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

2020年 12月1日　　第3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

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/ACアダプター
- 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 BLOCの接続方法について

本章では、BLOC の接続方法および接続確認、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。この場合、POP3でのスパム判定になります。

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。

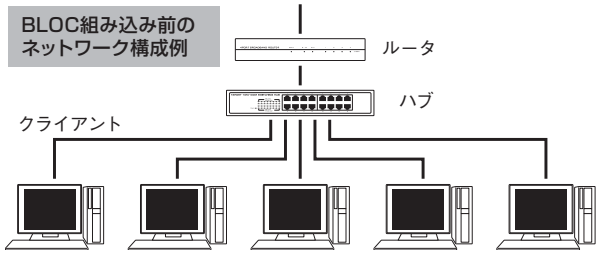


図2.1.1-1

BLOC 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に、必ずPortControl を通過することになります。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、必ず PortControl を経由することができます。

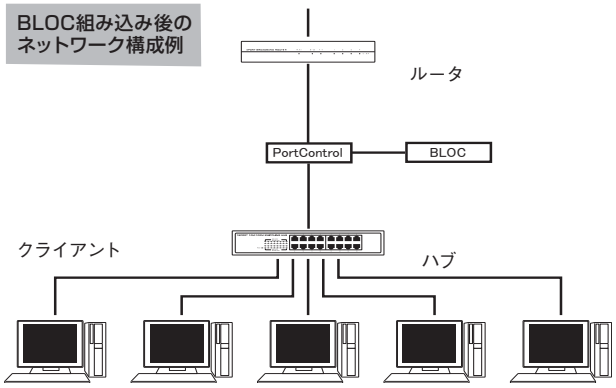


図2.1.1-2

※BLOC の導入によりクライアントからこれまでと同じようにインターネットに接続でき、メールの送受信、ホームページなどの閲覧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。

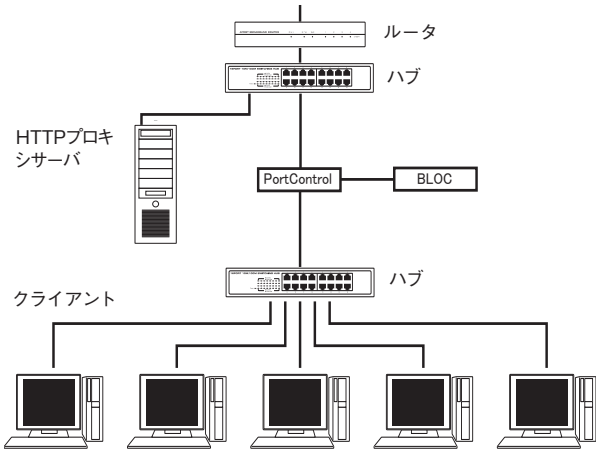


図2.1.2

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。

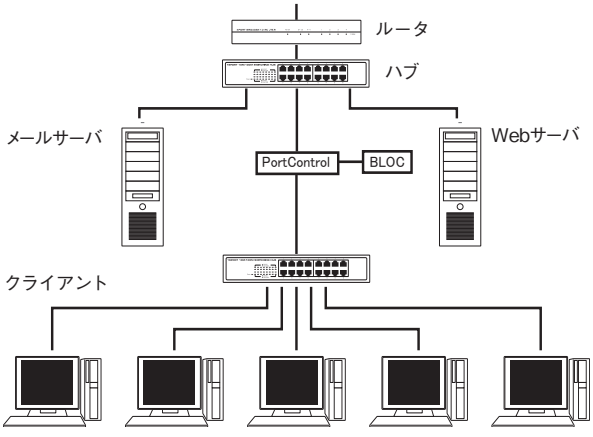
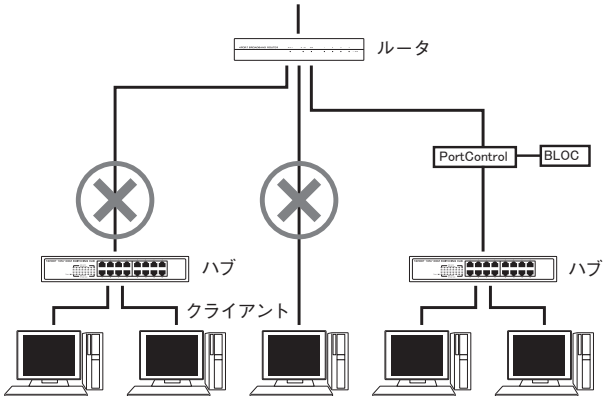


図2.1.3

2.2 BLOCの接続方法についてのご注意

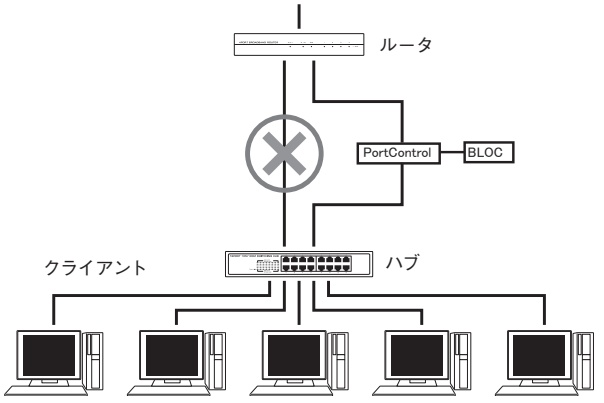
ルータと直結したネットワークの場合

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 の対象外になりますので、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

ルータとハブを下図のように、PortControl 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。



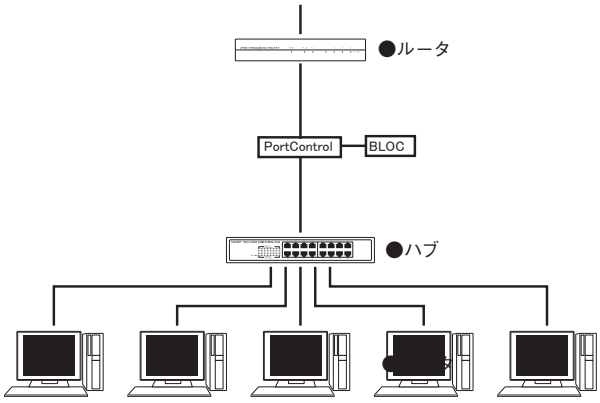
固定IPアドレスを設定している場合

BLOC を接続したときに、BLOC が自動でIP アドレスを取得できている（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。「8.2 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。

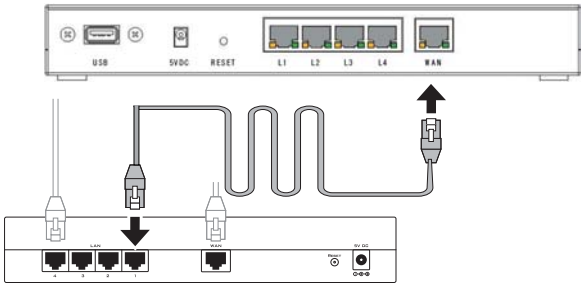
2.3 BLOCの接続とセットアップ

●セットアップに必要なもの　BLOC本体、PortControl、電源コード、ハブ、LANケーブル



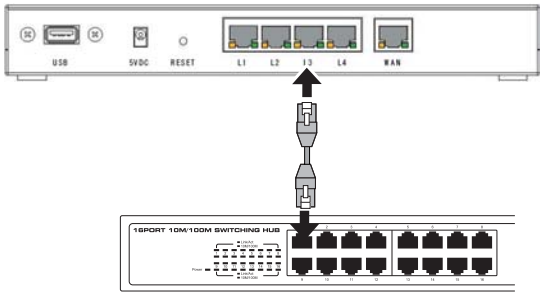
《手順1》　WAN側機器とPortControlの接続

PortControlのWANコネクタとルータなどのWAN側機器のLANコネクタを接続します。
また、WAN側機器とハブを接続しているLANケーブルを取り外します。
この段階で、インターネットとの接続ができなくなります。



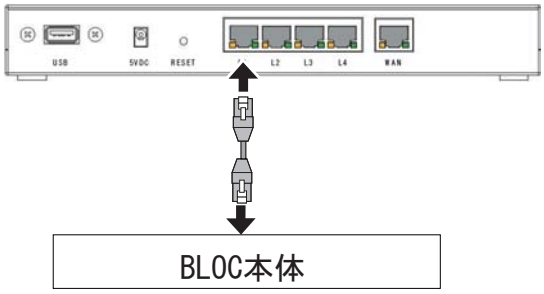
《手順2》 ハブとPortControlの接続

PortControlのL3コネクタとハブのLANコネクタを接続します。



《手順3》 BLOC本体とPortControlの接続

PortControlのL1コネクタとBLOC本体のLANコネクタを接続します。



《手順4》 電源コードの接続

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

《手順5》 電源をON

接続が全て終了したら、BLOCの電源を入れます。
電源がONになるとセットアップを開始します。 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。

2.4 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2.4-1

画面2.4-2

2.5 ログイン

管理･設定画面にアクセスすると、ログイン画面が表示されます。
ライセンス証書に記載され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

画面2.5-1

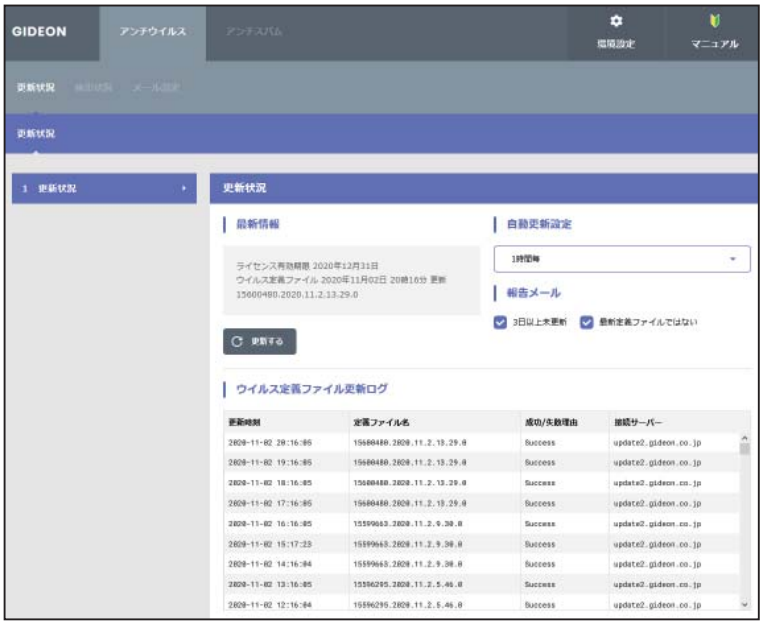
パスワードの変更

既存のパスワードを入力してログイン画面下部の［パスワードを変更］をクリックすると、画面2.7が表示されますので、この画面上でパスワードを再設定します。（半角英数20文字以内）

