ギデオン アンチウイルス GIDEON ブロック システム

ギデオン アンチウイルス BLOC system

ギデオン アンチウイルス BLOC system アンチスパムPlus

共通ユーザーズマニュアル

2008年10月20日 第10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 アンチウイルス BLOC system」および「ギデオン アンチウイルス BLOC system ア ンチスパムPlus」各製品共通ユーザーズマニュアルです。

本書「第4章 アンチスパム設定」は、アンチスパムPlusのみ該当する内容となっており、その他の 項目はすべて共通の内容となります。

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

■著作権など

本ユーザズマニュアルの著作権は株式会社ギデオンに帰属します。

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

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

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

その他、記載されている会社名、製品名は各社の商標および登録商標です。

目次

目次
ご注意
梱包内容の確認
笠1音 制只のご紹介
第1早 表面のと和月
第2章 BLOCの接続と動作
2.1 BLOCの接続方法について
2.1.1 シンプルなLAN構成
2.1.2 LAN側にプロキシなどがある場合
2.1.3 LAN側にメールサーバなどがある場合
2.2 BLOCの接続方法についてのご注意
2.3 BLOCの接続とセットアップ
2.3.1 インターネット接続を停止させないセットアップ
2.3.2 インターネット接続を一時的に停止してセットアップ
2.4 外部インターネット接続確認と動作検証
2.5 管理・設定画面のアクセス方法
26初回のログイン
2.8 官理画面について
第3章 アンチウイルス設定
2.1 更新代记
3.1 史利仪儿 23
3.2 検出状況
3.2 検出状況 ····································
3.2 検出状況······23 3.3 共通設定······25 3.3.1 基本設定······25
3.1 更新次況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27
3.1 更新认为 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28
 3.1 更新状況 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33
3.1 受新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35
3.1 受新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37
3.1 受新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40
3.1 受新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44 3.5.4 詳細設定2 44
3.1 受新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44 3.5.4 詳細設定2 44 3.5.5 チェック対象 48 3.5.7 エック対象 48
3.1 受新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44 3.5.4 詳細設定2 44 3.5.5 チェック対象 48 3.5.6 ホワイトリスト 49 3.5.7 単細設定1 48 3.5.6 ホワイトリスト 49 3.5.7 単細設定1 44 3.5.6 ホワイトリスト 49 3.5.7 単和設定1 44 3.5.6 ホワイトリスト 49 3.5.6 ホワイトリスト
3.1 更新秋光 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44 3.5.4 詳細設定2 46 3.5.5 チェック対象 48 3.5.6 ホワイトリスト 49 3.6.74 評細設定2 48 3.5.6 ホワイトリスト 49 3.6 スキャンコード一覧 51
3.1 更新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 27 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44 3.5.4 詳細設定2 44 3.5.5 チェックリスト 49 3.5.6 ホワイトリスト 49 3.5.6 ホワイトリスト 49 3.5.6 ホワイトリスト 49 3.6 スキャンコードー覧 51 第4章 アンチスパム設定 53
3.1 と新状況 23 3.2 検出状況 24 3.3 共通設定 25 3.3.1 基本設定 25 3.3.2 詳細設定 25 3.3.3 更新環境設定 28 3.4 メール設定 29 3.4.1 保守・状況 30 3.4.2 基本設定 31 3.4.3 詳細設定1 33 3.4.4 詳細設定2 35 3.4.5 ホワイトリスト 37 3.4.6 チェックリスト 39 3.5 ウェブ設定 40 3.5.1 保守・状況 41 3.5.2 基本設定 42 3.5.3 詳細設定1 44 3.5.4 詳細設定2 46 3.5.5 チェック対象 48 3.5.6 ホワイトリスト 49 3.6 スキャンコード一覧 51 第4章 アンチスパム設定 53 4.1 更新状況 53

4.3 共通設定
4.4 メール設定
4.4.1 保守 · 状況
4.4.2 基本設定
4.4.3 詳細設定1
4.4.4 詳細設定2
4.4.5 転送メール 67
4.4.6 ホワイトリスト・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
4.4.7 ブラックリスト・・・・・ 71
4.4.8 チェックリスト・・・・・・ 73
第5章 他サービス
51 他サービス
511保守, 护湿
5.1.2 基本設定
513 ホワイトリスト···································
第6章 サーバ環境
6.1 サーバ環境
6.1.1 保守・状況
6.1.2 ログ
6.1.3 基本設定
第7章 サポートツール
7.1 メールテストツール
7.7 サポート 焼結ツール 87
第8章 個別設定方法
8.1 接続方法
8.2 固定IPアドレスの設定 ······92
83 困った時の設定
8.3.1 ジートジェイの設定 8.3.2 設定の初期化 94
第9章 トラブルシューティング
9.1 動作しないときは
9.2 よくある質問と回答
9.3 お問い合わせ
サボートサービス

ご注意

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

取扱い上のご注意

■本製品を正しく安全に使用するために

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

梱包内容の確認

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

- BLOC 本体
- 電源コード
- ブロック システム ユーザーズマニュアル(本書)
- ハードウェア取扱い説明書
- ソフトウェア使用許諾書
- 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

■ 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
- スパムメールの転送機能、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、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。



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BLOC 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 BLOC を経由することができま す。





※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、BLOC 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BLOC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。



BLOC system

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、BLOC を経由せずバイパスで接続した場合、正常にネットワークのウイ ルス対策 (スパム対策)をすることができません。



固定IPアドレスを設定している場合

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

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、BLOU 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

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

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

2.3.1 インターネット接続を停止させないセットアップ

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

●セットアップに必要なもの BLOC 本体、ハブ、クライアントPC、LAN ケーブル 2本



《手順1》 ルータと接続

BLOC のLAN コネクタとルータのLAN コネクタを接続します。 ※BLOC のLAN ボードは、1Gbps/100Mbps/10Mbps を自動認識します。LAN ケーブルが正しく 接続されると、LAN コネクタが点灯します。



BLOC system

《手順2》 ハブと接続

1. BLOCのもう一方のLANコネクタとハブのLANコネクタを接続します。

2. クライアントを、既存ネットワークのハブからセットアップ用ハブに差し替えて接続します。



《手順3》 電源コードの接続

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



《手順4》 電源をON

接続が全て終了したら、BLOCの電源を入れます。

《手順5》 ネットワーク構成の変更

セットアップが終了したら、ネットワークの構成を変更します。

- 1.BLOCに接続しているセットアップ用ハブのLANコネクタを、既存ネットワークハブのLANコネクタに 差し替えます。
- 2. ルータと、既存ネットワークのハブとを接続しているLANケーブルを取り外します。
- 3. セットアップ用ハブに接続しているクライアントを、既存ネットワークハブのLANコネクタに差し替えま す。
- ネットワークの構成変更が終了したらセットアップ完了です。



BLOC system

2.3.2 インターネット接続を一時的に停止してセットアップ

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

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



《手順1》 ルータと接続

BLOCのLANコネクタとルータのLANコネクタを接続します。 また、ルータ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》 ハブと接続

