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）

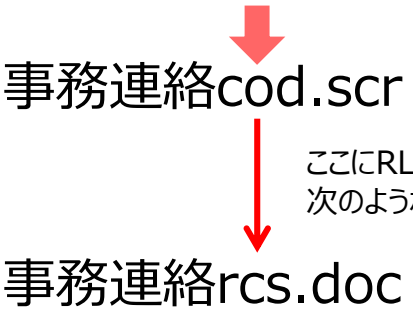
着眼点	過去の標的型攻撃で見られたケース
テーマ	• 知らない人からのメールだが、開封せざるを得ない内容 ① 新聞社・出版社からの取材申込・講演依頼 ② 就職活動に関する問合せ・履歴書の送付 ③ 製品やサービスに対する問い合わせ・クレーム ④ アンケート調査 ⑤ やり取り型メール
	• 誤って自分宛に送られたメールの様だが、興味をそそられる内容 ① 議事録・演説原稿などの内部文書送付 ② VIP訪問に関する情報
	• これまで届いたことがない、公的機関からのお知らせ ① 情報セキュリティに関する注意喚起 ② インフルエンザ流行情報 ③ 災害情報

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	• 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	• 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

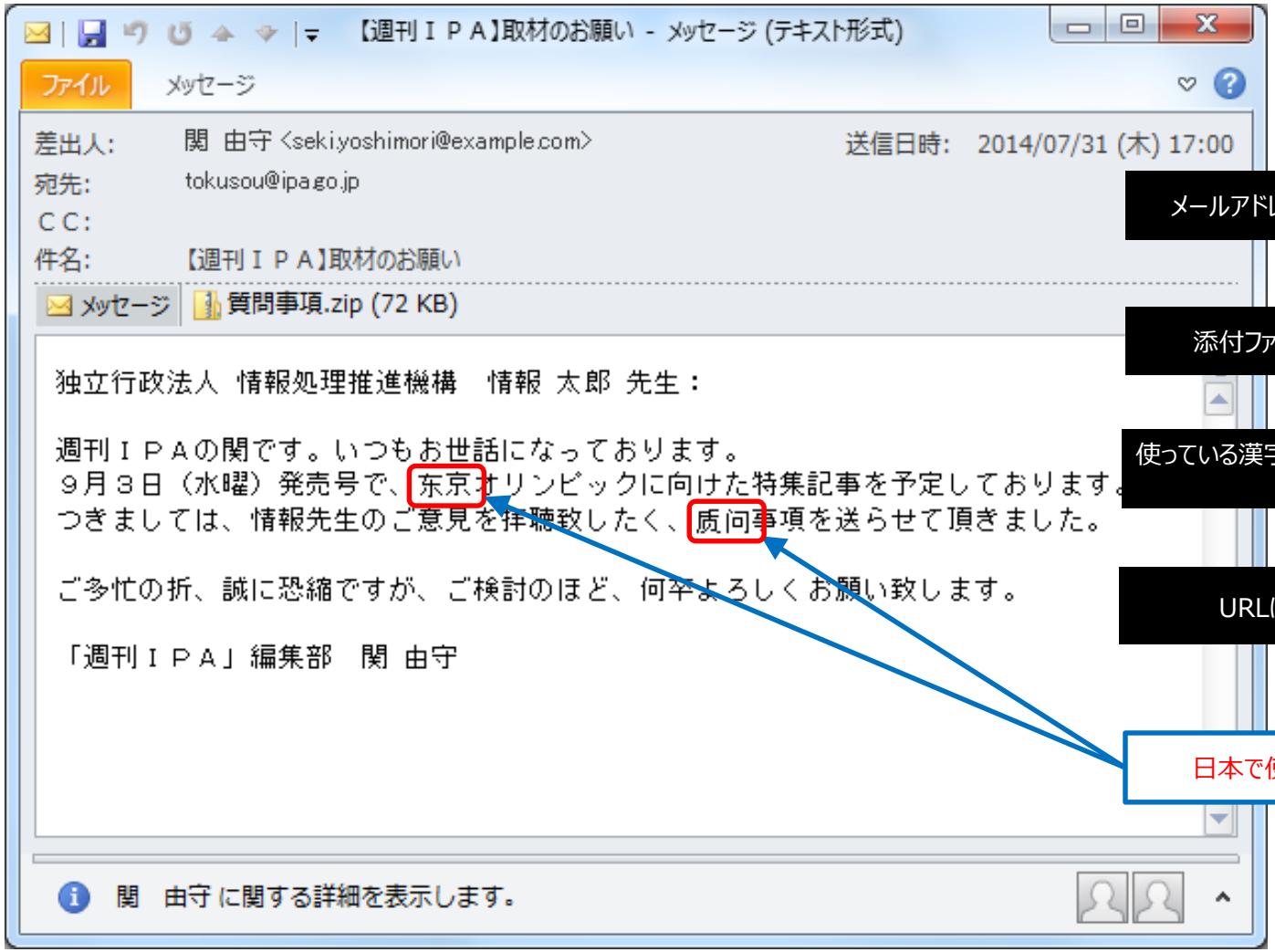
着眼点	過去の標的型攻撃で見られたケース
添付ファイル	• 実行形式ファイル（exe / scr / jar / cpl など）
	• ショートカットファイル（lnk / pif / url）
	• 実行形式ファイルなのに文書ファイルやフォルダのアイコン
	• ファイル名が不審 ✓ 二重拡張子 ✓ ファイル拡張子の前に大量の空白文字を挿入 ✓ 文字列を左右反転するRLOコードの利用 ✓ エクスプローラで圧縮ファイルの内容を表示するとファイル名が文字化け



