

## スパムメール対策システムの更新

和田 大樹 (ネットワンシステムズ株式会社)

hr-wada@netone.co.jp

### 1. はじめに

インターネットの普及により多くの人が、様々なインターネット上のコンテンツにアクセスできるようになり、今では人々の娯楽の一部となっています。その一方で悪質な有害コンテンツの配信を行う人、業者が存在するのも事実であり、スパムメールと呼ばれる迷惑メールもその一部です。弘前大学様では今までもスパムメール対策システムを導入し、自動隔離・自動削除を行なってきておりました。

しかし、その検知率が芳しくなく「正常なメール」を「スパムメール」と検知してしまったり(誤検知)、または「スパムメール」を検知できず「正常なメール」としてユーザに送られてしまったりすることがたびたびありました。

そのため、弘前大学様では昨年の学内LAN更新に合わせて、新たな対策システムとして「スパムメール対策装置」を導入し、その対処機能の改善を図られました。

本報告では、新しいスパムメール対策の「概要」と、スパムメールと認定され隔離されたメールの確認・復元(リリース)・削除方法を紹介します。さらに、システムの使い勝手を向上させる「セーフリストとブロックリストの機能および設定方法」も紹介します。

### 2. スパムメール対策

#### 2.1. スパムメール(迷惑メール)とは

そもそも、スパムメールを定義することは困難ですが、一般的には受信者の意思に関係なく送信されてくるメールのことを指し、チェンメールから始まり、クレジットカード番号、住所を収集するフィッシング詐欺が目的のもの、架空請求、匿名による嫌がらせ、マルウェア(ウイルス、スパイウェア、トロイの木馬など)の拡散が目的の物、と多種多様なスパムメールが存在します。また受信者が加害者になりうる場合もあり、見逃せない問題となっています。

スパムメールを受信した場合の対処法としては、無視(読まない、開かない)、または手作業による削除、なんらかのツールを使用して自動振り分け・自動削除といったものがあります。

誤って返信をしてしまうと送信者に“受信できる”ことを確認されてしまい、それ以降そのメールアドレスに対して大量のスパムメールが送られてくるようになってしまいます。

#### 2.2. スパムメール対策の概要

一般的に学外からのメールは、メールを管理しているPOPサーバに直接届きます。そのため、その中に含まれるスパムメールも当然ユーザに直接届いてしまいます。

本対策後の、学外から届くメールの処理フローを図1に表しました。今回の対策では、POPサーバの手前にスパムメール対策機器を置くことにより、まずすべてのメールをスパムメール対策機器で受信します。そしてその段階で「スパムメール」とそれ以外の「正常なメール」の振

り分けをおこない、スパムメールは隔離し、正常なメールのみをPOPサーバに届ける仕組みになっています。

問題はその検出『精度』となってきますが、今回導入した機器は、その製造元が運営している“世界最大規模で世界のメールサーバを監視するシステム”が作成したデータベースを参照しているため、スパムメールの検出精度は非常に優秀です。また、その精度をさらに高めるために弘前大学様用にチューニングも施されており、誤検知率は一層低くなっているはずですが、現に2011/01/11 執筆時点で運用を開始して1ヵ月が経過していますが、誤検知の報告はまだあがってきておりません。

ただし、医学用語などの専門用語を使用したメールに対しては検出精度が下がってしまいます。これにより誤検知を起こす可能性がまったくないわけではないということは記述させていただきます。

