アンチウイルス・ゲートウェイ
パワード・ブルー版

― インターネットからのメール・ウェブによるウイルス侵入を水際で防ぐ
包括的インターネット・ウイルス対策ソリューション ―

Version 5.20

管理者用ガイド

F-Secure.

はじめに

このたびは、「アンチウイルス・ゲートウェイ」をご購入いただきありがとうございます。本マニュアルでは、製品のインストールおよびアンインストール、一般的な設定例、および詳細な設定例などについて説明しています。
なお、本マニュアルでは、「アンチウイルス・ゲートウェイ」を本製品と表記します。
Red Hat Enterprize Linux は、RHEL と表記する場合があります。RHEL5 は、Red Hat Enterprize Linux 5 Server を、RHEL6 は、Red Hat Enterprize Linux 6 Server を指します。
Turbolinux Appliance Server 製品全般は、TLAS と表記します。TLAS2.0 は、Turbolinux Appliance Server 2.0 を指します。TLAS3.0 は、Turbolinux Appliance Server 3.0 を指します。

本マニュアルで使用するマーク

マーク	説　明
	注意していただきたいことを記載しています。
	ヒント・補足情報を記載しています。
	参照先を記載しています。

本マニュアルで使用する記号と書体

記号・書体	説　明	例
[　]	メニュー名、項目名	[プロキシ設定]－[HTTP] を選択します。 [SMTP プロキシ]－[全体設定]－[SMTP 認証] を無効にします。
〔　〕ボタン	ボタン名	〔設定, 開始〕ボタンをクリックします。
あいう ABCabc123	ウェブ管理画面の設定値。 チェックボックスにチェックする場合は「**チェック**」と表記	[HTTP プロキシ]　：**チェック** [ポート番号]　：**9080**
ABCabc123	コマンド名、ファイル名、ディレクトリ名、ディスプレイ上の出力、コード例など	# **rpm -Uvh virusgw-***XXX***.i386.rpm**
ABCabc123	コマンドラインでユーザが入力する文字列	
ABCabc123	コマンドラインの可変部分	

F-Secure、エフ・セキュアの名称およびロゴは F Secure Corporation および日本エフ・セキュア株式会社の商標または登録商標です。RED HAT は米国およびそのほかの国において登録された Red Hat, Inc. の商標です。Turbolinux、ターボリナックスの名称およびロゴはターボリナックス株式会社の商標または登録商標です。Linux は Linus Torvalds 氏の米国および他の国における商標です。UNIX は The Open Group の米国および他の国における登録商標です。Sun、SunMicrosystems、Java、JavaScript、Sun Cobalt、Sun Cobalt 、Sun Cobalt Qube は SunMicrosystems, Inc. の米国およびその他の国における商標または登録商標です。BlueQuartz は、Cobalt Users Group の登録商標です。その他、記載された会社名およびロゴ、製品名などは該当する会社の商標または登録商標です。本ガイドでは、©、®、(TM) の表示を省略しています。ご了承くださいますようお願い申し上げます。

目 次

1. 本製品について

本製品は、企業ネットワーク、ISP、家庭内 LAN を外部から侵入するウイルスから守るようにデザインされた、「アンチウイルス・ゲートウェイ・ソリューション」です。

コンピューターウイルスはコンピュータに保管されたデータを脅かす重大な脅威の一つです。特にプラットホームの共通化やインターネットの普及により、ネットワークを通じたウイルスが広がっています。ウイルスはデータの破壊・改ざんの他、ネットワークを通じてデータを他者に送信することで企業秘密や個人情報が漏れる等の被害を及ぼします。 また重要なデータがない場合でも、そのコンピュータを通じウイルスの感染を広げることで他者に被害を与えることもあります。

システム管理者は本製品を使用することで、LAN 内の全てのマシンのウェブサイトへの接続、全てのメールの送受信について、ウイルス検査を一箇所で集中的に行うことができます。

本製品は HTTP、SMTP、POP、FTP による通信のウイルス検査を行います。

RHEL、CemtOS 対応の弊社アプライアンス・サーバー（パワードブルー・シリーズ）および Turbolinux Appliance Server 製品(TLAS3.0)をサポートし、容易にインストールや設定が行えます。

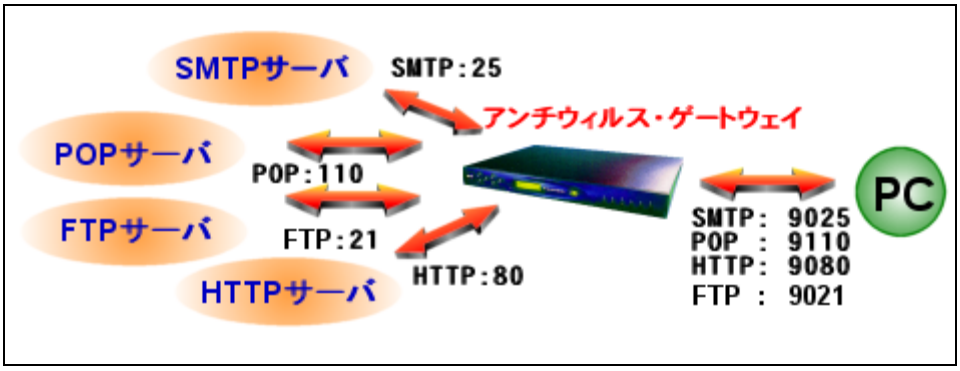
性能を重視しており高速に動作するため、大規模環境や高速ブロードバンド環境でもご利用いただけます。

また、RBL(Realtime Black List)、SURBL(SPAM URL Realtime Black LIST)サーバによるスパム判定と、スパム判定条件がカスタマイズ可能なデータベースを利用したスパム対策機能を備えています。

本製品のウイルス検出機構は、基本的にはプロキシサーバとして動作しますが、メールサーバと同時に機能できるように設計されています。目的に応じ、3 つの構成（モード）が選択できます。

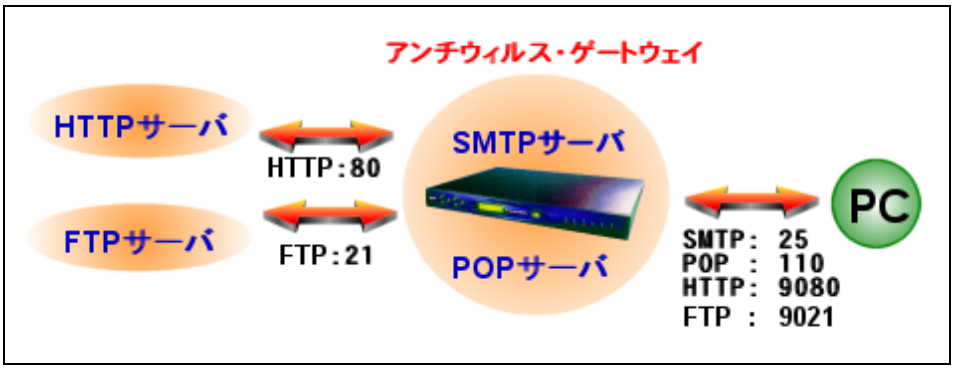
3つの動作モードの説明

「プロキシモード」 ― 代理サーバとして動作



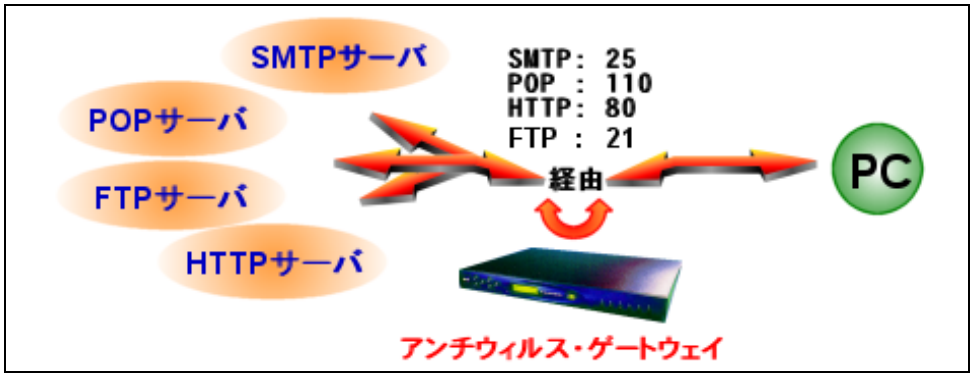
アンチウイルス・ゲートウェイは、プロキシサーバとしてウイルス検出を行います。アンチウイルス・ゲートウェイは、PC からメールの送受信の要求を受け取ると、あらかじめ登録されたメールサーバ（SMTP、POP）に対し、ウイルス検査を行いながらメールの送受信を行います。HTTP,FTP のウイルス検出もプロキシサーバとしての動作中に、ウイルス検査を行います。各サービスポートは、プロキシ用のポートが割り当てられます。

「メールサーバ共有プロキシモード」 ― メールサーバ上で動作



アンチウイルス・ゲートウェイは、メールサーバ上で、メールのウイルス検出を行います。SMTP と POP のポートは標準ポート(25、110)が利用できます。HTTP と FTP のウイルス検出については、プロキシサーバとして動作し、プロキシ用のポートが割り当てられます。

「透過プロキシモード」 ー　経路上でウイルスを検査（擬似的な透過）



アンチウイルス・ゲートウェイは、経路上で各サービスのウイルス検出を行います。この場合、クライアントはゲートウェイ IP として、アンチウイルス・ゲートウェイを指定します。このモードのメリットは、各クライアントの設定を変更しなくてもアンチウイルス・ゲートウェイの導入が可能なことです。この場合、アンチウイルス・ゲートウェイがサポートするイーサネットポートは eth0 のみです（ブリッジでは動作しません）。また、アンチウイルス・ゲートウェイ通過後はアドレス変換(NAT)が行われます。

「透過プロキシモード」を利用中、簡易ファイアウォール設定を操作すると IP パケットフィルタルールが上書きされるため、アンチウイルス・ゲートウェイが一時的に無効になります。この場合はサーバを再起動してください。

2. 機能一覧

2.1 機能概要

- さまざまなネットワークに対応し、ネットワーク全体をウイルスから守ります。
  - 社内ネットワーク
  - ISP
  - 家庭内ネットワーク
- 1 台で社内・ISP・家庭内の全マシンのネットワークアクセスを監視できます。
- ネットワーク上の各マシンの資源を消費しません。
- 既存の環境への導入・管理が簡単です。
- 大規模ネットワークだけでなく、低スペックなマシンでも十分動作します。

2.2 機能一覧

■ブラウザによる閲覧、メール送受信による通信を監視

- HTTP
- FTP
- SMTP
- POP

■インストールが簡単

- 管理サーバのインストーラおよび GUI に対応
- rpm または PKG 形式のインストールをサポート

■設定が簡単

- ３つの動作モードを選択することで、設定が簡単に行えます。メールサーバの設定変更が不要
- メールサーバにも用意にインストールできます。ネットワーク構成の変更が不要
- GUI の管理画面から簡単にインストール、アンインストールが行えます

■各種認証機能

- POP before SMTP 認証が可能
- 各プロトコルでプロキシ認証が可能
  (HTTP プロキシ認証、SMTP 認証、POP/FTP ユーザ制限)
  → プロキシ認証で、PAM (Pluggable Authentication Modules) を通じて、UNIX アカウント、LDAP、NIS、Radius 等との連携が可能（ただし、管理画面は未サポート）。
- 全プロトコルで IP アドレス、ホスト名、ドメイン名によるアクセス制御が可能
- SMTP 受信ドメイン制限により第三者中継が防止可能

- メールサーバの既存の SMTP 認証機能が利用可能
- メールサーバの既存の APOP 機能が利用可能

■ウイルス検出通知メッセージ

- メッセージを任意に編集可能
- メッセージで日本語が利用可能
- ウイルス検出時に管理者宛にメールを送信可能
- 通知メールでヘッダ・本文を確認可能

■柔軟な構成

- 透過プロキシが利用可能 (HTTP, SMTP, POP, FTP)
- 各ユーザが POP サーバを選択することが可能
- HTTP で送信するファイルのウイルス検査が可能 (POST／PUT メソッド対応)
- Microsoft の無料 Hotmail サービス(HTTP 接続)を Outlook から利用する場合にも対応。
- FTP 専用クライアントからの送受信にも対応
- 親プロキシ設定による多段接続が可能
- 親プロキシ設定により、特定のウェブサーバへの全ての接続の監視 (リバースプロキシ) が可能
- 任意の場所で動作するメールサーバと接続が可能
- 任意のメールサーバと接続が可能
- 同一マシンで動作する任意のメールサーバでも利用可能
- 受信用 SMTP、送信用 SMTP の別設定が可能

■ウイルス対策

- 豊富な実績のある F-Secure エンジンを使用
- 事実上全ての既存ウイルスに対応
- Windows、DOS、Microsoft Office、VBS、Linux 等のウイルスに対応
- 複数のエンジン (FS-Engine(Hydra), Aquarius) の組み合わせにより新種ウイルスへの迅速な対応
- 少ない誤検出
- 各種圧縮ファイルに対応 (ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2／6 階層まで)
- ウイルス定義ファイルの自動アップデートが可能

■ICAP サービスによるウイルススキャン

- ICAP サービスによるウイルススキャンに対応
- fsicapd デーモンが ICAP プロトコルを実行(RFC 3507 を参照)
- F-Secure テクノロジによるデータスキャン
- ICAPクライアントとして機能できるサードパーティHTTPプロキシとの連携[1]

[1] すべてのICAP対応製品に対応することを保証するものではありません。また、動作を保証するものではありません。

■スパム対策

- SMTP、POP ともにスパム検出が可能
- カスタム条件により、任意のヘッダ・本文等による優先度付きブラックリスト・ホワイトリストでスパムを検出
- RBL (Realtime Black List) により、スパム送信アドレスからのスパムを検出
- SURBL (SPAM URL Realtime Black List) により、本文中にスパムドメインの URL を含むスパムを検出
- スパムメールにスパム識別ヘッダ (X-Spam-Status: Yes)、を追加することにより、容易な振り分けが可能
- スパムメールの件名に指定文字列 ("[[SPAM]]"等) を付加することで、容易な振り分けが可能

■その他

- 拡張子、User-Agent、ファイルサイズ等によるファイルの通過・拒否設定が可能
- ActiveX／スクリプト (JavaScript／VBScript) のブロック機能
- squid 互換ログによるアクセス統計処理が可能
- syslog 等へのログの外部出力が可能
- https (暗号化 http) のプロキシ機能に対応
  ただし、https (SSL) については、暗号化されているためウイルス検査は行いません。
- ウイルス検出通知メールにウイルス識別ヘッダ (X-Virus-Status: infected) を追加することにより、容易な振り分けが可能

2.3 バージョン 4.0 からの変更箇所

2.3.1 新しい機能

- F-secure Real Time Protection Network のサポートが HTTP プロキシに追加されました。ホワイトリストとブラックリストの迅速な更新によって、問題のファイルを特定します。これは、システムリソースの節約とプロテクションを強化します。
- マルウェア操作能力が標準 ICAP インタフェースにより利用可能になりました。ICAP をサポートしたサードパーティの HTTP プロキシ製品との統合を可能にします。

2.3.2 名称およびパスの変更

- 製品内部で使用する名前 virusgw が fsigk (f-secure internet gatekeeper for Linux) に変更されました。これに伴い製品内部で virusgw を名前に使用していた複数のファイルの名前が変更されました。
- 構成ファイル virusgw.ini は、fsigk.ini に変更されました。
- ソフトウェア本体のインストール先が、/opt/f-secure/fsigk から /opt/f-secure/fsigk に変更されました。
- ウイルス検出やログで表示される検出名の開始文字列が、”VIRUSGW/” から “FSIGK/” に変更されました。

3. 動作環境

本製品が正常に動作するためには、以下の環境が必要です。

3.1 ハードウェア環境

■必須ハードウェア環境

CPU	x86 互換 CPU
MEMORY	512MB 以上
DISK	空きが 5GB 以上 (ファイルの一時保存に必要なサイズ以上)
NETWORK	TCP/IP 接続

■推奨ハードウェア環境

CPU	x86 互換 CPU 2GHz 以上
MEMORY	1GB 以上の空き
DISK	20GB 以上の空き
NETWORK	100BaseT 以上

3.2 対応プラットホーム

■対応プラットホーム

サーバー一覧	パワード・ブルー (Powered BLUE) 770 / 850 / 860 サーバアプライアンス ※上記サーバを、各々B770 / B850 / B860 と表記する場合があります。
	Turbolinux Appliance Server 3.0 搭載機

4. インストール

インストール方法の詳細については、各サーバのマニュアルをご参照ください。

4.1 アップデートに関する注意事項

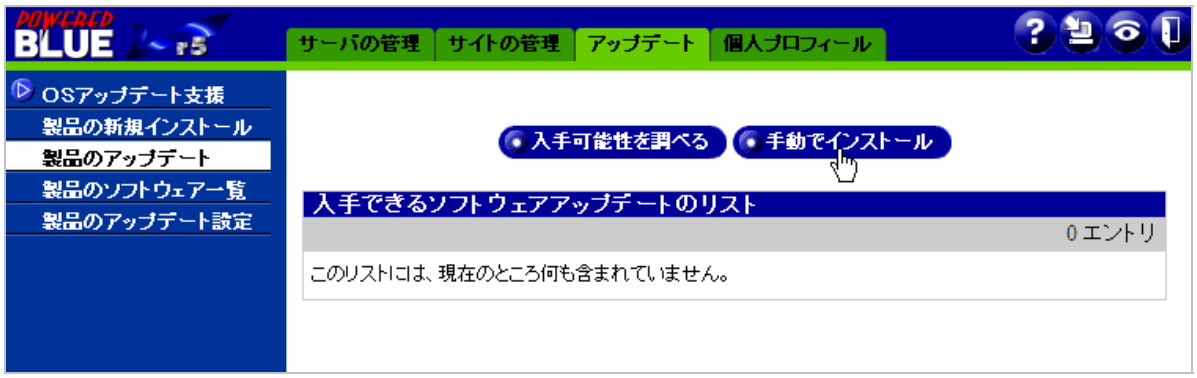
このソフトウェアは、バージョン４からのみのアップデートを実行することができます。万が一、バージョン３以前のソフトウェアを使用中の場合は、アンインストールしてから、本製品を新規にインストールしてください。

4.2 パワードブルー850/860 サーバーへのインストール（PKG 形式）

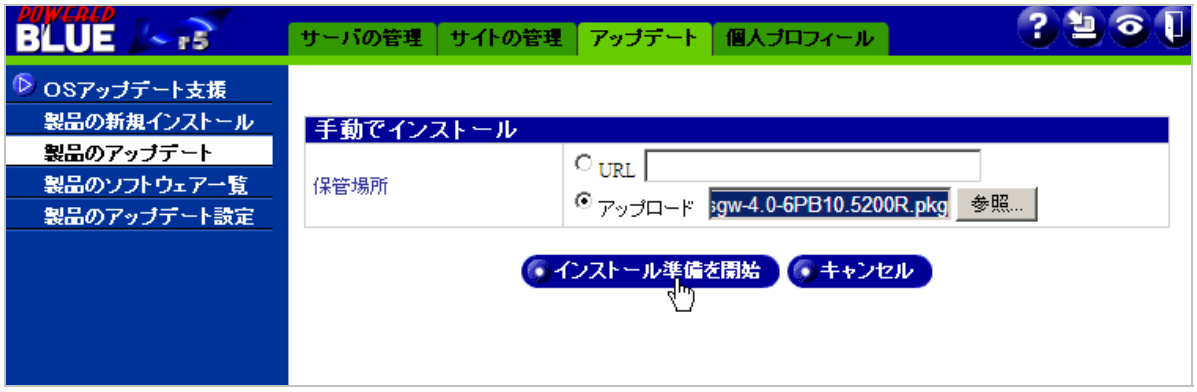
インストールは、サーバ管理画面の「アップデート」タブメニューの「製品の新規インストール」または「製品のアップデート」の「手動でインストール」で行います。インストール CD に含まれる、下記のファイル形式のインストールパッケージをインストールしてください。

mubit-virusgw-X.X-XXXX.XXXXX.pkg　（PKG 形式、X はバージョンおよびリリース番号）
例）mubit-virusgw-5.20-646PB1.5211Rc.pkg

（１）手動でインストールを選択



（２）インストールパッケージをアップロード



インストールパッケージファイルをアップロードし、「インストール準備を開始」ボタンをクリックし、インストールを開始します。

インストール終了後、ウェブブラウザの表示を更新させると、アンチウイルス・ゲートウェイのメニューが表示されます

Caution

６４ビットOSを使用する場合、３２ビットの実行環境（glibc、pam、libstdc++）が必要になります。３２ビット環境が見つからない場合インストールの際に自動的にインストールを試みます[2]。

Note

ウェブブラウザの表示の更新は、Internet Explorer や Mozilla Firefox の場合、タブメニュー内の表示更新機能や、Ctrl+r または F5 キー等のショートカットキーで行うことができます。

4.3 TLAS および B770 へのインストールインストール（RPM 形式）

インストールは、サーバ管理画面の「Turboplus」タブメニューの「他社製品のインストール」からインストールします。

アップグレード・インストールの場合も同様の操作でインストールします。この場合、前のバージョンのアンチウイルス・ゲートウェイが見つかれば、アップグレード・インストールが行われます。

インストール終了後、ウェブブラウザの表示を更新させると、アンチウイルス・ゲートウェイのメニューが表示されます。

Note

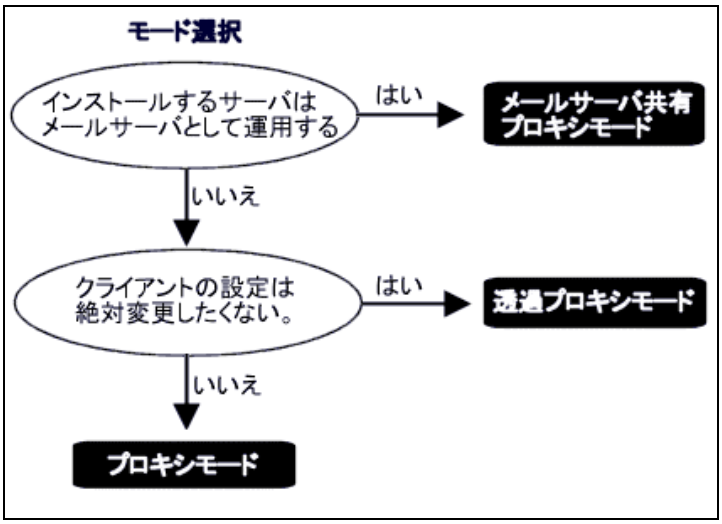
ウェブブラウザの表示の更新は、Internet Explorer や Mozilla Firefox の場合、タブメニュー内の表示更新機能や、Ctrl+r または F5 キー等のショートカットキーで行うことができます。

[2] RHEL6/CentOS6 (x86_64) の場合、glibc.i686 および pam.i686 、libstdc++.i686 がインストールされている必要があります。

5. 動作モードの説明

本製品を利用するには、最初に動作モードを決定してください。その後、必要な設定を行います。

３つの動作モードの内、使用したいモードを選択します。

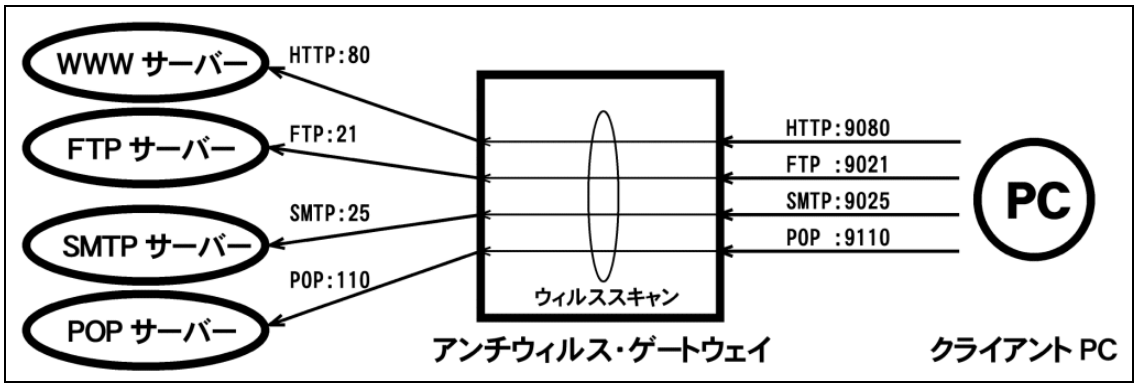


通常、インストール先のマシンがメールサーバの場合は、「メールサーバ共有プロキシモード」を選択します。プロキシサーバ（代理サーバ）として、接続を中継し、他のサーバとアクセスする場合は、「プロキシモード」を選択します。また、LAN 内から外部接続へのゲートウェイとしたい場合は、「透過プロキシモード」を選択することも可能です。

以下に、各動作モードについて説明します。

5.1「プロキシモード」

プロキシモードは、プロキシサーバ（代替サーバ）として、各サービス(HTTP,SMTP,POP,FTP)を中継し、ウイルス検査を行います。クライアントPCのアンチウイルス・ゲートウェイへの接続は、それぞれのサービスで割り当てられたプロキシポートへ接続する必要があります[5]。



Note

ウェブブラウザやメーラ等の各種クライアントのプロキシポートをそれぞれ指定された番号へ設定変更する必要があります。

5.1.1 HTTP 接続

クライアント PC のウェブブラウザは、アンチウイルス・ゲートウェイを経由してウェブサーバに接続し、ウイルス検査を行ったページを取得します。アンチウイルス・ゲートウェイはクライアントからの要求された URL に応じて適切なウェブサーバに接続します。（例：HTTP プロキシポート 9080）

5.1.2 SMTP 接続

メールクライアントは、アンチウイルス・ゲートウェイを経由して、あらかじめ設定されたメールサーバへ接続します。アンチウイルス・ゲートウェイは、メールの送信データのウイルス検査を行います。（例：SMTP プロキシポート 9025）

5.1.3 POP 接続

メールクライアントは、アンチウイルス・ゲートウェイを中継して、POP サーバと接続します。メールは、アンチウィル・ゲートウェイでウイルス検査を行った後、メールクライアントで受信します。あらかじめ設定した 1 台の POP サーバへ接続します。また、POP ユーザ名を「POP サーバのユーザ名@POP サーバ名」と指定することで任意の POP サーバに接続しウイルス検査を行うこともできます。（例：POP プロキシポート 9110）

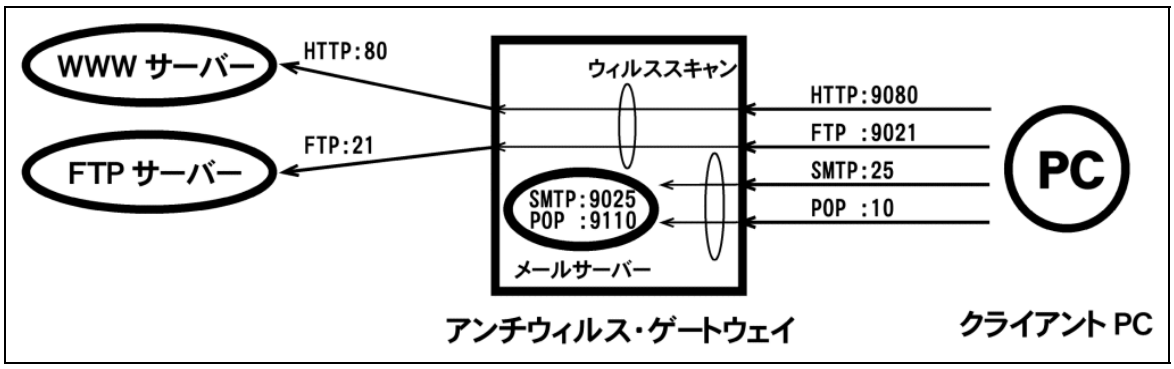
[5]図の例では、ウェブブラウザのプロキシサーバの設定は、アンチウイルス・ゲートウェイ（ポート9080）を指定します。メールクライアントでは、SMTP/POPサーバとしてアンチウイルス・ゲートウェイを指定し、各々のサービスポートは9025/9110を設定します。FTPクライアントも同様に、アンチウイルス・ゲートウェイのポート9110に接続するように設定します。

5.1.4 FTP 接続

FTP クライアントは、アンチウイルス・ゲートウェイを中継して、FTP サーバと接続します。データは、アンチウィル・ゲートウェイでウイルス検査を行った後、FTP クライアントで送受信します。あらかじめ設定した 1 台の FTP サーバへ接続します。また、FTP ユーザ名を「FTP サーバのユーザ名@FTP サーバ名」と指定することで任意の FTP サーバに接続しウイルス検査を行うこともできます。（例：FTP プロキシポート 9021）

5.2「メールサーバ共有プロキシモード」

メールサーバにアンチウイルス・ゲートウェイをインストールするモードです。HTTP と FTP に関しては、「プロキシモード」と同様にプロキシとして動作します。SMTP と POP については、その標準ポートでアンチウイルス・ゲートウェイが外部と接続し、ウイルス検査を行ってから、内部のメールサーバにデータを渡す形態をとります。そのため、クライアント PC からは、通常のメールサーバと変わらずにアクセスすることができます。



Note

SMTP および POP は標準ポートを利用するため、クライアント(メーラ)の設定は変更する必要はありません。ウェブブラウザや FTP クライアントは、プロキシ接続となるため接続ポートの設定変更が必要となります。

5.2.1 HTTP 接続

クライアント PC のウェブブラウザは、アンチウイルス・ゲートウェイを経由してウェブサーバに接続し、ウイルス検査を行ったページを取得します。アンチウイルス・ゲートウェイはクライアントからの要求された URL に応じて適切なウェブサーバに接続します。

5.2.2 SMTP 接続

メールサーバまたはメールクライアントからの接続要求（標準ポート 25）は、アンチウイルス・ゲートウェイに対して行われます。その後、アンチウイルス・ゲートウェイはサーバ内部の SMTP サーバと接続し、メールデータ転送の間にウイルス検査を行います(内部の SMTP サーバの待ち受けポートは、9025 が利用されます)。

