電子メールのセキュリティ確立について

SET ソフトウェア㈱

■ 執筆者Ｐｒｏｆｉｌｅ ■

河盛　英雄

執筆者略歴

1987年　SET ソフトウェア（株）入社
（当時の社名は、エスイーティ㈱）
SE として勤務
2010年　現在に至る

情報通信システムでの経験年数

23 年

■ 論文要旨 ■

電子メールは IT インフラの中でも使用頻度も高く、重要なツールである。反面、誤送信等による情報漏洩、スパムメール受信による被害などのセキュリティ上のトラブルも多数発生している。
本論文では、電子メールのセキュリティ問題を確認した上で、「インシデントから守り、安全かつ快適に使用するにはどうしたらいいのか」ということを、下記のツールの導入も含めて論じてみる。

- 「m-FILTER」Ver2.8
- 「Mail Luck!」

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

IT インフラは、現在の企業活動にとって不可欠なものとなっている。特に、電子メールは、IT インフラの中でも使用度も高く、重要なツールである。その反面、電子メールでは、情報漏洩、スパムメールによる妨害、メールサーバのダウンといった、セキュリティ上の問題も多々発生している。

IT インフラは高度化している。電子メールもハードウェアの発達により、回線速度は高度化し送信ファイルは肥大化しているので、使用頻度は非常に高くなっている。しかし、セキュリティの事故は増加傾向にある上、事故発生による損害金額も高額になっている。さらに、他社に対する信用の失墜という深刻な問題も多々発生している。

IT インフラの高度化と使用頻度の増大化により、IT 関係の費用は高額になるはずである。しかし、今の日本の景気はどの会社においてもどん底としか言えない状態であるので、企業もリストラや人員整理に追われる状態である。このため、IT インフラの設備投資は減少する一方であり、また IT インフラに携わる人員も増加がままならない状態である。それゆえ、当社でもそうであるが、IT インフラに携わる人員はいろんな案件を抱えているにも関わらず、日々の業務に大変な労力を強いられている。

当社でも、既存システムの抜本的な見直しを図って、運用・管理コストの削減を実現することは、懸案としてある。しかし、コスト等いろんな問題で、新規投資ができない状態になっている。

本論文では、IT インフラの中でも電子メールに限定して、セキュリティ問題を確認した上で、「インシデントから守り、安全かつ快適に使用するにはどうしたらいいのか」ということをテーマに、ツールの導入も含めて論じてみる。

２．電子メールの問題点

２．１　電子メールのセキュリティ上の問題点

セキュリティについては機密性（confidentiality）、完全性（Integrity）、可用性（Availability）と呼ばれる 3 要素がある。この 3 要素は二律背反の関係にあると考えられる。また 3 要素と並んで大切な問題は、コストである。3 要素とコストを両立させる必要性から、セキュリティは『妥協の産物』といわれているが、どこに妥協点を見つけるかは企業にとって大問題である。

電子メールに潜む主な脅威と脆弱性を整理すると、表１のようになる。

表１　電子メールに潜む主な脅威と脆弱性

種別	脅威	脆弱性	有効的な主な対策
機密性	データの盗難	メールによる書き込み送信	メールの制御
		添付ファイルのメール送信	メールの制御
	データの流出	メールの誤送信	メール送信後のリカバリー策の確立
	フィッシング詐欺	インターネット対策の不備	ウイルス対策、スパムメール対策
完全性	なりすまし	不正メールの受け取り	スパムメール対策
	データの改ざん	保存メールの改ざん	改ざん検知、防止
可用性	ブランド存続	情報漏洩	メールの制御
	データロストによる事業中断	バックアップの不備	アーカイブ

※「@IT ソリューション Live！ In Osaka」資料より

２．２　情報漏洩についての法律

電子メールは、セキュリティ上では「情報漏洩」が重要なキーワードとなっている。電子メールについての内部統制および情報漏洩対策は、次のように法律においても必要性が強調されている。

(1) 内部統制

2008 年 4 月以降、日本版 SOX 法において電子メールの全文保存・保全管理がほぼ必要になる。（金融庁の平成 19 年 10 月 1 日付の内部統制報告制度に関する Q&A では「電子メール等のデータを一律に記録。保存することをもとめているのではない」となっているが、今後の法改正には考慮が必要である。）
また、法務省主導で進められている電子メールの通信記録保存の法案でも、金融関連を中心に電子メールデータの複数保存が既に義務化されている。

(2) 個人情報保護法

個人情報を保有する行政機関、団体、企業などに適切な個人情報の管理を求める法律。

(3) e-文書法

税法や商法、労働法などの各種法令により、民間企業が作成・保存することを義務付けられている文書・帳票類の電磁化（電子的・磁気的）を、一部の例外を除いて一括して認める法律の通称。

(4) 情報セキュリティ管理基準（経済産業省）

管理基準の 6.7.4 項に「電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること」が規定されている。

このように、今までは『各企業の自主努力管理』で済んでいたものが、『法律による義

務化／遵守必』へと変化していることがわかる。

２．３　情報漏洩の原因について

電子メールのインシデントでは、情報漏洩が一番の問題である。

「JNSA2009 年度セキュリティインシデントに関する調査報告書」（以下、「JNSA2009 年の調査報告書」という)にあるデータを元に、情報漏洩の現状を見てみよう。

