日本国内におけるメールセキュリティに関する実態把握

澁谷 遊野[1,a)]　近藤 大嗣[2,b)]　山口 利恵[3]　中田 登志之[3]　浅見 徹[4]

概要：メールにおける添付ファイルの送信手法として用いられる，暗号化した ZIP ファイルを送付するセキュリティ対策手法（通称「PPAP」）はセキュリティリスク削減効果がない上，有害である場合もあるものの，国内の企業や公共団体を中心に広く利用されていて社会的課題となっている．そこで本研究では，国内企業・団体を対象とした質問紙調査およびメールセキュリティ解析に基づき，PPAP 等のメールセキュリティ対策の国内での利用状況の実態を明らかにする．本稿では調査の結果概要を速報値的に報告する．調査の結果，2022 年 6 月現在，質問紙調査に回答した組織 344 件のうち約 64%が PPAP を利用していて，PPAP 利用組織の 88%が PPAP の有害性・無効性を認識しているにも関わらず利用を続けていることが明らかになった．また，PPAP に対する攻撃に対して脆弱なメール運用を行なっている組織が多いことが明らかになった．

キーワード：メールセキュリティ，暗号化 ZIP 添付送付，PPAP，セキュリティシアター

A Study on Email Security Practices in Japan

Yuya Shibuya[1,a)]　Daishi Kondo[2,b)]　Rie Yamaguchi[3]　Toshiyuki Nakata[3]　Toru Asami[4]

Abstract: Japanese companies and organizations widely use PPAP (attaching an encrypted ZIP file to an email and then sending its password in the following email) as a security measure despite its ineffectiveness and potential harm. This study aims to clarify how, by whom, and why PPAP and other email security measures are chosen on the basis of a questionnaire survey and an email security analysis. This report provides a preliminary summary of the survey results. This survey revealed that approximately 64% of the 344 organizations that responded to the survey are still using PPAP (as of June 2022). Furthermore, 88% of the organizations that are using PPAP continue to use it even though they are aware of its harmfulness and ineffectiveness. It was also revealed that many organizations have e-mail operations that are vulnerable to attacks against PPAP.

Keywords: Email-security, PPAP, security-theater

[1] 東京大学空間情報科学研究センター
Center for Spatial Information Science, The University of Tokyo
[2] 大阪公立大学大学院情報学研究科
Graduate School of Informatics, Osaka Metropolitan University
[3] 東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター
Social ICT Research Center, Graduate School of Information Science and Technology, The University of Tokyo
[4] 株式会社国際電気通信基礎技術研究所
Advanced Telecommunications Research Institute International
[a)] yuya-shibuya@csis.u-tokyo.ac.jp (shared co-first authorship)
[b)] daishi.kondo@omu.ac.jp (shared co-first authorship)

1. はじめに

セキュリティ対策の導入では，単一的なリスクの大きさや頻度，リスク対応策の効果よりも，社会経済的，政治的，文化的，心理的な要因も影響が大きいことが指摘されてきた．特に，利用者がどのようにリスクを評価しセキュリティに関する意思決定を行うのかに着目するセキュリティ心理学研究 [1–4] ではセキュリティシアターと呼ばれる概念がある．セキュリティシアターとは，セキュリティを提供することを目的としながら，実際にはセキュリティを提供できない対策を指す [5–8]．セキュリティシアターのよ

く知られた例は，空港での保安検査であり，実際のセキュリティよりも，セキュリティの感覚（＝特定の手続きを受けさせること）が重要となっている．Schneier [5] は，「セキュリティは感覚であり，現実でもある．（中略）安全だと感じていなくても安全であり得る．そして，そうでなくても安全だと感じることができる（p.50)」と指摘する．そもそも絶対的なセキュリティというものは存在せず，セキュリティは常に何らかのトレードオフを伴う [7]．セキュリティのコストには金銭的コストのみならず，時間や利便性，能力，自由度なども含まれる．

また，組織のセキュリティに焦点を当てている研究群では，組織特有のセキュリティリスクや意思決定に関して様々に研究が行われている．Anderson [9] は組織における情報セキュリティは「情報リスクと統制のバランスがとれているという十分な安心感」とし，十分な情報を持たない経営者は，自らの組織の情報セキュリティについて実際的な安心を得ることはできないと指摘する．また，組織においては，組織の構成員のセキュリティに対する認識の欠如や情報を扱う際の行動など，内部セキュリティ脅威の方が喫緊の課題とみなされてきた [10–15]．多くの人々はセキュリティ脅威に対する懸念は持っているが，その脅威そのものや問題点を十分に理解しているとは言い難いからである．

国内では，パスワード付 ZIP ファイル添付送付の慣行（通称 PPAP）が 2010 年ごろから企業を中心に広まりをみせた [16]．PPAP もセキュリティシアターの一事例として位置付けることができる [17]．セキュリティ対策としては意味のない行為であるにも関わらず多くの企業や公官庁で情報漏洩対策として利用されていることから，日本特有の儀式的で無意味な慣行としての批判が広まった [16–19]．更には 2020 年 11 月 24 日にデジタル改革担当相が，2020 年 11 月 26 日に内閣府と内閣官房が PPAP 廃止を宣言しているものの，現在も多くの組織で PPAP が採用されている [20]．

