次に見据えるべきスパム対策
～display-name のなりすまし問題～

2014年10月8日

講師： 鈴木康平(ヤフー)
講師： 安元英行(トランスウエア)
コーディネーター： 加瀬正樹(ニフティ)

Copyright © NIFTY Corporation All Rights Reserved.

アジェンダ

- ✓ display-name **問題とは**
- ✓ **実際に発生している(しうる)問題**
- ✓ display-name **問題への戦い方(１)**
- ✓ display-name **問題への戦い方(２)**
- ✓ **質疑応答**

Copyright © NIFTY Corporation All Rights Reserved.

display-name とは

RFC5322(Internet Message Format)

-> 3.4. Address Specification

-> A.1.2. Different Types of Mailboxs

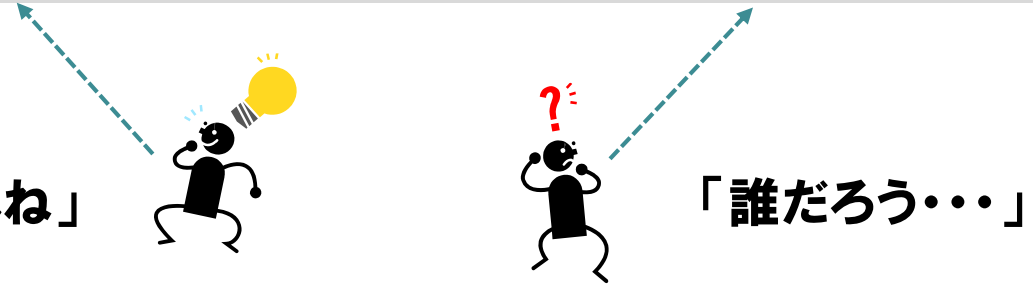
簡単に言えば、メールアドレスの”名前” を示すオプション

※会社によっては”コメント部分”、”表示名”と呼ぶことも

例)

From: Masaki Kase <kase.masaki@nifty.co.jp>

To: **“加瀬 正樹”** <softest@nifty.com>, <abc12345@example.com>



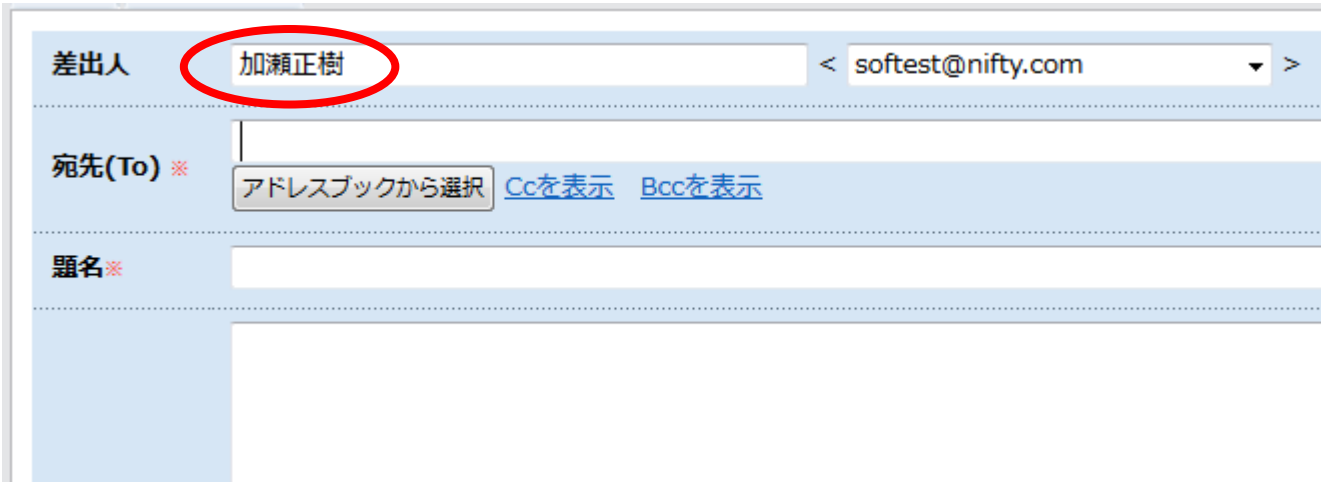
誰なのか、メールアドレスよりも視認しやすい

Copyright © NIFTY Corporation All Rights Reserved.

