GIDEONの企業理念

「次世代ネットワークコンピューティングの実現を目指して」

GIDEONは1990年に設立され、設立当初から「次世代ネットワークコンピューティングの実現」をテーマに掲げ、研究開発を積み重ねてきました。

単にソフトウェア開発のみに専念するのではなく、コンサルタントやシステム・エンジニア、公認会計士等のスタッフとともに、ユーザーが必要とする支援を的確に提供いたします。

「企業のメール・インフラを安全かつ効率的に」

製品ラインナップは、主としてメール・インフラに注目し、その安全かつ効率的な利用を支援する製品が主力となっています。

これは、企業ユーザーにとってメールが中核的なコミュニケーション手段となっている現実に対応したものです。

GIDEONの得意分野

「Linuxプラットフォーム」

プラットフォームとしてのLinuxの可能性にいち早く注目し、活用してきた経緯から、Linux環境に強みを持ち、豊富な経験と技術力を持っています。

また、インターネット／イントラネット・サーバ全般やアンチウイルス関連の技術力にも定評があります。最近は、アンチスパムやメール・アーカイブ製品も展開しています。

「独自のデータベーステクノロジー」

アンチウイルスやアンチスパムを、高速で効率の良いデータベース検索に基づいて判定を行なう点がGIDEONの製品群の独自の優れた特徴となっています。

また、メール・アーカイブでは、単にメールデータを保存するだけでなく、有用な情報源としての活用を促すようにデータベース化することを意図した設計となっています。

充実したユーザーサポート

「製品開発だけなく、充実したサポート体制を」

GIDEONは、製品開発だけに注力するのではなく、ユーザーが真に必要とするサポート体制を整えています。

多数のユーザーに対してOne to Oneサポートで対応しており、またオンラインでのサポートにも力を入れいます。Webを利用したサポート情報提供も充実しています。

開発コンセプト

ユーザーにとって使いやすいソリューション

「シンプルで手間いらず」

GIDEONが製品を開発するに当たって重視していることは、ユーザーにとって使いやすい製品とすることです。

また同時に、よく分からない"ブラックボックス"にならないよう心がけています。ユーザーに安心して使ってもらえるよう、Linuxその他のオープンソースソフトウェアも積極的に活用しています。

「使いやすさの追求」

GIDEONの製品は、「設定をシンプルに」、「分かりやすいWebインターフェイス」を、という使いやすさを追及しています。

さらに、内部でのソフトウェアの動作が標準プロトコルに準拠していることや、既存のネットワーク環境に極力影響を与えないように配慮されていることなども、使いやすさの追求の結果です。

優れたデータベース技術

GIDEONは、データベース技術に関しては創業当初からの長い経験を持っています。

セキュリティ製品は一見データベースとは縁が薄いように見られがちですが、実際には有害コードや迷惑メールの判定でもデータベースの整備と高速な参照がシステムの中核となっています。

データベース部分を最適に設計できるかどうかがシステムの使い勝手を大きく左右することになるのです。

「ウイルス／スパム データベース」

アンチウイルス／アンチスパム機能でも、データベースの技術が土台を支えています。

ウイルスの場合は添付のコードが既知のウイルスと一致するかどうかをデータベース検索によって調べます。

迷惑メールに関しても、自然言語解析で意味を理解した上で判定を下すといった作業よりも、実は誰がどのメールサーバから送信したメールか、に着目することで効率よく判定できます。

こうした「ブラックリスト」を整備することで、検索が高速化し、その上高精度で判定できるのです。

「検索データベース」

新たに加わったMail Archiveでも、データベースの技術が存分に活用されています。

情報活用を主目的としたアーカイブでは、必要なときに必要な情報を迅速に発見できることが何より重視されます。

次々と到着するメールを遅滞なくデータベース化し、効率よくインデックスを作成して検索に備える技術が重要なソリューションです。

GIDEON Mail Archiveでは、分散ストレージ／分散インデックスがサポートされており、大容量でも高速な検索速度が実現されています。

GIDEONの製品ラインアップ

機　能	 メールサーバMTA版	 ゲートウェイサーバ版	 BLOCsystem	機能特徴
アンチウイルス	ギデオン アンチウイルス メールサーバ Ver.3	—	ギデオン アンチウイルス BLOC system	・WEB管理インターフェース(httpsにも対応) ・ウイルス定義ファイルは1時間毎の自動更新 ・あらゆる圧縮方式(約1,000種類) /多段圧縮(256階層)のウイルスも検出可能。 ・スパイウェア、トロイの木馬、アドウェアに対応 ・Kaspersky社製コアエンジン (約563,000種類のウイルスパターン。新種のウイルス発見より1時間以内に対応) ・メンテナンスフリーの自動アップデート (ウイルス定義ファイル、検出エンジン、解析モジュールなど)
アンチウイルス アンチスパム	ギデオン アンチウイルス アンチスパムPlus	ギデオン ゲートセキュリティ	ギデオン アンチウイルス BLOC system アンチスパムPlus	・スパムメール検出率95%以上(当社調べ) ・ホワイトリスト、ユーザブラックリスト、メールヘッダ解析、本文URL、DNSチェック、シグネチャ DB、本文解析などの複合解析 ・独自開発のスコアリングロジックにより誤検知率を低減 ・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) ・スパムメール転送機能による不要メール削除 ・スパムDB自動更新 ・750万件の本文DBチェック ・アンチウイルス機能(同一WEB管理インターフェース)
メールアーカイブ (アンチウイルス機能)	ギデオン メールアーカイブ	—	ギデオン BLOC system メールアーカイブ	**アーカイブ共通仕様** ・通過するメールトラフィックを自動アーカイブ ・メールヘッダ・本文・添付ファイルテキストまでインデックス化※5 ・マルチストレージボリュームの検索機能 (インデックス化されたデータベースは外付HDDやiSCSI・SANなどのストレージへ保存が可能)※6 ・全文検索機能(マルチボリュームを対象に、インデックス化されたテキストから対象メールの全文検索が可能) ・検索アクセス制限 ・メールアカウントグループ化機能 ・アンチウイルス機能が標準搭載 ・メールアーカイブPlusには、アンチウイルス／アンチスパム機能搭載 **アプライアンス仕様** ・PortControlにより、POP3/SMTPプロトコルのみを通過するトラフィックから抽出を行うパケット転送方式を採用 ・BLOC system障害による影響を抑えるため、PortControlバイパス機能搭載 ・透過ブリッジタイプでネットワークの環境変更せずに導入可能 ・アーカイブデータは外付HDD及びネットワークストレージ(iSCSI/SAN)に保存が可能※6
メールアーカイブ (アンチウイルス アンチスパム機能)	ギデオン メールアーカイブ Plus	—	ギデオン BLOC system メールアーカイブ Plus	

