

セキュリティ・ミニキャンプ in 広島 2021

PPAPからの脱却

2021年11月26日

合同会社PPAP総研（法人番号：5010003033116）

代表社員 大泰司章

今日のお話

パスワード付きzipファイルとパスワード送付（PPAP 運用）の問題点を挙げ、ファイルを安全に送るにはどうすべきかを、セキュリティのみならず業務効率の面から、PPAP問題の第一人者が語ります。

0. はじめに
1. PPAP問題とは
2. 脱PPAPの方法
3. DXを阻む三大商習慣

0. はじめに

会社案内

- 合同会社 PPAP総研
(法人番号：5010003033116)
- 私たちは、PPAP、PHS、ネ申エクセル等の不合理な電子化を排し、真の業務の効率化と働き方改革を目指すコンサルタント集団です。
- 業務範囲： 電子契約、EDI、ERP、fintech、メールやWebサイトのなりすまし対策、メール送信マナー、サプライチェーン効率化、情報セキュリティ、営業秘密（個人情報）保護

法人プロフィール

CSVダウンロード

PDFダウンロード

【法人基本情報】

法人基本情報 (3情報)

法人番号	5010003033116
法人名	合同会社P P A P総研
法人名ふりがな	ぴーぴーえいぴーそうけん
法人名英語	
本店所在地	東京都中央区銀座1丁目22-1 銀座大竹ビジデンス2F (法人番号システム)

Webサイト作成中

<https://www.sharepages.jp/company/pri/>



合同会社PPAP総研

事業紹介

会社紹介

Q&A

会社概要

資料請求

CONTACT

PPAP総研テストテストテスト

PPAP総研テストテストテスト

プロフィール



PRI

- 三菱電機→JIP→JIPDEC→PPAP総研
営業/マーケティング/コンサル
営業現場で紙とハンコの山と格闘
電子契約、電子署名、メールのなりすまし対策
- Facebookにて以下のグループを運営
 - ◆ 【マイナンバー】 みんなで使おう法人番号
 - ◆ 電子契約元年
 - ◆ くたばれPPAP！

主な役職



- JIPDEC客員研究員（トラステッドサービス）
- 日鉄ソリューションズ株式会社 電子契約コンサルティンググループ特別顧問
- ペーパーロジック株式会社 顧問（電子契約）
- SKJコンサルティング合同会社 プリンシパル 電子契約コンサルタント
- 株式会社スマイルワークス プロジェクトマネージャー（ERP、EDI、FINTECH）
- シヤチハタ株式会社 エバンジェリスト（電子印鑑、決裁、署名）

【マイナンバー】 みんなで使おう法人番号

PRI

電子契約元年

PRI

電子契約元年

電子契約元年

公開グループ

情報

ディスカッション

メンバー

イベント

動画

写真

グループインサイト

動画ウォッチパーティ

グループを管理

グループのクオリティ

このグループを検索

ショートカット

参加済み

お知らせ

シェア

その他

投稿する

写真・動画

ライブ動画

その他

投稿のカテゴリを設定しよう + トピックを作成

投稿にトピックを追加して、グループのメンバーが興味がある情報を見つけやすくしよう。

くたばれPPAP！



1. PPAP問題とは

PPAPとは

Passwordつきzip暗号化ファイルを送ります

Passwordを送ります

Aん号化

Protocol

Internet Week 2016

- 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～

17:45
～
18:45

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



木村 泰司 大森司 章 中津留 勇

モデレータ

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)

パネリスト

大森司 章(一般財団法人日本情報経済社会推進協会)

中津留 勇(SecureWorks Japan 株式会社)

中村 素典(国立情報学研究所)

安福 広(NRIセキュアテクノロジーズ株式会社)

