これだけはやっておこう！
低予算でできる標的型メール対策

会社に戻ってすぐにできる標的型メール対策のあれこれ

自己紹介

縁マーケティング研究所（えんまーけてぃんぐけんきゅうじょ）は、

日本で唯一（おそらく世界でも唯一）、
自社内製で標的型メール訓練を実施するための
ツールセットを販売している会社です。

※標的型メール訓練をサービスとして販売している会社は沢山あります。

「標的型メール　訓練」でGoogle検索してみてください。

御社では従業員に情報セキュリティ教育を実施していますか？

セキュリティ対策については
どうでしょう？

（もちろん、やってますよね）

では、ラックが２月に発表している

DNSプロトコルを使用する事案への注意喚起

http://www.lac.co.jp/security/alert/2016/02/01_alert_01.html

についてはご存知ですか？

セキュリティ対策で一番気を付けるべきは、

思い込みです。

入口・出口対策は既にやっている。（という思い込み）
ウィルスなんてシステムが検知してくれる。（という思い込み）
従業員はexeなんて実行するわけない。（という思い込み）
従業員はセキュリティについてわかっている。（という思い込み）
対策は業者に任せているから大丈夫。（という思い込み）

etosetora,etosetora・・・

悲しいかな、万全のセキュリティ対策や
イザという時の対応には、兎にも角にも、

お金がかかります。

せめて、お金がかからない対策くらいは
しっかりやっておきましょう。

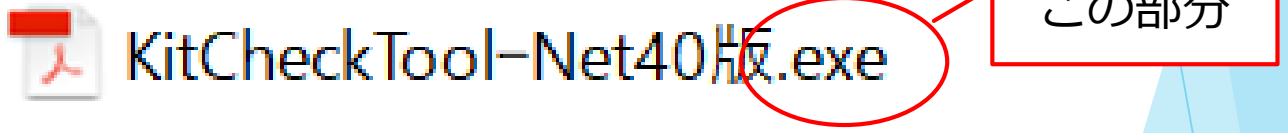
これだけはやっておこう！　その１

会社のドメイン名の管理者情報は
（whois データベースは）
常に最新にしておこう。

＜理由＞
情報漏えいや不正な通信が発見された場合、
警察などが御社への連絡先として参照するから。

これだけはやっておこう！　その２

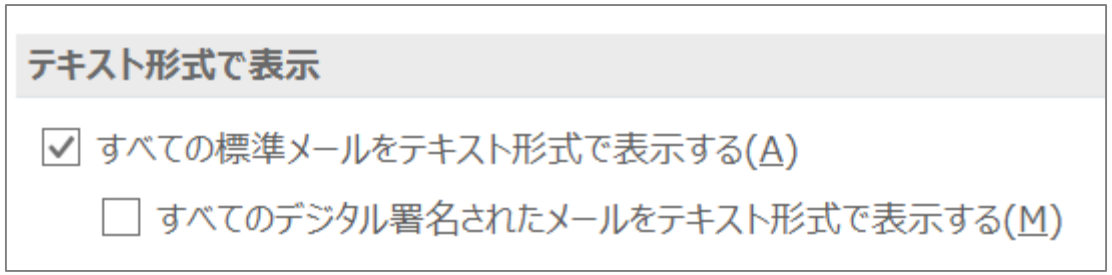
ファイルの拡張子は「表示する」
設定にしておこう。



＜理由＞
ファイルの拡張子がわからないと、
マルウェアかどうかの見分けがつかなくなるから。

これだけはやっておこう！　その３

HTMLメールは、標準では
テキスト形式で表示されるよう
設定しておこう。



＜理由＞
URL偽装に気づきやすくなるなど、
HTMLを悪用した攻撃を回避することができるから。

これだけはやっておこう！　その４

ExcelやWordなどの拡張子は
OpenOfficeなどのOffice代替製品に
紐づけておこう。（可能であれば）

＜理由＞
Office代替製品ではマクロ（VBA）が動かないので、
万一、不正なマクロが混入されていても、
マクロの実行を回避できるから。

これだけはやっておこう！　その５

Windows10へのアップグレードを
早急に検討しよう。

＜理由＞
Windows10では設計の根本的な見直しによって
セキュリティ対策が強化されており、
Windows7では防げない攻撃が防げるから。

他にも今すぐにできることは沢山あります。
その他の対策について知りたい方は、
キットのWebサイトまでお越しください。

https://kit.happyexcelproject.com/

自社内製での
標的型メール訓練実施を応援します！

標的型攻撃メール
対応訓練実施キット