広島大学における情報セキュリティインシデント対応訓練

渡邉 英伸 [1)], 相原 玲二 [1)], 西村 浩二 [1)]

1) 広島大学 情報メディア教育研究センター

h-watanabe@hiroshima-u.ac.jp

Information Security Incident Response Training in Hiroshima University

Hidenobu Watanabe [1)], Reiji Aibara [1)], Kouji Nishimura [1)]

1) Information Media Center, Hiroshima Univ.

概要

広島大学では，2017 年 11 月から情報セキュリティに関わるインシデント対応訓練を実施することになった．本論文では，実施予定の訓練内容について報告する．

1 はじめに

近年，情報セキュリティ教育・訓練を取り巻く環境は，目まぐるしく変化している．特に標的型メール攻撃は社会全体としての脅威となっており[1]，実際に情報漏洩が発生した事案も少なくない[2][3]．このような背景において，企業や学術機関においては，構成員に対して標的型攻撃を模擬したメール送付による対応訓練が実施されている[4][5][6]．標的型メール攻撃訓練は，構成員に対して怪しいメールを見極める機会を与えるとともに情報セキュリティの意識を向上する上で，一定の効果はあると考えられる．

一方で，標的型メールは年々巧妙化しており，実例を模擬した標的型メール攻撃訓練によって開封率 0%を実現することは非常に困難な状況にある．近年では，100%防御可能な情報セキュリティ対策を目指すよりむしろ情報セキュリティインシデント発生後の被害拡大を最小限に留めることを目指すべきという考えもある[7]ことから，構成員向けの訓練として事後対応にも焦点を当てた訓練がより重要と考える．

実際，岡山大学では事後対応に主眼を置いた対応訓練を実施している[8]．この訓練では，2016 年に情報セキュリティポリシーの改訂および CSIRT(Computer Security Incident Response Team)の設置したことを踏まえて，新たな体制の下で情報セキュリティインシデント発見後の CSIRT とインシデント発生部署との対応手順が機能するか否かの確認および課題の特定を目的に実施するものである．そのため，参加協力可能な 19 の部署（教職員 19 名）に限定した実施に留める代わりに，事務系と教育・研究系の 2 種類の感染端末を想定した訓練シナリオを用意し，標的型攻撃を模したメールの送信，開封時の不審通信の観測，調査・措置の依頼，NW 無効化等の当該端末の措置，報告書の提出等の一連の対応手順について訓練を行っている．

広島大学では，2017 年 11 月より情報セキュリティインシデント対応訓練を実施する予定である．今回の訓練は，岡山大学と同様に標的型メール攻撃訓練ではなく，事後対応を訓練するものである．しかしながら，本訓練は，常勤教職員約 3000 人を対象に情報セキュリティインシデント発生後の対応手順の一部であるウイルス対策ソフトの動作状態などの迅速な報告に絞った訓練を実施するものであり，その点が異なる．本論文では，今年度本学が実施予定の訓練内容を報告する．

2 情報セキュリティインシデント対応手順

本章では，広島大学における情報セキュリティ体制および情報セキュリティインシデント発生時の対応手順について述べる．

2.1 情報セキュリティ体制

広島大学では，情報セキュリティに関連する組織として最高セキュリティ責任者(CISO)の下で統括された情報セキュリティ委員会と情報セキュリティ推進機構が設置されている．情報セキュリティ委員会は大学の基本的な情報セキュリティポリシーの策定及び情報セキュリティに関する重要事項を検討する組織である．情報セキュリティ推進

