# <sup>ギデォン</sup> ブロック システム

່ທ ໂ **(**) U 

ギデォン BLOC system メールアーカイブ Plus ギデォン BLOC system メールアーカイブ

GIDEON

共通ユーザーズマニュアル

### はじめに

この度は、製品をお買い上げいただきまして、誠にありがとうございます。 本ユーザーズガイドは、「ギデオン BLOC system メールアーカイブ Plus」「ギデオン BLOC system メールアーカイブ」共通ユーザーズマニュアルです。

対象読者は、システム管理者、ネットワーク管理者です。本製品の運用・管理を行うには、システム管理やネットワークの知識が必要になります。製品概要、各種設定方法、導入後の運用上の注意事項などを説明していますので、ご使用前に必ずご一読いただきますようお願いいたします。

■著作権など

本ユーザズマニュアルの著作権は株式会社ギデオンに帰属します。

GIDEON、ギデオン、GIDEON AntiVirus、GIDEON AntiVirus BLOC systemの名称およびロゴは 株式会社ギデオンの商標または登録商標です。

Kaspersky Lab、カスペルスキーラブの名称およびロゴはカスペルスキー社の商標または登録商標です。

The Linux kernel is Copyright 1991-1996 Lius Torvalds and is licensed under the term of the GNU General Public License.

その他、記載されている会社名、製品名は各社の商標および登録商標です。

## 目次

	ご注意	9
	取扱い上のご注意	10
	梱包内容の確認	10
第	章 製品のご紹介・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	11
第2	2章 接続と動作	13
	2.1 接続方法について	13
	2.1.1 シンプルなLAN構成	13
	2.1.2 LAN側にプロキシなどがある場合	14
	2.1.3 LAN側にメールサーバなどがある場合	14
	2.2 接続方法についてのご注意	15
	2.3 接続とセットアップ	16
	2.3.1 インターネット接続を停止させないセットアップ	16
	2.3.2 インターネット接続を一時的に停止してセットアップ	20
	2.4 外部インターネット接続確認と動作検証	22
	2.5 管理・設定画面のアクセス方法	23
	2.6 初回のログイン	24
	2.7 ログイン	25
	2.8 管理画面について	26
	2.9 PortControl	27
	2.9.1 基本設定	28
	2.9.2 Port指定	31
第3	3章 アンチウイルス設定・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	33
	3.1 更新状况	33
	3.2 検出状況	34
	3.3 共通設定	35
	3.3.1 基本設定	35
	3.3.2 詳細設定	37
	3.3.3 更新環境設定	38
	3.4 メール設定	39
	3.4.1 保守 ・ 状況	40
	3.4.2 基本設定	41
	3.4.3 詳細設定 1	43
	3.4.4 詳細設定2	45
	3.4.5 ホワイトリスト・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	47
	3.4.6 チェックリスト・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	49
	3.5 ウェフ設定	50
	3.5.1 保守・状況	51
	3.5.2 基本設定	52
	3.5.3 詳細設定	54 50
	3.0.4	50
	3.5.5 フェック対象	50
	36 スキャンコードー覧	50
		00

第4章 アンチスパム設定
4.〕更新状況
42 検出状況
43 共通設定
441保守・状況
4.4.2 基本設定 67
4.4.3 詳細設定1
4.4.4 詳細設定2
4.4.5 転送メール
4.4.6 ホワイトリスト・・・・・ 77
4.4.7 ブラックリスト・・・・・ 79
4.4.8 チェックリスト 81
第5章 メールアーカイブ設定
5.1 概要
5.2 更新状況
5.3 保存状況
5.4 共通設定
5.5 メール設定
5.5.1 保守状況
5.5.2 基本設定
5.5.3 アカウント・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
5.5.4 グループ
5.5.5 アクセス制限
5.6 アーカイブ検索
5.6.1 ログイン
5.6.2 簡易検索
5.6.3 詳細検索 98
5.6.4 WEBからのユーザ登録······100
第6章 他サービス
6.1 他サービス
6.1.1 保守・状況・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
6.1.2 基本設定
6.1.3 ホワイトリスト
6.2 PortControl固有設定 ·······107
6.3 ボリューム
6.4 iSCSI ······ 111
第7音 サーバ 環境
/.I.I 保守・状況
7.1.3 奉平設正 116
第8章 サポートツール
8.1 メールテストツール
8.2 サポート接続ツール

第9章 個別設定方法 ······	123
9.1 接続方法	123
9.2 固定IPアドレスの設定	126
9.3 困った時の設定	128
9.3.1 ゲートウェイの設定	128
9.3.2 設定の初期化	128
第10章 トラブルシューティング・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	129
10.1 動作しないときは	129
10.2 よくある質問と回答	129
10.3 お問い合わせ	131

### ご注意

- ① 本書の一部または全部を弊社に無断で転載することは禁止されております。
- ② 本書の内容については万全を期しておりますが、万一ご不審の点がございましたら、弊社まで ご連絡くださいますようお願いいたします。
- ③ 本製品および本書を運用した結果による損失、利益の逸失の請求等につきましては、②項に 関わらず弊社ではいかなる責任も負いかねますので、あらかじめご了承ください。
- ④ 本書に記載されている機種名、ソフトウェアのバージョンなどは、本書を作成した時点で確認 されている情報です。本書作成後の最新情報については、弊社までお問い合わせください。
- ⑤ 本製品の仕様、デザイン及びマニュアルの内容については、製品改良などのために予告なく 変更する場合があります。
- ⑥ 本製品を使用して収納したデータが、ハードウェアの故障、誤動作、その他どのような理由によって破壊された場合でも、弊社での保証はいたしかねます。万一に備えて、重要なデータはあらかじめバックアップするようにお願いいたします。
- ⑦ 弊社は、本製品の仕様がお客様の特定の目的に適合することを保証するものではありません。
- ⑧ 本製品は、人命に関わる設備や機器、および高い信頼性や安全性を必要とする設備や機器 (医療関係、航空宇宙関係、輸送関係、原子力関係等)への組み込み等は考慮されていません。これらの設備や機器で本製品を使用したことにより人身事故や財産損害等が発生しても、弊社ではいかなる責任も負いかねます。
- ⑨ 本製品は日本国内仕様ですので、本製品を日本国外で使用された場合、弊社ではいかなる責任も負いかねます。また、弊社では海外での(海外に対してを含む)サービスおよび技術サポートを行っておりません。

### 取扱い上のご注意

### ■本製品を正しく安全に使用するために

同梱のハードウェア取扱い説明書をよくお読みいただき、記載事項にしたがって正しくご使用くだ さい。

### 梱包内容の確認

パッケージに以下の付属品が含まれていることを確かめてください。 不足品があるときは、販売店または弊社テクニカルサポートまでご連絡ください。

- BLOC 本体
- 電源コード
- ブロック システム ユーザーズマニュアル(本書)
- ハードウェア取扱い説明書
- ソフトウェア使用許諾書
- BLOCハードウェア保証書
- ソフトウェアライセンス及びサポートサービス証書
- PortControl 本体
- ACアダプター
- PortControl ハードウェア保証書

#### ■ 本製品の特長

- SMTP/POP3に対応したスパムメール対策、ウイルス対策専用ネットワークアプライアンス機器
- 透過ブリッジ接続で既存のネットワーク設定を変更することなく導入可能
- OSに依存しないため、混在したOS環境のネットワークでも利用可能
- わかりやすく操作しやすい管理インターフェース
- 定義ファイル、モジュールは自動更新でメンテナンスフリー

#### ■ アンチスパム機能

- SMTP/POP3でのスパム判定に対応
- スパムメールの転送および削除機能(SMTP/POP3対応)
- 日本語スパム対応。独自スコアリングロジックによるスパム誤検知率の低減
- メールヘッダ解析、メッセージの本文解析、メールシグニチャデータベース、DNSルックアップ、 URLデータベース解析、ユーザ定義(ホワイトリスト、ブラックリスト)などによる複合解析
- 企業のセキュリティポリシーにあわせたスパム判定スコアのカスタマイズが可能
- スパム検出ログの閲覧、CSV形式での各種ログのダウンロード

#### ■ アンチウイルス機能

- メール送受信(SMTP·POP3)、HTTPのウイルスを検知・削除
- あらゆる圧縮形式(約900種類以上)/255階層の多段圧縮に対応
- メールでの通知機能
- ユーザ、またはドメイン名毎にウイルスチェックのOn/Offが可能
- ソフトウェアモジュールの自動アップデート
- ●新種のウイルスにも1時間以内に対応するカスペルスキー社のコアエンジンを採用 (約25万種のウイルスパターン、新種ウイルスに数分間隔で対応)

#### ■ メールアーカイブ機能

- メールヘッダ・本文・添付ファイルテキストまでインデックス化
- マルチストレージボリュームの検索

ストレージまたはパーティションごとにボリュームを付与することができます。 アーカイブデータ管理や全文検索対象を絞り込む(ボリューム指定する)ことにより検索効率を上げ ることができます。

- 全文検索
- 検索アクセス制限
- メールアカウントグループ化

※以降「ギデオン BLOC system メールアーカイブ Plus」本体および「ギデオン BLOC system メールアーカイブ 」本体を「BLOC」と呼称します。



### 2.1 接続方法について

本章では、BLOC および PortControl の接続方法、接続確認、管理画面のログイン方法について説明します。

### 2.1.1 シンプルなLAN構成

メールサーバが外部にある場合や、ホスティングサービスを利用している構成です。主にクライアントからメール受信(POP3) する時に、ウイルス・スパム検知します。クライアントからの送信(SMTP) 時 にもウイルス・スパムを検知します。

#### ルータのLANポートを複数使用している場合

ルータのLAN ポートから、直接クライアントに接続しているネットワークの場合、ハブを導入して図 2.1.1-1 のネットワーク構成に変更します。



PortControl をルータとハブの間に導入し、図2.1.1-2 のような構成にします。このネットワーク構成では、クライアントから外部のインターネットにアクセスする場合、監視パケットがBLOC を経由します。 同様に外部からクライアント端末にデータが送信される場合、監視パケットがBLOC を経由します。



※PortControl およびBLOC の導入によりクライアントからこれまでと同様にインターネットに接続 でき、メールの送受信、ホームページの閲覧などができれば動作していることになります。

### 2.1.2 LAN側にプロキシなどがある場合

内部クライアントからHTTP で外部インターネットと接続する際に、HTTP プロキシサーバ経由でア クセスする環境の場合、PortControl をクライアントとHTTP プロキシサーバとの間に接続してくだ さい。このような場合は、図2.1.2 のようにBLOC を導入します。

この場合、BLOC がプロキシ経由で更新ファイルをダウンロードできるように設定する必要がありま す。「3.3.3 更新環境設定」のページを参照して、プロキシ経由で更新を行えるように設定してください。



### 2.1.3 LAN側にメールサーバなどがある場合

内部クライアントから、内側のメールサーバやWEB サーバにアクセスしてメール送受信、WEB メールの利用などをおこなっている場合は、図2.1.3のようにPortControlをメールサーバとハブとの間に接続してください。



### 2.2 接続方法についてのご注意

### ルータと直結したネットワークの場合

下図のようにルータと直接接続されたネットワーク・クライアントは、BLOC を経由しないため、ウイル ス対策 (スパム対策)をすることができません。



### ルータとハブをバイパスで接続した場合

下図のようにルータとハブをBLOC を経由せずバイパスで接続した場合、正常にネットワークのウイ ルス対策 (スパム対策)をすることができません。



#### 固定IPアドレスを設定している場合

BLOC を接続したときに、BLOC が自動でIP アドレスを取得できる (DHCP クライアントとして動作 している)場合は、初期設定の状況で正常に動作します。

個々のネットワーク端末に固定IP アドレスを設定している場合は、BLOC にも固定IP アドレスを設 定する必要があります。「9.2 固定IP アドレスの設定」のページを参照して設定してください。

### 2.3 接続とセットアップ

稼動中のネットワークにBLOCを接続してセットアップする場合、数分間インターネットと接続ができ なくなり、メールの送受信、ホームページの閲覧ができません。

セットアップ方法には、インターネット接続を停止させないセットアップと、一時的に停止させてセット アップする2 種類あります。

### 2.3.1 インターネット接続を停止させないセットアップ

インターネット接続を停止させずにセットアップする場合、以下のようなネットワーク構成に追加変更 します。

●セットアップに必要なもの BLOC、PortControl、クライアントPC、LAN ケーブル



### 《手順 1》 Portcontrol の接続

PortControlの電源を入れます。

PortControlの接続ポート「L3」と、クライアント側のハブとをLANケーブルで接続します。 PortControlの接続ポート「WAN」と、ルータとをLANケーブルで接続します。

PortControlの接続ポート「L1」と、BLOCのLANコネクタとをLANケーブルで接続します。



#### 《手順2》 電源コードの接続

付属の電源コードをBLOCのACコネクタとAC100Vのコンセントに挿します。



#### 《手順3》 電源をON

接続が全て終了したら、BLOCの電源を入れます。 セットアップには、数分かかります。正常にセットアップが完了すると、ビープ音でお知らせします。

BLOC system

### 《手順4》 ネットワーク構成の変更

セットアップが終了したら、ネットワークの構成を変更します。

1. PortControlをルータと既存ネットワークの間に接続します。

PortControlの電源を入れます。

PortControl背面の「L3」ポートと、クライアント側のハブとをLANケーブルで接続します。 PortControlの「WAN」ポートと、ルータとをLANケーブルで接続します。

- BLOCをPortControlに接続します。
   PortControlの「L1」ポートと、BLOCのLANコネクタとをLANケーブルで接続します。
   BLOCの電源を入れます。
- ネットワークの構成変更が終了したらセットアップ完了です。



### 2.3.2 インターネット接続を一時的に停止してセットアップ

インターネット接続を一時的に停止するセットアップの場合、図2.3.2 のようにネットワークの構成を変更します。

●セットアップに必要なもの BLOC、PortControl、LAN ケーブル



図2.3.2

#### 《手順1》 PortControlの接続

PortControlの電源を入れます。

PortControlの「L3」ポートと、クライアント側のハブとをLANケーブルで接続します。

PortControlの「WAN」ポートと、ルータとをLANケーブルで接続します。

PortControl背面の「L1」ポートと、BLOCのLANコネクタとをLANケーブルで接続します。



### 《手順2》 電源コードの接続

付属の電源コードを、BLOCのACコネクタとAC100Vのコンセントに挿します。



### 《手順3》 電源をON

接続が全て終了したら、BLOCの電源スイッチを押して電源を入れます。 セットアップには、数分かかります。 正常にセットアップが完了すると、ビープ音でお知らせしインターネットと接続が可能になります。

### 2.4 外部インターネット接続確認と動作検証

インターネットへの接続およびウイルス検出の動作検証をかねて、BLOC を経由しているクライアン トPC から、WEB ブラウザで以下の外部URL ヘアクセスしてください。

http://www.eicar.org/anti\_virus\_test\_file.htm

アクセスができたことをWEB ブラウザで確認します。アクセスに成功するとブラウザの一部に画面 2.4-1 が表示されます。



画面2.4-1

「Download area using the standard protocol http」にある「<u>eicar.com</u>」をクリックすると、画面2.4-2 のウイルス警告が表示されます。このウイルスファイルは無害なので、ダウンロードしても問題ありません。これでウイルス検出の動作検証が完了します。





### 2.5 管理・設定画面のアクセス方法

クライアントPCからBLOCの管理画面にアクセスします。 WEBブラウザで、以下のように外部URLとポート番号(555)を指定します。

#### http://www.google.co.jp:555/

BLOCに特定のIPアドレスを指定している場合には、直接IPアドレスとポート番号(777)を指定します。 (画面 2.5-2)

http://192.168.1.100:777/

セキュリティが気になる場合は、HTTPSでポート番号(999)を指定します。

https://192.168.1.100:999/

※WEBブラウザの設定で、上記のポート番号を許可するようにしてください。



画面2.5-1



#### 画面2.5-2

### 2.6 初回のログイン

BLOCご購入後、はじめて管理・設定画面にアクセスすると、画面2.6 パスワード設定画面が表示されます。同梱されている「ソフトウェアライセンス及びサポートサービス証書」に記載されているパスワードを入力します。(本製品は、ライセンス情報として、お客様登録No、パスワードが出荷時に設定されています。)

次回からログインするときには、このパスワードを入力する必要があります。



画面2.6

### 2.7 ログイン

管理・設定画面にアクセスすると、画面2.7 ログイン画面が表示されます。 初回のログインで設定したパスワードを入力します。パスワード入力後[ログイン]ボタンをクリックしま す。

### パスワードの変更

既存のパスワードを入力して[変更]ボタンをクリックします。 画面2.7が表示されます。初回のログインと同様にパスワードを再設定します。(半角英数20文字以内)



画面2.7

### 2.8 管理画面について

ログインすると、画面2.8 管理・設定画面が表示されます。



画面2.8

#### ■主に日常の管理で必要なメニュー

タブ名	説 明
更新状況	スパムDB、ウイルス定義ファイルやモジュールの更新状況を一覧 表示
検出状況	スパム検出、ウイルス検出の履歴情報を一覧表示
サーバ環境	負荷やエラーメッセージなどの状況を表示

#### ■初期に設定および確認するメニュー

タブ名	説 明
共通設定	ライセンス(お客様登録No, パスワード)の設定を確認 HTTPプロキシ経由で更新する場合の設定を 警告メール、報告メールの送信先アドレスの設定
メール設定	警告メールなどのメッセージのカスタマイズ
ウェブ設定	ウイルスをチェックしないファイルを確認
サーバ環境	BLOCに固定IPアドレスを指定

### 2.9 PortControl

画面2.8管理・設定画面の右上の「ポートコントロール」タブをクリックすると画面2.9が表示されます。



画面2.9

	説 明
基本設定	PortControlとBLOCを接続する際の設定をおこないます。初期 設定では、各種設定なしで自動で接続します。
ポート指定	個別ネットワークに適したパケットフィルタリングをします。

#### 確認

**BLOC**: 「ギデオン BLOC system メールアーカイブ Plus」本体および 「ギデオン BLOC system メールアーカイブ」本体の略称です。

### 2.9.1 基本設定

● ポートコントロール (PortControl) 接続

PortControl 接続/ 切断:

PortControlとBLOCとの内部通信の「接続/切断」をおこないます。 [PortControl]ボタンの右下が赤くなっていると「接続」している状態を表します。 初期設定は「接続」になっています。BLOCを再起動した場合にも設定を保持します。

### IPアドレス・プライオリティ自動設定:

通常はチェックマークを付けてIPアドレス・プライオリティ自動設定(ON)の状態にします。 手動で設定する場合はチェックマークを消してOFFの状態にしてから、「PortControlに付 与するIPアドレス」「自IPアドレス」「プライオリティ」を設定します。

PortControlとBLOCとの間では、独自の内部通信をおこないます。1個のPortConrolには 最大8台までBLOCを接続できます。

PortControlはカスケード接続が可能です。複数のPortControlをカスケード接続する場合、各PortControlのIPアドレス、各BLOCに割り当てられるIPはユニークである必要があります。

### PortControlに付与するIPアドレス:

PortControlとBLOCは同一ネッットワークセグメントのIPアドレスを設定します。 PortControlが接続されているLANのネットワークセグメントと同じである必要はありません。

同一PortControlに接続しているすべてのBLOCで同じIPアドレスを指定してください。 自動設定では、クラスBのローカルIPアドレス(i.e. 172.xx.xx.xx)が付与されます。

### -----例-----

「PortControlに付与するIPアドレス」に"172.31.0.1"を設定した場合、同一PortControlに接続しているすべてのBLOCで同じ"172.31.0.1"を指定します。

### 自IPアドレス:

PortControlとBLOCの内部接続のためのBLOC用のIPアドレスを設定します。 「PortControlに付与するIPアドレス」と同じネットワークセグメントである必要があります。 また同一PortControlに接続しているBLOCは、各々異なるIPアドレスを指定してください。 自動設定では接続順にクラスBのローカルIPアドレス(i.e. 172.xx.xx.xx)が付与されます。

### プライオリティ :

1から8迄の数字を設定します。最も優先度が高いのは1で、次が2の順になります。 2台以上のBLOCが同じ転送ポートを指定した場合、「プライオリティ」が一番高いBLOC がその転送ポートのパケットを処理します。自動設定ではBLOCを接続した順にプライオリ ティが設定されます。

#### -----例-----

BLOCを2台接続し、マスタBLOCがダウンした場合、スレイブBLOCに切り替えるHAシステム 構成ができます。転送ポートの指定がマスタ、スレイブで同じ場合、マスタBLOCに「プライオリティ1」、 スレイブBLOCに「プライオリティ2」を設定します。

プライオリティが高いマスタBLOCが転送ポートのパケット処理を行います。マスタBLOCがダウンした 場合、自動的にスレイブBLOCがパケット処理を行うよう切り替わります。

入力後、[更新]ボタンをクリックしてください。[更新]ボタンをクリックすることで、「PortControlに付与するIPアドレス」「自IPアドレス」「プライオリティ」の値が適用されます。 [更新]ボタンをクリックしてから、PortControlとBLOCが動作し始めるまでに3分程度かかります。

● 転送ポート

転送「ポート番号」を指定すると、そのポート番号のパケットを、BLOCが接続されている物理ポートL1もしくは物理ポートL2に転送します。

「SMTP」「POP」「HTTP」に関連づけされたポート番号を入力します。

複数の値を設定する場合には、各値の間に半角スペースを挿入します。最大10件のポート番号を設 定できます。

複数BLOCの転送ポート番号を登録した場合、プライオリティが最も高いBLOCにのみポートデータを 転送します。このBLOCの接続を切り離したりダウンした場合、自動的にPortControlから既存登録情 報が削除されます。同様のテーブルを登録している別BLOCがあれば、この別BLOCにポートデータを 転送します。

