社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2005－CSEC－29 (1)
2005／5／19

名古屋大学情報セキュリティ対策推進室の活動

竹内 義則[*1] 山口 由紀子[*2] 河口 信夫[*2]
山里 敬也[*3] 長谷川 明生[*4] 坂部 俊樹[*1]

*1 名古屋大学 情報セキュリティ対策推進室 〒464-8601 愛知県名古屋市千種区不老町
*2 名古屋大学 情報連携基盤センター 〒464-8601 愛知県名古屋市千種区不老町
*3 名古屋大学 エコトピア科学研究所 〒464-8601 愛知県名古屋市千種区不老町
*4 中京大学 生命システム工学部 〒470-0393 愛知県豊田市貝津町床立 101
E-mail: takeuchi@nagoya-u.jp

あらまし 名古屋大学情報セキュリティ対策推進室は，情報セキュリティインシデントに対して迅速に対応するため，日常的かつ機動的に活動可能な情報セキュリティ・情報技術に関する専門家集団として，平成１５年１１月に設置された．情報セキュリティ対策推進室の使命は大きく２つに分けられる．一つは，名古屋大学のすべての構成員に対する情報セキュリティの啓発活動の企画・実施であり，もう一つは，情報セキュリティインシデントへの緊急および日常的対応である．本報告では，情報セキュリティ対策推進室の活動内容として，情報セキュリティ研修，情報セキュリティインシデントデータベースの構築，無線 LAN 調査，情報セキュリティ監査について述べる．また，大学で発生したセキュリティインシデントについて報告する．

キーワード 情報セキュリティ研修，セキュリティインシデント

Activity Report of Information Security Promotion Agency, Nagoya University

Yoshinori TAKEUCHI[*1], Yukiko YAMAGUCHI[*2], Nobuo KAWAGUCHI[*2]
Takaya YAMAZATO[*3], Akiumi HASEGAWA[*4] and Toshiki SAKABE[*1]

*1 Information Security Promotion Agency, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8601, Japan
*2 Information Technology Center, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8601, Japan
*3 EcoTopia Science Institute, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8601, Japan
*4 School of Life System Science and Technology, Chukyo University, 101 Tokodachi, Kaizu-cho, Toyota -shi, Aichi-ken, 470-0393, Japan

E-mail: takeuchi@nagoya-u.jp

Abstract The Information Security Promotion Agency (ISPA), Nagoya University was established in November, 2003. It is an expert group of information security and technology operating as promptly and actively as possible to respond information security incidents. There are two missions in ISPA. One is to engage in educational activities on information security for all members in Nagoya University. The other is to respond information security incidents as promptly and actively. In this report, we describe information security training, building of information security incident database, investigation of wireless LAN and information security audit. We also report security incidents which occur in our university.

Keyword information security training, security incident

1. はじめに

名古屋大学情報セキュリティ対策推進室は，サイバーテロやネットワーク犯罪などの情報セキュリティインシデントに対して名古屋大学として迅速に対応するため，日常的かつ機動的に活動可能な情報セキュリティ・情報技術に

関する専門家集団が必要であり，平成１５年１１月に設置された．

情報セキュリティ対策推進室に課される使命は大きく２つに分けられる．一つは，名古屋大学のすべての構成員に対する情報セキュリティの啓発活動の企画・実施であり，情報セキュリティ意識向上のための講演会や新入生への情報セキュリティ研修の企画・実施，情報セキュリティインシデントに関する情報の収集・整理・提供などがある．

もう一つは，情報セキュリティインシデントへの緊急および日常的対応である．例えば，サイバー攻撃やコンピュータウィルスに対する緊急防御対策，また，それらに対する日常的予防対策などが上げられる．その他にも，学内の情報システムの監査（脆弱性の検査と改善勧告）の企画・実施，学外からの情報セキュリティに関する問い合わせや苦情への対応などがある．

