Vol.2013-IS-123 No.9
2013/3/15

大学における PC セキュリティ管理の課題

石坂徹[†]　刀川眞[†]　石田純一[†]　早坂成人[†]

大学においては教員の PC 管理は教員自身に任せられていることが多いが、情報セキュリティインシデントは組織としての責任が問われる。大学としては規程整備、状況把握、対策や教育などを行う必要がある。この中で我々は PC のセキュリティ状況に着目し、PC を個別に直接検査する必要があると考えた。室蘭工業大学では全学の PC の OS 更新、ウィルス対策ソフトの利用及びソフトウェアの管理状況の検査を行った。本稿では検査結果に基づき教員 PC の管理状態の改善を課題として提示する.

Subject of PC Security Management in University

Tohru Ishizaka[†] Makoto Tachikawa[†] Jun-ichi Ishida[†]
and Narihito Hayasaka[†]

It is surmised that a teacher's PC management is left to the teacher itself in a university. In many cases, the responsibility for an information security incident belongs to an organization. The university needs to perform regulation maintenance, assessment of the situation, a measure, education, etc. We thought in these that it was necessary to inspect PC directly individually paying attention to the security situation of PC. In Muroran Institute of Technology, use of the update state of OS of all the PCs in a university and antivirus software and the management state of software were inspected. From the result, the problem of management of PC in a university is mentioned and the policy for the improvement in security is proposed.

1. はじめに

情報セキュリティという言葉が世の中に定着している現在でも，教育機関における情報漏えいインシデントは絶えず報告されている[1][2]. これらのインシデントの多くは情報持ち出しや管理ミスなどのヒューマンエラーによるものが多いが，独立行政法人情報処理推進機構がまとめた情報セキュリティ白書[3]では，セキュリティ対策の優先度 1 位としてウィルス等を使った標的型攻撃が挙げられている. これらの脅威からの PC 及び情報を守るためには，ヒューマンエラーを防止する教育に加えて, PC のウィルス対策や脆弱性対応についての教育と管理状態の検査が必要である.

大学においては､教職員が業務に利用する PC の管理は、利用者自身に任せられていることが多い。情報セキュリティインシデントは組織としての責任が問われる．ほとんどの大学では情報セキュリティポリシーをはじめとする規程類を整備し､それに従ってセキュリティ対策を行っている。情報機器や組織におけるセキュリティ対策の選択方法としては，インシデント発生時の賠償リスクからみた対策選定の組合せ手法の定式化[4]や実際に教育機関で発生したインシデントの分析による定量的分析[5]など，いくつかの手法が提案されている．しかし、対策を選定・実施するにあたり，規程に遵守しているか，特に実際にセキュリティが保たれているかを把握する必要があり，そのためには個々の機器を直接検査する必要がある。本稿では，大学における情報セキュリティ状態の把握として，大学内に存在する情報機器のほとんどを占める PC に限定し，セキュリティ状態の調査を行った結果とその分析結果を述べる.

2. 室蘭工業大学における情報セキュリティ活動

室蘭工業大学（以下、本学という）では、情報セキュリティ維持・向上のため、セキュリティポリシーおよび関連規程に従い、様々な活動を行っている。以下に活動概要を示す.

(1) 大学構成員に対する講習

大学の構成員に対して、基礎講習をはじめとする講習会等を実施し教職員のセキュリティ意識向上を図った。表 1 に、講習の対象者と講習内容を示す。

表 1　対象者と講習内容
Figure 1 Target Parson and Course Contents.