入力後、[更新]ボタンをクリックしてください。[更新]ボタンをクリックすることで、PortControlは該当ポート番号のパケットをBLOCに転送します。

[更新]ボタンをクリックしてから、PortControlとBLOCが動作し始めるまでに3分程度かかります。

#### ● ファームウェアパッチの適用

PortControlのファームウェアのパッチを適用します。

#### 注意

ファームウェア適用中は、PortControlおよびBLOCの電源をOFFにしないでください。電源をOFFにした場合、ファームウェアが破損するのでPortControlが全く動作しなくなります。

[適用]ボタンをクリックした後、「ファームウェアの更新が成功しました。」のダイヤログが表示された 場合、PortControlの電源コネクタを抜き差し(OFF-->ON)してください。電源を抜き差しした後、 PortControlが復帰する迄約3分程度必要です。 パッチを適用した際に、ダイアログに以下のメッセージが表示されることがあります。

最新のファームウェアです。更新する必要はありません:

---> すでに最新のファームウェアである場合に表示されます。

#### PortControlが見つかりませんでした:

---> PortControlにIPを割り当てていない場合に表示されます。

BLOCとPortControlが正しく接続されていることを確認してください。

- ダウンロードしたファイルが壊れています:
- ---> ダウンロードしたファイルが壊れている場合に表示されます。 再度「適用」ボタンをクリックしてダウンロードを試みてください。
- ファームウェアファイルの取得に失敗しました:
- --> ファームの取得に失敗した(サーバに接続できなかった)場合に表示されます。
   httpプロキシやファイアウォールなどの設定により、ダウンロードサイトにアクセスできない場合があります。
- ファームウェアの更新が失敗しました:
- ---> その他(TFTPに失敗したなど)の場合に表示されます。
  再度[適用]ボタンをクリックして、ダウンロードを試みてください。
  同様のエラーが発生した場合、メーカーのサポートにご連絡下さい。

### 2.9.2 Port指定

PortControlでは個別ネットワークに適した効率のよいパケットフィルタ設定ができます。

GIDEON AntiVirus	- Mozilla F	irefox						
ァイル( <u>E</u> ) 編集( <u>E</u> )	表示⊙	移動( <u>G</u> )	ブックマー	ク(旦) ツール(工)	ヘルプ(円	)		
CIDEON								
Antil/iri	JS							
ポートコント	ロール							
								トページのアンドゥ
	基本設定	- ボ-	-ト指定					F ( 303 31 3 F ( 305 0) 10
ポート指定								
	ポート登	録·削除						
	ID	drop/pa	S TCP L	JDP ポート番号	範囲	IPアドレス		PortControlでは簡易なパケットフィルタリングを行う
AFT A		drop	•				▶登録	かできます。 (1)登録
								ID:登録するIDを指定します。 IDを指定することで任音の位置に登録できます。
●削除	ID						▶削除	登録一覧の最上位に登録する場合は、既存の
								TCP/IPセッションは切断されませんが、最上位 以外の登録時は一度切断されます。
● 登録一覧	ID	drop/pas	s TCP	UDP ポート番	号範囲	IPアドレス		drop/pass: dropは廃棄、passは通過を表しま TCP・TCP/IPパケットを表します
	10	drop	-	0 1-10		-		UDP: UDP/IPパケットを表します。
	30	drop	-	O 21-30		-		※TCP/UDP両方とも選択しない場合は、すべ の全てのIPパケットを表します。
								ポート番号範囲:フィルタするポート番号範囲を
								増圧します。 IPアドレス:フィルタするIPアドレスを指定します。
								<ol> <li>(2)削除</li> <li>(1)・削除するIDを指定します。</li> </ol>
								登録一覧の最上位のデータを削除する場合は、
								既存のTCP/IPセッションは切断されませんが、 最上位以外の削除は一度切断されます。
								(3)登録一覧 ま二されている したねとつっていがあたい。 長がたっ
					_			マッチしたフィルタが通用されます。IDは表示を行う ごとに10間隔で再割り当てされます。
								@GIDEON C
		1	1	1	面	面292	,	ごとに10間隔で再割り当てされます。 Форсо

#### ● ポート登録・削除

PortControlは、指定のパケットを破棄したり、BLOCへの転送で特定のIPアドレスのみスルーするなどの設定ができます。前述の「基本設定」の転送ポート設定が適用される前にここで登録した設定が優先的に適用されます。

#### -----例-----

「基本設定」でHTTP転送ポート番号を"80"と設定し、「ポート指定」でIPアドレス"192.168.1.1"の"80" 番ポートをスルーした場合、IPアドレス"192.168.1.1"との通信パケットは双方向(送信元、受信先のどち らかのIPアドレスが"192.168.1.1"である場合)で"80"番ポートをスルーします。IPアドレス"192.168.1.1"と の通信パケットはBLOCに転送しません。

み適用します。

「TCP」および「UDP」ともにONにしない場合、全てのパケットを対象にします。 「ポート番号範囲」はフィルタするポート番号の範囲を指定します。例えば、128番から256 番までをフィルタ対象とする場合、128-256を指定します。設定しない場合はポートでの フィルタはおこないません。

「IPアドレス」はフィルタするIPアドレスを指定します。設定しない場合はIPアドレスでの フィルタはおこないません。

削除: 既に登録されているフィルタリストの中から削除するフィルタ「ID」を指定します。

登録一覧 :登録されたフィルタの一覧を表示します。

表示されている上位から順番にフィルタのマッチングをおこない、最初にマッチしたフィルタ が適用されます。

表示「ID」の値は再表示する(別画面からこの画面に戻ってくる)ごとに10の値の間隔で リナンバリングします。

登録リストの最上位にフィルタを(追加)登録する場合、現在接続中のTCP/IPセッションはそのまま接続されます。登録リストの中途もしくは最後尾に(追加)登録する場合は、現在接続中のTCP/IPセッションは切断されます。

登録リストの最上位のフィルタを削除する場合、現在接続中のセッションはそのまま接続されます。登録 リストの中途もしくは最後尾のフィルタを削除する場合、現在接続中のセッションは切断されます。

### 3.1 更新状況

●ウイルス定義ファイル更新ログ(画面3.1 上段部分)

ウイルス定義ファイルの更新状況を表示します。

初期設定では1時間毎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、最新の定義ファイ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。

「報告メール」は、ウイルス定義ファイルの更新状況をメールでお知らせするものです。 「3日以上未更新」は、3日以上スパムDBの更新がない場合に管理者宛にメール送信します。 「最新定義ファイルでない」は、システム上のウイルス定義ファイルが最新でない場合に管理者宛に メール送信します。

[対応状況へ]ボタンをクリックすると、ウイルス定義ファイルに関する情報サイトを表示します。

●モジュール更新ログ(画面3.1下段部分)

各モジュール(修正パッチモジュール、アップデートモジュールなど)の更新状況を表示します。 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(AntiVirus、透過プロキシー、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(「MTAアドオン」はBLOCでは使用されません)。

		-						
アンチウイルス アンチスパム				サポート				
Antil/irus	更新状況 検出	出状況 共通設定	メール設定	▶ サーバ環境 ウェブ設定 他サービス				
更新状況								
本日15時10分更新	ウイルス定義ファイル更新ログ							
1172048520	更新時刻	定義ファイル名	成功/失敗理由	接続サーバー				
▶ 手動更新	2007-02-21 15:10	1172048520	Success	dnl-jp1.kaspersky-labs.com				
CONTRACT (AT BRAT	2007-02-21 13:28	1172042400	Success	dnl-jp4.kaspersky-labs.com				
●日期更新 1時間母 ▼	2007-02-08 11:11	11,0910260	Success	dni-jpl.kaspersky-labs.com				
<ul> <li>報告メール</li> <li>V3日以上未更新</li> </ul>								
最新定義ファイルでない								
▶対応状況へ								
	TAL-114138 A-53		3 8 8 fort2					
エペーール 井澤			ノ / 近回ノロキシ					
モジュール共通	∓ジューⅡ.毎新⊓グ							
	C/ 1/ 3C#10/							
2007年02月01日更新 パッチ名:20070201			and the file of the time of the					
2007年02月01日更新 パッチ名:20070201	更新時刻	パッチ名	5%30/大照理田	接続サーバー				
2007年02月01日更新 パッチ名:20070201	更新時刻 2007-02-01 00:00 2006-10-12 00:00	パッチ名 20070201 20061011	Success	抵抗サーバー ns3gideon.co.jp				
2007年02月01日更新 パッチ名:20070201 ▶ 手動更新 ● 目動更新	更新時刻 2007-02-01 00:00 2006-10-13 00:00	パッチ名 20070201 20061011	Success Success	接続サーバー ns3.gideon.co.jp ns3.gideon.co.jp				
2007年02月01日更新 バッチ名:20070201 ト 手動更新 自動更新 1日語 ・	更新時刻 2007-02-01 00:00 2006-10-13 00:00	パッチ名 20070201 20061011	Success Success	掲載サーバー ne3gideon.co.jp ne3gideon.co.jp				
2007年02月01日東新 バッチ名:20070201 > 手動変新 - 日載変新 - 日載変新 - 1日毎 ・ - 木具合数況	更新時刻 2007-02-01 00:00 2006-10-13 00:00	パッチ名 20070201 20061011	Success Success	?我成分→パー ns3gideon.co.jp ns3gideon.co.jp				
2007年12月01日至新 1/57名:20070201 > 手動変新 自動変新 1日音 • 本用会状況	更新時刻 2007-02-01 00:00 2006-10-13 00:00	パッチ:名 20070201 20061011	Success Success	≇Rstj—J,~ ni3 eldeonco.jp ni3 eldeonco.jp				
2007年12月01日至新 バナチ名:20070201 <b>&gt; 手加芝布</b> 自動更新 <b>1日毎 *</b>	更新49名/ 2007-02-01 00:00 2006-10-13 00:00	パッチ名 20070201 20061011	Success Success	≇Rstj−J/~ ro3eideoncojo ro3eideoncojo				
2007年12月01日至新 パッチ名:20070001 ・ 手動変新 ・ 自動変新 ・ 不具合状況	更新特別 2007-02-01 0000 2006-10-13 0000	パッチ名 20070201 20061011	But/J PERXMEN	Tately-D/- m3 eldenco jp m3 eldenco jp				
2007年12月01日至新 1/5年名:20070201 <b>&gt; 手到正年</b> 自然更新 1日音 • <b>&gt; 不具会状况</b>	更新特別 2007-02-01 0000 2006-10-13 0000	パッチ名 20070201 20061011	SUCCESS Success Success	Tatisfy-D/- misiaideon.co.jp noi3aideon.co.jp				

### 3.2 検出状況

BLOCが検出したウイルスの一覧を表示します。

「検出統計情報」では、「本日」「昨日」「今月」「先月」「総合計(検出開始時からの合計)」に分類して、各期間のウイルス検出件数を表示します。また検出頻度の高いウイルス名を、各期間ごとに表示します。

[月次詳細]ボタンをクリックすると、当月を含め、過去の月毎のウイルス検出サマリレポートを閲覧できま す。また管理者宛にそのレポートを送信することができます。

※「検出ログ」では最新の1000件までの検出ウイルスを表示します。

#### ● ダウンロード

検出ログを、http、smtp、pop3ごとに CSV ファイルとしてダウンロードできます。 ダウンロードする際は、『検出ログのダウンロード』ダイアログ中のリストより選択してからダウンロードボ タンをクリックしてください。ダウンロードした CSV ファイルには各ウイルスが検出された際の詳細な情 報が含まれています。

#### ● 詳細情報

検出ログのリストをクリックすることで、検出された際の詳細な情報が閲覧できます。 [検索]ボタンをクリックすると、表示項目の内容で検索することができます。 [全表示]ボタンをクリックすると、検索表示から元の一覧表示に戻ります。

アンチウイルス アン	チスパム						サポート
Antil/irus	-	更新状況 検出	状況 共通語	没定	メール設定 ウェブ設	定 他サービス	・サーバ環境
検出状況							
		検出統計情報					
最終ウイルス検5 2007年02月22日 サービス:smtp	3	本日 104	昨日	3 今月	107 先月	0 総合語	it 10
ワイルス名: Virus.MSWord.Z	mk.j	ウイルス名 今 1位 Virus.MSWord	/MPC-based	検出数	ウイルス名 5 先 1位		検出数
		月 2位 EICAR-Test-F	ile		4 月 <sub>2位</sub>		
		3位 Virus.MSWord.0	Diass.bd		3 3位		
				月次詳細	ウイルス名		検出数
					総 1位 Virus.MSW	Vord.VMPC-based	
					合 2位 EICAR-Te	est-File	
					3位 Virus.MSV	Word.Class.bd	
検出ログ				_	▶ 全表示	▶検索	▶ ダウンロート
		- 6017 <i>4</i>	_=_/_I.⊄	td2E	From	To	
2007-02-22	095214 em	to Visue MSWard Zerk i	27 1723	2/26/2154	Loopalaine Baideanaine	Long Street Back	and an in
2007-02-22	095214 sm	to Virus MSWord Furby b			kanadi ng kathan cola	<b>Complete physics</b>	ano in
2007-02-22	09:52:14 sm	to Virus MSWord Bur			kang himat kidemoola	<b>Lungthing Bailt</b>	encole
2007-02-22	095214 sm	to Virus MSOffice Halfcros.a			Long bing Printers and	Long Strength and	and a second
2007-02-22	09:52:14 sm	to Virus MSWord TNT.c			kang bing by the model	<b>Aussisting</b> (1995)	ancois 1
2007-02-22	09:52:14 sm	to Virus MSWord VMPC-based			investigation of the interview	<b>Longthing Bailt</b>	ancoia
2007-02-22	095214 sm	to Virus MSWord Mykah			Long-bins (Fridesman)	Long birth Print	and a second
2007-02-22	09:52:14 sm	to Virus MSWord Mary			kang dinarky ideas coig	kang phine physics	ano in
2007-02-22	095214 sm	tp Virus.MSWord.Margaret			kanashimathalakancola	<b>konsthimethold</b>	ancoia



BLOC system

### 3.3 共通設定

ライセンス情報や管理者のメールアドレスなどを設定します。

各種設定を行った後に[このページを以前の設定に戻す]ボタンをクリックすると、設定の変更を行った 状態の一つ前の状態に戻します。

[このページを初期設定に戻す]ボタンをクリックすると、このページで設定可能な項目を初期設定(工 場出荷時)に戻します。

### 3.3.1 基本設定

### ● ライセンス

「(お客様)登録No」「パスワード」が設定されていることを確認してください。 製品ご購入時に設定されていない場合、またはライセンスを変更された場合には入力が必要となりま す。「(お客様)登録No」および「パスワード」を入力後、[更新]ボタンをクリックしてください。

[検証]ボタンをクリックすると、入力された「(お客様)登録No」「パスワード」が正しいかどうか確認できます。誤って入力した場合は再入力してください。

※契約期間が終了している場合には認証できないことがあります。

#### ● 管理者のメールアドレス

「報告メール」には、保守運用のための報告メールや更新情報を送信するメールアドレスを登録します。 「警告メール」には、ウイルス検出時の警告メールを送信するメールアドレスを登録します。 複数アドレスを指定する場合、下記のように半角スペースで区切ります。

aaa@domain.jp bbb@domain.jp

メールアドレスを入力後、[更新]ボタンをクリックしてください。 初期設定値:なし

※ネームサーバで解決できない内部メールサーバなどへは送信できない場合があります。

#### ●警告メールに記入するFROMフィールド

警告メールに受信時のメール「From:」に記載される名前とそのメールアドレスを指定します。 「名前部」は、このシステムから送信されたことが判る名前を指定します。 「アドレス部」は、実際にアカウントが存在するアドレスを指定します。 「名前部」および「アドレス部」を入力後、「更新」ボタンをクリックしてください。 初期設定値: 「名前部」なし 「アドレス部」導入システム毎に異なるため、メール返信可能なメールアドレスを設定してください。


# 3.3.2 詳細設定

## ● メール送信で使用するSMTPサーバ

警告メールなどを送信するために使うメール(SMTP)サーバを指定します。 例えば、自社の正式なメールサーバ名(FQDN)が、mail.domain.jpであれば、そのメールサーバ名を 指定します。 入力後、[更新]ボタンをクリックしてください。 初期設定値:なし

## ● テンポラリディレクトリ

BLOCが一時的に使用するディスク領域です。絶対パスで指定します。容量は100MB以上必要とします。通常は変更の必要はありません。 初期設定値:/var/tmp(通常は変更不要) 変更する場合は入力後、[更新]ボタンをクリックしてください。

## ● エラーとして扱わないAntiVirusエンジンの戻り値

ある特定のエラーで警告メールを抑制する数値を指定します。 入力後、[更新]ボタンをクリックしてください。 初期設定値:なし

## ● 感染メール保存ディレクトリ設定

BLOCでは使用しません。

🕹 GIDEON AntiVi	us - Mozilla Firefox	
ファイル(E) 編集(E)	表示(2) 履歴(3) ブックマーク(8) ツール(1) ヘルブ(1)	0
アンチウイルス	アンチスパム サポ	K
GIDEON Antil/iru	▶ サー/EE S 更新状況 検出状況 共通設定 メール設定 ウェブ設定 他サービス	業境
共通設定	► <>077/P2 ► <>01	初期化
詳細設定	基本設定 詳細設定 更新建境設定	
	メール送信で使用するSMTPサーバー <th>メールサ</th>	メールサ
	テンポラリディレクトリ	
	/var/tmp     本リフドウェアが一時的に使用するディスが接触です。絶対パスで指定します       容量は少なとも1000kg/tebL上必要です。       ・東京	。空き
	エラーとして扱わないAntiVirusエンジンの戻り値	
	ある特定のエラーで警告メールなどを送信しないため(記述します。	
	感染メール保存ディレクトリ設定	
	保存容量 Mir/te <b>&gt; 又 等</b>	
	000	DEON Corp.
F		

画面3.3.2

# 3.3.3 更新環境設定

BLOCはHTTPを利用してモジュールおよび定義ファイルを更新します。 BLOCから特定のHTTPプロキシサーバを経由しないと外部のURLにアクセスできない場合には、 「更新のためにHTTPプロキシーを使用する」を選択してください。 「プロキシーのIPアドレス」「ポート番号」は必須項目です。 「ID」「パスワード」が設定されている場合には、それぞれ入力が必要です。

入力後、[更新]ボタンをクリックしてください。 初期設定値:更新のためにHTTPプロキシーを使用しない



# 3.4 メール設定

SMTPおよびPOP3でのウイルスチェックをする場合の管理・設定を行います。

「SMTP」はインターネットやイントラネット上で、電子メールを送信するためのプロトコルで、ここではその サービスを意味します。サーバ間でメールのやり取りをしたり、クライアントがサーバにメールを送信する 際に用いられるサービスです。

「POP3」は、インターネットやイントラネット上で、電子メールを保存しているサーバからメールを受信する ためのプロトコルで、ここではそのサービスを意味します。

「ウイルスチェックの有効/無効」の[SMTP]または[POP3]ボタンをクリックして次画面で有効または 無効を設定します。

[SMTP]ボタン、[POP3]ボタンのそれぞれ右下三角がオレンジ色になっている場合は有効になっている状態です。

😻 GIDEON AntiVir	ıs - Mozilla Firefox	
ファイル(E) 編集(E)	表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルブ(H)	<b>o</b>
アンチウイルス フ	<b>シンチスパム</b>	サポート
Antil/irus	更新状況 検出状況 共通設定	>サーバ環境 メール設定 ウェブ設定 他サービス
メール設定		
ウィルス	Fェックの有効/無効 トSMTP トロP3	▶ ページのアンドゥ ▶ ページの初期化
	保守·状況 基本設定 詳細設定1 詳細設定2	ホワイトリスト チェックリスト
基本設定		
	受信者への警告メール設定	
● 挙動 ● Subject	- 感染メールの場合、受信者にメールを送信しない ・ 感染メールの場合、智客をつけて送信する 書音メールに感染メールのハッグーを添付する - ✓ Virus warnine: + ✓ 感染メール Subject	ウイルスメールの使き者に近時する警告メールの設定です。 『本文』になりたきなことで感染メールの一部の情報をメールに埋か込むこ とができます。以下のタグが使用できます(スアンダーパーとつ話例)。 _SUBJEOT_ 感染メールのSubject _VIRUS_SENDER_ 送信者のメールアドレス(各称される可能性)
• • •	× ウイルス警告! × ・ × ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	▶ 更 新
	送信者への警告メール設定	
Subject	<ul> <li>送信者に警告メールを送信しない(推奨)</li> <li>●送信者に警告メールを送る</li> <li>Virus warning:</li> </ul>	ウイルスメールの送信者に送信する苦告メールです。ただし、送信者のメ ールアドレス信約称られている可能性が使ります。よって苦告メールを送 信しない設定が推奨となっています。 ア本文点に少なるなことで認知メールの一部の情報をメールに埋め込むこ
● 本文	************* ウイルスを検出しました ***********************************	とができます。以下のタグが使用できます(_はアンダーバー2つ連続)。 SUBJECT 想染メールのSubject 「▼夏 町
		@GIDEON Corp.