そこで，本研究では PPAP がなぜ，どの程度，国内組織で採用され，なぜ廃止に至らないのかを明らかにすることを目的に質問紙調査およびメールセキュリティ解析調査を実施した．本稿では，調査結果の概要を速報値的に報告する．なお，本研究では PPAP そのものの批判を目的としているのではなく，無意味なセキュリティ対策の慣行が広まってしまう要因や対応策の検討材料として PPAP 事例を検証することで，今後の組織におけるセキュリティ対策への示唆を得ることを目指している．

本稿は以下次のように構成される．まず 2 章で暗号化 ZIP 添付によるメールセキュリティの問題点をまとめる．続いて，3 章で本研究の研究方法を示す．4 章で結果を示す．5 章で本稿をまとめ，今後の展望を述べる．

2. 暗号化 ZIP 添付によるメールキュリティの問題点

多くの組織で，メールにファイルを添付して送信する際に，セキュリティ対策の一環として，1 通目に暗号化した ZIP ファイルを送信し，2 通目でそのパスワードを送信する方法が採用されている．この対策では，メールというメディアのみを介して，ZIP ファイルとそのパスワードを送信する．そのため，攻撃者が 1 通目のメールを取得できる場合，2 通目も同様に取得できると考えられ，セキュリティレベルの向上は見られない．むしろ，暗号化した ZIP ファイルはメール検疫機能を無効化させる可能性があり，攻撃者はこの対策を逆手取って，近年流行している Emotet のようなマルウェアを組織の網内に拡散することができるため，セキュリティレベルの低下に繋がる．このような対策は，「Password つき ZIP ファイルを送ります」，「Password を送ります」，「An 号化」，「Protocol」の頭文字から成る略語で PPAP と呼ばれている [16]．

現在の Domain Name System (DNS) を基盤にする組織間メールの場合，自社の DeMilitarized Zone (DMZ) やクラウド上に設置するメール送信側である組織の出口 Mail Transfer Agent (MTA，メールサーバ) とメール受信側である組織の入口 MTA 間を繋ぐインターネット上に，第 3 者の MTA が介在することは通常ない．また，出口と入口の MTA 間通信は，Transport Layer Security (TLS) 等の暗号化プロトコルを利用して暗号化されている場合が多い．

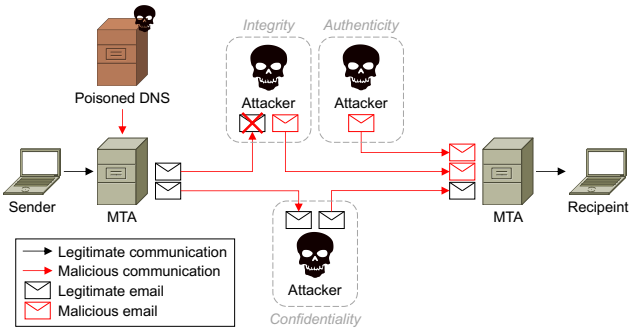

図 1 メールプロトコルに対する能動的攻撃者が関与する攻撃モデル [21]

PPAP を攻撃する方法を，機密性（正当な権限を持った者だけがメールを読むことができる状態），完全性（メールの内容に誤りや欠けが無いことが保証されている状態），真正性（メールの送信者がなりすました他人ではなく確かに本人であると保証されている状態）の 3 点に基づき説明する．PPAP の機密性は平文送信と同じである．機密性，完全性，真正性は PPAP では満足できず，MTA 間で利用される TLS 等の暗号化プロトコルの強度に依存している．能動的攻撃者が関与する攻撃モデル（図 1）では，機密性は StartTLS のような TLS 系暗号化プロトコルを無効化す

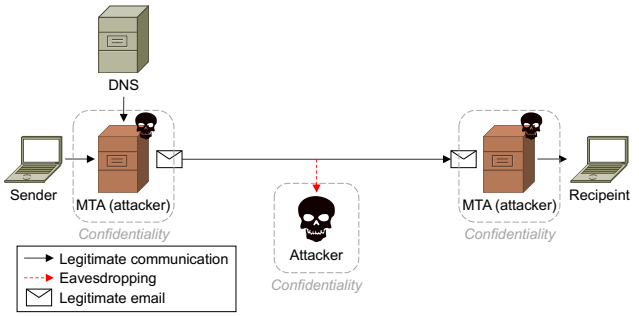

図 2 メールプロトコルに対する受動的攻撃者が関与する攻撃モデル [21]

るダウングレード攻撃によって侵害される．また，送信先 MTA の IP アドレスを含むリソースレコードを改ざんする攻撃（DNS キャッシュポイズニング）を利用して，攻撃者へメールを転送させることによっても侵害される [22]．これにより，攻撃者はメールを窃取することができる．完全性はメール改ざんによるマルウェア添付によって侵害される．マルウェアを攻撃相手に潜入させることにより，メールを窃取することができる．真正性はなりすましメールによって侵害される．攻撃者は，メールアドレスを偽ることによって，攻撃相手からメールを窃取することが可能になる．受動的攻撃者が関与する攻撃モデル（図 2）では，機密性は暗号化されていない通信の盗聴によって侵害される．また，信頼できない MTA にメールを送信した場合も，メールは窃取される．完全性と真正性の満足は 3.2 節で説明する技術に依る．