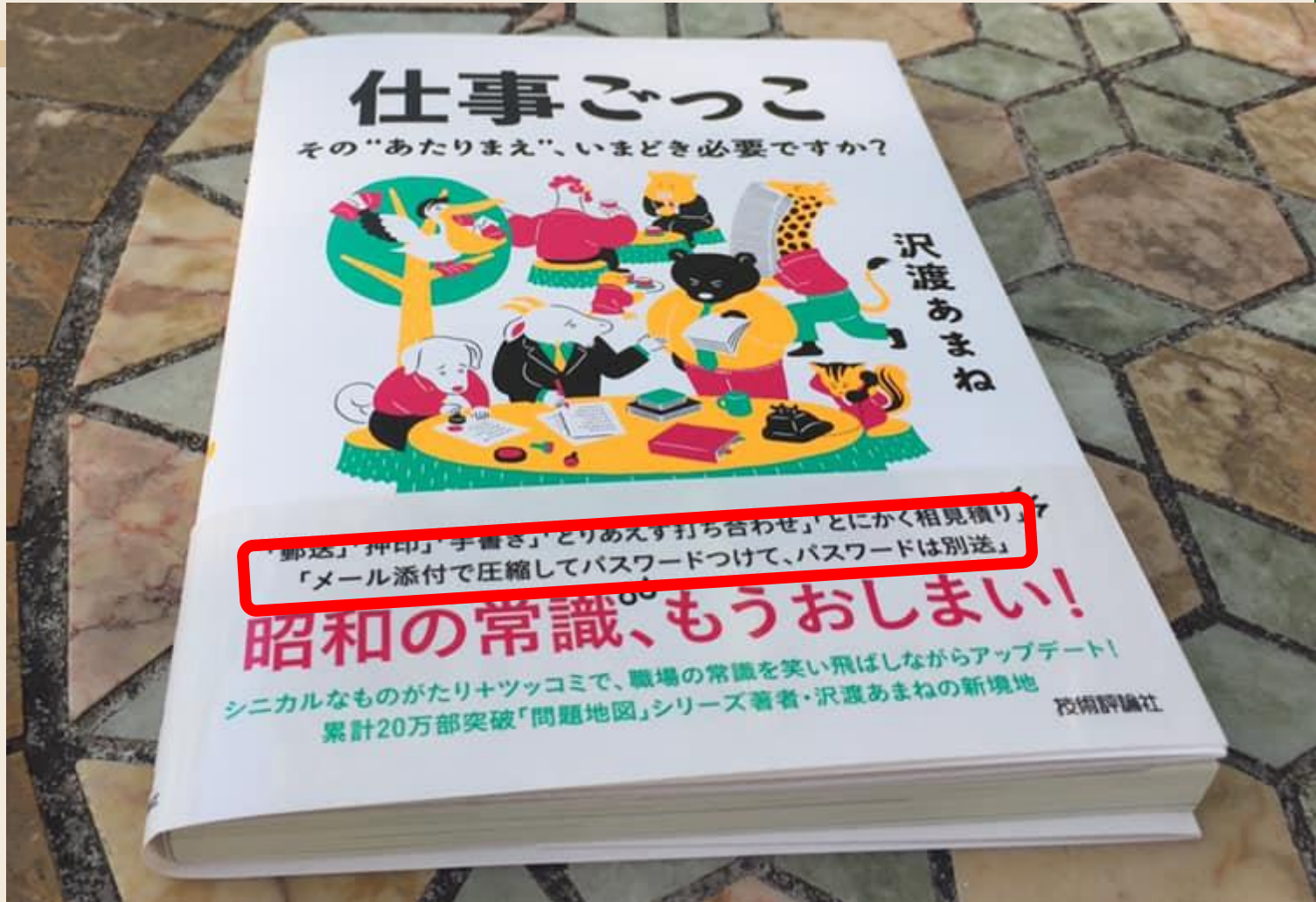
マルウェア対策ソフトウェアとの関係や、クラウドサービスを使ったファイルの受け渡し、IPSなどのセキュリティ機器との関係を含めてディスカッションします。

JIPDECのZIPLOC (2017年)



