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、チェー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、と多種多様の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。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。

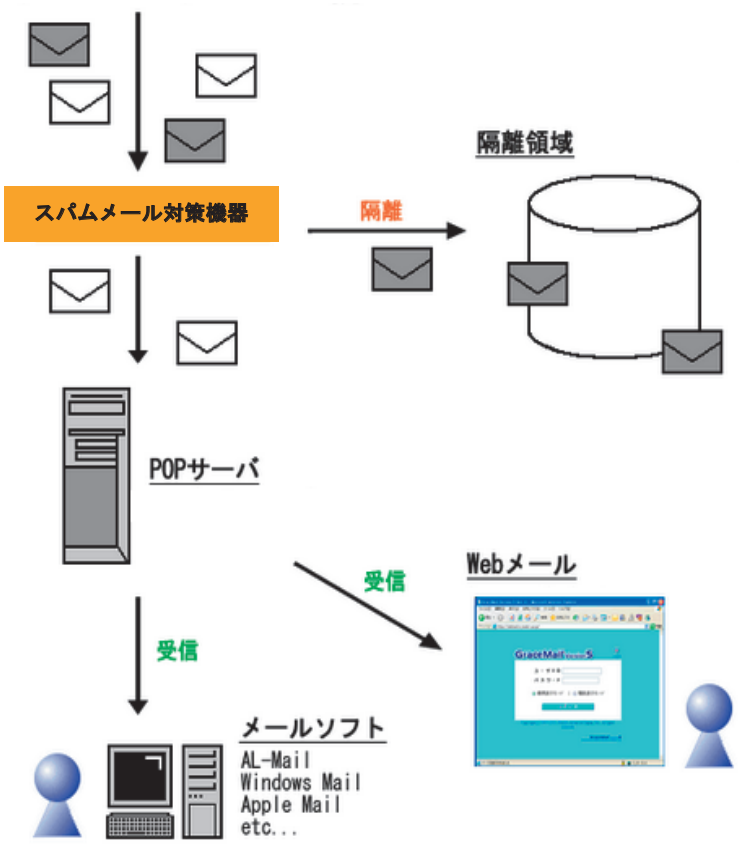

図１　学外からの届くメールの処理フロー図

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。

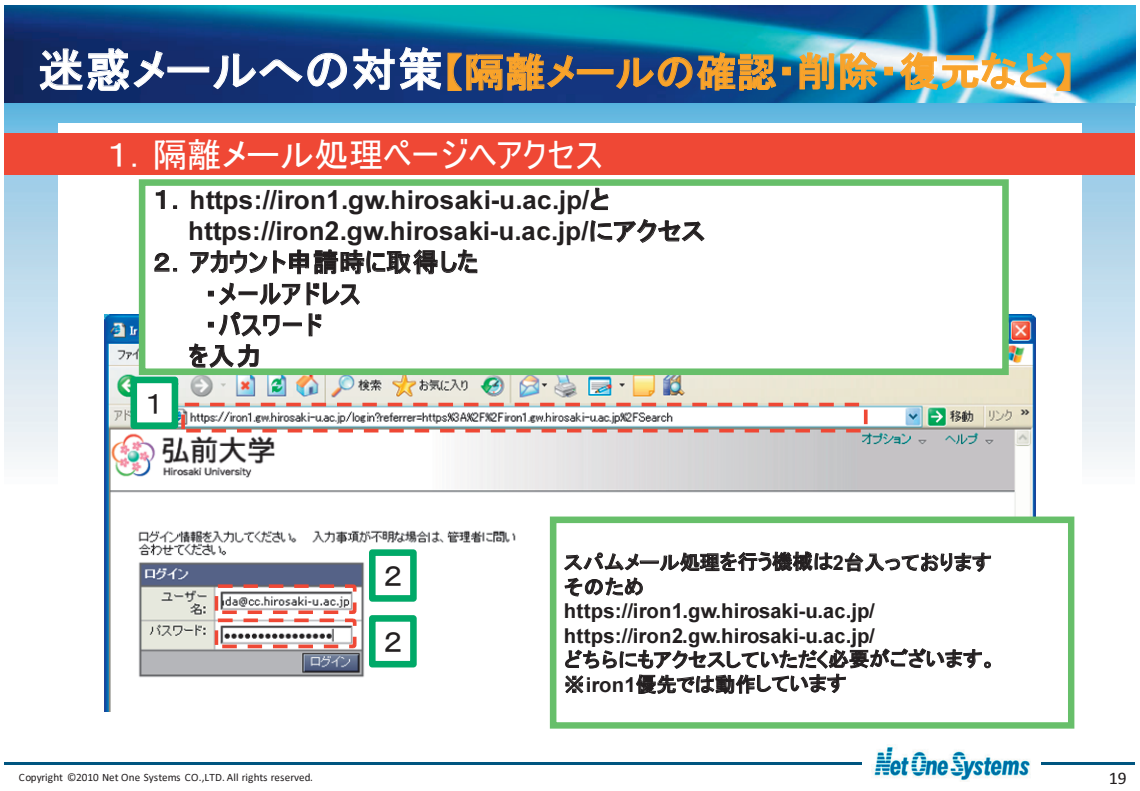