3. 研究方法

3.1 質問紙調査

質問紙調査では，PPAP がなぜ，どの程度，国内の組織で採用され，なぜ廃止に至らないのかを明らかにすることを目的とした．調査対象は，国内で従業員数が 1,000 人以上の企業および公共団体で，対象組織数は 3,055 社である．対象組織に郵送で質問紙調査票を送付し，回答は郵送・もしくは Web で受け付けた．調査票発送日は 2022 年 6 月 23 日で，回収期間は 7 月 22 日までとした．回収数は 344 で回収率は 11.3%であった．回答組織の内訳を表 1 に示す．官公庁には国家公務・地方公務が，民間企業・団体にはそれ以外全てが含まれる．質問では，(1) PPAP の利用実態，(2) PPAP 利用している場合は採用の理由と PPAP を廃止しない理由等, PPAP 利用を廃止した場合は廃止理由等を聞いた．また，全回答者を対象に (3) 情報セキュリティ一般に関する取り組み状況を聞いた．

3.2 メールセキュリティ解析

メールセキュリティ解析は, 欧州委員会 (European Commision) が運営しているメールセキュリティレベルを評価するツールである My Email Communications Security Assessment (MECSA) [21] を参考にし，機密性，完全性，真正性の 3 点に関係する以下の要素を基に評価する．

- DNS Security Extensions (DNSSEC)（デジタル署名を用いた DNS 応答検証技術）
- DNS-Based Authentication of Named Entities (DANE)（DNS を用いた認証技術）
- StartTLS または SMTPS（メールを暗号化する技術）
- Sender Policy Framework (SPF)（送信元の IP アドレスを利用する送信ドメイン認証技術）
- DomainKeys Identified Mail (DKIM)（デジタル署名を利用する送信ドメイン認証技術）
- Domain-based Message Authentication, Reporting, and Conformance (DMARC)（SPF および DKIM を補強する送信ドメイン認証技術）
- X.509（デジタル証明書と証明書失効リストのデータ形式を定めた標準規格）
- SMTP MTA Strict Transport Security (MTA-STS)（メール受信側がメール送信側に対して暗号化メール送信に関する方針（例：メール受信側 MTA が StartTLS に対応していない場合，メール送信側 MTA はメールを送信してはいけない）を宣言する技術）

先に述べたメールへの各種の攻撃に対して, 機密性は, StartTLS または SMTPS（両方向通信），X.509，MTA-STS が全て利用可能，または，DNSSEC，DANE，StartTLS または SMTPS（両方向通信），完全性は，DNSSEC，DKIM，DMARC，真正性は，DNSSEC，SPF，DKIM，DMARC が全て利用可能であれば理想的なセキュリティレベルで担保される．

本解析では，3.1 節の回答組織のうち，メールセキュリティ解析に協力した組織を対象にした．そのなかでも，ある組織が複数ドメインを保有している場合も存在していたが，本解析では送信元メールアドレスのユニークなドメインをもとに，メールセキュリティ解析を行った．この協力した組織には，組織のメールアドレスを利用して著者らにメールを送信してもらい，メールヘッダ解析に

表 1 質問紙調査回答組織内訳

種別	分類	回答数	小計
企業・団体	サービス業	130	
	製造業	68	
	卸売・小売業・飲食店	31	
	建設業	24	
	運輸・通信業	22	
	金融保険業	18	
	不動産業	3	
	電気・ガス・水道・熱供給業	1	
	農業	1	298
官公庁	地方公共団体	44	
	国	2	46
		合計	344

表 2 解析対象のメールアドレスドメインに含まれる eTLD とドメイン数

eTLD	ドメイン数
.biz	1
.com	24
.group	1
.jp	10
.ac.jp	15
.co.jp	73
.go.jp	1
.lg.jp	10
.ne.jp	2
.or.jp	13
.org	1

よって StartTLS または SMTPS（組織から著者らへの通信），SPF，DKIM，DMARC の利用可否を確認した．また，そのメールアドレス中のドメインを基に，MECSA のコマンドラインツールである MECSA-ST [23] を利用して，DNSSEC，DANE，StartTLS（著者らから組織への通信），X.509，MTA-STS の利用可否を確認した．X.509 の検証のために，Ubuntu 20.04 に含まれるルート認証局証明書を利用した．最終的に，メールセキュリティ解析対象となったドメインは 151 であり，表 2 は Publix Suffix List [24] にリスト化されている eTLD を基にドメイン数をまとめている．

4. 評価

4.1 質問紙調査

4.1.1 PPAP 採用状況と採用の理由

質問紙調査の結果，回答組織 344 のうち 64%にあたる 219 社が，PPAP を採用していると回答した．また，54 社は過去採用していたが現在は廃止していると回答した（16%）．全体としては，回答組織の約 80%は過去一度は PPAP を採用した実績があることになる．なお，現在 PPAP を採用中の 219 社のうち 42%に当たる 93 社が PPAP の廃止を検討中と回答した．図 3 に官公庁とそれ以外に分けて PPAP の採用状況を示す．