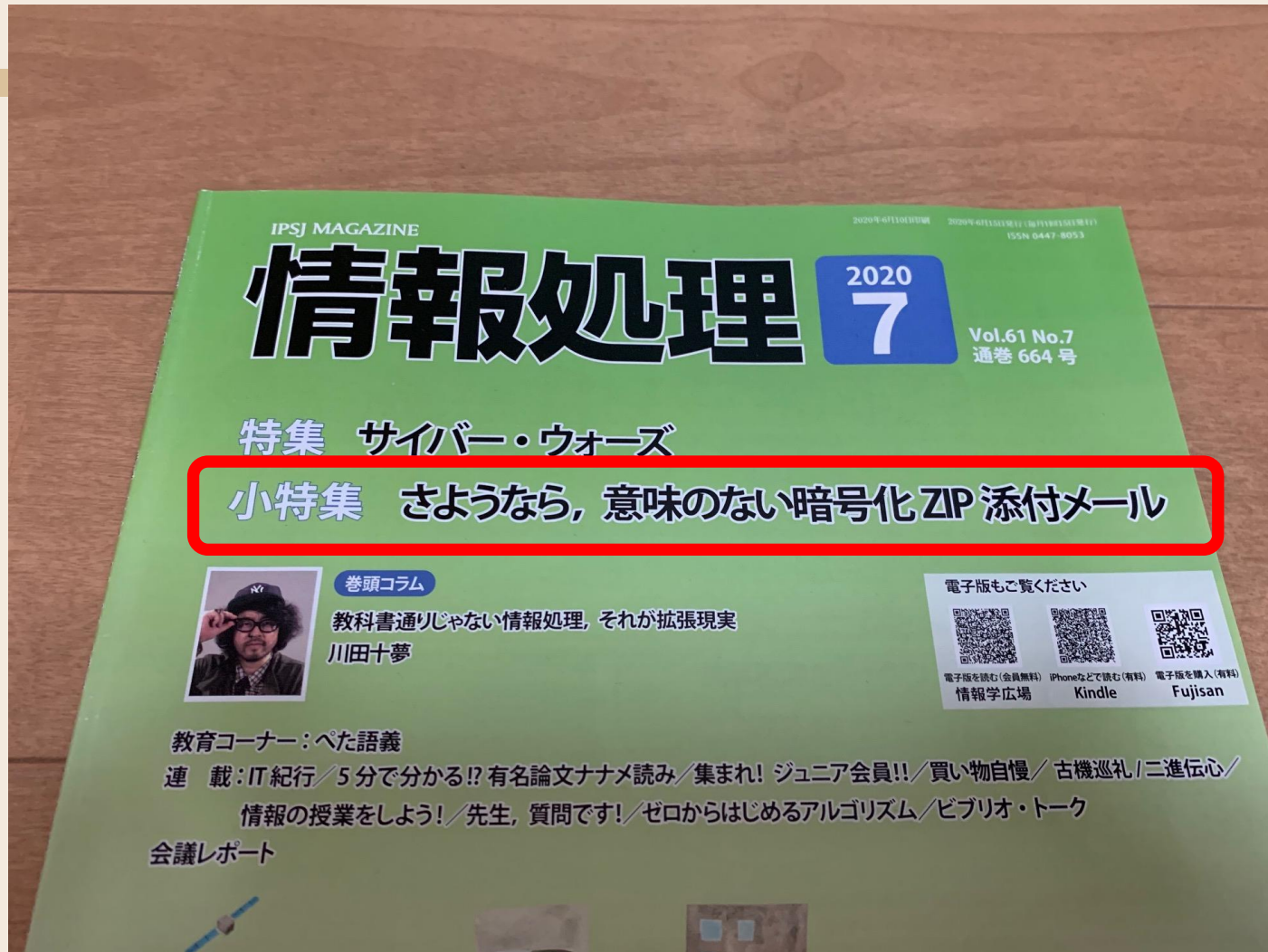
ベストセラーに掲載（2019年7月）

PRI



情報処理2020年7月号に掲載

PRI



マルウェアEmotetでPPAPが悪用

PRI

- 2019年末に蔓延
Wordファイル形式による添付 →マクロを実行させる
本文にURL →マルウェアをダウンロードさせる
- 2020年7月から第2波
パスワード付きzipファイルの添付で、マルウェアフィルタを回避
- IPA（独立行政法人情報処理推進機構） 2020年9月2日追記
「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」
- JPCERT/CC（JPCERTコーディネーションセンター） 2020年9月4日公表
「マルウェア Emotet の感染拡大および新たな攻撃手法について」

デジタル改革アイディアボックスで1位に

アイディア一覧（総合） 人気順1～5位

※11/6（金）時点で評価ポイント（賛成票数－反対票数）が高い順

- | | | |
|----|--|--|
| 1位 | 4. 省庁職員の声
232ポイント
249票
45コメント
一般
モグラさん | 暗号化した添付ファイルを送って、その直後にパスワードが来るPPAPと言われる日本特有のメールの悪慣習はセキュリティ上も意味がないと言われているし、管理を煩雑にしている。行政はPPAPをやめる、PPAPを受け取らない、としたらどうか。 |
| 2位 | 2. IT業界の声
184ポイント
228票
295コメント
一般
タナックス太郎さん | インターネットでの投票を実現してほしい。最近の投票率は50%を切るなど低迷している。20代は最も低い。インターネット投票を導入したら、投票率の上昇につながると思う。投票所に向く手間も省け、より気軽に選挙に参加できると思う。 |
| 3位 | 2. IT業界の声
145ポイント
166票
30コメント
一般
nabeponさん | 日本では公的機関でIEを前提とするものが多いが、セキュリティ面の懸念から使用するべきでない。IEの使用は危険が伴うとして非推奨だと宣言すべき。IE以外の使用が難しければ、Chromiumをベースにした日本国家のブラウザを作れば済む。 |
| 4位 | 1. 生活者・事業者の声
131ポイント
131票
23コメント
一般
ZZOさん | 国家資格は全てマイナンバーカードに登録可能にしてほしい。集約により携帯枚数が減るし、数年ごとの顔写真の更新が一括で行われるようになれば、「なりすまし」検出の手助けにもなるのではない。 |
| 5位 | 1. 生活者・事業者の声
120ポイント
139票
28コメント
EpochMaking_Piiさん | 高齢者や身体障害者、持病を持った人を投票所まで連れて行き、新型コロナウイルスなどの感染をしないか心配しながら投票して貰わなければならないので「マイナンバーカード」を使って自宅や施設からオンライン投票できるようにしてほしい。 |

14

※出典：https://www.kantei.go.jp/jp/singi/it2/dgov/houan_wg/dai3/siryou1.pdf

平井大臣がPPAP廃止に言及

PRI



平井卓也 (ひらいたくや)

@hiratakuchan

...