図２　隔離メール処理ページへアクセス

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。

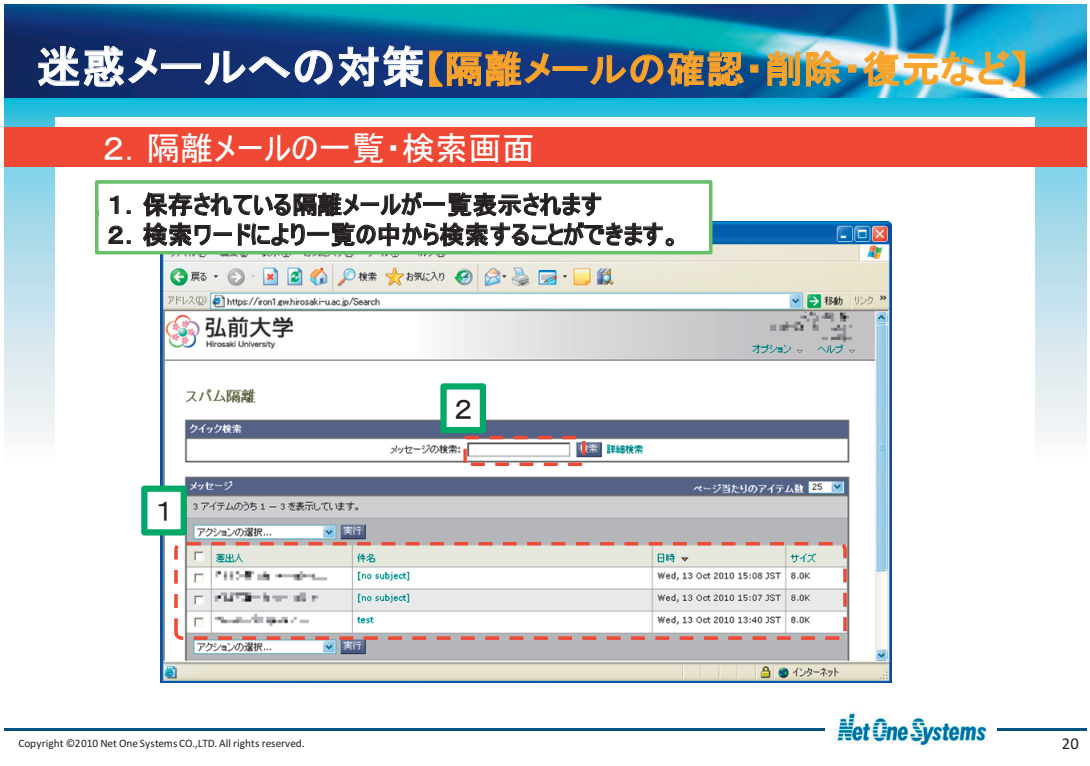

図３　トップ画面

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。