5.2.3 POP 接続

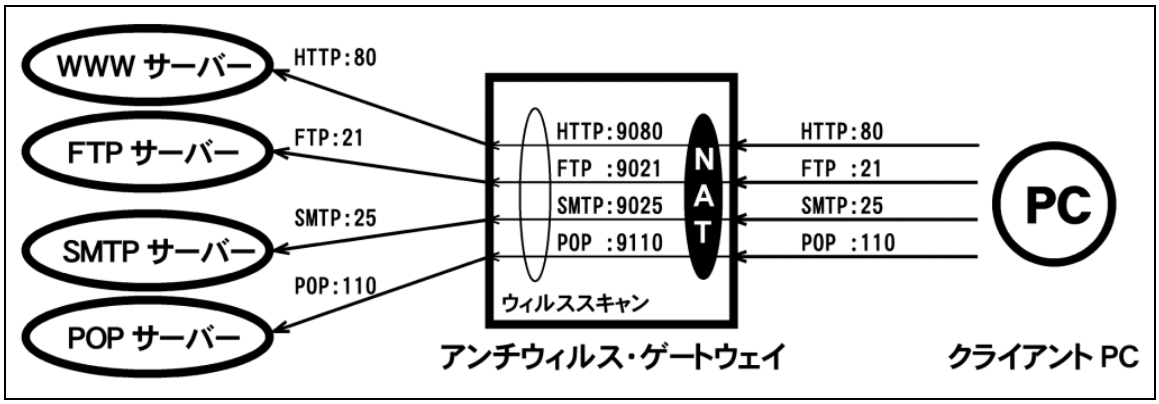
メールクライアントからの接続要求（標準ポート 110）は、アンチウイルス・ゲートウェイに対して行われます。アンチウイルス・ゲートウェイは、サーバ内部の POP サーバと接続しメールデータを受信します。メールは、アンチウィル・ゲートウェイでウイルス検査を行った後、メールクライアントに渡されます(内部の POP サーバの待ち受けポートは、9110 が利用されます)。

5.2.4 FTP 接続

FTP クライアントは、アンチウイルス・ゲートウェイを中継して、FTP サーバと接続します。データは、アンチウィル・ゲートウェイでウイルス検査を行った後、FTP クライアントで送受信します。あらかじめ設定した 1 台の FTP サーバへ接続します。また、FTP ユーザ名を「FTP サーバのユーザ名@FTP サーバ名」と指定することで任意の FTP サーバに接続しウイルス検査を行うこともできます。

5.3「透過プロキシモード」

このモードは、擬似的な透過装置として構成可能です。通常このモードでは、アンチウイルス・ゲートウェイを LAN 内に設置し、LAN 内の PC のデフォルト・ゲートウェイ設定をアンチウイルス・ゲートウェイに向けさせます。アンチウイルス・ゲートウェイ自体のデフォルト・ゲートウェイは、WAN への出口を指定します。クライアント PC の要求はすべてアンチウイルスを経由し、HTTP, FTP, SMTP, POP のウイルス検査が行われた後、外部へ転送します。



Note

クライアントの接続ポートの変更は必要ありません。クライアント PC のデフォルト・ゲートウェイは、アンチウイルス・ゲートウェイへ向けられている必要があります。

このモードのメリットは、クライアント PC の設定変更をしないでアンチウイルス・ゲートウェイの導入がが可能なことです。

留意点としては、アンチウイルス・ゲートウェイ通過後、アドレス変換（NAT）が行われるため、アンチウイルス・ゲートウェイの IP としてパケットが出て行く事です。

中継に使用するイーサネットポートはeth0 のみがサポートされます[6]。

[6]TLAS2.0/3.0では、WANポートがeth0です。ブリッジ構成には対応しておりません。

6. 一般的な設定例

一般的な設定方法を紹介します。

6.1 管理画面について

サーバ管理画面のメニュー「アンチウイルス GW」を表示してください。この最初のメニューの「アンチウイルス設定」で各プロキシサービスのウイルス検査を設定します。

「定義ファイル更新」は、ウイルスデータベースの更新設定を行います。更新のスケジュールも設定します。

「スパム検査設定」では、スパム検出のための設定を行います。データベースによる定義のほか、RBL サーバの指定が可能です。

「ログファイル」は、最新のログを表示します。

「隔離ディレクトリ」は、隔離されたウイルスが置かれるディレクトリが表示されます。

「サポート＆ヘルプ」は、マニュアルやシステム情報のダウンロードメニューを表示します。

6.2 電子メールサーバでウイルス検査を行う

電子メールサーバ上でウイルス検出を行います。この場合、「電子メール共有プロキシモード」を設定します。

このモードでは、アンチウイルス・ゲートウェイが SMTP ポート(25 番)で待ち受けます。よって、SMTP サービスのリレー設定や POP Before SMTP などの機能は、アンチウイルス・ゲートウェイ側が担当します。

HTTP および FTP プロキシは、プロキシモードの設定方法と同じです。

6.2.1 動作モードの選択

「電子メール共有プロキシモード」は、動作モードの

[2] 電子メールサーバと共用して構成する

を選択します。

簡易表示(推奨)は、チェック（有効）します。簡易表示が有効な場合、使用頻度の少ないメニュー項目を非表示にしたり、一部の項目を変更不可（リードオンリー）にします。

6.2.2 SMTP のウイルス検査を設定する

「SMTP Proxy」メニューで、SMTP のウイルス検査を設定します。

ウイルス検査を有効にする

デフォルトで有効になっています。このオプションは、簡易表示では設定できません。

ウイルス検出時の動作

ウイルスを検出した場合の動作を決定します。

最大同時接続数

アンチウイルス・ゲートウェイの SMTP プロキシの待ち受けプロセスの数になります。

受信ドメイン制限

公開サーバの場合、第三者からの中継を防止するために設定してください。メールの配信を受信先のドメインで制限します。注意点として、この機能を選択すると、中継そのものが制限されるため LAN 内のコンピュータも外部へ接続できなくなります。このため、外部へ接続する場合は、「除外ホスト」で外部へ接続するホストまたはネットワークを明記してください。

除外ホスト

受信ドメイン制限を除外するホストやネットワークを指定します。例えば、LAN あるいは LAN 側ゲートウェイを指定します。

この図の例では、自社ドメイン(example.com)にリレー先を制限し、LAN(10.0.0.0/24)を除外します。

POP Before SMTP

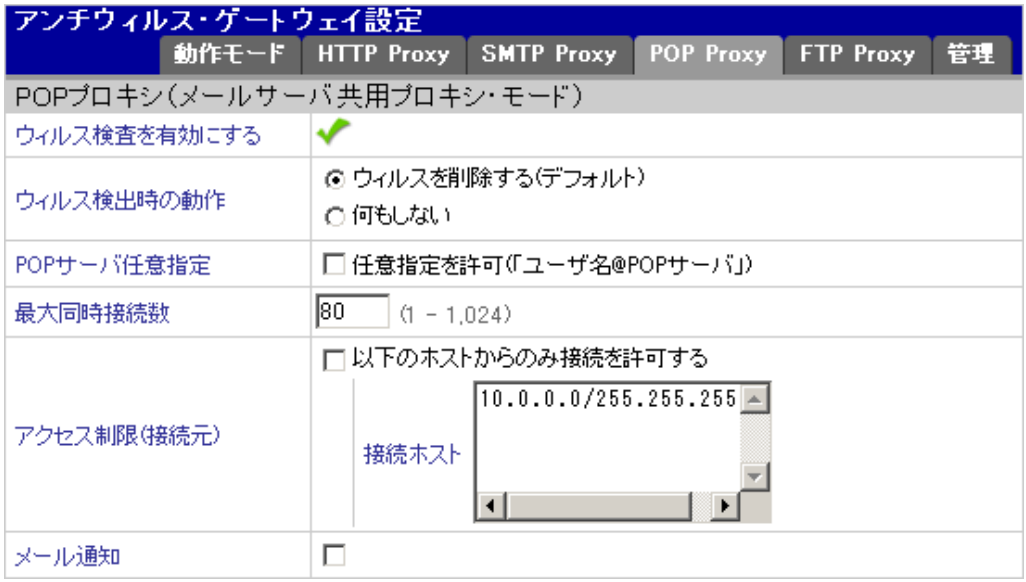
POP Before SMTP を有効にする場合、チェックしてください。

メール通知

ウイルスやスパムを検出した場合、「管理メール設定」で設定された管理者の電子メールアドレスへ、検出メッセージを送付します。

6.2.3 POP のウイルス検出を設定する

「POP Proxy」メニューで、POP のウイルス検査を設定します。



ウイルス検査を有効にする

デフォルトで有効になっています。このオプションは、簡易表示では設定できません。

ウイルス検出時の動作

ウイルスを検出した場合の動作を決定します。

POP サーバの任意指定

この機能が有効な場合、クライアント（メーラ）は、任意の POP サーバを指定することができます。メーラの POP 認証のユーザ名に “ユーザ名＠POP サーバ名”と指定することで、任意の POP サーバへ接続します。

最大同時接続数

アンチウイルス・ゲートウェイの POP プロキシの待ち受けプロセスの数になります。

アクセス制限

アクセスを制限する IP またはネットワークを指定することができます。

メール通知

ウイルスやスパムを検出した場合、「管理メール設定」で設定された管理者の電子メールアドレスへ、検出メッセージを送付します。

6.3 プロキシサーバとして使用する

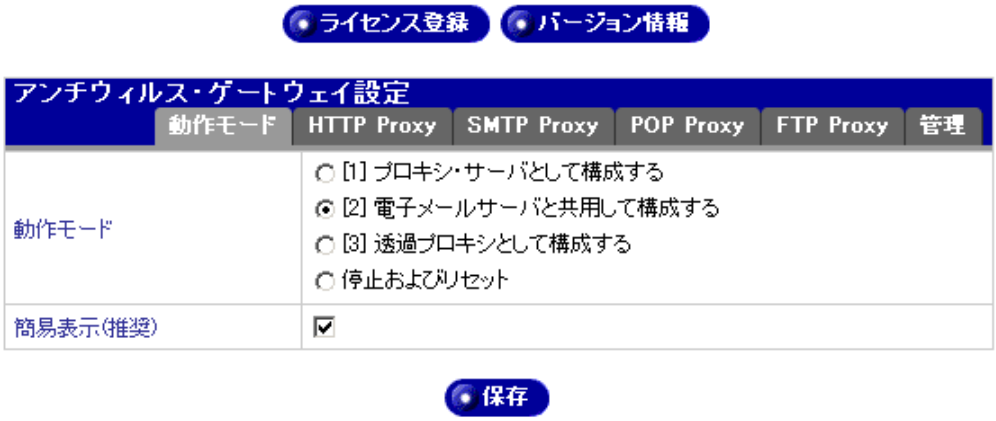
プロキシサーバとして構成します。
電子メールサーバとして利用しない場合のみ指定できます。

6.3.1 動作モードの選択

「電子メール共有プロキシモード」は、動作モードの

[1] プロキシサーバとして構成する

を選択します。



簡易表示(推奨)は、チェック（有効）します。簡易表示が有効な場合、使用頻度の少ないメニュー項目を非表示にします。

6.3.2 HTTP プロキシ設定

ウェブブラウザのプロキシサーバとして設定します。

HTTP プロキシを有効にする

HTTP プロキシを有効にします。

ポート番号

プロキシポート番号です。デフォルトでは 9080 番に設定されています。このオプションは、簡易表示では設定変更できません。設定する場合は、簡易表示をオフにしてください（詳細メニューの表示）。

ウイルス検出時の動作

ウイルスを検出した場合の動作を設定します。

最大同時接続数

クライアントから同時に接続できる最大数を設定します。指定した数のプロセスがクライアントからの接続に対して待機します。

アクセス制限

指定した IP アドレスまたはネットワークのリストからのみ接続を受け付けます。

アップロード検査

有効の場合、ファイル送信時のウイルス検査を行います。

メール通知

ウイルスやスパムを検出した場合、「管理メール設定」で設定された管理者の電子メールアドレスへ、検出メッセージを送付します。

6.3.3 SMTP プロキシ設定

SMTP プロキシとして設定し、上位の SMTP サーバ(172.16.0.1)へ接続します。

SMTP プロキシ

SMTP プロキシを有効にします。このとき、中継先の上位の SMTP サーバを指定します。SMTP サーバの SMTP ポートはデフォルトで 25 番です。SMTP ポート番号は、簡易表示では設定できません。

ポート番号

クライアント（メーラ）が接続するプロキシポート番号です。デフォルトでは、9025 番です。ポート番号は、簡易表示では変更できません。

Note

SMTP の標準ポート２５番を使用する場合、ポートが競合するため、サーバの SMTP サービスを停止するか待ち受けポートを２５番以外に変更する必要があります。プロキシモード時の SMTP サービスのポート変更は、「8.7.4　プロキシ時 SMTP ポート」で設定可能です。

ウイルス検査を有効にする

デフォルトで有効になっています。このオプションは、簡易表示では設定できません。

ウイルス検出時の動作

ウイルスを検出した場合の動作を決定します。

最大同時接続数

アンチウイルス・ゲートウェイの SMTP プロキシの待ち受けプロセスの数になります。

受信ドメイン制限

公開サーバの場合、第三者からの中継を防止するために設定してください。メールの配信を受信先のドメインで制限します。注意点として、この機能を選択すると、中継そのものが制限されるため LAN 内のコンピュータも外部へ接続できなくなります。このため、外部へ接続する場合は、「除外ホスト」で外部へ接続するホストまたはネットワークを明記してください。

除外ホスト

受信ドメイン制限を除外するホストやネットワークを指定します。例えば、LAN あるいは LAN 側ゲートウェイを指定します。

この図の例では、自社ドメイン(example.com)にリレー先を制限し、LAN(10.0.0.0/24)を除外します。

POP Before SMTP

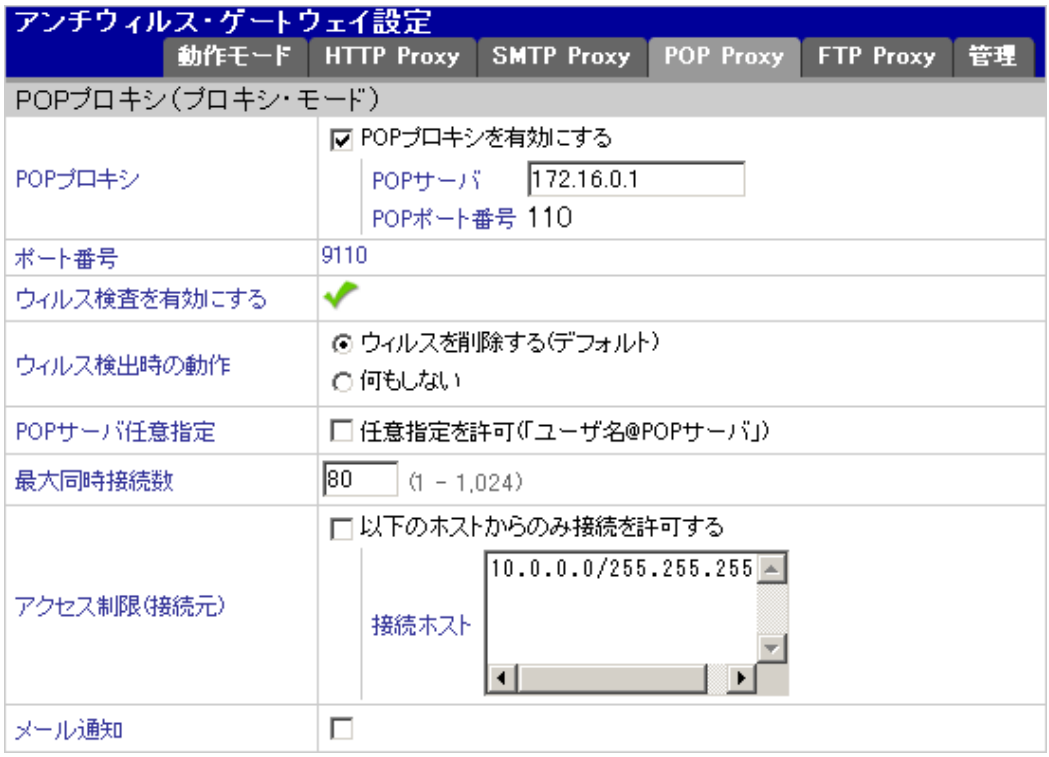
POP Before SMTP を有効にする場合、チェックしてください。

メール通知

ウイルスやスパムを検出した場合、「管理メール設定」で設定された管理者の電子メールアドレスへ、検出メッセージを送付します。

6.3.4 POP プロキシ設定

POP プロキシとして設定し、上位の POP サーバ(172.16.0.1)へ接続します。



POP プロキシ

POP プロキシを有効にします。このとき、中継先の上位の POP サーバを指定します。POP サーバの POP ポートはデフォルトで 110 番です。ポート番号は、簡易表示では変更できません。

ポート番号

クライアント（メーラ）が接続するプロキシポート番号です。デフォルトでは、9110 番です。ポート番号は、簡易表示では変更できません。

Note

POP の標準ポート１１０番を使用する場合、ポートが競合するため、サーバの POP サービスを停止する必要があります。

ウイルス検査を有効にする

デフォルトで有効になっています。このオプションは、簡易表示では変更できません。

ウイルス検出時の動作

ウイルスを検出した場合の動作を決定します。

POP サーバの任意指定

この機能が有効な場合、クライアント（メーラ）は、任意の POP サーバを指定することができます。メーラの POP 認証のユーザ名に “ユーザ名＠POP サーバ名”と指定することで、任意の POP サーバへ接続します。

最大同時接続数

アンチウイルス・ゲートウェイの POP プロキシの待ち受けプロセスの数になります。

アクセス制限

アクセスを制限する IP またはネットワークを指定することができます。

メール通知

ウイルスやスパムを検出した場合、「管理メール設定」で設定された管理者の電子メールアドレスへ、検出メッセージを送付します。

6.3.5 FTP プロキシ設定

FTP プロキシとして設定し、上位の FTP サーバ(172.16.0.1)へ接続します。

FTP プロキシ

FTP プロキシを有効にします。このとき、中継先の上位の FTP サーバを指定します。FTP サーバの FTP ポートはデフォルトで 21 番です。ポート番号は、簡易表示では変更できません。

ポート番号

FTP クライアントが接続するプロキシポート番号です。デフォルトでは、9021 番です。ポート番号は、簡易表示では変更できません。

ウイルス検査を有効にする

デフォルトは有効です。このオプションは、簡易表示では変更できません。

ウイルス検出時の動作

ウイルスを検出した場合の動作を決定します。

FTP サーバの任意指定

この機能が有効な場合、FTP クライアントは、任意の FTP サーバを指定することができます。FTP クライアントでユーザ名に “ユーザ名@FTP サーバ名”と指定することで、任意の FTP サーバへ接続することができます。

最大同時接続数

アンチウイルス・ゲートウェイの FTP プロキシの待ち受けプロセスの数になります。

アクセス制限

アクセスを制限する IP またはネットワークを指定することができます。

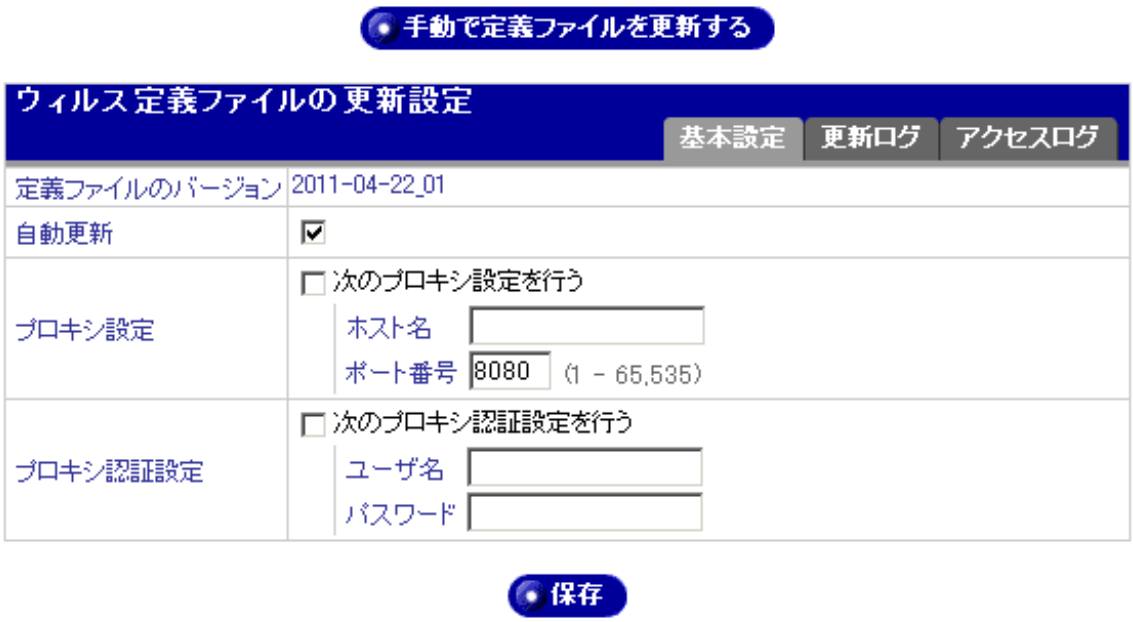
メール通知

ウイルスやスパムを検出した場合、「管理メール設定」で設定された管理者の電子メールアドレスへ、検出メッセージを送付します。

6.4 定義ファイル更新

定義ファイルの自動更新を設定します。自動更新が有効な場合、定期的（１時間毎）に定義ファイルを更新します。デフォルトは有効です。

「手動で定義ファイルを更新する」ボタンを実行すると、直ちに定義ファイルの更新プロセスが実効されます。定義ファイルのダウンロードには時間がかかる場合があります。新しい定義ファイルが段ロードされると、定義ファイルのバージョンの表記が更新されます。



本製品が設置されたネットワークから外部への HTTP アクセスが、プロキシサーバを経由しなければならない環境の場合、「プロキシ設定」でプロキシサーバを設定してください。

Note

定義ファイルは、**http://fsbwserver.f-secure.com/** から取得します。本製品がインストールされたサーバから、http://fsbwserver.f-secure.com/ へアクセスできる必要があります。定義ファイルの更新に失敗する場合は、上記サイトに対し HTTP ポート(80 番)が開かれているかネットワーク環境を確認してください。また、更新ログ(/opt/f-secure/fsigk/log/dbupdate.log)およびアクセスログ(/opt/f-secure/fsigk/log/　fsaua.log)もご確認ください。

7. 動作確認

設定が終了したら、以下の手順で動作確認を行ってください。

正しく動作しない場合は、以下のどちらかの方法でエラーログを参照してください。
エラーログは管理画面の「ログメニュー」から閲覧およびダウンロードが行えます。
コマンドラインからは、エラーログ
(`/opt/f-secure/fsigk/log/{http,smtp,pop,ftp}/error.log`) を参照します。

インターネットに接続できない場合、`/opt/f-secure/fsigk`ディレクトリで、`make eicar`コマンドを実行することで、テスト用ウイルスファイル (`eicar.com`) を生成できます。

7.1 HTTP の動作確認

以下の操作を行い、ウイルス検出表示が行われることを確認してください。

ウェブブラウザを立ち上げ、以下のサイトからテスト用ウイルス (eicar) をダウンロードする[7]。

http://www.eicar.org/

7.2 SMTP の動作確認

以下の操作を行い、受信者までウイルスが届かないことを確認してください。

1 ウェブブラウザを立ち上げ、以下のサイトからテスト用ウイルス (eicar) を入手する。

http://www.eicar.org/

テストウイルスのダウンロード時は、ダウンロード中に検知・削除されないようにブラウザのプロキシ設定を解除してください。

2 eicar を添付したメールを送信する。

[7] http://www.eicar.org/ のサイトのリンク ANTI MALWARE TEST FILE に移動し、DOWNLOAD のリンクを開いた場所に テスト用ウイルスがあります(2014年1月現在)。

POP の動作確認

以下の操作を行い、ウイルスが検出されたことを確認してください。

1 ウェブブラウザを立ち上げ、以下のサイトからテスト用ウイルス (eicar) を入手する。

http://www.eicar.org/

テストウイルスのダウンロード時は、ダウンロード中に検知・削除されないようにブラウザのプロキシ設定を解除してください。

2 eicar を添付したメールを送信する。

テストウイルスの送信時は、送信中に検知・削除されないように、アンチウイルス・ゲートウェイ・サーバを経由せずに送信してください。

3 メールを受信する。

7.4 FTP の動作確認

以下の操作を行い、ウイルスが検出されたことを確認してください。

1 ウェブブラウザを立ち上げ、以下のサイトからテスト用ウイルス (eicar) を入手する。

http://www.eicar.org/

テストウイルスのダウンロード時は、ダウンロード中に検知・削除されないようにブラウザのプロキシ設定を解除してください。

2 eicar ファイルを FTP で送受信する。

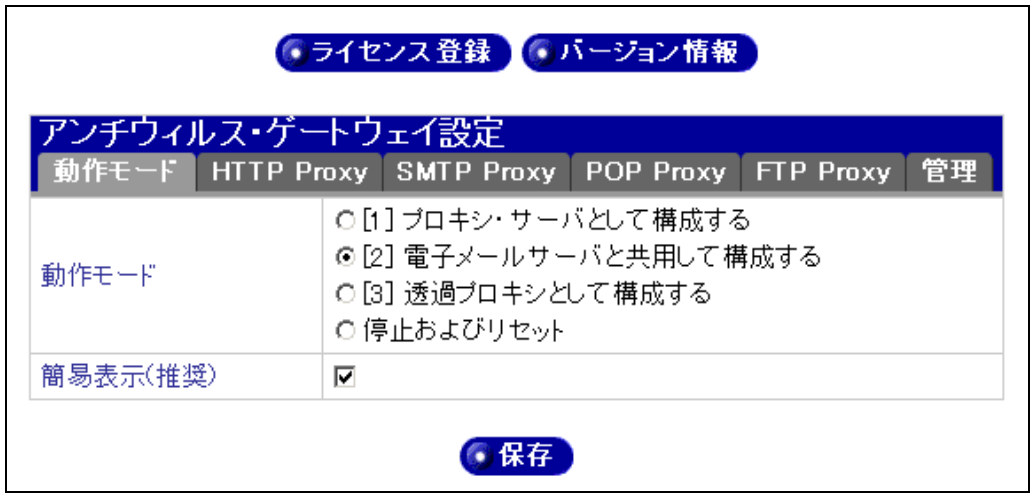
8. アンチウイルス設定

アンチウイルス設定メニューの詳細を説明します。

管理画面のアンチウイルス設定項目について説明します。

8.1 簡易表示について

インストール後の簡易表示の設定は、有効になっています。簡易表示は、一般に使用頻度の少ない機能を表示させません。。



簡易表示が無効の場合は、利用可能なすべてのメニューが表示されます。（下図では、メッセージ編集と認証ユーザリスト、ICAP サービスのメニューが表示されます）

動作モードによって、利用できる機能に制限があります。

本章で説明する機能の項目名で、その末尾にアスタリスク(*)が付くものは、簡易表示で省略されるメニューであることを示します。

8.2 動作モードの設定

「動作モード」タブメニューの下記の選択項目の中から、構成したいモードを選択してください。

[1] プロキシ・サーバとして構成する（プロキシモード）
[2] 電子メールサーバと共用して構成する（メールサーバ共有プロキシモード）
[3] 透過プロキシとして構成する（透過プロキシモード）

選択後、「保存」ボタンを押してモードを決定すると、選択した動作モードに対応した各プロキシ設定メニューが表示されます。

動作モードを変更すると、それまで設定された各プロキシの主要なパラメータはリセットされます。「停止およびリセット」を選択した場合は、主要なパラメータはリセットされ[8]、アンチウイルス・ゲートウェイのすべてのプロセスを停止します。

[8] 例えば、Pop-Before-SMTP の設定は、デフォルトの無効に戻されます。管理者の電子メール設定はリセットされません。

8.3 「HTTP Proxy」設定

HTTP プロキシの設定メニューです。

本章で説明する機能の項目名で、その末尾にアスタリスク(*)が付くものは、
簡易表示で省略されるメニューであることを示します。
動作モードによって、表示されるメニューが異なります。

8.3.1 HTTP プロキシを有効にする

チェックボックスで HTTP プロキシサービスの起動・終了を設定します。

8.3.2 ポート番号

プロキシサービスのポート番号です。

8.3.3 ウイルス検査を有効にする

ウイルス検査の有無を指定します。通常はチェックします。

8.3.4 ウイルス検出時の動作

ウイルス検出時の動作を選択します。通常は削除します。

8.3.5 ウイルス隔離*

ウイルスを隔離保存します。
隔離先は、/home/spool/virusgw/quarantine　ディレクトリです。
十分なディスク容量がある場合のみ指定してください。

8.3.6 中継サーバの指定*

全ての接続を指定したサーバに中継します
プロキシを多段で利用する場合、親となるプロキシを指定します。
リバースプロキシとして動作させる場合にはウェブサーバを指定します。

8.3.7 最大同時接続数

クライアントから同時に接続できる最大数を設定します。指定した数のプロセスがクライアントからの接続に対して待機します。

アクセスが集中しサーバの負荷が高くなると、メール(sendmail)等の他のサービスの動作を阻害する原因[9]となりますので、適正な値を設定してください。

利用している接続数は、アクセスログ (`access.log`) の [内部プロセスID] で確認できます。

この値を増やすと同時に接続できる数が増えますが、同時接続数が増えた場合にはメモリを消費します。メモリ消費量は 1 接続あたり約 500KB 程度です。
最大接続数に達した場合は、エラーログに警告が表示されます。
不明な場合、まずは 50～200 程度で様子を見ることをお勧めします。通常、2000 以内で設定します。

同時接続数が増加することにより、CPU の負荷は高くなります。メールサーバ共有プロキシモードの場合、HTTP プロキシによる CPU の過負荷が電子メールの動作を遅延させる可能性があります。この場合、同時接続数を少なくし、CPU の負荷を低減してください。

8.3.8 アクセス制限（接続元）

指定したホスト一覧からの接続のみ受け付けます。
[DNS 逆引き]を有効にするとホスト名・ドメイン名での指定も可能になります。

➔ 記述例については「8.14 アクセス制御」を参照してください。

ウェブ管理画面で [接続元] を編集すると、
`/opt/f-secure/fsigk/conf/hosts.allow`の`http_from`項目に反映されます。

8.3.9 プロキシ認証を行う*

「認証ユーザリスト」で編集したリストを使って、プロキシ認証を行います。

認証には PAM(Pluggable Authentication Modules)を用いており、認証方式を /etc/pam.d/fsigk_http ファイルで変更することも可能です。

➔ 詳細は「8.13 プロキシ認証について」を参照してください。

8.3.10 検査除外ユーザエージェント*

指定した User-Agent を持つクライアントからの接続に対してはウイルス検査を行いません。通常は、全てのデータを一度保存し、ウイルス検査を行った後にクライアントへの送信を開始しますが、指定

[9] Sendmail はロードアベレージがある一定の値まで高くなるとサービスを停止します。

した User-Agent のクライアントからの接続に対しては、受け取ったデータを順次転送します。ストリーム型のクライアントや、タイムアウトを発生しやすいクライアントを利用する場合に設定します。指定はコンマ (",") 区切りで行います。また、前方一致で検索します。大文字小文字は区別します。最大で 1999 バイトまで設定できます。


