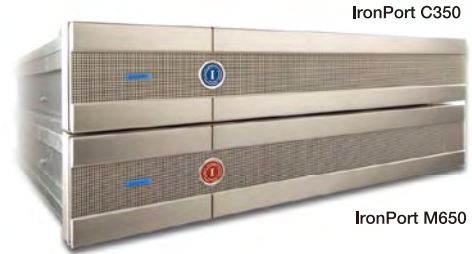


# スパムメールと新種ウイルスに対して トータルかつ効果的な対策を実現

建設・鉱山機械事業の分野において国内で高いシェアを誇るコマツは、情報セキュリティ強化の一環として、スパムメール対策に着手。アイアンポートシステムのメールセキュリティアプライアンス導入により、スパムメールはもちろん、それに付随するウイルス等の脅威への効果的な対策を実現している。



## KOMATSU



コマツ  
e-KOMATSU 推進室  
ネットワークテクノロジーグループ  
担当部長  
田畑 健一 氏



### プロフィール

会社名：コマツ  
(登記社名:株式会社小松製作所)

本社所在地：〒107-8414  
東京都港区赤坂二丁目  
3番6号(コマツビル)

売上高：連結 1兆8,933 億円  
(2007年3月期)、  
単独 7,585 億円

従業員：3万3,863 名(連結)、  
6,231名(単独)

主な事業：  
コマツグループでは主に、建設・鉱山  
機械、ユーティリティ(小型機械)、林業  
機械、産業用機械などの事業を展開。

### 急速に増えるスパムメール 情報セキュリティが重要課題に

「コマツでは、社内的に情報セキュリティの見直しを行うことになったそうですが、その経緯について教えてください。」

2004年7月、コマツでは、当時「個人情報保護法」や「日本版SOX法」といった法制の施行を控えて、自社のセキュリティ対策についての現状を正しく把握する必要があると判断し、第三者機関によるセキュリティ対策のアセスメント(評価)を実施しました。その結果、当社のセキュリティ対策は、強固なものではないことがわかり、我々はこの結果に大きな危機感を感じました。

「セキュリティ対策で一番の問題点は何だったのでしょうか。」

当社は、3年計画でグループ企業を含めた全社的なセキュリティ強化に向けた取り組みを推進していくことにしました。まずは、すでに陳腐化していたセキュリティポリシーの徹底的な見直しに始まり、情報資産の格付けや区分の明確化、有事の際のビジネス継続計画の策定などです。また、全社規模の情報セキュリティ委員会を設置するなど、体制面における整備にも着手しました。そうした一連の取り組みの中でも、とりわけ重要だったのがスパムメール対策でした。

### スパム検知率が低い製品に不満 新たなソリューション導入を検討

「IronPort導入前のスパムメール対策は?」

スパムメール対策として、まず2005年6月に、あるセキュリティベンダーのアプライアンス製品を導入しましたが、正直なところその製品のスパム検知率は低く、精度のよいものではありませんでした。それでも、当時は国内のグループ全社で

1日あたりのスパムメールが4万通くらいだったので、検知率が低くてもユーザー1人あたりに届くスパムメールは1日ほんの数通で、さほど大きな問題にはなりません。ところが、弊社においても2007年夏ごろからスパムメールが急速に増加し、8月にはその数が1日に20万通にも達しました。その結果、ユーザーに届くスパムメールの数も大幅に増加し、そのアプライアンス製品の検知率の低さが社内でも問題視され始めたのです。

また、一方でスパムメールの添付ファイル、あるいはその本文に記されたURLを経由してウイルス感染する問題が顕在化してきました。大きな問題となったのは、新種ウイルスのパターンファイルが間に合わず自動駆除できないことが頻繁に発生したことです。このため、導入していたアプライアンス製品のベンダーとの間で、ワクチンの提供やサポート担当者の派遣など、24時間体制のサービスを受けられるような契約を結んで対応せざるを得ませんでした。

### 定義ファイル提供以前の段階で 疑わしい添付ファイル付きメールを隔離

「そして、IronPortの導入に至るわけですね。その決め手は何でしたか。」

スパムメールの対症療法的な対応よりも、もっとプロアクティブな対策の必要性を感じ、高度な検知率を備え、新種のウイルスにも対応できる新たなソリューションを探し始めました。その結果、我々のニーズにちょうど合ったのが「IronPort C350」だったのです。導入の決め手となった大きなポイントは2つあります。1つ目は「IronPort Reputation Filters」と「IronPort Anti-Spam」による高精度のスパムメール検知機能。そして2つ目が「IronPort Virus Outbreak Filters (VOF)」です。VOFは、新種のウイルス発生直後、疑わしい添付ファイルつきメールを検知し、