画面2.5-2

2.6 管理画面について

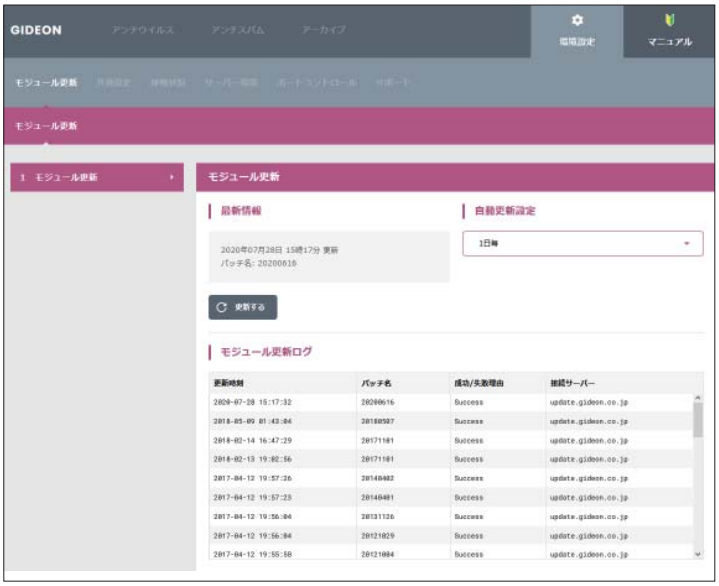
ログインすると、画面2.6が表示されます。管理・設定の方法につきましては後述の章をご参照ください。



画面2.6

3.1 設定画面

ログイン後、画面右上部の[環境設定]タブをクリックすると、図3.1が表示されます。



画面3.1

3.1.1 モジュール更新

環境設定画面の「モジュール更新」タブをクリックすると、画面3.1.1が表示されます。[更新する]ボタンをクリックすると、その時点で最新のモジュール（修正パッチモジュール、アップデートモジュールなど）の取得を行います。既に更新済みの場合は新たに更新されません。

自動更新の頻度は、初期設定では1日1回の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を行ってください。

画面3.1.1

3.1.2 共通設定

環境設定画面の「共通設定」タブをクリックすると、画面3.1.2が表示されます。

画面3.1.2

3.1.2.1 基本設定

●ライセンス

納入時にライセンス証書記載の「お客様登録No」「パスワード」が既に登録されていますので、改めて操作する必要はありません。

画面3.1.2.1-1

●管理者のメールアドレス

管理者のメールアドレスを登録すると、ウイルスの検出時に管理者にも警告メールを送信します。またその他のウイルスに関するレポートなども送信します。

メールアドレスを入力後、［更新する］ボタンをクリックしてください。複数アドレスを指定する場合は、下記のように半角スペースで区切ります。

```
aaa@domain.jp bbb@domain.jp
```

※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。

画面3.1.2.1-2

●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、［更新する］ボタンをクリックしてください。

画面3.1.2.1-3

●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、［更新する］ボタンをクリックしてください。

画面3.1.2.1-4

●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。

変更する場合は入力後、[更新する] ボタンをクリックしてください。

画面3.1.2.1-5

3.1.2.2 更新環境

共通設定画面の「更新環境」タブをクリックすると、画面3.1.2.2が表示されます。
本製品は外部HTTPサイトにアクセスすることで、モジュールおよび定義ファイルを更新します。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、[更新する] ボタンをクリックしてください。

画面3.1.2.2

3.1.2.3 サーバーホワイトリスト

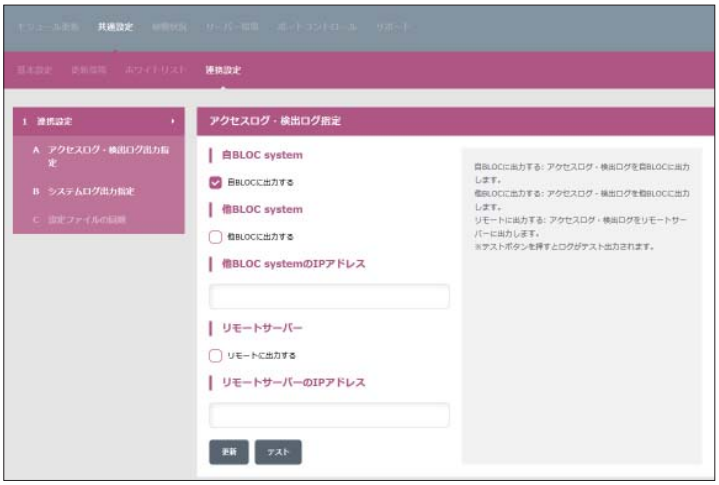
共通設定画面の「ホワイトリスト」タブをクリックすると、画面3.1.2.3が表示されます。
サーバのIPアドレス、またはIPアドレスとポート番号を指定することでアンチウイルス、アンチスパムの対象から除外します。チェック対象から除外することで、パフォーマンスの低下やトラブルを回避することが可能です。

記述方法は、
host=接続先のIPアドレス
port=ポート番号
入力後、[更新する] ボタンをクリックしてください。

画面3.1.2.3

3.1.2.4 連携設定

共通設定画面の「連携設定」タブをクリックすると、画面3.1.2.4が表示されます。
ネットワーク内にある他のBLOC systemとの連携(ログの転送、設定の動機)やログの転送やリモートサーバへのログ転送の設定を行います。



画面3.1.2.4

●アクセスログ･検出ログ指定

自BLOCに出力する:　　アクセスログ･検出ログを自BLOCに出力します。
他BLOCに出力する:　　アクセスログ･検出ログを他BLOCに出力します。
リモートに出力する:　　アクセスログ･検出ログをリモートサーバーに出力します。
入力後、[更新する] ボタンをクリックしてください。
※テストボタンを押すとログがテスト出力されます

画面3.1.2.4-1

●システムログ出力指定

自BLOCに出力する:　　システムログを自BLOCに出力します。
他BLOCに出力する:　　システムログを他BLOCに出力します。
リモートに出力する:　　システムログをリモートサーバーに出力します。
入力後、[更新する] ボタンをクリックしてください。
※テストボタンを押すとログがテスト出力されます

画面3.1.2.4-2

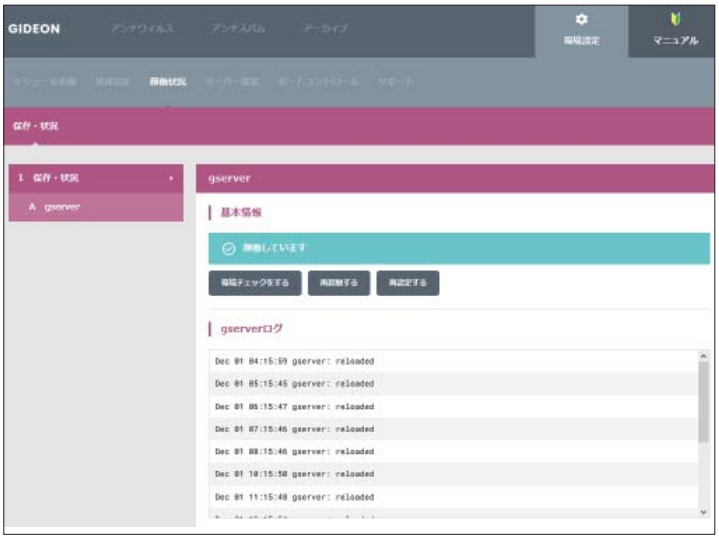
●設定ファイルの同期

「設定ファイル取得先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。
入力後、[更新する] ボタンをクリックしてください。

画面3.1.2.4-3

3.1.3 稼働状況

環境設定画面の「稼働状況」タブをクリックすると、画面3.1.3が表示されます。
ここでは製品の主要プロセスであるアンチウイルス(gserver)、パケットフィルタリング(iptablesd)
[アーカイブ機能付きの場合はアーカイブ(estmaster)]の稼働状況表示、再起動操作などが行えます。



画面3.1.3

3.1.4 サーバー環境

環境設定画面の「サーバー環境」タブをクリックすると、画面3.1.4表示されます。

画面3.1.4

3.1.4.1 保存･状況

BLOCのネットワーク状態、システム状態を表示します。

●ネットワーク

本製品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、ローカルシステムで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。

画面3.1.4.1-1

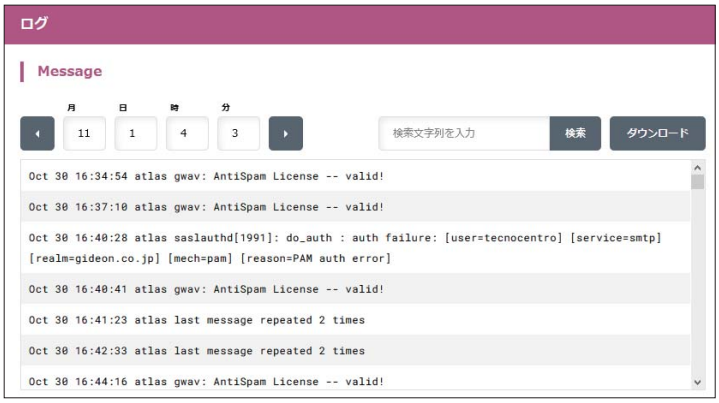
●サーバ状態

時刻　　:システムの内部時計の時刻
稼働時間　　:システムの連続稼働時間
CPU使用率　　:表示した時点でのCPUの利用度を%で表示します。
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。ウイルス検出プロセスなど
が増えると、プロセス数も増大します。
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します。
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。