	対象者	講習内容
基礎講習	新規採用・転入者ただし，初開催の 2008 年度は全教職員	法令及び利用規則の遵守 マナーの遵守 パソコン，情報の保護
定期講習	全教職員	最近の脅威の動向（Web によるビデオ閲覧）
システム管理者向け講習	サーバシステム管理者および責任者	システム管理の重要性 最低限知っておくべきセキュリティ対策
役職者向け講習	学長，副学長，理事，監事	ＣＩＯ補佐による本学の情報セキュリティ状況報告

[†] 室蘭工業大学
Muroran Institute of Technology

(2) **技術的セキュリティ対策**

ネットワーク，サーバの対策として，インターネット接続口でのファイアーウォールの設置，スパムメール，Web ウィルス対策を行っている．

また，個々の PC への対策として，全学情報教育システムの一部として，学内にある PC 全台を賄うウィルス対策ソフトを導入している．この大学支給ウィルス対策ソフトによって，教員は各自の研究費等を使うことなく，ウィルス対策を行うことができる．

さらに，部局や研究室などで設置しているサーバに対しては，疑似アタックによる脆弱性検査を行い，脆弱性発見時には改善手法の提示を行っている．

(3) **管理体制**

情報セキュリティの最小管理単位は教員である．教員は研究室ならびに配属されている学生がおり，これが最小のグループとなっている．統制上は全学総括責任者の直下にあり，学科，学部などの組織配下とはなっていない．教員が直接かかわらない事務局あるいはセンターなどは部局としての管理単位となっている．図 1 に本学のセキュリティ管理体制を示す．

PC のネットワーク接続は, 本学では情報メディア教育センターで一括管理しており, 部局内で IP アドレスの発行を行うことはない．したがって，ネットワーク接続状態は情報メディア教育センターがすべて把握している．

3. PC セキュリティ検査

3.1 検査に至る経緯

本学では，情報セキュリティポリシー施行以後，2012 年 1 月現在，PC のセキュリティが原因の情報漏えい，改ざんなどの大きな情報セキュリティインシデントは発生していない．しかし，現在の PC のセキュリティ状況を把握することは，前節で述べた活動の成果確認や今後の活動の見直しに役立つであろうと考えた．また，大学や自治体などの公共機関でソフトウェアの不正コピーなどの問題がいくつか発覚したことから，ソフトウェアライセンスの適正利用に関する証左を収集する観点からも資産管理システムを導入することが検討された．今回用いた資産管理システム (Easy Asset Manager)は PC のセキュリティ状態とソフトウェアライセンス管理の双方の機能を持っているため，このシステムを利用することとなった．

3.2 検査概要

前節で述べたセキュリティ対策を 2008 年度から継続した状態で, 2011 年度及び 2012 年度に学内の Windows 系 PC を対象にしたセキュリティ検査を実施した．Windows 系 PC のみを対象としたのは，この検査を行うことで，学内の大半の PC をカバーできるためである．

2011 年度と 2012 年度では，検査時の状況が異なっている．2011 年度は全学で検査の実施が決定されたが，実際は任意の検査として実施された．また，2012 年度は検査の実施義務およびペナルティを伴うよう学内規程を改訂した．

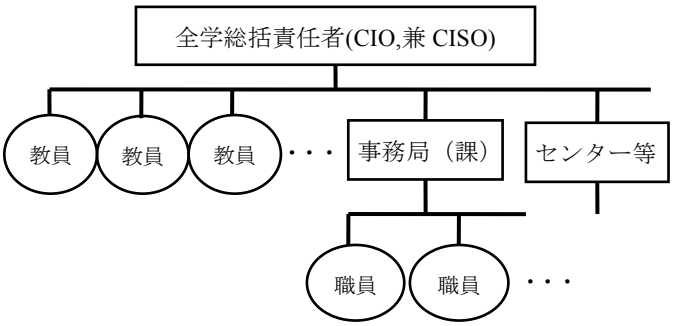

図 1 室蘭工業大学のセキュリティ管理体制
Figure 1 Security Management Organization of Muroran Institute of Technology.

3.3 検査方法

資産管理システムはデータを収集するサーバと，各 PC の情報を収集してサーバへ結果を送付するエージェントソフトで構成される．エージェントソフトは実施の通知文書とともに全教職員に配布した．エージェントソフトにより収集される情報を以下に示す．

表 2 エージェントソフトにより収集される情報
Table 2 Information Collected with Agent Software.

