【大学情報セキュリティ研究講習会】

JPCERT/CC IT セキュリティ予防接種に関して

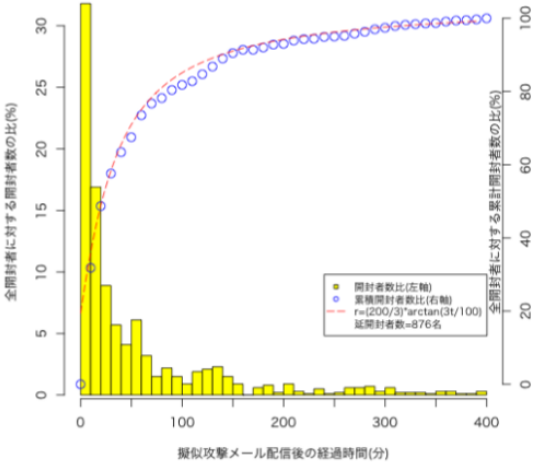
2018年 8月23日

JPCERT/CC
早期警戒グループ 洞田 慎一

JPCERT/CC ITセキュリティ予防接種

- 擬似的な標的型メール攻撃によるエンドユーザへのセキュリティ向上を図るトレーニング (予防接種）について調査を実施 (2011年度報告)
  【引用】JPCERT/CC, “IT セキュリティ予防接種調査報告書 2009年度”, https://www.jpcert.or.jp/research/inoculation2009.html

- 調査結果概要
  - 予防接種による短期的な効果
    - ２週間の感覚で擬似攻撃メールを配信
    - ２回目開封率の低下
  - 予防接種による長期的効果
    - ２年間の経年変化をみると非開封率が増加
    - 経験者は未経験者に比べ開封率が低くなる傾向
  - 「永遠のメール初心者」層
  - 配信から３０分以内に開封される



