JP AAWG Japan Anti-Abuse Working Group

ここが変だよPPAP

このセッションについて

- 基本記事化OK

※ただし、「オフレコでお願いします」と前置きした部分に関してはこの場限りでお願いします。

- 質問はzoomのQA機能にてお願いします

登壇者紹介

登壇者紹介

- 平野 善隆
  - 株式会社クオリティア
  - PPAP含め、メッセージング関連ソリューション開発・システム開発
- 関根 章弘
  - Vade Secure株式会社
  - TAMとしてメールフィルタの顧客をサポート
- 北川 直哉
  - 国立情報学研究所
  - メールシステムを含むネットワークサービスやセキュリティの研究に従事
- 森崎 聡
  - 株式会社オプテージ
  - メールシステム運用者

アンケートについて

JPAAWG

アンケート実施内容

- PPAPを中心に、メールでの暗号化ファイルの送受信の実態について質問

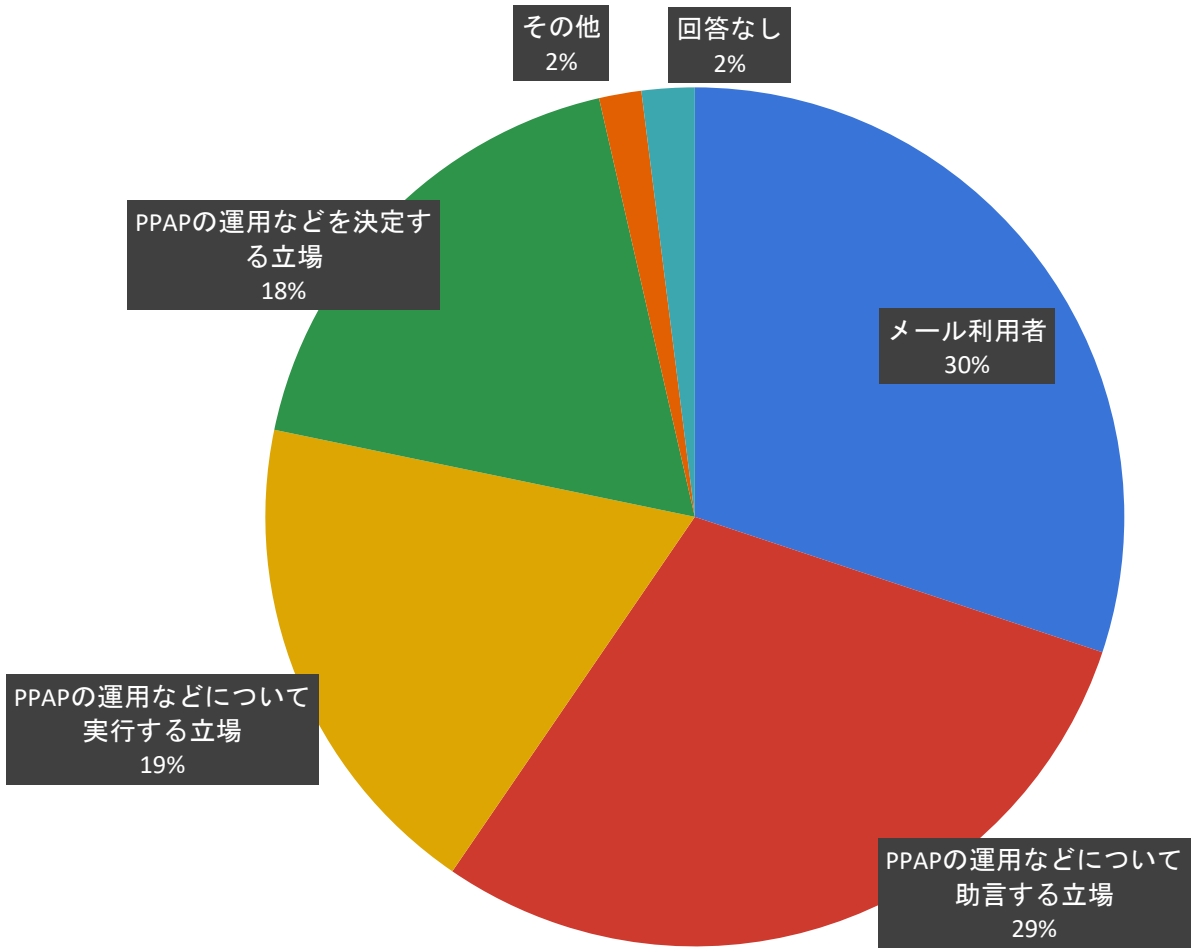
- 2つのチャンネルを利用してアンケートを実施
  - 本イベント申し込みサイトにて実施
    - 実施期間： 2021年2月1日～2月22日
    - 有効回答数：240件

  - 株式会社クオリティアの協力のもと、同社のメーリングリストにて依頼
    - 実施期間： 2021年2月4日～2月15日
    - 有効回答数：514件

- 速報版
  - https://www.jpaawg.org/docs/event/2021ppap/

回答者の内訳

- 有効回答数(N=754)