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）

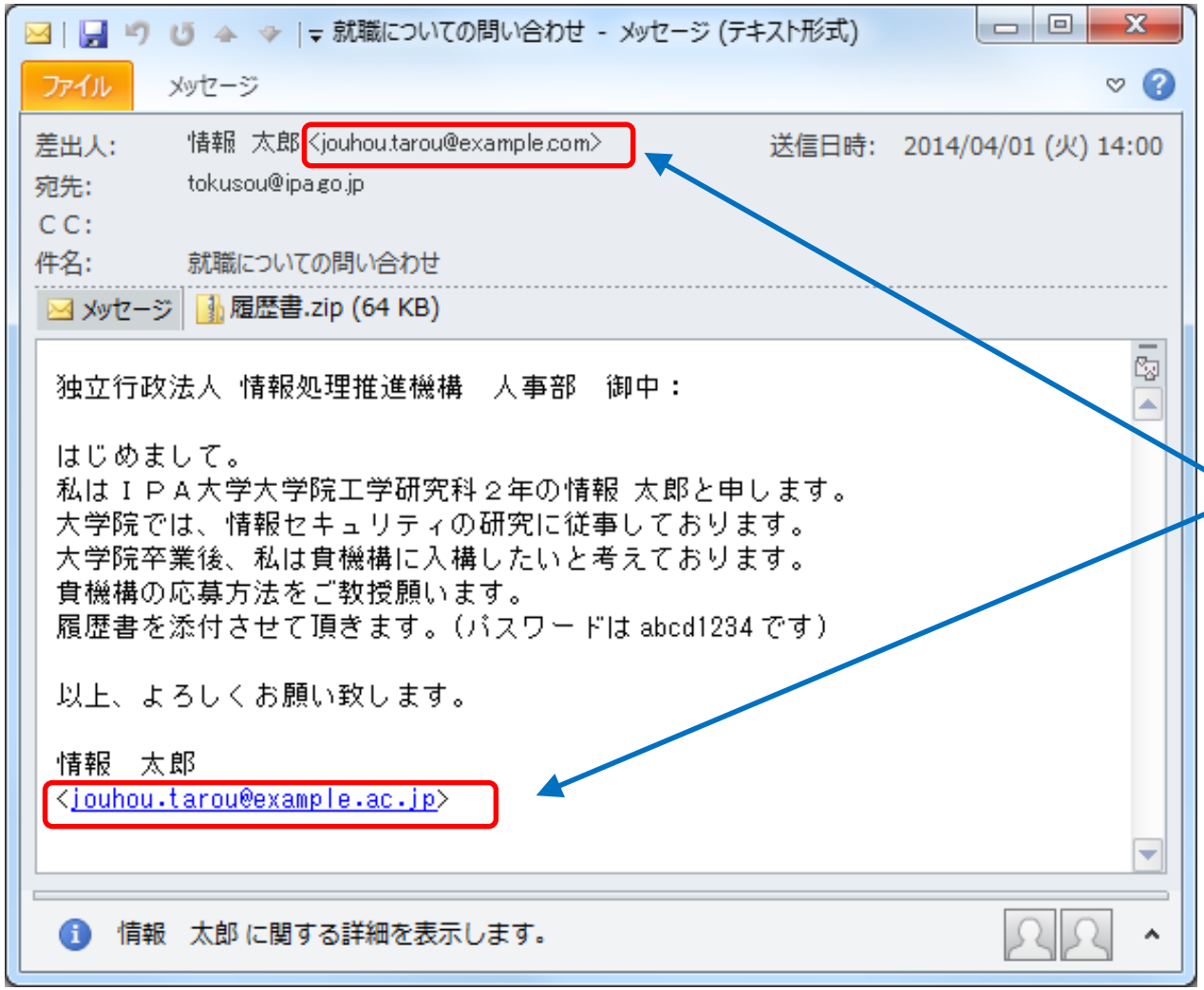
2.5.1 メールサンプル①

～取材を装ったケース～



2.5.2 メールサンプル②

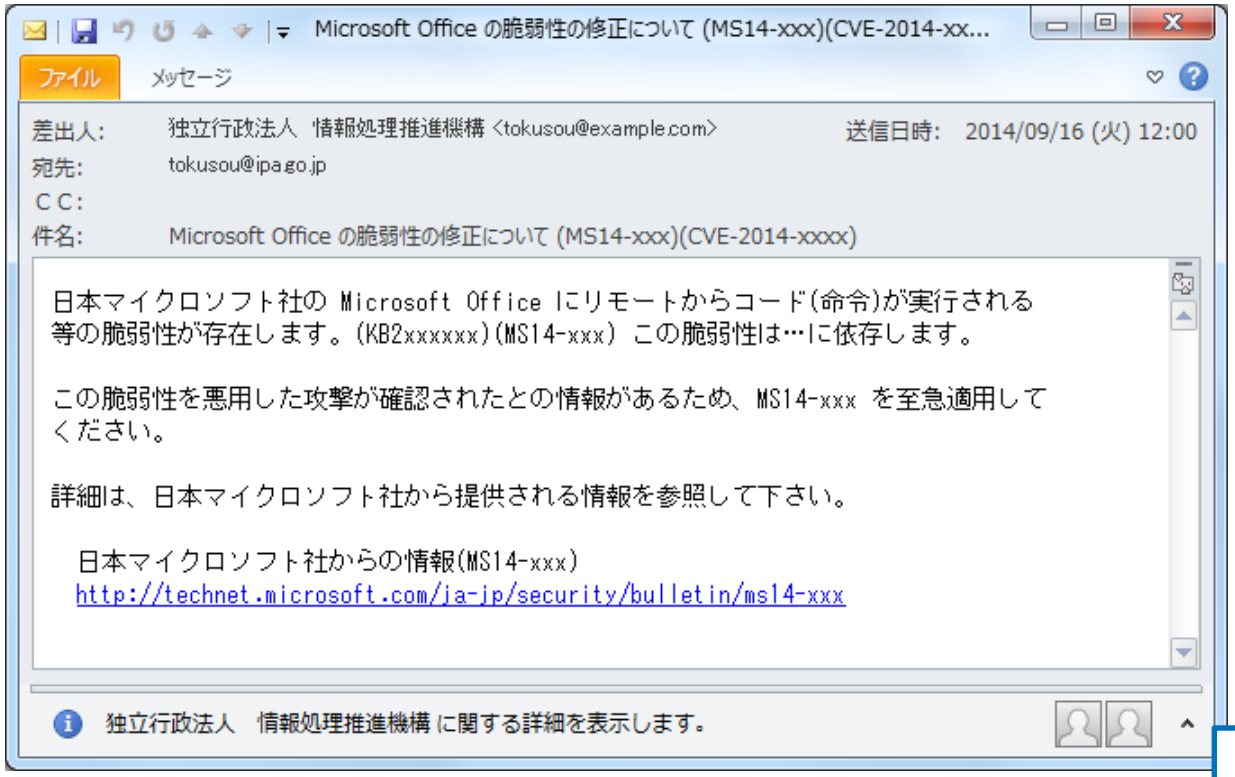
～就職を装ったケース～



署名とメールドメインが違う

2.5.3 メールサンプル③

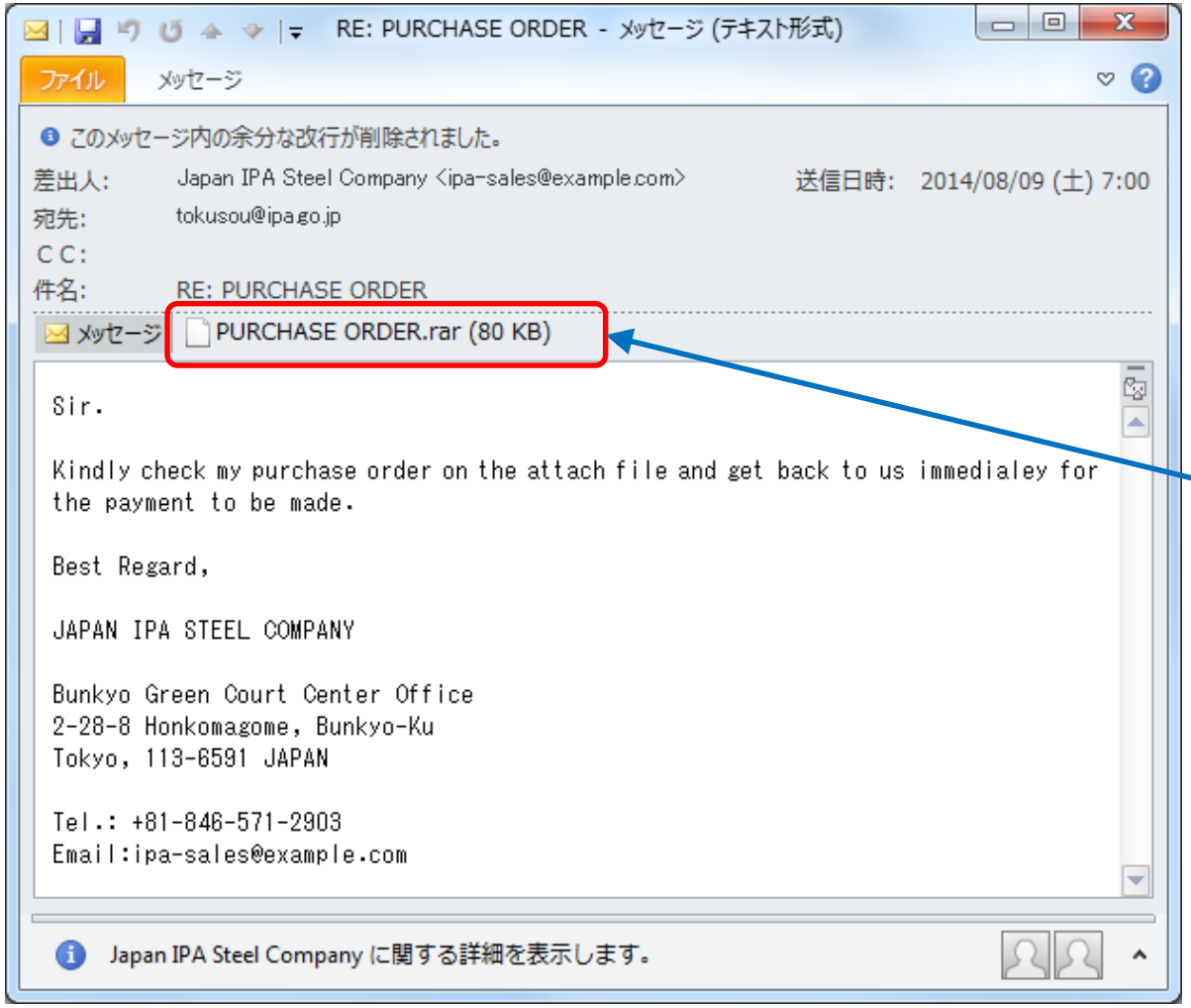
