

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



ウイルス・
スパム対策



メール無害化
サニタイズ



メール
誤送信防止

スパムメール、ウイルスメールをしっかりブロック！ メール無害化・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イルスからの保護、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。

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したメール無害化機能を備え、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。



主な機能



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、上長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。



添付メール・HTMLメール遮断

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

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。



ファイル無害化

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。

5つの特徴

1 チューニングせず検知率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、Varist 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 (Data443社と提携)
- ・SPF、DKIM、DMARC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

Sanitize Engine

- ・添付ファイルの脅威となるコンテンツの検出/無害化(Microsoft社Office系の検出/無害化)
- ・PDFファイルのスクリプト検査/無害化
- ・ZIP圧縮ファイル内の検出/無害化
- ・画像ファイルのコンテンツ検査/無害化

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、複数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



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

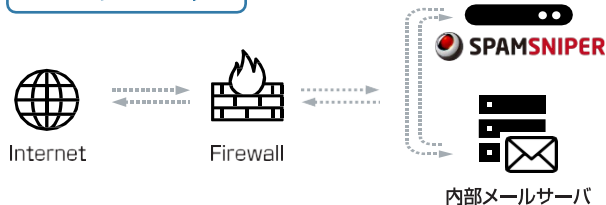
SPAMSNIPERはブリッジモード、プロキシモードのいずれの設置形態にも対応しています。DNSサーバのMXレコードや周辺サーバの設定変更を行わず、透過的に導入される場合は、ブリッジモードを選択。また、既存機器からのリプレースや耐障害性を重視されるのであればプロキシモードを選択、というようにお客様のご要望や環境に合わせて柔軟に設置することが可能です。

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」、「上長承認」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。



・上長承認機能(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。

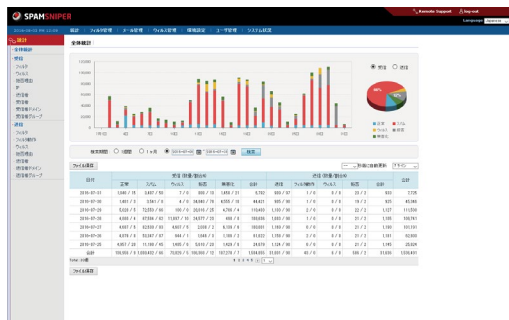
・添付ファイルのリンク変換: 添付ファイルの最小化/誤送信防止機能

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

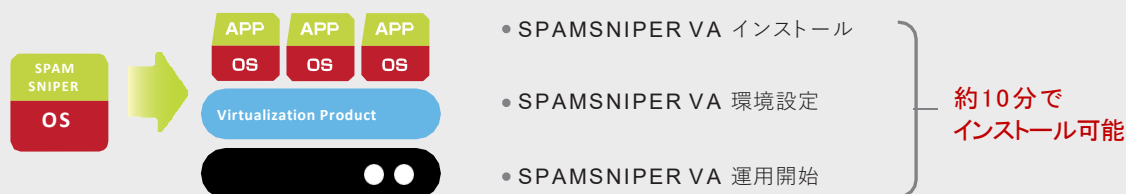
SPAMSNIPER Virtual Appliance

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、無害化エンジンなど、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