日本独自のPPAP

JP AAWG

アメリカにもあるのはあるらしい

- Compress files in .zip or .zipx formats
- Encrypt the compressed file using Advanced Encryption Standard (AES),
- Use a strong 256-bit encryption key string,
- Ensure a strong password or pass phrase is generated to encrypt the file and
- Communicate the password or pass phrase with the Safeguards Office through a SEPARATE email or via a telephone call to your IRS contact person. Do NOT provide the password or pass phrase in the same email containing the encrypted attachment.

https://www.irs.gov/privacy-disclosure/email-encryption-procedures-using-the-winzip-utility

ファイルの渡し方を聞いてみた-1/3

- Aさん（プリセールス）
  - クラウドストレージ（Box）を使ってファイルを渡す
  - 必要に応じてファイル単位、またはフォルダ単位でパスワードを設定することがある
  - パスワードはメールで送る
  - 宛先間違いに気づいたらファイルを消してしまえばいい
  - メールでファイルを送るとバージョンの異なる複数のファイルができてしまい、管理が大変なので嫌いだ

ファイルの渡し方を聞いてみた-2/3

- Bさん（サポート）
  - クラウドストレージ（Box）を使ってファイルを渡す
  - パスワードを設定し、パスワードはメールで送る
  - ダウンロード可能な期間を短く設定しておき、いつまでもアクセスできる状態で放置されないようにする
  - ファイルアクセス時にメールで通知が届くように設定しておくことで、不審な多量のアクセスに気づいて対応できるようにしている

ファイルの渡し方を聞いてみた-3/3

- Cさん（エンジニア）
  - オフィスドキュメントのやりとりはあまりない
  - 必要になったらクラウドストレージ（Box）を使うだろう
  - パスワードを設定し、パスワードはメールで送る
  - 自分はそこまでやらないが、セキュリティを考慮するならパスワードをメールで送る時はPGPで署名した暗号メールで送るのが安全だと思う

フィルタエンジニアのコメント

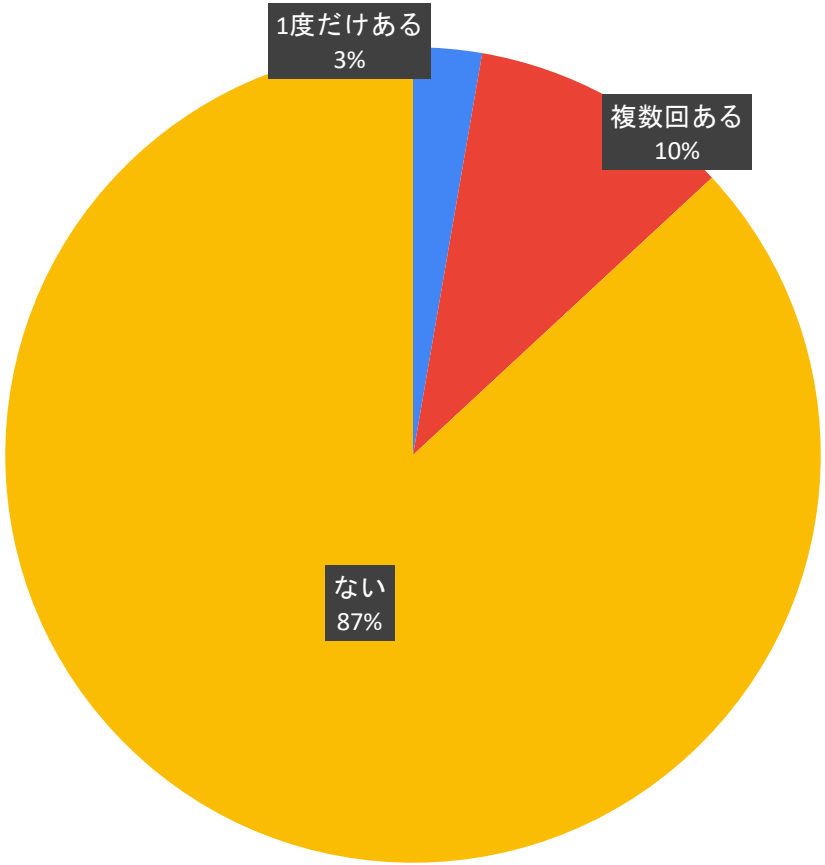
- フィルタでファイルをスキャンできないのはパスワード付きZipでもリンクでも変わらない
  - パスワード付きZip：解凍した時点でウィルススキャンされる
  - リンク：ファイルをダウンロードした時点でウィルススキャンされる
- ハックされた時に可能な対応に違いがある
  - リンク先のファイルを削除することで被害の拡大を止めることができる
- 大きな違いはストレージ
  - 大勢にコピーを送ると、その分ディスクを圧迫する。リンクなら変わらない

