your unix solution
KLJTECH

メール全体のセキュリティーを考えます

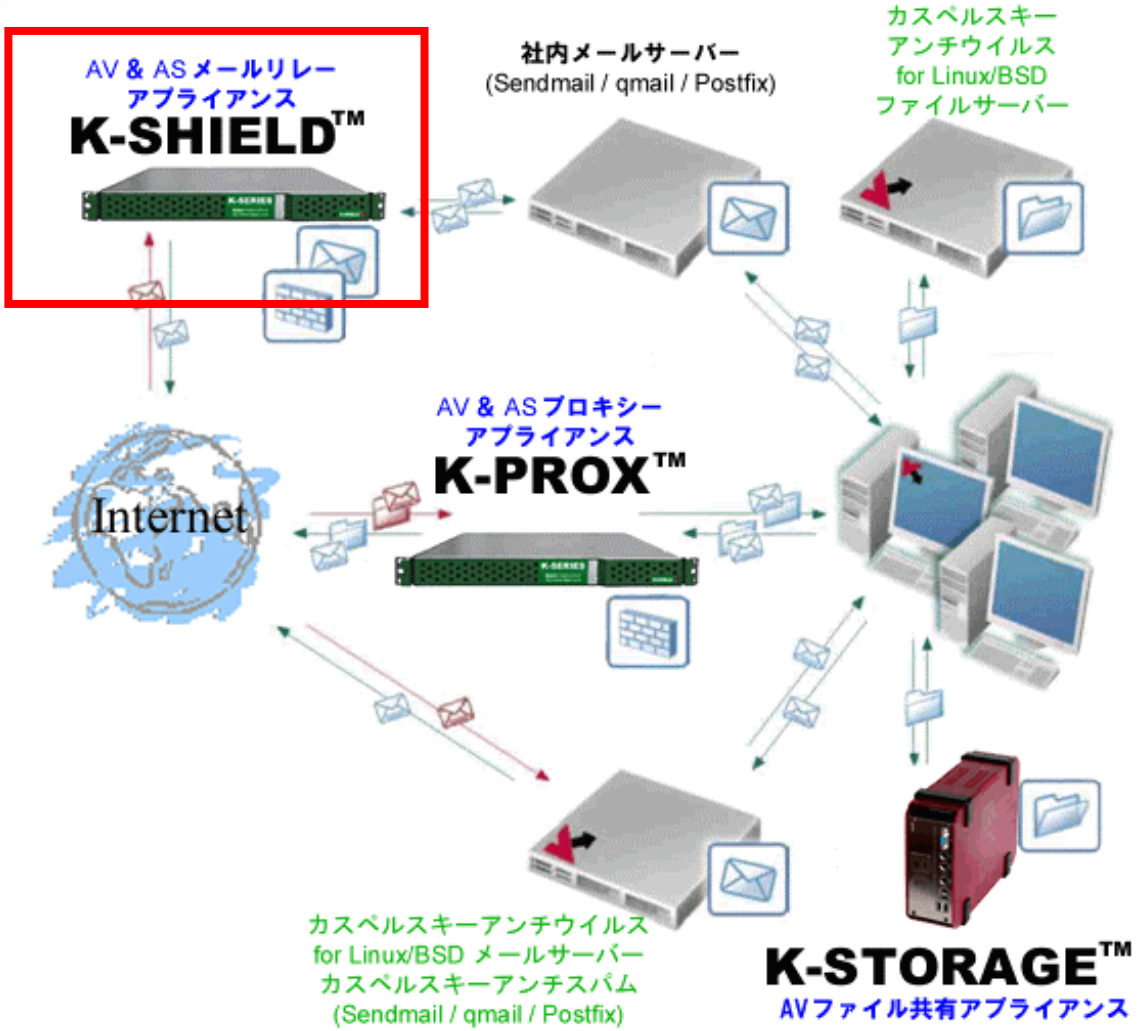
K-SHIELD™2.01

２０１１年２月

株式会社ケイエルジェイテック
http://www.kljtech.com/

your unix solution
KLJTECH

KLJTECH &メール・セキュリティ・サービス



K-SERIES™ 2.0

http://www.kljtech.com

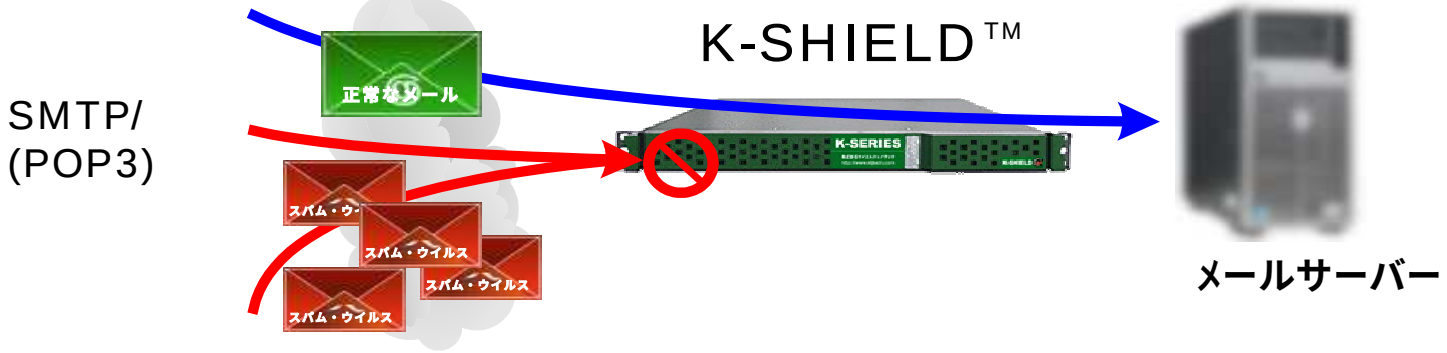
メールフィルター・アプライアンス

K-SHIELD™

日々増え続けるスパムメール、インターネット上で蔓延するウイルス。

スパムメールは業務効率を悪化させ、ウイルスやスパイウェアは情報漏洩を引き起こすなど社会問題にまで発展しています。メールを媒体として侵入するこれらの脅威に対し、インターネットとメールサーバの中間に文字通り「盾」の役割で防護壁としての機能を提供するアプライアンス――

それが「K-SHIELD」です。



K-SHIELDは、メールリレーの際にウイルス対策及び迷惑メール対策を行う、高性能、簡単導入、高パフォーマンスの三拍子そろったアプライアンスです。

メールリレーによるフィルタリングのため、ネットワークの構成をほとんど変えずに簡単かつ確実に企業やISPのメールを保護いたします。

ウイルス対策はカスペルスキーエンジンを採用しており、高いパフォーマンスと高い検知率も実現しております。迷惑メール対策は、カスペルスキーエンジンとベイジアンフィルタの併用構成で、日本語スパムの検知率も大幅に向上しています。

また、オプションでウイルス及び迷惑メール対策機能付POPプロキシも用意しています。

K-SERIES™ 2.0

http://www.kljtech.com

ウイルス対策更新頻度、新種対応、検知率の比較

更新頻度の集計

※2010年1月、公式リリースのみ

Kaspersky	573
Dr. Web	332
Sophos	83
Bitdefender	54
ClamAV	48
AntiVir	43
F-Secure	43
Panda	39
Hauri	38
Symantec (Intelligent Updates)	34
Trend Micro	30
eTrust (CA)	29
F-Prot	23
Fortinet	22
eTrust (VET)	19
Avast	17
AVG	17
Nod32	17
RAV	8
McAfee	7
eSafe	6
Symantec (LiveUpdates)	6

