パスワード付きzip添付メール問題を考える

アンケート集計結果

v1.0

JPAAWG　2021年2月25日

本資料は2021/2/25に行われたカンファレンスイベント「パスワード付きzip添付メール問題を考える」開催の際に実施したアンケートを集計したものです。

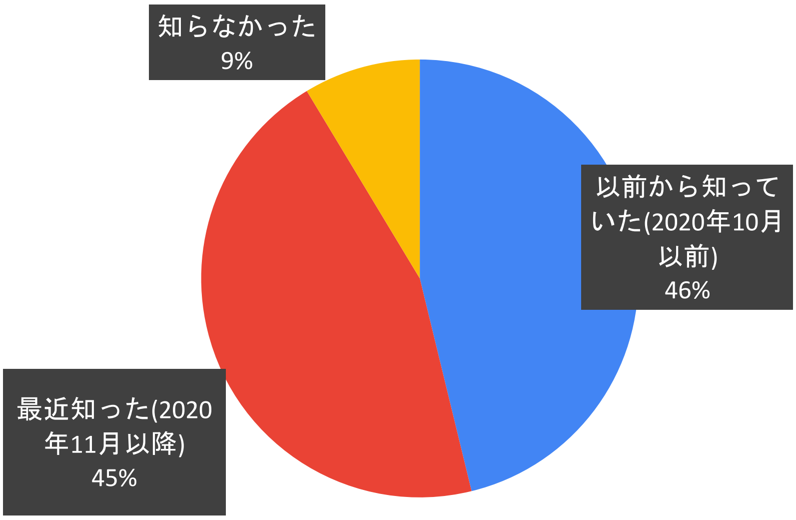
アンケートは下記2つのチャネルを利用して実施しました。

1. イベントの申し込みサイトや開催案内メールからのリンクとして実施
   実施期間: 2021年2月1日 ～ 2月24日
   有効回答数: 261件

2. 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1日 ～ 2月15日
   有効回答数: 514件

1. PPAPについて

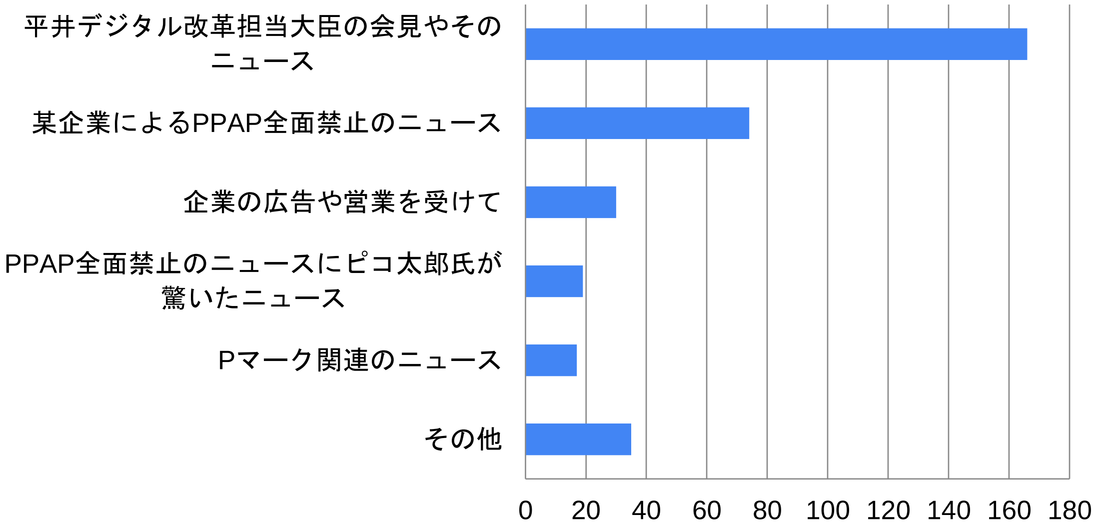
Q1-1. PPAPとはメールで添付ファイルを暗号化して、パスワードを別のメールで送ることを言います。PPAPという言葉を知っていますか。



N=775

以前から知っていた(2020年10月以前)	358
最近知った(2020年11月以降)	350
知らなかった	67

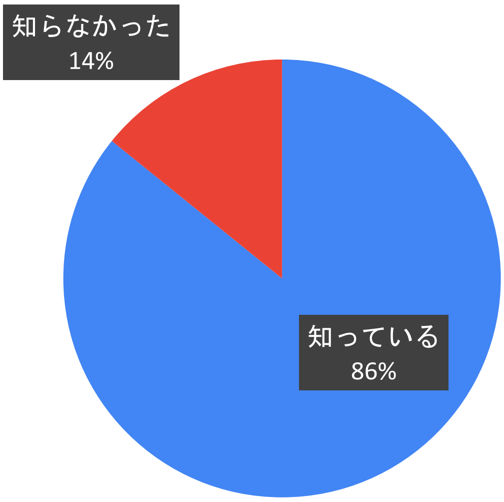
Q1-2. 最近知った方はどこで知りましたか。(最近知った方のみご回答ください)



N=341

平井デジタル改革担当大臣の会見やそのニュース	166
某企業によるPPAP全面禁止のニュース	74
企業の広告や営業を受けて	30
PPAP全面禁止のニュースにピコ太郎氏が驚いたニュース	19
Pマーク関連のニュース	17
その他	35

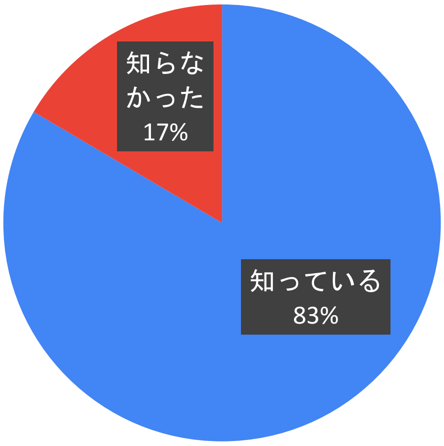
Q1-3. 平井卓也デジタル改革担当大臣の発表により2020年11月26日から内閣府及び内閣官房でのPPAPの利用が廃止されました。このことを知っていますか。



N=775

知っている	665
知らなかった	110

Q1-4. PPAPについて、セキュリティ観点から問題があると言われていることについて知っていますか。



N=775

知っている	647
知らなかった	128

Q1-5. 知っている場合、それはどのような問題ですか。(知っている方のみご回答ください)
(自由記述)

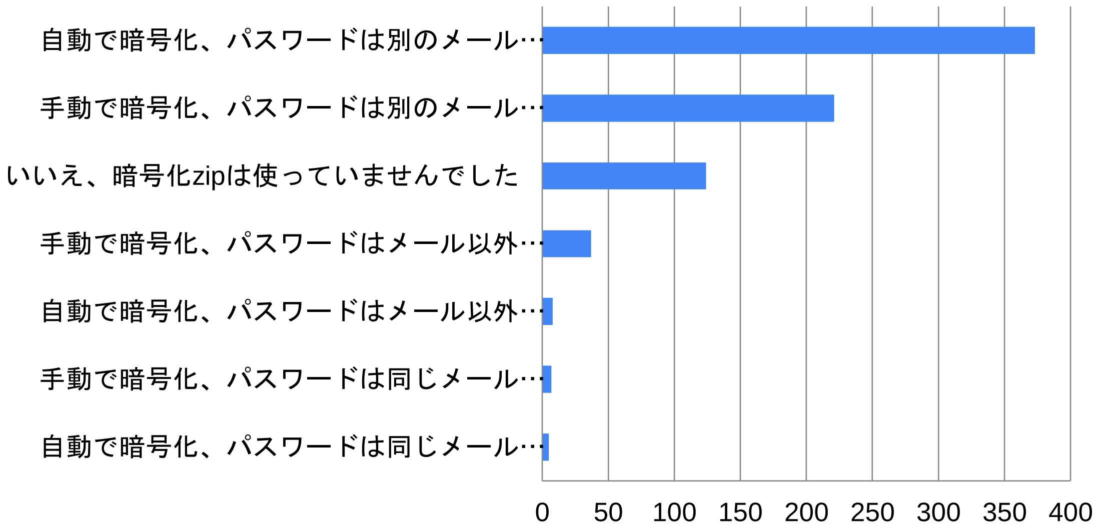
要約

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

などなど多数。詳細は8.自由記述欄回答を参照ください。

2. 暗号化zipでの送信運用について

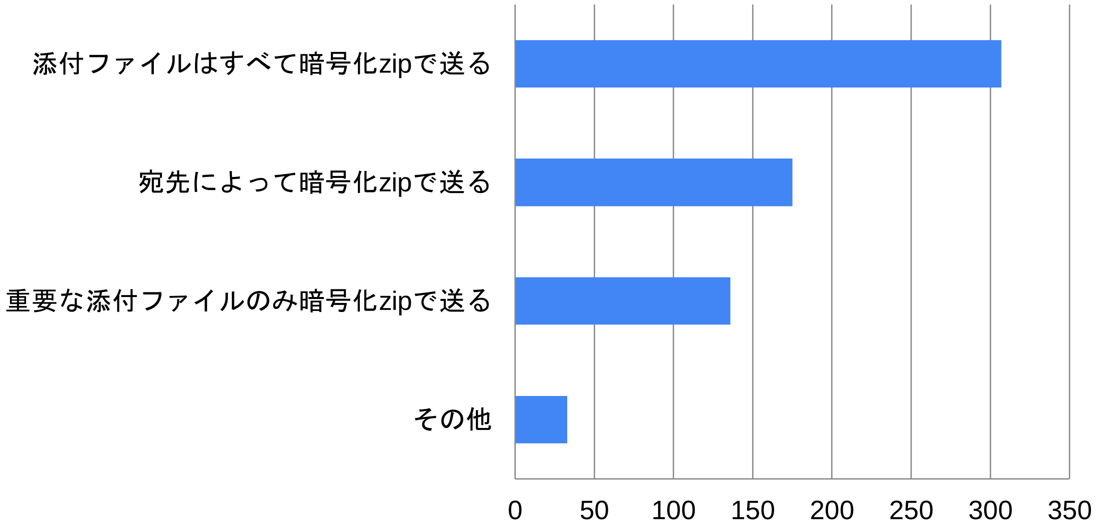
Q2-1. 2020年11月以前において、PPAPを含んだ暗号化zipを利用してメールを送っていましたか



N=775

自動で暗号化、パスワードは別のメール内に記載	373
手動で暗号化、パスワードは別のメール内に記載	221
いいえ、暗号化zipは使っていませんでした	124
手動で暗号化、パスワードはメール以外の別経路	37
自動で暗号化、パスワードはメール以外の別経路	8
手動で暗号化、パスワードは同じメール内に記載	7
自動で暗号化、パスワードは同じメール内に記載	5

Q2-2. 送信する添付ファイルのうち暗号化zipにする対象はどのようなものですか



N=651

添付ファイルはすべて暗号化zipで送る	307
宛先によって暗号化zipで送る	175
重要な添付ファイルのみ暗号化zipで送る	136
その他	33

Q2-3. 「重要な添付ファイルのみ暗号化zipで送る」を選択した場合、重要な添付ファイルとはどのようなものですか
(自由記述)

要約

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

などなど多数。詳細は8.自由記述欄回答を参照ください。

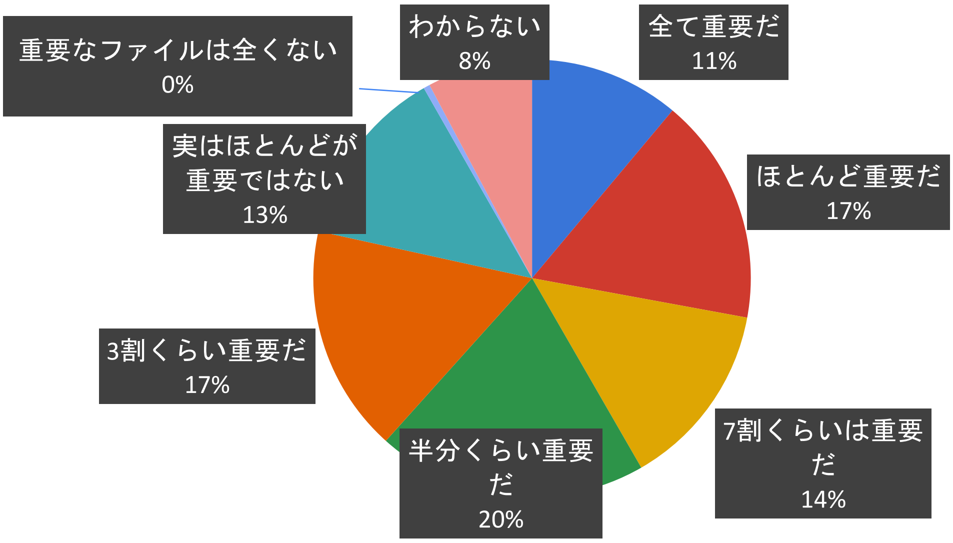
Q2-4. 「宛先によって暗号化zipで送る」を選択した場合、どのような宛先が対象ですか
(自由記述)

要約

社外・外部
暗号化ZIPで送ってきた相手先
暗号化ZIPを要求してくる相手先

などなど多数。詳細は8.自由記述欄回答を参照ください。

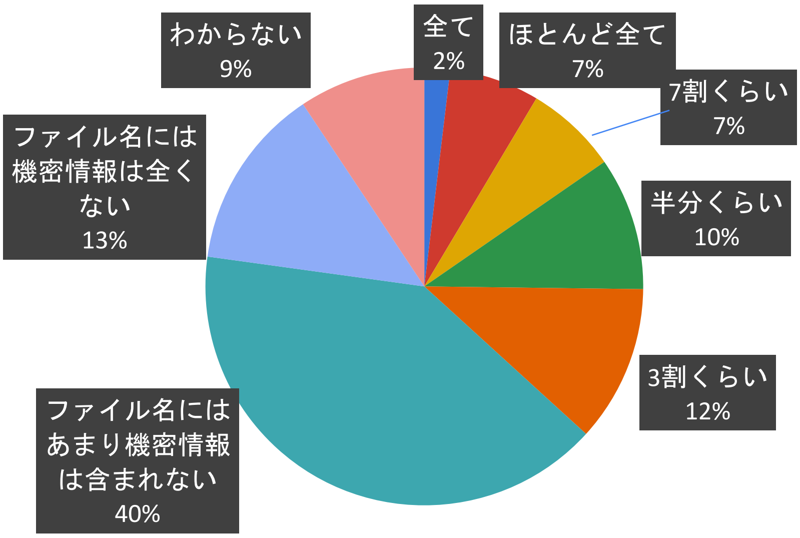
Q2-5. 暗号化zip処理をしているファイルのうち重要なファイルの割合はどのくらいですか



N=631

全て重要だ	70
ほとんど重要だ	106
7割くらいは重要だ	87
半分くらい重要だ	126
3割くらい重要だ	106
実はほとんどが重要ではない	84
重要なファイルは全くない	3
わからない	49

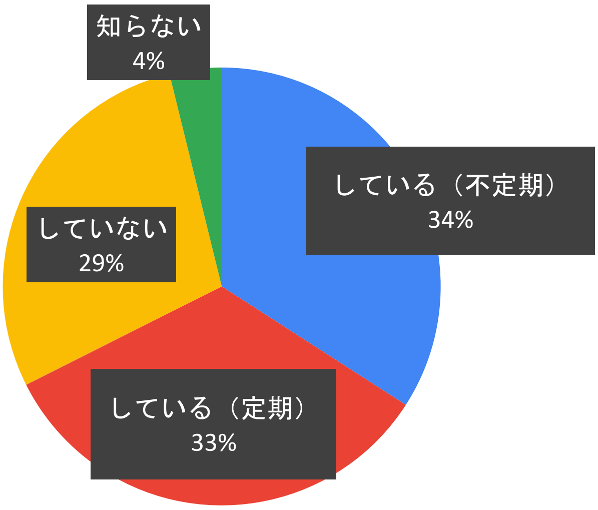
Q2-6. 暗号化zipの中に入れるファイルの「ファイル名」が機密情報になる割合はどのくらいですか



N=631

全て	12
ほとんど全て	42
7割くらい	43
半分くらい	62
3割くらい	73
ファイル名にはあまり機密情報は含まれない	255
ファイル名には機密情報は全くない	85
わからない	59

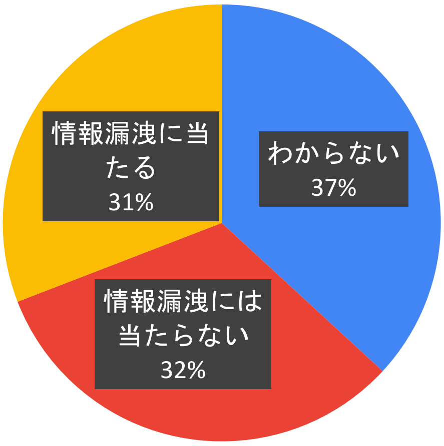
Q2-7 暗号化zipを利用されている場合、組織内でパスワード送信前の宛先、添付ファイルの見直しの徹底など、啓発・教育を実施していますか



N=651

している（不定期）	222
している（定期）	218
していない	186
知らない	25

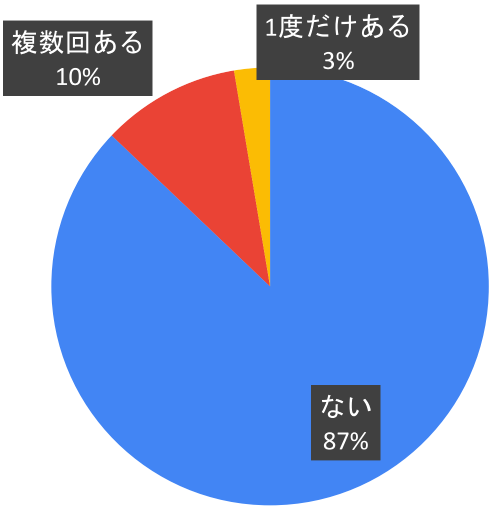
Q2-8. 暗号化zipファイルは相手に届いたが、誤送信に気が付いてパスワードを送信しなかった場合、組織内ではどのように扱われますか



