広島県庁事例紹介

県庁内における標的型攻撃メールによる感染と，その後のセキュリティ向上への取り組みについて

総務局　業務プロセス改革課
情報基盤グループ　西田　寛史

標的型攻撃メールからの感染

- 平成24年4月9日（月）
  保守員登庁時にアラートにより発覚。

メールの件名は「FW：【機2】対北朝鮮措置の延長について」
添付ファイル「対北朝鮮措置の延長について．zip」
送付時間は午前6時57分

メール本文内の送信者は実在する内閣府の所属名，担当者名および連絡先が記載されていた。

受信した標的型攻撃メール

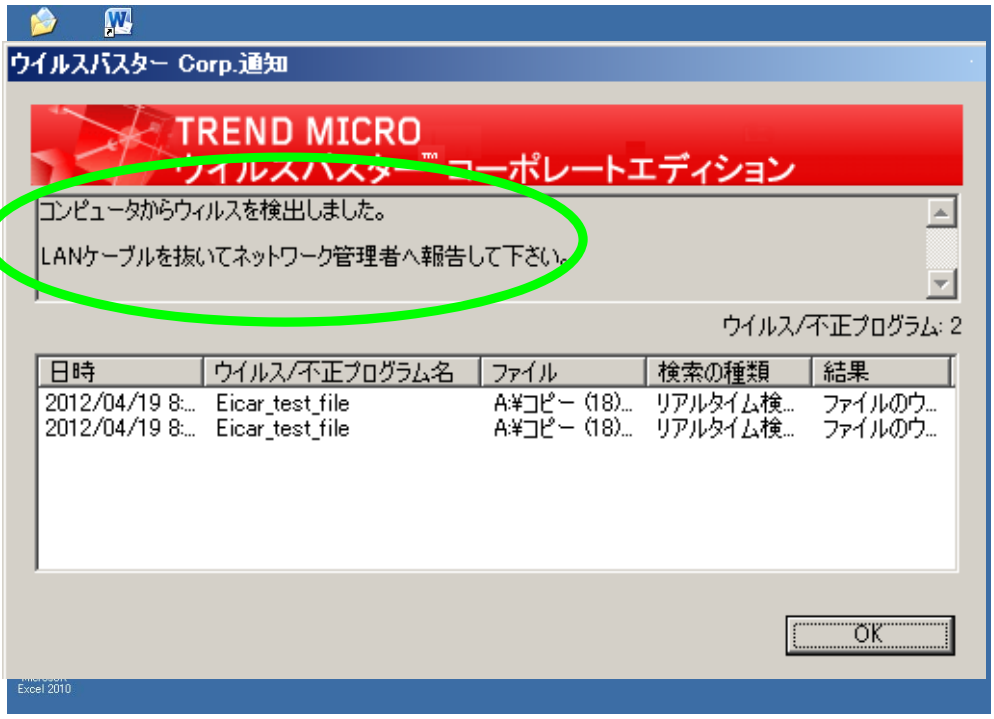
件　　名　Fw:【機2】対北朝鮮措置の延長について
差 出 人　XXXXXXX.XXXXXXXX@cao.go.jp
添付ファイル　対北朝鮮措置の延長について.zip
本文
>
>
>> 関係者各位
>>
>> 平素よりお世話になっております。
>> 標記についてお送りします。
>> 宜しくご査収ください。
>>
>> .....
>> 職員氏名（実在の職員）
>>　内閣府部署（実在の職員の所属）
>>　TEL：03－〇〇〇〇－〇〇〇〇（内〇〇〇〇〇）
>>　　03－〇〇〇〇－〇〇〇〇（直通）
>>　FAX：03－〇〇〇〇－〇〇〇〇
>>　E-mail：XXXXXXX.XXXXXXXX@cao.go.jp
>>
>> .....

