ギデオン

GIDEON

ブロック システム

BLOC system

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

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。

目次

目次

BLOC system

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。


KASPERSKY
ANTI-VIRUS

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。

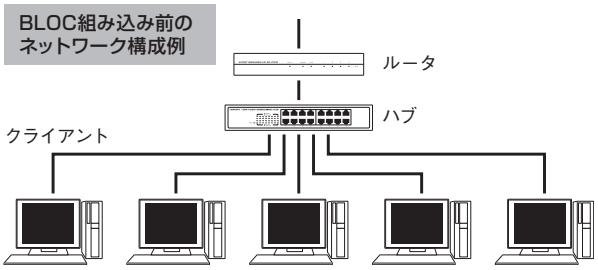


図2.1.1-1

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。

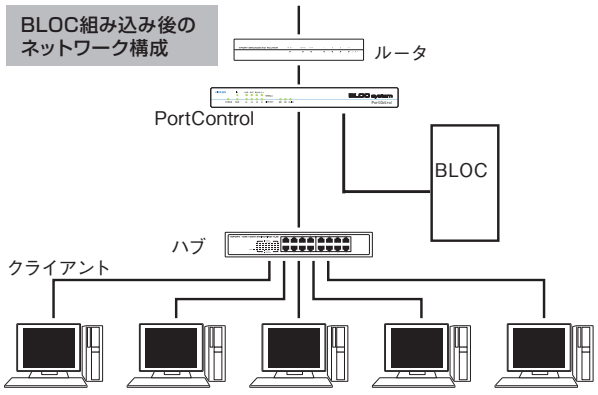


図2.1.1-2

※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。

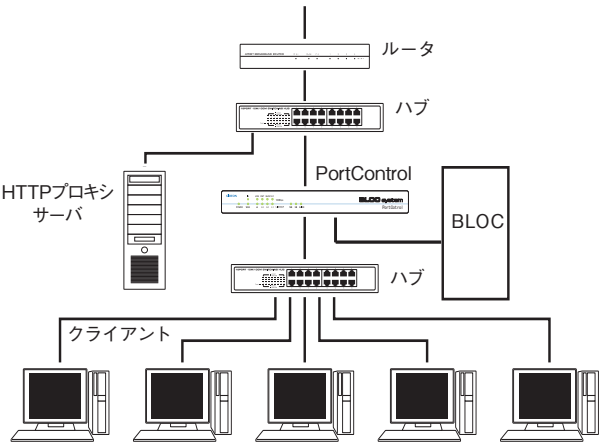


図2.1.2

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。

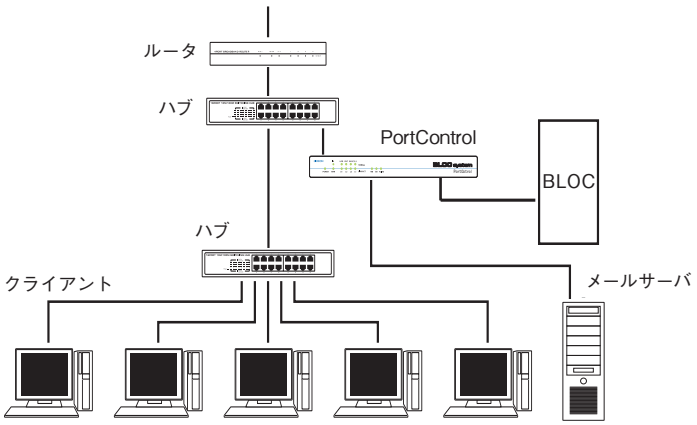
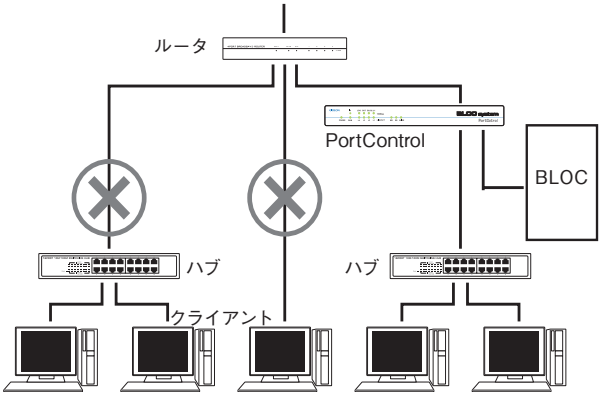


図2.1.3

2.2 接続方法についてのご注意

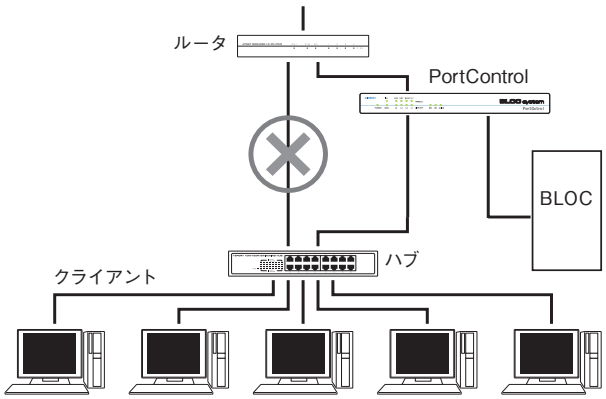
ルータと直結したネットワークの場合

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。

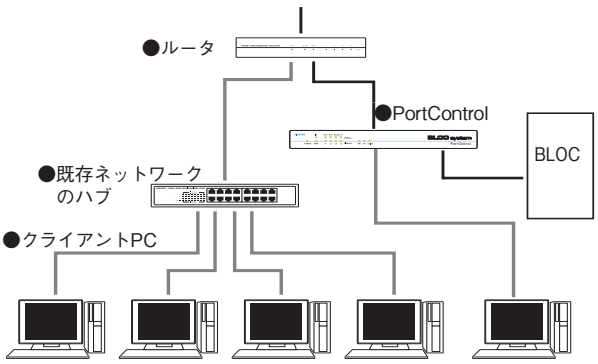
2.3 接続とセットアップ

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

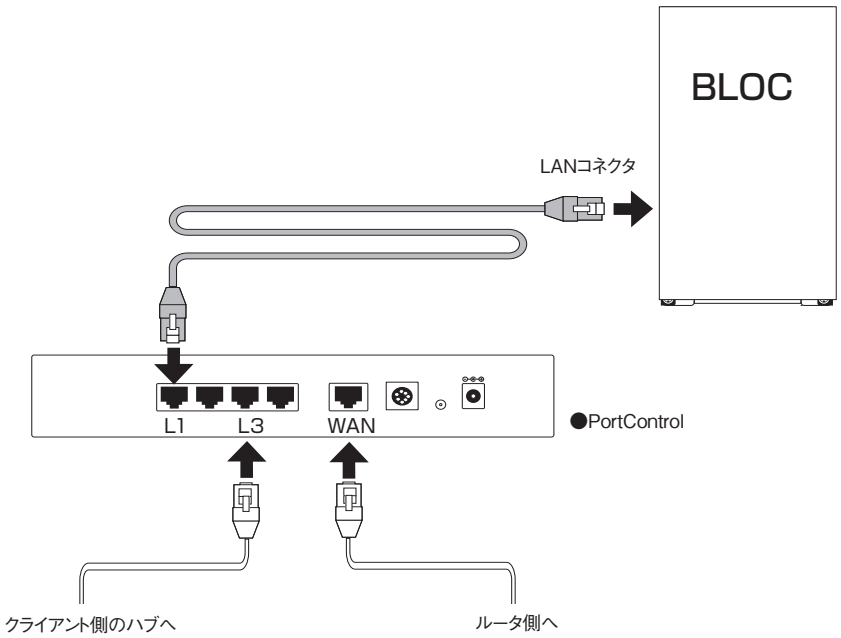
インターネット接続を停止させずにセットアップする場合、以下のようなネットワーク構成に追加変更します。

●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



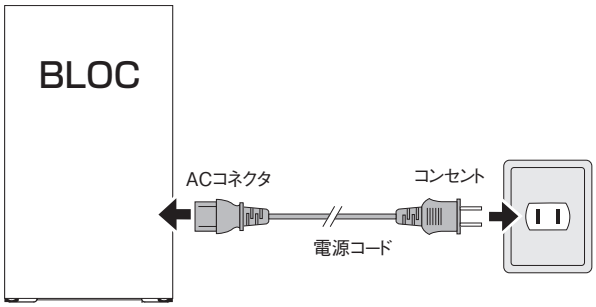
《手順 1》 Portcontrol の接続

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。

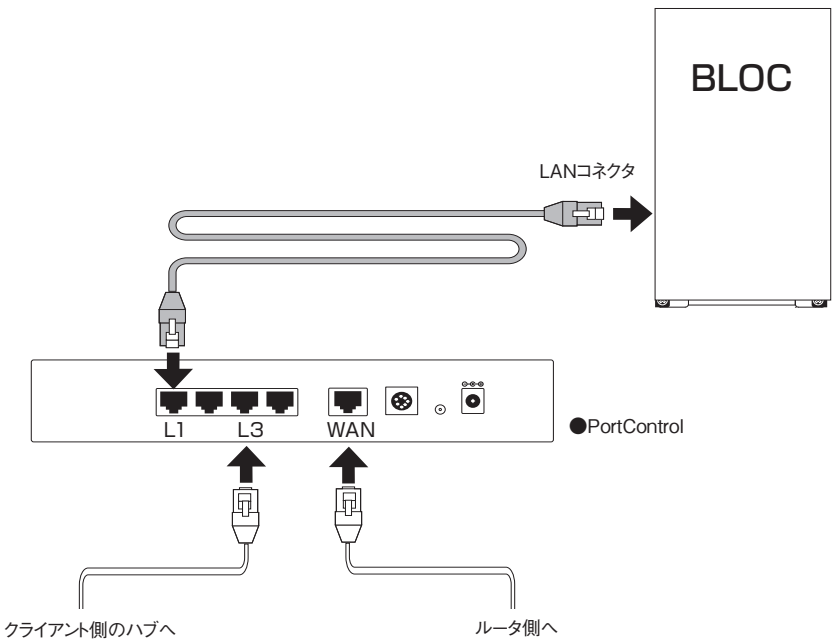
《手順4》 ネットワーク構成の変更

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。

2. 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

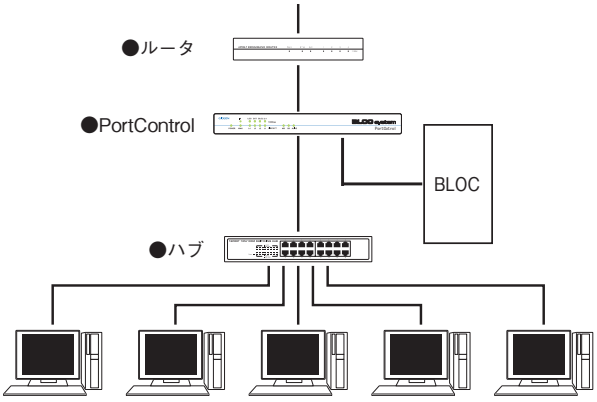


図2.3.2

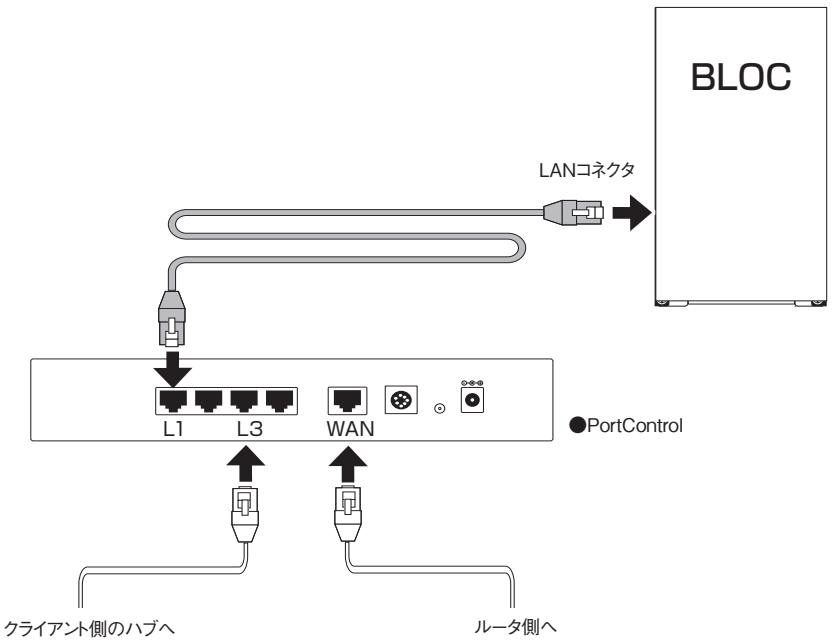
《手順1》 PortControlの接続

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。

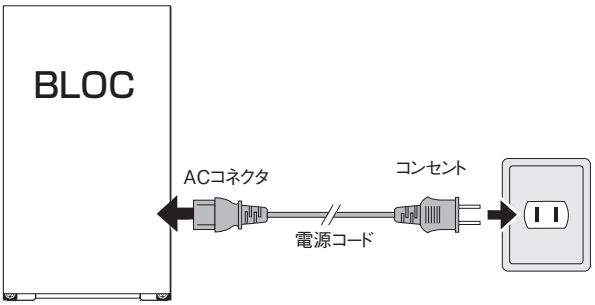
PortControlの「WAN」ポートと、ルータとをLANケーブルで接続します。