誤送信防止のPPAP

JP AAWG

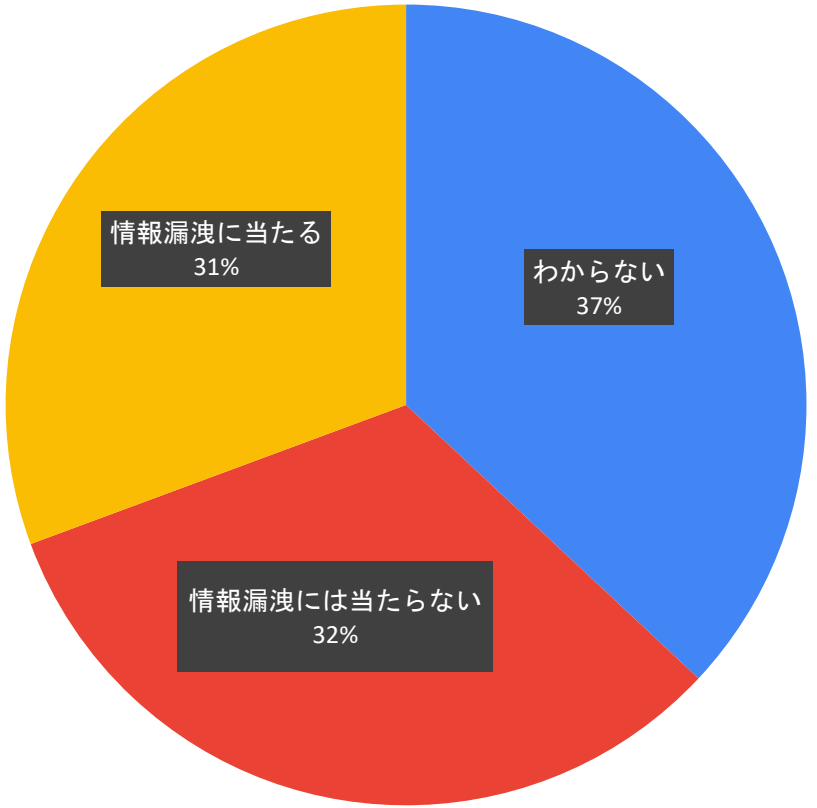
誤送信防止とPPAP

パスワードを送らないことで誤送信を防止できた経験がありますか



N=626

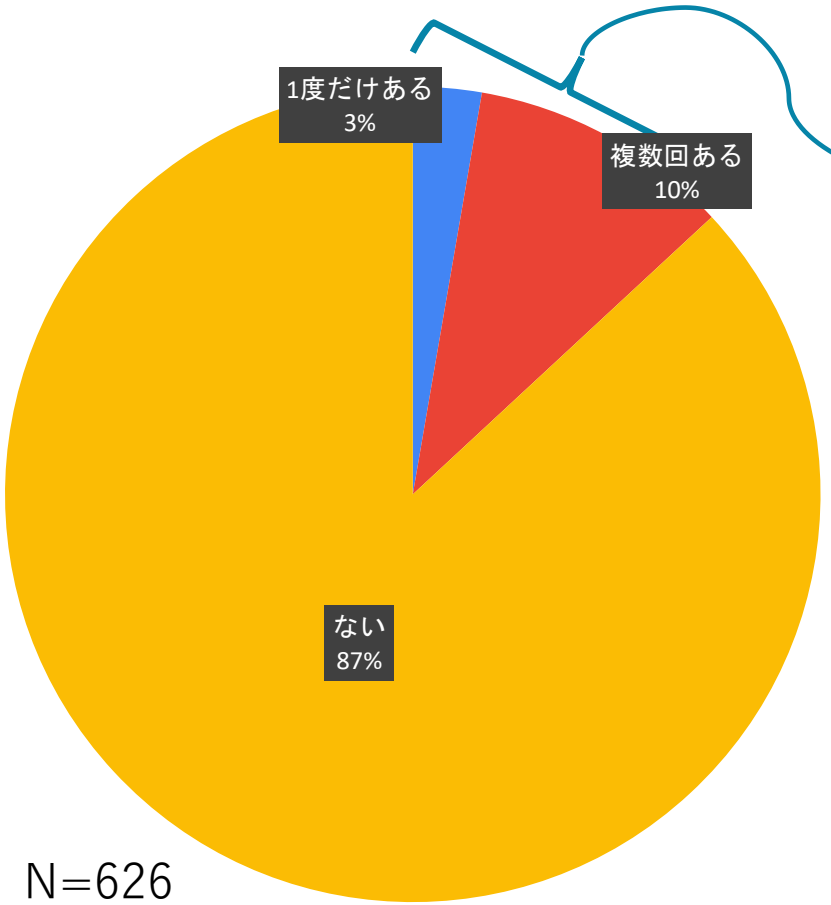
暗号化zipファイルは相手に届いたが、誤送信に気が付いてパスワードを送信しなかった場合、組織内ではどのように扱われますか