内閣府の実在する人物・所属
連絡先も実在するもの

感染経緯・時系列

- 平成24年4月5日（木）午前　庁内所属アドレス宛にメール着信。職員1名が開封し，添付ファイルを展開して感染も，この時点ではゼロデイのため検知せず。
- 平成24年4月5日午後　上記同一所属の別職員1名が開封し，添付ファイルを展開して感染。
- 平成24年4月5日午後　総務省自治行政局情報政策室から注意喚起のメールを受信。同日，職員への注意喚起を実施。
- 平成24年4月6日（金）夕方　感染したウイルスに対するパターンファイル更新。
- 平成24年4月7日（土）午前　感染した職員1名が休日出勤。端末起動時にウイルス対策ソフトからのアラート画面が表示されるも，無視して業務継続。
- 平成24年4月9日（月）午前　感染した職員もう1名が出勤。端末起動時にウイルス対策ソフトからのアラート画面が表示されるも，無視して業務継続。
- 平成24年4月9日（月）午前8時30分　登庁した運用SEがウイルス対策ソフトからのアラートを発見。当課に連絡後，当課より該当者2名にLANケーブルを抜くよう指示。PC回収。

感染時警告画面



感染経緯・時系列その2

- FWのログから，中国のアドレスにHTTPS通信（添付ファイル開封時）していることが確認されたが，通信時間及び通信内容については確認できなかった。

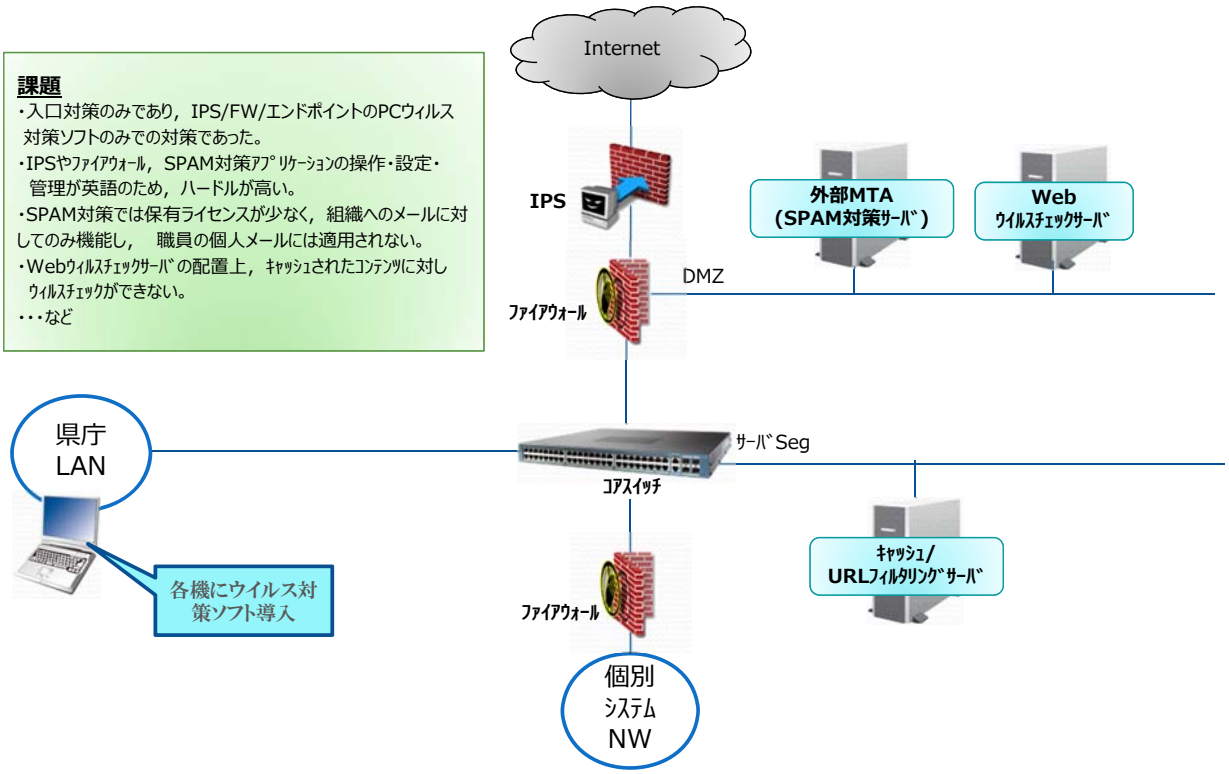
  しかし，バックドア系のウイルスであったこと，通信は1回であったことから，実行命令はされていないと推測された。

- 平成24年4月9日夕方　上記感染について記者発表。（全国的事例であったため。）
- 平成24年4月10日午前　通信解析業者に相談。解析を依頼。
- 平成24年4月11日　解析業者に検体を送付。
- 約1週間後　解析業者から回答。通信は微量であり，1回のみの通信のため情報漏えいの可能性は極めて低く，具体的な漏えいは無かったとの回答。

