会計専門職専攻 FD 研修
組織を狙う標的型メール攻撃の手口と対策

○吉川歩 [1]

[1] 甲南大学大学院社会科学研究科

2013 年 7 月 22 日

本日の流れ

組織で発生する情報セキュリティインシデント

情報セキュリティインシデントとは…

情報セキュリティを脅かす偶発事故や意図的攻撃の総称

- 望まない，又は予期しない一連の情報セキュリティ事象であって，事業運営や情報セキュリティを脅かす可能性が高いもの [ISO/IEC27001[1]]
- 事業活動又は情報セキュリティを損ねる可能性のある，予期しない又は望んでいない事象 [ISO/IEC13335[2]]

例：

- マルウェア感染（ウイルス，スパイウェア，ボットなど）
- 不正アクセス
- 情報漏えい

[1] JIS Q 27001: ISMS(Information Security Management System)
[2] JIS Q 13335-1: GMITS(Guideline for the Management of IT Security)

攻撃対象から見るインシデントの分類

攻撃対象：不特定多数から特定組織／個人へ

従来型 → 対象：不特定多数（誰でもよい）
目的：自己顕示欲，混乱目的

標的型 → 対象：特定組織／個人
目的：組織の情報の奪取 → 換金，転売，恐喝＝金銭

対処方法の見直し

インシデントは向こうからやってくる

- 「君子危うきに近寄らず」では心許ない
- 「知彼知己者　百戦不殆[3]」で説くところの，攻撃手法などを知ったうえで有効な手段を講じる必要

[3]孫子：兵法—謀攻編より「不知彼而知己　一勝一負，不知彼不知己　毎戦必殆」と続く

攻撃対象から見るインシデントの分類

攻撃対象：不特定多数から特定組織／個人へ

従来型 → 対象：不特定多数（誰でもよい）
目的：自己顕示欲，混乱目的

標的型 → 対象：特定組織／個人
目的：組織の情報の奪取 → 換金，転売，恐喝＝金銭

対処方法の見直し

インシデントは向こうからやってくる

- 「君子危うきに近寄らず」では心許ない
- 「知彼知己者　百戦不殆[3]」で説くところの，攻撃手法などを知ったうえで有効な手段を講じる必要

[3]孫子：兵法ー謀攻編より「不知彼而知己　一勝一負，不知彼不知己　毎戦必殆」と続く

閑話休題：セキュリティ関連クイズ

問 1：次のうちインシデント対策として確実に有効なものはどれか？

❶ メール中のリンクを開く際は本文中に表示された URL を確認する
❷ 怪しいウェブページを閲覧しない
❸ 添付ファイル付きメールの受信を同僚のみに限定する
❹ セキュリティ対策ソフトを導入し，最新の状態に保つ
❺ OS やアプリケーションソフトを更新して，最新の状態に保つ

❹，❺：ほぼ有効，❷，❸：場合により機能せず，❶：ほぼ機能せず

問 2：上のうち標的型攻撃対策として確実に有効なものは？

有効と言える対策は❺のみ，❹ですら有効な対策となりえない
❺も「未対策だと悪用されるのでやっていないと危ない」というレベル

閑話休題：セキュリティ関連クイズ

問 1：次のうちインシデント対策として確実に有効なものはどれか？

❶ メール中のリンクを開く際は本文中に表示された URL を確認する
❷ 怪しいウェブページを閲覧しない
❸ 添付ファイル付きメールの受信を同僚のみに限定する
❹ セキュリティ対策ソフトを導入し，最新の状態に保つ
❺ OS やアプリケーションソフトを更新して，最新の状態に保つ

❹，❺：ほぼ有効，❷，❸：場合により機能せず，❶：ほぼ機能せず

問 2：上のうち標的型攻撃対策として確実に有効なものは？

有効と言える対策は❺のみ，❹ですら有効な対策となりえない
❺も「未対策だと悪用されるのでやっていないと危ない」というレベル

閑話休題：セキュリティ関連クイズ

問 1：次のうちインシデント対策として確実に有効なものはどれか？

❶ メール中のリンクを開く際は本文中に表示された URL を確認する
❷ 怪しいウェブページを閲覧しない
❸ 添付ファイル付きメールの受信を同僚のみに限定する
❹ セキュリティ対策ソフトを導入し，最新の状態に保つ
❺ OS やアプリケーションソフトを更新して，最新の状態に保つ