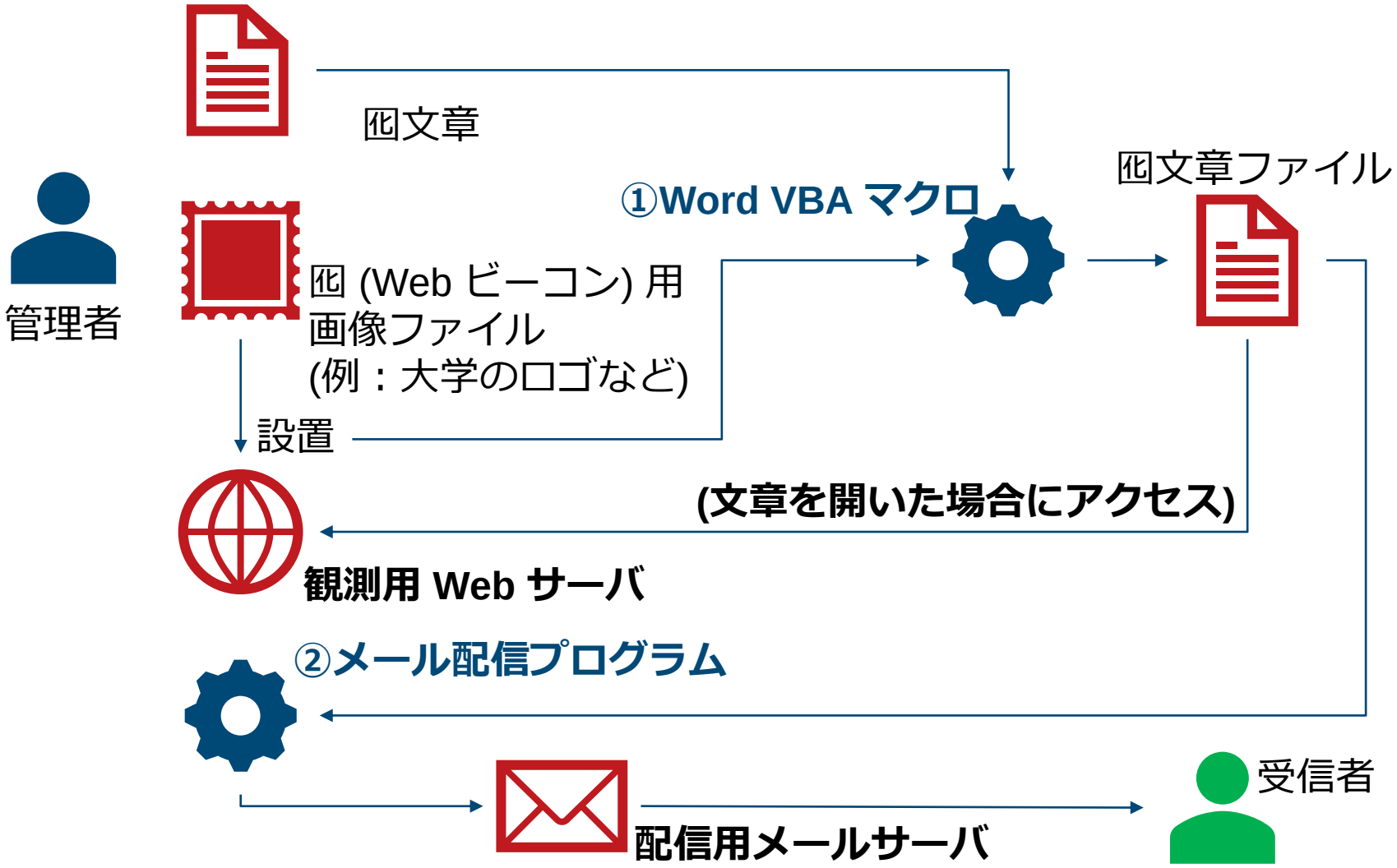
予防接種ツールの提供

- 予防接種に関する事業は終了しているため、個別のサポートはできませんが、実験に用いたツール (擬似攻撃メール配信ツール) を提供することは可能です
  - 最近では複数の事業者から擬似攻撃メール訓練のソリューションが提供されていますので、お付き合いのあるベンダに相談をしてみてください

- 利用する上では、ネットワークやシステム、プログラムに関する知識が必要です
  - メール (SMTP, POP3等) サーバや Web サーバを準備できること
  - Python2.x のプログラム知識があり、プログラムを適宜修正できること

