All for Mail Security

スパム・ウイルスメール対策・誤送信対策を1台で!

SPAMSNIPER

24時間 365日 あなたのメールを守ります

JSECURITY

SPAMSNIPER とは?

スパムメール、ウイルスメールをしっかりブロック!誤送信防止機能も搭載。

SPAMSNIPERは、スパムメールのブロックやウィルスからの保護、送受信メールのフィルタリングをリアルタイムで行います。また、添付ファイルの暗号化、遅延送信、承認後送信などの誤送信防止機能によって情報漏洩対策を実現する、統合メールセキュリティソリューションです。

SPAMSNIPER AGは、SPAMSNIPERの機能をベースとして、企業・団体でのより安全なメール環境を実現するべくメールフィルタリング機能を強化・拡張したメール無害化ソリューションです。インターネット経由で送られる添付メール・HTMLメールの遮断や、添付ファイルの削除、さらにHTMLメールをテキスト化する機能によって、安心して受信できるように電子メールを無害化します。

SPAMSNIPER

メール無害化機能をプラス!
SPAMSNIPER AG

主な機能

SPAMSNIPER
SPAMSNIPER AG

スパム・ウイルスメール遮断

インターネット経由のメールに潜むウイルスを駆除します。
大量に送られるスパムメールの遮断を行います。

メール誤送信防止

添付ファイル暗号化、送信遅延(再確認要請)添付ファイルリンク変換、上司承認などのメール誤送信防止機能を組み合わせ、きめ細かな情報漏えい対策が可能です。

受信メール保管

受信メールの保管が可能です。さらにSPAMSNIPER AGでは無害化されていない原本メールを指定のサーバに転送することができます。

SPAMSNIPER AG

添付メール・HTMLメール遮断

HTML

インターネット経由の添付ファイル付きメールやHTMLメールを強制的に遮断することで、未知のウイルスの侵入経路をふさぎます。メールを遮断したときは送信者、受信者にお知らせします。

添付ファイル削除

インターネット経由の添付ファイル付きメールから強制的に添付ファイルを削除することで、未知のウイルスの侵入経路をふさぎます。添付ファイルを削除したときは送信者、受信者にお知らせします。

HTMLメールのテキスト化

HTML
TXT

インターネット経由のHTMLメールを強制的にテキスト化することで、
悪意のあるマクロ実行やフィッシングのリスクがあるURLから防御します。

NEW

ファイル無害化

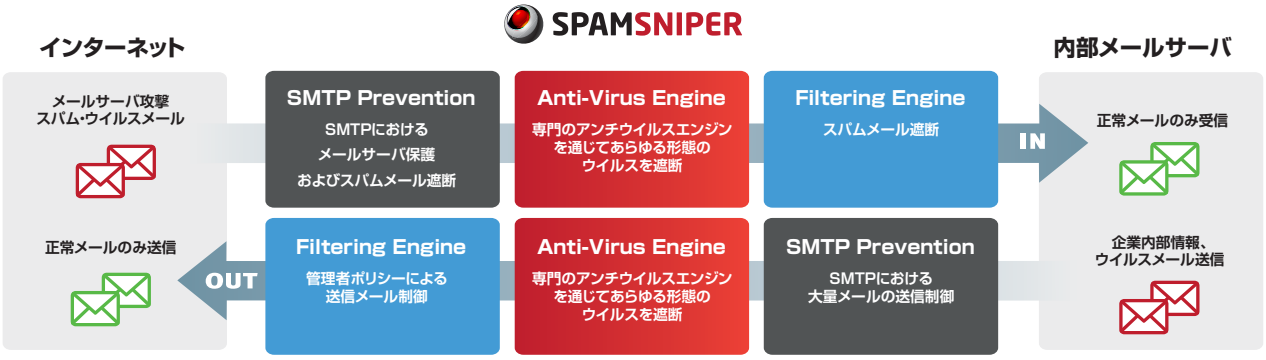
マクロ

Microsoft Office製品(Word、Excel、PowerPoint)に含まれるマクロの除去と、PDFに含まれるJavaScriptの除去を行い安全なファイルとして受信します。