Caution

なお、ここでの設定の有無に関わらず、以下の User-Agent に対しては必ずウイルス検査を省略します。
既定の除外 User-Agent
- “Service Pack Setup” (Microsoft Windows のサービスパックインストーラ)
- “Office Update” (Microsoft Office のアップデートプログラム)
- “Symantec LiveUpdate” (Symantec 社の定義ファイル更新プログラム)
- “TMhtload” (TrendMicro 社の定義ファイル更新プログラム)
- “GETDBHTP” (F-Secure の定義ファイル更新プログラム(getdbhtp))
- “RealPlayer” (Real Player)
- “RMA” (Real Player)
- “NSPlayer” (Microsoft Windows Media Player)
- “ urlgrabber” (Linux YUM パッケージ更新プログラム)
- “Microsoft BITS” (Microsoft Windows Update)
- “Windows-Update-Agent” (Microsoft Windows Update)
- “Adobe Update Manager” (Adobe のアップデートプログラム)

8.3.11 検査除外ホスト*

指定したホストへの接続に対してはウイルス検査を行いません。通常は、全てのデータを一度保存し、ウイルス検査を行った後にクライアントへの送信を開始しますが、指定したホストへの接続に対しては、受け取ったデータを順次転送します。

➲ 記述例については「8.14　アクセス制御」を参照してください。


Note

管理画面で [ホスト名] を編集すると、/opt/f-secure/fsigk/conf/hosts.allow のhttp_pass_to項目に反映されます。

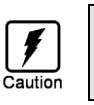
8.3.12 検査除外ファイル名*

指定したファイル、拡張子に対してはウイルス検査を行いません。
通常は、全てのデータを一度保存し、ウイルス検査を行った後にクライアントへの送信を開始しますが、指定したファイル、拡張子に対しては、受け取ったデータを順次転送します。
名前はコンマ (",") 区切りの後方一致で指定し、大文字小文字は区別しません。
また、圧縮ファイル内のファイルについても適用されます。圧縮ファイル内のファイルでファイル名/拡張子と一致した場合、該当ファイルについては検査を行いません。圧縮ファイル内の他のファイルについては検査を行います。
最大で 1999 バイトまで設定できます。

8.3.13 ファイルサイズ*

ファイルの指定サイズ以上の部分について、ウイルス検査を行いません。

通常は、全てのデータを一度保存し、ウイルス検査を行った後クライアントへの送信を開始しますが、指定サイズ以上の部分については、受け取ったデータを順次転送します。



この設定を行った場合、大きいファイルに含まれるウイルスが検出できないことがありますのでご注意ください。

8.3.14 リスクウェア検査*

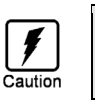
リスクウェア検査を有効にします。明らかなウイルス以外にリスクウェアも検出するようになります。リスクウェアの詳細については、「13.15　リスクウェア名称」を参照してください。

検査除外リスト

指定したリスクウェアについては検出しなくなります。
リスクウェアは”Category.Platform.Family”という名前で指定します。Categoriy, Platform, Family にはワイルドカード(*)を使用できます。たとえば「Client-IRC.*.*」は Client-IRC カテゴリのすべてのリスクウェアをスキャン対象外にします。
最大で 1999 バイトまで指定できます。
設定ファイル中では、セミコロン(“;”)区切りで指定します。

8.3.15 最大検査時間*

ファイル検査の最大時間を設定します。
0 を指定した場合、検査時間の制限をしません。
デフォルトは 90 秒です。



検査に時間がかかる場合、設定時間で検査を終了します。検査時間を短く設定するに従い、圧縮ファイル等で検査できる範囲が少なくなることがありますのでご注意ください。

8.3.16 アップロード検査

ファイル送信時のウイルス検査を行います。
無効の場合は受信ファイルの検査を行いますが、有効にすると送受信両方のファイルの検査を行います。POST メソッドで送信される multipart/form-data 形式のデータ、および PUT メソッドで送信されるファイル中のファイルのウイルス検査を行います。
有効にした場合、POST/PUT での送信時には、クライアントからの送信内容を一度全て保存し、ウイルス検査を行った後にサーバに接続・送信します。そのため、POST/PUT 送信時に、多少の動作速度の低下及び遅延が発生します。
PUT で検出した場合の応答行は"HTTP/1.0 403 Forbidden"になります。
ウイルス検査設定が無効の場合、この項目は利用できません。(有効にしてもウイルス検査は行いません。)

8.3.17 Keep-Alive 接続*

Keep-Alive 接続(Persistent Connection)を利用します。実際には、サーバとクライアントが Keep-Alive に対応している必要があり、以下のすべてを満たす場合に Keep-Alive 接続になります。

- Keep-Alive 接続設定が有効

- HTTP/1.1 の応答ヘッダで Connection が close ではない、又は HTTP/1.0 応答で Connection が keep-alive で始まる。
- 応答ヘッダで、Content-Length が 1 以上、又は応答コードが 304 か 204 か 1xx
- 要求ヘッダ、応答ヘッダに Content-Length が 2 回以上存在しない。
- ウイルス検出応答でない
- サーバへの接続が成功し、エラーが発生していない
- FTP over HTTP でない

タイムアウト（秒）

Keep-Alive 接続のタイムアウト時間(秒数)を 1 以上で指定します。HTTP 応答が終了してから指定時間が経過すると該当セッションを切断します。なお、Keep-Alive 接続を行っている間、処理を行うプロキシプロセスが 1 つ占有します。増加させる場合は、最大同時接続数に余裕があることをご確認ください。

8.3.18 匿名モード*

サーバにプロキシ及びクライアントに関する情報 (Via, X-Forwarder-For ヘッダ) を送付しません。

8.3.19 DNS 逆引き*

接続元の IP アドレスの DNS 逆引きを行います。
有効にすると [アクセス制御]=[接続元] のホスト名・ドメイン名指定が可能になり、アクセスログのアクセス元をホスト名で表示します。
ただし、動作速度が多少低下します。

8.3.20 メール通知

ウイルス検出時に管理者へメールで通知を行います。
通知メッセージ自身が検出されることを防止するため、ヘッダには "X-Admin-Notification-Id: [番号]" を付加して通常のメールと識別します。[番号] には、インストール時に乱数が設定ファイルの `admin_notification_id`として記述されます。

8.4 「SMTP Proxy」設定

SMTP プロキシの設定メニューです。

本章で説明する機能の項目名で、その末尾にアスタリスク(*)が付くものは、簡易表示で省略されるメニューであることを示します。
動作モードによって、表示されるメニューが異なります。

8.4.1 SMTP プロキシ

チェックボックスで SMTP プロキシサービスの起動・終了を設定します。
中継先の SMTP サーバのホスト名・ポート番号を指定します。
ポート番号は通常 25 番です

8.4.2 ポート番号

プロキシサービスのポート番号。プロキシモードでの、デフォルトは 9025 番です。

8.4.3 ウイルス検査を有効にする

ウイルス検査の有無を指定します。通常はチェックします。
ウイルス検査・スパム検査の両方を有効にした場合、ウイルス検査の結果が優先します。

8.4.4 ウイルス検出時の動作

[ウイルスを削除し、受信者に通知する（デフォルト）]
ウイルスを削除して、検出メッセージをメールで受信者に送付します。検出メッセージを受信者にも通知したい場合に選択してください。

**ウイルスメールの受信者は詐称されていることが多くなっています。
外部へのメールについて受信者へ通知を行った場合、無関係の第三者へ通知メールが送付されてしまします。
外部へのメールを処理する場合、受信者への通知は行わないでください。**

[ウイルスを削除し、送信者に通知する]
ウイルスを削除し、検出メッセージをメールで送信者に送付します。
送信者は偽造が可能なため、通常利用しません。

**ウイルスメールの送信者は詐称されていることが多くなっています。
外部からのメールについて送信者へ通知を行った場合、無関係の第三者へ通知メールが送付されてしまします。
外部からのメールを処理する場合、送信者への通知は行わないでください。**

[ウイルス感染メールの受信を拒否します]
ウイルス検出メールの送信を拒否します。SMTP セッション内で以下のエラーを返すことで、メーラやメールサーバに直接通知します。

554 Infected by [ウイルス名]

[ウイルス感染メールを削除し、何もしません]
ウイルス検出メールを削除します。検出メッセージは送信しません。

[何もしない]
ウイルスを検出しても何にもしません。通常は利用しません。
ログへの記録・管理者通知・ヘッダへの X-Virus-Status:の付加は行います。

8.4.5 ウイルス隔離*

ウイルスを隔離保存します。
隔離先は、/home/spool/virusgw/quarantine　ディレクトリです。
十分なディスク容量がある場合のみ指定してください。

8.4.6 最大同時接続数

クライアントから同時に接続できる最大数を設定します。指定した数のプロセスがクライアントからの接続に対して待機します。
利用している接続数は、アクセスログ (`access.log`) の [内部プロセスID] で確認できます。

この値を増やすと同時に接続できる数が増えますが、同時接続数が増えた場合にはメモリを消費します。メモリ消費量は 1 接続あたり約 500KB 程度です。
最大接続数に達した場合は、エラーログに警告が表示されます。
不明な場合、まずは 50 程度で様子を見ることをお勧めいたします。通常、200 以内で設定します。

8.4.7 受信ドメイン制限

サーバを公開する場合は、第三者中継を防止するために、受信ドメイン制限（「指定されたドメインで受信を制限する」）を有効にしてください。

受信するドメイン一覧を指定します。指定以外のドメイン宛のメールは拒否します。
ドメイン名はメールアドレス中の最初の "@" 以降を使用します。また、この項目を有効にした場合、"!" 及び"%"が含まれているアドレスは拒否します。ドメイン名部分がないアドレスは拒否しません。
[SMTP 認証]、[POP before SMTP 認証] を有効にした場合でも、指定ドメインについては認証なしで送信できます。

➲　記述例については「8.14　アクセス制御」を参照してください。

ウェブ管理画面で [受信先(RCPT)ドメインの制限] を編集すると、
`/opt/f-secure/fsigk/conf/hosts.allow`の`smtp_rcpt`項目に反映されます。

除外ホスト

除外ホストは、受信ドメイン制限を受けないホストやネットワークを指定します。通常、LAN から外部へ電子メールを送信するために利用します。
除外ホストで指定されたホストやネットワークは、内部のネットワークと見なされるため、このエリアから送信された電子メールはスパム検査の対象から除外されます。

8.4.8 アクセス制限(接続元)*

指定したホスト一覧からの接続のみ受け付けます。
[DNS 逆引き]を有効にするとホスト名・ドメイン名での指定も可能になります。

➲ 記述例については「8.14 アクセス制御」を参照してください。

ウェブ管理画面で [接続元] を編集すると、
/opt/f-secure/fsigk/conf/hosts.allowのsmtp_from項目に反映されます。

8.4.9 プロキシ認証を行う*

「認証ユーザリスト」で編集したリストを使って、プロキシ認証を行います。

認証には PAM(Pluggable Authentication Modules)を用いており、認証方式を /etc/pam.d/fsigk_smtp ファイルで変更することも可能です。

➲ 詳細は「8.13 プロキシ認証について」を参照してください。

8.4.10 POP Before SMTP

POP before SMTP 認証を有効にします。SMTP プロキシで POP before SMTP 認証を行う場合、POP プロキシと同時に動作させます。POP プロキシを通じて認証されたクライアントホスト (IP アドレス) に対して、一定期間 SMTP プロキシの利用が許可されます。
アンチウイルス・ゲートウェイまたはメールサーバの SMTP 認証も同時に利用する場合、SMTP 認証と POP before SMTP 認証のいずれかに成功した場合に送信できます。
[ドメイン受信制限] も同時に有効にした場合、指定ドメインについては認証なしでも送信できます。

有効期限は認証が有効な時間(分)を指定します。

8.4.11 ActiveX 拒否*

ActiveX が埋め込まれた HTML メールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_ACTIVEX" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。また、ウイルス検査が無効の場合、この項目での検査はできません。

8.4.12 スクリプト拒否*

スクリプト(JavaScript, VBScript 等)を含む HTML メールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_SCRIPT" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。また、ウイルス検査が無効の場合、この項目での検査はできません。

8.4.13 メール分割拒否*

分割メールを拒否します。メールヘッダの Content-Type フィールドに message/partial を含むメールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。

8.4.14 ZIP/RAR 拒否*

暗号化書庫ファイル(ZIP,RAR)を含むメールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_ENCRYPTED" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。また、ウイルス検査が無効の場合、この項目での検査はできません。

8.4.15 ファイル拒否*

指定したファイル名、拡張子の添付ファイルを含むメールを拒否します。
名前は後方一致で指定し、大文字小文字は区別しません。
"ALL" を指定すると、ファイルを含むメール全てを拒否します。
圧縮ファイル内のファイルのファイル名には適用されません。
最大で 1999 バイトまで設定できます[10]。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。
検出名称は "FSIGK/POLICY_BLOCK_EXT" になります。
設定例：.COM,.PIF,.EXE,.BAT

8.4.16 検査除外ファイル名*

指定したファイル、拡張子に対してはウイルス検査を行いません。
名前は後方一致で指定し、大文字小文字は区別しません。

[10] 正確には、設定ファイル内に記述可能なサイズを意味します。複数のファイルを指定する場合は、区切り文字に１バイトずつ消費します。

また、圧縮ファイル内のファイルについても適用されます。圧縮ファイル内のファイルでファイル名/拡張子と一致した場合、該当ファイルについては検査を行いません。圧縮ファイル内の他のファイルについては検査を行います。
最大で 1999 バイトまで設定できます[11]。

8.4.17 テキスト本文検査*

メールのテキスト本文の検査を行ないます。この設定の有無に関わらず、テキスト形式の添付ファイルや、HTML 形式の本文等は検査します。有効にすると動作速度が多少低下します。
テキスト形式の本文については実行されることがないため、通常この項目を設定する必要はありません。

8.4.18 HTML 全体の検査*

メールの HTML 部分について、スクリプトや ActiveX を呼び出す部分などのウイルスが動作する部分以外についても検査を行います。有効にすることで、ウイルス以外の疑わしいメール(詐欺メールや壊れたウイルス等)の一部を検出します。この設定の有無に関わらず、HTML に含まれるウイルスは検出します。有効にすると動作速度が多少低下します。
設定の有無に関わらずウイルスは検出されるため、通常この項目を設定する必要はありません。

8.4.19 リスクウェア検査*

リスクウェア検査を有効にします。明らかなウイルス以外にリスクウェアも検出するようになります。リスクウェアの詳細については、「13.15　リスクウェア名称」を参照してください。

検査除外リスト
指定したリスクウェアについては検出しなくなります。
リスクウェアは”Category.Platform.Family”という名前で指定します。Categoriy, Platform, Family にはワイルドカード(*)を使用できます。たとえば「Client-IRC.*.*」は Client-IRC カテゴリのすべてのリスクウェアをスキャン対象外にします。
最大で 1999 バイトまで指定できます。
設定ファイル中では、セミコロン(“;”)区切りで指定します。

8.4.20 ポート 587 転送

このオプションを有効にすると、外部からの 587 番ポートへのトラフィックを 25 番ポートへ転送します。サブミッションポートへの接続を 25 番ポートへリダイレクトすることで、サブミッションポートの通信のウイルス検査を行うことができます。
このオプションを有効にした場合、使用されない SMTP サーバのサブミッションポート設定は無効にしてください。「メールサーバ共有プロキシモード」でのみ設定できます。

[11]正確には、設定ファイル内に記述可能なサイズを意味します。複数のファイルを指定する場合は、区切り文字に 1 バイトずつ消費します。

8.4.21 最大検査時間*

ファイル検査の最大時間を指定します。検査に時間がかかる場合、設定時間で検査を終了します。短く設定するに従い、圧縮ファイル等で検査できる範囲が少なくなることがありますのでご注意ください。0(ゼロ)を指定した場合、検査時間の制限をしません。デフォルトは 90 秒です。

8.4.22 匿名モード*

プロキシでヘッダ情報(Received ヘッダ)を追加しません。

8.4.23 DNS 逆引き*

DNS の逆引きを行います。
有効にすると[アクセス制御]のホスト名・ドメイン名指定が可能になり、アクセスログのアクセス元をホスト名で表示します。 但し、動作速度が多少低下します。

8.4.24 メール通知

管理者へメールで通知を行います。
送信先アドレス・メールサーバは、「管理メール」で設定します。

8.5 「POP Proxy」設定

POP プロキシの設定メニューです。

本章で説明する機能の項目名で、その末尾にアスタリスク(*)が付くものは、簡易表示で省略されるメニューであることを示します。
動作モードによって、表示されるメニューが異なります。

8.5.1 POP プロキシ

チェックボックスで POP プロキシサービスの起動・終了を設定します。
中継先の POP サーバのホスト名・ポート番号を指定します。
POP ポート番号は、通常 110 番を指定します。

8.5.2 ポート番号

プロキシサービスのポート番号。プロキシモードでの、デフォルトは 9110 番です。

8.5.3 ウイルス検査を有効にする

ウイルス検査の有無を指定します。通常はチェックします。

8.5.4 ウイルス検出時の動作

ウイルス検出時の動作を選択します。
通常は削除します。
削除しない場合も、ログへの記録・管理者通知・ヘッダへの X-Virus-Status:の付加は行います。

POP プロトコルの仕様上困難なため、メール自身を完全に削除してユーザに届かないようにすることはできません。

8.5.5 ウイルス隔離*

ウイルスを隔離保存します。
隔離先は、/home/spool/virusgw/quarantine　ディレクトリです。
十分なディスク容量がある場合のみ指定してください。

8.5.6 POP サーバの任意指定

クライアントでの POP サーバ選択を許可します。

メーラのユーザ名に「ユーザ名@POP サーバ名」(又は「ユーザ名#POP サーバ名」)と指定することで POP サーバをユーザが指定できます。

8.5.7 認証ユーザ制限*

「認証ユーザリスト」で編集したリストのユーザ名を使って、接続するユーザの制限を行います。

認証には PAM(Pluggable Authentication Modules)を用いており、認証方式を /etc/pam.d/fsigk_pop ファイルで変更することも可能です。

➲ 詳細は「8.13 プロキシ認証について」を参照してください。

8.5.8 最大同時接続数

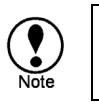
クライアントから同時に接続できる最大数を設定します。指定した数のプロセスがクライアントからの接続に対して待機します。
利用している接続数は、アクセスログ (access.log) の [内部プロセスID] で確認できます。

この値を増やすと同時に接続できる数が増えますが、同時接続数が増えた場合にはメモリを消費します。メモリ消費量は 1 接続あたり約 500KB 程度です。
最大接続数に達した場合は、エラーログに警告が表示されます。
不明な場合、まずは 50 程度で様子を見ることをお勧めいたします。通常、200 以内で設定します。

8.5.9 アクセス制限(接続元)

指定したホスト一覧からの接続のみ受け付けます。
「DNS 逆引き」を有効にするとホスト名・ドメイン名での指定も可能になります。

➲ 記述例については「8.14 アクセス制御」を参照してください。

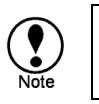


ウェブ管理画面で [接続元] を編集すると、
/opt/f-secure/fsigk/conf/hosts.allowのpop_from項目に反映されます。

8.5.10 アクセス制限(接続先)*

指定したホスト一覧への接続のみ受け付けます。

➲ 記述例については「8.14 アクセス制御」を参照してください。



ウェブ管理画面で [接続先] を編集すると、
/opt/f-secure/fsigk/conf/hosts.allowのpop_to項目に反映されます。

8.5.11 ActiveX 拒否*

ActiveX が埋め込まれた HTML メールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_ACTIVEX" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います。
また、ウイルス検査が無効の場合、この項目での検査はできません。

8.5.12 スクリプト拒否*

スクリプト (JavaScript, VBScript 等) を含む HTML メールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_SCRIPT" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います。
また、ウイルス検査が無効の場合、この項目での検査はできません。

8.5.13 メール分割拒否*

分割メールを拒否します。メールヘッダの Content-Type フィールドに message/partial を含むメールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。

8.5.14 ZIP/RAR 拒否*

暗号化書庫ファイル (ZIP, RAR) を含むメールを拒否します。
検出名称は "FSIGK/POLICY_BLOCK_ENCRYPTED" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[ウイルス検出時の動作]に従います。また、ウイルス検査が無効の場合、この項目での検査はできません。

8.5.15 ファイル拒否*

指定したファイル名、拡張子の添付ファイルを含むメールを拒否します。
名前は、後方一致で指定し、大文字小文字は区別しません。
"ALL" を指定すると、ファイルを含むメール全てを拒否します。
圧縮ファイル内のファイルのファイル名には適用されません。
最大で 1999 バイトまで設定できます[12]。
検出名称は "FSIGK/POLICY_BLOCK_EXT" になります。
検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います
設定例：.COM,.PIF,.EXE,.BAT

8.5.16 検査除外ファイル名*

指定したファイル、拡張子に対してはウイルス検査を行いません。
名前は後方一致で指定し、大文字小文字は区別しません。

[12]正確には、設定ファイル内に記述可能なサイズを意味します。複数のファイルを指定する場合は、区切り文字に１バイトずつ消費します。

また、圧縮ファイル内のファイルについても適用されます。圧縮ファイル内のファイルでファイル名/拡張子と一致した場合、該当ファイルについては検査を行いません。圧縮ファイル内の他のファイルについては検査を行います。
最大で 1999 バイトまで設定できます[13]。

8.5.17 テキスト本文検査*

メールのテキスト本文の検査を行います。この設定の有無に関わらず、テキスト形式の添付ファイルや、HTML 形式の本文等は検査します。有効にすると動作速度が多少低下します。
テキスト形式の本文については実行されることがないため、通常この項目を設定する必要はありません。

8.5.18 HTML 全体の検査*

メールの HTML 部分について、スクリプトや ActiveX を呼び出す部分などのウイルスが動作する部分以外についても検査を行います。有効にすることで、ウイルス以外の疑わしいメール (詐欺メールや壊れたウイルス等) の一部を検出します。この設定の有無に関わらず、HTML に含まれるウイルスは検出します。有効にすると動作速度が多少低下します。
設定の有無に関わらずウイルスは検出されるため、通常この項目を設定する必要はありません。

8.5.19 リスクウェア検査*

リスクウェア検査を有効にします。明らかなウイルス以外にリスクウェアも検出するようになります。リスクウェアの詳細については、「13.15　リスクウェア名称」を参照してください。

検査除外リスト

指定したリスクウェアについては検出しなくなります。
リスクウェアは”Category.Platform.Family”という名前で指定します。Categoriy, Platform, Family にはワイルドカード(*)を使用できます。たとえば「Client-IRC.*.*」は Client-IRC カテゴリのすべてのリスクウェアをスキャン対象外にします。
最大で 1999 バイトまで指定できます。
設定ファイル中では、セミコロン(“;”)区切りで指定します。

8.5.20 最大検査時間*

ファイル検査の最大時間を指定します。検査に時間がかかる場合、設定時間で検査を終了します。短く設定するに従い、圧縮ファイル等で検査できる範囲が少なくなることがありますのでご注意ください。0(ゼロ)を指定した場合、検査時間の制限をしません。デフォルトは 90 秒です。

8.5.21 DNS 逆引き*

[13]正確には、設定ファイル内に記述可能なサイズを意味します。複数のファイルを指定する場合は、区切り文字に 1 バイトずつ消費します。

DNS の逆引きを行います。
有効にすると[アクセス制御]のホスト名・ドメイン名指定が可能になり、アクセスログのアクセス元をホスト名で表示します。 但し、動作速度が多少低下します。

8.5.22 メール通知

管理者へメールで通知を行います。
送信先アドレス・メールサーバは、「管理メール」で設定します。

8.6「FTP Proxy」設定

FTP プロキシの設定メニューです。

本章で説明する機能の項目名で、その末尾にアスタリスク(*)が付くものは、
簡易表示で省略されるメニューであることを示します。
動作モードによって、表示されるメニューが異なります。

8.6.1 FTP プロキシ

チェックボックスで FTP プロキシサービスの起動・終了を設定します。
中継先の FTP サーバのホスト名・ポート番号を指定します。
FTP ポート番号は、通常 21 番を指定します。

8.6.2 ポート番号

プロキシサービスのポート番号。プロキシモードでの、デフォルトは 9110 番です。

8.6.3 ウイルス検査を有効にする

ウイルス検査の有無を指定します。
通常はチェックします。ウイルス検出時の動作を選択します。

8.6.4 ウイルス検出時の動作

ウイルス検出時の動作を選択します。
通常は削除します。
削除しない場合も、ログへの記録・管理者通知は行います。

8.6.5 ウイルス隔離*

ウイルスを隔離保存します。
隔離先は、/home/spool/virusgw/quarantine　ディレクトリです。
十分なディスク容量がある場合のみ指定してください。

8.6.6 FTP サーバの任意指定

クライアントでの FTP サーバ選択を許可します。

メーラのユーザ名に「ユーザ名@FTP サーバ名」(又は「ユーザ名#FTP サーバ名」)と指定することで FTP サーバをユーザが指定できます。

8.6.7 認証ユーザ制限*

「認証ユーザリスト」で編集したリストのユーザ名を使って、接続するユーザを制限します。

認証には PAM(Pluggable Authentication Modules)を用いており、認証方式を /etc/pam.d/fsigk_ftp ファイルで変更することも可能です。

➲ 詳細は「8.13 プロキシ認証について」を参照してください。

8.6.8 最大同時接続数

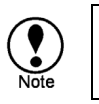
クライアントから同時に接続できる最大数を設定します。指定した数のプロセスがクライアントからの接続に対して待機します。
利用している接続数は、アクセスログ (access.log) の [内部プロセスID] で確認できます。

この値を増やすと同時に接続できる数が増えますが、同時接続数が増えた場合にはメモリを消費します。メモリ消費量は 1 接続あたり約 500KB 程度です。
最大接続数に達した場合は、エラーログに警告が表示されます。
不明な場合、まずは 10 程度で様子を見ることをお勧めいたします。通常、50 以内で設定します。

8.6.9 アクセス制限(接続元)

指定したホスト一覧からの接続のみ受け付けます。
[DNS 逆引き]を有効にするとホスト名・ドメイン名での指定も可能になります。

➲ 記述例については「8.14 アクセス制御」を参照してください。

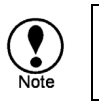


ウェブ管理画面で [接続元] を編集すると、
/opt/f-secure/fsigk/conf/hosts.allowのftp_from項目に反映されます。

8.6.10 アクセス制限(接続先)*

指定したホスト一覧への接続のみ受け付けます。

➲ 記述例については「8.14 アクセス制御」を参照してください。



ウェブ管理画面で [接続先] を編集すると、
/opt/f-secure/fsigk/conf/hosts.allowのftp_to項目に反映されます。

8.6.11 検査除外ホスト*

指定したホストへの接続に対してはウイルス検査を行いません。
通常は、全てのデータを一度保存し、ウイルス検査を行った後にクライアントへの送信を開始しますが、指定したホストへの接続に対しては受け取ったデータを順次転送します。

➲ 記述例については「8.14 アクセス制御」を参照してください。

Note

ウェブ管理画面で [ホスト名] を編集すると、
/opt/f-secure/fsigk/conf/hosts.allowのftp_pass_to項目に反映されます。

8.6.12 検査除外ファイル名*

指定したファイル、拡張子に対してはウイルス検査を行いません。
名前は後方一致で指定し、大文字小文字は区別しません。
また、圧縮ファイル内のファイルについても適用されます。圧縮ファイル内のファイルでファイル名/拡張子と一致した場合、該当ファイルについては検査を行いません。圧縮ファイル内の他のファイルについては検査を行います。
最大で 1999 バイトまで設定できます[14]。

8.6.13 ファイルサイズ*

ファイルの指定サイズ以上の部分について、ウイルス検査を行いません。
通常は、全てのデータを一度保存し、ウイルス検査を行った後クライアントへの送信を開始しますが、指定サイズ以上の部分については受け取ったデータを順次転送します。

Caution

この設定を行った場合、大きいファイルに含まれるウイルスが検出できないことがありますのでご注意ください。

8.6.14 リスクウェア検査*

リスクウェア検査を有効にします。明らかなウイルス以外にリスクウェアも検出するようになります。リスクウェアの詳細については、「13.15　リスクウェア名称」を参照してください。

検査除外リスト

指定したリスクウェアについては検出しなくなります。
リスクウェアは”Category.Platform.Family”という名前で指定します。Categoriy, Platform, Family にはワイルドカード(*)を使用できます。たとえば「Client-IRC.*.*」は Client-IRC カテゴリのすべてのリスクウェアをスキャン対象外にします。
最大で 1999 バイトまで指定できます。
設定ファイル中では、セミコロン(“;”)区切りで指定します。

8.6.15 最大検査時間*

ファイル検査の最大時間を設定します。
0 を指定した場合、検査時間の制限をしません。
デフォルトは 90 秒です。

Caution

検査に時間がかかる場合、設定時間で検査を終了します。検査時間を短く設定するに従い、圧縮ファイル等で検査できる範囲が少なくなることがありますのでご注意ください。

[14]正確には、設定ファイル内に記述可能なサイズを意味します。複数のファイルを指定する場合は、区切り文字に 1 バイトずつ消費します。

8.6.16 DNS 逆引き*

DNS の逆引きを行います。
有効にすると[アクセス制御]のホスト名・ドメイン名指定が可能になり、アクセスログのアクセス元をホスト名で表示します。 但し、動作速度が多少低下します。

8.6.17 メール通知

管理者へメールで通知を行います。
送信先アドレス・メールサーバは、「管理メール」で設定します。

8.7「管理」

管理者への通知設定を行います。各プロキシサービスで「メール通知」が有効な場合に、ウイルスあるいはスパム検出情報が通知されます。

8.7.1 メールアドレス

管理者のメールアドレスを指定してください。

8.7.2 メールサーバ

メールを送信するためのメールサーバを指定します。

8.7.3 ポート番号

通常 25 番ポートを利用します。

8.7.4 プロキシ時 SMTP ポート

動作モードが「プロキシモード」「透過プロキシモード」の場合、通常サーバの電子メールサービスは停止します。しかし、場合によっては電子メールサーバを任意の待ち受けポートで起動したい場合があります。プロキシ時 SMTP ポートは、「プロキシモード」「透過プロキシモード」を選択した場合の電子メールサーバの待ち受けポートを設定します。

「プロキシモード」「透過プロキシモード」設定後、電子メールサーバを起動すると、電子メールサーバの待ち受けポートはプロキシ時 SMTP ポートでしたポート番号で起動を試みます。
ポート番号は、「透過プロキシモード」の場合は 9025 番は使用できません。また、プロキシポートと同じ番号も設定できません。使用する場合は、未使用のポート番号を割り当ててください。
また、電子メールサービスが有効な場合、TLAS のアクティブモニタは 25 番ポートの動作チェックを行います。サーバーの 25 番ポートで電子メールサービスが動作していない場合は、アクティブモニタで電子メールサーバーのエラーが通知されます。この場合は、アクティブモニタの監視対象から電子メールサーバを外すことでエラーを回避できます。