ツールを用いた擬似攻撃メール演習概要

システム全体概要

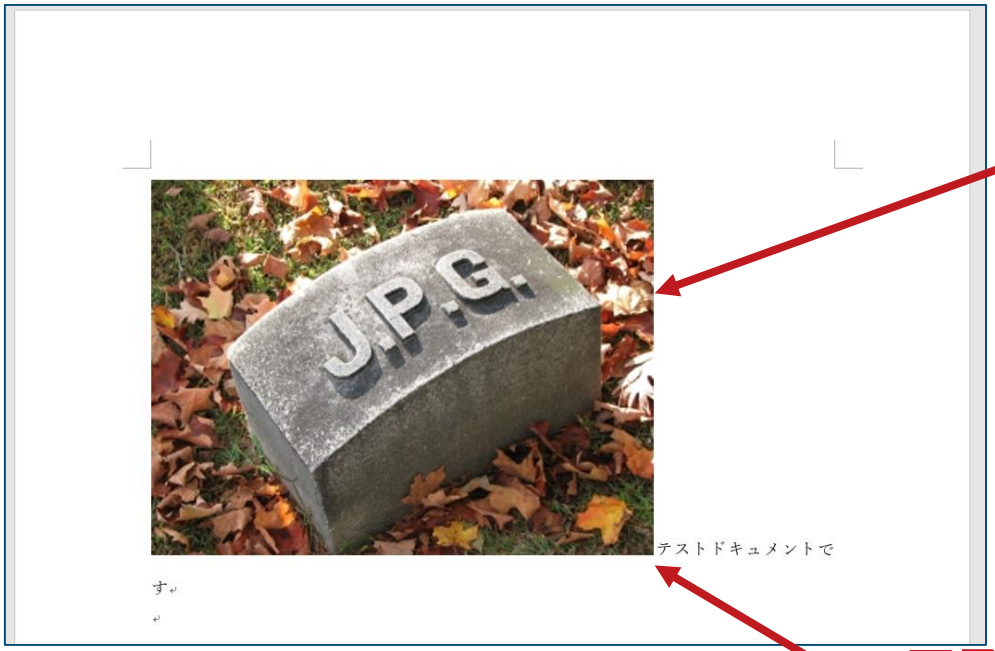


① Word VBA マクロ “BeaconSeeder.vba”

- Microsoft Word のマクロとして動作
  - Microsoft Office 2003 以上、Microsoft Office 2016 では動作することを確認
- 準備するもの
  - 囮文章 (教育用コンテンツ）の入った文書ファイル
  - Web ビーコン画像を作成し、あらかじめ観測用 Web サーバに格納しておく
- 出力されるもの
  - Web ビーコンが納められた囮文章ファイル
    （文頭に差し込まれるので、ヘッダ的な画像あるいは差し込んだ際に違和感の少ない画像が適する）

Web ビーコンが仕込まれた囮文章の例

- BeaconSeeder.vbaにより次のようなファイルが出力される



実際には、観測用
Web サーバ上の画像

マスターファイルの文頭に
イメージが差し込まれる

- このファイルをユーザが開くことにより、誰がいつ、ファイルを開いたかがわかる (Web サーバのアクセスログから)

②メール配信プログラム “massmailer.py”

- Python2 系のプログラムとして動作
  - Windows 版の Python 2.5 にて動作
  - Debian 9 上の Python 2.7 で動作を確認
    (※ ただしプログラムの一部に改変が必要。Unicode 変換時と、smtplib のconnect時)

- 準備するもの
  - ①のプログラムで作った囮文章ファイル
  - メール本文テキスト
  - 送信者リストを記載したCSVファイル (Unicode)
  - SMTP サーバ
  - 各種サーバの時刻はあらかじめ同期をとっておくと確認の際に時系列での比較が容易となります