PPAPやめます。 #平井卓也 #デジタル庁 bit.ly/3IKU6l2

午前7:47 · 2020年11月18日 · Twitter for iPad

166 件のリツイート **79** 件の引用ツイート **970** 件のいいね

※出典：twitter

日立製作所がPPAP全面禁止？








PRI

ニュース解説 + 連載をフォロー

日立がPPAP全面禁止へ、「秘文」の添付 ファイル自動暗号化ツールも既に販売終了

大川原 拓磨 日経クロステック／日経コンピュータ

2021.01.21
有料会員限定

※出典：日経XTECH

<https://xtech.nikkei.com/atcl/nxt/column/18/00001/05086/>

そして、奇跡が起きました...

PRI



ピコ太郎(PIKOTARO)(公式)

@pikotaro_ppap

日立さんが禁止に？

ピピい



この一木なんの木

リンゴの木

パイナポーも生えてる木ですから...

生えたら生えたで

ペンを刺すでしょう



会社名	PPAPの利用状況	脱PPAPの予定
NEC	当社グループで利用していない	—
NTTデータ	全社ポリシーで、電子メールにはファイルを添付せず、当社が提供するファイル共有サービスやコンテンツ・コラボレーション・プラットフォームを使用させている。ただし顧客との合意に基づきPPAPを利用する場合もある	2021年度にPPAPの使用を禁止する方向で社内規程を改訂予定
SCSK	現在ルールを含め検討中	回答なし
TIS	利用している	問題は認識しているが、現時点では廃止の予定はない
伊藤忠テクノソリューションズ(CTC)	数ある選択肢の1つとして使用している	予定はないが、今後の方向性について検討中。また既にチャットサービスやファイル共有サービスなどを並行して活用している
日本IBM	利用していない	—
日本ユニシス	2019年10月から当社グループで利用していない	—
日立製作所	利用している	2021年度の社内規則改正時に利用禁止とすることを検討している
富士通	利用しており、会社のセキュリティルールで禁止も推奨もしていない。最低限の対策と理解し容認している	廃止する方向で検討中
野村総合研究所(NRI)	グループ会社のファイル共有サービス利用や暗号化措置など、規程を設けて運用している。ただし詳細に関しては社内のセキュリティに関する事なので、回答できない	回答なし

表 大手ITベンダーの「脱PPAP」対応状況

大手ITベンダーの10社に6社が「脱PPAP」へ（注：2020年12月～2021年2月に日経コンピュータが調査）

※出典：日経XTECH

<https://xtech.nikkei.com/atcl/nxt/column/18/01609/032900001/>

日立グループにおけるパスワード付きZIPファイル添付メール(通称PPAP)の利用廃止に関するお知らせ

2021年10月8日
株式会社日立製作所

日立グループは、2021年12月13日以降のすべてのメール送受信において、パスワード付きZIPファイルの利用を廃止させていただくことを、お知らせいたします。

パスワード付きZIPファイルが添付されたメールは日立グループにて送受信されず、受信者/送信者の日立グループ従業員に対して、配送を抑止した旨がメールで通知されることとなります。

お客さまおよびお取引先さまにおかれましては、日立グループとのデータの授受の方法につきまして、適宜担当者にご相談頂きますと幸いです。

弊社施策に対するご理解とご協力を賜りますよう、何卒よろしくお願い申し上げます。

背景

従来、通称PPAP*は、多くの人々が利用可能で通信経路上の暗号化を保證する方式として日立グループにおいても利用されてきました。しかし、すでに暗号方式としてセキュリティを担保できるものでなく、昨今はパスワード付きZIPファイルを添付することでセキュリティチェックを回避する、Emotet(エモテット)やIcedID(アイスド アイディー)、QakBot(Qbot)などのマルウェアが広まっています。

こうした背景のもと、日立グループだけでなくお客さまや取引先さまのセキュリティを確保するために、日立グループ全体でPPAPを廃止することを決定しました。

※出典：日立製作所Webサイト <https://www.hitachi.co.jp/information/info/20211008.html>

ホーム > PPAPに対する当社運用の変更について

パスワード付きzipファイルが添付されたメールおよび別送のパスワード記載メール (PPAP) に対する当社運用の変更について

メールにファイルを添付して送信する際、「パスワード付きのzipファイルと、そのパスワードを別送する」という手順で行われている情報セキュリティ対策手法、いわゆる「PPAP」につきまして、当社は2022年1月26日より、社外の方からのIIJアドレスへのメール送信における対応を、原則として以下のように変更いたします。

2022年1月25日以前	従来通り、パスワード付きzipファイルが添付されたメールを受信する
2022年1月26日以降	パスワード付きzipファイルをフィルタにより削除し、メール本文のみ受信する