このオプションメニューは、「プロキシモード」「透過プロキシモード」の詳細表示の場合に表示されます。

8.8 ライセンス登録

ライセンス管理メニューを表示します。

8.8.1 ライセンスの登録方法

ライセンスコードの欄にライセンスを記入し、「保存ボタン」を押してください。

8.8.2 バージョンアップ ID

サーバマシンの識別 ID で、ライセンス発行時に使用されます。

8.8.3 ライセンスの状態

現在のライセンスの状態を表示します。

8.9 メッセージ編集

各ウイルス検出通知のメッセージの内容を編集できます。

8.9.1 メッセージの編集方法

メッセージを編集する場合は、編集したいサービス「HTTP 通知」「SMTP 通知」「POP 通知」「管理者通知」のタブメニューのいずれかを選択します。メッセージ編集後、「保存」ボタンを押します。最大 9000 バイトまでで指定してください。

8.9.2 メッセージの初期化

メッセージを初期の状態に戻したい場合は、編集したいサービス「HTTP 通知」「SMTP 通知」「POP 通知」「管理者通知」のタブメニューのいずれかを選択し、「メッセージを初期化する」ボタンを押してください。

8.9.3 プロセスの再起動

新たに編集されたメッセージは、プロキシサービスを再起動しないと有効になりません。直ちに反映させたい場合は、「プロセス再起動」ボタンを押してください。

8.9.4 ウイルス検出通知テンプレート

ウイルス検出通知テンプレートの先頭行には、ヘッダを記述できます。
SMTP サービスで送信者へ通知、及び管理者へ通知を行う場合は、先頭部分に "From: name@domain" を指定することで、ヘッダの From 行とエンベロープ From ("MAIL FROM:" コマンドのアドレス) を変更・指定できます。受信者へ通知の場合はエンベロープ From は変更できません。
"Subject:"、"From:" は、日本語 (JIS) で指定できます。
なお、テンプレート編集後はサービスの再起動が必要です。

■ウイルス検出通知で使用できる変数

`${SERVICE_TYPE}`
　サービスの種類 ("http" or "smtp" or "pop" or "ftp")
`${DETECTION_NAME}`
　ウイルス名 (W95/Klez.H@mm 等)
`${VIRUS_INFO_URL}`
　ウイルス情報への URL
　　例："http://www.f-secure.co.jp/vs?vn=W32/NetSky.D@mm"
`${CLIENT_HOST}`
　クライアントホスト名

ホスト名を表示する場合は、ウェブ管理画面で [DNS の逆引き] を有効にする必要があります。

${CLIENT_ADDR}
　クライアント IP アドレス
${SERVER_HOST}
　サーバホスト名(Liuux ゲートウェイからの接続先サーバ)
${SERVER_ADDR}
　サーバ IP アドレス(Liuux ゲートウェイからの接続先サーバ)
${STATUS}
　応答コード(アクセスログと同じ値になります)
${METHOD}
　要求メソッド

HTTP では HTTP の要求メソッド (GET,POST 等) です。FTP では送信時は PUT、受信時は GET です。他のサービスでは常に GET です。

${URL}
　アクセスしたサイトの URL
${CONTENT_TYPE}
　Content-Type が示す項目 (例：text/html)
${CONTENT_LENGTH}
　送受信したファイルのサイズ(バイト数)
${FILENAME}
　検出したファイル名
${QUARANTINE_FILE}
　隔離保存ファイル名
${TIME}
　アクセス時刻 (1970/01/01 を基点とした秒数)
${TIME_STR}
　アクセス時刻文字 (例：'Tue May　7 16:16:17 2002')
${HEADER}
　ヘッダの内容
${TEXT}
　テキストメッセージの内容
${MAILFROM}
　SMTP の送信者アドレス ("MAIL FROM:"コマンドの引数アドレス)
${RCPTTO}
　SMTP の受信者アドレス ("RCPT TO:"コマンドの引数アドレス一覧(","区切り))
${MESSAGE_ID}
　SMTP のヘッダの Message-ID フィールドの値
${ERROR_STR}
　エラーメッセージ(アクセスログの PROXY-ERROR と同じ内容)
${ACTION}
　検出した際の動作(アクセスログと同じ内容)
${PATH_QUERY}
　URL のパスおよびクエリ部分 (HTTP サービスのみで有効)
${X_FORWARDED_FOR}
　X-Forwarded-For ヘッダフィールドの内容 (HTTP サービスのみで有効)

8.10 認証ユーザリスト

認証ユーザリストは、ユーザ名とパスワードのリストです。各プロキシサービスの共有のプロキシ認証のためのデータベースとして利用されます。

8.10.1 認証ユーザリストの作成

管理画面のユーザリストの追加ボタンでユーザを追加できます。また、表示されるユーザエントリの右側のアイコンで、修正・削除の操作ができます。

8.10.2 認証ユーザリストのエクスポートとインポート

認証ユーザのリストは、エクスポート（外部へ保存）あるいは、インポート（外部からファイルを置換）できます。ファイルの形式は、カンマ区切りの CSV 形式です。Microsoft Excel 等のアプリケーションで管理・編集することが可能です。

8.11 ウイルス検査 ICAP サービス設定

ICAP デーモンは、ICAP プロトコルの REQMOD、RESPMO および OPTION メソッドを実装します。もし、REQMOD または RESPMOD リクエストがカプセル化された HTTP ボディを含んでいれば、ウイルス検査が実行されます。ウイルスを検出した場合、ICAP デーモンは、応答する内容をユーザーにコンテンツがブロックされたことをユーザに知らせる HTML ページに置き換えて修正します。
この HTML ページは、ウイルス検出通知用のテンプレートで編集することができます。
ICAP デーモンは、オプショナルな ”Allow:204” ICAP ヘッダーを認識します。このヘッダが提出された時、リクエストがいかなる修正も必要としなければ、ステータスコード２０４を応答します。ネットワークの負荷やディスクの消費を軽減するために、可能ならばクライアント・プロキシは２０４応答を使用することが推奨されます。

8.11.1 ICAP デーモン設定

ICAP サービスを有効にする

ウイルス検査 ICAP サービスを有効あるいは無効にします。デフォルトでは ICAP サービスはポート 1344 を通じて ICAP 要求に応答します。デーモンに要求を送信する ICAP サービスを使用するプロキシを設定します。

バインドアドレス

ICAP デーモンがバインドするネットワークアドレスまたはホスト名を指定します。
デフォルトではセキュリティの強化のためにデーモンはローカルインタフェース(127.0.0.1) にのみバインドします。0.0.0.0 を指定すると、デーモンをすべてのアドレスにバインドできます。

バインドポート

ICAP サービスが応答するポート番号を指定します。デフォルトは 1344 です。

最大検査サイズ

検査するコンテンツの最大サイズを指定してください。
この値は、検査するコンテンツのサイズを制限します。もし、ICAP リクエストがこの制限よりも大きな HTTP ボディを含んでいる場合、そのリクエストは検査無しでで許可されます。値が –1 の場合は、制限は無効になります。
長時間の検査によるプロキシの遅延を防止するために適切な検査サイズを持つことが推奨されます。また、それは ICAP デーモンが使用するテンポラリなディスクの容量も制限します。
デフォルトは、2048 MB（2147483648 bytes）です。

最大検査時間

ファイル検査の最大時間を設定します。
0 を指定した場合、検査時間の制限をしません。
デフォルトは、90 秒です。

検査に時間がかかる場合、設定時間で検査を終了します。検査時間を短く設定するに従い、圧縮ファイル等で検査できる範囲が少なくなることがありますのでご注意ください。

検査タイムアウト時ブロック

検査が最大検査時間に達した場合、コンテンツがウイルス感染したものと見なしてブロックします。デフォルトは無効です。この場合、検査時間内で感染が見つからなければ、コンテンツをブロックしません。

接続タイムアウト

接続に関するタイムアウトを設定します。
タイムアウトが発生する前に、ICAP リクエストが完了しないクライアントの接続を切ります。これは、クライアントが無作法な振る舞いをした場合の過負荷から、ICAP サービスを保護します。デフォルトは 600 秒です。

最大接続数

接続を許可する最大数を指定します。
ICAP デーモンが許可する最大同時接続数を設定します。この制限地に達している間は、新しいクライアントは、直ちに過負荷を意味する５０３ステータスコードの ICAP 応答を受け取ることになります。デフォルトは５００です。

Real Time Protecton Network（Security Cloud）でのファイル評価確認

F-Secure の Security Cloud を利用してファイルを定期的に更新されるホワイト・ブラックリストと照合します。
有効にすると一般のファイルに対するスキャンの負荷が低減されるため、新しい脅威に対する対応時間の短縮とシステムのリソース負荷の低減が可能になります。デフォルトは無効 で、Security Cloud に情報は送信されません。

注: この機能を通じて F-Secure のサーバへ送信される情報はすべて匿名で処理されます。詳細は、製品と一緒にインストールされる real-time-protection-network-policy.txt を参照してください。

ファイル評価検査タイムアウト

製品がファイルをローカルでスキャンを行う前に Security Cloud からの応答時間を設定します。単位はミリ秒で、デフォルトは 5000（５秒）です。

8.11.2 ICAP 応答ヘッダ

ICAP クライアントが'Allow:204' ICAP ヘッダを使用することを推奨します。サーバが短期間でクリーン(安全な) 要求に対応できるようになります。
感染が検出された場合、fsicapd は ICAP の結果コード 200 を返します(エラーが発生していないことを想定)。次の ICAP 応答ヘッダから感染に関連する情報を確認できます。

ヘッダ	概要	値	補足
X-Fsecure-Scan-Result	スキャンの結果を報告します。REQMOD と RESPMOD のすべての応答にヘッダが含まれます。	clean infected suspected grayware spam whitelisted	メッセージがスパムおよびマルウェアである場合、マルウェアの検出が優先されます。
X-Fsecure-Infection-Name	感染名を報告します。	感染名 (文字列)	感染が検出されない場合、ヘッダは含まれませ

			ん。
X-Fsecure-FSAV-Duration	fsavd デーモンがウイルススキャンにかかった実際の時間を報告します。	スキャン時間 (秒)	スキャンを完了するために必要ヘッダのみ含まれます。
X-Fsecure-Transaction-Duration	単一の要求を処理するために費やした時間を報告します。サーバが ICAP 要求ヘッダを受信してから ICAP 応答ヘッダが作成されるまでの秒数です。	スキャン時間 (秒)	
X-Fsecure-Spamcheck-Duration	fsasd デーモンがスパムスキャンにかかった実際の時間を報告します。	スキャン時間 (秒)	
X-Fsecure-Infected-Filename	感染したファイルの名前を報告します。	ファイル名 (文字列)	ファイルの名前が知られている場合、ヘッダは含まれません。ファイル名は、圧縮ファイル内のファイルまたは MIME のメール添付ファイルにより感染が検出された場合に報告されます。ファイル名は非 ASCII 文字を含めるために URL エンコー ドされます。

8.11.3 ICAP サービスデーモン（fsicapd）一時ファイル

ICAP サービスデーモン(fsicapd) が HTTP 要求・応答をスキャンする場合、包含されたボディは chunked エンコード形式から解読され、一時ファイルに書き込まれます。一時ファイルは ICAP 要求が完了するまで残ります。
一時ファイルの数と最大サイズは fsicapd 設定と ICAP クライアントの動作に依存します。

- 一時ファイルの最大数は接続しているクライアント数(max_conn) になります。ICAP 要求が Allow:204 ヘッダを含めている場合、一時ファイルの最大サイズはスキャンサイズの制限(max_scan_size)に設定されます。
- ICAP 要求が Allow: 204 ヘッダを含まない、またはサイズ制限が設定されていない場合、ボディ全体が保管されます。その場合、一時ファイルのサイズに上限はありません。

一時ディスク容量の不足を防ぐために適切なディスク容量を割り当て、スキャン制限と最大接続数を慎重に設定してください。fsicapd が ICAP 要求の処理中に一時ファイルの書き込みに失敗した場合、クライアントにエラーコード 500 が返されます。ICAP サービスを使用しているプロキシは感染しているコンテンツを誤って許可しないように適切に設定してください。

8.11.4 ICAP エラーおよびステータスコード

次の表は、ICAP サービスデーモンより返されるエラーICAP のステータスとエラーコードを示します。

コード	理　由
200	ICAP サーバが変更された可能性のある応答または要求を返す。また成功した OPTIONS 応答にも使用されます。
204	HTTP リクエストまたは応答に問題がない。 プロキシは変更のない元のリクエストや応答を使うべきです。
400	ICAP プロトコルエラー：クライアントからの ICAP リクエストの構文解析に失敗しました
500	内部エラー：ICAP デーモンのディスクあるいはメモリ不足の可能性が高い
503	許可された最大接続数にすでに達した、サービスの過負荷

ICAP プロトコルに関するより詳細な説明については、RFC3507 および、あなたが ICAP クライアントとして使用する HTTP プロキシのマニュアルを参照してください。

8.12 バージョン情報

現在の製品バージョンを表示します。
定義ファイル情報では、現在インストールされているウイルス定義ファイルを表示します。

8.13 プロキシ認証について

アンチウイルス・ゲートウェイ自身が各ユーザの入力するパスワードによる認証を行います。HTTP サービスでは HTTP プロキシ認証、SMTP サービスでは SMTP 認証、POP サービスでは POP ユーザ名、FTP サービスでは FTP ユーザ名による接続制限が行えます。

本製品のインプリメントでは、各サービス共通の「認証ユーザリスト」での認証方式を提供します。ただし、以下に記述するように、PAM 認証の設定をカスタマイズすることで外部認証方式を利用することも可能です。ただし、本製品では、カスタマイズはお客様の責任で行っていただくものとし、製品サポートの対象外となります。

アンチウイルス・ゲートウェイのユーザ認証（PAM 認証）について

認証リストは/opt/f-secure/fsigk/conf/pam/ディレクトリの userdb.txt ファイルに保存されます。直接編集した場合は、create_userdb userdb.db < userdb.txt コマンドでデータベースファイルの userdb.db を更新します。
POP、FTP については設定内容でユーザ名の確認を行います。ここで、ユーザ名はクライアント側で設定するユーザ名となり、複数サーバを用いる場合は「ユーザ名@サーバ名」(又は「ユーザ名#サーバ名」)を指定します。指定したサーバで、全てのユーザの利用を許可する場合は「@サーバ名」と入力します。パスワードについてはサーバ側の認証をそのまま利用します。

ユーザ名は、クライアント側で設定するユーザ名です。
パスワードは、サーバ側の認証をそのまま利用します。

PAM 設定ファイル(/etc/pam.d/fsigk_{http,smtp,pop,ftp})を編集することで、UNIX アカウント、NIS、LDAP、Radius 等の外部の認証方式を用いることが可能になります。これらの PAM 設定ファイルは /opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pam のシンボリックリンクとなっています。

アップデート時の上書きを防ぐため、編集する場合はシンボリックリンクを切り離してコピーを作成してから編集してください。

8.14 アクセス制御

プロキシの設定等で、ホスト、ネットワークによるアクセス制御を行うことができます。
設定は以下のように記述します。

アクセス制御は tcpwrapper で行います。tcpwrapper についての詳細は、コマンドラインから "man 5 hosts_access" を実行して確認してください。

■記述例

123.456.789.123　999.999.999.999
　IP アドレスが "123.456.789.123" または "999.999.999.999" の時に接続を許可します。
host.domain.jp
　ホスト名が host.domain.jp の時に接続を許可します。
　xxx.host.domain.jp は許可しません。
.domain.jp
　ホスト名が.domain.jp で終わるときに接続を許可します。
　"xxx.domain.jp" は許可しますが、"domain.jp" 自身は許可しません。
192.168.
192.168.0.0/255.255.0.0
　IP アドレスが 192.168.3.4 のように指定されたネットワークに含まれるときに接続を許可します。
　ネットマスクに "255.255.255.255" は記述できません。
ALL
　全てのホストからの接続を許可します。
ALL EXCEPT 1.2.3.4 4.5.6.7
　IP アドレスが "1.2.3.4" または "4.5.6.7" 以外を許可します。
ALL EXCEPT 192.168.0.0/255.255.0.0
　ネットワークが 192.168.0.0/255.255.0.0 以外を許可します。
.domain.jp EXCEPT 999.999.999.999 987.654.321.123
　ホスト名が.domain.jp で終わり、かつ IP アドレスが 999.999.999.999 でも 987.654.321.123 でもない時に接続を許可します。
/etc/fsigk_allow_list.txt
　一覧ファイル (/etc/fsigk_allow_list.txt) に記述されたアドレスからの接続を許可します。一覧ファイルは各アドレスを 1 行ずつ、または空白区切りで記述します。
ALL EXCEPT /etc/fsigk_deny_list.txt
　一覧ファイル (/etc/fsigk_deny_list.txt) に記述されたアドレス・ホストからの接続を拒否し、それ以外を許可します。一覧ファイルは各アドレスを 1 行ずつ、または空白区切りで記述します。

●1 行が 2047 バイトを超える場合の注意事項

アクセス制御の設定ファイル (/opt/f-secure/fsigk/conf/hosts.allow) では、1 行に最大 2047 バイトまで記述できます。それを超える場合、以下のような方法で設定してください。

別ファイルに一覧を記述する方法

別ファイル (例：/etc/fsigk_smtp_rcpt_allow_list.txt) に、以下のようにホスト・ドメイン一覧を記述します。

```
aaa.com
bbb.com
ccc.com
```

また、アクセス制御の設定で、ファイル (/etc/fsigk_smtp_rcpt_allow_list.txt) を指定します。これは、ウェブ管理画面で設定するか、アクセス制御の設定ファイル (/opt/f-secure/fsigk/conf/hosts.allow) に記述することで行います。

```
smtp_rcpt: /etc/fsigk_smtp_rcpt_allow_list.txt
```

ファイルに複数行で記述する方法

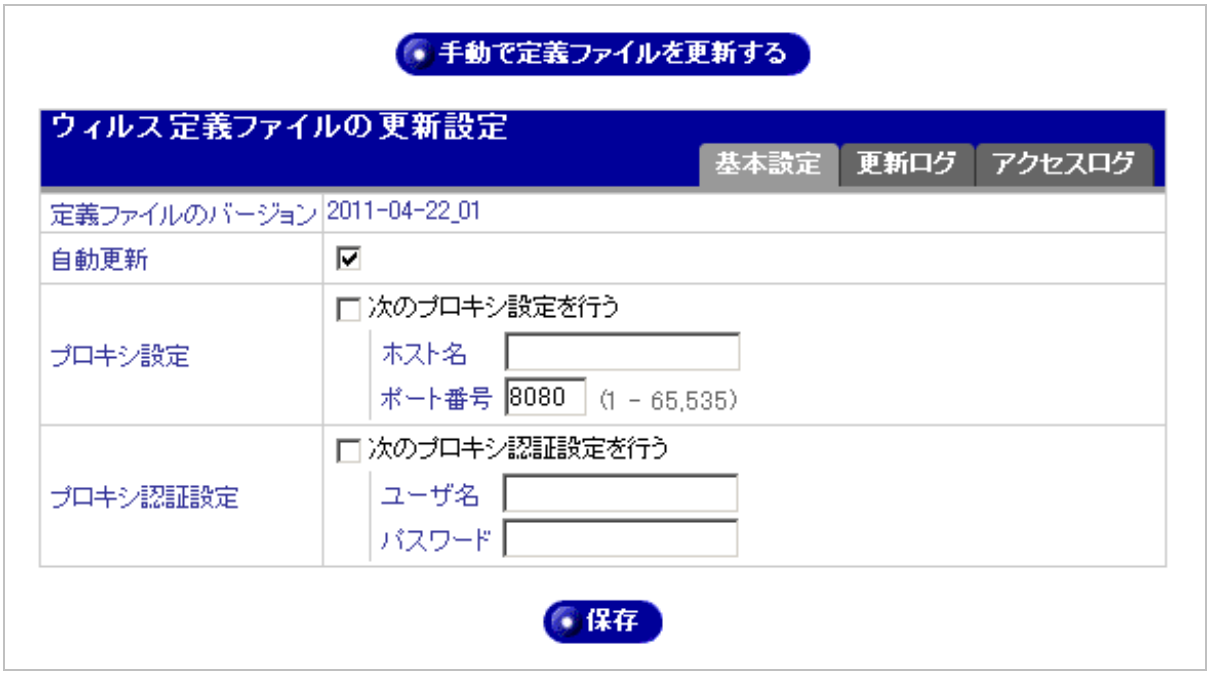
アクセス制御の設定ファイル (/opt/f-secure/fsigk/conf/hosts.allow) 上で、以下のように複数で記述します。

この場合、ウェブ管理画面上では最初の 1 行のみ表示されます。

```
例：smtp_rcpt: aaa.com bbb.com ccc.com
    smtp_rcpt: ddd.com eee.com fff.com
```

9. 定義ファイル更新

定義ファイルの更新は、HTTP プロトコルを用いて行います。
定義ファイルは、http://fsbwserver.f-secure.com/ から取得します。
また、HTTP プロキシサーバ経由での定義ファイルを更新する場合は、プロキシサーバと利用ポートを設定してください。



9.1 定義ファイル情報について

定義ファイル情報欄には、ウイルス定義ファイルの最終バージョンが表示されます。

9.2 手動で定義ファイルを更新する

〔手動で定義ファイルを更新する〕をクリックすると、定義ファイルの更新を直ちに実行します。
定義ファイルの更新はdbupdate コマンド[15]を使用しています。

[15] dbupdate コマンドは、AUA(Automatic Update Agent(自動更新エージェント),コマンド名:fsaua)を通じて、http://fsbwserver.f-secure.com/からファイルを取得し、databases ディレクトリ置きます。

9.3 自動更新設定について

自動更新設定を有効にすると、定期的（１時間間隔）で定義ファイルを最新にします。

9.4 プロキシ設定

HTTP プロキシサーバ経由での定義ファイルを更新する場合に設定します。

プロキシ設定

プロキシサーバの設定は、「プロキシ設定」項目の「次のプロキシ設定を行う」をチェックすると有効になります。
ホスト名はプロキシサーバを指定します。ポートは、プロキシサービスのポート番号を指定します。

プロキシ認証設定

プロキシ認証を利用する場合は、「プロキシ認証設定」項目の「次のプロキシ認証設定を行う」をチェックします。認証に必要なユーザ名とパスワードを指定します。

10. スパム検査設定

10.1 スパム検査方法

スパム検査方法を指定します。スパム検出時にはメールヘッダに "X-Spam-Status: Yes(製品名) with [検出名称]" の行が付加されます。
複数の条件に一致した場合、カスタム条件、スパム検査エンジン(Spam detection engine)、RBL、SURBL の順での検出になります。

10.1.1 スパムデータベース

スパムの判定条件を個別に指定することができます。この機能を使用するには、「カスタム条件の編集」でスパム判定のためのデータベースを編集し、「カスタム設定」をチェック（有効）します。

〔カスタム条件の編集〕
この操作は、custom.txt を編集するための作業です。この中にスパム判定のための独自のルールを記述します。カスタム条件は、他の検査方法より優先されるので、ブラックリスト・ホワイトリストとして利用できます。
カスタム条件は 100 個まで指定でき、また 1 つの条件に複数の検査文字列を指定できます。
[カスタム条件] をチェックした場合、`/opt/f-secure/fsigk/conf/spam/files.txt` に "`CUSTOM <タブ>custom.txt`" 行が追加されます。

記述する内容は次の４つの項目です。

検査フィールド
判定を行う部分を指定します。指定できる内容は以下の通りです。

フィールド名	内　容	文字列
件名(Subject)	Subject フィールドを検査。	Subject
送信先アドレス(To,CC)	To フィールド、 CC フィールドを検査。	To,Cc
送信元アドレス(From)	From フィールドを検査。	From
Content-Type ヘッダ	Content-Type フィールドを検査。	Content-Type
添付ファイル名	ファイル名を検査。	FILENAME
添付ファイルサイズ	ファイルサイズを検査。	FILESIZE
テキスト本文	テキスト本文を検査。	TEXTBODY
HTML 本文	HTML 本文を検査。	HTMLBODY
リンク先ホスト	リンク先ホスト（URL）を検査。	URLHOST
中継アドレス	Received フィールドに含まれる IP アドレスで判定します。SMTP の場合、接続元 IP アドレスでも判定します。	RELAYIP

常時適用	常にスパム又は非スパムとして判断します。	ALWAYS
その他	上記以外のヘッダウィールドを任意を指定できます。29 文字まで指定できます。大文字・小文字は区別しません。	任意

検査文字列

フィールド名で指定した部分について、指定した文字列と一致するかを検査します。複数指定できます[16]。日本語 (UTF-8) も指定できます。記述が困難な文字は、16 進数で "¥xFF" のように指定できます。"¥"は"¥¥"と記述できます。

メールアドレスを指定する場合、前方一致・後方一致は指定しないようしてください。ヘッダの From/To などのメールアドレスは"Xxx Yyy <aaa@example.com>"のようにメールアドレスの前後に文字があるため、前方一致・後方一致を指定した場合、正しく判定できません。

日本語で直接指定した場合、UTF-8 コードでの比較になります。
From(送信元)フィールドについては、UTF-8 に変換後比較を行います。UTF-8 以外のコード (Shift-JIS, Unicode 等) の文字列を検査する場合は、16 進数で直接指定してください。
例えば、Shift-JIS で書かれた「完全無料」を検出する場合、以下のように指定いただけます。
¥x8a¥xae¥x91¥x53¥x96¥xb3¥x97¥xbf
なお、漢字コードの変換は、例えば以下のツールをご利用いただけます。
Linux の場合:
iconv コマンドで、以下のように設定いただけます。
echo -n '検索した文字列' | iconv -f 現在の Linux における文字コード -t 変換したい文字コード | od -t x 1
例：
echo -n '完全無料' | iconv -f EUC-JP -t SJIS | od -t x1
0000000 8a ae 91 53 96 b3 97 bf
0000010
※各 16 進数の間には「¥x」入れてください。
(例: ¥x8a¥xae¥x91¥x53¥x96¥xb3¥x97¥xbf)
Windows の場合:
以下のようなツールをご利用いただけます。
StrHex(http://www.pleasuresky.co.jp/strhex.php3)

比較方法

比較方法を指定します。

比較方法	内　容	文字列
大文字小文字を区別しない*	大文字と小文字を区別しないで比較します。	IGNORECASE
前方一致	指定フィールドの先頭と一致するかを比較します。	HEADMATCH
後方一致	指定フィールド末尾と一致するかを比較します。	TAILMATCH

[16] 設定ファイル custom.txt では、コンマ (",") 区切りで記述されます。

不一致	指定文字列と一致しない場合に条件を満たします。	NOT
前の条件とAND	1つ前の条件と両方を満たした場合に条件を満たします。通常、1つ前の条件の「判定」は"何もしない"を指定します。	AND
前の条件とAND(同一MIMEパート)	同じMIMEパートについて、1つ前の条件と両方を満たした場合に条件を満たします。例えば、ある添付ファイルのContent-Typeとファイル名の両方について条件を設定する場合に指定します。通常、1つ前の条件の「判定」は「何もしない」を指定します。	AND_SAMEPART
* IGNORECASEが記述されていない場合、大文字・小文字は区別される		

メールアドレスを指定する場合、前方一致・後方一致は指定しないようしてください。ヘッダのFrom/To などのメールアドレスは"Xxx Yyy <aaa@example.com>"のようにメールアドレスの前後に文字があるため、前方一致・後方一致を指定した場合、正しく判定できません。

スパム判定

指定条件を満たした場合の判定結果を指定します。"スパム"、"非スパム"、"何もしない"のいずれかから選択します。

スパム判定	内　容	文字列
スパム	指定条件を満たした場合、スパムと判定します。	BLACK
非スパム	指定条件を満たした場合、非スパムと判定します。	WHITE
何もしない	「比較方法オプション」の「前の条件と AND」、「前の条件と AND(同一 MIME パート)」を利用する場合の１つ前のルールで選択します。	NONE

10.1.2 スパム検査エンジン (Spam detection engine)

Spam detection engine によるスパム検査の有無を指定します。Spam detection engine は SMTP,POP のスパム検査機能を提供します。

- 問い合わせには、ウイルス定義ファイルのプロキシサーバ設定を利用します。

- 本機能では、スパム検査時に以下のサーバに問い合わせを行います。
  (1) ホスト名: ct-cache%d.f-secure.com (%d: 1～9 の数字)
  (2) ポート番号: TCP/80
  (3) プロトコル: HTTP

- 本機能を利用した場合、SMTP/POP サービスのメモリ使用量が増加します。

- 検出名は以下の通りです。

  FSIGK/SPAM_CT/[Class]/[ThreatLevel]/RefID

  Class:
  0: 信頼された送信元から送信されています。本分類はほとんど利用されません。
  1: 情報はなく、現時点では特に分類できません。
  2: メッセージは平均より多少広い範囲に送信されています。
  3: スパマーと確認されていない送信元から送信されたスパムです。
  4: 既知のスパム送信元(ゾンビ等)から送信されたスパムです。

  ThreatLevel:
  0: ウイルスかどうかは不明です。
  1: ウイルスの可能性があります。
  2: ウイルスの可能性が高いです。
  3: ウイルスです。

  RefID:
  RefID は Spam detection engine でメッセージを分類した際に付加される ID で、分類された理由を調査する場合に必要な情報を含みます。

10.1.3 RBL サーバ

RBL (Realtime Black List) によるスパム検査の有無と、スパム検査で参照する RBL サーバを指定します。設定ファイル内のサーバリストの指定は 199 文字までに制限されます。
各メールについて、接続元 IP アドレス (SMTP の場合) および Received ヘッダに記載されている IP アドレスが RBL サーバに登録されているか確認することで検査を行います。各メールについて、RBL および SURBL の問い合わせは一斉に行いますが、サーバからの応答待ちにより数 100ms 程度未満の遅延が発生します。1 秒以内に応答がない場合は、タイムアウトし、スパムではないと判断します。
各メールについて、問い合わせ数の最大は 32 です。
RBL での検出名称は "FSIGK/SPAM_RBL/(検出アドレス)[(RBL サーバ名):(RBL 応答アドレス)]" です。

検出アドレス　　: RBL サーバに登録されていたアドレス
RBL サーバ名　　: 検出した RBL サーバ名
RBL 応答アドレス : 検出時の RBL サーバからの応答アドレス

SURBL 問い合わせは DNS の名前引きにより行います。問合せ先 DNS サーバは/etc/resolf.conf の最初の nameserver になります。

サーバーリスト

サーバーリストに RBL サーバを設定します。

(**初期設定**: bl.spamcop.net, sbl-xbl.spamhaus.org, list.dsbl.org)

除外リスト

指定したアドレスについては、RBL による検査を行いません。
(初期設定：127. 10. 192.168. 172.16.0.0/255.240.0.0)

➔ 記述例については「8.14　アクセス制御」を参照してください。

ウェブ管理画面で [除外アドレス] を編集すると、/opt/f-secure/fsigk/conf/hosts.allow の spam_rbl_pass 項目に反映されます。