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。

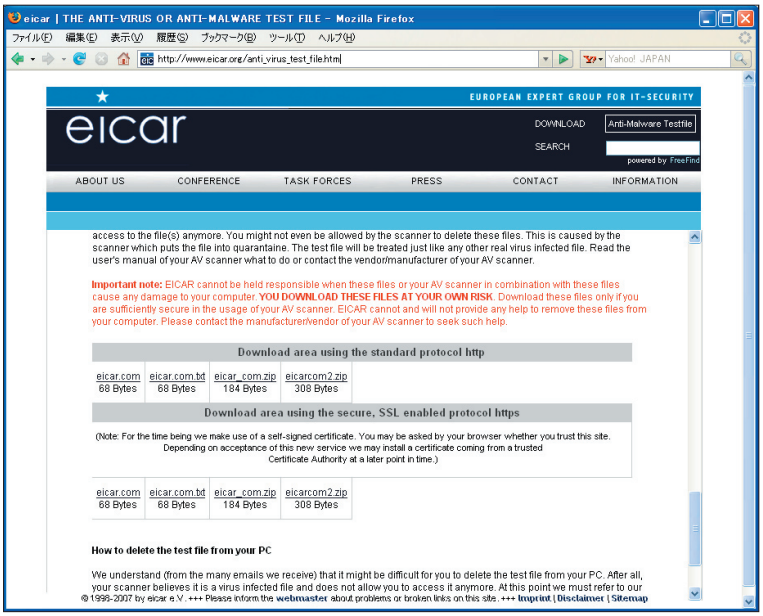
正常にセットアップが完了すると、ビープ音でお知らせしインターネットと接続が可能になります。

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 へアクセスしてください。

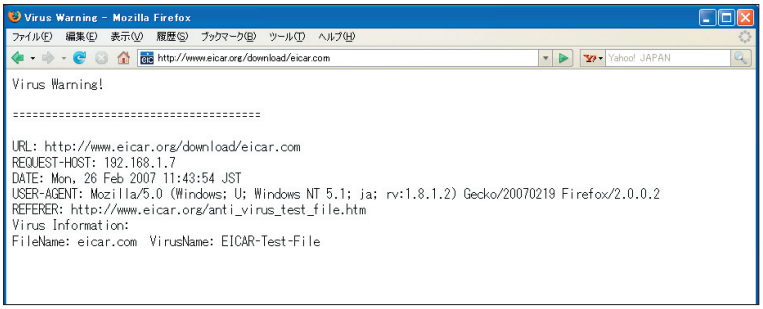
http://www.eicar.org/anti_virus_test_file.htm

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「eicar.com 」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。



画面2.4-2

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。

画面2.9.2

● 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。

登録　：PortControlでフィルタする場合のフィルタ適用の優先順位「ID」、パケットの「drop/pass」等設定を登録します。
フィルタ適用の優先順位「ID」を指定することで適用順位が決められます。
「drop/pass」はフィルタにマッチングしたパケットを破棄するか、スルーさせるかを選択します。
「TCP」にチェックマークを付けてONの状態にすると、フィルタをTCP/IPのパケットにのみ適用します。
「UDP」にチェックマークを付けてONの状態にすると、フィルタをUDP/IPのパケットにの

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）

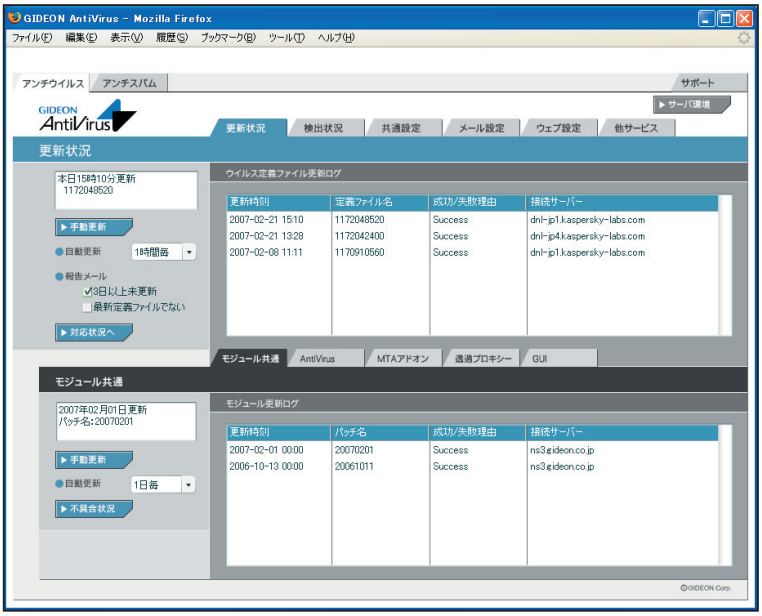
ウイルス定義ファイルの更新状況を表示します。
初期設定では1時間毎の自動更新に設定されています。緊急対策が必要な場合は[手動更新]ボタンをクリックし、最新の定義ファイルを取得してください。
※既に更新済みの場合は、新たに更新されません。

「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）。



画面3.1

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。

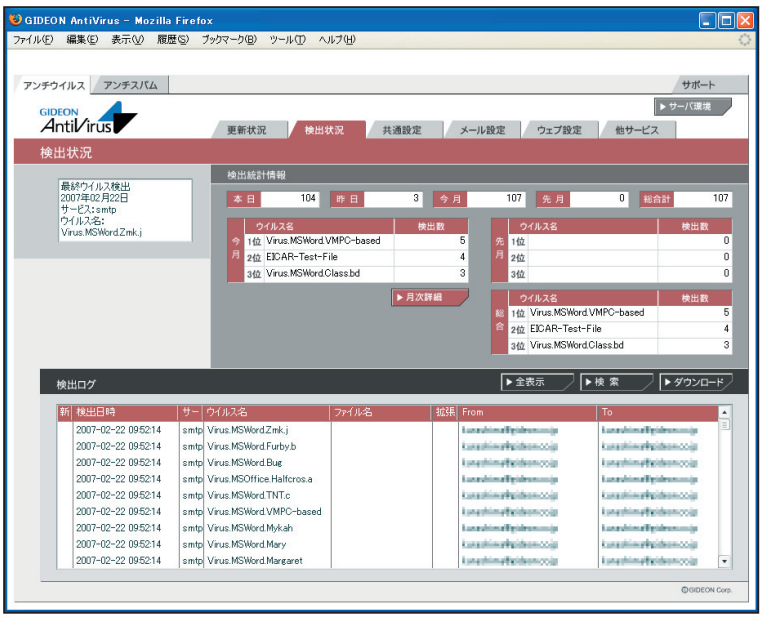
※「検出ログ」では最新の1000件までの検出ウイルスを表示します。

● 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。



画面3.2

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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
GIDEON AntiVirus
▶サーバ環境
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
共通設定
▶ページのアンドゥ
▶ページの初期化
基本設定
詳細設定
更新環境設定
基本設定
ライセンス
●登録No.
●パスワード
▶検証
▶更新
本ソフトウェアの契約期間のご利用、ウイルス定義ファイルや更新パッチを取得するために使用します。
正確に入力されているか確認するためには、インターネットが利用可能な状態で検証ボタンを押してください。※検証ボタンでは情報の更新は行われません。
管理者のメールアドレス
●報告メール
▶更新
●警告メール
▶更新
報告メールには、保守運用のための報告メールや管理画面の情報を送信するメールアドレス先を記述してください。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先を記述してください。
記入は、postmaster@example.comのようにアドレスだけ指定してください。
複数記入するときは、アドレスとアドレスの間に半角スペースを記述してください。
postmaster@example.com virus-admin@example.com
警告メールに記入するFROMフィールド
●名前部
ウイルス対策システム
●アドレス部
MAILER-DAEMON@localhost
▶更新
警告メールや、報告メールに記述するFromフィールドを記入します。メールのFromに記述されます。
名前部には、ユーザーが見て分かりやすい名前を、アドレス部には返信可能なアドレスを記入してください。
名前部：ウイルス対策システム
アドレス部：virus-error@example.com
©GIDEON Corp.

画面3.3.1

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

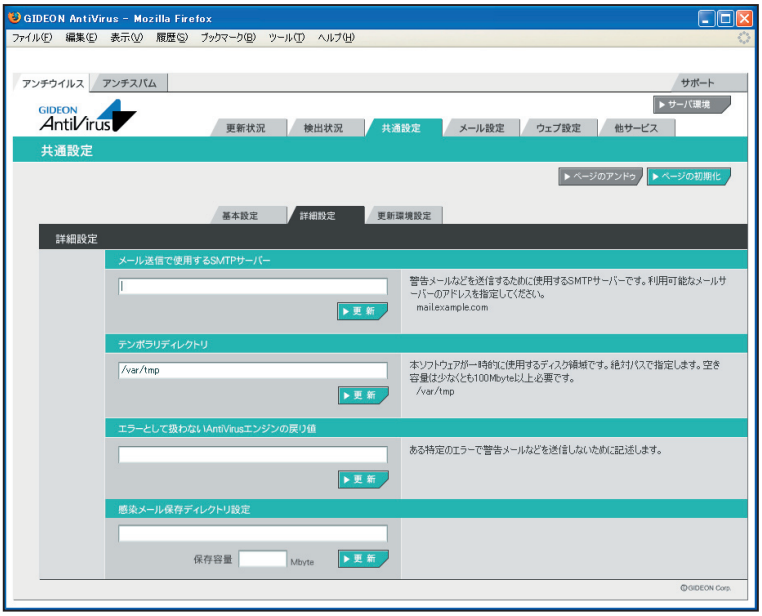
BLOCが一時的に使用するディスク領域です。絶対パスで指定します。容量は100MB以上必要とします。通常は変更の必要はありません。
初期設定値：/var/tmp（通常は変更不要）
変更する場合は入力後、［更新］ボタンをクリックしてください。

● 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。

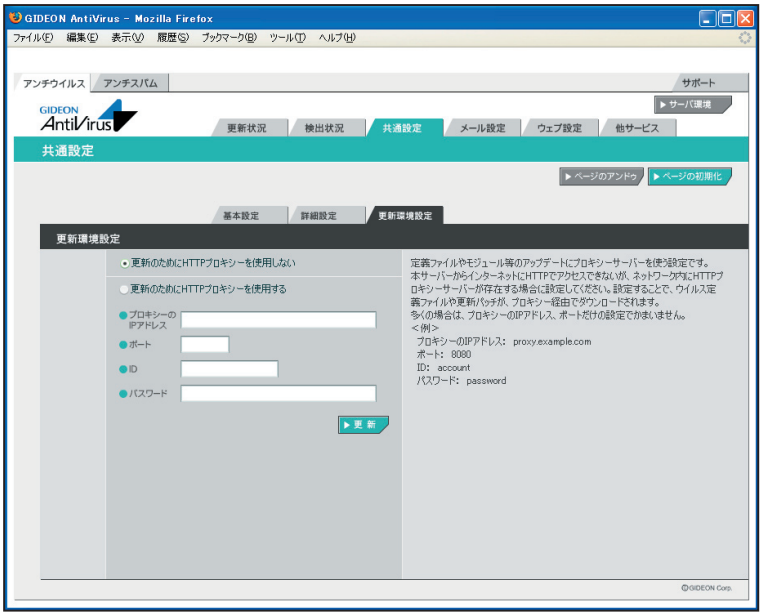


画面3.3.2

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



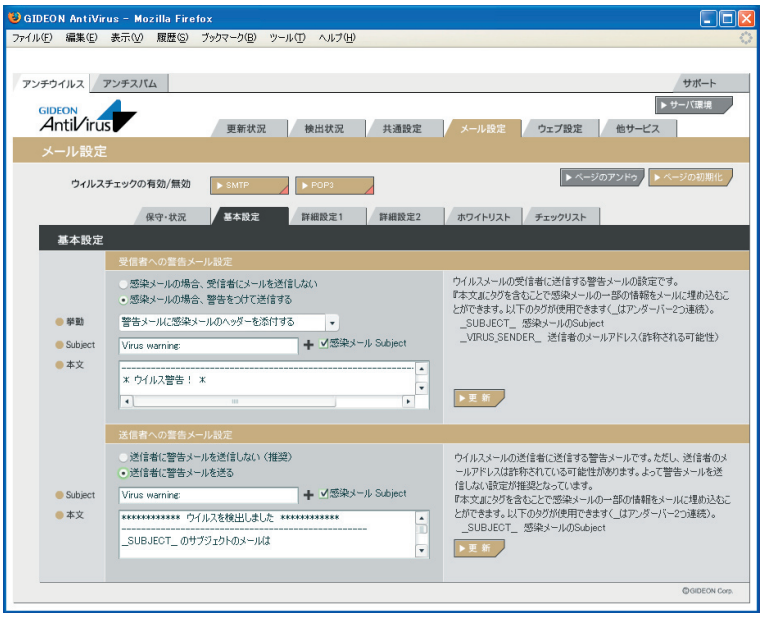
画面3.3.3

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。



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。

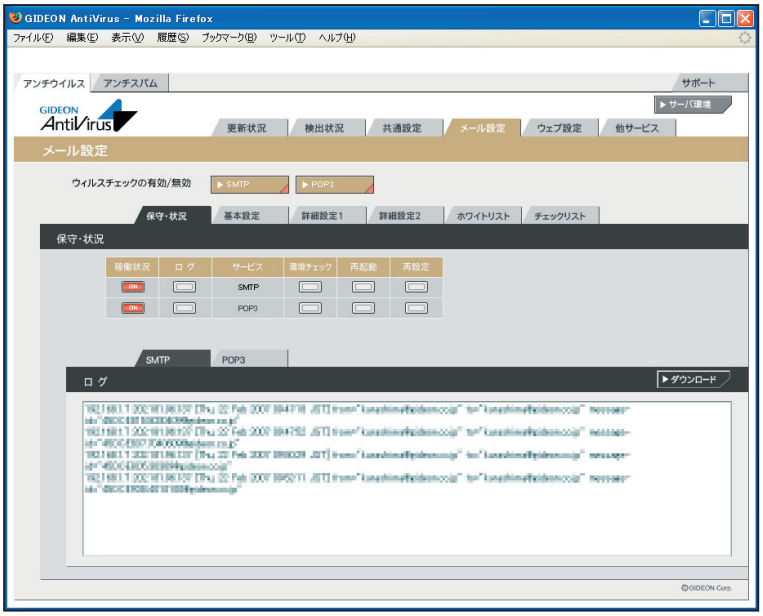
環境チェック　：該当ボタンをクリックすると、システムの詳細情報を表示します。[管理者に結果を送信する]ボタンをクリックすると、表示されている内容を管理者宛に送信します。