情　報	内　容
Windows Update 状況	Windows Update の設定状態，確認・更新日など
ウィルス対策状況	ウィルス対策ソフトウェア名，ウィルス対策パターン情報など
ソフトウェア集計	インストールされているソフトウェア
プリンタ	設定されているプリンタ
ドライブ	HDD,CD 等の容量，空き容量
ネットワーク	ネットワーク設定情報
詳細情報	コンピュータ名, OS 名, サービスパック，Internet Explorer バージョン，CPU，解像度など
基本情報	コンピュータ名，CPU,メモリ容量など詳細情報の一部

4. 実施結果

4.1 全体受検率

まず, 表 3 に 2011 年と 2012 年の対象 PC 数, 受検 PC 数, 受検率を示す.

表 3 受検 PC
Table 3 Inspected PC.

	2011 年	2012 年
対象 PC 数	1,958	1,759
受検 PC 数	932	1,154
受検率	47.6%	65.6%

対象 PC 数は本学学内 LAN に登録されている Windows 系 PC の数である．この値が 2012 年に減少しているのは，

登録管理簿の整理が行われ，廃棄などで存在していない機器などが削除されたためである．また，受検数，受検率とも 2011 年に比べて 2012 年に増加しているのがわかる．

4.2 データ集計及び分類方法

次に，PC のセキュリティ状況についての結果を示す．表 2 で示した情報の内，セキュリティ検査として，「Windows Update 状況」，「ウィルス対策状況」のデータを用いた．このシステムでは，検査結果を送付した PC に対して固有の ID を付与している．ID から機器を特定するため，「ネットワーク」のデータに記載されている IP アドレスと，学内 LAN の管理簿にある IP アドレスを照合し，管理者の所属で分類した．

我々は，大学内の組織によってセキュリティに対する意識，スキルが異なると考え，以下のように分類して，データを集計した．

1) 学科系教員
ほとんどの教員がここに分類される．本学は，工学部のみの単科大学であるため，PC やネットワークに関する基礎的な知識・スキルを持っているものと推測される．また，卒論生，大学院生を抱える研究室を持ち，保有・管理する PC の数も多い．

2) 共通科目教員
一般教養科目を担当する教員が属する分類である．保有する PC は，ほとんどが各自で業務に利用するためのものである．

3) 事務系職員
事務職員及び図書館，国際センター等に属する職員を分類した．

4.3 Windows Update 状況

図 2-1 から図 2-3 まで示した Windows Update 状況は，更新の実行日と PC セキュリティ検査日との期間である．

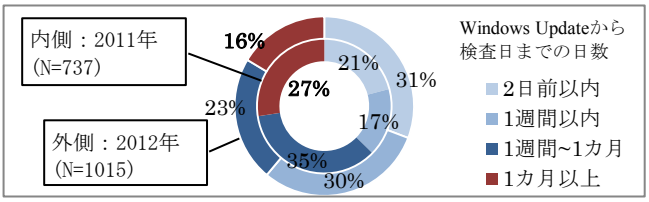

図 2-1 Windows Update 状況(学科系教員)

Figure 2-1 Windows Update Status (teacher who belongs to a subject of study).

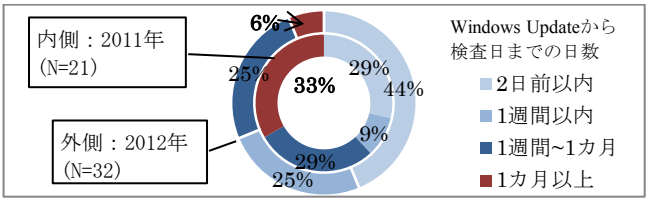

図 2-2 Windows Update 状況（共通科目教員）

Figure 2-2 Windows Update Status (teacher who takes charge of liberal arts).