10.1.4 SURBL サーバ

SURBL (SPAM URL Realtime Black List) によるスパム検査の有無と、スパム検査で参照する SURBL サーバを指定します。設定ファイル内のサーバリストの指定は 199 文字までに制限されます。
各メールについて、テキスト本文と HTML 本文に含まれる URL のドメイン名部分が SURBL サーバに登録されているか確認することで検査を行います。各メールについて、RBL および SURBL の問い合わせは一斉に行いますが、サーバからの応答待ちにより数 100ms 程度未満の遅延が発生します。1 秒以内に応答がない場合は、タイムアウトし、スパムではないと判断します。各メールについて、問い合わせ数の最大は 32 です。
SURBL での検出名称は "FSIGK/SPAM_SURBL/(検出ドメイン名)[(SURBL サーバ名):(SURBL 応答アドレス)]" です。

検出ドメイン名　　: SURBL サーバに登録されていたドメイン名
SURBL サーバ名　　: 検出した SURBL サーバ名
SURBL 応答アドレス : 検出時の SURBL サーバからの応答アドレス

SURBL 問い合わせは DNS の名前引きにより行います。問合せ先 DNS サーバは/etc/resolf.conf の最初の nameserver になります。

[サーバリスト]
SURBL サーバを指定します。
(初期設定 multi.surbl.org)

10.2 SMTP スパム検査設定

[有効にする]

スパム検査の有無を指定します。検出された場合、ヘッダに "X-Spam-Status:" が付加されます。
スパム検査方法として RBL/SURBL を使用する場合、RBL/SURBL サーバからの応答待ちにより数 100ms 程度未満の遅延が発生します。
外部からのスパムへの対応が目的のため、受信ドメイン設定を有効にした場合、LAN 内のホストから外部への送信メールについてはスパム検査は行いません。
ウイルス検査・スパム検査の両方を有効にした場合、ウイルス検査の結果が優先します。

[スパム検査]
スパム検出時の動作を選択します。

[何もしない]
スパムを通過します。スパムと判定されたメールはヘッダに "X-Spam-Staus:" が付加されます。クライアントの振り分け設定を利用して、"X-Spam-Status:" が "Yes" で始まる場合はスパムとして振り分けを行います。ログへの記録・管理者通知は行います。

[件名変更]
スパムと判定したメールの件名を変更します。追加文字列で指定した文字列を件名の先頭に付加します。追加文字列は 99 文字まで指定できます。日本語も指定できますが、この場合日本語部分は UTF-8 としてエンコードを行います。そのため、検出したメールの件名が ISO-2022-JP でエンコードされている場合、Outlook 等では文字化けする場合があります。基本的には英語で指定することを推奨します。

[削除する]
スパムを削除します。スパムの誤認識に対応する場合、削除は行わずにクライアント (メーラ) 側で振り分けを行います。

[管理者へ通知]
「管理者へ通知する」が有効な場合は、アンチウイルス設定で行った管理者へ、検出メッセージが送信されます。
通知メッセージ自身が検出されることを防止するため、ヘッダには"X-Admin-Notification-Id: [番号]" を付加して通常のメールと識別します。[番号] には、インストール時に乱数が設定ファイルの `admin_notification_id` として記述されます。

[隔離保存]
「隔離保存」が有効な場合は、隔離ディレクトリに保存されます。
十分なディスク容量がある場合のみ指定してください。

10.3 POP スパム検査設定

[有効にする]

スパム検査の有無を指定します。検出された場合、ヘッダに "X-Spam-Status:" が付加されます。
スパム検査方法として RBL/SURBL を使用する場合、RBL/SURBL サーバからの応答待ちにより数 100ms 程度未満の遅延が発生します。
外部からのスパムへの対応が目的のため、受信ドメイン設定を有効にした場合、LAN 内のホストから外部への送信メールについてはスパム検査は行いません。
ウイルス検査・スパム検査の両方を有効にした場合、ウイルス検査の結果が優先します。

[スパム検査]
スパム検出時の動作を選択します。

[何もしない]
スパムを通過します。スパムと判定されたメールはヘッダに "X-Spam-Staus:" が付加されます。クライアントの振り分け設定を利用して、"X-Spam-Status:" が "Yes" で始まる場合はスパムとして振り分けを行います。ログへの記録・管理者通知は行います。

[件名変更]
スパムと判定したメールの件名を変更します。追加文字列で指定した文字列を件名の先頭に付加します。追加文字列は 99 文字まで指定できます。日本語も指定できますが、この場合日本語部分は UTF-8 としてエンコードを行います。そのため、検出したメールの件名が ISO-2022-JP でエンコードされている場合、Outlook 等では文字化けする場合があります。基本的には英語で指定することを推奨します。

[削除する]
スパムを削除します。スパムの誤認識に対応する場合、削除は行わずにクライアント (メーラ) 側で振り分けを行います。

[管理者へ通知]
「管理者へ通知する」が有効な場合は、アンチウイルス設定で行った管理者へ、検出メッセージが送信されます。
通知メッセージ自身が検出されることを防止するため、ヘッダには"X-Admin-Notification-Id: [番号]"を付加して通常のメールと識別します。[番号] には、インストール時に乱数が設定ファイルの `admin_notification_id` として記述されます。

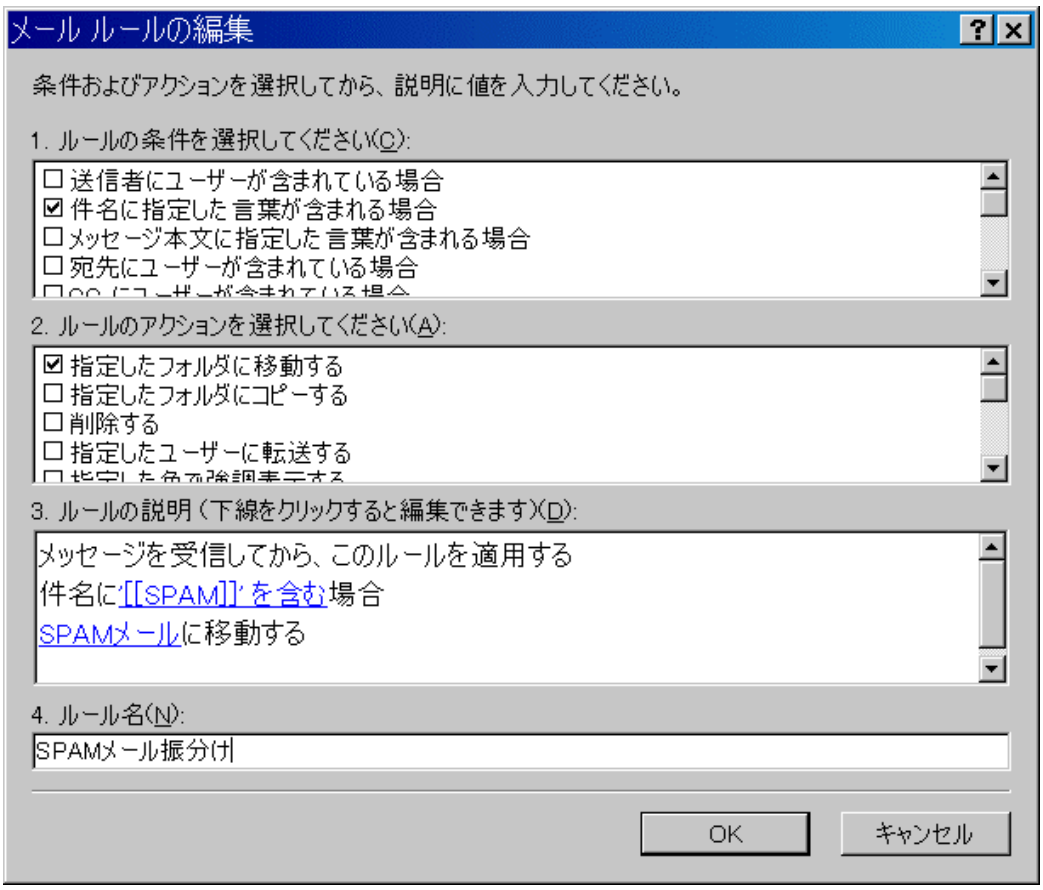
[隔離保存]
「隔離保存」が有効な場合は、隔離ディレクトリに保存されます。
十分なディスク容量がある場合のみ指定してください。

10.4 メールクライアントでの振り分け

メールヘッダによるメールの振り分けに対応したメールクライアントは、スパム認識ヘッダ (X-Spam-Status: Yes) を参照して、スパム検出されたメールを特定のフォルダに振り分けることができます。

OutlookExpress の場合は、ヘッダによるメールの振分け機能はサポートされていません。この場合、「件名変更」を利用し、件名に含まれる文字列でスパムメールを振り分けることができます。

下図は OutlookExpress 6 の[ツール]→[メッセージ ルール]→[メール]のメールルール編集メニューの設定例です。



11. ログファイル

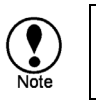
本製品ではアクセス状況の把握、ウイルス検出状況、エラー発生状況等の情報をログファイルとして残します。ログファイルは/opt/f-secure/fsigk/log/の各サービスごとのディレクトリに保存されます。必要に応じて参照してください。

11.1 ログファイル

HTTPログ、SMTPログ、POPログ、FTPログのログファイルのメニューがあります。
それぞれのサービスには、アクセスログ、ウイルスログ、エラーログ、情報ログに分かれています。
管理画面メニューでのログは最新の300行を表示します。ログファイルのダウンロードは、「ダウンロード」ボタンで行います。

11.1.1 アクセスログ (access.log)

本製品を通じてサーバへの接続を行った記録を全て保存します。
ログのフォーマットは以下のとおりです。



Squid のログフォーマットと互換ですので、各種ログ解析ツールが利用できます。

■ログフォーマット

接続状況が 1 行ずつ記録されます。以下の各項目がスペースで区切られています。

- 時刻
  クライアントから接続された時刻です。エポックタイム (1970/01/01 00:00:00(UTC)) からの秒数をミリ秒単位で表示します。
- 接続時間
  クライアントとの接続時間をミリ秒単位で表示します。
- クライアントホスト
  クライアントのホストが表示されます。逆引きが可能な場合はホスト名が表示され、それ以外は IP アドレスが表示されます。
- 処理結果
  [キャッシュ状況]／[HTTP 状態コード] を返します。
  キャッシュ状況は利用しません。常に TCP_MISS です。
  HTTP 状態コードは、クライアントに送信する HTTP レスポンスの状態コード (3 桁の数字) です。HTTP 以外では成功時は 200、エラー時は 500、それ以外(データ中継を行わずに接続直後に切断した場合など)は 000 を返します。

- ファイルサイズ
  転送したファイルのサイズです。
- 要求メソッド
  HTTP では HTTP の要求メソッド (GET, POST 等) です。FTP のデータ送信時は PUT です。それ以外では常に GET です。
- URL
  接続先の URL です。
  pop の場合は、"pop://POP ユーザ名@POP サーバ名:ポート番号" になります。
  smtp の場合は "mail:送信先" になります。
- ユーザ名
  プロキシ認証を行った場合のユーザ名が記録されます。
  認証を行っていない場合は "-" です。
- hierarchy code
  "[Hierarchy 文字列]/接続先 IP アドレス" を返します。
  [Hierarchy 文字列] は利用しません。常に "DIRECT" です。
- Content-Type
  送受信するファイルの Content-Type を表示します。利用できない場合は "-" となります。

- 検出情報
  "DETECT-STAT:[検査結果]:[ウイルス名]:[ファイル名]:[隔離保存ファイル名]::"
  を返します。

検査結果	INFECTED(ウイルス検出)、SPAM(スパム検出)、CLEAN(ウイルス検出なし) のいずれか
ウイルス名	ウイルス名称
ファイル名	送受信ファイルにつけられた名前
隔離保存ファイル名	感染ファイルの隔離を有効にした場合のみ設定されます。

- 動作
  "ACTION:[動作]:"を返します。

動作	検査結果に応じた以下の動作のいずれかを返します。 ・ NONE 何もしない(検出しなかった) ・ PASS 検出したが通過させた(ログには記録) ・ DELETE 削除した(SMTP の場合、削除後受信者へ通知) ・ SENDBACK SMTP で送信者へ通知した ・ BLACKHOLE SMTP で削除した(送受信者への通知なし) ・ CHANGE_SUBJECT SMTP でスパム検出により件名を変更した

- プロキシ情報
  "PROXY-STAT:[サービスの種類]:[内部プロセス ID]: [プロセス ID]: [接続元 IP アドレス]: [処理ファイル数] :[検査回数]: [検査時間]:[検査情報詳細]:"
  を返します。

サービスの種類	サービスの種類 (http, smtp, pop, ftp)
内部プロセス ID	処理を行った内部プロセス ID (0 からはじまる識別子) 基本的には小さい数字から使われます。 [内部プロセス ID]+1)が該当アクセスの接続開始時点での同時接続数になります。
プロセス ID	処理を行ったプロセス ID
接続元 IP アドレス	接続元の IP アドレス
処理ファイル数	同一セッション内で処理した要求の数。1 から始まり、同一セッション内でアクセ

	スログに出力する度に 1 づつ増えます。POP では常に 1 です。
検査回数	1 回の接続の中でウイルス検査を行った回数 (ただし、最後にアクセスログで出力してからの回数)
検査時間	1 回の接続の中でウイルス検査エンジンによりウイルス検査を行った時間 (ミリ秒) (ただし、最後にアクセスログで出力してからの時間)
検査情報詳細	検査状況を表す以下の文字列をコンマ区切りで表示します。 ・ VSD_ENCRYPTED 暗号化ファイル ・ VSD_MAXNESTED 最大検査階層に到達した ・ OVER_FILESIZE 検査除外対象で指定したファイルサイズを超えた ・ PASS_TO 検査除外対象のホスト名に一致した ・ PASS_USER_AGENT 検査除外対象の User-Agent に一致した ・ PASS_EXT 検査除外対象のファイル名・拡張子に一致した (HTTP,FTP のみ)

- プロトコル情報

  各プロトコル独自の情報を記録します。現在 SMTP サービスのみで有効です。
  SMTP サービスの場合：
  "PROTOCOL-STAT:[送信元アドレス]:[Message-ID]:"
  を返します。

送信元アドレス	SMTP の送信者アドレス ("MAIL FROM:" コマンドの引数アドレス) (URL エンコードを行い表示します。)
Message-ID	メールヘッダの Message-Id フィールド (URL エンコードを行い表示します。)

  HTTP サービスの場合：
  "PROTOCOL-STAT:[プロトコル情報詳細]:"
  を返します。

KEEPALIVE 有無	検査状況を表す以下の文字列をコンマ区切りで表示します。 ・ KEEPALIVE: 該当セッションで Keep-Alive（Persistent-Connection)接続を行った。。 ・ PROGRESS* 該当セッションでダウンロード状況表示ダイアログを表示した。(上級者向けオプションで"progress"の設定を行った場合) ・ TRICKLE: 該当セッションで trickle によりダウンロード完了前に転送を開始した。(上級者向けオプションで"trickle"の設定を行った場合)
X-Forwarded-For	要求ヘッダの X-Forwarded-For フィールドの値 (URL エンコードを行い表示します。)

- エラー情報

  プロキシ処理により発生したエラーメッセージを表示します。
  "ERROR-STAT:[エラーメッセージ]:"
  を返します。

エラーメッセージ	以下のエラーメッセージが表示されます (URL エンコードを行い表示します。) 各プロトコル共通 ・CONNECT(ホスト名:ポート番号/接続エラーメッセージ 「13.12 接続エラーメッセージ一覧」のエラーメッセージ HTTP の場合

	「13.6　HTTP エラー応答一覧」のエラーメッセージ SMTP の場合: ・ SERVER/ERROR Reply(MAIL): buf=[XXX] SMTP サーバへ"MAIL FROM"コマンドを送信した際のエラー応答 ・ SERVER/ERROR Reply(RCPT): buf=[XXX] SMTP サーバへ"RCPT TO"コマンドを送信した際のエラー応答 ・ SERVER/ERROR Reply(AUTH): buf=[XXX] SMTP サーバへ"AUTH"コマンドを送信した際のエラー応答 ・ ROXY/550 Relaying denied. Internet Gatekeeper が中継を拒否した。受信先ドメインの制限や認証により拒否された場合に表示されます。(クライアントからの中継を許可する場合、該当クライアントアドレスを LAN 内からのホストに設定するか、PbS/SMTP 認証を有効にします。外部からの中継を許可する場合、受信先ドメインを設定します。)

11.1.2 ウイルス検出ログ (virus.log)

ウイルスに感染したファイルの送受信時を全て記録します。

➔　ログ形式については「11.1.1　アクセスログ(access.log)」と同じです。

11.1.3 エラーログ（error.log）

エラー発生時に記録されます。本製品の動作に問題がある場合等に参照してください。
エラーメッセージの形式は以下のとおりです。なお、メッセージの形式・文面等は適時変更する可能性があります。

■エラーメッセージの形式

時刻(秒数) [日付 時刻 ポート 内部プロセス ID クライアント IP アドレス:クライアントホスト名:クライアントポート番号 サーバ IP アドレス:サーバホスト名:サーバポート番号] エラーメッセージ

日時はエラー発生時の時刻です。最初の時刻はエポックタイム (1970/01/01 00:00:00(UTC)) からの秒数をミリ秒単位で表示します。
また、OS のシステムコールに関係するエラーが発生した場合、エラーメッセージの最後に以下の記述を追加します。

/strerror(エラーコード)=エラーメッセージ
　エラーコード: システムコールのエラーコード
　エラーメッセージ: システムコールのエラーメッセージ

■エラーメッセージの内容

メッセージ

###ERROR### bind(port=ポート番号,addr=アドレス). # Please check whether other service(mail/web server,etc...) is already running on port ポート番号."
/strerror(98)=Address already in use

説明

設定したポート、アドレスで接続待ち受けを行えず、サービスを起動できません。本製品は、Linux の bind() システムコールにより指定したポート番号で待ち受け準備を行いますが、既にポート番号が利用されており bind() に失敗した場合に表示されます。

対処法

同じポートを利用している他のサービスをご確認ください。不要なサービスの場合は停止させてください。必要なサービスの場合、他のサービスと本製品の待ち受けポート・アドレスを別に設定してください。
各ポート・アドレスで待ち受けを行っているプロセスは、"netstat -anp" (診断情報では "system/netstat_anp.txt") で確認できます。

メッセージ

###ERROR### Maximum connections: warning: Client connections reached maximum connections(最大接続数). More request will be blocked/rejected. If there is many warnings, please increase 'Maximum Connections' settings(pre_spawn value of fsigk.ini) of this service.(暫定値 will be good value as start line).

説明

クライアントの同時接続数が、設定した "最大同時接続数" に達した場合に記録されます。最大接続数を超えた接続要求は、同時接続数が減少し、空きが出るまでプロキシ処理を行いません。
なお、最大接続数を超えた場合の、バックログ (Linux の listen() システムコールのバックログ) は 5 に設定されています。したがって、通常、最大接続数を超えて 6 接続要求までは TCP 接続要求を受け付けて接続状態が "ESTABLISHD" になりますが、それ以上については TCP 接続要求に応答しないため接続状態は "SYN_RECV" になります。TCP 接続要求を Linux が受け付けた場合でも、最大同時接続数を超えた接続についてプロキシ処理は行いません。
利用した同時接続数はアクセスログで「PROXY-STAT:[サービスの種類]:[内部プロセス ID]:..」として記録される[内部プロセス ID]で確認いただけます。内部プロセス ID は 0 からはじまる識別子で、小さい数字から順次使われるため、([内部プロセス ID]+1)が該当アクセスの接続開始時点での同時接続数になります。
また、現在利用中の接続数については、以下のように netstat コマンドで該当ポート番号が ESTABLISH 状態の数で確認いただけます。

```
# netstat -anp | grep :9080 | grep ESTABLISHED | wc -l
```

(ポート番号 9080 の場合)

対処法

- メッセージの表示頻度が少なく (1 時間に 1 回程度エラーが記録される場合)、動作上の問題がない場合、一時的な接続数の増加と考えられます。
  この場合、特に設定変更の必要はありません。
- 最大検査時間はデフォルトで 90 秒ですが、無効(0)にするか大きくした場合、特定のファイルの検査に時間がかかり、検査プロセス(fsavd)の処理に長時間待ちが発生してプロキシ処理が行えずに最大接続数に達する可能性があります。
  この場合、最大検査時間はデフォルト(90 秒)に戻していただきますようお願いいたします。
- 本製品とサーバ間または本製品とクライアント間でネットワーク障害が発生している場合、プロキシ処理が行えずに最大接続数に達する可能性があります。
  この場合、ネットワーク障害を解決してください。
- 多数のエラーが記録され、最大検査時間設定に変更がなく、ネットワーク障害がないにもかかわらず、全てのサーバへの接続ができずにタイムアウトする場合、必要な同時接続数が設定した最大同時接続数を超えている可能性がございます。
  この場合、最大同時接続数を必要な数以上に設定する必要があります。
- 必要なクライアントの最大同時接続数が不明な場合は、以下の暫定値程度に設定して様子を見ていただけます。その後、必要に応じて変更してください。通常、最大同時接続数は 2000 以内に設定します。
  －HTTP 200
  －SMTP 50
  －POP 50
  －FTP 10

最大同時接続数設定を増やすと、同時に接続できる数が増えますが、同時接続数が増えた場合にはメモリを消費します。メモリ消費量は 1 接続あたり約 500KB 程度です。

メッセージ

```
###ERROR### notify_admin:gethostbyname error:admin_mx_host=[ホスト名]
hstrerro=[エラー原因詳細]
```

説明

ウイルス・スパム検出時に管理者への通知を行うため、管理者への通知設定の SMTP サーバ (/opt/f-secure/fsigk/conf/fsigk.ini の admin_mx_host) の名前引きを行いましたが、失敗しました。

対処法

管理者への通知設定で設定した、SMTP サーバのホスト名が名前引きできるかご確認ください。

メッセージ

```
###ERROR### notify_admin:cannot connect to admin mail server[ホスト名:ポート番号] / strerror(xxx)=xxx
```

説明

ウイルス・スパム検出時に管理者への通知を行うため、管理者への通知設定の SMTP サーバ (/opt/f-secure/fsigk/conf/fsigk.ini の admin_mx_host,admin_mx_port) へ接続しましたが失敗しました。

対処法

管理者への通知設定で設定した SMTP サーバのホスト名・ポート番号に接続できるかご確認ください。

メッセージ

```
###ERROR### notify_admin:smtp error:[送信コマンド名]: buf=[応答行]
/strerror(xxx)=xxx
```

説明

ウイルス・スパム検出時に管理者への通知を行うための SMTP 接続中の応答メッセージでエラーが返りました。
"送信コマンド" 名は SMTP 接続の状態をあらわし、"HELO/MAIL FROM/RCPT TO/DATA/QUIT"(各コマンド送信時)、"GREETING"(接続開始時)、"DATA END"(データ送信終了時)のいずれかです。

対処法

[応答行] を確認し、管理者への通知設定で設定した SMTP サーバにメールを送信できるかご確認ください。

メッセージ

```
###ERROR### semget failure. Childnum(pre_spawn=[最大同時接続数])
may be large. If needed, maximum semaphore number(SEMMNI)
can increase by adding like 'kernel.sem=250 128000 32 512' on
'/etc/sysctl.conf' and running 'sysctl -p'./strerror(28)=No space
left on device
```

説明

セマフォの確保に失敗し、サービスを起動できませんでした。

対処法

サービスプロセス(fsigk_xxx)を、"kill -KILL"コマンドなどにより強制終了したさせた場合、セマフォが開放されずに残るたメーラが発生することがあります。この場合、サーバ(OS)を再起動することで復旧を行います。なお、現在の利用中のセマフォについては、"/proc/sysvipc/sem"で確認することも可能です。

また、最大同時接続数が多い場合、必要なセマフォ数が増えるために、このエラーが発生することがあります。特に必要がない場合、最大同時接続数を 2000 以内に設定してください。通常、2000 以上設定する必要はありません。

なお、本製品ではプロセス数に応じたセマフォ数が必要になります。同時接続数を多く設定する必要がある場合や他のプロセスがセマフォを多く利用している場合などは、以下の方法により OS 側で利用できるセマフォ数を増やすことができます。

1 以下の行を/etc/sysctl.confに追加する。

```
kernel.sem=250 128000 32 512
```

2 以下のコマンドを実行する。

```
# sysctl -p
```

3 以下のコマンドでセマフォ数が設定できたことを確認する。

```
# cat /proc/sys/kernel/sem
250 128000 32 512
```

メッセージ

```
###ERROR### sendfile timeout: No data can send while 120 sec. There maybe
temporary network trouble between receiver.) / URL=[...] ...
```

説明

120 秒間データを送信できず、セッションを切断した場合に記録します。

対処法

ネットワーク環境に問題がないかご確認ください。

メッセージ

```
###ERROR### get_response_header: Too Large Header
```

説明

HTTP の応答ヘッダが長い (10KB 以上の) 場合に表示されます。サービスの動作には問題ありません。

対処法

特定の URL、ブラウザで発生する問題かご確認ください。

メッセージ

```
###ERROR### main:diskspace_check: not enough diskspace in temporary
directory [ディレクトリ名].
```

説明

一時ディレクトリに空き容量が 5MB 以上ない場合に表示されます。サービスは開始しません。

対処法

空き容量を確保してください。

メッセージ

```
###ERROR### realtimescan_check : cannot open [%s]. Realtime virus scan seems
be enabled. Please stop realtime virus scan, or exclude scanning for temporary
directory [ディレクトリ名].
```

説明

本製品以外の何らかのウイルス検査ソフトが導入されており、一時ディレクトリに対してリアルタイムウイルス検査が有効になっている場合に表示されます。サービスは開始しません。

対処法

リアルタイムウイルス検査機能を無効にするか、一時ディレクトリに対してリアルタイムウイルス検査を除外してください。

メッセージ

```
###ERROR### smtp_data_cmd_senddata:[検出時の動作]:smtp error:[送信コマンド名]:
buf=[応答行] /strerror(xxx)=xxx
```

説明

ウイルス・スパム検出時に、送受信者への通知を行うための SMTP コマンドの応答メッセージでエラーが返りました。[検出時の動作] は、"DENY"(拒否)、"DELETE"(削除後送信者または受信者へ通知)、"SENDBACK"(削除後送信者へ通知)、"BLACKHOLE"(削除) です。[送信コマンド] 名は SMTP 接続の状態をあらわし、"RSET/MAIL FROM/RCPT TO/DATA/QUIT"(各コマンド送信時)、"DATA END"(データ送信終了時) のいずれかです。

対処法

[応答行] を確認し、転送先 SMTP サーバにメールを送信できるかご確認ください。

メッセージ

```
###ERROR### smtp_data_cmd_itr:AUTH buf=[応答行] /strerror(xxx)=xxx
```

説明

SMTP サーバとの SMTP 認証中に通常の応答コード (334, 5xx, 235) 以外が返った場合に表示されます。[応答行] が SMTP サーバの応答メッセージです。

対処法

SMTP サーバの応答メッセージが正しいかご確認ください。特に問題ないと考えられる場合、診断情報と認証中のパケットキャプチャ (tcpdump) の結果を送付してください。

メッセージ

```
###ERROR### ftp_noop_callback:NOOP command reply error [応答
行]/strerror(xxx)=xxx
```

説明

FTP サーバへの NOOP コマンド送信時に 200 以外の応答が返った場合に表示されます。

対処法

FTP サーバが接続を切断していないか、また FTP サーバが NOOP コマンドに正しく応答しているか確認ください。

メッセージ

```
###ERROR### XXXX /strerror(23)=Too many open files in system
```

説明

XXX には"open"等のファイルを開くことに関するメッセージが表示されます。
システム全体で開いているファイルの数が制限を越えた場合に発生します。
ファイルハンドルの数は /proc/sys/fs/file-nr で以下のように確認できます。

(表示コマンド) cat /proc/sys/fs/file-nr
[割り当て済みファイルハンドル数] [使用中のファイルハンドル数] [ファイルハンドルの最大数]
(例: # cat /proc/sys/fs/file-nr
1864 504 52403)

対処法

"lsof"コマンド等で、ファイルハンドルを異常に多く消費しているプロセスなどがないかご確認ください。
正常な状態で、使用中のファイルハンドル数がファイルハンドルの最大数に近くなっている場合、以下のように"/proc/sys/fs/file-max"を変更してシステムのファイルハンドル数を増やしてください。

1. sysctl.conf に以下のような行を追加(最大値を 65535 に設定する場合)
   fs.file-max = 65535
2. 以下のコマンドで設定を反映
   sysctl -p

メッセージ

```
###ERROR### ###ERROR### XXX cannot open
[/var/tmp/fsigk/proxytmp-xxx]/strerror(2)=No such file or directory
```

説明

本製品が利用している一時ファイルが開けない場合に表示されます。

対処法

一時ディレクトリのファイルを、コマンドや他のプログラムで削除していないか
ご確認ください。

メッセージ
```
###ERROR### Cannot find tproxy(version2) interface.
```

説明

TPROXY 利用設定(ソース IP 保持, transparent_tproxy=yes")を行っているが、
tproxy パッチが動作していない場合に表示されます。

対処法

tproxy パッチが kernel に適用されていない可能性があります。
ファイル/proc/net/tproxy が存在するかご確認ください。
Turbolinux 10 Server の場合は、以下の点をご確認ください。

- kernel-2.6.8-5 以降をご利用していること
  "uname -a"コマンドの結果で、カーネルバージョンが 2.6.8-5 以降に
  なっていることをご確認ください。
  カーネルバージョンが古い場合、Turbolinux10 の kernel を最新に
  アップデートしてください。
- iptable_tproxy モジュールが組み込まれていること。
  "lsmod"コマンドの結果に、"iptable_tproxy"モジュールが含まれているか
  ご確認ください。
  含まれていない場合、以下の手順でモジュールの組み込みを行ってください。
  1. /etc/sysconfig/iptables-config で、IPTABLES_MODULES の設定行を
     以下のように記述し、iptables が iptable_tproxy を読み込むように設定
     IPTABLES_MODULES="iptable_tproxy"
  2. iptables を再起動
     # /etc/rc.d/init.d/iptables restart
  3. /proc/net/tproxy が存在することを確認
  4. Internet Gatekeeper を再起動

また、旧バージョンの tproxy(version1)をご利用の場合は"transparent_tproxy_version=1"を設定ファイルに追加して、サービスを再起動してください。なお、tproxy version1 については今後対応を終了する可能性がございます。できるだけ version2 をご利用いただくことをおすすめいたします。

メッセージ
```
###ERROR### vsd_start() error
```

説明

定義ファイルや、検査エンジンライブラリの読み込みに失敗した。

対処法

定義ファイルやエンジン等の必要なファイルを削除した場合、以下のようなコマンドで上書きインストールを行ってください。

```
# rpm -Uvh --force fsigk-bin-xxx-0.i386.rpm
```