N=633

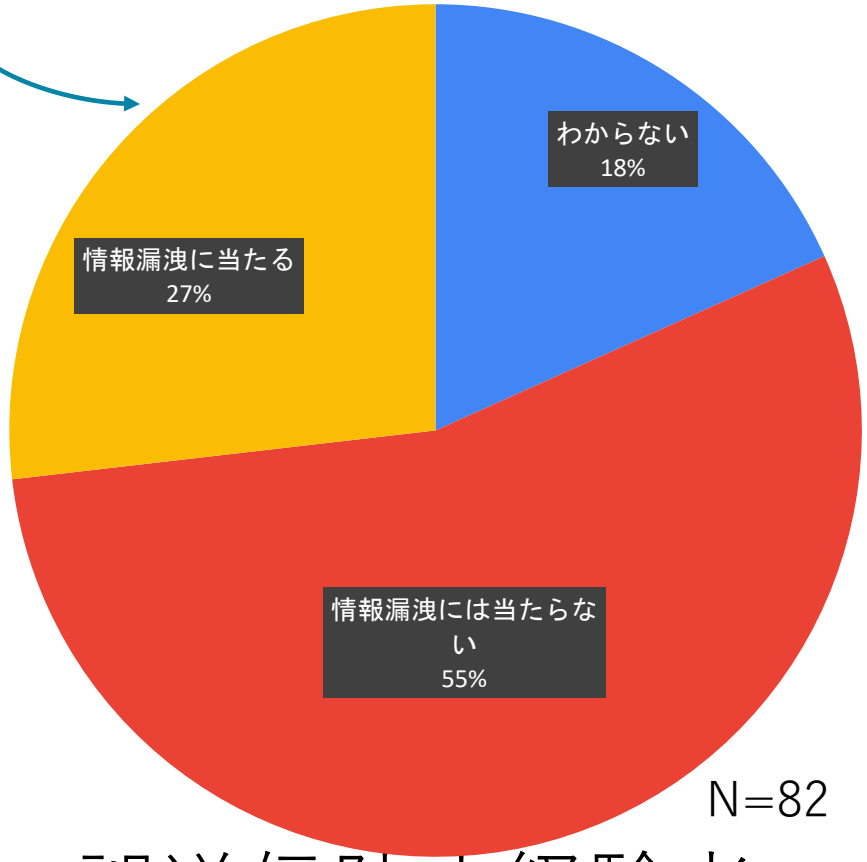
誤送信防止とPPAP

上記のようにパスワードを送らないことで誤送信を防止できた経験がありますか



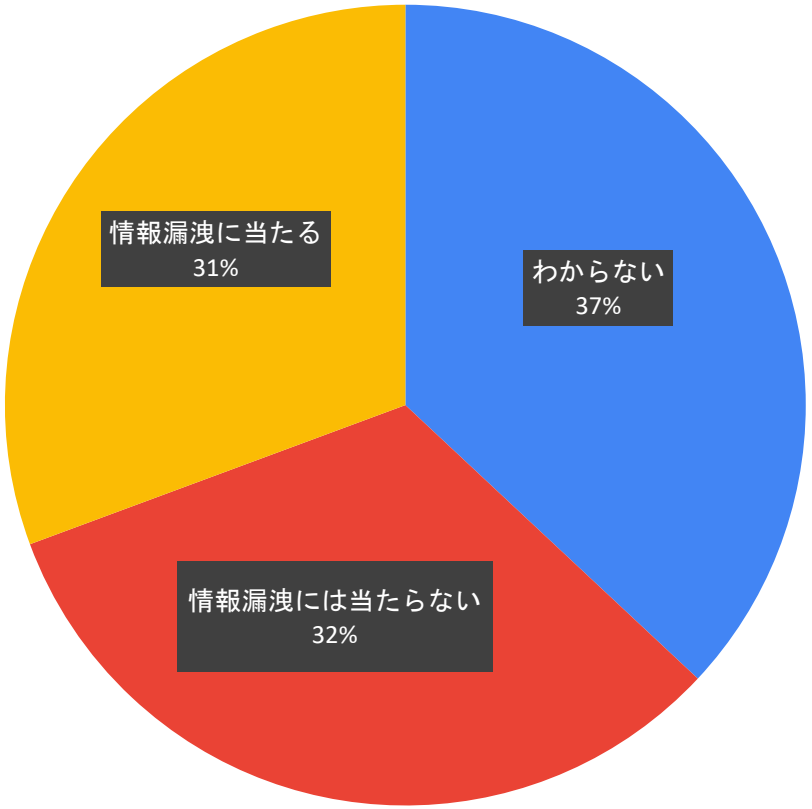
N=626

暗号化zipファイルは相手に届いたが、誤送信に気が付いてパスワードを送信しなかった場合、組織内ではどのように扱われますか



N=82

誤送信防止経験者



N=633

全体

暗号化としてPPAP

JPAAWG

暗号化zipは弱いらしい

- ほんとにパスワードを解読できるのか?!
- できるとしたら、時間は? コストは?
- OfficeやPDFの暗号化も弱いの?

