［さようなら，意味のない暗号化 ZIP 添付メール］

1 PPAP とはなにか
―その発展の黒歴史―

大泰司章 | PPAP 総研

PPAP とはなにか

企業間の取引においては，見積書，発注書，発注請書，請求書，契約書等の取引文書をはじめとして，技術文書やイベントの案内等，さまざまな文書が，メールにファイル添付という形で共有されている．その際，これは日本特有の現象だと思われるが，パスワードつき ZIP ファイルが添付され，そのパスワードが 2 通目のメールで届く，という実に奇妙なことが行われている．1 通目の添付ファイルを奪えるようであれば，2 通目も奪うことができるはずで，セキュリティ的な意味がないように思われる．それにもかかわらず，受信側は毎回復号化しなければならず，負荷は非常に高い．

このようなメールの送り方を PPAP と名付けて，やめようという活動をしている．

【P】assword つき ZIP ファイルを送ります
【P】assword を送ります
【A】n 号化
【P】rotocol

話は 2016 年にさかのぼる．当時，S/MIME（エスマイム，Secure/Multipurpose Internet Mail Extensions）用の電子証明書を販売していた関係でパネルを制作することになった．そのときに作ったコピーが「まだ ZIP ファイル＋パスワードで消耗してるの?」というものであった．いまひとつだな，もう少しインパクトがほしいなと思っていたところ，ちょうど PPAP（もちろん Pen-Pineapple-Apple-Pen のほうである）が流行っており，「PPAP って何かのプロトコルみたいだよね」と誰かが Facebook で言ったのを見て，思いついたものである．

Internet Week 2016 では「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～」というテーマでパネルをした．このころは，PPAP に反対すると，PPAP を自動で行うソリューションのベンダが放っておかないぞと警告されていたが，実際に彼らと話をしてみると，「PPAP 自体はやめたいがユーザがいるのでやめられない．PPAP の代わりのオンラインストレージの機能はすでに持っているし，設定で簡単に変更可能」と言われて拍子抜けした．

2017 年 3 月には「くたばれ PPAP !」という Facebook グループを作った．今ではメンバが 1,000 人近いグループになっている．PPAP の事例から情報セキュリティまで多様な話題が飛び交っており，有益な情報交換ができたと思っている．

2018 年には「働き方改革」がさかんに言われるようになった．そこで，PPAP を非効率な取引慣行の象徴と捉え，紙やハンコの廃止（電子契約元年）に加えて，PPAP をやめることで，組織や働き方を改革しようという打ち出し方をしている．

PPAP の歴史

2000 年前後から，それまでの郵便や FAX に代わって，メールに取引文書等のファイルを添付して送ることが増えたように思う．送受信の手間も少なく，スピードも速く，ディジタルデータのまま再利用できることもあり，取引文書のやりとりは画期的に効率化されたが，赤い印影つきの紙にこだわる経理等管理部門が壁となって全面的に電子化とまではいかなかった．電子ファイルをカラー印刷することで赤い印影をつけたり，FAX を併

用したりした．不思議なことに，FAX は経理担当によっては原本扱いをしてもらえるのだ．

当初は Word や Excel，PDF ファイルがそのまま添付されていたが，徐々に添付ファイルのみが ZIP 暗号化されるようになってきた．もちろん，PGP（Pretty Good Privacy）や S/MIME によって本文ごとの暗号化は可能であったが，一般のユーザには導入が難しかった．

exe ファイルを送って受信側で自動解凍するというものもあった．exe ファイルは受信側で受け取れないことがあるので，拡張子をいったん ex_ にして送信し，受信者側で exe に戻すということも行われていた．

ZIP ファイルのパスワードは，「御社の名前です」「今日の日付です」というものだったり，そのつど生成する複雑なものだったりしたが，やがて，2 通目に自動で送られてくるようになる．これが 2010 年頃からどんどん増えたという印象を持っていて，2010 年代の中頃には，大企業の多くが PPAP になってしまった．

