

2.4 メールの見分け方

- 4つの着眼点
 - テーマ（件名）
 - 送信者
 - メール本文
 - 添付ファイル

「見分ける」
= 添付ファイルを開く、実行してしま
う前に不審点を見つける

2.4.1 テーマ（件名）

着眼点	過去の標的型攻撃で見られたケース
テーマ	<ul style="list-style-type: none"> • 知らない人からのメールだが、開封せざるを得ない内容 <ul style="list-style-type: none"> ① 新聞社・出版社からの取材申込・講演依頼 ② 就職活動に関する問合せ・履歴書の送付 ③ 製品やサービスに対する問い合わせ・クレーム ④ アンケート調査 ⑤ やり取り型メール
	<ul style="list-style-type: none"> • 誤って自分宛に送られたメールの様だが、興味をそそられる内容 <ul style="list-style-type: none"> ① 議事録・演説原稿などの内部文書送付 ② VIP訪問に関する情報
	<ul style="list-style-type: none"> • これまで届いたことがない、公的機関からのお知らせ <ul style="list-style-type: none"> ① 情報セキュリティに関する注意喚起 ② インフルエンザ流行情報 ③ 災害情報

2.4.2 送信者とメール本文

着眼点	過去の標的型攻撃で見られたケース
送信者	<ul style="list-style-type: none"> • フリーメールアドレスからの送信 • 送信者のメールアドレスが署名（シグネチャ）と異なる
メール本文	<ul style="list-style-type: none"> • 言い回しが不自然な日本語 • 日本語では使用されない漢字（繁体字、簡体字）カタカナ • 正式名称を一部に含むような不審URL • HTMLメールで、表示と実際のURLが異なるリンク • 署名の記載内容がおかしい、該当部門が存在しない

2.4.3 添付ファイル

着眼点	過去の標的型攻撃で見られたケース
添付ファイル	<ul style="list-style-type: none"> 実行形式ファイル (exe / scr / jar / cpl など)
	<ul style="list-style-type: none"> ショートカットファイル (lnk / pif / url)
	<ul style="list-style-type: none"> 実行形式ファイルなのに文書ファイルやフォルダのアイコン
	<ul style="list-style-type: none"> ファイル名が不審 <ul style="list-style-type: none"> ✓ 二重拡張子 ✓ ファイル拡張子の前に大量の空白文字を挿入 ✓ 文字列を左右反転するRLOコードの利用 ✓ エクスプローラで圧縮ファイルの内容を表示するとファイル名が文字化け