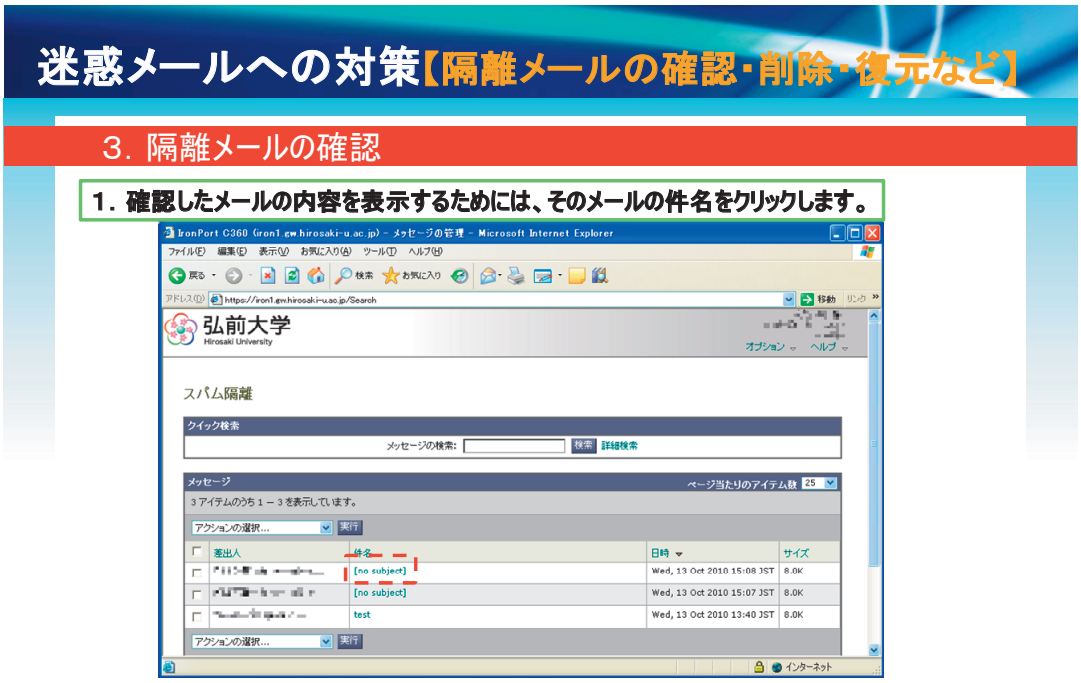

図４　隔離メール確認

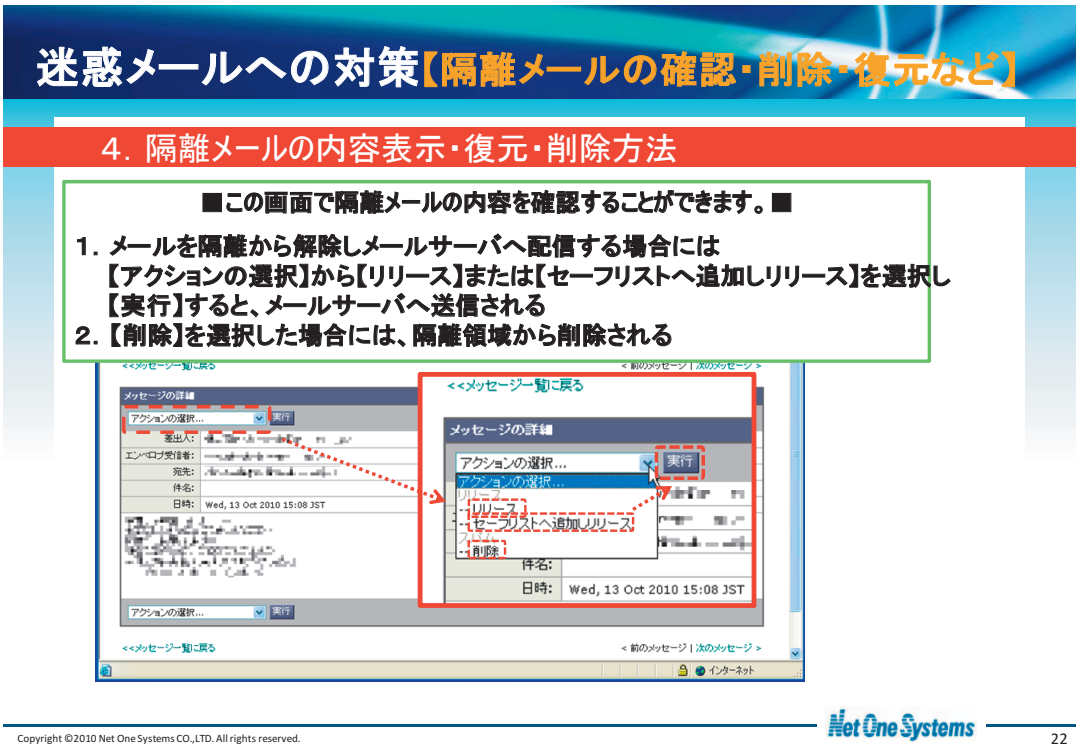

図５　隔離メールの処理１

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。

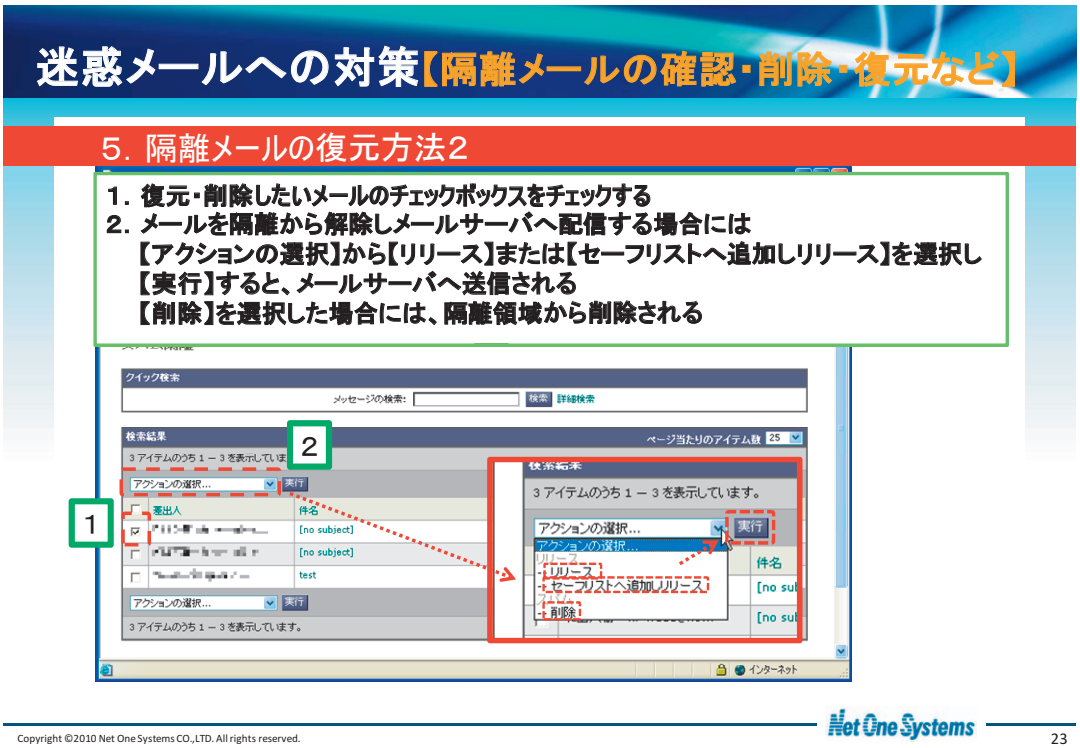