ソフトウェア動作環境

サーバ	CPU	Intel Pentium III 1GHz以上(アンチウイルス・アンチスパム)
		Intel Pentium4 3GHz以上 (アーカイブ)
	メモリ	512Mbyte以上(アンチウイルスの場合)
		1Gbyte以上(アンチスパム、ゲートセキュリティの場合)
		2Gbyte以上 (アーカイブ)
	HDD	・/usr/localディレクトリ以下HDD空き容量 200MByte以上 (アンチウイルス・アンチスパム)
		・10GB以上 (インデックス作成領域含む)
Linux カーネル		x86 アーキテクチャ glibc 2.2 以降
MTA		postfix/sendmail/qmail

アプライアンス仕様

接続方式	透過ブリッジ
検出ポート	POP3、SMTP、HTTP、FTP
ハードウェアスペック	ユーザ数により可変
管理画面	GIDEON オリジナル Flash GUI
ミニボックスタイプ	アンチウイルス・アンチスパム機能：50ユーザ
1Uタイプ	アンチウイルス・アンチスパム機能：100ユーザ以上 メールアーカイブ機能：50ユーザ以上
PortControl	WAN：1ポート L1：BLOC接続ポート L2：BLOC接続ポート L3：ローカルポート L4：管理ポート

※1　アンチウイルス /アンチスパムでは、50ユーザ: ミニボックスタイプ、100ユーザ以上: 1Uタイプとなります。メールアーカイブの場合は、50ユーザ以上: 1Uタイプとなります。
※2　メールアーカイブをご利用の場合は PortControlが必要です。PortControlは冗長化及び負荷分散などの構成が可能です。
※3　BLOC system/ハードウェアメーカー保証期間は 3年間です。ハードウェア保証期間は、次年度更新ライセンスをお申込いただくと有効になります。
保証期間内に障害が発生し、ハードウェア交換が必要と当社にて確認が出来た場合は、センドバック方式にて対応いたします。
交換機につきましては、工場初期出荷状態での出荷となりますので、お客様ご自身で BLOC system初期設定を行ってください。
3年以降は、オプションで BLOC system ハードウェア延長有償保守がお申込いただけます。
※4　PortControl製品保証期間は 1年間です。
保証期間内に障害が発生し、ハードウェア交換が必要と当社にて確認が出来た場合は、センドバック方式にて対応いたします。
1年以降は、オプションで PortControl ハードウェア延長有償保守がお申込いただけます。
※5　圧縮ファイル及びパスワード付圧縮ファイルはファイル名のみインデックス化されます。
※6　最大ボリューム数は 255です。ストレージごとにボリュームをつけたり、パーティションごとにボリュームをつけることが可能です。ファイルシステムは VFAT、EXT3に対応しています。
※7　詳しい対応バージョン等につきましては、弊社ホームページまたは営業担当までお問い合わせください。

スパム／ウイルスの現状

スパムやウイルスは、電子メール・コミュニケーションに対する大きな脅威となっている。LAN内に一気に感染を広げるような大規模なワームの被害こそ少なくなったが、これは事態の沈静化を意味するのではなく、逆により悪質化したことの表われだ。
現在のスパムやウイルスは、特定個人をターゲットにし、オンライン・バンキング・サービスのID／パスワードといった個人情報を収拾し、経済的な利益を得ることに主眼を置くようになってきている。
大規模感染を引き起こすようなものではないので、気付かぬうちに深刻な被害を受けているということもある。

ウイルスは大規模感染型から、ゼロデイ攻撃型に

ウイルス感染は2004年～2005年辺りをピークに、被害届け出が減少する傾向が見られるが、ウイルス対策の必要が薄れたことを意味するものではない。大規模感染は減少傾向だが、一方でゼロデイ攻撃も目立つようになってきている。OSなどのソフトウェアに脆弱性が見つかると、間髪を入れずにその脆弱性を攻撃するなど、対策が間に合わないケースも増えている。

ウイルス作成が商用化され、「ウイルス開発キット」がサポート付きで販売されているという話もある。こうしたキットを使い、限定されたターゲットにピンポイントで攻撃を仕掛ける例が増加しており、的確な防御がますます難しくなる傾向がある。

スパムメールがサイバー攻撃の起点に

迷惑メール(スパムメール)は、インターネットのメール・トラフィックの90%以上を占めるとも言われている。初期の迷惑メールは物販サイトの宣伝などを目的としたものが主で、名前の通り単に迷惑な存在だったのだが、現在ではいわゆるサイバー攻撃の起点として、より直接的な経済利益を狙う手法が目立つようになってきた。

たとえば、言葉巧みに関心を引きそうな文面を工夫し、ユーザーにメールに記載されたURLをクリックさせるよう仕向けた上で、アクセス先となるサイトに有害コードを仕込んでおき、Webブラウザや特定のファイルタイプの処理を行なうブラウザ・プラグインの脆弱性を突くといった攻撃を行なうものだ。