N=651

わからない	240
情報漏洩には当たらない	210
情報漏洩に当たる	201

Q2-9 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

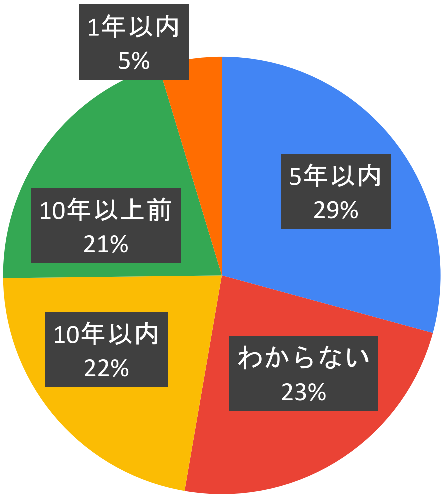


N=644

ない	561
複数回ある	66
1度だけある	17

3. 導入目的・経緯について

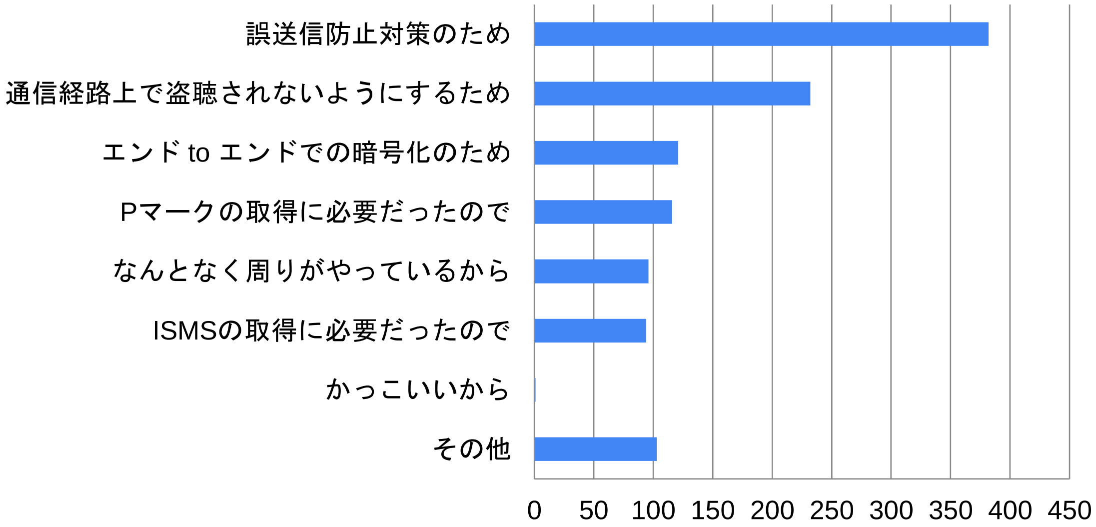
Q3-1. 暗号化zipでのファイル送信方式の導入時期について



N=643

5年以内	188
わからない	151
10年以内	142
10年以上前	132
1年以内	30

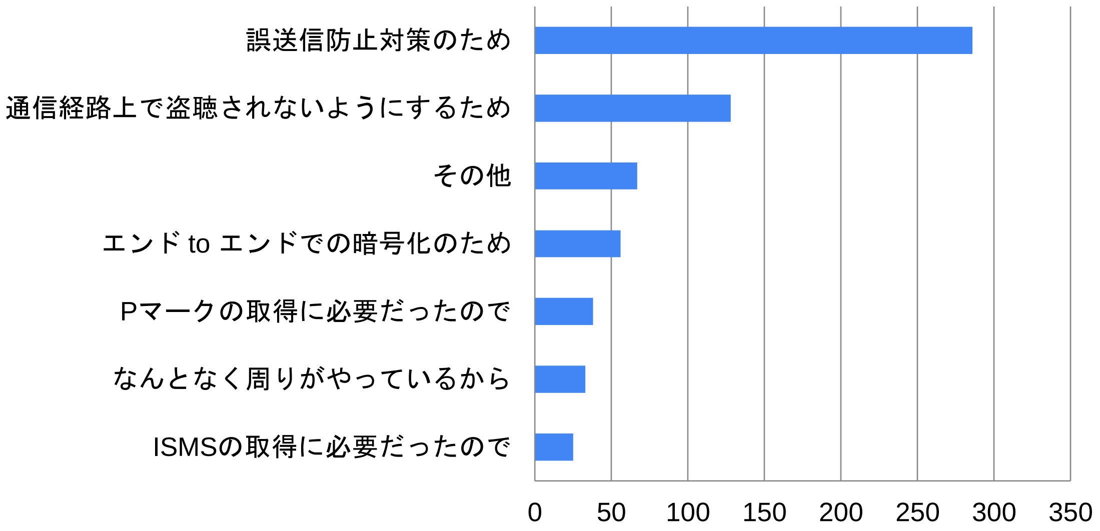
Q3-2. なぜ暗号化zipでのファイル送信を使用することになりましたか(複数回答)



N=633

誤送信防止対策のため	378
通信経路上で盗聴されないようにするため	230
エンド to エンドでの暗号化のため	120
Pマークの取得に必要だったので	114
なんとなく周りがやっているから	94
ISMSの取得に必要だったので	91
かっこいいから	0
その他	102

Q3-3. 上記のうちもっとも重要な要素はどれですか

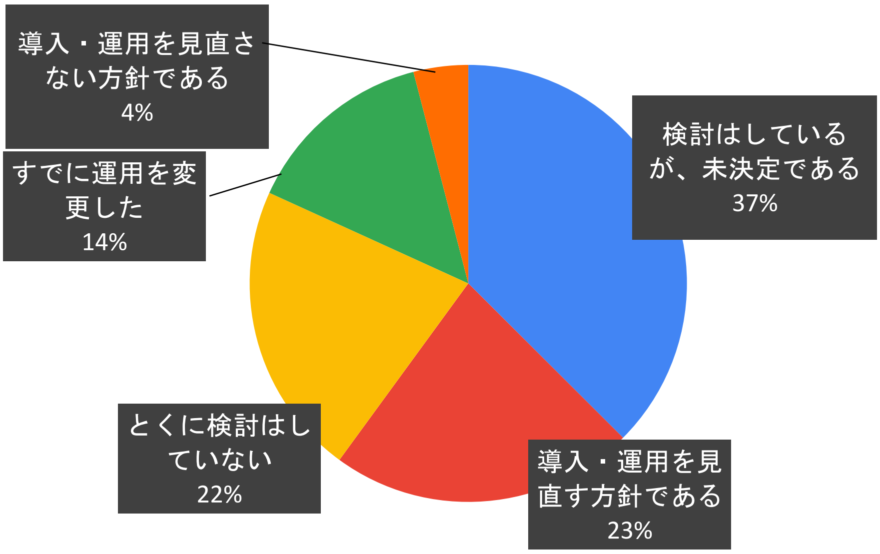


N=633

誤送信防止対策のため	286
通信経路上で盗聴されないようにするため	128
その他	67
エンド to エンドでの暗号化のため	56
Pマークの取得に必要だったので	38
なんとなく周りがやっているから	33
ISMSの取得に必要だったので	25

4. 今後の対応

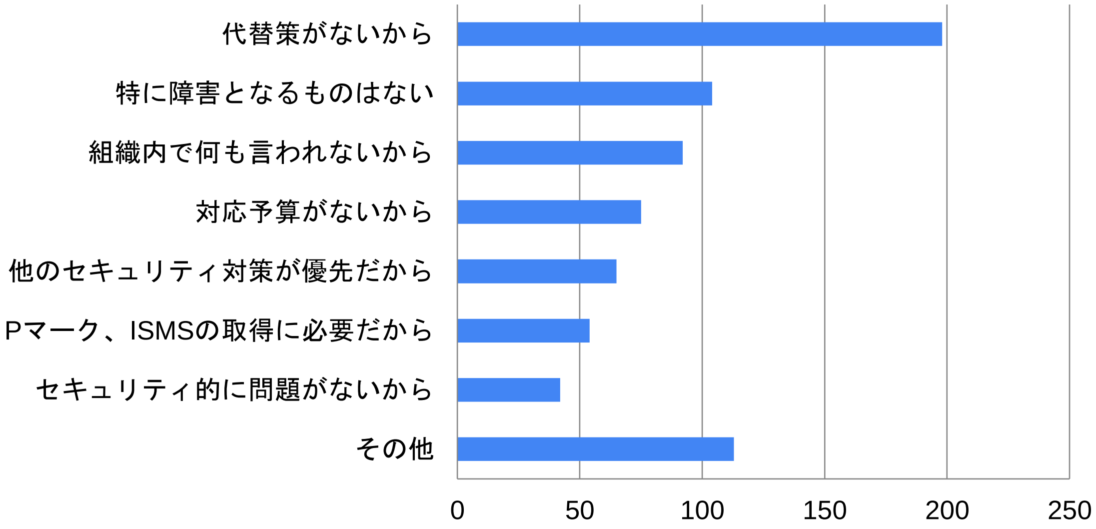
Q4-1. 平井デジタル担当相の会見や最近のニュースを見て、今後の暗号化zipによるファイル送信の導入・運用方針に変更はありますか。またはすでに変更しましたか。



N=643

検討はしているが、未決定である	241
導入・運用を見直す方針である	145
とくに検討はしていない	140
すでに運用を変更した	91
導入・運用を見直さない方針である	26

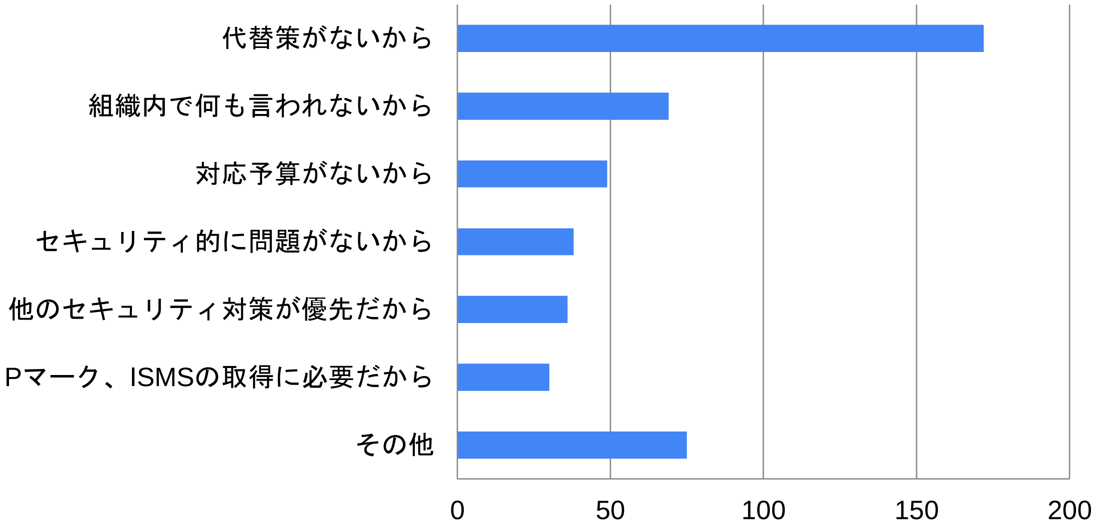
Q4-2. 見直しをされない、あるいは今後検討するうえで見直しの障害となりうる理由は何ですか。また、すでに運用を変更した方は何が障害になりましたか。(複数回答)



N=525

代替策がないから	198
特に障害となるものはない	104
組織内で何も言われないから	92
対応予算がないから	75
他のセキュリティ対策が優先だから	65
Pマーク、ISMSの取得に必要だから	54
セキュリティ的に問題がないから	42
その他	113

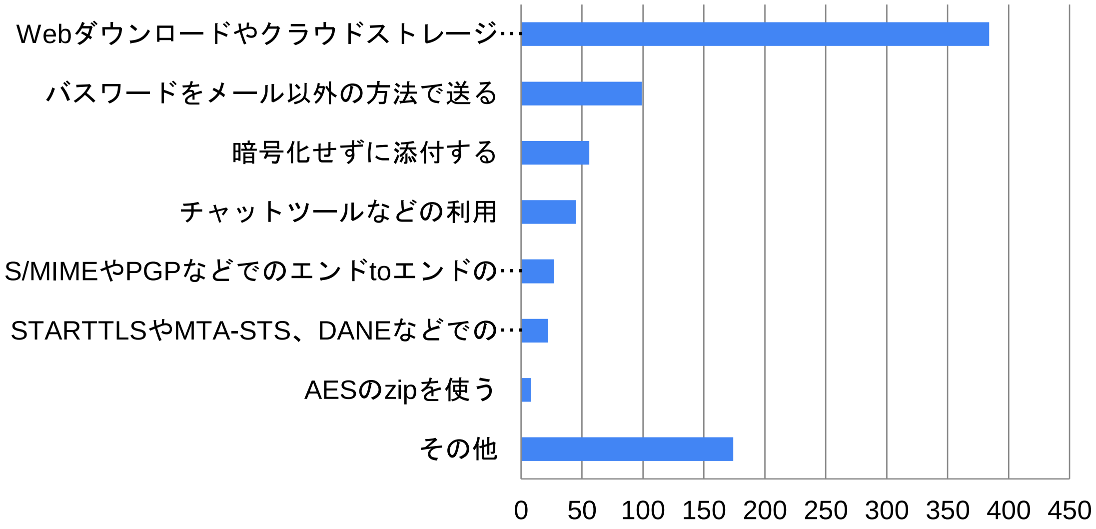
Q4-3. 上記のうち最も大きい、あるいは大きいと思われる理由は何ですか



N=469

代替策がないから	172
組織内で何も言われないから	69
対応予算がないから	49
セキュリティ的に問題がないから	38
他のセキュリティ対策が優先だから	36
Pマーク、ISMSの取得に必要だから	30
その他	75

Q4-4. 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

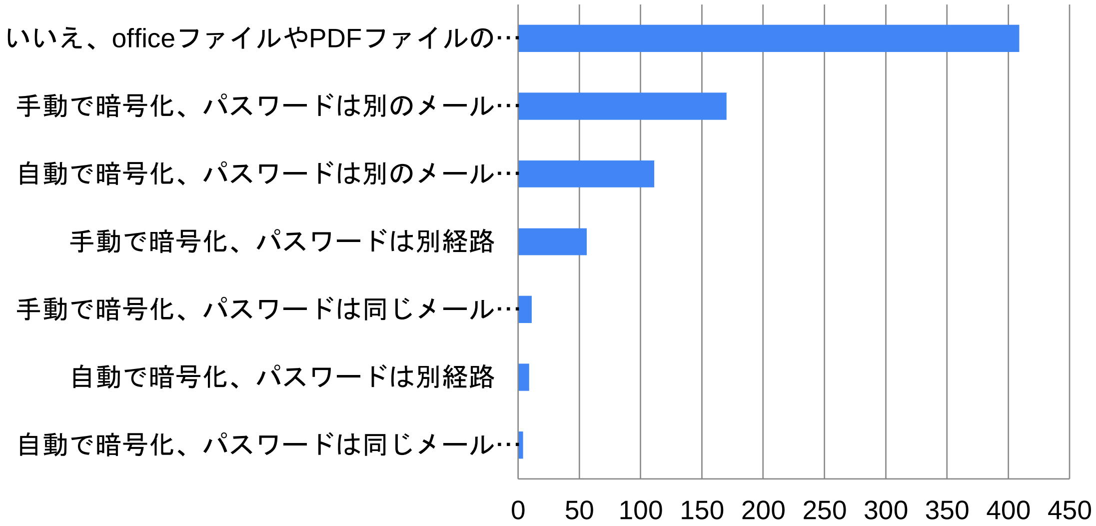


N=576

Webダウンロードやクラウドストレージの利用	384
パスワードをメール以外の方法で送る	99
暗号化せずに添付する	56
チャットツールなどの利用	45
S/MIMEやPGPなどでのエンドtoエンドの暗号化	27
STARTTLSやMTA-STS、DANEなどでの通信経路の暗号化	22
AESのzipを使う	8
その他	174

5.ZIP以外での暗号化方法について

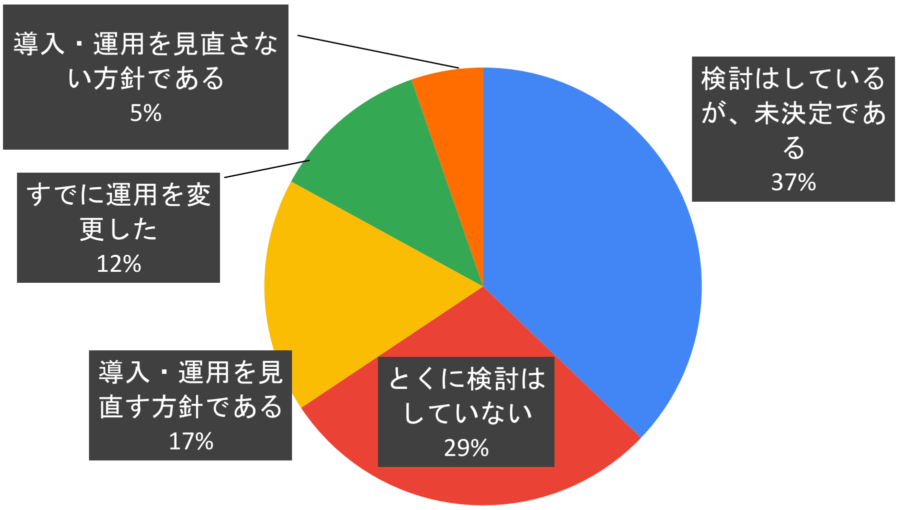
Q5-1. 2020年11月以前において、Officeファイルや PDFファイルの暗号化機能を利用してメールを送っていましたか



N=766

いいえ、officeファイルやPDFファイルの暗号化機能は使っていませんでした	405
手動で暗号化、パスワードは別のメール内に記載	170
自動で暗号化、パスワードは別のメール内に記載	111
手動で暗号化、パスワードは別経路	56
手動で暗号化、パスワードは同じメール内に記載	11
自動で暗号化、パスワードは別経路	9
自動で暗号化、パスワードは同じメール内に記載	4

Q5-2. 平井デジタル担当相の会見や最近のニュースを見て、今後のOfficeファイルやPDFファイルの暗号化によるファイル送信の導入・運用方針に変更はありますか。またはすでに変更しましたか。

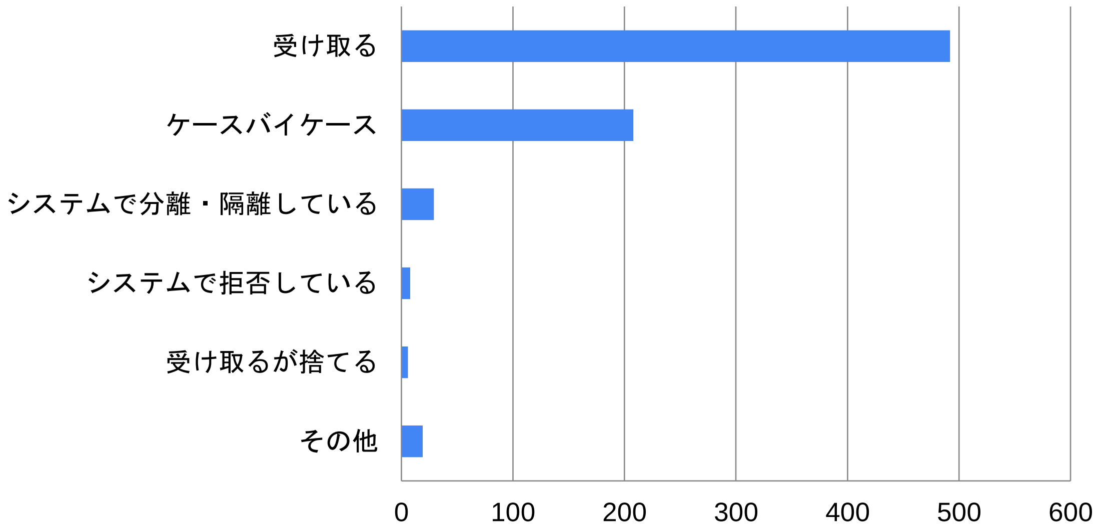


N=358

検討はしているが、未決定である	133
とくに検討はしていない	102
導入・運用を見直す方針である	62
すでに運用を変更した	42
導入・運用を見直さない方針である	19

6.暗号化ファイルを受信した時の対応について

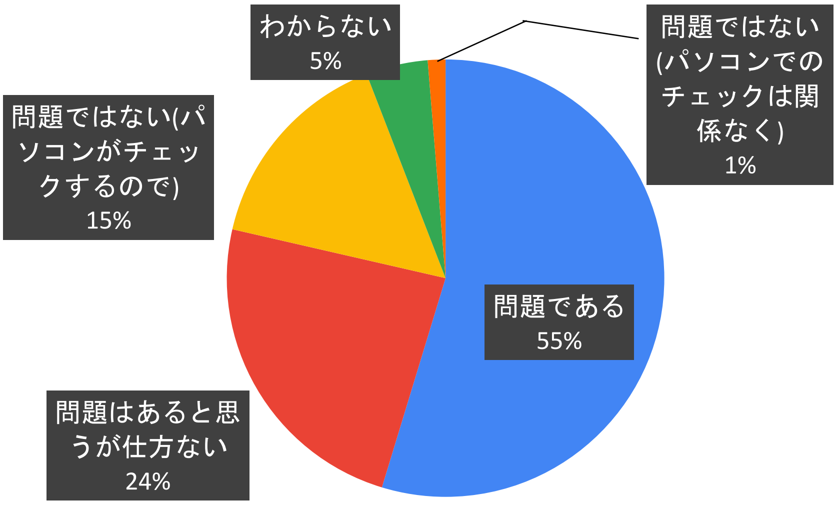
Q6-1. zipやoffice、PDFによる暗号化処理されたファイル(以下、暗号化ファイル)を受信したとき、どのように処理していますか



