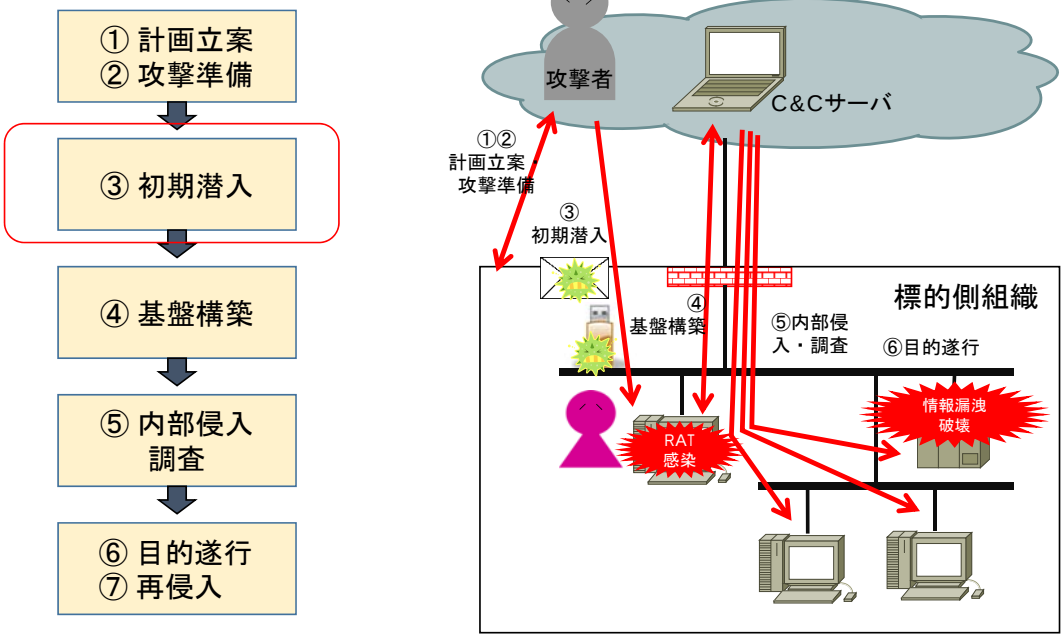
S-3. 標的型攻撃メールの偽装方法の特徴

文京学院大学
浜　正樹

このセッションの目的

1. 標的型サイバー攻撃メールによく使われる偽装方法について確認する
2. 自大学での標的型サイバー攻撃対策訓練用の偽装メール作成のヒントをつかむ

標的型サイバー攻撃の流れ



標的型攻撃メールについて

標的型サイバー攻撃は、メールとその添付ファイルやURL表記を悪用して「初期潜入」することが多い

① 一般ユーザーにもメールの偽装を見抜くリテラシーが必須
（サブジェクト・本文・送信者など）

② セキュリティ担当者もメールヘッダー情報のチェック方法を確認して、インシデントレスポンスへ活用

1. 偽装メールのチェック方法
（メール本文他編）

表1　標的型攻撃メールの偽装の特徴

項目	特徴
サブジェクト	① 知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容 （例1）大学への問い合わせを装ったメール （例2）大学への苦情を装ったメール （例3）研究内容への質問や論文の送付
	② 心当たりのないメールだが、興味をそそられる内容 （例1）議事録、プレゼン資料などの内部文書送付 （例2）他大学学長等の訪問に関する情報 （例3）海外での盗難に対する救済依頼
	③ これまで届いたことがない公的機関からのお知らせ （例1）情報セキュリティに関する注意喚起 （例2）防災情報
	④ 組織全体への案内 （例1）辞令などの人事情報 （例2）学長・理事長からの年次方針説明資料 （例3）全学教授会・FD/SD 資料の再送・差し替え
	⑤ 心当たりのない、決裁や配送通知 (英文の場合が多い) （例1）航空券の予約確認 （例2）医療費・保険料の通知
	⑥ ID やパスワードなどの入力を要求するメール (例1) メールボックスの容量オーバーの警告 (例2) 銀行からの登録情報確認
送信者	⑦ フリーメールアドレスから送信されている ⑧ 送信者のメールアドレスが署名と異なる
本文	⑨ 日本語の言い回しが不自然である ⑩ 日本語では使用されない漢字（繁体字、簡体字）が使われている ⑪ 実在する名称を一部に含むURL が記載されている ⑫ 表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合） ⑬ 署名の内容が誤っている （例1） 組織名や電話番号が実在しない （例2）電話番号がFAX 番号として記載されている
添付ファイル	⑭ 添付ファイルがある ⑮ 実行形式のファイル（exe / scr / jar /cpl 等）の添付 ⑯ ショートカットファイル（lnk / pif / url）の添付 ⑰ 拡張子と異なるファイルアイコンに偽装されている （例1）二重拡張子 （例2）拡張子の前に大量の空白文字の挿入