画面3.1.4.1-2

3.1.4.2 ログ

サーバ環境画面の「ログ」タブをクリックすると、画面3.1.4.2が表示されます。
システムログとして、「messages」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は特定のエラーを絞ることができま
す。
さらに、[ダウンロード]ボタンをクリックするとサーバ上の「messages」ファイルがダウンロードできます。



画面3.1.4.2

3.1.4.3 設定

BLOC本体のネットワーク情報や時刻情報を設定します。

●IPアドレス

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、[更新する]ボタンをクリックしてください。

画面3.1.4.3-1

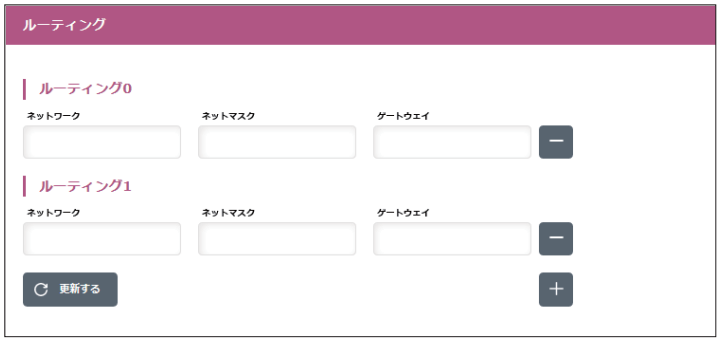
●ルーティング

BLOCのネットワーク配下に拠点間VPNルーターなどで別セグメントのネットワークが存在する場合にルーティング情報を設定します。

[設定例]BLOCのネットワーク(192.168.1.0/24)配下に192.168.3.0/24のネットワークがIPアドレス192.168.1.100のIPアドレスを持つゲートウェイから繋がっている場合

ルーティング0　　IPアドレス：192.168.3.0
　　ネットマスク：255.255.255.0
　　ゲートウェイ：192.168.1.100

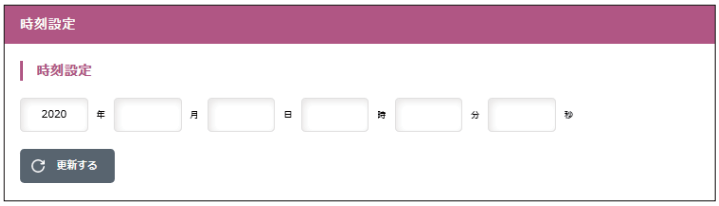
入力後、[更新する]ボタンをクリックしてください。



画面3.1.4.3-2

●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ーを設定することで、時刻を適切に修正することができます。

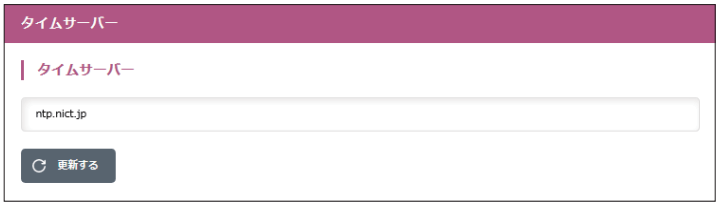


画面3.1.4.3-3

●タイムサーバー

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ーを設定します。

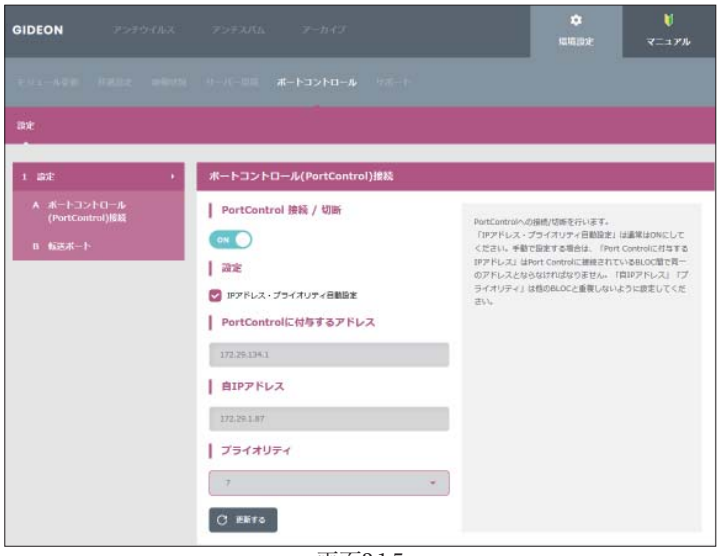
デフォルト値: ntp.nict.jp



画面3.1.4.3-4

3.1.5 ポートコントロール

環境設定画面の「ポートコントロール」タブをクリックすると、画面3.1.5が表示されます。



画面3.1.5

●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。[更新する]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。

画面3.1.5-1

●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。

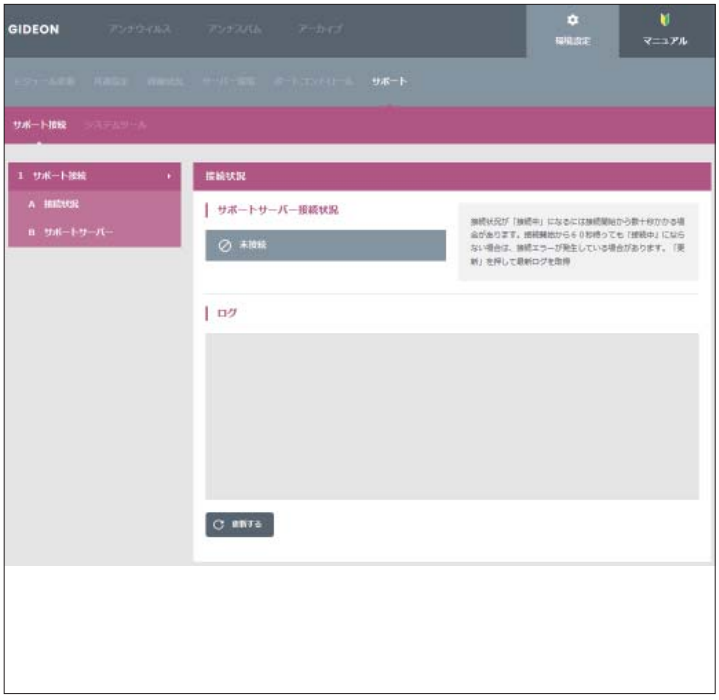
複数BLOCの転送ポート番号を登録した場合、プライオリティが最も高いBLOCにのみポートデータを転送します。このBLOCの接続を切り離したりダウンした場合、自動的にPortControlから既存登録情報が削除されます。同様のテーブルを登録している別BLOCがあれば、この別BLOCにポートデータを転送します。

入力後、[更新する]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。

画面3.1.5-2

3.1.6 サポート

環境設定画面の「サポート」タブをクリックすると、画面3.1.6が表示されます。ここではBLOCのシステム調査の際に利用する機能を操作できます。



画面3.1.6

3.1.6.1 サポート接続

BLOCとギデオンのサポート用サーバーとをVPN接続してギデオンのサポートセンターからシステム調査並びに調整を行えるようにします。
※サポート接続はギデオンサポートセンターからの指示があった時のみご利用ください。

●接続状況

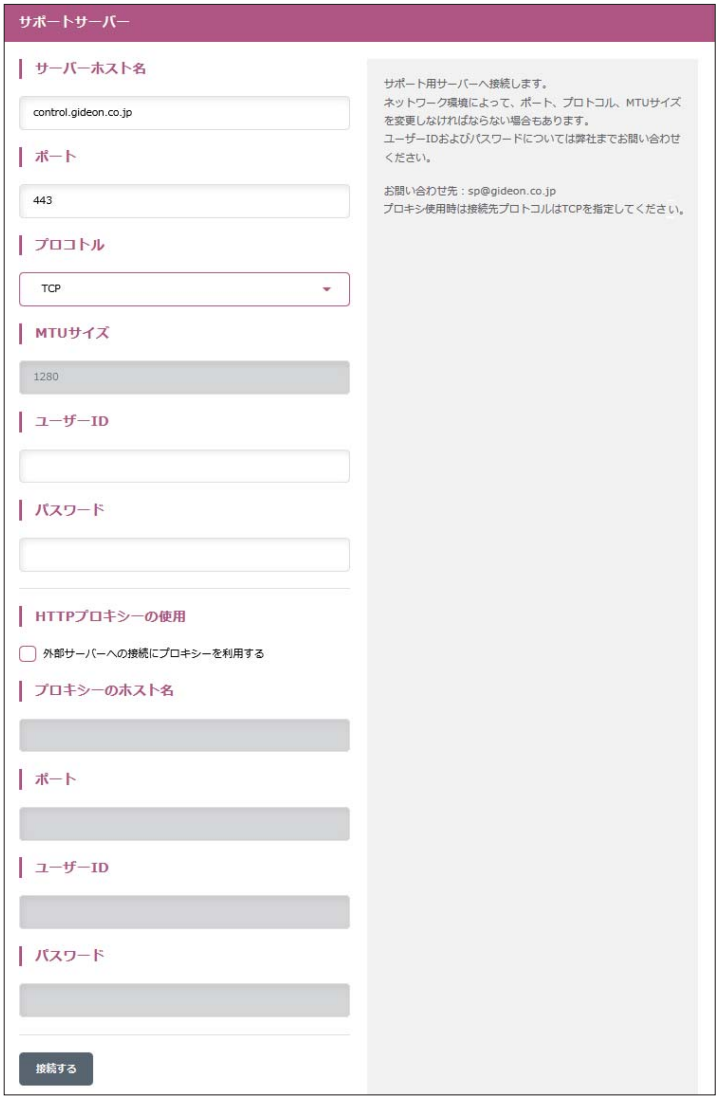
接続状況が「接続中」になるには接続開始から数十秒かかる場合があります。60秒待って「更新する」ボタンを押しても「接続中」にならない場合は、接続エラーが発生している場合があります。