サイズがゼロのフレームを用意して、そこにスクリプトを仕掛けておくといった巧妙な手法が利用されることが多く、画面を見ているユーザーも気づかないうちに手元のPCにマルウェアが仕掛けられるといったことも起こっている。

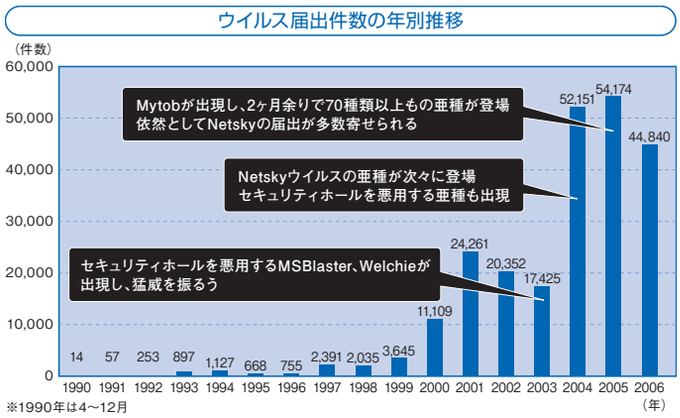
サーバ上でのスパム対策が効果的

こうした状況下で、有効な対策となるのが、サーバ上でのアンチスパム・フィルタの導入だ。ユーザーがそもそも迷惑メールを受信しないようにしてしまうことがもっとも効果的な対策といえる。

迷惑メールのトラフィック急増による回線帯域の浪費も深刻な問題となってきているが、この問題に対処するには、メールサーバなど、大本に近いところで対処することが効果的だ。また、迷惑メールがユーザーに到達してしまうと、ユーザーごとのメールボックスサイズが肥大したり、バックアップ容量が増加したりといった副次的な被害も拡大してしまう。

メールトラフィックの90%を迷惑メールが占めているとすれば、これを入り口で遮断できれば回線帯域やストレージをこれまでの10倍活用できることにも繋がる。最後の防衛戦としてクライアントPC上での対策もこれまで通り必要ではあるが、まずサーバ上でウイルスやスパムに対応することの重要性が高まっているのが現状だ。

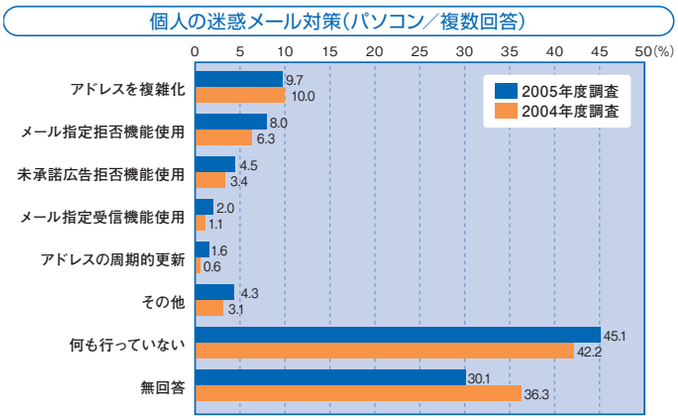
ウイルス届出件数の年別推移



※1990年は4～12月

IPAが2007年3月に発表した「情報セキュリティ白書2007年版」から引用

個人の迷惑メール対策(パソコン／複数回答)



総務省発表の「平成18年版 情報通信白書」より

アンチウイルス・アンチスパム機能

アンチウイルス／アンチスパムは、それぞれがソフトウェア製品として提供されるほか、ハードウェアに組み込んでアプライアンス化したBLOC systemも用意されている。機能面では特に違いがないので、ここではソフトウェアとアプライアンスを特に区別せず、その特徴を紹介する。

どちらも、コアとなるエンジン部分に優れた実績を誇る技術を採用した上で、Linuxメールサーバに関して深い経験を有するGIDEONが開発したソフトウェアであり、Linux系のメールサーバを利用している場合には容易にセットアップでき、高精度での検出が実現できる。

設定不要の簡単導入

導入時に設定するのは管理者のメールアドレスやスパムメールの転送先などのユーザー環境に固有の情報だけで、わずらわしいパラメータ調整などの必要なく、運用を開始できる。

ソフトウェア版が対応するMTAはsendmail、qmail、postfixの3種で、Linux系のメールサーバのほとんどをカバーできる。アンチウイルス／アンチスパム共、MTA内部で動作するため、別のサーバを用意する必要はなく、ネットワーク構成の変更なども不要だ。

ウイルス／スパムのチェックはアカウント／ドメインごとにON／OFFの設定ができる。設定変更、ログやレポートの閲覧は管理用のWebインターフェイスのGUI画面で行なえる。

自動アップデートで素早く対応

セキュリティ・ソフトウェアに不可欠なアップデートに関しては、365日24時間体制で対応する。

ウイルス検出とスパム本文解析のためのコアエンジンにはロシアのKaspersky社の技術が導入されている。新種ウイルスは発見から1時間以内に定義ファイルが作成され、サーバ側の定義ファイル更新は1時間ごとに差分更新が実行される。

また、スパムの本文解析データベースは3時間ごとに差分更新が行なわれる。これらの更新はインターネットを介した自動更新であり、管理者の関与は不要で、管理負担も生じない。

高い検知率

アンチスパムは内容がテキスト主体のため、明瞭な特徴を見つけにくい。

GIDEONのアンチスパム技術では、データベースを構築し、その照合によって判定を行なう。本文ではなく、ヘッダから得られる情報に基づいて発信元の信頼度を判定するというのが基本的な考え方だ。

実環境検証では、スパムの98%を正しく判定し、1.99%に対して可能性アリとの判定を行なった。スパムでありながらフィルタを通過したのはわずか0.01%であり、正常なメールをスパムと誤検出した例は皆無だった(公式な誤検知率は0.001%)。