N=761

受け取る	492
ケースバイケース	208
システムで分離・隔離している	29
システムで拒否している	8
受け取るが捨てる	6
その他	19

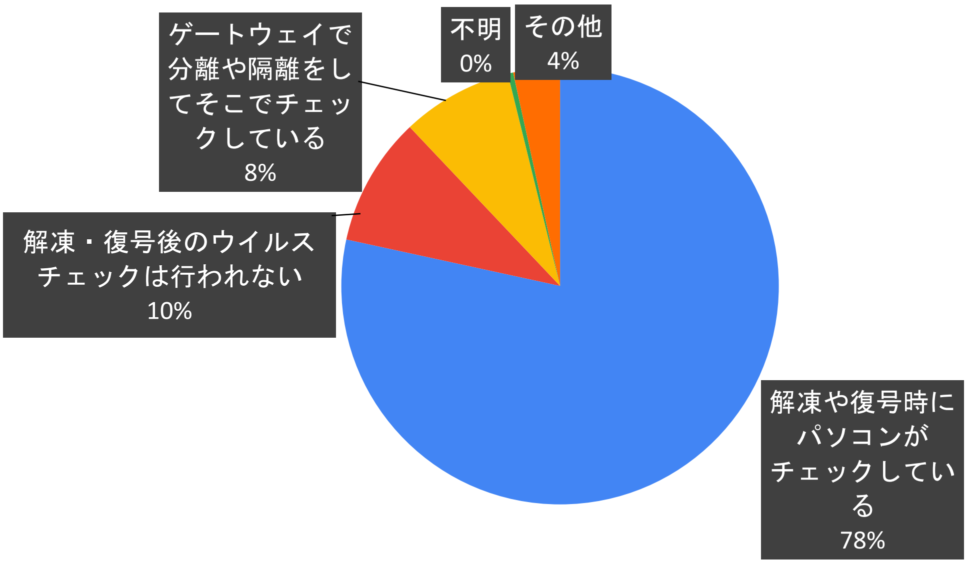
Q6-2. 暗号化ファイルは、受信時にゲートウェイでウイルスチェックを行えないことが問題といわれています。このことについてどう思いますか



N=766

問題である	419
問題はあると思うが仕方ない	183
問題ではない(パソコンがチェックするので)	119
わからない	35
問題ではない(パソコンでのチェックは関係なく)	10

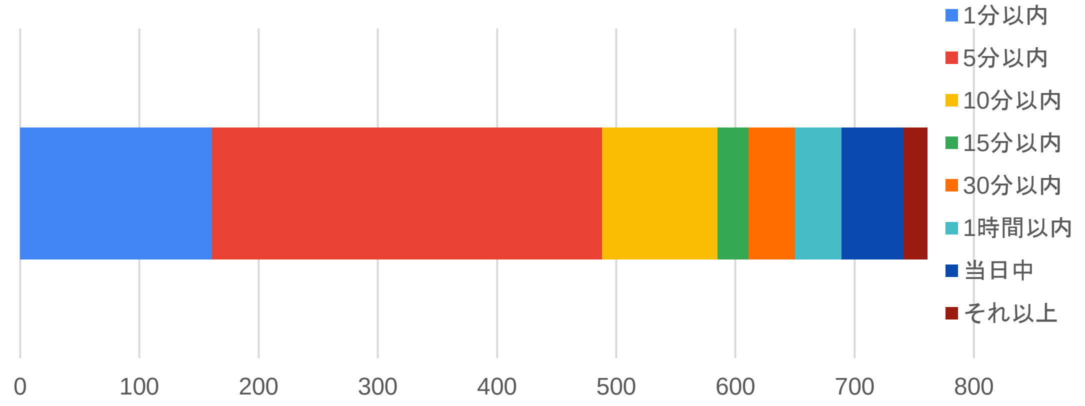
Q6-3. 暗号化ファイルの中身についてなにかウイルスチェックを行っていますか



N=755

解凍や復号時にパソコンがチェックしている	592
解凍・復号後のウイルスチェックは行われない	72
ゲートウェイで分離や隔離をしてそこでチェックしている	62
不明	3
その他	26

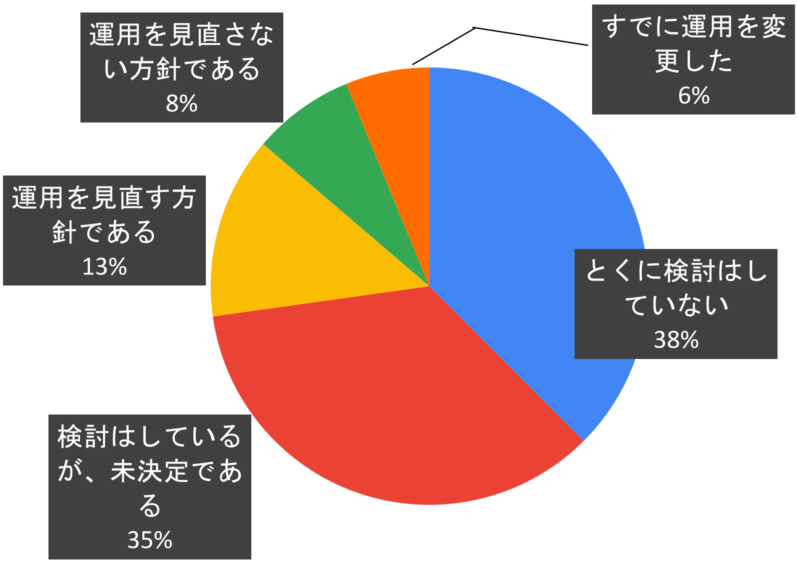
Q6-4. 暗号化ファイル付きメールを受け取った場合、パスワードが来るまでどの程度であれば待てますか



N=767

1分以内	161
5分以内	327
10分以内	97
15分以内	26
30分以内	39
1時間以内	39
当日中	52
それ以上	20

Q6-5. 今後の暗号化ファイル受信の運用方針に変更はありますか

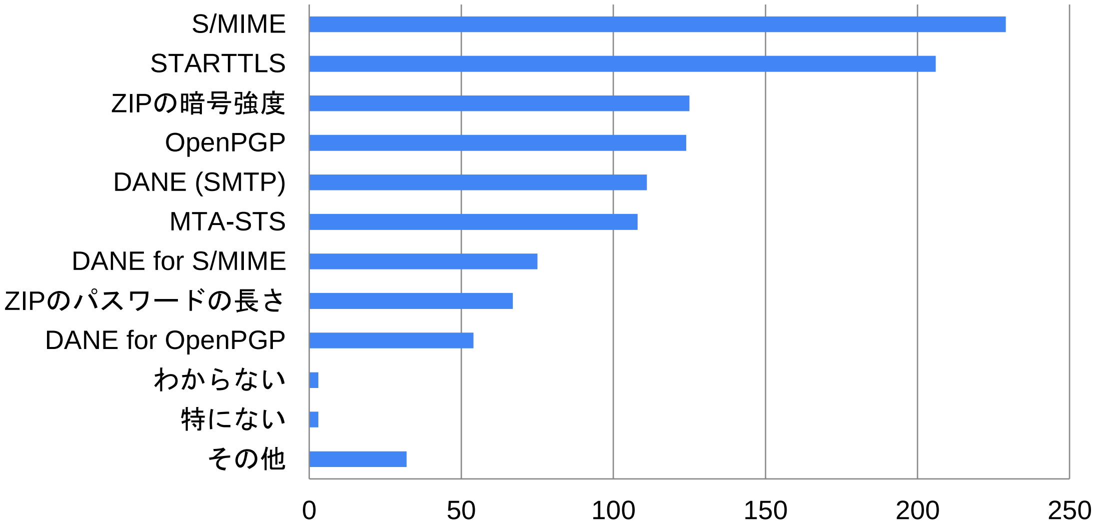


N=757

とくに検討はしていない	284
検討はしているが、未決定である	267
運用を見直す方針である	102
運用を見直さない方針である	57
すでに運用を変更した	47

7. その他

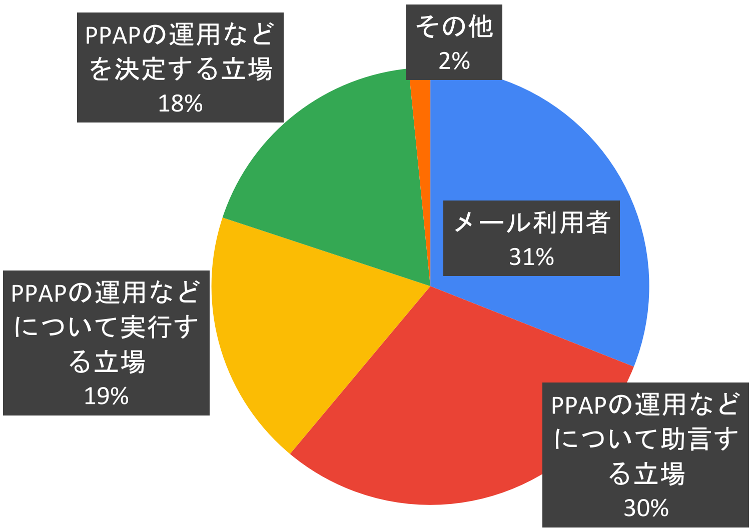
Q7-1. 添付ファイルやメールの暗号化方式として技術的に興味のあることがあれば教えてください



N=489

S/MIME	229
STARTTLS	206
ZIPの暗号強度	125
OpenPGP	124
DANE (SMTP)	111
MTA-STS	108
DANE for S/MIME	75
ZIPのパスワードの長さ	67
DANE for OpenPGP	54
わからない	3
特にない	3
その他	32

Q7-2. あなたについて教えてください



N=758

メール利用者	235
PPAPの運用などについて助言する立場	228
PPAPの運用などについて実行する立場	144
PPAPの運用などを決定する立場	139
その他	12

8. 自由記述欄回答

Q1-2. 最近知った方はどこで知りましたか。(最近知った方のみご回答ください)(その他の自由記述)

11月中、自社でPPAPを原則廃止し、Webダウンロードを標準とする事になったと報告を受けた際

IT関係のメルマガのリンクを辿ってウェブサイトの記事で

Netニュース

PPAPにリスクがあると社内会議で共有された

PPAP全面禁止のニュースにピコ太郎氏が驚いたニュース

Pマーク関連のニュース

Twitter

お客様の会話ではじめてきいた

クオリティア社のメールで初めて知りました

システム検討資料に記載があった。

セキュリティベンダのセミナー

セキュリティ系の何らかのニュースで

セキュリティ著名人のtwitter

セミナー

ネットニュースやダイレクトメールなど

ネット記事

何かのネットニュースで見たが詳細は覚えていない

会社でその話題が出たため

会社の同僚との会話

覚えていない

企業の広告や営業を受けて

記憶にないが、インターネットのセキュリティに関する記事だと思う

時系列を覚えてません。

社内で話題となった。

社内にて

社内のメール

上部団体からの利用廃止に伴う代替検討の案内

情報サイトのメールマガジンで

情報担当職員からの情報提供

他者からの相談

同僚からのネットニュース転送

日経コンピュータ

日経ネットワーク

部内からの注意喚起

平井デジタル改革担当大臣の会見やそのニュース

某企業によるPPAP全面禁止のニュース

Q1-5. 知っている場合、それはどのような問題ですか。(知っている方のみご回答ください)(自由記述)

(1) 暗号化されたファイルはゲートウェイでマルウェアチェックできないため感染リスクが高まる (2) パスワードが同一経路で配送されるため、盗聴対策にはならない (3) パスワードを自動で同じ宛先に送るため、誤送信対策にはならない

(メール傍受可能な前提で)平文であるので、意味を成さないこと ウイルスチェックなど の事前防御が利かないこと 等。

1. パスワード付きZIPファイルとパスワードが別メールとはいえ、同一経路でメール自信が暗号化されない状態で送信されているため、第三者に両メールが盗聴されていた場合に簡単に復号化できてしまう危険性があること。2. ZIPファイルをパスワードで保護した としても、パスワードを解除するためのツール等がインターネット上に存在し、簡単に復号化できてしまう危険性があること。

1. 同一経路(メールで添付ファイルを暗号化して、パスワードを別のメールで送っているが、どちらも盗聴されていれば、無意味) 2. 検出困難(添付ファイルを暗号化していると、ウィルスチェックをすけ抜ける可能性有り)

1.NW上のセキュリティ製品での検査を回避される。2.PW伝達手段が同じメールである

1.セキュリティのためパスワード付きzipを送る,ということになっているからパスワードが届けば何の疑問も抱かずに開封してしまう。ここにマルウエア入っていたらどうするんだい,という問題。2.仮に,真に重要なメールだったとして,同じ経路の別メールでパスワードを送っていたのでは元メールが盗み取られていたら当然パスワードも盗まれる。3. パスワードを待つ間と開錠の手間が無駄。送信側も同様。4.セキュリティ確保のため,と言って無能な上司や情シがPPAPを強要するパワハラ。

1.パスワードがパスワード付きファイルと同じ通信経路でやりとりされるため、その通信経路を不正に利用され、両方を不正に入手された場合に、ファイルの暗号化解除が可能になってしまうこと。2.パスワード付きzipファイル内をマルウェア対策ソフトがチェックできないため、マルウェアの侵入経路になりかねないこと 3.パスワード付きzipのパスワード解析自体、今では天文学的時間を要しないこと

1.暗号化したファイルとパスワードを同一経路で送信　2.受信側のマルウェアチェックをすり抜ける

①Zip 暗号化キーとファイルが同じ経路で送られて、且つ、保存先も同じ。②暗号化されPWロックがかかっているので、UTM 等をすり抜ける。③暗号化ファイルを解凍する際にPWを入れる前にファイル名や階層構造が判ってしまう。

①zipファイルがウィルスチェックをすり抜ける②同一宛先にパスワードも送るので機密 化されない。

①ZIP暗号化したファイルとそのパスワードを同じ経路で送るのは、セキュリティ上意味 がない。②ZIP暗号化してしまうと、ウィルスチェックができないのでEmotetの様なウィ ルスが入っていてもチェックできない

①メールを別けても、同じ経路で送付されているので、セキュリティ面からは意味がない。②添付ファイルに保護がかかっていることで、添付ファイルのウィルスチェックが働 かない。不用意にファイルを開けただけで感染するリスクがある。

1通目のメールを取得できる第三者なら、2通目(パスワード記載あり)も取得可能なので、情報漏えいの防止にはならない。

1通目の暗号化メールを盗むことができるのであれば、2通目のパスワードも盗むことが可能

2通になろうが同じ経路をたどるので意味はないかと

2通を同じ人から同じ宛先に送っている

AntiVirusフィルターすり抜け

Emotetでの利用、アンチウイルスソフトでの検知不可

Emotetに対応できない

EMOTETの送信に利用されやすい。

Emotet云々もそうだが、そもそも暗号化ZIPのパスワード解析ソフトが出回っているなか 形骸化した「なんちゃって情報セキュリティ」をやっていると思っている企業やユーザーが多いことが一番の問題。根本から「やりかた/考え方」を変えていかなければ。

Emotet等マルウェアが検知ができない点 同じルートでPWを送付している場合、盗聴リス クに対応ができない点

GateWayでのウィルススキャンができない。誤送信対策になっていない。

GWでのMalware検査ができないなど

mail gateway での virus scan ができない

MTA上でウイルスチェック等ができないことによるリスクがある

PASSが掛かっている場合、SMTPgatewayでVirusチェックができないまま、Clientまで届いてしまう。Client端末でリアルタイムVirusScanを実施していない場合、感染するりすく がある。

pass付zip化することで中身のウイルスチェックが行われない、経路が同じなので誤送信 したら意味がない、等

PPAPが当たり前になっていると、パスワード付きファイルを疑うことなく開いてしまい、マルウエア被害にあいやすい

PPAPで暗号化されたファイルがウィルススキャンでチェックできない

PPAPで送信してもファイルとパスワード両方盗聴されるとデータが漏洩する。

PPAPについてはメール誤送信を再確認するために暗号送付時あて先を再確認するものと理解している。暗号情報を機械的に返信送付すると情報が漏洩する。

PPAPによりZIP化されたファイルが感染していても、検出ができないため。

PPAPをどのように実現(手動か自動か)しているかでも問題の程度は違うかとは思いますが、セキュリティ製品でZIP暗号化されたものを紐解けない、というのが一番の問題だと感 じています。誤送信対策の一つとしてはアリだと思います。

PWを自動で送付されること→誤送信防止の役に立たない

SMTPで送信されている情報を傍受された際同じ経路にZIP・パスワードが存在するため、 解除されてしまう。また、暗号化ZIPは受信者側で事前ウイルスチェックができない為、なりすましが発生した場合わからず感染してしまうことがある。

webメールサービスにて中身をスキャンできないから

zipそのものが、比較的容易に破られるものである。

ZIPで暗号化されるとウィルスチェックできない。メールでパスワードを送るのも意味が ない。

zipとパスワードが同一経路で配送させる可能性が高いこと

zipのパスワードは解析可能なので意味が薄いこと、マルウェアが混入していてもメール ゲートウェイで検知出来ないこと、パスワードを添付ファイルと同じ経路で送るために誤送信対策としての効果性は薄いこと及びメール経路上での窃取は防げないこと、送受信者双方に手間をかけること

zipの暗号強度で強度の低いZipCryptoを使用し、安易なパスワードを設定した場合、パスワードが攻撃者の手元になくても専用のツールを使うことで短い時間でパスワードを突破されてしまう可能性がある。 パスワード付きzipファイルとパスワードが同じ通信経路で送られている。 パスワード付きzipファイルを用いマルウェア対策製品を回避するマルウェアが存在する。

ZIPの場合、パスワードなしにファイル名が見られること。マルウェア検知の仕組みをす る抜けること。

ZIPの脆弱性

ZIPパスワード総当たり解凍　同じ方法での連絡の為、両方傍受されれば意味がない

ZIPファイルがウイルススキャンできない。パスワード通知が同じ通信経路だと意味がな い。

zipファイルが添付されたメールと併せてパスワードが記載されたメールも盗み見られる と、セキュリティ敵に意味がなくzipファイルの内容を盗み見られてしまうため。

ZIPファイルが添付されているメール本文とパスワード通知が同一経路で送信されるので 、意味がない。

zipファイルでは、ウイルスチェックが出来ない。

zipファイルとPWの送信経路が同一

ZIPファイルとパスワードを同じ経路で送っているため、その経路で窃取されていたらZIPファイルとパスワードの両方とも窃取されるため意味がない。 ZIPファイルが暗号化されているとウイルス対策ソフトなどがスキャンできない。

zipファイルとパスワードを同一手段で別送しても、zip付きメールを不正に入手できる攻撃者は容易にパスワードメールも入手出来てしまう。

ZIPファイルと複合用パスワードが同じ経路で流通する場合、盗聴者は両方を手に入れる ことができること。

ZIPファイルと別送のパスワードが同一経路で送られることによる盗聴リスク。 添付ファイルが暗号化されているため、セキュリティ対策製品などで検査できず、マルウェアが検知できない。

