ここで指定したパスワードでiSearch システムにログインできます。



追補マニュアル
「メールアーカイブ設定」

2009年3月30日 第1版発行

発行所 株式会社ギデオン
〒223-0056
神奈川県横浜市港北区新吉田町3448-4
<http://www.gideon.co.jp/>

本誌からの無断転載を禁じます。
乱丁、落丁はお取替え致します。上記発行所までご連絡下さい。

Copyright(c)2009 GIDEON Corp.
Printed in Japan