送信者リスト CSV ファイル

- 送信者リストファイルの概要

便宜上折り返していますが、一行です

Horata,horata@example.com, ← **受信者情報**

System,root@example.com, ← **送信者情報**

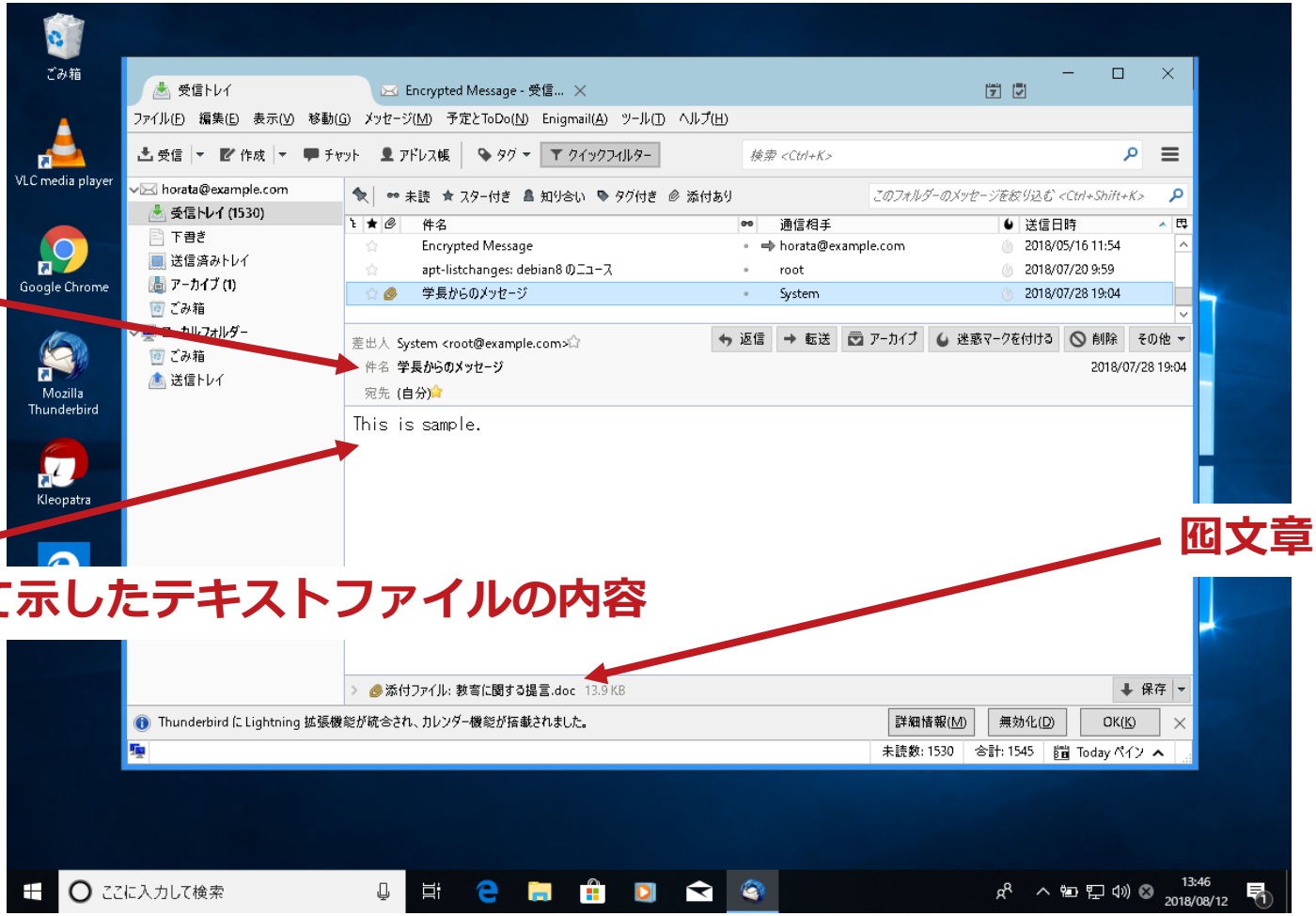
学長からのメッセージ,body.txt,教育に関する提言.doc

↑ **Subject** ↑ **本文 (body)** ↑ **添付ファイル名**

- CSV ファイルを準備してプログラムを動作させると順次メールを配送していきます

受信者イメージ

- 通常のメールとして受信する



最後に

- 開封率を低くすることだけに気を取られない
- 報告率を高くすることも注意
- 内容にあまり凝りすぎない。不審に思った利用者が、囮文章やファイルがそのまま VirusTotal に登録したり、IPAやJPCERT/CCに報告したりすることもあります

- メールセキュリティ対策への施策
  - 機械的に分かるメールはふるい落とす
    - DMARC などの技術の活用
  - ユーザが普段どの手段でメールを読んでいるかの理解
    - 外部メールサーバへの転送など
  - ユーザによる不審なメールの切り分け
    - どうやって不審なメールに気が付くか？
    - 秘書の存在

【参考】不審なメールの例

このメール怪しいけど、見てもらえない？

- **標的型攻撃マルウエアの**
  スピアフィッシングに用いたメール・添付ファイル

Daserf（重要インフラ事業者、その関連事業者）

水飲み場攻撃の場合もあるが…
- クリスマス、正月時期のお祝いメールなど
- 添付ファイル「新年アニメーション.exe」など

引用：LAC Cyber Grid View vol.2
https://www.lac.co.jp/lacwatch/pdf/20160802_cgview_vol2_a001t.pdf