画面3.1.6.2-1

●サポートサーバー

ギデオンのサポート用サーバーへ接続します。
ネットワーク環境によって、ポート、プロトコル、MTUサイズを変更しなければならない場合もあります。
ユーザーIDおよびパスワードについては弊社までお問い合わせください。

お問い合わせ先:sp@gideon.co.jp



画面3.1.6.2-2

3.1.6.3 システムツール

メールの送信元IPアドレスやドメインについての調査ツールやメンテナンスに利用するツールを提供します。

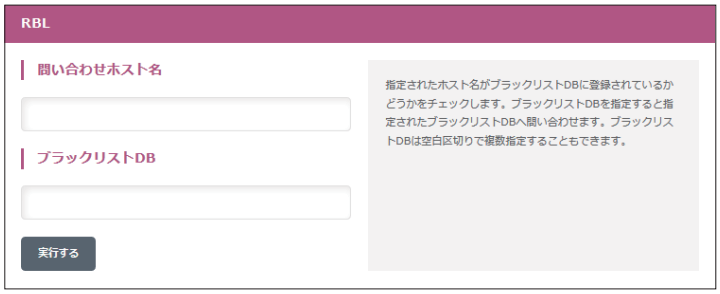
●DNS

指定されたホスト名の情報を取得します。DNSサーバーを指定すると指定されたDNSサーバーへ問い合わせます。

画面3.1.6.3-1

●RBL

指定されたホスト名がブラックリストDBに登録されているかどうかをチェックします。ブラックリストDBを指定すると指定されたブラックリストDBへ問い合わせます。ブラックリストDBは空白区切りで複数指定することもできます。



画面3.1.6.3-2

●WHOIS

指定されたドメインのWHOISクエリを行います。

画面3.1.6.3-3

●SSH

SSHサービスの起動・停止、SSHサービスを利用できる接続元IPアドレスの指定やSSHでログインする際のSSHパスワードの変更を行います。

< アクセス範囲 >
SSHサービスを利用できるIPアドレスの範囲を指定します。空白区切りで複数指定することもできます。
例:192.168.0.0/255.255.255.0/192.168.100.1

※登録されたadminパスワードは次回表示のときに「*」で表示されます。
adminパスワードを編集したい場合は「*」を消去し、新たなadminパスワードを入力してください。

画面3.1.6.3-4

●サポート診断

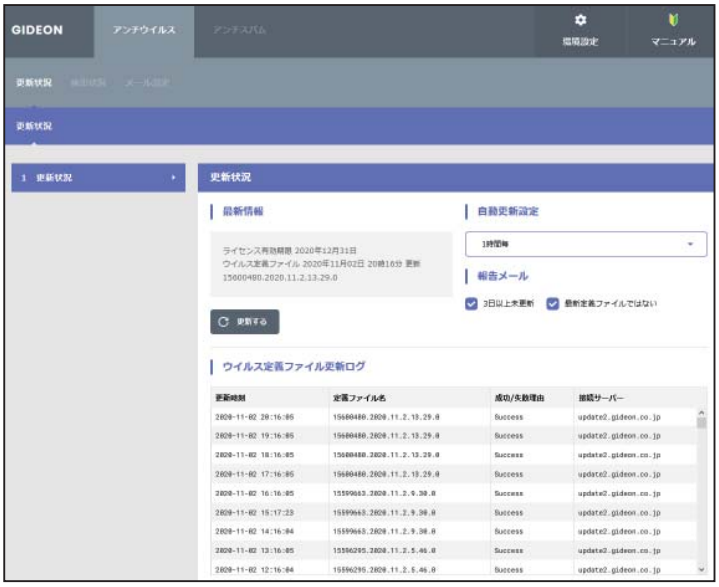
診断プログラムを実行し、システムの設定やログをギデオンサポートセンターに送信します。
※実行時はギデオンサポートセンターまでご連絡ください。

画面3.1.6.3-5

4.1 更新状況

アンチウイルス設定画面の「更新状況」タブをクリックします。ここではウイルス定義ファイルの更新状況を閲覧できます。

カスペルスキーのアンチウイルスエンジン（種別：kav）が利用するウイルス定義ファイルを更新します。



画面4.1

「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日以上ウイルス定義ファイル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。

●ウイルス定義ファイル更新ログ

最新のウイルスに対応する、定義ファイルの更新状況を表示します。

［更新する］ボタンをクリックすると、その時点で最新の定義ファイルの取得を行います。既に更新済みの場合は、新たに更新されません。

自動更新の頻度は、初期設定では1時間毎に設定されています。緊急対策が必要な場合は手動更新を行ってください。

4.2 検出状況

アンチウイルス設定画面の「検出状況」タブをクリックすると、画面4.2が表示されます。

画面4.2

●検出状況

検出状況画面の上部「最新情報」欄では、最終ウイルス検出の日時、サービス(mta)、ウイルス検出名が表示されます。

続いて、「検出統計情報」欄では、直近 1 週間の日別検出数グラフと「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。

●ウイルス検出数ランキング

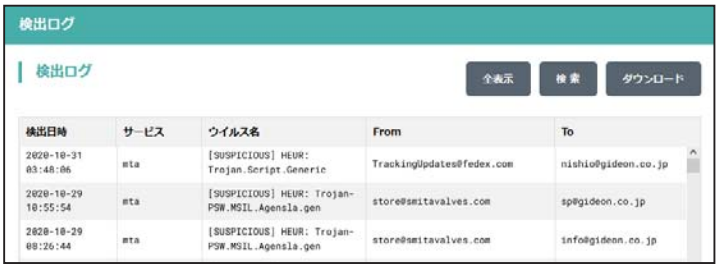
検出頻度の高いウイルス名を、各期間ごとに表示します。

［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。

画面4.2-1

●検出ログ

最新の150KBまでの検出ウイルスをリスト表示します。



画面4.2-2

ここで［検索］ボタンをクリックすると、図4.2-3のようなウインドウがポップアップして表示項目の内容で絞り込検索を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4.2-3

さらに、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4.2-4

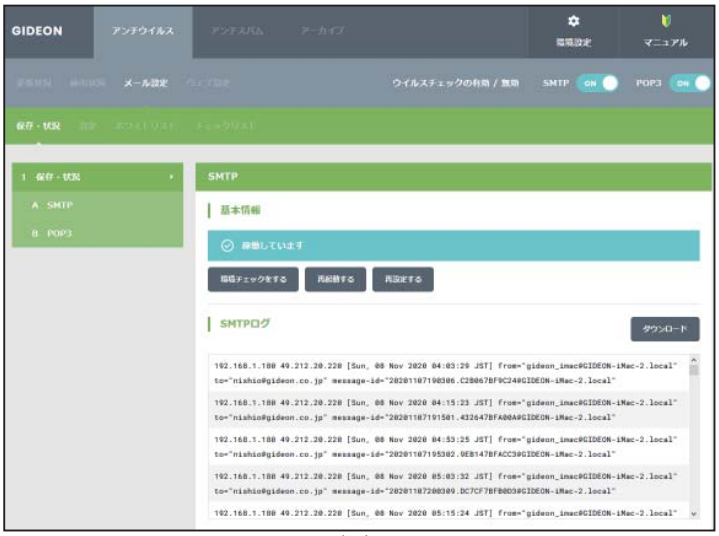
4.3 メール設定

管理･設定画面の「メール設定」タブをクリックすると、画面4.3が表示されます。

ここでは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のスイッチをスライドさせて有効または無効を設定します。



画面4.3

4.3.1 保守･状況

送信(SMTP)、受信(POP3)に分かれて表示されます。

稼働状況　：稼働状況を表示します。
ログ　：最新のログを取得し、下のログ一覧に表示します。
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。
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。
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、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、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4.3.1

4.3.2 設定

メール設定画面の「設定」タブをクリックすると、画面4.3.2が表示されます。

画面4.3.2

●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、[更新する] ボタンをクリックしてください。

画面4.3.2-1

●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。

入力後、［更新する］ボタンをクリックしてください。

画面4.3.2-2

●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。「3.1.2.1 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、[更新する] ボタンをクリックしてください。

画面4.3.2-3

● 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、[更新する]ボタンをクリックしてください。
初期設定値 ：SMTP 9025　 POP3 9110

画面4.3.2-4

● 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

画面4.3.2-5

● 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

画面4.3.2-6

● 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

画面4.3.2-7

● 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

画面4.3.2-8

● 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）

画面4.3.2-9

● 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』

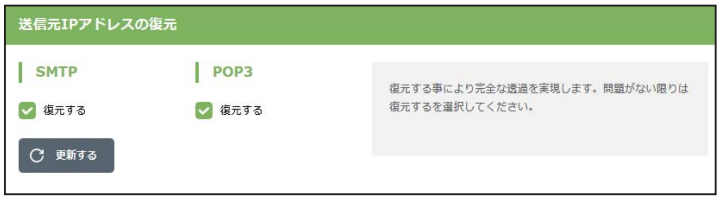
画面4.3.2-10

● 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。

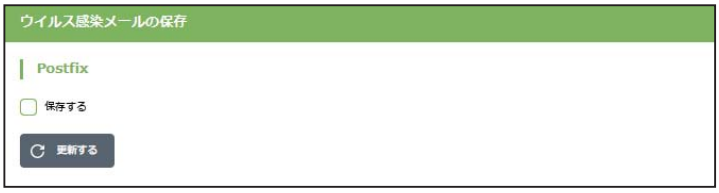
SMTPまたはPOP3でこの機能を有効もしくは、無効にするには、[復元する]ボタンをクリックしてチェックマークが付けば有効化され、無印であれば無効化されます。



画面4.3.2-11

●ウイルス感染メールの保存

ウイルス感染したメールを、特定のディレクトリに保存することができます。
隔離ディレクトリの設定は、「感染メール保存ディレクトリ設定」で行います。
入力後、[更新する] ボタンをクリックしてください。