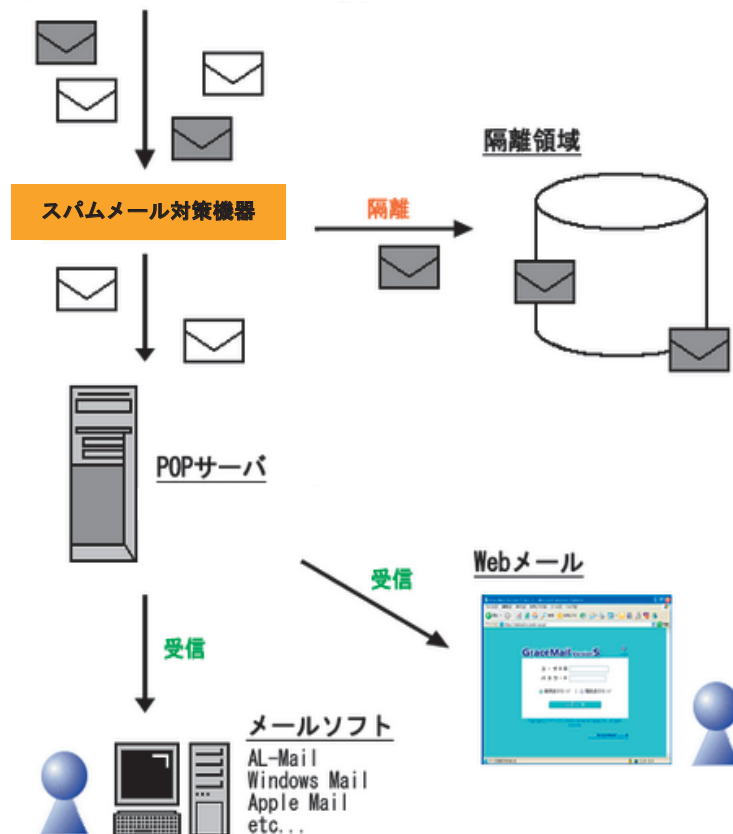


図1 学外からの届くメールの処理フロー図

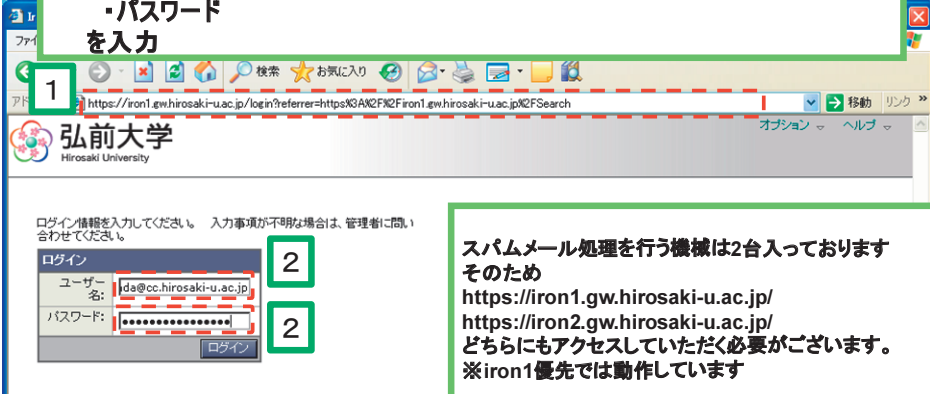
### 2.3. 隔離されたメールの確認・復元（リリース）・削除方法

隔離されたメールの確認・復元・削除の操作方法を次ページ以降の図にて説明します。ただし削除は自動的におこなうようセットしているので必ずしも手動で行う必要はありません。まず図2に示す通り、スパムメール対策機器にアクセスします。

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### 1. 隔離メール処理ページへアクセス

1. <https://iron1.gw.hirosaki-u.ac.jp/>と  
<https://iron2.gw.hirosaki-u.ac.jp/>にアクセス
2. アカウント申請時に取得した
  - ・メールアドレス
  - ・パスワード
 を入力



スパムメール処理を行う機械は2台入っております  
そのため  
<https://iron1.gw.hirosaki-u.ac.jp/>  
<https://iron2.gw.hirosaki-u.ac.jp/>  
どちらにもアクセスしていただく必要があります。  
※iron1優先では動作しています

Net One Systems

Copyright ©2010 Net One Systems CO.,LTD. All rights reserved.