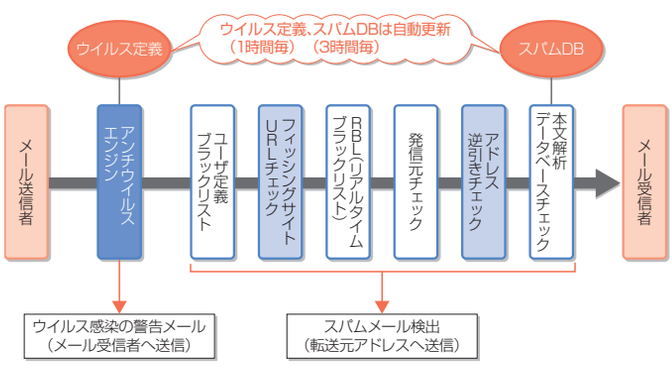
なお、他のアンチスパム製品には、メーリングリストなどを誤ってブラックリスト登録してしまう例も見受けられるが、GIDEONのアンチスパムでは、配信元確認で問題がなく、さらにメール本文のチェックにおいてもスパムと判定される要素がない場合には、単に大量に配信されたというだけの理由でスパムと誤認識することはない。

プリフェッチ機能

アプライアンス版の BLOC systemでは、アンチスパム機能を「プリフェッチ」という手法を使って実現している。

これは、ユーザーが通常実行している POPによるメール受信と同じ動作を BLOC systemが実行してメールを取得、判定を行ない、スパムと判定したメールに関してはメールサーバ上のメールボックスから削除してしまうという機能だ。

この方式のメリットは、利用しているメールサーバの種類を問わないことだ。小規模な組織では、自前のメールサーバを用意するのではなく、ISP等が提供するサーバを利用する例が多いが、通常のユーザーアクセスと全く同じ動作のため、メールサーバの種類や設定によらず処理が可能だ。また、プロキシ方式とも違うため、ユーザー側のメール・クライアントの設定を変更する必要もない。



アンチスパムはアンチウイルスのオプションと位置づけられており、動作時はアンチウイルスに続く後段処理として実行される。

アンチウイルスがKasperskyエンジンによる処理なのに対し、アンチスパムは本文解析のみKasperskyで実行し、それ以外の信頼性確認は独自手法によるデータベース参照で実現される。

送信元のアドレスをDNSで逆引きするなど、さまざまな手法で信頼性を確認し、その結果を組み合わせて総合判定すると同時に、スパムと判定されたRBLやURLは高速化のためメモリにキャッシュされ、その後も参照される。

逆に、スパムではないと判定されたメールの配信元IPアドレスやドメインも「ノーマルキャッシュ」として同様に保存され、判定処理速度を向上させるために参照される。

こうして、同じようなスパムが連続して大量に到着するような場合には処理速度が低下することもなく効率的に判定できる。

メールアーカイブ機能

業種・業態を問わず、電子メールはコミュニケーション手段の中核と位置づけられるようになってきている。
文書化され、定式化されたビジネス・プロセスとは異なり、メールは非定型で整理しにくい情報ではあるが、現場の生の情報であり、定式化が追いつかない豊穣な領域をカバーする広範な情報源となりうるものだ。
GIDEON Mail Archive は、コンプライアンス対応のための「死んだ情報の集積」や大規模な Knowledge Base System のような硬直化したシステムとは異なる手法で、組織内を行き交う知恵をデータベース化することができる。

設定不要の簡単導入

GIDEON Mail Archiveもメールサーバ版とアプライアンス版が用意されている。製品群を貫くポリシーは一貫しており、簡単にインストールでき、設定も容易という点は維持されている。

アンチウイルス／アンチスパムと組み合わせて利用することも可能で、ウイルスやスパムを除いた後の、意味のあるメールだけをアーカイブ対象とすることができる点も大きなメリットだ。

この結果アーカイブのデータ量が減り、不要な情報を排除する必要もないため、セットアップ後はほとんど何の作業もいらず、自動的にアーカイブが蓄積され、データベースの価値が日々高まっていくことになる。

自動アーカイブ

BLOC systemを利用したアプライアンス版では、メール送受信経路上にBLOC systemを設置するだけでよく、ネットワークの設定変更等は不要だ。

通過していくトラフィックを監視し、SMTP／ POP3のトラフィックを見つけ出して自動的にアーカイブするため、外部のメールサーバを利用している場合でも問題なくアーカイブできる。

メールサーバ版でも同様で、メールサーバを通過するメール・トラフィックを自動的にアーカイブしていくので、設定変更等は不要だ。

アーカイブはアクセス権などを参照して検索範囲を限定できるので、セキュリティ面の問題も生じない。

メールのナレッジベース化

企業活動の実態を示す証拠として電子メールの保存を求める動きもあるが、GIDEON Mail Archiveの設計意図はメールを重要な情報源として活用していくことにある。

単にメールデータをコピーして保存するのではなく、差出人や宛先、件名といたヘッダ情報や本文内容に対して、アーカイブの時点でインデックス作成を行ない、データベース化していく。情報保護の観点から、アーカイブは非読化も可能だ。

アプライアンス版の場合は、PortControlを併用することで冗長構成や負荷分散も可能だ。外部ストレージを併用すれば数百人規模の組織でも問題なく運用できる拡張性も確保されている。