このメール怪しいけど、見てもらえない？

- **標的型攻撃マルウエアの**
  スピアフィッシングに用いたメール・添付ファイル

Asurex（富山大学[正式な asurex への感染発表はなし]）

2016/04/18 (月) 15:11

[redacted]@yahoo.co.jp

[redacted]先生、早稲田大学の[redacted]と申します。

宛先 [redacted]ac.jp

画像をダウンロードするには、ここをクリックします。プライバシー保護を促進するため、メッセージ内の画像は自動的にはダウンロードされません。

メッセージ　document.zip (15 KB)

こんにちは、先生。
前回の学会でお目にかかった[redacted]と申します。
学会では短い時間お話ししただけですが、ずっと尊敬に思っていた先生にお会いすることができてすごく嬉しかったです。
実は、僕が今研究しているプロゼックトに関して少しお伺いしたいことがありまして失礼ながらもメールお送りします。
詳細な質問は添付いたします。
この分野に詳しい先生から僕のプロゼックトについてご意見を伺いできればこれからの研究に大きな力になると思います。
お忙しいなか、突然のメールで申し訳ございませんが、何卒よろしくお願いいたします。
ありがとうございます。

早稲田大学 [redacted]
[redacted]@yahoo.co.jp

引用：(n)inja csirt　富山大学 水素同位体科学研究センターへの攻撃に利用された通信先調査メモ
https://csirt.ninja/?p=932

このメール怪しいけど、見てもらえない？

- **標的型攻撃マルウエアのスピアフィッシングに用いたメール・添付ファイル**

Chches（日米関係や国際問題、外交などの機関及びそのサプライチェーン）

ファイル名
日米拡大抑止協議
潮１２月号
日米関係重要事項一覧表
ロシア歴史協会の設立と「単一」国史教科書の作成
安全保障条約変更通知
平成29年日米安保戦略対話提言(未定稿)
11月新学而会
保障関係団体要望と回答
２０１６新大統領の下での米国の経済・外交安保政策
２１世紀における日米同盟の展望
【H29科研費】繰越申請について

【今回確認されたメール】
========= ここから
差出人： xxxxxxxx@gmail.com
件名：【H29科研費】繰越申請について
添付ファイル：【H29科研費】繰越申請について.zip

