
よろしく
お願いします！

P P A P


ペッパイナッポーアッポーペン

P Password付きZIPファイルを送ります

P Passwordを送ります

A Angouka（暗号化）

P Protocol（プロトコル）

セキュリティシアター
（劇場型セキュリティ）

実際にはセキュリティを向上させていないにもかかわらず、安全対策をしているように見せかける施策のこと。

見せかけのセキュリティのことで、「見世物小屋セキュリティ」と呼ぶ人も…

PPAPの危険性

1　暗号化されたファイルとパスワードを同一の手段（メール）で送るため、
最悪の場合データとパスワードが同時に漏洩する。

2　送信者はデータの暗号化、ファイルとパスワードを二通送信する手間、
受信者はデータを解凍・暗号化を解除する手間など。倍の作業量。

3　ZIPファイル自体がそこまでセキュリティが高くなく、
攻撃者がマルウェアなどのウイルスを仕込む経路になり得る。

4　パスワード付きZIPファイルは、多層防御のセキュリティをすり抜ける。


PPAP♡


ヨシ！

なぜ意味のない仕組みが生まれたのか？

- JIPDEC（一般財団法人日本情報経済社会推進協会）のPマーク取得のため、会社のセキュリティ対策として暗号化したファイルを送信し、ファイルとは別の経路でパスワードを伝えるという手法が誤って広まった。
- その後、Pマーク取得のためのコンサル会社などのセキュリティサービスとして、PPAPは営利目的の後押しもあり現在でも悪習として定着する。
- 本来は、ファイルをメールで送信したならパスワードは書面や電話、口頭など全く違う経路で伝えるという手法である。
- PPAPは海外には存在しない日本独自の悪習で、令和2年には内閣府から意味が無いどころかシステムの安全性を損なうとしてPPAPの撤廃を呼び掛けている。

セキュリティシアターの問題点

最大の問題点は誤った安心感を生み出すこと

- 潜在的なリスクを放置しているのに対策していると錯覚する。
- 限られたリソース（時間・労力・予算・人員）を浪費する。
- 本当に必要な対策が後回しになる。
- 従業員に負担を強いるだけで悪意の攻撃者には何の防御になっていない。

大事なのは安心感ではなく安全性である

セキュリティシアターを見抜くポイント

- **見た目重視**　：経営層や顧客へのアピールが目的になっている
- **不便で無意味**　：従業員に負担をかけるが、攻撃者は簡単に回避できる
- **測定不可能**　：効果を数値で示せない、示そうとしない
- **思考停止**　：「とりあえずやっておく」「他社もやっているから」が理由
- **古い脅威モデル**：現在の攻撃手法に対応していない過去の対策

本当に効果的な対策になっているか？

本質的なセキュリティとは

- **脅威モデルに基づく**：想定される攻撃者と攻撃手法を明確にし、それに対する防御を設計する。
- **多層防御**：単一の施策に依存せず、複数の防御層を組み合わせる。
- **継続的改善**：一度やって終わりではなく、継続的に監視・評価・改善する。
- **費用対効果**：リソースを重要度の高いリスクに集中投下する。
- **人間中心設計**：ユーザーが守れる、守りたくなる仕組みを作る

物事の構造や仕組みを知らないと対策できない

まとめ

- セキュリティシアターとは見た目だけの意味のないセキュリティのこと
- PPAPは無くすべき悪習
- 見せかけのセキュリティ対策はセキュリティを脆弱にする
- 安心感よりも安全性を重視するべき
- 本当に必要な対策になっているか分析し、効果的な対策をする
- 効果的な対策には知識が必要


ご安全に
PPAP♡