画面3.4

#### 3.4.1 保守・状況

- 稼働状況 :ONはウイルスチェックが有効になっており動作しています。 OFFはウイルスチェックが無効で動作していません。
- ログ :ボタンをクリックすると最新のログを取得し、下のログ一覧に表示します。
- サービス :SMTPまたは POP3 のサービスの種類。
- 環境チェック :該当ボタンをクリックすると、システムの詳細情報を表示します。[管理者に結果を送 信する〕ボタンをクリックすると、表示されている内容を管理者宛に送信します。
- 再起動 :サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力 されている)の場合にONにします。
- : サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生してい 再設定 る場合にONにします。
- SMTP ログ ダウンロード
  - :ダウンロードボタンをクリックすることで、SMTPのアクセスログがダウンロードできま す。ダウンロードする際は、『SMTPログのダウンロード』ダイアログ中のリストより選択 してからダウンロードボタンをクリックしてください。

#### POP3 - ログ - ダウンロード

:ダウンロードボタンをクリックすることで、POP3のアクセスログがダウンロードできます。 ダウンロードする際は、『POP3ログのダウンロード』ダイアログ中のリストより選択して からダウンロードボタンをクリックしてください。



Page 40

**BLOC** system

## 3.4.2 基本設定

#### ● 受信者への警告メール設定

メールがウイルスに感染していた場合、メールの受信者に送信する警告メールについての設定です。

**挙動** : 警告メール送信する場合、「警告メールに感染メールのヘッダーを添付する」または 「警告メールのみを送信する」の選択ができます。

メールヘッダーには送信経路などの情報が含まれています。

- Subject : 警告メールのサブジェクト名と感染メールSubject(元メールのサブジェクト)を連結する ことができます。
- 本文 : 置換文字列を使用して、警告メール本文に感染メールの情報を表示することができま す。

(置換文字列)	(表示内容)
SUBJECT	:感染メールSubjectを表示します。
VIRUS_SENDER	:送信者のメールアドレスを表示します。ただし、詐称されている場
	合もあります。
MESSAGE_ID	:感染メールMessage-Idを表示します。
MESSAGE HEADER	:感染メールのヘッダー全てを表示します。

入力後、[更新]ボタンをクリックしてください。

初期設定値:感染メールの場合、受信者にメールを送信しない

#### ● 送信者への警告メール設定

メールがウイルスに感染していた場合に、メールの送信者に送る警告メールについての設定です。 ウイルス感染メールは、送信者のメールアドレスを詐称している可能性が高いため、警告メールを送信 した場合スパムのように扱われることがあります。

したがって「送信者に警告メールを送信しない」設定を推奨します。

Subject :警告メールのサブジェクト名と感染メールSubject(元メールのサブジェクト)を連結する ことができます。

本文 :置換文字列を使用して、警告メール本文に感染メールの情報を表示することができま す。

(置換文字列)	(表示内容)
_SUBJECT_	:感染メールSubjectを表示します。
VIRUS_SENDER	:送信者のメールアドレスを表示します



BLOC system

# 3.4.3 詳細設定1

## ● チェックに使用するポート

BLOCではウイルスチェックのために、別ポートにパケットを転送します。 他のサービスなどで既に利用している場合は、未使用ポート番号に変更してください。 入力後、[更新]ボタンをクリックしてください。 初期設定値: SMTP 9025 POP3 9110

### ● 監視する接続先のポート

SMTPまたはPOP3のサービスが使っているポート番号を指定します。 通常、SMTPのポート番号は25、POP3のポート番号は110を指定します。 入力後、[更新]ボタンをクリックしてください。 初期設定値: SMTP 25 POP3 110

#### ● 送信元IPアドレスの復元

BLOCを通すとBLOCが使用しているIPアドレスを送信元とし、通信パケットを送信します。送信も元の IPアドレスをBLOCを通過する前の元アドレスに変換する機能を実現する場合にはこのモードを有効 にします。

復元することにより完全な透過を実現しますが、パフォーマンスは低下します。

SMTPまたはPOP3でこの機能を有効もしくは、無効にするには、[復元する]ボタンをクリックしてチェックマークが付けば有効化され、無印であれば無効化されます。

#### ● 管理者への警告メール設定

メールがウイルスに感染していた場合、警告メールを管理者に送信することができます。「3.3.1 基本 設定」で設定した、警告メールの送信先へ送信します。

- Subject : 警告メールのサブジェクト名と感染メール Subject (元メールのサブジェクト)を連結する ことができます。
- **本文** : 置換文字列を使用して、警告メール本文に感染メールの情報を表示することができま す。

(表示内容)
:感染メールSubjectを表示します。
:送信者のメールアドレスを表示します。ただし、詐称されている場
合があります。
:感染メールMessage-Idを表示します。
:感染メールのヘッダー全てを表示します。

入力後、[更新]ボタンをクリックしてください。 初期設定値:管理者に警告メールを送る



画面3.4.3

BLOC system

# 3.4.4 詳細設定2

#### ● 初期の接続待機数

サービスを効率良く処理するため、同時並行処理を行う初期のプロセス待機数を指定します。 この初期接続待機の数を多く設定すると同時接続数が多い場合ni処理効率は上がりますが、システムのメモリなどをより多く消費します。SMTPもしくはPOP3のサービスで、初期で接続待機する数を設定します。

初期設定值: SMTP 50 POP3 10

## ● 最大同時接続数

同時接続可能な接続(セッション)数です。この接続数以上はビジーとなり、接続待ち状態になります。 SMTPもしくはPOP3の場合は、同時利用者の最大数にほぼ同数です。 初期設定値: SMTP 250 POP3 250

#### ● 待機数を超えた場合の接続増加数

現在の接続待機数より多くの接続要求がきた場合、待機数を増やす単位。 初期設定値: SMTP 10 POP3 10

## ● 最大ファイルサイズ

チェックするメールの最大サイズを指定します。最大サイズを超えるメールはウイルスチェックされずエ ラーになります。 初期設定値:SMTP 100(MB) POP3 100(MB)

## ● 最大ファイルサイズを超えた場合の処理

『最大ファイルサイズ』を超えた時の処理で『エラー添付』もしくは『通過』が選択できます。『エラー添 付』は、元のメールにエラーメッセージを付けます。『通過』は、元メールをそのまま送受信します。 初期設定値:SMTP『エラー添付』 POP3『エラー添付』

## ● ウイルス感染メールの保存

BLOC では使用しません。



画面3.4.4

## 3.4.5 ホワイトリスト

特定のSMTPサーバやメールアドレスをウイルスチェックの対象外にする場合、ホワイトリストにその条件を記述します。

## SMTP

host: 有効送信元IPアドレス。 IPアドレス/マスクと指定することで範囲も設定可能。 ホスト名は不可

from: エンベロープのFromメールアドレス

to: エンベロープのToメールアドレス

有効送信元とは、前項の「4.4.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。

#### -----例1-----

送信元IP アドレス192.168.1.2 から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.2

#### -----例2-----

送信元IP アドレス192.168.1.2 から送信され、from がsender@example.net の場合、スパムチェック しない指定は、以下のように入力します。

host=192.168.1.2 from=sender@example.net

#### -----例3-----

送信元IP アドレス192.168.1.0 ~192.168.1.255 から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.0/255.255.255.0

#### -----例4-----

送信元IP アドレス192.168.1.2 から送信され、from が@example.net の場合、スパムチェックしない 指定は、以下のように入力します。。

この指定の場合、example.netの該当メールアドレスは全てスパムチェックしない指定になります。

host=192.168.1.2 from=@example.net

### 第3章 アンチウイルス設定

### POP3

host: 有効送信元IPアドレス。 IPアドレス/マスクと指定することで範囲も設定可能。 ホスト名は不可 from: メールヘッダ内のFromメールアドレス user: POP3アカウント

有効送信元とは、前項の「4.4.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。

## -----例1-----

送信元sender@example.comから送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

form=sender@example.com

# -----例2-----

有効送信先IP アドレス192.168.1.2 のID:user-one を、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.2 user=user-one

チウイルス アンチスパム		**************************************
Antil/irus	更新状況	▶ サーバ語 定 メール設定 ウェブ設定 他サービス
メール設定		
ウィルスチェックの有効/無効	► SMTP	・ページのアンドゥ
保守·状況	基本設定 詳細設定1 詳細設定	2 ホワイトリスト チェックリスト
ホワイトリスト		
SMTP	POP3	
SMTP	1010	
ホワイトリスト (記述部): fr	m≃nfo@example.net to=@example.com)	デックしたくない場合、条件を指定するとつ、 デックしたい一所可能となります。11行けにし 項目を1つすり指定でき、11行けにこう 項目を1つすり指定でき、11行けにこう ゴンドンドンドンドンドンドン デッレアドンドンには知らったがよさまう。 デッレアドンドンには知らったがようまう。 オーンドンドンドンドンドン マーンドンドンドンドン マーンドンドンドン マーンドンドン マーンドンドン マーンドンドン マーンドンドン マーンドンドン マーン マーン

Page 48

**BLOC** system

# 3.4.6 チェックリスト

メール設定画面の「チェックリスト」タブをクリックすると、画面3.4.6が表示されます。チェックリストに何も 記載しない場合には、サーバで処理するすべてのメールアドレスがウイルス検出対象となります。チェッ クリストに登録すると、登録されたメールアドレスのみが検出対象となります。

チェックリストの欄に、検出対象とするメールアドレス(例:eee@fff.co.jp)またはドメイン名(例:@fff. co.jp)を入力します。「@fff.co.jp」を登録すると、@fff.co.jpが含まれるメールアドレスすべてがメー ル送受信時に検出対象となります。

※チェックリストに登録がある場合、ホワイトリストをチェックした後にチェックリストをチェックします。

入力後[更新]ボタンをクリックしてください。 初期設定値:なし

GIDEON AntiVirus - Mozilla Fire	fox	
>イル(E) 編集(E) 表示(⊻) 履歴(S)	ブックマーク(B) ツール(T) ヘルプ(H)	
アンチウイルス アンチスバム		サポート
Antil/irus	更新状況 検出状況 打	▶ サーバ環境 共通設定 メール設定 ウェブ設定 他サービス
メール設定		
ウィルスチェックの有効/無効	SMTP POP3	▶ ページのアンドク
保守·状況	基本設定 詳細設定1 前	細設定2 ホワイトリスト チェックリスト
チェックリスト		
SMTP	POP3	
SMTP		
チェックリスト (記述例: 0	example.com)	テレジストレスを通常すると、そのシーリ アドレスパンールに含まれている場合の、クイルス チェンタドド、はち、最近かさくはい、場合はホクト リストの登録を解、まてのシールアドレスをまっとし はます。バンカンマトシリンズナーシスティンスキョン目の になった。 メールアドレスの地に、@OOMAINのよどにユーザー名 を高くしておいまするとして、@OOMAINのよどにユーザー名 を高くしておいまするとして、@OOMAINのよどにユーザー名 を高くしておいまするとして、@OOMAINのよどにユーザー名 を高くしておいまするとして、@OOMAINのよどにユーザー名 を高くしておいまするとして、@OOMAINのよどにユーザー名 を高くしておいます。 ドレスタービントのテレーンのように、 のしていたいたいです。 ・intol@example.com ・@XITF/sexample.comのときつイルスチェックする intol@example.com
		-
		@GIDEON Carp

画面3.4.6

# 3.5 ウェブ設定

HTTPでのウイルスチェックをする場合の管理・設定を行います。

「ギデオン BLOC system PortControl Plus」ではFTPのウイルスチェックはご利用いただけませんのでご了承ください。

HTTPは、WEBサーバとクライアント(WEBブラウザなど)がデータを送受信するのに使われるプロトコ ルで、ここではそのサービスを意味します。

「ウイルスチェックの有効/無効」の[HTTP]ボタンをクリックして、次画面で有効または無効を設定します。

[HTTP]ボタンの右下三角がオレンジ色になっている場合は有効になっている状態です。

GIDEO	N AntiVirus	: - Mozil	la Firefo	x							
rイル(E)	編集(E) 考	‱⊘ №	夏歴(S) フ	「ックマーク( <u>B</u> ) ツ	-11(II) ~11	ブ( <u>H</u> )					
アンチウィ	イルス アン	チスバム									サポート
GIDE	ON									► t	ナーバ環境
Ar	ntil∕irus			更新状況	検出状	況 #	通設定	メール設定	ウェブ設定	他サービス	
ウェ	ブ設定										
	ウィルスチョ	ロックの有効	加/無効	► HTTP	FTP	4					
				@@.#2	基本設定	121	細設定1	詳細詩定2	チェック対象	ホワイトリスト	i i
6	20.49										
-	N.J. 1A.06	_				_					
	*	家働状況	ログ	サービス	環境チェック	再起動	再設定				
		ON		HTTP							
				FTP							
		НТТ	Р	FTP	1						
	HTTP									<u>ا</u>	ダウンロード
	192.168. HTTP/1	1.7 www.ya 1″ 200	hoo.co.jp:58	55 [Wed, 21 Feb	2007 14:40:57	JST] "GET /	cgi−bin/mair	n.ogi?func=4158.a	I=SMTP&sid=9447	40929&timer=630642	
	192.168. UTTR/1	1.7 www.ya	hoo.co.jp:58	55 [Wed, 21 Feb	2007 14:40:59	JST] "GET /	cgi−bin/mair	n.ogi?func=417&ai	I=SMTP&sid=9447	40929&timer=632401	
	192.168	1.7 www.ya	hoo.co.jp:58	55 [Wed, 21 Feb	2007 14:41:01	JST] "GET /	cgi−bin/mair	n.ogi?func=4158.a	I=SMTP&sid=9447	40929&timer=634754	
	192.168	.1° 200 1.7 www.ya	hoo.co.jp:58	55 [Wed, 21 Feb	2007 14:41:03	JST] "GET /	cgi-bin/mair	n.ogi?func=415&a	I=POP3&sid=94474	10929&timer=635989	HTTP/1.1"
	200 192.168.	1.7 www.va	hoo.co.ip:58	55 Nied, 21 Feb	2007 14:41:04	JST1 "GET /	cgi-bin/mair	n.cgi?func=4178ai	I=SMTP&sid=9447	40929&timer=637074	
	HTTP/1 192169	.1″ 200	hoo co in 50	55 Dated 21 Each	2007 14:41:49	ISTI "GET /	ogi-hin/mair	cei?tunc=4178×	=POP3&oid=0447	10020&timer=682002	HTTP/11"
	200		noo.co.jpoi	NO 2000, 21 100	2001 194149	Jong GET /	ogi oso man	1001-1010-141703		1002000	
_											(DGIDEON Co
											0.00000000

画面3.5

# 3.5.1 保守·状況

稼働状況 : ON はウイルスチェックが有効になっており動作しています。 OFFはウイルスチェックが無効で動作していません。

ログ :最新のログを取得し、下のログ一覧に表示します。

- サービス : HTTPのサービス。
- 環境チェック :ボタンをクリックすると、システムの詳細情報を表示します。 [管理者に結果を送信する]ボタンをクリックすると、表示されている内容を管理者 宛に送信します。
- **再起動** : サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力 されている)の場合にONにします。
- 再設定 :サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生している場合にONにします。
- HTTP ログ ダウンロード
  - :ダウンロードボタンをクリックすることで、HTTPのアクセスログがダウンロードできます。 ダウンロードする際は、『HTTPログのダウンロード』ダイアログ中のリストより選択して からダウンロードボタンをクリックしてください。

GIDEON An	tiVirus - Mozilla Fir	efox						
イル(E) 編集	(E) 表示(V) 履歴(S)	ブックマーク(B) い	ール① ヘルブ(出)					
アンチウイルス	アンチスパム							サポート
GIDEON							► <del>7</del> -	ーバ環境
Antil	'irus	更新状況	検出状況	共通設定	メール設定	ウェブ設定	他サービス	
ウェブ設	定							
-								
	パルスチェックの1月30/悪30	► HTTP	FTP					
		保守·状況	基本設定	詳細設定1	詳細設定2	チェック対象	ホワイトリスト	
保守	状況							
	旅艇建筑 口子	יד ++	環境チェック 正	42.04. 再90次				
		нттр	\$\$\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\					
		T FTP						
	· · · · · · · · · · · · · · · · · · ·	2						
	НТТР	FTP				_		
	нттр						▶ 5	/ウンロード
[	192.168.1.7 www.yahoo.co	jp:555 [Wed, 21 Feb	2007 14:40:57 JST] *	'GET /cgi-bin/mair	n.cgi?func=415&a1	=SMTP&sid=94474	0929&timer=630642	
	HTTP/1.1" 200 192.168.1.7 www.yahoo.co	ip 555 [Wed, 21 Feb	2007 14:40:59 JST] *	'GET /cgi-bin/mair	n.cgi?func=417&a1	SMTP&sid=94474	0929&timer=632401	
	HTTP/1.1" 200 192168.1.7 www.vahoo.co	in:555 [Wed. 21 Feb	2007 14:41:01 JST] *	GFT /cgi-bin/mai	n cei?func=415&a1	SMTP8sid=94474	0929&timer=634754	
	HTTP/1.1" 200		9007 14/41/03 UST] 1	OFT /ori-hin/mai	ri2huno=415&a1	-POP38-id=94474	109021imar=635089 H	TTP /1 1"
	200	Droop fined of Each	2007 1441-00 0013	GET /- jubis /mai	-:04	CHITPS SHEDAA74	19250011161-000000	LIPZIA -
	HTTP/1.1" 200	Jpt005 [weat 21 neu	2007 1441:04 3313	GET / Cgimbin/ mair	ncerrunc=41 raai	=5M1F0SI0=94474	J929&rtimer=037074	
	192.168.1.7 www.yanoo.co. 200	jp:555 (Wed, 21 Heb	2007 14:41:49 JSTJ	GET /cgi=bin/mair	n.cgi?func=41 /6a)	=POP38sid=944740	1929&timer=682083 H	TTP/1.1"
								GIDEON Cor

画面3.5.1

### 3.5.2 基本設定

#### ● ファイル種別、ウイルスチェックの有効/無効

アクセス効率化のために、ウイルスチェックをするファイルの種類を選択をします。 [画像][動画][サウンド][ウェブ文書]ボタンは、それぞれ有効/無効のトグルになっています。 有効化した場合、右下三角がオレンジ色になります。 初期設定値:「画像」「動画」「サウンド」「ウェブ文書」が無効

## ● 感染時にファイルに埋め込む、もしくは置き換えるメッセージ

ファイルが感染していることを知らせる場合のメッセージを設定します。HTMLの場合、ウイルスが検出 された時にこのメッセージを表示します。 メッセージは日本語の表示はできません。半角英数文字で記述します。 入力後、[更新]ボタンをクリックしてください。 初期設定値:画面表示文字列

#### ● 最大受信サイズを超えた際に置き換えるメッセージ

最大受信サイズを超えたことを知らせる場合のメッセージを設定します。 日本語のメッセージ表示が可能です。 入力後、[更新]ボタンをクリックしてください。 初期設定値:画面表示文字列

#### ● すでに感染していたページにアクセスした際に置き換えるメッセージ

すでに感染しているページにアクセスした際に表示するメッセージを設定します。 ウイルスを検出したURLのサイトに、60分以内に再度アクセスした場合、ウイルスチェックをすること無し にウイルスと判断します。ウイルスサイトに同時に多くのユーザーがアクセスすることを回避するためで す。

日本語でのメッセージ表示が可能です。 初期設定値:表示されている文字列 該当項目入力後、「変更」ボタンをクリックして更新してください。



画面3.5.2

# 3.5.3 詳細設定1

## ● チェックに使用するポート

BLOCではウイルスチェックのために別ポートにパケットを転送します。 他のサービスなどですでに利用している場合は、未使用ポート番号に変更してください。 入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 9080

# ● 監視する接続先のポート

HTTPサービスが使用しているポート番号を指定します。 通常、HTTPのポート番号は80を指定します。 プロキシサーバ経由でインターネットに接続している場合、HTTPポートにプロキシサーバが受け付け るポート番号を指定してください。 例:HTTP 8080

プロキシサーバを使用するネットワーク環境の多くは、ブラウザでプロキシサーバの設定がされていま す。ブラウザからその設定を参照してポート番号を指定することもできます。ほとんどの場合、「3.3.3 更 新環境設定」で設定するプロキシサーバのIPアドレス・ポートと同じ設定になります。

入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 80, 3128, 8080

## ● 送信元IPアドレスの復元

BLOC を通すとBLOCが使用しているIPアドレスを送信元とし、通信パケットを送信します。送信も元 のIPアドレスをBLOCを通過する前の元アドレスに変換する機能を実現する場合にはこのモードを有 効にします。

復元することにより完全な透過を実現しますが、パフォーマンスは低下します。 HTTP でこの機能を有効もしくは、無効にするには、[復元する]ボタンをクリックしてチェックマーク が付けば有効化され、無印であれば無効化されます。

# ● 管理者への警告メール

HTTPサービスでウイルスに感染していた場合、警告メールを管理者に送信することができます。 「3.3.1 基本設定」で設定した、警告メールの送信先へ送信します。

Subject :警告メールのサブジェクト名を設定します。

本文 :警告メールに固有のメッセージを記載します。

入力後、[更新]ボタンをクリックしてください。

初期設定值:画面表示文字列

● ウイルス感染メールの保存 BLOCでは使用しません。



画面3.5.3

# 3.5.4 詳細設定2

## ● 初期の接続待機数

サービスを効率良く処理するため、同時並行処理を行う初期のプロセス待機数を指定します。この 初期接続待機の数を多く設定すると同時接続数が多い場合処理効率は上がりますが、システムの メモリなどをより多く消費します。

HTTP のサービスで、初期で接続待機する数を設定します。 クライアントからWEB サーバには一回のサイトアクセスで複数セッションを同時に使用するためデ フォルト値を大きく設定しています。 入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 500