<参考文献>
IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」
（https://www.ipa.go.jp/files/000043331.pdf）

大学における標的型攻撃被害例

1. 大学におけるRAT感染被害
   - 報道だけでも、標的型攻撃メール偽装の特徴「②、③、⑤」の文面が確認されている
2. 大学におけるフィッシング被害
   - 職員がフィッシングサイトへアクセスし、ID・パスワードを窃取された
   - 窃取アカウント経由で学生の個人情報が漏えい
   - Office365アカウントの懸念点

大学を狙ったフィッシングについて　その1

大学を狙ったフィッシングが2016年4月から発生

1. 発生時期
   - 2016年4月未明
2. フィッシングメールサンプル

From: Nagoya University Admin
件名: こんにちは

あなたは、電子メールのストレージスペースの名古屋アクティブが少なくなっています。ここをクリック
あなたの名古屋アクティブ電子メールストレージにスペースを追加します。

どうもありがとうございました。

大学を狙ったフィッシングについて　その1

大学を狙ったフィッシングが2016年4月から発生

1. 発生時期
   - 2016年4月未明
2. フィッシングメールサンプル

From: Nagoya University Admin
件名: こんにちは

あなたは、電子メールのストレージスペースの名古屋アクティブが少なくなっています。ここをクリック
あなたの名古屋アクティブ電子メールストレージにスペースを追加します。

どうもありがとうございました。
C著作権2016年名古屋大学。 全著作権所有。

⑨日本語の言い回しが不自然

フィッシング対策協議会
Council of Anti-Phishing Japan

大学を狙ったフィッシングについて　その1

大学を狙ったフィッシングが2016年4月から発生

1. 発生時期
   - 2016年4月未明
2. フィッシングメールサンプル

フィッシング対策協議会
Council of Anti-Phishing Japan

大学を狙ったフィッシングについて　その1

大学を狙ったフィッシングが2016年4月から発生

1. 発生時期
   - 2016年4月未明
2. フィッシングメールサンプル

> You are less active in Nagoya's e-mail storage space. click here
> Add space to your Nagoya active e-mail storage.
>
> Thank you very much.
>

フィッシング対策協議会
Council of Anti-Phishing Japan

おまけ

問題

次に出てくる2つのURLのうち、本物のURLはどちらでしょうか？

www.komaba.com

www.komaba.com

「Punycode(ピュニコード)」を悪用した進化型ホモグラフ攻撃
「komaba」の中に見える「o」(オー)は、ギリシャ文字の「o」(オミクロン)

でも従来からの問題として・・・
「L」「Z」問題
小文字の「L」と大文字の「I」はフォントによっては見分けがつきにくく、また数字の「2」と「Z」も手書きの場合は区別がつきにくい