PPAP 採用組織に PPAP の具体的実施方法を尋ねたところ，パスワード付 ZIP ファイルをメール添付し（もしくはクラウドファイル共有サーバーにアップしてメールで連絡）その後同じメールの宛先にパスワードを別送という方法を採用している組織がほとんどであった．同じ宛先へのメールでのパスワード付 ZIP ファイル送付とは別の方法でパスワードを伝えるケースは（電話・事前に決めたパスワード等）PPAP の機密性向上が見込まれるが，採用組織は 16 社にとどまった．PPAP 採用開始時期は 2017 年が最も多く（12 社）次いで 2016 年で（11 社）あった（図 4）．ただし，採用時期は不明と回答した組織が最も多い（139 社）．

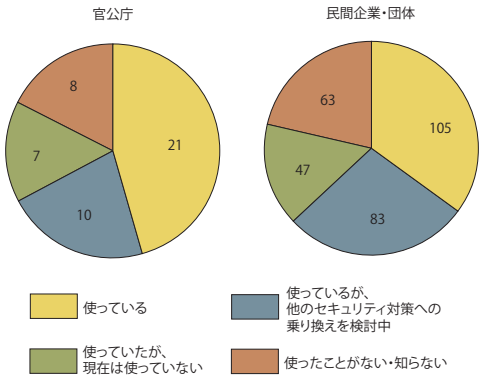

図 3 PPAP 採用状況

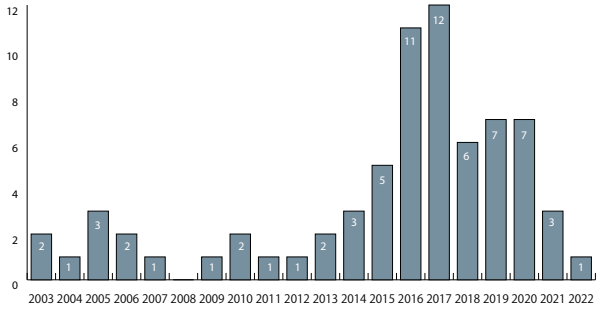

図 4 PPAP の採用開始時期（139 社が不明と回答）

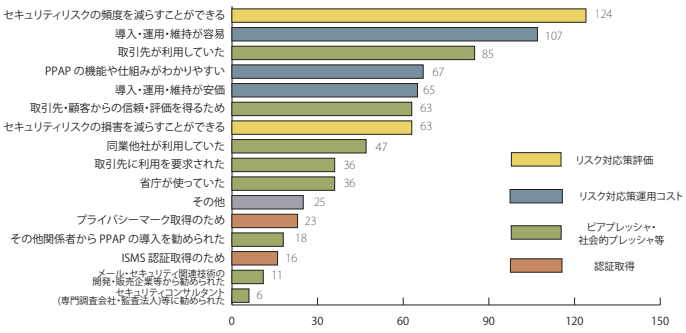

図 5 PPAP の採用理由（複数回答可）

続いて，PPAP を採用している組織に対して，採用理由を聞いた．セキュリティリスク頻度を減らすことができるからが最も多く，採用組織の半数以上が理由として回答した（124 社）．次いで多いのは，導入・運用・維持が容易であるからという理由であった（図 5）．全体として，リスク対策評価に関する理由（同図黄色）や運用コストに関する理由（同図青色）が採用理由として多い．

4.1.2 PPAP の有害性・無効性の認識

PPAP を現在採用中の組織（219 社）の約 88 %は，PPAP の有害性・無効性を認識していることが明らかになった（図 6）．また，デジタル改革担当相や内閣府と内閣官房が 2020 年 11 月に PPAP 廃止を宣言したことを知っている組織も 179 社（79.5%）にのぼった．暗号をかけずに送ったほうが総合的なセキュリティリスクが PPAP より小さいことを知っている組織は 104 社と PPAP 採用組織の半

数を下回った．

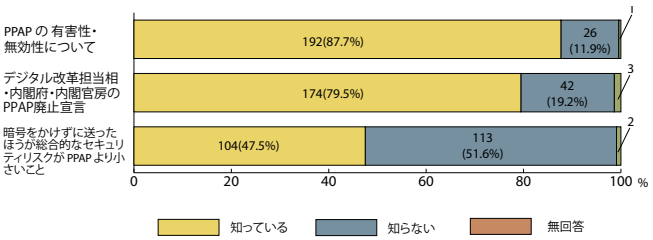

図 6　PPAP を採用している組織の PPAP をめぐる認識状況

4.1.3　PPAP を廃止しない理由

PPAP 採用組織が PPAP を使い続けている理由を尋ねたところ，セキュリティ対策変更のコスト・工数を考えるとシステム変更できないからが最も多く（43 社），次いで PPAP は運用のために社員が取るべき手順が明確であるからが続いた（38 社）．また，同業他社も PPAP を使っているからが 36 社，PPAP よりや平文メールよりもセキュリティリスクが小さい方法が見つからないからが 34 社であった（図 7）．さらに，PPAP 採用組織に PPAP をやめることを検討しうるきっかけとなる事象について聞くと，最も多い回答はより有効性のあるセキュリティ対策があった場合（127 社）で，次いで取引先から廃止を求められた場合が 99 社であった．また，府省からの指針がでた場合と回答する組織も多い（図 8）．なお，その他と回答した組織の中では所管業務の省庁からの指針（農水省，文科省，厚労省等）との回答が最も多かった．