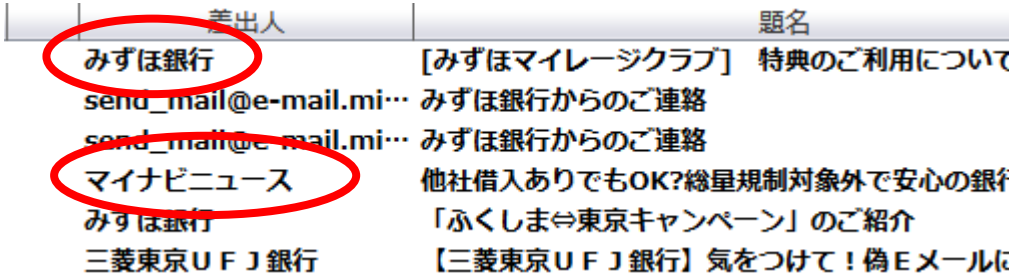
display-name 現在の使われ方（良い例）

@nifty

メールソフトやWebMailで「差出人」を**わかりやすく表示**することができる



※@nifty Webメール



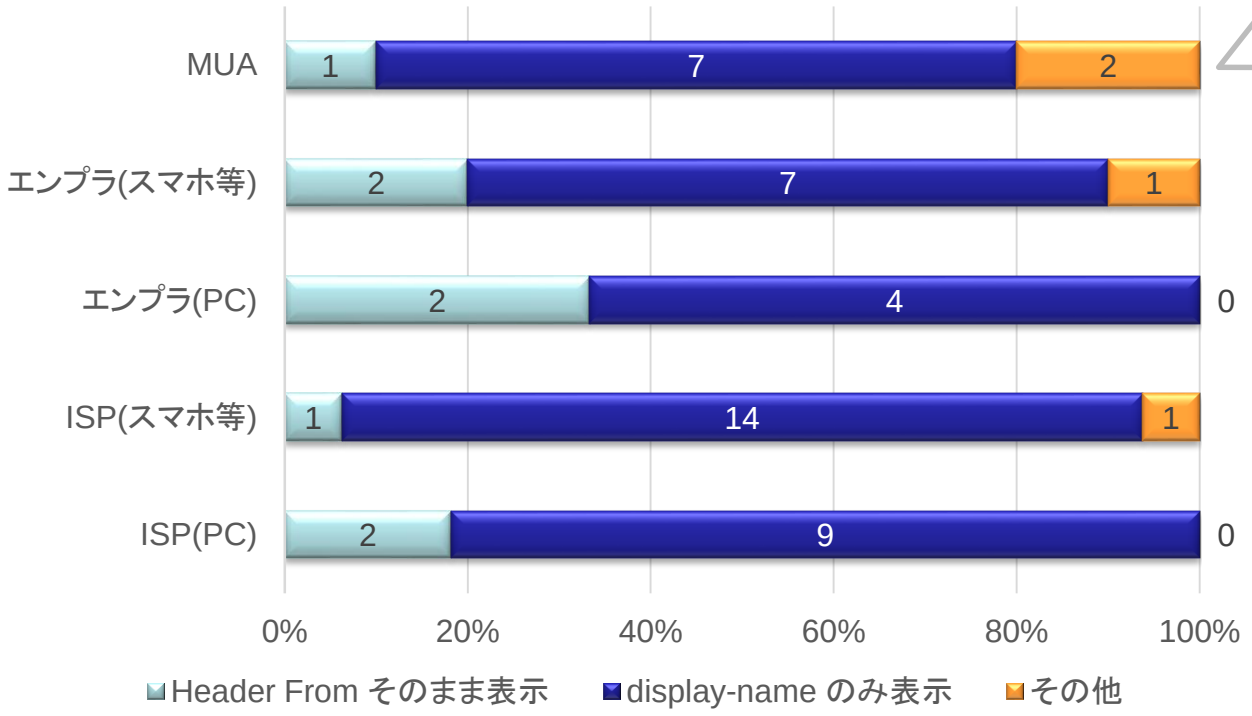
※@nifty Webメール

Copyright © NIFTY Corporation All Rights Reserved.