19

図2 隔離メール処理ページへアクセス

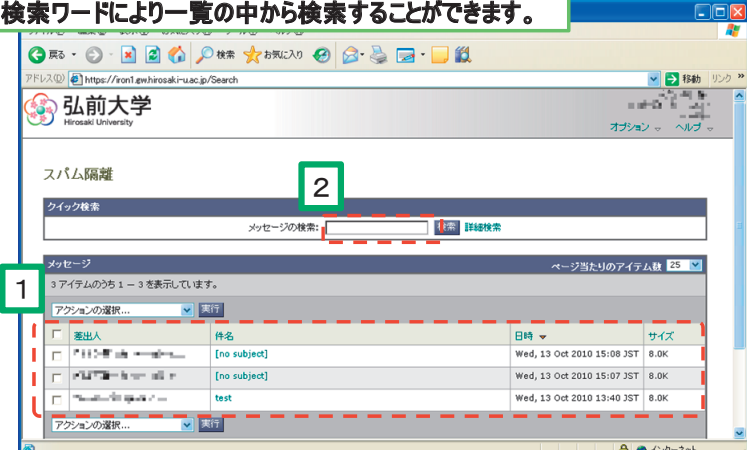
ログイン後のトップ画面は図3のようになります。

この画面では隔離されたメールの一覧を確認することができます。

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### 2. 隔離メールの一覧・検索画面

1. 保存されている隔離メールが一覧表示されます
2. 検索ワードにより一覧の中から検索することができます。



送出入	件名	日時	サイズ
[no subject]	[no subject]	Wed, 13 Oct 2010 15:08 JST	8.0K
[no subject]	[no subject]	Wed, 13 Oct 2010 15:07 JST	8.0K
test	test	Wed, 13 Oct 2010 13:40 JST	8.0K

Net One Systems

Copyright ©2010 Net One Systems CO.,LTD. All rights reserved.