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。

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。

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。



画面3.4.1

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

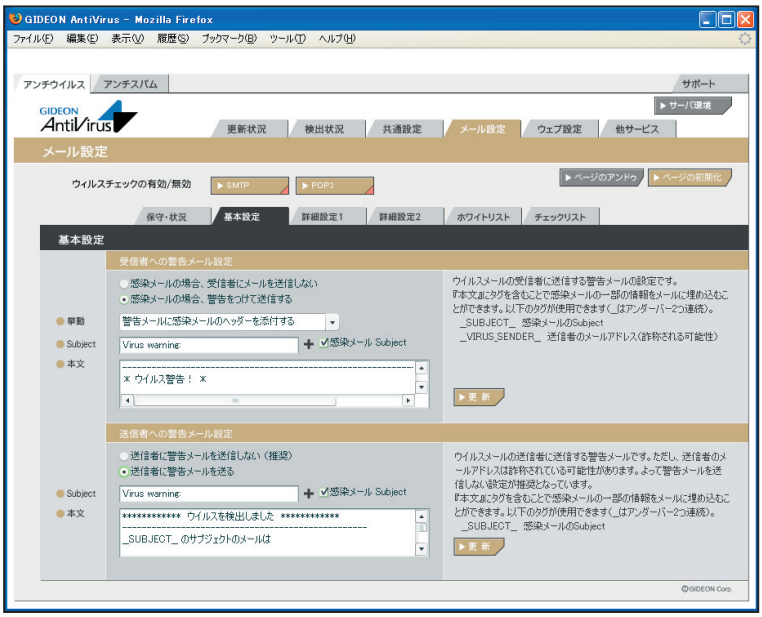
● 送信者への警告メール設定

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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
GIDEON AntiVirus
サーバ環境
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
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
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、警告をつけて送信する
単動
警告メールに感染メールのヘッダーを添付する
Subject
Virus warning:
感染メール Subject
本文
x ウイルス警告！ x
ウイルスメールの受信者に送信する警告メールの設定です。
『本文』にタグを含むことで感染メールの一部の情報をメールに埋め込むことができます。以下のタグが使用できます(_はアンダーバー2つ連続)。
SUBJECT 感染メールのSubject
_VIRUS_SENDER_ 送信者のメールアドレス(詐称される可能性)
更 新
送信者への警告メール設定
送信者に警告メールを送信しない（推奨）
送信者に警告メールを送る
Subject
Virus warning:
感染メール Subject
本文
********** ウイルスを検出しました **********
SUBJECT のサブジェクトのメールは
ウイルスメールの送信者に送信する警告メールです。ただし、送信者のメールアドレスは詐称されている可能性があります。よって警告メールを送信しない設定が推奨となっています。
『本文』にタグを含むことで感染メールの一部の情報をメールに埋め込むことができます。以下のタグが使用できます(_はアンダーバー2つ連続)。
SUBJECT 感染メールのSubject
更 新
©GIDEON Corp.

画面3.4.2

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

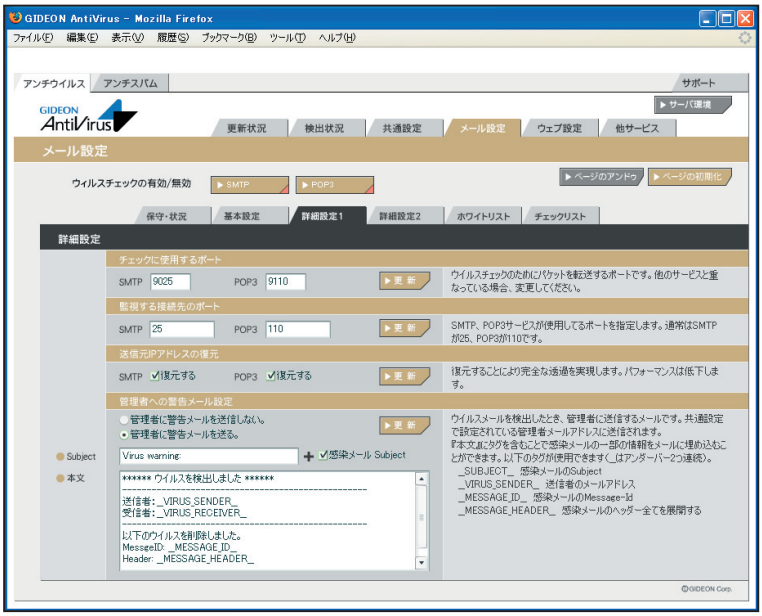
メールがウイルスに感染していた場合、警告メールを管理者に送信することができます。「3.3.1 基本設定」で設定した、警告メールの送信先へ送信します。

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。

（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があります。
__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：管理者に警告メールを送る


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
GIDEON AntiVirus
サーバ環境
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
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
詳細設定
チェックに使用するポート
SMTP 9025
POP3 9110
更新
ウイルスチェックのためにパケットを転送するポートです。他のサービスと重なっている場合、変更してください。
監視する接続先のポート
SMTP 25
POP3 110
更新
SMTP、POP3サービスが使用してるポートを指定します。通常はSMTPが25、POP3が110です。
送信元IPアドレスの復元
SMTP 復元する
POP3 復元する
更新
復元することにより完全な通過を実現します。パフォーマンスは低下します。
管理者への警告メール設定
管理者に警告メールを送信しない。
管理者に警告メールを送る。
更新
ウイルスメールを検出したとき、管理者に送信するメールです。共通設定で設定されている管理者メールアドレスに送信されます。
『本文』にタグを含むことで感染メールの一部の情報をメールに埋め込むことができます。以下のタグが使用できます(_はアンダーバー2つ連続)。
SUBJECT 感染メールのSubject
_VIRUS_SENDER_ 送信者のメールアドレス
_MESSAGE_ID_ 感染メールのMessage-Id
_MESSAGE_HEADER_ 感染メールのヘッダー全てを展開する
Subject
Virus warning:
感染メール Subject
本文
****** ウイルスを検出しました ******
送信者: _VIRUS_SENDER_
受信者: _VIRUS_RECEIVER_
以下のウイルスを削除しました。
MesseeID: _MESSAGE_ID_
Header: _MESSAGE_HEADER_
GIDEON Corp.

画面3.4.3

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。
初期設定値 : 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

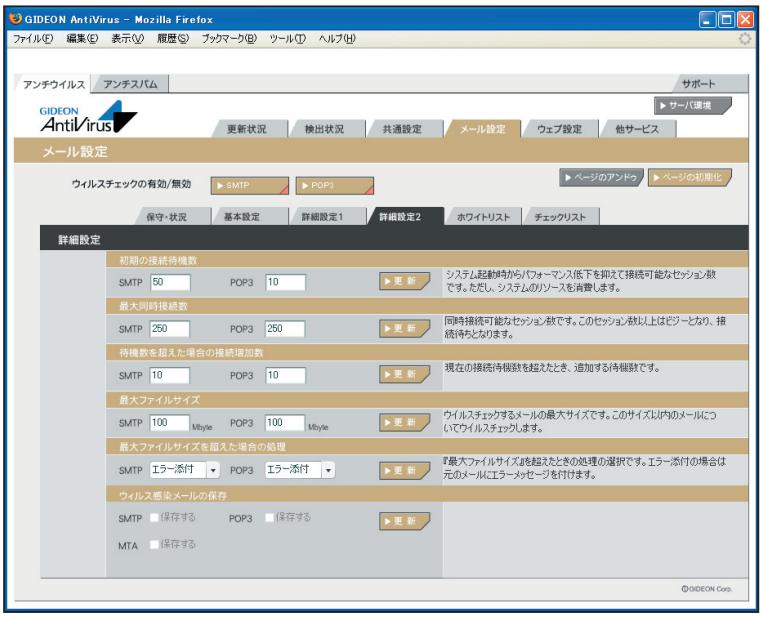
チェックするメールの最大サイズを指定します。最大サイズを超えるメールはウイルスチェックされずエラーになります。
初期設定値 : SMTP 100（MB）　POP3 100（MB）

● 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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
サーバ環境
GIDEON AntiVirus
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
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
詳細設定
初期の接続待機数
SMTP 50 POP3 10
更新
システム起動時からパフォーマンス低下を抑えて接続可能なセッション数です。ただし、システムのリソースを消費します。
最大同時接続数
SMTP 250 POP3 250
更新
同時接続可能なセッション数です。このセッション数以上はビジーとなり、接続待ちとなります。
待機数を超えた場合の接続増加数
SMTP 10 POP3 10
更新
現在の接続待機数を超えたとき、追加する待機数です。
最大ファイルサイズ
SMTP 100 Mbyte POP3 100 Mbyte
更新
ウイルスチェックするメールの最大サイズです。このサイズ以内のメールについてウイルスチェックします。
最大ファイルサイズを超えた場合の処理
SMTP エラー添付 POP3 エラー添付
更新
『最大ファイルサイズ』を超えたときの処理の選択です。エラー添付の場合は元のメールにエラーメッセージを付けます。
ウィルス感染メールの保存
SMTP 保存する POP3 保存する
更新
MTA 保存する
©GIDEON Corp.

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

● 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-----

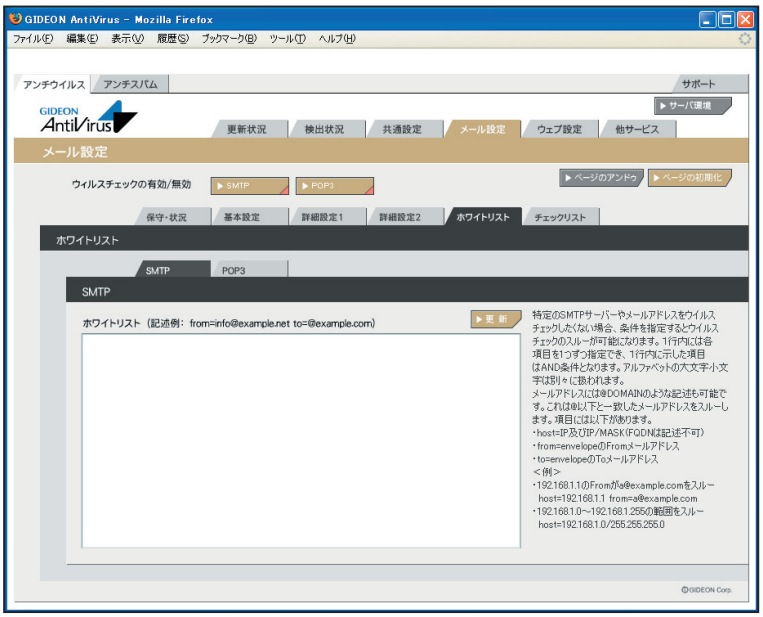
送信元sender@example.com から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

