

ギデオン アンチウイルス
ブロック システム

GIDEON

BLOC system

ギデオン アンチウイルス BLOC system PortControl Plus

ユーザーズマニュアル

はじめに

この度は、製品をお買い上げいただきまして、誠にありがとうございます。本ユーザーズガイドは、「ギデオン アンチウイルス BLOC system PortControl Plus」のユーザーズマニュアルです。

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

■著作権など

本ユーザズマニュアルの著作権は株式会社ギデオンに帰属します。

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

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

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

その他、記載されている会社名、製品名は各社の商標および登録商標です。

ご注意	7
取扱い上のご注意	8
梱包内容の確認	8
第1章 製品のご紹介	9
第2章 BLOCの接続と動作	11
2.1 BLOCの接続方法について	11
2.1.1 シンプルなLAN構成	11
2.1.2 LAN側にプロキシなどがある場合	12
2.1.3 LAN側にメールサーバなどがある場合	12
2.2 BLOCの接続方法についてのご注意	13
2.3 BLOCの接続とセットアップ	14
2.4 管理・設定画面のアクセス方法	16
2.5 ログイン	17
2.6 管理画面について	18
第3章 環境設定	19
3.1 設定画面	19
3.1.1 モジュール更新	19
3.1.2 共通設定	20
3.1.3 稼働状況	27
3.1.4 サーバー環境	28
3.1.5 ポートコントロール	33
3.1.6 サポート	36
第4章 アンチウイルス設定	41
4.1 更新状況	41
4.2 検出状況	42
4.3 メール設定	45
4.3.1 保守・状況	46
4.3.2 設定	47
4.3.3 ホホワイトリスト	55
4.3.4 チェックリスト	59
4.4 ウェブ設定	61
4.4.1 保守・状況	62
4.4.2 設定	63
第5章 アンチスパム設定	69
5.1 更新状況	69
5.2 検出状況	70
5.3 メール設定	73
5.3.1 保守・状況	73
5.3.2 設定	74
5.3.3 転送メール設定	80
5.3.4 ホホワイトリスト	82
5.3.5 ブラックリスト	86
5.3.6 チェックリスト	90
第6章 個別設定方法	91
6.1 接続方法	91
6.2 固定IPアドレスの設定	94

目次

6.3 困った時の設定	96
6.3.1 ゲートウェイの設定	96
6.3.2 設定の初期化	96
第7章 トラブルシューティング	97
7.1 動作しないときは	97
7.2 よくある質問と回答	97
7.3 お問い合わせ	99
サポートサービス	100

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

- 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

- POP3でのスパム判定に対応
- スпамメールの転送機能、削除機能
- 日本語スパム対応。スコアリングロジックによるスパム誤検知率の低下
- 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пам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、FTP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)

※以降「ギデオン アンチウイルス BLOC system」を「BLOC」と呼称します。



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。

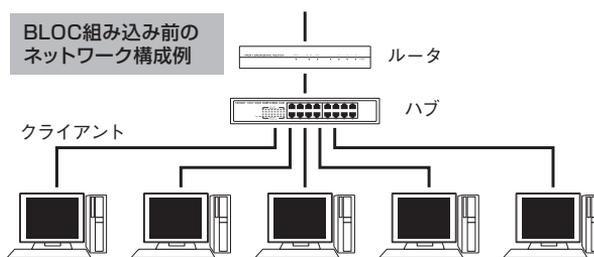


図2.1.1-1

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。

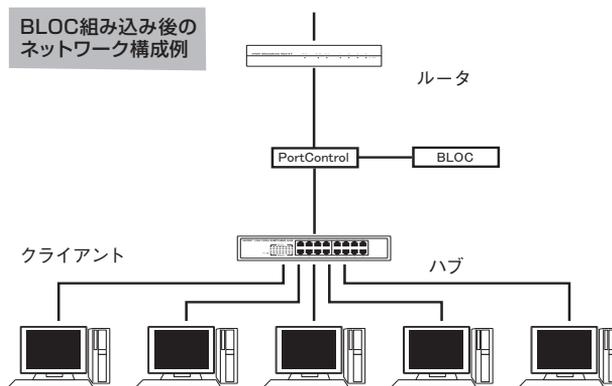


図2.1.1-2

※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。

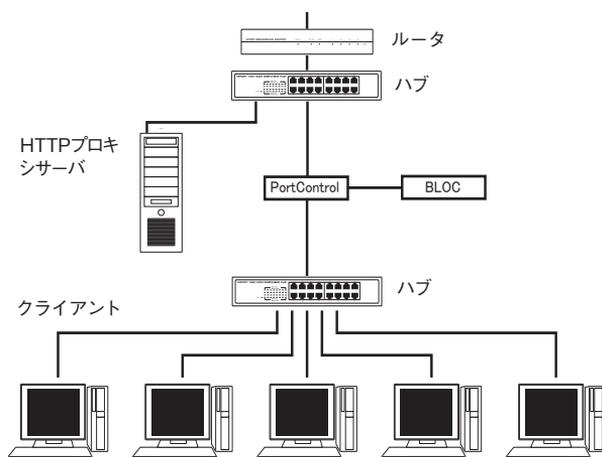


図2.1.2

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。

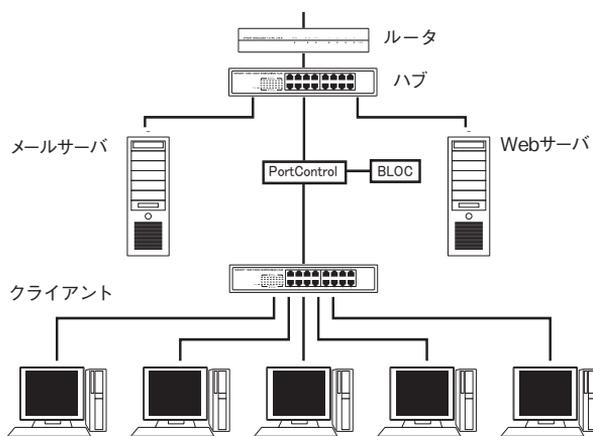
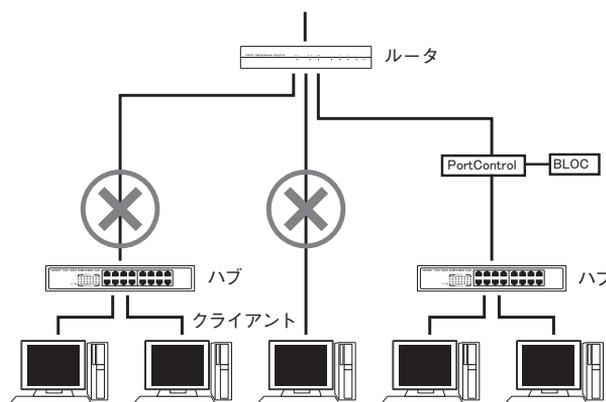