～情報セキュリティに関する注意喚起を装ったケース～



実際にクリックした際に表示されるウェブページのURL

2.5.4 メールサンプル④

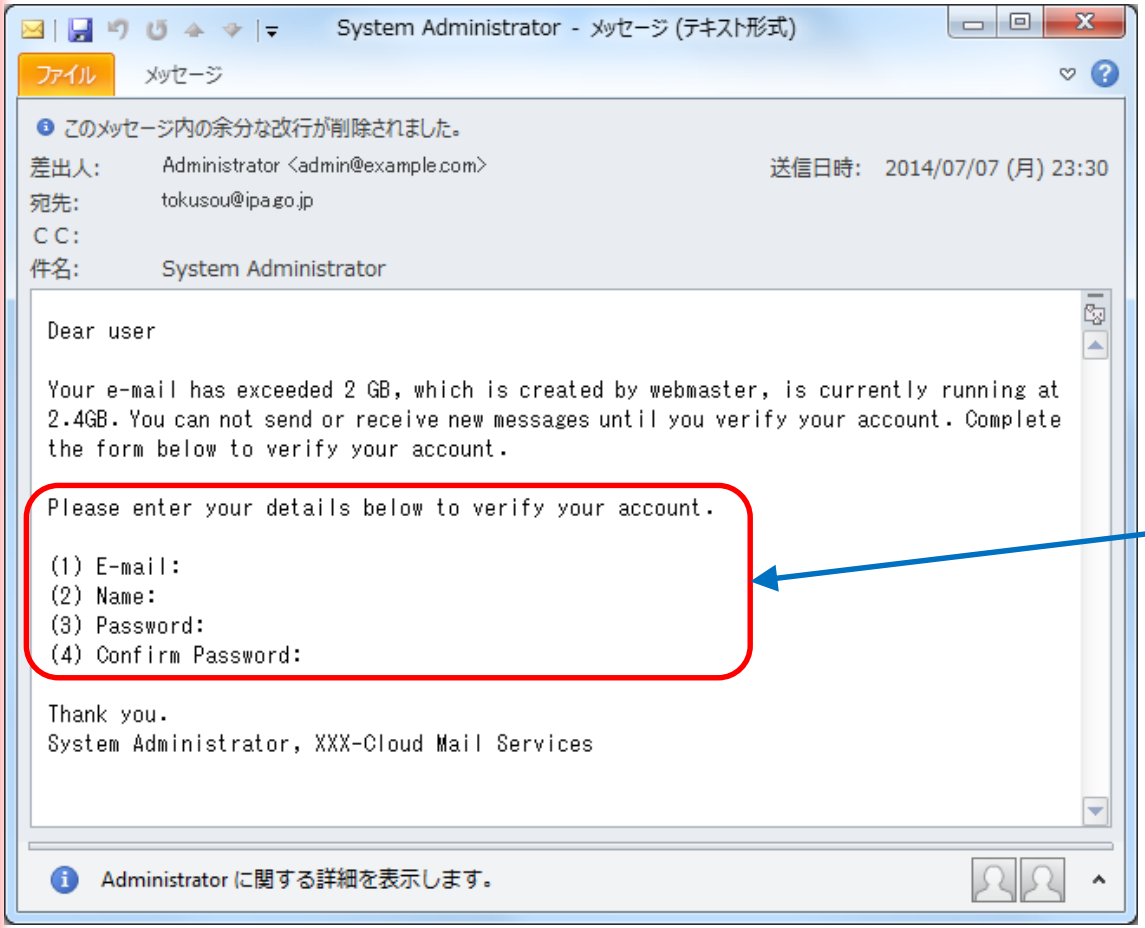
～心当たりのない決済・配送通知を装った標的型～



日本であまり使われない圧縮形式
（rar）

2.5.5 メールサンプル⑤

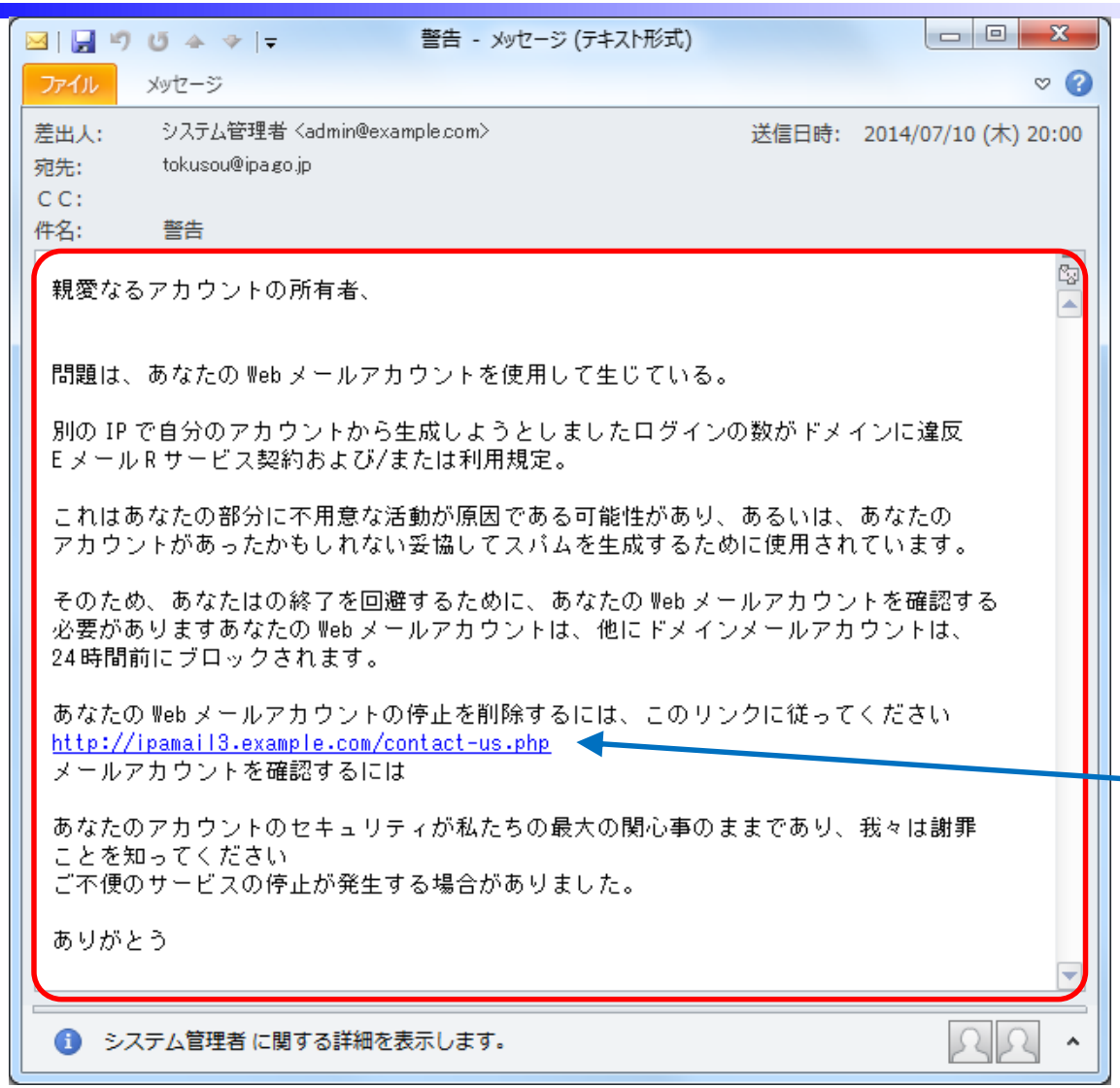
～IDやパスワードの入力を要求する標的型～