❹，❺：ほぼ有効，❷，❸：場合により機能せず，❶：ほぼ機能せず

問 2：上のうち標的型攻撃対策として確実に有効なものは？

有効と言える対策は❺のみ，❹ですら有効な対策となりえない
❺も「未対策だと悪用されるのでやっていないと危ない」というレベル

閑話休題：セキュリティ関連クイズ

問 1：次のうちインシデント対策として確実に有効なものはどれか？

❶ メール中のリンクを開く際は本文中に表示された URL を確認する
❷ 怪しいウェブページを閲覧しない
❸ 添付ファイル付きメールの受信を同僚のみに限定する
❹ セキュリティ対策ソフトを導入し，最新の状態に保つ
❺ OS やアプリケーションソフトを更新して，最新の状態に保つ

❹，❺：ほぼ有効，❷，❸：場合により機能せず，❶：ほぼ機能せず

問 2：上のうち標的型攻撃対策として確実に有効なものは？

有効と言える対策は❺のみ，❹ですら有効な対策となりえない
❺も「未対策だと悪用されるのでやっていないと危ない」というレベル

標的型攻撃の定義

標的型攻撃

定義： 特定の組織／団体／個人を攻撃対象として行われるサイバー攻撃

目的： 攻撃対象である組織／団体／個人が所有する情報の奪取，改ざん，破壊もしくは情報の換金，脅迫による現金奪取などの金銭目的
まれに私怨，思想・政治的対立に起因する妨害・破壊目的

特徴： ①できるだけ攻撃されていることを相手に悟らせない
②攻撃者はプロのクラッカー[4]が多い

$\longrightarrow$ 攻撃されていることに気づきにくく，気づいたときには相当の被害

[4]優れた IT スキルを有するハッカーの中で，その能力を犯罪目的に悪用する者

標的型攻撃の手口の特徴

初動攻撃は電子メール

ピンポイント攻撃には電子メールが有効（ウェブは不特定多数型）

- マルウェア添付
- サイトへ誘導しマルウェアをダウンロード

ソーシャルエンジニアリングの手口を併用

単純なメールではひっかからない
うまく読ませるための工夫は IT ではなく，いわゆる詐欺の手口

- 政府／公的機関／企業などに偽装
- 知人に偽装（SNS などの公開情報を悪用）

電子メールの泣き所 $\longrightarrow$ 開いて読ませる必要

標的型攻撃メールのパタン

同じ内容でもだまされやすさが異なる

- 見知らぬ企業から懸賞当選手続きのサイトを知らせるメール
- 応募していた懸賞の企業から当選手続きのサイトを知らせるメール
- 見ず知らずの他人から写真を添付したメール
- 同窓会で偶然再開した友人から記念写真を添付したメール

業務上読まざるをえないメール

- 理事長，学長，専攻長，事務室から資料を添付したメール
- 学生からレポートを添付したメール
- 学会からシンポジウムサイトの URL を連絡するメール

標的型攻撃メールのパタン

同じ内容でもだまされやすさが異なる

- 見知らぬ企業から懸賞当選手続きのサイトを知らせるメール
- 応募していた懸賞の企業から当選手続きのサイトを知らせるメール
- 見ず知らずの他人から写真を添付したメール
- 同窓会で偶然再開した友人から記念写真を添付したメール

業務上読まざるをえないメール

- 理事長，学長，専攻長，事務室から資料を添付したメール
- 学生からレポートを添付したメール
- 学会からシンポジウムサイトの URL を連絡するメール

標的型攻撃メールのパタン

同じ内容でもだまされやすさが異なる

- 見知らぬ企業から懸賞当選手続きのサイトを知らせるメール
- 応募していた懸賞の企業から当選手続きのサイトを知らせるメール
- 見ず知らずの他人から写真を添付したメール
- 同窓会で偶然再開した友人から記念写真を添付したメール