一方で，ここ数年，ファイル共有はより便利な方法にシフトしつつあるのも事実である．

まず，オンラインストレージの使用頻度が上がっている．昔から無料で手軽に使える宅ふぁいる便がよく使われていたが，最近は OneDrive，Google Drive，Dropbox，Box 等での共有も普通になってきた．それ以外にも，グループウェア，特にサイボウズ Live は企業や団体間の情報共有でよく使われていた．

技術部門，特に IT 関係では，すでにメールではなく Slack 等のメッセンジャーが利用されているし，また，昨今テレワーク対応ということで Zoom，Webex，Skype といったオンラインミーティングのツールでもファイル共有がされている．

ここ数年注目すべき動向としては電子契約の爆発的拡大である．契約や受発注の業務プロセスの中で，自然とファイルを送受信することになるので，これも PPAP メールを減らす要因になるだろう．

なお，以上は主に企業間取引の販売部門での状況であり，他の分野では様相が違っているかもしれない．特定の分野では Rights Management や S/MIME，PGP も使われている．

PPAP の分類

すべてのファイルが対象か，パスワードを別経路で送っているかを軸にすると，表 -1 のように4つに分類できる．

- タイプ A:すべての添付ファイルを暗号化し，パスワードを同じ経路で送る．送信者は情報の機密性を評価する必要がなく，一律に暗号化される．添付ファイルは暗号化することが社内規定で決まっていることが多い．送信者は，手動の場合は暗号化の負荷が高いため，PPAP 自動化ソリューションが使われることになりやすい．狭義の PPAP．
- タイプ B：すべての添付ファイルを暗号化し，パスワードを別の経路で共有するもの．
  タイプ A に比べて，送信者側も受信者側も負荷がかかる．多くの案件を抱えている人にとっては非常にきつい．
- タイプ C：暗号化が必要なファイルのみを暗号化し，パスワードを同じ経路で送るもの．
  送信者がせっかく暗号化が必要だと自分で判断し，暗号化をしているにもかかわらず，パスワードを同じ経路を送ってしまうのは惜しい．
- タイプ D：暗号化が必要なファイルのみを暗号化し，パスワードを別の経路で共有するもの．これが本来は望ましい形．送信者側はファイルの暗号化の必要性を判断しなければならないし，手動で暗号化することが多いため，送信側の負荷は高いが，受信側は復号するファイルの数が減る．

狭義の PPAP（タイプ A）なのか，広義の PPAP（タイプ A，B，C，D）なのか区別をしないと，議論が発散しがちである．ここでは狭義の PPAP に絞って述べたい．

■表 -1　PPAP の分類

		暗号化する対象となるファイル	
		すべて	暗号化が必要なもののみ
パスワードの送信経路	同	タイプ A	タイプ C
	別	タイプ B	タイプ D

なぜ PPAP を使うのか

受信側からすると負荷が高い PPAP であるが，なぜ使われるのであろうか？

「PPAP は，ISMS やプライバシーマークを取得するタイミングで社内に導入された．ISMS やプライバシーマークが悪いのだ」と言われることがある．それは本当だろうか？

メール誤送信防止サービスの一部として市場では取引されていることから，メール誤送信防止市場の規模の推移から広まった時期を推定することができる可能性がある．市場規模については図 -1 のとおり ITR 社の調査を見つけることができた．2016 年度以降のものしか公表されていなかったが，2015 年度以前のデータがあれば分かることがあるかもしれない．

一方，ISMS やプライバシーマークで，PPAP を実際に推奨する審査員やコンサルタントを探したが，残念ながら今のところ見つかっていない．どうも，ISMS，プライバシーマーク犯人説は都市伝説の様相を見せている．