また、SELinux 等を有効にしている場合、ポリシーで拒否している可能性がないか確認するため、/var/log/messages ファイル等にエラーなどが表示されていないかご確認ください。また、SELinux 等を無効にしても発生するかご確認ください。SELinux の無効化は、/etc/sysconfig/selinux で"SELINUX=disabled"と記述し、サーバを再起動することで行っていただけます。

メッセージ

```
###ERROR### main:quit_signal:child(nnn)
stopped.(sig=17[SIGCHLD],si_code=3[CLD_DUMPED],status=xxx,childid=-1,cur
_pid=xxx,pid=xxx)
###ERROR### main:core dumped(child proxy process). Please send core
file(core or core.xxx) on the installation directory and diag.tar.gz to
F-Secure.
###ERROR### Error recovery: restarting service...
```

説明

プロキシプロセスが異常終了(コアダンプ)した。またサービスを再起動することで自動復旧を行いサービスを継続した。

なお、上記の３つのメッセージは連続して表示されます。

対処法

何らかの理由でプロキシプロセスが異常終了した場合に表示されます。サービスを再起動することで自動復旧を行いますので、サービスは引き続き提供できます。ただし、再起動の間 10 秒程度サービスが停止します。

このメッセージが表示された場合、本製品に何らかの問題が存在している可能性が高いです。

調査を行いますので、インストールディレクトリ(/opt/f-secure/fsigk/)の core で始まる名前のファイルをお送りください。

また、最新版以外をご利用の場合、できましたら最新版へのアップデートしてください。

メッセージ

```
###ERROR### main/accept_loop/accept(s=x):/strerror(104)=Connection reset
by peer
```

説明

kernel2.2 環境で接続直後に切断された場合に表示されることがあります。動作上は問題ありません。

対処法

kernel2.2 のサポートは終了しておりますので、できましたらディストリビューションのアップデートしてください。

メッセージ

```
###ERROR### LICENSE_ERROR#ret=-1#msg=License Expired
```

説明

エンジン親プロセスの終了前に子プロセスが終了した場合に表示されます。

対処法

体験版の試用期限が切れています。

メッセージ

```
###ERROR### fsav_open_session: Cannot connect to
fsavd'ssocket(./fsavd-socket-0). fsavd may be not running. Please
run'rc.fsigk_fsavd restart' to restart fsavd.
```

説明

検査エンジンプロセス(fsavd)のソケット(./fsavd-socket-0)に接続できませんでした。検査エンジンプロセス(fsavd)が起動していない可能性があります。

対処法

ウェブ画面から操作した場合、検査エンジンプロセス(fsavd)は自動的に起動します。コマンドラインからプロキシサービスを起動する場合などは、予め検査エンジンプロセス(fsavd)を起動してください。検査エンジンプロセスの再起動は、”/opt/f-secure/fsigk/rc.fsigk_fsavd restart”で行っていただきます。

メッセージ

(その他のメッセージ)

説明

通常発生しない問題の可能性があります。

対処法

状況を把握するため、エラーログファイルの内容と診断情報の送付をお願いいたします。

11.1.4 情報ログ(info.log)

その他の一般的な情報が記録されます。

■メッセージの形式

時刻(秒数) [日付 時刻 ポート 内部プロセス ID クライアント IP アドレス:クライアントホスト名:クライアントポート番号 サーバ IP アドレス:サーバホスト名:サーバポート番号] メッセージ

日時はエラー発生時の時刻です。最初の時刻はエポックタイム (1970/01/01 00:00:00(UTC)) からの秒数をミリ秒単位で表示します。

メッセージの形式・文面等は適時変更する可能性があります。

■サービス起動時の主なメッセージ

メッセージ

```
main: ### START ###(argv=[/opt/f-secure/fsigk/fsigk_xxx --daemon --http -f
conf/fsigk.ini ],ver=[バージョン],pid=プロセス ID)
```

説明

サービス開始メッセージです。サービス起動時に表示されます。

メッセージ

```
main: entering daemon mode. (daemon pid=4923)
```

説明

デーモン状態 (バックグランドプロセス) に移行したメッセージです。サービス起動時に表示されます。

メッセージ

```
main:entering debug mode...
```

説明

デバッグモードで起動した場合に表示されます。

メッセージ

```
main: accept_loop(sock=ソケット番号,pid=プロセス番号). Starting to accept
connection on each proxy process.
```

説明

プロキシプロセス起動時のメッセージです。サービス起動時に表示されます。

■サービス終了時のメッセージ

メッセージ

```
main: ### STOP ### (ver=[バージョン番号], pid=プロセス ID, sig=15[SIGTERM])
```

説明

終了メッセージです。サービス終了時に表示されます。

メッセージ

```
main:signal_handler(sig=15[SIGTERM], errno=0[Success], code=0[SI_USER],
status=0[], pid=xxxx, uid=0)/cur_pid=xxxx
```

説明

プロキシプロセスの SIGTERM シグナル受け取りメッセージです。サービス終了時に表示されます。

■サービス動作中のメッセージ

メッセージ

```
is_alivesocket:recv=XXX, Client closed connection. Client may be cancel the
session. url=[YYY], elasped=TTTms
```

説明

セッション接続中、通常のプロトコル動作が完了する前に、クライアントから接続終了した場合に表示されます。クライアントがキャンセル動作を行った場合等に表示されます。
TTT はセッション監視からの経過時間です。

メッセージ

```
is_server_alivesocket: select(s=AAA):ret=BBB,cur_pid=CCC: Server closed
connection while transaction. There may be timeout on the server because of
no traffic. (elasped=TTTms)
```

説明

セッション接続中、通常のプロトコル動作が完了する前に、サーバから接続終了した場合に表示されます。サーバ側でタイムアウトが発生した場合等に表示されます。
TTT はセッション監視からの経過時間です。

メッセージ

```
sendfile canceled: n=AAA, written=BBB, filelen=CCC writesize=DDD
```

説明

本製品から、クライアントまたはサーバにファイルを送信中に中断した場合に表示されます。AAA は sendfile システムコールの応答コード、BBB は送信済みファイルサイズ、CCC はファイルサイズ、DDD は現在送信中のデータサイズです。

メッセージ

```
http_forward_response_storeforward_trickle_send: sendfile canceled:
ret=AAA, tmpfile_offset=BBB, bytes=CCC: errno=xxx(xxx)
```

説明

本製品から、クライアントへの中継に trickle 機能を利用しており、ファイル中継中に中断した場合に表示されます。AAA は sendfile システムコールの応答コード、BBB は転送開始バイト数, CCC はファイルサイズ、DDD は現在送信中のデータサイズです。

メッセージ

```
file uploading is interrupted by client.
```

説明

HTTP サービスで、クライアントから本製品へのファイルアップロード中に中断した場合に表示されます。

メッセージ

```
From: %s:%d(%s) To: %s:%d(%s) Message-Id: %s Infected: %d VirusName: %s
```

説明

SMTP サービスで "From: クライアントアドレス:クライアントポート(送信元アドレス)" から、"To: サーバアドレス:サーバポート(送信先アドレス)" に、"Message-Id: メッセージ ID" を持つメールを送信しました。
検査結果は、"Infected: 検出結果(0 以外で検出)"、"Virusname: ウイルス名" です。

メッセージ

```
ERROR DATAEND url=[XXX] buf=[YYY]
```

説明

SMTP サービスで､DATA コマンドで XXX 宛にメール送信時にメールサーバがエラーコード YYY を返しました。

メッセージ

```
Access Denied from [アドレス:ホスト名]
```

説明

アクセス制御で接続元制限を有効にしており、該当サーバが接続元一覧に登録されていないため、接続を拒否しました。

メッセージ

```
Access Denied to [アドレス:ホスト名]
```

説明

アクセス制御で接続先制限を有効にしており、該当サーバが接続先一覧に登録されていないため、接続を拒否しました。

メッセージ

```
read extra CRLF for POST method
```

説明

Internet Explorer で、POST メソッドでのデータ送信時に、通常は不要な CRLF コードが付加されることがあります。
この不要な CRLF コードを取り除いた場合に表示されるメッセージです。動作上は問題ございません。
(参照: Microsoft Knowledge Base 823099
Extra CRLF Character Is Added to a POST Request That Is Sent to an HTTP 1.1 Server
http://support.microsoft.com/default.aspx?scid=kb;en-us;823099&Product=ie600)

メッセージ

```
ERROR Reply(DATA) url=[%s] buf=[%s]
ERROR Reply(DATAEND): url=[%s] buf=[%s]
ERROR Reply(MAIL): buf=[%s]
ERROR Reply(RCPT): buf=[%s]
ERROR Reply(AUTH): buf=[%s]
ERROR Reply(QUIT): buf=[%s]
```

説明

SMTP サービスで、SMTP サーバへ送信したコマンドに対してエラー応答が返った場合に表示されます。buf=xxx には応答メッセージが含まれます。カッコ内は送信したコマンド名(DATAEND はメール本文送信をあらわす)になります。

11.2 時刻表示変換ツール（logconv）

多くのログの時刻表示がエポックタイムからの秒数で表示されていますが、logconv ツールで年月日時分秒表示を行頭に追加できます。logconv ツールは以下のように実行します。オプションは省略可能です。

/opt/f-secure/fsigk/misc/logconv [ログファイル名]

(Windows 上で実行する場合”/opt/f-secure/fsigk/misc/logconv.exe”を利用いただけます。)

■オプション

--tail [num] 最後の [num] 行を出力します。

--tailsec [sec] 最後の [sec] 秒分を出力します。

--cgi CGI から呼び出す場合に利用します。

--today 本日分のログを出力します。

--noconv 時刻変換を行いません。

-r 変換後のデータを変換前のデータに戻します。

変換結果は標準出力に表示されます。--tail <num>オプションを指定するとログの最後からの指定行数のみ表示します。
logconv コマンドが扱えるログサイズは 2GB が上限です。それ以上の場合、head、tail コマンド等で分割、抽出後に変換できます。
なお、ウェブ管理画面からアクセスログ・ウイルス検出ログを確認した場合は、変換後の内容が表示されます。

11.3 ログの外部出力設定（syslog 等）

ログは通常ファイルとして保存されますが、必要に応じて syslog 等のファイル以外への出力が可能です。外部への出力は、外部コマンドにパイプを通じて送信することで行います。設定は、設定ファイル (/opt/f-secure/fsigk/conf/fsigk.ini) に以下のように記述することで行います。

```
access_log=|外部コマンド (アクセスログの場合)
detect_log=|外部コマンド (ウイルスログの場合)
info_log=|外部コマンド (情報ログの場合)
error_log=|外部コマンド (エラーログの場合)
```

例えば、SMTP のウイルス検出情報、エラー情報を syslog の local0 ファシリティ、err レベルに出力する場合、/opt/f-secure/fsigk/conf/fsigk.ini の [smtp] グループに以下のように設定を追加します。

```
[smtp]
detect_log=|logger -t fsigk -p local0.err
error_log=|logger -t fsigk -p local0.err
```

ファイル出力も同時に行う場合は、以下のように設定します。

```
[smtp]
detect_log=|tee -a log/smtp/detect.log | logger -t fsigk -p local0.err
error_log=|tee -a log/smtp/error.log | logger -t fsigk -p local0.err
```

設定ファイル変更後は、ウェブ管理画面またはコマンド (rc.fsigk_smtp)によりサービスの再起動を行います。

11.4 ログローテーション

ログローテーションを有効にすると、ログのローテーション(分割)が行われます。
ログローテーションの設定ファイルは、/etc/logrotate.d/virusgw　です。

11.5 利用統計グラフ

アクセス解析ツール webalizer による利用統計グラフを表示します。
webalizer による解析は、cron で定期的に実行され、/etc/cron.d/virusgw.cron 内の updateWebalizer.pl 行で設定されています。

12. 隔離ディレクトリ

検出されたウイルスファイルやスパムメールの隔離先のディレクトリです。隔離ディレクトリは、/home/spool/virusgw/quarantine です。隔離ディレクトリを使用する場合は、ディスクの空き容量に配慮してください。

13. 製品動作仕様

13.1 動作仕様一覧

本製品の動作仕様は以下のとおりです。

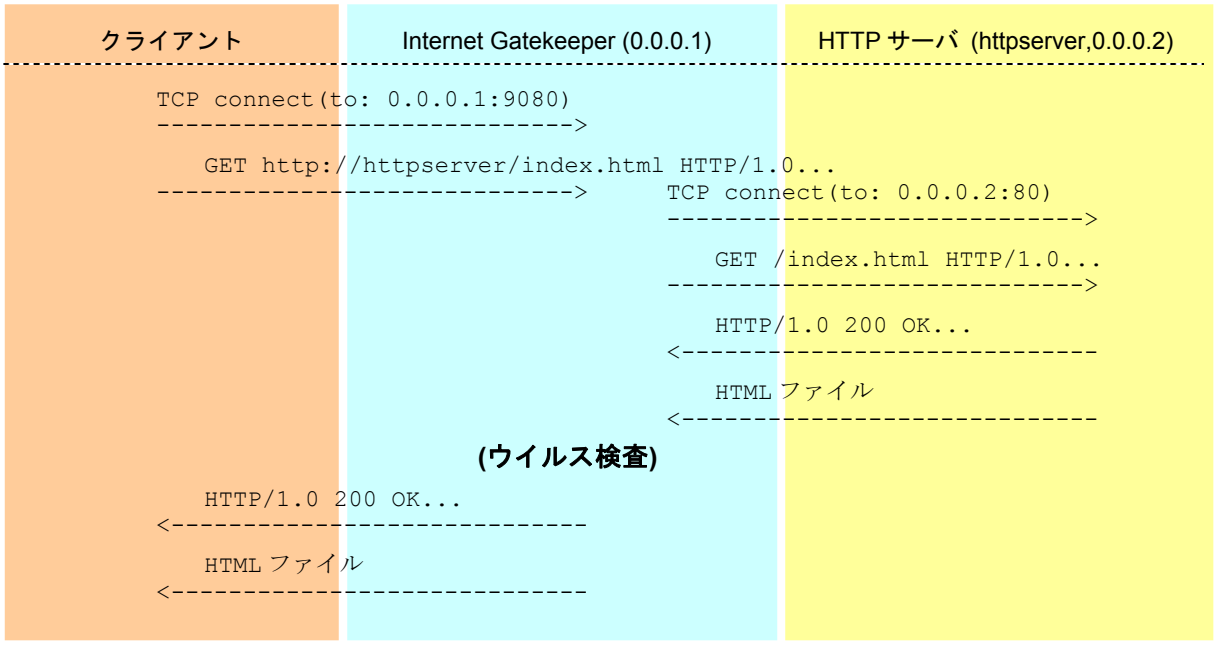
ウェブ管理画面	日本語
インストーラ	rpm
対応ネットワークプロトコル	IPv4(RFC791) / TCP(RFC793)
対応アプリケーションプロトコル	HTTP, FTP, SMTP, POP
対応モード	プロキシ型（プロキシモード、メールサーバ共有プロキシモード） 透過ルータ型（透過プロキシモード）
HTTP 検査対象メソッド	GET/POST/PUT
HTTP 利用可能メソッド	GET/POST/PUT/HEAD/CONNECT/OPTIONS,/DELETE/TRACE/PROPFIND/PROPPATCH/COPY/MOVE/LOCK/UNLOCK, その他同様の要求応答型のメソッド ※ CONNECT(SSL/HTTPS) は暗号化されているため、ウイルス検査は行いません。
HTTP プロキシ対応スキーマ	http://,ftp://
HTTP 対応プロトコル仕様	HTTP/1.0(RFC1945), HTTP/0.9(RFC1945), HTTP/1.1 (RFC2616), WEBDAV(RFC2518) (HTTP/1.1 要求は HTTP/1.0 に自動変換)
HTTP 対応認証方式	HTTP プロキシ認証 (Basic)
HTTP 最大転送サイズ	制限なし
HTTP URL 最大長	2098 バイト
SMTP 検査対象コマンド	DATA
SMTP 利用可能コマンド	MAIL/RCPT/DATA/RSET/VRFY/EXPN/HELP/NOOP/QUIT/XFORWARD/ AUTH
SMTP 対応プロトコル仕様	SMTP(RFC 2821), SMTP Auth(RFC2554)
SMTP 対応認証方式	SMTP Auth(PLAIN, LOGIN), POP before SMTP
SMTP 最大転送メールサイズ	2,000,000,000 バイト
POP 検査対象コマンド	RETR/STOR
POP 利用可能コマンド	USER/PASS/APOP/UIDL/TOP/STAT/LIST/RETR/DELE/NOOP/RSET/QUIT/ AUTH,その他同様の要求応答型コマンド ※ APOP は、プロキシ型で [親サーバのユーザによる選択] を有効にした場合は利用できません。
POP 対応プロトコル仕様	POP3(RFC1939), POP3 Auth(RFC1734) ※ APOP は、プロキシ型で [親サーバのユーザによる選択] を有効にした場合は利用できません。
POP 対応認証方式	ユーザ名 (USER コマンドの引数)

POP 最大転送サイズ	2,000,000,000 バイト
FTP 検査対象コマンド	RETR/STOR/STOU/APPE
FTP 利用可能コマンド	USER/PASS/RETR/LIST/NLST/STOR/STOU/APPE/QUIT/PORT/PASV, その他同様の要求応答型コマンド
FTP 対応プロトコル仕様	FTP (RFC959)
FTP 対応認証方式	ユーザ名 (USER コマンドの引数)
FTP 最大転送サイズ	制限なし
検査可能最大サイズ	2GB (圧縮ファイルの場合、展開前・展開後ともに 2GB が上限)
検査圧縮形式	ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2 / 6 階層
利用するセマフォ	セマフォ集合ごとのセマフォ数(SEMMS): 250 以内 セマフォ識別子の数(SEMMNI): 各サービス(http,smtp,ftp,pop,admin)ごとに、 (最大同時接続数 / 25) + 10 以内
利用する共有メモリ	共有メモリ識別子の数(SHMMNI): 各サービス(http,smtp,ftp,pop,admin)ごとに 10 以内 メモリサイズ(SHMMAX): 各サービス(http,smtp,ftp,pop,admin)ごとに 1MB 以下

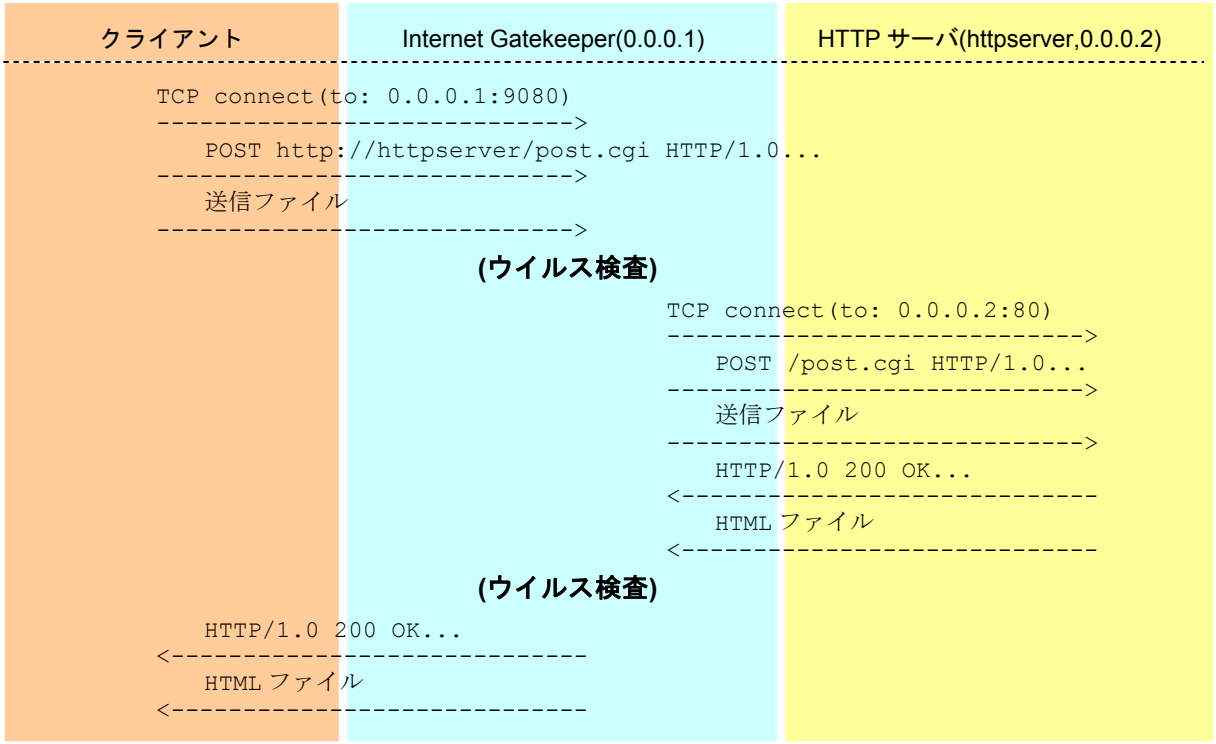
13.2 HTTP プロキシのプロトコル処理例

HTTP プロキシでの一般的なプロトコル処理例は以下のとおりです。

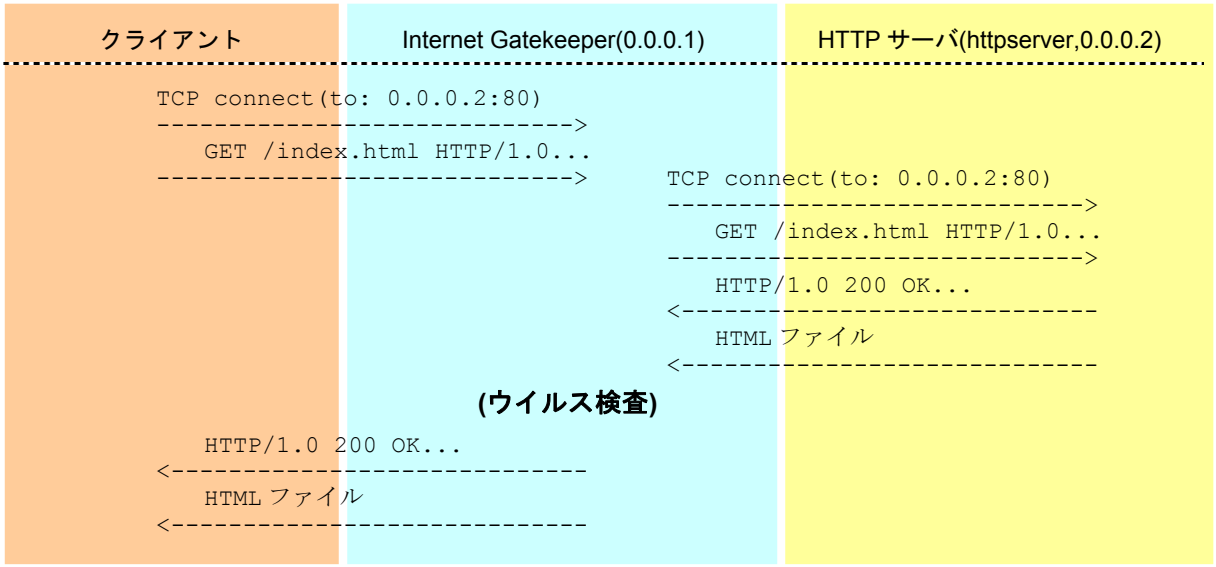
■プロキシ型、GET メソッドの場合



■プロキシ型、POST メソッド（ファイル送信時、送信ファイルの検査あり）の場合



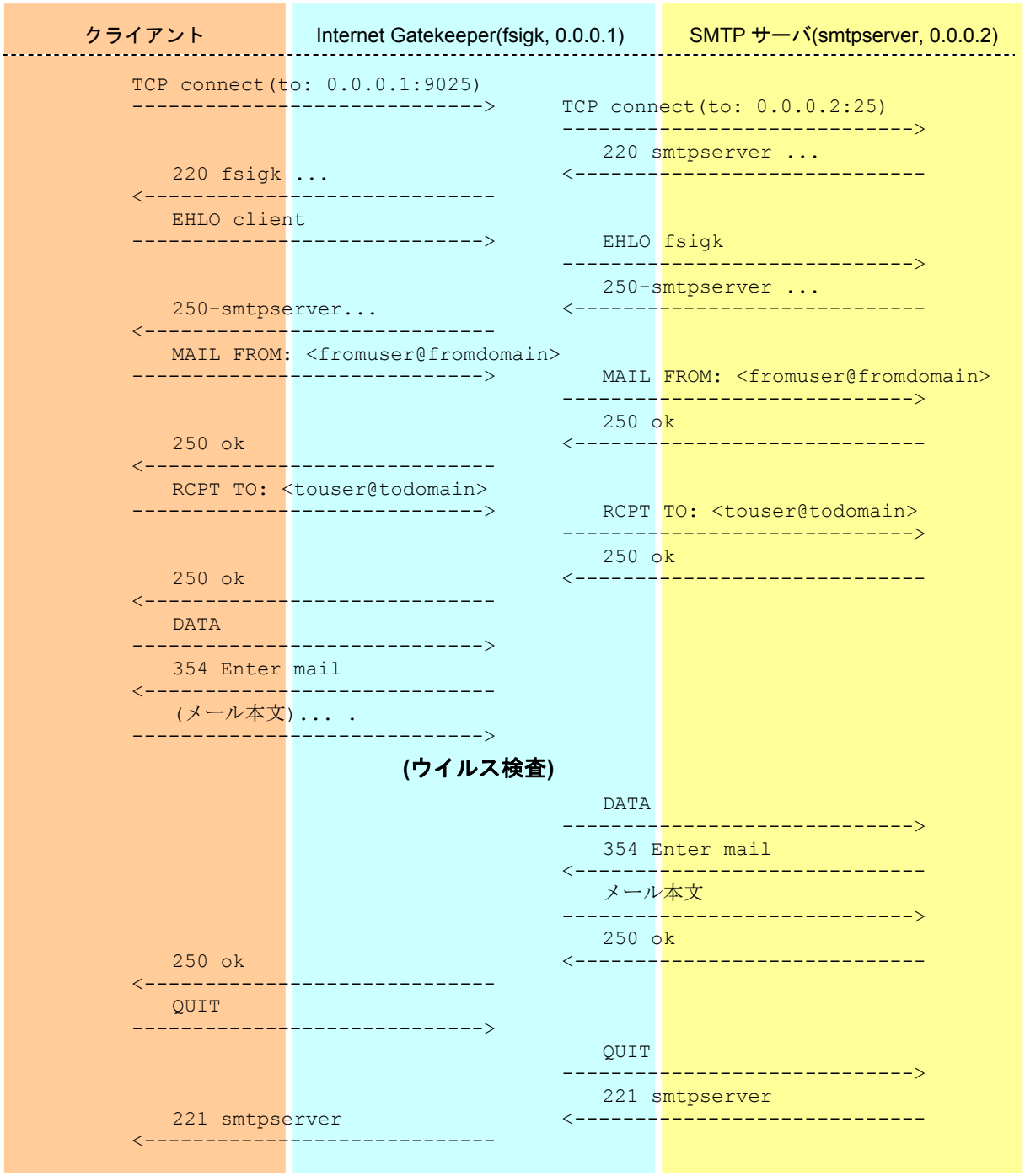
■透過型、GET メソッドの場合



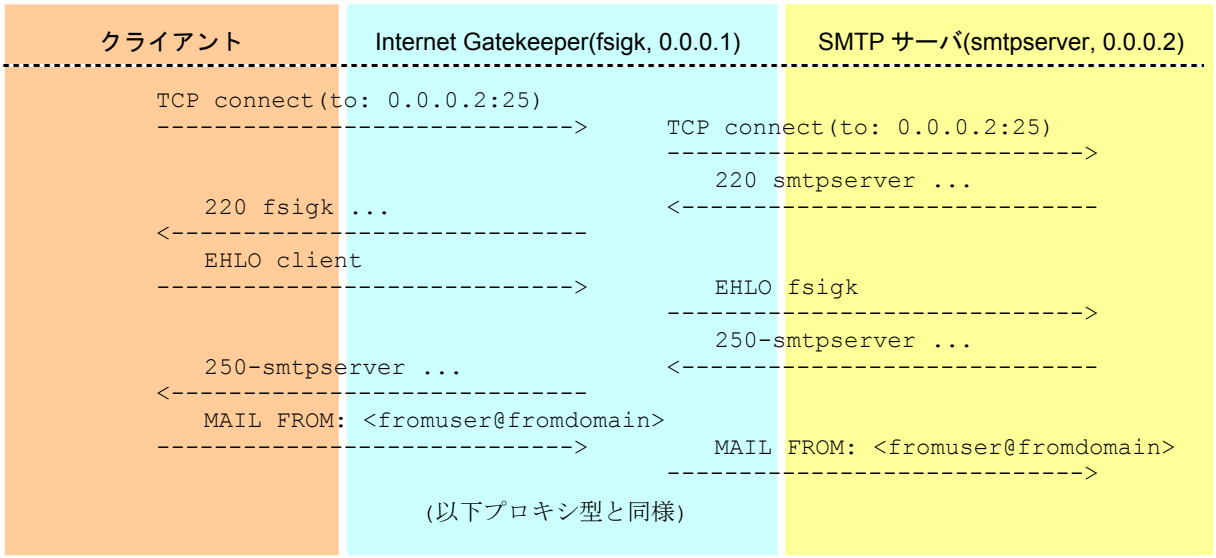
13.3 SMTP プロキシのプロトコル処理例

SMTP プロキシでの一般的なプロトコル処理例は以下のとおりです。

■プロキシ型の場合



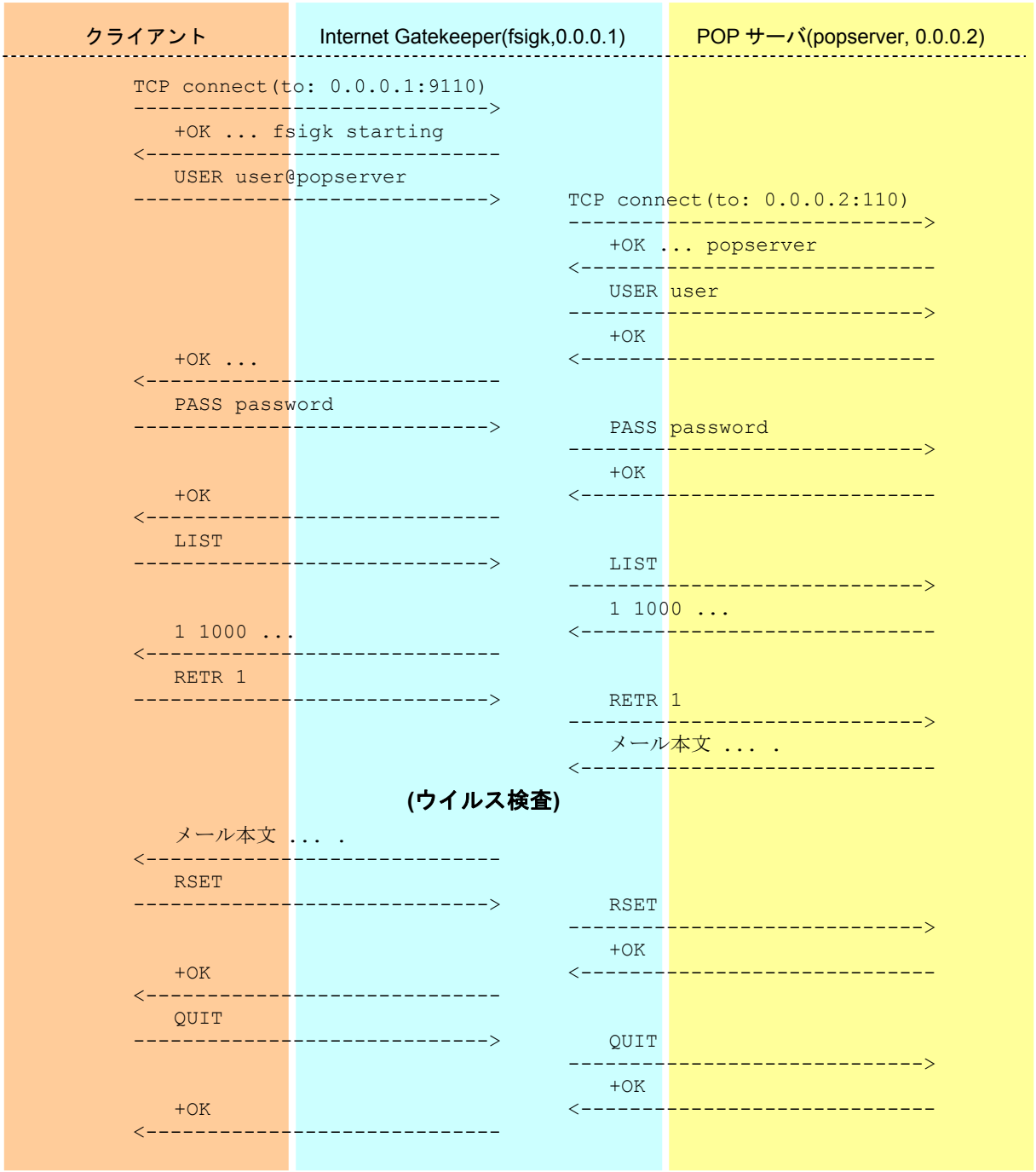
■透過型の場合


クライアント
Internet Gatekeeper(fsigk, 0.0.0.1)
SMTP サーバ(smtpserver, 0.0.0.2)
TCP connect(to: 0.0.0.2:25)
TCP connect(to: 0.0.0.2:25)
220 smtpserver ...
220 fsigk ...
EHLO client
EHLO fsigk
250-smtpserver ...
250-smtpserver ...
MAIL FROM: <fromuser@fromdomain>
MAIL FROM: <fromuser@fromdomain>
(以下プロキシ型と同様)