事務連絡cod.scr

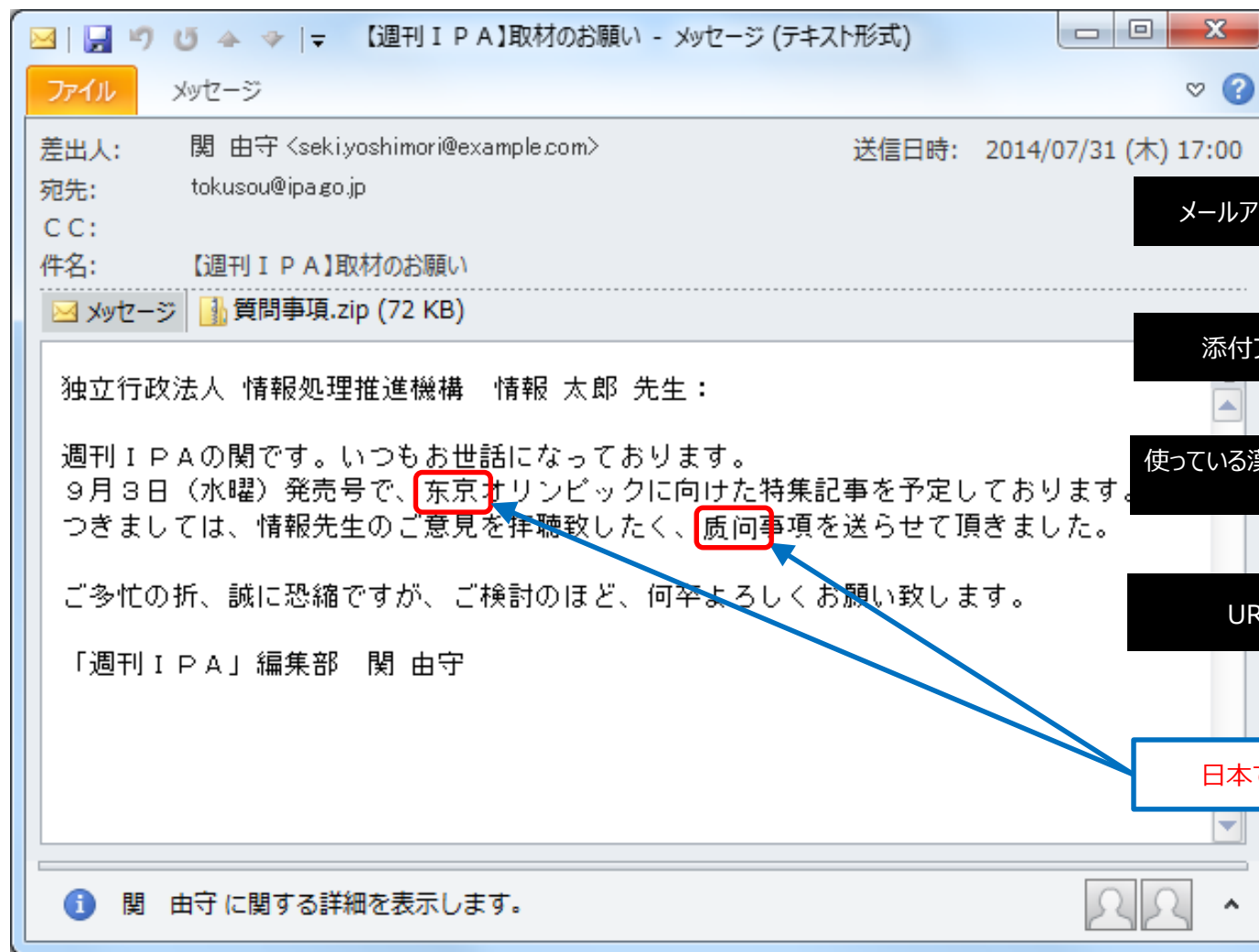
ここにRLO文字を挿入すると、
次のような見た目になる。

事務連絡rcs.doc

RLO: Right-to-Left Override
アラビア語やヘブライ語などをパソコンで使うため
の特殊な文字 (表示はされない)