BLOCのもう一方のLANコネクタとハブのLANコネクタを接続します。



《手順3》 電源コードの接続

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



《手順4》 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インターネットと接続が可能になります。

2.4 外部インターネット接続確認と動作検証

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

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

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

ABOUT US CONFERENCE TASK FORCES PRESS CONTACT INFORMAT Second Texture Textur	re Testfile by FreeFind TION
ADDUT US CONFERENCE TASK FORCES PRESS CONTACT INFORMAT access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantaine. The lest file will be treated justilike any other real virus infected file. Read the user's manual of Your X's canner what do do croatact the endormanual/duriter of your AV scanner in combination with these files	re Testfile by FreeFind TION
SEARCH Powered I ABOUT US CONFERENCE TASK FORCES PRES CONTACT INFORMAT access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantaine. The lest file will be treaded just like any other real virus infected file. Read the user's manual of Your XV scanner. Important note: EICAR cannot be held responsible when these files or your AV scanner in combination with these files	by FreeFind
ABOUT US CONFERENCE TASK FORCES PRESS CONTACT INFORMAT access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantaine. The test file will be treated just like any other real virus infected file. Read the user's manual of your AY scanner what to do or contact the vendorimmundaturer of your AY scanner. Important note: EICAR cannot be held responsible when these files or your AY scanner in combination with these files	TION
access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantane. The test file will be treated justike any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendorimanufacturer of your AV scanner. Important note: EICAR cannot be held responsible when these files or your AV scanner in combination with these files	
access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantaine. The test file will be theated justike any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner. Important note: EICAR cannot be held responsible when these files or your AV scanner in combination with these files	
your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help. Download area using the standard protocol http elcar.com elcar.com tot elcar.com tot 68 Bytes 18 A Bytes 308 Bytes	
Download area using the secure, SSL enabled protocol https	
(Note: For the time being we make use of a self-signed certificate. You may be asked by your browser whether you trust this site. Depending on acceptance of this new service we may install a certificate coming from a trusted Certificate Authority at a site provint in the prov	
eicar.com eicar.com.bt eicar.com.zip eicarcom.2.zip	

画面2.4-1

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



画面2.4-2

2.5 管理・設定画面のアクセス方法

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

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

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

http://192.168.1.100:777/

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

https://192.168.1.100:999/

※WEBブラウザの設定で、上記のポート番号を許可するようにしてください。



画面2.5-1





2.6 初回のログイン

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

次回からログインするときには、このパスワードを入力する必要があります。



画面2.6

2.7 ログイン

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

パスワードの変更

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



画面2.7

2.8 管理画面について

ログインすると、画面2.8 管理・設定画面が表示されます。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2.8

■主に日常の管理で必要なメニュー

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

■初期に設定および確認するメニュー

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

BLOC system

3.1 更新状況

●ウイルス定義ファイル更新ログ(画面3.1 上段部分)

ウイルス定義ファイルの更新状況を表示します。

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

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

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

●モジュール更新ログ(画面3.1下段部分)

各モジュール(修正パッチモジュール、アップデートモジュールなど)の更新状況を表示します。 初期設定では1日1回の自動更新に設定されています。緊急対策が必要な場合は[手動更新]ボタン をクリックし、最新のモジュールを取得してください。 ※既に更新済みの場合は、新たに更新されません。

[不具合状況]ボタンをクリックすると、モジュールの不具合などに関する情報サイトを表示します。 各タブ(AntiVirus、透過プロキシー、GUI)をクリックすることでモジュールそれぞれの更新状況が表示されます(「MTAアドオン」はBLOCでは使用されません)。

アンチウイルス アンチスパム				サポー
GIDEON Antil/irus	更新状況 検出	状況 共通設	定メール設定	▶ サーバ環境 ウェブ設定 他サービス
史和4000	ウイルス定義ファイル更新	前ログ		
1172048520	更新時刻	定義ファイル名	成功/失敗理由	接続サーバー
	2007-02-21 15:10	1172048520	Success	dnl-jp1.kaspersky-labs.com
▶于副更新	2007-02-21 13:28	1172042400	Success	dnl-jp4.kaspersky-labs.com
 自動更新 18時間毎 	2007-02-08 11:11	1170910560	Success	dnl-jp1.kaspersky-labs.com
● 報告メール				
☑3日以上未更新				
□最新定義ファイルでない				
A STRATE				
► XSXD4X.0C*				
► XYASACAT∧	モジュール共通 Antily		オン 漫過プロキシー	GII
	モジュール共通 AntiV	irus MTA7H	オン 透過プロキシー	GUI
モジュール共通	モジュール共活 Antiv	irus MTA7P	オン 透過プロキシー	- GUI
モジュール共通 2007年02月01日更新 Kief 2::0007001	モジュール共通 AntiV モジュール更新ログ	irus MTAアド	オン 透過プロキシー	GUI
モジュール共通 2007年02月01日更新 パッチ名:20070201	 モジュール共通 AntiV モジュール更新ログ 更新時刻 	irus MTAアド パッチ名	オン 通道プロキシー 成功/失敗理由	GUI
	 モジュール共通 AntiV モジュール更新ログ 更新時刻 2007-02-01 00:00 	irus MTAアド パッチ名 20070201	オン 透過プロキシー 成功/失敗理由 Success	GUI 相応サーバー ns3gideoncojo
ビリコール共通	 モジュール共活 AntiV モジュール更新ログ 更新時刻 2007-02-01 00:00 2006-10-13 00:00 	irus MTAアド パッチ名 20070201 20061011	オン 透過プロキシー 成功/失敗理由 Success Success	GUI 接続サーバー nSgidencojp nSgidencojp
ビジュール共通 CO07年02月01日更新 バッチ会:20070201 チョンを 日間数更新 1日毎 ・	モジュール共活 AntiV モジュール更新ログ 更新計約 2007-02-01 00:00 2006-10-13 00:00	irus MTAアド パッチ名 20070201 20061011	オン 参週プロキシー 成功/失敗理由 Success Success	GUI 指続サーバー ns3grideencojo ns3grideencojo
	モジュール共著 AndW モジュール更新ログ 更新特別 2007-02-01 00:00 2006-10-13 00:00	irus MTAアド パッチ名 20070201 20061011	オン 参選プロキシー	GUI 1般後サーバー ns3 tideonco jp ns3 tideonco jp
	モジュール共選 AntiV モジュール更新ログ 更新430 2007-02-01 00:00 2006-10-13 00:00	itus / MTA7 H //9 5-8 20070201 20061011	オン あ び 功 / 大 数 理 由 Success Success	GUI 18底サーバー ns3grideoncojo ns3grideoncojo
* 7420人で * 7420月0日夏新 //5/考:2007年02月0日夏新 //5/考:2007201 * 手覧更新 ・ 目動更新 1日春 ・ ・ 木属会校派	モジュール共選 AntiV モジュール更新ログ 更新時急! 2007-02-01 00:00 2006-10-13 00:00	ius // MTA7H //5 7-8 20070201 20061011	オン 意識プロキシー 応功/失測で理由 Success Success	GUI 1般症サーバー ns3grideencojo ns3grideencojo
	モジュール共選 Antibu モジュール更新ログ 更新時刻 2007-02-01 00:00 2006-10-13 00:00	itus MTA7PP パンテ名 20070201 20061011	オン 意識プロキシー 成功/失敗現由 Success Success	GUI 諸続サーバー nS3gridemoojo nS3gridemoojo
* NEXKAN *	モジュール共選 Antib モジュール更新ログ 更新特別 2007-02-01 0000 2006-10-13 0000	nus MTA7P 1757名 20070201 20061011	オン 意識プロキシー 応功/失敗理由 Succes Succes	GUI 1般後サーバー ns3gideoncojp ns3gideoncojp

