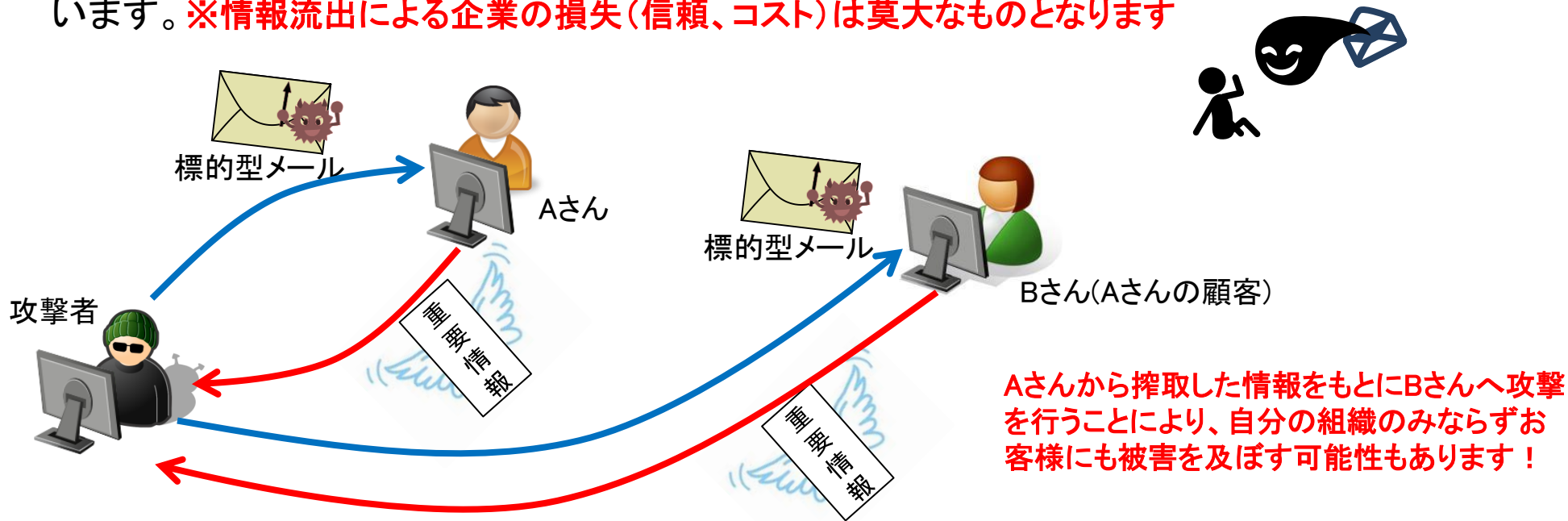


## 【標的型メール攻撃とは？】


- ✓ メールに添付されているファイルを開いたり、記載されているURLにアクセスすることでPCをウイルスに感染させ、遠隔操作で組織の機密情報などを盗むことを指します。
- ✓ 日常の業務内容に近い文面で送られてくるため、不審なメールかどうかの判断が難しいことからうっかり開いてしまうケースが多いのが特徴です。
- ✓ 従来のウイルス対策ソフトでは検知が難しいなどの理由から、「標的型メール攻撃」を受けたことに気づかず**長期にわたり機密情報を流出させてしまう**という危険性を持っています。**※情報流出による企業の損失(信頼、コスト)は莫大なものとなります**



ING WARNING WARNING WARNING WA

## 【標的型メールの主な特徴】

①差出人は実在の人物だがアドレスのドメインが違う

送信者： 攻撃 太郎 <kougeki@kunnrenn**test**.co.jp> 送信日時： 2016年8月4日 10:58  
宛先： 標的 次郎 <hyouteki@kunnren.co.jp>  
CC：  
件名： 【重要】経費精算システムバージョンアップのご連絡  
添付ファイル：  経費精算システム操作マニュアル.exe

②タイトルに【重要】【緊急】などメール受信者がメールを開くことを促すような文言が入っている

③添付ファイルのアイコンと拡張子が異なる

宛先各位

お疲れ様です。総務部の攻撃です。

この度経費精算システムのバージョンアップに伴い新規機能が追加されました。  
通常の経費申請方法も一部変更となりますので、添付のマニュアルを確認のうえ申請をお願いします。

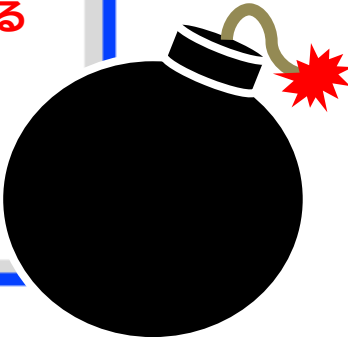
マニュアルは下記URLからも確認可能となっています。

<http://intra.manual/keihi/test/>

④URLが不正（社内イントラにアクセスする文面にも関わらず、実際のURLは外部）

ご不明な点は総務部までご連絡ください。

総務部 攻撃太郎



ING WARNING WARNING WARNING WA

## 【標的型メールを受信した際の対処方法】

- ✓ 一見業務と関係のあるメールのように見えても、差出人や内容をきちんと確認を行ったうえでアクセスを行う
- ✓ 不審なメールを受信した場合、自社の規定に則り、しかるべき担当者(窓口)に報告を行う
- ✓ 万が一不審なメールのURLをクリックしたり、添付ファイルを開いてしまった場合は、即座にネットワークから切断し、担当者(窓口)に報告を行う

## 【最後に】

- 標的型メールとは何か理解できましたか？
- メールを受信した際の対処方法は理解できましたか？
- 何かあった際の自社の担当窓口を把握していますか？



ING WARNING WARNING WARNING WA