2.5.1 メールサンプル①

～取材を装ったケース～



メールアドレスに不審点はないか

添付ファイルはどんな形式か

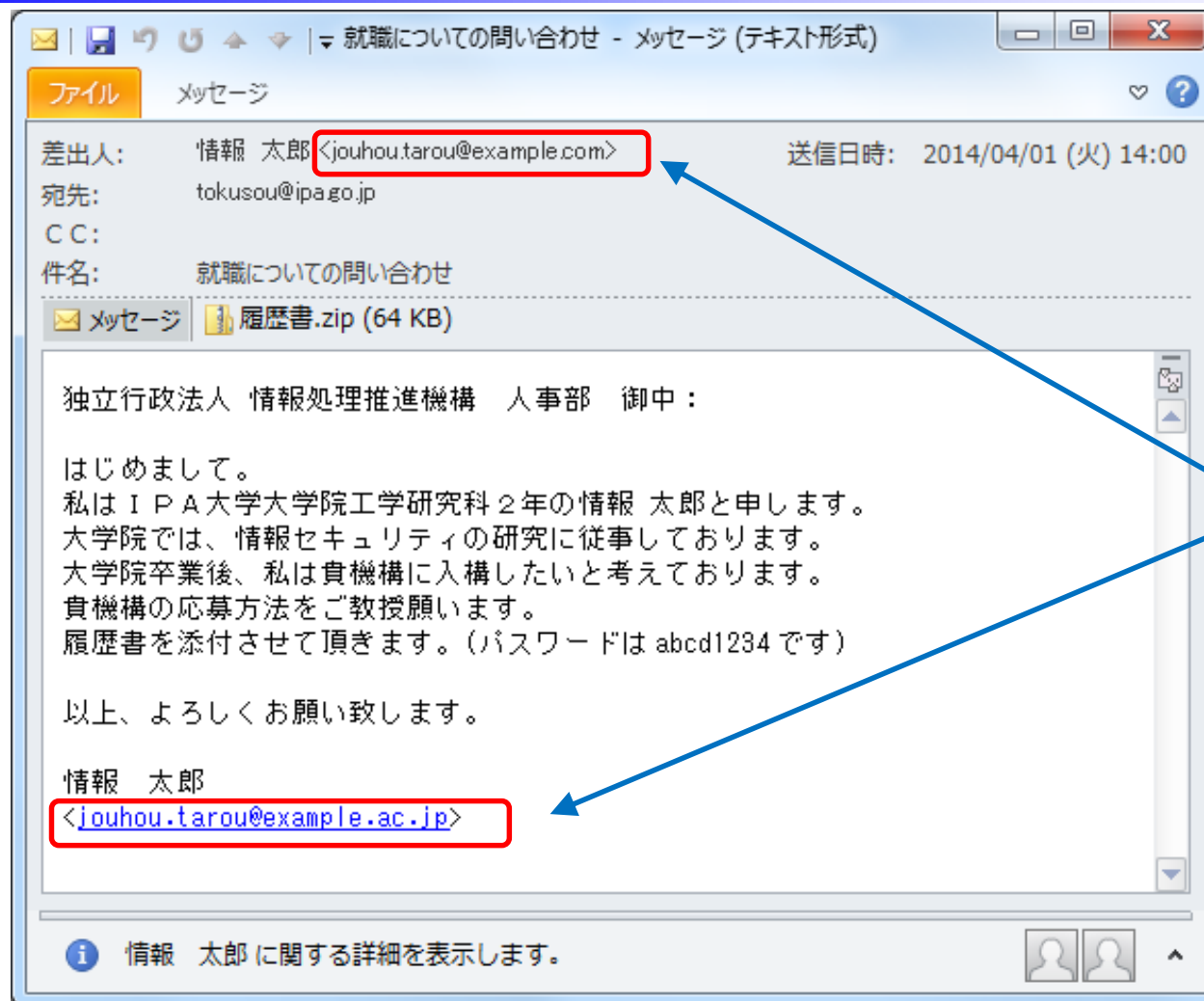
使っている漢字や言い回しに不審的はないか

URLは正規のURLか

日本で使われていない漢字

2.5.2 メールサンプル②

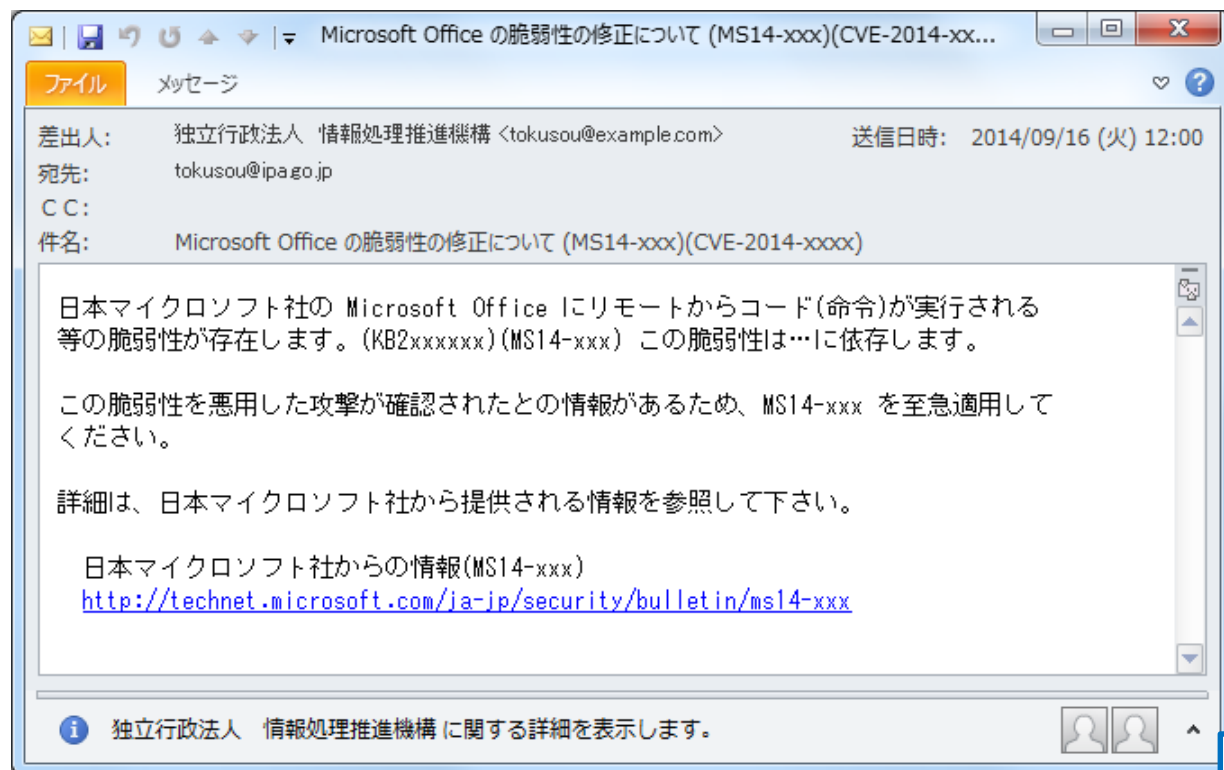
～就職を装ったケース～



署名とメールアドレスが違う

2.5.3 メールサンプル③