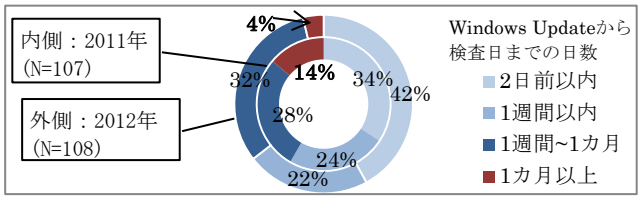

図 2-3 Windows Update 状況（事務系職員）

Figure 2-3 Windows Update Status (Office personnel).

4.4 ウィルス対策状況

ウィルス対策状況は，ウィルス対策ソフトがインストールされているもののうち，最も利用されている Symantec 社，Trendmicro 社，そして McAfee 社のウィルス対策ソフトのウィルス定義ファイル・パターンファイルのリリース日とデータ収集日の差をまとめた．受検した PC のうち，82%(2011 年),92%(2012 年)がこの 3 種のソフトウェアを利用していた．

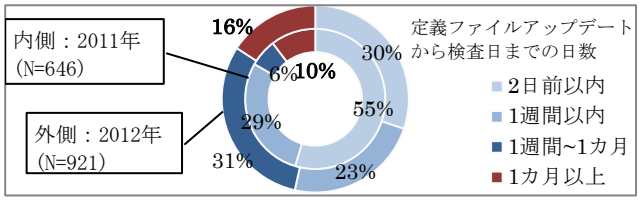

図 3-1 ウィルス対策ソフトの状況（学科系教員）

Figure 3-1 Anti-Virus Software Status (teacher who belongs to a subject of study).

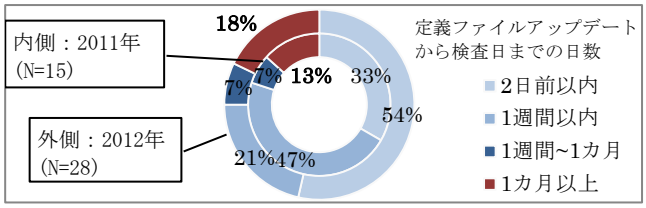

図 3-2 ウィルス対策ソフトの状況（共通科目教員）

Figure 3-2 Anti-Virus Software Status (teacher who takes charge of liberal arts).

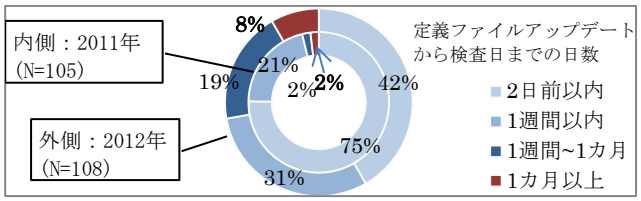

図 3-3 ウィルス対策ソフトの状況（事務系職員）

Figure 3-3 Anti-Virus Software Status (Office personnel).

本学では，McAfee 社のウィルス対策ソフトを一括購入し，校費購入の PC に対しては大学支給として利用可能としている．表 4 にこのソフトの利用率を示す．

表 4　大学支給ウィルス対策ソフトの利用率
Table 4 Rate of Utilization of Antivirus Software Offered by Institute.

	2011		2012	
	導入数/対象数	比率（%）	導入数/対象数	比率（%）
学科系教員	541/737	73.3	557/1075	58.3
共通科目教員	14/21	66.7	13/32	41.9
事務系職員	105/107	97.2	95/108	93.1

5. 考察

5.1 Windows Update について

図 2-1 から図 2-3 の各分類において，更新日から検査日の期間を２日，１週間，１カ月で区分けしているが，１カ月未満の区分けには大きな意味を持たない．Windows Update は基本的にひと月に 1 度であり，それ以外は不定期に緊急の更新がある．最長 1 カ月間アップデートがないこともあり得るため，毎日更新をチェックするようにしていても PC セキュリティ検査を受けた日によっては１カ月近くの期間が空いてしまうこともある．そこで，このデータにおいては，１カ月以上の区分に着目する．