情報セキュリティ対策推進室は，現在のところ，室長（兼任教授），室員（専任助教授），事務補佐員（非常勤職員）からなる．そして，平成１７年度からは室員（専任助手相当）の配置が認められている．

同室の活動は，専任助教授が採用された平成１６年度から本格的に開始された．以来，ウイルスによる被害，サーバ侵入被害，著作権侵害問題など，日々のインシデント対応に追われる中，ポスター，パンフレットの発行，セキュリティ研修，セキュリティ講習会，Web サーバのセキュリティ調査，無線 LAN の脆弱性検査，インシデントデータベースの共用開始などを行ってきた．同室は，情報連携基盤センター，情報メディア教育センター，附属図書館と連携・協力して活動を行い，名古屋大学の情報セキュリティレベル維持のために努力してきた．

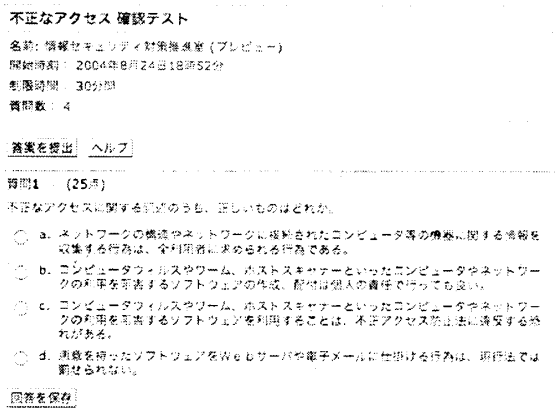
以下でその活動内容について詳細に述べるとともに，名古屋大学で発生した情報セキュリティインシデントについて紹介する．

2. 情報セキュリティ啓発活動

名古屋大学の構成員の情報セキュリティに関する意識を向上させるため，ポスターを掲示したり，パンフレットを配布したりする活動を行っている．特に，新入生を対象とした情報セキュリティ研修について以下で述べる．

表 1　情報セキュリティ研修実施要項

対象	情報メディア教育センターの新規利用者（学部新入生）
研修内容	情報セキュリティガイドラインに沿った内容
実施時期	平成16年４月１日ー４月３０日まで情報メディア教育センター利用の最初の講義の最後の３０分に実施
実施方法	・ 講義担当教員より情報セキュリティガイドラインの概要を説明（５分程度） ・ 次に，WebCT 上の研修プログラムにより自主的に受講させる ・ 研修は合格するまで（授業時間外に）繰り返し受講させる ・ ４月３０日までに合格しない者に対しては，情報メディア教育センターより個別指導を行う


不正なアクセス 確認テスト

名前: 情報セキュリティ対策推進室 (プレビュー)
開始時刻: 2004年8月24日18時52分
制限時間: 30分間
質問数: 4

答案を提出　ヘルプ

問題1　(25点)

不正なアクセスに関する記述のうち、正しいものはどれか。

a. ネットワークの構成やネットワークに接続されたコンピュータ等の情報に関する情報を収集する行為は、全利用者に求められる行為である。

b. コンピュータウィルスやワーム、ホストスキャナーといったコンピュータやネットワークの利用を妨害するソフトウェアの作成、配付は個人の責任であっても良い。

c. コンピュータウィルスやワーム、ホストスキャナーといったコンピュータやネットワークの利用を妨害するソフトウェアを利用することは、不正アクセス防止法に抵触する恐れがある。

d. 通常を得たソフトウェアをWebサーバや電子メールに仕掛ける行為は、現行法では罰せられない。

回答を保存

図 1　確認テストの例

2.1. 情報セキュリティ研修

この研修の目的は，ネットワーク社会における大学の教育研究活動を安全なものにするため，名古屋大学が提供するコンピュータなどの情報機器やデータベースなどの情報資源の利用について定められている名古屋大学ネットワーク利用ガイドラインの周知・徹底を図ることである．