～情報セキュリティに関する注意喚起を装ったケース～



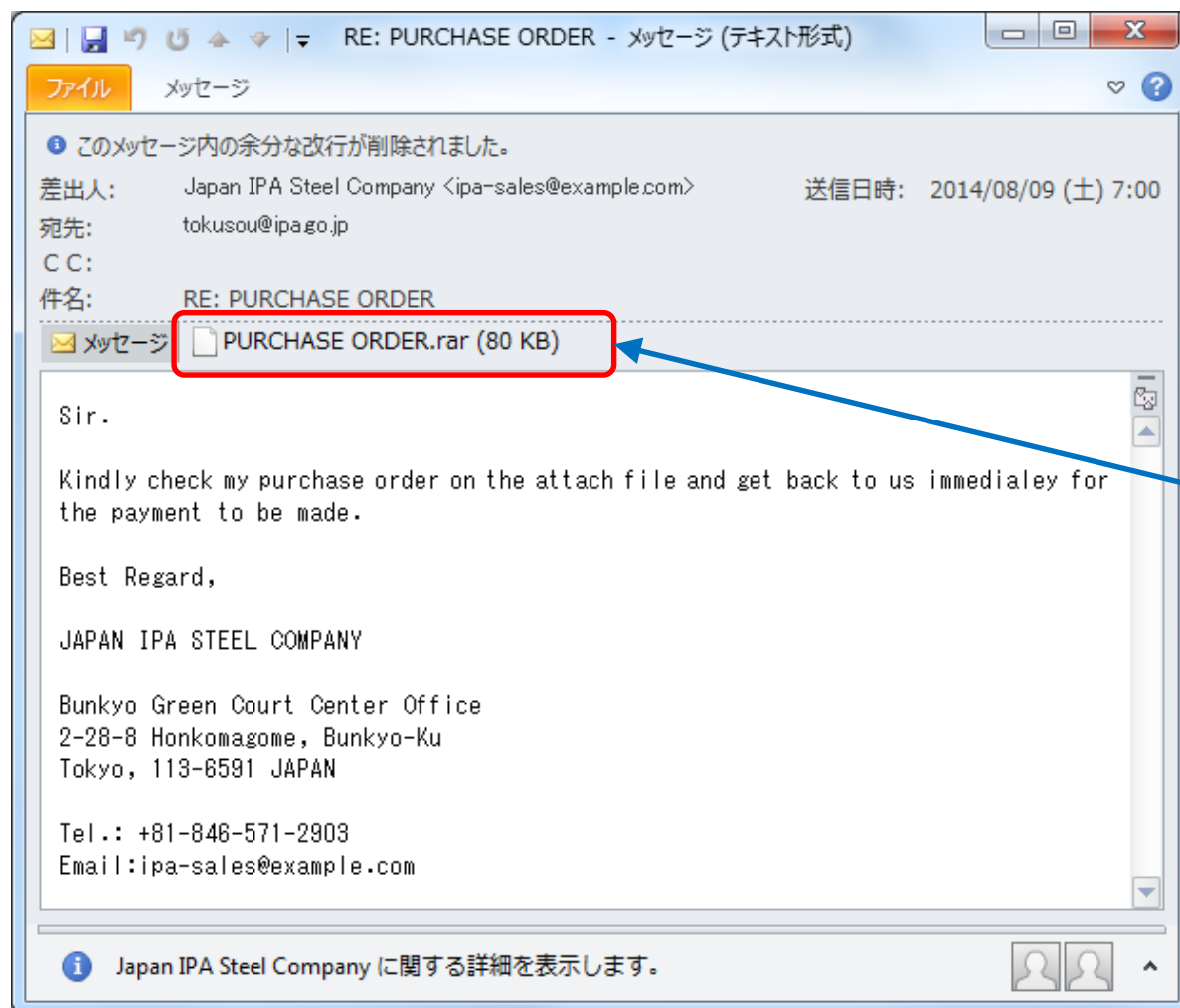
実際にクリックした際に表示されるウェブページのURL

日本マイクロソフト社からの情報(MS14-xxx)

<http://technet.microsoft.com/ja-jp/security/bulletin/ms14-xxx>
 <<http://technet.microsoft.com.xx/ja-jp/security/bulletin/ms14-xxx>>