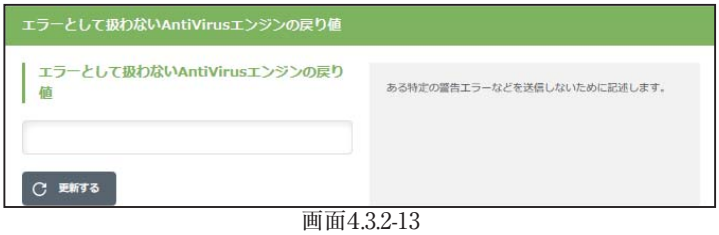


画面4.3.2-12

●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、[更新する] ボタンをクリックしてください。

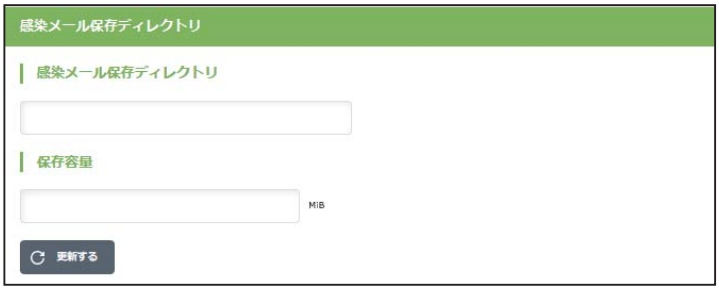


画面4.3.2-13

●感染メール保存ディレクトリ

ウイルス検知された感染メールを保存するためのディレクトリを指定します。
保存用ディレクトリを作成し（例 /var/tmp/virus）、ルートディレクトリから指定してください。
保存容量とは、保存する容量の上限値を入力します。この上限値を超えた場合、古いデータから消去されますのでご注意ください。

入力後、[更新する] ボタンをクリックしてください。



画面4.3.2-14

4.3.3 ホワイトリスト

メール設定画面の「ホワイトリスト」タブをクリックすると、画面4.3.3が表示されます。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。

画面4.3.3

● 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

-----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、ウイルス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、ウイルス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、ウイルス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、ウイルス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=@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

-----例1-----

送信元sender@example.com から送信されてきた場合、ウイルス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、ウイルス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

拡張ホワイトリスト設定

アンチウイルス設定画面の上部「メール設定」タブをクリックし、続いて「ホワイトリスト」タブ「拡張」メニューをクリックします。拡張ホワイトリスト設定では部分一致による設定やエンベロップ情報とヘッダ情報を区別した設定が可能となっています。

画面 4.3.3-1

拡張ホワイトリスト記入上の注意

(1)設定の際は、従来のホワイトリストとは異なり、
from-name="GIDEON"
などのように『"』(ダブルクォーテーション)で囲うようにしてください。

(2)拡張ホワイトリストに記述する書式は以下の通りです。
ホストのIPアドレスを記述する場合:
host="ip_address" もしくは　host="ip_address/mask"

● 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
envelope-from:	エンベロープのFromメールアドレス
envelope-to:	エンベロープのToメールアドレス
from:	メールヘッダ中のFromメールアドレス
body:	メール本文中に記載されたキーワード(部分一致)

-----例-----

envelopeのfromがexampleに後方一致した場合にスルー

envelope-from="*.example.com"

● 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:	メールヘッダ中のFromメールアドレス
body:	メール本文中に記載されたキーワード(部分一致)

-----例-----

メールヘッダ中のfromがexampleに後方一致した場合にスルー

from="*.example.com"

4.3.4 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4.3.4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すべてのメール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、登録された条件に合致するメールのみが検出対象となります。

画面 4.3.4

● SMTP

チェック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がメールに含まれている場合のみウイルスチェックを行います。

メールアドレスの他に、@DOMAINのようにユーザー名を省略して記述することで、@DOMAINが含まれるアドレス全てのウイルスチェックを行います。

※チェックリストとホワイトリスト双方に登録がある場合はチェックリストのみ使用されます。登録は1行1メールアドレス(ドメイン)です。

-----例1-----

info@example.com宛のメールをウイルスチェックする

info@example.com

-----例2-----

@以下がexample.com宛のメールをウイルスチェックする

@example.com

● POP3

チェックリストに登録された項目が一致した場合のみウイルス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全てのメールをチェックします。
記述はユーザーID@IPアドレスとなります。@IPアドレスと記述するとPOP3サーバー全てのユーザーを示すことになります。
※チェックリストとホワイトリスト双方に登録がある場合はチェックリストのみ使用されます。

-----例1-----
POP3サーバーが192.168.1.1でユーザーIDがuser1の場合、ウイルスチェックする

user1@192.168.1.1
-----例2-----
POP3サーバーが192.168.1.1の全てのユーザーのメールをウイルスチェックする

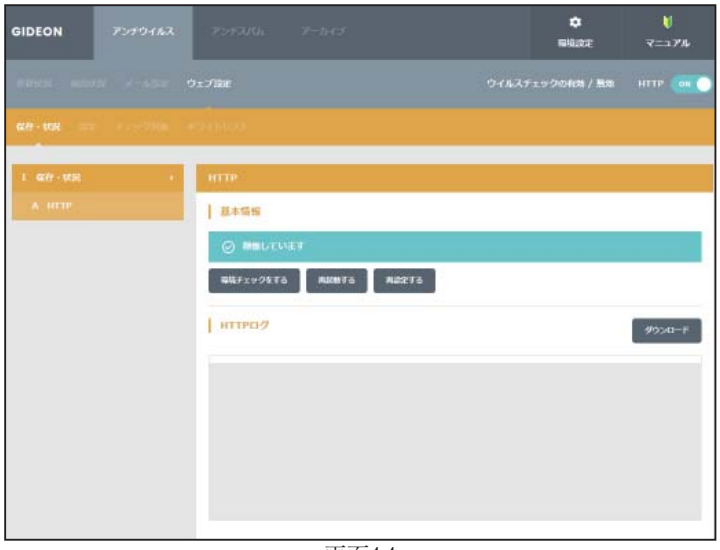
@192.168.1.1

4.4 ウエブ設定

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。

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のスイッチをスライドさせて有効または無効を設定します。

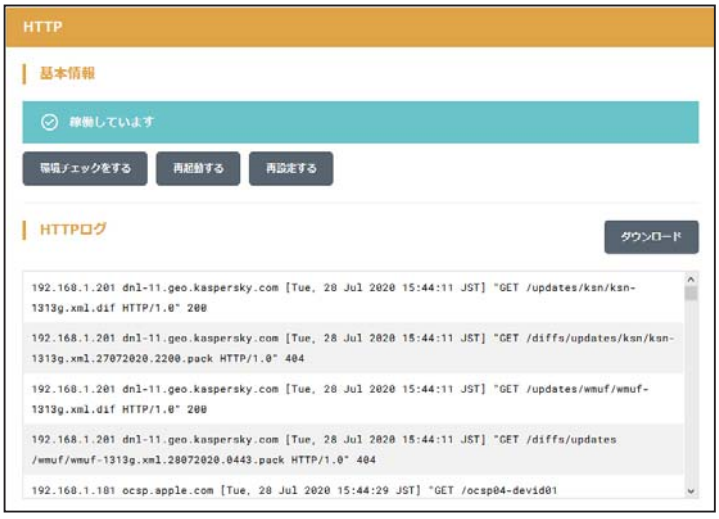


画面4.4

4.4.1 保守･状況

ウエブ(HTTP)について表示されます。

稼働状況　　：稼働状況を表示します。
ログ　　：最新のログを取得し、下のログ一覧に表示します。
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。
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。
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、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、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4.4.1

4.4.2 設定

ウエブ設定画面の「設定」タブをクリックすると、画面4.4.2が表示されます。

画面4.4.2

●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]において、それぞれ有効/無効をチェックボックスで選択してください。

画面4.4.2-1

●管理者への警告メール

HTTP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。「3.1.2.1 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、[更新する]ボタンをクリックしてください。

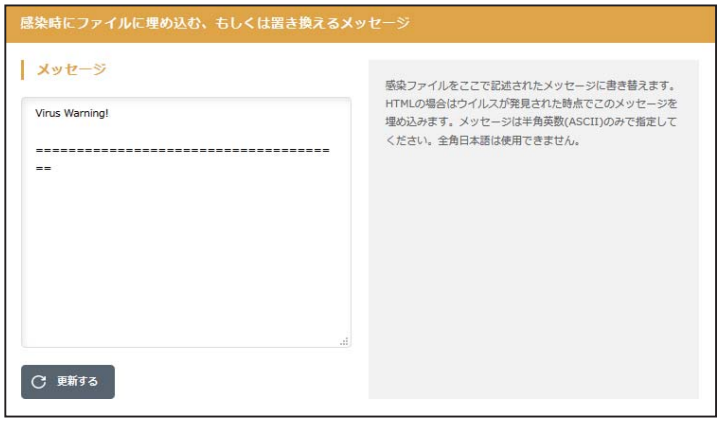
画面4.4.2-2

●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、[更新する]ボタンをクリックしてください。



画面4.4.2-3

●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、[更新する]ボタンをクリックしてください。

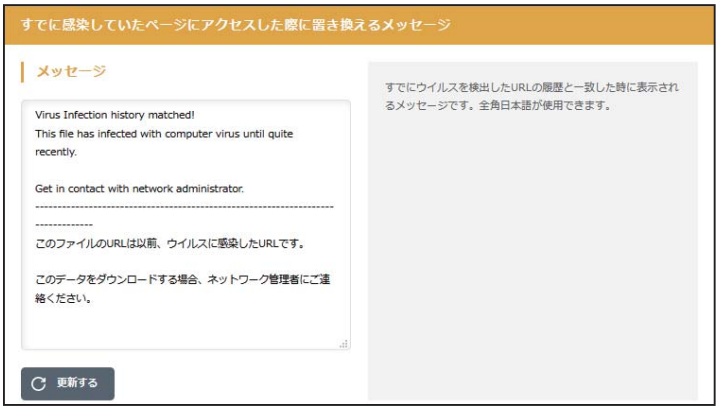
●すでに感染していたページにアクセスした際に置き換えるメッセージ

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。

該当項目入力後、[更新する]ボタンをクリックしてください。



画面4.4.2-4

● 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、[更新する]ボタンをクリックしてください。

初期設定値 ：9080

画面4.4.2-5

● 監視する接続先のポート

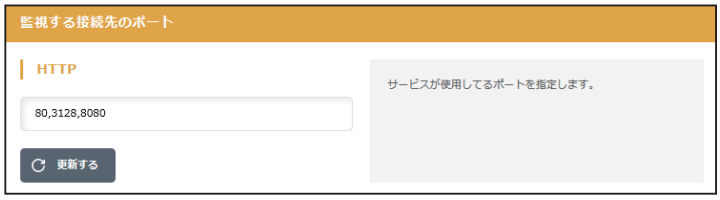
HTTPサービスが使用しているポート番号を指定します。

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。



面4.4.2-6

●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 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、[更新する]ボタンをクリックしてください。