試してみました

GPU構成	GPU費用	提供開始時期	ハッシュ演算速度(実測)※1
GeForce RTX2080Ti x 2枚 Ubuntu 18.04.5 LT CUDA 10.1.105	1枚当たり10万円～	2018年　9月	20GH/s
GeForce GTX1660 SUPER(Thunderbolt接続) Windows10 CUDA 11.2.0	2.5万円～	2019年10月	5GH/s
AWS EC2 p3.2xlarge (Tesla V100)	3.06USドル～/h (購入すると300万円ぐらい)	2017年10月	27GH/s ※未確認

※1　ZipCrypto方式の内部ハッシュ(鍵長96bit)を演算した場合の速度

zipパスワードの解析

文字数	最大解析時間（理論値）	パスワード	実際の解析時間
4	0.003秒	tyui	7秒
		C7*m	8秒
5	0.3秒	Nuwan	8秒
		Nuw4&	10秒
6	34秒	fhkldf	13秒
		f4kLdf	15秒
		fHk*d6	19秒
7	54分	mekasha	55秒
		mekAsha	55秒
		meks*ha	55秒
		me7s*h)	22分
		mK7s*h+	20分
		#K7s*h+	20分

文字数	最大解析時間（理論値）	パスワード	実際の解析時間
8	85時間	passw0rd	62分
		pa*sw0rd	64分
		pa*sw0(d	47時間
9	331日	h*kL0m(D+	断念
10	85年		
11	8021年		
12	74万年		
13	7088万年		
14	66億年		
総当たり	6263億年		

RTX 2080Ti 2枚
➔ 200億Hash / 秒

JPAAWG

zipパスワードの解析(文字種別)

文字数	英小文字のみ (26種類)	英数のみ (62種類)	英数記号 (94種類)
6	0.01秒	2.8秒	34秒
7	0.4秒	3分	54分
8	10秒	3時間	85時間
9	4.5分	7.8日	331日
10	2時間	1.3年	85年
11	2日	82年	8021年
12	55日	5100年	74万年
13	4年	31万年	7088万年
14	100年	2000万年	66億年

RTX 2080Ti 2枚
➔ 200億Hash / 秒

OfficeやPDFのパスワードの解析

Office

文字数	最大解析時間（理論値）	パスワード	実解析時間
4	32分		
5	50時間	nuwan	78分
		nu$an	78分
6	200日	He%4o-	断念
7	51年		
8	4800年		
9	45万年		
10	4300万年		
11	40億年		
12	3800億年		
13	35兆年		

RTX 2080Ti 2枚
➔ 4万Hash / 秒

PDF 128bit

文字数	最大解析時間（理論値）	パスワード	実解析時間
4	1.1秒		
5	110秒	nuwan	13秒
		nu$an	13秒
6	170分	He%4o-	75分
7	11日	l4sanTh	6日14時間
8	2.8年		
9	270年		
10	2.5万年		
11	240万年		
12	2.2億年		
13	210億年		