２．３．１　情報漏洩の概要

表 2 は、2009 年度の個人情報漏洩インシデントの概要データである。

表 2　2009 年 個人情報漏洩インシデント 概要データ

漏洩人数	572 万 1,498 人	（－152 万人）
インシデント件数	1,539 件	（＋166 件）
想定損害賠償総額	3,890 億 4,289 万円	（＋1,532 億円）
一件あたりの漏洩人数	3,924 人	
一件あたりの平均想定損害賠償額	2 億 6,683 万円	
一人あたり平均想定損害賠償額	4 万 9,961 円	

※「JNSA2009 年度セキュリティインシデントに関する調査報告書」より

*1　括弧内は前年比。

「JNSA2009 年の調査報告書」を要約すると次の通りである。

(1) 漏洩件数の 1,539 件は過去最高の件数であり、想定損害賠償総額は約 3,890 億円（＋1,523 億円）と約 1.6 倍にも増加している。これらは、「金融業・保険業」での増加が大きく影響している。

(2) 漏洩人数の約 572 万人（－152 万人）は減少傾向にある。これは、「漏洩人数が 10 万人を超える大規模な個人情報漏洩アクシデント」が 12 件（－7 件）と減少したことが大きく影響している。

このように、インシデントの件数も損害金額も大きく増加している状況からも、セキュリティインシデントに対する適切な対策を、早急に立てる必要があることがわかる。

２．３．２　情報漏洩の原因と経年変化

2009 年度の情報漏洩の原因の経年変化は、図 1 の通りである。

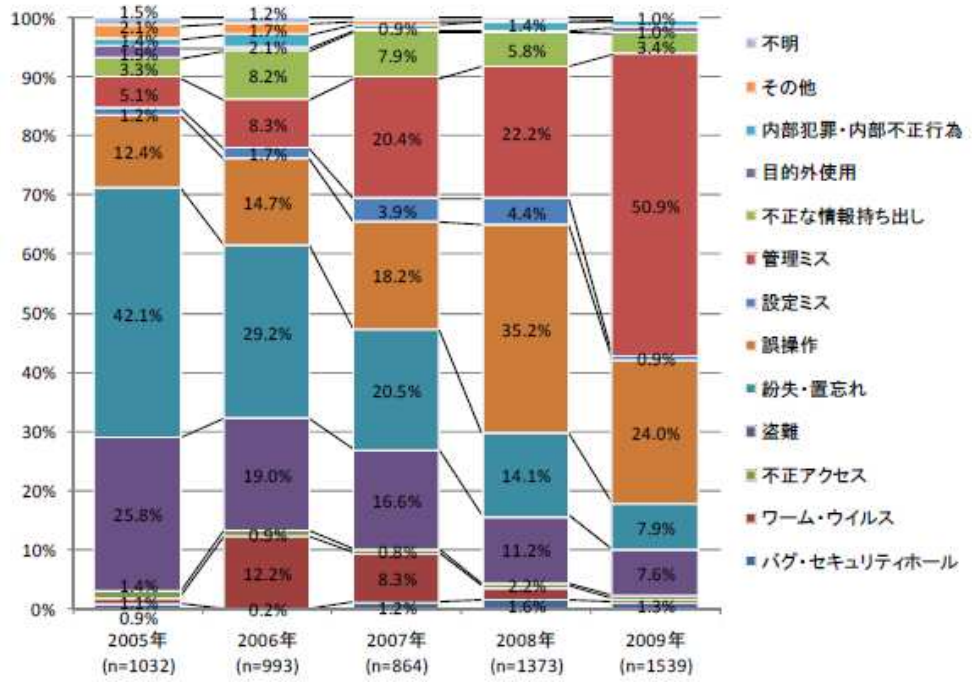

図 1　情報漏洩原因比率の経年変化（件数）

※「JNSA2009 年度セキュリティインシデントに関する調査報告書」より

「JNSA2009 年の調査報告書」を要約すると次の通りである。

(1) 2009 年度は「管理ミス」が原因の約半分を占め、「誤操作」(24%)「紛失・置忘れ」(8%)が続いている。

(2) 2008 年度と 2009 年度を比べると、「管理ミス」は 22.2%⇒50.9%と 2.3 倍も増加しているのに対し、「誤操作」は 35.2%⇒24.0%と 2/3 に減少し、第 1 位が交代している。

(3) 「管理ミス」が大きく増加したのは、全組織的な内部統制とコンプライアンスの意識が浸透したことによることが原因のひとつとなっている。

(4) 「誤操作」は電子メールの宛先間違いが多く、「紛失・置忘れ」は、社外でのノートパソコン、電子媒体や紙ファイルの紛失が多い。これらは人間系のエラーであるが、これに対しては、担当者へのセキュリティ教育が不可欠であるが、組織的な対策も考慮する必要がある。

(5) 「誤操作」「紛失・置忘れ」「盗難」「不正な情報持ち出し」の件数は減少しているので、これらのインシデント対策の効果が出ている、と考えられる。

(6) 2005 年から 2009 年の全体の傾向をみると、社外でのインシデントの原因となる「紛失・置忘れ」が減少傾向にあるので、これはうまくいっていると思われる。但し、社内のインシデントの原因である「管理ミス」が増大傾向にあるので、今後は社内の対策を考慮しなければならないことを示している。