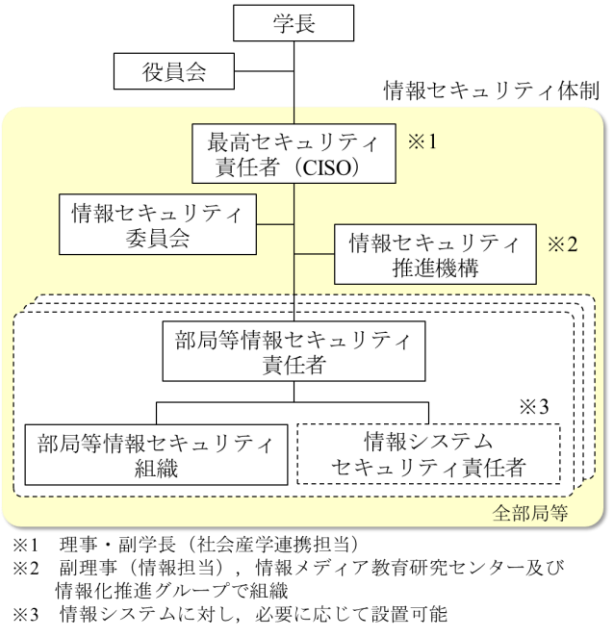

図 3 広島大学情報セキュリティ体制

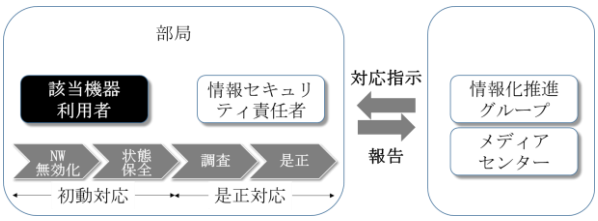

図 2 情報セキュリティインシデント対応手順概要

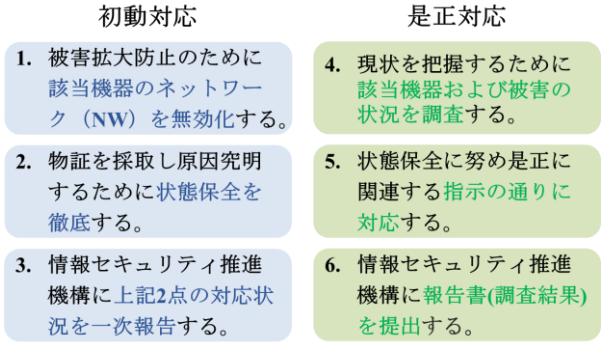

図 1 初動対応手順・是正対応手順

機構は企画立案，啓発や教育などの業務を遂行する組織であり，本学の CSIRT も担っている．情報メディア教育研究センターは，情報セキュリティ推進機構の一組織としても活動しており，全学の取り組みである情報セキュリティインシデント対応訓練の業務を委託されている．図 1 に広島大学情報セキュリティ体制を示す．

2.2 情報セキュリティインシデント対応手順

図 2 に本学における情報セキュリティインシデント対応手順の概要を示す．情報セキュリティ推進機構は，ウイルス感染の可能性がある怪しい通信に関する検知や警告を受けた場合，検知・警告内容ならびに広島大学キャンパス情報ネットワーク[9]上の様々なログから該当機器や利用者を特定し，該当部局の情報セキュリティ責任者にメールにてインシデント発生の可能性および対応指示を通知する．多くの場合，該当機器の利用者や部局等情報セキュリティ組織にも通知する．また，必要に応じて情報セキュリティシステム責任者あるいは該当機器が接続されている NW 管理者・副管理者にも通知される場合もあり，情報セキュリティ責任者あるいは該当機器利用者が不在や対応できない場合においても関係者が NW 無効化や状態保全といった迅速な初動対応を行える連絡体制となっている．