AV-Test.org Research Group, Magdeburg University, Mar 2009

新種パターン提供速度

※Dumaru.Y、MyDoom.A、Bagle.A、Bagle.Bでの平均値 （時：分）

Kaspersky	06:51
Bitdefender	08:21
F-Secure	09:08
F-Prot	09:16
RAV	09:16
AntiVir	09:24
AVG	12:00
Avast	12:17
Sophos	12:22
Dr. Web	12:31
Trend Micro	13:06
Panda	14:04
Esafe	17:16
McAfee	26:11
Symantec	27:10

AV-Test.org Research Group, Magdeburg University, Feb 2008

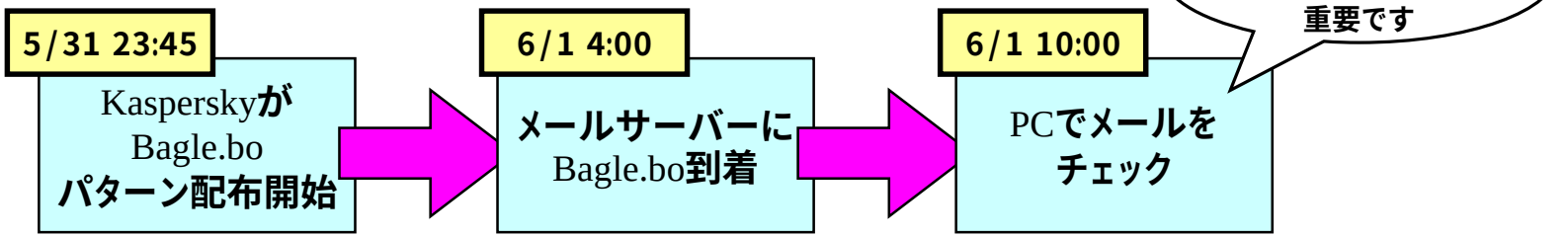
各社検知率比較

※ウイルス、ワーム、トロイ、スパイウェア等多種多様な悪性プログラムで集計

	Total	within DOS & Other OS	Spyware
Kaspersky	**99.9%**	**99.9%**	**99.9%**
Symantec	98.8%	99.4%	98.1%
NOD32	97.4%	98.3%	95.8%
BitDefender	96.6%	97.3%	96.0%
McAfee	95.8%	98.2%	92.4%
Antivir	93.0%	93.6%	96.4%
F-Prot	90.9%	95.9%	86.5%
Doctor Web	88.3%	92.4%	84.2%
Trend Micro	86.6%	91.3%	82.1%
Avast	84.4%	91.1%	78.8%
AVG	83.3%	87.4%	81.6%
Sophos	78.4%	89.1%	68.2%

www.av-comparatives.org, Aug 2009

実例: Bagle.bo(’05/6/1)



K-SERIES™ 2.0
http://www.kljtech.com

迷惑メール対策によるコスト軽減

昨今急増する迷惑メールは、企業ユーザーに「メールの選別」という無駄な作業を強いる結果となっております。今や、ウイルス対策以上に深刻な迷惑メール対策は、企業のコスト軽減として、非常に注目されている分野です。

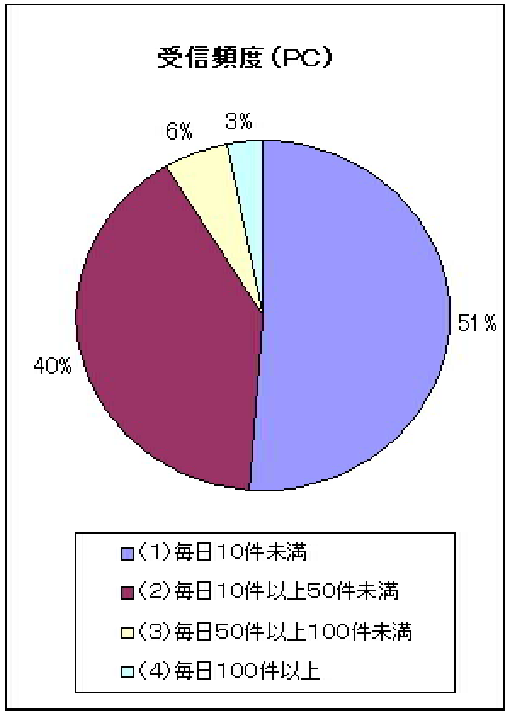
セキュリティベンダーとして世界的に有名なカスペルスキーラブス社は、ウイルス被害の深刻なロシア国内のアンチスパムベンダー各社と協力し、新しい迷惑メール対策製品「Kaspersky Anti-Spam」を開発しました。
ロシア最大にして世界有数のWebメール「mail.ru」で採用されたその性能は、日本国内の団体やISPにも採用され、注目されている製品です。

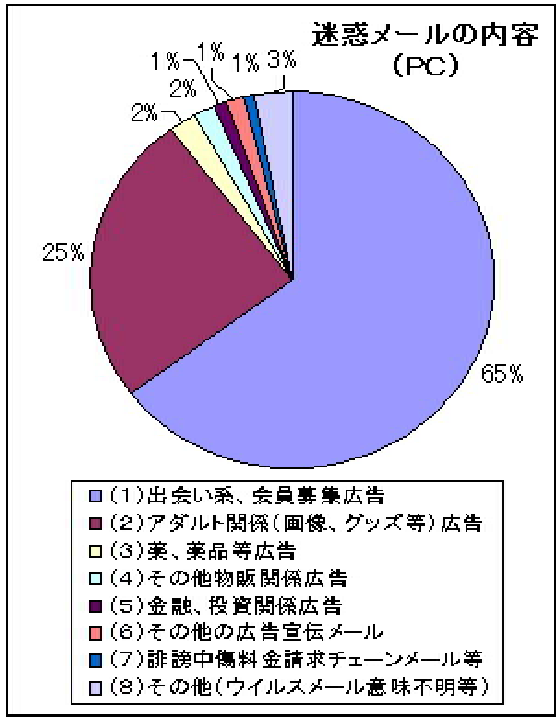
迷惑メール対策を日本国内マーケットに提供する為には、日本語スパムに強い技術、日本語の単語チェックが必要となります。日本語スパムメール対策の為に株式会社ケイエルジェイテックのオリジナルフィルター機能を用意しました。これにより、日本語のスパム検知率は格段に向上しました。

