緑消防署管理指導課
電子メールのフィルタリング機能を活用した標的型攻撃メールの明確化

もし、標的型攻撃メールの被害をうけたら？

- 業務で使用しているインターネット・イントラネット・パソコンが使用不可能に
- 警察からの事情聴取
- マスコミ対応
- 関係者へのお詫び
- 問い合わせ窓口の設置

事故対応に時間と手間がとられ、通常業務の遅れにつながります

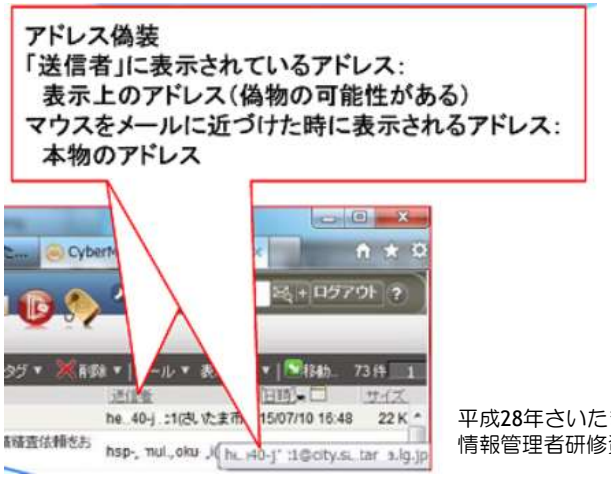
＋

流出した個人情報は、
取り戻すことはできません

本市の重大な信用失墜となり、多額の損害賠償が必要になる可能性も。

標的型攻撃メール等の不審なメールの被害を受けないためには
メールの差出人や件名、メール内容を確認し、
心当たりのないメールの
添付ファイルを開いたりや本文中のURLにアクセスしないことが重要です。

メールアドレスの確認は重要ですが、
メール一覧に表示されているアドレスは
偽装されている可能性があります。
マウスカーソルを送信者名に近づけて本物の
アドレスを確認する必要があり、
手間がかかります。



平成28年さいたま市
情報管理者研修資料より

そこでメールのフィルタリング機能を活用してカイゼンしました

注意すべきメールが一目瞭然

本物のアドレスで振り分けられるので、アドレス確認の時間を短縮

アドレス帳に登録済みの送信元からのメールは緑色のラベル色が自動的に付くようにしました。

アドレス帳にない送信元からのメールは赤色のラベル色が付くのと同時にタグ、フラグが自動的に付くようにしました。

自動的に付いたフラグ

自動的に付いたタグ