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



画面3.4.5

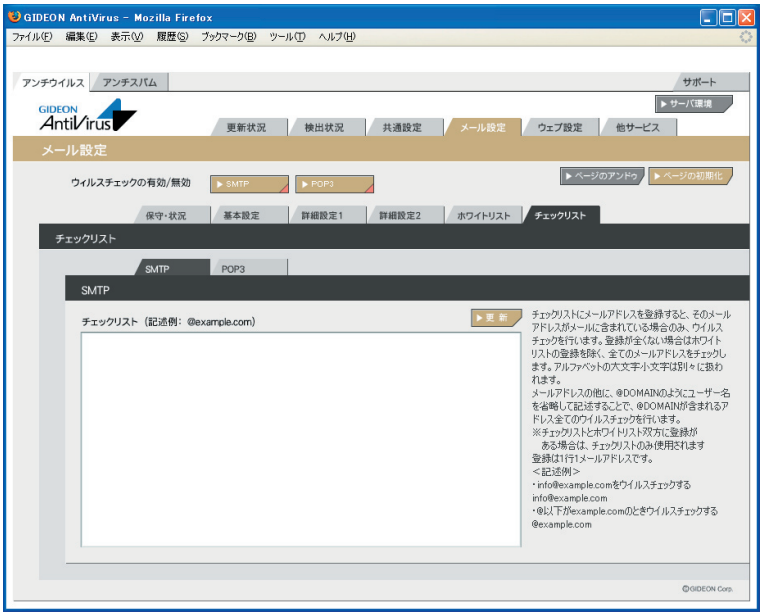
3.4.6 チェックリスト

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



画面3.4.6

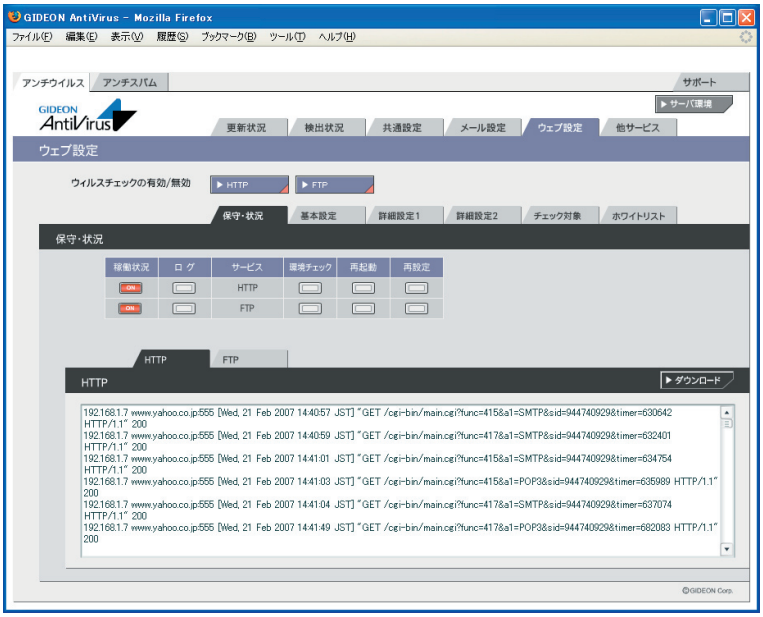
3.5 ウェブ設定

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。



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。

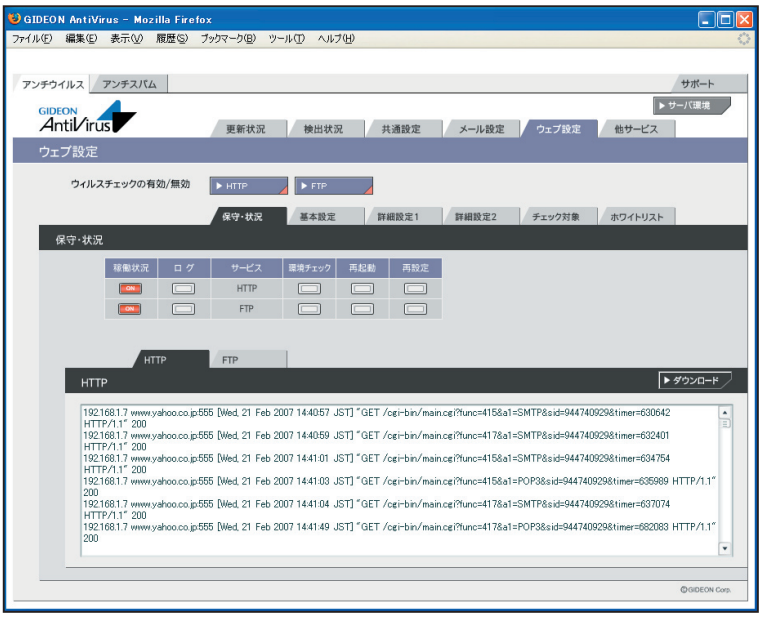
サービス　：HTTPのサービス。

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。



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

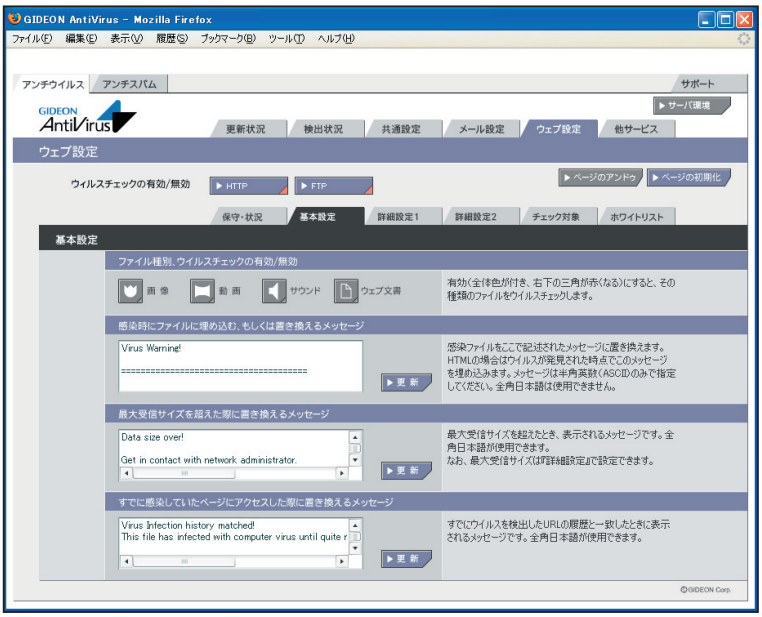
● 最大受信サイズを超えた際に置き換えるメッセージ

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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
サーバ環境
GIDEON AntiVirus
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
ウィルスチェックの有効/無効
HTTP
FTP
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
チェック対象
ホワイトリスト
基本設定
ファイル種別、ウイルスチェックの有効/無効
画像
動画
サウンド
ウェブ文書
有効(全体色が付き、右下の三角が赤(なる)にすると、その種類のファイルをウイルスチェックします。
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
Virus Warning!
更新
感染ファイルをここで記述されたメッセージに置き換えます。HTMLの場合はウイルスが発見された時点でこのメッセージを埋め込みます。メッセージは半角英数(ASCII)のみで指定してください。全角日本語は使用できません。
最大受信サイズを超えた際に置き換えるメッセージ
Data size over!
Get in contact with network administrator.
更新
最大受信サイズを超えたとき、表示されるメッセージです。全角日本語が使用できます。
なお、最大受信サイズは[詳細設定]で設定できます。
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
Virus Infection history matched!
This file has infected with computer virus until quite r
更新
すでにウイルスを検出したURLの履歴と一致したときに表示されるメッセージです。全角日本語が使用できます。
©GIDEON Corp.

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

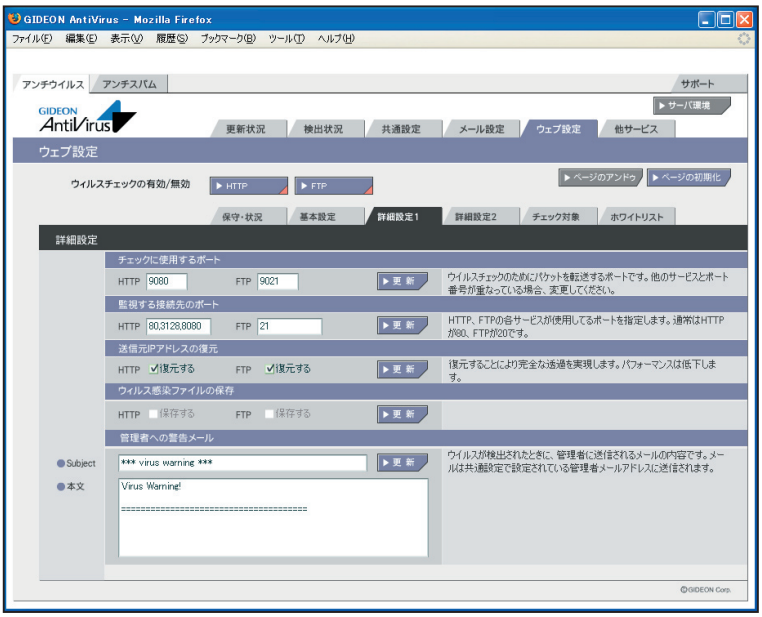
BLOC を通すとBLOCが使用しているIPアドレスを送信元とし、通信パケットを送信します。送信も元のIPアドレスをBLOCを通過する前の元アドレスに変換する機能を実現する場合にはこのモードを有効にします。
復元することにより完全な透過を実現しますが、パフォーマンスは低下します。
HTTP でこの機能を有効もしくは、無効にするには、[復元する]ボタンをクリックしてチェックマークが付けば有効化され、無印であれば無効化されます。

● 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。
初期設定値：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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
サーバ環境
GIDEON AntiVirus
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
ウィルスチェックの有効/無効
HTTP
FTP
ページのアンドウ
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
チェック対象
ホワイトリスト
詳細設定
チェックに使用するポート
HTTP 9080
FTP 9021
更新
ウイルスチェックのために パケットを転送するポートです。他のサービスとポート番号が重なっている場合、変更してください。
監視する接続先のポート
HTTP 80,3128,8080
FTP 21
更新
HTTP、FTPの各サービスが使用してるポートを指定します。通常はHTTPが80、FTPが20です。
送信元IPアドレスの復元
HTTP 復元する
FTP 復元する
更新
復元することにより完全な透過を実現します。パフォーマンスは低下します。
ウィルス感染ファイルの保存
HTTP 保存する
FTP 保存する
更新
管理者への警告メール
Subject
*** virus warning ***
更新
ウイルスが検出されたときに、管理者に送信されるメールの内容です。メールは共通設定で設定されている管理者メールアドレスに送信されます。
本文
Virus Warning!
==========
©GIDEON Corp.

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。
初期設定値 : HTTP『通過』

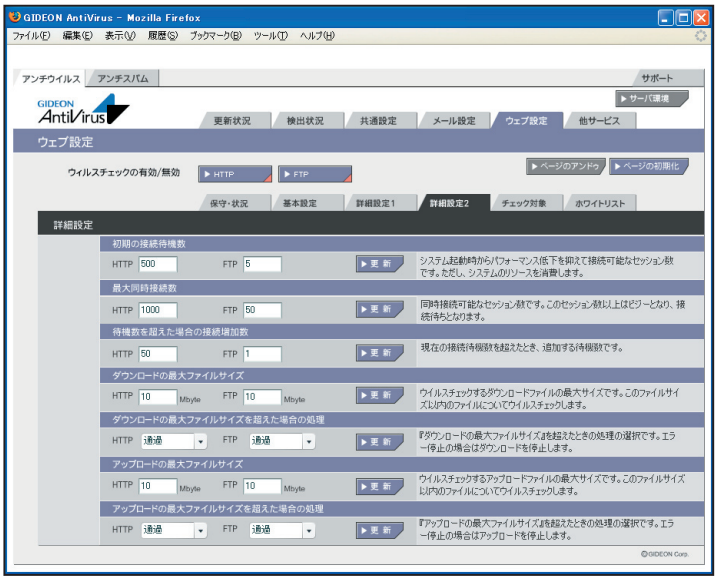
● アップロードの最大ファイルサイズ

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』



画面3.5.4

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初期設定値：

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

画面3.5.5

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

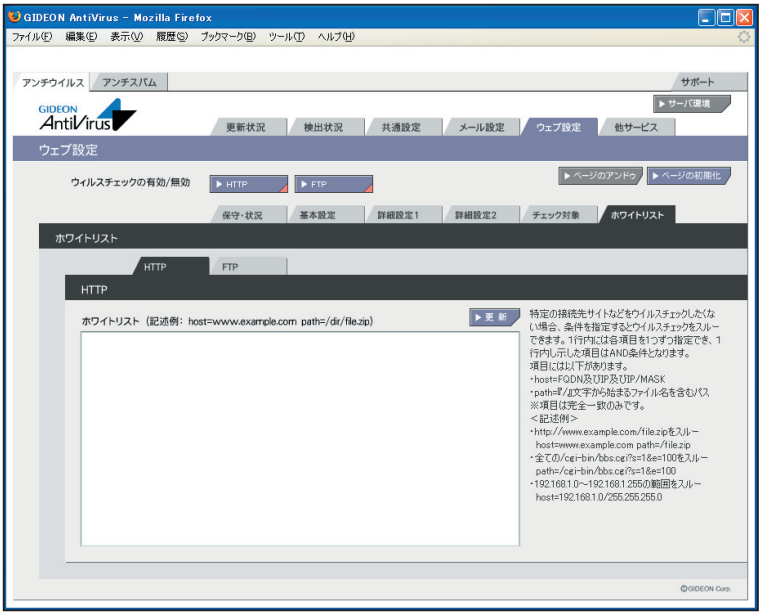
ホストリストの書式は以下の通りです。一行内に項目のどちらか一項目もしくはAND 条件の場合は両項目が記述できます。

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



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。

数値	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
6	スキャン結果不明 （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 （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。

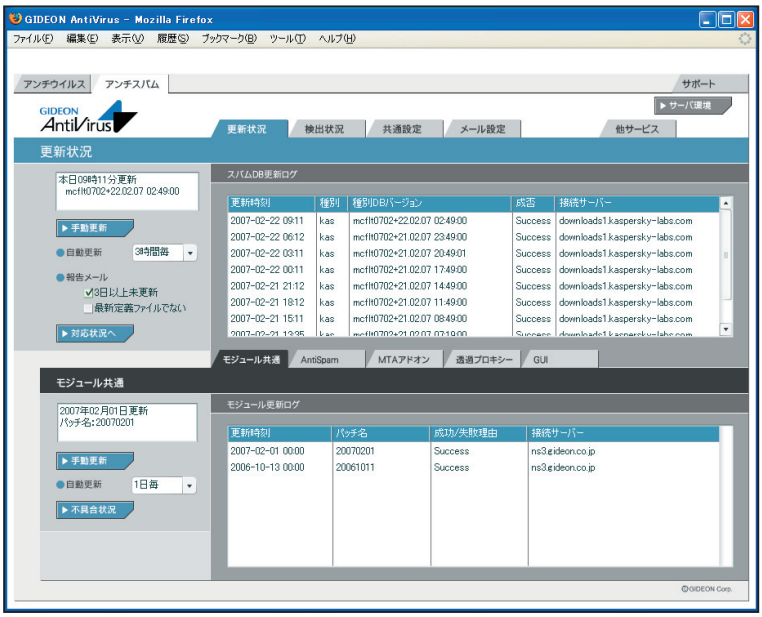
「報告メール」は、スパムDB の更新状況をメールでお知らせするものです。
「3 日以上未更新」は、3 日以上スパムDB の更新がない場合に管理者宛にメール送信します。
「最新定義ファイルでない」は、システム上のスパムDB が最新でない場合に管理者宛にメール送信します。

［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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
▶サーバ環境
GIDEON AntiVirus
更新状況
検出状況
共通設定
メール設定
他サービス
更新状況
本日09時11分更新
mcfit0702+22.02.07 02:49:00
▶手動更新
自動更新
3時間毎
報告メール
3日以上未更新
最新定義ファイルでない
▶対応状況へ
スパムDB更新ログ
更新時刻
種別
種別DBバージョン
成否
接続サーバー
2007-02-22 09:11 kas mcfit0702+22.02.07 02:49:00 Success downloads1.kaspersky-labs.com
2007-02-22 06:12 kas mcfit0702+21.02.07 23:49:00 Success downloads1.kaspersky-labs.com
2007-02-22 03:11 kas mcfit0702+21.02.07 20:49:01 Success downloads1.kaspersky-labs.com
2007-02-22 00:11 kas mcfit0702+21.02.07 17:49:00 Success downloads1.kaspersky-labs.com
2007-02-21 21:12 kas mcfit0702+21.02.07 14:49:00 Success downloads1.kaspersky-labs.com
2007-02-21 18:12 kas mcfit0702+21.02.07 11:49:00 Success downloads1.kaspersky-labs.com
2007-02-21 15:11 kas mcfit0702+21.02.07 08:49:00 Success downloads1.kaspersky-labs.com
モジュール共通
AntiSpam
MTAアドオン
透過プロキシー
GUI
モジュール共通
2007年02月01日更新
パッチ名:20070201
▶手動更新
自動更新
1日毎
▶不具合状況
モジュール更新ログ
更新時刻
パッチ名
成功/失敗理由
接続サーバー
2007-02-01 00:00 20070201 Success ns3.gideon.co.jp
2006-10-13 00:00 20061011 Success ns3.gideon.co.jp
©GIDEON Corp.