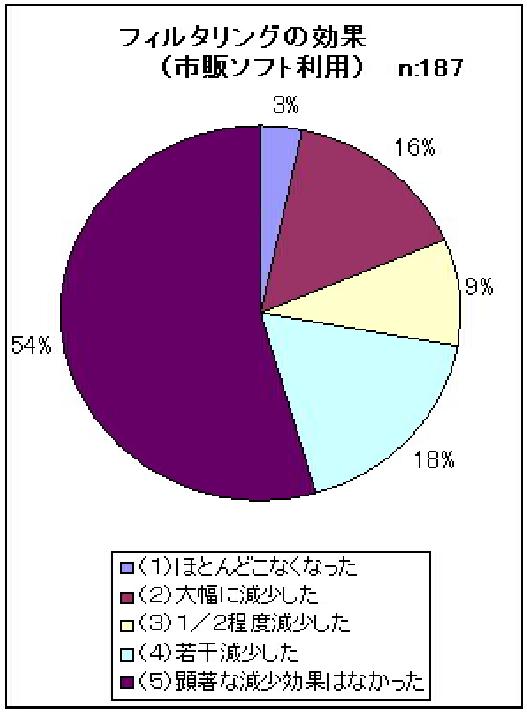
K-SHIELD2.0のフィルター機能の特長として、SMTPフィルター機能があります。従来のフィルタリング技術に加え、SMTPのトラフィックのコントロールを行い、無駄な迷惑メールトラフィックの削減に対応しました。

現状：迷惑メールの影響

- 約５０%のユーザが**毎日１０通以上**の迷惑メールを受信している
- 迷惑メールの９割が**出会い系・アダルト関係**の内容である
- 市販ソフトの利用では、半数以上のユーザが**効果がない**と証言している

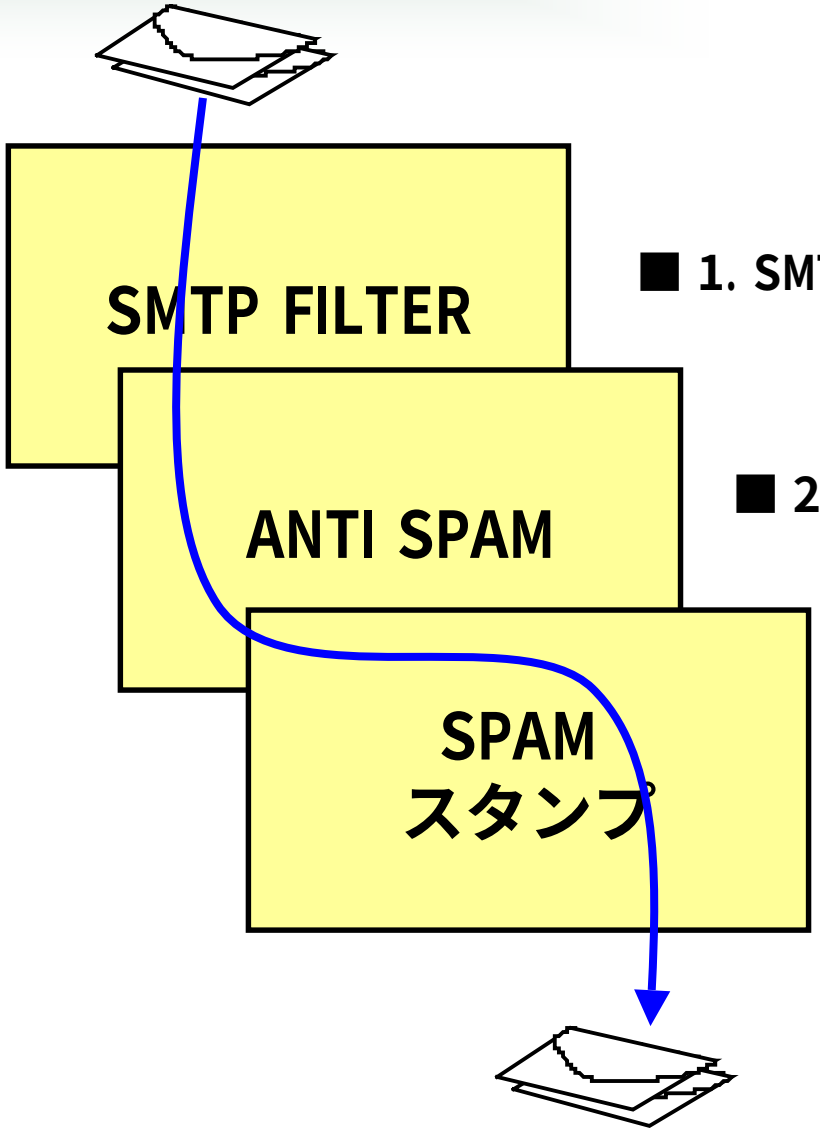






参考：迷惑メール相談センター

K-SHIELD™2.0 スパムフィルター機能のSTEP



■ 1. SMTPトラフック制限/Control機能

■ 2.メールスパムのコンテンツフィルター機能

■ 3. スパム・スタンプ機能

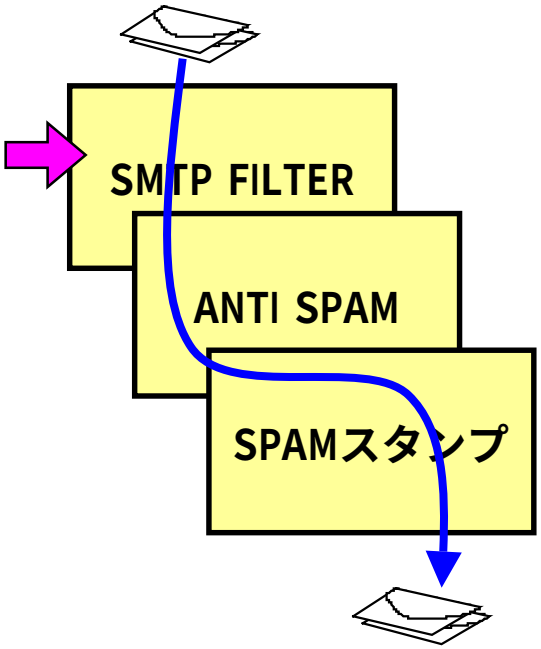
K-SERIES™ 2.0
http://www.kljtech.com

SMTPフィルター・トラフィック制限

K-SHIELD2.0ではプロキシでSMTPでのトラフィック制限又は
トラフィックコントロール(control)が出来ます。
K-SHIELDオリジナルMTA経由でSMTP REJECT機能は弊社システムで標準
対応となります。
メール流量制御技術は、現時点で下記の機能に対応しております。
・接続あたりのメール数（mail connection limit)
・IPあたりの接続数（smtp IP access limit)
・全体での接続数（mail send limit per SMTP connection)
・リレーIPアクセス制限
・SMTPディレイ（SMTP delay limit)

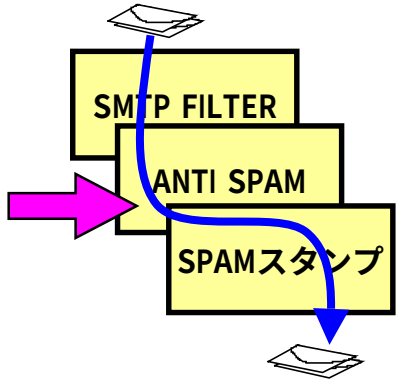
また、下記の機能についても現在開発中となります。
・一定時間単位で、同一IPからの接続が多い場合、制限をかける
Ex）30分あたり同一IPからメールが100通着たら、100通目以降
はREJECTする。
REJECTした場合、30分間葉そのIPからの通信を全てREJECTする