Zipファイルにウィルス添付されていても対策ソフトで削除できない

ZIPファイルのパスワードは総当たり方式で解除可能。また、パスワードは通常元のメー ルと同じ受信者が受け取るので、宛先を間違えたり悪意のある者が受信すると危険。

ZIPファイルはウイルスチェックが出来ない場合があるため

ZIPファイルはマルウェア検索できない、メールボックスをクラックされたら意味がない 、PWを自動送信する仕組みもあり、宛先を間違えていれば意味がない

ZIPファイルを入手できるならば、後から送付されるパスワードも入手可能であること。 また、ZIPファイルだけ入手できたとした場合、ZIPの暗号が総当たりなどの方法で解読可能であること。

ZIPファイル内の各ファイルのセキュリティスキャンが行なえない。

zipを添付したメールとパスワードを記載したメールの両方が盗聴された場合、対策とし て意味をなさない

ZIP暗号の脆弱性、メールの盗聴

zip暗号化がそもそも脆弱、誤送信対策としても2通目が自動化されていると無意味、盗聴に対して脆弱

ZIP暗号化されたZipt添付ファイルがウイルスチェックツールで検知できない

ZIP暗号化された添付ファイル付きメールとその解凍パスワード記載のメールが同じ経路 上でやり取りされている

Zip暗号化された添付ファイル付きメールとパスワードを同一経路で送付するため、メー ルを盗聴された場合に、パスワードも取得できてしまい簡単にファイルが閲覧されてしまうため、情報漏えいのリスクがある。

ZIP暗号化されている場合、スキャンできないウイルスがある ・パスワードを同じ宛先に別送した場合、暗号化の意味がない

zip暗号化そのものの問題もあるがそれよりも同一宛先にパスワードが自動で送られ、抑 止されない点が一番の課題。

zip暗号化のパスワード自体が脆弱で誰でも簡単に解除できてしまう問題。

ZIP暗号化の強度、同通信経路でのパスワード通知(誤送信の場合でも開封可能)、ZIP形式が検知・ブロックをスルーするなど

ZIP暗号化の脆弱性と 暗号化ファイルとパスワードが同一経路で送信されること。

ZIP暗号化はスパムフィルターのスパム判定を通過してしまう ・同じ宛先にパスワードを別送してもセキュリティリスク対策にはならない

ZIP暗号化ファイルと、解読するパスワードが同じ経路で流れるので両方盗聴される可能 性がある。

ZIP暗号化ファイルとパスワードの送付先メールアドレスが同じなので意味がない

Zip暗号化マルウェアスキャン問題とパスワード同経路通知問題

ZIP暗号化強度の問題、パスワードが同じ通信経路で送っていることの問題、それに加え て送信者の工数がかさむ問題。ZIPを用いたマルウェアはセキュリティを突破する問題。

ZIP化されたファイルがウイルス検知されない

zip化時の暗号強度が弱い(強くすると運用に耐えない)、パスワードを別のメールで送る ことにほぼ意味がない、zip暗号化が広く使われていることでメールサーバーのウイルス チェックが働かず間接的にウイルスを蔓延させるきっかけになる

ZIP形式添付ファイルと解凍パスワードを別送しても、経路としては同じである点。メー ルサーバのウィルスチェックのすり抜け

zip自体のセキュアと、同一ルートでのパスワード配送と言う意味の無さ。

ZIP内にはセキュリティ製品の効果が及ばない

あまり意味がない

あまり意味がない。

アンチウィルスが機能しない
アンチウィルスが検知できない。暗号化本体とパスワードが同じ送信者・宛先で流れる。
アンチウイルスすり抜け ZIP復号可
アンチウィルスソフトがファイルの中身を調査できない
アンチウィルスソフトが働かなくなるので、メール内にウィルスがいた場合検知できない
アンチスパムシステムでスキャンできない
ウイルスが含まれる場合に、ウイルス対策ソフトが機能しない
ウィルスが含まれる添付ファイルによる攻撃を受けてしまう。
ウィルスが紛れ込む
ウイルススキャンがきかなくなる。同じ経路を使ってパスワードが送られるなど。
ウイルススキャンができない
ウイルススキャンが有効に機能しない
ウィルススキャンを通り抜け、マルウエア(ウイルス)攻撃を受けるリスクがある ・別メ ールであれ、zipファイルと解凍パスワードが同じ通信経路で送付されると、解凍パスワ ードを解読されてしまうリスクがある ・zipの暗号強度が低い場合、パスワードを突破されるリスクがある
ウイルスチェックができないケースあり
ウィルスチェックができないと聞きました。
ウィルスチェックができなくなってしまう。
ウィルスチェックが行えない。
ウィルスチェックできない
ウィルスチェック漏れと情報漏えいの危険性
ウイルスの検知ができない
ウィルス検査が行えない・パスワードとファイルが同経路で送られるためその経路で情報が盗まれた場合に意味を為さない
ウイルス検知ができない
ウイルス検知が不十分
ウイルス攻撃に悪用される
ウィルス対策製品などを通過する
エモテットの流行でPPAPで送られる暗号化ファイルが、クラウドメールサービスのセキュリティーチェックやネットワーク上のウイルスチェックを通らず、マルウェアに感染すると知らずに、なりすましメールの添付ファイルを開いてしまう可能性がある
エンドポイントでのチェックしか行えないため
クラウドメールサービスのセキュリティーチェックやネットワーク上のウイルスチェックを通らないため、マルウェアに感染していると気づかず、なりすましメールの添付ファイルを開いてしまう
ゲートウェイにおいてマルウェアの検査などをすり抜けるおそれがある
ゲートウェイ上で検出できない、ZIPCryptの強度が低い、パスワードも盗まれ易い等
ご送信による情報漏洩のリスクがある。セキュリティ製品のチェックをすり抜ける。
サーバー上で中身のセキュリティチェックができない
サイバー攻撃として、ウイルスを混入し暗号化された添付ファイルがついたメールを、除外することが難しい
スキャンされない、パスワードと一緒に盗聴される、ファイル名が見れる
セキュリティソフトがチェックできない
セキュリティチェックをすりぬけ、データ、通知経路が一緒、安易なパスワードの共有
セキュリティに何の効果もないこと、暗号化されるのでウイルススキャンで対処ができないこと
セキュリティ効果が見込めない ・利便性が低い
セキュリティ上あまり意味がないこと、特に自動パスワード送信
セキュリティ製品でのスキャンができないため、攻撃に使われるようになっている。 パ スワードを同じ経路で送信すると盗聴されている場合に意味がない(パスワードも知られ てしまう)
セキュリティ製品で暗号化zipファイルを検疫できない
セキュリティ製品をスルーしてしまう
セキュリティ対策
セキュリティ対策としてはあまり意味がない
セキュリティ担保に成っていない
セキュリティ的に意味がないこと
セキュリティ面で安全とは言い難いこと。送受信ともに(特に受信側に)無用の手間がかかること。
セキュリティ問題の解決にはならない
セッションが盗聴されている場合、パスワードを設定しても直後にパスワードを送るので意味がない
そもそもアドレスが間違っていたら、間違った人にパスワードを教えてしまう。
そもそもの利用目的が間違っていて、メールの盗聴対策としては全く役に立っていないこと。

そもそもメールは盗聴される可能性があり、仮に盗聴された場合、ファイルとパスワードを別に送っても、同じ経路を経由するので、セキュリティ対策として微妙だと思います。また、最近、パスワード付 zip ファイルが、セキュリティ機能をバイパスする目的等もあり、Emotet の攻撃にも利用されています。そのため、パスワード付きzipファイルは 受信しないことが推奨されているという認識です。 上記を踏まえると、パスワード付 zip ファイルを使用することは、自社側のセキュリティ対策としても微妙かつ受信側のセキュリティ対策強化の妨げにもなってきているという認識です。（もともと受信側に効率的な面で負担を強いていましたが）

そもそも対して意味がない、電子メールゲートウェイでの対策をすり抜ける、ウイルスの感染手口に応用されていて混同しやすくなる、

たいていZIPファイルとパスワードが同じ経路で送信されており、パスワードとともに窃取される可能性 ZIPファイルを利用した攻撃が増加している点

タイミングを変えるとはいえ同じメールアカウント向けに解凍パスワードを送ること、およびパスワード付きzip圧縮する事によりgメールが提供しているウィルス検知システムに掛からなくなる可能性が発生してしまう事

のぞき見されたらPWも盗まれて意味がない

パスワードがメールで送付される

パスワードがメールと同一ルートで配送される。パスワード付zipをウイルス検査できない。

パスワードが添付ファイルと同メール(もしくは後メール)に記載されているため、セキュリティレベルが低い

パスワードが盗み見られる可能性がある。

パスワードが同じメールアドレスに送られること

パスワードが同経路で通達されるため、秘匿の意味がない。暗号化されているがゆえに 、ウイルスチェックやマルウェアなどのフィルターができない。

パスワードが同時期に同じアドレスに同送されると意味がない。

パスワードが付いていない添付ファイルのついたメールなので、宛先を間違えて送信した時点で、意図しない者に添付ファイルの内容が見れてしまう。

パスワードが漏れて、危険

パスワードと、パスワード付きzipファイルを同じ通信経路で送信している

パスワードの運用不備によるセキュリティレベルの低下

パスワードの送付先が同じアドレス、アンチウイルスでチェックできない。

パスワードは簡単に解読可能であること。同じ経路でZIPファイル添付のメールとパスワードを記述のメールを送ることから、2つのメールを入手可能であるので、ZIPファイルにしたファイルの秘密を守れない。

パスワードは総当たり攻撃で解読できる。同じメールでパスワードを送ると宛先が間違っていた場合、パスワードも漏えいする可能性が高いなど・・・

パスワードメールが自動送信の場合、同一の宛先に送信するため送信を分けるメリットがない。

パスワードメールも自動されているため意味がない。盗み見されていたら一緒等

パスワードメールも同じ通信経路を通ることになり、簡単に奪取されてしまう点

パスワードもメールで送ることから、盗聴の対策にはならない。添付ファイル対策のためのセキュリティソリューションが機能しない。

パスワードもメールで送ると盗聴に対してはほぼ意味がない

パスワードも一緒に送る

パスワードも同じ通信回線から送られるために傍受される可能性があるため

パスワードも平文で送付される、サンドボックスでチェックできない、など

パスワードをメールで送るのはセキュアでない。

パスワードをメールで送信すると、パスワードの解読、ファイル解凍され、情報漏洩に繋がるため。

パスワードを同じアドレスに送付するため、暗号化の意味をなさない

パスワードを同じメールに書く、別便のメールにしても同じ経路で老親される。

パスワードを同じ経路で送ること。ZIP化されているので受信時にチェックが効かないこと

パスワードを同じ手段で送付することから、誤送信による情報漏えいの危険性を回避できない

パスワードを同一経路で送る。暗号化するとウイルススキャン等で検知できない。

パスワードを同一経路で送付しており、盗聴されていれば意味がない事

パスワードを付加したZipファイルを送り、別メールで相手にパスワードを送付する際、Zipファイルを送った人のメールを流用するなどするため

パスワードを付与しても解析できる ・同一伝送経路であればパスワードも取得できる ※時間を置いたパスワード通知は意味が無い ・パスワードが付与されている場合、ウィルスチェックが出来ない

パスワードを平文(メール)で通知していると意味がない

パスワードを平文で送信する、という操作の時点で安全性上は何も意味がない。

パスワードを別メールで送ることに何の意味があるのかと思っていた。

パスワードを別メールで送信しているが、そもそも宛先を誤っていた場合には漏洩してしまう。

パスワード暗号化は経路での盗聴防止が目的とされているが、本人にパスワードも送られる為両方を入手することが可能。また、UTM等のゲートウェイセキュリティ対策製品では、通常はスキャンされないため、ウイルス感染リスクが高まることになる。

パスワード送付(別メール)する際のメール経路が同一であること

パスワード通知メールも誤送信すれば意味がないこと

パスワード付ZIPではウイルスの流入が容易である。

パスワード付zipファイルをメールに添付し、パスワードを同じメールで通知する問題

パスワード付きzipは、ウイルスの有無を判別できず、ウイルスソフトを通過してしまう ため、危険である

パスワード付きZIPはウィルス検査できない、パスワードをメールで別送しても経路が同 じである点

パスワード付きZIPファイルがマルウェア対策製品によるスキャンをすり抜けてしまい、 かえって危険な場合がある

パスワード付きzipファイルが攻撃者によって窃取された場合、同じ通信経路で送信して いるパスワードも攻撃者に同様に窃取されてしまう。Emotetなど、パスワード付きzipを使ったマルウェアもあり、パスワード付きzipの場合、マルウェア対策製品はzipファイルを解凍することができずパスワード付きzipファイルはウィルスチェックやスキャンを回 避してしまう可能性があります。

パスワード付きZIPファイルとパスワードを知らせるメールを同一経路で送ること。

パスワード付きZIPファイルとパスワードを同経路で送信すること

パスワード付きZipファイルにマルウェア「Emotet(エモテット)」が仕込まれた攻撃メー ル

パスワード付きzipファイルのため、マルウェア対策を回避するマルウェアの存在

パスワード付きzipファイルは、ウィルスチェックなどの検疫ができない

パスワード付きZIPファイルはウィルスが入っていても検知できない可能性がある

パスワード付きzipファイルはメールゲートウェイでのチェックができないため

パスワード付きzipを利用したランサムウェア、標的型攻撃が流行した際に格好の的とな る

パスワード付きzip自体がセキュリティ対策として脆弱である。など

パスワード付きzip添付ファイルとパスワードとが、同じ経路で送られているので、両方 とも不正に入手される危険性がある

パスワード付きzip添付メールと同じ経路でパスワードを送信することによって、第三者 にデータが流出するリスクがある

パスワード付きのZipファイルに対して、セキュリティ対策ソフトが働かない場合がある

パスワード付きのファイルがウイルスチェックできない

パスワード付きファイルがメール受信時のマルウエアCHKが出来ない

パスワード付添付ファイルだと、GW部分でウイルスやマルウェアのチェックがでいない。

パスワード付与でファイルが暗号化されている場合、メールセキュリティ製品などで検査ができず、マルウェアが通過する可能性がある(Emotet,IcedID等)。また、PPAPの運用上、同経路でパスワードが送信されるため「メールの盗聴によるファイルの中身の漏洩を防止」という目的を果たせていない(本問題についてはPPAPという用語を知る以前から既知 。新入社員のときから何がやりたいのかよくわからない運用だと思っていた=ほとんど意 味がない、目的を果たせていないことは認知)。誤送信防止の効果も一応あるが、自動zip化など運用によっては対策にならない環境も多いと思うため、個人的にはおまけ的な位 置づけ(一般的にPPAPの利点として言われているが、セキュリティ観点からあまりそうは 思わない、達成されていない環境が多いと思う)。

パスワード別送運用におけるパスワードメールの盗聴リスク、パスワード付きZIPファイ ルが受信時にスパムチェックできない点

パスワード保護が気やすめ程度の効果しかない

パスワード保護されているため、境界型ウイルスチェックが実施できないこと

パスワード漏洩

ハッキングされていたら、何の意味もない。

ファイアウォールを通過する際に、Zippファイルに対してウイルスチェックを行うことができない。

ファイルが圧縮されていることでウイルスチェックがすり抜けられること。時間差とは言え同一メールにパスワードが送られることは盗聴者にとってはさほど問題が無い上、総当たりで容易に破られる強度のパスワードである事。　あとは受信者にとって単純にめんどくささ=生産性効率が落ちる事。

ファイルが暗号化(あるいはzip圧縮)されていると、当該ファイルがウィルス等に汚染さ れていても、各種セキュリティツールによる検知が正しく実施できないおそれがある

ファイルが暗号化されるので、パソコンの手前でウイルスチェック等ができない。UTMも 無効になってしまう。

ファイルとkeyが同一経路を用いる脆弱性、ファイル暗号化方式そのものの脆弱性

ファイルとパスの送信経路が同一。ペイロードのマルウェアチェックができない、。

ファイルとパスワードが同じ経路で送信されているため、実質意味がない

ファイルとパスワードが同じ経路で流れること。ファイルが暗号化されていることでゲートウェイでのマルウェア対策ができないこと。

ファイルとパスワードを同じ経路で送信することになるので、セキュリティの対策効果が手間の割には薄い。

ファイルにウィルスが含まれていても感知できない

ファイルへのパス総当たりや、ファイルとパスワードの同一ルート使用などにより盗聴されるリスクが高い。

ファイルを暗号化してメール添付するとゲートウェイでのウイルスチェックができないなど…。

ファイルを添付したメールの宛先を間違えた場合に別途送信するパスワードを記載したメールの宛先も同様に間違えることが想定され、宛先を間違えた場合の対策としての効果が限定的である

ファイルを渡す形式とパスワードを送る形式が同じため、情漏洩リスクをカバーできない。また、ZIPファイルのためウイルス検知ができない。

ファイル送付後直接同じ手段であるメール送付でPWを告知してしまっているから。

ファイル付きメールとパスワードが同じ経路で送られる

フィルタのチェックをすり抜けてしまう。

マルウエアが含まれていた場合もチェックができない、パスワード再送ならびに開けるのが面倒で生産性低下につながっている

マルウェアが埋め込まれたファイルが暗号化されていることによって、マルウェア対策システムの検知をすり抜けてエンドユーザーまで届いてしまう問題。

マルウェアチェックができない

マルウェアのリスク、パスワード解析の容易さ、盗聴リスク等

マルウェアの侵入を許してしまう。

マルウェアの送信に悪用される

マルウェアフィルタすり抜け感染リスク高。誤送信先にて復号可能。生産性低下(暗号化/復号化)などなど

マルウェアを含む暗号化ZIPファイルをメールサーバのウイルスチェック機能で検知でき ない

マルウェア感染の経路

マルウェア検知が出来なくなるため。

マルウェア検知不可。後追いパスワード効果なしなど。

マルウエア攻撃に悪用。受信者の作業負荷高める。

マルウェア攻撃に悪用される

マルウェア攻撃に悪用される(メールサーバーのチェックを回避できてしまうため、圧縮 ファイルの中にマルウェアが含まれていても検知することが出来ない)

マルウェア攻撃に悪用されるおそれがあること

マルウェア対策(検査されない)、メール誤送信+ZIP暗号化が解除さるリスク等の問題ある反面、関係者間でそれぞれ手間が掛かることを行っている。

マルウェア対策ソフトでスキャンできない、PWの送信経路が同じ

マルウェア等の混入

マルウェア付きのZIPファイルのすり抜け。そもそも、害しか無い。

マルウェア付きのメールがセキュリティフィルタをすり抜けてしまう。フィルタに守られているユーザは添付ファイルに対する警戒が薄めなため、マルウェアの拡散を手助けしてしまう場合がある。

メールGWのウイルスチェックでウイルスを検知できない。 パスワードの通知がメールで あれば、そもそもZip暗号化する意味がない。

メールアカウントが乗っ取られていた場合、ファイルとパスワードを両方とも奪取されてしまう

メールから情報漏洩したらPWも一緒に漏洩する。ウイルスチェックができないなど

メールが盗聴されていた場合、ファイルもパスワードもどちらも取得され情報を保護することができないという問題

メールが盗聴されている場合、ZIP暗号化は無意味となるため

メールが盗聴されている場合、パスワードの別送は無意味なこと。

メールが盗聴されれば意味は無い

メールゲートウェイ上で添付ファイルのウイルススキャンができない

メールサーバーにおけるウイルススキャンができない

メールサーバーのアンチウイルスフィルタをすり抜けて、エンドポイントに到達してしまう。

メールサーバーの時点でウイルスを検知できない、多くの使用法では誤送信・盗聴対策としては脆弱

メールサーバーやメールゲートウェイでウイルス対策ソフトによるマルウェアの検査ができない。また、パスワードを別メールで連絡した場合、通信経路上の盗み見対策としては十分なセキュリティ担保策となっていない。

