

GIDEON AntiSpam Plus

「ギデオン アンチウイルス アンチスパムPlus」 製品資料

「メールサーバに簡単導入のウイルス&スパム対策」

GIDEON
株式会社ギデオン

スパム対策の重要性

スパムメールとは

一方的に大量配信される不用なメール。商業宣伝・広告、テマやいたずらのチェーンメールなど種類もさまざま、発信元を偽り無差別に配信し、中には不正なメールサーバ利用もあります。その被害はウイルスの次に多く、スパイウェアや個人情報の流出、ワンクリック詐欺など今や社会問題とされています。

GIDEON

- 業務効率の悪化 → スпам選別の無駄な時間
- インフラへの負荷 → メールサーバ処理能力低下、ネットワーク負荷
- セキュリティへの脅威 → ウィルス、スパイウェア、フィッシング詐欺

しかし企業では、スパム対策にコストの高い機器や、設定が煩雑なソフトウェアの導入に対しては抵抗があります。さらに不正確なスパム判定で間違っ重要なメールをスパムと判断されては導入した意味がありません。

ギデオン アンチウイルス アンチスパムPlusとは？

稼働しているLinuxメールサーバに
アンチウイルス機能+アンチスパム機能
を追加するソフトウェア。



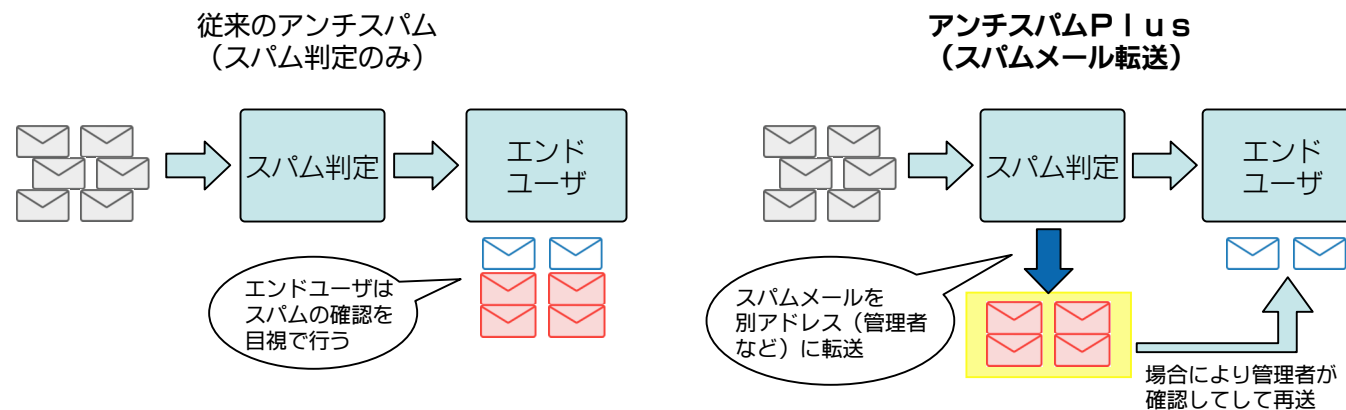
GIDEON

- ・MTAアドオンタイプで容易なインストール&セットアップ
- ・他のネットワーク機器を気にせず導入可能
- ・ウイルス対策とスパム対策を、一台のメールサーバで効率よく運用
- ・スパムメールの検知率、95%
- ・自動アップデート機能で日々の管理は必要なし
- ・誤検知率を低減させるスコアロジック機能
- ・メールサーバー内で動作するため、セキュリティポリシーは維持
- ・既存ネットワークの設定変更は不要

アンチスパムPlusの特徴は？

- ・これまでのアンチスパムソフトではおもにベイジアン理論（用語に依存した条件確率）が用いられていましたが、「アンチスパムPlus」ではこれに加えて、**スパムデータベース（メール発信元URL・発信元のIPアドレス等）とメールを照合**することで、検知率アップを実現しました。
- ・一般的なアンチスパムソフトは、スパム検出結果をクライアントに通知するものがほとんどです。これでは、メールを削除する作業は変わらないので、業務の効率化は図れません。当社アンチスパムPlusは、**スパムメール転送機能**により、クライアントには直接届きません。（管理者設定によりクライアントに届けることも可能です。）

GIDEON



基本機能・特徴

アンチスパム機能

- ・スパムメールの検知率95%
- ・メールヘッダ解析、メッセージ本文のフルテキスト解析、メールシグニチャデータベース、DNSルックアップ、URLデータベース解析、ユーザー定義などによる複合解析
- ・スパムDBの自動更新
- ・スパムメール転送機能
- ・スパム判定ロジックのカスタマイズ（自由度の高いポリシー設定）
- ・WEB管理インターフェース など