３．電子メールのセキュリティの考え方

電子メールのインシデントの原因と対策を整理すると、表３のようになる。

表３　電子メールのインシデントの原因と対策の例

項目	インシデントの原因	対策
情報漏洩(*1)	中間者攻撃による盗聴	電子メールの暗号化(PGP、S/MIME 等)
	添付ファイルの電子メール送信	電子メールの施行ルールの確立
		フィルタリングソフトの導入
	メール誤送信	電子メール送信先の確認の徹底
	運用ルールの浸透不足	注意喚起
スパムメール・ウィルス	不正メールの受け取り	スパムメール対策ソフトの導入
	サーバを踏み台にしたスパムメールの送信	「POP before SMTP」または「SMTP-AUTH」の導入
アーカイブ	電子メールの紛失	電子メールの保存 メールアーカイブソフトの導入
	データの改ざん	

※「@IT ソリューション Live! In Osaka」資料より

*1　この他、スパムメール・ウィルスで情報漏洩が発生する場合があるが、この表では「スパムメール・ウィルス」の項目にまとめた。

表３に挙げた電子メールのインシデント対策について、問題点を考えてみよう。

(1) 電子メールの暗号化

a.「盗聴を防ぐには暗号化メール」これは定石である。また、SSL を利用した暗号化メールでは、次のメリットもある。

- 通信経路を暗号化するので、盗聴ばかりでなく、なりすましや改ざんといった被害も防げる。

b. 但し、次のことに注意する必要がある。

- 送信メールと同時に復号キーを送信すれば、メール受信と同時に解読が可能になるので、メール送信先を間違えれば情報漏洩することになる。これを防ぐには、「送信メールと複号キーは同時に送信しない」といったメール送信ルールの確立が必要である
- 暗号化を行うと、メールアーカイブ、ウィルスチェック および メッセージフィルタリングができなくなるので、これらは暗号化の前に実行する必要がある。

(2) フィルタリングソフトの導入

フィルタリングソフトは、「100%確実なソフトはない」ということに注意しなくてはならない。というのは、次のような場合が必ず発生する。

a. 誤検出：フィルタリングエラーでないのに、エラーと検出した場合

b. 非検出：フィルタリングエラーなのに、エラーでないと検出した場合

(3) スパムメール対策ソフトの導入

スパムメール対策ソフトでも、(2)であげた問題は発生する。また、スパム判定されたメールの確認作業を人間が行う場合は、

a. 管理者が確認する場合

管理者の作業が膨大になるので、ノーチェックか全削除になってしまう可能性がある。

b. 作業者が確認する場合

スパムメールの洪水となり、作業効率の低下、業務メールの見落としが発生する。また、HDD の浪費のため、ムダなハードウェア投資が発生する。

(4) 「POP before SMTP」または「SMTP-AUTH」の導入

これらは、電子メールを送信するためのプロトコルである SMTP に認証機能を持たせるものである。サーバを踏み台としたスパムメールやウィルスの送信による被害の拡大を起こさないためにも、これらの機能が必要となる。

(5) 電子メールの保存 および メールアーカイブソフトの導入

a. 電子メールのアーカイブは次のために必要である。

- PC がクラッシュ等によるメール消失の場合の復元
- 電子メールによる情報漏洩の証拠のチェック
- メールデータの改ざんチェック

b. 2.2 でも示したように、電子メールの保存は法的な要請となってきている。

c. 一般にメールアーカイブには専用ソフトを用いるが、次の問題点もある。

- メールアーカイブによるディスクの消費量が嵩む場合等、ネットワークやディスクに負担がかかる場合がある。
- 暗号化したファイルではアーカイブしても監査ができくなるので、「暗号化前にアーカイブする」という送信ルールの確立が必要である。

(6) 電子メールの施行ルールの確立

(7) 電子メール送信先の確認の徹底

(8) 注意喚起

a. これらは、人間系のエラーである。2.3.2 でも述べたが、人間系のエラーに対しては、次の 2 つの対策が必要とされる

- 社員に対するセキュリティ教育による社員のセキュリティレベルの向上
- 電子メール送信先の間違いに対する組織的な対策

b. 電子メールの施行ルールは、程度を考慮する必要がある。というのは、

- 電子メールの施行ルールを厳しくしすぎると、従業員に大きな負担がかかり、作業効率を損なうこととなる。このような場合は、遵守しない従業員も出てきて、施行ルールが有名無実化してしまう恐れがある
- 反対に、電子メールの施行ルールが甘いと、インシデントが発生する危険性が高くなるので、これではセキュリティの意味がなくなる。

c. 組織的な対策が必要な理由は、次の通り。

- どんな施行ルールをとっても、うっかりによる操作ミスは必ず発生する。

d. 操作ミスに対する組織的な対策は、フィルタリングソフトの導入等が考えられるが、完璧にできるものではない。完璧に近い状態にしようとするならば、専用ツールの導入が不可欠である。

４．電子メールのセキュリティツール

この章では、電子メールのセキュリティツールを導入することにより、セキュリティ問題を解消する方法を考えよう。前章でも述べたが、電子メールのセキュリティツールでは次の機能が必要となる。