結果的に事なきを得たが，改めて通信ログの追跡，脅威の可視化の必要性を痛感した。

改修以前の技術的対策状況

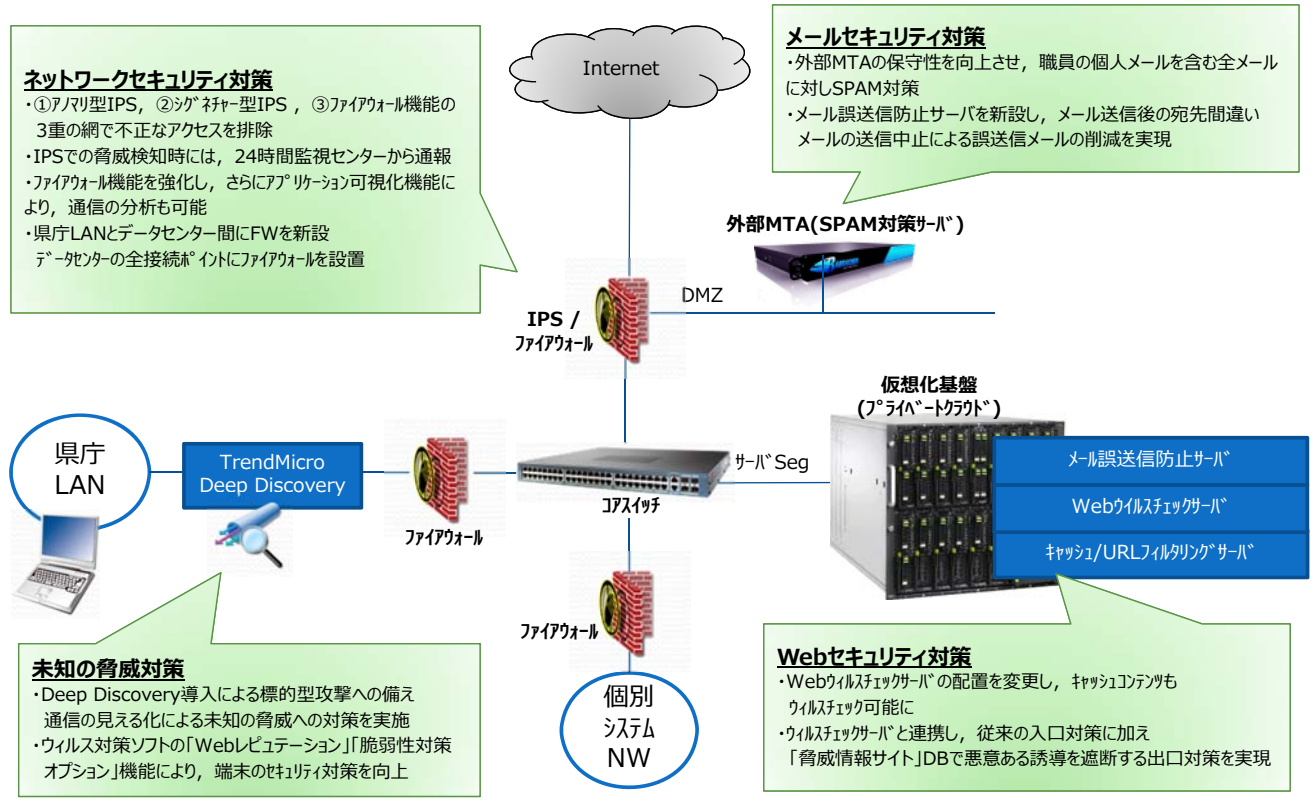
課題
・入口対策のみであり，IPS/FW/エンドポイントのPCウィルス対策ソフトのみでの対策であった。
・IPSやﾌｧｲｱｳｫｰﾙ，SPAM対策ｱﾌﾟﾘｹｰｼｮﾝの操作・設定・管理が英語のため，ハードルが高い。
・SPAM対策では保有ライセンスが少なく，組織へのメールに対してのみ機能し，　職員の個人メールには適用されない。
・Webｳｨﾙｽﾁｪｯｸｻｰﾊﾞの配置上，ｷｬｯｼｭされたｺﾝﾃﾝﾂに対しｳｨﾙｽﾁｪｯｸができない。
・・・など