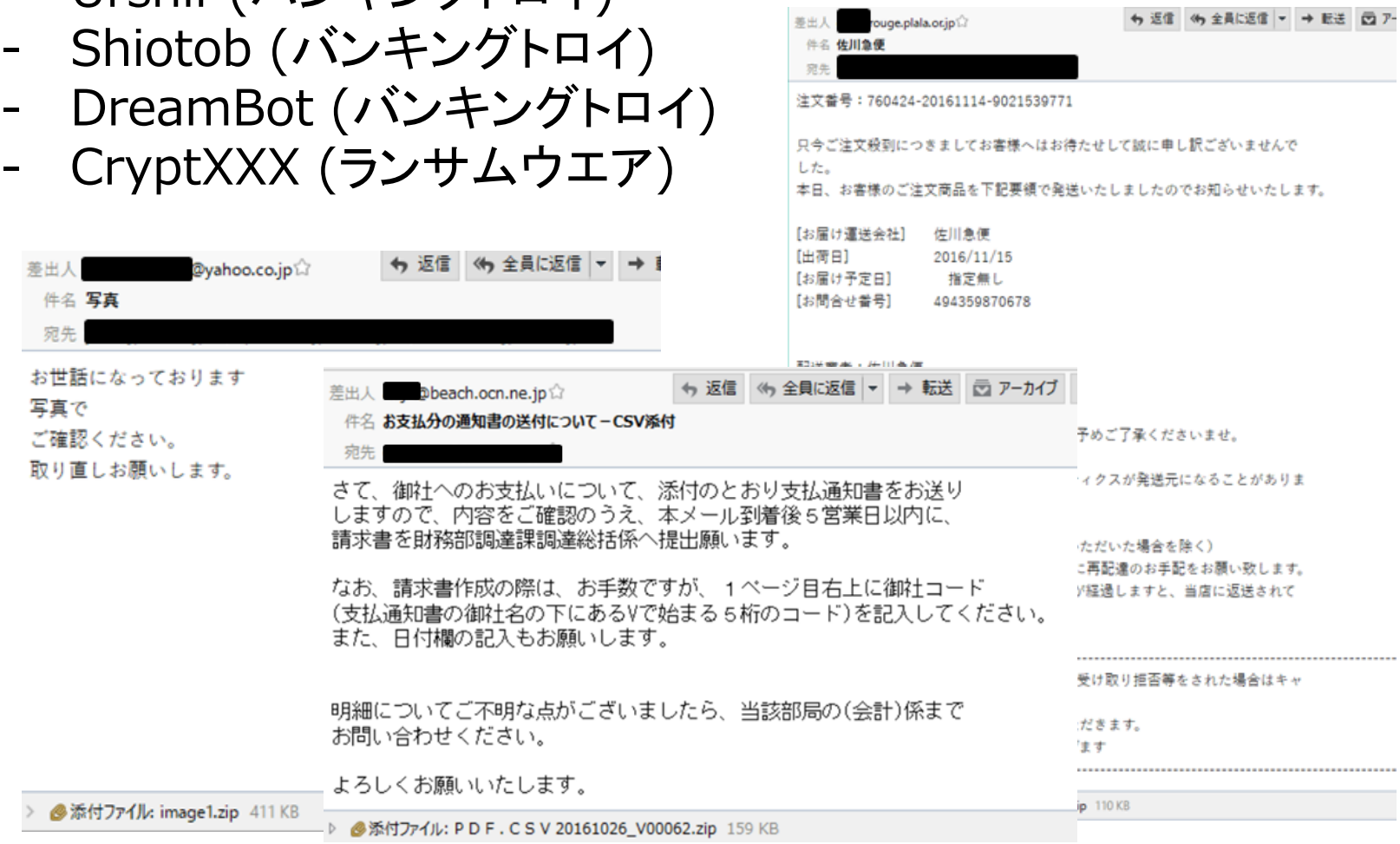
お世話になっております。
今年度の科学研究費助成事業（科学研究費補助金）の
繰越についてお知らせいたします。
翌年度に繰り越すことができるのは、計画の変更等に伴い当該年度中に使用することができなかった科研費です。例えば、研究計画の終了後に余った科研費は、繰越の対象にはなりません。
■申請の有無についての回答期限
平成２９年１月２６日（木） １２時【厳守】
■○○係提出期限
平成２９年２月２日（木） １２時【厳守】
――――共通――――――――――――――――――――――――――――――――
※特別研究員奨励費の場合、最終年度の方は科研費を繰り越すことができません。
※基金化されている課題については、手続きなく繰越が可能です。
※他機関から配分を受けている分担金の場合、繰越申請は代表者の研究機関にて取りまとめます。締切は各所属機関によって違いますので、速やかに代表者の先生にご連絡ください。
ご不明な点がございましたら、○○係までご連絡くださいませ。
どうぞよろしくお願いいたします。

日本学術振興会 ○○係
○○ ○○
xxxx@jsps.go.jp
TEL：03-3263-xxxx
FAX：03-3221-xxxx
========= ここまで

引用：中央大学【注意喚起】日本学術振興会を装った不審なメールにご注意ください。
http://www.chuo-u.ac.jp/research/rd/grant/news/2017/01/51783/

このメール怪しいけど、見てもらえない？

- **スパムメール（ランサムウエア、情報窃取型マルウエア）**
  - Ursnif (バンキングトロイ)
  - Shiotob (バンキングトロイ)
  - DreamBot (バンキングトロイ)
  - CryptXXX (ランサムウエア)



【参考】標的型メール攻撃訓練を始める前に注意したいこと

背景

- **標的型メール攻撃の訓練メールが不審なメールとして、届けられたり、VirusTotal などのサービスを使って確認されていたりします。**
  - 利用者が「これは不審である！」と判断できていますが、大学の対応フローとしては大丈夫でしょうか？
  - 大学内で「不審なメールを受信したときのルールや手順」は共有されていますか？