教職員の分類ごとに見ると，この区分はすべての分類で 2012 年（外側）の比率が，2011 年（内側）の値よりも小さくなっている．これは 2011 年よりも適切に Windows Update を適用するようになっていることを示している．そもそも Windows Update は OS インストール時または PC 購入時にすでに，自動的に更新を確認，インストールするように設定されている場合が多い．1 カ月以上の期間が空いている機器の多くは，故意に設定を変更しているものと考えられる．

また，学科系教員は 1 カ月以上の区分の比率が事務系職員に比べて大きい．学科系教員は適切なセキュリティ状況である初期状態で使用せず，セキュリティ状態を悪くするように変更していることが多いと推測される．一方，ほとんどの事務系職員は初期設定のまま，利用する傾向が強いことが多いと考えられる．2012 年の共通科目教員の分類では 1 カ月以上の区分が事務系職員と同程度で，2011 年は学科系教員と同程度の数値となっている．この分類は母数が小さいため経年及び他の分類と比較で差異が大きいが，1 カ月以上の区分は明らかに減少しているため，セキュリティ状態は向上していると思われる．

5.2 ウィルス対策状況について

Windows Update 状況では 2011 年よりも 2012 年の方が 1 カ月以上の区分ではすべての分類で減少しているのに対して，ウィルス対策ソフトの定義ファイルの更新については，すべての分類で増加しており，セキュリティ状態が悪化しているといえる． Windows Update が初期設定のままで良好な状態を保てるのに対して，ウィルス対策ソフトは能動的に対策しなければならない．最近は OS プレインストール PC を導入すると，ウィルス対策ソフトウェアが期間限定版などの形態でインストールされている場合がある．また，特定のソフトウェアをインストールすると自動的にウィルス対策ソフトウェアもインストールされる場合もある．この状態で使い続けることにより，いつの間にかウィルス定義ファイルが更新できなくなり，危険な状態で利用することになる．一方，大学支給のソフトの場合，各自でインストール作業を行う必要があるため，スキルや知識に自信のない利用者は二の足を踏むこともある．また，表４の大学支給のウィルス対策ソフトの利用率をみると， 2010 年と比較して 2012 年は利用率が低下している．この原因として，意図的または恣意的にこのソフトウェアを利用しないことが考えられるが，大学支給のソフトウェアの存在を知らない，あるいは忘れられていることも想定される．このソフトウェアを導入したのは 2010 年 3 月であり，導入当初は以前使用していたソフトウェアからの変更などのアナウンスを行っていたが，その後は積極的な利用促進活動を行っていない．この観点からは，情報センターなどの運用者がサポートや啓発活動を積極的に行う必要があると考えられる．

6. PC セキュリティ管理の課題

6.1 PC 利用者の課題

検査を行った結果からは，事務系職員の分類がセキュリティ状態は良好であることがわかる．むしろ課題を多く抱えているのは，教員であるといえる．実際，文献[2]で報告されている事例でも多くのインシデントは教員によるものである．

本学では，教員は研究費などの独自の予算を持っていることもあり，各自で利用する PC を導入することに対して，事務系職員は課単位など組織的に導入を行っている．これは古くから大学の特徴であり，他の大学でも同様の形態がみられるのではないだろうか．この結果，教員は個人の所有意識が強くなり，PC に対する知識やスキルがあることも手伝ってセキュリティが低い状態に変更することが想定される．一方，事務系職員では PC は組織，延いては大学の備品という意識が強いため，独自の変更を加えることが少ないことが考えられる．

また，研究室を持つ教員の場合，導入自体は教員が行っても，実際の管理を学生任せにしていることも推察される．さらに，研究室内では学生の持ち込み機器などにより，セキュリティ脅威も大きくなる．しかし，セキュリティのために，事務職員と同じ管理形態にするなど，教員の裁量を大きく制限するような管理形態の変更を行うことは難しいと思われる．裁量と責任は一体であり，教員が独自の裁量を持つ以上，それと同等の責任を持つべきである．したが