IDパスワードを要求

2.5.6 メールサンプル⑥

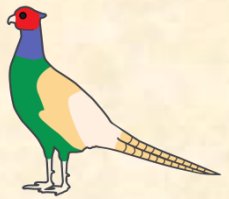
～データエントリー型フィッシング～



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

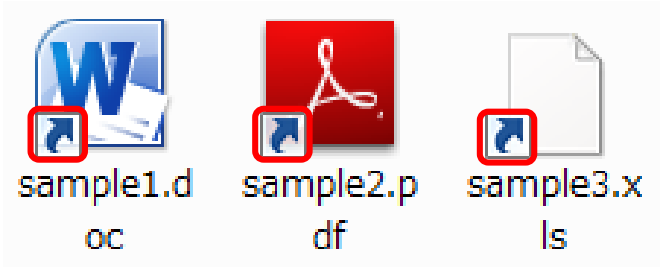
- Windowsデフォルト
  - exe
  - com
  - bat
  - scr
  - cmd
  - pif
- スクリプト拡張子
  - js
  - vbs
- アプリケーション
  - lnk
  - url
  - swf

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

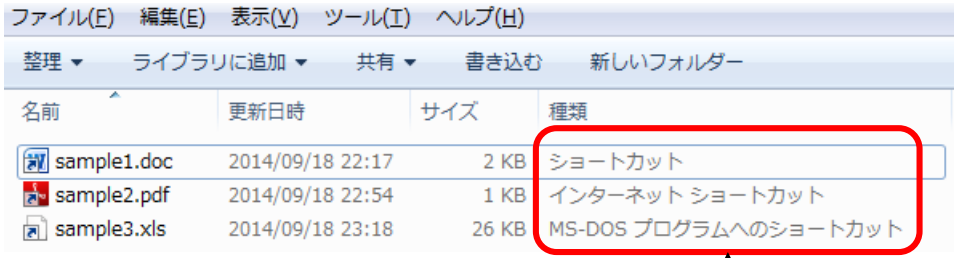
リンク先にコマンドを保持



アイコン上は文書ファイルの様に見えるが…

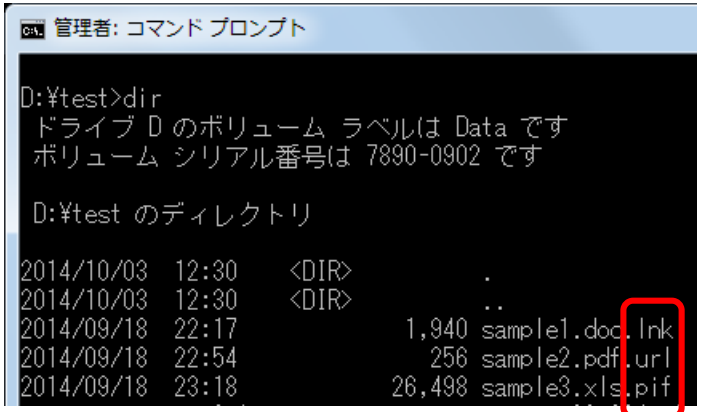
ショートカットであることを示す「矢印のマーク」

エクスプローラの詳細表示で見ると…



ショートカットであることがわかる

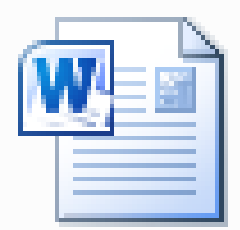
コマンドプロンプトで表示すると…

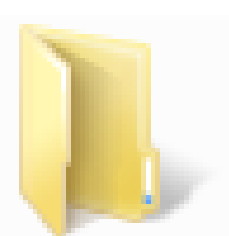


ショートカットの拡張子

3.3 アイコン偽装

アイコンを他のものに変更





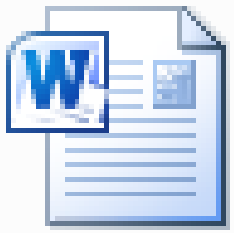
全てexeファイルだが、アイコンを変更しているため
ぱっと見、アプリケーションファイルに見える

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

連絡帳.xls

…

資料
rcs.pdf

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

拡張子を表示しないと見えない

「RLO」による拡張子偽装

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