◇◇◇◇◇◇
解　説
◇◇◇◇◇◇

九州工業大学における標的型攻撃メール訓練の実施について

中村　豊[1]

1　はじめに

社会保険庁の情報漏洩事件をきっかけにして、特定の組織の情報を狙った標的型攻撃メールが注目されるようになった。標的型攻撃メールは、その組織の構成員宛にウィルスが添付された電子メールやURL 付きメールを送信するところから開始される。特に 2016 年に発生した JTB での情報漏洩事件では、攻撃か業務かの区別がつかないようなメールが送信されウィルス感染することで、最終的に約 700 万件近い個人情報の漏洩の可能性が報じられた。一度、ウィルス感染、情報漏洩発生という事象が起きると、経済的損失やブランド価値の毀損など非常に大きな問題となる。

九州工業大学情報基盤運用室では、2015 年度からこのような標的型攻撃メールを疑似送信し組織構成員の訓練を図るとともに、標的型攻撃メールへの啓蒙活動を行ってきた。実際の送信作業や偽装サイトの構築に関しては株式会社キューデンインフォコムの標的型攻撃メール訓練サービスを利用した。2015 年度に実施した訓練は最初のメール送信であったため、どの程度のデータが取得できるか？を主眼において訓練を行った。2016 年度では 2015 年度の結果を踏まえて、e-learning にアンケートを付加して、訓練者からの情報取得に努めた。本報告ではメール訓練に当たっての経緯、事前調査、準備事項、訓練結果などについて述べる。

2　事前準備、調査

キューデンインフォコムの標的型攻撃メール訓練サービスを用いて訓練を実施するに当たり、本学で事前に決めておかないといけない項目が複数存在する。以下にそれらの項目について述べる。

2.1　メール受信者の範囲の決定

予算との兼ね合いも考慮する必要があるが、メール受信者の範囲を広げると必要な予算は多くなる。限られた予算の範囲内で訓練を実施するために何名程度に対して訓練メールを送信するのか？を決定する必要がある。本学での訓練の場合、常勤職員および非常勤職員とした。非常勤講師は含まれていない。この理由は本学の教職員用ポータルサイトにおけるアカウント配布者と同等程度が望ましいという判断からである。実際のメール送信数は約 900 アカウントであった。

[1]情報基盤運用室　yutaka-n@isc.kyutech.ac.jp


ID管理者
2015年10月26日 15:01
宛先： 中村豊
【重要】認証IDシステムパスワード更新のお願い

※このメールは対象者にのみ自動送信しています。

認証IDシステムに登録されている、一部の利用者のパスワード情報が外部に
漏洩した疑いがあり、現在、影響範囲を調査中です。

このメールを受信した方は、悪意のある第三者に漏洩した情報を悪用される
恐れがありますので、以下のＵＲＬの手順に従って至急パスワードを更新して
ください。
（クリックすると手順が表示されます。）

http://hyo.imitapt-q.jp/password/password.html?wpmthJHp

図 1: 2015 年度の訓練メール文面

2.2 メール送信日時の決定

業務的な繁忙期は避け、かつ、情報セキュリティに対して意識を高めるために、本学で行っている「情報モラル向上週間」の期間中での実施とした。2015 年度の訓練では、登録されたアカウントへの一斉送信であったため、メール受信を不審に思った職員が他の職員に口頭で確認するなどの事象が確認された。2016 年度の訓練では、これを避けるために送信アカウントを 4 グループに分割し、2 時間毎のメール送信を実施した。