図2.1.3

2.2 BLOCの接続方法についてのご注意

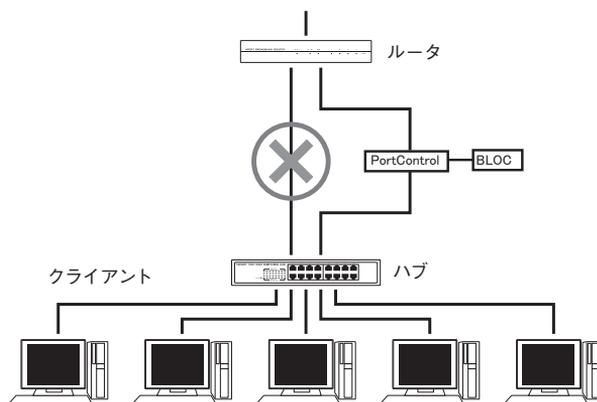
ルータと直結したネットワークの場合

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。



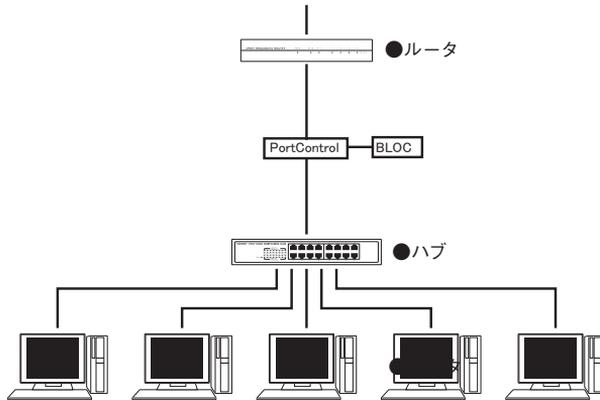
固定IPアドレスを設定している場合

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

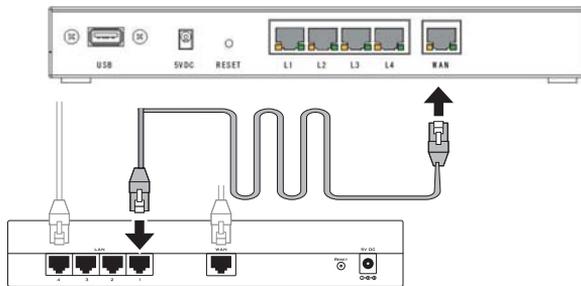


《手順1》 WAN側機器とPortControlの接続

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。

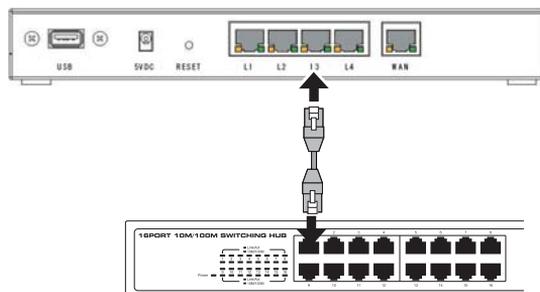
また、WAN側機器とハブを接続しているLANケーブルを取り外します。

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。

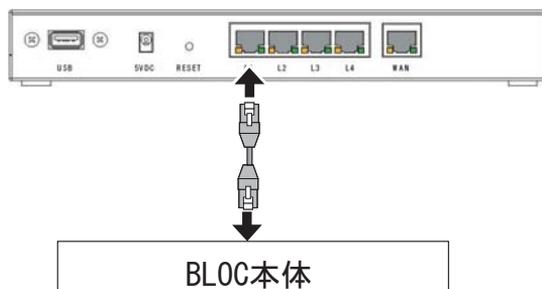


《手順2》 ハブとPortControlの接続

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、ピ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

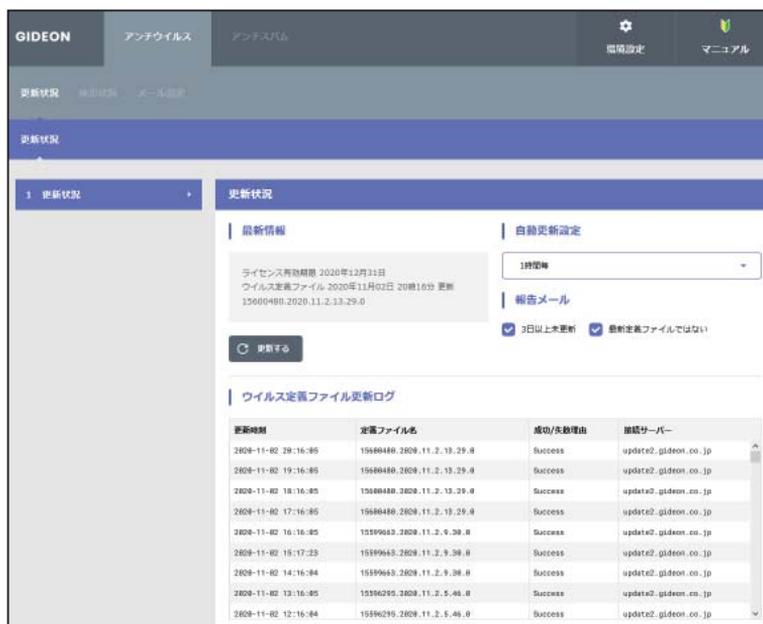
既存のパスワードを入力してログイン画面下部の[パスワードを変更]をクリックすると、画面2.7が表示されますので、この画面上でパスワードを再設定します。(半角英数20文字以内)



画面2.5-2

2.6 管理画面について

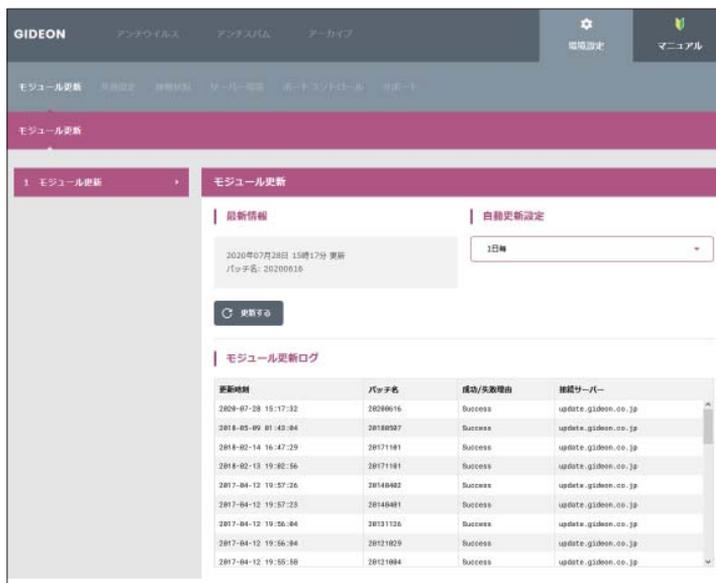
ログインすると、画面2.6が表示されます。管理・設定の方法につきましては後述の章をご参照ください。