上記カスタマイズ分まで含めれば、流量制限としてかなりの効果
が得られるかと思われます。



K-SHIELD™2.0 スパム対策　スパムエンジンの説明

K-SHIELD™ は、Kasperskyアンチスパムと
KLJTECH独自のスパムＤＢを
複合したスパムエンジンを採用しております。



KASPERSKY ANTI·SPAM

＋

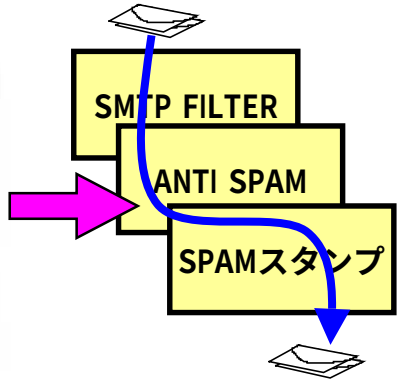
your unix solution
KLJTECH

- 大規模トラフィック向けの設計思想に基づく高速処理の実現
- 前後のMTAからの大規模トラフィックでも安定した動作
- 使用メモリの効率化を実現
- ログレポートシステムの改良
- KeepUp2Date™採用により、DB更新の安定化と複数サーバラウンドロビンに対応

K-SERIES™ 2.0
http://www.kljtech.com

K-SHIELDスパム・フィルター

スパム対策はどのようなフィルタリングを行っているか？



K-SERIES™ 2.0

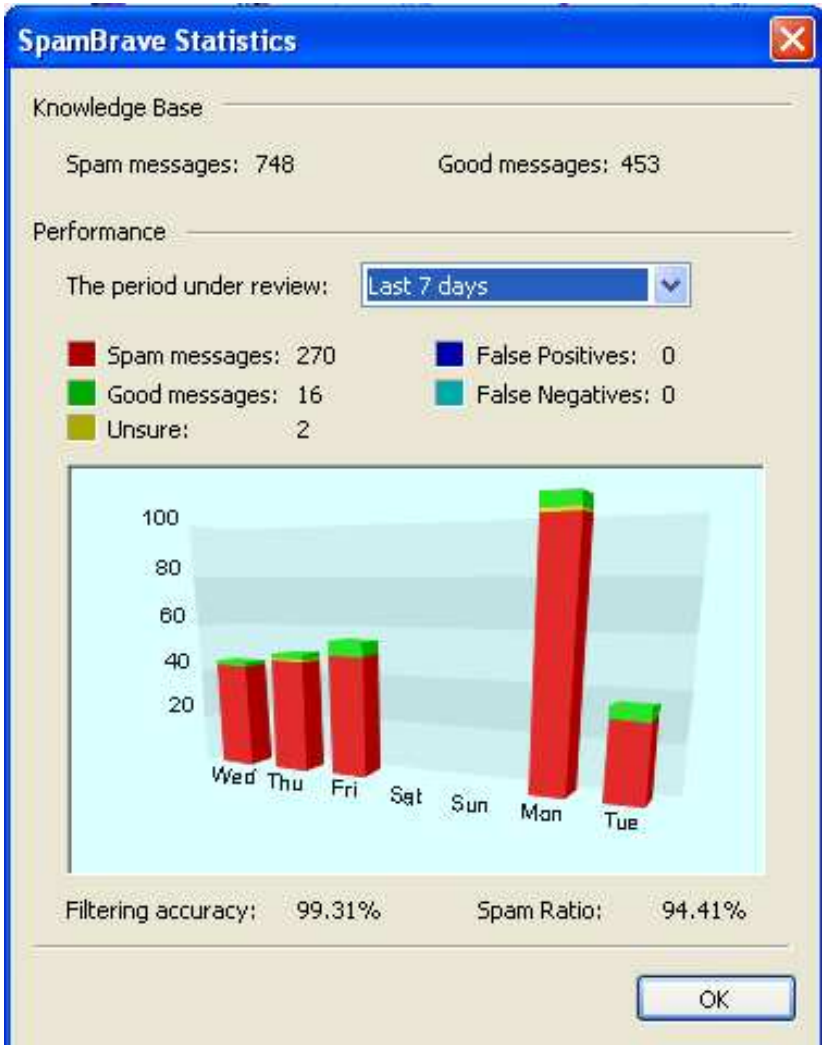
http://www.kljtech.com

K-SERIESのKLJTECHベイジアン技術とは？

BAYESIAN・フィルター

- ベイジアンという単語を最近良く聞くかと思いますが、ベイジアンフィルターの核となるベイズ理論とは、文章の要素からその分類である確率を求める、統計学の理論の一つです。
ベイズの定理は、そもそもベイジアンフィルターの利用を目的として作成されたものではなく、したがって、ベイズの定理をみせて「これがベイジアンだよ」と言うのは間違いです。
ベイズ理論とそうでない（古典）統計学は、サンプル数をNとすると 異なる結果は1/N程度となりそれほど大きな違いがあるものではありません。Nが数百くらいになると、その差は問題ではなくなります。現在のベイジアンフィルターの隆盛は、N=数百から数千の非線形なモデルを扱う事ができる程度にコンピュータの能力が上がってきた為です。
ベイズ理論は、スパムメールを分類する場合に計算を導きやすいという特徴があります。ベイジアンフィルターは、スパムメールの中の単語、URL、ヘッダ情報より「スパムメール」及び「正常メール」の可能性を導き出し、他の複雑なフィルタリング技術より単純かつ正確な値を導き出すことが可能となりました。
しかし、日本語の文章は単語の間に空白がないため、英語圏のロジックのままでは一文を一単語として認識してしまいます。日本語の単語分かちの技術と併用することで、初めて日本語スパムでもフィルタリングがまともに動作いたします。

- ケイエルジェイテックは、スパムフィルター技術について、Kaspersky AntiSpam 3.0と、完全日本語対応のベイジアンフィルター設定を用意しました。これにより、全世界全体のスパムフィルター技術と、日本ローカルなフィルター技術で、効率的なフィルタリングが行えます。

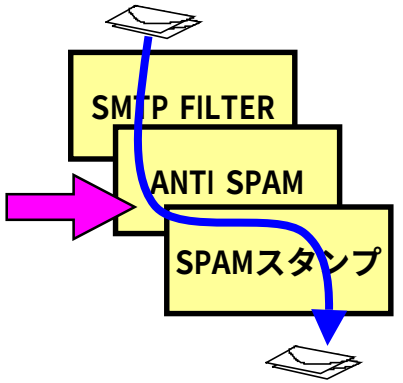


K-SERIES™ 2.0
http://www.kljtech.com

Kaspersky Anti-Spam

大規模トラフィックに耐える処理能力

- ISP等の大規模トラフィック向けの設計思想に基づく、高速処理の実現
- 前後のMTAからの大規模トラフィックでも安定した動作
- 使用メモリの効率化を実現
- ログレポートシステムの改良
- KeepUp2Date™採用により、DB更新の安定化と複数サーバラウンドロビンに対応



新しいスパムフィルタリング技術

- ウイルスやスパイウェアが自動生成するスパムに対応
- SPF及び DCCフィルタリングに対応
- 本文中のURLブラックリスト(SURBL) に対応
- OCR画像処理に対応した画像スパム対応技術の採用
- DNSベースのブラックリストであるDNSBLに対応
- 大量配信スパムに即時対応するUDS (Urgent defense System)技術
- 改良されたブラックリスト/ホワイトリストシステム（BL/WL）
- Base64及びMIMEのデコードに対応し、エンコードされた本文のフィルタリングも可能