また、IIJより社外の方へパスワード付きファイルを添付し送信する場合においても、今後順次別の手段へ変更いたします。

上記の変更にとまもない、ファイルを共有するための別的手段を用意し、移行いたします。その利用につきましては、お客様、お取引先様に、個別にご連絡を差し上げます。

変更に至った背景

メールにパスワード付きのzipファイルを添付して送信し、そのパスワードを後送する「PPAP」は、日本において多く見られる情報セキュリティ対策の一つですが、効果が薄いだけでなく、ウイルススキャンをすり抜けてしまうことから、米国のサイバーセキュリティ・インフラセキュリティ庁においてもブロックすることが推奨されています。この仕組みを悪用したマルウェアは今後も発生することが予想されることから、当社だけでなく、お客様、お取引先様よりお預かりする情報を守るためにも、対応が必要との考えに至りました。

当社のお客様、お取引先様におかれましては、何卒、ご理解・ご協力のほど、よろしくお願い申し上げます。

ご参考

> IIJエンジニアによる、PPAPの危険性と対策についての解説：[パスワード付き\(暗号化\)ZIP廃止の考え方と対策](#)

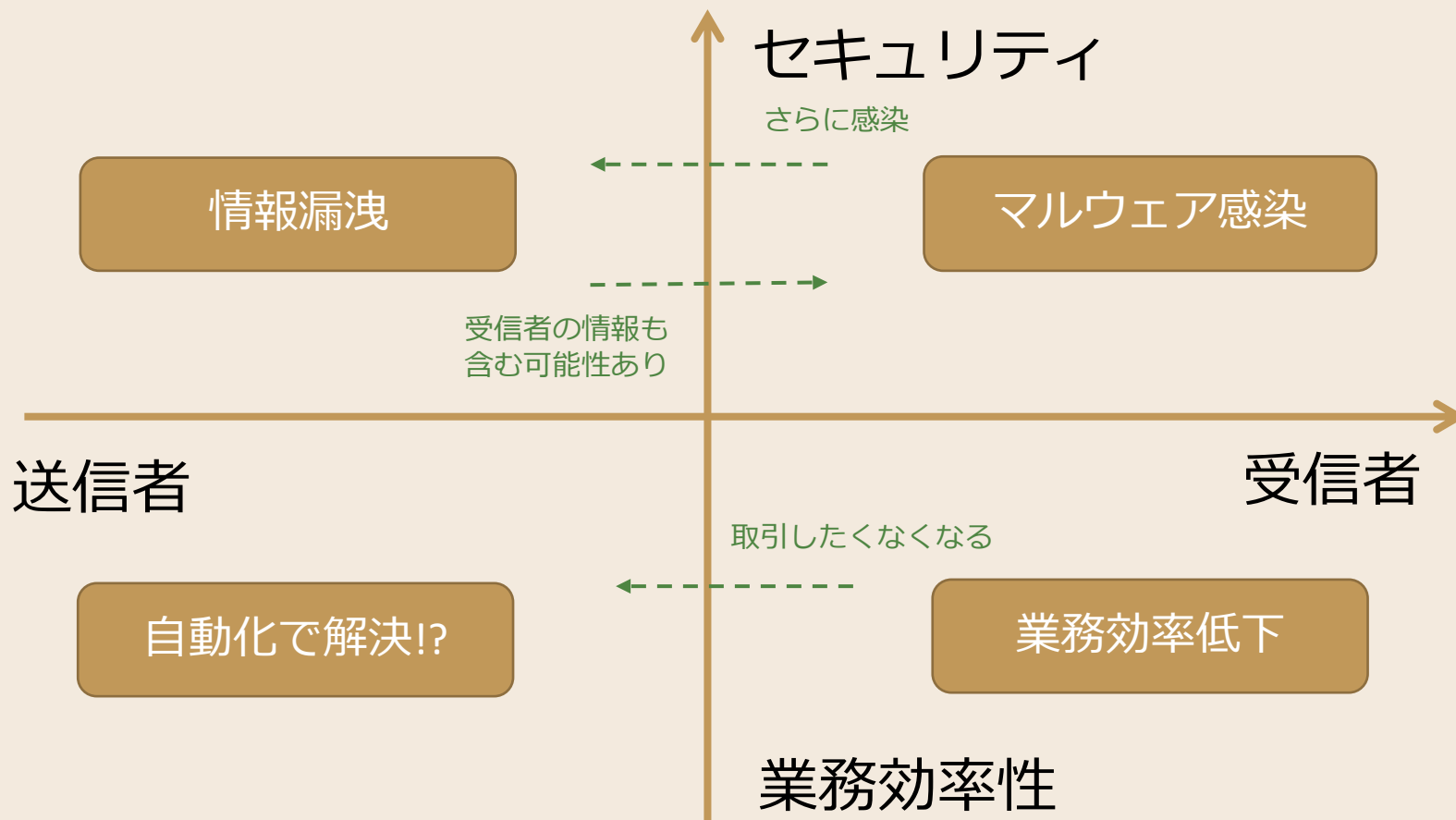
PPAPの分類 (Ver4.0)