情報セキュリティ責任者ならびに該当機器利用者は，3 つの初動対応および 3 つの是正対応を実施する．図 3 に初動対応手順・是正対応手順を示す．初動対応の 1 つ目は，被害の拡大を防ぐために該当機器のネットワーク(NW)無効化である．なお，広島大学では影響が拡散されることが予想されると情報セキュリティ推進機構が判断した場合には，該当ネットワークの停止及びアカウント停止の措置を実施する．初動対応 2 つ目は，物証を採取し原因究明を行うために状態保全を徹底することである．該当機器の利用者の多くが報告前にウィルススキャンを行う実態があるため，原因究明を困難にしないためにも指示があるまで現状維持を徹底させる．初動対応 3 つ目は，情報セキュリティ推進機構に NW の無効化および状態保全の対応状況について一次報告することである．また，是正対応の 1 つ目は，現状を把握するために該当機器および被害の状況について調査することである．調査対象の項目については次節で述べる．是正対応の 2 つ目は，状態保全に努め，是正に関連する指示通りに対応することである．基本的に対応指示や報告はメールを介して行うが，状況によっては情報セキュリティ推進機構が現場視察や該当機器を押収する場合もある．是正対応の 3 つ目は，情報セキュリティ推進機構に報告書(調査結果)を提出することである．報告書の内容は最終的に情報セキュリティ推進機構を通じて情報セキュリティ委員会に報告される．

2.3 調査対象項目

情報セキュリティ責任者ならびに該当機器利用者が調査する項目を以下に示す．構成員はいつで

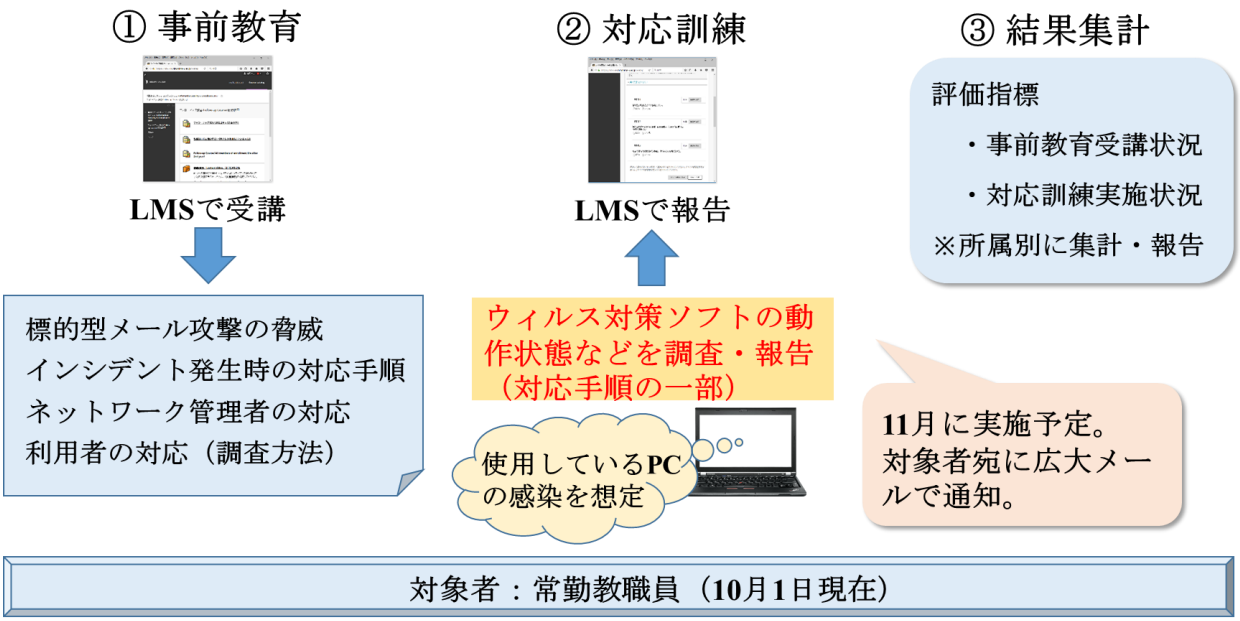

図 4 情報セキュリティインシデント対応訓練手順全体像

も自分で調査できるようになっておくことが重要である．

- 該当するコンピュータについて
  - メーカー，型番，OS のエディションやバージョン，システムの種類，プロセッサ情報など
- 該当するコンピュータの使用目的について
  - 共同利用や生活用途など
- 該当するコンピュータに保存されている情報について
  - 個人情報などの重要情報の有無など
- 該当するコンピュータの使用状況について
  - OS の最終更新日，ウィルス対策ソフト名，パターンファイルの最終更新日，最終スキャン日など
- 該当するコンピュータのファイルの異常について
  - 異常の有無，異常があった場合の具体的な状況など
- 指摘された原因について
  - 思い当たる事象など
- ウィルススキャンの検知結果について
  - フルスキャン時の検知の有無，検知された場合のウィルス名や駆除状況など