特長

1 チューニングしなくても検知率96%以上を達成するエンジンを搭載

強力な「SMTP Prevention」、「Anti-Virus」、「Filtering Engine」と24時間･365日更新を行うスパムパターンアップデートにより、高い検知率･低い誤検知率を実現します。
チューニング作業をほとんど必要としない設計により、管理者の手間を省きます。
【チューニングしなくても96%以上の検知率。ほぼ0%の誤検知率を達成-当社調査】



SMTP Prevention Engine

不正リレー遮断･RBL（リアルタイムブラックリスト）

- 許可されていないメールのリレー遮断機能
- RBLに基づいたスパムメール遮断
- Mail Bomb、スパムメール自動遮断機能

SMTPセッション制御（メールサーバ防御、ハッキング防止）

- サーバ接続制限、データ入力制限、キュースケジューリング

Anti-Virus Engine

数多くの認証取得により信頼と実績を誇る、CYREN AntiVirus Engineを採用

- VPS（Virus Pre-Process System）Filtering
- 3rd Party AntiVirus Filtering:ウイルス検査

Filtering Engine

- タイトル、本文、ヘッダ、イメージ、添付ファイル、URL
- RFC※1 規約遵守検査
- RPD※2（CYREN社と提携）
- SPF、DKIMのドメイン対応

※1 RFC（Request For Comments）:インターネットで利用されるプロトコル、および技術仕様･要件
※2 RPD（Recurrent Pattern Detection）: 大量メールのパターン分析を行い、分類したメールの特性によりスパムを判断

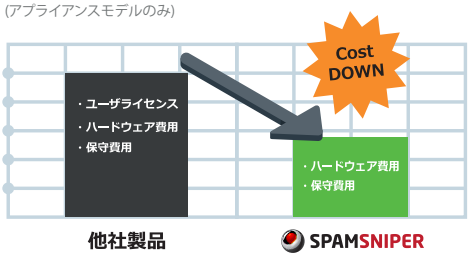
2 マルチドメインに対応。抜群のコストパフォーマンス

1台につき、最大1000個までのドメイン管理が可能です。
システム全体･ドメイン･グループ･個人別にフィルタリングを設定することができます。
フィルタリングされたメールに対しては下記のような様々なアクションを指定することができます。
【削除･隔離･一定期間保管･送信者への警告メッセージなど】

アプライアンスモデルはユーザ数に制限がありません。
ユーザライセンス不要ですので、大幅にコストダウンが可能です。メール流量に合わせて機種選定してください。

ユーザ数制限なし！抜群のコストパフォーマンス

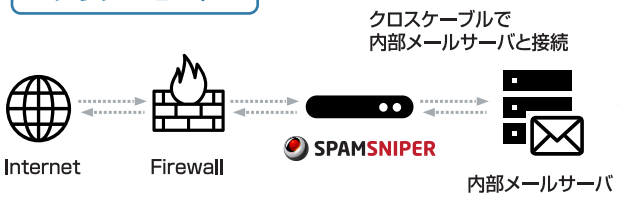
（アプライアンスモデルのみ）



3 ブリッジモード、プロキシモード 2つの設置形態に対応

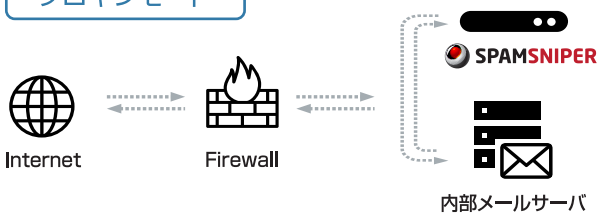
SPAMSNIPERはブリッジモード、プロキシモードのいずれの設置形態にも対応しています。
DNSサーバのMXレコードや周辺サーバの設定変更を行わず、透過的に導入される場合は
ブリッジモードを選択。また、既存機器からのリプレースや耐障害性を重視されるのであれば
プロキシーモードを選択、というように、お客様のご要望や環境に合わせて柔軟に設置する
ことが可能です。