メールサーバー上でウイルスチェックができない。経路上盗聴があった場合にはパスワードも盗聴されるので意味がない。(自動パスワード送信だった場合)誤送信時にパスワードも予期せぬ相手に届くので、情報流出防止の意味もない。

メールサーバー側で復号できないのでウイルススキャン不可、広く利用されてしまっているため、無警戒に開いてしまうため、ユーザーの振る舞い的な問題でついうっかり開きやすい状況になる ※ これがMIPなら(不幸にも)あまり普及されていないのでクラッカーから狙わんれない

メールサーバ上でのセキュリティ対策が困難

メールサービス内やエンドポイント側のウイルス対策ソフトでウイルスチェックが実施できない

メールセキュリティ製品でのウイルスチェックなどが実施できないことや、盗聴対策としては不十分であること。

メールでパスワードを送付するため盗聴に弱い

メールでパスワードを送付するのだから本質的に無意味かつ検査用メールサーバでのウィルスチェックができないという弊害もある

メールという同一経路で暗号化ファイルとパスワードを送る場合、 メールが盗聴されて いればパスワードも露呈してしまうので セキュリティ対策としては脆弱である。 特に、アプライアンスなどでパスワードが自動送付される場合は、 宛先確認の効果もない。

メールという同一媒体でパスワードを送付すること、zipファイル暗号化の解除が比較的 容易であること。

メールなどが搾取されていた場合、パスワードを別送しても送付した添付ファイルを搾取している第3者に閲覧されてしまう。 またウィルスチェックができない。

メールに添付された暗号化ZIPのマルウエアを警戒しなくなる。

メールの送信先を間違えて場合、パスワード通知メールが送信される前に誤送信に気が付かないとzipファイルとパスワードが誤送信相手に送られ添付ファイルが解凍できてしま う。

メールの盗聴

メールの盗聴に関しては無力。また、「Emotet 」の蔓延を許した。

メールの盗聴を考えた場合、別便とはいえ同じメールというシステムでパスワードを受け渡す点や、誤送信を行ってしまった場合に取り消しが困難である点、また送信者に渡ったファイルの追跡が容易ではない点など

メールの返信によりパスワードが送信されるがreferencesから手繰れてしまう。パスワードが平文。PPAPベンダーに自社のメールアドレスを丸ごと預けてしまうリスクなどなど

メールの傍受による機密情報の漏洩

メールフィルタリングが無意味になる・パスワード別送の意味(

メールへの添付をやめ、Webサイトからのダウンロード方式に変える

メールボックスでマルウェアなどのチェックができない

メールを誤送信した場合にパスワード通知も誤送信した先に送信されてしますため無意味になってしまう。

メールを中間で観測すれば、添付ファイルを解凍できてしまう。

メールを盗聴されているなら暗号化の意味がない、暗号化によりセキュリティチェックに漏れる可能性がある

メールを盗聴されるなら、パスワード通知メールも盗聴される

メールを盗聴され暗号化解除された場合、すべての情報が流出してしまう問題

メールを盗聴できる人はパスワードメールも添付ファイルも盗聴できる可能性が高い。暗号化zipはマルウェアチェックをスルーしてしまう。

メールを分割しているだけで、パスワードを知られないこと自体を担保できない問題

メールを傍受された場合に両方のメールが見られてしまうこと。それ以上にそもそもZip ファイルの暗号方式ZipCryptoの暗号強度が低いこと。

メールを傍受できる場合、暗号化ZIPもパスワードも別メールにしても両方取得できてし まう

メール経路が監視されている場合意味がない、ファイルの内容確認ができない

メール経路でのウイルスチェックがされない。 PPAPすることにより機密性の高い情報を 送ってしまう。 当初は宛先の確認をしていたが、流れ作業になり宛先を確認しなくなる 。

メール検疫の障害となる

ﾒｰﾙ誤送信時、攻撃者に窃取されたときパスワードも相手が取得可能なため

メール受信サーバーで検疫ができない。個人の操作で被害がでる可能性があり、またパスワードがメールで別送されること自体セキュリティが甘い。

メール送信経路でハッキングできる技術があればの前提ですが、パスワードをお知らせするメールもハッキングができるので結果としてパスワードが判明する。 また、昨今のPC スペック向上に伴いパスワード解析ツールを用いれば8文字程度だと1日かからずに解析されてしまう。 メール受信時にウィルススキャンされない。

メール中継でのアンチウイルスなどの検査をすり抜けてしまう。

メール添付されている、パスワードで暗号化されたZipファイルがメールサーバなどのゲ ートウェイでマルウェアチェックすることができず、そのままクライアントに送られる。仮に添付ファイルにEmotetなどのマルウェアが仕込まれていた場合、クライアントが添付ファイルを解凍し、実行した時にマルウェアに感染し、情報漏えい等の問題を引き起こす。

メール添付の場合、セキュリティスキャン対象から外れる可能性が高いなど

メール添付ファイルのウイルススキャンできない

メール盗聴のリスク

メール盗聴リスク、ウィルスチェックが出来ないためウィルスメールのリスク

メール盗聴リスクに弱い。ウィルスチェックができない

ﾒﾘｯﾄが限定的であるにも関わらず、マルウェアや内部不正などの検知・監視を無効化するなどでﾒﾘｯﾄが大きい

もともと通信経路での盗聴リスクへの打ち手だったが、O365やGmailなど暗号化が普及し てきたため、この打ち手自体に意味が無くなってきてるとの認識。クラウド上のメールボックスごと詐取されてしまうセキュリティインシデントが多いと認識してるため、PPAPは対策にならない。

悪意のあるプログラムが圧縮されているとファイヤーウォール等をすり抜けて受診してしまう恐れがある

悪意を持った者がzipファイル添付のメールを入手できるならばパスワードが記載された メールも入手できる可能性が高く、受信者の手間の割に無意味。

圧縮ファイルがセキュリティソフトで検査できないことが多い為、今流行りの「Emotet」などの脅威から守れない。 そもそもパスワードも同じ経路で渡しているため、盗聴され るから意味がない など

圧縮ファイルが添付されたメールと解凍パスワードのメールが同じ経路で送信されるので、傍受されるときは両方とも傍受される。

圧縮ファイルにウィルスが含まれているファイルがあってもセキュリティフィルターが検知出来ない。 パスワードを追っかけで平文で送るため、セキュリティ確保の意味が無い

圧縮ファイルにパスワードがかかっているとウイルスチェックができない。

宛先が同じところにZipファイルとパスワードを送るので、盗聴されると意味がない。

宛先を間違えて送ったら意味がない。ファイル送った後にパスワードも送るという二度手間がある。暗号化することでメールフィルタを通り抜けるので中身の検査ができない。

宛先を間違った場合に、パスワードも送られてしまうこと。また、可能性は低いでしょうけれど…通信路が暗号化されていない場合に、ファイル添付メールと合せて、パスワード付きメールも傍受されてしまう恐れがある。

宛先を誤ってメール送信した場合、暗号化した添付ファイルを解凍するパスワードも誤った相手に自動で送られてしまう為、セキュリティ上のリスクとなる、

宛先間違いによる情報漏洩リスクを低減させるという触れ込みでありながら、実際にはほとんどチェックせずに添付ファイルと同じ宛先にパスワードを追送してしまう為、意味を成さないことが多い。（添付ファイルにパスワードをかけて自動で同じ宛先に追送するというサービスも出回っていた。） 通信傍受のリスクについても、添付ファイルのついた メールだけ傍受されたりパスワードの書かれたメールだけ傍受されることは考えにくく、傍受されるとしたら結局セットになるのでリスク低減になっていない。 zip に限らず、暗号化されたファイルを添付すると受信側でのマルウェア検出ができず、相手方のセキュリティリスクを高めてしまうという事態を招く。

安全かどうかを完全に担保できていないもしくは担保できない状態で、相手にファイルを投げつける行為。ファイルの内容を暗号化してチェックできないように投げつけるので 、やっていることはその辺のスパム業者と同じであり非常識とされ思える。

暗号PWを追加送信する方法だとセキュリティー対策にはならない。

暗号データとそのパスワードが同一経路で伝達される

暗号の強度や同一経路でパスワードが送付されるなど

暗号化zipされることによって、アンチウイルスソフトをすり抜けてしまうことがある。

暗号化ZIPだと受信時にウィルスチェックが出来ない。パスワードを同経路でプレンテキストで送るので意味がない

暗号化ZIPでマルウエアを許してしまう。運用上の負荷。

暗号化zipとパスワードメールの経路が同じであるため、暗号化zipを受け取れる人はパスワードも受け取れる

暗号化ZIPによるマルウェアが侵入する可能性。PPAPによるデータ保護は有用性が低いこと。暗号化ZIPのセキュリティが低いこと。

暗号化Zipの場合、添付ファイルのスキャンが不可。マルウェア対策が困難になる。

暗号化ZIPの添付ファイルは、メールのウィルススキャンをパスしてしまい、Emotet等で利用される攻撃の被害にあってしまう。また、誤送信をした場合に同一のメールアドレスにパスワードも送付してしまうため、漏洩の危険性を高めてしまう。

暗号化ZIPはセキュリティソフトで検閲しずらくそれを逆手に取って暗号化ZIPで不正ファイルを送付する攻撃手法が出てきているため。

暗号化Zipはブルートフォースで破られること。「パスワードは他の手段で通知」という推奨項目を、同じ手法であるeメールで別セッションで受け渡して適合としてしまっていること

暗号化ZIPはメールセキュリティではスキャンされないため、標的メールに利用されやすい。

暗号化ZIPファイルがネットワークセキュリティ製品のスキャンを通り抜けてしまう。

暗号化zipファイルが内にマルウェアを含むファイルが存在する場合、マルウェア検出ツールをすり抜けてしまう。

暗号化zipファイルとその通知PW同じ経路で送信されるので窃取されると暗号化が解除できてしまう。

暗号化されたZIPファイルがUTMによる検知を回避するため

暗号化されたZIPファイルと解凍パスワードが同一ルートで送られていること。

暗号化されたウイルス侵入

暗号化されたことによりAV等のセキュリティスキャンをすり抜け内部NWに脅威が侵入する可能性がある

暗号化されたファイルと解凍パスワードを同一チャネルで送る問題。

暗号化されたファイルと同一経路でPWも送られるので、盗聴されるときはどちらも盗聴され、暗号化/複合の手間がかかるだけでセキュリティ上意味がない。

暗号化されたファイルにマルウェアが仕込まれていても、検知することができない

暗号化されたファイルはウイルススキャンができない ・メールで送付したファイルのパスワードを後からメールで送付しても、通信経路・保存場所が同じなので意味がない

暗号化されたファイル内のウィルスチェックができない。また現在の暗号化では総当り方式であまり時間を掛けずにパスワードを突破できてしまう。

暗号化されたファイル本体と復号のためのキーワードはそれぞれ別の媒体で送信しなければならないというガイドラインに反している

暗号化された添付ファイルにメールサーバのウィルスチェック機構が働かない

暗号化された添付ファイルはメールサーバなどでウイルススキャンできず、感染リスクが上がってしまう。

暗号化された添付ファイルを送られてるのが日常となり、悪意のあるファイルを送りつける土壌となる

暗号化されていないメールを利用して添付ファイルと、パスワードを送ること。

暗号化されていることによりゲートウェイでのウィルスチェック等ができない。

暗号化されているため、ウィルスチェックができない。

暗号化されているため、中身のチェックが困難(Emotetなどマルウェア攻撃に悪用されるケースがある) ・添付ファイルを盗聴できれば、パスワードも盗聴可能であること。

暗号化されているため受信側のメールサーバでマルウェアのチェックができない

暗号化されてもファイル名やディレクトリ構成は分かる。暗号化によりウイルススキャンがスルーされる。

暗号化されることでメールサーバー側で内容が確認できず、マルウェアの混入が特定出来ない可能性があるため

暗号化したデータと、復号用パスワードを同じ経路で送るため、その経路1つが侵害されるとデータが盗まれる点。

暗号化したファイルと同一経路で暗号鍵を送るので意味がない無駄仕事問題。

暗号化したファイルのウイルスチェックできない

暗号化したファイルをメールに添付して送り、同一経路で後追いパスワードを受信者に伝えることは、その経路上を第三者に盗聴されていたとしたら添付ファイルにパスワードを掛けていたとしてもパスワードまで傍受されるため暗号化の意味がなく、セキュリティ上あまり効果がないと言われている。

暗号化した添付ファイルがウィルスチェックをすり抜けて相手に届いてしまう

暗号化した添付ファイルを送った先と同じところにパスワードも送るから。

暗号化していないパスワードをメールで送付した場合の傍受の危険性があること。

暗号化しても、すぐ同じ差出人からパスワードが届くため、乗っ取られた場合開くことは安易

暗号化しても、パスワードも同じ経路で送付している。暗号化しているため、添付ファイルのウイルスチェックができない。

暗号化して送ることでマルウェアフィルターをすり抜けてしまい、実際にマルウェアが入ったものを送られても気付くことが出来ない。・1通目と2通目を同じところに送るので、手間の割にあまり意味をなさない

暗号化することでウイルスが入り込んだ添付ファイルがスキャンで検知されない恐れがある

暗号化の方法がZIPである場合、バージョンによっては簡単に解読されてしまう。また、パスワードを同一経路のメールで送信する場合には、盗聴という観点から考えた場合、ほとんど防衛の意味をなさない。

暗号化ファイルとパスワードが同一通信経路で送信されている

暗号化ファイルとパスワードを同じメールアドレスに送信する

暗号化ファイルとパスワードを同じ経路で送っていること(メール盗聴された場合は意味 をなさない)

暗号化ファイルとパスワードを同じ経路で送信するため、手間がかかるが、セキュリティ上の効果が見込めない。

暗号化ファイルとパスワードを同一経路で送信しているのなら,その経路を見ている第三 者にはどちらも見られているので暗号化の意味がない。そもそも,暗号化ファイル自体, 知識があれば簡単に解除できること。

暗号化ファイル付き添付メールとパスワード通知の経路が同じ場合、経路途中で盗られたら添付ファイルとパスワードの両方が盗られ、復号化されてしまう。

暗号化添付ファイルがメールセキュリティを通過してしまう

暗号化添付ファイルと同じルートでパスワードを送信することによって盗聴に対す安全が確保されない、AntiVirus等でZIPファイルの検証ができない

意味がない、作業負荷が増える

意味がないばかりか、マルウエアに感染してもチェックできないという弊害がある。

解除するパスワードを容易に知ることが出来る

解除パスワードの通達方法が、メール上で同一となっているため、本来の対策としての乗っ取り型攻撃に関しては意味をなさない

解凍パス付メールも同一経路。暗号化ZIPはセキュリティスキャンを透過する。

解凍ファイルのファイル名等の取得が可能となるため。

開封しないとセキュリティソフトでチェックできず、セキュリティから漏れるおそれがある。 盗聴者に対しては、パスワードを送付しないことにしない限りは、意味がない。

外部からファイルを取得できるのであれば、パスワードも見れる

企業などで利用する場合,メール検閲できないためマルウエアなどがすり抜ける可能性が ある.またzipにされる対象がファイル名を騙ったexeファイルであり,ユーザが誤って実行させられるケースも考えられる. プロトコル(手順)を考えると,配送時の利用されるどこ かのノードで,暗号化Zip添付とパスワード記載の2通のメールを受けとることで復元でき ることから,Confidentialityを確保できているように見えて,実はできていない. パスワードの再利用(以前送っていたメールに記載のパスワードを,時間しばらく経ってからも同じものを再利用)を行うメール,例えば「以前これこれで共有したパスワードで開いてください」と書いてあったら,そのメールの出処を信じてしまい,本来とは違う方からのメールであったとしても,意図せず開いてしまう可能性がある.つまりメールのやりとりに関する前後の文脈から,あたかも署名が付与されたかのような錯覚を受けることとなる.

既存のウィルスチェックでは検知対象外になる

既存のセキュリティソフトでは添付zipをスルーしてしまうこと

具体的には詳細は理解していないが、web上のニュース等で問題となっている事を知って おりました。

経路が同じ、ZIPされたファイルにたいするVirusチェック

経路が同じなので暗号化しても意味がない

経路での監視に対応不能であること。

経路上でウイルスチェックが効かない

経路上でデータを盗聴していた場合、暗号化ZIPのパスワードを取得できてしまい、暗号 化を解除できてしまうため。

経路上暗号化ファイル付きメールが入手できるなら、パスワード付メールも入手できるはずなので意味が無い。

結局、誤った宛先にパスワードを送信するリスクがある

結局、同じメールアドレスにPWを送るので意味がない。・ZIP化することによって、添付ファイルがファイヤーウォールをすり抜けてしまう。

結局同じメールしすてむでパスワードも送られる 成りすましメールで暗号化ZIPでマルウエアが送られてくる等

鍵と金庫をほぼ一緒に送るのと同じ

現実的には、情報を守れない。

後から送ったパスワードが傍受可能なリスクがある

御社の場合、暗号化という点では良いが何処向けに対してのセキュリティか、もしくは、情報漏洩対策も含んでのセキュリティなのかが不明です。理由として、元メールを送った先に暗号化しパスワードを送るということは、メール自体暗号化しファイルにはパスワードをかけているため、どこかで中身を抜かれる心配はありません。しかし、情報漏洩(誤 送信)の観点からは、メールを送った先に同じようにパスワードを発行していているため 、誤送した先にでも受け取った方はパスワードが届くため、開くことが出来ます。御社と同じ仕組をつかう業者でクリプト便という仕組みがあります。クリプト便は、最初のメールの後にパスワードを送る時、パスワードは再度、宛先を選んで送る仕組みを採用しています。その場合は、セキュリティでも情報漏洩(誤送信)、ハッキングの両方を満たして いると私は考えています。

誤って違う宛先に送った場合でも、それに気づかずパスワードも送ってしまうことが起きうる。

誤送のzipファイルが相手にあるので総当たりで解凍される

誤送信、メールの盗聴により情報漏洩する可能性がある

誤送信した場合、2通目のパスワードも誤送信されてしまう。それを自動で行っている場合は、大変なことになる。

誤送信などでは意味がない

誤送信による情報漏洩、Zipによりウイルス検知漏れの可能性、パスワードクラックなど により脆弱

誤送信に対応できない、メール盗聴には無意味など、セキュリティ上意味をなさない運用にも関わらず、セキュリティ上「正しい」運用として広く一般に認知され実際に利用していること。

誤送信の場合、後送のパスワードも誤送信先に届くので情報漏洩対策にはならない

誤送信先にパスワードも送付することから、個人情報漏えいの可能性がある。セキュリ ティ対策送付とでのチェックがかからないため、解凍後にウィルスに感染するリスクがある。」

効果がないこと

攻撃者がメールの情報にアクセスすることができる場合、zipファイルとパスワードを別 々のメールで送信する意味がないため

攻撃者のパスワードZipの悪用、セキュリティ製品での検査、誤送信対策の不備

採用されている暗号化アルゴリズムが現在主流の方式よりも古く、脆弱であると聞いています。

事務負担を増やすだけで、あまり意味が無いといった課題がある。

自動で送信されたメールパスワードは同じ経路を通るため、別々に送付する意味がない。

自動的に同じ宛先にパスワード通知も送られるケースがほとんどで、誤送信時の情報漏洩対策になっていない

実効性がない。

実態として形骸化している

守りたい情報が守れない点

手間がかかるだけで、それほどセキュリティを高める効果がない運用

手間がかかるわりにセキュリティ的に意味がない、ウイルスチェックにひっかからない

手間がかかる割にセキュリティ保全効果がない

手間が増える、zipファイルへのセキュリティチェック、パスワード漏えいの危険性

手間が増えるだけであまり意味がない。

受け取った会社側でセキュリティチェックをすり抜けること

受け取る側に負担がかかること、パスワードも平文で別途送るため漏洩のリスクは避けられないこと、Zipの暗号は総当りで解けること、など

受信時にウイルスチェック等の検疫に支障がある

受信者側のウイルス対策ソフトが検知しないままemotetなどのマルウェアを受信する

受信側のMTAなどで、マルウェアを検知できない

受信側のマルウェアフィルタをすりぬけてしまう。

十分なセキュリティ対策とはいえない

上記はどれも何となくしか知りませんが、知っている問題としては、ZIPファイルを送付 したメールが盗み見らた場合、同経路で送られたパスワードの通知メールも見られてしまい、意味が無いという点です。

情報の漏えい

情報漏洩

情報漏洩の対策にならない。

情報漏洩対策になっていない。サンドボックス検査が出来ない。業務効率の悪化など?