- **標的型メール攻撃の訓練は、何を確認するための訓練なのかをまず考えてください。**
  - 利用者を騙すことが目的でしょうか？
  - 目的は様々考えられます。
    - 例１）不審なメールの文章に触れてもらい利用者に勘を養ってもらう
    - 例２）不審なメールが届いた場合のルールを利用者に確認してもらう

- **想像するよりも多く、ユーザはメールに添付されたファイルを開き、リンク先にアクセスしています。（つまり感染等しています）**
  - 情報系センターに届出がないから何もおきていない、と果たしていえるでしょうか？
    - そもそもフローがない・理解されていないということはないですか？
  - 利用者はメールにアクセスしてしまう、自分自身で解決をしようとする（放置する場合も含め）、ということを前提とした対策を考えることが望ましいのが現状です。

どんなことに注意して訓練をすればよいか？

- **基本的には、他の訓練と同じです**
  - **「訓練」**
    - ①実際にあることを行って習熟させること
    - ②**一定の目標に到達させるため**の実践的教育活動
  - 「演習」
    - ①物事に習熟するために練習を行うこと
    - ②軍隊・艦隊などが**実戦の状況を想定して行う**訓練
  - みなさんが行いたいのは、演習ですか？訓練ですか？

- **消火「演習」ですか？、それとも避難「訓練」ですか？**
  - では、避難訓練の際に、どのような手続き、段取りで行っていますか？
  - 「わかりきっていることだから・・・」ではないはずです

演習の例

- **セキュリティ演習では、シナリオに沿って逐次に状況をインプットする「テーブルトークRPG(TRPG)」が多く見られる (参考: JNSA CISO ハンドブック)**

- **シナリオ例**
  - 事務局長、総務部長に文部科学省担当官からと見られる「（機密２）平成３１年度概算要求における私立大学研究ブランディング事業の後継事業に掛かるヒアリング」と題するメールが送られた
  - JPCERT/CC より早期警戒情報、文部科学省より悪性ドメインが記載されたインディケータ情報が発行され、情報基盤センターに届いた
  - 上述のインディケータ情報を大学が委託するベンダーに確認を依頼したところ大学のDNSサーバの通信履歴に悪性ドメインと見られるドメインの名前解決が行われた痕跡が見つかった
  - 文部科学省からの追加の情報があり、文部科学省を騙る「（機密２）平成３１年度概算要求における私立大学研究ブランディング事業の後継事業に掛かるヒアリング」という題目を持った標的型メール攻撃に関する注意喚起が発行された
  - さあ、インシデント対応を始めてください！準備はできていますか？必要な分析技術は分析コースで習得しているはずです

- **標的型攻撃メール訓練と、上述の演習は同じですか？違いますか？**
  - 同じだとする方は、どこが同じですか？
  - 違うとする方は、どこが違いますか？

標的型メール攻撃訓練と避難訓練との比較

- **避難訓練**
  - 事前に日程を知らせ、どう行動するか、どのマニュアルを参照するか、誰がどの役割を担うかはすでに「決まっている」
  - 「決まっていること」を「決まっているとおりに」できるかどうかを確認している
  - どのくらいの時間をかけて「それができるのか」を「計測している」
  - 本部長に「総員○名避難完了しました」と報告するまでが、避難訓練
- **標的型メール攻撃訓練**
  - これと同じように考えてみてください
  - 火元は？原因は？誰がどのように行動するべき？マニュアルは？問い合わせは？完了は？何を計測する？