## ● 最大同時接続数

同時接続可能な接続 (セッション)数です。この接続数以上はビジーとなり、接続待ち状態になりま す。HTTP の場合は、同時利用者の最大数にほぼ同数です。

入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 1000

## ● 待機数を超えた場合の接続増加数

設定した接続待機数を超えた接続要求がきた場合に、待機数を増加させる処理を実行します。以下 の初期設定値では、1回の処理で50 待機プロセスを増分します。

入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 50

# ● ダウンロードの最大ファイルサイズ

ウイルス検出するダウロードファイルの最大ファイルサイズです。 この最大ファイルサイズ未満のファイルはウイルスを検出する対象になります。

入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 10[MB]

# ● ダウンロードの最大ファイルサイズを超えた場合の処理

『ダウンロードの最大ファイルサイズ』を超えた時の処理で 『通過』もしくは 『エラー停止』 が選択できます。

『通過』は、ウイルスチェックせずそのまま通信をおこないます。『エラー停止』の場合は、ダウンロード を停止します。

入力後、[更新]ボタンをクリックしてください。

初期設定值:HTTP『通過』

### ● アップロードの最大ファイルサイズ

ウイルス検出するアップロードファイルの最大ファイルサイズです。 この最大ファイルサイズ未満のファイルはウイルスを検出する対象になります。 入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 10[MB]

## ● アップロードの最大ファイルサイズを超えた場合の処理

『アップロードの最大ファイルサイズ』を超えた時の処理で『通過』もしくは『エラー停止』が選択できます。『通過』は、ウイルスチェックせずそのまま通信をおこないます。『エラー停止』の場合は、アップロードを停止します。

入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 『通過』



# 3.5.5 チェック対象

#### ● ウイルスチェックしないファイル

ウイルスチェックをしないファイルを個別に指定できます。 HTTPではContent-Typeと拡張子が一致したファイルはチェックしません。 入力後、[更新]ボタンをクリックしてください。

HTTP初期設定值:

Content-Type	:画面表示文字列
拡張子	:画面表示文字列
スクリプト	:ウェブ文書中のスクリプトのウイルスチェックを行わない



# 3.5.6 ホワイトリスト

ホワイトリストは、特定の接続先サイトなどをウイルスチェック対象外とするリストです。

# • HTTP

ホストリストの書式は以下の通りです。一行内に項目のどちらか一項目もしくはAND 条件の場合は 両項目が記述できます。

項目は以下の2個の指定が可能です。 host=FQDN または IP または IP/MASK path=『/』文字から始まるファイル名を含むパス

例

http://www.example.com/file.zip をスルーする場合、以下のように記載します。 host=www.mple.com path=/file.zip

全ての/cgi-bin/bbs.cgi?s=1&e=100 をスルーする場合、以下のように記載します。 path=/cgi-bin/bbs.cgi?s=1&e=100

192.168.1.0 ~ 192.168.1.255 をスルーする場合、以下のように記載します。 host=192.168.1.0/255.255.255.0

😉 GIDEON AntiVirus - Mozilla Firet	ox	
ファイル(E) 編集(E) 表示(V) 履歴(S)	ブックマーク(風) ツール(① ヘルブ(山)	
アンチウイルス アンチスパム		サポート
Antil/irus	更新状況 検出状況 共通設定	▶ サーバ環境 メール設定 ウェブ設定 他サービス
ウェブ設定		
ウィルスチェックの有効/無効		▶ ページのアンドゥ ▶ ページの初期化
	保守·状況 基本設定 詳細設定1 1	詳細設定2 チェック対象 ホワイトリスト
ホワイトリスト		
нттр	FTP	
HTTP		
ホワイトリスト (記述例: ho	st=www.example.com path=/dr/file.zip)	▶ 正都 特定の特徴先生サイトなどをクイルスタエックしたな に場合、条件を指定するとつくれスタエックを入ルー に場合、条件を指定するとつくれスタエックを入ルー にすっていてはなが見ましてつくが感じてき、1 一行れしていなが見ました。1 一行れしていながらない。 ・ のはモースのいみといか。 ・ のはモースのいみという。 ・ 私立例う ・ したは、アドがのはまっかイルを含むいて、 ※項目は安全ー気のみとす。 ・ 私立例う ・ したい、のかいまっか。 ・ 私立例う ・ したい、のかいまっか。 ・ ないまっか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ひょうか。 ・ ないまっか。 ・ ないまっか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ かっか。 ・ ないまっか。 ・ ひょうか。 ・ かっか。 ・ ないまっか。 ・ ひょうか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ひょうか。 ・ ひょうか。 ・ かっか。 ・ ないまっか。 ・ ひょうか。 ・ ひょうか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ないまっか。 ・ ひょうか。 ・ ひょうの。 ・ ひょうか。 ・ ひょうの。 ・ ひょうか。 ・ ひ
		@ GIDEON Corp.

画面3.5.6

# 3.6 スキャンコード一覧

メールログに "SCANNED: X"として表示される、Xの番号について説明します。

数值	状況
0	ウイルスに感染していない
1	aveserverに接続することができない
3	ウイルスである疑いがある
4	ウイルスに感染している
G	スキャン結果不明
0	(暗号化されている、パスワードが掛かっている)
7	gwavが原因のエラー
1	(ファイルが見つからない、ファイルを読むことができない)

上記スキャンコードは」、受信者宛の元メールに "Virus Check ERROR(X)" という記述が追加されます。0、9の場合は、元のメールをそのまま配信します。

# 4.1 更新状況

● スパムDB更新ログ (画面4.1 上段部分)

スパムデータベース (スパムDB) の更新状況を閲覧できます。 スパムDB は、カスペルスキーのアンチスパムエンジン (種別:kas)が利用する、スパムメールを特定 するための情報を格納したデータベースです。 初期設定では3時間毎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、最新のデータベース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。

「報告メール」は、スパムDBの更新状況をメールでお知らせするものです。 「3日以上未更新」は、3日以上スパムDBの更新がない場合に管理者宛にメール送信します。 「最新定義ファイルでない」は、システム上のスパムDBが最新でない場合に管理者宛にメール送信 します。

[対応状況]ボタンをクリックすると、スパムDBに関する情報サイトを表示します。

● モジュール更新ログ (画面4.1 下段部分)

各モジュールの更新状況を表示します。モジュールとは、アンチスパム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、透過プロキシー、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(「MTAアドオン」はBLOCでは使用されません)。

※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。



# 4.2 検出状況

スパムメールと判定したメール情報の履歴や統計情報などを閲覧できます。

## ● 検出情報

検出状況画面の上部「検出情報」欄では、スパムメールと判定したメールの検出数が表示されます。 「本日」、「昨日」、「今月」、「先月」のスパムメール検出数を表示します。

· · · · · · · · · · · · · · · · · · ·					
(ルビ)編集(2) 表示(2) 原 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	歴 © ブッウマーク(E) 更新状 使出情 本日	ッール① 況 様	ヘル749 出状況 共通設定 メー 計 日 10 今月	-ル設定 10 <u>先月</u>	サポー  ▶サーバ田   他サービス   0
判定方法:>S(3)	RBL— 今 11 月 21 31	改ドメイン統書 RBL一致ドメイン 立 justlsikdark 立 nightlightsu 立 suplounge.h	情報 ealcom 4 ninfo 2 k 2 ▶月次詳細	FBL一致ドメイン       先     1位       2位     3位	機出者
	_	_			
検出ログ				▶ 全表示	▶検 索 ▶ダウンロ

画面 4.2-1

#### 第4章 アンチスパム設定

#### ● RBL一致ドメイン統計情報

検出状況画面の「RBL 一致統計情報」欄では、スパムメール判定方法の1つであるxSPAM 方式の統計情報が表示されます。

xSPAM 方式はメール本文中に含まれるURL が、ブラックリストにのっていないかどうかをチェック します。実際にはRBL (Realtime Black List) と言われるDNS サービスを検索します。 表示された検出数は、スパムと判定されたドメインが何通のメールに含まれていたかを表します。

[月次詳細]ボタンをクリックすると、月内にスパムと判定した全てのRBL 一致ドメインとその検出数 を閲覧できます。

[管理者に結果を送信]ボタンをクリックすると、その内容を管理者へメールで送信します。



画面 4.2-2

#### 検出ログ

検出状況画面の下部「検出ログ」欄では、検出したスパム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。

[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。



画面 4.2-3

# 4.3 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、「3.3 共通設定」の項を参照してください。



# 4.4 メール設定

# 4.4.1 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「3.4.1 保守・状況」の項を参照してください。

## 4.4.2 基本設定

ここではスパム判定スコアなどの基本的な設定を行います。

アンチスパムPlusではスパム判定基準に、検知率を高め誤検知を防ぐスコアリングロジック を用いています。複数の判定方法ごとにスコア(点数)を設定し、該当した場合にスコアが 加算されます。高スコアほどスパムである可能性が高く、合計が一定の値を超えた場合にス パムと判定します。

イルビ編集団	表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルブ(H)	
アンチウイルスア	マンチスパム	サポート
		トサーバ環境
GIDEON Aptil/irus		
	史新获况 楼出状况 共通設	た メール設定 他サービス
メール設定		
7.000		▶ ページのアンドゥ ▶ ページの初期化
2/14/1	SMIP FOR	
保守·状況	基本設定 詳細設定1 詳細設定2 転送メー	ル ホワイトリスト プラックリスト チェックリスト
基本設定		
墨本設足		
	スパムと判定した場合のSubject	
	[SPAM + Jスコア + J判定名 + ] + J元Su	ubject アクジョンFSubject変更」の結合スコアを超えていた場合し き換えられるSubjectです。
	フパム判定基準	
	スパム判定基準	************************************
	スパム特定基準 ● 推奨設定を利用する ● カンネップズを利用する	▶更新 ※カスマイズを利用する場合は設定項目に注意して 行ってばだい
	<ul> <li>スパム非定憲率</li> <li>         ・ 推奨設定を利用する         ・カスタマイズを利用する         ・</li> </ul>	**カスがマイズを利用する場合は設定項目に注意して 行ってください 利定方法だいて 利定方法だいて 利定方法だいて
● 判定方法	スパム市定業手         ・ 推奨設定を利用する カスパマイズを利用する           D         利定方法         スコア         D         利定方法	*カスタマイズを利用する場合は設定項目に注意して 行ってただい 単に方法について BL 「ブラジリストで指定した項目に一致したメール。高スコア推奨 XS メール本文本で記録が広たドメーンのRD チェック、高スコア推奨
● 判定方法	スパム物定基準         スパム物定基準           ・加速鉄空を利用する カスタマイズを利用する         カスタマイズを利用する           ・加速などのクロックのクロック         ・加速などのクロックのクロック           ・ローザー定着プランリスト         4         525         発展大子ワン           ・ローザー定着プランリスト         4         525         発展大子ワン           ・ローザー定着プランリスト         4         525         発展大子ワン	*カムダマイズを利用する場合は設定項目に注意して 行ってたろい EL「ブラックストにを指した項目に一致したメール。高スコア構築 EL「ブラックストにを指定した項目に一致したメール。高スコア構築 EL「読着元がPTPトンのPRUFェック、高コア構築 SSD、Rescurate IPはなわたのを注意ののですか。低コア構築
● 判定方法	スパム特定基準           ・損退設定を利用する カスタイパを利用する           0         特定方法           日         サイズを利用する           日         サイズを利用する           日         サインド	*カスカマイズを利用する場合は設定項目に注意して 行ってにない 形定方法について にしてラックストイを着にし承担し、一般したメール。高スコア構築 15:50
● 判定方法	スパム和定業率           ・指提設定を利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カスマイパを利用する           ・カンマイパを利用する           ・カーナー           ・カンマイパを利用する           ・カンマイパを利用する           ・カンマイパを利用する           ・カーナー           ・カーナー <tr< td=""><td>*カスカマイズを利用する場合は設定項目に主要して 「日本方などい」 取定方法にない 取に方かがスパンで確認した場合にしている。 おしてクラがスパンで確認した場合にしていた。 など、小はな大いに記載されたりメインの応じまたが、 あっア用提供 できたいではなけたいである時のにの予想だ。 そのためにはなけたいである時のにの予想だ。 そのためにはないたいである時のにのできた。 そのためにはないため、 など、クリーンで相応。 そのためにはないため、 そのため、</td></tr<>	*カスカマイズを利用する場合は設定項目に主要して 「日本方などい」 取定方法にない 取に方かがスパンで確認した場合にしている。 おしてクラがスパンで確認した場合にしていた。 など、小はな大いに記載されたりメインの応じまたが、 あっア用提供 できたいではなけたいである時のにの予想だ。 そのためにはなけたいである時のにの予想だ。 そのためにはないたいである時のにのできた。 そのためにはないため、 など、クリーンで相応。 そのためにはないため、 そのため、
<ul> <li>・ 判定方法</li> <li>・ アクション</li> </ul>	スパム1地定業率         ・ 油提設定を利用する           カスPマイズを利用する         カスPマイズを利用する           カスPマイズを利用する         第           日         コーザー定者プランジスト           日         コーザー定者プランジスト           1         825           2         ア           1         825           2         アクション           1         84           1         825           2         84.8           1         92.5           1         82.5           2         KAS           7         1           1         82.0           1         82.0           1         82.0           2         1           2         1           3         1           5         2           1         84.2.27           70/120         1	*カスタマイズを利用する場合は設定項目に主なして 行ってくたろい 単に方ふたっいて BL 「ブラクリスト」を指定した項目に一致したメール。高スコア推奨 な メールは文寸に記載なしたドメインの作用チェック、高スコア推奨 の 高い、単成元がPFドレスの用しチェック、高スコア推奨 の たいのでのは記述されたドメインの作用チェック、高スコア推奨 の たいのでのは記述された中心の用しチェック、高スコア推奨 の たいのでのは目した。このでは、一般であった。 本人の「日本」の「日本」の「日本」の「日本」の 「日本」の「日本」の「日本」の「日本」の「日本」の 「日本」の「日本」の「日本」の「日本」の 「日本」の「日本」の「日本」の 「日本」の「日本」の「日本」の 「日本」の「日本」の「日本」の 「日本」の「日本」の 「日本」の「日本」の 「」の 「日本」の 「日本」の 「日本」の 「日本」の 「日本」の 「日本」の 「日本」の 「日本」の 「日本」の
<ul> <li>・ 判定方法</li> <li>・ アクション</li> </ul>	スコア 0 料準方法           1 増速方法           D         ギネカ方法         スコア         0         料準方法           BL         ユージーン定員ブランワント         4         S25         養養奈方127           XS         ロルフィルタリング         3         RES         裏目参チュック           X1         印ルフ・パングリング         3         RES         裏目参チュック           アクション         FGカニア         アクション         FGカニア         アクション         F	*カスカマイズを利用する場合は設定項目に注意して 行ってだない。 形にすみない、ア 単にすみない、ア サモオあない、ア ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
<ul> <li>判定方法</li> <li>アクション</li> </ul>	スパムも地定基準           ・指提該先を利用する ・カスマイズを利用する           ・日本が売           ・日本が売           ・日本が売           ・日本が売           ・日本が売           ・日本が売           ・日本が売           ・日本が売           ・日本が売           ・日本のか売           ・日本の売	*カンカイズを利用する場合は設定項目に主意して 行ってはない 単になったようい。 も、ロクラッパストインを利用に一切したシール。ホンコア構築 は、ロクラッパストインを読むたけがくのが見ティン。ホンコア構築 で、現金のDFがしのPREFメアン。ホンコア構築 で、現金のDFがしのPREFメアン。ホンコア構築 PRE 送信をオンク、化コア構築 RS DEを利用したメリム単定。中一ホンコア構築 メスタ DEを利用したメリム単定。中一ホンコア構築 アグシンシ コアクライトアン・ションの生まで、このア アグシンシ コアクライトアン・ションの生まで、このア PPSのからなって、見ませんな、このア
<ul> <li>利定方法</li> <li>アウション</li> <li>追加ourダ</li> </ul>	スパムも地定基準           ・ 指提設定を利用する           ・カスパマイズを利用する           ・カスパマイズを利用する           ・カスパマイズを利用する           ・カスパマイズを利用する           ・カンパマイズを利用する           ・カンパマーズのシーン           ・カンパーズ	*カスカマイズを利用する場合は設定項目に主意して 行ってください 甲度方法について BL 「ブラッジスト」で考定した「少したトール」高スコア推奨 SS ReなったアドレンのReliston」高ンコア推奨 SS ReなったまたによういのReliston」低コア推奨 SS ReなったまたによういのReliston」低コア推奨 AS DBを利用したンバム利定。中一本スコア推奨 アンジョン フアション ステントナントロールを対応、単一本本スコア推奨 SS Read State (1)のPOののよった文庫のいと書替 税名をなった設定(1)した総合スコドレムになったたちに適用たれます。 Subject 死達した総合スコドレムになったたちに適用たれます。 Subject 不定 (1)により、「小型」になったたちに適用たれます。 Subject 不定 (1)にようにあった」のと書替 税名をなった設定(1)によった。
<ul> <li>・ 判定方法</li> <li>・ アクション</li> <li>・ 追加へッダ</li> </ul>	スコア ロ 料本方法           ・ 指述放在を利用する         カスタイスを利用する           ・ 指定方法         スコア ロ 料本方法           ● 「非志方法         第日           ● 「非志方法         第日           ● 「非志方法         スコア ロ 料本方法           >Starting         第日           >Starting         日           > 「日         ● 「ウイース           アクション         単合           ● 「ウロウムのみ本太夏夏         Starting           Starting         ● 「日           ● 「ウロウムのみ本太夏夏         ● 「日           ● 「日         ● 「日           ● 「日         ● 「日	**カスカマイ大を利用する場合は設定項目に注意して 行ってにない。 和定方為なべ、X 甲定方為なべ、X 甲定方為なべ、X 平になった。 マングスノストで各国にし項目に一致したパール。あスコア構築 ジ、メール本文中に追触されたドメインのRBJェア構築 び、タール本文中に追触されたドメインのRBJェア構築 び、タール本文中に追触されたドメインのRBJェア構築 び、タール本文中に追聴されたドメインのRBJェア構築 び、タール本文中に追聴された。 アンラン スア会社が、該定した総合スコドルにたるったちに適用されます。 Sageで見て、ノムレンドに大場合のSubmicitizまでの アンラン スアを引かれ、該定した総合スコドルにたるったちに適用されます。 Sageで見て、ノムレンドに大場合のSubmicitizまでの アンタン スアを引かれ、該定した総合スコドルにたるったちに適用されます。 Sageで見て、ノムレンドに大場合のSubmicitizまでの アンタン Submicitizまでは、一般の日本の本文文を見のと注意書 Submicitizまでは、一般の日本の本文文を見のと注意書 Submicitizまでは、一般の日本の本文文を見のと注意書 Submicitizまでは、一般の日本の本文文を見のと述る書 Submicitizまでは、一般の日本の本文文を見のと述る書 Submicitizまでは、 Submicitizまでは、 Submicitizまでは、 Submicitizまでは、 Submicitizまでは、 Submicitizまでは、 Submicitization - Submicitization -
<ul> <li>・ 判定方法</li> <li>・ アクション</li> <li>・ 道道へッダ</li> </ul>	マノバム特定基準           ・ 指皮技巧を利用する ・カスタイズを利用する           ・ 加スタイズを利用する           ・ 加スタイズを利用する           ・ 加スタイズを利用する           ・ 加スタイズを利用する           ・ 加スタイズを利用する           ・ コージーンボスラックリスト           ●           ・ コージーンボスラックリスト           ・ コージーンボスラックリスト           ・ コージーンボスターンボスターンボスターンボスターンボスターンボスターンボーンボーンボーンボーンボーンボーンボーンボーンボーンボーンボーンボーンボー	*カフラマイズを利用する場合は設定項目に注意して 行ってはない *現在カ点のパ、 ・現在カ点のパ、 に、カランパ、 を、リールま文本は設めれたドメインの応じまつか、高スコア構築 に、サランパ、 に、サランパ、 に、サランパ、 を、リールま文本は設めれたドメインの応じまつか、高スコア構築 の、日本のプロドル。スロロトロション、高スコア構築 ・、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、

画面 4.4.2

#### 第4章 アンチスパム設定

#### ● スパムと判定した場合のSubject

受信したメールがスパム判定で一定のスコアを超えた場合、ユーザにはSubject にコメントを付した メールが送信されます。

メール設定 基本設定画面の「スパムと判定した場合のSubject」欄に、画面の表示例のように指定した場合、ユーザは以下のSubjectを受信します。

[SPAM 3: RES KAS] 元Subject

これはスパム判定名RESおよびKASの合計スコアが3であり、スパムの疑いがあることを表します。

変更する場合は、入力後に [更新]ボタンをクリックしてください。

## ● スパム判定基準

アンチスパムPlusでは以下の6通りの判定方法を基にスパム判定を行っています。

## BL:ユーザ定義ブラックスリスト

- ・ユーザが設定したブラックリストに基づく判定
- ・推奨スコア4 (検知度上位)

## XS: URLフィルタリング

- ・メール本文中のURL がRBL に登録されているか否かをチェック
- ・推奨スコア3(検知度中位)
- ・稀にスパムではないドメインがRBL に登録されることがある。

## R1:RBL(リアルタイムブラックリスト)

- ・接続元のIP アドレスがRBL に登録されているか否かをチェック
- ・推奨スコア3 (検知度中位)
- ・稀にスパム送信の踏み台にされている企業などのサーバからのメールがスパムと判定されることが ある。

## S25:発信元チェック

- ・メールヘッダのReceivedに記述された命名規則がスパムでよく用いられる形式か否かをチェック
- ・推奨スコア1(検知度低位)
- ・形式的なチェックのため検知率は高くない。