改修後の技術的対策状況１

ネットワークセキュリティ対策
・①ｱﾉﾏﾘ型IPS，②ｼｸﾞﾈﾁｬｰ型IPS，③ﾌｧｲｱｳｫｰﾙ機能の3重の網で不正なアクセスを排除
・IPSでの脅威検知時には，24時間監視センターから通報
・ﾌｧｲｱｳｫｰﾙ機能を強化し，さらにｱﾌﾟﾘｹｰｼｮﾝ可視化機能により，通信の分析も可能
・県庁LANとデータセンター間にFWを新設
ﾃﾞｰﾀｾﾝﾀｰの全接続ﾎﾟｲﾝﾄにﾌｧｲｱｳｫｰﾙを設置

メールセキュリティ対策
・外部MTAの保守性を向上させ，職員の個人メールを含む全メールに対しSPAM対策
・メール誤送信防止サーバを新設し，メール送信後の宛先間違いメールの送信中止による誤送信メールの削減を実現



未知の脅威対策
・Deep Discovery導入による標的型攻撃への備え
通信の見える化による未知の脅威への対策を実施
・ウィルス対策ソフトの「Webレピュテーション」「脆弱性対策オプション」機能により，端末のｾｷｭﾘﾃｨ対策を向上

Webセキュリティ対策
・Webｳｨﾙｽﾁｪｯｸｻｰﾊﾞの配置を変更し，ｷｬｯｼｭｺﾝﾃﾝﾂもｳｨﾙｽﾁｪｯｸ可能に
・ｳｨﾙｽﾁｪｯｸｻｰﾊﾞと連携し，従来の入口対策に加え「脅威情報サイト」DBで悪意ある誘導を遮断する出口対策を実現

改修後の技術的対策状況2（DDI）

ネットワークをモニタリングし、脅威を分析　Deep　Discovery　Inspector　の導入

1. 入口対策

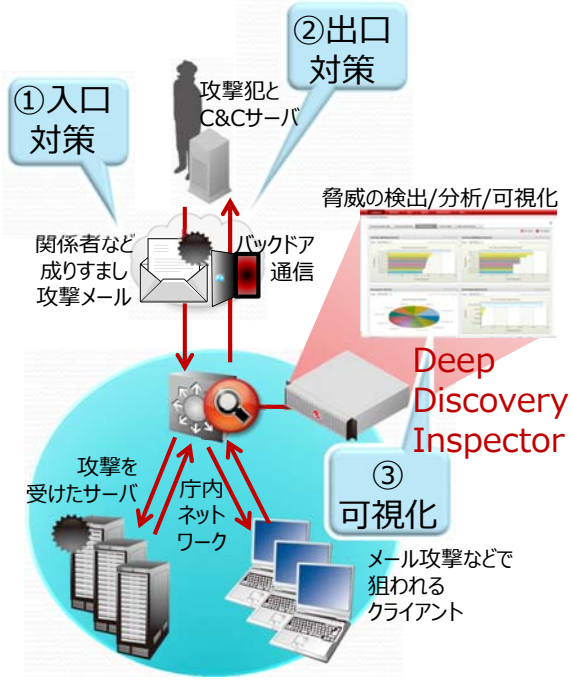
- ルールベースでのNetwork検出とヒューリスティックルールによる検出、仮想環境を用いた動的解析の「多段解析」により、効率よく脅威を分析
- プロトコルを幅広くカバレッジすることで、多様な攻撃に対応