RTX 2080Ti 2枚
➔ 6800万Hash / 秒

JPAAWG

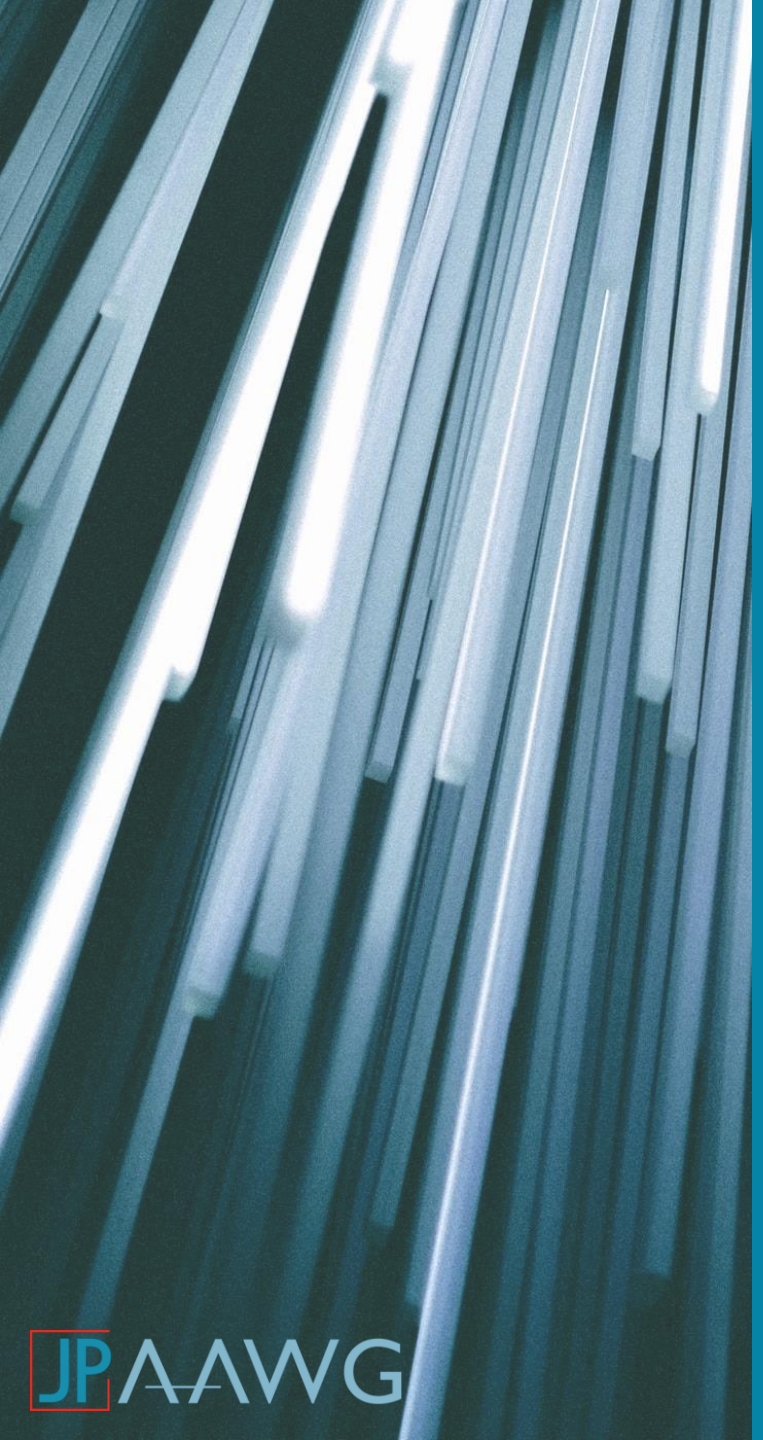
パスワード回復ツールの実測値からの、全パスワード解析想定時間

	文字数	パターン数	解析時間※1	費用※2	
アルファベット(大文字、小文字)、数字 併せて62種	8	$62^8 \fallingdotseq 218$兆$\fallingdotseq 2^{48}$	約2時間	約676円	ホビーレベル
	10	$62^{10} \fallingdotseq 84$京$\fallingdotseq 2^{60}$	約340日	約260万円	企業レベル
	12	$62^{12} \fallingdotseq 32$垓$\fallingdotseq 2^{71}$	約3500年	約100億円	犯罪者レベル
	14	**$62^{14} \fallingdotseq 12$抒$\fallingdotseq 2^{83}$**	**約1360万年**	**約38兆円**	
アルファベット(大文字、小文字)、数字、記号31種(“、スペース以外の印字可能なアスキー文字) 併せて93種	8	$93^8 \fallingdotseq 5596$兆$\fallingdotseq 2^{52}$	約2日	約1.7万円	ホビーレベル
	10	$93^{10} \fallingdotseq 4840$京$\fallingdotseq 2^{65}$	約53年	約1.5億円	
	12	**$93^{12} \fallingdotseq 4186$垓$\fallingdotseq 2^{78}$**	**約46万年**	**約1.3兆円**	犯罪者レベル
	14	**$93^{14} \fallingdotseq 3620$抒$\fallingdotseq 2^{92}$**	**約40億年**	**約1.1京円**	

※1 AWS EC2 p3.2xlarge(Tesla V100)を利用した場合の全ハッシュ計算時の最大時間(27GH/sで計算)
※2 全ハッシュ解析に伴うEC2 p3.2xlarge利用で発生する想定コスト(3.06USドル/h=323円/hで計算)