それでは，ISMS やプライバシーマークでメールの暗号化がどのように取り扱われているか見ていこう．

ISMS でのメールの添付ファイル暗号化の取り扱い

ISMS とは

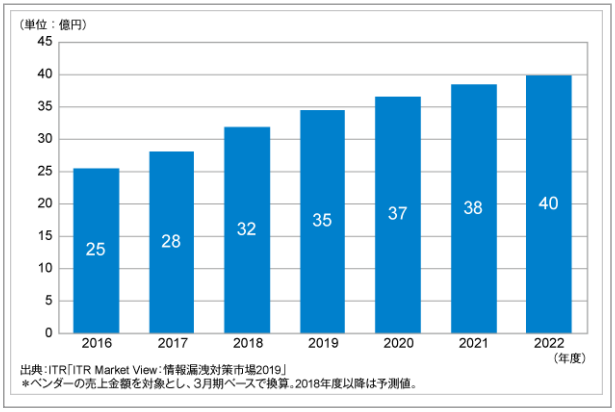
ISMS とは，Information Security Management System（情報セキュリティマネジメントシステム）の略で，情報の CIA（「機密性（Confidentiality）」，「完全性（Integrity）」，「可用性（Availability）」）を保護するための体系的な仕組みである．

ISMS を構築するにあたって，必要となるのが ISO/IEC 27001（JIS Q 27001）という ISMS の国際規格である．この規格には，ISMS をどのように構築，実施，維持，改善すべきなのかが記載されている．特に管理策については，ISO/IEC 27002 というガイドライン規格があり，管理策を導入する際の参考になる．

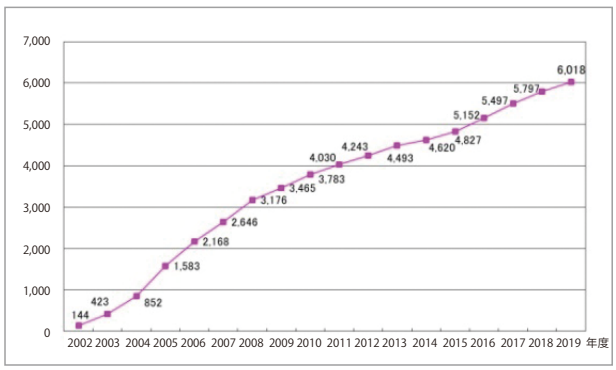
「ISMS 認証」とは，第三者である ISMS 認証機関が，組織の構築した ISMS が ISO/IEC 27001 に基づいて適切に運用管理されているかを，利害関係のない公平な立場から審査し証明することである．したがって，「ISMS 認証」によって，組織は，ISO/IEC 27001 という国際規格に沿って，情報セキュリティを画するための仕組みを持ち，その仕組みを維持し継続的に改善していることを，顧客や取引先に対して客観的に示すことができる．この「ISMS 認証」を取得するには，ISMS 認証機関に申請し，審査を受ける必要がある．

ISMS 認証の取得数は図 -2 のとおり，年々増え続けており，昨年度 6,000 件を超えている．PPAP が広まったのが 2010 年前後だとすると，増勢が落ち着いている時期にあたるようにも見える．

JIS Q 27000:2014（情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項）においては，「電子的メッセージ通信に含まれた情報は適



■図 -1　メール誤送信防止市場規模推移および予測（2016 ～ 2022 年度予測）[1]



■図 -2　ISMS 認証登録数の推移（数値は各年度末．2019 年度は 11 月 11 日現在）[2]

切に保護しなければならない」とあるだけで，当たり前のことながら抽象的な記述になっている．

一方，JIS Q 27002:2014（情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範）においても，メールの添付ファイルの暗号化というレベルの記述はない．

情報資産の他社への転送方法は，自社でリスク分析をした上で決めるべきことで，それが維持できており，できれば改善することが望ましいということだ．

関係者周辺からも，PPAP 蔓延に関する有益な情報は得られなかった．

プライバシーマークでのメールの添付ファイル暗号化の取り扱い

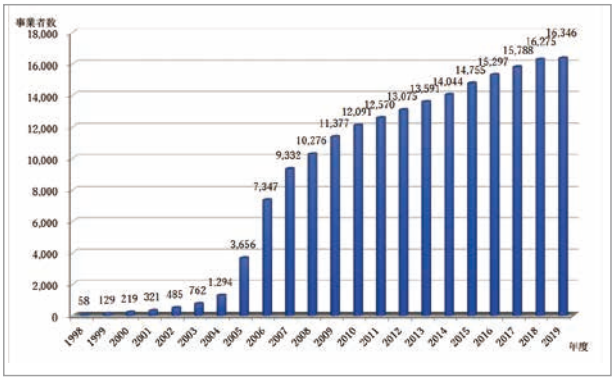
プライバシーマーク制度は，事業者の個人情報を取り扱う仕組みとその運用が適切であるかを評価し，その証として事業活動においてプライバシーマークの使用を認める制度である．