2. 出口対策

- 入り込んだ脅威が、バックドアを通じて外部サーバと通信し、攻撃を悪化させる様子をネットワークモニタリングで検出

3. 脅威の可視化

- 今起こっている脅威状況を、グラフィカルなウィジェットを用いて把握
- 長期にわたるログを分析したレポートを待つことなく、脅威に気付き、対応を行うことが可能



1．入口対策（DDI）

脅威に対する多面的分析による検出

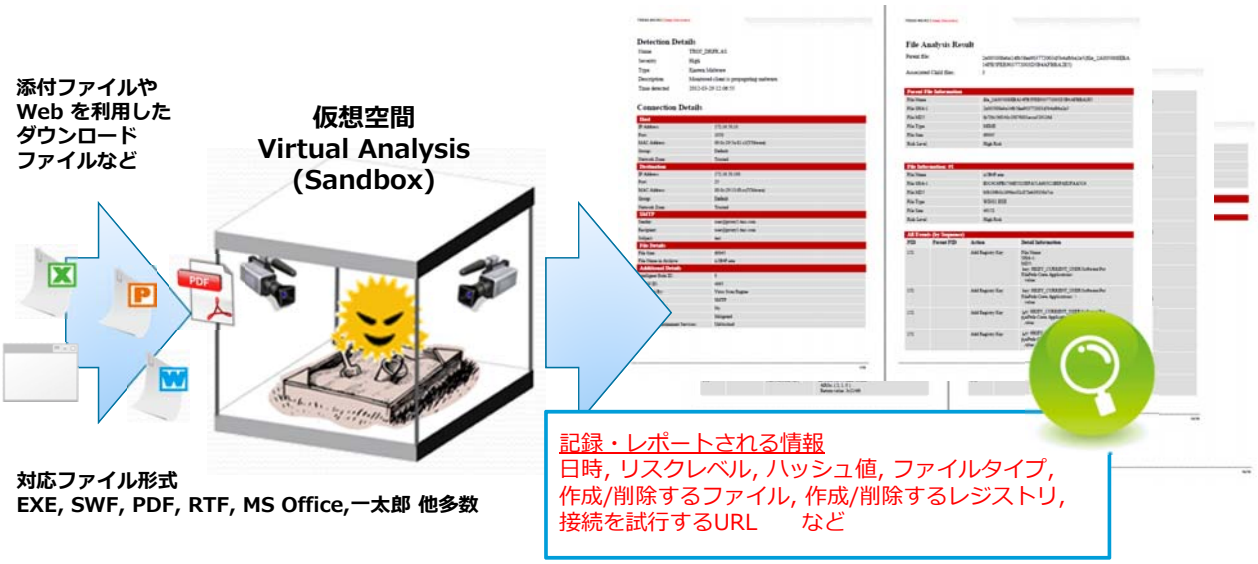
- **ルールに基づく、複数ロジックを用いた脅威解析**
  - 多面的な分析の結果、問題ないと判断されたファイルはこの時点で終了
  - 脆弱性攻撃と思われる不審なファイルのみが、次のプロセスである動的解析(Sandbox)へ送られる

- **仮想空間で実際に実行し、その結果や振る舞いの観察に基づいた脅威分析**
  - まずは仮想空間で問題のファイルを実行し、その結果得られる情報を収集
  - その結果を用いた相関分析を行い、最終的にどのような影響を及ぼすものかを判断
  - 新たな脅威の場合、ルールを静的解析にフィードバック

仮想アナライザによる動的解析の実施

不正ファイルや不正プログラムに類似する特徴を有する不審なデータを仮想空間（Sandboxシステム）で実行することで，実行によって生じるプロセス動作やシステム変更などの情報を確認し，該当データと共に保存します。

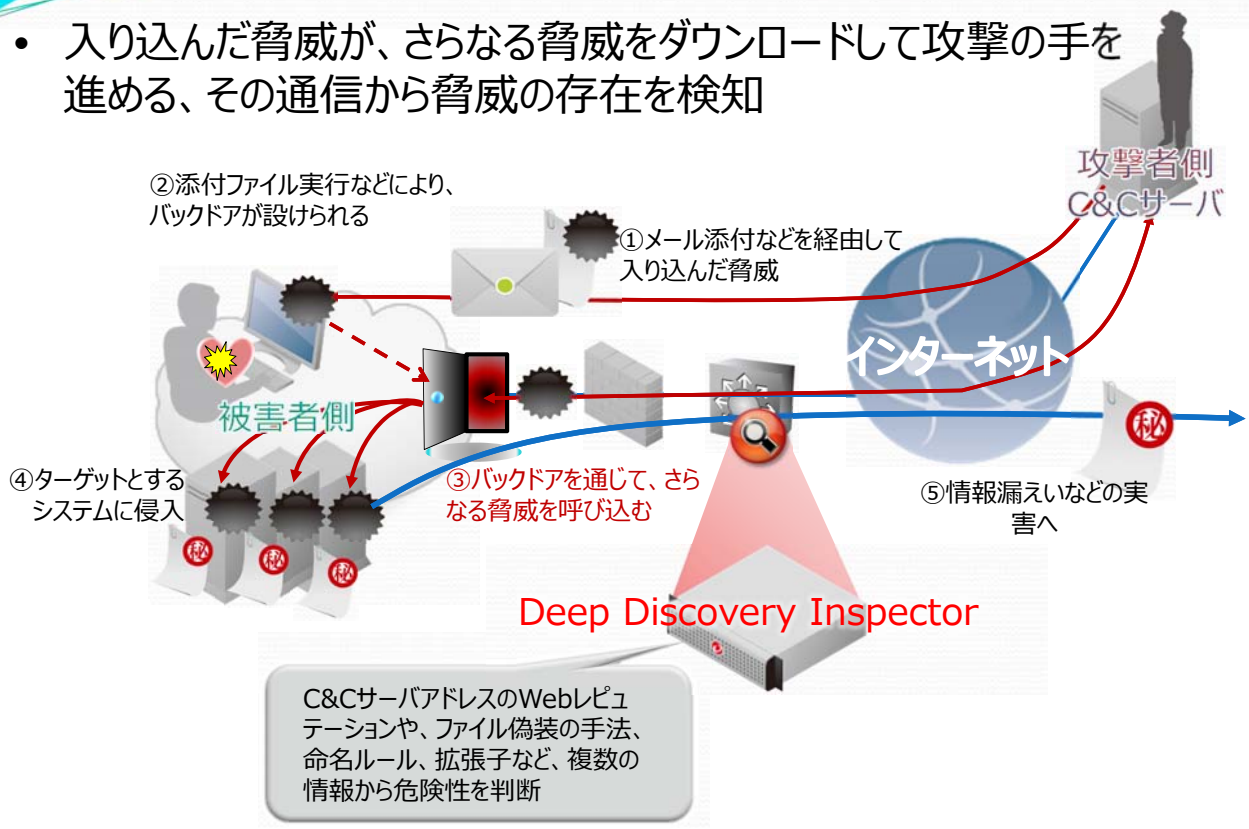
これにより，リスクレベルの高いデータ（不正プログラムの可能性のあるデータ）の確認，回収が容易となります。