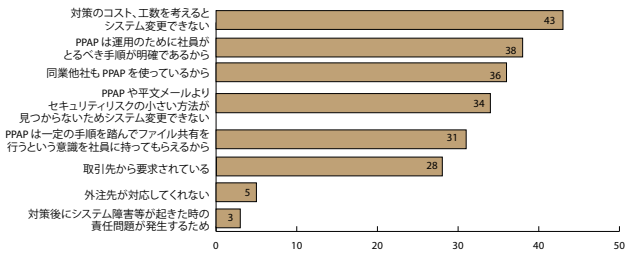

図 7　PPAP を現在も使い続けている理由（複数回答可）

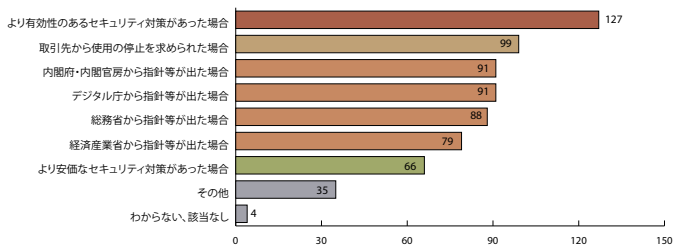

図 8　PPAP をやめることを検討しうるきっかけとなる事象（複数回答可）

4.1.4　PPAP を廃止した理由

本質問紙調査では 54 の組織（官公庁 7, 企業団体 47）が過去に PPAP を採用も現在は利用していないと回答しているが（図 3），現在 PPAP を利用していない理由としては，PPAP はセキュリティ対策として意味をなさないからや（33 社），デジタル庁・内閣府・内閣官房の PPAP 廃止宣言等を受けて（30 社）が多い．なお，現在 PPAP を利用していない組織（54 社）と PPAP を一度も使ったことがない組織（125 社）で採用中のファイル添付の方法としては，ファイル共有クラウドサービス（Google ワークスペース，Dropbox 等）が最も多く（45 社），組織内もしくは関係者専用のファイル共有サーバーを利用している組織も多い（31 社）．

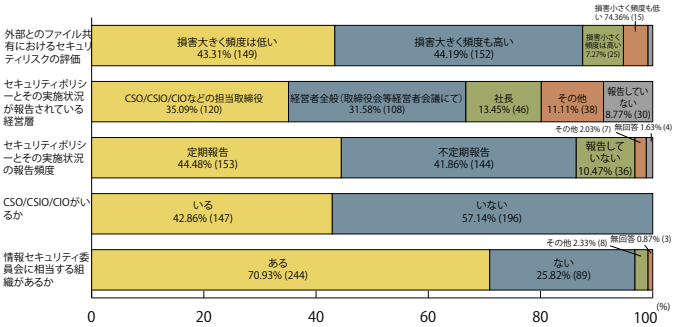

図 9　セキュリティポリシーに関する取り組み状況

4.1.5　組織における情報セキュリティポリシー

続いて，PPAP に限らず情報セキュリティ一般の取り組み状況を把握するために，全回答者にセキュリティポリシーの実施状況等を聞いた（図 9）．外部とのファイル共有に関するセキュリティリスクの評価を尋ねると，損害の大きさと頻度とも大きいと評価をしている組織が多く，全体としては損害の大きさは大きいと評価している組織が多い．情報セキュリティ関連業務のうち，回答組織が外注している工程を図 11 に示す．開発や運用の外注が最も多く，システム用件の作成や仕様書の作成から外注している組織も 100 以上あった．また，情報セキュリティに関する情報源については，IPA のガイドラインが最も多く（251 社）次いで JPCERT/CC やセミナー情報，総務省のガイドラインが続く．

各種情報セキュリティに関する取り組み状況と PPAP 採用の関連性を確認するために，PPAP 採用の割合について比率の検定を行った（表 3）．CSO（もしくは CIO・CSIO）に相当する役職が組織に存在する場合の PPAP の採用率は 56.38%で CSO 等の役職が存在しない組織に比べて PPAP の採用率は低い傾向にある．他方，情報セキュリティ委員会に相当する組織が存在する場合の PPAP 採用率（74.43%）はむしろ情報セキュリティ委員会に相当する組織が存在しない場合（57.73%）に比べて高い傾向にある．情報セキュリティ関連業務を全て内製しているかどう

かや，情報システム関連人材はなるべく社内育成しているかどうか，情報セキュリティ業務の要件や仕様書の外注有無による PPAP 採用率の大きな違いは見られなかった．これらの関連性をさらに確認するため，PPAP の現在の採用有無をアウトカム，組織規模や情報セキュリティへの取り組み状況や業種を共変量としてロジスティクス回帰分析を行った．表 4 に記述統計量を，図 10 に分析結果のオッズ比と 95%信頼区間を示す．従業員数については標準化した値（z-score）を用いた．ロジスティクス回帰分析においても，CSO 等が存在する組織は PPAP を採用しない傾向にあることが確認された．

表 3　情報セキュリティへの取り組みに応じた PPAP 採用率

	Yes	No	Z test score
CSO/CIO/CSIO がいる	56.38%	69.23%	-2.456**
情報セキュリティ業務は全て内製	61.90%	63.91%	-0.253
情報セキュリティ委員会がある	74.43%	57.73%	2.968***
情報シス関連人材はなるべく組織内育成	64.50%	62.86%	0.316
要件や仕様書の外注	64.71%	64.84%	-0.027