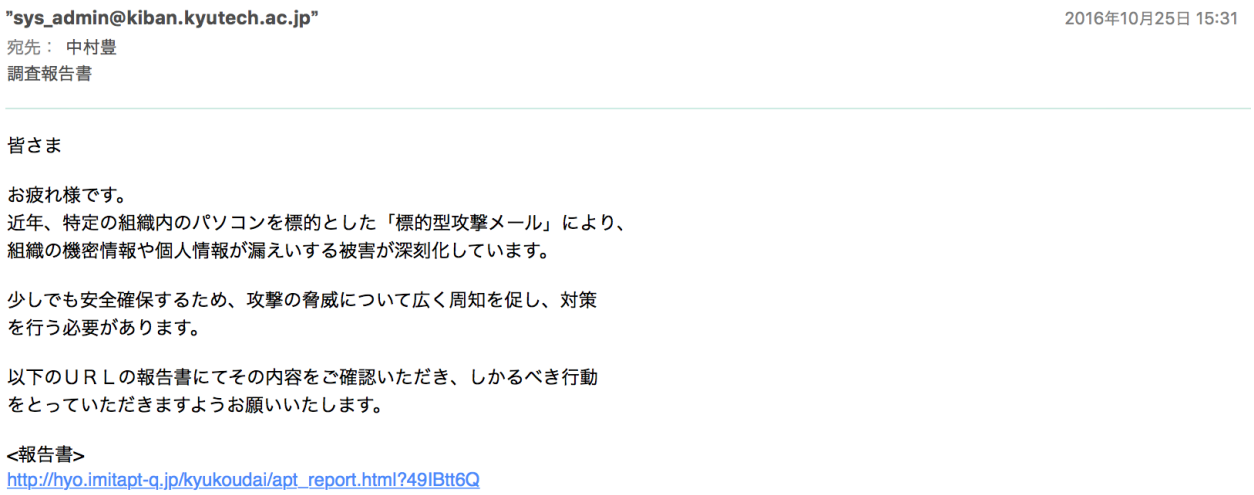
2.3 メールの文面の決定

メール受信者に共通で、かつ注意を引きそうな話題を選択する必要があると考え、2015 年度では全学統合 ID 管理システムからの情報漏洩疑いに関する文面での訓練を行った。図 1 に実際に送信されたメール文面を示す。From 行に関しては、置換機能を用いて「ID 管理者」とし、実体のメールアドレスは gmail を用いた。また、添付ファイルではなく URL 型とした。キューデンインフォコムのサービスの制限で添付ファイルの場合はワードファイルに限定されることや、ポップアップでのブロックがかかるかもしれない、という問題を回避するためである。

2016 年度では標的型訓練の e-learning を行ってくださいという旨の訓練メールの文面とした。図 2 に 2016 年度のメール文面を示す。2015 年度同様に From 行は「sys_admin@kiban.kyutech.ac.jp」と実際に存在しそうなアドレスを記述し、実体は yahoo メールとした。

2.4 URL リンク開封後の画面の決定

メール文面を決めた後に実際に標的型攻撃メールの URL をクリックした際に現れる画面を決定する必要がある。ほとんどはキューデンインフォコムの雛形通りの画面であるが、本学向けに修正が必要な場所も存在する。最終的な開封後画面を図 3 に示す。2016 年度版では、この画面から学内ポータルへ誘導するアンカーを設け、URL をクリックした人が冷静に指示通りに動けているかどうか？の確認を行った。


"sys_admin@kiban.kyutech.ac.jp" 2016年10月25日 15:31
宛先： 中村豊
調査報告書

皆さま

お疲れ様です。
近年、特定の組織内のパソコンを標的とした「標的型攻撃メール」により、
組織の機密情報や個人情報が漏えいする被害が深刻化しています。

少しでも安全確保するため、攻撃の脅威について広く周知を促し、対策
を行う必要があります。

以下のＵＲＬの報告書にてその内容をご確認いただき、しかるべき行動
をとっていただきますようお願いいたします。

<報告書>
http://hyo.imitapt-q.jp/kyukoudai/apt_report.html?49IBtt6Q

図 2: 2016 年度の訓練メール文面

2.5 事前通知文の決定と送信

実際に訓練メールが送信される 1 か月程度前に訓練の事前通知を行った。図 4 に 2016 年度に送信した事前通知文を示す。メール訓練の意義とその内容についての案内となっている。

2.6 訓練メールの送信テスト

実際に全教職員へメール送信する前に、SPAM 対策に処理されるか？正しく送信されるか？といった事前テストを行った。2015 年度での訓練では、部局の SPAM 対策アプリケーションに処理されて訓練メールを受け取れない教室が存在した。2016 年度ではこの対策のために、当該教室でメールアカウントを持っている技術職員に訓練メールテストの受信をしてもらい、SPAM 対策をすり抜ける事ができるかどうか？のテストも行った。

3 訓練本番とデータ解析

実際の訓練メール送信は 2015 年度は 10 月 26 日 (月) 15:00 からの一斉送信とした。種明かしメールの送信を 2 日後の 28 日に実施し、それまでに URL をクリックした人数を集計した。メール受信者総数 895 名中 URL をクリックした人数は 145 名であった。図 5 に職種毎の開封者数・開封率の内訳を示す。これより、常勤職員と非常勤職員に開封率の差が大きく出ていることがわかる。おおよそ 2 倍程度の差となっており、非常勤職員への訓練の重要性が確認できる。図 6 に 1 時間毎の開封者数の遷移を示す。10/26 15:00 に送信された直後の 1 時間以内に開封している人が 80 名となっており、全体の開封者の半分以上を占めている。当日と翌日で開封が収束していることがわかる。