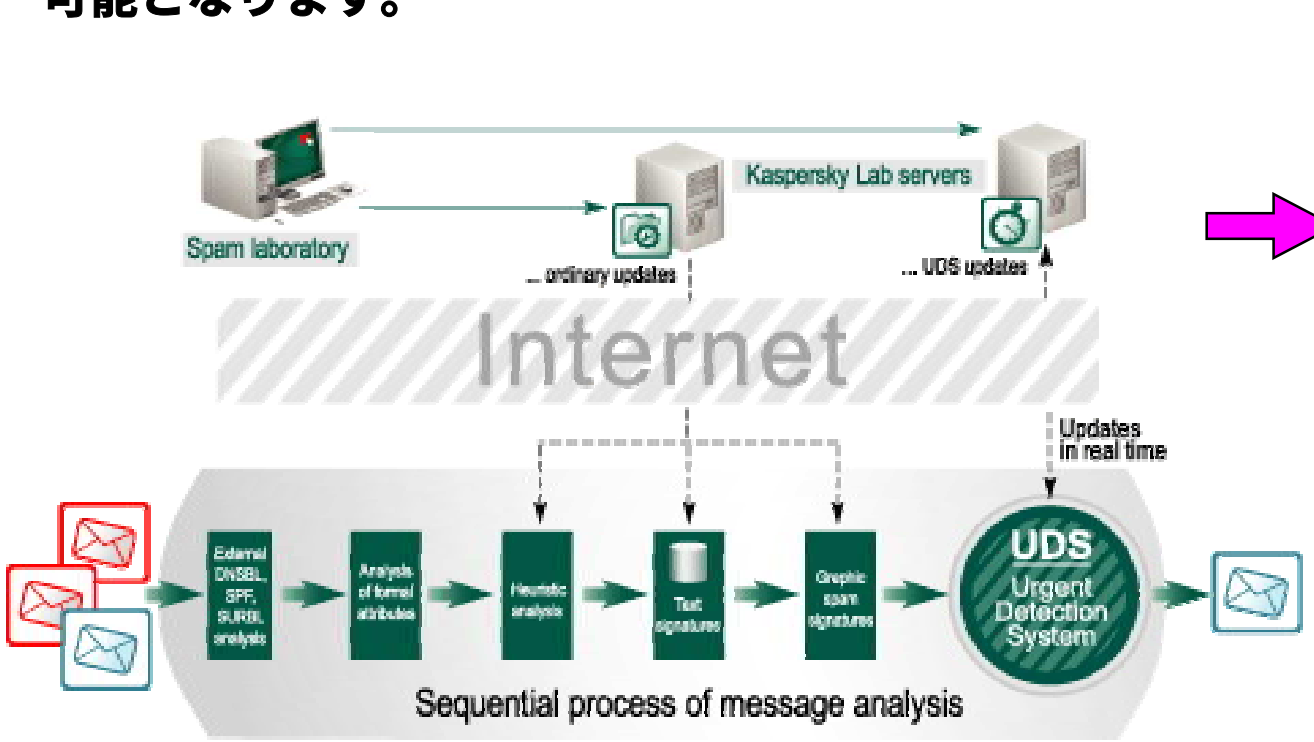
新GUIによる簡単な管理

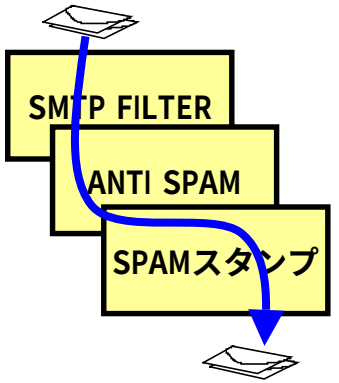
- スパムの統計レポートに対応し、グラフィカルな分析とCSV/HTMLレポート出力
- スパムエンジンの設定管理に対応
- 階層化されたポリシーとグループ管理で直感的なルール設定が可能に
- 日本語を含む複数のアジア圏文字コードに対応

K-SERIES™ 2.0
http://www.kljtech.com

Kaspersky スパムフィルターUDSとは？

カスペルスキーは都度センターに問い合わせるUrgentDetectionSystem サービスを採用。全世界で爆発的に発生したスパムに対し、迅速に対応可能となります。



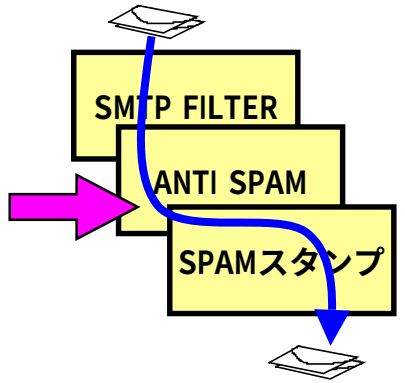


K-SHIELD™ のスパム対策検知率

all spam			
kas	hit	5081	
	pass	950	84.2%
bays	hit	5852	
	pass	179	97.0%
kas+bays	hit	5955	
	pass	76	98.7%
rbl	hit	664	
	pass	5367	11.0%
kas+rbl	hit	5160	
	pass	871	85.6%
bays+rbl	hit	5856	
	pass	175	97.1%
kas+bays+rbl	hit	5956	
	pass	75	98.8%
surbl	hit	3774	
	pass	2257	62.6%
kas+surbl	hit	5664	
	pass	367	93.9%
bays+surbl	hit	5985	
	pass	46	99.2%
kas+bays+surbl	hit	6009	
	pass	22	99.6%
rbl+surbl	hit	4118	
	pass	1913	68.3%
kas+rbl+surbl	hit	5710	
	pass	321	94.7%
bays+rbl+surbl	hit	5987	
	pass	44	99.3%
all	hit	6010	
	pass	21	99.7%

japanese only			
kas	hit	1045	
	pass	289	78.3%
bays	hit	1188	
	pass	146	89.1%
kas+bays	hit	1273	
	pass	61	95.4%
rbl	hit	3	
	pass	1331	0.2%
kas+rbl	hit	1045	
	pass	289	78.3%
bays+rbl	hit	1189	
	pass	145	89.1%
kas+bays+rbl	hit	1273	
	pass	61	95.4%
surbl	hit	918	
	pass	416	68.8%
kas+surbl	hit	1283	
	pass	51	96.2%
bays+surbl	hit	1311	
	pass	23	98.3%
kas+bays+surbl	hit	1320	
	pass	14	99.0%
rbl+surbl	hit	918	
	pass	416	68.8%
kas+rbl+surbl	hit	1283	
	pass	51	96.2%
bays+rbl+surbl	hit	1311	
	pass	23	98.3%
all	hit	1320	
	pass	14	99.0%

others			
kas	hit	4036	
	pass	661	85.9%
bays	hit	4664	
	pass	33	99.3%
kas+bays	hit	4682	
	pass	15	99.7%
rbl	hit	661	
	pass	4036	14.1%
kas+rbl	hit	4115	
	pass	582	87.6%
bays+rbl	hit	4667	
	pass	30	99.4%
kas+bays+rbl	hit	4683	
	pass	14	99.7%
surbl	hit	2856	
	pass	1841	60.8%
kas+surbl	hit	4381	
	pass	316	93.3%
bays+surbl	hit	4674	
	pass	23	99.5%
kas+bays+surbl	hit	4689	
	pass	8	99.8%
rbl+surbl	hit	3200	
	pass	1497	68.1%
kas+rbl+surbl	hit	4427	
	pass	270	94.3%
bays+rbl+surbl	hit	4676	
	pass	21	99.6%
all	hit	4690	
	pass	7	99.9%