3.2 検出状況

BLOCが検出したウイルスの一覧を表示します。

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

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

※「検出ログ」では最新の1000件までの検出ウイルスを表示します。

● ダウンロード

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

● 詳細情報

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

ァイル(E)	編集(E) 表示(V) 」	履歴(S) ブックマーク(B) ツール(T)	ヘルプ(圧)				
アンチウィ						サポ- ▶ サーバ環	
An	til/irus	更新状況	出状況 共通語	受定 メール	設定 ウェブ設プ	き 他サービス	
検出	状況						
		検出統計情報					
1	最終ウイルス検出 1007年02月22日 ナービス:smtp ウイルス名:	本日 10-	4 昨日	3 今月	107 <u>先月</u>	0 総合計	10
	/irus.MSWord.Zmk.j	ウイルス名 会 1位 Vinus MSW	rd VMPC-based	検出数	ウイルス名 歩 1位	検出	8
		月 2位 EICAR-Tes	t-File	4	月 2位		
		3位 Virus.MSW	ord.Class.bd	3	3位		
				日次課題	0.0120	1000	**
					1/10 Vinus MSW	rd VMPC-based	ex.
					合 2位 EICAR-Tes	t-File	
					3位 Virus.MSW	rd.Class.bd	
_							
材	出口グ				▶ 全表示	▶検索 ▶ダウン	0-1
ľ	所 検出日時	サーウイルス名	ファイル名	拡張 From		To	
	2007-02-22 09:52:14	smtp Virus.MSWord.Zmk.j		Local	in all pairs and a	Loss dans Pridraming	
	2007-02-22 09:52:14	smtp Virus.MSWord.Furby.b		kanad	ingly item cois	kang dinaphy item colg.	
	2007-02-22 09:52:14	smtp Virus.MSWord.Bug		koned	ineffeitencoig	kanashima@aibancoig	
	2007-02-22 09:52:14	smtp Virus.MSOffice.Halfcros.a		Longit	den all gibben mig	Long-bioselly ideason in	
	2007-02-22 09:52:14	smtp Virus.MSWord.TNT.c		kanad	ingly item coig	kang trimply item colg.	
	2007-02-22 09:52:14	smtp Virus.MSWord.VMPC-bas	ed	konech	and the second	kanashi mali kalengo ja	
	2007-02-22 09:52:14	smtp Virus.MSWord.Mykah		Barren 1	and galaxies and	Long Arises (Figure 2014)	
	2007-02-22 09:52:14	smtp Virus.MSWord.Mary		kanad	inspigitum cois	kung dring degide on colg	
	2007-02-22 09:52:14	smtp Virus.MSWord.Margaret		kanad	sinafteihen cois	kunschimetheihen colg	
_						(Dana	ECAL C.
						WOIDY	

画面3.2

3.3 共通設定

ライセンス情報や管理者のメールアドレスなどを設定します。

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

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

3.3.1 基本設定

● ライセンス

「(お客様)登録No」「パスワード」が設定されていることを確認してください。

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

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

※契約期間が終了している場合には認証できないことがあります。

● 管理者のメールアドレス

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

aaa@domain.jp bbb@domain.jp

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

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

●警告メールに記入するFROMフィールド

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



3.3.2 詳細設定

● メール送信で使用するSMTPサーバ

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

● テンポラリディレクトリ

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

● エラーとして扱わないAntiVirusエンジンの戻り値

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

● 感染メール保存ディレクトリ設定

BLOCでは使用しません。

😺 GIDEON AntiVir	us - Mozilla Fire	fox		
ファイル(E) 編集(E)	表示(⊻) 履歴(≦)	ブックマーク(B) ツール(D) へ	ルプ(団)	¢
アンチウイルス	アンチスパム			サポート
Antil/iru	s	更新状況 検出	大況 共通	▶ サーバ環境 設定 メール設定 クェブ設定 他サービス
共通設定				トページのアンドク
		基本設定 詳細設	定 更新3	境設定
詳細設定				
	メール送信で使用 	するSMTPサーバー	▶更新	警告メールなどを送信するために使用するSMTPサーバーです。利用可能なメールサ ーバーのアドルスを指定してだだい。 mailexample.com
	テンポラリディレク	FU		
	/var/tmp		▶更新	本リフトウェアガー時的に使用するディスク確糊です。絶対パスで指定します。空き 容量は少なくとち100Mbyteに上必要です。 /var/tmp
	エラーとして扱わな	に \AntiVirusエンジンの戻り値		
			▶更新	ある特定のエラーで警告メールなどを送信しないために記述します。
	感染メール保存デ	ィレクトリ設定		
		保存容量 Mbyte	▶更新	
				@GIDEON Corp.

画面3.3.2

3.3.3 更新環境設定

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

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



3.4 メール設定

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

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

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

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

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

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

画面3.4

3.4.1 保守・状況

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

ログ:ボタンをクリックすると最新のログを取得し、下のログ一覧に表示します。

- サービス : SMTPまたは POP3 のサービスの種類。
- 環境チェック :該当ボタンをクリックすると、システムの詳細情報を表示します。[管理者に結果を送 信する]ボタンをクリックすると、表示されている内容を管理者宛に送信します。
- **再起動** : サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力 されている)の場合にONにします。
- 再設定 : サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生してい る場合にONにします。

SMTP - ログ - ダウンロード

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

POP3 - ログ - ダウンロード

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



画面3.4.1

3.4.2 基本設定

● 受信者への警告メール設定

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

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

メールヘッダーには送信経路などの情報が含まれています。

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

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

入力後、[更新]ボタンをクリックしてください。

初期設定値:感染メールの場合、受信者にメールを送信しない

● 送信者への警告メール設定

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

したがって「送信者に警告メールを送信しない」設定を推奨します。

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

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

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



3.4.3 詳細設定1

● チェックに使用するポート

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

● 監視する接続先のポート

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

● 送信元IPアドレスの復元

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

復元することにより完全な透過を実現しますが、パフォーマンスは低下します。

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

● 管理者への警告メール設定

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

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

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

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



BLOC system

3.4.4 詳細設定2

● 初期の接続待機数

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

初期設定值: SMTP 50 POP3 10

● 最大同時接続数

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

● 待機数を超えた場合の接続増加数

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

● 最大ファイルサイズ

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

● 最大ファイルサイズを超えた場合の処理

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

● ウイルス感染メールの保存

BLOC では使用しません。



画面3.4.4
3.4.5 ホワイトリスト

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

SMTP

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

from: エンベロープのFromメールアドレス

to: エンベロープのToメールアドレス

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

-----例1-----

送信元IP アドレス192.168.1.2 から送信されてきた場合、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。。

この指定の場合、example.netの該当メールアドレスは全てウイルスチェックしない指定になります。

host=192.168.1.2 from=@example.net

第3章 アンチウイルス設定

POP3

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

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

-----例1-----

送信元sender@example.comから送信されてきた場合、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

😻 GIDEON AntiVirus – Mozilla Firefox	
ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(E) ツール(T) ヘルブ(H)	0
アンチウイルス アンチスパム	サポート
GIDEON Antil irus 更新状況 検出状況 共通設定 メール設定	> サーバ環境 ウェブ設定 他サービス
メール設定	
ウィルスチェックの有効/無効	▶ ページのアンドゥ
保守・状況 基本設定 詳細設定1 詳細設定2 ホワイトリスト	チェックリスト
ホワイトリスト	
SUTP POP3	
SMTP	
オワイトリスト(記述句: from=info@example.net to=@example.com)	特定のSMTPサーバーやシールアドレスをゲルス チョンのとない様常。会体も数定者をなどがAIス チョンのとない様常。会体も数定者をなどがAIス チョンのとないます。15行のに18 項目を19 つすが起きでき、15行のにした項目 はAIAの条件とかきす。アルファントのス文字・J文 学は201 に名かにます。 メールアドレスには8DOMAINはジルを注意す言定 *、こては0.8LTと一変化とシーアドレスをスルーし ます、項目にはして形成のます。 * したいまで見なして形成のます。 * したいまで見なしていためます。 * したいまで見なしていためます。 * したいまで見なした。 * したいまで見ないたまですり * したいまで見ないため、 * したいまで見ないため、 * したいまでした。 * したいまた。 * したいまた. * したい
	@GIDEON Corp.

画面3.4.5

3.4.6 チェックリスト

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

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

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

入力後[更新]ボタンをクリックしてください。 初期設定値:なし

GIDEON AntiVirus - Mozilla Firet	ox		
☞イル(E) 編集(E) 表示(V) 履歴(S)	ブックマーク(目) ツール(工) ヘルプ(日)		4
アンチウイルス アンチスパム			サポート
	更新状況 検出状況	共通設定 メール設定	▶ サーバ環境 ウェブ設定 他サービス
ウィルスチェックの有効/無効	SMTP POPS	l	▶ ページのアンドゥ ▶ ページの初期化
保守·状況	基本設定 詳細設定1	詳細設定2 ホワイトリスト	チェックリスト
チェックリスト SMTP	POP3		
チェックリスト (記述例: @w	xample.com)	▶ 更 新	チェックソストにメールアドレスを登録すると、そのメール アドレスポメールにされている場合のあ、ウイルス ティンを行いてきれている場合のあ、ウイルス はまっ、アレスマットと数件なく、などのメールアドレスをチェックし はまっ、アレスマットのなどスティンズで見得いく認わ れます。 メールアドレスを注意で見合いのメールアドレスを を省略して足話さずることで、GODMAIMの主人にユーザー名 を省略して足話さずることで、GODMAIMの主人にユーザー名 を省略して足話さずることで、GODMAIMの主人はな ある場合は、チェックリストと次行プロジェス ある場合は、チェックリストの必要形がます を引きたけ、メールアドレスでき。 く気活送別~ ・ infolesample.comのときウイルスチェックする Gecample.com
			@GIDEON Corp.