		暗号化する対象となる添付ファイル	
		全て	一部のみ
パスワードの伝え方	同じ経路 (2通目等)	PPAP	準PPAP
	別の経路	大変	アリ

PPAPのメリット/デメリット

- 送信側にとっては手軽。
- 2通目を自動で送らなければ、誤送信防止にはなる。
- ×× 受信側はパスワードを探して入力して開く。効率が悪い。
- × そもそも2通目にパスワードを送るのであれば秘匿性なし。
- × 受信側のマルウェアフィルタをすり抜ける。

PPAP問題の構造



PPAPはなぜ広まったのか

- Pマーク、ISMS取得がきっかけと言われるが、本当??
- 当初は、丁寧な送り方とされていた。
 - セキュリティ的に意味がないとしても。
 - 風呂敷や熨斗紙のようなもの。
- その後の環境変化
 - メールの増加
 - ビジネスのスピードアップ
- さらに、自動で送られるようになり、もはや「丁寧な送り方」ではなくなった。

二つのカベ

どう思われているか想像力が及ばない。

経営者
総務
情シス



購買等
社内の現場



取引先

・一度作った規則は変えたくない。そんなに大変じゃないでしょ。

・取引先には申し訳ないけど、社内の規則変えるのが一番大変なんだよね。

・カンベンしてくれよ。できれば付き合いたくないな...

PPAPが象徴する本当の問題点

- 少し考えれば不合理だと分かることを変えられない企業文化・風土
- 「意味を考えずに規則だけを守る」 = 思考停止
→情報セキュリティにとって最も危険
- 現場・担当者の意見より、外部の権威を重視する経営層と管理部門
 - 結果的には、政府やメディアに取り上げられて、山が少し動いたが…
- 一方で、「DXを推進」!?

2. 脱PPAPの方法

代替案出せ！？

PPAPで送ってないですね!?

今まで

これから

機密性の高い情報
「別の手段で送信」

機密性の高い情報
「別の手段で送信」

何も変わらないはず

機密性の仕分け

機密性の低い情報
「PPAPで送信」

機密性の低い情報
「そのまま送信」

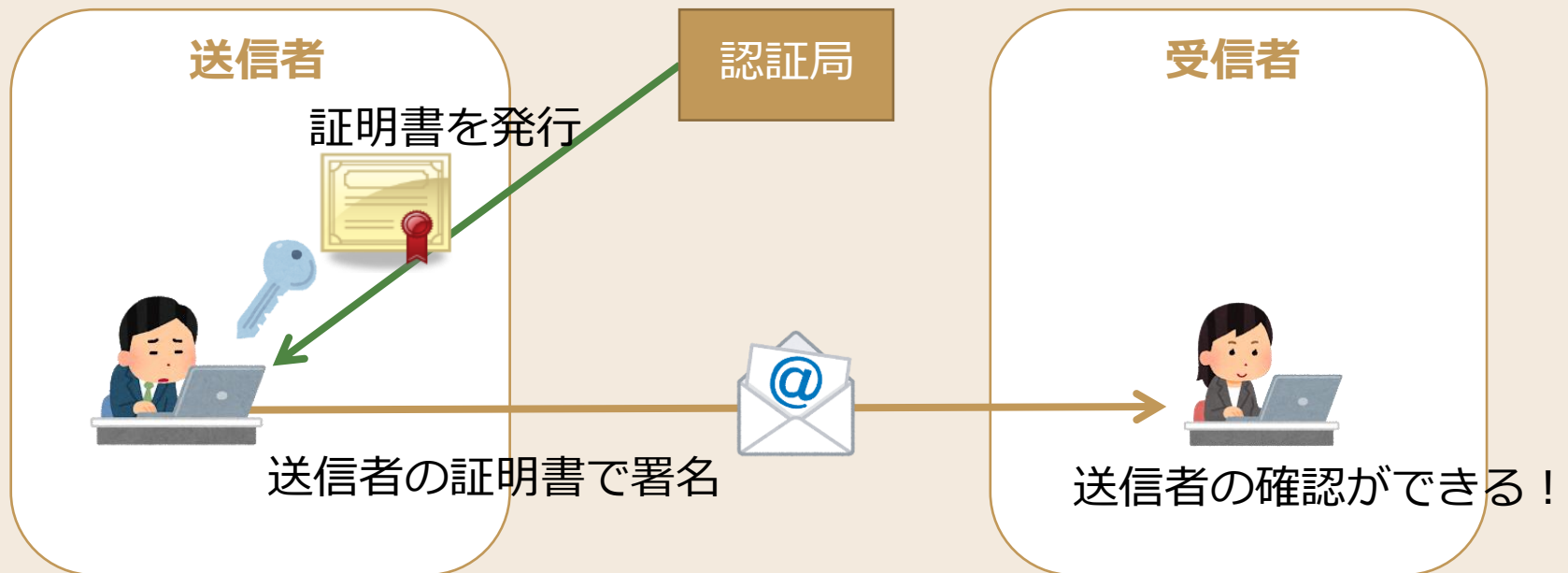
PPAP廃止

メールだけで決着をつけるなら S/MIME

- S/MIME
(エスマイム : Secure / Multipurpose Internet Mail Extensions)
- 詳細は、JIPDECのWebサイトを参照ください。
<https://itc.jipdec.or.jp/jcan/smime-index.html>
 - 署名 : 送信者のなりすましや改ざんを防止
 - 暗号化 : 盗聴を防止