2016 年度では、2015 年度からの改善として 4 グループに分割して送信を実施した。10/25(火) 8:45, 10:45, 13:45, 15:30 の 4 回とした。2015 年度と同様に 2 日後に種明しメールを送信し、それまでに URL をクリックした人数を集計した。2016 年度ではメール受信総数 865 名に対して、URL をクリックした人数は 65 名であった。前回の訓練の結果を踏まえて踏まなくなったのか？文面が簡単な内容であったため踏まなくなったのか？の判断は難しく、次回以降の課題である。図 7 に職種ごとの開封者数・開封率の内訳を示す。2015 年度と同様に常勤職員と非常勤職員で開封率の差が 2 倍近く見られた。非常勤

職員への情報セキュリティ教育が今後の課題であると思われる。図 8 に 1 時間毎の開封者数の遷移を示す。上から順に 8:45 に送信、10:45 に送信、13:45 に送信、15:30 に送信した際の時間遷移となっている。これからわかるようにメール送信から 3 時間以内で開封していることがわかる。また、翌日に開封する人が若干見られ翌々日は 0 名であることがわかる。これより訓練メール送信から 48 時間程度で種明しメールを送信すれば良いことがわかる。

2016 年度の訓練では訓練後の e-learning においてアンケートを実施し、開封者が e-learning を受講したかどうか？の確認を行った。その結果、開封者 65 名中 30 名がアンケートに回答していたが残りの 35 名は e-learning を受講していないことがわかった。さらに 2015 年度と 2016 年度の 2 回続けて開封した人が 10 名いることがわかった。また、開封直後の画面から指示通りに本学のガルーンへ報告した人が 65 名中 13 名であった。これより開封者の半数は e-learning を受講しておらず、また、開封直後に冷静に判断できる人は 10%程度であることがわかった。

4　まとめと今後の課題

構成員の 1 名でも標的型攻撃メールを開封しウィルス感染してしまうと、そこからの 2 次被害や情報漏洩につながる可能性が非常に高いため、訓練の実施は定期的に必要であるということが明らかになった。しかし、開封者 0 名を達成することは非常に困難であることも事実であるため、開封されることを前提に訓練メールの文面を作成することや、ネットワークフォレンジックの仕組みを構築することが重要であることが明らかとなった。また開封率の高い非常勤職員への教育をどのようにして実施するのか？が課題としてあげられる。