ブリッジモード



- DNSサーバ、メールルーティング等の設定変更が不要
- 導入、検証がかんたん
- バイパスカードの採用により障害発生時もメールサービスは運用可能

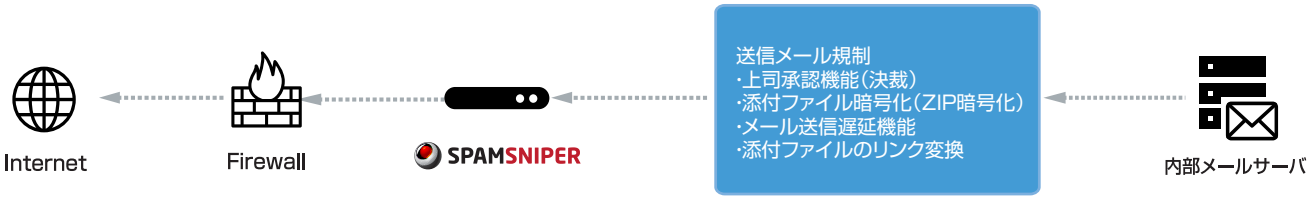
プロキシモード



- 既存メールサーバのリプレース時に最適
- 新規導入の場合、DNSサーバ、メールルーティングの設定変更が必要
- 障害発生時にDNSサーバ、メールルーティングの設定変更が必要

4 送信メール制御機能

「添付ファイル暗号化」、「送信遅延(再確認要請)」、「添付ファイルリンク変換」、「上司承認」などの
送信メール制御機能を組み合わせ、お客様の要望に合ったセキュリティポリシーを実現できます。
複数の条件を柔軟に適用することで、きめ細かな内部情報漏洩対策が可能です。



- 上司承認機能(決裁): 情報漏洩防止対策

  設定された“キーワード”が送信メールに含まれる場合、上長や管理者を経由してからメールを送信します。

- メール送信遅延機能: 時間差配信による誤送信防止

  設定された“キーワード”が送信メールに含まれる場合、上長や管理者を経由してからメールを送信します。

- 添付ファイル暗号化(ZIP暗号化): 添付ファイル送信時の情報流出防止

  送信メールに添付ファイルがある場合、パスワード付きのZIPファイルに自動変換して送信します。

- 添付ファイルのリンク変換: 添付ファイルの最小化/誤送信防止機能

  送信メールの添付ファイルを自動的にHTMLリンクに変換して送信することにより、メールサイズを最小化します。さらに、
  誤って送信したファイルに対する取り消しが可能です。

5 使いやすいインターフェース

マニュアルをほとんど必要としない管理画面により簡単に設定変更を行うことができます。
日常の迷惑メールはドメイン管理者、グループ管理者、各ユーザ毎に管理することができますので、
管理者の負担を軽減することが可能です。

統計管理

- 全体統計：Inbound/Outbound別状況、正常/スパム/ウイルス状況、日/週/月別状況
- 遮断統計：遮断フィルタ、ウイルス、拒否、IP状況
- ユーザ統計：送信者、受信者、ドメイン、グループ別遮断状況

メール管理

- 送受信メールをリアルタイム検索
- 件名、送受信者、IP、フィルタなどの多彩な条件検索
- 正常/スパム/ウイルス/拒否メールをリアルタイム監視
- 送信メールに対する規制管理

マルチドメイン設定管理

- ドメイン別、詳細設定：メール設定、フィルタリング設定、ロギングポリシー、認証ポリシーなど

フィルタ管理

- すべての権限フィルタ管理：全体/ドメイン/グループ/個人フィルタのすべてが管理可能
- 送受信メールのフィルタを個別制御
- 遮断フィルタ、許可フィルタを個別管理

ユーザ管理

- ユーザ追加/削除、グループ/ドメイン追加/削除
- 個人/グループ/ドメイン別ポリシー設定が可能

詳細バックアップ

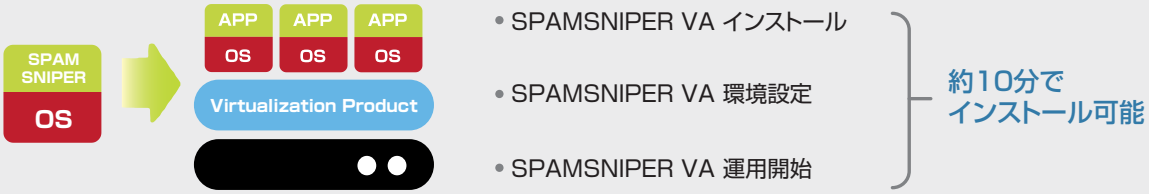
- 自動バックアップ:毎日のconfigファイル、DB、送受信メール
- 保存:FTPサーバ、ストレージへの自動送信により長期保存
- アラート:バックアップ結果を管理者に通知