(1) 情報漏洩防止機能
暗号化ソフト使用による暗号化メールでも、経路での情報漏洩は防げる。
しかし、メール送信先の間違いによる情報漏洩を防ぐには、セキュリティツールが必要である。

(2) 電子メールのアーカイブ
アーカイブは、情報漏洩の証拠チェックや改ざんチェックに必要である。
但し、アーカイブは暗号化前に行う必要があるので、確実な形で実現するには、セキュリティツールが必要である。

(3) スパムメール・ウィルスの防止機能
スパムメール・ウィルス対策ソフトは様々な製品が市販されている。
但し、ウィルスチェックは暗号化前に行う必要があるので、確実な形で実現するにはセキュリティツールが必要である。

尚、当社の現状は、次の通りである。

(1) スパムメール・ウィルス対策には、専用ソフトを導入している。
(2) 暗号化ソフト使用による暗号化メールは行っているが、その前にウィルスチェックを行うことはしていないので、ウィルス対策は確実ではない。
(3) メール送信先の間違いによる情報漏洩防止やメールのアーカイブは行っていない。

よって、当社もメールセキュリティを確実な形で行うには、セキュリティツールが必要である。

メールセキュリティツールは、様々な製品またはサービスが販売されている。本論文では、次の２つのツールの導入を提案し、導入メリットの比較を行う。

(1) 「m-FILTER」Ver.2.8（以下、「m-FILTER」で記述。デジタルアーツ㈱の製品）
メールサーバにインストールするソフトウェアである。
(2) 「Mail Luck!」（㈱NTTPC コミュニケーションズのサービス）
SaaS 形式でアウトソーシングサービスである。

本論文で、この 2 つのツールを取り上げた理由は次の通り。

(1) 2 つのツールは、両方とも次の導入メリットがある。
a. 上記に挙げた、3 つの電子メールのセキュリティツールとしての必要事項が確実な方法で実現できる。
b. メール送信に特別な操作が必要でないので、施行ルールは簡単である。作業者や管理者の負担も少ないので、導入に対する抵抗感も少ない。
c. 導入費用が妥当な価格である。

４．１　「m-FILTER」の導入について

「m-FILTER」は、メールサーバにインストールするソフトウェアである。このソフトウェアの機能は、表４のとおりである。

表４　「m-FILTER」の機能

機能	製品名	解消できるインシデント	機能の詳細
電子メールの送受信制御	m-FILTER MailFilter	情報漏洩	ウィザード形式の簡単なルール設定
			添付ファイル自動パスワードロック機能
			うっかり誤送信防止機能
			複数管理者承認機能
電子メールの全文保存と検索	m-FILTER Archive	アーカイブ	メールアーカイブ（保存）機能
			検索機能
			改ざん検知機能
スパムメール対策	m-FILTER Anti-Spam	スパムメール・ウィルス	スパムメールフィルタ機能

※「m-FILTER」Ver.2.8 ご紹介 資料より

*1　「m-FILTER」の製品には３つの機能をセットした「フルセット」という製品がある。以下、この論文では「m-FILTER」はフルセットを対象とする。

４．１．１　「m-FILTER」の各機能

(1)　添付ファイル自動パスワードロック機能（m-FILTER MailFilter）

図 2 に示すファイル送信システムであり、当社で行っていない情報漏洩対策として一番重要な機能である。

図２　添付ファイル自動パスワードロック機能

※「m-FILTER」Ver.2.8 ご紹介 資料より

この機能では、次のことが解決できる。

a. 送信メールは暗号化されているので、情報漏洩の心配がない。

b. 送信先へのパスワード送信はメール本体と別に送信するので、電子メールの宛先

を間違えた場合でも、送信先へのパスワードの送信をしなければ、相手先には内容がわからない。

c. 「m-FILTER」までのメール送信はパスワードなしとしている。これは、この状態でウィルスチェックとアーカイブを行えるようにするためである。

(2) うっかり誤送信防止機能（m-FILTER MailFilter）

「m-FILTER」に電子メールを一定時間サーバに保留しておく機能。誤送信に気づいた場合は、保留中ならば送信者自ら削除が可能となる。

(3) 複数管理者承認機能（m-FILTER MailFilter）

複数の管理者がすべて承認した場合のみ、電子メールの送信可能とする機能。管理者の「うっかり」にも対応できる。

(4) ダウンロードアーカイブ機能（m-FILTER Archive）

外部への電子メールだけでなく、内部の電子メールも簡単に保存する機能。社内における情報漏洩対策になる。

(5) 保存メールの改ざん検知機能（m-FILTER Archive）

アーカイブした電子メールの改ざんチェックをする機能。（改ざん防止はできない）

(6) バックアップのスケジュール機能（m-FILTER Archive）

「毎週土曜日の深夜にバックアップ処理を行う」といった、バックアップのスケジュール化を行う機能。管理者の作業負担が大幅に軽減される。

(7) スパムメールの個人判断機能（m-FILTER Anti-Spam）

図 3 に示す方法で、各人宛の電子メールを選択受信する機能である。

図 3 スパムメールの個人判断機能

※「m-FILTER」Ver.2.8 ご紹介 資料より

この機能では、前章のスパムメール対策ソフトの問題が解決される。というのは、

a. 管理者側はメールフィルタリングの必要がないので、作業負担が軽減される。

b. ユーザー側は、電子メールを作業領域から選択してメール受信を行うので、正規の電子メールの受信漏れがなくなる。

４．１．２　「m-FILTER」の価格

「m-FILTER」の価格を表５に示す。

表５　「m-FILTER」（フルセット)の価格(抜粋)