【Tips】display-name の普及状況

@nifty

MUA/WebMail のリスト表示形式



例）Becky! の例

※ISP各社に調査をご協力いただきました
ありがとうございます m(_ _)m

“display-name” なので表示に広く利用

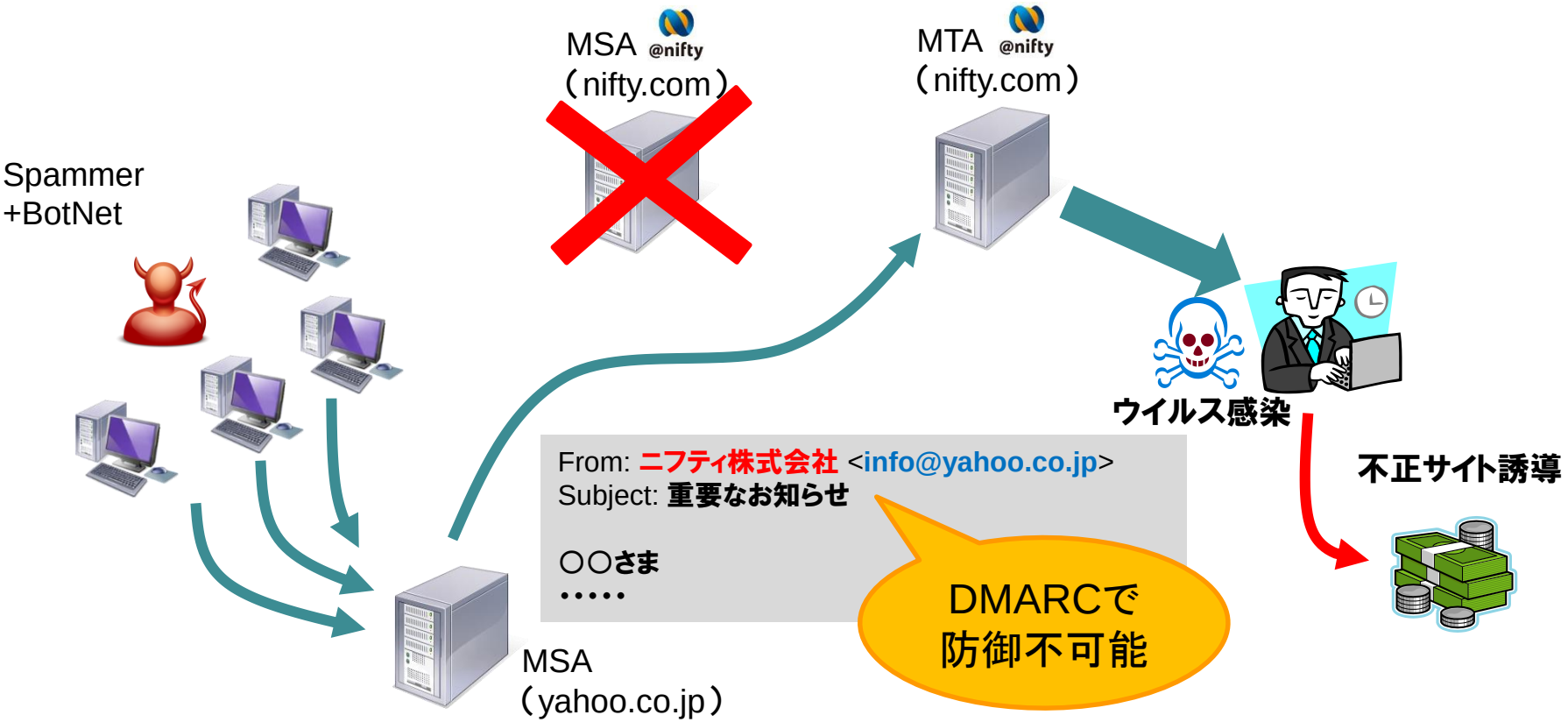
Copyright © NIFTY Corporation All Rights Reserved.

display-name 現在の使われ方（悪い例）

@nifty

金融機関やウェブサービスの企業名・窓口を名乗り、不正サイトへの誘導・不正送金ウイルスの感染をさせる。

⇒ Fromヘッダーの display-name を使って企業名・窓口を名乗るので送信ドメイン認証（DMARC）ではなりすましを見抜くことは不可能



Copyright © NIFTY Corporation All Rights Reserved.