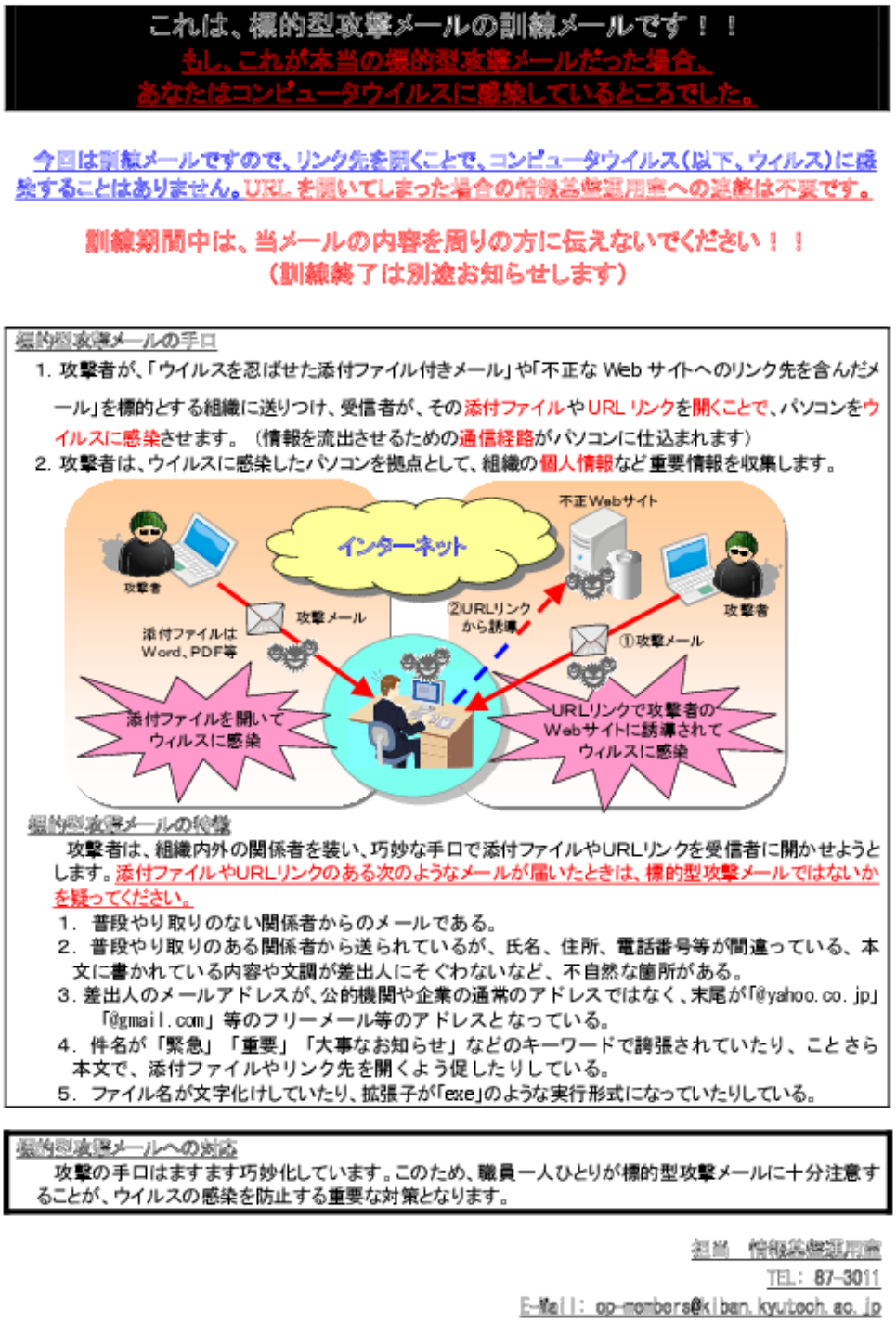


図 3: URL リンク開封後の画面 (2015 年度版)

平成28年 9月 6日

全教職員各位

情報基盤運用室長

標的型攻撃メール訓練の実施について（通知）

昨今、国内において、組織の機密情報や個人情報が漏えいする事故が多発していますが、その攻撃手段として、標的型攻撃メールが利用される事例が数多く確認されています。
標的型攻撃メールは、メールフィルタリング機能をくぐり抜け受信者へ届くものも多く、職員自身が判断し対応することが求められることから、職員への意識啓発が必要となっています。
つきましては、対策強化を図る一つの施策として、標的型攻撃メール訓練を下記のとおり実施しますので、ご理解とご協力をお願いします。

記

１　訓練実施時期
平成２８年度内（複数回実施します。）

２　訓練対象者
全教職員

３　訓練実施方法
訓練対象者へ標的型攻撃メールを模した訓練メールを送付し、受信後の動向を確認します。

４　その他
・現在の攻撃成功可能性を測るため、訓練メールの詳細については控えさせていただきます。ご了承ください。
・訓練用メールの送付数日後に、今回の訓練内容について説明する種明かしメールを訓練対象者全員に送付します。

担当: 情報基盤運用室
TEL: 87-3011
E-Mail: op-members@kiban.kyutech.ac.jp

図 4: 事前通知文 (2016 年度版)

職種		開封者数	対象者数	開封率
事務職員		60	368	16.3%
	うち事務補佐員	34	136	**25.0%**
	事務補佐員除く	26	202	12.9%
教育職員		55	396	13.9%
	うち特任教授等	6	18	**33.3%**
	特任教授等除く	49	378	12.9%
技術職員		14	104	13.5%
	うち技術補佐員	2	20	10.0%
	技術補佐員除く	12	84	14.2%
研究職員等(※)		16	57	**28.1%**
合計		145	895	16.2%

※研究職員，支援研究員，科学研究支援員，産学官連携研究員，技術移転アソシエイト，教務補佐員

図 5: 職種ごとの開封者数・開封率の内訳 (2015 年度)