2.5.4 メールサンプル④

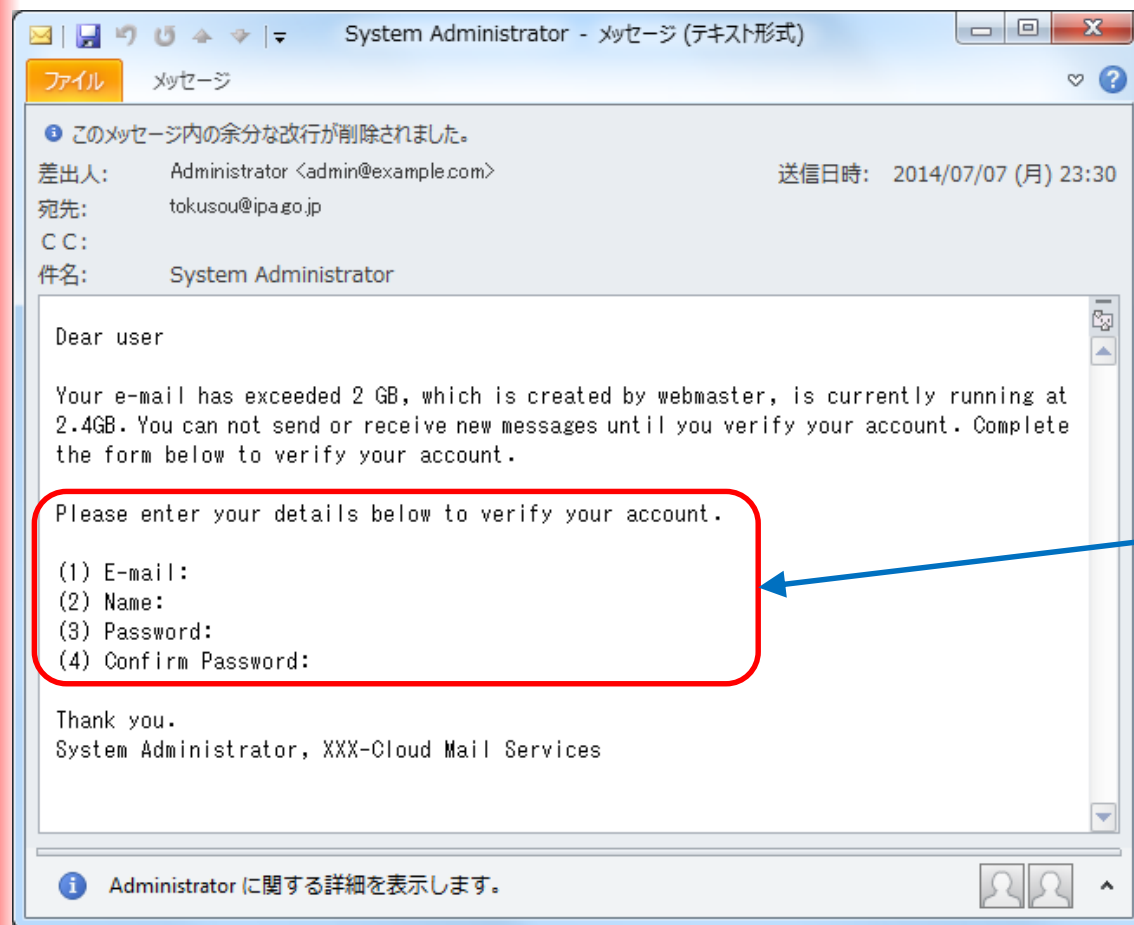
～心当たりのない決済・配送通知を装った標的型～



日本であり使われない圧縮形式
(rar)