対応ファイル形式
EXE, SWF, PDF, RTF, MS Office,一太郎 他多数

2．出口対策（DDI）

- 入り込んだ脅威が、さらなる脅威をダウンロードして攻撃の手を進める、その通信から脅威の存在を検知



3. 脅威の可視化（DDI）

- さまざまな脅威表示ツール(ウィジェット)を用いて、オリジナルの管理画面を構築

- ログ解析レポートなどを待つことなく、今の脅威状況把握が可能に
  - 脅威へのすばやい対応が可能
  - インターネットを経由した、ログやファイル、メールなどの情報の送付不要
  - インターネットに直接つながっていない環境でも利用可能

さまざまなウィジェット群から・・・

お好みのダッシュボードに
カスタマイズ！

Deep Discovery Inspector等　セキュリティ向上製品導入のための工夫

・DDI，メール誤送信防止等，セキュリティ向上製品の導入は不可欠。

・ファイルサーバストレージの拡大，災害対策として遠隔地バックアップは不可欠。

予算確保はどうするか。

・サーバを仮想化させて経費の効率化を図った。

物理的に80台のサーバを25台に削減し，コスト削減

・別契約だった運用保守契約を統合し，経費の削減を実行。

前年度までの経費内で，求める構築をすることができた。

人的対策

- **人的セキュリティの向上**
  - 「技術対策だけではセキュリティは保てない」。
  - 最後は「個」。（ベネッセも同様）
  - 様々な啓発は行っているが，なかなか浸透しない。
- **訓練メールの実施**
  - 模擬メールによる訓練を実施。
  - 「予算が無い」は理由にならない。
  - 運用SEやサポートダイヤルに協力してもらい，自前で訓練模擬メールを作成。
  - 開封者の情報から背景や経緯など多角的な分析を継続。

実際に攻撃者が存在する以上，
こちらも継続して対策が必要。

・職員の教育・意識向上。
・インシデントを風化させない。

標的型攻撃メールの訓練

＜差出人＞
自治体情報ジャーナル[k-sakai@lg.gmail.jp]

＜宛先（BCCによる）＞
「標的型攻撃メール対処訓練模擬メール宛先（個人アドレス）」

＜件名＞
取材のお願い

＜添付ファイル＞
履歴書.zip

＜文面＞
広島県　ご担当者様

いつもお世話におります。
自治体情報ジャーナル 酒井和義です。

私、行政・公共編集グループの記者をしております。
先日、依頼した件で更なる広島県の各種取組みを
取材依頼をお願いしたくご連絡いたしました。

私のプロフィールをお送りいたしますので、
ご確認ください。

よろしくお願いいたします。

¥¥
自治体情報ジャーナル
酒井 和義
tel:(082) 228-2152
mail: k-sakai@lg.gmail.jp
¥¥

訓練メール（例）

この添付ファイルをクリックすると・・・。

不審な添付ファイルを開いたら即連絡！
絶対に放置しない！

あなたが，開いたメール・添付ファイルは，行政管理課が，
「標的型攻撃メール対処訓練」のため送付した「模擬メール」です。

今回は，ウイルス感染しません。※1
しかしながら，今回のメールのように，あなたの知らない相手から唐突に送られてきたメールが，本当の攻撃メールだったら，情報漏えいやネットワーク障害が生じた可能性がありました。※2