20

図3 トップ画面

隔離メールの確認と復元・削除方法は2つあります。

1つ目は、図4、5の手順で示す方法です。

※メールの保持期間は30日間に設定されているため、必ず「削除」する必要はありません。

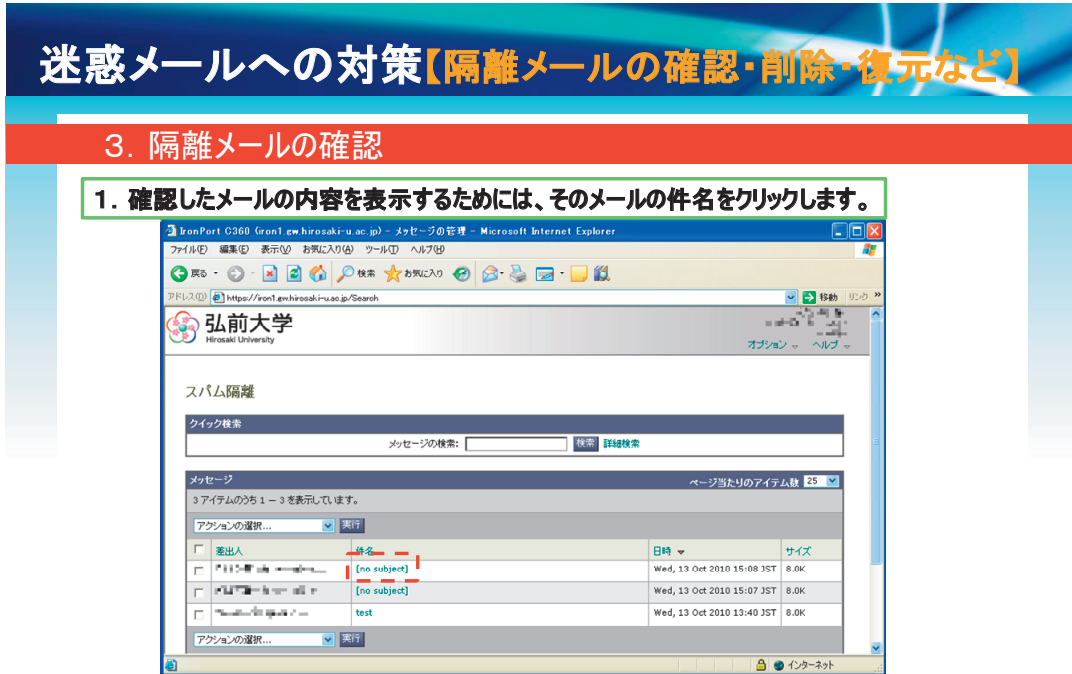


図4 隔離メール確認

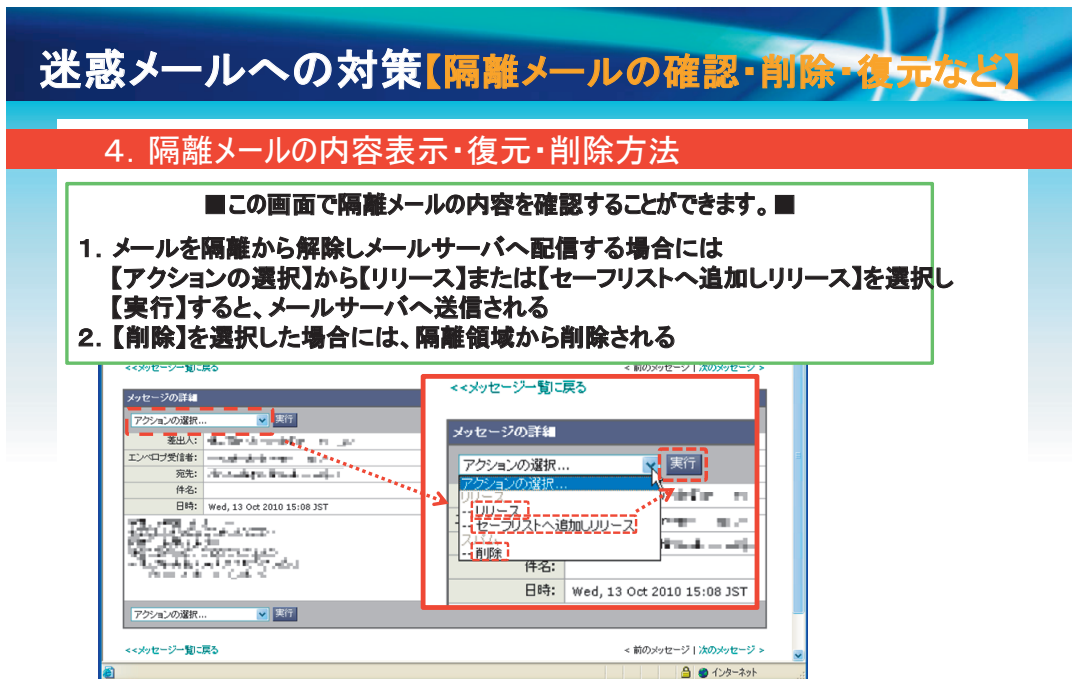


図5 隔離メールの処理1

2 つ目は図6 に示す方法です。これはメールの内容確認を省略した方法です。

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### 5. 隔離メールの復元方法2

1. 復元・削除したいメールのチェックボックスをチェックする
2. メールを隔離から解除しメールサーバへ配信する場合には【アクションの選択】から【リリース】または【セーフリストへ追加しリリース】を選択し【実行】すると、メールサーバへ送信される  
【削除】を選択した場合には、隔離領域から削除される

Copyright ©2010 Net One Systems CO.,LTD. All rights reserved. Net One Systems 23

図6 隔離メールの処理2

#### 2.4. セーフリストとブロックリスト

次の図7と図8にてセーフリストとブロックリストについて説明します。

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### セーフリスト機能

- SPAM 判定されたくないメールの送信元メールアドレスを登録することで、誤判定を防ぐ機能
- 隔離領域を利用するユーザ毎に設定可能(各ユーザー毎100件まで)

**標準の状態**

From: test@yahoo.com → SPAM??? (誤検知) → In-box

**セーフリストに yahoo.com または test@yahoo.com を登録**

From: test@yahoo.com → セーフリストのアドレスは SPAM判定をパス → 無事到着

Copyright ©2010 Net One Systems CO.,LTD. All rights reserved. Net One Systems 24

図7 セーフリスト機能の説明

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### ブロックリスト機能

- SPAMもしくは受信したくないメールを登録したい場合、送信元メールアドレスを登録することで、メールアドレスのみで無条件に隔離する機能
- 隔離領域を利用するユーザー毎に設定可能(各ユーザー毎 100件まで)