Note 1: Z test score は比率の差の検定の値（両側検定）．
***: $p < 0.01$, **: $p < 0.05$

表 4　ロジスティクス回帰分析で用いた変数の記述統計量

N =344	mean	std	min	max
PPAP 採用	0.64	0.48	0	1
CSO/CSIO/CIO の存在	0.43	0.50	0	1
情報セキュリティ委員会有無	0.72	0.45	0	1
従業員数	2684.67	3298.84	622	48179
情報セキュリティ業務は全て内製	0.12	0.33	0	1
要件定義を外注	0.30	0.46	0	1
仕様書作成を外注	0.36	0.48	0	1
建設業	0.07	0.26	0	1
製造業	0.20	0.40	0	1
卸売・小売・飲食業	0.08	0.28	0	1
運輸・通信業	0.06	0.25	0	1
サービス業	0.38	0.49	0	1
公務	0.13	0.34	0	1

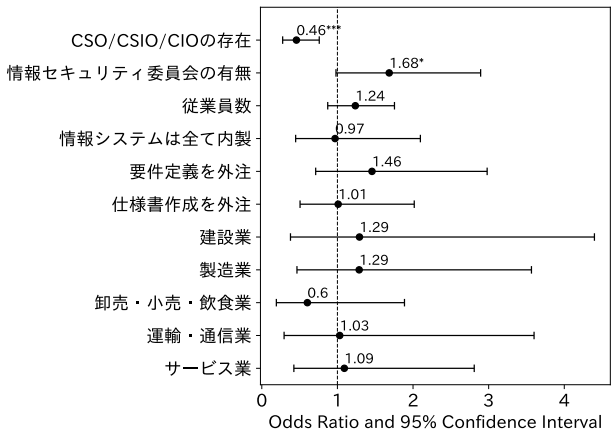

図 10　ロジスティックス回帰分析で求めたオッズ比とオッズ比の 95%信頼区間．図中 *** は 0.01 有意水準で，* は 0.1 有意水準でオッズ比が有意であることを示す．

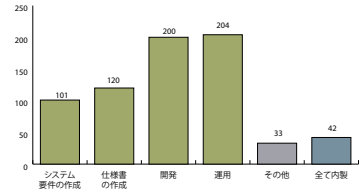

図 11　情報セキュリティ関連の業務のうち（一部，全部問わず）外注しているもの

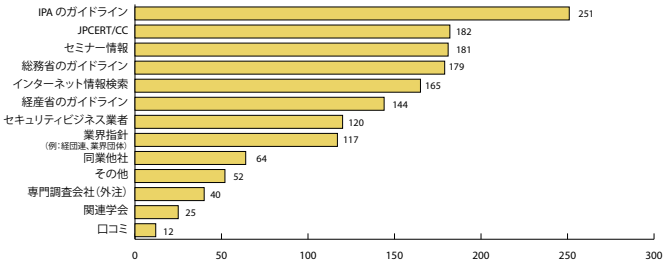

図 12　情報セキュリティに関する情報源

ここまで，質問紙調査結果概要を示した．質問紙調査結果からは，調査に協力した国内の組織のおよそ 64%が PPAP を 2022 年 6 月現在も利用していて，PPAP 利用組織の 88%は PPAP の有害性・無効性を認識しているにも関わらず利用を継続していることが明らかになった．さらに PPAP を廃止しない理由としては，対策システム変更のコストの他，PPAP は利用者がとるべき手順が明確であることも理由となっていることが明らかになった．PPAP は何らかの手順を踏んで実施することによって「何かをやった気になる」心理的な安心感を与えていて，この安心感も採用継続に寄与している可能性がある．これらのことから，より有効なファイル共有方法等の代替対策があったとしても，システム変更コストへの組織の受容度が低い場合や明確な手順を踏む心理的な安心感が得られない場合は組織における無意味なセキュリティ慣行の廃止には至らない可能性が示唆される．また，CSO 等が組織に存在する場合は，PPAP の採用率は低い傾向にあることが示された．情報技術と経営の双方に関する知見を有する人材が組織に存在することで，より有効なセキュリティ対策を検討し採用している可能性がある．他方，本調査の結果からは情報セキュリティ委員会が存在する場合の PPAP 採用率はやや大きい傾向があり，組織として有効なセキュリティ対応策を出せていない可能性も示唆される．

4.2　メールセキュリティ解析

表 5 は，PPAP 採用の動機でもあるメールの機密性に関わるメールセキュリティ要素の利用可否の組み合わせとドメイン数を表し，6 要素の利用可否による存在した組み合わせ数は 6 である．残念ながら，MTA-STS と DNSSEC（したがて DANE も）はどの組織も導入していない．したがって，本解析において機密性に関するセキュリティレベ

表 5 機密性に関わるメールセキュリティ要素の利用可否の組み合わせとドメイン数

メールセキュリティ要素の利用可否の組み合わせ						ドメイン数											合計
DNSSEC	DANE	Enc. (out†)	Enc. (in††)	X.509	MTA-STS	.biz	.com	.group	.jp	.ac.jp	.co.jp	.go.jp	.lg.jp	.ne.jp	.or.jp	.org	
✗	✗	✓	✓	✓	✗	1	21	1	4	12	52	1	0	1	4	1	98
✗	✗	✗	✓	✓	✗	0	0	0	1	0	4	0	0	0	0	0	5
✗	✗	✓	✓	✗	✗	0	1	0	2	0	2	0	6	0	1	0	12
✗	✗	✓	✗	✗	✗	0	1	0	1	1	9	0	1	0	2	0	15
✗	✗	✗	✓	✗	✗	0	0	0	0	0	1	0	0	0	0	0	1
✗	✗	✗	✗	✗	✗	0	1	0	2	2	5	0	3	1	6	0	20

† 組織から外部組織への通信.
†† 外部組織から組織への通信.