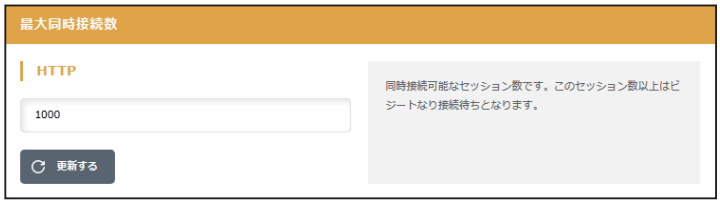
画面4.4.2-7

●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、[更新する]ボタンをクリックしてください。



画面4.4.2-8

●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、[更新する]ボタンをクリックしてください。

画面4.4.2-9

●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ン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、[更新する]ボタンをクリックしてください。

画面4.4.2-10

●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、[更新する]ボタンをクリックしてください。

画面4.4.2-11

●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、[更新する]ボタンをクリックしてください。

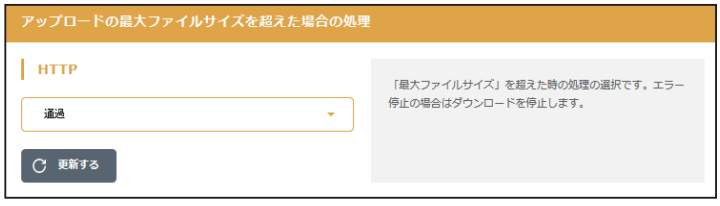
画面4.4.2-12

●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、ダウンロードを停止します。

入力後、[更新する]ボタンをクリックしてください。

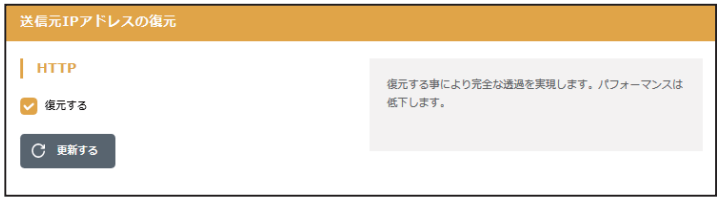


画面4.4.2-13

●送信元IPアドレスの復元

復元する事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。

入力後、[更新する]ボタンをクリックしてください。



画面4.4.2-14

●ウイルス感染ファイルの保存

BLOCでは使用しません。

5.1 更新状況

アンチスパム設定画面の「更新状況」タブをクリックします。ここでは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、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。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DB を更新します。

画面5.1

このスパムDB は、初期設定では3 時間毎に自動更新します。自動更新の間隔を変更することも可能です。推奨は1 時間毎です。

[更新する]ボタンをクリックすると、現時点での最新のスパムDB への更新を試みます。
通常は自動更新によりスパムDB の更新が行われるため、手動更新を実行する必要はありません。

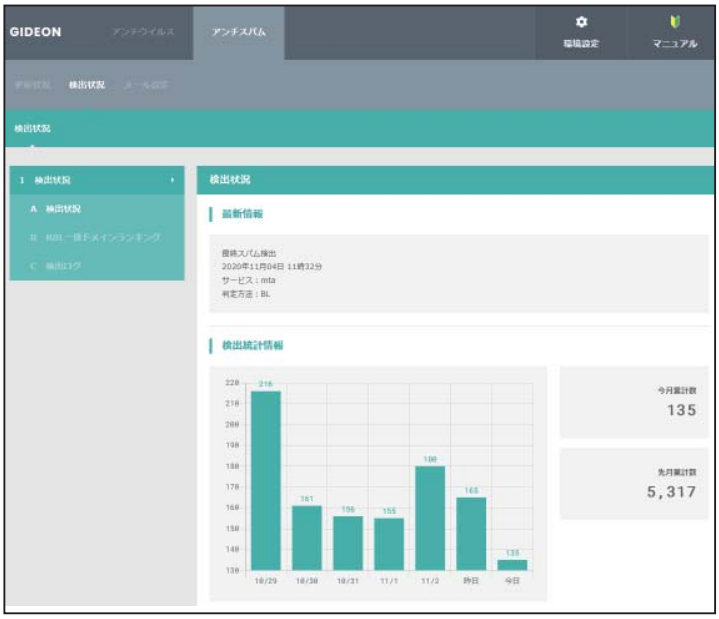
「報告メール」は、スパムDB の更新状況をメールでお知らせするものです。
「3 日以上未更新」は、3 日以上スパムDB の更新がない場合に管理者宛にメール送信します。
「最新定義ファイルでない」は、システム上のスパムDB が最新でない場合に管理者宛にメール送信します。

5.2 検出状況

アンチスパム設定画面の「検出状況」タブをクリックします。ここでは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「最新情報」欄では、最終スパム検出の日時、サービス(mta)、判定方式が表示されます。
続いて、「検出統計情報」欄では、直近1 週間の日毎スパム検出数グラフと、今月/ 先月の月毎スパム検出数が表示されます



画面5.2

●RBL一致ドメインランキング

検出状況画面のメニュー「RBL 一致ドメインランキング」では、スパムメール判定方法のひとつであるxSPAM 方式(XS) 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。
「RBL 一致ドメインランキング」では、今月/ 先月の月毎と稼働開始からのRBL 一致ドメイン検出数上位3 つが表示されます。

画面5.2-1

[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5.2-3

●検出ログ

検出状況画面のメニュー「検出ログ」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。

画面5.2-4

[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。

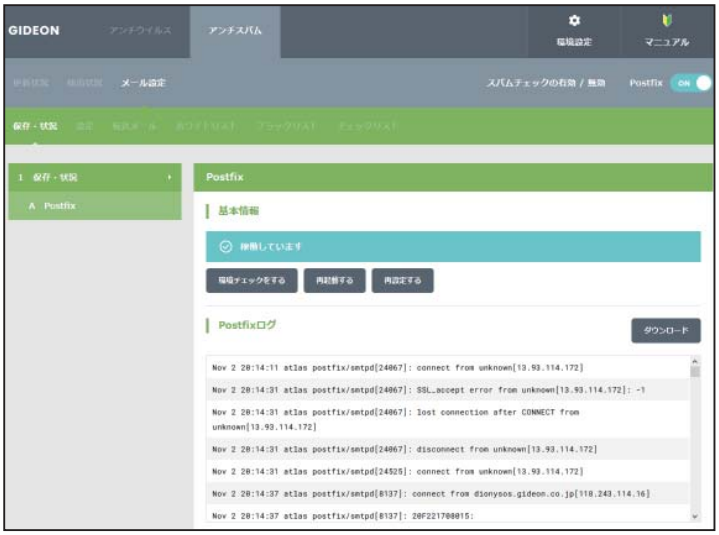
画面5.2-5

さらに、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5.2-6

5.3 メール設定

アンチスパム設定画面の「メール設定」タブをクリックすると、画面5.3が表示されます。



画面5.3

5.3.1 保守･状況

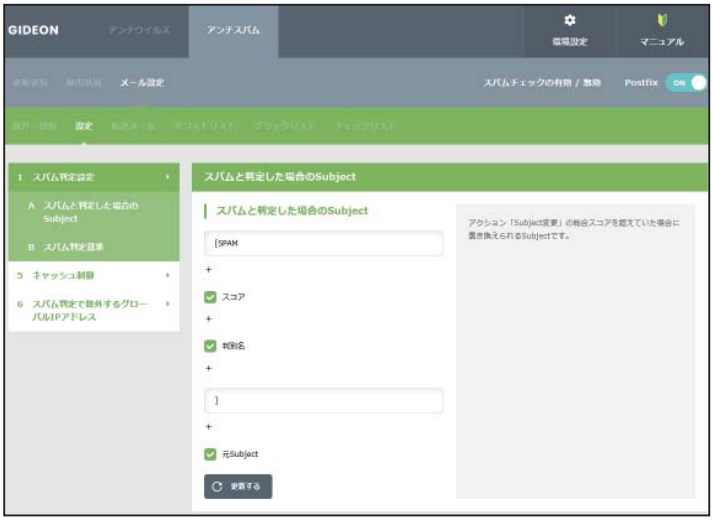
メール設定画面の「保守・状況」タブをクリックすると、画面 5.3.1 が表示されます。本項は、アンチウイルスでの設定と共通です。詳細は本書「4.3.1 保守 ･状況」を参照してください。

画面5.3.1

5.3.2 設定

メール設定画面の「設定」タブをクリックすると、画面5.3.2が表示されます。ここではスパム判定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5.3.2

●スパムと判定した場合のSubject

「設定」画面でメニュー「スパム判定した場合の Subject」をクリックすると、画面 5.3.2-1 が表示されます。。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。

「スパムと判定した場合のSubject」にて、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 4: KAS RES］元Subject

これはスパム判定名KAS および RES の合計スコアが 4 であり、スパムと判定されたことを表します。変更する場合は、入力後に［更新する］ボタンをクリックしてください。

画面5.3.2-1

●スパム判定基準

「設定」画面でメニュー「スパム判定基準」をクリックすると、画面5.3.2-2が表示されます。

スパム判定設定

判定方法、アクション、追加ヘッダに関するスコア設定を推奨設定のままにするか、カスタマイズするかを選択します。(「推奨設定を利用する」を選択した場合、判定方法、アクション、追加ヘッダに関するスコア設定項目は入力できなくなります)