情報漏洩防止の役目を果たさない

信頼できない経路に平文で復号用パスワードを送信すること

総当たりでの解析が可能

送信したメールの同じ宛先にPASSWORDが送信されるため

送信先(to)を間違って送ってしまえば情報漏洩につながる。送信サーバー、受信サーバー両方が通信暗号化の実施がされていなければメールの中身は平文で送られる。悪意ある第三者がその通信を盗み見した場合、中身は確認されてしまう。

送付したファイル名の隠蔽に効果がない パスワードZIPの暗号化強度が低いケースが多い メール盗聴に対して脆弱 メールのAnti-Virus機能をすり抜ける

送付先が自動的に同じになっているケースがある。

送付先を誤った場合でも、取り消しが出来ない。

多くのサービスは、パスワードを自動で送付すること。自前で構築しているので、弊社は手動なので関係がない

大きく3点　1. 盗聴リスク 暗号化圧縮ファイルを送った経路と同じ経路でパスワードを 教えるため、結局誤送信等により不手際があった場合、漏洩を防げない。また、暗号化 と言っても比較的短時間で解析できる場合も多い。 2. ウィルチェックができない メールサーバーやクライアントPCで準備しているウィルスチェックソフトが暗号化圧縮ファイルをチェックできない。そのため、マルウェア感染等のリスクは高くなる。 3. 受信者側の効率低下 多くの場合、暗号化ファイルを受診後、パスワードが送られてくるため、 受信側は2回の手間を掛けてファイルを取得する必要がある。単純に考えて「倍」の作業をしていることになる。

第三者に盗聴されていた場合に前後して送られるパスワード通知も盗聴される危険性が高い

端的に言って、対策とは言えないこと。

中間者攻撃された場合、パスワード別送しても意味が無い等

通信への暗号化対策であり、メール内容が解析されるのであればパスワード送付メールも解析されるため、有効な対策にならない

通信を傍受されている場合にあまり意味がない事と、受信の際にマルウェア等のチェックが出来ない。

添付されたファイルのセキュリティ強度は、送信側に委ねられてしまう。

添付されたファイルはパスワード付きで圧縮されておりセキュリティチェックが受け手側で自動で実施出来ない。

添付して送ったファイルの内容を監査できないから。

添付ファイル(パスワード付きZIPファイル)とパスワードが同一経路で送信されており暗 号の意味がない(盗聴リスク)。・パスワード付きZipファイルはウイルスチェックができない。

添付ファイルがパスワードZip化されていると、ウイルスチェックできない。同じ経路で暗号化ファイルとパスワードを送るので、盗聴リスクを軽減できない。

添付ファイルが暗号化されているためウイルスの判断ができい。最近暗号化したウイルスメールが送付されている。

添付ファイルとパスワードが同じ経路で送られれれば、どちらも盗聴されて解読される危険性がある。

添付ファイルとパスワードが同じ経路で送信される点。

添付ファイルとパスワードが同一の経路で配信されている。

添付ファイルとパスワードが同一経路であるため、情報漏えいリスクあり

添付ファイルとパスワードが同一経路で送られるため、情報漏洩的に意味がない。またZIPファイルはパスワードがなくても構造が見えてしまう。最大の問題はマルウェアの侵入 がZIPファイルであることが多いため、被害を受け入れるきっかけになってしまう。

添付ファイルとパスワードが同一経路にて送信されるから

添付ファイルとパスワードを「メール」で送付しているため、メールを盗聴するだけでパスワードも取得できるので、簡単に添付ファイルを閲覧出来てしまう。

添付ファイルとパスワードを同一経路で送信している。ファイル暗号化するとウィルスチェックができないケースがある。

添付ファイルとパスワードを同一経路のメールで送信することで両方が傍受される。また添付文書が暗号化されていることで、セキュリティツールでの検疫が出来ない。

添付ファイルとパスワードを別のメールにしても、宛先は同じままなので、宛先を間違えた場合は結局添付ファイルを開けてしまう。

添付ファイルと同一の経路でパスワードが送信されることにより、通信傍受に対しての防御策として有効ではないこと。

添付ファイルにパスワードがかかっているので、中身をスキャンできない。

添付ファイルにマルウェアが含まれていても検知できない問題

添付ファイルのウイルスチェックができない

添付ファイルのウイルスチェックを行えない

添付ファイルのウイルス検知が行えない。パスワード保護の意味をなしていない。

添付ファイルのセキュリティスキャンをすり抜ける

添付ファイルのセキュリティチェックができない、 同一通信経路でパスワードを送付す ると意味がない

添付ファイルの内容が他人に読まれてしまう

添付ファイルをウイルススキャンできない

添付ファイルを暗号化するため、ファイルの中身のウイルスチェックなどができない。

添付ファイルを暗号化するためマルウェアのチェックができない

添付ファイルを送る際に誤送信していると、別メールで渡しているパスワードも誤送信相手に送られることが多く、セキュリティ対策として意味を成さない場合があるということ。

添付ファイルを盗める攻撃者は後から送るパスワードも盗聴可能だから

添付ファイル自体の問題、同じ経路でパスを送付する問題など

添付ファイル内にウィルスが混入していても、暗号化をしていると検出できないという問題。

添付ファイル本体とパスワードを同じ送信形態(メールで本体とパスワードを同時に送る)で送ると、悪意のある盗聴者はパスワードも入手できる

添付を送った後にパスワードを別送で送っても意味が無いことと、暗号化することで、色々なセキュリティ機器を通過してしまうなど。

添付付きメールとパスワードを同じ経路で送信すると盗聴されていた場合に情報漏えいにつながってしまう

転送による流出不可 ・誤送信後の追跡不可

電話やチャット等別ルートでパスワードを送らないと意味がない問題。

途中で盗聴されたら結局同じなため

盗聴による情報漏洩

盗聴の問題やウイルスチェック

盗聴リスクが高い

盗聴リスクやウイルスチェック不可など技術的問題があるため

盗聴対策にならない。ウイルススキャン対象外となることがある。

盗聴対策にはならない。誤送信対策としても、誤送信に気づかず同じ宛先に送付してしまっては、全く意味がない。

同じアドレスにパスワードを送付すると誤送信リスクの軽減にはならない ZIPファイルパスワードはそもそも脆弱である

同じメールアカウントに自動的に送信しているため、アドレス間違いや乗っ取りされている場合にパスワードも流出し意味が無くなる

同じメールアドレスでPWを送信するのはナンセンス

同じメールアドレスで数秒ずれで送信していれば、本体を盗み見れる人はパスワードメールも盗み見れるので意味が殆どない。

同じメールアドレスにパスワードが送られる。

同じメールアドレスにパスワードが送られるため、意味がない

同じメールアドレスに回数を分けるだけなので有効性に疑問がある

同じメールアドレスに送られるので、もし漏れたら圧縮ファイルとパスワードがペアであるわけなので容易に解凍できてしまう。

同じメールアドレスに対してそれぞれ送付するため、盗聴されると情報が漏えいされやすい。

同じメールアドレスを使って発信されている

同じメールアドレス宛に添付ファイルとパスワードを送付するため、誤送信した場合ファイルが開かれる恐れがある。・添付ファイルを受信した側において、セキュリティソフ トがパスワード付きZIPファイルを検査しないため、ウイルス等が入っていた場合防ぐこ とができない。

同じメールでパスを配信しても意味がない。パス付きZIPが横行することで、マルウェアがすり抜ける原因になる。

同じメール配送経路の場合にパスワードの窃取が可能

同じ宛先に暗号化ファイルとパスワードの両方を送るので誤送信対策としては不十分

同じ経路(アカウントが乗っ取られた場合)、ZIPファイルの検疫されない状況

同じ経路でパスワードが来るのでわかってしまう。

同じ経路でパスワードを送ることは意味がなく、暗号化添付ファイルによってウィルスのチェックが不十分になる。

同じ経路でパスワード送る

同じ経路でメール本文とパスワードを送信すると解析されてしまう

同じ経路で時間差パスワード送信の問題点は古くから認識されている。

同じ経路で情報のやり取りを行うことになるので、容易に情報を搾取されてしまう。

同じ経路で送ること

同じ経路で送るので。誤送信に未対応。

同じ経路で送信しているのでネットワークをハッキングされれば解読されてしまう。

同じ経路で平文のパスワードを送信しているため漏洩対策になっていないという提言。暗号化することでウィルス検知をすり抜けるという問題もある。但し、Pマーク認証における個人情報の送信手段として許容されていたり、顧客からのセキュリティ要件に含まれていることもある。

同じ経路で本文とパスワードを別のメールで送信しても、経路途中で通信内容を取得されれば、意味がなくなってしまうので。

同じ経路で立て続けに解読パスワードを平文で受信したときは「こいつ本物の馬鹿だ。」と思った。

同じ手段で同じ相手にパスワードを送るため、誤った相手に届く可能性が高い。また、古くからのZIP鍵では解読が簡易

同じ送信経路での送付は意味が無い

同じ送信経路で送信しているために盗聴されたときにパスワードまで開示され暗号化の意味がない

同じ通信経路

同じ通信経路でファイルとパスワード情報を流すことになるので、盗聴された場合は両方とも盗まれるリスクが高い。

同じ通信経路上でzipファイルとそのパスワードが流れる問題、ネットワーク上にあるアンチウィルス機器でzipファイルを検査できない問題

同じ通信路を使うので意味がないこと

同じ平文のメール送信するため

同一アドレスから連続してオープンな文書で送られるパスワードに存在意義はない。監視者がこちらを見れば、簡単に解除出来てしまうので。

同一の経路でファイルと暗号情報が送付されており、盗聴等に対する秘匿性の効果が見込めない。メールリレー時のウイルスチェックが機能しない。等

同一の送信先にパスワードが送られるため、誤送信対策にはなっていない。

同一メールアドレスにパスワードを送るため、秘匿性がない。

同一メールへ圧縮ファイルも解凍キーワードも送るため。

同一ルートでパスワードも送信するため、第三者に漏れた場合の保険になっていない ・Zipファイル内のデータがウィルスに感染していた場合、通常のウィルスチェックではすり抜けてしまう可能性がある

同一経路

同一経路、自動送信など使い方がずさんであれば暗号化が無意味であるうえ、暗号化ZIPファイルへのセキュリティ対策が不十分な受信者が相当数あること。

同一経路、同一ツール配信のセキュリティリスク

同一経路かつ近しい時間にメール本文とパスワードが送られる点 多くの場合パスワードが平文で通信路上を通る点 暗号の長さが短い、または容易に想像できる暗号の場合、Zip本体から容易にパスワードが解析されてしまう点

同一経路でのパスワード送信、暗号化されたZIPファイルのアンチウィルス対策

同一経路での送付

同一経路でパスワードが送られる問題

同一経路でパスワードも送っているため、盗聴された場合には結果的に情報が漏洩する。

同一経路でパスワードを送信する点。EMOTETなどの同様の手法のマルウェアが登場した点。

同一経路でフ暗号化zipファイルと、復号化パスワードが送られるので、盗聴された場合、復号化される。内容によっては情報漏洩となりうる。

同一経路でほぼ同時に添付ファイルとパスワードが送られるため、誤送信したときに情報流出の恐れがある。

同一経路で暗号化データと暗号キーを送るのでセキュリティ上の効果が相当に薄い。(ゼロとまでは言わないが)

同一経路で暗号化文書とパスワードを送付することは機密性向上にほとんど効果がない

同一経路で送信、暗号化によるマルウェア検知など

同一経路で送付される点、平文で流れる点

同一経路に錠前と鍵を流すこと、暗号化されているためウィルスがすり抜けること

同一手段でパスワードを送るため、本質的なリスク回避になっていないこと。

同一手段でパスワード送信している

同一手法で暗号化済みデータと復号用PWを送信することがセキュリティ上有効とは考えられないといった問題

同経路で暗号鍵を送っても盗聴対策にならない一方で、悪意あるコンテンツが含まれていてもゲートウェイセキュリティ製品のフィルタで検知できない

同時にパスワードを送ることと、圧縮ファイル内のウイルスチェックが困難であること

同時に流出し、セキュリティ上の効果が非常に薄い

内包されている悪質なファイルがスキャンをすり抜けて入り込んでくる 簡単なパスワー ドが設定されていたり、ファイルを添付したメール本文に記載されていたりしており手間がかかる割にファイル保護の観点で十分とは言えない

二つのメイルが同じ経路を取って送られることが多い。

入り口でウイルススキャンができない、パスワード付きファイルとパスワードを別々のメールで送る場合であっても「時間差を開けず」送信するのは意味がない。

任意のメールが傍受できれば暗号化されたファイルが見られてしまう。

非暗号化メールを盗聴されていれば意味がない。暗号化ファイルはアンチマルウェアスキャンできない

標的型攻撃に使われるリスクがある

不正プログラムを含むファイルが暗号化されて、スクリーニングできず、エンドポイントまで配送されてしまうリスクがある。

複合パスワードの通知メールが誤送信されてしまった場合、取り返しがつかない問題。

物理的にファイルを送る。PWを送る。同じ宛先に誤送信をしてしまった場合には意味のないセキュリティとなる。

平文でメールで通知される為、意味がない。

平文で送信するSMTPでは、”パスワード”を記載したメールが傍受された場合、暗号化されたファイルが解読される恐れが有る。

別メールにしたとしても、同じ通信経路で送っているのであまり意味がない。

別送とはいえ、平文のメールで.zipファイルのパスワードを送付するため、セキュリティの観点からは本来まったく意味をなさない。であるにも関わらず、なにか対策を行っているようなイメージを一般の方々には持たせてしまう、という弊害がある。一時、パスワード送付メールを手動で送っていた際には、別送するメールの宛先を正しく送ってさえいれば、先に送った.zipファイルを開かれることもなく、結果として情報漏洩を防ぐ意味もあり得る、との言説もあった。しかし後年、添付メール送信時に .zip 化とパスワードメールの送付までを自動化する仕組みが備わってしまい、この限定的な効果さえもまったく無くなってしまった。

傍受された際に意味がない

本質的なセキュリティ保護の方法にはなっていない

本文とパスワードを同一手法で送るため、その手法が盗聴などされることで悪意を持つものに情報を取得されてしまう。

本文と同経路であるメールでパスワードも送るので、暗号化していてもパスワードも丸見えとなり、暗号化解除可能となる。

本文の漏洩、添付ファイルの改ざん

本文メールと同じアドレスに自動でPWメールを送ることで、本文メールを入手できた人は、PWメールも入手できる。またZIPにウィルスを仕込むことでアンチウィルスソフトが機 能しないことがある。

面倒なだけで誤送信防止にあまり効果がない(自動でパスワード送るツールの場合、パス ワードも一緒に誤送信先に送られる) - Emotet/IcedID のようにマルウェアが添付されていても、添付ファイルをスキャンできないので各種ウイルスチェックをすり抜けてしまう

問題があると言われている事は知っていますが、問題の内容自体は分かっていない

容易にパスワードが盗聴可能なためセキュリティ上の意味が薄い

容易に解読可能、パスワード漏洩の可能性

両方入手された場合開かれてしまう

Q2-2. 送信する添付ファイルのうち暗号化zipにする対象はどのようなものですか (その他の自由記述）

5MB以下は暗号化zip、それ以上はWebダウンロード方式。先方から暗号化しないで欲しいとお願いされた場合は除く。

html含めてテキストデータ以外は暗号化しようとする

ZIPファイルの受け取りができない宛先以外

アップロードし、URLを送っている

グループ会社以外への添付資料ありのメール送信時

サイズが2MB以下、特定の宛先以外は暗号化zipで送る

そもそも暗号かZIPを使用していない

なし

ファイル共有のオンラインストレージを利用

プロバイダで添付ファイルを全部暗号化

メールに重要な情報は添付しない

暗号化zip 完全廃止

暗号化zipで送られてきたメールへ添付メールを返信する時

一人歩きした場合に問題になりそうな恐れのあるものはDL/UPサイトを使ったファイル転送を利用。

外部とのセキュアなファイル共有サービスを導入しているので、サービスを利用する

外部と個人情報を含むやり取りをする従業員が対象

外部宛て添付ファイル付きメール

拡張子やサイズによる例外はあるが、原則自動暗号化

元メールが暗号化zipのファイルを転送する場合で,送信元に敬意を払う必要があれば。転送先の手間を省く方が重要であれば開錠して添付。

現在は暗号化zipをまだ使用しています。廃止に向け検討中

社外かつ、Googleカレンダー等の招待メール添付ファイルを除き全て

社外者の添付ファイルを転送する場合

社内を除き全て暗号化zipで送る

社内宛は暗号化なし。社外宛は自動でメールから切り離してWebダウンロード、パスワードは別メール。

相手の要望によって対応する

相手先のルールなど、望まれる場合のみ暗号化zipで送る

大容量ファイル送信システムがその仕様になっていたため、重要度にかかわらず暗号化zipで送付していた。

添付するファイルが予め暗号化されている場合は、.zip暗号化はされない仕組みが導入されている。

添付ファイルはすべて暗号化zipで送るが、添付ファイル全体のサイズが5MBより大きい場合、全宛先宛に対してはwebダウンロードを使用する。

添付ファイル自体利用せず、外部のファイル預かりサービスでファイルは送付し、その際の暗号化パスワードをメールで送付。基本的には外部への送付は別送の子の経路を利用する。

内容と宛先両方で仕方ない場合のみ。

必要に応じて

複数ファイルはzip化するが、Excelやword、powerpointなどの1ファイルの場合、アプリの機能でパスワード付加し送付

Q2-3. 「重要な添付ファイルのみ暗号化zipで送る」を選択した場合、重要な添付ファイルとはどのようなものですか
(自由記述)

n/a
PDF, JPGファイル以外の文書ファイル
アカウント情報や個人情報が含まれるファイル
いわゆる社外秘情報
お客様情報を含むもの
お金、機密にかかわるもの
コンサル資料
パスワードなどのセキュリティ情報
パスワード含有ファイル
パスワード情報、個人情報、機器情報など
パスワード等が記載されている書類
宛先を間違えたとき、機密を漏えいしてしまう時
一般公開(インターネット含む)で公開されていないもの
会社のルールに従って実施する
会社の数字が含まれているなど
会社の秘密情報を含む資料
会社規程で機密情報と定めているもの
外部に漏洩すると不都合なファイル
関係者のみに知らせるメール
企業の秘密に該当する情報
機密に当たる情報
機密事項、センシティブ情報、個人情報が含まれる書類
機密情報 (2件)
機密情報、個人情報などが含まれるファイル
機密情報、個人情報に該当するもの
機密情報・個人情報が含まれており漏洩時にNDAや個人情報保護法に抵触する恐れのある もの
機密情報がふくまれているもの
機密情報が含まれている
機密情報またはそれに準ずる情報を含む添付ファイル
機密情報や個人情報を含むもの
機密情報を含むデータ
機密情報を含むファイル
機密情報を含む文書
機密性が高いと判断されたデータを含むもの
業務上第三者に見られたくないもの
金額や個人情報等を含むファイル
契約書
研究データ等
見積もり等
個人の氏名や電話番号が書かれたもの
個人情報 (2件)
個人情報、IPアドレスなど個人個別を判断できるもの
個人情報、会社情報を含むもの
個人情報、機密にあたるもの
個人情報、機密情報
個人情報、機密情報を含む