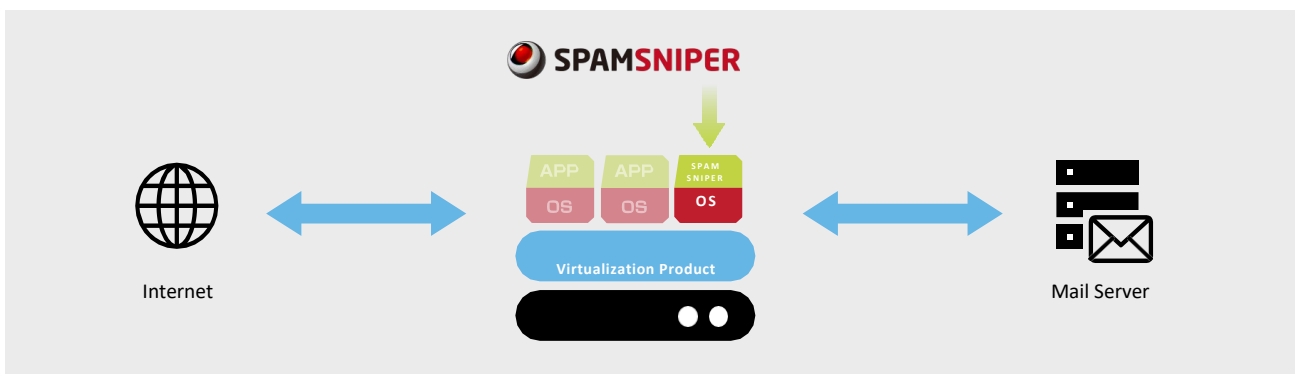


仮想化の特徴

- 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

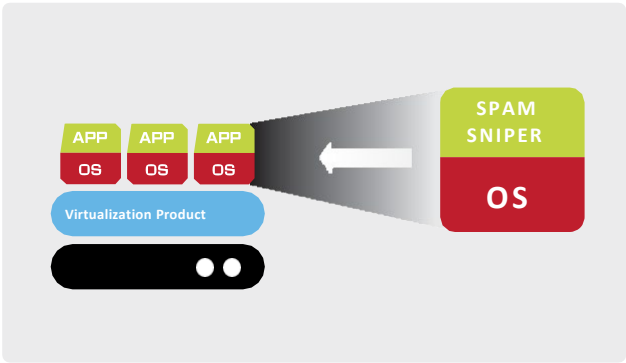
- スパム/ウイルス/フィッシングなど悪意のあるメールを遮断
- 送受信メールの制御とモニタリング
- 誤送信防止
 - ✓添付ファイル暗号化 (ZIP暗号化)
 - ✓上長承認
 - ✓メール送信遅延
 - ✓添付ファイルのリンク変換
- 簡単に運用できるWEBベースの管理ツール
- リアルタイムアップデート
- 多言語GUI&レポート
- ドメイン/ユーザ別運用モード
- データ/バックアップ/復元に完全対応