ﾗｲｾﾝｽ	標準価格	保守価格
100	1,511,250	257,000
250	2,245,500	382,000
500	2,816,250	479,000

※「m-FILTER」Ver.2.8 ご紹介 資料より

*1　ライセンス数は接続するパソコン数である。
*2　標準価格は購入時の価格であり、保守価格はメインテナンス料として毎年支払う金額である。
*3　「m-FILTER」は、メールサーバ数に制限がない。複数の事務所があって、各事務所にメールサーバがある場合でも価格は同じである。

当社は従業員約 300 名なので、ライセンス数が 100／250／500 の例を示した。
500 ライセンスを考えると、購入費用が約 282 万円、保守費用は年間約 48 万円となる。
これを、償却期間を 1～5 年で考えると、導入費用（購入費用と保守費用の合計費用）は表６の通り。

表６　「m-FILTER」(500 ライセンスのフルセット)の導入費用

償却期間	１年	２年	３年	４年	５年
月間費用	27.5	15.8	11.8	9.9	8.7

(単位：万円)

*1　月額費用は、購入費用と保守費用の合計費用を月割にした値を示す。

４．１．３　「m-FILTER」の評価

＜機能面の評価＞

機能面は下記の通りメリットが大きいので、当社でも導入の価値があると思われる。

(1)　電子メールの送受信制御（m-FILTER MailFilter）
  a. メール送信手順は、情報漏洩を防ぐ方法として最適である。しかも、メール送信はパスワードを別便で送信するだけの単純なルールなので、導入に対して抵抗を感じない。
  b. 「うっかり誤送信防止機能」や「複数管理者承認機能」で従業員のうっかりを防ぐ機能もある。これは、2.3.2 で述べた組織的な対策にもなっている。
  c. このように、情報漏洩を、単純な送信ルールで実現している上、組織的な対策も考慮しているので、導入のメリットは非常に大きい。
  d. 当社では、このような情報漏洩に対する具体的な対策を行っていない。セキュリティでも最重要項目である情報漏洩対策には、このようなツールが必要である。
(2)　電子メールの全文保存と検索（m-FILTER Archive）

a. アーカイブの目的である「情報漏えいの証拠チェック」や「電子メールの改ざんチェック」を社内メールも含めて難なく行える。
b. 第 3 章で「アーカイブはツール導入が必要」ということを述べた。「m-FILTER」では、管理者の負担が少ない状態でできるので、導入のメリットは大きい。
c. 当社ではアーカイブは行っていない。メールセキュリティ対策として、このようなツールは必要である。

(3) スパムメール対策（m-FILTER Anti-Spam）

a. スパムメール対策もメールセキュリティ対策として必須の項目である。「m-FILTER」では効率よいスパム判定が可能である。
b. さらに、「スパムメールの個人判断機能」は管理者／作業者共に負担が軽減される上、正規のメールの受信漏れも防げる。
c. 第 3 章で「スパムメール対策はツール導入が必要」ということを述べた。「m-FILTER」では、高効率である上、高精度の判断もできるので、導入のメリットは大きい。
d. 当社ではスパムメール・ウィルス対策は行っているが、「ウィルスチェックは暗号化前に行う」という施行ルールがないので、このようなツールは必要である。

(4) 機能のアップデートについて

a. セキュリティ（特に、スパムメール・ウィルス）は、日々新たな脅威が発生しているので、それに対応しているかということも留意点である。「m-FILTER」では、保守価格でバージョンのアップデートも行うことができるので、この点は大丈夫である。

＜価格面の評価＞

価格面では、次のことに注意しなければならない。

(1) 購入金額の 282 万円は決して安価でないので、長期間使用することを考える必要がある。（表 6 で示したように、1 年償却では月額 25.5 万円、2 年償却では 15.8 万円、3 年償却では 11.8 万円である）セキュリティ対策としてのインシデント費用としては、3 年位を考えると妥当なコストと思われる。

＜その他の問題点＞

「m-FILTER」では、機能／コスト以外に次の問題点がある。

(1) 購入金額が必ずしも安価ではないので、一度購入すれば他の商品（またはサービス）に変えるとムダが発生する。（償却を終了した場合は別であるが）
(2) 「m-FILTER」は接続パソコン数単位なので、メールを使用するパソコンを制限しなければ、ライセンス数にムダが生じることを考慮しなければならない。

４．２　「Mail Luck!」 の導入について

「Mail Luck!」は、SaaS 形式のメールサーバのアウトソーシングサービスである。
このサービスには次の 4 タイプがある。

(1)　セキュアタイプ（略称「Ｓ」）
　　メールサーバを「Mail Luck!」内に作成するシステムであり、メールセキュリティ強化のための機能(*1)がついている。