SPAMSNIPER Virtual Appliance

SPAMSNIPER Virtual Appliance (以下SPAMSNIPER VAと省略)は、仮想化インフラに最適なメールセキュリティ環境を提供します。

スパムメール、フィッシング、ウイルス、スパイウェアなどの脅威からメールサーバを保護するとともに、企業内の情報漏洩を防止します。
SPAMSNIPER VAは、強力なフィルタリングエンジン、デュアルアンチウイルスエンジン、フィッシングメール遮断エンジン、DLP(※)エンジンなど、これらすべてを含めた統合ソリューションであり、仮想化インフラにおける高い性能と安定性を実現した仮想アプライアンス製品です。

※ DLP : Data Loss Prevention

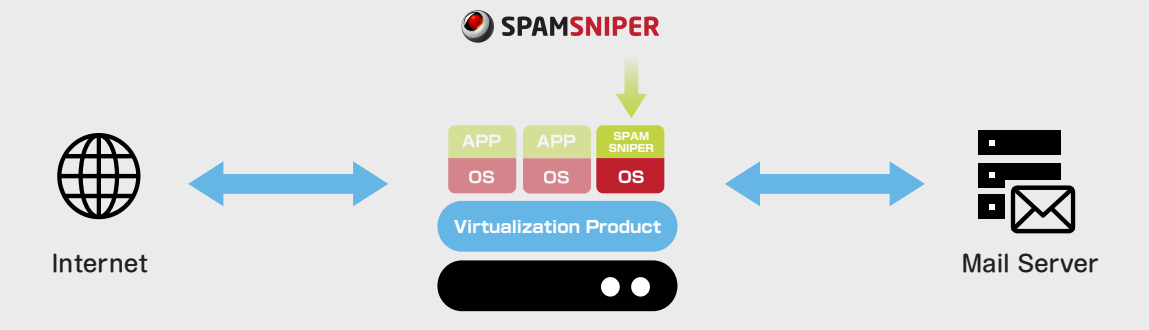


仮想化の特長

- ハードウェアや、OSのインストールが不要な仮想化システムにおいて簡単かつ短時間のインストールが可能
- SPAMSNIPER VAの追加インストールが容易
- 別の仮想化インフラへの移行が便利
- 他の仮想化アプリケーションとの統合運用により、管理費用、電力、スペースの節約が可能になり、TCOを低減できる
- 多重化インストールが容易

SPAMSNIPER VAの主な機能

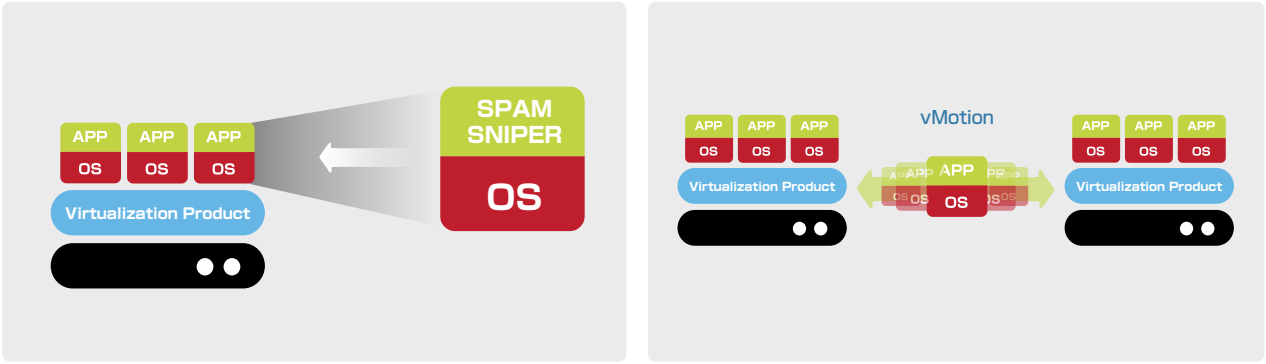
- スパム/ウイルス/フィッシングなど、悪意のあるメールを遮断
- 送受信メールの制御とモニタリング
- 誤送信防止
  - ✔ 添付ファイル暗号化(ZIP暗号化)
  - ✔ 上司承認
  - ✔ メール送信遅延
  - ✔ 添付ファイルのリンク変換
- 簡単に運用できるWEBベースの管理ツール
- リアルタイムアップデート
- 多言語GUI&レポート
- ドメイン/ユーザ別運用モード
- データ/バックアップ/復元に完全対応