判定方法

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。

注意

「アクション」の「MTA 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。

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。

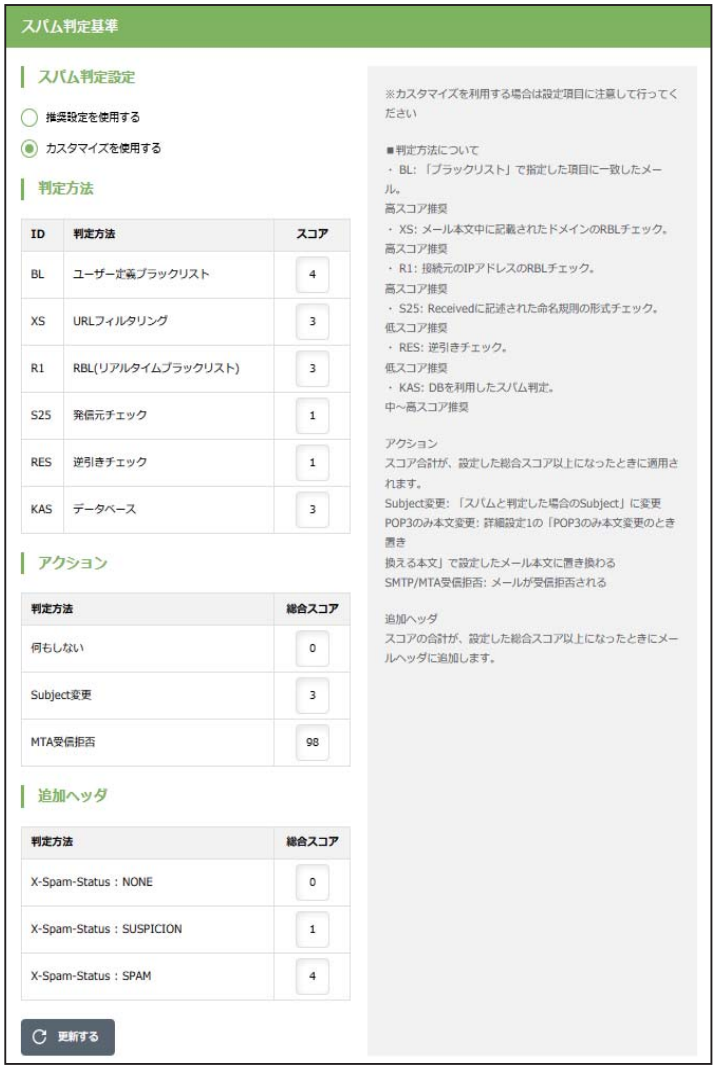
（ヘッダ表示）	（内容）
X-Spam-Status: NONE	スパムに該当せず
X-Spam-Status: SUSPICION	スパムと疑わしい
X-Spam-Status: SPAM	スパムに該当

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。



画面5.3.2-2

● チェックに使用するポート

アンチウイルス設定と同じ設定となります。詳細は「4.3.2 設定」をご覧ください。

● 監視する接続先のポート

アンチウイルス設定と同じ設定となります。詳細は「4.3.2 設定」をご覧ください。

● 初期の接続待機数

アンチウイルス設定と同じ設定となります。詳細は「4.3.2 設定」をご覧ください。

● 最大同時接続数

アンチウイルス設定と同じ設定となります。詳細は「4.3.2 設定」をご覧ください。

● 待機数を超えた場合の接続増加数

アンチウイルス設定と同じ設定となります。詳細は「4.3.2 設定」をご覧ください。

● 送信元IPアドレスの復元

アンチウイルス設定と同じ設定となります。詳細は「4.3.2 設定」をご覧ください。

●キャッシュ制御

「設定」画面でメニュー「キャッシュ制御」をクリックすると、画面5.3.2-3が表示されます。

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。

［キャッシュクリア］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。

画面5.3.2-3

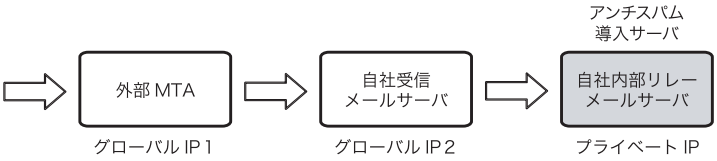
●スパム判定で除外するグローバルIPアドレス

「設定」画面でメニュー「スパム判定で除外するグローバルIPアドレス」をクリックすると、画面5.3.2-4が表示されます。

アンチスパムPlusでは、受信したメールの直前のグローバルIPアドレスをチェックしてスパム判定を行います。したがって本製品を導入したサーバと、外部との間に転送用その他のサーバが接続されている場合には、それらのグローバルIPアドレス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、本製品を導入したメールサーバでメールを受信する経路上の、スパム判定しないグローバルなIPを指定します。

-----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にアンチスパムを導入した場合を例にとります。

- アンチスパム導入サーバの直前におかれたすべての受信メールサーバIPアドレスを、スパム判定対象外に指定します。グローバルIP2を「スパム判定で除外するグローバルIPアドレス」に入力して下さい。その後［更新する］ボタンをクリックします。
- 外部MTAが転送目的のサーバであれば、グローバルIP1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。

重要

メール受信の経路上にあるメールサーバのグローバルIPを漏れなく記載する必要があります。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などを参照してください。

画面5.3.2-4

5.3.3 転送メール設定

メール設定画面の「転送メール」タブをクリックすると、画面8.4.3が表示されます。

画面5.3.3

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します。

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。

● POP 3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、「5.3.6 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。

-----SMTP 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

-----SMTP 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

-----POP3 例 1-----

POP3 のユーザーID がuser-one、POP3 サーバのIP アドレスが192.168.0.1 の適合メールをspam-admin@example.com に転送する場合は、以下のように入力します。

user-one@[192.168.0.1] spam-admin@example.com

5.3.4 ホワイトリスト

メール設定画面の「ホワイトリスト」タブをクリックすると、画面5.3.4が表示されます。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。

画面5.3.4

● 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

-----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。

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

-----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

拡張ホワイトリスト設定

アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「ホワイトリスト」タブ「拡張」メニューをクリックします。拡張ホワイトリスト設定では部分一致による設定やエンベロップ情報とヘッダ情報を区別した設定が可能となっています。

画面 5.3.4-1

拡張ホワイトリスト記入上の注意

(1)設定の際は、従来のホワイトリストとは異なり、
from-name="GIDEON"
などのように『"』(ダブルクォーテーション)で囲うようにしてください。

(2)拡張ホワイトリストに記述する書式は以下の通りです。
ホストのIPアドレスを記述する場合:
host="ip_address" もしくは　host="ip_address/mask"

● 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
envelope-from:	エンベロープのFromメールアドレス
envelope-to:	エンベロープのToメールアドレス
from:	メールヘッダ中のFromメールアドレス
body:	メール本文中に記載されたキーワード(部分一致)

-----例-----

envelopeのfromがexampleに後方一致した場合にスルー

envelope-from="*.example.com"

● 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:	メールヘッダ中のFromメールアドレス
body:	メール本文中に記載されたキーワード(部分一致)

-----例-----

メールヘッダ中のfromがexampleに後方一致した場合にスルー

from="*.example.com"

5.3.5 ブラックリスト

メール設定画面の「ブラックリスト」タブをクリックすると、画面5.3.5が表示されます。
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、「スパム判定基準」画面の「BL ユーザ定義ブラックリスト」で指定します。

画面5.3.5

● 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

-----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。

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

-----例1-----

送信元sender@example.com 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。

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、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 user=user-one

拡張ブラックリスト設定

アンチウイルス設定画面の上部「メール設定」タブをクリックし、続いて「ブラックリスト」タブの「拡張」メニューをクリックします。拡張ブラックリスト設定では部分一致による設定やエンベロップ情報とヘッダ情報を区別した設定が可能となっています。

画面 5.3.5-1

拡張ブラックリスト記入上の注意

(1)設定の際は、従来のブラックリストとは異なり、
from-name="GIDEON"
などのように『"』(ダブルクォーテーション)で囲うようにしてください。

(2)拡張ブラックリストに記述する書式は以下の通りです。
ホストのIPアドレスを記述する場合:
host="ip_address" もしくは　host="ip_address/mask"

● 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
envelope-from:	エンベロープのFromメールアドレス
envelope-to:	エンベロープのToメールアドレス
from:	メールヘッダ中のFromメールアドレス
body:	メール本文中に記載されたキーワード(部分一致)

-----例-----

envelopeのfromがexampleに後方一致した場合に拡張ブラックリストを適用

envelope-from="*.example.com"

● 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:	メールヘッダ中のFromメールアドレス
body:	メール本文中に記載されたキーワード(部分一致)

-----例-----

メールヘッダ中のfromがexampleに後方一致した場合に拡張ブラックリストを適用

from="*.example.com"

5.3.6 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】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5.3.6

6.1 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。

6.2 更新状況

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

・メールデータは、使用中のボリュームに保存します。
・当日のインデックスについては、サーバ内部のストレージに作成します。
・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時点から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を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までのインデックスに追加する場合は、"mail-merge"を表示します。
件数　：インデックス化された件数を表示します。
成否　：インデックス作成の成否(成功"Success"、失敗"Fail")を表示します。
対象ディレクトリ　：メールデータを書き込むディレクトリを表示します。
　メールがない場合は表示されません。
ボリューム　：当日のインデックスはサーバ内部のストレージのパーティション(/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容量(MByte)を表示します。

[手動作成] ボタンをクリックすると、まだインデックスを作成していない当日のメールについて、インデックスを作成します。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日以上未更新イ　：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。


GIDEON
アンチウイルス
アンチスパム
アーカイブ
環境設定
マニュアル
更新状況
メール設定
更新状況
1 更新状況
更新状況
最新情報
ライセンス有効期限 2028年12月31日
インデックス作成 2020年11月18日 10時40分
件数: 0
更新する
自動更新設定
1時間毎
報告メール
3日以上未更新
スタート時刻
00時
40分
インデックス作成ログ
更新時刻
種別
件数
成否
対象ディレクトリ
ボリューム
空容量[MiB]
2020-11-18 10:40:04
mail
0
Success
/mnt/gideon_archive /vol0/20201118
/dev/sda1
199,231
2020-11-18 09:40:05
mail
0
Success
/mnt/gideon_archive /vol0/20201118
/dev/sda1
199,232
2020-11-18 08:40:05
mail
0
Success
/mnt/gideon_archive /vol0/20201118
/dev/sda1
199,234