(2)　インターネットタイプ（略称「Ｉ」）
　　メールサーバを「Mail Luck!」内に作成するシステム。

(3)　セキュアタイプゲートウェイタイプ（略称「ＳＧ」）
　　自社内のメールサーバを流用するシステムであり、メールセキュリティ強化のための機能(*1)がついている。

(4)　ゲートウェアタイプ（略称「G」）
　　自社内のメールサーバを流用するシステム。

*1　「メールセキュリティ強化のための機能」は次の通り。(表 7 参照)
　(1)　添付ファイルセキュリティ機能
　(2)　監査保存機能

「Mail Luck!」の各機能は、表 7 の通り。

表 7　「Mail Luck!」の機能

機能名称	機能の説明	対応タイプ
添付ファイルセキュリティ	誤送信の大きな原因である、添付ファイルによる情報漏洩を防ぐ。次のサブ機能がある。 ・添付ファイルの誤送信防止機能	「S」 「SG」
監査保存機能	従業員のすべての電子メールを添付ファイルを含めて別領域に複製保存する。次のサブ機能がある。 ・メールアーカイブ ・メール検索 ・メール監査（フィルタリング）	「S」 「SG」
アクセスセキュリティ	アクセス元 IP 制限で電子メールを送受信できる利用環境を制限できる。	「S」
WEB メール	社外からの利用時に高いセキュリティを確保する、高性能な WEB メールを提供する。	「S」 「I」
スパム・ウィルス対策	世界最高水準の検索エンジンを搭載し、的確にスパム・ウィルスを検知し、クリーンな電子メールだけをお客様に届ける。次のサブ機能がある。 ・スパムフィルタ機能 ・ウィルスチェック機能	「S」 「I」 「SG」 「G」

※　NTTPC「Mail Luck!」資料より

以下、本論文では「Mail Luck!」は「Ｓ」タイプを対象とする。

４．２．１　「Mail Luck!」の各機能

(1)　添付ファイルの誤送信防止機能（添付ファイルセキュリティ）

図４に示す、当社で行っていな情報漏洩を考慮したファイル送信システムである。

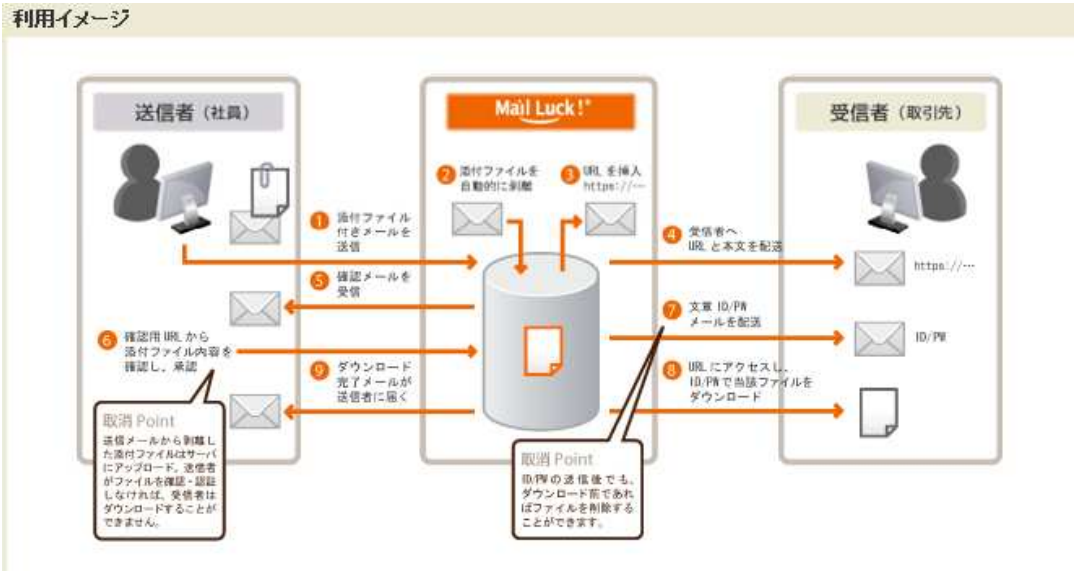

図４　「Mail Luck!」でのメール送信方法

※　NTTPC「Mail Luck!」資料より

この機能のメリットは次の通り。

a. メール送信時には、ファイル暗号化は不要である。（「Mail Luck!」サーバで暗号化を実行する。）

b. 「Mail Luck!」サーバでは、添付ファイルを剥離し、添付ファイルのダウンロード用 URL を本文に挿入し送付する。URL アクセスのための ID およびパスワードは別メールで送付する。（この方法ゆえ、相手側のメールサーバのサイズに関わらずメール送信が可能である。）

c. 「Mail Luck!」への送信も、受信者へのメール送信も、SSL と HTTPS を使用した暗号化送信をしているので、通信経路での盗聴の心配がない。

d. 人的ミスも防ぐ情報漏洩対策として、次の 2 つの方法が可能である。

- 添付ファイル内容を確認しない限り、ID／パスワードが受信者へ送付されない。
- ID／パスワードが受信者に送信された後でも、ファイルのダウンロード前では、ファイルを削除することができる。

e. 「どこに、どんな添付ファイルが送信され、誰がどの電子メールを承認（確認）したのか」という承認（確認）履歴・ダウンロード履歴が残る。承認ミスまたは承認ポリシー違反もチェックできる。

f. メール送信機能を応用すると、重要文書の保存も可能である。これは、重要文書を「Mail Luck!」サーバ内に保管しておくことにより、外部への情報漏洩を防止することもできるからである。