図６　隔離メールの処理２

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。

図７　セーフリスト機能の説明

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。

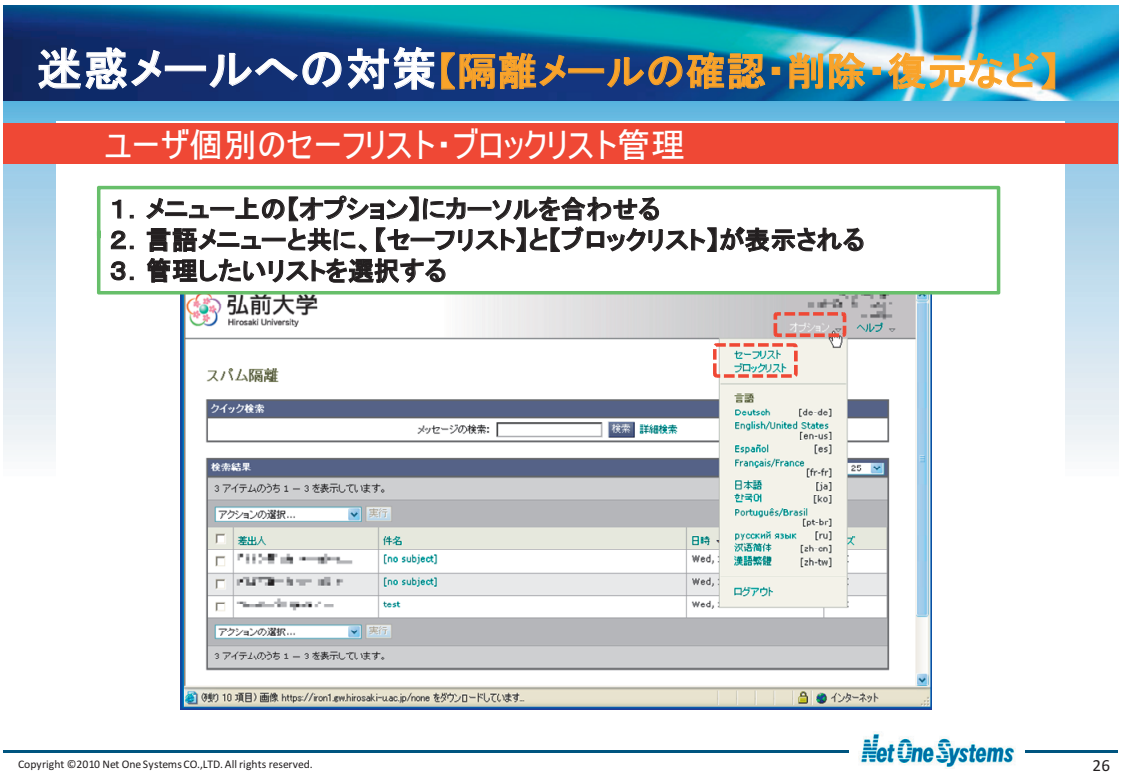

図９　セーフリスト・ブロックリストの管理