Q. display-name 偽装は「送信者偽装」か？

@nifty

A. そのような総務省の解釈は今まで出ていない

電気通信役務提供の拒否

- 第11条
- 電気通信事業者は、送信者情報を偽った電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生じ、又はその利用者における電子メールの送受信上の支障を生ずるおそれがあると認められるとき…(略)…当該支障を防止するために必要な範囲内において、当該支障を生じさせるおそれのある電子メールの送信をするものに対し、電子メール通信役務の提供を拒むことができる。

[引用] 第6回迷惑メール対策推進協議会
http://www.iajapan.org/anti_spam/event/2008/conf1105/pdf/3-1.pdf

Copyright © NIFTY Corporation All Rights Reserved.

事業者2社からご登壇いただきました

@nifty

鈴木　康平

ヤフー株式会社

安元　英行

株式会社トランスウエア

Copyright © NIFTY Corporation All Rights Reserved.

実際に発生している（発生しうる）問題

鈴木さん ▶ 安元さん ▶ 加瀬(おまけ)

Copyright © NIFTY Corporation All Rights Reserved.

実際に発生している（発生しうる）問題

鈴木さん ▶ **安元さん** ▶ 加瀬(おまけ)

Copyright © NIFTY Corporation All Rights Reserved.

トランスウエアにて実際に発生している問題

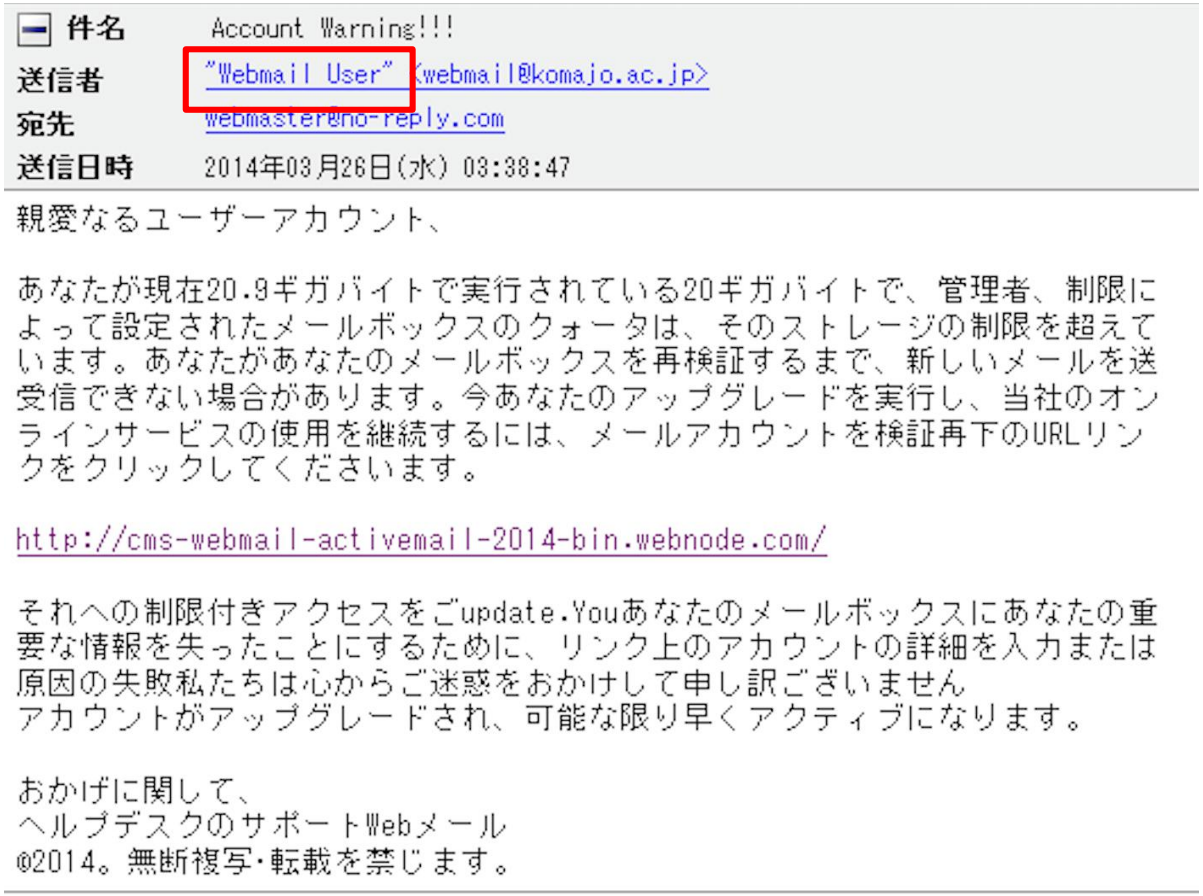
トランスウエアを模倣(なりすました)したメールの事例紹介

- **具体的には何をされた？:**
  大学マーケットを中心にフィッシングメールを送られた。
- **目的は？:**
  アカウント情報を盗みSpamメールを大量に送る。(Submission Spam)