(2)　メールアーカイブ／メール検索機能（監査保護機能）

送受信すべての電子メールを別領域で完全保存する機能。暗号化されていない状態で

保存しておくので、監査にも耐えられる。

(3)　メール監査（フィルタリング）機能（監査保護機能）

フィルタリング機能により、送受信や情報漏洩を水際でブロックする。

(4)　アクセス元 IP 制限（アクセスセキュリティ）

指定されたグローバル IP アドレスからのみ送受信可能にすることにより、情報漏洩やウィルス感染した PC からのアクセスを防止することができる。

(5)　WEB メール

WEB メールを使用すると、社外からもアクセス可能になる。

「Mail Luck!」では、SSL を使った通信により、インターネットからのアクセス時の通信を暗号化する。基本的にメールデータを端末にダウンロードしない為、端末の盗難・紛失時の情報漏洩リスクを軽減する。

(6)　スパムフィルタ機能（スパム・ウィルス対策）

言語の種類に関係なく、高い検知機能にてスパムメールよる脅威を防御する。

(7)　ウィルスチェック機能（スパム・ウィルス対策）

利用実績の高い Symantec 社のアンチウィルスエンジンを標準搭載し、ウィルスメールから防御する。

4．2．2　「Mail Luck!」の価格

「Mail Luck!」の価格を表 8 に示す。

(当社は従業員約 300 名なので、メールアドレス数が 100／300／500 の例を示した。)

表 8　「Mail Luck!」(「S」タイプ)の価格(抜粋)

初期費用	
項目	金額
初期費用	¥315,000／FQDN
SSL 証明書	¥161,595／FQDN
ID/PW データ移行費	¥105,000 ／1,000ID まで
接続 IP 制限	¥21,000／作業

月額費用		
ﾒｰﾙ ｱﾄﾞﾚｽ数	保存領域	金額
100	20GB	¥283,500
300	60GB	¥367,500
500	100GB	¥472,500

*1　初期費用の SSL 証明書は、WEB メール及び監査・保存管理用サイトの証明書であり、毎年更新費用が発生する。

4．2．3　「Mail Luck!」の評価

＜機能面の評価＞

機能面は下記の通りメリットが大きいので、当社でも導入の価値があると思われる。

(1) 添付ファイルセキュリティ

a. 「Mail Luck!」のメール送信方法は、暗号化通信と承認機能の両方で情報漏洩を防止していることが重要である。承認機能は、2.3.2 で述べた組織的な対策にもなっている。

b. 添付ファイルを URL でアクセスするので大容量のファイルの送信も可能である。

つまり、相手先のメールサーバ容量にも配慮している、ということである。

c. しかも、作業者側から見れば、メール送信は送信者の承認と ID／パスワードの相手先への送信だけの単純なルールであるので、抵抗を感じない。

d. このように、セキュリティでも最重要項目である情報漏洩を、単純な施行ルールで確実な方法で実現している上、組織的な対策も考慮しているので、導入のメリットは非常に大きい。

e. 当社では、このような情報漏洩に対する具体的な対策を行っていない。セキュリティでも最重要項目である情報漏洩対策には、このようなツールが必要である。

(2)　電子メールの送受信制御

a. アーカイブは、メールの監査（情報漏洩の証拠チェックや改ざんチェック）を行えるので、セキュリティ対策として重要な項目である。。

b. フィルタリング機能は、セキュリティとしても最重要項目である情報漏洩対策を行える。

c. このように、セキュリティで重要な項目である、アーカイブとフィルタリング機能を同時に実現する機能なので、導入のメリットは非常に大きい。

d. 当社ではアーカイブやフィルタリングは行っていない。メールセキュリティ対策として、このようなツールは必要である。

(3) アクセスセキュリティ

a. この機能も情報漏洩に対応しているが、重要度は(1)(2)よりは低いので、導入のメリットはそれほど大きくないと思われる。

(4) Web メール

a. Web メールは当社でも使用している。社外からメールサーバにアクセスする場合に必要であり、社外勤務者や外回りの営業ではこれがないと仕事が捗らない。

b. Web メールは社外で使用するのでセキュリティの問題があるが、「Mail Luck!」は高セキュリティであるので大丈夫である。

c. このように Web メールが可能であることは、導入のメリットが大きい。

(5) スパム・ウィルス対策

a. スパム・ウィルス対策もメールセキュリティ対策として必須の項目である。

b. 第 3 章で「スパム・ウィルス対策はツール導入が必要」ということを述べた。「Mail Luck!」では、この機能を高能率で行っているので、導入のメリットは大きい。

c. 当社ではスパムメール・ウィルス対策は行っているが、「ウィルスチェックは暗号化前に行う」という施行ルールがないので、このようなツールは必要である。

＜価格面の評価＞

価格面では、次のことに注意しなければならない。

(1)　メールアドレス数 300 の場合では、初期費用は約 60 万円、月額費用（SSL 証明書の年間更新費用を含む）は約 38 万円である。

(2)　「Mail Luck!」は、SaaS 形式のアウトソーシングによる次のメリットがある。

a. 自社にメールサーバを持つ必要がないので、メールサーバの維持費用及び空調費用がいらなくなる。また、「Mail Luck!」では、365 日 24 時間の保守・運用を