www.worldisnotenough.com

http://gigazine.net/news/20170418-fake-domain-homograph-attack/

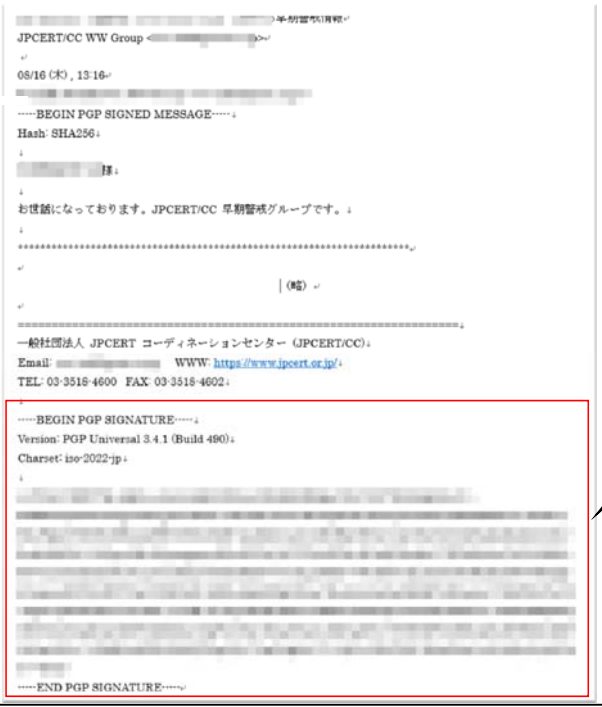
2. 偽装メールのチェック方法

（メールヘッダー編）

メールヘッダー情報の基礎知識

1. Date情報：日本からの送信であれば “+0900” が普通
2. Received情報：送信元メールアドレス（From情報）は偽装可能だが、Receivedは偽装不可能

安全なメール例（JPCERT/CCからのメール）


JPCERT/CC WW Group <[redacted]>

08/16 (木) , 13:16

[redacted]

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

[redacted]様

お世話になっております。JPCERT/CC 早期警戒グループです。

****

(略)

==========

一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)

Email: [redacted] WWW: https://www.jpcert.or.jp/

TEL: 03-3518-4600 FAX: 03-3518-4602

-----BEGIN PGP SIGNATURE-----

Version: PGP Universal 3.4.1 (Build 490)

Charset: iso-2022-jp

[redacted]

-----END PGP SIGNATURE-----

電子署名（PGP）が使われている

安全なメールのヘッダー例

Received: from vmta01.cc.example.jp (vmta01.cc.example.jp [172.16.1.11])
 by vmta03.cc.example.jp (Postfix) with ESMTPS id E10EA40975
 for <contact@ml.example.jp>; Thu, 24 Dec 2015 17:26:09 +0900 (JST)
Received: from mx.jpcert.or.jp (mx.jpcert.or.jp [210.148.223.5])
 by vmta01.cc.example.jp (Postfix) with ESMTP id 0BF1940E6A
 for <contact@ml.example.jp>; Thu, 24 Dec 2015 17:26:08 +0900 (JST)
X-PGP-Universal: processed;
 by pgpgw.jpcert.or.jp on Thu, 24 Dec 2015 17:26:06 +0900
References:
<SG2PR06MB0856205AB47FCF15FA898378E2E70@SG2PR06MB0856.apcprd06.prod.outlook.com>
To: "contact@ml.texample.jp" <contact@ml.example.jp>
From: JPCERT/CC WW Group <ww-info@jpcert.or.jp>
X-Enigmail-Draft-Status: N1110
Date: Thu, 24 Dec 2015 17:25:59 +0900

TLD “.jp” は日本
IPアドレスも日本

+0900は日本時間

疑わしいメール例（ヤマト運輸を騙ったメール）

疑わしいメールのヘッダー例

Received: from vmta01.cc.example.jp (150.7.250.201) by
DB3FFO11FD026.mail.protection.outlook.com (10.47.217.57) with Mic
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P
15.1.577.8 via Frontend Transport; Fri, 17 Aug 2018 09:19:39 +0000
Received: from public-gprs353102.centertel.pl (public-gprs353102.centertel.pl [37.47.10.143])
by vmta01.cc.example.jp (Postfix) with ESMTP id 6ACD040A37
for someone@example.jp; Fri, 17 Aug 2018 18:18:07 +0900 (JST)
From: =?iso-2022-jp?B?GyRCJWQlXiVIMT9NIhsoQg==?= <mail@kuronekoyamato.co.jp>
Subject: =?iso-2022-jp?B?GyRCQnA1XkpYPHU8aDtYRGokNDBNTWo8dUlVNDBOOyROJCpDTiRpJDsbKEI=?=
To: <someone@example.jp>
Message-ID: <f1fb-50366@GKW4FL1ZH1172.tnt.kuronekoyamato.co.jp>
Date: Fri, 17 Aug 2018 10:18:21 +0100
MIME-Version: 1.0
Return-Path: someone@example.jp

TLD “.pl” はポーランド
IPアドレスはポーランド
※ ポーランド：中央ヨーロッパ

+0100は中央ヨーロッパ時間