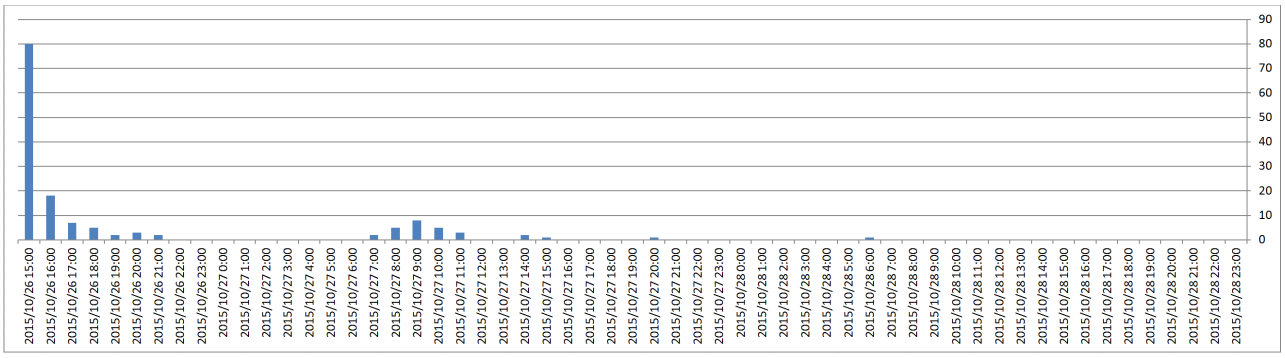


図 6: URL クリックの時間遷移 (2015 年度)

職種	開封者数	対象者数	開封率
事務職員	28	317	8.8%
うち事務補佐員	18	145	**12.4%**
事務補佐員除く	10	172	5.8%
教育職員	25	386	6.5%
うち特任教授等	4	18	**22.2%**
特任教授等除く	21	368	5.7%
技術職員	7	116	6.0%
うち技術補佐員	4	30	**13.3%**
技術補佐員除く	3	86	3.5%
研究職員等(※)	5	46	**10.9%**
合計	65	865	7.5%

※研究職員，継続研究員，支援研究員，科学研究支援員，産学官連携研究員，技術移転アソシエイト，教務補佐員

図 7: 職種ごとの開封者数・開封率の内訳 (2016 年度)

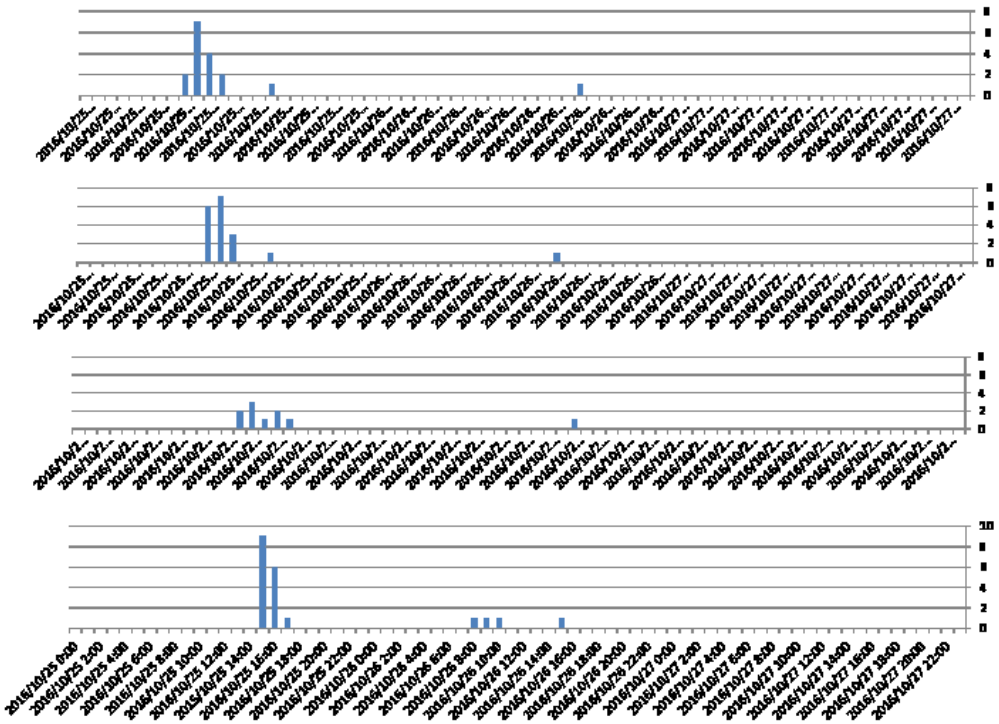


図 8: URL クリックの時間遷移 (2016 年度)