画面3.4.6

3.5 ウェブ設定

HTTPおよびFTP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。

FTPは、インターネットやイントラネットなどのTCP/IPネットワークにおけるファイル転送に使用されるプロ 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]または[FTP]ボタンをクリックして、次画面で有効または 無効を設定します。

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

(ル(E) 編多	集(E) 表示(⊻) 履歴(S)	ブックマーク(<u>B</u>) ツー	ール① ヘルプ(世)					
シチウイルン	ス アンチスパム						サポー	÷
GIDEON Antil	rus ^{快定}	更新状況	検出状況	共通設定	メール設定	ウェブ設定	▶ サーバ環境 他サービス	1
, i	イルスチェックの有効/無効	► HTTP	FTP	4				
保守·	·状況	保守·状況	基本設定	詳細設定1	詳細設定2	チェック対象	ホワイトリスト	
	核働状況ログロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロロ<	サービス HTTP FTP	環境チェック 再起 	 画 再設定 二 二 				
	нттр	FTP	1				▶ ダウンロ・	-۲
	192.168.1.7 www.yahoo.co.jp5 HTTP/1.1" 200 192.168.1.7 www.yahoo.co.jp5 HTTP/1.1" 200 192.168.1.7 www.yahoo.co.jp5 HTTP/1.1" 200 1921.168.1.7 www.yahoo.co.jp5	255 [Wed, 21 Feb 21 255 [Wed, 21 Feb 21 255 [Wed, 21 Feb 21 255 [Wed, 21 Feb 21	007 14:40:57 JST] "0 007 14:40:59 JST] "0 007 14:41:01 JST] "0 007 14:41:03 JST] "0	aET /cgi-bin/mair aET /cgi-bin/mair aET /cgi-bin/mair aET /cgi-bin/mair	n.cgi?func=415&a1 n.cgi?func=417&a1 n.cgi?func=415&a1 n.cgi?func=415&a1	=SMTP&sid=9447 =SMTP&sid=9447 =SMTP&sid=9447 =POP3&sid=94474	409298timer=630642 409298timer=632401 409298timer=634754 409298timer=6354754	1″
	200 192.168.1.7 www.yahoo.co.jp5 HTTP/1.1" 200 192.168.1.7 www.yahoo.co.jp5 200	355 [Wed, 21 Feb 21 355 [Wed, 21 Feb 21 355 [Wed, 21 Feb 21	007 14:41:04 JST] "0 007 14:41:49 JST] "0	aET /ogi-bin/mair AET /ogi-bin/mair AET /ogi-bin/mair	nogi?tunc=417&a1 nogi?tunc=417&a1	=1 0F3681d=94474 =SMTP&sid=94474 =POP3&sid=94474	40929&timer=637074 10929&timer=682083 HTTP/1.	17

画面3.5

BLOC system

3.5.1 保守·状況

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

ログ : 最新のログを取得し、下のログ一覧に表示します。

サービス : HTTPまたはFTPのサービス。

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

- **再起動** : サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力 されている)の場合にONにします。
- 再設定 : サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生している場合にONにします。
- HTTP ログ ダウンロード
 - :ダウンロードボタンをクリックすることで、HTTPのアクセスログがダウンロードできます。 ダウンロードする際は、『HTTPログのダウンロード』ダイアログ中のリストより選択して からダウンロードボタンをクリックしてください。
- FTP ログ ダウンロード
 - : ダウンロードボタンをクリックすることで、FTPのアクセスログがダウンロードできます。 ダウンロードする際は、『FTPログのダウンロード』ダイアログ中のリストより選択してか らダウンロードボタンをクリックしてください。

GIDEON	AntiVirus - Mozilla Firefox	
(ル(圧) 器	扁果(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルブ(H)	
アンチウイル	レス アンチスパム サ	ボート
CIDEO	► 1 - 1	(環境
Ant	ivirus 東新井沢 神田井沢 井通設定 メール設定 ウェブ設定 他サービス	
·J£J	款 上	
	ウィルスチェックの有効/無効 トHTTP トFTP	
_	保守・状況 基本設定 詳細設定1 詳細設定2 チェック対象 ホワイトリスト	
保守	r·状况	
	お 単 が パー ビ - ビ ビ	
	HTTP FTP	
	HTTP ・ダウ	ンロード
	192168.1.7 www.yahoo.co.jp:555 [Wed, 21 Feb 2007 14:40:57 JST] "GET /cgi-bin/main.cgi?func=4158a1=SMTP8sid=9447409298timer=630642 HTTP/1 1" 200	-
	1921681.7 www.yahoo.co.jp555 [Wed, 21 Feb 2007 14:40:59 JST] "GET /cgi~bin/main.cgi?func=4178a1=SMTP8sid=9447409298timer=632401	
	1921681.7 www.yahoo.co.jp555 [Wed, 21 Feb 2007 14:41:01 JST] "GET /cgi-bin/main.cgi?tunc=415&a1=SMTP&sid=944740929&time=634754	
	HTTP/1.1" 200 1921681.7 www.yahoo.co.jp555 [Wed, 21 Feb 2007 14:41:03 JST] "GET /cgi-bin/main.cgi?func=4158a1=POP38sid=9447409298timer=635989 HTT	P/1.1"
	200 19216817 www.vahoo.co.in555 [Wed 21 Eab 2007 14/41/04 UST] "GET (ogi=hin/main.og/2/unc=4178:a1=SMTP8:oid=94474092984img=687074	
		D (1 1 5
	192.108.1.7 www.yahoo.co.pbbb [Wed, 21 Feb 2007 14/41/49 US1] "GE1 /ogi=bin/main.ogi?func=4178a1=POP38.sid=9447409298timer=682083 HTT 200	P/1.1"
		[
-		
	00	SIDEON Co

画面3.5.1

3.5.2 基本設定

●ファイル種別、ウイルスチェックの有効/無効

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

●感染時にファイルに埋め込む、もしくは置き換えるメッセージ

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

●最大受信サイズを超えた際に置き換えるメッセージ

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

●すでに感染していたページにアクセスした際に置き換えるメッセージ

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

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



画面3.5.2

3.5.3 詳細設定1

●チェックに使用するポート

BLOCではウイルスチェックのために別ポートにパケットを転送します。 他のサービスなどですでに利用している場合は、未使用ポート番号に変更してください。 入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 9080 FTP 9021

●監視する接続先のポート

HTTPまたはFTP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、FTPのポート番号は21を指定します。 プロキシサーバ経由でインターネットに接続している場合、HTTPポートにプロキシサーバが受け付け るポート番号を指定してください。 例:HTTP 8080

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

入力後、[更新]ボタンをクリックしてください。 初期設定値:HTTP 80, 3128, 8080 FTP 21

●送信元IPアドレスの復元

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

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

●管理者への警告メール

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

Subject :警告メールのサブジェクト名を設定します。

本文 :警告メールに固有のメッセージを記載します。

入力後、[更新]ボタンをクリックしてください。

初期設定值:画面表示文字列

●ウイルス感染メールの保存

BLOCでは使用しません。



画面3.5.3

3.5.4 詳細設定2

●初期の接続待機数

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

HTTP もしくはFTP のサービスで、初期で接続待機する数を設定します。 クライアントからWEB サーバには一回のサイトアクセスで複数セッションを同時に使用するためデ フォルト値を大きく設定しています。 入力後、[更新]ボタンをクリックしてください。 初期設定値: HTTP 500 FTP 5