2.5.5 メールサンプル⑤

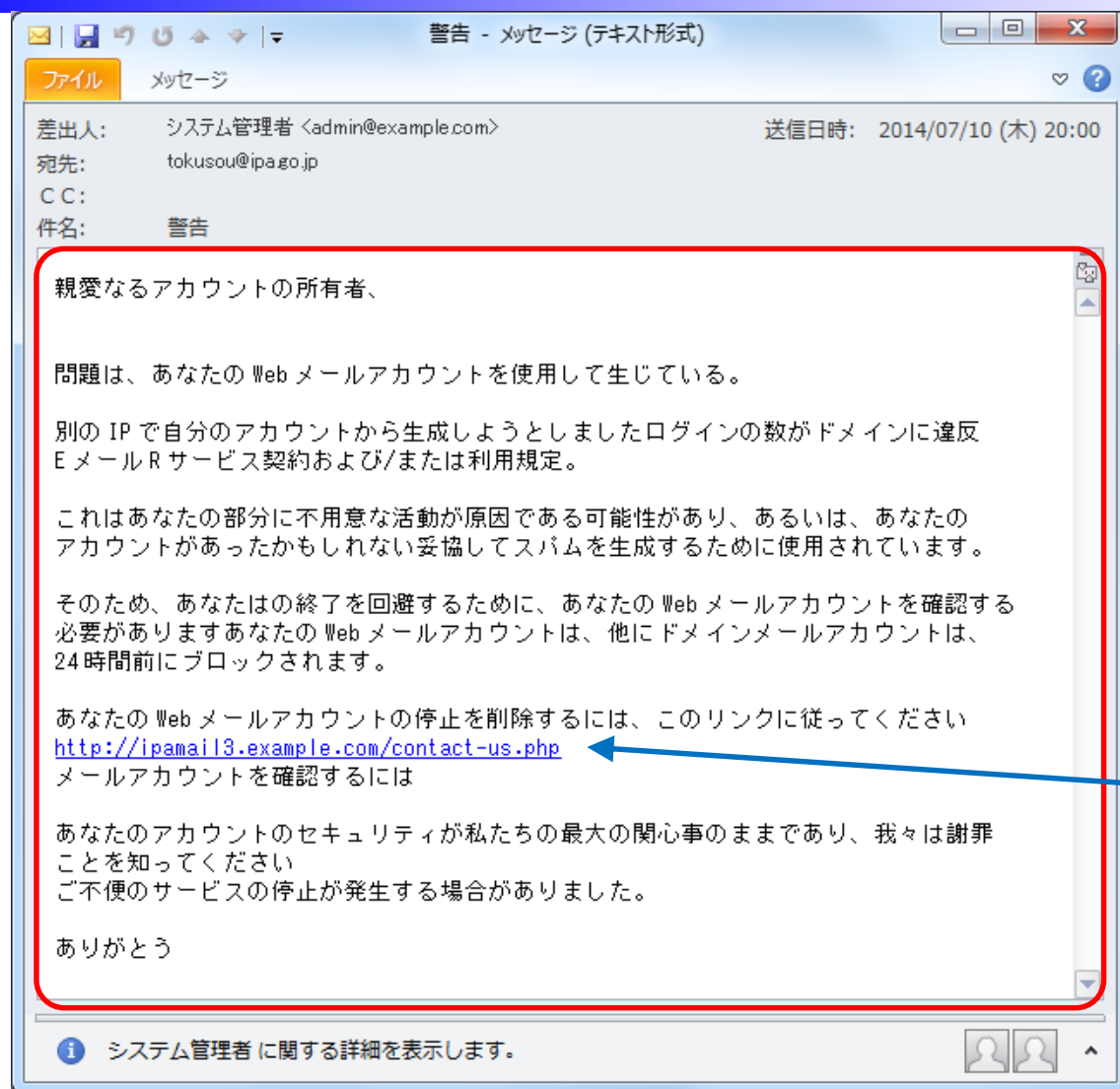
～IDやパスワードの入力を要求する標的型～



IDパスワードを要求

2.5.6 メールサンプル⑥

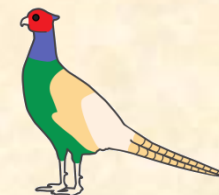
～データエントリー型フィッシング～



窃取されたメールアカウントの認証情報は、SPAMメールの踏み台や、標的型攻撃メールの素材収集に利用される恐れも。

データエントリーを要求

1. 標的型サイバー攻撃への取り組み
2. 標的型攻撃メールの見分け方
3. 添付ファイルの見分け方
4. 標的型攻撃メールを見つけたら



3.1 実行形式ファイルの例

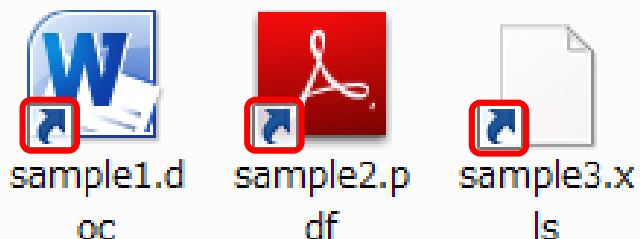
- Windowsデフォルト
 - exe
 - com
 - bat
 - scr
 - cmd
 - pif
- スクリプト拡張子
 - js
 - vbs
- アプリケーション
 - lnk
 - url
 - swf

巧妙に隠される実行形式ファイル
気付くにはいくつかのポイントがあります

- メールから直接開かない！
- ファイルの詳細を必ず見る！

3.2 ショートカットファイル

リンク先にコマンドを保持



アイコン上は文書ファイルの様に見えるが...

ショートカットであることを示す「矢印のマーク」

エクスプローラの詳細表示で見ると...

名前	更新日時	サイズ	種類
sample1.doc	2014/09/18 22:17	2 KB	ショートカット
sample2.pdf	2014/09/18 22:54	1 KB	インターネットショートカット
sample3.xls	2014/09/18 23:18	26 KB	MS-DOS プログラムへのショートカット

ショートカットであることがわかる

コマンドプロンプトで表示すると...