## RES:逆引きチェック

- ・送信元のIP アドレスなどが逆引き可能か否かで信頼性をチェック
- ・推奨スコア1(検知度低位)
- ・検知率は一般に高いが誤検知もある。

## KAS:本文解析

・カスペルスキーアンチスパムDB を検索してメール本文をチェック

・推奨スコア3(検知度中位)

・英語、ロシア語などのメール解析に優れている。

「カスタマイズを利用する」を選択すると判定基準スコアを変更できます。

#### 注意

判定方法のスコアは推奨値を使用することをお勧めします。また「アクション」の「SMTP のみ受信 拒否」のスコア変更は慎重に行ってください。

#### • アクション

スコアの合計が、設定した総合スコア以上になったときに該当するアクションが実行されます。

#### Subject変更:

変更設定したスコアに達したとき、メールの Subject が「スパムと判定した場合の Subject」で設 定したものに変更されます。スコアの値を高く設定すると、スパムの可能性がより高いメールのみ Subject が変更されます。

#### ・POP3のみ本文変更:

設定したスコアに達したとき、詳細設定1の「POP3のみ本文変更のとき置き換える本文」で設定し たメール本文に置き換ります。

#### ・SMTP/MTA受信拒否:

設定したスコアに達したとき、メールを受信しません。従って、このメールは保存されません。スコアを カスタマイズする際は、特に慎重に行ってください。

#### ● 追加ヘッダ

スパム判定の総合スコアが設定した値になると、自動的にメールヘッダに以下の情報を付加します。 メールクライアントのメールヘッダによるメールの振り分けの判断に利用できます。

(ヘッダ表示)	(内容)
X-Spam-Status: NONE	スパムに該当せず
X-Spam-Status: SUSPICION	スパムと疑わしい
X-Spam-Status: SPAM	スパムに該当

また、ヘッダには以下に類する行も付加されます。

(ヘッダ表示例)	(内容)
X-Spam-Level: 3	スパム判定スコア3
X-Spam-Method: R1	判定方法R1でチェック

## 重要

送られてきたメールをスパムと判定する総合スコアは、「追加ヘッダ行」のX-Spam-Status: SPAMで 指定した値を用います。この値を高く設定するとスパムの可能性がより高いメールに限定し てスパムと判定します。値はお客様のポリシーに応じてカスタマイズを行って下さい。

## 4.4.3 詳細設定1

● チェックに使用するポート

BLOC では変更する必要はありません。

### ● 監視する接続先のポート

SMTP、POP3 が使用しているポートを指定します。

※スパムメール対策としてOP25B (Outbound Port 25 Blocking)を実施しているホスティングサービスを利用している場合、SMTP にポート番号 「587」を追加してください。

例 25,587

## ● キャッシュ制御

逆引きチェック (RES)で得た結果、もしくはRBL への登録問い合わせをキャッシュとして保存しておきます。

[クリア]ボタンをクリックすると、保存したキャッシュを消去します。逆引きキャッシュとRBL キャッシュの双方のキャッシュを消去します。

「保存期間」は、逆引きの結果やRBL の登録問い合わせを行って追加されたキャッシュ項目の有効 日数を決定します。

#### ● POP3のみ本文変更のとき置き換える本文

基本設定のアクションの「POP3のみ本文変更」で設定した総合スコアを超えたときに置き換わる 本文です。本文の中には、以下のタグ文字列を含むことで、スパムメールの特定の情報に置き換わり ます。

(ヘッダ表示)	(内容)
SPAM_STATUS	: NONE/SUSPISION/SPAM のいずれか。基本設定の
	追加ヘッダと同等
SPAM_TOTAL_SCORE	: このメールのスパム判定方法による総合スコア
SPAM_JUDGE_NAME	: このメールの判定方法 (複数ある場合空白区切り)
SUBJECT	: このメールのSubject (MIME デコードあり)
ORIGINAL_SUBJECT	: このメールのSubject (MIME デコードなし。メール
	ヘッダに書かれている形式)



画面 4.4.3

BLOC system
### 4.4.4 詳細設定2

- 初期の接続待機数
- 最大同時接続数
- 待機数を超えた場合の接続増加数

上記3項目はアンチウイルスの設定と共通です。

### ● スパム判定で除外するグローバルIPアドレス

BLOCでは、信頼できるメールサーバ(グローバルIPが振られている自社もしくはホスティングサーバ) の直前のサーバのIPアドレスをチェックしてスパム判定を行います。 従って利用しているメールサーバやリレーサーバをスパム判定対象から除外する指定が必要です。

「スパム判定で除外するグローバルIPアドレス」の欄に、BLOCでメールを受信する経路上にあるスパム判定の対象外のサーバのグローバルIPを登録します。



上記の経路で外部からのメールを受信し、自社内部リレーメールサーバの後ろにBLOCを導入した場合を例にとります。

- BLOCの直前におかれたすべての受信メールサーバ(リレーサーバ含む)IPアドレスを、スパム判定 対象外に指定します。上記例の場合、「メールサーバ1」「メールサーバ2」のIPを「スパム判定で除 外するグローバルIPアドレス」に入力します。その後[更新]ボタンをクリックします。
- ・ 転送目的のサーバ(例:メールサーバ1)のグローバルIPも入力してください。
- ・ プライベートIPはスパム判定には使わないため、グローバルIPのみを指定します。

※グローバルIPが不明な場合は、受信しているメールソフトのヘッダ情報を参照してください。

#### 重要

スパム判定から除外するサーバのグローバルIPを漏れなく登録する必要があります。正しく登録され ないと検知率が低くなる場合があります。



画面 4.4.4

### 4.4.5 転送メール

#### 4.4.5.1 基本

スパム判定で総合スコアが「転送下限スコア」で指定した値を超えた場合に、そのメールを転送する 設定をします。

初期設定値:転送しない

転送する場合は「転送下限スコアに達していたら転送」ラジオボタンにチェックを入れます。 チェックを入れると以下の項目が入力可能になります。

#### ● 転送下限スコア

転送する下限のスコアを入力します。入力したスコア以上のメールはすべて転送されます。

#### ● 受信先への配信を停止する

チェックを入れることにより、smtp の場合、受信先へメールを送信しません。POP3 では適用されません。

#### ● POP3サーバのメール削除

チェックを入れることによりPOP3 サーバ上にあるスパムメールを削除します。 チェックを入れると「POP 認証」「APOP 認証」のタブが有効になります。

#### ● 転送の指定方法

smtp の場合、転送下限スコアに達した場合にそのメールを転送することができます。 POP3 の場合、上記「POP3 サーバのメール削除」が有効な場合、転送の指示によりPOP3 サーバの メールを削除します。ただし、「4.4.6 チェックリスト」の「POP3 削除」による削除リストが指定された 場合は、そのリストが優先されます。

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。

#### -----例1-----

user-one@example.com 宛のメールを、spam-admin@example.com と mail-admin@example.com に転送する場合は、以下のように入力します。

user-one@example.com spam-admin@example.com mail-admin@example.com

-----例2-----

#### 第4章 アンチスパム設定

@example.com に後方一致するメールアドレス宛のメールをspam-admin@example.com に転送す る場合は、以下のように入力します。

@example.com spam-admin@example.com

#### 4.4.5.2 POP認証

「自動的にユーザリストを追加する」にチェックを入れると、クライアントPC からPOP3 で接続した ユーザ情報を自動的に取得します。

### 4.4.5.3 APOP認証

メールの取得にAPOP (パスワードの暗号化)を利用している場合、利用ユーザすべての登録が必要になります。

記載例:

POP3 のユーザID が「user-one」、パスワードが「1234」、POP3 サーバIP アドレスが「192.168.0.1」 の場合、以下のように記載します。

user=user-one password=1234 host=192.168.0.1

レビ 編集ビ 表示(型) 腹腔(型)	ブックマーク(目) ツール(① ヘルブ(日)		
ッチウイルス アンチスパム			サポート
GIDEON			▶ サーバ環境
Antil/irus	更新状況 検出状況 共識	11日 メール設定	他サービス
メール設定			
フパノエールクの支付/無効			▶ ページのアンドゥ ↓ ▶ ページの初期
スパムチェックの有効/無効	▶ SMIP		
保守·状況 基本設定	詳相設定1 詳細設定2 転送	メール ホワイトリスト プラ・	ックリスト チェックリスト
転送メール			
基本	POP認証 APOP認証		
基本			
基本 <ul> <li>転送しない <ul> <li>転送下限スコアに達していな</li> <li>転送下限スコアに達していな</li> <li>転送下限スコアに</li> <li>転送</li> <li>転送</li></ul></li></ul>	6 転送	総合: メール POP3	スコアが「転送下限スコア」を超えた場合にそ を転送します。 の場合はユーザID@[POP3サーバIPアドレ
基本 ●転送しない ●転送下税入コアに通していた 転送下税入コア 3	<b>5時3送</b> □受信完への配信を停止する ⊡PoP3サーバの	総合: メール PDF3 を した スで2 ルアド レス その その その その その その マー の ア マー し ア に マー レ マー に の ア マー レ マ の マー マ マー レ マ の マ マー レ マ の マ マー レ マ マ マ マ マ ロ マ マ マ マ マ マ マ マ マ マ マ マ マ	ユアが「転送 下隊スフア」を起えた場合に 後征送します。 の場合はユーザロを(POP3サー)、3P7下し、 打不りれるの場合は気気を入っいアドレスは 相定します。転送ン・リンドレスは年入、 地によす。転送ン・リンドレスは年入、 地によす。低速ン・リンドレスは年入、 低ごなき、電気と、アビレスドー・厳し、 転送す気にできます。 のコーザログルはer-cna、POP3サー/UF7 と188010/増高>)、 2972の場合)、 2972の場合、 一での時をいわりとのの死の(通信人・) をexample.com(電気) 一での時をいわりとの死の(通信人・) たまの 1972 1972 1
基本 ●転送しない ●転送下税スコアに通していた 転送下税スコア 3	563送 - 学信先への配信を停止する 「パPOP3サーバの	総合	コアが「転送下限スワドを起えた場合に 転送しす。 の場合はコーリの6月P03サー、UTPドドレス。 指定し、本月スインス級にく転送シー、 が高し、本月スインス級になどしまっ、 が認し、本月スインス級になどしまっ、 が認し、本月スインス級になど、 などした。 などのまた。 などうないでは、 を送けるにつきないであった。 のP3のが着こう のののから、 ののののから、 ののののから、 ののののから、 ののののから、 ののののから、 ののののから、 ののののから、 ののののから、 ののののから、 ののののから、 のののののから、 のののののから、 ののののから、 のののののののののから、 のののののののののののののののののののののののののののののののののののの

# 4.4.6 ホワイトリスト

ホワイトリストに登録することで、スパムチェックを行わない条件を指定できます。 1行内に指定した条件は、複数のAND条件となります。 指定できる条件は以下のものがあります。

### SMTP

host: 有効送信元IPアドレス。 IPアドレス/マスクと指定することで範囲も設定可能。 ホスト名は不可

from: エンベロープのFromメールアドレス

to: エンベロープのToメールアドレス

helo: HELO で指定されるアドレス

有効送信元とは、前項の「4.4.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP ア ドレス」以外の送信元IP アドレスを指定します。

#### -----例1-----

送信元IP アドレス192.168.1.2 から送信されてきた場合、スパムチェックしない指定は、以下のように 入力します。

host=192.168.1.2

#### -----例2-----

送信元IP アドレス192.168.1.2 から送信され、from がsender@example.netの場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.2 from=sender@example.net

#### -----例3-----

送信元IP アドレス192.168.1.0 ~192.168.1.255 から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.0/255.255.255.0

#### -----例4-----

送信元IP アドレス192.168.1.2 から送信され、from が@example.net の場合、スパムチェックしない 指定は、以下のように入力します。。 この指定の場合、example.net の該当メールアドレスは全てスパムチェックしない指定になります。

host=192.168.1.2 from=@example.net

### 第4章 アンチスパム設定

### • POP3

host: 有効送信元IPアドレス。 IPアドレス/マスクと指定することで範囲も設定可能。 ホスト名は不可 from: メールヘッダ内のFromメールアドレス user: POP3アカウント

有効送信元とは、前項の「4.4.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。

### -----例1-----

送信元sender@example.comから送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

form=sender@example.com

## -----例2-----

有効送信元IP アドレス192.168.1.2 のID:user-one を、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.2 user=user-one

😻 GIDEON AntiVirus - Mozilla Firefox	
ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(E) ツール(T) ヘルブ(H)	0
アンチウイルス アンチスパム	サポート
GIDEON Antil irus 更新状況 検出状況 共通設定 メール設定	▶ サーバ環境 他サービス
メール設定	
スパムチェックの有効/無効 ▶ SMTP ▶ POP3	▶ ページのアンドゥ
保守・状況 基本設定 詳細設定1 詳細設定2 転送メール ホワイトリスト	ブラックリスト チェックリスト
ホワイトリスト	
SMTP POP3	
SMTP	
オワイトリスト (記述例: host=127.0.0.2 from=sender@example.com)	<ul> <li>バムニックを悪め、する条件も特定できす。</li> <li>「行った活電」と条件をさている。それやくなります。</li> <li>「行った活電」と条件をさている。それやくなります。</li> <li>「行った活電」となります。</li> <li>「ないた」を、たります。</li> <li>「ないた」を、ないた」を、ないた」を、ないた」を、ないた。</li> <li>「ないた」を、ないた。こので、ないた」を、ないた」を、ないた」を、ないた。こので、ないた」を、ないた」を、ないた」を、ないた。こので、ないた」を、ないた。こので、ないた」を、ないた」を、ないた。こので、ないた」を、ないた。こので、ないた」を、ないた。こので、ないた。こので、ないた」を、ないた。こので、こので、ないた。こので、ないた。こので、ないた。こので、こので、こので、こので、こので、こので、こので、こので、こので、こので、</li></ul>
	@GiDEON Corp.

画面 4.4.6

### 4.4.7 ブラックリスト

ブラックリストはスパム判定方法のひとつとして適用します。判定スコアは、「4.4.2 基本設 定」の「BL ユーザ定義ブラックリスト」で指定します。指定できる条件には以下のものがあ ります。

#### SMTP

host: 有効送信元IP アドレス。IP アドレス/マスクと指定することで範囲も設定可能。ホスト名 は不可

from: エンベロープのFrom メールアドレス

to: エンベロープのTo メールアドレス

有効送信元とは、前項の「4.4.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。

#### -----例1-----

送信元IP アドレス192.168.1.2 から送信されてきた場合、ブラックリストを適用するには、以下のよう に入力します。

host=192.168.1.2

#### -----例2-----

送信元IP アドレス192.168.1.2 から送信され、from がsender@example.net の場合、ブラックリスト を適用するには、以下のように入力します。

host=192.168.1.2 from=sender@example.net

#### -----例3-----

送信元IP アドレス192.168.1.0 ~192.168.1.255 から送信されてきた場合、ブラックリストを適用する には、以下のように入力します。

host=192.168.1.0/255.255.255.0

### -----例4-----

送信元IP アドレス192.168.1.2 から送信され、from が@example.net の場合、ブラックリストを適用 するには、以下のように入力します。 この指定の場合、example.net の該当メールアドレスは全てブラックリスト適用となります。

host=192.168.1.2 from=@example.net

#### 第4章 アンチスパム設定

# ● POP3 host: 有効送信元IPアドレス。 IPアドレス/マスクと指定することで範囲も設定可能。 ホスト名は不可

from: メールヘッダ内のFromメール青dれす

user: POP3アカウント

有効送信元とは、前項の「4.5.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。





### 4.4.8 チェックリスト

個別のメールアドレスの入力や、@DOMEINのようにドメインごとに設定をすることができます。

#### SMTP

特定のアドレスのみスパム判定をする場合に、そのメールアドレスを登録します。登録が全くない場合にはホワイトリストの登録を除き、すべてのメールアドレスをチェックします。 個別のメールアドレスの入力や、@DOMEIN のようにドメインごとに設定をすることができます。

### POP3

登録された項目が一致した場合のみ「POP3 でスパムチェック」を行います。チェックリストに登録が 全くない場合は、ホワイトリストに登録されている以外のすべてのメールをチェックします。 記述方法は、ユーザID@IP アドレスとなります。「@IP アドレス」と記述すると、POP3 サーバすべて のメールをスパムチェックします。

### ● POP3削除

登録された項目が一致した場合のみ「POP3 サーバのメール削除」を行います。 ※POP3 サーバのメール削除は、「メール設定」-「転送メール」-「基本」で設定可能です。 チェックリストに登録がなく、「POP3 サーバのメール削除」が有効になっている場合は、転送メール 指定を行ったPOP3 アカウントすべてにメール削除が実行されます。

記述方法は、ユーザID@IP アドレスとなります。「@IP アドレス」と記述すると、POP3 サーバすべてのメールをスパムチェックします。

※チェックリスト、ホワイトリスト双方に同じ登録がある場合、チェックリストのみ有効となります。

🥹 GIDEON AntiVirus – Mozilla Firefox	
ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(E) ヘルブ(H)	<u>ه</u>
アンチウイルス アンチスパム	サポート
GIDEON	▶ サーバ環境
Antivirus 更新状況 検出状況 共通設定 メール設定	他サービス
メール設定	
スパムチェックの有効/無効 ▶ SMTP ▶ POP3	▶ ページのアンドゥ ▶ ページの初期化
保守・状況 基本設定 詳細設定1 詳細設定2 転送メール ホワイトリスト	ブラックリスト チェックリスト
チェックリスト	
SMTP	
デェックリスト (記述例: @example.com)	サングリストにメールアドレスを登録すると、そのメール アドレスガメールに含まれている場合のみ、スパ ムランやち行いなる場合のみ、スパ レランな方ではないる場合なかイ ドレスをついたしている場合なかイ リストの登録を続く、全てのメールアドレスをチェック します。アルファンクトのプステイナンデギが多くにあわ インディンクリストないの、そのいAIADがなクリスー・サーム そ40%して記述することで、900MADが含まれるア ドレスをてのスパムチェックを行います。 メールFT いたいのは、900 AIADがなりスー・サーム を増加して記述することで、900MADが含まれるア ドレスをてのスパムチェックが行います。 メールFT いたいのものになったります。 メールFT いたいのものになったります。 ・Indeexample.comのときスパムチェックする @example.com
	@ BIDEON Corp.