『解析時間』は全てのハッシュ値を計算するのにかかる最大時間であるため、実際はこれより速い時間にパスワードを解析できる

JPAAWG

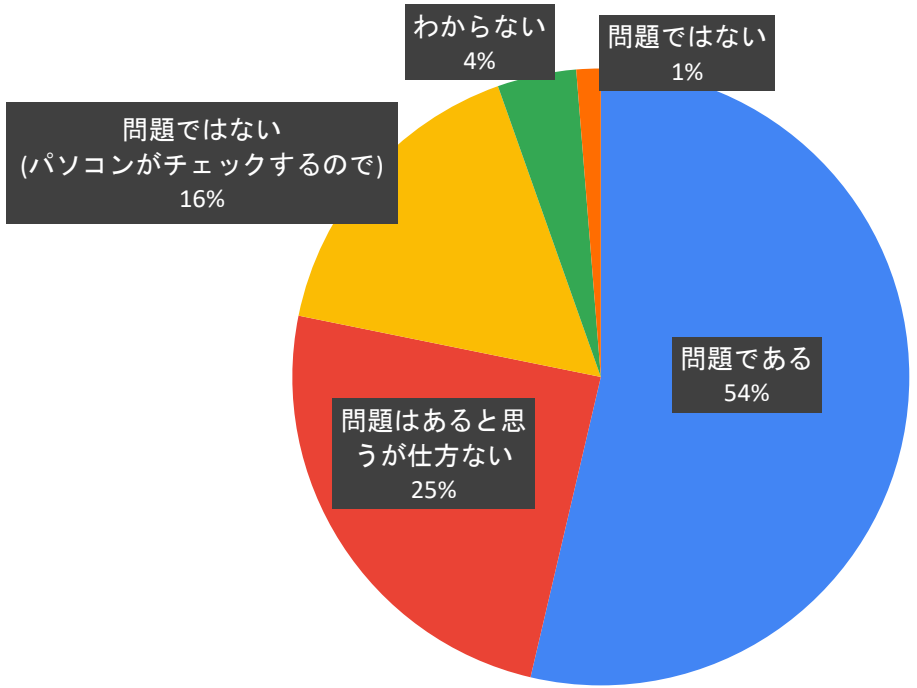


PPAPはウィルスフィルタが効かないからよくない?!

