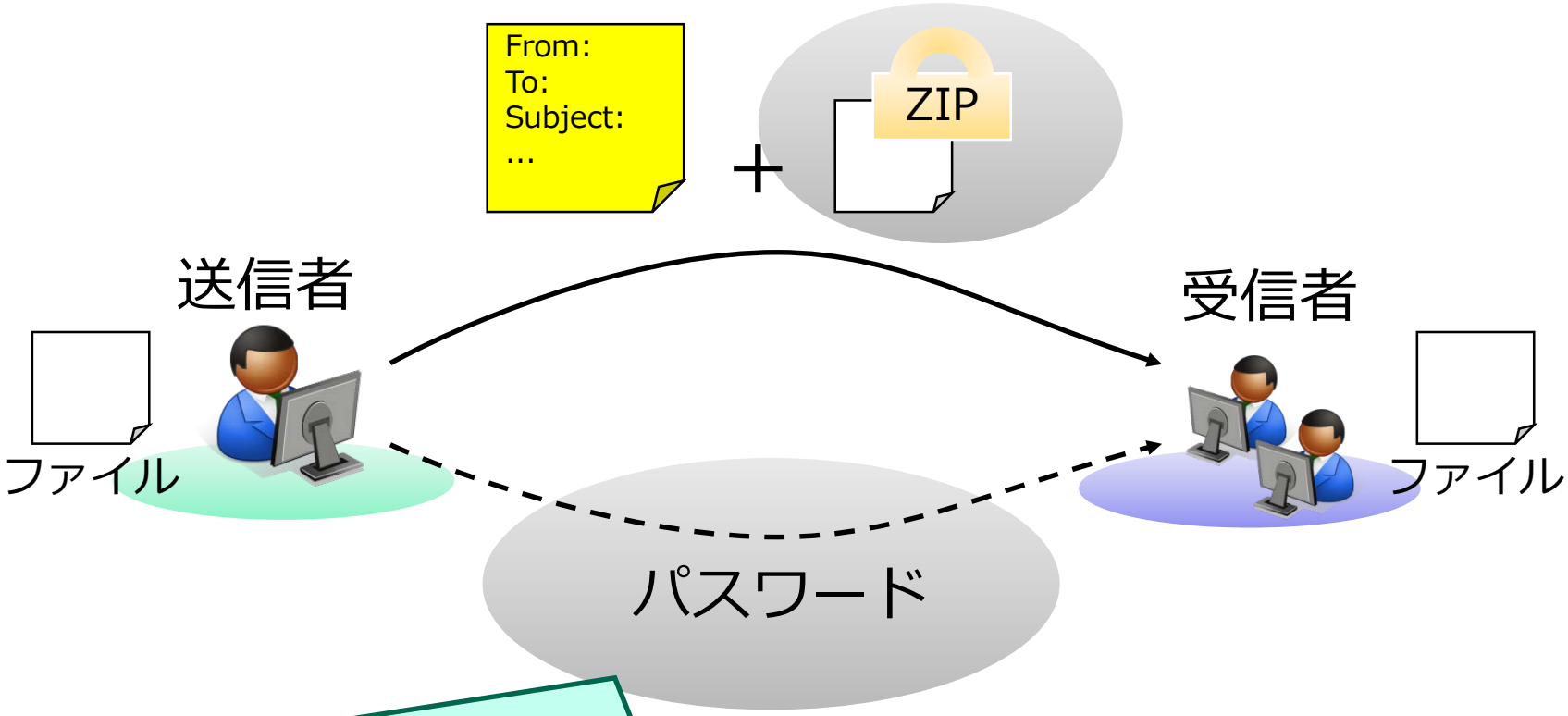
T17
組織間の安全なファイル送受信を考える
～暗号化ZIPは何のため～

木村泰司

一般社団法人 日本ネットワークインフォメーションセンター

ZIPファイルによるファイルの送受信



ZIPファイルにかけたパスワードを相手に伝えることでファイルを(セキュアに)共有する。

なぜこの方法なのか

- **セキュリティ**
  - 情報漏洩対策
    - メールの誤送信
- **認定基準をクリアするため(?)**
  - Pマーク，ISMS/ISO27001
- **その他…**
  - あとでファイルを取り出しやすい
  - 担当者が変わってもファイルが取り出しやすい
  - 今までのユーザ環境を使ってできる
  - 顧客/親会社などに指定された