※1 取りまとめのため，誰がこのファイルを実行（開封）したかは，記録しています。
※2 広島県は標的型攻撃メールを受けており，今回と同様に添付ファイルを開いた事で情報流出を試みる新型のウイルスに感染します。しかも，新型ウイルスは，ウイルス対策ソフトでは対応できません。ウイルスの多くは，画面に変化を起こさず情報流出を行うため，職員が感染に気付かずに放置するケースが発生しています。
不審なメールの受信，添付ファイルを開いたら直ちに連絡をするようにしてください。

クリックしてください。

組織別開封率

- **添付ファイル開封率**

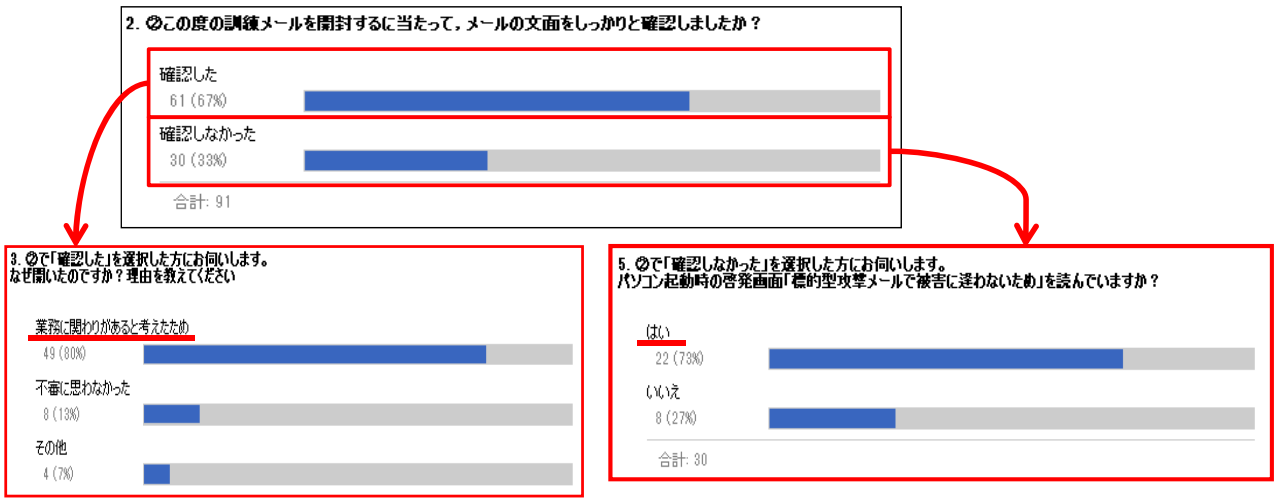
個人メール宛　5.7％　*前回と条件等を変更
前回　6.0％
前々回　12.7％

（　）内の数字は，個人メール宛は開封職員数を示す。

部　局　区　分	個人メール宛		
	今回	前回	前々回
テーマによって部局の開封率は変動する。（業務への関係度等）	4.0%（　3）	3.5%（　3）	15.6%（ 14）
	10.3%（　7）	16.4%（ 11）	16.4%（ 11）
	4.3%（ 54）	4.0%（ 50）	10.7%（134）
	8.0%（　9）	3.4%（　4）	6.3%（　7）
	11.9%（ 26）	9.8%（ 22）	13.7%（ 31）
	4.0%（ 42）	8.3%（ 86）	12.8%（129）
	11.3%（ 46）	4.5%（ 18）	17.8%（ 69）
	3.3%（ 30）	5.5%（ 49）	12.3%（108）
	6.0%（ 75）	6.5%（ 77）	12.9%（152）
	6.1%（　8）	8.0%（ 12）	9.9%（ 15）
	5.9%（　8）	4.3%（　5）	9.9%（ 11）
	3.4%（　2）	1.7%（　1）	18.6%（ 11）
	7.7%（ 43）	6.0%（ 30）	15.2%（ 83）
	5.2%（　4）	6.9%（　4）	10.2%（　6）
計	5.7%（357）	6.0%（372）	12.7%（781）