仮想アプライアンス

一般的な導入方法

仮想化インフラ上にSPAMSNIPER VAをインストール

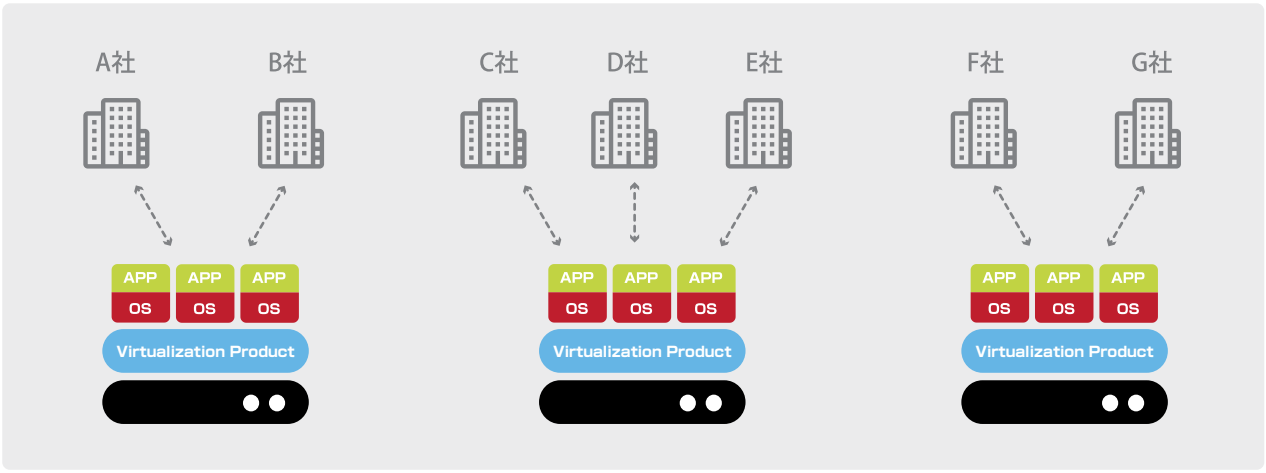


HA導入方法

VMwareのvMotionを利用してHA構成を実現

データセンターサービスにおける導入

データセンターのメールセキュリティサービスとして、効果的な運用が可能



システム動作環境

仮想化インフラ

VMware
VMware ESX / ESXi6
VMware ESX / ESXi5
VMware Server
VMware Workstation

Citrix
XenServer 5.5以上

ハードウェア推奨要件

項目	デフォルト	最小	推奨
CPUs	4	1	1- 50ユーザ : 1 CPU 50 - 2000 ユーザ : 2 CPU 2001ユーザ以上 : 4CPU以上
メモリ	2GB	1GB	1- 500ユーザ : 2GB 501- 2000ユーザ : 4GB 2001ユーザ : 8GB以上
ディスク領域	160GB	160GB	160GBを超えて保存する場合は、 LVMを利用して拡張できます。
NIC	1	1	1個の仮想NICを使用します。

