表1　標的型攻撃メールの偽装の特徴

項目	特徴
サブジェクト	① 知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容 （例1）大学への問い合わせを装ったメール （例2）大学への苦情を装ったメール （例3）研究内容への質問や論文の送付
	② 心当たりのないメールだが、興味をそそられる内容 （例1）議事録、プレゼン資料などの内部文書送付 （例2）他大学学長等の訪問に関する情報 （例3）海外での盗難に対する救済依頼
	③ これまで届いたことがない公的機関からのお知らせ （例1）情報セキュリティに関する注意喚起 （例2）防災情報
	④ 組織全体への案内 （例1）辞令などの人事情報 （例2）学長・理事長からの年次方針説明資料 （例3）全学教授会・FD/SD資料の再送・差し替え
	⑤ 心当たりのない、決裁や配送通知（英文の場合が多い） （例1）航空券の予約確認 （例2）医療費・保険料の通知
	⑥ ID やパスワードなどの入力を要求するメール （例1）メールボックスの容量オーバーの警告 （例2）銀行からの登録情報確認
送信者	⑦ フリーメールアドレスから送信されている ⑧ 送信者のメールアドレスが署名と異なる
本文	⑨ 日本語の言い回しが不自然である ⑩ 日本語では使用されない漢字（繁体字、簡体字）が使われている ⑪ 実在する名称を一部に含むURL が記載されている ⑫ 表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合） ⑬ 署名の内容が誤っている （例1）　組織名や電話番号が実在しない （例2）電話番号がFAX 番号として記載されている
添付ファイル	⑭ 添付ファイルがある ⑮ 実行形式のファイル（exe / scr / jar /cpl 等）の添 ⑯ ショートカットファイル（lnk / pif / url）の添付 ⑰ 拡張子と異なるファイルアイコンに偽装されている （例1）二重拡張子 （例2）拡張子の前に大量の空白文字の挿入