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。

管理者のメールアドレス

報告メール

報告メールは、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

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。

警告メールに記入するFROMフィールド

名前部

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、アドレス部には適宜可能なアドレスを記入してください。

<記述例>
名前部：ウイルス対策システム
アドレス部：virus-error@example.com

アドレス部

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プロキシを使用する」を選択してください。

「プロキシの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。

更新環境

更新環境

HTTPプロキシの使用

更新のためにHTTPプロキシを利用する

プロキシのIPアドレス

ポート

ユーザーID

パスワード

更新する

定義ファイルやモジュール等のアップデートにプロキシサーバを使用します。
本サーバーからインターネットにHTTPでアクセスできないが、ネットワーク内にHTTPプロキシサーバが存在する場合には設定してください。設定することで、定義ファイルや更新プログラムが、プロキシ経由でダウンロードされます。多くの場合は、プロキシのIPアドレス、ポートだけの設定で構いません。

<記述例>
プロキシのIPアドレス: proxy.example.com
ポート: 8080

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

第3章 環境設定

●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

システムログ出力指定

自BLOC system

自BLOCに出力する

リモートサーバー

リモートに出力する

リモートサーバーのIPアドレス

更新 テスト

自BLOCに出力する: システムログを自BLOCに出力します。
リモートに出力する: システムログをリモートサーバーに出力します。
※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。

設定ファイルの同期

設定ファイル取得先IPアドレス

自動同期

24時間毎

更新

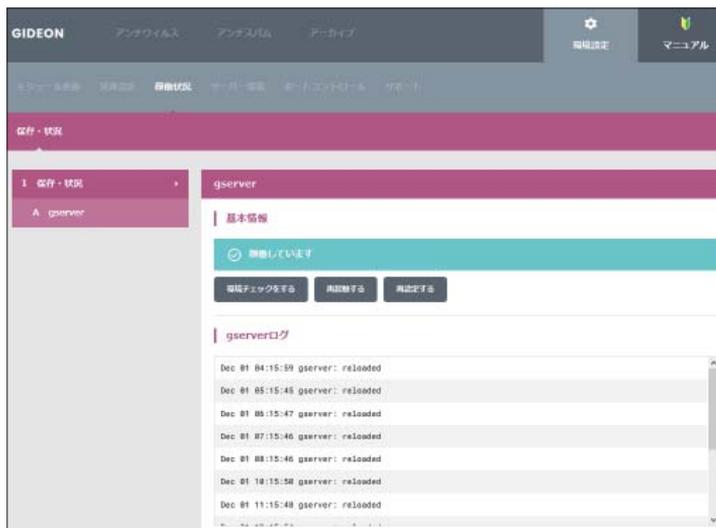
「設定ファイル取得先IPアドレス」で指定したBLOCから「自動同期」で設定した時間ごとに設定ファイルを同期します。

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)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。

サーバ状態

サーバ状態

時刻	2020年 10月 30日 18時 1分
稼働時間	103688711.830000
CPU使用率	0.000000 %

プロセス

合計	138
待機中	137
実行中	1
停止中	0
異常	0

メモリ

物理メモリ合計	4,151,600 K1B
物理メモリ空き	265,552 K1B
仮想メモリ合計	2,096,472 K1B
仮想メモリ空き	2,094,216 K1B

ディスク

マウントディレクトリ	全容量 (K1B)	空き容量 (K1B)
/	101,572,548	4,090,436
/boot	18,277,200	17,271,812
/dev/shm	2,075,848	2,073,704

画面3.1.4.1-2

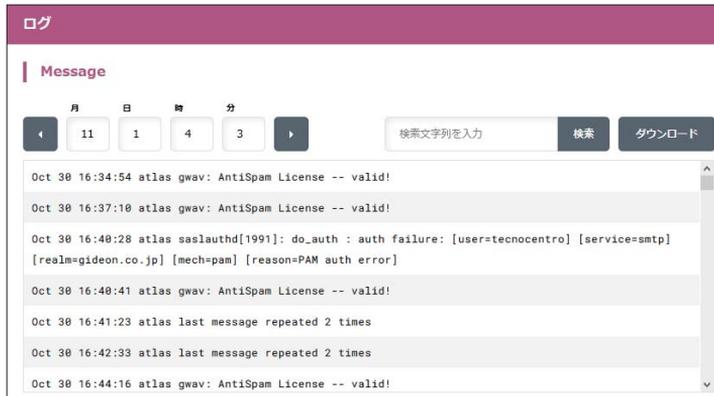
3.1.4.2 ログ

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

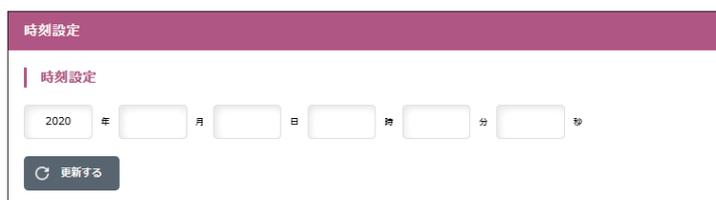
入力後、[更新する]ボタンをクリックしてください。

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。



時刻設定

時刻設定

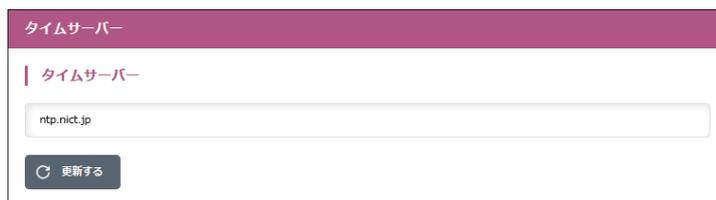
2020 年 月 日 時 分 秒

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



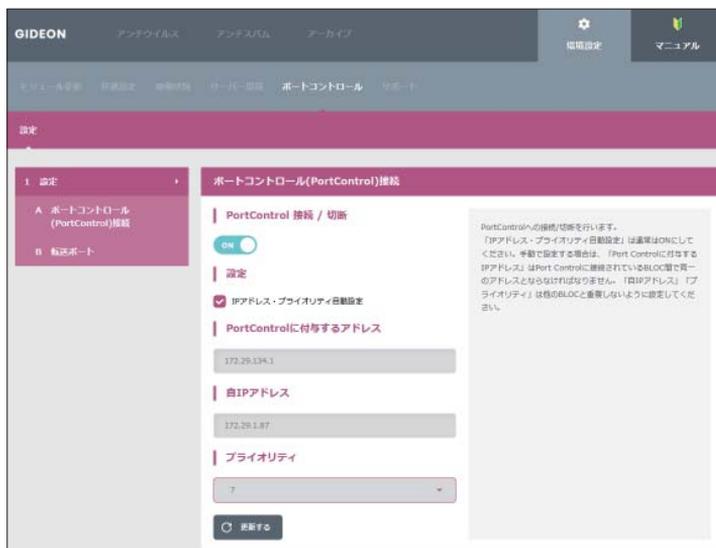
タイムサーバー

タイムサーバー

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PortControl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 packets 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。