仮想アプライアンス

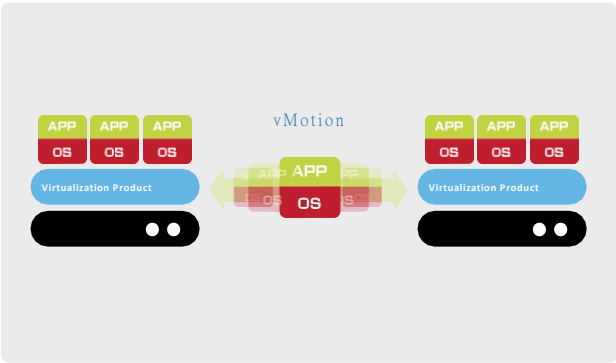
一般的な導入方法

仮想化インフラ上にSPAMSNIPER VAをインストール



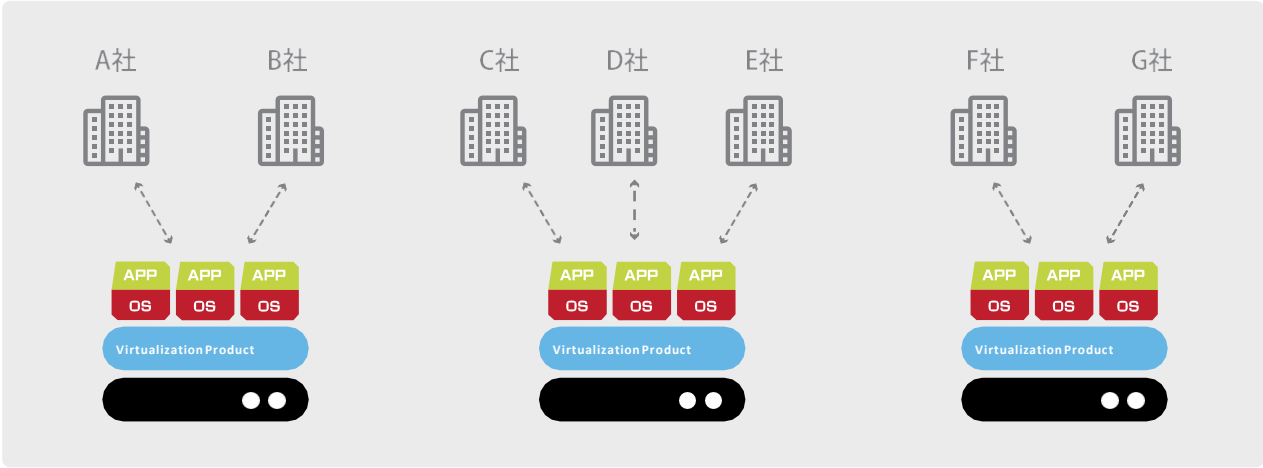
HA導入方法

VMwareのvMotionを利用してHA構成を実現



データセンターベースにおける導入

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
ESXi 6.5以降、7.x・8.x

ハードウェア推奨要件

項目	デフォルト	最小	推奨
CPU	4	1	1- 50 ユーザ：1 CPU 51 - 2000 ユーザ：2 CPU 2001 ユーザ以上：4 CPU 以上
メモリ	4 GB	2 GB	1- 500 ユーザ：2 GB 501- 2000 ユーザ：4 GB 2001 ユーザ：8 GB 以上
ディスク領域	160 GB 以上	160 GB	160 GB 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

	SA1000	SA3000	SA7000	
外観				
CPU	Intel Quad Core 2.0GHz	Intel i3 8100, 4Core 4Threads,3.6GHz,65w	i7 10700, 8Core 16Threads,2.9GHz,65w	
メモリ	8GB	16GB	32GB	
SSD	SSD 2TB	SSD 1TBx2(RAID1)	SSD 2TB x 2 (RAID1)	※SA7000のみHot-swap対応
ネットワーク	Bypass 1Pair	Bypass 1Pair	Bypass 1Pair	
サイズ	438W/225D/44H mm	430W/390D/45.2H mm	438W/422D/44H mm	
重量	4Kg	6.5Kg	12Kg	
電圧	AC 90-264V	AC 90-264V	AC 90-264V	
消費電力	60W Single Power	300W Single ATX Power	250W×2 Redundant ATX Power	(SA3000のみdualに変更可能:オプション)
動作環境	0-45°C/10-95%RH	0-60°C/5-95%RH	0-40°C/5-95%RH	
	Non-condensing	Non-condensing	Non-condensing	

※1: ハードディスクの容量は変更可能です。

※2: ハードウェアスペックは予告なく変更する場合があります。

ソフトウェア

Anti-Spam	DOS防御(Sever)	○	○	○	
	DOS防御(Self)	○	○	○	
	RBL,SPF、DKIM、DMARC	○	○	○	
	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, Data443 RPD	SSPE, Data443 RPD	SSPE, Data443 RPD	※SSPE:SpamSniper Spam Protection Engine
Anti-Virus	A/Vエンジン	Varist AV Engine	Varist AV Engine	Varist 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	
	セキュア送信	SMTPSSL,STARTTLS	SMTPSSL,STARTTLS	SMTPSSL,STARTTLS	
メール無害化		○	○	○	
システム	マルチドメイン	○	○	○	
	マルチサーバ	○	○	○	
	多国語UI	○	○	○	日本語・英語・韓国語
グループおよび パターン管理	システム全体	○	○	○	
	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	
	メールサーバ情報	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 Edge, 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



株式会社 JSecurity

東京都港区浜松町2-4-1 世界貿易センタービルディング 南館17階

TEL:03-4567-2823 FAX:03-4567-2824

E-mail: sales@jsecurity.co.jp

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