●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もしくはFTPの場合は、同時利用者の最大数にほぼ同数です。

入力後、[更新]ボタンをクリックしてください。 初期設定値: HTTP 1000 FTP 50

●待機数を超えた場合の接続増加数

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

入力後、[更新]ボタンをクリックしてください。 初期設定値: HTTP 50 FTP 1

●ダウンロードの最大ファイルサイズ

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

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

●ダウンロードの最大ファイルサイズを超えた場合の処理

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

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

入力後、[更新]ボタンをクリックしてください。

初期設定值:HTTP『通過』FTP『通過』

●アップロードの最大ファイルサイズ

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

●アップロードの最大ファイルサイズを超えた場合の処理

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

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



3.5.5 チェック対象

●ウイルスチェックしないファイル

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

HTTP初期設定值:

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



BLOC system

3.5.6 ホワイトリスト

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

HTTP

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

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

例

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

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

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

FTP

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

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

例

ftp://192.168.1.100/pub/file.exe をスルーする場合、以下のように記載します。 host=192.168.1.100 path=/pub/file.zip

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



3.6 スキャンコード一覧

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

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

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

この章は「BLOC system アンチスパムPlus」に該当する内容です。「BLOC system」には本章で説明するアンチスパム機能は搭載されていませんのでご留意ください。

4.1 更新状況

● スパムDB更新ログ (画面4.1 上段部分)

スパムデータベース (スパムDB) の更新状況を閲覧できます。 スパムDB は、カスペルスキーのアンチスパムエンジン (種別:kas)が利用する、スパムメールを特定 するための情報を格納したデータベースです。 初期設定では3時間毎の自動更新に設定されています。緊急対策が必要な場合は[手動更新]ボタ ンをクリックし、最新のデータベースを取得してください。 ※既に更新済みの場合は、新たに更新されません。

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

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

● モジュール更新ログ (画面4.1 下段部分)

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

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

※各モジュール内の [強制更新]ボタンは通常はクリックしないでください。



4.2 検出状況

スパムメールと判定したメール情報の履歴や統計情報などを閲覧できます。

● 検出情報

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

(IL(F) 編集(F) 表示(A) 歸足						
10 0 000 0 001 0 180	壁(S) ブックマーク(目	シール ①	ヘルプ(円)			
ンチウイルス アンチスパム					.	ボート
GIDEON					▶ サーバ	(環境
Antilirus	再新計	1	金田状況 共通設定 メー	一儿纷定	他サービス	
+AUU4420	2.470	(DC		7F BAAL		
使山朳沉						
最終2パル検出	検出作	9般				
2007年02月21日	本 E		0 昨日 10 今月	10 先月	0	
サービス: 判定方法:XS(3)	DDI	みにマストのない	14/# 80			
	HDL	301 - ハートノ わし	1 1 PH TR			
		RBL一致ドメイ:	ン 検出数	RBL一致ドメ	イン 検	出数
	今1	位 justIsikdar	keal.com 4	先 1位		
	/3 2	位 nightlights	un.into 2	月 2位		
		the second second second	5k (2)	0.00		
	3	12 subiourige.	2	3122		_
	3	l <u>a</u> sobiocrige:	► 月次詳細	310		
	3	t⊈ sabiotinge.	▶月次詳細	312		
	3	<u>(</u> 2 subiourige:	▶ 月次詳細	310		
検出口が	3	<u>a</u> solutinge:	▶ 月次詳細	310)▶検索)▶ダウ	20-
検出ログ	3	<u>u</u> soprounge.	► 月次算過	300 ▶全表示	> ▶検索	-םעו
検出ログ 新 検出日時	3 サー 判定方法	<u>。</u> soprotrige. スコア	▶月次詳細 りブジェクト	310 ▶全表示 From	▶検索 ▶ダウ To	-םעי
検出ログ 新 検出日時 2007-02-21 152526		2 suprounge. 2.37 3	● ● 月次詳細 ● サブジェクト [SPAM 3 KAS] Full of health? Then	310 ▶ 全表示 From	▶検索 ▼● To Lagentman	-םעי
検出ログ 新 検出日時 2007-02-21 152528 2007-02-21 152351	サー 判定方法 XS XS	2, suprounge. 2,37 3 3	975720h SPAM 3: KAS] Full of health? Then [info 38955] [SPAM 3: R1] Pe-Chan	3位 ▶全表示 From	▶検索 To 「To 「」」	-םעו
検出ログ 新 18出日時 2007-02-21 152526 2007-02-21 15251 2007-02-21 15251	サー 判定方法 メス メス メス メス 、 、 、 、 、 、 、 、 、 、 、 、 、	2 suprounge. 3 3 3		3位 ▶全表示 From	▶ 検 索 ▶ ダウ To Line set into Line set into Line set into Line set into	-םעי
検出ログ 17: 検出日約 2007-02-21 15:25:20 2007-02-21 15:22:51 2007-02-21 15:22:17 2007-02-21 15:42:59	サー 判定方法 メS XS XS XS XS XS XS XS XS	2 Schularge. 3 3 3 3	9792125 (SPAM 3: KAS] Full of health? Then (Info 30085) (SPAM 3: K1] Pec Chan (SPAM 3: K1] File Change) (SPAM 3: K1] File Change)	3位 ▶全表示 From	▶ 枝 紫 ▶ 593 To Sanations Readifients Readifients Readifients	-םעי
検出ログ	サー 判定方法 ×S ×S ×S pop3 ×S pop3 ×S	2 Schularge. 3 3 3 3 3 3	# #25/206 (\$754M 3, KAS] Full of health? Then (frick 38958 [SPAM 3, R1] Re-Charge (Info 38959 [SPAM 3, KAS] All proc (Frick 38930 [SPAM 3, KAS] All products for your	3位 ▶全表示 From	2 ▶検索 TO Least-Inter Least-Inter Least-Inter Least-Inter Least-Inter Least-Inter	-םעי
検出ログ ini 1%出日か 2007-02-21 152520 2007-02-21 152551 2007-02-21 144939 2007-02-21 144939 2007-02-21 144939	サー 判定方法 ※ ※ ※ ※ pop3 ※ ※ pop3 ※ pop3 ※	2,37 3 3 3 3 3 3 3 3 3 3 3 3 3		3账 ▶全表示 From	► Ht # ► 9/2 To Instantions Nonathines Nonathines Nonathines Nonathines Nonathines Nonathines Nonathines Nonathines	-םעי
検出ログ 17 検出日時 2007-02-21 152520 2007-02-21 152551 2007-02-21 15251 2007-02-21 144939 2007-02-21 144937 2007-02-21 144937	サー 料底方法 ×S ×S ×S ×S pog3 ×S pog3 ×S pog3 ×S pog3 ×S pog3 ×S	7.37 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	9757275 (SPAM 3: KAS) Full of health? Then (Info 30950) (SPAM 3: R1) Re-Charge (Info 30950) (SPAM 3: R1) Re-Charge (SPAM 3: KAS) All products for you (SPAM 3: KAS) All products for you (SPAM 3: KAS) Full of health? Then (Info 30950) (SPAM 3: R1) Re-Charge	▶ 全表示 From	▶枝文)▶9つ To Recentine Rec	-םע
検出ログ	サー 料底方法 ※ ※ pog3 ※ pog3 ※ pog3 ※ pog3 ※ pog3 ※	X_17 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	STATE STATE	J址 ▶全表示 From	To To Recent lines Recent lines Recent lines Recent lines Recent lines Recent lines Recent lines Recent lines Recent lines Recent lines	- -
検出ログ	サー 単応方法 メミ メミ レの3 メミ	2,237 3 3 3 3 3 3 3 3 3 3 3 3 1		▶ 全表示 From	▶ 枝 常 To To Rear Self-Inde Rear Self-Inde Rear Self-Inde Rear Self-Inde Rear Self-Inde Rear Self-Inde Rear Self-Inde Rear Self-Inde	-םעי