情報メディア教育センターでは，この研修を行うために e-learning の教材を，WebCT を用いて作成した．教材は，名古屋大学ネットワーク利用ガイドラインに沿って作成した．以下に示す全９章からなり，それぞれの章は，いくつかの節，確認テスト，事例集，ビデオクリップか

らなる．この教材を使って，表1に示す実施要領で研修を行った．

1章　利用の開始
2章　メディアセンターの利用
3章　情報の受信と生成
4章　情報の管理
5章　情報発信
6章　危機管理
7章　紛争処理，8章　関連情報，9章　相談窓口

それぞれの章の終わりに，図1に示すような簡単な確認テストを用意し，それぞれの章で80点以上取れるまで繰り返し受講させた．最後の章までの確認テストで，すべて80点以上取った者を合格者とした．

この情報セキュリティ研修を実施した結果，受講率は全体で67%，合格率は，理系が94%に対し，文系では68%であった．受講率が学部によりばらつきがあることが確認された．また，全体として，受講率の高い学部は合格率も高くなっていた．研修にかかった時間については，早い者の場合，15分程度で終了しており，ほとんどの受講生が30分で終了できた．しかしながら，30分以上かかった学生も何人かいた．時間がかかった理由としては，ビデオコンテンツの閲覧をしたためと推測される．それ以外では，WebCTの操作ミス（回答を送らなかったなど）によるためと思われる．

学生からは，WebCTはどうやって使うのか，という質問が多くあった．そもそもログインでてこずる学生もいた．しかし，いったんWebCTの使い方が分かれば，後はスムーズに研修を受講できたようである．これより，研修内容もさることながら，WebCTの利用についての導入教育が重要であることが分かった．

現在のところ情報セキュリティ研修は日本語コンテンツしか用意していない．留学生への対応も今後の課題である．

コンテンツについては，研修の全体像が分かりにくい点が指摘された．今回は，各章の公開条件を設定したため，初めにアクセスした時点では全部で何章あるのか分からない．これより，1章のみで終了した学生も何人かいた．もっとも，研修については詳細な説明を載せていたのだが，殆どの学生が読まずにいた．ガイドライン自体が，ともすれば常識的なことを述べているにすぎないため，いきなり確認テストから始める者もいた．また，テストのバリエーションが乏しい点も改善する必要がある．問題数としては，各章ごとに提示するものとして少なくともう5問は欲しい．となると，各章毎にその10倍程度は必要となり，全部で300問以上は答案データベースに登録する必要があるだろう．

今後，情報セキュリティ研修の周知を行い，受講率を上げていくことが課題である．また，今回は情報メディア教育センターを最初に使う講義で研修を行ったが，学生の中には情報メディア教育センターを使う講義を受講しない者もおり，その学生のケアをしていくことも必要である．

3. インシデント対応

情報セキュリティ対策推進室の2番目の任務は，情報セキュリティインシデントに迅速に対応することである．学内で発生したウイルス感染のインシデントに効率よく対応するために，情報連携基盤センターと協力し，情報セキュリティインシデントデータベースを構築し，運用を行っている．これについて，次節で詳しく述べる．また，学内で発生したセキュリティインシデントの内容や傾向，学外からの苦情・問い合わせについて紹介する．

3.1. 情報セキュリティインシデントデータベースの構築

名古屋大学キャンパスネットワーク（NICE）では，2003年8月のMS-BLASTERウイルスなど，しばしば大規模なウイルス感染が発生した．これらのウイルスは，ネットワーク内の他の端末を攻撃して感染を広げるだけでなく，攻撃時に大量のパケットを発生し，正常な通信へも悪影響を及ぼす場合がある．そのため，情報連携基盤センターでは，ウイルス感染を検出した場合は，まずルータで感染端末の通信を遮断し，管理者へ感染を通知し，端末の対策がとられたことを確認した上でルータの通信遮断を解除するという手段をとっている．このような運用では，通信を遮断したために管理者への通知が届かなくなってしまうという悪循環も発生していた．そのため，各インシデントの処置状況を明確にし，NICEの利用者に自分の端末が通信遮断されているか否かを確認するための手段として「情報セキュリティインシデントデータベース」を構築し，平成16年7月から運