6つのキーワードで読み解く

そのパスワードをどう伝えるか(1)

- 会議などで予め伝えておく
- 別の手段で伝える
  (電話/口頭/別アドレスに送信 ...)
- 次に送るメールで伝える

1

パスワードの伝達方法

そのパスワードをどう伝えるか(2)

パスワードの伝達方法

1

について考えてみる。

- **想定外の人にパスワードが届いてしまったら...(二通目のメールは?)**
- **パスワードが伝わる相手を把握できているか**
  →ファイルを開ける人の範囲は?

パスワード自体は強いのか(1)

- 第三者による推測が難しいように生成する
- 定期的に変更する　例：work2016
  ※ここでは定期変更自体の有効性は議論しません
- 都度、新たなパスワードを生成する

2

パスワードの強さ

パスワード自体は強いのか(2)

パスワードの強さ

2

について考えてみる。

- **オフラインでパスワードを色々試すと解けてしまうのでは？**
- **推測可能なパスワードに意味はあるのか？**
- **都度生成すると、複数の盗聴をしようとする人には困難になりそうだが...(毎回セキュアに伝達する必要が出てくる)**

ファイルを暗号化する方法は...?(1)

- ZIPファイルで暗号化
- アプリケーションの機能を使って暗号化
- OSの機能を使って暗号化
- GnuPGでファイル/メールを暗号化
- S/MIMEでメールを暗号化

3

暗号や仕組みとしての強さ

ファイルを暗号化する方法は...?(2)

暗号や仕組みとしての強さ

3

について考えてみる。

- **ZIPファイルの暗号アルゴリズムは総当たり攻撃に対して弱い？**
- **GnuPGやS/MIMEの公開鍵暗号技術を使えば秘密のパスワードを伝えなくてよくなるが?**

パスワード解析にかかる時間(参考)

測定結果

桁数	4桁	6桁	8桁	10桁
英小文字　(26字)				
ZIP	1秒以下	1秒以下	46秒	9時間
ZIP(256bitAES)	1秒以下	5分	2日	4年
DOC	1秒以下	26秒	5時間	136日
DOCX	20秒	44分	105日	195年
英大小文字+数字　(62字)				
ZIP	1秒以下	13秒	13.5時間	6年
ZIP(256bitAES)	14秒	15時間	7年	26千年
DOC	1秒以下	1時間20分	211日	2,218年
DOCX	10分42秒	29日	301年	1,158千年
英大小文字+数字+記号　(93字)				
ZIP	1秒以下	2分24秒	14日	341年
ZIP(256bitAES)	1分11秒	7日	169年	1,462千年
DOC	6秒	15時間	15年	128千年
DOCX	55分	326日	7,800年	66,726千年

ZIPに設定したパスワードの強度と暗号化(AES256)について
http://www.zippassword.net/510.html

第2回：そのパスワードで大丈夫？ ～ GPGPUによる高速パスワード解析
暗号化ファイルと無線LANパスワード解析スピード
http://www.dit.co.jp/report/security_report/forensic_center/20141001.html

なぜZIPファイルで送るのか(1/4)

4 利便性

5 ルール/基準

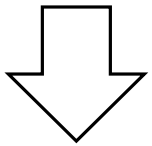
6 ファイル送受信の目的

なぜZIPファイルで送るのか(2/4)

4

利便性

- 色々な環境で復号できる
- 新たな仕組みを必要としない (通信の要件 / 準備 / 習得やその共有)



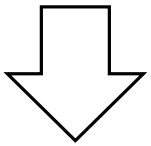
- 利便性を下げてしまうと改善策が普及しにくいと考えられる。

なぜZIPファイルで送るのか(3/4)