3 情報セキュリティインシデント対応訓練

本章では，2017 年 11 月に実施予定の情報セキュリティインシデント対応訓練の内容について述べる．図 4 に 2017 年 11 月実施予定の情報セキュリティインシデント対応訓練の全体像を示す．対応訓練は①事前教育，②対応訓練，③結果集計の 3 つから構成される．対象者は常勤教職員約 3000 人(2017 年 10 月 1 日時点)である．

3.1 事前教育

事前教育は，訓練を実施する前に情報セキュリティインシデント発生時の対応手順の確認と対応訓練の内容について理解することを目的に実施するものである．事前教育は LMS(Learning Management System)上に電子教材を用意する．

電子教材の内容には，標的型メール攻撃の脅威，インシデント発生時の対応手順，ネットワーク管理者の対応，利用者の対応(調査方法)ならびに 11 月実施予定の対応訓練の手順を含めることを想定している．例えば，標的型メール攻撃の脅威については，特徴と事後対処の重要性を説く内容を予定している．インシデント発生時の対応手順，ネットワーク管理者の対応，利用者の対応(調査方法)については，情報セキュリティインシデント対応手順概要(図 2)，初動対応手順・是正対応手順(図 3)，2.3 節の調査対象項目の内容が候補となる．加えて，利用者の調査方法の参考資料として，メーカー名・型番等の調査方法，OS 情報(Windows10 と Mac OS)の確認方法，ウイルス対策ソフト(Windows Defender と SCEP for Mac)の確認方法等も紹介する予定としている．対応訓練の手順につ

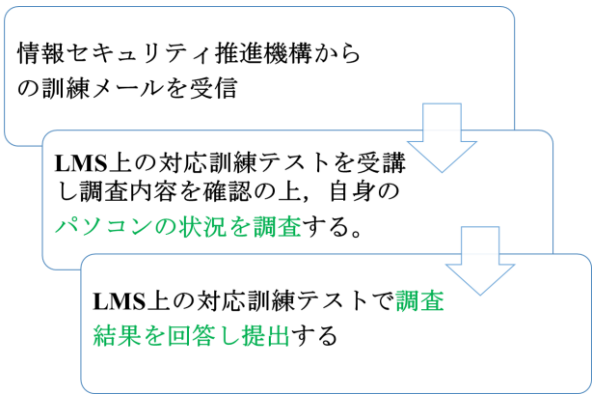

図 5 対応訓練手順

いては，全体像(図 4)に触れた後，対応訓練の手順を説明する計画である．なお，事前教育の教材は日本・英語を用意する予定である．

3.2 対応訓練

3.2.1 対応訓練手順

2017 年 11 月に実施する対応訓練は，是正対応の一部を実施し，その対応時間を明確にすることで常勤教職員全体の対応の速さの向上を目的に行うものである．図 5 に対応訓練手順を示す．はじめに，情報セキュリティ推進機構から対象者に訓練メールを送信する．訓練対象者はメールを受信した後に，LMS にアクセスし，対応訓練テストを受講する．対応訓練テストでは，2.3 節で述べた調査対象項目に関する質問があり，その内容について自身のパソコンの状況を調査する．最後に，調査結果を対応訓練テスト上で回答し提出する．なお，対応訓練テストにおいても日本・英語を用意する予定である．