表 6 完全性に関わるメールセキュリティ要素の利用可否の組み合わせとドメイン数

メールセキュリティ要素の利用可否の組み合わせ			ドメイン数										合計
DNSSEC	DKIM	DMARC	.biz	.com	.group	.jp	.ac.jp	.co.jp	.go.jp	.lg.jp	.ne.jp	.or.jp	.org	
✗	✓	✓	1	20	1	3	6	41	1	1	0	0	0	74
✗	✓	✗	0	2	0	1	5	9	0	0	0	1	1	19
✗	✗	✗	0	2	0	6	4	23	0	9	2	12	0	58

表 7 真正性に関わるメールセキュリティ要素の利用可否の組み合わせとドメイン数

メールセキュリティ要素の利用可否の組み合わせ				ドメイン数										合計
DNSSEC	SPF	DKIM	DMARC	.biz	.com	.group	.jp	.ac.jp	.co.jp	.go.jp	.lg.jp	.ne.jp	.or.jp	.org	
✗	✓	✓	✓	1	20	1	3	6	39	1	1	0	0	0	72
✗	✓	✓	✗	0	2	0	1	5	8	0	0	0	1	0	17
✗	✗	✓	✓	0	0	0	0	0	2	0	0	0	0	0	2
✗	✓	✗	✗	0	2	0	5	4	20	0	9	2	10	0	52
✗	✗	✓	✗	0	0	0	0	0	1	0	0	0	0	1	2
✗	✗	✗	✗	0	0	0	1	0	3	0	0	0	2	0	6

ルが最も高いのは，X.509 と組織から外部組織へと外部組織から組織への両方向通信の暗号化がサポートされている場合で，全体の 65%を占めている．しかし，MTA-STS が実装されていないため，TLS を強制できず，攻撃は可能である．MTA-STS の実装が遅れているのは，仕様確定が 2018 年と比較的新しいためと考えられる．一方，機密性に関するセキュリティレベルが最も低い（全要素がサポートされていない）状況も確認され，全体の 13%を占めた．87%は TLS による防御は志向しているが，DNSSEC もしくは MTA-STS の未実装により，理想的な機密性は実現できていない．また，外部組織から組織への通信において暗号化を利用する際に，その組織の X.509 は取得できるが，検証時に問題がある X.509（例：信頼されていない認証局を利用）を利用している場合があり，地方公共団体が利用するドメイン（.lg.jp）で最も多く確認された．

表 6 は完全性に関わるメールセキュリティ要素の利用可否の組み合わせとドメイン数を表している．3 要素の利用可否による存在した組み合わせ数は 3 であった．DKIM と DMARC がサポートされている状況が，本解析において完全性に関するセキュリティレベルが最も高く，全体の 49%を占めていた．一方，完全性に関するセキュリティレベルが最も低い（全要素がサポートされていない）状況も確認され，全体の 38%を占めた．

表 7 は真正性に関わるメールセキュリティ要素の利用可否の組み合わせとドメイン数を表している．4 要素の利用可否による存在した組み合わせ数は 6 であった．SPF，DKIM，DMARC がサポートされている状況が，本解析において真正性に関するセキュリティレベルが最も高く，全体の 48%を占めていた．SPF のみがサポートされている状況は，全体の 34%を占めていた．

本解析では，3.2 節で示した理想的なセキュリティレベルを達成するメール運用を行っている組織はないことが明らかになった．そのため，2 節で示した PPAP に対する攻撃に対して脆弱である．抜本解である DNSSEC サービスを格安で提供する事業者もあるため，短期的視点でコストの高い PPAP 代替手段を探すよりも，長期的視点に立って，低コストの DNSSEC の導入を検討すべきである．

5. おわりに

本稿では，日本国内の暗号化 ZIP 添付によるメールセキュリティに関する実態把握を目的とした調査研究の結果を速報値的に報告した．本研究では，暗号化 ZIP 添付によるメールセキュリティ対策（通称 PPAP）を採用している組織の 88%がその有害無効性を認識しているにも関わらず利用を継続していることや，PPAP に対する攻撃に対して脆弱なメール運用を行なっている組織が多いことが明らかになった．

これまでも，一般的に技術的に優位なセキュリティ対策

が組織で採用されるとは限らないことは指摘されてきたが，運用中のセキュリティ対策の有害・無効性を認識しながら採用撤廃に至らない状況がなぜ解消されないのかに関する知見は十分とは言えない．今後の研究課題としたい．また，メールセキュリティ解析の結果からは，TLS 志向は強いが，コア技術である DNSSEC，DANE，MTA-STS をサポートしたメール運営は確認できていないなど，PPAP に対する攻撃に脆弱なメール運営であることが分かったが，各種コア技術採用の判断をめぐる組織担当者の知見や役割，メール運営を巡る組織を取り巻くビジネス構造等を検証することが求められる．

謝辞 本調査にご協力くださった組織の皆様に感謝を申し上げます．

本研究は東京大学空間情報科学研究センター研究倫理委員会でのヒトを対象とする研究倫理審査において承認を受けて実施した．

参考文献

[1] West, R.: The psychology of security, *Communications of the ACM*, Vol. 51, No. 4, pp. 34–40 (online), DOI: 10.1145/1330311.1330320 (2008).