業務上読まざるをえないメール

- 理事長，学長，専攻長，事務室から資料を添付したメール
- 学生からレポートを添付したメール
- 学会からシンポジウムサイトの URL を連絡するメール

フィッシング対策がまず基本

フィッシングとは

- ソーシャルエンジニアリングを駆使した攻撃手法
- フィッシング $\neq fishing$，$phishing =$ “$sophisticated + fishing$”
- HTML メールを利用したリンクの偽装
  例えば， 甲南大学
- マルウェアを言葉巧みにインストール $\longrightarrow$「警告は無視してよい」
  など

フィッシング対策

残念ながら 100%有効な対策はない

- HTML メールを利用しない $\longrightarrow$ あんなもんは百害あって一利なし
- 不審な処理（添付ファイル，サイトへの誘導）は相手先に問合せ

フィッシング対策がまず基本

フィッシングとは

- ソーシャルエンジニアリングを駆使した攻撃手法
- フィッシング $\neq fishing$，$phishing = \text{“}sophisticated + fishing\text{”}$
- HTML メールを利用したリンクの偽装
  例えば， 甲南大学
- マルウェアを言葉巧みにインストール $\longrightarrow$「警告は無視してよい」など

フィッシング対策

残念ながら 100%有効な対策はない

- HTML メールを利用しない $\longrightarrow$ あんなもんは百害あって一利なし
- 不審な処理（添付ファイル，サイトへの誘導）は相手先に問合せ

攻撃手法は巧妙化

偽装手法の巧妙化

正規のユーザアカウントやサイトを乗っ取った攻撃

- 専攻のページにマルウェアを募集要項の PDF として埋め込み
- 学生のアカウントを乗っ取り，教職員にマルウェアを送信

$\longrightarrow$ ガードの低いところを足がかりにする

頼みの綱のセキュリティ対策ソフトが機能しない

クラッカが予め入手可能な対策ソフトで検出されないことを確認

$\longrightarrow$ 守るより攻撃する側が有利

潜伏しているため感染に気づきにくい

韓国の 320 攻撃のように，1 年以上も前から攻撃準備

攻撃手法は巧妙化

偽装手法の巧妙化

正規のユーザアカウントやサイトを乗っ取った攻撃

- 専攻のページにマルウェアを募集要項の PDF として埋め込み
- 学生のアカウントを乗っ取り，教職員にマルウェアを送信

$\longrightarrow$ ガードの低いところを足がかりにする

頼みの綱のセキュリティ対策ソフトが機能しない

クラッカが予め入手可能な対策ソフトで検出されないことを確認
$\longrightarrow$ 守るより攻撃する側が有利

潜伏しているため感染に気づきにくい

韓国の 320 攻撃のように，1 年以上も前から攻撃準備

攻撃手法は巧妙化

偽装手法の巧妙化

正規のユーザアカウントやサイトを乗っ取った攻撃

- 専攻のページにマルウェアを募集要項の PDF として埋め込み
- 学生のアカウントを乗っ取り，教職員にマルウェアを送信

$\longrightarrow$ ガードの低いところを足がかりにする

頼みの綱のセキュリティ対策ソフトが機能しない

クラッカが予め入手可能な対策ソフトで検出されないことを確認
$\longrightarrow$ 守るより攻撃する側が有利

潜伏しているため感染に気づきにくい

韓国の 320 攻撃のように，1 年以上も前から攻撃準備

完全に有効な対策はなし

ソーシャルエンジニアリング対策として有効そうなもの

- 簡単な内容を添付形式で送信しない $\longrightarrow$ 本文中に記載
- ヘッダーの確認も有効な場合あり $\longrightarrow$ 発信元情報が確認可能

ソフトウェアの脆弱性対策は最低限必要

- マルウェアはソフトの欠陥＝脆弱性を利用して攻撃
  $\longrightarrow$ ソフトの最新化，セキュリティパッチの適用は必須
- セキュリティ対策ソフトを過信しない $\longrightarrow$ 従来攻撃対策には有効

- 同業他社よりは対策を強化 $\longrightarrow$ 狙いやすい方を攻撃
- バックアップも復旧時に有効

完全に有効な対策はなし

ソーシャルエンジニアリング対策として有効そうなもの

- 簡単な内容を添付形式で送信しない $\longrightarrow$ 本文中に記載
- ヘッダーの確認も有効な場合あり $\longrightarrow$ 発信元情報が確認可能