画面 4.4.8

### 5.1 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ッジボ リューム(論理
- パーティション)ヘ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BLOC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、BLOCを通過する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ッジをBLOCと接続します。
- (2)上記ストレッ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ッジは別途ご用意ください。

USB HDD、iSCSIにも対応しています。

・PortControlと連動して動作するためPortControlを先に電源投入(起動)してください。

- ・PortContrlとBLOCを接続し、BLOCの電源を投入します。
- ・BLOCの管理画面からストレッジの認識(iSCSIの場合)、ストレッジをマウントします。

# 5.2 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画面5.2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、BLOC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BLOC内部のHDDのパーティション(/dev/sdal)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ィ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(MBvte)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、透過プロキシー、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(「MTAアドオン」はBLOCでは使用されません)。

※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。

(ル(E) 編集(E) 表示(V) 履歴(S)	ブックマーク(B) ツール(T)	へルプ(日)						
シチウイルス アンチスパム アー	カイブ					ホスト管理	里 ボートコ	ントロールサポート
Antilirus	更新状況	保存状況	共	動定 .	メール設定		他想	▶ サーバ環境 ナービス
更新状況								
本日18時40分更新	インデックス作成ログ	1						
1+90:184	更新時刻	種別	件数	成否	対象ディレク		ポリューム	空容量[Mbyte] 🔺
> TRACT	2008-07-15 1840	mail	184	Success	/mnt/gideo	n_archive	/dev/sda1	68,077
P	2008-07-15 15:40	mail	123	Success	/mnt/eideo	n_archive	/dev/sda1	68,080
●自動更新 3時間毎 ▼	2008-07-15 12:40	mail	287	Success	/mnt/gideo	n_archive	/dev/sda1	68,082
● 報告 メーⅡ.	2008-07-15 09:40	mail	597	Success	/mnt/gideo	n_archive	/dev/sda1	68,086
19日トレトキ面新	2008-07-15 06:40	mail	13	Success	/mnt/gideo	n_archive	/dev/sda1	68,091
	2008-07-15 03:40	mail	0	Success	-		/dev/sda1	68,094
●スタート時刻	2008-07-15 00:51	mail-merge	928	Success	/mnt/gideo	n_archive	/dev/sdb1	634,974
00時 • 40分 •	9008-07-14 91-40	mail	02	Surrere	Imnt laidan	n archiva	/dau/eda1	69.090
	モジュール共通 🎵	アーカイブ	MTA	アドオン 2	8過プロキシー	GUI	ボート	コントロール
モジュール共通								
2008年07月01日更新	モジュール更新ログ							
パッチ名:20080630	更新時刻	パッチネ	3	成功/5	夫敗理由	接続サー		
	2008-07-01 00:18	20080	630	Succes	25	ns3.gide	on.co.jp	
▶ 于副史新	2008-03-03 00:00	20080	303	Succes	22	ns3.gide	on.co.jp	
●自動更新 1日毎 ▼	2008-03-03 00:00	20080	303	Succes	88	ns3.gide	on.co.jp	
	2008-03-03 00:00	20080	303	Succes	88	ns3.gide	on.co.jp	
▶ 不具合状況	2008-03-03 00:00	20080	303	Succes	88	ns3.gide	on.co.jp	
	2007-11-01 00:00	20071	101	Succes	22	ns3.gide	on.co.jp	
	2006-10-13 00:00	20070	301	Succes	22	ns3.gide	on.co.jp	
			54010					

画面 5.2

# 5.3 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画面5.3-1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〇印を付けます。
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	:論理ディ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	: 論理ディバイスの総容量(KByte)を表示します。
空容量	: 論理ディバイスの空容量(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。



画面 5.3-1

Page 86

### ● 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〇印を表示します。
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	:smtp もしくはpop のいずれかを表示します。
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。

IDEON AntiVirus 「ル(E) 編集(E)	- Mozilla Firefox 表示(业) 履歴	(S) ブックマーク(B)	ツール(① ヘル	げ(日)				
ンチウイルス	アンチスパム	アーカイブ				ホスト管理	ポートコントロ	ールサポート
Antil/int	JS	更新状況	保存状	況 共通設定	メール設定	E	他サービ	▶ サーバ環境 ス
保存状況								
		アーカイン	7状況					
最終保存 2008年07 サービス:p ポリューム/ /mot/gide	日時 月17日 の3 ペス: top archive/vol0	<u>本日</u> ポリューム	594	昨日	今月	594	先月 0	
		現 ボ	リュームバス	デバイス名	利用開始日	総容量(KB)	空容量(KB) 使月	用率 最終更新日
		0 /m		4			650,035,656	2% 2008/07/17
		/m	GIDEON	-				
		/mi	Antil/iru	s			-	
		/mi					-	
		/mi	● 検出日時			111	-	
		/m	- ++V7-7				-	
			-U-LAB	· · · · ·				
アーカイブ	n#		● ボリューム				▶検索 /	▶ ダウンロード
, ,,,,,								
新 保存日	時	サー ポリューム	· ////////////////////////////////////					結果
O 2008-	07-17 11:50:00	pop3 /mnt/gideon	From				deon.co.jp	add
○ 2008-	07-17 11:50:00	pop3 /mnt/gideon	<ul> <li>結果</li> </ul>	-			deon.co.jp	add
O 2008-	07-17 11:49:56	smtp /mnt/gideon					deon.co.jp	add
○ 2008-	07-17 11:47:47	pop3 /mnt/gideon				▶ クリア	a@gideon.co.jp	add
O 2008-	07-17 11:47:47	pop3 /mnt/gideon					s@gideon.co.jp	add
○ 2008-	07-17 11:46:18	pop3 /mnt/gideon					master@mailyał	noo.c add-noattr
O 2008-	07-17 11:45:20	pop3 /mnt/eideon			> 拾 宏	トキャンセル	ome-mail.info	add
○ 2008-	07-17 11:45:20	pop3 /mnt/gideon			- IN - M	1.05 210	nome-mail.info	add
○ 2008-	07-17 11:45:20	pop3 /mnt/gideon_a	rchive/vol0  2	20080717_114520.8472.12	16262720.23658	5.mht  shio	kawa@gideon.co.jp	add

画面 5.3-2

# 5.4 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、「3.3 共通設定」の項を参照してください。



Page 88

## 5.5 メール設定

### 5.5.1 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「3.4.1 保守・状況」の項を参照してください。

### 5.5.2 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。



画面 5.5.2

### 5.5.3 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"、" 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 リストを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「5.5.2 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。



### 5.5.4 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、selesB、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「5.5.3 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願います。



### 5.5.5 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。

OIDEON AntiVirus - Mozilla Firefox	-OX
ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルブ(H)	0
アンチウイルス アンチスバム アーカイプ	ボートコントロール サポート
GIDEON Antil irus 更新状況 保存状況 共通設定 メール設定	▶ サーバ環境 他サービス
メール設定	
アーカイブの有効/無効 ▶ SAYTP ▶ POP3	<ul> <li>ページのアンドゥ</li> <li>ページの初期化</li> </ul>
保守・状況 基本設定 アカウント グループ アクセス制限	
アクセス制限	
	Searchへのアクセンを制味します。記述がない場合は 全てのクライアントからのアクセスを許可します。記述 がある場合は、記述してあるクライアントからのアクセ スのみを許可します。
	記述方法に以上のとおり。 ・host=ウライアントのIPアドレス ・host=ウライアントのIPアドレス/ネットマスク
	< 記述例 > 192108111からのアセンを詳辛丁 host=19210811 りないました。 りないました。 りないました。 りないました。 りないました。 りないました。 りたいでは、 りたいで、 うたいで うたいで、 うたい う う う う う う つ
► R R	

画面 5.5.5

# 5.6 アーカイブ検索

# 5.6.1 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BLOCのIP:777/isearch

例えば、アーカイブBLOC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。

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(E) ヘルプ(H)		
<ul> <li> <ul> <li></li></ul></li></ul>	👻 🕨 💽 🗸 Google	Q
DE Possword: Password: ユーザを除 eccore oldecon corp.		

BLOC system

# 5.6.2 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」かつ「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。
То	: 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

😻 iSearch -	- Mozilla F	refox								_ 0 ×
ファイル(E)	編集( <u>E</u> )	表示①	履歴(S)	ブックマーク( <u>B</u> )	ツール①	ヘルプ(田)				()
	iS€	aro	h <sup>*</sup>	表示数 並び替え: k文 サブジェクト: From:	10 V	date 食索 IDEON Corp.	To:	size	簡易検索 詳細検索 ヘルブ ログアウト	

画面 5.6.2

### 5.6.3 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。

アイルビ 編集(2) 表示(3) 履歴(2) 75/70(2) ソール(2) ヘルブ(2)         デークタイブ: mail         表示数 並び答え: 10 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	😻 iSearch – I	Mozilla Fi	refox							
データタイナ: mail 10 0 date 2007 120 140 150 150 150 150 150 150 150 150 150 15	ファイル(E) i	編集(E)	表示①	履歴(S)	ブックマーク(B)	ツール①	ヘルプ(日)			
テータタイ: mail 10 0 date score size 11 48株衆 表示数 起び答: 10 0 date score size 11 48株衆 日付: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1										
ま示数 近び覧え: 10					データタイ	ブ: mail		_		簡易検索
ISearch ISearch From: From: Te: State:					表示数 並び替	え: 10	▼ date	score	size	詳細検索
					B	付:	<b>•</b>	<b>*</b> -	<b>•</b>	- D570F
サゴジェクト: From: Ce: 広けファイル: 日 有 ファイル 名: ローローローローローローローローローローローローローローローローローローロー					本	文:				
From: Ce: Ce: 添付ファイル: 「有ファイル名:[ admin 「all 「announce グループ検索対象: 「前を 「jobs 」 meeting 「office 」 query [ sales 日前を 「 query [ sales 年本 を2008 ODEON Corp.					サブジェク	ואל:				
To: Cc: 添付ファイル: □ 有 ファイル名: [ □ admin □ all □ announce ヴルーナ検索対象: □ info □ jobs □ meeting ヴルーナ検索対象: □ infice □ query □ sales □ sp □ spambox □ tech <u>検索</u> eccos o GDEON Corp.		:0			Fro	om:				
Cc: 添付ファイル: 「 有 ファイル名: 「 admin 」 all 「 announce グルーブ検索対象: 「 info 「 jobs 「 meeting グルーブ検索対象: 「 infice 「 query 「 sales □ sp □ spambox □ tech <u> 検索</u> eccome GIDECN Corp.		10	ear	ch	6	To:				
添付ファイル: □ 有 ファイル名: □ admin □ all □ announce グループ検索対象: □ hfo □ jobs □ meeting □ office □ query □ sales □ 申 □ spambox □ tech ■ 検索 e2006 oDEON Corp.					0	Cc:				
□ admin □ all □ announce グルーブ検索対象: □ office □ query □ sales □ sp □ spambox □ tech <u>夜衆</u> excoos otDEON Corp.					添付ファイ	ル: 🗆 有	〒 ファイル名:			
グルーナ検索対象: □ info □ jobs □ meeting のffice □ query □ sales □ sp □ spambox □ tech <u>検索</u> @2006 GDEON Corp.						🗖 ad	min 🗆 all 🗖	announce		
□ office □ query □ sales □ sp □ spambox □ tech ■ 検索 @2008 GDEON Corp.					グループ検索対	æ: □inf	o ⊡jobs ⊡r	neeting		
L sp L spambox L tech 使完 ©2008 GDEON Corp.					210 2 60001	∽ ⊑ off	ice 🗆 query I	sales		
複葉本 ezoos gibeon Corp.						L sp	L spambox	L tech		
@2008 GIDEON Corp.							検索			
						@200	8 GIDEON Corp.			



BLOC system

#### ● 検索結果

「表示数」で設定してある数の検索結果が表示されます。 サブジェクトがリンクになっていますので、これをクリックするとメール内容を参照できます。添付ファ イルがある場合、サブジェクトの右側にメールアイコンが表示されます。 [display] リンクをクリックすると検索キーワード(本文のみ)がハイライトされて表示されます。

「表示数」を超える検索結果がある場合、 検索結果の下部に以下のようなページリンクが表示されます。 このリンクをクリックすることで任意のページを表示することができます。 自分が属しているグループのみ表示されます。

#### ● メール内容表示

・メール内容が表示されます。

・添付ファイル名リンクをクリックすると添付ファイルがダウンロードできます。
 ・メールサイズがestproxy.confの「limitsize」を超える場合、添付ファイル名は表示されません。
 初期設定値:32MB

❸Search Result 日経 - Mozilla Firefox	
ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(E	) y-hO ~h7W 🔿
iSearch	表示数 並び替え: 10 0 date score size 防島検告 本文 サジジェクト: 日径
検索結果	Results of 1 - 10 of about 4613 for 日程 (7.699 sec.)
IntroductiveS and Originational Riskelph co jp / To. code From: codgbizmalia Riskelph co jp / To. code 社 ◆ 展示会・フォーラムの革前登録』こちら>> ち知らせぎ 希望	<u>L=D-1(market)と少</u> (14) <u>(18</u> (マクロフド)(イ 参約7/23 / 40 - 55(金) ◆ 会場 港選ルッセ ◆ 主催 日輩8P http:ケー(の)教 (uz)によった(部った)なったの)ため(日間PD)(スペーと登納において,詳社からの) - Copyright(C) 目 鍵の上しの3 書紙記事の)機能変換にます。「103-8646 (2020097178) (2016 日 : 2005 春紙記事の)機能変換にます。「103-8646 (2020097178) (2016 日 : 2005 春紙記事の)機能変換にます。「103-8646 (2020097178) (2016 日 : 2005 春紙記事の)機能変換にます。 (18) (18) (18) (18) (18) (19) (18) (19) (18) (19) (1

画面 5.6.3-2

第5章 メールアーカイブ設定

#### 5.6.4 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。

😻 ISearch Sign Up - Mozilla Firefox 📃 🗆 🗙					
ファイル(E) 編集(E) 表示(M) 履歴(S) ブックマーク(B) ツール(T) ヘルブ(H)					
iScoweb					
IDearch					
入力されたメールアドレスに仮パスワードを送信します。					
メールアドレス:					
再入力:					
送信					
iSearch					
@2008 GIDEON Corp.					
画面 564					

# 6.1 他サービス

アンチウイルス、アンチスパム設定画面の「他サービス」タブをクリックすると、画面6.1.1 が表示されます。

# 6.1.1 保守·状況

稼働状況 : ON の場合はBLOCが透過型ブリッジとして動作します。 OFF の場合はBLOCが非透過型ブリッジとして動作します。 ONの場合、アクセス先からはBLOCの存在が見えず、各PCが直接アクセスしてい るように見えます。 ログ :最新のログを取得し、下のログ一覧に表示します。 サービス : iptablesd(透過型ブリッジ)のサービス。 環境チェック :ボタンをクリックすると、システムの詳細情報を表示します。 [管理者に結果を送信する]ボタンをクリックすると、表示されている内容を管理者 宛に送信します。 再起動 :サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力 されている)の場合にONにします。 再設定 : サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生してい る場合にONにします。 ホワイトリスト:サーバのIPアドレスもしくはサーバのIPアドレスとポート番号を指定することで、指定 に一致したサーバをウイルスチェックから完全に除外することができます。 メール設定やウェブ設定のホワイトリストはHTTP/SMTPなどのプロトコルを監視し ながらチェックのみ行わないという方法ですが、本項目のホワイトリストの場合は監視 そのものも行いません。

> よって本項目を指定することにより、プロトコルを監視によって発生していたパフォーマンスの低下や、プロトコル解析に失敗していたために発生していたトラブルを回避 することができます。

設定項目は以下となります。

- ・host=接続先のIPアドレス
- ・port=ポート番号
- (例)
- ・サーバ192.168.1.1 のポート80番をスルーする場合、以下のように1行に記載します。 host=192.168.1.1 port=80



画面6.1.1

### 6.1.2 基本設定

#### ● ウイルスチェック、スパムチェックするネットワークの範囲

ウイルスチェック、スパムチェックをする接続元のネットワークの範囲を設定します。例えばローカルネット ワークが、 192.168.1.1 から 192.168.1.255 の範囲でのアクセスに制約する場合、 192.168.1.0/255.255.255.0 と設定します。 設定しない場合は、全てのネットワーク範囲についてウイルスチェック、スパムチェックを行います。 入力後、[更新]ボタンをクリックしてください。

初期設定値:設定なし



画面6.1.2

# 6.1.3 ホワイトリスト

サーバのIPアドレス、またはIPアドレスとポート番号を指定することでアンチウイルス、アンチスパムの対象から除外します。チェック対象から除外することで、パフォーマンスの低下やトラブルを回避することが可能です。

記述方法は、 host=接続先のIPアドレス port=ポート番号

初期設定値:設定なし



BLOC system

# 6.2 PortControl固有設定

PortControlを利用している場合、アンチウイルス、アンチスパム設定画面の「他サービス」タブを クリックしさらに「連携設定」タブをクリックすると画面6.2が表示されます。

### ● アクセスログ・検出ログ出力指定

自BLOCに出力する	:チェックマークを付けるとアクセスログ(プロトコル別アクセスログ)、検出ログ
	(ウイルス、スパム)を自BLOCに出力します。
他BLOCに出力する	:チェックマークを付けるとアクセスログ(プロトコル別アクセスログ)、検出ログ

(ウイルス、スパム)を他BLOC(自BLOC以外のBLOC)に出力します。 「IPアドレス」には自BLOC以外の他BLOCのIPアドレスを指定してくださ い。

 リモート出力 : チェックマークを付けるとアクセスログ(プロトコル別アクセスログ)、検出ロ グ(ウイルス、スパム)をリモートサーバに出力します。リモートサーバは、自 BLOC、他BLOC以外サーバを意味します。
 「IPアドレス」には、BLOC以外のリモートサーバIPアドレスを指定してくだい。

[更新]ボタンをクリックすることで、設定の入力、変更が有効になります。 [テスト]ボタンをクリックすることで、テストログを出力します。

ログ出力には、syslog-ngをサポートしている必要があります。

BLOCへ出力する場合、BLOCのアクセスおよび検出ログ先の設定に従って出力されます。

リモートに出力する場合、httpに関するログは以下のパスに書き込まれます。

/var/log/gwav/IPaddr/gproxy-http/access.log infection.log spam.log 上記パスのIPaddrは自BLOCのIPアドレスです。

http以外は、gproxy-ftp gproxy-smtp gproxy-pop としてパスが生成されます。

# ● システムログ出力指定

自BLOCに出力する ・システムログ(messages,syslog)を自BLOCに出力します。 リモート出力 ・システムログ(messages, syslog)をリモートサーバに出力します。リモート サーバは、自BLOC以外のサーバを意味します。 「IPアドレス」には、BLOC以外のリモートサーバIPアドレスを指定してくだ い。

[更新]ボタンをクリックすることで、設定の入力、変更が有効になります。 [テスト]ボタンをクリックすることで、テストログを出力します。

ログ出力には、sysylog-ngをサポートしている必要があります。 リモートに出力する場合、システムログは以下のパスに書き込まれます。 /var/log/gwav/IPaddr/messages syslog 上記パスのIPaddrは自BLOCのIPアドレスです。

### ● ファイル設定の同期

設定ファイル取得先IPアドレス : 指定したBLOCから「自動同期」で設定したインターバルで設定ファイルを同期(同一の設定内容)します。

[更新]ボタンをクリックすることで、設定の入力、変更が有効になります。

設定ファイルの同期 :通信はsshを利用しています。もし通信上でssh通信が使えない 場合には利用できません。

一部設定内容を反映できない項目があります。 例えば、BLOC に付与したIP や、パケットフィルタ情報などは同期化されません。

ファイル(E) 編集(E) 表示(V) 履歴(S) ブッ	クマーク(B) ツール(T) ヘルプ(H)		
Gideon Antil/irus	更新状況 検出状況	共通設定	ホートコントロール サホート ▶サーバ環境 メール設定 ウェブ設定 他サービス
他サービス			▶ ページのアンドゥ ▶ ページの初期化
3 <b>2</b> /010-0-	保守·状況 基本設定	ホワイトリスト	連携設定
連携設定 アクセスログ・検出ログ	出力指定		白印のパーリカオス・ つわせつ れん 検田市がた白可 のパーリカト ます
✓自BLOCに出力する 他BLOCに出力する リモート出力	IPアドレス IPアドレス	▶ 更 新 ▶ <del>7</del> スト	他ELOCIE出力する、アクセスログ・検出ログを他ELOCIE出力します。 リモート出力:アクセスログ・検出ログを他ELOCIE出力します。 ※テストボタンを押すとログがにテスト出力されます。
システムログ出力指定			
✓自BLOCに出力する リモート出力	IPアドレス	▶ 更 新 ▶ <del>7</del> スト	自BLOCに出力する:システムログを自BLOCに出力します。 リモート出力:システムログをリモートサーバに出力します。 ※テストボタンを押すとログがにテスト出力されます。
設定ファイルの同期			
設定ファイル取得先時	アドレス 自動同期 <sup>24時間毎</sup> ▼	▶更新	「設定フィイル取得先IPアドレス」で指定したBLOCから「自動同期」で設定した時間ごとに設定ファイルを同期します。
	画面6.2	2	

BLOC system
# 6.3 ボリューム

アーカイブ設定画面の「他サービス」 タブをクリックしさらに「ボリューム」 タブをクリックすると画面6.3が表示されます。

#### ● マウントするボリューム

- 使用中のボリューム : 現在使用中のボリュームが表示されます。初期の場合は、「初期 ボリューム」が表示されます。
- ボリュームローテーション有効:チェックすると、現在利用しているボリュームを使い回します。初期 設定では、ボリュームが95%に達すると、最も古い保存ディレクトリ からメールデータおよびインデックスを10日分削除します。95%以 下になるまで追加で10日分を削除します。

GUIからは上記の設定値を変更できません。この初期設定を変更する場合、以下の設定ファイルを変更します。

/etc/GwAV/archive/setting.conf

- ボリュームのデータを削除するボリュームの最大容量(パーセンテージ)の指定 VOLUME\_CHANGE\_PERCENT=95
- ローテーション時に最も古いデータから削除する日数の指定 VOLUME\_ROTATION\_DELETE\_DAYS=10

初期設定では、メールデータは所定のボリュームに日付毎ディレクトリにアーカイブしています。この日付 ディレクトリの古い順番で削除されます。

ボリューム(論理パーティション)のマウント指示を以下のリスト上でおこないます。

ファイルシステム	:表示されるリストから選択(vfat,ext3)します。
デバイス名	: マウントする論理パーティションを指定します。例えば、USBの
	HDDは /dev/sdal などとしてLinux は認識します。
利用開始日	:「ボリュームローテーション有効」にチェックマークがない場合にボ
	リューム使用開始する日付を入力します。

[更新]ボタンをクリックして、実際に指示されたボリュームに読み書きできる状態になると、左のボタンが「ON」になります。



BLOC system

## 6.4 iSCSI

メールアーカイブ設定画面の「他サービス」 タブをクリックしさらに「iSCSI」 タブをクリックすると 画面6.4-1が表示されます。

#### ● 基本設定

iSCSI : BLOCがおかれているネットワーク上で接続できるiSCSIが存在する場合、ボタンをクリックし、iSCSIのデーモンを起動します。

接続元(イニシエータ名) :自動的に採番しますので、通常は変更する必要はありません。変更したい場合は、欄に入力し[更新]ボタンをクリックします。

相互認証設定(必要な場合は設定)

: BLOCとiSCSIとの通信が必要な場合、CHAP認証方式ではユーザ 名、パスワードを入力します。

#### ● iSCSIディスク一覧

検索先IPアドレス :検索したいIPアドレスを入力します。

ポート番号 :検索したいポート番号(通常は3260)を入力します。

[検索]ボタンをクリックすることで、検索します。

検索時の認証(必要な場合は設定)