5

ルール/基準

- ルールを守るため/認定基準をクリアするため



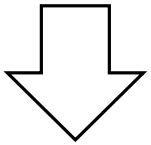
- 認定基準をクリアする「解」になっているか?
  本当は別の方法でもOKかも。

なぜZIPファイルで送るのか(4/4)

6

ファイル送受信の
目的

- 後で取り出せるようにするため(アーカイブ)
- 丁寧に送った感じがする(ユーザエクスペリエンス)



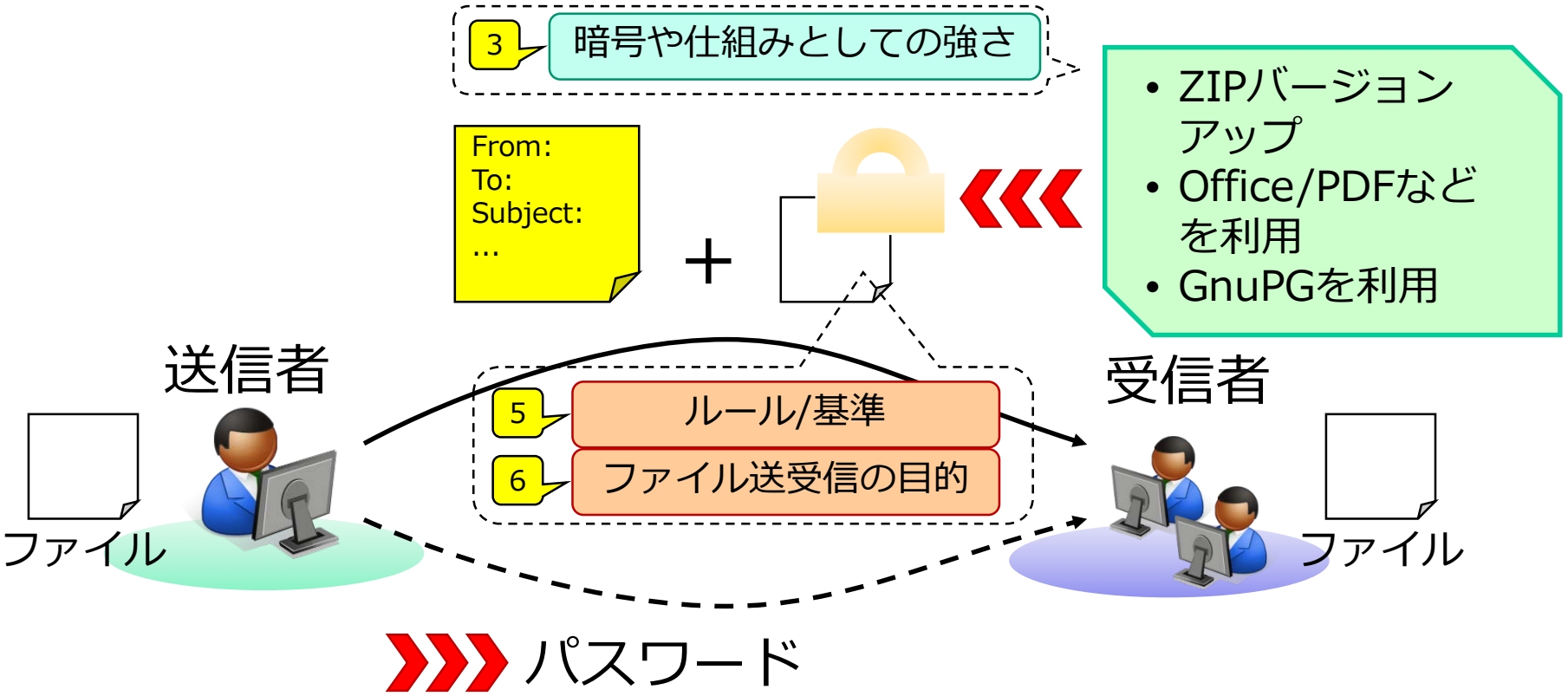
- 本当の目的を「見抜いて」改善できないか?