S/MIMEで署名（ご参考）

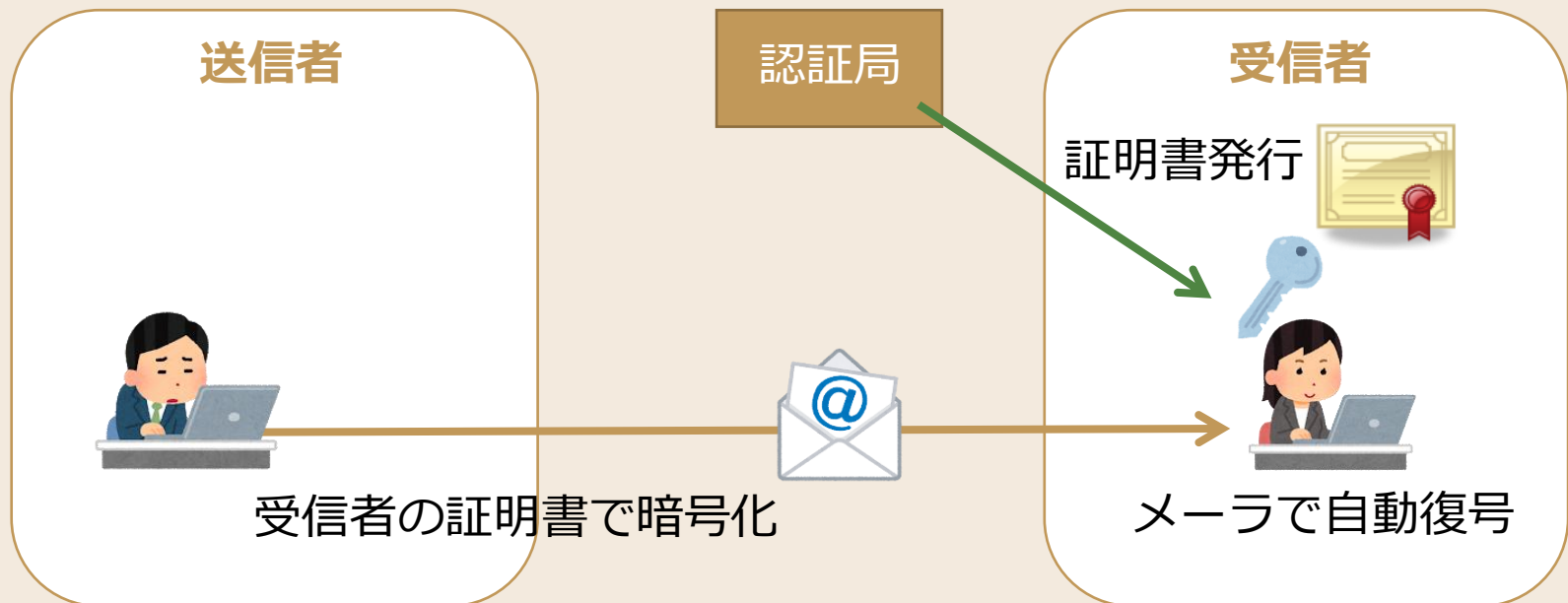
- 送信者側が、S/MIMEの証明書を取得し、署名。



※公開鍵と秘密鍵の関係等は省略しています。

S/MIMEで暗号化

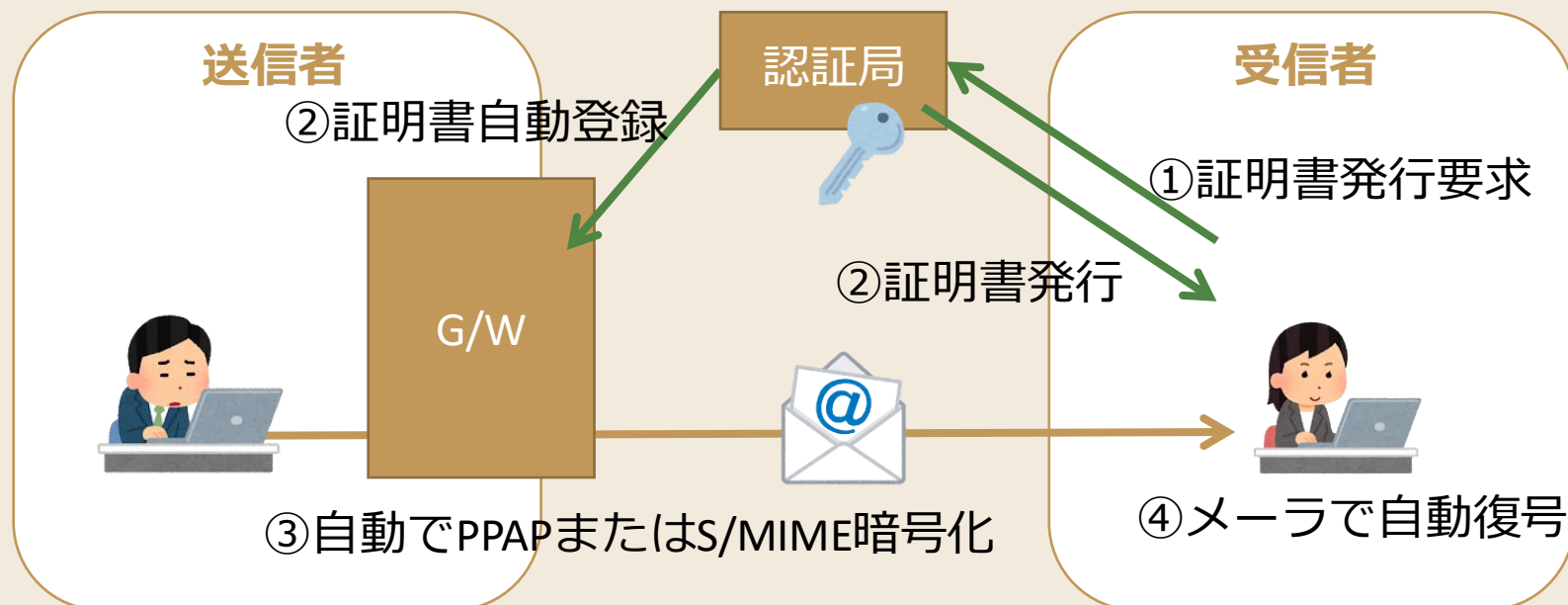
- 受信者側が、S/MIMEの証明書を取得し、送信者はそれを使って暗号化



※公開鍵と秘密鍵の関係等は省略しています。

受信者の自己防衛策

- 受信者側が、S/MIMEの証明書を取得。送信者側のG/W（PPAP自動化ソリューション）に公開鍵を登録



※仕組み作りに賛同くださる認証局、G/Wのベンダ様を募集しています。

メールで送らない方法もあります

PRI

- そもそも、機密性の高い情報を送る関係であれば、業務の効率性を考えても、メール以外のサービスを使えばよいのでは？
 - 送信者がURLを発行して誰でもアクセスできるタイプ
 - 受信者もアカウントを持って認証するタイプ

メール以外でのファイル共有

- オンラインストレージ
- ビジネスチャット
- グループウェア
- 電子契約サービス
- ERP
- SNS

今後のシナリオ

- 送信者側が、自主的にやめる
 - 日本政府
 - 日立製作所
- 受信者側が、パスワード付き添付ファイル自体の受取を拒否
 - freee社が2020年12月から受取拒否
 - IJが2022年1月から受取拒否
 - 以前より、gmailでは警告が出ている

3. DXを阻む三大商習慣

一方、2019年10月PHS登場



PPAPを何とかしたいのだが
PHSも何とかしたい

テツ太郎@CSSx2.0 in CSS2019
Produced by **上原哲太郎**@立命大

PHSとは

メールに添付したファイルを

Printしてから

Hanko押して


Scanして

送って下さい**プロトコル**




PHS反対運動の父
立命館大 上原氏

ネ申エクセル問題

河野太郎  @konotarogomame · 2016年11月2日

行革推進本部で文科省をよんで、こういう**神エクセル**を至急、全廃することになりました。また、科研費関係の問題提起の窓口をつくり、順次、対応することになりました。

 **Haruhiko Okumura** @h_okumura · 2016年11月1日

順番がおかしくなりましたが twitter.com/tarenyanco_10/... が出典です
RT @h_okumura: Excel原稿用紙

11	---									
12	(1) フリガナ(カタカナ)									
13										
14	(2) 氏名									
15										
16										
17	4 生年月日									
18		年(西暦)		月		日				
19										
20										
21	5 現住所									
22	(1) 郵便番号									
23				-						
24	(2) 住所									
25										
26										

58 3,629 1,929

DXを阻む日本三大商習慣

- PPAP
- PHS
- ネ申エクセル

お伝えしたいこと

- 自社の社内規則や商習慣を率先して変えてください。
ぜひ広島から新しい風を！
- 情報産業の方へ
脱PPAPのソリューションをぜひご提案願います。

ご清聴
ありがとうございました