:BLOCとiSCSIとの通信が必要な場合、CHAP認証方式ではユーザ 名、パスワードを入力します。相互認証が必要な場合には「相互認証」 にチェックします。

😻 GIDEON AntiVirus -	- Mozilla Firefox						
ファイル(E) 編集(E)	表示(V) 履歴(S)	) ブックマーク(目) ツール	① ヘルプ(出)				
アンチウイルス	アンチスパム	アーカイプ				ホスト管理	ボートコントロール サポート
Antil/iru	s	更新状況	保存状況	共通設定	メール設定	1	▶ サーバ環境 他サービス
他サービス							
		保守·状況	基本設定	ホワイトリスト	連携設定	ポリューム	ISCSI
iSCSI							
	基本設定						
	iSCSIデーモン 起 接続元(イニシエ 相互認証設定()	動・停止 ▶ iSCSI ータ名) ign.2008-06.jp.c 必要な場合は設定)	ogideon.bloc:327e	4556927	▶更新	iSCSIデーモン きは停止でき しているiSCS iSCSIディスク	Aは、接続しているISOSIディスクがあると ません。接続元イイニシエータ名やも接続 iディスクがあるときは変更できません。 を切断してから停止・変更してください。
	CHAP認証	ユーザ名	パスワード		▶更新	してください。	定は、相互認識が必要なこそのの設定
	iSCSIディスク一覧	i					
●検索	検索先IPアドレス 検索時の認証( CHAP認証	め要な場合は設定) ユーザ名	ボート	3260 相互	忍証 ▶検索	検索先IPアト れているiSCS CHAP認証 検索先IPアト は、同じIPで	ドレスを指定し、検索することで提供さ SIディスクを検出できます。必要に応じて 音報を入力してください。 ドレスの情報がすでに一覧に存在するとき 検索するとそのIPアドレスのiSCSIディスク
●一覧	接続 接続先	接続ディスク名	Weller TS, ICI DOD	00160175100030	デバイス名	情報(自動語) 注音(ださい)	8続と認証情報)が初期化されますのでご
	UN 192.108.	1,200 npr.2004-08;jp.00	maio no-latuau-	uunuunveli Däüriai	x / uev/sdb	検索されたに iSCSIディスク クします。必要 定を行ってくた	・ COSIディスクは一覧に表示されます。 の2詳細を設定するには、該当行をクリッ 要に応じて、自動接続と認証情報の設 だとい。

画面6.4-1

検索されたiSCSIのディバイスリストを一覧に表示します。

リストの行をクリックすると、画面6.4-2が表示され、iSCSIに関する詳細な情報を示します。

接続	:ON になっていれば接続状態です。
接続先IPアドレス	: 接続しているiSCSIのIPアドレスを表示します。
接続先ポート	: 接続しているiSCSIのポートを表示します。
割当デバイス名	: 接続しているiSCSIのディバイス名を表示します。
	[詳細]ボタンをクリックするとより正確なディバイス名を表示します。
自動接続	: チェックした場合、次回のBLOC起動時に自動接続します。
CHAP認証設定	: iSCSIの接続時に認証が必要な場合、ユーザ名およびパスワードを入
	力します。相互認証が必要名場合には「相互認証」にチェックします。

[接続]ボタンをクリックすると、接続がOFFの場合、接続を試みます。接続に成功するとONになります。
[切断]ボタンをクリックすると、接続がONの場合切断を試みます。
[リストから削除]ボタンをクリックすると、接続先リストを削除します。
接続ONになっているリストを削除する場合には、必ず切断してから実行してください。
[キャンセル]ボタンをクリックすると、この画面での操作を無効にします。



**BLOC** system

# 7.1 サーバ環境

ハードウェアやネットワークの情報の取得と変更、messages やsyslog などのログのダウンロードなど を行う管理画面です。

## 7.1.1 保守·状況

#### ● ネットワーク

BLOCがネットワークに接続されており、正常に動作している場合、BLOCが検出したネットワークに関 連する情報を表示します。初期のBLOC設置時やネットワークの設定を変更した場合、このネットワー ク情報を確認してください。

[再設定]ボタンをクリックすると、ネットワーク情報を再取得します。ネットワーク接続を再起動するため、 画面アクセスが一時的に切断されます。

**ホスト名**: gideon-bloc (初期設定値)

DHCPからIPアドレス取得する場合、IPアドレス、サブネットマスク、デフォルトゲートウェイ、ネームサーバ 情報を自動取得します。

DHCPクラインアント接続ではなく、個別にIPアドレスを設定した場合、その設定情報が表示されます。

● サーバ状態	
時刻	:BLOC の内部時計の時刻
稼働時間	: BLOC の連続稼働時間
CPU使用率	:表示した時点でのCPUの利用度を%で表示します。
	BLOCのシステム稼働状態を表示します。
プロセス	:稼働中のプロセス数などを表示します。
メモリ	:メモリ(実メモリ、仮想メモリ)の使用容量(KB)を表示します。特に仮想メモリを
	多く使っている場合、パフォーマンスが極端に低下することがあります。このよう
	な場合、再起動することで解消する場合があります。
ディスク	: ディスクの使用容量(KB)を表示します。通常は十分な空き容量が残っていま
	す。空き容量が極端に少ない場合、再起動することを推奨します。

[再起動]ボタンをクリックすると、BLOCのサービスを一旦停止します(WEBアクセスやメール受信など のサービスも一時停止します)。その後約3分でサービスが再開し、利用できるようになります。 モジュール更新によっては、再起動を必要とする場合があります。再起動が必要な場合には、更新パッ チにその情報が記載されます。

[シャットダウン]ボタンをクリックすると、BLOCのサービスを停止し、電源を切ります。 ※サーバ情報は、自動的に更新表示されません。新しい情報を閲覧したい場合は、どこか別のタブを 一旦クリックしてから再度この画面に戻る必要があります。



## 7.1.2 ログ

サーバ環境画面の「ログ」タブをクリックすると、画面7.1.2が表示されます。

システムエラーログとして、「messages」または「syslog」の一覧が表示され、エラーや異常を発見する ために利用します。また、ログの一覧で検索したい文字列で特定のエラーを絞ることができます。

We その Mark And	ァイル(F) 🕴	編集(E) 表示(V) 履歴(S)	ブックマーク(B) ツー	ル(T) ヘルプ(H)					
クサナバム         クサナバム         サボル           ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・									
The Control of									
Control (1997)     Contro	アンチウイ	ルス アンチスバム							サホート
	GIDEO								
サーバー環境	Ant	ti <b>Virus</b>	更新状況	検出状況	共通設定	メール設定	ウェブ設定	他サービス	
#97-th2     07       message:     sydice       #2     12       #2     12       #2     12       #2     12       #2     12       #2     12       #2     12       #2     12       #2     12       #2     12       #2     12       #3     12       #4     #4        #4     #4		「一環境							
ARY-R2     D     BARE       Image: Contract Contrant Contract Contract Contract Content Contract Contrant Co									
MY-RR         P         Name           P         Name         Name <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
Image: Second			<b>风口</b> ,并汉	L 7 //	基本設定				
P         Pressure         System           Feb 21 142919 gidson-bloc grocy-pop[19242] License valid         Image: Control of the system of the sy			休可 402		善平政定				
messages         messages           Feb. 21 14:2919 eldoor-bloc groov-pop[19242]. Leense valid         Feb. 21 14:2919 eldoor-bloc groov-pop[19242]. AntiSpan Liense valid           Feb. 21 14:2919 eldoor-bloc groov-pop[19242]. AntiSpan Liense valid         Feb. 21 14:2919 eldoor-bloc groov-pop[19242]. AntiSpan Liense valid           Feb. 21 14:2919 eldoor-bloc groov-pop[19242]. AntiSpan Liense valid         Feb. 21 14:2919 eldoor-bloc groov-pop[19242]. AntiSpan Liense valid           Feb. 21 14:2919 eldoor-bloc groov-pop[19243]. Dettispan Liense valid         Feb. 21 14:2919 eldoor-bloc groov-pop[19243]. Dettispan Liense valid           Feb. 21 14:2920 eldoor-bloc upon-umn()PI0153]. session closed for user admin         Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4           Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4         Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4           Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4         Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4           Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4         Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4           Feb. 21 14:2927 eldoor-bloc dellem DHOPACK from 1921081.4         Feb. 21 14:2920 eldoor-bloc dellem DHOPACK from 1921081.4           Feb. 21 14:2926 eldoor-bloc dellem DHOPACk from 1921081.4         Feb. 21 14:2926 eldoor-bloc dellem DHOPACk from 1921081.4           Feb. 21 14:2926 eldoor-bloc dellem DHOPACk from 1921081.4         Feb. 21 14:2926 eldoor-bloc dellem DHOPACk from 1921081.4 <td></td> <td>9</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>		9							
Image: Control (Control (Contro) (Contro) (Control (Contro) (Control (Control (Control (Contro) (		messages	syslog						
Fab 21 142019 elsbort-bic groov-pap[0262]. License valid       Fab 21 142019 elsbort-bic groov-pap[0262]. AnGiam License valid         Fab 21 142019 elsbort-bic groov-pap[0262]. AnGiam License valid       Fab 21 142019 elsbort-bic trables(200) cache flab         Fab 21 142019 elsbort-bic groov-pap[0262]. MaGiam License valid       Fab 21 142019 elsbort-bic groov-pap[0263]. License valid         Fab 21 14202 elsbort-bic groov-pap[0263]. License valid       Fab 21 14202 elsbort-bic groov-pap[0263]. License valid         Fab 21 14202 elsbort-bic sulpap.mini/D103]. sois no Losed for user admin       Fab 21 14202 elsbort-bic sulpap.mini/D103]. Sois no Losed for user admin         Fab 21 14202 elsbort-bic sulpap.mini/D103]. sois no Losed for user admin       Fab 21 14202 elsbort-bic sulpap.mini/D103]. Sois no Losed for user admin         Fab 21 14202 elsbort-bic sulpap.mini/D103]. Sois no Losed for user admin       Fab 21 14208 elsbort-bic sulpap.mini/D103]. Sois no Losed for user admin         Fab 21 14208 elsbort-bic sulpap.mini/D103]. Sois no Losed for user admin       Fab 21 14208 elsbort-bic delsbirt bound to 120181182 remevel a 28 sconds.         Fab 21 14208 elsbort-bic delsbirt DHCPACK tron 1221811       Fab 21 14208 elsbort-bic delsbirt DHCPACK tron 122181.         Fab 21 14308 elsbort-bic trables(2003) cache fish       Fab 21 14308 elsbort-bic trables(2003) cache fish         Fab 21 14388 elsbort-bic trables(2003) cache fish       Fab 21 14308 elsbort-bic trables(2003) cache fish         Fab 21 14388 elsbort-bic trables(2002) cache fish       Fab 21 14388 elsbort-bic		<b>4</b> 2 <b>5</b> 22 <b>5</b> 10 <b>4</b>	36 o b					1 10 F	► # do: rp = k
Feb.21 142919 eideon-bloc groov-pop[19242]. License valid         Feb.21 142919 eideon-bloc groov-pop[19242]. AntiSpan License valid         Feb.21 142919 eideon-bloc staffeagm.in/19183         Feb.21 142920 eideon-bloc staffeagm.in/19183]. eession closed for user admin         Feb.21 142928 eideon-bloc staffeagm.in/191873]. eession closed for user admin         Feb.21 142928 eideon-bloc dellemt DHSPRAVE tiors 1127.0811.4         Feb.21 142928 eideon-bloc dellemt DHSPRAVE tiors 1127.0814         Feb.21 142928 eideon-bloc dellemt DHSPRAVE tiors 1127.0814         Feb.21 142928 eideon-bloc dellemt DHSPRAVE tiors 1127.0814         Feb.21 14285 eideon-bloc dellemt DHSPRAVE tiors 1127.0814         Feb.21 14285 eideon-bloc dellemt DHSPRAVE tiors 1127.0814         Feb.21 14385 eideon-bloc dellemt DHSPRAVE tiors 1127.0814			8 00 St -					× 201	P9000-F
Feb. 21 142919 elsborn-bic strong-roph(13242) AntiSpan License – valid         Feb. 21 142910 elsborn-bic strong-roph(13242) AntiSpan License – valid         Feb. 21 142910 elsborn-bic strong-roph(13242) AntiSpan License – valid         Feb. 21 142920 elsborn-bic strong-roph(13243) AntiSpan License – valid         Feb. 21 142920 elsborn-bic strong-roph(13243) AntiSpan License – valid         Feb. 21 142920 elsborn-bic strong-roph(13283) AntiSpan License – valid         Feb. 21 142926 elsborn-bic strong-roph(13183) AntiSpan License – valid         Feb. 21 142926 elsborn-bic strong-roph(131873) essis no lossed for user sdmin         Feb. 21 142926 elsborn-bic strong-roph(131873) essis no lossed for user sdmin         Feb. 21 142926 elsborn-bic delstrong-roph(131873) essis no lossed for user sdmin         Feb. 21 142926 elsborn-bic delstrong-roph(131873) essis no lossed for user sdmin         Feb. 21 14292 elsborn-bic delstrong-roph(131873) essis no lossed for user sdmin         Feb. 21 14292 elsborn-bic delstrong-roph(131873) essis no lossed for user sdmin         Feb. 21 14292 elsborn-bic delstrong-roph(211873) essis no lossed for user sdmin         Feb. 21 14292 elsborn-bic delstrong-roph(211873) essis no lossed for user sdmin         Feb. 21 14395 elsborn-bic delstrom-roph(211873) essis no lossed for user sdmin         Feb. 21 14395 elsborn-bic delstrom-roph(211873) essis no lossed essoches         Feb. 21 14395 elsborn-bic delstrom-roph(201873) essis no lossed essoches         Feb. 21 14395 elsborn-bic revol-reur-merul(		Feb 21 14:2010 gideon-blo	c #07022-000[10242]	License valid					
red 21 142919 eldon-bio ta Intersected 30 times red 21 142919 eldon-bio ta Intersected 30 times red 21 14293 eldon-bio tarros-man[1303] Lonce - valid red 21 14293 eldon-bio tarros-man[1303] Lonce - valid red 21 14293 eldon-bio tarros-man[1303] assin closed for user root red 21 14293 eldon-bio tarros-man[1303] assin closed for user admin red 21 14293 eldon-bio tarros-man[1303] assin closed for user admin red 21 14293 eldon-bio tarros-man[1303] assin closed for user admin red 21 14293 eldon-bio tarros-man[1303] assin closed for user admin red 21 14293 eldon-bio tarros-man[1303] assin closed for user admin red 21 14299 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 67 red 21 14395 eldon-bio dellem thOPROLEST no tho 1821081 April 70		Feb 21 14:29:19 gideon-blo	c gproxy-pop[19242]	AntiSpam License -	valid!				1
Feb 21 142920 adiobarchica garoox=mit(p19983) License — valid         Feb 21 142920 adiobarchica garoox=mit(p19983) License — valid         Feb 21 142923 adiobarchica sulpam,mix(p1813) assistion closed for user admin         Feb 21 142923 adiobarchica sulpam,mix(p1873) assistion closed for user admin         Feb 21 142923 adiobarchica sulpam,mix(p1873) assistion closed for user admin         Feb 21 142926 adiobarchica sulpam,mix(p1873) assistion closed for user admin         Feb 21 142926 adiobarchica subgaro,mix(p1873) assistion closed for user admin         Feb 21 142926 adiobarchica subgaro,mix(p1873) assistion closed for user admin         Feb 21 142926 adiobarchica subgaro,mix(p1873) assistion closed for user admin         Feb 21 142926 adiobarchica subgaro,mix(p1873) assistion closed for user admin         Feb 21 142926 adiobarchica bindimet DH2PAON from 152108114         Feb 21 142807 adiobarchica declineth DH2PAON from 152108114         Feb 21 143857 adiobarchica ducletineth DH2PAON from 152108114         Feb 21 143858 adiobarchica ducletineth DH2PAON from 152108114         Feb 21 143858 adiobarchica tables[4020] cache fisht         Feb 21 143845 adiobarchica tables[4020] cache fisht         Feb 21 143858 adiobarchica tables[40200] cache fisht         Feb 2		Feb 21 14:29:19 gideon-blo Feb 21 14:29:20 gideon-blo	⇒ iptablesd[4206]; ca c last message repe	she flash ated 36 times					
red 2.1 14:303 dilborn-bic dproor-timp() 3503 Annobal Letride — valid Fe 2.1 14:303 dilborn-bic dproor-timp() 3503 Annobal Letride — valid Fe 2.1 14:203 dilborn-bic dproor-timp() 3503 Annobal Letride — valid Fe 2.1 14:203 dilborn-bic stafforg munici()15073] assistion closed for user admin Fe 2.1 14:203 dilborn-bic delicite DHOFACUEST on the 0 12/151811 April 67 Fe 2.1 14:209 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:209 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:209 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:309 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:357 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:357 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:356 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:385 dilborn-bic delicite DHOFACK tron 152/1681 4 Fe 2.1 14:3856 dilborn-bic trobles(2000 cache fish Fe 2.1 14:3856 dilborn-bic challed(2000 cache fish Fe 2.1 14:3856 dilborn-bic enver-eui-menu(20086) response - no http protocol <000CTYFE html PUBLIC *-//NGC//0TD XHTML 1.0 Transitional//EN ** http://www.dor.ff.k.html/DTD.html*-transitional.dtf> - Atnu		Feb 21 14:29:20 gideon-blog	c gproxy-smtp[19363	3]: License valid					
Feb 21 142925 gidsom-bioc staffigam, unio)[19142] session closed for user admin Feb 21 142926 gidsom-bioc staffigam, unio)[19142] session closed for user admin Feb 21 142929 gidsom-bioc dhellemt DHOPREQUEST no tho 1921/881 Aport 67 Feb 21 14290 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 14395 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 143957 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 143957 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 143957 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 143957 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 143957 gidsom-bioc dhellemt DHOPREQUEST on tho 1921/881 Aport 67 Feb 21 143955 gidsom-bioc ginalbergid(300) cacher fabrin Feb 21 143955 gidsom-bioc gamegia-mexiga(300) Feb 2000 = no thip protocol 4000CTYPE html PUBLID *-//M60//DTD XHTML 1.0 Transitional//EW */http://www.sorg/TR/shtml1/DTD/shtml=transitional.dtd*> dtml		Feb 21 14:29:20 gideon-bio Feb 21 14:29:23 gideon-bio	c su(nam unix)[1930;	3) AntiSpam License 3) session closed for	valid! r user root				
Feb 21 142928 disborr-bio stafulgamu,unix)[10073] assission closed for user admin         Feb 21 142928 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 14209 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 14209 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 14209 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 14205 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143657 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143657 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143657 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143858 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143858 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143858 disborr-bio decliment DH2PROLUSET on the for U2180.1 port 67         Feb 21 143858 disborr-bio tableslef2005 cache fish         Feb 21 143858 disborr-bio tableslef2005 cache fish         Feb 21 143858 disborr-bio ense-seur-menru/D30500 (response - no http protocol. 4D0C)TPE html PUBLID *-//M307//DTD XHTML 1.0         Transitional//EN***********************************		Feb 21 14:29:25 gideon-blo	c sshd(pam_unix)[18	142] session closed	for user admin				
Fab. 21 14209 gidebrech defailer bH02P6X from 1221081 4         Fab. 21 14209 gidebrech defailer bH02P6X from 1221081 4         Fab. 21 142657 gidebrech defailer bH02P6DUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6DUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6DUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6CUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6CUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6CUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6CUEST no b10 n1221081 4         Fab. 21 142657 gidebrech defailer bH02P6CUEST no b10 n1221081 4         Fab. 21 142658 gidebrech defailer bH02P6CUEST no b10 n1221081 4         Fab. 21 142658 gidebrech defailer bH02P6CUEST no b10 n120181 4         Fab. 21 142658 gidebrech defailer bound to 1921081 152 renewal in 228 seconds.         Fab. 21 142658 gidebrech defailer berne berne b10 protocol (DOCTYPE html PUBLIC *-//WGC//OTD XHTML 1.0         Trans tional//EW *http://www.w3.org/TR/.shtml1/DTD/.shtml1-trans tional.dtd* > 4thml         Fab. 21 4280 gidebrech with with with with with with with wit		Feb 21 14:29:28 gideon-blo Feb 21 14:22:09 gideon-blo	c sshd(pam_unix)[18]	J73]: session closed UEST on br0 to 102	for user admin				
Feb 21 142209 getdsom-bloc dhellem bound to 192169.1182 renewel in 228 seconds.         Feb 21 142557 sidesom-bloc dhellem bHOPRACUEST on the 01 5210814 per rif         Feb 21 143557 sidesom-bloc dhellem bHOPRACUEST on the 01 5210814 per rif         Feb 21 143557 sidesom-bloc dhellem bHOPRACUEST on the 01 5210814 per rif         Feb 21 143557 sidesom-bloc dhellem bHOPRACUEST on the 01 5210814 per rif         Feb 21 143854 sidesom-bloc dhellem bHOPRACUE renewells in 288 seconds.         Feb 21 143894 sidesom-bloc (pdbledd2005) cache fisht         Feb 21 14384 sidesom-bloc (pdbledd2005) cache fisht         Feb 21 14281 sidesom-bloc (pdbledd2005) cache fisht		Feb 21 14:32:09 gideon-blo	c disclient: DHOPACH	( from 1921681.4	Tue.1.4 port of				
Feb 21 143557 sideon-bloc dhellem DHCPREQUEST on b10 to 152/16814 port 67 Feb 21 143557 sideon-bloc dhellem DHCPREQUEST on b10 to 152/16814 port 67 Feb 21 143557 sideon-bloc dhellem DHCPREQUEST in 152 renewal in 288 seconds. Feb 21 143856 sideon-bloc intables(2005) cache fisish Feb 21 143856 sideon-bloc intables(2		Feb 21 14:32:09 gideon-blo	c dholient bound to "	192.168.1.152 rene	wal in 228 seconds.				
Feb 21 (4385) relidentiation declarity UMX/MX. train (1921)001.4       Feb 21 (4385) relidentiation declarity tourist (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity tourist (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity tourist (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity tourist (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity tourist (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity (1921)031 (182 - renewal in 288 seconds.       Feb 21 (4385) relidentiation declarity (1921)031 (19		Feb 21 14:35:57 gideon-blog	c dholient DHOPREG	UEST on br0 to 192.	.168.1.4 port 67				
Feb 21 143949 eideon-bic ptables(#209) cache flash Feb 21 143959 eideon-bic ptables(#209) cache flash Feb 21 143956 eideon-bic ptables(#209) cache flash Feb 21 143956 eideon-bic ptables(#209) Feb 21 143956 eideon-bic ptables(#209) Feb 21 143956 eideon-bic enderson-bic enderson-		Feb 21 14:3557 gideon-blo Feb 21 14:3557 gideon-blo	a declient: DHCPACE c declient: bound to '	. from 192.168.1.4 192.168.1.152 rene	wal in 288 seconds				
Feb 21 143858 gishor-bic (ptables[d208] cache flash Feb 21 143856 gishor-bic (ptables[d208] cache flash Feb 21 143856 gishor-bic war-exi-menuZio88) response – no http protocol: (DOCTYPE html PUBLIC "-//WGC//OTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/.shtml1/DTD/.shtml1-transitional.dtg" > (html		Feb 21 14:38:49 gideon-blo	c iptablesd[4206]; ca	che flash					
Feb 21 143856 eidenr-bloc erwar-gui-meru/20886 response - no http protocol: COCCTYPE html PUBLIC "-//MSC//DTD XHTML 1.0 Transitional//EN " http://www.w3org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> khtml 		Feb 21 14:3853 gideon-blog	c iptablesd[4206] ca	che flash					
		Feb 21 14:3856 gideon-blog	c gwav-gui-menu[20	d36]: response - no h	nttp protocol: DOC</td <td>STYPE html PUE</td> <td>3FIC//M8C//</td> <td>DTD XHTML 1.0</td> <td></td>	STYPE html PUE	3FIC//M8C//	DTD XHTML 1.0	
		indiational//En intep///	mmmotorg/ rito xitch	invortovatoint dan	is nonatorial 2 strain				
									@GIDEON Co