プライバシーマーク制度は，日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」をベースとした審査基準による審査を経て，事業者の個人情報の取扱いが適切であるかを評価している．JIS Q 15001 は，個人情報保護法等，法令への遵守も包含している．そのため，事業者にとっては法律への適合性はもちろんのこと，自主的により高い保護レベルの個人情報の管理体制を確立し運用していることを，取引先や消費者に示すことができる制度として活用されている．

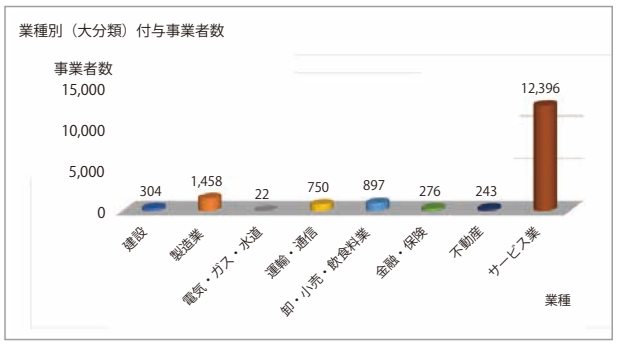
図 -3 がプライバシーマークの付与事業者の推移である．個人情報保護法が施行されたのが 2005 年度であり，やはりその前後で急増していることが分かる．その後の伸びと PPAP との関係はあるのだろうか．

図 -4 は，業種別（大分類）の付与事業者数である．サービス業が圧倒的に多いので，表 -2 にサービス業の内訳を掲載した．PPAP 企業といえば，官公庁，金融機関，製造業等伝統的大企業というのが直観的なイメージだが，実際にプライバシーマークを取得している企業の業種分布とは一致しそうにない．

「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン―第 2 版―」によると，「盗聴される可能性のあるネットワーク（たとえばインターネットや無線 LAN 等）で個人情報を送信する際に，個人情報の暗号化又はパスワードロック等の秘匿化の措置を講じていること」とある．



■図 -3　付与事業者の推移（1998 年度～ 2019 年 9 月 30 日時点）[3)]



■図 -4　業種別（大分類）付与事業者数 [3)]

■表 -2
業種別（中分類）付与事業者数（抜粋）[3)]

洗濯・利用・浴場業	12
駐車場業	12
その他の生活関連サービス業	142
旅館，その他の宿泊所	5
娯楽業	21
自転車整備業	6
機械・家具等修理業	30
物品賃貸業	47
映画・ビデオ制作業	60
放送業	54
情報サービス・調査業	6,667
広告業	548
専門サービス業	1,007
協同組合	18
その他の事業サービス業	3,298
廃棄物処理業	83
医療業	39
保健衛生	170
社会保険，社会福祉	72
教育	46
学術研究機関	11
政治・経済・文化団体	48

はたしてPPAPが「秘匿化の措置」といえるかどうかだろうか.

一方で，Webサイトに掲載されているためか，添付ファイル暗号化の根拠としてJISAの審査基準[4]が引用されることもあるようである.

【書類審査】において，「(3)【第23条】個人情報を含む添付ファイルを取扱う際に，セキュリティ対策（データの暗号化，パスワード設定など）の措置を講じることを新たに追加した」と書かれている.

PPAPは，確かに「データの暗号化，パスワード設定」ではあるが，「セキュリティ対策」なのだろうか.