個人情報、機密情報を含むファイル
個人情報、機密情報を含む場合
個人情報、機密情報等
個人情報、重要会議の情報
個人情報および企業情報
個人情報が記載されているファイルや、ID/PASSを通知する等の場合
個人情報が入っているもの
個人情報の含まれたファイル
個人情報または秘密情報を含む場合
個人情報や、見積金額など、他社にわたっては問題がある情報を含む場合
個人情報や会計情報を含む書類
個人情報や機微な情報を含むもの
個人情報や機微情報が含まれるもの
個人情報や機密情報が含まれるもの
個人情報や機密情報を含むもの（2件）
個人情報や機密情報を含む場合
個人情報や機密情報等が含まれているもの
個人情報や社外秘情報に関わる情報
個人情報や守秘義務に相当する内容を含んだもの。
個人情報や発表以前の情報など
個人情報を含む
個人情報を含むデータなど
個人情報を含むもの、契約、注文に関するもの
個人情報を含むもの、社外秘情報を含むもの　注文・請求・見積・契約書などの受発注証憑
個人情報を含むもの、商取引の情報(取引先の情報や金額の情報)、セキュリティキー(パ スワードなど)を含む資料
個人情報等会社の機密情報
個人情報有
固有情報の書かれた添付ファイル
顧客情報、秘密情報、設計資料など
顧客情報・案件情報を含むファイル
顧客情報が含まれるもの
公開されている資料以外
公開情報以外の情報が記載されたファイル
公開文書ではないもの全て
財務、個人情報、守秘義務のあるもの等
氏名・住所・電話番号などのいわゆる個人情報
自社やお客様ともに秘密とされている情報が含まれているもの。
社外秘、機密情報
社外秘には当たらないものの、社内情報等の記載があるファイル
社外秘のもの
社外秘の情報が記載されているもの
社外秘の情報を含む場合
社外秘や、先方の保持している情報が含まれてる資料
社外秘や個人名などパブリックに公表していない情報が含まれる場合
社内の規定で、社外に公開できないレーティングの対象になるもの
社内の情報を含むファイル
社内の人事情報関連や社外では当社の情報に関わる物など
社内機密情報に類する情報。経営、費用に関するもの。親会社のルールのため情報やりとり時に
社内規定で機密に分類される情報を含むファイル
主に個人情報

取引情報や設定情報を含むﾌｧｲﾙ
守秘情報
従業員リスト
情報が公になったら困るﾌｧｲﾙ
情報サービスのアカウント情報や部外秘情報など
図面や請求書等、情報を秘匿したいとき
請求書
請求書、納品書
組織内の非公開情報に関するもの
他人に見られてはいけないもの。
大半がPDF
第三者に閲覧されることが望ましくないもの。
第三者に開示できない情報
知的財産や契約に関わる書類
提案資料等
捺印済み注文書のイメージ
任意に判断
秘匿情報が含まれるもの
秘匿情報を含む場合
非開示情報
非公開情報
不動産書類など、個人情報が入った書類

Q2-4. 「宛先によって暗号化zipで送る」を選択した場合、どのような宛先が対象ですか (自由記述)

Boxリンクで共有できない外部の会社
ITリテラシーが低く、解凍等の処理が難しい取引先へPDF 化したものを送っています。
ITリテラシーが低く、順応性の低い会社宛て(zipじゃないとクレームを入れてくるところなど)
ZIPファイルが受け取れない顧客以外
zipファイル送信不可対象を除く
インターネットを経由する宛先の場合(外部の宛先)
グループ会社以外
グループ企業以外の他社
こちらから送る場合はリスクとPPAPの無意味さ (むしろやる方が良くないということ) を付記して暗号化しないで添付することにしましたが、現状では相手方のリテラシーレベルやルールに合わせて柔軟に対応しています。
ストレージサービス経由での提供が困難な場合
ファイル送付時の暗号化zipを希望されるお客様宛
メールサーバによる自動暗号化ファイルが復号できない相手
ルールで決まってる相手先
宛先の希望に応じて
安全なファイル共有手段がない宛先(現実的には多いはずです)
暗号化ZIPで送ってきた相手先
暗号化zipで送られてきた宛先
暗号化ZIPの送信を拒否しなかった取引先すべて
暗号化zipを使ってメールを送ってくる宛先
暗号化zipを前提としている送信先
暗号化zipを送ってくる大手企業
暗号化ZIPを要求してくる宛先
暗号化zipを要望される宛先
暗号化は社外のみで、社内へのメールは暗号化対象外としている
暗号化を必要とするあてsくぁき
外部
外部(自社ドメイン外)発信時のみ
外部ドメイン
外部ドメイン宛に送付するすべてのメール(同社内のドメインにはZip化されない)
外部に送付する場合
外部ネットワーク
外部のドメインのメールアドレス
外部メールアドレスが宛先に含まれている場合
外部宛(自社ドメイン以外)
外部宛先
外部団体
関連企業以外が対象
企業間
基本的に外部宛先(zipファイルを送れる宛先)
機密保持契約を締結している相手等
原則暗号化。相手先事情により暗号化zipが処理できない場合に非暗号化で送付(登録宛先のみ)
顧客
公官庁及び一部の民間企業
施主
自ドメイン以外が送信先に含まれる場合
自ドメイン以外の宛先

自社およびグループ会社と、ホワイトリスト指定した会社以外のアドレスが対象
自社グループ外
自社ドメイン以外
自社ドメイン以外の不特定多数
自社ドメイン外
自社と親会社を除く社外ドメインすべて
自社以外のすべての宛先
自社内以外の宛先の場合は全て
自組織以外
社員以外
社外（25件）
社外（ドメインが異なる）
社外（同一ドメイン以外）
社外、別ドメイン
社外アドレス（ドメイン）宛
社外が対象の場合
社外すべて。※社内は暗号化しない
社外ドメイン（3件）
社外ドメイン、Zipでの受け取り拒否以外
社外ドメインアドレスすべて
社外ドメインに対して
社外ドメイン宛
社外ドメイン宛（グループ企業を除く）
社外ドメイン全て。（自社子会社、関連会社を除く）
社外と判断されるアカウント宛
社外に送る場合のみ
社外に送付する時
社外のアドレス宛
社外の宛先（4件）
社外の宛先に対して
社外の関係者
社外の取引先
社外へ
社外へのメール
社外への宛先
社外への送信
社外への送信すべて
社外への送付の場合。
社外宛（5件）
社外宛て
社外宛ての添付ファイルは暗号化Zipで送る。社内宛ては暗号化圧縮しない。
社外宛のメール
社外宛は全て
社外宛メール
社外宛先（2件）
社外向けの宛先
社外向けの宛先はすべて暗号化zipで送る
社外向けは暗号化zipで送る
社外全てのユーザー
社外全般

社内
社内・グループ会社以外の宛先
社内と、ZIPファイルの受信を許可していない宛先を除いたすべて
社内ドメインのみに送信の場合
社内ドメイン以外のもの
社内はクラウドの共有フォルダ
社内メールアドレスには暗号化しないで送付。
社内メールのみの場合
社内向けは暗号化しない
主として社外
主にお客様
取引先（3件）
職員以外の外部関係者すべて
先方から要求される場合
先方が求めるとき
先方が拒否した場合
先方と当方のセキュリティポリシーの兼ね合いで仕方なく
先方要望
組織外に対する宛先全て
組織内ドメイン以外すべて
相手がそれで送ってきた場合
相手のセキュリティポリシ
相手の希望
相手先のセキュリティポリシー
相手側のメールサーバが TLS 非対応、かつ、他の手段が見つからない場合
総務部より社員宛(送信元と送信先が同一ドメイン)に送付する全体メール
送信先が社外の場合は全て
添付ファイルを暗号化zipで送付してくる社外の宛先
当社グループ会社以外
同一グループ内
同一ドメイン(社内)以外
同一ドメインは対象外
得意先
予め合意した宛先

Q3-2. なぜ暗号化zipでのファイル送信を使用することになりましたか(複数回答)(その他の自由記述)

IPOの条件

IT統制でメールの添付ファイルへの対応が求められたため

PPAPベンダーを利用しているが、Pマークで推奨していること、誤送信防止対策を間違っ た理解が社内にある

Pマーク・ISMSの審査に通りやすいと考えていたから

Pマークコンサルによる強制的として。

Pマーク取得取引先が、同等のセキュリティを他社(弊社含む)に求めていたため

お客様側のポリシーに従い、双方の交換で実施することになった

グループ会社からの指示

システム部門主導で導入されることが決定したようだが、内実は不明。決定事項を知らされただけ。

すでにそういうルールがあった

セキュリティ対策意識をステークホルダーへ示すため

それまで手動でやっていて面倒だったから

ファイル容量の問題

メーカーからの要請のため（2件）

メールサーバー付帯サービスの大容量ファイル送信システムだったため、（宅ふぁいる便 などの）他社サービスを介さずに大容量ファイルを送信できたため。

メールの容量削減

やっていないことが情報に関して意識が薄いと思われそうだったから。

意味はないが気を使っているというポーズ

何が重要等を個人で判断し暗号化するよりは、会社の業務で取扱う以上、全てが重要書類という考え方が正しいと思っています。

過去経緯で

会社からの指示。通信相手からの要望。

会社が運用したから

会社のルール、ファイル置きが目的の人もいる。

会社の運用

会社の規程で取り決められているため

会社の規程に従っている

会社の方針でしかたなく。

会社規則だから

会社指示

覚えていない

慣習化しているため、周囲は適切と判断するため

関連グループ会社の仕様に合わせた為

関連会社とのセキュリティ制約による

機密情報へのパスワード付け忘れ防止

客先要望

業界のデファクトスタンダードだから

区役所基準

経緯不明

顧客の中で暗号化されていないメールを拒否するところが有ったため

顧客指示、会社ルール

顧客要望

誤送信時に先方から対策として要求されたため

事業者のシステムとして組み込んである

自社のきっかけとなった理由は知らない

自社の運用規定

社の規定

社内ルール
社内ルールとして
社内規定により、暗号化zipでないと送信ができない
主な取引先がPPAPを行っているため弊社社長より要望があり導入
取引先からの希望により
取引先からの要請
取引先からの要望
取引先から要求されたから
取引先が暗号化zipファイルしか受け取らないことが多かったため
取引先が採用しているため
取引先が始めたから
取引先との取り決めで決まっている
取引先などから問い合わせ等が度々あったため
取引先の要請
取引相手からの要請
取引相手からの要望や対外的アピール
手作業での暗号化を指導していたが徹底されなかったため
手動での暗号化の手間を省くため
受信元の要求
受信者の不注意で転送しても、データが漏れないようにするため。
従業員のITリテラシー、技術が低いため。
所属する会社の決まりで。
上部組織が推奨したため
情報セキュリティ対策を実施している姿勢を示すため
親会社からの指示（2件）
親会社からの要求
親会社の情報システム部で処理されているため
先方からの依頼
先方様からの依頼により。
全て自動で行う為、各個人に依存せずにセキュリティが保てる。
相手がそれしか使えないから
相手が要求するから
相手に求められるため
相手の要求
相手先がその方法でしかやり取りできないため
相手先に求められる時がある。現実的に代替手段がないこともある。
相手先のポリシーによるから
相手先の対応にあわせた
相手先の要求されたから
他に選択肢がなかった為
他に代替策がないため。自分が送信するデータは重要な企業情報であることをユーザに認識させるため。
対外的に必要に迫られて
大容量ファイル送信の一環として
通信経路上で盗聴されないようにするため、情報保護のためですがその手段に疑問はありました。やらないよりはましですが、効果のほどは不明でした。やらないことに目くじらを立てるほどのものでもない気もしていました。
通信相手からの要求
当時の親会社意向
得意先からの要望により
入社時すでに導入していた
入社時には仕組みあり
発注者に合わせて

不適切な情報送信・不正持出しの防止

付き合いのようなもの。（実態は意味が少ないことは認識したうえで）

保険会社の指導

本質的に無意味であることは知られていても、ISMS的には相手方あっての話になる為、意味があることであるという認識が大勢を占めているうちはビジネス的には無意味ではない、という考えによります。
無意味と思っていたが、ルールとなったためわからない

Q4-2. 見直しをされない、あるいは今後検討するうえで見直しの障害となりうる理由は何ですか。また、すでに運用を変更した方は何が障害になりましたか。(複数回答)
(その他の自由記述)

「世間で一般的に認められる」代替え策が無いから。
PPAPが習慣化した年配者の抵抗
PPAPに代わる対策が完璧ならいいが、そう言い切れないのなら、その仕組み変更の投資説明を経営者が納得しない
PPAPを使わなくても悪いイメージがつかなくなったから
PPAPを止める、とルールしても重要なファイルを送る方法をどうするかが定まらない。送付先への体裁もある。
PPAP代替策を取引先へ浸透させる面倒さ
SMTPサーバー間の暗号化通信
Webダウンロード形式が完全な代替とならないから
WEBダウンロード方式と併用してるから
お客様が指定する場合
クラウドサービスなどを利用するほど頻度が多くない
クラウドストレージ方式に変更する予定であるが、アクセスできない取引先が発生する恐れがある
システム更改時に検討
セキュリティからクラウドストレージへのアクセス制限をしている顧客に対して、暗号化なしでファイル連携出来ない
セキュリティリテラシの低い管理者の「パスワードつけときゃ安全」という思い込み
そもそも機密情報のメールへの添付は規程で禁じている。
ﾃﾞｰﾀ授受の可能期間について等
トップマネジメントの意思決定が遅いから
どのような対策が最も適しているのかまだ把握出来ていないし、PPAPをするメリットも元々あまり理解できていないい
どの代替手段が適切かが客観的にわからないから
パスワードを付ける付けないの判断レベルが低い人がゼロではないので、社内ルールはそれに合わせたものにせざるを得ない。
ハッキングに関しては、防ぐことができないこと、会社責任ではないこと世界が認めているならばセキュリティ的に問題ないと思います。
ファイル送信手順を変更した場合の社員教育
ユーザースキル
ユーザーに負担をかけない運用変更が困難
ユーザー教育
ルールを決定してもそれが遵守されるかどうか不安がある
わからない
運用上の手間が増えるため理解が得られない。
運用変更に伴うコストに見合うほどのセキュリティ問題とは思わない
運用方法の変更による大混乱
会社および通信相手の意向によるため。
外して誤送信が起こった際の追及
監査対応で何かしらの対策をしなければならない
簡便でミスの怒りにくい代替策が無い事(OneDrive/Google Drive共有も、相手先毎に共有フォルダを用意しない、用意しても上位フォルダを共有してしまうなどのミスが発生している)
基準となる区役所が未導入のため
基本的には親会社の対応待ち
機密な内容はPPAPで送らないから
経営者判断
経営陣が事の重大さに気付けないから(ITリテラシーが無いから)
見直すことで周囲の方から、違和感を持たれるため
現時点で対策が必要な「不特定の全ての受信者」(ここが重要だと思っています)に有効な手段が見いだせない
現実的な良い策はない。
現状に甘んじている。
現状被害が出ていないから
顧客ポリシー

顧客側の取り組み

誤送信により情報を漏えいされた側がファイル共有の仕組みを受け入れずにメールに添付はさせつつ絶対誤送信をするなという事を言い出さない事

誤送信のリスクはなくならないから

自社のスキル。相手企業にセキュリティ対策を弱めるとか言われるという社員が多数

自身が検討する立場ではないため不明

自分だけがやめても会社のルール上違反だから

社会的に全体的な流れを見て対応していく

社内での検討をきちんと行って見直しをしたい

社内の偉い人の考え方を変えるのがめんどくさい。

社内規則

社内的に問題があり、変更することに対する理解を得ること

社内理解

取引先がまだ変えていないから

取引先からの指定条件で該当取引先とのやり取りだけ手段が残る

取引先が暗号化Zipでやり取りしてくるため、こちらからはやめずらいという問題

取引先が実施しているから

取引先の運用ルール上、PPAPを求められる可能性があること

取引先の対策に依存する

取引先の動きを見て動く

取引先他社がまだPPAPのため、自社だけの独断で変更できない。「webに載せています。URLはxxx、パスワードはyyy、zzz日後に自動削除されます」で伝えると『うちは特定URL以外はweb表示できないシステムが入ってるのでweb経由ダウンロードはできない』と言われた

取引相手の運用ポリシー

手間が増えた

習慣

小職の個人的見解ではさっさと見直すべき(そもそも導入したこと事態が間違い)と考えているが、本社上層部の見解は不明。現状、DXに躍起になっているが、中身をどれだけ理解しているのか…。

上とか担当部署とかが考えてるのかどうかさえ伝わってこないから

情報漏えいとセキュリティ対策は同じ土俵で考えられない

職員のセキュリティに関する教育

親会社のメールシステムに自動暗号化zip機能がセットだから

親会社の方針に変更が無いから

人員の再教育

世の中のデファクトスタンダードを模索中

世間がPPAPで回っている間はやめられない。

組織の意識が障害、なんとなく実施しているからトレンドではなくなったらやめる方向に行く

組織内で見直しの必要性を訴えても賛同者がいない

組織内への利用方法の変更を浸透させること

相手先がzip暗号化ありきの場合に継続が必要

相手先によるから

相手先の対応による

送信時CC・BCCやメーリングリストの利用で、自身にもZIPとパスワードが送信される場合も考え、メーラーに復号化できるZipファイルが残る事が便利だと思う。

対応するマンパワーの不足

代替案としてあるオンラインストレージは、添付するだけより手間がかかるため、ユーザに受け入れられない可能性

代替案の選定に手間、時間を要している。

代替策がいくつかあるのは知っているが、どれがスタンダードになるかわからないから

代替策で何がよいのか分からないから

代替策のコストの問題。PPAPを継続するよりコストか手間のいずれかがかかる

代替策へ移行した場合の社内の抵抗(操作が変わることへの)

代替策を検討中

代替手段があるため

単純な廃止だとリスクアップに繋がりかねない為適切な変更策を検討する必要がある。
担当でないため組織がどう考えているかわからない
通信相手の要求
提案はしたが運用が変わることについて否定的な意見が上位陣であり変更に至らなかった
当初から意味がないと考えていたから
得意先の承認が必要
内部規定にかかる修正、一部上部層の説得
必要に応じて使い分けするから
頻繁にファイルの送信をし合うので,リンクを送信してその都度ダウンロードしてもらう 方法だと手間がかかるため。
不明
分からない
弊社販売店で、エンドユーザー様への提案を含めて慎重に検討する必要があるから
別のWebサービスを使った機能もあるため
変えられない組織だから
変更対応にかかる工数がない
保険会社のガイドライン
本文暗号化などで日本国内に広く普及している形式がない
有効な代替手段の見極め
利用者への説明。そもそもの目的(誤送信防止等)が棚上げされている。

Q4-3. 上記のうち最も大きい、あるいは大きいと思われる理由は何ですか (その他の自由記述)