画面7.1.2

## 7.1.3 基本設定

#### ● ネットワーク

BLOCは外部から更新するため、BLOC自体に固有のIPアドレスを使用します。BLOCをネットワーク上 に接続したときに、DHCPサーバから自動でIPアドレスが取得できる場合は、「DHCPサーバよりIPアド レス等を取得する」(初期設定値)にチェックします。

自動でIPアドレスが取得できない場合は、「DHCPサーバよりIPアドレス等を取得しない(手動設定)」 にチェックし、以下の項目を入力してください。

ローカルネットワーク上のプライベートアドレスを設定する例を説明します。

ホスト名	: bloc
IPアドレス	: 192.168.1.1
サブネットマスク	: 255.255.255.0
デフォルトゲートウェイ	: 192.168.1.250
ネームサーバ1	: プライマリネームサーバのIPアドレスを指定します。
ネームサーバ2	:セカンダリネームサーバのIPアドレスを指定します。

デフォルトゲートウェイは、コンピューターやルーターなどの機器です。所属するネットワークから外部のコ ンピューターへアクセスする際に使用する「出入口」の代表となります。アクセス先のIPアドレスについ て特定のゲートウェイを指定していない場合に、デフォルトゲートウェイに指定されているホストにデータ が送信されます。

設定元のBLOCからデフォルトゲートウェイまでは直接アクセスできることが必須です。 入力後、[更新]ボタンをクリックしてください。

#### ● 時刻設定

BLOCはサーバとして動作しています。サーバの内部時計は誤差が生じ、時刻がずれることがあります。正しい時刻を設定してください。

下記のタイムサーバを設定することで、時刻を適切に修正することができます。

#### ● タイムサーバ

BLOCの内部時計を、ネットワークを介して正しく調整するためのサーバを設定します。 デフォルト値:ntp.nict.jp

GIDEON AntiVi	irus - Mozilla Firefox	
ŀァイル(E) 編集(E)	表示(V) 履歴(S) ブックマーク(B) ツール(D ヘルブ(H)	
アンチウイルス	דידאגונג	サポート
Antil/irt	JS 更新状況 検出状況 共通設定 メール設定 ウェブ脱定 他サービ	2
サーバー環境		
	► <-ジのアンドゥ	▶ ページの初期化
	保守・状況 ログ 基本設定	
基本設定		
	ネットワーク	
	ODCOD 3 / 1 & 2017 / 1 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 5 / 2 # 8 2019 / 2 # 2 # 8 2019 / 2 # 2 # 8 2019 / 2 # 2 # 2 # 2 # 2 # 2 # 2 # 2 # 2 # 2	
	27.28477=12.23 2≈4.547-(1-1 2≈4.547-(1-2) ► E B	
	時刻設定 2007 m 2 m 22 m 10 m 23 m 25 m	_
	htpristjp	
		GIDEON Corp.

画面7.1.3

# 8.1 メールテストツール

### ● 受信テスト

外部サーバから「通常メール」「ウイルスメール」「スパムメール」を送信し、アンチウイルス機能、アンチ スパム機能が正しく動作しているかのテストを行います。 「受信アドレス」に受信可能なメールアドレスを入力し、「通常メール」「ウイルスメール」「スパムメール」 のいずれかをチェックして[受信]ボタンをクリックしてください。 その後、ユーザのメーラでメールを受信します(下記②の場合)。 受信テストは以下の手順で行います。

smtp① POP② BLOC → テストメール送信指示 → 受信メールサーバ → メーラによるメール受信 (管理画面) (送信メールサーバより メール配信)

① smtp経由:受信メールサーバの前の①にBLOCを設置した場合、[更新]ボタンをクリックすることで受信ログが取得できます。

② POP3経由:受信メールサーバとメーラ間の②にBLOCを設置した場合、メーラによるメール受信 が必要です。[更新]ボタンをクリックすることで受信ログが取得できます。

#### ● 転送テスト

BLOCから外部へのメール転送が可能かどうかのテストを行います。

転送先は、【アンチスパム】-【メール設定】-【詳細設定2】の転送メール設定や、警告メールなどで利用されます。

「転送アドレス」に利用する転送アドレスを入力し、「転送」ボタンをクリックしてください。

転送成功時には転送ログに「転送成功」を表示されます。

転送失敗時には転送ログに「転送失敗」と表示され、転送エラー内容も同時に表示されます。



## 8.2 サポート接続ツール

BLOC をリモートでサポートするためのツールです。ご利用につきましては弊社サポートセンターまで ご連絡ください。

ギデオンサポートセンター sp@gideon.co.jp

ご利用のBLOCからサポートセンターに安全な通信による接続を行います。サポートセンターから接続先の情報など指示がでますので、その情報を入力して接続してください。ネットワーク環境によっては、ファイアウォールなどの設定により接続ができないことがあります。

なお、直接サポートセンターに接続することによりBLOCの内部情報が一旦開示されますが、サポート目的の範囲で行います。ご了承をお願いいたします。

😺 GIDEO I	N AntiVi	us - Mo	zilla Fire	fox						
ファイル( <u>F</u> )	編集( <u>E</u> )	表示⊙	履歴( <u>S</u> )	ブックマーク( <u>B</u> )	ツール①	ヘルプ(円)				<
GIDE Ar	ntil/iru	s								
サが-	-1-									
++	#_L ###	メールナス	F / V	小一下按続						
9.	JV1-19240	-								
		9-1-								11.30   FE311 (FA 49768) +-+
·	按机力	アドレ ポート プロト MTU ユーヤ	·ス ・コル サイズ ∮−ID	• UDP 1280	_ TCP					り かったが ジーゲル Reactor A so ネットワーク J W M によって、ボート、フロトコル、MTUサ イズを変更しなければならない場合もあります。 ユーサーロ A おび バスワードについては野社までお 間 いらわせ だだい。 問合せ先:sp@eideonco.jp
•	プロキシ	●外 ●外 ● ア	フード 部サーバー 部サーバー ドレス	への接続にプロキ: への接続にプロキ:	ンを利用しな ンを利用する	0				プロキシ使用時は接続先プロトコルはTCPを指定し て下さい。
		か。 エー ハー	ート ーザーID スワード	E			_		接 統 切 断	
		接続状況	2					_	_	
•	接続状況 接続ログ	接続	状況	未接続					更新	播続式児が「建築中」になるには建築間結から数十 秒かを増合があります。構築間始からの砂持って ら「建築中」にならない場合になるない構成です。小野生し ている場合があります。「更新」各種して最新ログを 取得しログの内容を確認してください。
										GIDEON Corp.

画面8.2

# 9.1 接続方法

本章では、BLOCに直接モニター、キーボードを接続して個別にIPアドレスなどを設定する方法につい て説明します。

① キーボード、モニターをBLOCに接続します。

図9.1-1 のようにキーボードを接続します。モニターは図9.1-2 のように接続します。



BLOC本体の電源を入れます。

③ BLOCにログインします。

電源を入れてしばらくの間メッセージが続いた後、画面に以下のメッセージが表示されます。

Gideon Antivirus release xxx(Yokohama) Kernel xxx.gideon4 on an i686 login:

以下のイタリック部分を入力して「Enter」キーを押します。

login: admin

さらに以下のイタリック部分を入力して「Enter」キーを押します。 ただし、入力しても画面には表示されません。

Password: *gwantivirus* 

画面に以下のメッセージが表示されます。

[admin@gideon-bloc ~]\$

ルート権限ユーザーとなるために、以下のイタリック部分を入力して「Enter」キーを押します。

[admin@gideon-bloc ~]\$ SU -

さらに以下のイタリック部分を入力して「Enter」キーを押します。 ただし、入力しても画面には表示されません。

Password: *gwantivirus* 

画面に以下のメッセージが表示され、root権限ユーザーとしてログインされました。

[root@gideon-bloc admin]#

④ メニュー選択

③ でroot権限ユーザになると、画面8.1-3が表示されます。

BLOC system

**********	
Gideon	Antivirus BLOC System基本設定
キー)	メインメニュー
,	
a) 現在0	)設定を見る
b) 設定変	変更する
c) アップ	デートする
r) 障害復	夏田
z) メニュ	ーの終了
*****	**********
キーを選打	尺してEnterを押してください =>

画面9.1-3

「キーを選択してEnterを押してください =>」のあとにそれぞれ「a」「b」など該当するキーを入力します。

このコンソールメニューから、現在のBLOCの設定情報の閲覧や設定の変更などが可能です。また、 初期の工場出荷時の設定に戻すこともできます。

※基本設定画面はtelnetなどのリモートアクセスからも実行できます。その場合、リモート端末の文 字コードをSJISに設定してください。SJIS以外は文字化けします(DOSプロンプトでは設定は不要で す)。

# 9.2 固定IPアドレスの設定

ログイン後のメインメニューから固定IPアドレスを設定する方法を説明します。 画面9.2-1で、以下のイタリック部分を入力して「Enter」キーを押します。

キーを選択してEnterを押してください =>b

続いて以下のメッセージが表示されます。



図9.2-1

画面9.2-1で以下のイタリック部分を入力して「Enter」キーを押します。

キーを選択してEnterを押してください =>a

以下の画面が表示されます。

------IP アドレスを手入力する場合は'a'、DHCPサーバから取得する場合は'b'、 デフォルトゲートウェイを設定するには'c'を入力してEnterを押してください。

IPアドレスを再設定した場合は、いったんネットワークが切断されます。 (メインメニューに戻るには'm'を入力してください)

a/b/c/m =>

画面9.2-2

画面9.2-2で以下のイタリック部分を入力して「Enter」キーを押します。

a/b/c/m =>**a** 

指示に従って、IPアドレスとサブネットアドレスを入力します。 設定後は、画面9.1-3 「a)現在の設定を見る」から現在の設定を確認します。 正しく設定されていることを確認した後、一旦BLOCの電源をOFFにします。その後、ネットワーク接続 後に電源をONにしてください。 こうすることで、今行った設定を確定することができます。

## 9.3 困った時の設定

#### 9.3.1 ゲートウェイの設定

IPアドレス、サブネットマスクを正しく設定したにも関わらずインターネットにアクセスできない場合、ゲートウェイが正しく設定されていない可能性があります。

BLOCは、DHCPサーバー上でゲートウェイが記述されていれば、DHCPサーバーからIPアドレス取得 時にそのゲートウェイを参照します。DHCPクライアントとしてではなく、IPアドレスを入力して設定した場 合、必ずゲートウェイも入力して設定する必要があります。

いずれの場合でも、画面9.1.3の「a). 現在の設定を見る」でゲートウェイを確認してください。空欄また は異なっている場合、画面9.2-2で以下のイタリック部分を入力して「Enter」キーを押します。

a/b/c/m => C

指示に従って入力しゲートウェイを再設定します。

## 9.3.2 設定の初期化

設定を初期化したいとき、およびログインパスワードを忘れた場合は、画面9.1で以下のイタリック部分 を入力して「Enter」キーを押します。

キーを選択してEnterを押してください =>r

次に基本設定を工場出荷状態に戻すの"b"を選択します。

キーを選択してEnterを押してください =>b

BLOCの設定内容が、工場出荷時の設定に戻ります。

続く画面の指示に従って入力してください。

# 10.1 動作しないときは

- ●本製品の電源スイッチを押しても電源ランプが点灯しない。
- ⇒ 電源コードの接続状態、コンセントの状態を確認してください。
- ⇒ 異常が発見できない場合には、弊社サポートセンターへ修理をご依頼ください。

# 10.2 よくある質問と回答

#### Windowsファイル共有、P2Pファイル共有には対応していますか?

現在のところWindowsファイル共有には対応しておりません。P2Pファイル共有については、HTTP経 由で行うものについてはウイルスチェックしますが、それ以外のプロトコルを使用するものについては対 応していません。また、HTTP経由でもプロトコルが暗号化されている場合はパケットの中身を検査でき ないため、ウイルスチェックは行われません。

#### ファイアウォールやVPN機能はありますか?

ありません。本製品は、ウイルス、スパイウェア、マルウェア、スパムメールなどの検出に特化した位置付けの製品です。ファイアウォールやVPN機能につきましては、別の機器で対応していただくことになります。

#### アドウェア、スパイウェアには対応していますか?

はい、対応しています。

# URLフィルタリング(コンテントフィルタリング)には対応していますか?

対応しておりません。

# 本製品を導入することで、クライアントPCのアンチウイルスソフトは必要なくなるのでしょうか?

BLOC sytemはネットワークでのウイルス検知には対応しますが、クライアントPCのフロッピーやCD-ROM、USBメモリなどのメディアから直接感染するウイルスには対応していません。このような場合、 個別にクライアントソフトをお使いいただき、本製品と併用することでより強固なセキュリティ対策となりま す。

#### ユーザ数とは何を意味しているのでしょうか?

BLOCを通過するクライアントPCの台数です。メールサーバ同士のSMTP通信をウイルスチェックする 場合は、クライアントPCの台数が存在しません。詳しくは、お問い合わせください。

#### 機器の設定等行ってもらえるのでしょうか?

原則、お客様ご自身で設置・設定をお願いいたします。ユーザマニュアルをご覧いただくか、購入後の 技術サポート窓口にご連絡いただきますと、メールまたはお電話にて迅速な対応が可能です。 また、弊社で提携しているパートナー様により、別途(別料金にて)設置サービスをとりおこなうことも可 能です。詳しくはお問い合わせください。 株式会社ギデオンインフォーメーションセンター (こちらは技術サポート窓口ではありませんのでご注意ください) E-Mail:info@gideon.co.jp TEL:045-590-1216

#### 機器が故障してしまったようですが、どうすればいいですか?

故障後すぐに技術サポート窓口にご連絡ください。まずは操作方法の問題か、機器が本当に故障して いるのか、切り分けをさせていただきます。

万一、BLOCのハードウェア障害により修理が必要となる場合、モデルにより修理交換の手順が異なります。ご連絡いただいた後、技術サポートより改めてご案内差し上げます。

## ウイルス定義ファイル、スパムDBの更新の仕組みはどうなっていますか?

BLOCからHTTPポートを使い、インターネット上のアップデートサーバに接続して更新ファイルをダウン ロードします。したがって、BLOCからインターネット上の任意のウェブサイトに対してアクセスできなけれ ばなりません。

HTTPプロキシが存在する場合、BLOCでそのプロキシを設定することにより、更新ファイルのダウン ロードが可能です。設定方法については本マニュアルをご覧ください。

## システムにリモートログインできませんが、設定を教えてください。

システムへのリモートログインはtelnetもしくはsshで可能ですが、デフォルトではオフになっています。モ ニター、キーボードを装着しコンソールログインして、コマンドメニューから必要なログイン方法をオンにし てください。その際、WAN側のみ、LAN側のみ接続を許可する・しない、の設定も可能です。

## GUI管理画面にログインするパスワードを忘れてしまいました。

GUI管理画面を開いたときに、パスワード入力フィールドでパスワードを入力しても「パスワードが違う」 と言われる、もしくはログインパスワードを忘れてしまった場合、以下の方法でパスワードをリセットできま す。

## モニターとキーボードを直接BLOCに接続してください。

BLOCにrootユーザでローカルログインします。初期パスワードは製品に同梱された「ソフトウェアライセンス及びサポートサービス証書」に記載されていますので参照してください。rootアカウントにてログイン後、コマンドメニューが表示されます。b).設定変更-> h).GUI管理画面のパスワード変更を選択してください。

あるいは、"z"でコマンドメニューを終了して、直接"/etc/GwAV/cgi.password"ファイルを消しても 同じです。(rm /etc/GwAV/cgi.passwordを実行。)次回GUI管理画面にアクセスして、新しいパス ワードを入力してください。 なお、お客様に納入直後のGUI管理画面のログインパスワードは初期設定が /usr/local/gwav/. userInfo ファイルの2行目になります。パスワードが違う場合は、上記の手順でパスワードリセットしてく ださい。もし、1行目のお客様登録Noが、お手持ちの証書に記載されているお客様登録Noと異なる場 合、恐れ入りますが弊社までご連絡ください。インフォーメーションセンターにて対応させていただきま す。

#### ログに PHASE\_ENDsizeerror が多発しています。

システムログに PHASE\_ENDsizeerror が数多く見られる場合がありますが、実害はありません。一 部のウェブサイトで、インターネットのルールRFCに準拠していない振る舞いをするものがあり、そのレス ポンスがBLOCで想定していないものであるために、このメッセージが表示されます。

アンチウイルス検出エンジンは、スキャンするファイルの形式により様々な「リターンコード」という番号 を返します。"8"は「破損したファイル」を意味します。実際に「破損したファイル」が存在する場合もあ りますが、ログに多発している場合、WindowsUpdateなどが原因となっていることが考えられます。 WindowsUpdateでは、ファイルが破損しているというよりも、スキャンエンジンが「破損している」と解 釈してこのような出力をするだけなので、実際に問題はありません。WindowsUpdateをはじめとして、 HTTPプロトコルを使って様々な種類のやりとりをするクライアントエージェントがあります。このメッセー ジが出ないようにするには /usr/local/gwav/ave/gwav.conf ファイルの中に "VIRUS\_SCAN\_FA ILED\_NOWARNING\_CODE=8" 行を追加して、HTTPのウイルスチェックサービスを再起動してく ださい。

#### 定義ファイルはどの程度の頻度で更新されるのでしょうか?

新種のウイルスの対応は、開発センターで数分おきに行われています。24時間、365日体制で新種・亜 種のウイルスに対応しております。

# 10.3 お問い合わせ

製品に関するお問合わせは、弊社ホームページからご依頼下さい。また良くある質問(FAQ)等の最 新情報も併せて掲載していますので、下記のURLをご参照願います。

http://www.gideon.co.jp/

# サポートサービス

BLOCは、原則1年ごとの契約となっております。(契約期間につきましては別途発行される「サポート サービス証書」をご覧ください。)更新時期が近づきましたら「更新のご案内」をお送り致します。

サービス内容は以下のとおりです。

#### ■サービス内容

- 1.HTTPからのダウンロードによる最新バージョンの提供
- 2.E-Mailと電話によるお問い合わせの受付および回答 \*1\*2
- 3.E-Mailによる情報提供(不定期)
- 4. ウイルス感染の疑いがあるファイルの検証
  - (ウイルス誤認識の場合のファイル検査)
- 5.導入・運用に関わるコンサルティング \*1\*2\*3
  - \*<sup>1</sup>回数:3件まで
  - \*2出張によるサポートは別料金となります。
  - \*3導入・運用の請負は別契約となります。

#### ●注意事項

- a. サポートを受ける窓口は、1契約あたり1ヶ所のみに限定させていただきます。
- b.本製品では、定義ファイルおよびモジュールは、インターネット経由で最新のものに自動更新されます。
- c.更新は、1年ごとの継続更新が原則となります。継続更新がなされなかった場合は、再契約の際に、正規更新料の 120%の費用がかかります。

#### ■お問合せ方法

状況を正確に把握するため、メールで以下の項目を記載してお問合せください。

- 1.登録No.(製品購入時に発行されたナンバーです。「サポートサービス証書」に記載されていま す。)、または製品シリアルNo「S/N」(BLOCの底面もしくは側面に記載されています。)
- 2.お客様のお名前
- 3. 返信先E-Mail アドレス
- 4.電話番号
- 5.製品名(『ギデオン アンチウイルス ブロック システム』)
- 6.発生現象、ご質問内容
  - できるだけ具体的に記述してください。
- ・発生頻度
- ・メールログの記録などの具体的な情報
- ・再現テスト手順(特に再現性がある場合) など

#### ■お問合せ先

**JC** system

M

株式会社ギデオン テクニカルサポートセンター

E-mail / sp@gideon.co.jp

TEL. 045-590-3655 (横浜)

受付時間 / 9:00~17:00(祝祭日を除く、月~金曜日)

ギデオン BLOC system メールアーカイブ Plus ギデオン BLOC system メールアーカイブ 共通ユーザーズマニュアル

## 2009年 8月8日 第2刷

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 Inc Printed in Japan