画面 4.2

● RBL一致ドメイン統計情報

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

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

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

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



画面 4.2.1

検出ログ

検出状況画面の下部「検出ログ」欄では、検出したスパムメールの情報リストを閲覧できます。 選択行をクリックすると詳細情報を表示します。各タイトル項目をクリックするとソートします。

[全表示]ボタンをクリックすると、検出ログの最新リストを再表示します。[検索]ボタンをクリックする と、項目での絞り込み検索ができます。また、検出ログは [ダウンロード]ボタンをクリックすることで、 CSV ファイルとしてクライアントPC に保存することができます。



画面 4.2.2

4.3 共通設定

本項は、アンチウイルスでの設定と共通です。詳細は、「3.3 共通設定」の項を参照してください。



4.4 メール設定

4.4.1 保守·状況

本項は、アンチウイルスでの設定と共通です。詳細は「3.4.1 保守・状況」の項を参照してください。

4.4.2 基本設定

ここではスパム判定スコアなどの基本的な設定を行います。

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

GIDEON AntiVirus	- Mozilla Firefox	
ファイル(E) 編集(E) 表示	〒V/ 履歴(S) ブックマーク(B) ツール(T) ヘルブ(H)	0
アンチワイルスアン		サホート
Antil Irus	更新状況 検出状況 共通設定	▶ サーバ環境 メール設定 他サービス
メール設定		
スパムチェッ	クの有効/無効 ▶ SMTP ▶ POP3	▶ ページのアンドゥ
保守·状況	基本設定 詳細設定1 詳細設定2 転送メール	ホワイトリスト プラックリスト チェックリスト
基本設定	A PART AND A PART	3.511.511
7	バムと判定した場合のSubject	
[SPAM + 신지고까 + 신判定名 +] + 신元Subject	アクション「Subject変更」の総合スコアを超えていた場合に置き換えられるSubjectです。
7		
	 推奨設定を利用する カスタマイズを利用する 	※カスタマイズを利用する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 BI:「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
● 判定方法	D 刊走方法 スコア D 刊走方法 スコア D コーゼー中美でのかけつし 4 525 数度テチェック 5	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
	BL ユーリール戦ノリックリスト 4 020 光信ルリエック 1 YS URIフィルリング ○ RFS 逆引きチェック 1	RI:接続元のJPアトレスのRBLチェッジ。両スコア推奨 S25: Receivedに記述された命名規則の形式チェック。低スコア推奨
	R1 RBL 3 KAS データベース 3	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	アクション 総合スコア アクション 総合スコア	
	何もしない 0 POP3のみ本文変更 99	スコア音計が、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
	Subject変更 3 SMTP/MTA受信拒否 99	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
●追加へッダ	追加ヘッダ行 総合スコア	SMTP/MTA受信拒否:メールが受信拒否される
	X-Spam-Status: NONE	追加ヘッダ
	X-Spam-Status: SUSPICION 1	スコアの吉計が、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。
	X-Spam-Status: SPAM 4	
		@ GIDEON Corp.

画面 4.4.2

● スパムと判定した場合のSubject

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

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

[SPAM 3: RES KAS] 元Subject

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

変更する場合は、入力後に [更新]ボタンをクリックしてください。

● スパム判定基準

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

BL:ユーザ定義ブラックスリスト

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

XS: URLフィルタリング

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

R1:RBL(リアルタイムブラックリスト)

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

S25:発信元チェック

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

RES:逆引きチェック

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

KAS:本文解析

・カスペルスキーアンチスパムDB を検索してメール本文をチェック

・推奨スコア3(検知度中位)

・英語、ロシア語などのメール解析に優れている。

「カスタマイズを利用する」を選択すると判定基準スコアを変更できます。

注意

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

• アクション

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

・Subject変更:

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

・POP3のみ本文変更:

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

・SMTP/MTA受信拒否:

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

● 追加ヘッダ

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

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

また、ヘッダには以下に類する行も付加されます。

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

重要

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

4.4.3 詳細設定1

● チェックに使用するポート

BLOC では変更する必要はありません。

● 監視する接続先のポート

SMTP、POP3 が使用しているポートを指定します。

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

例 25,587

● キャッシュ制御

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

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

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

● POP3のみ本文変更のとき置き換える本文

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

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



画面 4.4.3

4.4.4 詳細設定2

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

上記3項目はアンチウイルスの設定と共通です。

● スパム判定で除外するグローバルIPアドレス

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

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



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

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

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

重要

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



4.4.5 転送メール

4.4.5.1 基本

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

初期設定値:転送しない

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

● 転送下限スコア

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

● 受信先への配信を停止する

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

● POP3サーバのメール削除

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

● 転送の指定方法

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

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

-----例1-----

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

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

-----例2-----

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

@example.com spam-admin@example.com

4.4.5.2 POP認証

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

4.4.5.3 APOP認証

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

記載例:

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

user=user-one password=1234 host=192.168.0.1

1700 MM9602 - \$61102 - 1802-07	ブックマーク(目) ツール(工) ヘルプ(日)		
アンチウイルス アンチスパム			サポー
GIDEON			▶ サーバ環境
	更新状況 検出状況	共通設定 メール設定	他サービス
メール設定			
スパムチェックの有効/無効	SMTP		 ページのアンドゥ ページの初期
保守·状況 基本設定	詳細設定1 詳細設定2	転送メールホワイトリスト	ブラックリスト チェックリスト
転送メール			
**	PODING ADDRESS		
基本	TOTISSE ATOTISSE		
●転送しない			総合スコアが「転送下限スコア」を超えた場合に
○転送下限スコアに達していた	肺动性		メールを転送します。
転送下限スコア 3	受信先への配信を停止する VPOP3	サーバのメール削除 🛛 🕨 更 新	POP3の場合はユーザLU@LPOP3サーハIPアドレ を、SMTP/MTAの場合は受信メールアドレスを、
			頭がら指定し、半角スペースに続いて転送メール
			し2を指定します。 転送メールアドレスは半角ス
			レスを指定します。転送メールアドレスは半角ス・ スで区切ることで複数指定可能です。また、受け
			レスを指定します。転送メールアドレスは半角ス- スで区切ることで複数指定可能です。また、受 イルアドレスは、@から始めることで@以下が一致し ものを転送対象にできます。
			レスを指定します。転送メールアドレスは半角ス- スで区切ることで複数指定可能です。また、受け ルアドレスは、色から始めることで@LV下が一致し ものを転送対象にできます。 < 内ド POP2の場合
			レスを指定します。転送メールアドレスは半角ス、 スペ区 切ることで複数指定可能です。また、愛ケ ルアドレスは、仓から始めることで使し下が一致し ものを転送対象にできます。 < 例F POP20場合 > のPOP20場合 > パドログログログログログログログログログログログログログログログログログログログ
			しえる推定します。転送シールアドレスは事項ン 入で区切らことで諸数指定可能です。また、受 ルアドレスは、色が込めることでも以下が一致し ものを転送す第にできす。 く例 POP200項合シー ・POP302一サログUsersone、POP3サー/UP7 入が121680100音ンナルをSpan®example にまだ送 user-oneの102718011 - nam®example C
			しえ名指定します。転送シートルアドレスは事項ン 入で区 切らしとで複数指定可能です。また、安 しアドレスは、eからぬめることでe以下が一致し ものを転送す像にできす。 < やり POP 2001 二 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
			した若確にはす。若語メーバアドレスは年界ン アロビッジングでは大きいた。 アロビッジングでは大きいた。 アロジンジングでは、 アロジンジングでは、 アロジンジング アロジンジング アロジンジング アロジンジング アロジンジング アロジンジング アロジンジング アロジンジング アロジンジング アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジンジン アロジン アロジンジン アロジンジン アロジン アロジンジン アロ アロジン アロ アロジン アロ アロ アロ アロ アロ アロ アロ アロ アロ アロ
			1.入名物理(法す,単語メーバ)アドノは半界入 アスピマ防シンでが数単にすいであっまた、受 リッドレンは、40%を始めたとでおして、パーサロ とのを経どすが良いでであす。 くの時で200時会> POP201世代しなーマース。PDP301世であっ 2012(18010)連合メールをspam®example co とおざ user round(1921(8011) spam®example co く例 SMTP/MTA> user round(1921(8011) spam®example co くの) SMTP/MTA> user round(1921(8011) spam®example co user round(1921(8011) spam®ex
			八方物理(1点す,数15×10)ドレスは年外、 アログロンズ(2015)になった。 リッドレンズ(2015)になった。 の内を延ざ対象(2015)になった。 の内を延ざ対象(2015)になった。 の内を延ざ対象(2015)になった。 ののも近づか。 とのPSの)二、1000(用金)・ 人が102(1600)(別金)メールをspam®example co にまご。 usar crosel(192(1600)) spam®example co くめ SMT/MTA usar crosel@example.comの死の通合メールを spam®example.comの死の通合メールを spam®example.comの死の通合メールを spam®example.comの死の通合メールを spam®example.comの死の通合メールを spam®example.comの方面のであった。
			(入名韓軍)はず、韓語メーバアドンは年界ン アスピッ防シンでは新潟宣コ堂の学、また、受 ルアドンは、4時から約3とどや以下が一致し のかき延づきないでできま。 < 9時 10930)借合う ・ 80930)は一学びがLase-rose、0993サービア とか9930」は一学びがLase-rose、0993サービア とか9930」は、1993の場合う ・ 1993の日本・1993の日本・1984 ・ 1993の日本・1993の日本・1984 ・ 1993の日本・1993の日本・1984 ・ 1993の日本・1993の日本・1984 ・ 1993の日本・1993の日本・1984 ・ 1993の日本・1993の日本・1993の日本・1984 ・ 1993の日本・1993の日本・1993の日本・1993の日本・1993の日本・1993の日本 ・ 1993の日本・19930日本・19930日本 199300000000000000000000000000000000000