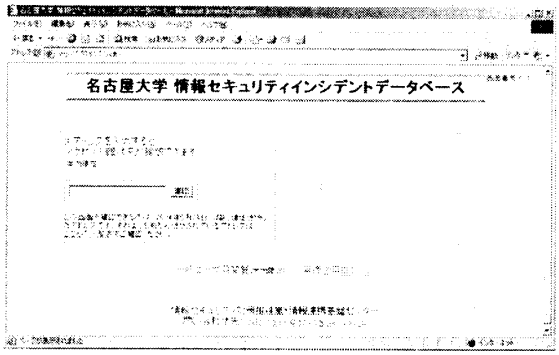


図 2 情報セキュリティインシデントデータベース：一般利用者向けアクセス制限確認画面

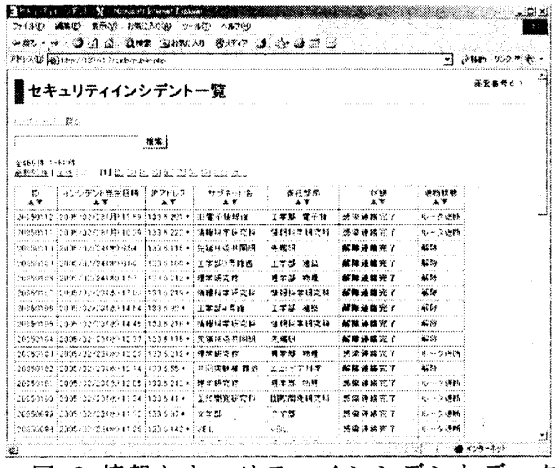


図 3 情報セキュリティインシデントデータベース：インシデント一覧(学内専用)画面

用を開始した．

この情報セキュリティインシデントデータベースの利用目的は以下の 3 点である．

1. 端末の通信遮断状況を Web ページで確認できる手段を提供し，NICE 利用者の利便性を向上させる．
2. ウイルス感染，ルータでの遮断状況，端末管理者への通知状況などの情報を蓄積し，NICE の安全な運用のために利用する．
3. 将来的なセキュリティ戦略立案に利用する．

データベースへのインシデント登録や情報更新は情報連携基盤センターおよび情報セキュリティ対策推進室のスタッフが行う．一般利用者に対しては，図 2 に示すような，利用している端末がアクセス制限されているか否かを確認する機能を提供し，学内管理者に対しては，インシデントの詳細情報の閲覧機能を提供する．(図 3)

表 2 学内で発生したセキュリティインシデント統計情報

年月	インシデント発生数	主要なワーム，ウィルス
2004/02	82	Welchia
2004/03	65	Welchia,Netsky
2004/04	62	Welchia, Netsky
2004/05	85	Sasser, Welchia
2004/06	100	Spybot, Sasser
2004/07	57	Spybot, Korgo, Sasser
2004/08	22	Spybot, Netsky
2004/09	40	Spybot
2004/10	78	Spybot, Bagle
2004/11	24	Spybot, Bagle
2004/12	45	Spybot, Netsky
2005/01	11	Spybot, Netsky
2005/02	101	Spybot

3.2. 学内で発生したインシデント

平成 17 年 2 月までに発生したセキュリティインシデントの状況は表 2 に示すとおりである．

- ウイルス，ワーム感染
  電子メールを媒介とするウイルスや，スキャンして対象を検出するワームなどに多数感染した．
  最近では，ウイルス検出ソフトウェアで検出するためのパターンファイルが対応できる前に感染する例が増えてきた．
- 著作権侵害行為
  P2P 利用に関する指摘があり調査した例があった．
  管理者が知らないうちに Anonymous FTP サーバが起動されてしまい，著作権を侵害している音楽データなどの交換場所に利用されてしまった例があった．
- 不正アクセス
  管理者が知らないうちに open proxy として設定されてしまい，掲示板荒らしに利用されたり，学内専用サービスを不正