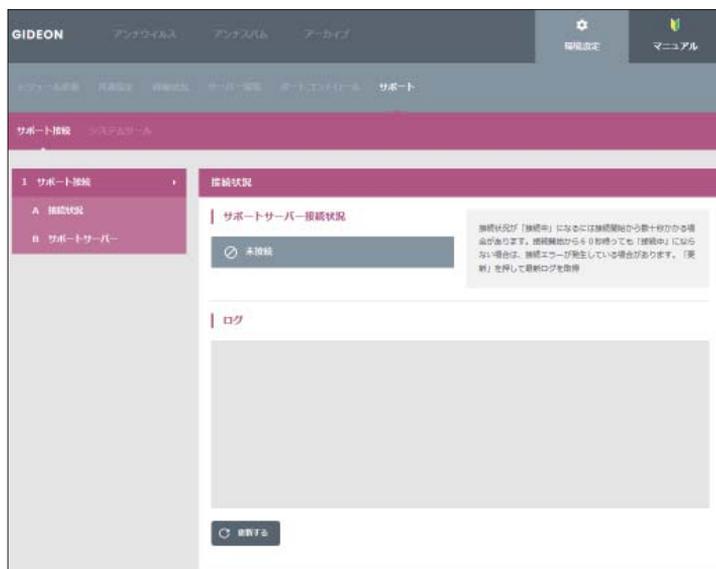
入力後、「更新する」ボタンをクリックしてください。[更新]ボタンをクリックすることで、PortControlは該当ポート番号の packets をBLOCに転送します。

[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进行操作できます。



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。



接続状況

サポートサーバー接続状況

接続中

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。接続開始から60秒待っても「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。「更新」を押して最新ログを取得

ログ

```
Sat Nov 28 12:19:18 2020 OpenVPN 2.1_rc2 i386-redhat-linux-gnu [SSL] [LZO2] [EPOLL] built on Mar 3 2007
Sat Nov 28 12:19:18 2020 WARNING: file '/usr/local/gwaw/vpnclient.key' is group or others accessible
Sat Nov 28 12:19:18 2020 LZO compression initialized
Sat Nov 28 12:19:18 2020 Control Channel MTU parms [ L:1576 D:140 EF:40 EB:0 ET:0 EL:0 ]
Sat Nov 28 12:19:18 2020 Data Channel MTU parms [ L:1576 D:1450 EF:44 EB:135 ET:32 EL:0 AF:3/1 ]
Sat Nov 28 12:19:18 2020 Local Options hash (VER=V4): '31fdf004'
```

更新する

画面3.1.6.1-1

●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があります。

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

サポートサーバー

サーバーホスト名	<input type="text" value="control.gideon.co.jp"/>
ポート	<input type="text" value="443"/>
プロトコル	<input type="text" value="TCP"/>
MTUサイズ	<input type="text" value="1280"/>
ユーザーID	<input type="text"/>
パスワード	<input type="password"/>
HTTPプロキシの使用	<input type="checkbox"/> 外部サーバーへの接続にプロキシを利用する
プロキシのホスト名	<input type="text"/>
ポート	<input type="text"/>
ユーザーID	<input type="text"/>
パスワード	<input type="password"/>

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があります。
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
プロキシ使用時は接続先プロトコルはTCPを指定してください。

画面3.1.6.1-2

3.1.6.2 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3.1.6.2-1

●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3.1.6.2-2

●WHOIS

指定されたドメインのWHOISクエリを行います。

画面3.1.6.2-3

●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。

SSH

SSHサービス 起動 / 停止

ON

アクセス範囲

adminパスワード

※登録されたpasswordは次回表示ときに「*」で表示されます。
passwordを編集したい場合は「*」を消去し、新たなpasswordを入力してください。

更新する

SSHサービスの起動・停止を行います。

< 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

画面3.1.6.2-4

●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。

サポート診断

診断プログラム

実行する

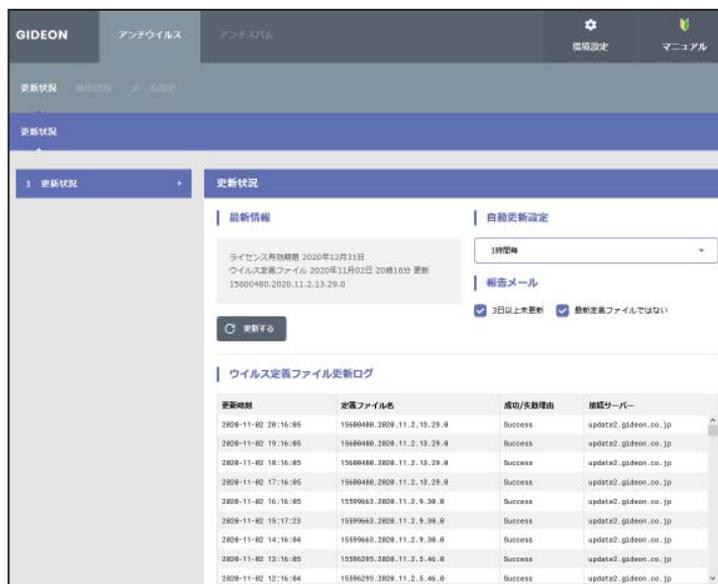
診断プログラムを実行し、結果をサポート宛に送信します。

画面3.1.6.2-5

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。



更新時刻	定義ファイル名	成功/失敗理由	接続サーバー
2020-11-02 20:16:05	15680480.2020.11.2.13.29.0	Success	update2.gideon.co.jp
2020-11-02 19:16:05	15680480.2020.11.2.13.29.0	Success	update2.gideon.co.jp
2020-11-02 18:16:05	15680480.2020.11.2.13.29.0	Success	update2.gideon.co.jp
2020-11-02 17:16:05	15680480.2020.11.2.13.29.0	Success	update2.gideon.co.jp
2020-11-02 16:16:05	15599683.2020.11.2.9.38.0	Success	update2.gideon.co.jp
2020-11-02 15:17:23	15599683.2020.11.2.9.38.0	Success	update2.gideon.co.jp
2020-11-02 14:16:04	15599683.2020.11.2.9.38.0	Success	update2.gideon.co.jp
2020-11-02 13:16:05	15596295.2020.11.2.5.46.0	Success	update2.gideon.co.jp
2020-11-02 12:16:04	15596295.2020.11.2.5.46.0	Success	update2.gideon.co.jp