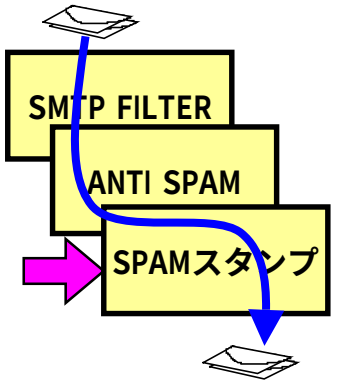
2006/8/1 0:00 ～ 8/31 23:59

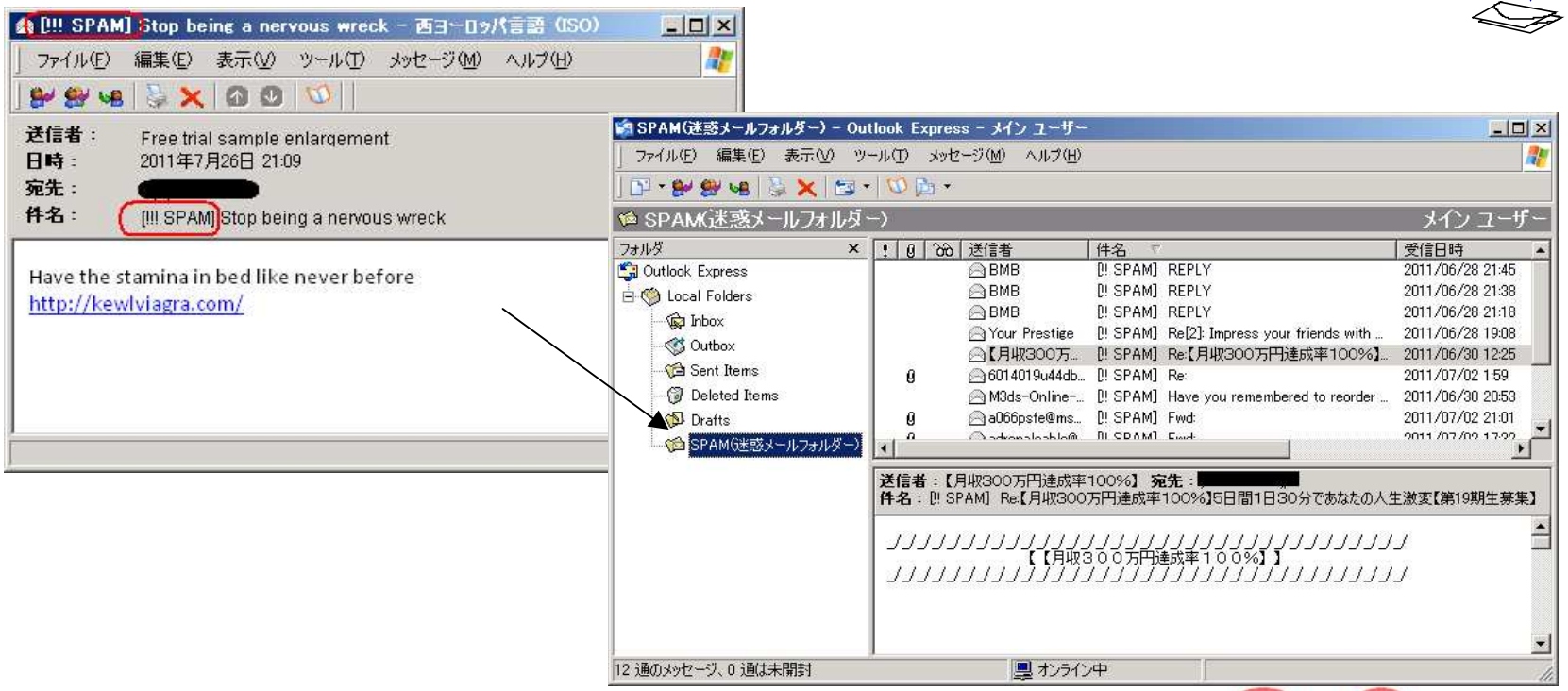
japanese spam	1334
other spam	4697
total	6031

K-SERIES™ 2.0
http://www.kljtech.com

スパム隔離機能 ユーザー単位の設定画面 その１

- K-SHIELD2.0では確実にスパムが判定されたメールに[SPAM]のスタンプする事が出来ます。
- 目的はSPAMスタンプされたメールをメーラソフトウェアで切り分けて、メーラーソフトウェアで隔離フォルダーに保存する事です。
- 下記はスタンプされたメールサンプルとなります