訓練結果

➢ アンケート結果



⇒ メールの文面を確認したが
業務の関わりがあると考え開く人が多い

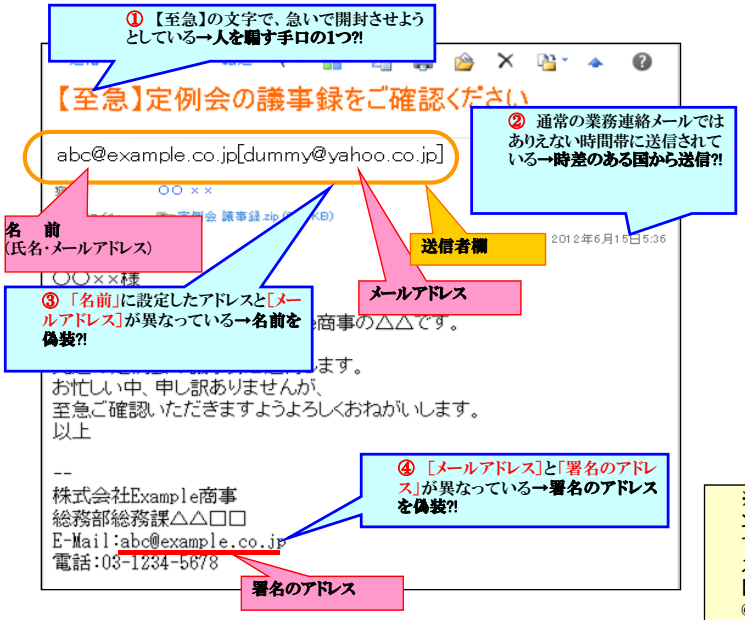
⇒ 啓発の内容は読まれているが，
実際は文面を確認できていない

アンケートにより感染の経緯や背景を分析し次回につなげる。

最大要因の人的セキュリティの向上は，継続して教育するしかない。

各種研修での啓発

【不審メールの例】



※　インターネット上では，登録に必要な事項（希望のアカウント，パスワードなど）を入力するだけでメールアドレスが無料で取得できるサービスが数多く提供されています。このサービスを利用したメールのことをフリーメールといいます。
【代表的なフリーメール】
@yahoo.co.jp，@yahoo.com，@hotmail.co.jp，@hotmail.com，@goo.jp，@mail.goo.ne.jp，@gmail.com，@infoseek.jp　など

定期的に朝の起動時にポップアップにより意識向上を図るための啓発画面を表示させています。

不審なメールには正しく対応しよう！

（不審なメールを受信したら･･･）

標的型攻撃メール：相手に添付ファイルを実行させ，外部に情報を漏えいさせます

明らかに不審なメールは相手にせずに，直ちにネットワーク管理者へ報告！！
判断が難しい場合は，まずは周囲に確認・相談するなど
個人で判断しないようにしてください
そのうえで，相手に電話で確認も行ってください

標的型攻撃メール訓練の職員の対応について

1　返信メールで開いてよいか確認する
⇒攻撃者の場合，開くように指示してきます。
電話で連絡することで，相手の組織，存在が確認できることから有効です。
2　外部アドレスへの転送
⇒被害の拡大や，広島県が加害者と見られる行動は慎んでください。
3　メールの内容を確認せずに添付ファイルを開いている
⇒メールの内容は必ず確認してください。
特に外部からのメールは必ず確認してください。

行政管理課　情報基盤G　内線2442

最後に

- **技術的対策はもちろん，人的セキュリティの向上**
  - 攻撃者は無くならない。→対策が必要。
  - 人的セキュリティの確保は必須要件。
  - 浸透は困難だが，工夫をして教育を継続する。
  - 「知らなかった（無知）」，「つい（無意識）」は理由にならない。
  - 必要ならば予算を確保してでも教育を行う。（本県では外部講師によるセキュリティ管理者を対象とした研修を実施。）→内部講師だけでは，対策の必要性や危機感を与えるには限界がある。
- **訓練模擬メールによる成果**
  - 題名，発信者，アドレス，発信時間への意識は向上している。
  - 所属セキュリティ管理者の責任感の向上。
  - 開封者アンケートから，開封への分析が可能。対策へフィードバックできる。（独自作成が無理でも予算があれば，外部の模擬訓練メール配信サービスを利用することも有効と思います。）