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

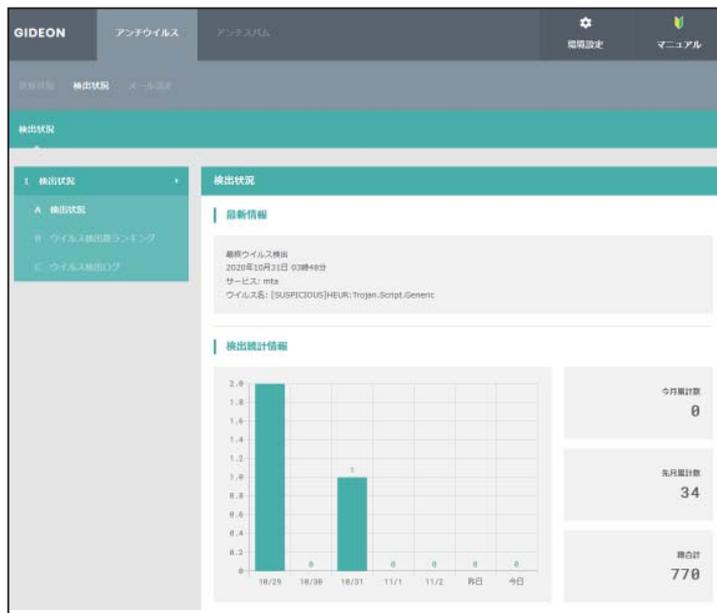
最新のウイルスに対応する、定義ファイルの更新状況を表示します。

[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。

ウイルス検出数ランキング					
11月 (今月)			10月 (先月)		
順位	ウイルス名	検出数	順位	ウイルス名	検出数
1位	なし	0	1位	[SUSPICIOUS]HEUR:Exploit.MSOffice.Generic	12
2位	なし	0	2位	[SUSPICIOUS]HEUR:Trojan.Script.Generic	7
3位	なし	0	3位	[SUSPICIOUS]HEUR:Trojan-PSW.MSIL.Agensla.gen	6
総合					
順位	ウイルス名	検出数			
1位	[SUSPICIOUS]HEUR:Trojan-Downloader.Script.Generic	290			
2位	[SUSPICIOUS]HEUR:Exploit.MSOffice.Generic	192			
3位	[SUSPICIOUS]HEUR:Trojan-PSW.MSIL.Agensla.gen	32			
<input type="button" value="月次詳細"/>					

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。

検出ログ					
<input type="button" value="全表示"/> <input type="button" value="検索"/> <input type="button" value="ダウンロード"/>					
検出日時	サービス	ウイルス名	From	To	
2020-10-31 03:48:06	mta	[SUSPICIOUS] HEUR: Trojan.Script.Generic	TrackingUpdates@fedex.com	nishio@gideon.co.jp	↑
2020-10-29 10:55:54	mta	[SUSPICIOUS] HEUR: Trojan-PSW.MSIL.Agensla.gen	store@mitavalves.com	sp@gideon.co.jp	
2020-10-29 08:20:44	mta	[SUSPICIOUS] HEUR: Trojan-PSW.MSIL.Agensla.gen	store@mitavalves.com	info@gideon.co.jp	

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のようなウィ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

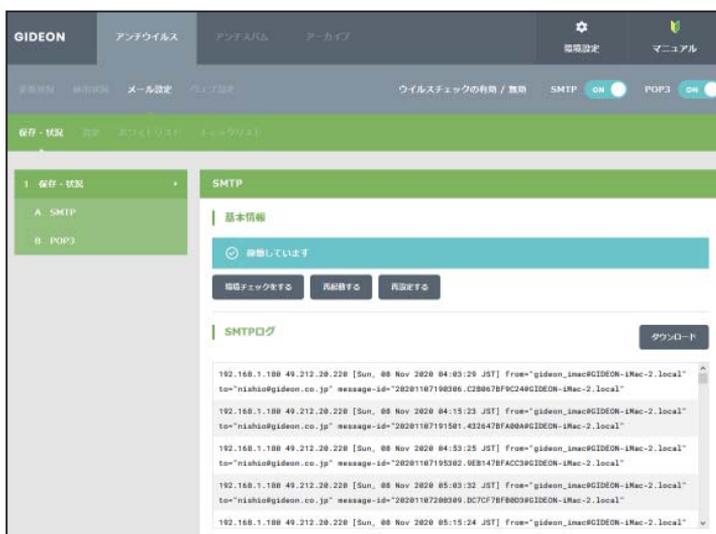
管理・設定画面の「メール設定」タブをクリックすると、画面4.3が表示されます。

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。

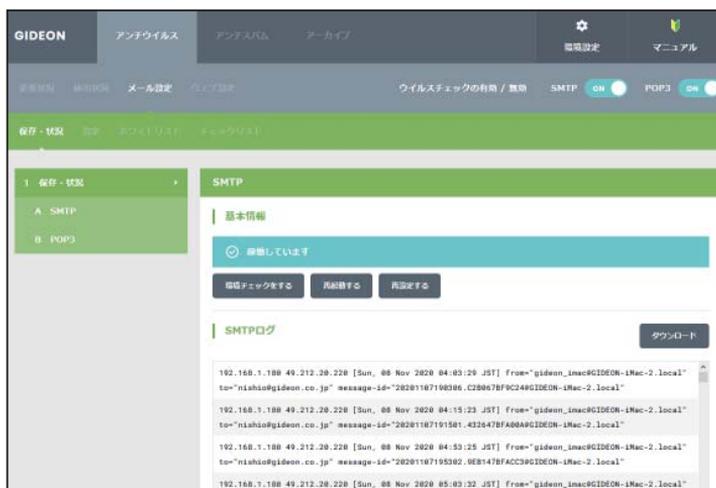


画面4.3

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

第4章 アンチウイルス設定

●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)
<code>__SUBJECT__</code>	: 感染メールSubjectを表示します。
<code>__VIRUS_SENDER__</code>	: 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。
<code>__MESSAGE_ID__</code>	: 感染メールMessage-Idを表示します。
<code>__MESSAGE_HEADER__</code>	: 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。

受信者への警告メール設定

警告設定

- 感染メールの場合、警告をつけて送信する
- 感染メールの場合、警告をつけて送信しない

挙動

警告メールに感染メールのヘッダーを添付する

Subject

Virus warning:

- 感染メールの場合、Subjectをつける
- 感染メールの場合、Subjectをつけない

本文

* ウイルス警告! *

このメールは、ウイルスチェックプログラムにより自動送信されております。

あなた宛てにウイルスに感染したファイルを含むEメールが送られました。送信者は__VIRUS_SENDER__で、オリジナルタイトルは__SUBJECT__です。

添付書類の内容は、破棄されました。

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)

更新する

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。

送信者への警告メール設定

警告設定

送信者に警告メールを送信する

送信者に警告メールを送信しない (推奨)

Subject

感染メールの場合、Subjectをつける

感染メールの場合、Subjectをつけない

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
ウイルスに感染していました。

以下のウイルスを削除しました。

更新する

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

画面4.3.2-2

第4章 アンチウイルス設定

●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。

管理者への警告メール設定

警告設定

管理者に警告メールを送信する

管理者に警告メールを送信しない

Subject

Virus warning:

感染メールの場合、Subjectをつける

感染メールの場合、Subjectをつけない

本文

***** ウィルスを検出しました *****

送信者: __VIRUS_SENDER__

受信者: __VIRUS_RECEIVER__

以下のウィルスを削除しました。

MessageID: __MESSAGE_ID__

Header: __MESSAGE_HEADER__

更新する

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

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

第4章 アンチウイルス設定

● 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も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)

最大ファイルサイズ

SMTP

100000 MByte

POP3

100000 MByte

更新する

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。

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』

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

更新する

「最大ファイルサイズ」を超えた時の処理の選択です。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。

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。

送信元IPアドレスの復元

SMTP

復元する

POP3

復元する

更新する

復元する事により完全な透過を実現します。問題がない限りは復元するを選択してください。

画面4.3.2-11

第4章 アンチウイルス設定

●ウイルス感染メールの保存

BLOCでは使用できません。

●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。



The screenshot shows a web interface for setting the 'Error return value for AntiVirus engine not treated as error'. The title bar is green and contains the text 'エラーとして扱わないAntiVirusエンジンの戻り値'. Below the title bar, there is a label 'エラーとして扱わないAntiVirusエンジンの戻り値' and a text input field. To the right of the input field, there is a note: 'ある特定の警告エラーなどを送信しないために記述します。'. At the bottom left of the form, there is a button labeled '更新する' (Update) with a refresh icon.

画面4.3.2-12

●感染メール保存ディレクトリ

BLOCでは使用できません。

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

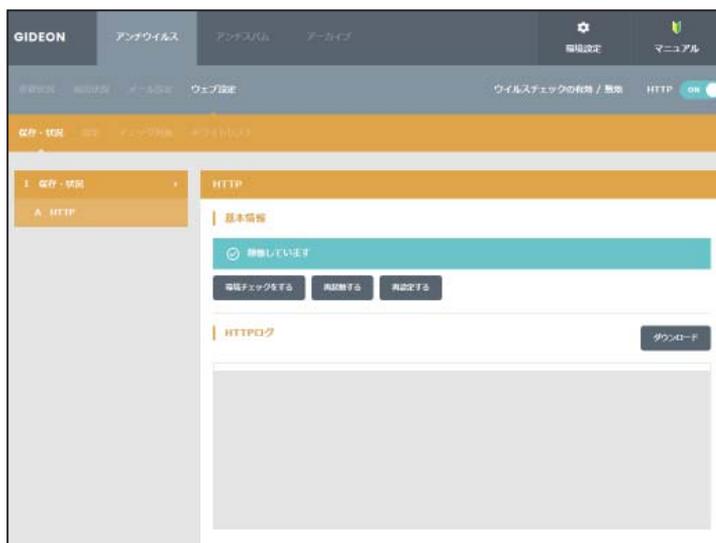
@192.168.1.1

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。

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。

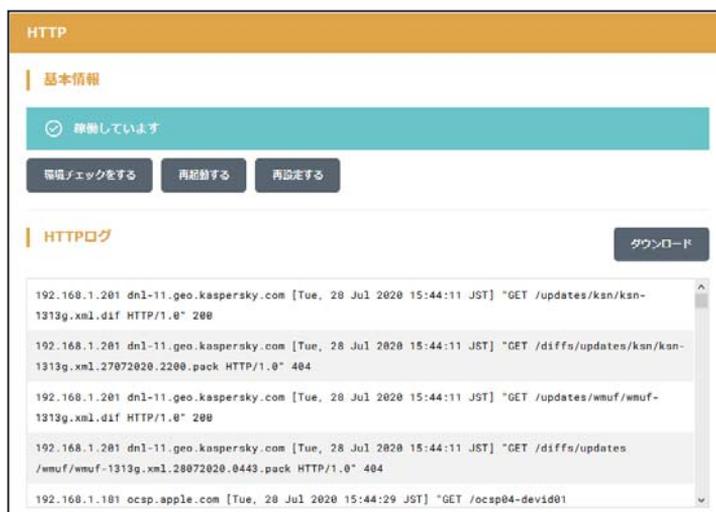


画面4.4

4.4.1 保守・状況

ウェブ(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

ウェブ設定画面の「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。



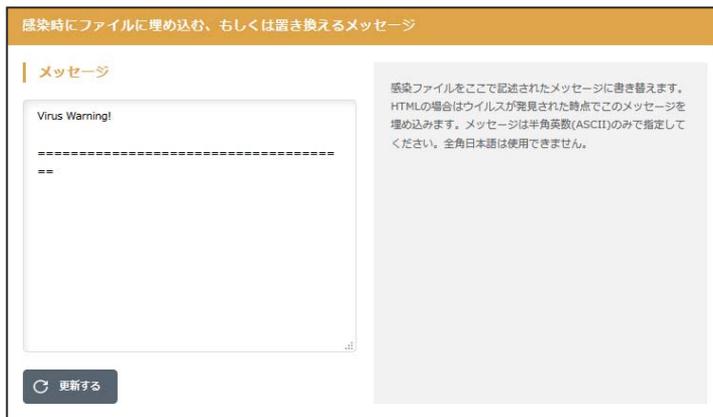
画面4.4.2-2

●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

第4章 アンチウイルス設定

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も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。

The screenshot shows a configuration page titled "待機数を超えた場合の接続増加数" (Number of connections to increase when the number of waiting connections is exceeded). Under the "HTTP" section, there is a text input field containing the value "50". Below the input field is a button labeled "更新する" (Update) with a refresh icon. To the right of the input field is a grey informational box containing the text: "現在の接続待機数を超えた時、追加する待機数です。" (This is the number of waiting connections to be added when the current number of waiting connections is exceeded).

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。

The screenshot shows a configuration page titled "ダウンロードの最大ファイルサイズ" (Maximum download file size). Under the "HTTP" section, there is a text input field containing the value "10", followed by the unit "Mbyte". Below the input field is a button labeled "更新する" (Update) with a refresh icon. To the right of the input field is a grey informational box containing the text: "ウイルスチェックするダウンロードファイルの最大サイズです。このサイズ以内のファイルについてウイルスチェックします。" (This is the maximum size of the download file to be checked for viruses. We will check for viruses on files within this size).