JP AAWG

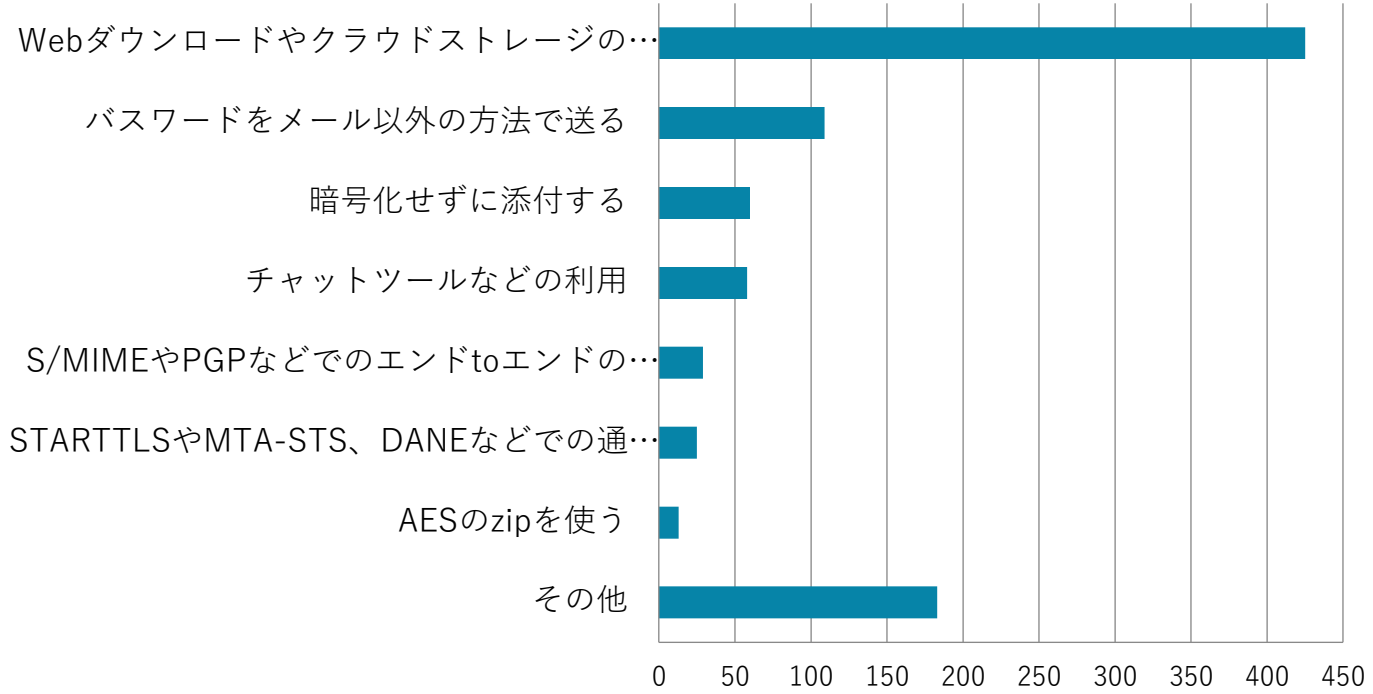
ゲートウェイでのウィルスフィルタ

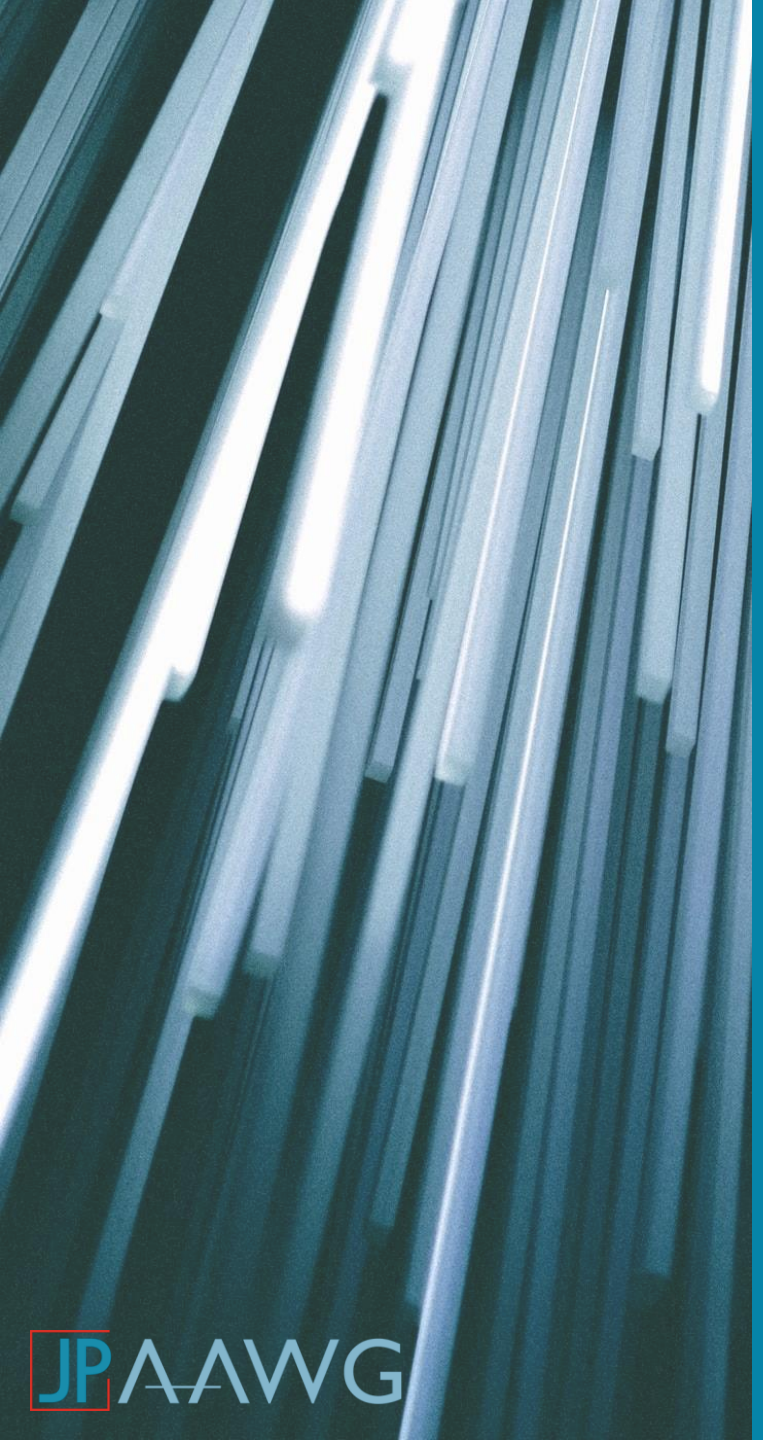
暗号化ファイルは、受信時にゲートウェイでウイルスチェックを行えないことが問題といわれています。このことについてどう思いますか



N=754

暗号化zipファイル送信の運用を検討をしている場合どのような方法を検討されていますか、またすでに運用を変更した場合どのように変更しましたか





アンケートで多かった意見（自由記述欄編）

JPAAWG

PPAPの問題点とは？

- メールが盗聴されていた場合、そもそも無意味（多数）
- 同じ宛先に自動でパスワードを送ったら誤送信防止にもならない（多数）
- 暗号化zipファイルはウィルスチェックが出来ない（多数）
- 暗号化添付ファイル送信が日常化すると、かえって悪意あるファイルを送りやすくなる
- 暗号化zipファイルは解読が容易なため、そもそも暗号化が無意味である
- 二度手間で、生産性を低下させるだけ
- 「なんちゃってセキュリティ」として形骸化しているだけ
- パスワードが自動送信される場合、誤送信防止としても無意味

重要な添付ファイルってどんなもの？

- 社外秘情報（人事情報、顧客情報、契約・注文情報など）
- 社内規定で「機密情報」とされている資料
- 取引先が保持している情報が含まれる資料
- 捺印済みの発注書
- アカウント情報や電話番号等、個人情報が含まれるファイル
- 会計情報が含まれる資料
- 図面
- パスワードが記載されたファイル
- 漏洩時にNDAや個人情報保護法に抵触する恐れのあるもの

暗号化ファイル受信の運用方針は？

- 暗号化ファイルの添付があった場合、メール自体の受信を拒否する
- クラウドストレージでファイル受け渡しを行う
- ファイル転送サービスを利用する
- メール以外の経路を検討する（パスワードは電話等で連絡）

（困っている点として）

- 自組織でPPAPで送るのを取りやめても、他部署や他社から送られてくるものはどうしようもない

Thank you for your listening!