って，セキュリティインシデント発生時などにペナルティが発生することを認識させることも必要である．結果として，大学としては教員と事務組織のダブルスタンダードが存在することを認識することが必要であると考えられる．

2012 年度に行った検査は規程として義務化したうえで実施されたが，これにより PC のセキュリティ向上が見られたとは判断できない．特にウィルス対策ソフトについては，低下ともみられる結果が表れている．規程はあくまで，”受検“を義務づけるものであり，セキュリティ対する意識向上には直接的につながっていないと考えられる．

これらを解決するためには，まず学内構成員への啓発・教育が第一であると考える．本学のように強制することも一定の効果はあるが，利用者が OS やアプリのアップデートの“必要な行動”をすること，自動アップデートなどの設定を変えるなど“余計なこと”をしないことを身に着けるように教育することが必要であると考える．

6.2 検査実施者の課題

検査自体について検査実施者（情報センター等）の課題としては，十分な体制を準備する必要があることが挙げられる．実施を行うことで発生する技術的問題や利用者からの質問・意見への対応策などを事前に調査・検討する必要がある．実際，今回用いたシステムでは被検査 PC に別途ミドルウェアが必要だったこともあり，実施担当者が対応に追われた．

検査実施当初，本学では検査結果は PC が Windows Update を全く行っていない，ウィルス対策ソフトをインストールしていないなど，特に危険な状態で運用している PC に対してのみ，注意喚起という形で結果を返送する予定であった．しかし， PC 利用者から，「情報の収集結果を知りたい」という意見が数件寄せられたこともあり，PC 利用者が登録している PC の確認の意味で全員に結果を返送した．これによって，ネットワーク機器の登録管理簿の整理を行うことができた．本学では検査実施者と学内ネットワーク管理者が同じ部局であったが，大学によってはセキュリティ対策室と情報センターというように別の部局になることも考えられる．この場合，部局間の連携方法も十分に検討する必要がある．

また，利用者へのフィードバックは，「利用認定」「保証」などといったインセンティブを与える，セキュリティ監査の一部として利用するなど，より効果的なセキュリティ維持活動への活用が考えられる．

7. おわりに

本稿では，室蘭工業大学を事例として，大学の PC 管理の状態を把握し，問題点を挙げた．結果として多くの PC が適切に管理されていることが分かったが，教員の管理する PC では不適切な状態で利用されているものも多く存在した．今後大学における PC 管理の実情を踏まえながら，これらへの対応を行うことが課題となる．

今回行った検査では，実施者の労力がかなり大きく感じられた．義務化した 2012 年でも受講率は低く，2013 年 2 月現在でも未受講者（PC）への照会・督促作業が続いている．しかし，ネットワーク管理部門としては，機器の棚卸の意味でも今回行った検査は大きな意義を持っていると考える．

今回本学では Windows 系 PC に対してのみ検査を行ったが，MacOS や Linux などの OS は無視できない数が稼働している．これらに対しても同様の検査を行うことが必要であると考え，Windows 系以外の OS にも対応したシステムの導入を現在検討している．また，2011 年の検査時には少なかったタブレット PC やスマートフォンも現時点でかなり多くなっている．これらは現在もっとも狙われやすい機器と思われるため，今後の対応が急務である．

参考文献

1) 日本ネットワークセキュリティ協会，2011 年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～ (Feb,2013)
http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.2.pdf
2) 学校情報セキュリティお役立ち Web(Feb,2013)
http://school-security.jp/
3) 情報処理推進機構，情報セキュリティ白書 2012(2012)
4) 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45,No.8,pp.2022-2033(2004).
5) 杉浦昌，諏訪博彦，太田敏澄：教員 PC で発生したセキュリティ事例の分析－組織の IT セキュリティ対策推進モデルを用いた分析，情報処理学会論文誌，Vol.53,No.9,pp.2160-2170(2012).