標的型メール攻撃訓練

- **そもそものルールを明らかにしておく**
  - メールを受け取ったとき、どう行動するべきか
    - ユーザのリテラシー任せ？
    - ユーザに何らかの実施手順がある？
    - 実施手順があるとしたら、通常業務（教育・研究・事務）との調整はできていますか？
  - 不審なメールを受け取ったとき、どう行動するべきか？
    - 連絡手段は？そもそも誰に相談？
    - 「あー、やっぱりあいつ開いてるよ」と影でコソコソすることは「やってはいけないこと」です。しっかりと「統括班として機能しましょう」
  - そのために事前にポリシーと実施手順が必要なのです
- **行う日程、対象を明らかにしておく**
  - 大事なことは事前に決めたとおりに行動できるか？ということです。
  - 小学生のころから身に染み付いているからこそ、今でもこの瞬間で火災が起きてもどうしなければならないか理解していて、行動できるはずです
- **火元や原因は明確にする**
  - あらかじめ「このようなメールが送られます」と予定を示してもよいということです。
  - 「だますことが本質ではなく、決められた手続きどおりに実施できるか」が本質です
- **どう行動したらよいか、ゴールを決める**
  - 最終的に、この訓練のゴールは、どうなったらよいのでしょう？
    - 関係者が不審なメールを開かなければよい？
    - どうしても職務上開かなければならない人はどうする？
  - どうなることがよいかは大学によって異なる
    - 絶対にエラーは許さないパーフェクトを目指す校風なのか、エラーがあっても速やかな回復ができるレジリエンスを目指す校風なのか、戦略によって大きく異なります
    - どれがよいかは、一概には言えません

実施例

- 3通のメールを使う例
  - １通目：　**（事前に訓練であることを通知）**
    - 件名：【情報基盤センターからのお知らせ】メール訓練に関するお知らせ
    - 内容
      各位
      本学では、学長裁定によりメール訓練を行うこととなりました。
      情報基盤センターより、○月○日に訓練としての不審なメールを配布します。訓練メールを受け取った方は、情報セキュリティポリシーに従い適切な行動を図ってください
  - ２通目：**（明らかにおかしいことがわかるような内容で十分。内容はなんでもよい）**
    - 件名：＊情報基盤センターからのお知らせ/訓練＊利用状況調査
    - 内容：
      親愛なるユーザ
      大学（だいがく、英: college、university）は、学術研究および教育における高等教育機関である。日本の現在の学校教育制度では、高等学校もしくは中等教育学校卒業者、通常の課程による12年の特別教育を修了した者、またはこれと同等以上の学力を有する者を対象に専門的な高等教育を行うものとされている。学生の教育課程と修了要件の充足に応じて学位（短期大学士、学士、修士、専門職学位、博士）の学位授与を行う（なお、学位の名称・定義も国や地域によって異なる）。
      添付：学長信息.doc
  - ３通目：　**（インジェクションをするとともに効果の回収を計る）**
    - 件名：【情報基盤センターからのお知らせ】不審なメールに関する連絡（訓練）
    - 内容：
      各位
      情報基盤センターより、訓練メールを送りました。
      件名：＊情報基盤センターからのお知らせ/訓練＊利用状況調査
      訓練にご協力いただきありがとうございました。今回の訓練につきましてアンケートを実施しています。いただいた結果は、情報セキュリティ委員会にて検討します。

実際のインシデントにおいて気にしてほしいこと

- **ユーザにヒアリングする際には叱らない、コソコソ面白がらないように注意する**
  - 開いてしまったことを面白がったり恥をかかせることが目的ではありません
    - 逆に利用者との間で不信感が芽生える可能性も考えられます。
    - 「インシデントを起こすことが恥ずかしいこと」につながり、「隠す」ことにつながってしまうことも考えられます
  - 実際のインシデント調査において、ユーザの協力は不可欠です

- **ルール・手続きは常にブレークする**
  - 「人は易きに流れる」
  - 業務上、ルールの解釈の変更や例外の設定は起こりうること
    - ただし、そうすることで、インシデント調査の際に「どうしてこんなことが」と想定外の自体を招く可能性があります
  - 実情にあったルールや手続きを心がけ、一度決めたルールも直していくことを考える

- **想像してほしいこと**
  - いまこの瞬間に扉を開けたら、いきなり武装したテロリストが乱入したとします、この空間では何が起こりますか？
    - ルールや手続きが決められていない中でのパニックの発生
  - パニックを発生させないためにも、コンティンジェンシー・プランを想定したルール作りや訓練が必要なのです