- **被害は？:**
  - **メールを送られた人:**
    - ✓ IDとPassword情報を盗まれ、大量のSpamを送られる。
    - ✓ RBLにMTAが登録され、正常なメールの配送が阻害される。
  - **弊社:**
    - ✓ xxxxxxxxxxxxxxx(非公開)xxxxxxxxxxxxxxxxxxxxx
- **時期は？:**
  - 2013年9月の終わり頃から現在
  - 弊社への発生報告は、概ね月2回、多い時で4回。2014年9月は無い。

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

トランスウエアにて実際に発生している問題

実際のフィッシングメールの実例



件名　Account Warning!!!
送信者　"Webmail User" <webmail@komajo.ac.jp>
宛先　webmaster@no-reply.com
送信日時　2014年03月26日(水) 03:38:47

親愛なるユーザーアカウント、

あなたが現在20.9ギガバイトで実行されている20ギガバイトで、管理者、制限によって設定されたメールボックスのクォータは、そのストレージの制限を超えています。あなたがあなたのメールボックスを再検証するまで、新しいメールを送受信できない場合があります。今あなたのアップグレードを実行し、当社のオンラインサービスの使用を継続するには、メールアカウントを検証再下のURLリンクをクリックしてくださいます。

http://cms-webmail-activemail-2014-bin.webnode.com/

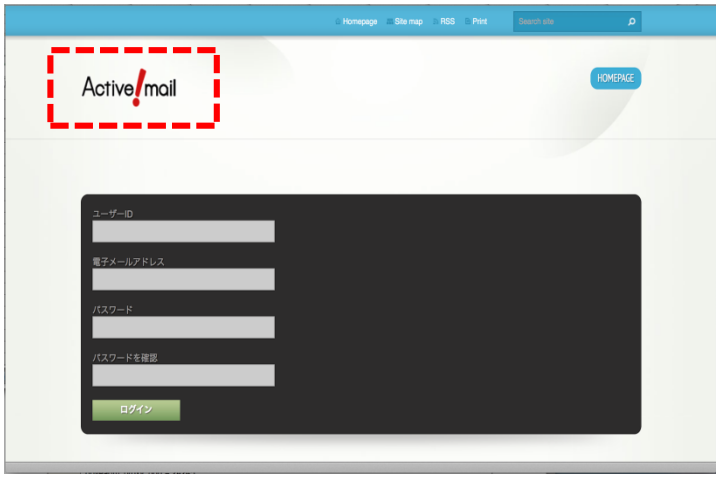
それへの制限付きアクセスをごupdate.Youあなたのメールボックスにあなたの重要な情報を失ったことにするために、リンク上のアカウントの詳細を入力または原因の失敗私たちは心からご迷惑をおかけして申し訳ございません
アカウントがアップグレードされ、可能な限り早くアクティブになります。