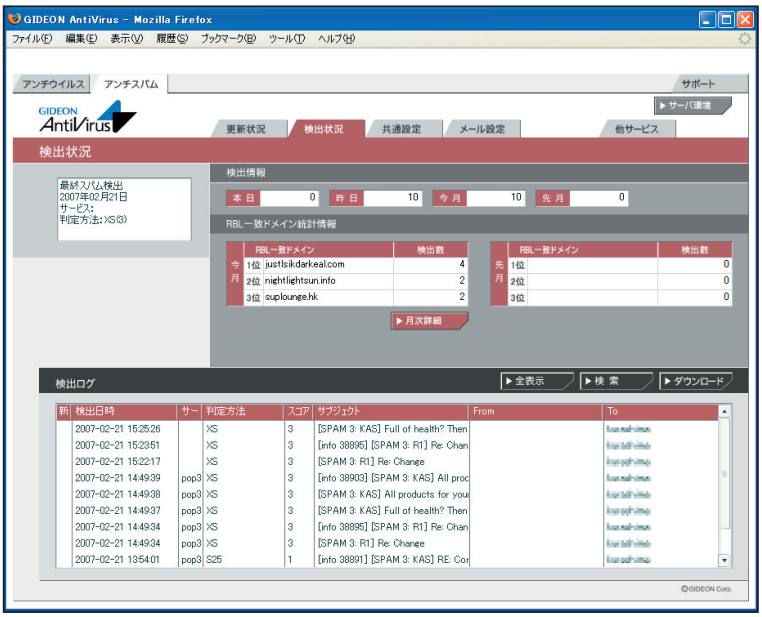
画面 4.1

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。



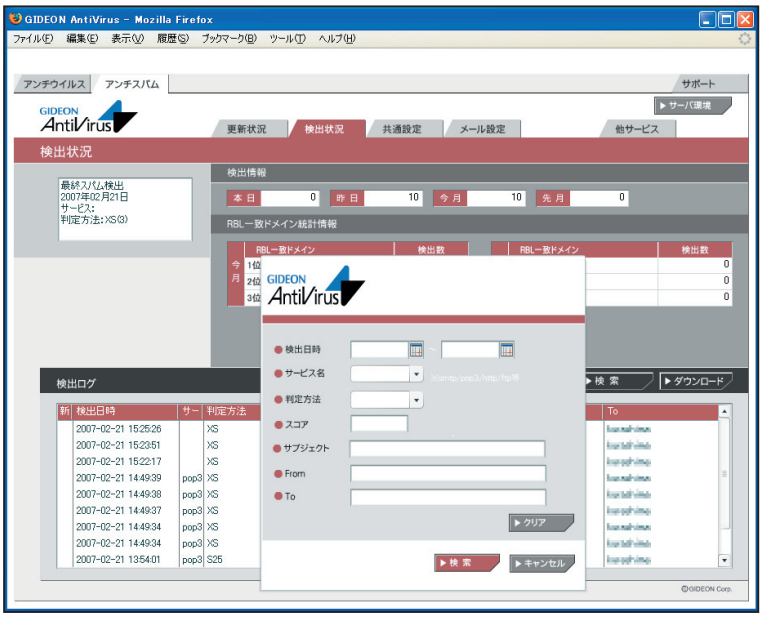
画面 4.2-1

● 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。

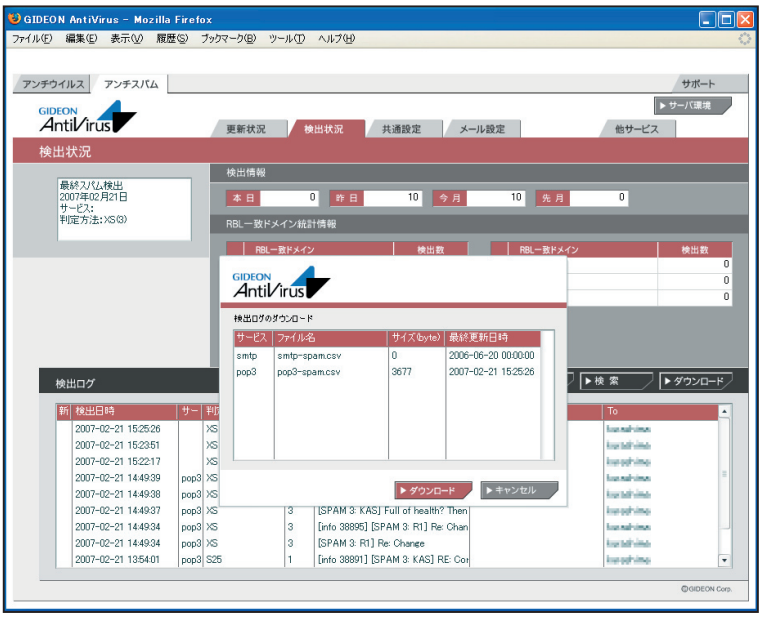


画面 4.2-2

● 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。

画面 4.3

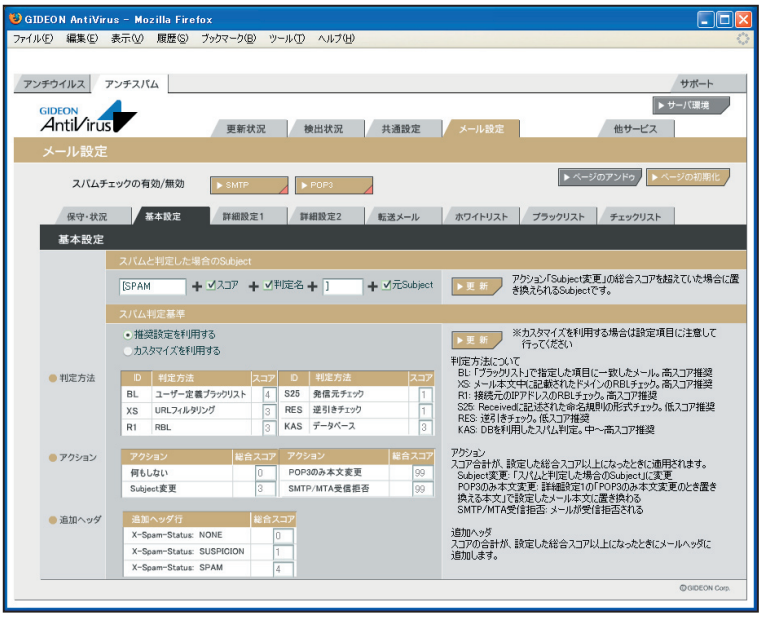
4.4 メール設定

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。



画面 4.4.2

● 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

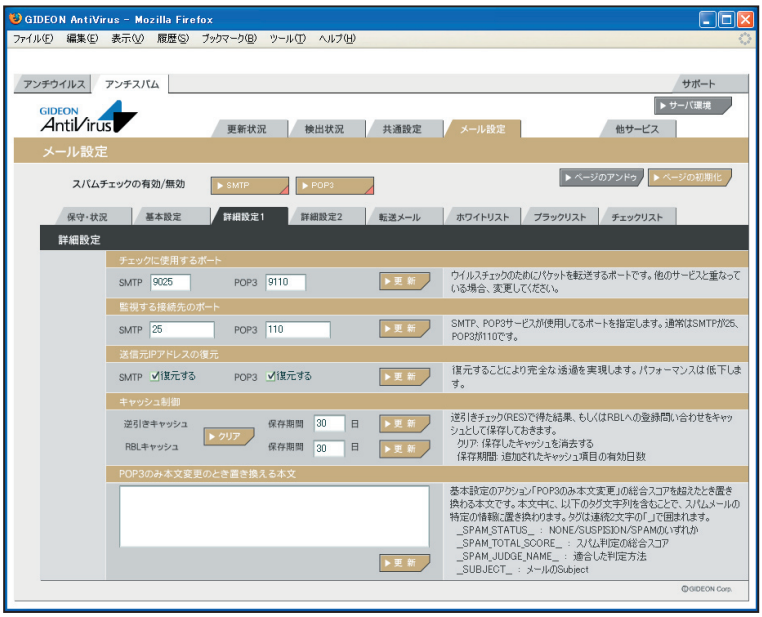
● キャッシュ制御

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)


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
サーバ環境
GIDEON 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
詳細設定
チェックに使用するポート
SMTP 9025
POP3 9110
更新
ウイルスチェックのためにパケットを転送するポートです。他のサービスと重なっている場合、変更してください。
監視する接続先のポート
SMTP 25
POP3 110
更新
SMTP、POP3サービスが使用してるポートを指定します。通常はSMTPが25、POP3が110です。
送信元IPアドレスの復元
SMTP 復元する
POP3 復元する
更新
復元することにより完全な 透過を実現します。パフォーマンスは 低下します。
キャッシュ制御
逆引きキャッシュ
RBLキャッシュ
クリア
保存期間 30 日
保存期間 30 日
更新
更新
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: 保存したキャッシュを消去する
保存期間 追加されたキャッシュ項目の有効日数
POP3のみ本文変更のとき置き換える本文
更新
基本設定のアクション「POP3のみ本文変更」の総合スコアを超えたとき置き換わる本文です。本文中に、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。タグは連続2文字の「_」で囲まれます。
_SPAM_STATUS_ : NONE/SUSPISION/SPAMのいずれか
_SPAM_TOTAL_SCORE_ : スパム判定の総合スコア
_SPAM_JUDGE_NAME_ : 適合した判定方法
SUBJECT : メールのSubject
GIDEON Corp.

画面 4.4.3

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**

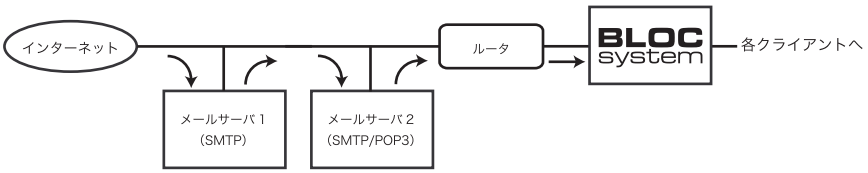
上記3項目はアンチウイルスの設定と共通です。

● **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。

-----例-----



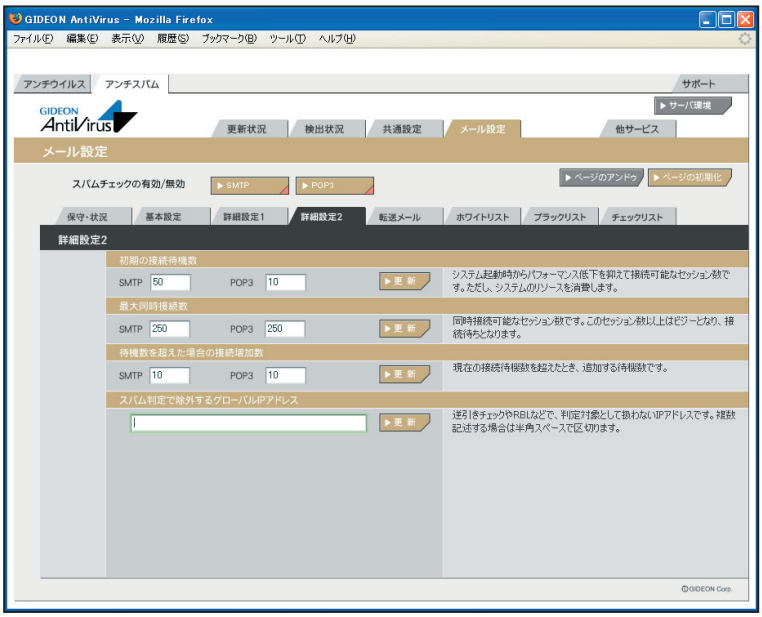
上記の経路で外部からのメールを受信し、自社内部リレーメールサーバの後ろにBLOCを導入した場合を例にとります。

- 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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
サーバ環境
GIDEON 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
詳細設定2
初期の接続待機数
SMTP 50 POP3 10
更新
システム起動時からパフォーマンス低下を抑えて接続可能なセッション数です。ただし、システムのリソースを消費します。
最大同時接続数
SMTP 250 POP3 250
更新
同時接続可能なセッション数です。このセッション数以上はビジーとなり、接続待ちとなります。
待機数を超えた場合の接続増加数
SMTP 10 POP3 10
更新
現在の接続待機数を超えたとき、追加する待機数です。
スパム判定で除外するグローバルIPアドレス
更新
逆引きチェックやRBLなどで、判定対象として扱わないIPアドレスです。複数記述する場合は半角スペースで区切ります。
©GIDEON Corp.