ActiveGageSSをすでに利用はしてるが、結局PPAPではないか、という会話がある。
PPAPが習慣化した年配者の抵抗
PPAPを使わなくても悪いイメージがなくなったから
PPAP以外の方法でも共有先を誤っていたら手段が異なるだけで事象発生の蓋然性および結果が同じと評価したから
PPAP代替策を取引先へ浸透させる面倒さ
Webダウンロード形式が完全な代替とならないから
グループ内での方針
スキルが低い
ストレージにアクセスできない取引先の調査
セキュリティリテラシの低い管理者の「パスワードつけときゃ安全」という思い込み
そもそも機密情報のメールへの添付は規程で禁じている。
とりあえず代替案があれば試行したい
マンパワー不足
ユーザースキル
ユーザーに負担をかけない運用変更が困難
ユーザー教育
暗号化Zipがセキュリティ的に問題ないと考えていることもあるが、クラウドストレージ も導入済み。かつ、会社として推奨はクラウドストレージと案内済み
暗号化を維持しながら取れる対応策の選択肢が少ない
右へ倣えの意識
運用・費用面から最適なサービスが見いだせていない
運用上の手間が増えるため理解が得られない。
会社および通信相手の意向によるため。
基準となる区役所が未導入のため
基本的には親会社の対応待ち
経営者判断
経営陣にセキュリティ意識が全く無いから。
見直すことで周囲の方から、違和感を持たれるため
元々、メール送信セキュリティメーカーでZip 暗号化問題にもある程度対応出来ているので
顧客ポリシー
顧客側の取り組みと従業員の意識
辞めたところで誤送信のリスクはなくならないから
社内の偉い人の考え方を変えるのがめんどくさい。
社内規則
社内的な理解を得ることが大変なため
社内理解
取引先からの指定条件で該当取引先とのやり取りだけ手段が残る
取引先が実施しているから
取引先の運用ルール上、PPAPを求められる可能性があること
取引相手の運用ポリシー
習慣
上に同じ
上記と同様
上記回答のとおり
職員のセキュリティに関する教育
親会社から特別指示がない　※親会社のセキュリティ要件は満たしている
親会社で全部管理されている

親会社のメールシステムに自動暗号化zip機能がセットだから
親会社の方針に変更が無いから
世の中のデファクトスタンダードを模索中
世間がPPAPで回っている間はやめられない。
先述のため略
組織のルールで規定されてしまっている
組織内で見直しの必要性を訴えても賛同者がいない
相手が確認する前にﾃﾞｰﾀが削除される等
相手先がzip暗号化ありきの場合に継続が必要
代替案の選定に手間、時間を要している。
代替策がいくつかあるのは知っているが、どれがスタンダードになるかわからないから
代替策で何がよいのかわからないから
担当部門での検討が進んでいない
通信相手の要求
同一経路で暗号化Zipファイルと、復号化パスワードが送られること。
得意先が求めている
特になし
特に障害となるものはない
特に障害となるものはないです。
特に変更には障害はないが、システム担当者自身が客先案件もしているため社内展開などの対応に手が回らない
内部調整、規程修正案、話の持っていきかた
不明
分からない
別の手法がある
変えられない組織だから
変化を嫌われる。
変更対応にかかる工数がない
有効な代替手段の見極め
理由なし

Q4-4. 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
(その他の自由記述)

「Activegate」で添付ファイルの送信全て「ファイルDL」にする。<期待できる効果>・暗号化ZIPは送られない。(マルウェアt対策　受信側への配慮)・DL期間があるので、リ スクは減る。・誤送信など、何かあったときはDLを強制停止できる。

「検討はしているが、未定である」とは回答しているが、小職の職場は導入/決定部門で はないため、システム部門がおそらく検討はしているはずであろう、という希望的観測である。

Boxなどの利用

BoxやDropBoxなどのクラウドストレージを使って、共有先を限定するなどして、運用方法を変更する。

CSMPでのスコアが高い製品を選びたい

GoogleWorksにアドオンのアプリを入れて対応

MicrosoftのRights Managementなどで権限管理を行う

n/a

online strage の利用

PPAPの代替手段の検討

PPAPを止める方向では考えている。パスワード付与の「ルール」を予め送付先と決めて、2通目でパスワードを送るようにはしないようにする。ただ、大容量のファイルを送る場 合の問題もあるので、それと一緒にツールを検討したいが、CSMPスコアが高いものを選びたいと考える。

PPAP以外の方法でメールのセキュリティを高め、誤送信を防止する管理策

PWは別途ルール化してある

sandboxの導入の検討

Teamsへの外部招待

UTMの強化

Web Download形式

Webサイトからのダウンロード方式

WEBダウンロード　パスワードは電話など

Webダウンロード、クラウドサービスに切り替え

Webダウンロードの運用に変更

webダウンロードへの切り替え

Webダウンロードやパスワードをヒントで送る等

Webダウンロード形式等を検討

WEBダウンロード方式、ダウンロード回数や期間制限　など

Webダウンロード方式への変更を社内セキュリティ委員会で承認の上、変更

WEBダウンロード方式へ変更

Webダウンロード方式へ変更する予定

Webによるダウンロードモードに変更

WEBへのリンクからのダウンロード

zipではなくOfficeのPW

あくまで個人的見解だが、本来的には S/MIME とすべき。次点でPGPとは思うが、対応メ ールソフトの問題がある。

あらかじめパスワードを取り決める、会員サイトの利用等

アンチウイルスソフトに Cylance PROTECT を利用しているため、マルウェア対策はある 程度できている。Cylance をすり抜けたマルウェアに対しての対策を検討中。

オンラインストレージの導入

オンラインストレージを利用したファイルの送受信を検討するか、暗号化ファイルを拒否する方法を検討中

クラウド‘ストレージの利用

クラウドからのダウンロード

クラウドサービスの活用

クラウドサービスの利用

クラウドサービス導入

クラウドサービス利用(送信は実現済み/受信は具体的方法を検討中)

クラウドストレージサービスを利用する

クラウドストレージでの共有を推奨

クラウドストレージとの併用

クラウドストレージなどの利用の検討

クラウドストレージなどを用いた運用

クラウドストレージのリンク使用

クラウドストレージの共有リンク

クラウドストレージの検討

クラウドストレージの利用に代替した

クラウドストレージまたはその他の送信手段

クラウドストレージをつかう

クラウドストレージを利用した代替サービス

クラウドストレージを利用する方針です

クラウドストレージ等とパスワード運用のハイブリッド

クラウド上に置き、URL、パスワードを送り、万が一消せるようにする。

ゲートウェイで分離や隔離をする予定

この問題に限らず従来のFW+エンドポイントに加えEDRの導入を検討しているが、これに対応出来るかは未知数。

すでにGSuiteでのアドオンで対応している

すでにあるWebファイル共有のシステムを使う

ストレージサービスなど

セキュリティ(経路暗号化・メール暗号化等)と誤送信防止を両立させる方法を検討。PPAP対策と言って暗号化自体をやめてしまわないような誤った対策をしないよう検討中。

ダウンロードサイトの利用

ダウンロード形式

チェックサービスを追加する。

どうすれば運用負担が減るか

ノンテック社員がめんどくさがらずに使えるツールを選択したい

パスワードの送信方法の変更

パスワードをSMSやチャットツールで送信する。

パスワードをメール以外の手段で伝えることに変更した。

パスワードを事前渡しの暗号表を使ったものを使用

ファイルの添付を行わない

ファイル共有サービスの導入を検討中。

ファイル共有サービスの利用。

ファイル共有サービスの利用を検討中と聞いています。

ファイル共有ツールの活用

ファイル転送サービス

ファイル転送システムの導入

ファイル転送用クラウドやサーバーによる方法

ファイル保護ツールを使うことを検討

まだ具体的には検討していない

まだ具体的に検討出来ていない

まだ情報収集段階のため、どのような方法を検討していくかも定まっていない

マル秘

メールサーバにレピュテーションフィルタ機能を持つものを導入し、エンドポイントにアンチウイルスと標的型マルウェア対策を実施した。

メールセキュリティサービスの利用

メールセキュリティで復号できない添付ファイルは一律拒否する

メールフィルタリングサーバの追加機能待ち

メール以外の安全な方法で渡す

メール添付ファイルの利用を禁止し、クラウドストレージ、もしくは自社開発のファイル転送システムのみを利用する様にルール変更する。

メール添付以外のファイル送受信手段の拡充

メジャーな方法を取り入れたい。現時点では、送信側、受信側ともに利便性を損なわず安全な方法として、メールと添付ファイルを自動分離し、WEBダウンロードさせる形式が好 ましいと考えているが、G Suiteでこれを実現するための手段がないか検討している。

よくわからない

宛先によりzip化、ストレージ格納をわけている

暗号化Zipファイル、または復号化パスワードが別経路で送信できる仕組み

暗号化された添付ファイルがある場合の自動拒否

暗号化したファイルをメールに添付して送ることを原則禁止した。添付してよいのは機 密情報や個人情報に当たらないファイルに限ることとし、それらは暗号化せずにそのまま添付して送る。メールに付記する「運用と理由の説明を行う文章」のサンプルを社内に 展開した。機密情報や個人情報に当たるファイルを社外共有する場合には Box 等のサービスを利用し、トラッキングができるようにすることとした。ただし、現時点では上記 説明をした上でも相手方が求める場合には PPAP 対応を行うし、相手からの暗号化ファイルの受取拒否まではしていない。

暗号化せずに機密性を保つ方法

暗号化の主流を見定めてから変更を検討する

暗号化ファイルが添付ファイルにあった場合、メール自体の受信を拒否し、返送する

暗号化ファイルは受信しない方向で調整したい

暗号化ファイルをゲートウェイでブロックする

暗号化ファイル拒否

暗号化ファイル付きメールは受信しない

暗号化をやめて、Webダウンロードだけ利用する方法を検討

暗号化を行い、パスワードを添付しない方法は実現できないか検討中

暗号化共有ストレージ

暗号化対象ファイルの緩和

運用方針について社内アンケートを募る予定

何らかの形で受信拒否する予定です。

開発メーカーなので、今までどおり自社製品

外部ストレージの利用の検討

外部ストレージを介して

銀行など外部ネットワークを遮断している環境ではWebダウンロードは使えないのでzipパスワードは残る可能性があります。パスワードをメールで送るのではなく事前に会社間で決めたパスワードでやり取りするなど検討したいと思います。

検討しようとしてる段階

検討はしているが代替案にそれぞれメリットデメリットがあるので少し待っている段階

検討中

検討中、未定

原則、メールへのファイル添付の禁止。クラウドストレージの利用。

現在はダウンロードの回数で確認している。

現在答えはありません。

現状、手動で暗号化しているので、まずこれを自動化したい。別経路でのパスワードの送信も考えているが、煩雑であり導入には二の足を踏む。

顧客次第

誤送信防止のため、方法自体は変えない。全部にパスワードを付けるとしている社内ルールを変えることを検討中。ただし、その判断レベルが低い人も想定して、社内ルールを厳しくせざるを得ない。

今後の世間の動きに合わせる

自社だけで取り組めることには限界があるので、社会的コンセンサスを見ながら。

自社で開発している製品に、先方にファイルアップロードを依頼する機能があるのでそれを利用する。先方がインターネット使えない、メールでしか情報送れない場合は仕方なく。

自動暗号化の廃止を検討中です。

自動的なファイル分離とクラウドストレージへの格納。

自動的に添付ファイルを保護できるような仕組みを探しています。

社内システム部で検討しているはず

取引先が使う以上、拒否はできない為、統一された方針を打ち出しにくい

受信についてはノーアイデアである

受信拒否を検討しているが、お客様のポリシーによる別手段がとれないケースもあるため、決定までには至っていない。

受信時はZip暗号化ファイル分離、送信時はファイル転送サービス(WebD/L方式)、をそれ ぞれ検討

受信先のITリテラシーもあるので、できるだけ簡単に利用できるものが望ましいが、何を使えば良いのか正直わからない

重要な情報は、クラウドストレージで共有する

出口対策の強化を検討。メール上で暗号化されたファイルのやり取りは今後もしばらくは続くと思われる。またZIP暗号化に限らず、PGPやS/MIME等の方法で同様に暗号化メールが送られるためウイルスチェックを抜けてしまう話はある。

少なくともPPAPベンダーの利用を中止で検討しようとしている

情シ部門の対応待ち中

情勢をウォッチしているのみ

情報収集中

親会社で処理検討しているようである。

推奨を探している。できればパスワードをどうするか。クラウドは顧客によりソリューションが違い、またその製品にもなんとなく信頼が持てず困っている

先述の通りではあるが、webの導入をしたところ「webに載せています。URLはxxx、パスワードはyyy、zzz日後に自動削除されます」で伝えると『うちは特定URL以外はweb表示できないシステムが入ってるのでweb経由ダウンロードはできない』と言われた。そのためま だ完全に切り替えができておらず代替手段も用意できていない。パスワードは別送信ではなく事前暗号表を用いたものにすることを検討している

先方によって運用を使い分ける

選択肢を抽出中

前述の通り、リンクへの強制変換とストレージへの格納 運用自体を日立さんやFreeeさんの様に公表するなど

全てファイル共有(送信)サービスでのやり取りに切り替え検討

相手の運用によるのでこちら側で検討はしていない

送信については先のQAのとおりオンラインストレージを介した方法が現実解と考えている。受信については、大手がすでにやっているようにZIPファイルは弾くのが望ましく取引 先等へもその旨のアナウンスは必要と考える。ただし・・・、相手が送ってくるメールの対応はなかなか困難である。

送信に関してはクラウドストレージを使用する

送信元の氏名・メールアドレス、件名や本文などで開くかどうかを大半は判断可能と考えています。また、ダウンロード方式にした場合のWebコンテンツ許可や 解読可能な状態でクラウドストレージに情報をアップロードする問題は運用・セキュリティの問題がある為、利便性とセキュリティの面で検討が必要と考えています。

送信時の一時保留

送信者認証(SPF・DKIM等)の設定見直し

他の暗号化ツールを利用する

代替えツールの検討

代替案の選択肢がありすぎるため未決定

担当部門からの方針、方式を聞いてから判断する

調査中

低コストで簡単(ユーザーにとって負担が少ない)方法

添付をリンクへの置き換える施策を導入検討中

導入済みシステムの仕様を徹底/社内啓蒙

特定顧客とはクラウドストレージの共有領域を利用 ・不正メールのより厳格運用(DMARC) ・サンドボックの利用

廃止する

必要なものだけ暗号化する(対象判断が難しい)、Emotet等の攻撃にも使われるのでとにかくやめる

分からないので今回のカンファレンスで参考情報を得たい

変更方法を含めて検討中

方法から検討中

方法論も含めて対応方法を調査中

未定

未定。まずは情報収集したい。

Q6-1. zipやoffice、PDFによる暗号化処理されたファイル(以下、暗号化ファイル)を受信したとき、どのように処理していますか
(その他の自由記述)

AV,ATP対策がとられた端末で伸張、スキャン

Gmailのためwarning

Office2003形式のファイルが添付されていたら迷惑メールフォルダに振り分けている

ウイルスチェックされていないファイルを開けることになるのでリスクになるが、導入しているEDR製品がそれを防いでくれる認識でいるが、リスクはある。

エンドポイントセキュリティソフト任せ(Webメール利用のため)

クラウドストレージの運用を機にされている企業からのメールは受け取らざるを得ないことがある

メールサーバのウイルスチェック時にタイトルにUNCHECKEDが付加されるのでそれを見て 判断

わからない

宛先が正当な先かを判断した後に受け取る

暗号化ZIPのみ受け取るが捨てる

暗号化されたZIPファイルのみ自動削除

以前からやり取りのある相手のみ受け取る。その他はごみ箱に自動振り分け。

今のところ受け取るが、EDR等でその後の挙動は監視

送信先が信用できる場合は受け取る

適切な相手という前提であれば受け取る

二重ZipやEXEなどが入ったZipはシステムで拒否している

不明

利用しているgoogleポリシーに準ず

Q6-3. 暗号化ファイルの中身についてなにかウイルスチェックを行っていますか (その他の自由記述)

1.解凍時のウイルスチェック 2.送信元、表題、本文など別要素でのメール検疫
EDR入ってるのでおk
Gmailのため、Googleが弾いていると思われる
Gmailの機能として実行ファイルが含まれている場合は削除になります。また、開封時に はウイルスソフトのスキャンが実行されます。
Googleがチェックしている?
PW付でなければUTM でチェックされる。PW付はPCでチェック
sandboxにてパスワード入力後チェックしている
ウイルスチェックだけでは防げない脅威があるので、ウイルスチェックしつつ、それ以外のツールも活用して安全を保つ。
エンドポイント製品で対応
ゲートウェイとPCでのダブルチェック
サンドボックスでの開封
セキュリティクラウドによるメール・ファイル無害化。
ファイルのオープン時、実行時にセキュリティソフトがチェックする
ファイル拡張子で振り分け、ゲートウェイでのチェック、解凍時のウイルスチェックを行なっている。
メールサーバーサービスにてチェックしている
わからない
解凍後サニタイズ無害化している
解凍後に無害化し取り込み
解凍時にチェックしていると思われるが定かではない
解凍時に別セグメントでチェックが入る
実行ファイル形式を含む暗号化ファイルは受信しない。及び解凍や復号時にチェックしている。
手動でチェック
信頼出来る送信アドレスをホワイトリスト管理している
展開前に手動でウィルススキャン
日次のウイルススキャンを実施している
分離したインターネット環境からLGWAN環境にファイルを移動させる処理のなかでウイル スチェックを行っている

Q7-1. 添付ファイルやメールの暗号化方式として技術的に興味のあることがあれば教えてください
(その他の自由記述)

AIP

IRM

Microsoft Office365を利用している会社における具体的な対応(例)ログ分析(暗号化ファイル送受信件数)、暗号化ファイルブロック手順等

SMTPを使ったメール転送システム自体の設計が古いので、エンドtoエンドで暗号化ができて、相手側の証明ができて、且つ運用が面倒でない仕組みを一般化する必要はある

ZIP暗号化が廃れるとして、どの送信方法がスタンダートになるのかの情勢を見守ってい る。今更S/MIMEとかはないと思う…。

ありません

インターネット黎明期のポリシー「悪事はやがてばれ、成敗される」を愚直に行う

クラウド暗号

その他アーカイブツールの暗号化強度

そもそもメールを使わないこと。PGPは20年以上前に興味を持った(オライリー本を買った)が、普及度合いではそれから進んでいない。

なし

ハフマン符号のランダム化

ファイル添付の全面禁止

メール以外でのパスワードの汎用的な送信方法

安全でかつ使用者が負担にならなければどの方式でも問題はない。

暗号化手法から調査する予定

何が良いか解らない

技術的な意味や特徴が理解できていない。

具体的には考えていない

現時点では、あまりこれらを理解していないです(クラウドストレージとかに寄せていい くべきという認識)

証明書認証関係全般

短期的にはオンラインストレージの利用を促す。中長期的にはビジネスチャットに移行しメール運用は限定的にする。

添付すること自体をやめるべき

添付ファイルの暗号化に代わる現実的な技術はどれかが興味があります。

添付ファイルの無害化

特になし (2件)

特に無い

変更したところで意味はない。設定や受け取りが煩雑なら本末転倒。

勉強不足のためどれがどのような技術なのか不明

良く分かっていない

Q7-2. あなたについて教えてください
(その他の自由記述)

3年前は助言・実行の立場であったが、現在は利用者(当時からPPAPは運用していない)
ISP
PPAPについて世の中に警鐘を鳴らし、自社製品の販売を促す立場です。
PPAPの運用などのルールを策定・管理する立場
PPAPの運用などを選定・助言・実行する立場
システム設計・管理者、情報セキュリティ関係者
事務
会社代表者
提案業者
自社の決定かつ他社への助言
調査検討し提案の上、必要であれば実行する立場
部局の情報システムの管理運用担当