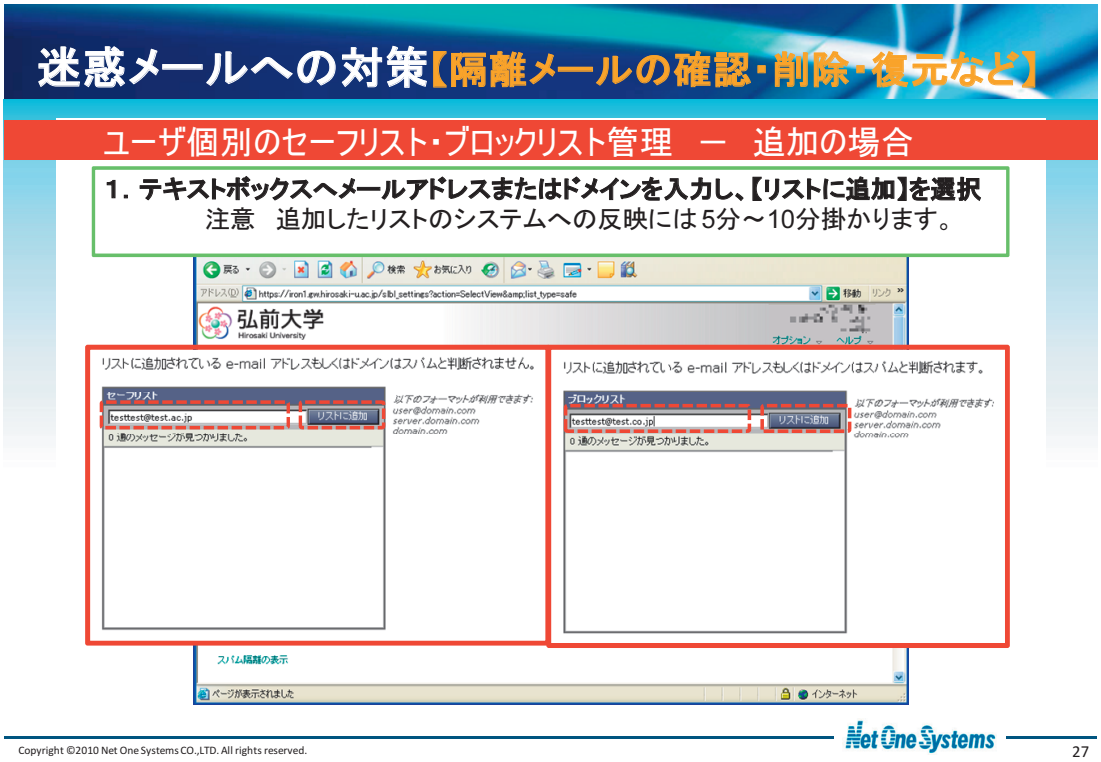

図 10　セーフリスト・ブロックリストの管理（追加）

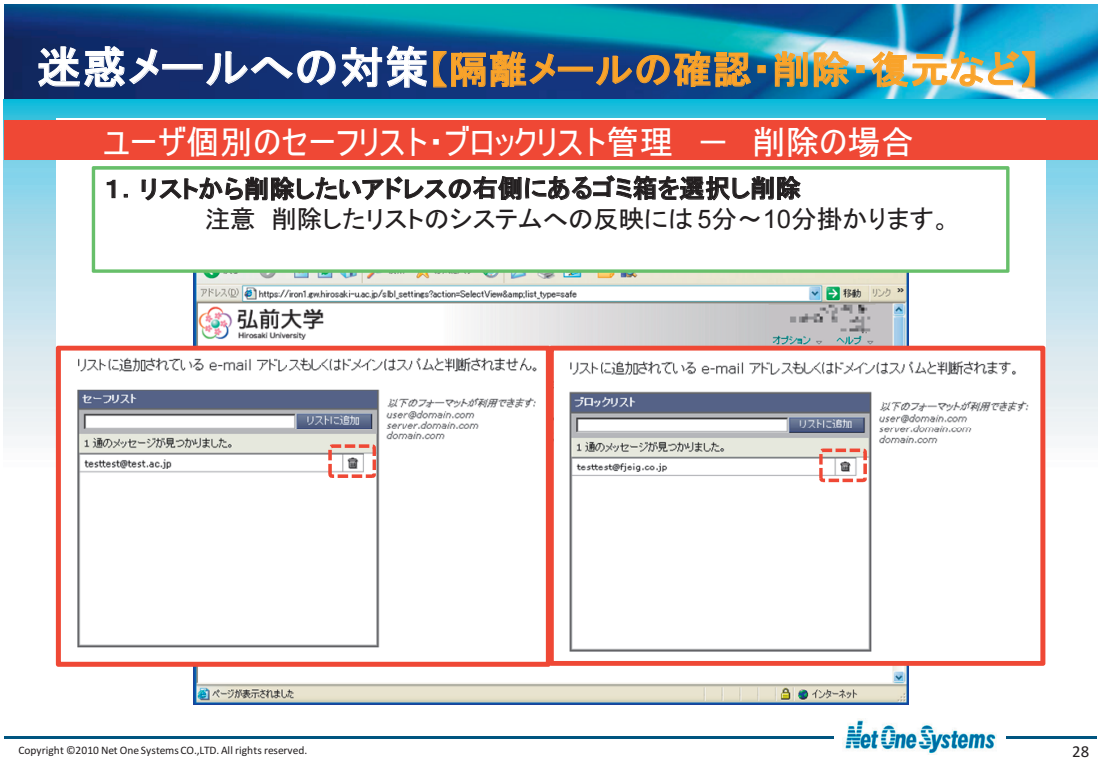

図 11　セーフリスト・ブロックリストの管理（削除）

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）