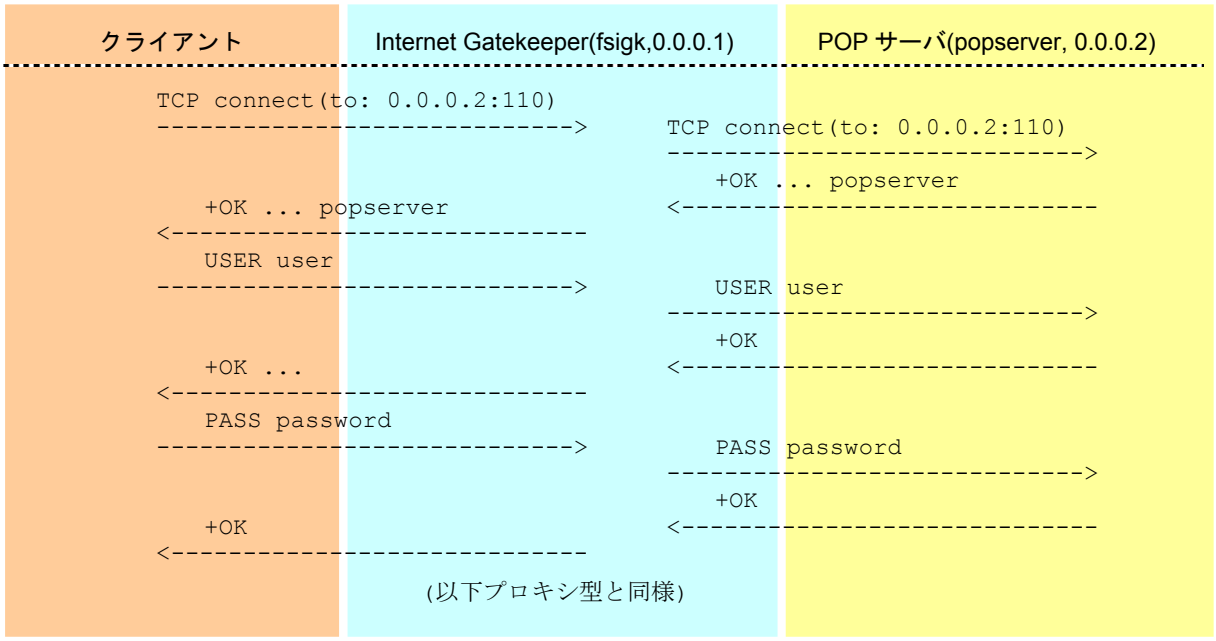
13.4 POP プロキシのプロトコル処理例

POP プロキシでの一般的なプロトコル処理例は以下のとおりです。

■プロキシ型の場合



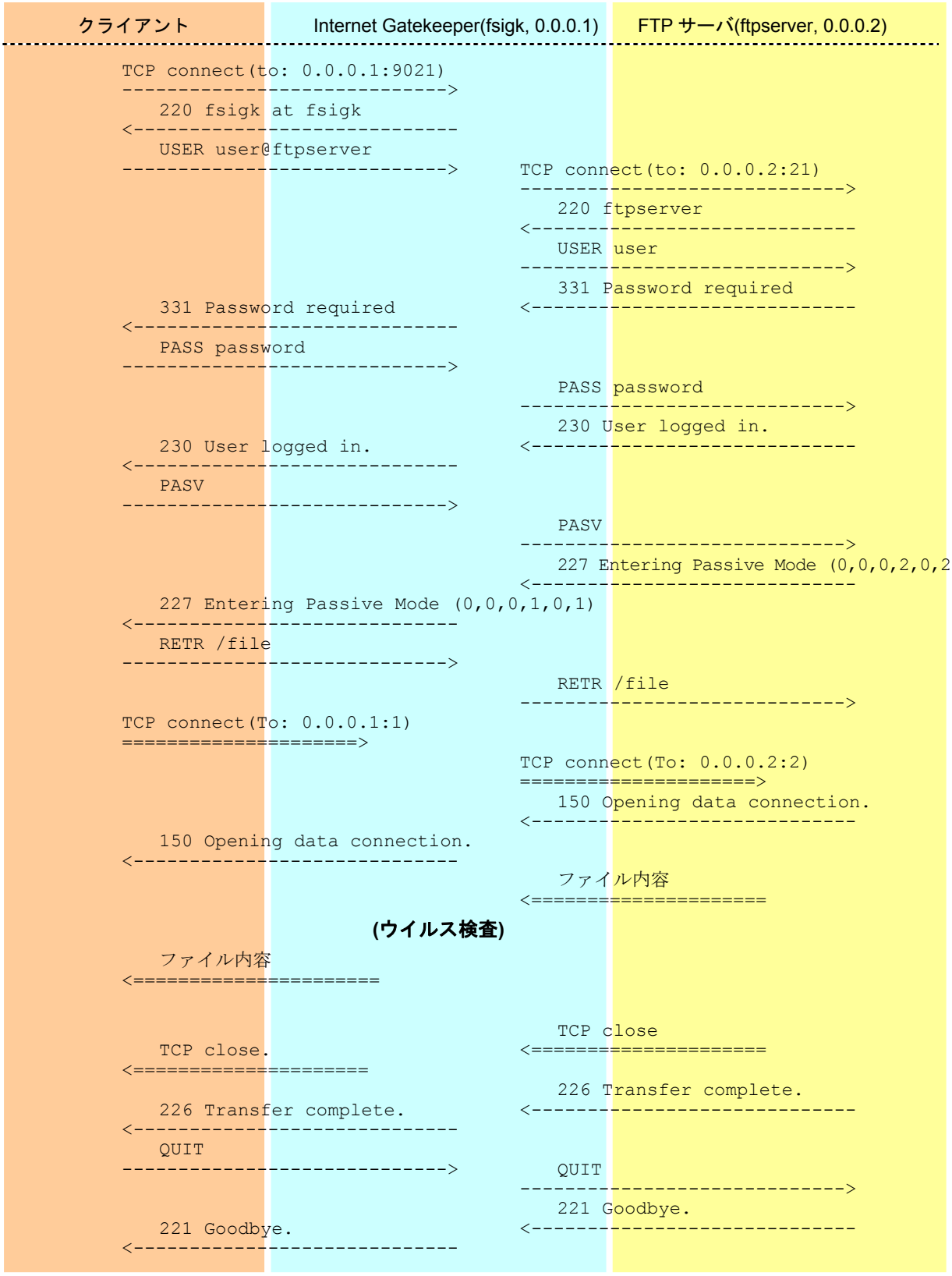
■透過型の場合


クライアント
Internet Gatekeeper(fsigk,0.0.0.1)
POP サーバ(popserver, 0.0.0.2)
TCP connect(to: 0.0.0.2:110)
TCP connect(to: 0.0.0.2:110)
+OK ... popserver
+OK ... popserver
USER user
USER user
+OK
+OK ...
PASS password
PASS password
+OK
+OK
(以下プロキシ型と同様)

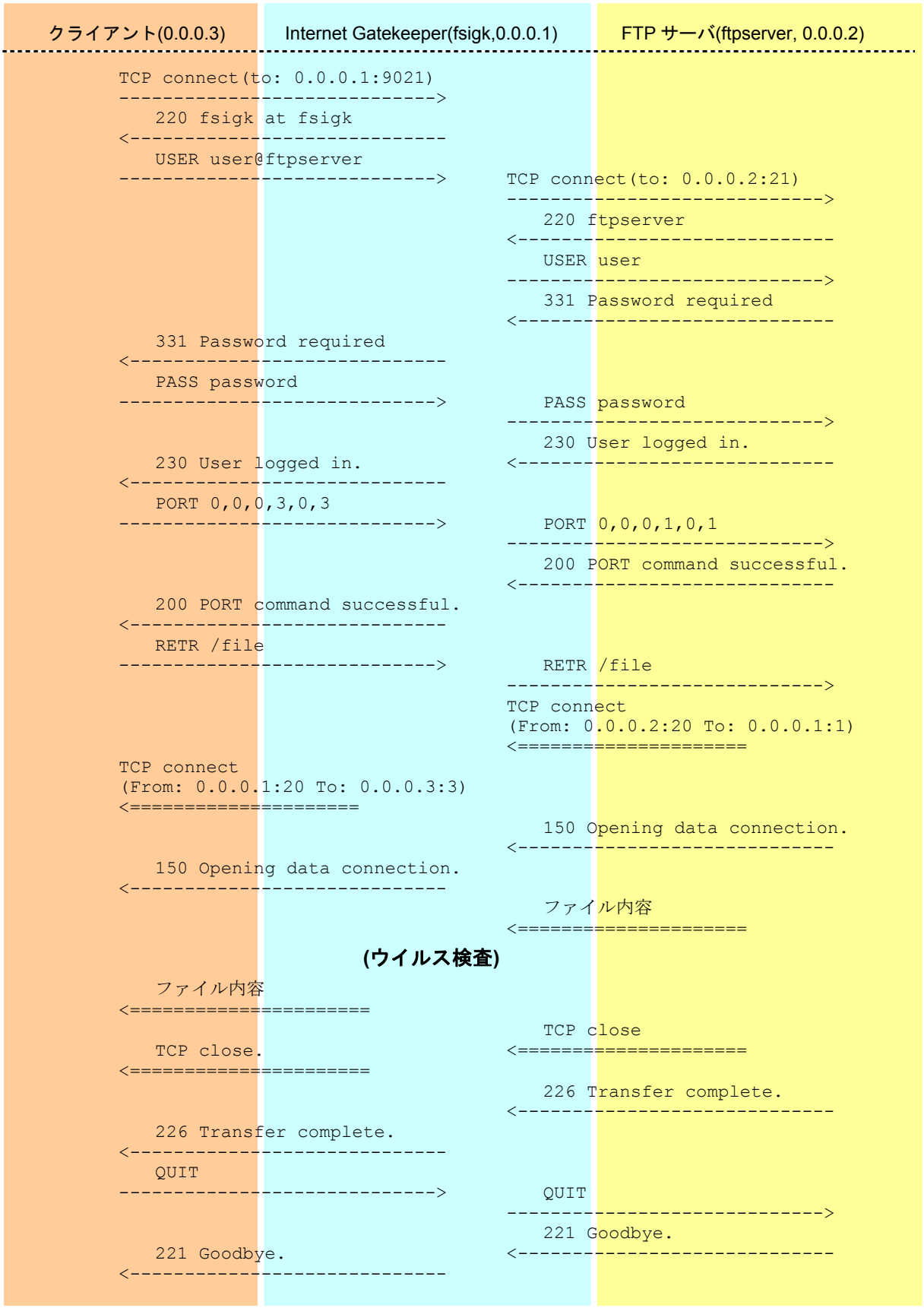
13.5 FTP プロキシのプロトコル処理例

FTP サービスでは、コントロールセッションとデータセッションの両方を中継します。FTP プロキシでの一般的なプロトコル処理例は以下のとおりです。

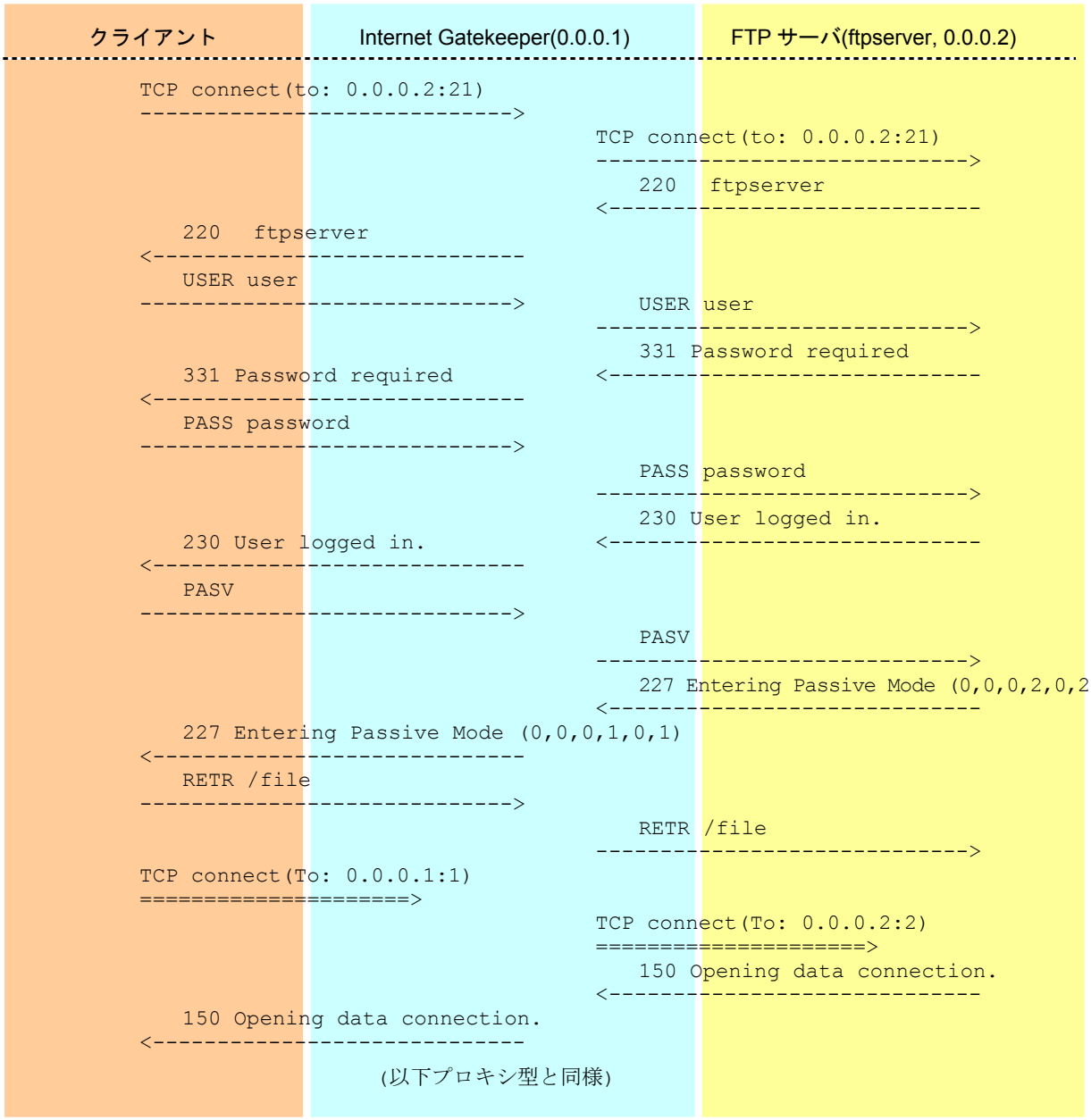
■プロキシ型、パッシブモード FTP の場合



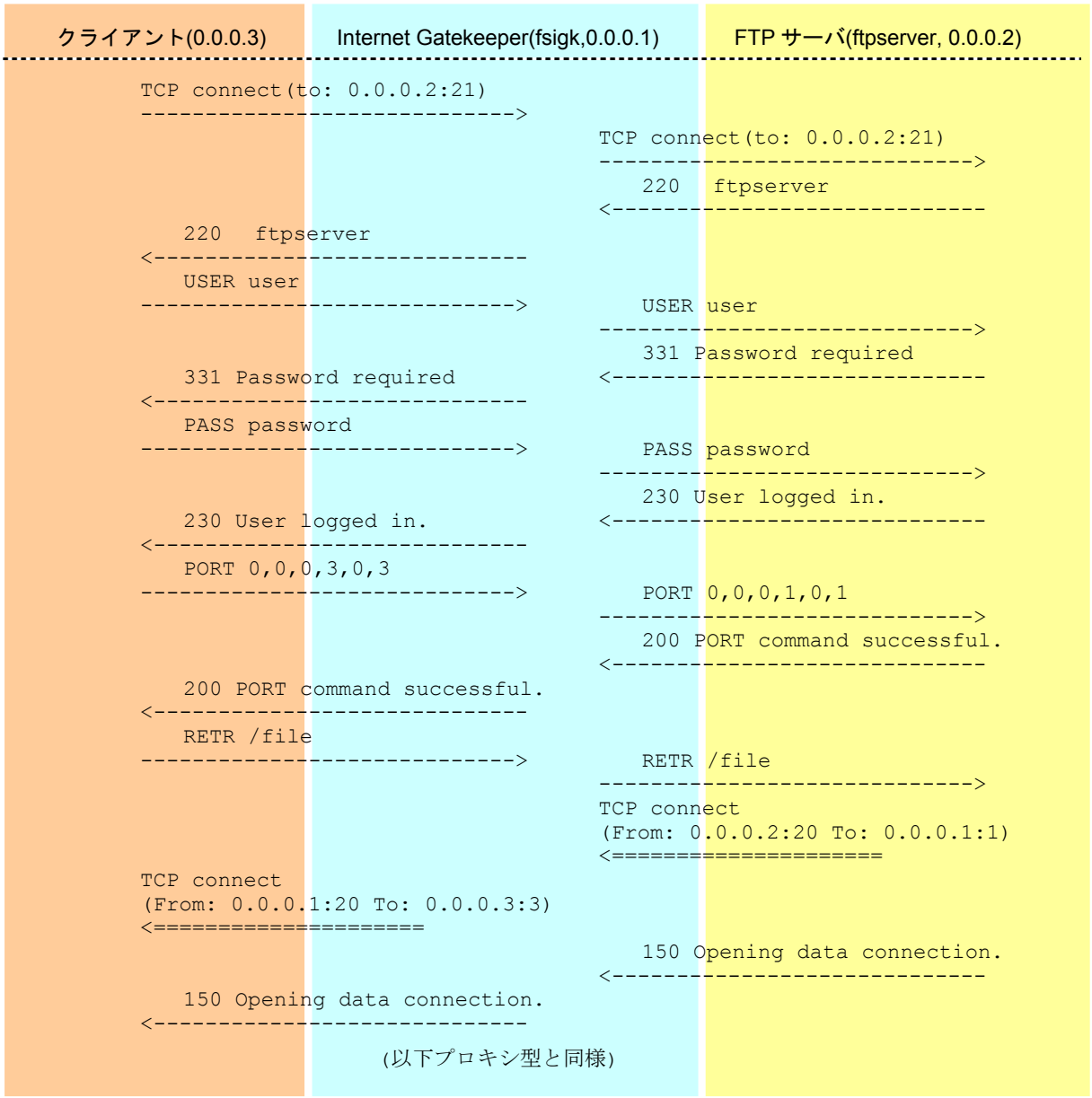
■プロキシ型、アクティブ FTP の場合



■透過型、パッシブモード FTP の場合



■透過型、アクティブ FTP の場合



13.6 HTTP エラー応答一覧

HTTP 接続時にエラーが発生した場合の、応答内容一覧は以下のとおりです。クライアントに表示されるメッセージは、エラーメッセージのテンプレートファイル (`/opt/f-secure/fsigk/conf/template_http_error.html`) で編集できます。

■サーバ接続エラー

概要	サーバへの接続に失敗した
応答コード	503
応答理由	Service Unavailable
応答メッセージ	接続エラーメッセージです。 詳細は「13.12　接続エラーメッセージ一覧」を参照してください。

■要求メソッド長エラー

概要	要求メソッドが最大長 (98 バイト) を超えた
応答コード	400
応答理由	Bad Request
応答メッセージ	Too long Request Method

■要求メソッド文字エラー

概要	要求メソッドに不正な文字(文字コード 0x20 未満の文字)が使われていた
応答コード	400
応答理由	Bad Request
応答メッセージ	Illegal method character

■要求 URL 長エラー

概要	要求 URL が最大長 (2098 バイト) を超えた
応答コード	414
応答理由	Request-URI Too Long
応答メッセージ	Request-URI Too Long

■要求 URL 文字エラー

概要	要求メソッドに不正な文字(文字コード 0x20 未満の文字)が使われていた
応答コード	400
応答理由	Bad Request
応答メッセージ	Illegal URL character

■要求 URL フォーマットエラー

概要	要求 URL の形式が不正
応答コード	400
応答理由	Bad Request
応答メッセージ	Invalid URL format

■要求バージョン長エラー

概要	要求 HTTP バージョンが最大長 (98 バイト) を超えた
応答コード	400

応答理由	Bad Request
応答メッセージ	Too long Request Version

■要求バージョンエラー

概要	要求 HTTP バージョンとして、"HTTP/1.0"、"HTTP/1.1"、""(HTTP/0.9)以外が指定された。
応答コード	505
応答理由	HTTP Version Not Supported
応答メッセージ	Only support HTTP/0.9, HTTP/1.0, HTTP/1.1

■プロキシ認証エラー

概要	プロキシ認証に失敗した
応答コード	407
応答理由	Proxy Authentication Required
応答メッセージ	Proxy Authentication Required
追加ヘッダ	Proxy-Authenticate: Basic realm="input proxy user/pass"

13.7 HTTP 要求・応答ヘッダの扱い

HTTP の要求ヘッダ・応答ヘッダの内容は基本的に変更しませんが、以下のヘッダについては変更を行います。

■要求ヘッダの変更

- 要求行

  要求バージョンが"HTTP/1.1"の場合、"HTTP/1.0"に変更

  親サーバ設定がなく透過型でない場合、URL のパス名より前の部分は削除。

  (例: http://xxx:yyy/aaa/iii/uuu => /aaa/iii/uuu)

- Connection

  既存の Connection ヘッダは削除。
  Keep-Alive 接続の場合、Connection: Keep-Alive を追加。

- Proxy-Connection

  既存の Proxy-Connection ヘッダは削除。

- Via

  匿名プロキシの場合は変更なし。
  それ以外の場合は以下の内容で追加します。

  Via : 1.0 ホスト名:待ち受けポート (製品名)

  既存の Via ヘッダが存在する場合は","区切りで後ろに追加します。

- X-Forwarded-For

  匿名プロキシの場合は変更なし。
  それ以外の場合は、以下のように接続元の IP アドレスを追加します。

  X-Forwarded-For: 接続元 IP アドレス

  既存の X-Forwarded-For ヘッダが存在する場合は","区切りで後ろに追加します。

- Keep-Alive
  既存の Keep-Alive ヘッダは削除。

- Trailer
  既存の Trailer ヘッダは削除。

- Proxy-Authorization
  プロキシ認証が有効な場合は削除。

■応答ヘッダの変更

- 応答行

  バージョンが"HTTP/1.1"の場合、"HTTP/1.0"に変更

- Connection

  既存の Connection ヘッダは削除。

  Keep-Alive 接続の場合は、以下の内容で追加。

  Connection : Keep-Alive

- Proxy-Connection

  既存の Proxy-Connection ヘッダは削除。

- Proxy-Support

  "WWW-Authenticate"ヘッダがあり、透過型でなく、親サーバがない場合に以下の内容で追加します。

  Proxy-Support : Session-Based-Authentication

  ("Proxy-Support: Session-Based-Authentication "は NTLM 認証などをプロキシで利用する場合に必要です。RFC-4559 を参照ください。)

13.8 SMTP コマンド応答一覧

SMTP 接続時には基本的にサーバからの応答をクライアントに中継しますが、Internet Gatekeeper 自身が生成する応答もあります。以下のメッセージが Internet Gatekeeper 自身が生成する応答一覧になります。

[応答メッセージ] (製品名)
(例: 500 Unknown Command: "TEST" (F-Secure/fsigk_smtp/230/gwdev.gw.f-secure.co.jp))

■DATA コマンド応答

応答メッセージ	354 Enter mail
応答理由	送信メールデータ受信を開始します。

応答メッセージ	250 Message accepted for delivery
応答理由	送信メールデータ受信を完了しました。

応答メッセージ	554 SENDBACK:smtp error[COMMAND] (Server Reply: XXX)
応答理由	送信者へ通知を行う場合に送信したコマンド(COMMAND)でエラー応答(XXX)が返りました。 COMMAND は RSET/MAIL FROM/RCPT TO のいずれかです。

応答メッセージ	250 Message accepted for delivery
応答理由	送信メールデータ受信を完了しました。

応答メッセージ	554 Too long message
応答理由	データサイズが指定した最大サイズを超えました。 最大サイズは、上級者向けオプションの block_messagesize/block_message_len で指定した数字、又は 2,000,000,000 バイトです。

応答メッセージ	554 Infected by [検出名]
応答理由	ウイルス検出時の動作が"拒否"の場合に、ウイルスを検出した際に表示されます。

■接続時応答

応答メッセージ	421 server open error(ホスト:ポート) errmsg=[XXX]
応答理由	指定したホスト、ポートへの接続に失敗しました。 ERRMSG は「13.12　接続エラーメッセージ一覧」の内容が表示されます。

応答メッセージ	421 Cannot get correct greeting message from mail server(ホスト:ポート). return code=DDD
応答理由	SMTP サーバ接続後のグリーティングメッセージが正しくありませんでした。SMTP サーバからの応答コードが 220 以外の場合に表示されます。

■任意のコマンドの応答

応答メッセージ	500 Too long line
応答理由	コマンド行の長さが 9999 バイト以上でした。

■HELO, EHLO, AUTH, QUIT, RSET コマンド以外の応答

応答メッセージ	500 Authentication Required"
応答理由	メール送信に必要な認証が完了していません。以下の場合に表示されます。 · POP before SMTP 認証または SMTP 認証が有効 · 認証が成功していない · LAN 内からの接続ではない · 受信ドメインの制限を行っていない

■HELO/EHLO コマンドの応答

応答メッセージ	421 (COMMAND) disconnected from (ホスト:ポート)
応答理由	COMMAND 送信時にサーバが切断していた。 COMMAND は HELO、EHLO のいずれか。

■MAIL コマンドの応答

応答メッセージ	501 Syntax error ("MAIL FROM:").
応答理由	MAIL コマンドが不正。(FROM がない)

■RCPT コマンドの応答

応答メッセージ	500 RCPT command must begin with "RCPT TO:.
応答理由	RCPT コマンドが不正。(TO がない)

応答メッセージ	250 Recipient ok"
応答理由	中継を拒否しました。 受信ドメインの制限を行っており、必要な認証が終了していない場合に表示されます。

■AUTH コマンドの応答

応答メッセージ	504 this mechanism not available
応答理由	指定の認証方式(PLAIN,LOGIN 以外)はサポートしていません。

応答メッセージ	235 ok authed
応答理由	認証に成功しました。 Internet Gatekeeper 自身で SMTP 認証を行っている場合のみ表示します。SMTP サーバ側で認証を行っている場合、SMTP サーバの応答を中継します。

応答メッセージ	535 authorization failed
応答理由	認証に失敗しました。 Internet Gatekeeper 自身で SMTP 認証を行っている場合のみ表示します。SMTP サーバ側

	で認証を行っている場合、SMTP サーバの応答を中継します。

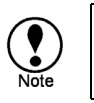
応答メッセージ	500 disconnected from server(AUTH).
応答理由	認証中にサーバが切断しました。

■未知のコマンド受信時

応答メッセージ	500 Unknown Command: "COMMAND"
応答理由	指定したコマンド(COMMAND)はサポートしていない

13.9 SMTP コマンド動作概要一覧

SMTP 接続時に、クライアントから送信されたコマンドに対する動作概要は以下のとおりです。



[製品名] は、デフォルトで "F-Secure/fsigk_smtp/バージョン/ホスト名" になります。
上級者向けオプションの "product_name=" で設定変更可能です。

■クライアント接続時

1 サーバに接続

2 サーバ接続失敗時

① クライアントへ送信: 421 server open error([サーバホスト]:[サーバポート]) errmsg=[接続エラーメッセージ]

➔ 接続エラーメッセージについては「13.12　接続エラーメッセージ一覧」を参照してください。

② セッション終了

3 サーバ応答受信

4 応答コードが 220 以外の場合は接続終了

5 クライアントへ送信：220 [ホスト名] [製品名]

■各コマンド行受信時

1 1 行が 9998 バイト以上の場合

① クライアントへ送信：500 Too long line ([製品名])

② 接続終了

2 以下の全ての条件を見たし、HELO, EHLO, AUTH, QUIT, RSET コマンド以外を受け取った場合

POP before SMTP 認証または SMTP 認証が有効

認証が成功していない

LAN 内からの接続ではない

受信ドメインの制限を行っていない

① クライアントへ送信：500 Authentication Required ([製品名])