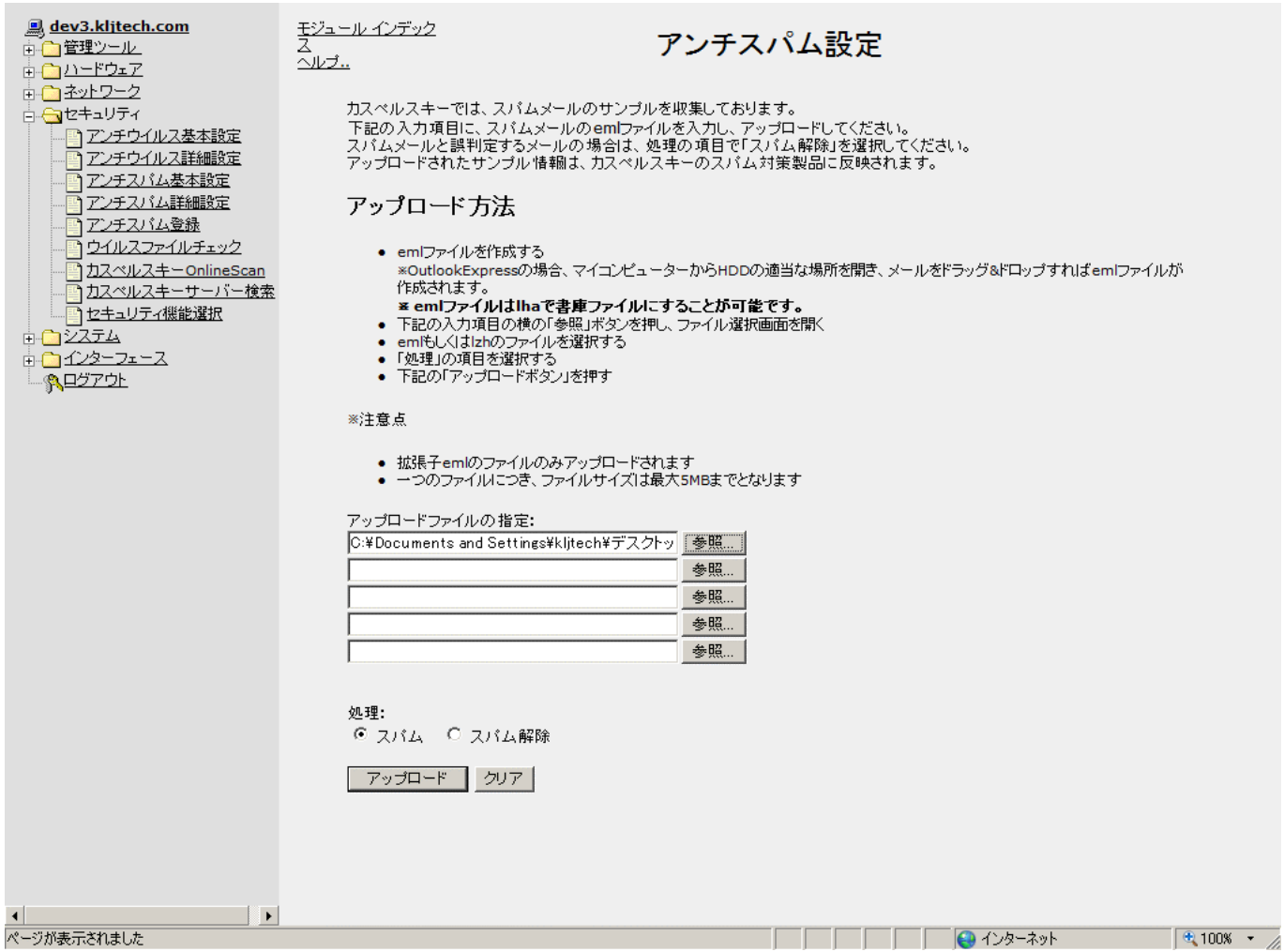




K-SERIES™ 2.0
http://www.kljtech.com

スパムのサンプルの登録

アプライアンスの画面から、スパムメールの検体サンプルを登録することができます。



K-SERIES™ 2.0
http://www.kljtech.com

ウイルス統計情報

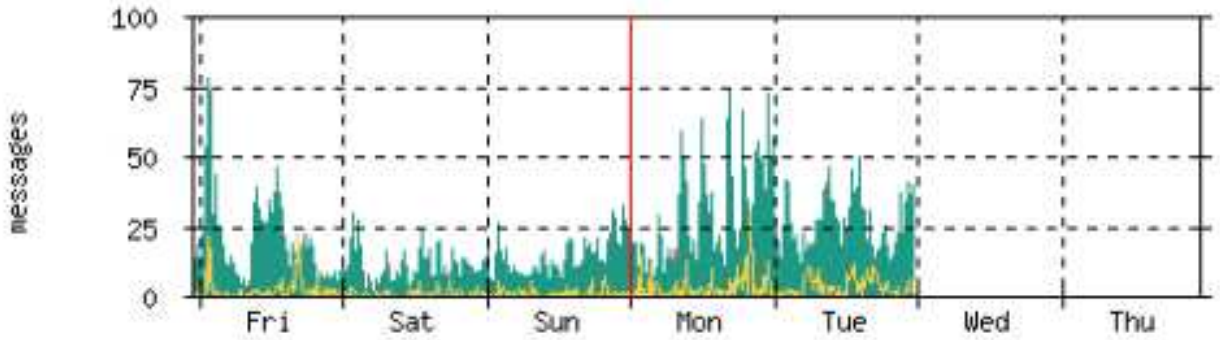
ウイルスの統計受信状況を確認できます。

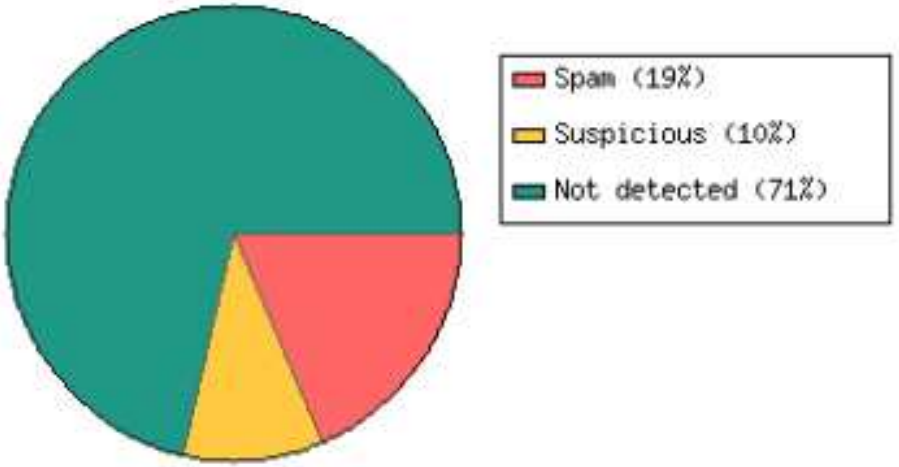
K-SERIES™ 2.0

http://www.kljtech.com

スパム統計情報

スパムの統計受信状況を確認できます。

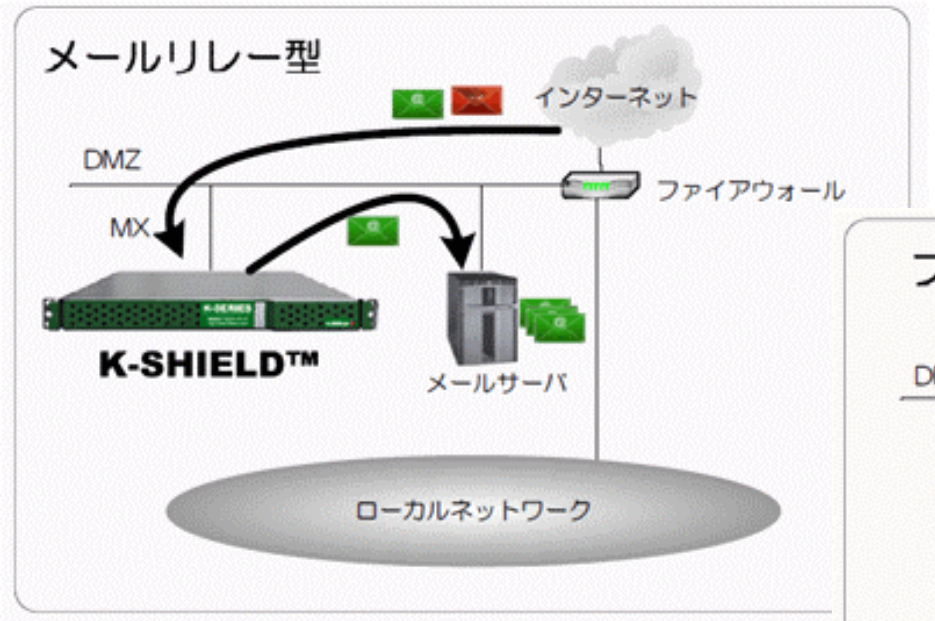


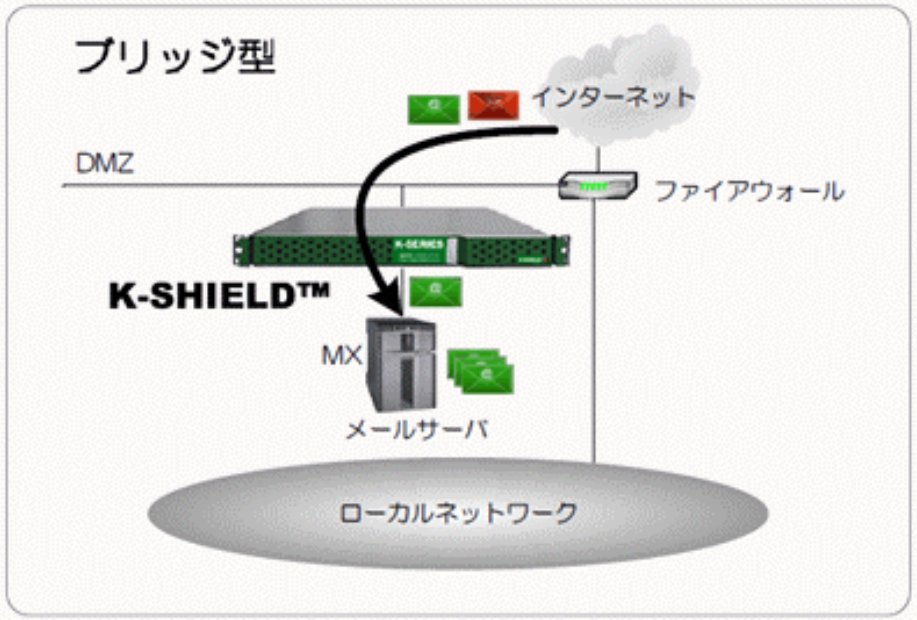


K-SHIELD™ の導入は非常に簡単

K-SHIELDは、メールリレー型のアプライアンスという特性を生かし、現状のネットワークデザインにほとんど手を加えることなく導入することができます。

構成例





K-SERIES™ 2.0
http://www.kljtech.com

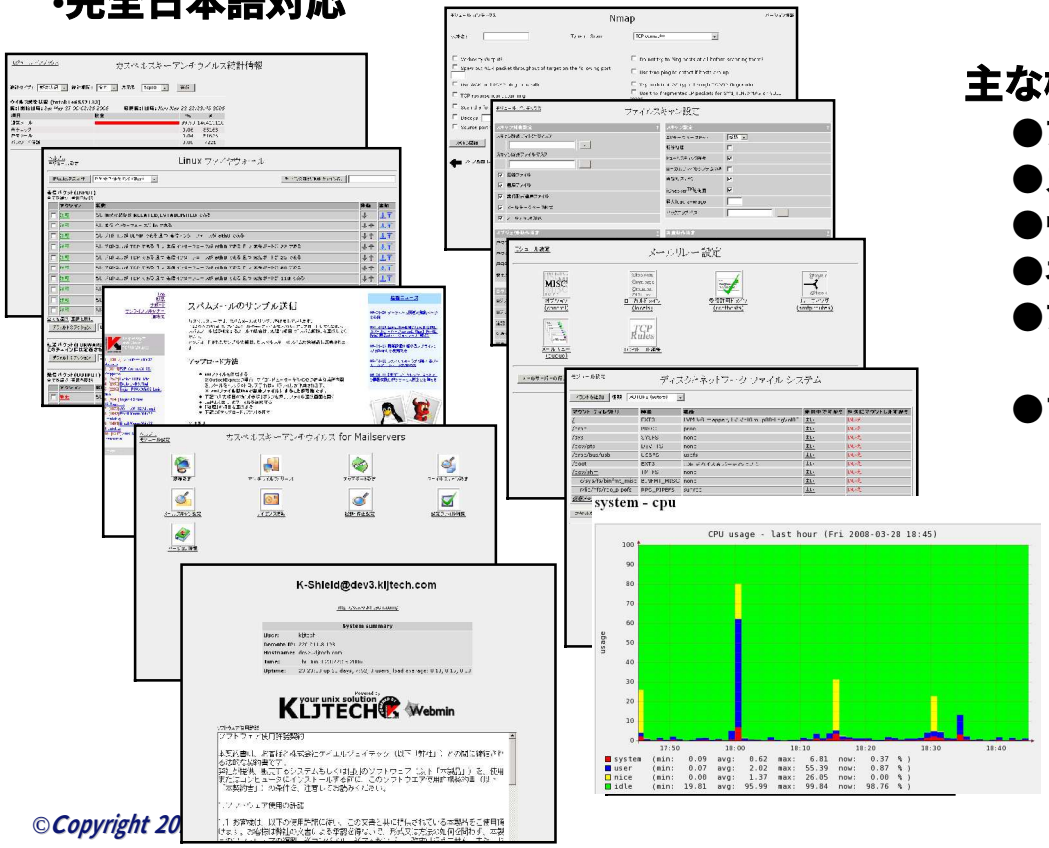
K-SHIELD™日本語GUIインターフェースによる管理機能

•Webインターフェースによる簡単操作
専用クライアントソフトは必要ありません。

•管理者権限の階層化
インターフェースへのログイン権限を階層化。運用担当者･代理店担当者等、立場に応じて操作レベルを使い分けることが出来ます。

•セキュリティ
インターフェースへのログインについては厳正なセキュリティ対策を講じています。

•完全日本語対応



主な機能

- ●アンチウイルス，アンチスパム管理
- ●スパムメール登録機能
- ●ウイルスチェッカー
- ●ネットワーク設定
- ●アプライアンスのヘルスチェック
  (CPU、メモリ、HDD、ネットワーク等)