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-----

@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

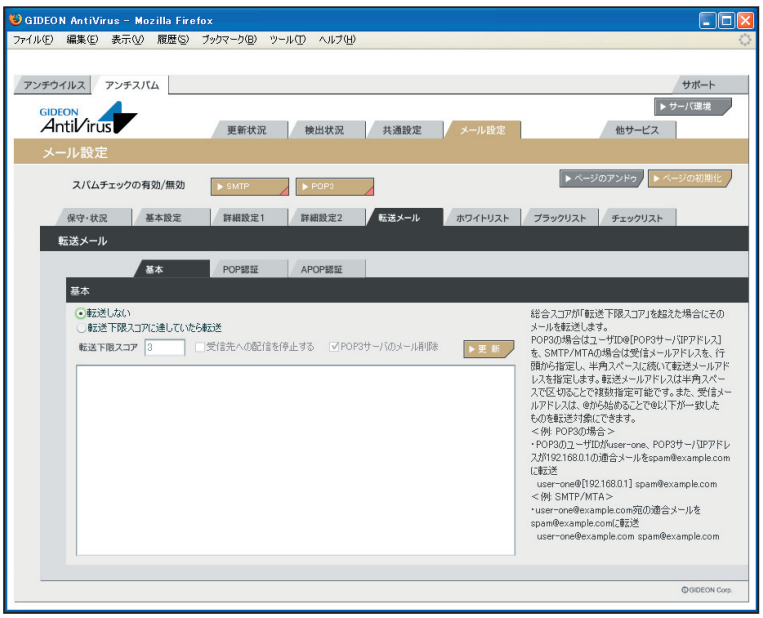
「自動的にユーザリストを追加する」にチェックを入れると、クライアントPC からPOP3 で接続したユーザ情報を自動的に取得します。

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



画面 4.4.5.3

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

● 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-----

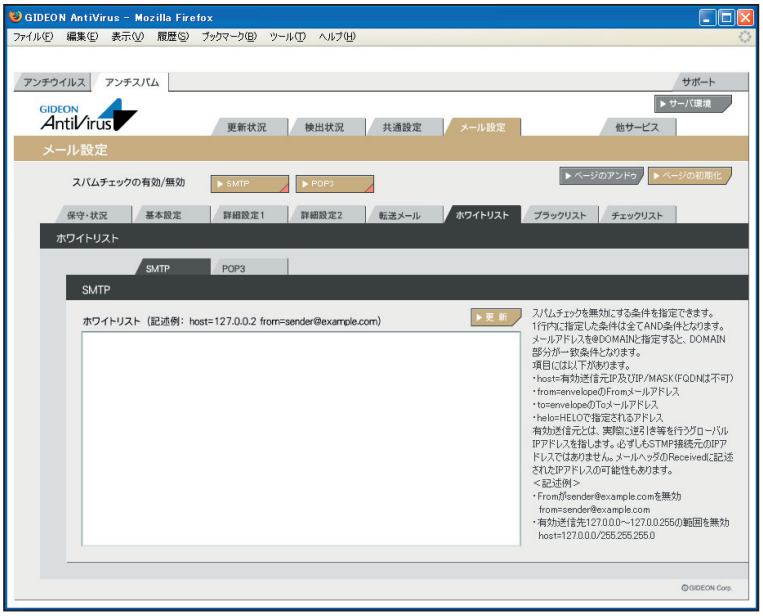
送信元sender@example.com から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

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



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

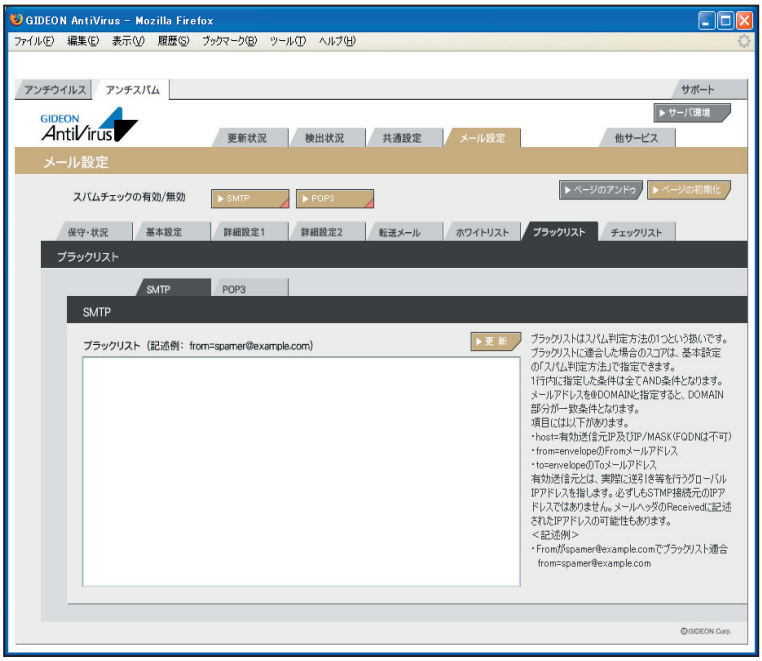
● POP3

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。



画面 4.4.7

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

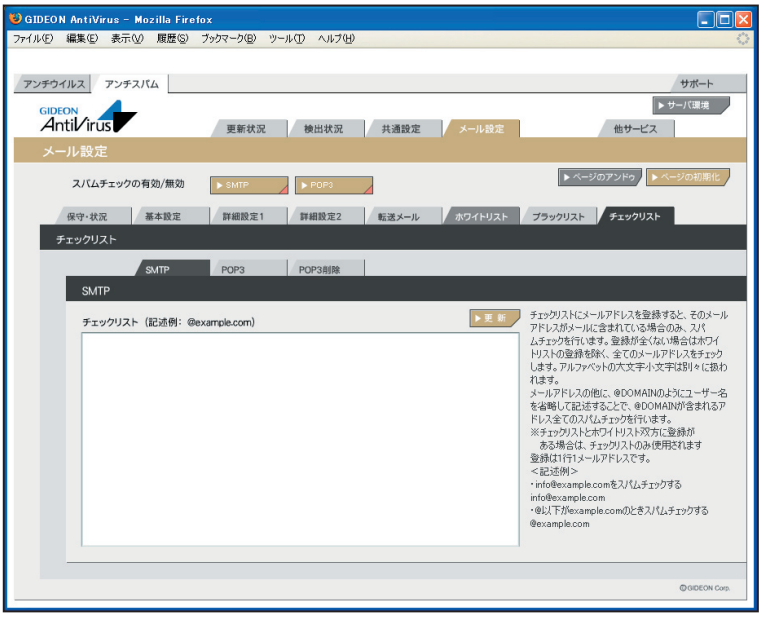
特定のアドレスのみスパム判定をする場合に、そのメールアドレスを登録します。登録が全くない場合にはホワイトリストの登録を除き、すべてのメールアドレスをチェックします。
個別のメールアドレスの入力や、@DOMEIN のようにドメインごとに設定をすることができます。

● 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。



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)へメールを保存します。
・メールの他に、そのメールに関連する属性情報(暗号化の有無、添付ファイルの有無など)を記述されたファイルも保存します。
・オプションにより、メール内容を暗号化します。

検索用のインデックスの作成

・本日のメールデータのインデックスを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/sda1)が使われます。外部のメールアーカイブしているボリュームがSCSIインタフェースの場合、/dev/sdb1 などと表示されます。実際にマウントしたデ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(MByte)を表示します。

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

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

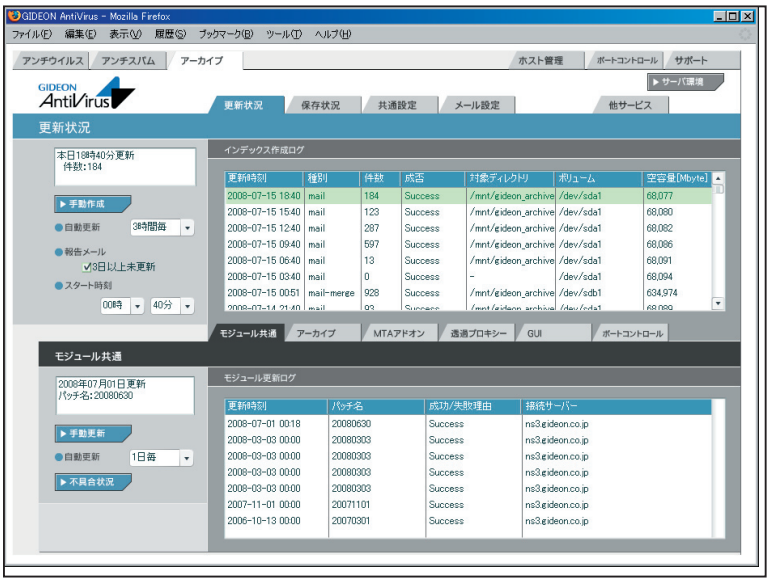
手動更新、自動更新を行っている最中はデータ検索ができません。
インデックス作成に要する時間は件数の増分に比例します。

● モジュール更新ログ

各モジュールの更新状況を表示します。モジュールとは、アーカイブが動作するために必要な実行ファイルやスクリプト、またはそれらが参照するファイルを指します。
初期設定では1日1回の自動更新に設定されています。緊急対策が必要な場合は[手動更新]ボタンをクリックし、最新のモジュールを取得してください。
既に更新済みの場合は、新たに更新されません。

［不具合状況］ボタンをクリックすると、モジュールの不具合などに関する情報サイトを表示します。
各タブ（AntiSpam、透過プロキシー、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。



画面 5.2

5.3 保存状況

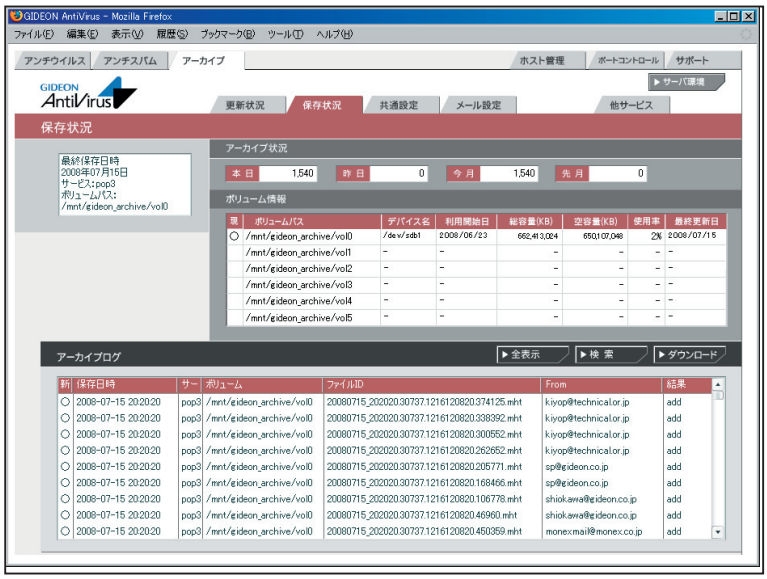
アーカイブ設定画面の「保存状況」タブをクリックすると画面5.3-1が表示されます。
メールをアーカイブした履歴や統計情報などを閲覧できます。

● 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○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。



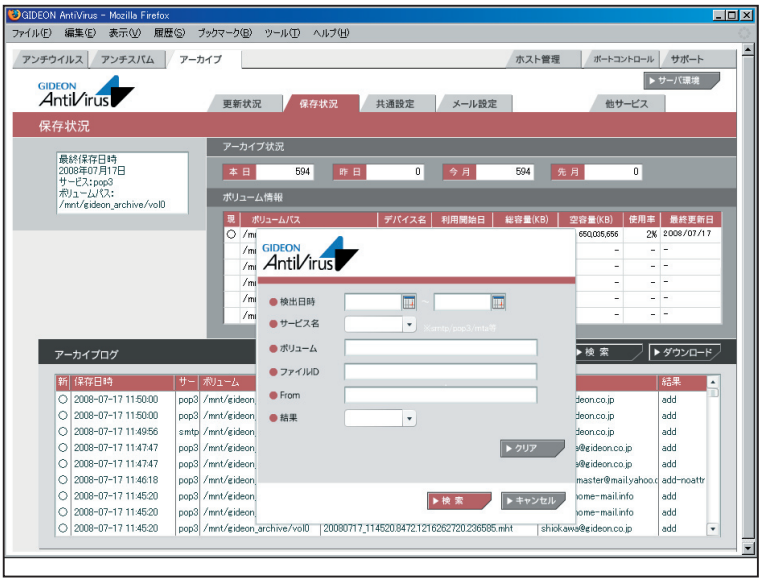
画面 5.3-1

● アーカイブログ

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

新	：初めて表示するリストの場合は○印を表示します。
保存日時	：メールデータをアーカイブした日時を表示します。
サービス	：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。



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。

画面 5.4

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"、" 無効"、" 管理者" の3種類から選択します。
" 有効" を選択すると、各々のアカウントで登録したサーチID のメールを検索することができます。
" 無効" を指定すると一切検索できなくなります。
" 管理者" を指定するとすべてのメールを検索できます。
" 管理者" の場合はサーチID リスト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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
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
サーバ環境
GIDEON AntiVirus
更新状況
保存状況
共通設定
メール設定
他サービス
メール設定
アーカイブの有効/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
アカウント
グループ
アカウント管理
アカウントリスト
属性
アカウント
サーチIDリスト
kataoka
kataoka@gideon.co.jp
kitazawa
kitazawa@gideon.co.jp
mitz
mitz@gideon.co.jp
nishio
noguchi
noguchi@gideon.co.jp
okita
okita@gideon.co.jp
shiokawa
shiokawa@gideon.co.jp
shioya
shioya@gideon.co.jp
※変更するには項目をクリックする
追 加
アカウントリストについて
アカウントリストにアカウント登録することで、
アーカイブされたメールを参照することができます。
項目の意味は以下の通り。
属性：属性は以下の3種
★ 管理者(全てのメール参照可)
○ 有効(自メール、自グループのメール参照可)
× 無効(メールの参照不可)
アカウント：アカウント名
通常はメールアドレスとなる。
サーチIDリスト：
そのアカウントが参照できるメールのアドレス
(空白区切りで複数登録可)
登録例
test@example.comアカウントの登録例
例1)
属性：有効
アカウント：test@example.com
サーチID：test@example.com test2@example.com
例2)
属性：管理者
アカウント：test@example.com
サーチID：なし
※管理者の場合、サーチIDの登録は必要ありません。