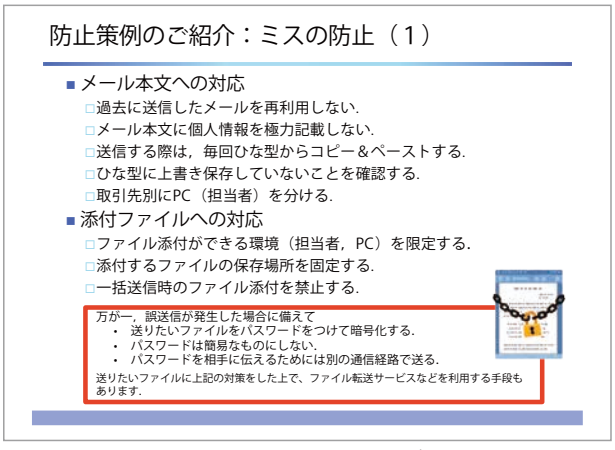
なお，JIPDECには，「お役立ちツール，社内教育用参考資料，基本編：個人情報の取扱いに関する事故を起こさないために」というも資料があったので，図-5に示す.

「パスワードを相手に伝えるためには別の通信経路で送る」と書かれている.

IPA「対策のしおり」

さらに，少々古いものであり，直接ISMSやプライバシーマークとは関係がないが，「IPA対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり(2012年6月8日第4版)」という資料があった. 図-6に示す.

「復号のためのパスワード等は，別の通信手段を利用して相手に伝えることが重要ですが，」と書かれている.



■図-5　防止策例の紹介：ミスの防止（1）[5]

なぜ都市伝説が生まれたのか

以上見てきたように，すべての添付ファイルを一律にZIP暗号化し，同じ経路の2通目でパスワードを送るような事態は，制度や基準，ガイドライン作成の場では，想定されていなかったようだ. 直接の要求事項ではないとはいえ，パスワードは「別の通信経路で送る」と明示的に書かれている文書もある.

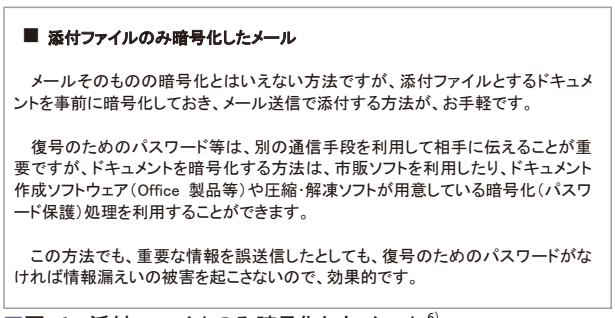
PPAPを利用している企業（以下，PPAP企業）は，ISMSもプライバシーマークも審査に通りそうにない. それにもかかわらず，通るためにPPAPを始めた，通るためにはPPAPソリューションが必要，と言う人がいるのは不思議なことだ.

審査に割ける限られた時間の中で，おそらくメールの添付ファイルの暗号化の方法にまでコンサルも審査員も考えが及んでいないのであろう.

あるいは，取引先にのみ負荷をかける，意味のない「送信側自己中心的セキュリティ」ということに気付いていて，その後ろめたさから，認証取得のためという言い訳をしているのだろうか.

このように，情報セキュリティや個人情報にかかわりたくないし，まして情報の秘匿性の判断などしたくない送信側ユーザ，形式を整えて認証が取れればよい送信側管理部門，ユーザの要望に応えざるを得ないメールソリューションベンダ，特にメールについては関心がない審査関係者，そして発注元企業の発信するメールに対してものが言えない受信者，これらの関係者が見事にバランスしている状態が生じている可能性がある.

こうした謎を解くため，今後ISMSとプライバシーマー


■ 添付ファイルのみ暗号化したメール

メールそのものの暗号化とはいえない方法ですが、添付ファイルとするドキュメントを事前に暗号化しておき、メール送信で添付する方法が、お手軽です。

復号のためのパスワード等は、別の通信手段を利用して相手に伝えることが重要ですが、ドキュメントを暗号化する方法は、市販ソフトを利用したり、ドキュメント作成ソフトウェア（Office 製品等）や圧縮・解凍ソフトが用意している暗号化（パスワード保護）処理を利用することができます。

この方法でも、重要な情報を誤送信したとしても、復号のためのパスワードがなければ情報漏えいの被害を起こさないので、効果的です。

■図-6　添付ファイルのみ暗号化したメール[6]