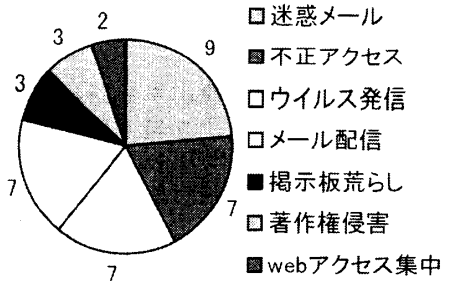


図4　セキュリティインシデントの内訳

に利用されたりしてしまった．

このようなインシデントが発生した場合には，サブネットの入り口のルータで通信を遮断するとともに，管理者に調査および対処を依頼する．

3.3. 学外からの問い合わせ・苦情

今までに，38件の問い合わせ・苦情を受け付けている．図4にその内訳を示す．

最も多い迷惑メールとは，名古屋大学のドメイン（nagoya-u.ac.jp）から，SPAMメールやウイルスメールが届いているというものである．このうち7件は，名古屋大学のドメインを詐称されて学外から発信されたものであった．また，ウイルス感染により，メールを中継するツールを入れられ，スパムメールを発信している事例もあった．

2番目の不正アクセスは，学内の機器からいろいろなアカウントでログインを試みた事例，DoS攻撃を行った事例，附属図書館の契約している電子ジャーナルを大量にダウンロードした事例がある．調査の結果，これらは学外から計算機に不正に侵入され，侵入者に悪用されたものだと分かった．

ウイルス発信は，名古屋大学からウイルスメールが届いたという苦情である．このうち2件は，実際にウイルスに感染していることが明らかになった．

メール配信は，2004年10月より実施したメール配送制限の強化によってメールが届かなくなったという問い合わせである．

掲示板荒らしは，学内の機器から学外の掲示板に不適切な書き込みを大量に行ったというものである．このうち1件は，オープンプロキシが原因で，学外から学内の端末を悪用されたことが分かった．もう1つは，苦情元の情報不足により，調査できなかった．

著作権侵害は，学内の計算機が音楽などの著作物を不法にダウンロードできるようにしているという著作権団体からの苦情である．このうち2件は，P2Pソフトウェアを使用しているという指摘であった．調査の結果，指摘されたことは確認できなかった．もう1つは，FTPサーバに，著作物が置かれているという指摘であった．調査の結果，anonymous FTPサービスによって行われたものであることがわかった．

Webアクセス集中は，学内の機器からウェブサイトに短時間に大量のアクセスが行われたというものである．このうちの1件は，ウェブ巡回プログラムの不備によるものであった．もう1つは，おそらく講義の課題でアクセスが集中したものだと思われる．

情報セキュリティ対策推進室では，これらの問い合わせ・苦情の事例に基づき，対応マニュアルを整備し，運用を行っている．

4. 情報セキュリティ調査

情報セキュリティインシデントに対する予防策として，学内の情報機器を調査し，改善を勧告することによって，セキュリティレベルの維持・向上に役立てる活動を行っている．今までに，無線ＬＡＮに関する調査と，主にウェブサーバにたいする脆弱性検査を行った．それぞれについて，以下で述べる．

4.1. 無線ＬＡＮのセキュリティ

最近の無線LANの普及に伴い，大学キャンパス内にも，多数の無線LAN基地局が設置されている．これら基地局の中には，セキュリティを十分に考慮していない無線LAN基地局も見受けられる．特に不特定の第三者により，NICEに接続可能な基地局は，不正アクセスや不正ファイル転送などの違法行為によって，学内の情報セキュリティに深刻な問題を引き起こす可能性がある．そこで，今後のセキュリティ対策の参考とするために，情報連携基盤センター情報基盤ネットワーク研究部門の協力のもと，名古屋大学キャンパス内におけるワイヤレスネットワーク利用状況の調査を行った．