```

C:\> 管理者: コマンド プロンプト

D:\test>dir
ドライブ D のボリューム ラベルは Data です
ボリューム シリアル番号は 7890-0902 です

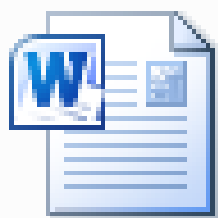
D:\test のディレクトリ

2014/10/03 12:30 <DIR>          .
2014/10/03 12:30 <DIR>          ..
2014/09/18  22:17                1,940 sample1.doc.lnk
2014/09/18  22:54                 256 sample2.pdf.url
2014/09/18  23:18             26,498 sample3.xls.pif
  
```

ショートカットの拡張子

3.3 アイコン偽装

アイコンを他のものに変更



意見書.exe



連絡帳.exe



資料.exe



議事録.exe

全てexeファイルだが、アイコンを変更しているため
ぱっと見、アプリケーションファイルに見える



アイコンや拡張子を信用しない！
 (「ファイルの種類別」を表示して確認する)

- 圧縮ファイルも「ファイル詳細」で見れば
アイコン表示されずにチェック可能

3.4 拡張子偽装 3種

2重拡張子とRLO表示



資料.

doc.exe

拡張子を表示し
ないと見えない



連絡帳.xls

...



資料

rsc.pdf

「RLO」による拡
張子偽装

RLO: Right-to-Left
Override
アラビア語やヘブライ語などを
パソコンで使うための特殊な
文字。右→左

実際のファイル名

連絡帳.xls

.exe

↑ファイル名の中に空白を入れている

実際のファイル名

資料fdp.scr

スクリーンセーバー