クのコンサルとして現場に入ってみようと思う．しかるべき時期に続報ができれば幸いである．

今後の新たな歴史の創造に向けて

PPAP 企業は，少なくとも，意味のない自社のルールにこだわり，取引先に負担を強いても何とも思わないカルチャーを持つ企業だということがいえる．PPAP 企業の現場では，実はやめたいが管理部門に到底言えないという声もよく聞く．このような企業は効率的な取引を行えない企業だというシグナルとして PPAP を活用することができるだろう．

そこで，どの企業が PPAP 企業なのかという情報を集めて公開することには意味があると考えられる．また，PPAP に限らず，さらに，以下のようなデータを集めることにより，取引の効率性をスコアリングできるかもしれない．

●取引文書に紙とハンコを要求するか
● FAX を使っているか
●対応している電子契約，EDI（Electronic Data Interchange）の種別
●業者登録，取引口座開設時の手続き
●決済方法
● SDGs（Sustainable Development Goals），CSR（Corporate Social Responsibility）に関する取引先への要求事項
●情報セキュリティに関する取引先への要求事項
●個人情報保護に関する取引先への要求事項

こうしたスコアができれば，取引の効率性を評価されることなく，取引先にのみ負担を強いていた調達方法が変わるきっかけになるだろう．優秀な取引先を確保するためには自ら変わらなければならないということだ．

あわせて，こうしたスコアが投資家からの評価に影響することになれば，PPAP をはじめとする非効率な取引慣行は大きく変わるだろう．

今や，取引文書のやりとりだけでなく，企業の枠を超えてコラボレーションを行うことが必須となっている．その際に，自社の営業秘密の秘匿性を評価し，先方の会社と共有すべき情報と共有すべきでない情報の選別ができない従業員は，そもそもコラボレーションに参加すべきでないし，しても成果は上げられないであろう．PPAP に頼った情報共有をするような従業員は使えないということだ．

もちろん，情報の選別ができない従業員がいることは事実である．そのような従業員は，そもそも対外的な情報のやりとりが発生する業務をやらせてはいけない．それこそ PPAP の強制によるコントロールをするのではなく，社外へのすべての情報発信を禁止すべきだ．

いずれにせよ，メールに限らず社外への情報発信の方法を全従業員一律に規制するやり方はすでに限界に来ている．もっとも，それらの教育や基準作成，評価を個別企業が行うことは負担が大きい．営業秘密の取り扱いや社外との共有のスキルを評価できる資格が必要になってくるだろう．

取引先への迷惑も顧みず，全社員が全添付ファイルを自動的に暗号化する PPAP は，各個人が得意なやり方に応じて，場所や時間に縛られない働き方をする「真の働き方改革」とはまったく相いれない．遅かれ早かれ PPAP はなくなるに違いない．

参考文献

1) ITR：メール誤送信防止市場規模推移および予測（2016 ～ 2022 年度予測），https://www.itr.co.jp/company/press/190207PR.html
2) ISMS-AC：ISMS 認証登録数の推移（数値は各年度末．2019 年度は 11 月 11 日現在），https://isms.jp/topics/news/20191112.html
3) JIPDEC：プライバシーマーク付与事業者情報（2019 年 9 月 30 日時点），https://privacymark.jp/certification_info/jdi6lq00000017af-att/pmark_data_20190930.pdf
4) JISA におけるプライバシーマーク審査項目の一部改訂について，https://www.jisa.or.jp/service/privacy/tabid/831/Default.aspx?itemid=31
5) JIPDEC：お役立ちツール 社内教育用参考資料 基本編：個人情報の取扱いに関する事故を起こさないために，https://privacymark.jp/system/reference/pdf/tools_accidents_1_note.pdf
6) IPA：対策のしおり シリーズ（7）電子メール利用時の危険対策のしおり（2012 年 6 月 8 日第 4 版），https://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf

（2020 年 3 月 31 日受付）

■**大泰司章** otaishi@gmail.com

三菱電機，日本電子計算，JIPDEC を経て，PPAP 総研設立．電子契約，電子署名，メールや Web のなりすまし対策を普及．PPAP やハンコ等の非効率な取引慣行を変えて，真の働き方改革を目指す IT コンサルとして活動中．