ソフトウェアの脆弱性対策は最低限必要

- マルウェアはソフトの欠陥＝脆弱性を利用して攻撃
  $\longrightarrow$ ソフトの最新化，セキュリティパッチの適用は必須
- セキュリティ対策ソフトを過信しない $\longrightarrow$ 従来攻撃対策には有効

- 同業他社よりは対策を強化 $\longrightarrow$ 狙いやすい方を攻撃
- バックアップも復旧時に有効

完全に有効な対策はなし

ソーシャルエンジニアリング対策として有効そうなもの

- 簡単な内容を添付形式で送信しない $\longrightarrow$ 本文中に記載
- ヘッダーの確認も有効な場合あり $\longrightarrow$ 発信元情報が確認可能

ソフトウェアの脆弱性対策は最低限必要

- マルウェアはソフトの欠陥＝脆弱性を利用して攻撃
  $\longrightarrow$ ソフトの最新化，セキュリティパッチの適用は必須
- セキュリティ対策ソフトを過信しない $\longrightarrow$ 従来攻撃対策には有効

- 同業他社よりは対策を強化 $\longrightarrow$ 狙いやすい方を攻撃
- バックアップも復旧時に有効

むすび：リテラシ教育＝セキュリティ教育

IT で完全防御は不可能

技術（＝装置，ソフト）に頼るだけでなく，教育や規則により危険回避
$\longrightarrow$ リテラシ教育：IT 機器の使い方の教育よりまず安全利用の教育

組織のセキュリティレベル

10 人の組織で 9 人は対策 100%，1 人だけ 50% のとき全体のレベルは？
$\longrightarrow$ 95% ではなく 50% ＝最小値で全体のレベルは決まる
組織内で 1 人目の被害者を食い止めることが重要

セキュリティ関連の情報源

情報処理推進機構:IPA $(http://www.ipa.go.jp/)$

- インシデント，脆弱性関連情報 $\longrightarrow$ デマはない
- 各種インシデント対策のしおり

むすび：リテラシ教育＝セキュリティ教育

IT で完全防御は不可能

技術（＝装置，ソフト）に頼るだけでなく，教育や規則により危険回避
$\longrightarrow$ リテラシ教育：IT 機器の使い方の教育よりまず安全利用の教育

組織のセキュリティレベル

10 人の組織で 9 人は対策 100%，1 人だけ 50% のとき全体のレベルは？
$\longrightarrow$ 95% ではなく 50% ＝最小値で全体のレベルは決まる
組織内で 1 人目の被害者を食い止めることが重要

セキュリティ関連の情報源

情報処理推進機構:IPA $(http://www.ipa.go.jp/)$

- インシデント，脆弱性関連情報 $\longrightarrow$ デマはない
- 各種インシデント対策のしおり

むすび：リテラシ教育＝セキュリティ教育

IT で完全防御は不可能

技術（＝装置，ソフト）に頼るだけでなく，教育や規則により危険回避
$\longrightarrow$ リテラシ教育：IT 機器の使い方の教育よりまず安全利用の教育

組織のセキュリティレベル

10 人の組織で 9 人は対策 100%，1 人だけ 50% のとき全体のレベルは？
$\longrightarrow$ 95% ではなく 50% ＝最小値で全体のレベルは決まる
組織内で 1 人目の被害者を食い止めることが重要

セキュリティ関連の情報源

情報処理推進機構:IPA $(http://www.ipa.go.jp/)$

- インシデント，脆弱性関連情報 $\longrightarrow$ デマはない
- 各種インシデント対策のしおり

むすび：リテラシ教育＝セキュリティ教育

IT で完全防御は不可能

技術（＝装置，ソフト）に頼るだけでなく，教育や規則により危険回避
$\longrightarrow$ リテラシ教育：IT 機器の使い方の教育よりまず安全利用の教育

組織のセキュリティレベル

10 人の組織で 9 人は対策 100%，1 人だけ 50% のとき全体のレベルは？
$\longrightarrow$ 95% ではなく 50% ＝最小値で全体のレベルは決まる
組織内で 1 人目の被害者を食い止めることが重要

セキュリティ関連の情報源

情報処理推進機構:IPA $(http://www.ipa.go.jp/)$

- インシデント，脆弱性関連情報 $\longrightarrow$ デマはない
- 各種インシデント対策のしおり