＊（注）上記ハードウェアスペックは、Virtual Machineのリソースとなります。

ハードウェア

	SPAMSNIPER SPAMSNIPER AG	SA1000 AG SA1000	2000B AG 2000	5000B AG 5000	10000A AG10000	備考
外観						
CPU		Intel Atom 1.8GHz	Intel Core i3 3.3GHz	Intel Core i5 3.1GHz	Xeon Quad Core 2.0GHz x 2CPU	
メモリ		2GB	8GB	8GB	8GB	
HDD		1TB	2TB	2TB	146GB x 4（RAID5）	※容量はご希望に応じて変更可能です。
ネットワーク		10/100/1000 6Port	10/100/1000 6Port	10/100/1000 6Port	10/100/1000 4Port	
サイズ		1U Rack Size	1U Rack Size	1U Rack Size	2U Rack Size	
		438W x 225D x 44H mm	443W/292.1D/44H mm	443W/292.1D/44H mm	443W/680D/86H mm	
重量		4Kg	5Kg	5Kg	26Kg	
電圧		AC 90-240V	AC 90-240V	AC 90-240V	AC 90-240V	
消費電力		最大：60(W)	最大：200(W)	最大：200(W)	最大：750(W)	
動作環境		0-45℃/10-90% RH	0-40℃/5-95% RH	0-40℃/5-95% RH	0-35℃/5-95% RH	
		Non-condensing	Non-condensing	Non-condensing	Non-condensing	
認証		CE, KCC,VCCI, RoHS	CE, FCC,UL,VCCI, RoHS	CE, FCC,UL,VCCI, RoH	FCC, ICES, CE, VCCI,BSMI, CCC, MIC	

※仕様は予告なく変更する可能性があります。

ソフトウェア

						備考
Anti-Spam	DOS防御(Server)	○	○	○	○	
	DOS防御(self)	○	○	○	○	
	RBL, SPF	○	○	○	○	
	フィッシング遮断	○	○	○	○	
	添付ファイル（ファイル名）	○	○	○	○	
	A/Sエンジン	SSPE, CYREN RPD	SSPE, CYREN RPD	SSPE, CYREN RPD	SSPE, CYREN RPD	※SSPE：SpamSniper Spam Protection Engine
Anti-Virus	A/Vエンジン	CYREN AV Engine	CYREN AV Engine	CYREN AV Engine	CYREN AV Engine	
	Zero-Day Attack対応	○	○	○	○	
Outbound	内部情報漏洩防止機能 （DLP統制Data Loss Prevention）	○	○	○	○	メール送信時、 管理者の許可・統制・監視が可能 添付ファイルの自動暗号化 誤送信防止添付ファイルのリンク変換
	Relayサポート範囲	IP/Domain/SMTP AUTH	IP/Domain/SMTP AUTH	IP/Domain/SMTP AUTH	IP/Domain/SMTP AUTH	
	セキュア送信	SMTPSSL, STARTTLS	SMTPSSL, STARTTLS	SMTPSSL, STARTTLS	SMTPSSL, STARTTLS	
メール無害化		○	○	○	○	※SPAMSNIPER AGのみ
システム	マルチドメイン	○	○	○	○	1000ドメインまで
	マルチサーバ	○	○	○	○	
	多国語UI	○	○	○	○	日本語・英語
グループおよび	システム全体	○	○	○	○	
パターン管理	階層別遮断ポリシー	○	○	○	○	ドメイン別/グループ別/個人別 遮断ポリシーサポート
	方向別遮断ポリシー(In/Out)	○	○	○	○	
ネットワーク構成	ブリッジモード	○	○	○	○	
	プロキシモード	○	○	○	○	
運用モード	統計モード	○	○	○	○	
	遮断モード	○	○	○	○	
	タグ付けモード	○	○	○	○	
	イン/アウト同時統制	○	○	○	○	※1
運用環境	メールクライアント情報	変更なし	変更なし	変更なし	変更なし	
	メールサーバ情報	変更なし	変更なし	変更なし	変更なし	※2
サービス	ASPサービス構成	○	○	○	○	
管理ツール	管理ブラウザ	Microsoft Internet Explorer 8.x以降、Mozilla Firefox　24.x以降、Google Chrome　31.x以降				

※1 プロキシモード構成時：メールサーバの設定変更が必要

※2 プロキシモード構成時：Outbound統制を使用する場合、メールサーバの設定変更が必要

開発元

JSECURITY

株式会社 JSecurity

東京都港区東新橋二丁目12番1号 PMO東新橋7階

TEL:03-6826-1915　FAX: 03-6826-1916

E-mail : sales@jsecurity.co.jp

URL : https://www.jsecurity.co.jp

お求めは信頼の