画面 5.4.3

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

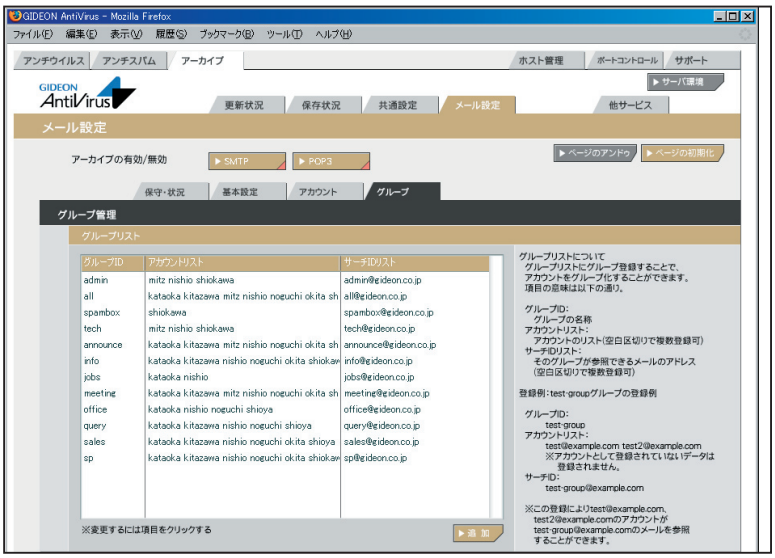
名称を"sales" とすると、
「グループID」　は"sales"とし、「アカウントリスト」には、利用アカウントを
salesA@domain.co.jp salesB@domain.co.jp salesC@domain.co.jp のように登録します。「サーチIDリスト」はsales@domain.co.jp とすることで、"sales" グループは
salesA、selesB、salesC の登録アカウントすべてで検索できます。
同様に、部課単位に定義すると課別のアカウントをまとめて部の検索も可能になります。
個々の組織内部統制ルールに従って、メール検索範囲をグループ化することで可能になります。
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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
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
GIDEON AntiVirus
サーバ環境
更新状況
保存状況
共通設定
メール設定
他サービス
メール設定
アーカイブの有効/無効
SMTP
POP3
ページのアンドウ
ページの初期化
保守・状況
基本設定
アカウント
グループ
グループ管理
グループリスト
グループID
アカウントリスト
サーチIDリスト
admin
mitz nishio shiokawa
admin@gideon.co.jp
all
kataoka kitazawa mitz nishio noguchi okita sh
all@gideon.co.jp
spambox
shiokawa
spambox@gideon.co.jp
tech
mitz nishio shiokawa
tech@gideon.co.jp
announce
kataoka kitazawa mitz nishio noguchi okita sh
announce@gideon.co.jp
info
kataoka kitazawa nishio noguchi okita shiok
info@gideon.co.jp
jobs
kataoka nishio
jobs@gideon.co.jp
meeting
kataoka kitazawa mitz nishio noguchi okita sh
meeting@gideon.co.jp
office
kataoka nishio noguchi shioya
office@gideon.co.jp
query
kataoka kitazawa nishio noguchi shioya
query@gideon.co.jp
sales
kataoka kitazawa nishio noguchi okita shioya
sales@gideon.co.jp
sp
kataoka kitazawa nishio noguchi okita shiok
sp@gideon.co.jp
※変更するには項目をクリックする
追 加
グループリストについて
グループリストにグループ登録することで、
アカウントをグループ化することができます。
項目の意味は以下の通り。
グループID:
グループの名称
アカウントリスト:
アカウントのリスト(空白区切りで複数登録可)
サーチIDリスト:
そのグループが参照できるメールのアドレス
(空白区切りで複数登録可)
登録例:test-groupグループの登録例
グループID:
test-group
アカウントリスト:
test@example.com test2@example.com
※アカウントとして登録されていないデータは
登録されません。
サーチID:
test-group@example.com
※この登録によりtest@example.com、
test2@example.comのアカウントが
test-group@example.comのメールを参照
することができます。

画面 5.5.4

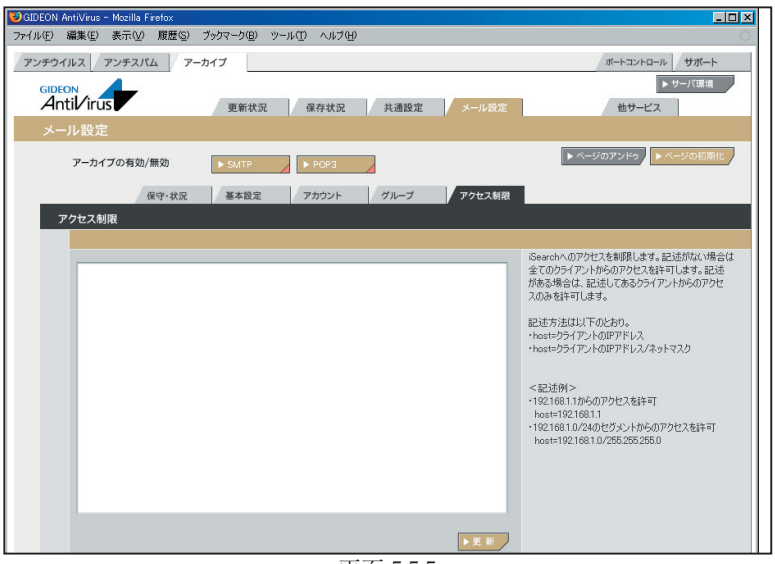
5.5.5 アクセス制限

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。



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。

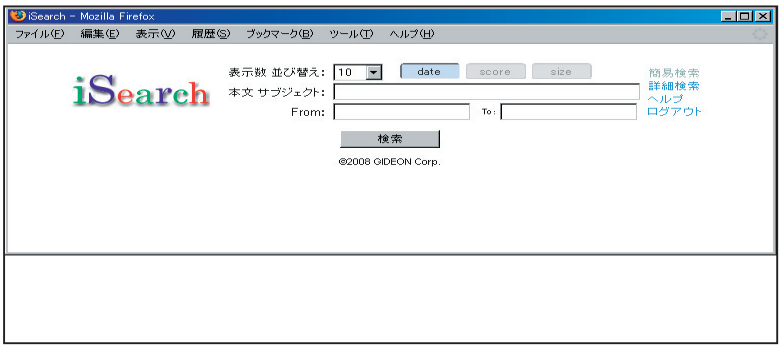
画面 5.6.1

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。
To	：To に含まれる文字列を検索します。複数キーワードを指定することはできません。

転送の対象となるメールアドレス（例：user-one@example.com）を行頭から指定し、半角スペースに続いて転送先メールアドレス（例：spam-admin@example.com）を指定します。
転送先メールアドレスは半角スペースで区切ることで複数指定可能です。
また、転送対象のメールアドレスは、@ から始めることで、ドメインが一致するメールアドレスをすべて転送対象にすることができます。
@example.com spam-admin@example.com



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

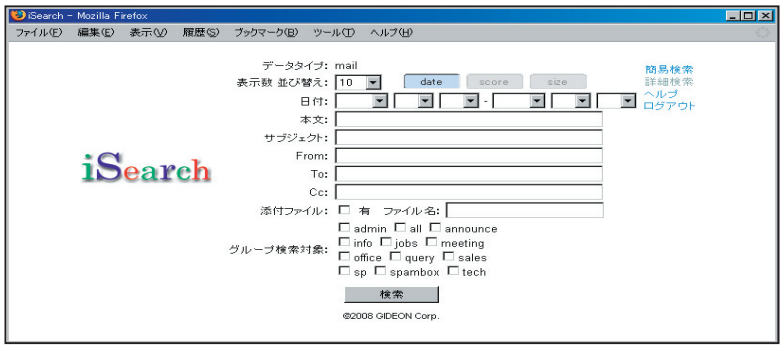
・グループにチェックが入っていない場合は、

「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。



画面 5.6.3-1

● 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

画面 5.6.3-2

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

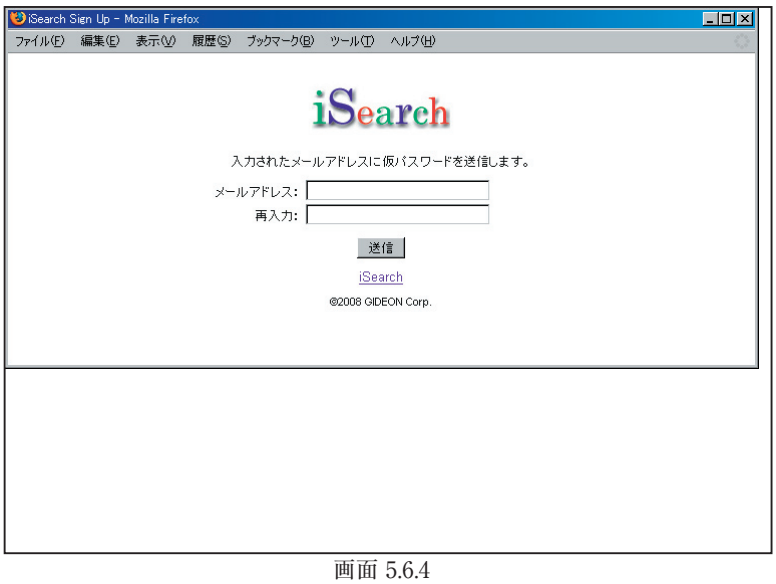
---

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(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)
iSearch
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 5.6.4

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。

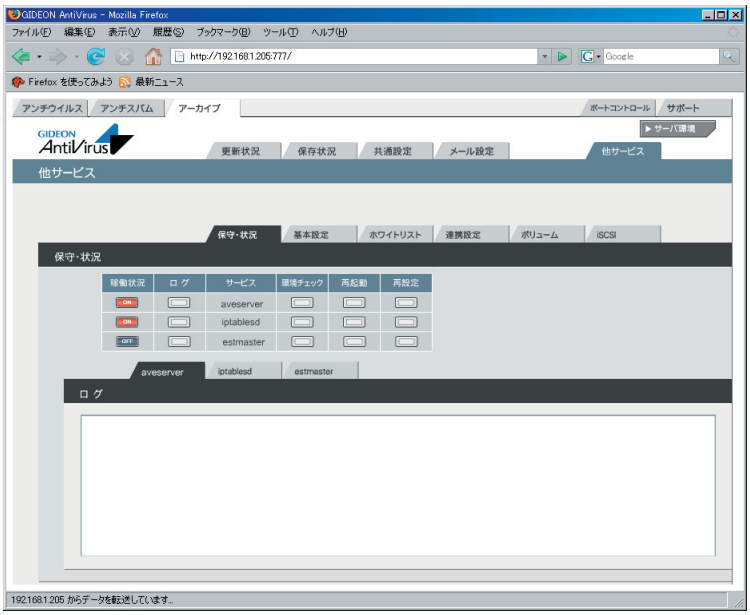
ホワイトリスト：サーバのIPアドレスもしくはサーバのIPアドレスとポート番号を指定することで、指定に一致したサーバをウイルスチェックから完全に除外することができます。
メール設定やウェブ設定のホワイトリストはHTTP/SMTPなどのプロトコルを監視しながらチェックのみ行わないという方法ですが、本項目のホワイトリストの場合は監視そのものも行いません。

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


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
http://192.168.1.205:777/
Firefox を使ってみよう 最新ニュース
アンチウイルス
アンチスパム
アーカイブ
ポートコントロール
サポート
サーバ環境
GIDEON AntiVirus
更新状況
保存状況
共通設定
メール設定
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
ボリューム
iSCSI
保守・状況
稼働状況
ログ
サービス
環境チェック
再起動
再設定
ON
aveserver
ON
iptablesd
OFF
estmaster
aveserver
iptablesd
estmaster
ログ
192.168.1.205 からデータを転送しています...