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。

The screenshot shows a configuration page titled "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" (Action when maximum download file size is exceeded). Under the "HTTP" section, there is a dropdown menu with "通過" (Pass) selected. Below the dropdown menu is a button labeled "更新する" (Update) with a refresh icon. To the right of the dropdown menu is a grey informational box containing the text: "「最大ファイルサイズ」を超えた時の処理の選択です。エラー停止の場合はダウンロードを停止します。" (This is the selection of the action when the maximum file size is exceeded. In the case of error stop, the download will be stopped).

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。

第4章 アンチウイルス設定

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

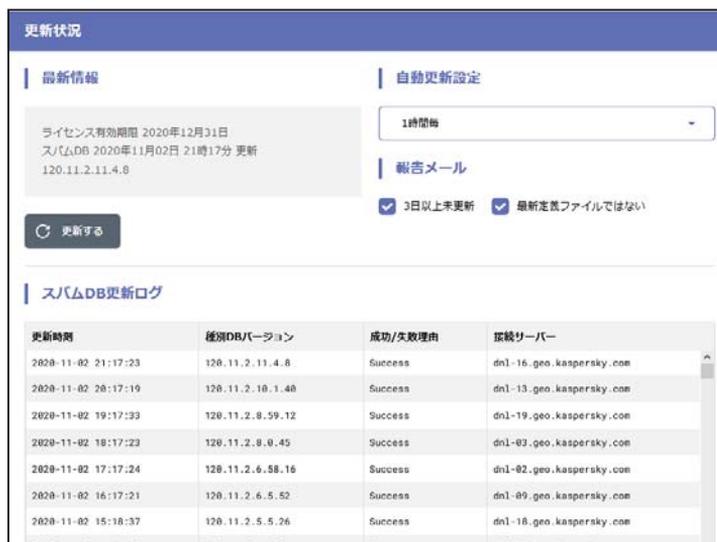
●ウイルス感染ファイルの保存

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。



The screenshot displays the '更新状況' (Update Status) page. It includes a '最新情報' (Latest Information) section with license expiration and update details, an '自動更新設定' (Automatic Update Settings) section with a dropdown menu set to '1時間毎' (Every 1 hour) and checkboxes for '3日以上未更新' and '最新定義ファイルではない', and a 'スパムDB更新ログ' (Spam DB Update Log) table.

更新時刻	種別DBバージョン	成功/失敗理由	接続サーバー
2020-11-02 21:17:23	120.11.2.11.4.8	Success	dn1-16.geo.kaspersky.com
2020-11-02 20:17:19	120.11.2.10.1.40	Success	dn1-13.geo.kaspersky.com
2020-11-02 19:17:33	120.11.2.8.59.12	Success	dn1-19.geo.kaspersky.com
2020-11-02 18:17:23	120.11.2.8.0.45	Success	dn1-03.geo.kaspersky.com
2020-11-02 17:17:24	120.11.2.6.58.16	Success	dn1-02.geo.kaspersky.com
2020-11-02 16:17:21	120.11.2.6.5.52	Success	dn1-09.geo.kaspersky.com
2020-11-02 15:18:37	120.11.2.5.5.26	Success	dn1-18.geo.kaspersky.com

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。

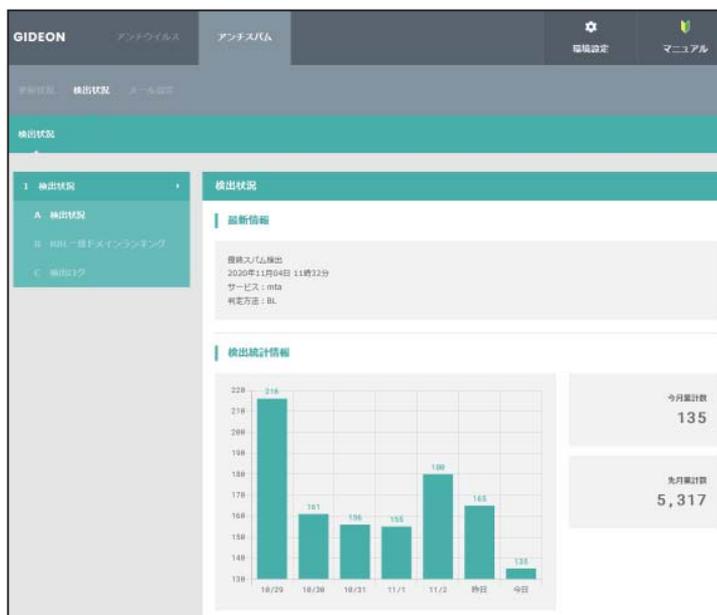
5.2 検出状況

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。

RBL一致ドメインランキング					
11月 (今月)			10月 (先月)		
順位	RBL一致ドメイン	検出数	順位	RBL一致ドメイン	検出数
1位	fastwelnesstrade.su	9	1位	127.0.0.1	72
2位	nollerschluht.de	2	2位	tokomachiko.com	42
3位	newaidssist.com	1	3位	wakocobi.com	38

総合		
順位	RBL一致ドメイン	検出数
1位	fastwelnesstrade.su	9
2位	nollerschluht.de	2
3位	newaidssist.com	1

[月次詳細]

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。

GIDEON ×

11月 ← 2020年 ←

RBL一致ドメイン	検出数
fastwelnesstrade.su	9
practise-information.com	1
iphove3026.net	1
2biamp.com	1

[管理者に結果を送信する]
[キャンセル]

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。

検出ログ

検出ログ

全表示 検索 ダウンロード

検出日時	サービス	判定	スコア	サブジェクト	From	To
2020-11-02 21:39:44	nta	KAS	3	Take Advantage Of Fall Savings With Renewal By Andersen	renewal.by.andersen.offer-nishio@gideon.co.jp@bridgefs.casa	nishio@gideon.co.jp
2020-11-02 21:21:58	nta	R1 KAS	6	当選権利を活かして最大月収1000万円を手に入れろ!	rtuomsherr56195s929@tokomachi.ku.com	yukari@gideon.co.jp