また、文章検索属性の追加やメール文章以外のドキュメント拡張も準備している。

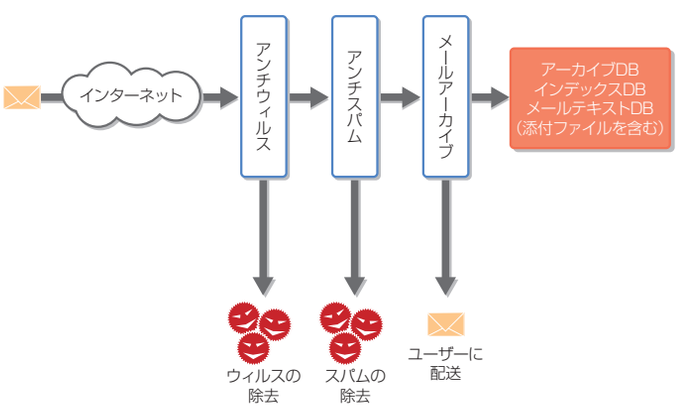
高速な全文検索

情報として活用することを目的としたアーカイブでは検索機能が極めて重要となる。

GIDEON Mail Archiveでは、データとそのインデックスを保存するストレージは分散可能で、検索も分散ストレージに対応しているため、データ量の増大にも対応が容易だ。実システムの例では、10万通のメールに対する全文検索が1秒以内で完了している。

インデックスの作成はローリング方式で、受信・送信メール（添付ファイル本文を含む）のインデックスが自動で生成され、アーカイブデータとして蓄積保存されていく。このため、規模が大きくなっても、インデックスの統合のために時間が掛かることはない。

検索範囲も、アクセス権に基づくもののほか、特定のメーリングリストだけを検索対象とするといった設定も可能で、検索精度を高める上でも役立つ。



GIDEON Mail Archiveは通信経路上に設置され、トラフィックの内容を監視している。
メール(SMTP／POP3)であれば自動的にアーカイブ処理を行なうので、既存のネットワーク環境の変更は不要だ。プロキシではなく、透過プロキシとして動作するイメージだ。
さらに、プロトコル・レベルでの監視であるため、ユーザーのメール・クライアントや、メールサーバの種類、サーバの設置場所といった条件には全く影響を受けない点もポイントだ。
ユーザーが複数のメールサーバ／メールアドレスを使い分けている場合でも、その全てをアーカイブ対象にできる。
アプライアンス版では、PortControlを併用することでプロトコルレベルでのトラフィックの振り分けをPortControlに任せられるため、さらに高度な構成が可能になる。

PortControl

アプライアンス版の BLOC system を使用する場合、メールのトラフィックすべてが BLOC system を経由するように設置する必要があるため、万一 BLOC system が動作停止することがあればネットワークが事実上機能停止に陥るという懸念もあるかもしれない。

アプライアンスである BLOC system は、アプライアンスとして汎用サーバよりも高い信頼性と安定性を備えるが、それでも多重化等の高信頼性対策を施したいという場合には、「PortControl」を併用することで複数の BLOC system を接続して処理を分散させることが可能になる。

トランスペアレントなパケット･ルーティング

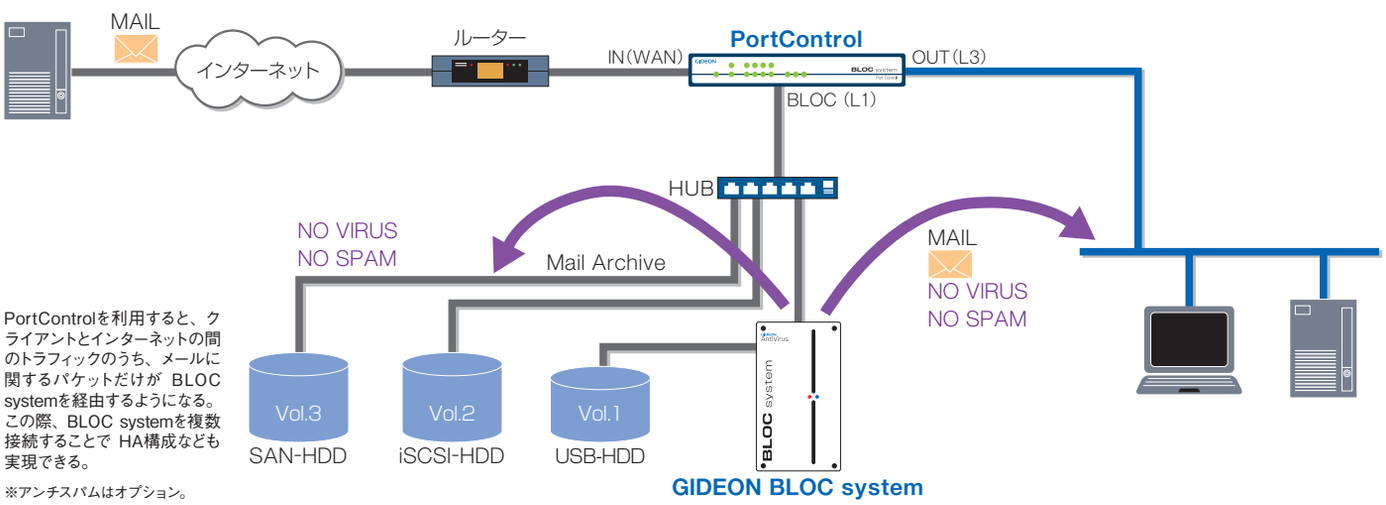
PortControlはクライアントからメールサーバへの通信経路の途中に設置する。クライアント接続用のLANポートと、BLOC systemを接続するためのポートが備わっており、一見するとルーターのように見えるネットワーク機器だ。

外部からのメール･トラフィックはまずPortControlに到着し、そこからBLOCsystem宛に送られる。BLOC systemがウイルスやスパムを除去した結果、重要なメールだけがクライアントに届くことになる。このため、BLOC systemの設置場所は、ユーザーの都合に応じて自由に選べ、場所の制約を受けない柔軟な運用が可能になる。

