メールの暗号化

とみたまさひろ

NSEG #40

2013/06/08

自己紹介

- とみた まさひろ
- プログラマー (Ruby & C)
- http://d.hatena.ne.jp/**tmtms**
- http://twitter.com/**tmtms**
- 好きなもの
  - Ruby, MySQL, Linux Mint, Emacs, Git

「メールで資料送ってください」

「はい」

「暗号化してくださいね」

「PGPでいいですか？」

(°Д°)ﾊｧ？「なにそれ？」

orz

世間のメールの暗号化

その1

zip

ファイル添付します。

パスワードは後でメールで送ります。

添付ファイル.zip

今どき zip の暗号化は
暗号と言えるのか
強度的な意味で

別便で送ると言っても
送信元と送信先は同じ

添付メールが見れる人は
パスワードのメールもきっと見れる

せめてパスワードはメール以外の手段で伝えよう

その2

zip

ファイル添付します。

パスワードは「123456」です。

添付ファイル.zip

目をさませ！！

('д'⊂彡☆))Д´) ﾊﾟｰﾝ

その3

exe

暗号化強度の高いソフトで暗号化しました。
自己解凍形式で送ります。
exe の添付が禁止されているので、
ex_ にしています。
拡張子の ex_ を exe にして
実行してください。

添付ファイル.ex_

パスワードの伝え方

Windows じゃないと開けない

exe を禁止している意味を理解してない

なりすましかもしれない

本人だったとしても
何かに感染しているかもしれない

メールに添付された exe の正しい開き方

VM 上で Windows を起動

VM のスナップショットを取る

ネットワークを切断

exe ファイルをドラッグ＆ドロップでゲストに移動

exe を実行

展開されたファイルを
ドラッグ＆ドロップでホストに移動

VM のスナップショットを復元

めんどくせー

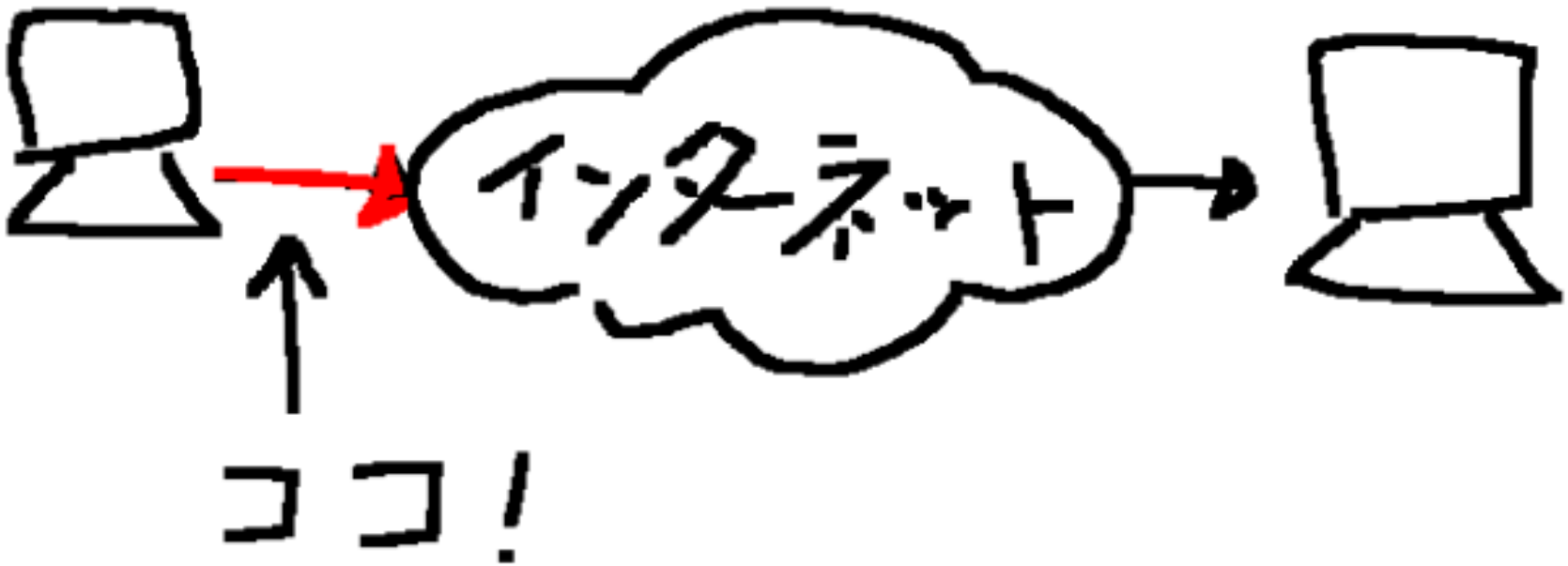
(ノ°Д°)ノ　＝＝＝＝　┻━━━━┻

やめて

その4

「SMTPSだから大丈夫です」

それココだけだから！



まとめ

- PGP は普通の人は使ってない
- パスワードはメール以外の手段で伝える
- exe を添付しない
- メールに添付しない
- メールはオワコン