行っているので、サーバを管理している情報システム部員の手間も大幅に削減できる。

b. 「Mail Luck!」のサービス品質は、SaaS 業界最高品質であるので、メールサーバの信頼性も自社のメールサーバより高い。

c. Web メールが可能であることも、優れていることのひとつである。

d. このように、メールサーバの維持費用及び空調費用、情報システム部員の手間といったメリットがある。月額費用 38 万円は確かに安価ではないが、これらの費用や手間を考慮するならば妥当ではないか、と思われる。

e. SaaS 形式であるということは、新しいサービスに切り替えることも簡単であるというメリットもある。

4．3 「m-FILTER」と「Mail Luck!」の比較

では、「m-FILTER」と「Mail Luck!」を比較してみよう。（条件は「m-FILTER」は 500 ライセンス、「Mail Luck!」は 300 メールアドレスとする。）

(1) 「m-FILTER」は毎月 27.5 万円（1 年間償却）／11.8 万円（3 年間償却）に対して、「Mail Luck!」は毎月 43 万円（1 年間償却）／39.6 万円（3 年間償却）である。コストは、「m-FILTER」のほうが安い。

(2) 両者とも、セキュリティツールとしての重要な機能である、次の項目は確実な方法で実現できる。

a. 情報漏洩の防止のための承認機能

b. メールの暗号化通信機能（復号キーは別メールで送信するので、送信間違いによる情報漏洩も防げる）

c. 電子メールのアーカイブ機能（暗号化していない状態で行うので、監査も可能である）

d. スパムメール・ウィルスの防止機能（ウィルスチェックは、暗号化していない状態で行うので確実である）

(3) 機能を比較すると、「Mail Luck!」のほうが次の点で優れている。

a. ツール導入のポイントであるメール送信間違いの防止機能は、「m-FILTER」より「Mail Luck!」の方が確実である。

b. 「Mail Luck!」は URL アクセスを用いるので、相手先のメールサーバ容量に関係なく大容量の添付ファイルの送信も可能である。

(4) 「Mail Luck!」は、SaaS 型のサービスであるので、次のメリットがある。

a. 自社のメールサーバをもたないので、維持費用及び空調費用、さらにはメインテナンスに携わる要員の人件費が節約できる。（この費用によっては「Mail Luck!」のほうが安くなる。）

b. 「Mail Luck!」では、Web メール使用により外部のパソコンよりアクセスしても使用料金が変わらない。「m-FILTER」では、外部のパソコンよりメールサーバにアクセスすることになるので、ライセンス数のムダにつながる。

(5) 私は 2 つのツールを比較すると、次のことがいえると思う。

a. コストを抑えるならば、「m-FILTER」のほうが優れている。

b. ある程度コストを掛けても確実なシステムを構築したいならば、「Mail Luck!」

を導入すべきである。

c. 当社では、確実なシステム構築できることと SaaS 型のサービスのメリットがあることを考慮するならば、「Mail Luck!」の方がお勧めである。

５．おわりに

本論文では、IT インフラの中でも電子メールに限定して、セキュリティ問題の解消方法をセキュリティツールの導入も含めて論じてきた。「アクシデントが発生してからでは遅い」これは肝に銘じておかなければならないことである。

電子メールのセキュリティでは情報漏洩の問題が重要である。情報漏洩の一番の原因は人間系のエラーである。この対策には、従業員のセキュリティレベルの向上も大切であるが、どんな方法をとっても従業員のうっかりだけはどうしても避けられないものである。そこで、セキュリティツールの導入という方法を提案した。本論文で挙げた「m-FILTER」と「Mail Luck!」は、承認機能をもたせることにより、人間系のエラーに対処するツールである。

承認機能は情報漏洩のリスクを軽減するものであるが、100%の情報漏洩は防げるものではない。(例：すべての承認者が間違いを起こした場合)これは、使用する人間に関わる問題であるから、ツールを導入したとしても、従業員のセキュリティレベルの向上はかかせない。

もちろん、電子メールのセキュリティツールはこの 2 つだけでないし、電子メール以外の IT インフラのセキュリティ問題も解消する必要がある。最後に、IT インフラについては、コストと機能を考えて、よりよい環境を構築することが必須であることも述べて本論文を完了する。

参考文献

[１] JNSA2009年度セキュリティインシデントに関する調査報告書 第1.0版
NPO日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ

[２] 「m-FILTER」Ver2.8ご紹介
デジタルアーツ株式会社（2009.11）

[３] メールサーバのアウトソーシングなら Mail Luck!（ホームページ）
http://www.luckda.net/

[４] @IT ｿﾘｭｰｼｮﾝ Live! In Osaka　セミナー資料
アイティメディア株式会社主催（開催日：2009/12/9）

[５] 持たずに使う IT、クラウドインテグレーションのインパクト！セミナー資料
パナソニック電工インフォメーションシステムズ株式会社主催（開催日：2010/1/25）