3 1,2 以外の場合は各コマンドを処理する。

■HELO コマンド受信時

1 サーバへ送信：HELO [ホスト名]

2 サーバ応答受信

3 クライアントへ送信：[サーバ応答内容]

■EHLO コマンド受信時

1 サーバへ送信：EHLO [ホスト名]

2 サーバ応答受信

3 応答内容から以下のオプション行を削除する。
CHUNKING, BINARYMIME, PIPELINING

4 応答内容の SIZE オプションに、サーバからの SIZE オプション応答と最大メッセージサイズ (デフォルト:2,000,000,000) の小さい方を設定する。

5 プロキシ認証が有効の場合、応答内容に以下のオプション行を追加する。
250-AUTH PLAIN LOGIN

6 クライアントへ送信：[応答内容]

■MAIL コマンド受信時

1 コマンド構文が正しくない場合
① クライアントへ送信：501 Syntax error (MAIL FROM:) ([製品名])

2 サーバへ送信：[クライアント受信内容]

3 サーバ応答受信

4 クライアントへ送信：[サーバ応答内容]

■RCPT コマンド受信時

1 コマンド構文が正しくない場合
① クライアントへ送信：500 RCPT command must begin with "RCPT TO:" ([製品名])

2 受信ドメインの制限を行っており、必要な認証が終了していない場合
① クライアントへ送信：550 Relaying denied. ([製品名])

3 サーバへ送信：[クライアント受信内容]

4 サーバ応答受信

5 クライアントへ送信：[サーバ応答内容]

6 応答コードが 250 以外の場合
① セッション終了

■AUTH コマンド受信時

1 SMTP 認証設定が有効の場合
① 認証成功した場合
1) クライアントへ送信：235 ok authed ([製品名])
② 認証失敗した場合
1) クライアントへ送信：535 authorization failed ([製品名])
③ サポートしていない認証の場合 (PLAIN,LOGIN 以外)
1) クライアントへ送信：504 this mechanism not available ([製品名])

2 SMTP 認証設定が無効の場合
① 認証要求、認証応答をサーバとクライアント間で転送

■DATA コマンド受信時

1 クライアントへ送信：354 Enter mail ([製品名])

2 メールデータ受信

3 ウイルス・スパム検査

4 ウイルス・スパム検出した場合

① ウイルスログへの記録

② 管理者への通知 (有効な場合)

5 メールサイズが最大メッセージサイズを超えた場合

① クライアントへ送信：554 Too long message ([製品名])

6 ウイルス・スパム検出した場合で、検出時の動作が "駆除"、"何もしない"、"件名変更"以外の場合

① 検出時の動作が拒否の場合

1) サーバへ送信：RSET
2) サーバ応答受信
3) 応答コードが 250 以外の場合、セッション終了
4) クライアントへ送信：554 Infected by [検出名称] ([製品名])

② 検出時の動作が送信者へ通知の場合

1) サーバへ送信：RSET
2) 応答コードが 250 以外の場合
   a) クライアントへ送信：554 :SENDBACK:smtp error[RSET]: (Server Reply: [サーバ応答内容]) ([製品名])
3) サーバへ送信：MAIL FROM: [テンプレートの送信者アドレスまたは管理者アドレス]
4) 応答コードが 250 以外の場合
   a) クライアントへ送信：554 SENDBACK:smtp error[MAIL FROM] (Server Reply: [サーバ応答内容]) ([製品名])
5) サーバへ送信：RCPT TO: <メール送信者アドレス>
6) 応答コードが 250 以外の場合
   a) クライアントへ送信：554 SENDBACK:smtp error[RCPT TO]　(Server Reply: [サーバ応答内容]) ([製品名])

③ 検出時の動作が、[送信者へ通知] または [受信者へ通知] の場合

1) サーバへ送信：DATA
2) 応答コードが 354 以外の場合:
   a) コマンド処理終了
3) サーバへ送信：
   Received: from [クライアントホスト名] ([クライアント IP アドレス])
   by [ホスト名] ([製品名]) ;
   [現在時刻(RFC822 形式)]
4) スパム検出した場合：
   a) サーバへ送信：X-Spam-Status: Yes(製品名) with [検出名称]
5) ウイルス検出した場合：
   a) サーバへ送信：X-Virus-Status: infected(製品名) with [検出名称]
6) サーバへ送信：Data: [受信メールの Date フィールド内容]
7) 検出時の動作が送信者へ通知の場合
   a) サーバへ送信：To: [受信メールの送信元アドレス]
8) 検出時の動作が受信者へ通知の場合
   a) サーバへ送信：To: [受信メールの To アドレス]
   b) サーバへ送信：Cc: [受信メールの Cc アドレス]

9) 感染メール通知テンプレートに From フィールドがない場合
a) サーバへ送信：From: [管理者のメールアドレス]
10)サーバへ送信：Content-Transfer-Encoding: 7bit
11)感染通知メッセージの内容を送信
12)サーバへ送信："¥r¥n.¥r¥n"
13)クライアントへ送信：サーバ応答内容
14)応答コードが 250 以外の場合
a) セッション終了
④ 検出時の動作が [削除] の場合
1) サーバへ送信：RSET
2) 応答コードが 250 以外の場合
a) セッション終了
3) クライアントへ送信：250 Message accepted for delivery ([製品名])

7 6 以外の場合

① サーバへ送信：DATA
② 応答コードが 354 以外
1) クライアントへ送信：[サーバ応答内容]
2) コマンド処理終了
③ 匿名プロキシモードではない場合
1) サーバへ送信：
Received: from [クライアントホスト名] ([クライアント IP アドレス])
by [ホスト名] ([製品名]) ;
[現在時刻(RFC822 形式)]
2) スパム検出した場合
a) サーバへ送信：X-Spam-Status: Yes([製品名]) with [検出名称]
3) ウイルス駆除した場合
a) サーバへ送信：X-Virus-Status: disinfected([製品名]) from [検出名称]
4) ウイルス感染していた場合
a) サーバへ送信：X-Virus-Status: infected([製品名]) with [検出名称]
5) ウイルス、スパムを検出しない場合
a) サーバへ送信：X-Virus-Status: clean([製品名])
④ サーバへ送信：メール内容
⑤ クライアントへ送信：サーバ応答内容

8 アクセスログに記録

■RSET/XFORWARD/NOOP/EXPN コマンド受信時

1 サーバへ送信：[クライアント受信内容]

2 サーバ応答受信

3 クライアントへ送信：[サーバ応答内容]

■未知のコマンド受信時

1 クライアントへ送信：500 Unknown Command: "[受信コマンド]" ([製品名])

13.10 POP コマンド動作概要一覧

POP 接続時に、クライアントから送信されたコマンドに対する動作概要は以下のとおりです。

[製品名] はデフォルトで "F-Secure/fsigk_pop/バージョン/ホスト名" になります。
上級者向けオプションの "product_name=" で設定変更可能です。

■クライアント接続時

1 **"親サーバのユーザによる指定" が無効または透過型の場合**
- ① サーバへ接続
- ② 接続失敗時
  - 1) クライアントへ送信：-ERR Can't Connect to (サーバホスト:サーバポート) errmsg=[接続エラーメッセージ]
    - ➔ 接続エラーメッセージについては「13.12　接続エラーメッセージ一覧」を参照してください。
  - 2) セッション終了
- ③ サーバ応答受信
- ④ クライアントへ送信：[サーバ応答内容]

2 **それ以外の場合**
- ① クライアントへ送信：+OK [製品名] starting.

■各コマンド行受信時

1 **1 行が 998 バイト以上の場合**
- ① クライアントへ送信：-ERR Too long line

2 **サーバに接続しておらず、USER/QUIT 以外のコマンドが送信された場合**
- ① クライアントへ送信：-ERR please use USER command at first.

3 **1,2 以外の場合は各コマンドを処理する。**

■USER コマンド受信時

1 **"親サーバのユーザによる指定" が無効または透過型の場合**
- ① サーバへ送信：クライアント受信内容

2 **1 以外の場合**
- ① ユーザ認証が有効な場合
  - 1) ユーザが登録されていない場合
    - a) クライアントへ送信：-ERR Invalid Account Auth.
- ② ユーザ名に "@" または "#" が含まれる場合
  - 1) 最後の "@" または "#" 以降で指定されたサーバに接続
- ③ それ以外の場合
  - 1) 親サーバが空の場合
    - a) クライアントへ送信：-ERR USER format is USER username@hostname or username#hostname
    - b) コマンド処理終了
  - 2) 親サーバに接続

④ 接続に失敗した場合
1) クライアントへ送信：-ERR Can't Connect to (サーバホスト:サーバポート) errmsg=[接続エラーメッセージ]
➔ 接続エラーメッセージについては「13.12　接続エラーメッセージ一覧」を参照してください。
⑤ サーバへ送信：USER [ユーザ名]
⑥ サーバ応答受信
⑦ クライアントへ送信：[サーバ応答内容]

■QUIT コマンド受信時

1 サーバ接続済みの場合
① サーバへ送信：[クライアント要求内容]
② サーバ応答受信
③ クライアントへ送信：[サーバ応答内容]

2 1 以外の場合
① クライアントへ送信：+OK Quit

■PASS/APOP/AUTH コマンド受信時

1 APOP コマンドでユーザ制限が有効の場合
① ユーザが登録されていない場合
1) クライアントへ送信：-ERR Invalid Account Auth.

2 サーバへ送信：クライアント受信内容

3 サーバ応答受信

4 サーバ応答が成功の場合
① POP before SMTP データベースに接続元クライアント IP を登録

■RETR コマンド受信時

1 サーバへ送信：クライアント受信内容

2 メール受信

3 ウイルス検査・スパム検査

4 ウイルス・スパムを検出した場合
① ウイルスログへの記録
② 管理者への通知 (有効な場合)

5 ウイルスを検出し、駆除を行わず、検出時の動作が削除の場合
① クライアントへ送信：
Received from FSIGK：現在時刻(RFC822 形式)
X-Virus-Status：infected([製品名]) with [検出名称]
Date：[ヘッダの Date] (存在する場合)
To：[ヘッダの To] (存在する場合)
Cc：[ヘッダの Cc] (存在する場合)
[感染通知メッセージの内容]

6　5 以外の場合

① スパム・ウイルス検出時

1) クライアントへ送信：Received: from FSIGK: 現在時刻(RFC822 形式)

② スパム検出時

1) クライアントへ送信：X-Spam-Status: Yes(製品名) with [検出名称]

③ ウイルス駆除時

1) クライアントへ送信：X-Virus-Status: disinfected(%s) from [検出名称]

④ ウイルス検出時

1) クライアントへ送信：X-Virus-Status: infected(%s) with [検出名称]

⑤ クライアントへ送信：メール内容

■上記以外のコマンド受信時

1　サーバへ送信：[クライアント受信内容]

2　サーバ応答受信

3　クライアントへ送信：[サーバ応答内容]

13.11 FTP コマンド動作概要一覧

FTP 接続時に、クライアントから送信されたコマンドに対する動作概要は以下のとおりです。

[製品名] はデフォルトで "F-Secure/fsigk_ftp/バージョン/ホスト名" になります。
上級者向けオプションの "product_name=" で設定変更可能です。

■クライアント接続時

1 **"親サーバのユーザによる指定" が無効または透過型の場合**
- ① サーバへ接続
- ② 接続失敗時
  - 1) クライアントへ送信：500 Can't Connect to (サーバホスト：サーバポート) errmsg=[接続エラーメッセージ]
    - ➲ 接続エラーメッセージについては「13.12　接続エラーメッセージ一覧」を参照してください。
  - 2) セッション終了
- ③ サーバ応答受信
- ④ クライアントへ送信：[サーバ応答内容]

2 **1 以外の場合**
- ① クライアントへ送信：220 [製品名] at ホスト名 starting.

■各コマンド行受信時

1 **1 行が 998 バイト以上の場合**
- ① クライアントへ送信：500 Too long line

2 **サーバに接続しておらず、USER/QUIT 以外のコマンドが送信された場合**
- ① クライアントへ送信：530 please use USER command at first.

3 **1,2 以外の場合は各コマンドを処理する。**

■USER コマンド受信時:

1 **"親サーバのユーザによる指定" が無効または透過型の場合**
- ① サーバへ送信：クライアント受信内容

2 **1 以外の場合**
- ① ユーザ認証が有効な場合
  - 1) ユーザが登録されていない場合
    - a) クライアントへ送信：500 Invalid Account Auth.
- ② ユーザ名に "@" または "#" が含まれる場合
  - 1) 最後の "@" または "#" 以降で指定されたサーバに接続
- ③ それ以外の場合
  - 1) 親サーバが空の場合
    - a) クライアントへ送信：500 USER format is USER username@hostname or username#hostname
    - b) コマンド処理終了
  - 2) 親サーバに接続

④ 接続に失敗した場合
1) クライアントへ送信：500 Can't Connect to (サーバホスト：サーバポート) errmsg=[接続エラーメッセージ]
➔ 接続エラーメッセージについては「13.12　接続エラーメッセージ一覧」を参照してください。
⑤ サーバへ送信：USER [ユーザ名]
⑥ サーバ応答受信
⑦ クライアントへ送信：[サーバ応答内容]

■QUIT コマンド受信時

1 **サーバ接続済みの場合**
① サーバへ送信：[クライアント受信内容]
② サーバ応答受信
③ クライアントへ送信：[サーバ受信内容]

2 **それ以外の場合**
① クライアントへ送信：221 Quit

■PASV コマンド受信時

1 **サーバへ送信**：PASV

2 **サーバ応答受信**

3 **クライアントへ送信**：227 Entering Passive Mode (xx,xx,xx,xx,yy,yy)
(xx,yy はプロキシの IP アドレス、ポート番号)

■PORT コマンド受信時

1 **サーバへ送信**：PORT (xx,xx,xx,xx,yy,yy)
(xx,yy はプロキシの IP アドレス、ポート番号)

2 **サーバ応答受信**

3 **クライアントへ送信**：[サーバ応答内容]

■RETR/LIST/NLST/STOR/STOU/APPE コマンド受信時

1 **PASV/PORT コマンドを実行していない場合**
① クライアントへ送信：530 please use PORT/PASV command at first.
② コマンド処理終了

2 **PASV モードの場合**
① データセッション接続受付
② データセッションとコントロールセッションの接続元が違う場合
1) クライアントへ送信：530 Invalid Connection Source.
2) コマンド処理終了
③ データセッションでサーバに接続
④ サーバ応答受信
⑤ クライアントへ送信：サーバ応答内容
⑥ 応答コードが 1xx 以外の場合
1) コマンド処理終了

3 Active モードの場合
① サーバ応答受信
② 応答コードが 1xx 以外の場合
1) コマンド処理終了
③ データセッションでクライアントへ接続
④ クライアント接続失敗時
1) クライアントへ送信：530 Cannot connect client
2) セッション終了

4 ファイル受信

5 LIST/NLST コマンド以外の場合
①ウイルス検査

6 ウイルス検出時
① クライアントへ送信：530 Infected by [検出名]
② コマンド終了

7 ファイル転送

■上記以外のコマンド受信時

1 サーバへ送信：[クライアント受信内容]

2 サーバ応答受信

3 クライアントへ送信：[サーバ応答内容]

13.12 接続エラーメッセージ一覧

サーバへの接続に失敗した際に表示されるエラーメッセージの一覧です。

CONNECT(ホスト:ポート)/connect error: [接続エラー詳細]

サーバの IP アドレスへ接続要求を行ったが失敗した。

接続は Linux の connect() システムコールを通じて行います。"接続エラー詳細" には、connect() システムコールのエラーメッセージが含まれ、通常以下のいずれかになります。

Connection refused	：サーバが接続を拒否した。
Connection timed out	：接続タイムアウトが発生した。
Network is unreachable	：サーバのネットワークに接続できなかった。

CONNECT(ホスト:ポート)/connection timeout(>$1 sec)

接続が指定秒数 ($1) 以内に確立せず、タイムアウトした。

上級者向けオプションのサーバ接続タイムアウト設定 ("connect_timeout=yes , connect_timeout_sec=nnn") を有効にした場合のみ表示されます。

CONNECT(ホスト:ポート)/connect canceled

接続中にクライアントから切断してキャンセルした場合に表示されます。

CONNECT(ホスト:ポート)/hostname lookup error: [名前引きエラー詳細]

ホスト名の名前引きに失敗した。

名前引きは Linux(glibc) の gethostbyname() 関数を通じて行います。"名前引きエラー詳細" には、gethostbyname() 関数のエラーメッセージが含まれ、通常以下のいずれかになります。

Unknown host	：指定したホストが見つからなかった。
Host name lookup failure	：指定したホストの名前引きに失敗した。(DNS サーバから応答がない場合等。DNS サーバに問題がない場合、Internet Gatekeeper サーバから nslookup で名前引きができるか確認ください)
Unknown server error	：DNS サーバでのエラー
No address associated with name	：指定ホストの IP アドレスがなかった。

CONNECT(ホスト:ポート)/Access Inhibited by Proxy(FSIGK)

アクセス制御設定 (接続先) により、接続が拒否された。

13.13 サービスプロセス一覧

本製品ではサービス提供のために以下のプロセスが動作します。

`fsigk_admin`
F-Secure アンチウイルス Internet Gatekeeper(Linux 用)のウェブ管理画面用のウェブアプリケーションサーバですが、本製品（TLAS 版）では TLAS の管理画面に対応するため使用しません。

`fsigk_http`
HTTP サービス用のプロセス
クライアント、サーバとの HTTP 通信を行います。
セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に 1 プロセスが動作します。
必要に応じて、検査エンジンプロセス (fsavd) と通信を行います。通信は UNIX ドメインソケット(インストールディレクトリ fsavd-socket-0 ファイル)を通じて行います。
処理プロセス 1 個あたりの、共有できないメモリ消費量は 500KB 未満です。

`fsigk_smtp`
SMTP サービス用のプロセス
クライアント、サーバとの SMTP 通信を行います。
セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に 1 プロセスが動作します。
必要に応じて、検査エンジンプロセス (fsavd) と通信を行います。通信は UNIX ドメインソケット(インストールディレクトリ fsavd-socket-0 ファイル) を通じて行います。
処理プロセス 1 個あたりの、共有できないメモリ消費量は 500KB 未満です。

`fsigk_pop`
POP サービス用のプロセス
クライアント、サーバとの POP 通信を行います。
セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に 1 プロセスが動作します。
必要に応じて、検査エンジンプロセス (fsavd) と通信を行います。通信は UNIX ドメインソケット(インストールディレクトリ fsavd-socket-0 ファイル) を通じて行います。
処理プロセス 1 個あたりの、共有できないメモリ消費量は 500KB 未満です。

`fsigk_ftp`
FTP サービス用のプロセス
クライアント、サーバとの FTP 通信を行います。
セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に 1 プロセスが動作します。
必要に応じて、検査エンジンプロセス (fsavd) と通信を行います。通信は UNIX ドメインソケット(インストールディレクトリ fsavd-socket-0 ファイル) を通じて行います。
処理プロセス 1 個あたりの、共有できないメモリ消費量は 500KB 未満です。

fsavd

検査エンジンプロセス
ウイルスの検査を行います。プロセス数は適時増減します。各サービス (http, smtp, pop, ftp) ごとに最大で論理 CPU 数 (ただし最低 2 個、(例： 1CPU：2 個、2CPU：2 個、4CPU：4 個)) の検査処理プロセスを利用します。また、1 個の管理プロセスが動作します。
処理プロセス 1 個あたりの、共有できないメモリ消費量は通常 50MB 程度です。

fsasd

スパム検査プロセス
スパム検査を行います。最低 3 個のスレッドが動作します。
メモリ消費量は通常 40MB 程度です。

13.14 検出名称

本製品でウイルスを検出した場合、ウイルス名をログ等に出力します。各ウイルスの情報については以下のウェブページで情報提供しています。

http://www.f-secure.co.jp/v-descs/virusindex.html

また、一般的なウイルス以外でも、各種条件により検出する場合があります。この場合の検出名称は "FSIGK/" で始まり、以下のとおりです。

FSIGK/POLICY_FORMAT_MIME_BOUNDARY
不正な文字をメールヘッダの boundary 部分に含む
(不正な文字: ""、0x1f 以下のコード、0x7f 以上のコード)

FSIGK/POLICY_FORMAT_MIME_FILENAME
不正な文字をメールヘッダの filename 部分に含む
(不正な文字: 0x1f 以下のコード(0x1b を除く))

FSIGK/POLICY_BLOCK_ENCRYPTED
暗号化されたファイル(暗号化書庫ファイルを拒否する設定の場合)

FSIGK/POLICY_BLOCK_SCRIPT
スクリプトを含む HTML を検出 (スクリプトを拒否する設定の場合)

FSIGK/POLICY_BLOCK_ACTIVEX
ACTIVE-X を含む HTML を検出 (Active-X を拒否する設定の場合)

FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE
分割メール (分割メールを拒否する設定にした場合)

FSIGK/POLICY_BLOCK_MAXNESTED
最大圧縮階層を越えた
(上級者向けオプションで、最大圧縮階層を越えた場合に拒否する設定をした場合
(block_maxnested=yes))

FSIGK/POLICY_BLOCK_SCANTIMEOUT
最大検査時間以上の検査時間が経過した
(上級者向けオプションで、最大検査時間を越えた場合に拒否する設定をした場合
(block_scantimeout=yes))

FSIGK/POLICY_BLOCK_MESSAGESIZE
メールサイズが指定サイズより大きい場合
(上級者向けオプションでメールサイズ設定を行った場合、または 2GB を超えた場合
(block_messagesize_len=xxx))

FSIGK/POLICY_BLOCK_FILESIZE
ファイルサイズが指定サイズより大きい場合
(上級者向けオプションで指定サイズより大きい場合に拒否する設定を行った場合
(block_filesize=yes))

FSIGK/SPAM_LIST/CUSTOM/(条件番号)/(ヘッダフィールド名)
スパムをカスタム条件で検出した。
条件番号はデータベースファイル中で検出した行数です。

FSIGK/SPAM_LIST/UCE/([条件番号])/(ヘッダフィールド名))
スパムをデータベース(未承諾広告)で検出した
条件番号はデータベースファイル中で検出した行数です。

FSIGK/SPAM_LIST/ADVERTISEMENT/(条件番号)/ (ヘッダフィールド名)
スパムをデータベース(広告一般)で検出した
条件番号はデータベースファイル中で検出した行数です。

FSIGK/SPAM_LIST/HTMLMAIL/(条件番号)/ (ヘッダフィールド名)
スパムをデータベース(HTML 主体メール)で検出した
条件番号はデータベースファイル中で検出した行数です。

FSIGK/SPAM_LIST/VIRUSERROR /(条件番号)/ (ヘッダフィールド名)
スパムをデータベース(ウイルス・スパム通知メール)で検出した
条件番号はデータベースファイル中で検出した行数です。

FSIGK/SPAM_LIST/ERROR/(条件番号)/ (ヘッダフィールド名)
スパムをデータベース(エラーメール)で検出した
条件番号はデータベースファイル中で検出した行数です。

FSIGK/SPAM_RBL/(検出アドレス)[(RBL サーバ名)：(RBL 応答アドレス)]
スパムを RBL 検査で検出した
検出アドレス　　：RBL サーバに登録されていたアドレス
RBL サーバ名　　：検出した RBL サーバ名
RBL 応答アドレス　：検出時の RBL サーバからの応答アドレス

FSIGK/SPAM_SURBL/(検出ドメイン名)[(SURBL サーバ名)：(SURBL 応答アドレス)]
スパムを SURBL 検査で検出した
検出ドメイン名　　：SURBL サーバに登録されていたドメイン名
SURBL サーバ名　　：検出した SURBL サーバ名
SURBL 応答アドレス　：検出時の SURBL サーバからの応答アドレス

13.15 リスクウェア名称

リスクウェアはマルウェア(悪意のあるソフトウェア)ではありません。リスクウェアはコンピュータに害を与えるためのプログラムではありませんが、誤って用いることで、セキュリティ上の害を与えることが可能な機能を持っています。これらのプログラムは役に立が、悪用される可能性のある機能を持っています。
これらのプログラムの例は以下のようになります。
- リモート管理プログラム(例: VNC)
- インスタント・メッセンジャー(例: IRC)
- インターネットを通じてファイル転送を行うプログラム
- インターネット電話プログラム(VoIP)

プログラムがリスクウェアとして判定されても、意図して送受信している場合には害はありません。

リスクウェアの検出名称は、”Catagoriy.Platform.Family”という名前になります。

Category は以下のいずれかになります。
Adware
AVTool
Client-IRC
Client-SMTP
CrackTool
Dialer
Downloader
Effect
FalseAlarm
Joke
Monitor
NetTool
Porn-Dialer
Porn-Downloader
Porn-Tool
Proxy
PSWTool
RemoteAdmin
RiskTool
Server-FTP
Server-Proxy
Server-Telnet
Server-Web
Tool

Platform は以下のいずれかになります。
Apropos
BAT
Casino
ClearSearch
DOS

DrWeb
Dudu
ESafe
HTML
Java
JS
Linux
Lop
Macro
Maxifiles
NAI
NaviPromo
NewDotNet
Palm
Perl
PHP
Searcher
Solomon
Symantec
TrendMicro
UNIX
VBA
VBS
Win16
Win32
Wintol
ZenoSearch

14. 既知の問題

14.1 サブミッションポート

SMTPのウイルス検出は１つのポートのみの対応となっているため、複数のSMTPポートのウイルス検出には対応しておりません。「電子メール共有プロキシモード」の場合、サブミッションポートの通信をSMTPポートへリダイレクトすることで、サブミッションポートのウイルス検出を行うことができます。

14.2 Postfix でのプロキシポート 25 番の使用について

Postfix において、「プロキシモード」「透過プロキシモード」時にSMTPサーバを停止した場合、仕様によりローカル配送ができなくなります[17]。このため、これらのモードでもSMTPサーバは停止するべきではありません。しかし、プロキシモードでプロキシポートを２５番で使いたい場合は、SMTPサーバとの競合のため使用できません。

この解決方法として、SMTPサーバの待ち受けポートの変更が挙げられます。「プロキシ時SMTPポート」の設定は、「プロキシモード」「透過プロキシモード」下でのSMTPサーバの待ち受けポートを設定します。この設定を25番以外の空きポートを使用することで、SMTPサーバと２５番ポートを使用したプロキシを共存させることができます。

[17] Postfixの仕様によりローカル配送はできなくなります。

15. トラブルシューティング

15.1 電子メールサーバの配送が遅延する

アンチウイルス・ゲートウェイをインストールした電子メールサーバで、メール配送に遅延が発生する場合、次の要因が考えられます。

- HTTPプロキシによるウイルス検査を行っている場合
  HTTPプロキシのよるウイルス検査を使用した場合、CPUの負荷が高くなりSMTPサービスの動作に影響を与える場合があります。この場合、HTTPプロキシの同時接続数を制限するなど、CPUの過負荷を避ける設定を行ってください。

- 空きメモリが不足している場合
  メモリの増設をご検討ください。

- バージョンが最新でない場合
  最新のバージョンにアップデート後、動作を確認しください。

メモリ不足や CPU の過負荷は、サーバのアクティブモニタで検出可能です。admin のメールの転送先に、サーバ管理者の電子メールアドレスを設定することが推奨されます。

原因がわからない場合は、原因を切り分けるためにアンチウイルス・ゲートウェイを無効にした状態で正常に電子メールが配送できるかご確認いただけますようご検討ください。

16. 著作権

Copyright (c) 1993-2004 F Secure Corporation. All Rights Reserved.
Portions Copyright (c) 1991-2004 Kaspersky Labs, Ltd.

This product may be covered by one or more F Secure patents, including the
following: B2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233.

本製品は以下のソフトウェアが含まれています。各ソフトウェアのライセンス情報はパッケージの doc/以下に含んでいます。

詳細は Original Package の URL を参照してください。

tcp_wrappers(libwrap.a)
　　Original Package: ftp://ftp.porcupine.org/pub/security/index.html
pam_userdb
　　Original Package: http://www.kernel.org/pub/linux/libs/pam/
zip
　　Original Package: http://www.info-zip.org/pub/infozip/
BerkeleyDB 1.85
　　Original Package: http://www.sleepycat.com/download/
SHA-1 in C
　　Original Package: ftp://ftp.funet.fi/pub/crypt/hash/sha/sha1.c
Perl-Compatible Regular Expressions
　　Original Package: http://www.pcre.org/
libaes
　　Original Package: http://sourceforge.net/projects/libaes/
Digest::Perl::MD5
　　Original Package: http://search.cpan.org/~delta/Digest-Perl-MD5-1.8/lib/Digest/Perl/MD5.pm
Text::Iconv
　　Original Package: http://search.cpan.org/~mpiotr/Text-Iconv-1.4/Iconv.pm
jcode.pl
　　Original Package: ftp://ftp.iij.ad.jp/pub/IIJ/dist/utashiro/perl/
JRE (Java(TM) Platform, Standard Edition Runtime Environment)
　　Original Package: http://java.sun.com/javase/downloads/index.jsp
Apache Tomcat
　　Original Package: http://tomcat.apache.org/
Apache Myfaces(Myfaces Core / Myfaces Tomahawk)
　　Original Package: http://myfaces.apache.org/
GNU wget
　　Original Package: http://www.gnu.org/software/wget/

Location: “tool/wget” on installation directory
License: GPL

17. 問い合わせ先

本製品に関する情報、問い合わせは以下の場所までお願いいたします。

17.1 本製品の情報

本製品のアップグレードや評価版のダウンロードは、下記のサイトで提供されます。

http://www.mubit.co.jp/

17.2 ウイルス情報データベース

ウイルス情報データベース等を以下のページで提供しております。

http://www.f-secure.co.jp/

17.3 購入に関する問い合わせ

本製品の購入・ライセンス更新・ライセンス変更に関しては、販売代理店または株式会社ムービットまでお問合せください。

株式会社　ムービット
電話番号 03-5390-3553
FAX 番号 03-5390-3650
電子メール info@mubit.co.jp

17.4 電子メールによるサポート

本製品に関してマニュアルや WEB 情報で解決できない場合は、販売代理店または株式会社ムービットまでお問合せください。電子メールでのお問合せは、下記のメールアドレスまでお願いいたします。

info@mubit.co.jp

お問合せの際には、以下の送付をお願いいたします。

■お問い合わせの際に必要な情報

サポートに関するお問い合わせ時には、以下の情報をお知らせください。
本製品のバージョン番号、サーバの機種と OS の種類
発生した問題の詳細な内容
情報ファイル
　少なくとも、「システム情報」ファイル。
　－ 管理画面のヘルプメニューからダウンロードできる「システム情報」ファイル。
　－ "cd /opt/f-secure/fsigk; make diag" コマンドで作成される診断情報ファイル
　　/opt/f-secure/fsigk/diag.tar.gz