PortControlによるパケットの経路変更は自動的に行なわれ、ユーザーからはその存在自体を意識する必要がない。

SMTPやPOP3など、メールに使用されるポート番号を見て、メールに関するパケットであればBLOC systemを経由させ、メールと無関係な通信のパケットはそのまま通過させることができるため、仮にBLOC systemの負荷が高まったときでも、メール以外のトラフィックの配送遅延などが発生することを回避できる。

PortControlは常にBLOC systemと通信して動作状況を確認している。仮にBLOC systemに障害が発生して応答が途絶えた場合には、PortControlはメール･パケットの振り分けを停止して直接配送に切り替えるので、アンチウイルス／アンチスパムは停止するが、メール自体の送受信は継続でき、業務に支障を来たすことはない。



PortControlを利用すると、クライアントとインターネットの間のトラフィックのうち、メールに関するパケットだけが BLOC systemを経由するようになる。この際、BLOC systemを複数接続することで HA構成なども実現できる。

※アンチスパムはオプション。

分散配置の実現

PortControlには複数のBLOC systemを接続することができるため、万一の障害に備えた冗長化構成も実現できる。

BLOC systemが障害を起こすことに備えるのであれば、二重化によるHA構成が可能だ。これは、万一に備えた予備機を用意しておき、障害発生時には予備機に切り替えるという動作だ。

PortControlは常に配下のBLOC systemと通信しており、BLOC systemが正常に動作しているかどうかを監視している。障害を検知したら、パケットの送り先を予備機に変更することで処理を継続できる。

また、複数台のBLOC systemを使い分けることで負荷分散を実現することが可能だ。

クライアントをグループ分けし、それぞれ異なるBLOC systemを割り当てて処理を分散させることでBLOC systemの負担を軽減し、信頼性を高めることが可能となる。

たとえば、JSOX法などのコンプライアンス上の要件からメールのアーカイブが必須となる部署のメールのみをアーカイブするなど、ユーザー固有のポリシーに応じた運用が実現できる。

なお、PortControlによるパケットの振り替えはL2レベルで実行されるため、メールヘッダの書き換えなどは起こらない。このため、ユーザーレベルでは従来通りのメールのやりとりが実現し、クライアント側での設定変更などの余分な作業を発生させることなく、高信頼性対策を導入できる点がメリットとなる。

ギデオンの製品導入例

GIDEON のメール・ソリューションは、導入が容易な点を特徴とするが、効果的に運用するためには、ネットワーク上のどの位置に設置するかなど、ネットワーク構成については検討すべき要素がある。ここでは、ネットワークの規模に応じたいくつかの設置例を紹介しておきたい。

ユーザーに送られてくるすべてのメールが、GIDEON のソフトウェアもしくはアプライアンスを通過するネットワーク構成が必要となる。迂回できる経路が存在すると、ウイルスチェック、スパムメールの排除、メール・アーカイビングの効果を最大限に得ることはできない。

BLOC system単体での小規模構成例

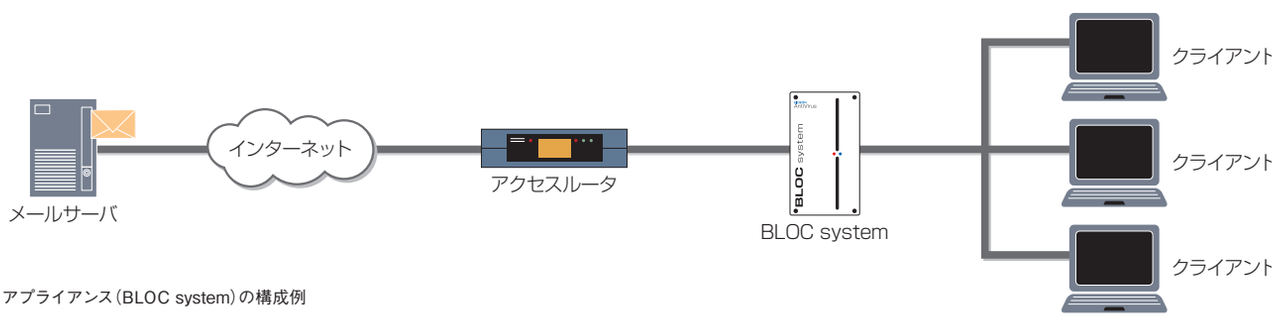
ユーザー数が数人～数十人規模の組織であれば、アプライアンス版であるBLOC systemを単体で導入するだけで充分な保護が可能だ。

また、こうした小規模な環境では、メールサーバが内部に設置される例は稀で、多くはISP等が提供するメールサーバを利用しているケースが多いので、メールサーバに導入するソフトウェア版よりもアプライアンスの方が親和性が高い。

この構成の場合、メールサーバからのメールの受信にはPOP3を利用するのが一般的だが、BLOC systemはユーザーがPOP3でアクセスを実行した際にユーザー IDとパスワードをキャプチャして記録しておき、以後は一定時間ごとにメールサーバのメールをチェックし、スパムを発見するとメールサーバのスプールから削除する。※

このため、ユーザーがメールを受信する際には常にスパム以外のメールだけが送られてくる。ユーザーによる事前設定等が不要であり、ユーザーアカウントを作成するなどの手間もいらないため、運用管理の負担もほとんど発生しない。