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

画面6.1.3

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さい。

[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さい。

[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。

画面6.2

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/sda1 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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
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
GIDEON AntiVirus
サーバ環境
更新状況
保存状況
共通設定
メール設定
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
ボリューム
iSCSI
ボリューム
マウントするボリューム
使用中のボリューム
初期ボリューム
ボリュームローテーション有効
ファイルシステム
デバイス名
利用開始日
使用率
ON
初期ボリューム
ext3
/dev/sdb1
2008/06/23
2%
OFF
追加ボリューム1
追加ボリューム2
追加ボリューム3
追加ボリューム4
追加ボリューム5
更 新
ボリュームについて
ここではアーカイブを保存するボリュームの設定を行います。登録項目は以下の通り。
ボリュームローテーション有効:
ボリュームローテーションを有効にすると、すべてのディスクがいっぱいになったときに古いデータが削除されボリュームがローテーションします。
ファイルシステム:
vfat,ext3に対応しています。
デバイス名:
デバイス名を指定します。
例)
/dev/sda1
利用開始日:
利用開始日にそのボリュームを利用開始します。 ボリュームローテーションを有効にしている場合は、利用開始日は無視されます。

画面6.3

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。

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。

画面6.4-2

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）

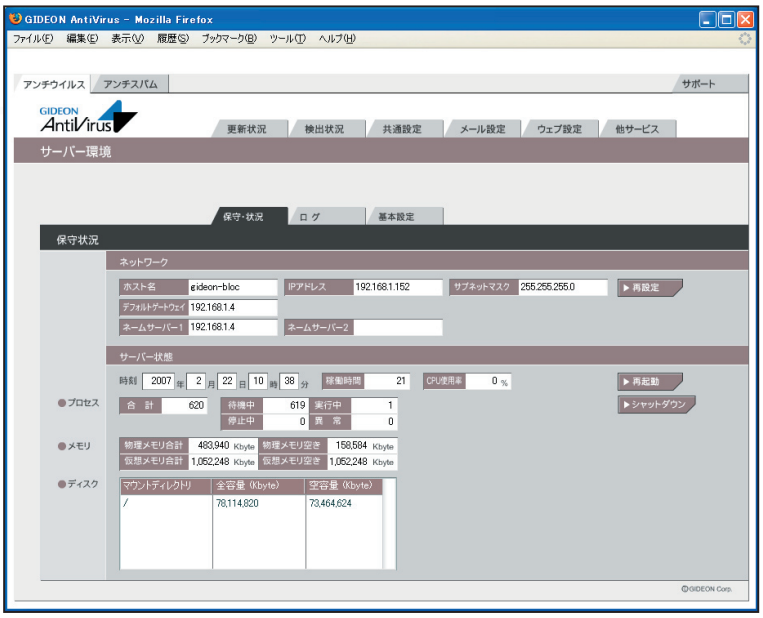
DHCPからIPアドレス取得する場合、IPアドレス、サブネットマスク、デフォルトゲートウェイ、ネームサーバ情報を自動取得します。
DHCPクラインアント接続ではなく、個別にIPアドレスを設定した場合、その設定情報が表示されます。

● 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。

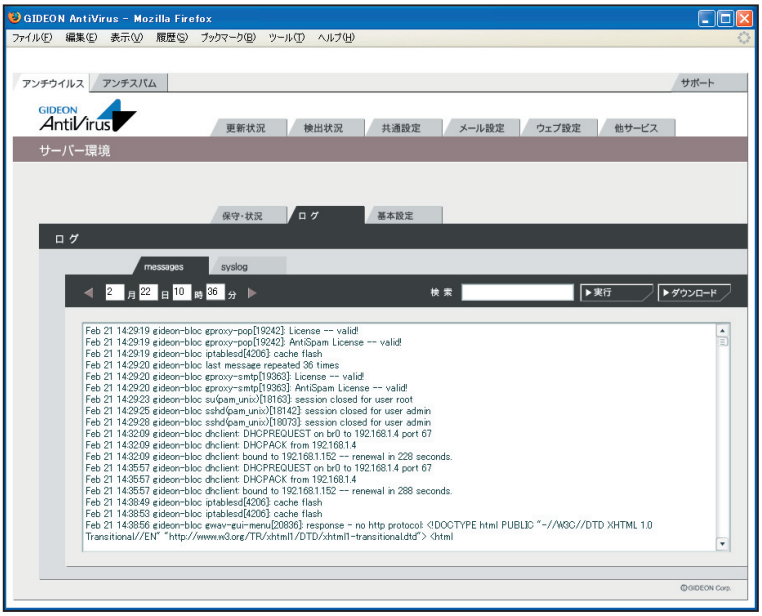
［シャットダウン］ボタンをクリックすると、BLOCのサービスを停止し、電源を切ります。
※サーバ情報は、自動的に更新表示されません。新しい情報を閲覧したい場合は、どこか別のタブを一旦クリックしてから再度この画面に戻る必要があります。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
GIDEON AntiVirus
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
サーバー環境
保守・状況
ログ
基本設定
保守状況
ネットワーク
ホスト名
gideon-bloc
IPアドレス
192.168.1.152
サブネットマスク
255.255.255.0
再設定
デフォルトゲートウェイ
192.168.1.4
ネームサーバー1
192.168.1.4
ネームサーバー2
サーバー状態
時刻
2007 年 2 月 22 日 10 時 38 分
稼働時間
21
CPU使用率
0 %
再起動
シャットダウン
プロセス
合 計
620
待機中
619
実行中
1
停止中
0
異 常
0
メモリ
物理メモリ合計
483,940 Kbyte
物理メモリ空き
158,584 Kbyte
仮想メモリ合計
1,052,248 Kbyte
仮想メモリ空き
1,052,248 Kbyte
ディスク
マウントディレクトリ
全容量 (Kbyte)
空容量 (Kbyte)
/
78,114,820
73,464,624
©GIDEON Corp.

画面7.1.1

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。



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。

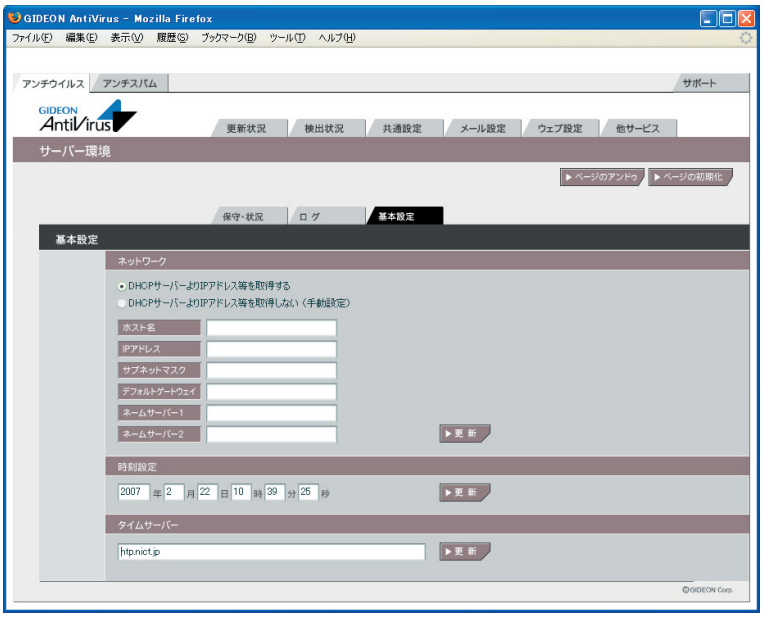
デフォルトゲートウェイは、コンピューターやルーターなどの機器です。所属するネットワークから外部のコンピューターへアクセスする際に使用する「出入口」の代表となります。アクセス先のIPアドレスについて特定のゲートウェイを指定していない場合に、デフォルトゲートウェイに指定されているホストにデータが送信されます。
設定元のBLOCからデフォルトゲートウェイまでは直接アクセスできることが必須です。
入力後、［更新］ボタンをクリックしてください。

● 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 AntiVirus - Mozilla Firefox
ファイル(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)
アンチウイルス
アンチスパム
サポート
GIDEON AntiVirus
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
サーバー環境
▶ページのアンドゥ
▶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
DHCPサーバーよりIPアドレス等を取得する
DHCPサーバーよりIPアドレス等を取得しない（手動設定）
ホスト名
IPアドレス
サブネットマスク
デフォルトゲートウェイ
ネームサーバー1
ネームサーバー2
▶更 新
時刻設定
2007 年 2 月 22 日 10 時 39 分 25 秒
▶更 新
タイムサーバー
ntp.nict.jp
▶更 新
©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。


GIDEON AntiVirus - Mozilla Firefox
ファイル(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)
GIDEON AntiVirus
サポート
メールテスト
サポート接続
メールテスト
受信テスト
受信メール
受信アドレス
メール種別
通常メール
ウイルスメール
スパムメール
プロキシ
外部サーバーへの接続にプロキシを利用しない
外部サーバーへの接続にプロキシを利用する
アドレス
ポート
ユーザーID
パスワード
▶受 信
受信ログ
▶更 新
受信テストを行います。
外部サーバーから「通常メール」または「ウイルスメール」または「スパムメール」を送信し、BLOC経由でメールを受信します。
外部サーバーへはHTTP経由で接続しますのでプロキシの設定が必要な場合があります。
POP3でのテストの場合、ユーザのメーラーでメールを受信後にテスト完了となります。メーラーでメールを受信後に更新ボタンを押してください。
受信が正常に行われた場合には、受信ログの最後に「---ウイルス受信テスト終了---」と表示されます。
転送テスト
転送メール
転送アドレス
▶転 送
転送ログ
本システムから外部のメールサーバにメールが転送可能かどうかのテストを行います。転送は、アンチスパムのメール設定の詳細設定2の転送メール設定や、各警告メール等で利用されます。
転送成功時には転送ログに「転送成功」と表示されます。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。
©GIDEON Corp.

画面8.1

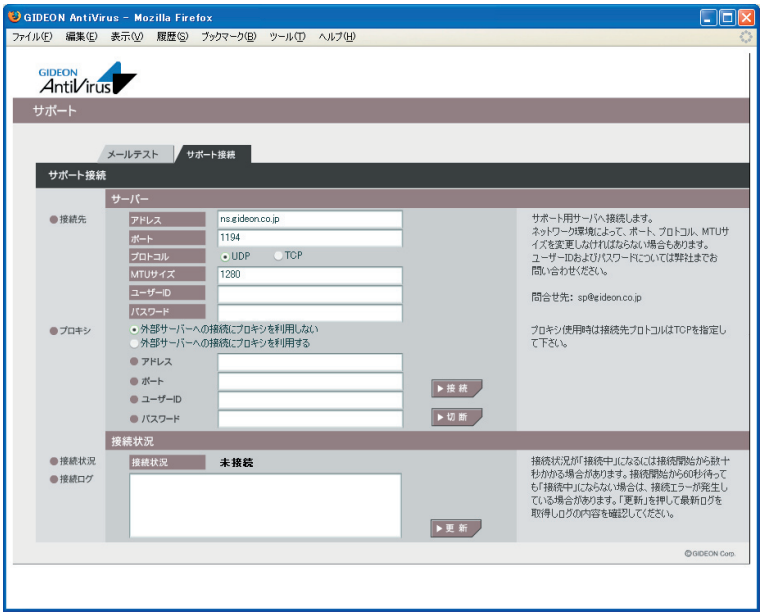
8.2 サポート接続ツール

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。



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。

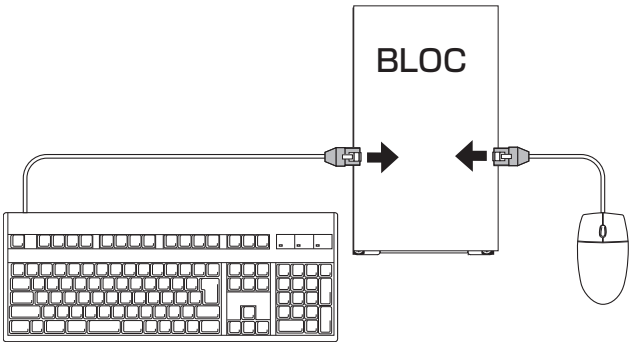


図9.1-1

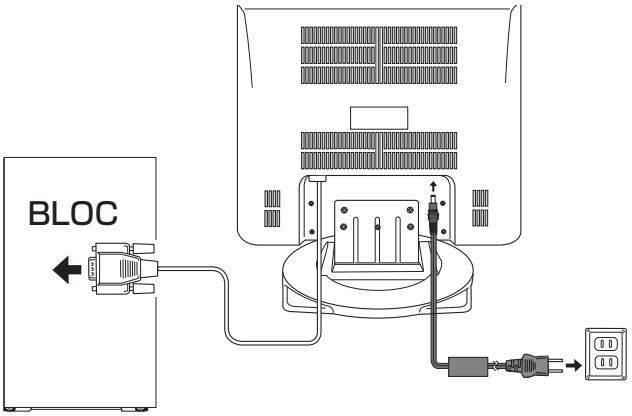


図9.1-2

② 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 -*

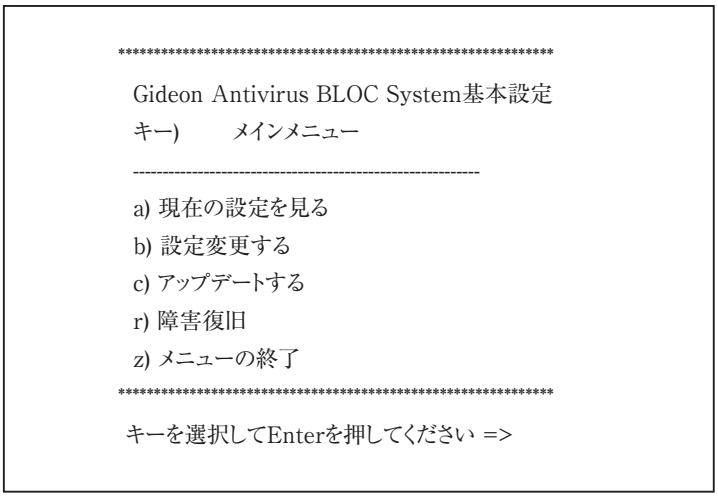
さらに以下のイタリック部分を入力して「Enter」キーを押します。
ただし、入力しても画面には表示されません。

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。



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。

```
**************************************************************
Gideon Antivirus BLOC System基本設定
キー)       サブメインメニュー
------------------------------------------------------------
    ネットワーク:
        a) IP アドレス & デフォルトゲートウェイ
        b) プライマリネームサーバ
        c) BLOCのWAN側にあるHTTPプロキシ
        d) フィルタリング設定の初期化（上級者向け）
        e) スパニングツリープロトコル(STP)の設定
    ユーザ:
        f) 管理者（root）パスワードの変更
        g) リモートログインユーザ（admin）のパスワード変更
        h) GUI 管理画面のログインパスワード変更
    ログインサービス:
        i) ssh サービスの起動・停止
        j) telnet サービスの起動・停止
        k) GUI管理ツールサービスの起動・停止
        l) シリアルコンソールログイン
    起動オプション:
        s) システム起動時の音
m) メインメニュー
z) メニューの終了
**************************************************************
 キーを選択してEnterを押してください =>
```

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_FAILED_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

*1 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

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/