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。

GIDEON

検索する検出日の範囲

サービス名

判別方法

スコア

サブジェクト

From

To

クリア

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。

GIDEON

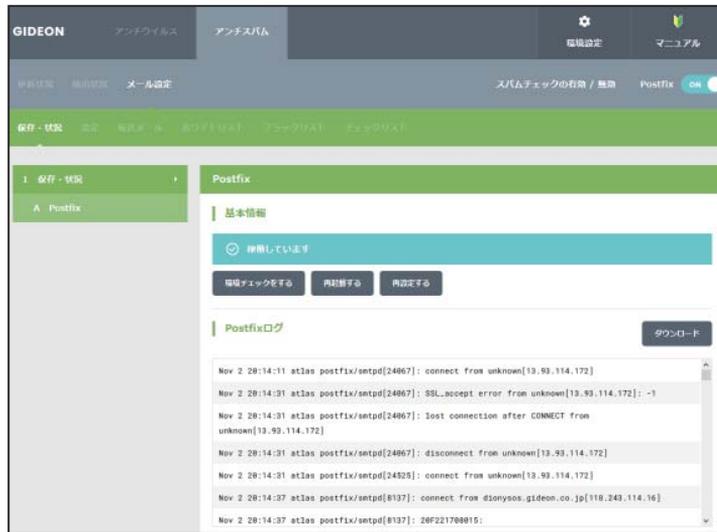
検出ログのダウンロード

サービス	ファイル名	サイズ(byte)	最終更新日時
nta	nta-spam.csv	489,433	2020-10-30 14:26:21
nta	nta-spam_1.csv	656,896	2020-10-25 03:40:24
nta	nta-spam_2.csv	592,332	2020-10-18 03:49:32
nta	nta-spam_3.csv	560,593	2020-10-11 04:01:36
nta	nta-spam_4.csv	632,402	2020-10-04 04:00:58
nta	nta-spam_5.csv	554,631	2020-09-27 03:53:30
nta	nta-spam_6.csv	717,315	2020-09-20 03:49:56
nta	nta-spam_7.csv	993,294	2020-09-13 03:54:56
nta	nta-spam_8.csv	1,069,182	2020-09-06 03:58:58

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)

第5章 アンチスパム設定

- ・ 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」で設定したものに更新されます。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えます。

・ 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。

スパム判定基準

スパム判定設定

推奨設定を使用する
 カスタマイズを使用する

判定方法

ID	判定方法	スコア
BL	ユーザー定義ブラックリスト	4
XS	URLフィルタリング	3
R1	RBL(リアルタイムブラックリスト)	3
S25	発信元チェック	1
RES	逆引きチェック	1
KAS	データベース	3

アクション

判定方法	総合スコア
何もしない	0
Subject変更	3
MTA受信拒否	98

追加ヘッダ

判定方法	総合スコア
X-Spam-Status : NONE	0
X-Spam-Status : SUSPICION	1
X-Spam-Status : SPAM	4

更新する

※カスタマイズを利用する場合は設定項目に注意して行ってください

■判定方法について

- ・ BL: 「ブラックリスト」で指定した項目に一致したメール。高スコア推奨
- ・ XS: メール本文中に記載されたドメインのRBLチェック。高スコア推奨
- ・ R1: 接続元のIPアドレスのRBLチェック。高スコア推奨
- ・ S25: Receivedに記載された命名規則の形式チェック。低スコア推奨
- ・ RES: 逆引きチェック。低スコア推奨
- ・ KAS: DBを利用したスパム判定。中～高スコア推奨

アクション

スコア合計が、設定した総合スコア以上になったときに適用されます。

Subject変更: 「スパムと判定した場合のSubject」に変更POP3のみ本文変更: 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わるSMTP/MTA受信拒否: メールが受信拒否される

追加ヘッダ

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メールヘッダに追加します。

画面5.3.2-2

第5章 アンチスパム設定

● 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。

キャッシュ制御

逆引きキャッシュ

保存期間 時間

RBLキャッシュ

保存期間 時間

更新する キャッシュクリア

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。
保存期間: 追加されたキャッシュ項目の有効時間

画面5.3.2-3

● スпам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、以下のように入ります。

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、以下のように入ります。

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、以下のように入ります。

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

----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: エンベロップのFromメールアドレス

envelope-to: エンベロップの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: エンベロップのFromメールアドレス

envelope-to: エンベロップの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、@DOMAIN 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、@DOMAIN 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 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6.1-1 のようにキーボードを接続します。モニターは図6.1-2のように接続します。

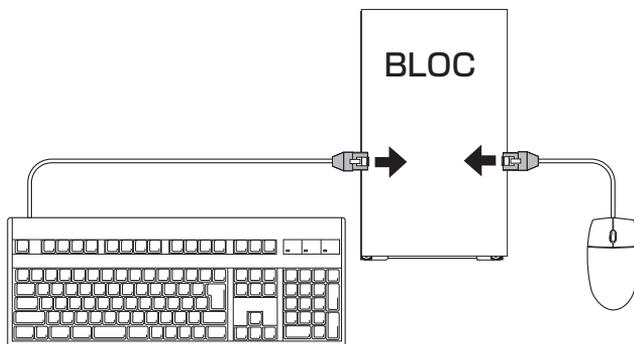


図6.1-1

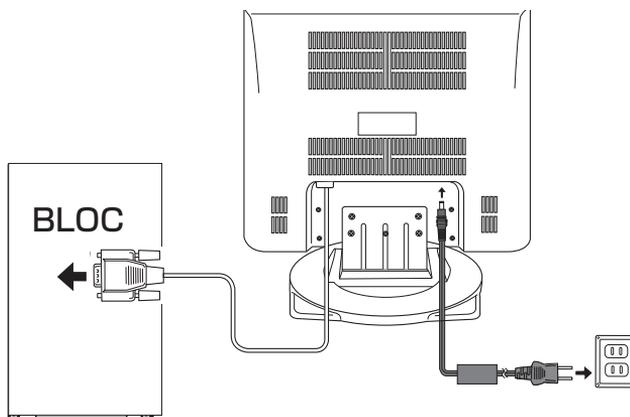


図6.1-2

② BLOC本体の電源を入れます。

第6章 個別設定方法

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6.1-3が表示されます。

```
*****
Gideon Antivirus BLOC System基本設定
キー)   メインメニュー
-----
a) 現在の設定を見る
b) 設定変更する
c) アップデートする
r) 障害復旧
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6.1-3

「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)。

6.2 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6.1-3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6.2-1

画面6.2-1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6.2-2

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6.1-3 「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。

6.3 困った時の設定

6.3.1 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かか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6.1-3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。

6.3.2 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。

7.1 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。

7.2 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(コンテンツフィルタリング)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 system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ください。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。

第7章 トラブルシューティング

株式会社ギデオンインフォ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」が存在する場合がありますが、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。

7.3 お問い合わせ

製品に関するお問い合わせは、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)

「ギデオンの BLOC system PortControl Plus」
ユーザーズマニュアル

2020年12月1日 第13刷

発行所 株式会社ギデオンの
〒223-0056 神奈川県横浜市港北区新吉田町3382-7
<http://www.gideon.co.jp/>

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

Copyright(c)2020 GIDEON Inc
Printed in Japan