おかげに関して、
ヘルプデスクのサポートWebメール
©2014。無断複写・転載を禁じます。

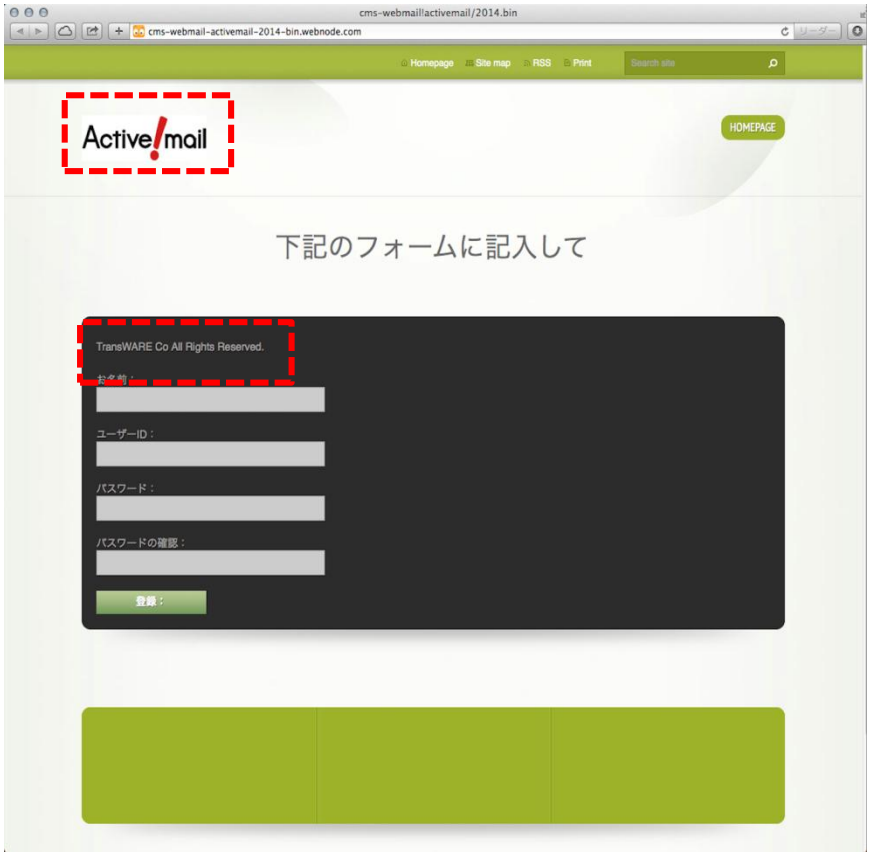
Copyright© 2013 TransWARE Co. All Rights Reserved.

トランスウエアにて実際に発生している問題

実際のフィッシングサイトの実例（2014年2月での実例）



実際のフィッシングサイトの実例（2014年3月での実例）



Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

トランスウエアにて実際に発生している問題

実際のフィッシングサイトの実例（一番悪質と考えられる）

弊社のlogin画面

Copyright© 2013 TransWARE Co. All Rights Reserved.

トランスウエアにて実際に発生している問題

トランスウエアを模倣(なりすました)したメールの事例紹介

- disply nameでの実例:
  - Active!Mail ≪upgrade4@accountant.com≫
  - "Active! Mail" <ta-kai@m2.gyao.ne.jp>
  - "Active Mail Account" <ayudadgip@larioja.gov.ar>
  - It's Administrator <ahumadaosvaldo@arnet.com.ar>

Copyright© 2013 TransWARE Co. All Rights Reserved.

実際に発生している（発生しうる）問題

鈴木さん ▶ 安元さん ▶ **加瀬(おまけ)**

Copyright © NIFTY Corporation All Rights Reserved.

ニフティでの display-name 詐称

メモ禁止

@nifty

当日のみ公開

Copyright © NIFTY Corporation All Rights Reserved.

display-name 問題との戦い方

安元さん ▶ 鈴木さん

Copyright © NIFTY Corporation All Rights Reserved.