6つのキーワード

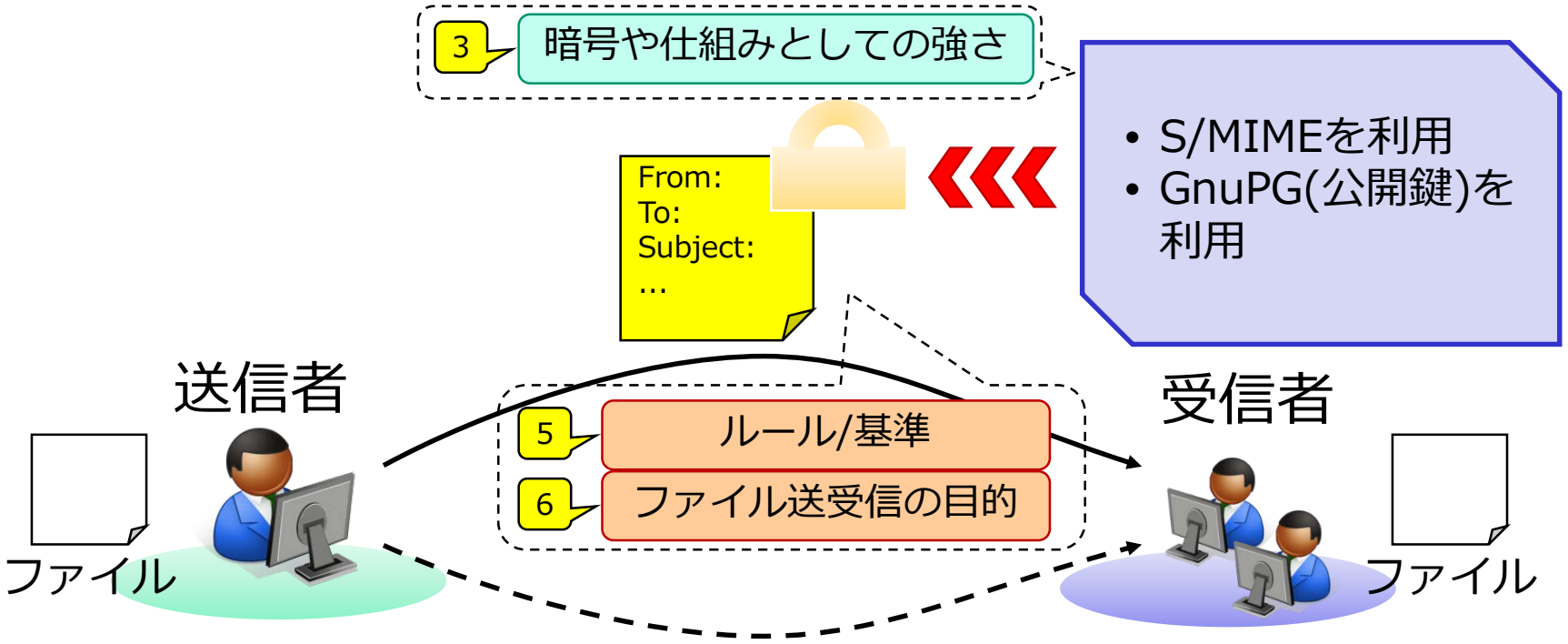
1. パスワードの伝達方法
2. パスワードの強さ
3. 暗号や仕組みとしての強さ
4. 利便性
5. ルール/基準
6. ファイル送受信の目的