4.1.1. キャンパス内の無線ＬＡＮ状況調査

無線LANに関するセキュリティ状況調査を以下のように行った．

調査予定期間	：平成１６年４月２９日（木）～４月３０日（金）
調査範囲	：名古屋大学東山キャンパス内
調査方法	：IEEE802.11b 無線 LAN 調査システムによる調査，アクセス可能性調査

この際には，名古屋大学の構成員に対し，以下の事項をお願いした．

1．キャンパス内に無線 LAN 基地局を設置されている場合，上記の調査期間以前に，次の資料を参考にセキュリティ対策を実施してください．
名古屋大学情報連携基盤センター　情報基盤ネットワーク研究部門
無線 LAN の情報セキュリティに関する情報

http://www.net.itc.nagoya-u.ac.jp/wnet/security/

2．アクセス可能性を確認するために，ping 等で確認する場合がありますので，ご了承ください．
3．調査のため，建物内の廊下等に立ち入ることがありますので，ご了承ください．基本的には部屋に入ることは必要ありませんが，場合によっては部屋への入室をお願いすることがありますので，その場合はご協力をお願いいたします．
4．調査の結果，問題があることが判明した場合は，情報セキュリティ対策推進室で検討の上，何らかの対応をとらせていただく可能性がありますことをご了承ください．

4.1.2. 無線ＬＡＮ調査結果

調査方法は，IEEE802.11b 無線 LAN 端末を用いたアクセスポイント接続可能性調査である．接続後は，NICE 内への ping によりネットワーク到達性調査（DHCP 利用，ping 調査は 2 秒以内に接続できたもののみ）を行った．WEP 使用のアクセスポイントには接続調査は行っていない．

調査範囲は，東山キャンパスで，屋外からの調査のみである．

調査結果として，無線 LAN アクセスポイント数は 255 個見つかった．そのうち，暗号化／認証を行っていないアクセスポイント数は 114 個であった．また，２秒以内に接続可能/ ping 到達アクセスポイント数が 9 個見つかった．

予備調査の結果から，東山キャンパス内では約半数のアクセスポイントが暗号化，もしくは認証を行っておらず，全体の４％弱の基地局が，認証なしに NICE 内に接続可能となっていることがわかった．今回の調査では，屋外からの調査で電波状態の良くない状態で接続を試みている点，ping 接続調査については２秒間しか接続を試みていない点から，実際にはより多数のアクセスポイントが脆弱性を持つ可能性がある．

4.2. 外部機関によるセキュリティ監査

NICE に設置された侵入検知装置によると，学外からの弱点探査行為は毎日のように起きており，特に，ウェブサーバを標的としたスキャンが多く発生している．このような現状をふまえて，NICE に設置されたウェブサーバや重要な情報機器に対して，外部機関による脆弱性検査を行った．この検査の主旨は，学外の機関から中立な立場で監査することによって，セキュリティホールの発見やその対策を行うためのものである．

検査は，学外のスキャンサーバから，従来の疑似アタックではなく，RFC に準拠したパケットを使用し，攻撃的な方法を含まないスキャニングを行う．そのため，通常，正常に運用が行われているサーバに影響を与えることはない．検査対象となるセキュリティホールは，既知のものをほぼ網羅した 3974 項目(2005.1.7 現在)である．

検査の結果，複数のホストでセキュリティ上問題のあるサービスが動作していることが指摘された．

5. まとめ

名古屋大学情報セキュリティ対策推進室の設置とその活動内容について報告した．また，大学内で発生している情報セキュリティインシデントを紹介した．