3.2.2 対応訓練テスト

対応訓練テストの質問候補を以下に示す．

1. 該当するコンピュータについて教えて下さい．
   - (ａ) メーカー名と型番(シリーズ名などでも可)を教えて下さい．
   - (ｂ) デスクトップですか？ノートパソコンですか？
   - (ｃ)OS およびシステム の情報(バージョン，エディション，システムの種類，CPU など)を教えてください．
     - 例)Windows 10 Pro, 1607, 14393.1593, 64 ビット, Intel core i7-4500U
     - 例)OS X EI Capitan, 10.11.6, MacBook Air (11-inch, Mid 2012), Intel Core i5
2. 該当するコンピュータの使用目的について教えて下さい．
   - 例)学生が 研究室で共同利用しているパソコン
   - 例)教員が普段使用しているパソコン
3. 該当するコンピュータに個人情報など重要なデータが保存されていますか？保存されている場合，それはどのような情報ですか？具体的に教えて下さい．
4. OS の最終アップデートはいつですか？
   - 例)2017 年**月**日
5. ウイルス対策ソフトは何を使用していますか？
   - 例)Windows10 標準の Defender
   - 例)大学提供の SCEP または FEP
   - 例)パソコンに標準添付のウィルスバスタークラウド
6. ウイルス対策ソフトのパターンファイルの最終アップデートはいつですか？
   - 例)2017 年**月**日
7. ウイルス対策ソフトの最終スキャンはいつですか？そのときウイルスは検知されましたか？
   - 例)2017 年**月**日， 検知なし
8. ウィルススキャン(フルスキャン)を行ってください．ウイルスは検知されましたか？検知された場合，ウイルス名と駆除できたか否かについて教えてください．
   - 例)検知なし
   - 例) 検 知 あ り ， ウ イ ル ス 名 ： WORM_******，駆除できた

3.3 結果集計

今年度の情報セキュリティインシデント対応訓練の評価としては，所属別に結果を集計し報告する予定である．評価指標は，事前教育受講状況ならびに対応訓練実施状況の 2 点である．事前教育受講状況は，電子教材のアクセスログを参考にす

る．対応訓練実施状況は，対応訓練テストの提出ログを参考にする．なお，AXIES2017 の発表時には，速報として結果を報告する予定である．

4 まとめ

本論文では，2017 年 11 月に約 3000 人の常勤教職員に対して実施予定の情報セキュリティインシデント対応訓練の内容について報告した．本訓練は，多くの組織が実施している標的型メール攻撃訓練のような事前対策訓練ではなく，情報セキュリティインシデント発生後の迅速な調査および報告を見据えた事後対応を訓練するものである．

参考文献

[1] 警察庁, 平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について，2016，https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf

[2] 日本年金機構，日本年金機構における不正アクセスによる情報流出事案について，2015，http://www.nenkin.go.jp/oshirase/topics/2015/0104.html

[3] JTB，不正アクセスによる個人情報流出の可能性について―現状報告と再発防止策―，2016，https://www.jtbcorp.jp/jp/160824.html

[4] 伊藤史人，高見澤秀幸，佐藤郁哉，標的型攻撃メールの予防対策，学術情報処理研究，No.16，pp.100-110，2012.

[5] 寺田剛陽，鳥居悟，安野智子，瀧澤弘和，新真知，リスク認知に基づく標的型メール対策の検討, 情報処理研究報告, Vol.2013-GN-88, No.9，pp.1-8，2013.

[6] 木村壮太，メール攻撃危険予知訓練システムの開発，情報処理学会研究報告，Vol.2013-CSEC-63，No.4，pp.1-6，2013.

[7] IPA，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」，2015，https://www.ipa.go.jp/files/000043331.pdf

[8] 村上昌己，大隅淑弘，藤原崇起，岡田学昭，川上祐介，信江輝治，早竹昭人，稗田隆，標的型メール攻撃によるセキュリティインシデントへの対応訓練, 第 21 回学術情報処理研究集会発表論文集，pp.49-56，2017.

[9] 近堂徹，田島浩一，岸場清悟，岩田則和，相原玲二，自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価, 情報処理学会論文誌，Vol.57，No.3，pp.998-1007，2016.