- ●ファームウェア更新、設定のバックアップ・リストア

K-SERIES™ 2.0
http://www.kljtech.com

製品仕様

	小規模事業所向け	小中規模事業所向け	大規模事業所向け	大規模ネットワーク向け
型番	KS100T	KS300T	KS600I	KS1000I
対応メール ユーザー数	～100	～1000	～10000	10001～
CPU	Celeron 2.66GHz	Celeron 2.26GHz	Pentium4 3GHz	Xeon Dual 3.2GHz
RAM	512MB	512MB	1GB	4GB
HDD	30GB以上×1	30GB以上×2	30GB以上×2	30GB以上×2
RAID	-	RAID-1	RAID-1	RAID-1 ホットスワップ
ネットワーク インターフェース	10/100×1	10/100×2	10/100/1000×2	10/100/1000×2
機能	ウイルス及び スパム対策	ウイルス及び スパム対策	ウイルス及び スパム対策	ウイルス及び スパム対策
筐体タイプ	デスクトップタイプ	1Uラックマウント	1Uラックマウント	1Uラックマウント
筐体寸法 (WxHxD)(mm)	19'×1U×580	19'×1U×580	19'×1U×559	19'×1U×686
質量	11.0kg～12.7kg	11.0kg～12.7kg	11.0kg～12.7kg	12.7kg～15.6kg
電源	AC100V	AC100V	AC100V	AC100V
消費電力	250W	250W	350W	550W（二重化可能）

※KS2000I = カスタム・モデル

K-SERIES™ 2.0
http://www.kljtech.com

お問い合わせ

your unix solution
KLJTECH

株式会社ケイエルジェイテック
〒101-0025 **東京都千代田区**
神田佐久間町1-14 **第二東ビル**5**階**

TEL: 03-5297-4004 / FAX: 03-5297-4005
E-mail: support@kljtech.com
Site: http://www.kljtech.com/