BLOC system

4.4.6 ホワイトリスト

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

SMTP

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

from: エンベロープのFromメールアドレス

to: エンベロープのToメールアドレス

helo: HELO で指定されるアドレス

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

-----例1-----

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

host=192.168.1.2

-----例2-----

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

host=192.168.1.2 from=sender@example.net

-----例3-----

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

host=192.168.1.0/255.255.255.0

-----例4-----

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

host=192.168.1.2 from=@example.net

• POP3

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

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

-----例1-----

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

form=sender@example.com

-----例2-----

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

host=192.168.1.2 user=user-one

C and C solution and C	ブックマーク(国) ツール(① ヘルブ(H)		
チウイルス アンチスパム			サポ-
GIDEON			▶ サーバ環
Antil/irus	更新状況 検出状況 共通設定	メール設定	他サービス
メール設定			
スパムチェックの有効/無効	► SMTP	► <->	のアンドゥ
保守·状況基本設定	詳細設定1 詳細設定2 転送メール	ホワイトリスト ブラックリスト	チェックリスト
ホワイトリスト			
SMTP	POP3		
SMTP			
ホワイトリスト (記述例: hc	st=127.0.0.2 from=sender@example.com)	アリン スパムチェックを無 1行内に指定した メールアドレスを必 第公が、一切ために	効にする条件を指定できま 条件は全てAND条件となり DOMAINと指定すると、DO らかります
		項目には以下が	しょうよう。 50ます。
			元IP及OIP/MASK(FQD)
		・host=有効近日 ・from=envelope	のFromメールアドレス
		・host=有効活動 ・from=envelopeの ・to=envelopeの ・helo=HELOで指	のFromメールアドレス Foメールアドレス F定されるアドレス
		・host=有効通行 ・from=envelope ・to=envelopeの ・helo=HELOで引 有効販注信元とは IPTを以こを報わ	のFromメールアドレス Foメールアドレス i定されるアドレス . 実際に道引き等を行うグロ htt小ずしたSTMP接待示
		 host=有効だfi from=envelope to=envelope to=envelope helo=HEL0で引 有め送信元とは IPアドレスを指し IPアドレスを指し ドレスではありま キャロマドレス 	のFromメールアドレス foメールアドレス f定されるアドレス , 実際にご送引き等を行うグロ td。、メールへッダのReceive 、コンチルトッダのReceive、 コンを始ます・シャナ
		 ・host=有功活目 ・from=envelope ・to=envelope30 ・helo=tELOで3 有効が注意元には ビアドレスを指し ビアレスをはのま されたドアドレス < < 	のFromメールアドレス 「ロメールアドレス 」定されるアドレス 実際にご逆引き等を行うびし はす。必ずしもSTMP接続元 たん。メールヘッダのReceive)可能性もあります。
		・hot=r=有効式 from=mewkpe to=mewkpey helo=HELO71 特別法信元には ドレスではありま をれたビアドレスス く記述例> ・FromUsender from=sender8	のFromがメールアドレス 「ロメールアドレス i定されるアドレス 、実気能ご送引き等を行うグロ はす。心ずしらSTMP接続元 イム。メールへ次ダのReceive)可能性もあります。 Pexample.comを無効 example.com
		- hots 1年初次日 - from=mervelope - tos=mervelope) + helo=HELIOCT 物が信告元には ドアアトレスな物は - たいたサアトレス、 - くまたがか - FromがEnander - 行っかど用いた。 - 行っかが目のたけ - 行っかが目のたけ - 行っかが目のたけ - 行っかど目かけ - 行っかが目のたけ - 行っかが目のたけ - 行っかが目のたけ - 行っかが目のたけ - 行っかど目かけ - 行っかが目的に - 行っかが目的に - 行っかど目かけ - 行っかが目的に - 行っかが目のたけ - 行っかが目的に - 行っかが目的に - 行っかが目的に - 行っかが目的に - 行っかが日のに - 行っかが日の - 行っか - 行 - 行っか - 行 - 行っか - 行 - 行っか - 行 - 行っか - 行っか - 行 - 行っか - 行っか - 行 - 行っか - 行 - 行 - 行っか - 行 - 行っか - 行 - 行っか - 行 - 行 - 行 - 行 - 行 - 行 - 行 - 行	0Fromスールアドレス うたシールアドレス うたされるアドレス 実際に送る1と専家行うグロ はす。心ずしたらTMF掲続元 た、ムットールッダのReceiver う可能性もあります。 Attach Apple.comを無効 example.com 7000~1270.0255.0範囲 265.255.255.0
		 hot=可約応1 trom=revelope tor=revelope tor=re	0Fromメールアドレス Goメールアドレス 定されるアドレス 実際に送きは専者行うびロ は、必ずしたSTMF掲続元 た、メールへからのReceive joi 能性もあります。 example.comを無効 xeample.comを無効 xeample.comを 2000~1270.0256の範囲 265.255.2550
		 host=有功応1 from=revelope tors=revelope hela=HEL073 特別法信先には ドレスを掲し ドレスを掲し ドレスでは初りよ されたドアレスを掲し デのの形をの相付 from-zendette 有効が正常た2 host=127.00.0 	0From3・ルアドレス (ホイールアドレス 定定されるアドレス 実際に注意引き考え行うグロ はす。必ずしたSTMF1時応- になっ、メールックのDReceivee)可能性もあります。 texampla.comを無効 exampla.comを悪効 2056.255.255.0 のopp

BLOC system

4.4.7 ブラックリスト

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

SMTP

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

from: エンベロープのFrom メールアドレス

to: エンベロープのTo メールアドレス

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

-----例1-----

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

host=192.168.1.2

-----例2-----

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

host=192.168.1.2 from=sender@example.net

-----例3-----

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

host=192.168.1.0/255.255.255.0

-----例4-----

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

host=192.168.1.2 from=@example.net

POP3

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

from: メールヘッダ内のFromメール青dれす

user: POP3アカウント

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



画面 4.4.7
4.4.8 チェックリスト

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

SMTP

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

POP3

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

● POP3削除

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

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

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

😻 GIDEON AntiVirus - Mozilla Firefox	
ファイル(1) 編集(1) 表示(1) 履歴(3) ブックマーク(13) ツール(1) ヘルブ(14)	<u>ه</u>
アンチウイルス アンチスパム	サポート
GIDEON	▶ サーバ環境
Antivirus 更新状況 検出状況 共通設定 メール設定	他サービス
メール設定	
スパムチェックの有効/無効 ▶ SMTP ▶ PDP3	▶ ページのアンドゥ ▶ ページの初期化
保守・状況 基本設定 詳細設定1 詳細設定2 転送メール ホワイトリスト	ブラックリスト チェックリスト
チェックリスト	
SMTP POP3 POP38/08	
SMTP	
チェックリスト (記述例): @example.com)	テレジストにシールアドレスを登録すると、そのメール アドレスポールに含まれている場合のみ、スパ しまつかられいよう場合のみ、スパ しまつかられいないる場合のみ、スパ しまつかられいないないます。シェンマントレスをキョンク します。アドレスのといめたスキーンを手は割いに取れ します。アドレスのといめたスキーンを手は割いに取れ します。アドレスのといめたスキーンを手は割いに取れ します。アドレスのといめたスキーンを手は割いに取れ たいために、自ついたり、たいため、日本の、日本の、日本の、日本の、日本の、日本の、日本の、日本の、日本の、日本の
	@ GIDEON Corp.