[2] AlHogail, A.: Design and validation of information security culture framework, *Computers in Human Behavior*, Vol. 49, pp. 567–575 (online), DOI: 10.1016/j.chb.2015.03.054 (2015).

[3] Dhillon, G., Oliveira, T., Susarapu, S. and Caldeira, M.: Deciding between information security and usability: Developing value based objectives, *Computers in Human Behavior*, Vol. 61, pp. 656–666 (online), DOI: 10.1016/j.chb.2016.03.068 (2016).

[4] Greenwald, S. J., Olthoff, K. G., Raskin, V. and Ruch, W.: The User Non-Acceptance Paradigm: INFOSEC's Dirty Little Secret, *Proceedings of the 2004 Workshop on New Security Paradigms*, NSPW '04, New York, NY, USA, Association for Computing Machinery, p. 35–43 (online), DOI: 10.1145/1065907.1066032 (2004).

[5] Schneier, B.: Airplane hackers, *IEEE Security Privacy*, Vol. 1, No. 6, pp. 92–92 (2003).

[6] Felten, E.: Security Theater, , available from ⟨https://freedom-to-tinker.com/2004/07/09/security-theater/⟩ (accessed Aug. 15, 2022).

[7] Schneier, B.: The Psychology of Security, *Progress in Cryptology – AFRICACRYPT 2008* (Vaudenay, S., ed.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 50–79 (online), DOI: 10.1145/1330311.1330320 (2008).

[8] Geer, D. E.: Security Theater, the Beat Goes On, *IEEE Security & Privacy*, Vol. 18, No. 4, pp. 75–76 (online), DOI: 10.1109/MSEC.2020.2992210 (2020).

[9] Anderson, J. M.: Why we need a new definition of information security, *Computers & Security*, Vol. 22, No. 4, pp. 308–313 (online), DOI: 10.1016/S0167-4048(03)00407-3 (2003).

[10] AlHogail, A. and Mirza, A.: Information security culture: A definition and a literature review, *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Hammamet, Tunisia, IEEE, pp. 1–7 (online), DOI: 10.1109/WCCAIS.2014.6916579 (2014).

[11] AlHogail, A.: Design and validation of information security culture framework, *Computers in Human Behavior*, Vol. 49, pp. 567–575 (online), DOI: 10.1016/j.chb.2015.03.054 (2015).

[12] Tolah, A., Furnell, S. M. and Papadaki, M.: A Comprehensive Framework for Understanding Security Culture in Organizations, *Information Security Education. Education in Proactive Information Security* (Drevin, L. and Theocharidou, M., eds.), Vol. 557, Springer International Publishing, pp. 143–156 (online), DOI: 10.1007/978-3-030-23451-5_11 (2019).

[13] Furnell, S.: Recognising and Addressing Barriers to eSafety and Security Awareness, p. 12 (2009).

[14] Leach, J.: Improving user security behaviour, *Computers & Security*, Vol. 22, No. 8, pp. 685–692 (2003).

[15] Michelberger, P. and Lábodi, C.: After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model), *Acta Polytechnica Hungarica*, Vol. 9, No. 4, p. 16 (2012).

[16] 大泰司章：PPAP とはなにかーその発展の黒歴史ー，情報処理， Vol. 61, No. 7, pp. 08–713 (2020).

[17] 崎村夏彦：さようなら，意味のない暗号化 ZIP 添付メール，情報処理， Vol. 61, No. 7, pp. 706–707 (2020).

[18] 楠正憲：PPAP のセキュリティ意義, 情報処理, Vol. 61, No. 7, pp. 714–718 (2020).

[19] 上原哲太郎：我々はなぜ PPAP するようになってしまったのか，情報処理， Vol. 61, No. 7, pp. 714–718 (2020).

[20] 日経新聞朝刊：サイバー攻撃広がる裏口（下）ウイルス，カプコン仕様に，暗号ファイルに隠れ侵入も，端末監視対策，費用の壁 (2021 年 1 月 14 日).

[21] Kambourakis, G., Gil, G. D. and Sanchez, I.: What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security, *IEEE Access*, Vol. 8, pp. 130066–130081 (online), DOI: 10.1109/ACCESS.2020.3009122 (2020).

[22] Spring, J. and Metcalf, L.: Probable Cache Poisoning of Mail Handling Domains, Carnegie Mellon University's Software Engineering Institute Blog (2014. [Online]).

[23] European Comission: MECSA Standalone Tool, , available from ⟨https://github.com/mecsa/mecsa-st⟩ (accessed Aug. 16, 2022.)

[24] Mozilla Foundation: Public Suffix List, , available from ⟨https://publicsuffix.org/⟩ (accessed Aug. 14, 2022.)