画面 6.2

6.3 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6.3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。
「今月」、「先月」のメールアーカイブ数と直近7 日間のメールアーカイブ数グラフを表示します。

● 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。

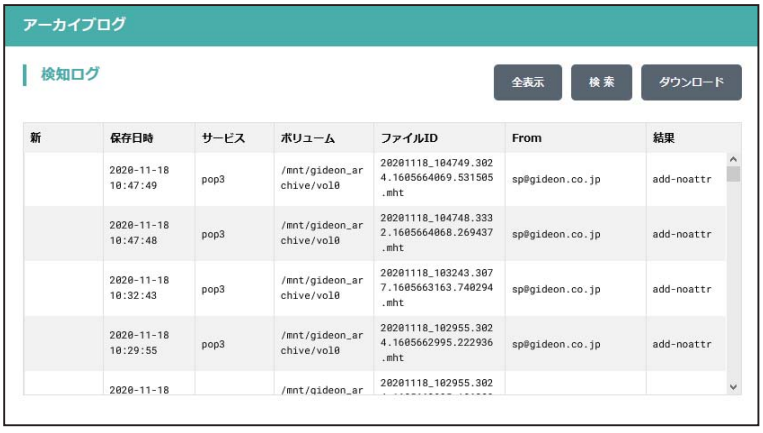
画面 6.3

● 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の閲覧が可能です。
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	：受信したメールを、アーカイブした日時を表示します。
サービス	：mta と表示します。
ボリューム	：アーカイブの対象ボリュームを表示します。
ファイルID	：アーカイブ時につけたユニークなID です。
From	：From のメールアドレスを表示します。
結果	：add　メールデータおよびインデックスが作成された場合
	add-noattr　メールのアーカイブに成功したが、インデックスは作成されない場合
	fail　メールデータが作成できない場合

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



画面 6.3-1

6.4 メール設定

6.4.1 保守状況

本項は、アンチウイルスやアンチスパムでの設定と共通です。

6.4.2 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可能です。
（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、主ホスト名をdomain.co.jpと登録することで、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」に登録することで、主ホスト名による検索が可能です。

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。

[追加する]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可能です。
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、項目の変更が可能です。

画面 6.4.2-1

●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。

[更新する]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。

[更新する]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ストレージのご利用を推奨します。

「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 6.4.2-2

6.4.3 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可能です。

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可能です。
" 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の検索が可能です。
" 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　　：検索画面にログインする際に用いるID を登録します。test@domain.co.jp のようなメールアカウントを登録することも可能です。

サーチID リスト　：各アカウントにて検索できるメールアカウントを登録します。

（例）

test@domain.co.jp というアカウント保有者が、test1@domain.co.jp とtest2@domain.co.jp 宛てのメールも検索できるようにするための登録は次の通りです。

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「6.4.2 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可能です。
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、項目の変更が可能です。


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
○
abc
abcd
○
○
○
○
★
○
★
○
追加する
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事で、アーカイブされたメールを参照する事ができます。項目の意味は以下の通り。
属性：属性は以下の3種
★：管理者（すべてのメール参照可）
○：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 6.4-3

6.4.4 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可能です。
（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が可能です。
同様に、部課単位で定義すると、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。
※「アカウントリスト」に登録するに先立ち、前項の「6.4.3 アカウント」でアカウントの登録をしてください

[追加する]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可能です。
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、項目の変更が可能です。

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。

画面 6.4.4

6.4.5 アクセス制限

アーカイブ検索iSearch へのアクセスをIP アドレスで制限することが可能です。
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です。
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

[更新する] ボタンをクリックすると、リストの更新が可能です。

画面 6.4.5

6.4.6 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 : 現在使用中のボリュームが表示されます。初期の場合、「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、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。

[更新する] 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、該当ボリュームのステータス表示が「未マウント」から「マウント中」に変わります。


マウントするボリューム
基本設定
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
初期ボリューム - 使用率 40%
マウント中
ファイルシステム
デバイス名
ext3
/dev/sdb1
利用開始日
2015/03/19
クリア
追加ボリューム1
未マウント
ファイルシステム
デバイス名
利用開始日
クリア
追加ボリューム2
未マウント
ファイルシステム
デバイス名
利用開始日
クリア
ボリュームについて
ここではメール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と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 6.4.6

6.5 アーカイブ検索

6.5.1 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。

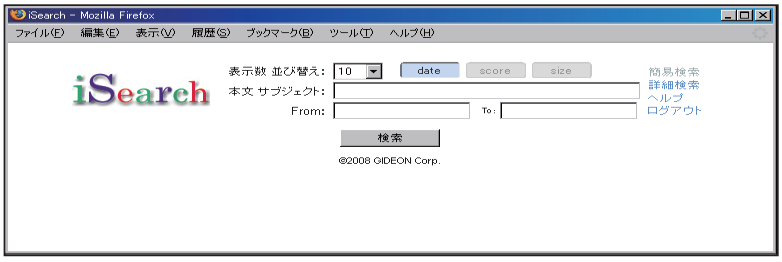
画面 6.5.1

6.5.2 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 6.5.2

6.5.3 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。

※両方の日付を入力する場合、右側の日付より左側の日付が大きくならないように入力してください

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。

プロトコル　: 送受信全てのメール(All)、送信メール(SMTP))、受信メール(POP3) を選択して検索できます

メッセージID 重複抑制: 同一メッセージID のメールを検索結果から除外します。

検索ボタン　: 上記項目による絞込みした条件下で検索を実行します。

CSV Download ボタン: 検索した結果のサマリーをCSV 形式でダウンロードします。

※検索結果をダウンロードしますので、検索結果が表示される前にはクリックしないでください。

[出力項目の順番]

メールの件名、送信元名< メールアドレス>、信先名< メールアドレス>、メールヘッダ上に記載されている日付日時、サーチID(=実際の送受信アカウント)、添付ファイル有無(Attached =添付あり、Not attached= 添付なし)

画面6.5.3-1

● 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。

[注意事項]
「検索結果」の右側に表示されます件数表記[例. Results of 1 - 50 of about XXXXX for BLOC]ですが、この件数は1ページ目を検索し終わったタイミングでの件数ですので、最終検索件数とは一致しないことがございます。(そのため"about"という表現となっております。)もし、正しい件数を確認されたい場合は2ページ目以降の表記を確認するか、或いはcsvダウンロードしたファイルにてご確認ください。

● 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

[注意事項]
HTML 形式のメール、或いは添付ファイルがHTML 形式の場合、弊社製品ではHTML 部分をテキスト化して表示いたします。そのため、HTML タグも検索結果に表示されてしまうことをどうかご了承ください。

画面 6.5.3-2

6.5.4 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 6.5.4

7.1 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本体にUSB接続します。
図7.1-1 のようにキーボードを接続します。モニターは図7.1-2のように接続します。

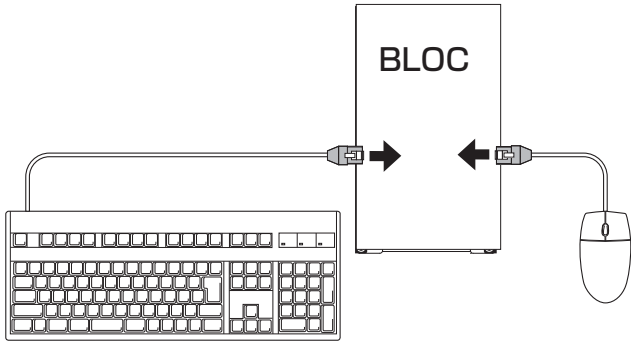


図7.1-1

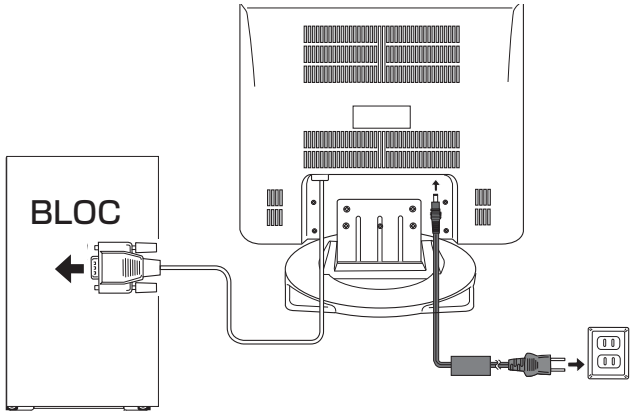


図7.1-2

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 -*

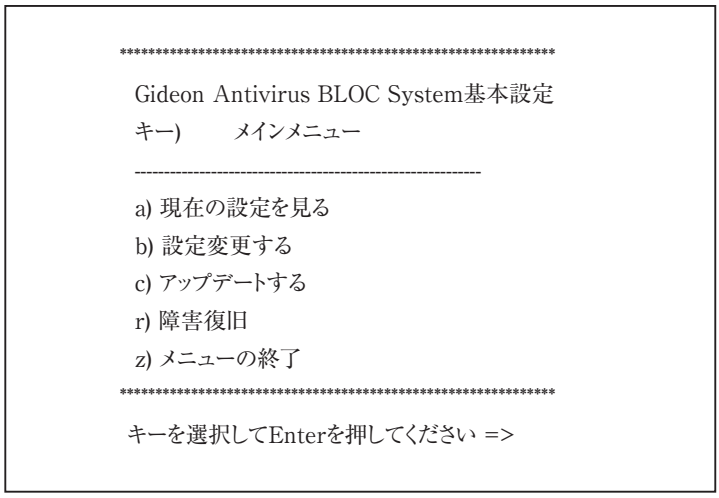
さらに以下のイタリック部分を入力して「Enter」キーを押します。
ただし、入力しても画面には表示されません。

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7.1-3が表示されます。



画面7.1-3

「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）。

7.2 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7.1-3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 =>
```

画面7.2-1

画面7.2-1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7.2-2

画面6.2-2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7.1-3「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。

7.3 困った時の設定

7.3.1 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7.1-3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6.2-2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。

7.3.2 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8.1-3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。

8.1 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。

8.2 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。

8.3 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

2020年 12月1日　　第3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3382-7
http://www.gideon.co.jp/