画面 4.4.8

5.1 他サービス

アンチウイルス、アンチスパム設定画面の「他サービス」タブをクリックすると、画面5.1.1 が表示されます。

5.1.1 保守·状況

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

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

設定項目は以下となります。

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



5.1.2 基本設定

● ウイルスチェック、スパムチェックするネットワークの範囲

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

初期設定値:設定なし



画面5.1.2

5.1.3 ホワイトリスト

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

記述方法は、 host=接続先のIPアドレス port=ポート番号

初期設定値:設定なし



6.1 サーバ環境

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

6.1.1 保守·状況

● ネットワーク

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

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

ホスト名:gideon-bloc(初期設定値)

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

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

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

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

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



BLOC system

6.1.2 ログ

サーバ環境画面の「ログ」タブをクリックすると、画面6.1.2 が表示されます。 システムエラーログとして、「messages」または「syslog」の一覧が表示され、エラーや異常を発見する ために利用します。また、ログの一覧で検索したい文字列で特定のエラーを絞ることができます。



画面6.1.2

6.1.3 基本設定

● ネットワーク

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

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

ローカルネットワーク上のプライベートアドレスを設定する例を説明します。

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

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

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

● 時刻設定

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

下記のタイムサーバを設定することで、時刻を適切に修正することができます。

● タイムサーバ

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

🕹 GIDEON AntiVirus - Mozilla Fire	fox	
ファイル(E) 編集(E) 表示(V) 履歴(S)	ブックマーク(目) ツール(工) ヘルブ(日)	4
アンチウイルス アンチスバム		サポート
GIDEON		
	更新状況 検出状況 共通設定 メール設定 ウェブ設定	他サービス
サーハー環境		
	▶ ベージの	アンドゥ トページの初期化
	保守・総況 ログ 総構設定	
基本設定		
ネットワーク		
・ DHCPサーバーよ のHCPサーバーよ	IFアドレス等を取得する。 JFアドレス等を取得しない(手動設定)	
ホスト名		
IPアドレス .		
サブネットマスク		
デフォルトゲートウェイ		
ネームサーバー1		
ネームサーバー2	▶更 新	
時刻設定		
2007 年 2 月	22 日 10 時 39 分 25 秒	
タイムサーバー		
htp.nict.jp	▶更 新	
		CODEON Com

画面6.1.3

7.1 メールテストツール

● 受信テスト

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

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

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

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

● 転送テスト

BLOCから外部へのメール転送が可能かどうかのテストを行います。

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

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

転送成功時には転送ログに「転送成功」を表示されます。

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



BLOC system

7.2 サポート接続ツール

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

ギデオンサポートセンター sp@gideon.co.jp

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

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

😺 GIDEO N	AntiVir	us - Mo	zilla Fire	fox								
ファイル(<u>F</u>)	編集(<u>E</u>)	表示⊙	履歴(<u>S</u>)	ブックマーク(<u>B</u>)	ツール①	ヘルプ(円)						
GIDE An	tiViru	s										
サポー	·ŀ											
			_									
	_	メールテス	F / ♥	ボート接続								
97	(一ト接続											
		サーバー	Ş.				 					
• #	8統先 10キシ	アドL ボーL ブロU ユー・ バス ・外 外 の ボ ・ コー・ の ボ ・ し ロ ・ フロU	/ス - コル サイズ チーD フード ヨサーバー ドレス ート ーザーID スワード	nsgideon 1194 ・UDP 1280 への接続にプロキャ	20.jp TCP シを利用しな シを利用する	0		接切新	ガボート用 ネットワーン イズを変更 ユーザーロ 間いまれ 間合せ先: プロキシ使 て下さい。	サーバイ接続して、ボ 環境によって、ボ しなければならな およびパスワード ください。 sp@gideon.coj	ミタ。 ート、プロトコル い場合もあり については弊対 ア ロトコルはTCP	、MTUサ ます。 ままでお を指定し
		接続状況	2									
• H • H	Se続状況 Se続ログ	接続	状況	未接続				更新	接続状況 秒かかる場 も「接続中 ている場合 取得しログ	FF接続中」になら 合があります。村 してならない場合 があります。「更佳 DI内容を確認し	5には接続開始 6統開始から60 は、接続エラー 所」を押して最 てください。	台から散十 1秒待って が発生し 新ログを
											C	GIDEON Corp.

画面7.2

8.1 接続方法

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

① キーボード、モニターをBLOCに接続します。

図8.1-1 のようにキーボードを接続します。モニターは図8.1-2 のように接続します。



BLOC本体の電源を入れます。

③ BLOCにログインします。

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

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

以下のイタリック部分を入力して「Enter」キーを押します。

login: admin

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

Password: gwantivirus

画面に以下のメッセージが表示されます。

[admin@gideon-bloc ~]\$

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

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

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

Password: *gwantivirus*

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

[root@gideon-bloc admin]#

④ メニュー選択

③ でroot権限ユーザになると、画面8.1-3が表示されます。

BLOC system

Gideon Antivirus BLOC System基本設定
キー) メインメニュー
a) 現在の設定を見る
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8.1-3

「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)。

8.2 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 =>b

続いて以下のメッセージが表示されます。



画面8.2-1

画面8.2-1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8.2-2

画面8.2-2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8.1-3「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。

8.3 困った時の設定

8.3.1 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8.1-3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8.2-2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。

8.3.2 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。

第9章 トラブルシューティング

9.1 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。

9.2 よくある質問と回答

Windowsファイル共有、P2Pファイル共有には対応していますか?

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

ファイアウォールやVPN機能はありますか?

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

アドウェア、スパイウェアには対応していますか?

はい、対応しています。

URLフィルタリング(コンテントフィルタリング)には対応していますか?

対応しておりません。

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

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

ユーザ数とは何を意味しているのでしょうか?

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

機器の設定等行ってもらえるのでしょうか?

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

機器が故障してしまったようですが、どうすればいいですか?

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

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

ウイルス定義ファイル、スパムDBの更新の仕組みはどうなっていますか?

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

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

システムにリモートログインできませんが、設定を教えてください。

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

GUI管理画面にログインするパスワードを忘れてしまいました。

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

モニターとキーボードを直接BLOCに接続してください。

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

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

ログに PHASE_ENDsizeerror が多発しています。

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

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

定義ファイルはどの程度の頻度で更新されるのでしょうか?

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

9.3 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

OC system

M

株式会社ギデオン テクニカルサポートセンター

E-mail / sp@gideon.co.jp

TEL. 045-590-3655 (横浜)

受付時間 / 9:00~17:00(祝祭日を除く、月~金曜日)

「ギデオン アンチウイルス BLOC system アンチスパムPlus」 「ギデオン アンチウイルス BLOC system」 共通ユーザーズマニュアル

2008年10月20日 第10刷

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

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

> Copyright(c)2004 GIDEON Inc Printed in Japan