※判定されたスパムメールは、転送メールボックスに転送されあとに削除を行なうので、メール紛失はしない。



アプライアンス（BLOC system）の構成例

PortControlを併用した中規模構成

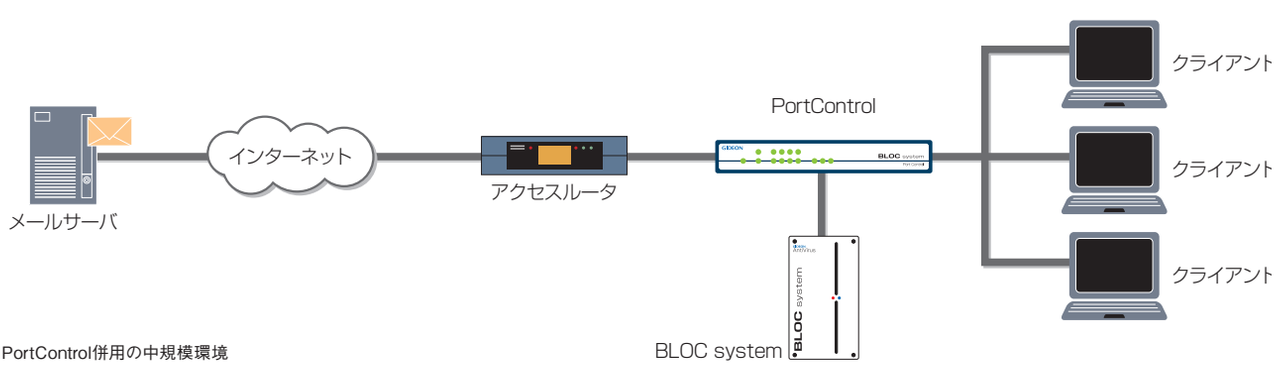
BLOC systemを単独で使うのではなく、PortControlを併用すると、より高度な要件に対応できる。

接続は、全トラフィックが通過するアクセスルータの手前にPortControlを置き、その配下にクライアント側LANとBLOC systemを並列に置くことになる。

PortControlがSMTP／ POP3のトラフィックだけを選んでBLOC systemに転送し、戻った結果だけを元の経路に戻すため、ユーザー側がその存在を意識しない点はBLOC system単独での利用と同様だ。

この構成のメリットは、PortControlによってトラフィックの選別が行なわれるため、仮にBLOC systemが過負荷等の理由でスループットが低下するようなことがあっても、メール以外のトラフィックには影響を与えない点だ。重要な業務アプリケーションを実行している場合などで特に有効だ。

また、PortControlの配下に複数台のBLOC systemを接続することでHA構成や負荷分散も実現できるため、ユーザー数が増えてきた場合や、メール･システムが業務遂行上極めて重要な場合に役立つ。



PortControl併用の中規模環境

外部ストレージやHA／負荷分散を意識した大規模構成

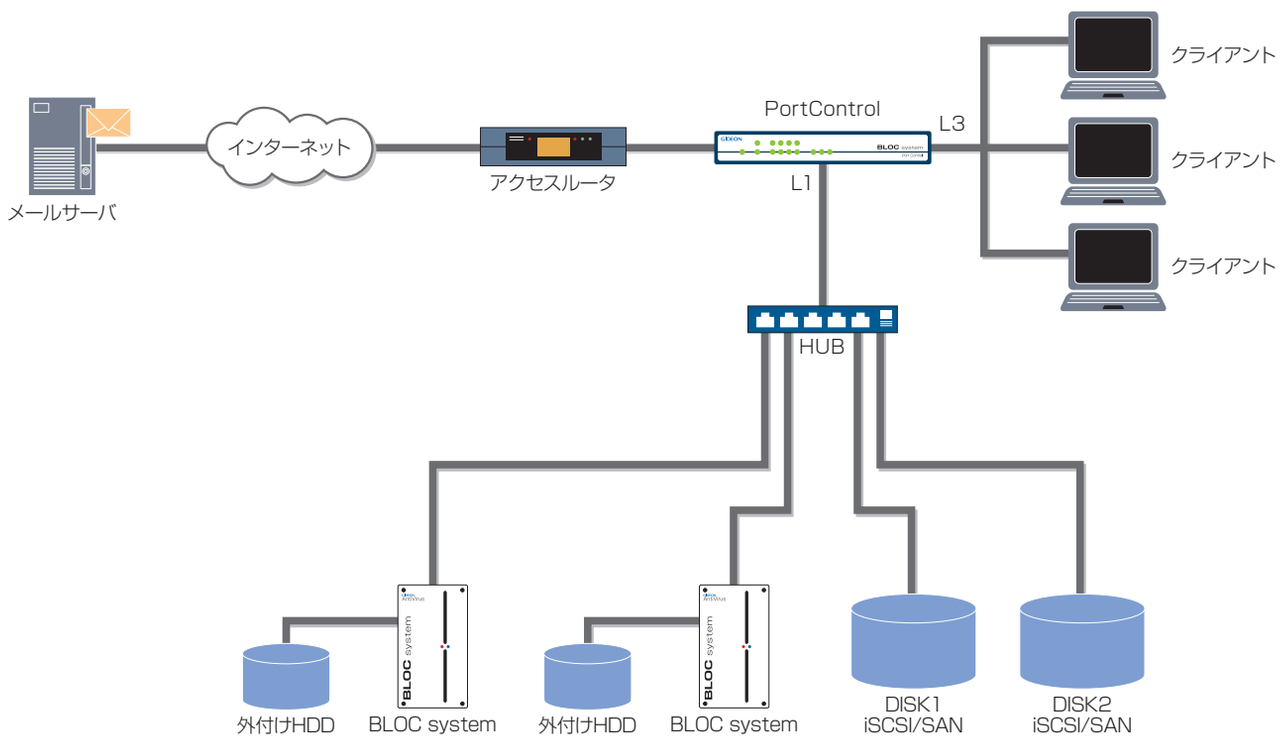
BLOC systemはアプライアンスではあるが、PortControlと併用することで大規模環境にも拡張可能だ。

HA(High Availability)構成の場合、障害に備えてBLOC systemの予備機を用意し、待機させておくという使い方になる。

また、Mail Archiveに関しては、BLOC systemの外付けハードディスクのほかに、iSCSIやSANを利用した外部ストレージ構成も可能だ。増大するメール容量に対応する上でも重要な機能となる。