改善の方向性

(1)暗号化方式とパスワードを見直す



(2)GnuPGやS/MIME

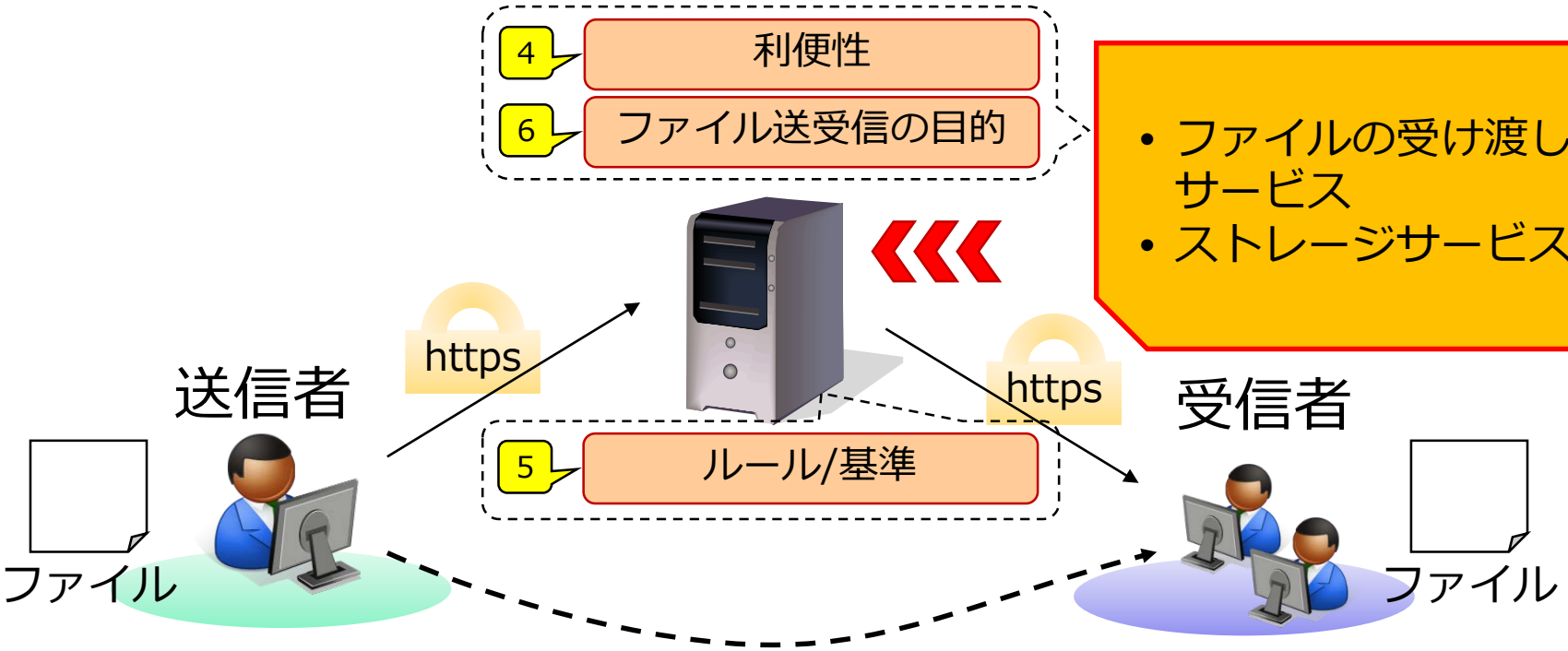


相手の鍵の確認

- 相手の担当者の鍵を初回のミーティングで確認する(名刺にフィンガープリント印刷)
- 双方で使える認証基盤を決める(JCANなど)

パスワードの問題はなくなり、鍵の管理に配慮することになる。

(3)ファイルの受け渡しサービス



パスワード/認証情報を共有

- 送信相手だけが取り出せるように設定する
- パスワードを難しくする
  文字数(10桁)　文字種(大小 英数字 記号)
- 別の経路で伝わる範囲を確認して伝える

1 パスワードの伝達方法

2 パスワードの強さ

セッションの流れ

セッションの流れ

- **イントロダクション**
  - 暗号化ZIPは何のため？(このお話)
- **チュートリアル**
  - チュートリアル GnuPGとS/MIME ～組織間での利用を見据えて～(中村素典さん)
  - クラウドサービスを使った安全なファイル送受信について～サービス選定の注意点～(安福広さん)
- **パネルディスカッション**
  - ファイルの受け渡しにまつわるケーススタディ(中津留さん/中村素典さん/安福広さん/大泰司さん/木村)