トランスウエアでの対策/課題

1.トランスウエアを模倣(なりすました)したメールへの対策

- 被害届け:
  - 風評被害として届け出はできないものか?→対警察
- 現実に実施している事:
  - JPCERT/CCに対しての報告
    - ✓ フィッシングサイトの閉鎖 → 翌日には閉鎖が確認できる。
    - ✓ 加盟団体への通達による、積極的な注意喚起。
  - 自社ホームページへの情報の記載/注意喚起
  - RBLへの登録があった場合の対応

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

トランスウエアでの対策/課題

撮影禁止

メモ禁止

Active!mail

1.トランスウエアを模倣(なりすました)したメールへの対策(続き)

当日のみ公開

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

TransWARE

トランスウエアでの対策/課題

撮影禁止

メモ禁止

Active!mail

1.トランスウエアを模倣(なりすました)したメールへの対策(続き)

当日のみ公開

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

TransWARE

トランスウエアでの対策/課題

撮影禁止 メモ禁止 Active!mail

1.トランスウエアを模倣(なりすました)したメールへの対策(続き)

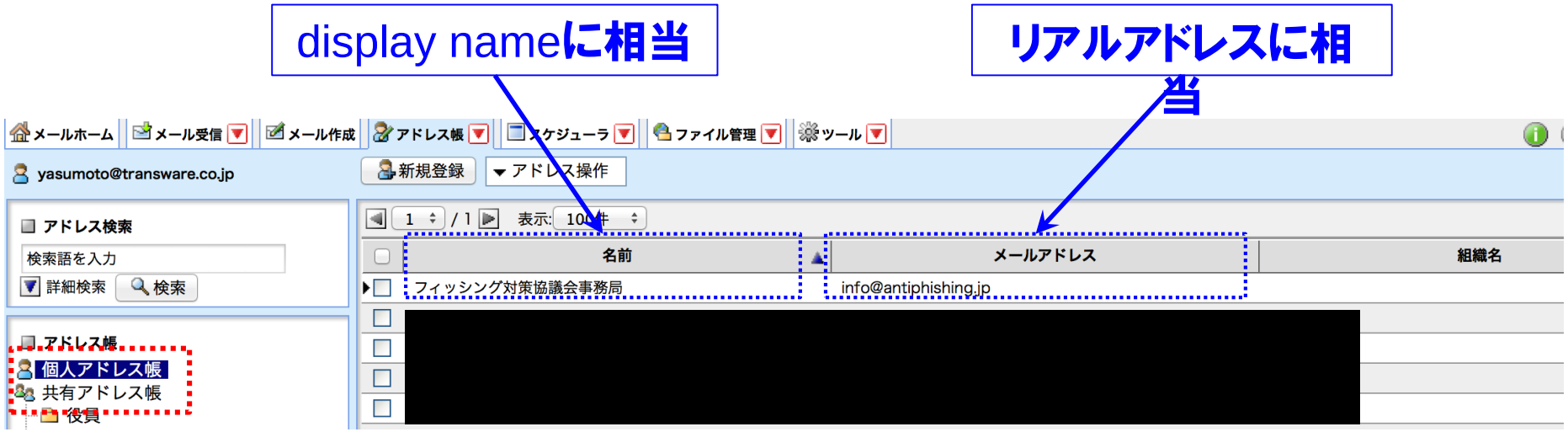
当日のみ公開

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

トランスウエアでの対策/課題

2.製品(Active!mail)にて考えられる対策。その前に！

- アドレス帳の説明



Copyright© 2013 TransWARE Co. All Rights Reserved.

トランスウエアでの対策/課題

撮影禁止

メモ禁止

Active!mail

2.製品(Active!mail)にて考えられる対策。その前に！

当日のみ公開

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

TransWARE

トランスウエアでの対策/課題

撮影禁止

メモ禁止

Active!mail

当日のみ公開

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

TransWARE

トランスウエアでの対策/課題

撮影禁止

メモ禁止

Active!mail

当日のみ公開

Copyrightⓒ 2013 TransWARE Co. All Rights Reserved.

TransWARE

display-name 問題との戦い方

安元さん ▶ **鈴木さん**

Copyright © NIFTY Corporation All Rights Reserved.

ディスカッション・質問など

Copyright © NIFTY Corporation All Rights Reserved.

終わりに

今後もこの問題・対策について
取り組んでいきます

Copyright © NIFTY Corporation All Rights Reserved.