HA構成では、高信頼性のために予備機をスタンバイさせておくことになるが、これを常時稼働とすれば負荷分散構成となる。複数のBLOC systemで負荷を分散することにより、クライアント数が増えた場合でも対応できる。これらの構成は、ネットワークの対外接続点が1カ所に限定される場合に有効だ。

一方、大企業の場合はフロアや部門ごとに分散するケースがある。この場合は、オフィスや部門の単位でBLOCsystemを独立に配置することも可能だ。この場合の構成は中小規模に準じたものとなる。



負荷分散＋外部ストレージの構成例

ソフトウェア版の活用

アンチウイルス／アンチスパムには、ソフトウェア版も用意され、Linuxサーバ上で動作する主要なMTAであるsendmail、qmail、postfixに対応する。いずれもメールサーバ上で稼働するため、ユーザーにインパクトを与えることはないし、ネットワーク構成上もトラフィックの経路について悩む心配はない。

メールサーバ上にインストールするため、メールサーバを組織内部で運用している場合に限られるが、これは必ずしも独自メールサーバの運用を意味せず、ISP等のメールサーバとの間でメールの中継を行なうリレーサーバを組織内に設置し、その上でアンチウイルス／アンチスパムを動作させる構成も考えられる。

専用ハードウェアがない分メールサーバの処理能力に余裕が必要となるが、構成がシンプルになる点は大きなメリットだ。

ゲートウェイ版ソフトウェアの構成

GIDEONゲートセキュリティは、Linuxゲートウェイ(GW)上で動作するアンチウイルス／アンチスパムソフトウェアだ。

基本的な動作はメールサーバ版ソフトウェアと同様だが、SMTP／ POP3だけではなく、HTTPやFTPも監視対象とし、より広範な保護が実現できる。

また、メールサーバと「セキュリティサーバ」を分離し、セキュリティ関連機能を集約できるため、運用管理の見通しが向上するといったメリットもある。

アプライアンスであるBLOC systemとも共通するメリットとしては、プラットフォームがLinuxに限定されず、インターネット標準プロトコルを利用して通信していれば監視対象にできる点もポイントだ。

メールサーバ／クライアントともにWindows環境のものを使っていたとしても、問題なく対応できる。組織内でメールサーバにMicrosoft Exchangeを利用している場合などには、ゲートセキュリティの導入を検討するとよいだろう。

GIDEONのサポート体制

使いやすく技術的に優れた製品であっても、適切なサポートが提供されなければ、ミッションクリティカルな用途に使用することはできません。
電子メールは現在、停止しては困る基本的なサービスであるため、アンチウイルスやアンチスパムに関しても、トラブルフリーであることが求められます。そのためには、基本的な安定性や信頼性が高いことに加え、万一の際に備えた万全なサポート体制が整っていることが必要です。
GIDEON では、ユーザーが製品を導入する前に充分な検討を行なえるよう、導入前サポート体制を整えており、導入後のサポートと合わせ、ユーザーが不安なく製品を利用できるよう配慮しています。

導入前サポート

電子メールのようなユーザーにとって重要なサービスに関わるソフトウェアの導入の際には、機能面での検討に加え、ネットワーク構成に与えるインパクトや、実環境での性能など、確認すべき要素が多くあります。こうした事前検証の要望に対応するため、GIDEONでは製品の評価版を用意しています。

ソフトウェア版では3ヶ月間試用できる評価版がWebサイトからダウンロード可能となっています。なお、評価版を導入後、正規に購入を決定した場合は、ライセンスを購入すればそのまま継続して利用できるようになっているため、評価版をアンインストールして再度製品版をインストールする、といった負担は発生しません。

また、アプライアンス版に関しては、2週間の機器貸し出しも行なっており、実環境に導入してテストを行なうことが可能です。

一般的な質問など

株式会社ギデオン インフォーメーションセンター

Email	info@gideon.co.jp
TEL	045-590-1216
FAX	045-590-1217
受付時間	9:00～17:00　※土･日･祝祭日･年末年始を除きます。

導入前に動作検証確認が可能

・ソフトウェア版:3ヶ月評価版	・アプライアンス:2週間お貸出し

※評価版はインストール後3ヵ月間、すべての機能を利用することができる。

導入後サポート

製品導入後のサポートは、電子メール／電話／ FAXで受け付けています。製品は3インシデントまで無償でサポートされるほか、製品に関する機能アップ･起因するバグ･不具合についての問い合わせは無償で受け付けていますので、サポートコストが高額になる心配もありません。

製品のアップデートや、ウイルス／スパムに関する判定情報はインターネットを通じて自動更新が行なわれます。サポート料金は年間ライセンス料に含まれていて、その点の心配も不要です。

一般的な質問など

株式会社ギデオン サポートセンター

Email	sp@gideon.co.jp
TEL	045-590-3655
サポート対応時間	9:00～17:00 ※土･日･祝祭日･年末年始を除きます。 ※状況を正確に把握するため、メールでこちらの情報を記載してお問い合わせください。上記時間帯以外のお問い合わせにつきましては翌営業日以降の対応となりますので、お急ぎの場合は上記時間内にご連絡をお願いいたします。

既存ユーザ更新手続き

株式会社ギデオン インフォーメーションセンター

Email	info@gideon.co.jp
TEL	045-590-1216
FAX	045-590-1217
受付時間	9:00～17:00　※土･日･祝祭日･年末年始を除きます。

GIDEONのWebサイト

GIDEONのWebサイトには、製品のアップデート状況はもちろん、ウイルスの最新動向などのセキュリティ情報も詳細にアップされており、充実したセキュリティポータルサイトとなっています。

また、最新の製品ユーザマニュアルやFAQが公開されており、これらの情報を事前検討の際の材料として活用することもできます。Web上のフォームに入力することにより、簡単に評価版のダウンロード、製品貸し出しの申し込みや、見積もりを取ることも可能です。

http://www.gideon.co.jp/