アンチウイルス機能

- ・カスペルスキー社アンチウイルスエンジン
- ・一時間ごとのウイルス定義ファイル自動更新
- ・検出エンジン、解析モジュールの自動アップデート
- ・ウイルス検知時のメール通知機能
- ・月次レポート、ログの管理機能
- ・WEB管理インターフェース など

既存ユーザさまへの乗り換え価格

契約期間途中で、アンチスパムPlusに移行

- ・ ギデオン アンチウイルス メールサーバ Ver.3をお使いのお客さま
「Ver.3」と「アンチスパムPlus」の新規価格の差額の1/2
- ・ アンチウイルス Ver.2をお使いのお客さま
「Ver.3」と「アンチスパムPlus」の新規価格の差額の1/2
※Ver.3へのバージョンアップ手数料 ¥20,000は無償です。

GIDEON

契約更新時に、アンチスパムPlusに移行

- ・ ギデオン アンチウイルス メールサーバ Ver.3をお使いのお客さま
「アンチスパムPlus」の更新価格を新たに適用
- ・ アンチウイルス Ver.2をお使いのお客さま
「アンチスパムPlus」の更新価格を新たに適用
※Ver.3へのバージョンアップ手数料 ¥20,000は無償です。

動作環境

- ・Linuxカーネル x86アーキテクチャ
- ・glibc 2.2以降
- ・sendmail 8.9.3以降
- ・qmail 1.03以降
- ・postfix 0.0.20000529以降

対応Linuxディストリビューション

- ・RedHat Linux 7.1/7.2/7.3/8/9
- ・RedHat EL AS/ES/WS 2.1/3/4
- ・Fedora Core 1/2/3/4
- ・Debian 2/3 (potato/woody/sarge)
- ・SuSE Linux
- ・Turbolinux 6.5/7/8/10 Server
- ・Turbolinux ApplianceServer 1.0/2.0
- ・その他 商用/フリーのディストリビューション

※SunCobalt後継機につきましてはお問い合わせください。

管理インターフェース（デフォルト画面）

GIDEON

GIDEON AntiVirus - Mozilla Firefox

アンチウイルス | アンチスパム

更新状況 | **検出状況** | 共通設定 | メール設定 | 他サービス

検出状況

検出情報

最終スパム検出
2006年05月30日
サービス: mta
判定方法: XS(3)
spammer@example.com

RBL一致ドメイン統計情報

本日	5	昨日	180	今月	185	先月	90
----	---	----	-----	----	-----	----	----

RBL一致ドメ
今月
1位 fortyk.ic
2位 deai-allf
3位 meguriai

検出ログ

新	検出日時	サー	判定方法	スコア
	2006-05-30 17:16:36	mta	XS	3
	2006-05-30 17:16:35	mta	XS	3
	2006-05-30 17:16:35	mta	R1	3
	2006-05-30 17:16:35	mta	KAS	3
	2006-05-30 17:16:35	mta	XS	3
	2006-05-30 17:16:35	mta	R1	3
	2006-05-30 17:16:33	mta	XS	3
	2006-05-30 17:16:33	mta	R1	3
	2006-05-30 17:16:32	mta	KAS	3

GIDEON AntiVirus - Mozilla Firefox

アンチウイルス | アンチスパム

更新状況 | 検出状況 | 共通設定 | **メール設定** | 他サービス

メール設定

スパムチェックの有効/無効 sendmail

保守・状況 | **基本設定** | 詳細設定1 | 詳細設定2 | ホワイトリスト | ブラックリスト | sendmail

基本設定

スパムと判定した場合のSubject

[SPAM] + \スコア + \判定名 +] + \元Subject

スパム判定基準

- 推奨設定を利用する
- カスタマイズを利用する

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

アクション	総合スコア	アクション	総合スコア
何もしない	0	POP3のみ本文変更	
Subject変更	3	SMTP/MTA受信拒否	99

追加ヘッダ行	総合スコア
X-Spam-Status: NONE	0
X-Spam-Status: SUSPICION	1
X-Spam-Status: SPAM	3

判定方法について
BL: 「ブラックリスト」で指定されたドメインのRBLチェック。高スコア推奨
XS: メール本文中に記載されたドメインのRBLチェック。高スコア推奨
R1: 接続元のIPアドレスのRBLチェック。高スコア推奨
S25: Receivedに記述された命名規則の形式チェック。低スコア推奨
RES: 逆引きチェック。低スコア推奨
KAS: DBを利用したスパム判定。中～高スコア推奨

アクション
スコア合計が、設定した総合スコア以上になったときに適用されます。
Subject変更: 「スパムと判定した場合のSubject」に変更
POP3のみ本文変更: 詳細設定1の「POP3のみ本文変更のとき置き換える本文」で設定したメール本文に置き換わる
SMTP/MTA受信拒否: メールが受信拒否される

追加ヘッダ
スコアの合計が、設定した総合スコア以上になったときにメールヘッダに追加します。