**標準の状態**

From: test@yahoo.com

SPAM判定  
SPAMで無ければそのまま配送

メール到着

**ブロックリストに yahoo.com または test@yahoo.com を登録**

メール隔離

From: test@yahoo.com

ブロックリスト  
マッチ

Net One Systems

図8 ブロックリスト機能の説明

図9、図10、図11にはセーフリストとブロックリストの設定の手順を説明します。

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### ユーザ個別のセーフリスト・ブロックリスト管理

1. メニュー上の【オプション】にカーソルを合わせる
2. 言語メニューと共に、【セーフリスト】と【ブロックリスト】が表示される
3. 管理したいリストを選択する

Net One Systems

図9 セーフリスト・ブロックリストの管理

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### ユーザ個別のセーフリスト・ブロックリスト管理 — 追加の場合

**1. テキストボックスへメールアドレスまたはドメインを入力し、【リストに追加】を選択**  
 注意 追加したリストのシステムへの反映には5分～10分掛かります。

リストに追加されている e-mail アドレスもしくはドメインはスパムと判断されません。

リストに追加されている e-mail アドレスもしくはドメインはスパムと判断されます。

以下のフォーマットが利用できます:  
 user@domain.com  
 server.domain.com  
 domain.com

以下のフォーマットが利用できません:  
 user@domain.com  
 server.domain.com  
 domain.com

0 通のメッセージが見つかりました。

0 通のメッセージが見つかりました。

スパム隔離の表示

ページが表示されました

Copyright ©2010 Net One Systems CO.,LTD. All rights reserved.



27

図 10 セーフリスト・ブロックリストの管理 (追加)

## 迷惑メールへの対策【隔離メールの確認・削除・復元など】

### ユーザ個別のセーフリスト・ブロックリスト管理 — 削除の場合

**1. リストから削除したいアドレスの右側にあるゴミ箱を選択し削除**  
 注意 削除したリストのシステムへの反映には5分～10分掛かります。

リストに追加されている e-mail アドレスもしくはドメインはスパムと判断されません。

リストに追加されている e-mail アドレスもしくはドメインはスパムと判断されます。

以下のフォーマットが利用できます:  
 user@domain.com  
 server.domain.com  
 domain.com

以下のフォーマットが利用できません:  
 user@domain.com  
 server.domain.com  
 domain.com

1 通のメッセージが見つかりました。

testtest@test.ac.jp

1 通のメッセージが見つかりました。

testtest@fjeig.co.jp

ページが表示されました

Copyright ©2010 Net One Systems CO.,LTD. All rights reserved.



28

図 11 セーフリスト・ブロックリストの管理 (削除)

### 3. 最後に

以上の説明のポイントをつぎのとおりにまとめます。

#### <改善効果>

スパムメール対策を更新したことで弘前大学様のスパムメール対策は以下のように改善されています。

- ・世界最大規模を誇るデータベースを参照することでの高精度なスパムメール対策
- ・セーフリスト・ブロックリストを使用しての、ユーザ毎の個別のフィルタリング機能

#### <注意点>

##### ▼隔離領域について

- ・ユーザ毎の保存容量は5GB、保持期間は30日間。容量を超えた場合、古いものから自動的に削除される

##### ▼セーフリスト／ブロックリスト

- ・リストは変更しても、システムに反映するまで5分～10分かかる
- ・両リストに同一のメールアドレス、ドメイン名を登録することはできない
- ・サブドメイン名には未対応  
(例：ブロックリストに“ac.jp”を登録。→“tsato@cc.hirosaki-u.ac.jp”からのメールは届く)
- ・より細かなリストの内容が適用される  
(例：ブロックリストに“cc.hirosaki-u.ac.jp”を登録。セーフリストに tsato@cc.hirosaki-u.ac.jp を登録。→セーフリストが適用されユーザにメールは届く)