Vol.2018-IOT-43 No.16
Vol.2018-SPT-30 No.16
2018/9/28

九州大学におけるセキュリティ対策ソフトの切り替え

上田将嗣[†1, a)]　佐々木睦美[†1]　横山大輔[†1]　知識拓弥[†1]
先立英喜[†1]　山本保文[†1]　藤村直美[†1]

概要：九州大学情報統括本部（以下，「情報統括本部」という.）では，2017 年から 2018 年にかけて，キャンパスライセンスを締結するセキュリティ対策ソフトの切り替えを実施した．本稿では，切り替えに至る経緯及び切り替え作業の内容と遭遇した問題点について報告する．

Replacing Anti-Virus Software in Kyushu University

Masatsugu UEDA[†1, a)]　Mutsumi SASAKI[†1]　Daisuke YOKOYAMA[†1]
Takuya CHISHIKI[†1]　Hideki SENDACHI[†1]　Yasufumi YAMAMOTO[†1]
Naomi FUJIMURA[†1]

1. はじめに

1.1 情報統括本部ソフトウェア事業室

九州大学では，情報政策担当理事（CIO，CISO）の下，教育・研究および学術全般並びに大学運営の全てにわたって一元的に ICT 支援サービスを行うために，2007 年度に情報統括本部を立ち上げている．情報統括本部内には，情報サービス毎に事業室を設置し，情報基盤研究開発センターとサイバーセキュリティセンターの教員，情報システム部職員が参画している．

ソフトウェア事業室は，IT の教育・研究環境を整備すること，ソフトウェアのライセンスに関するコンプライアンス（法令遵守）体制を確立すること，大学全体としてのソフトウェア整備に係る経費削減を図ることを目的として，2007 年度からコモディティソフトウェアを全構成員に提供している．ソフトウェア事業室の体制を図 1 に示す．

事業室長	副事業室長	事業室員
専門職員	特任教授　1 課長補佐　1	准教授　1 職員　１１

図 1　ソフトウェア事業室体制図
（2018 年 8 月現在）

1.2 キャンパスライセンス

ソフトウェア事業室が提供しているソフトウェアにはマイクロソフトの Office やセキュリティ対策ソフトがある．セキュリティ対策ソフトに関しては，当初シマンテック社とトレンドマイクロ社の製品をそれぞれ一括契約していたが，需要や価格，事務処理の手間を考慮して，2011 年度からシマンテック社とのアカデミックサブスクリプション契約に一本化し，Symantec Endpoint Protection（以下，「SEP」という.）を学内の全構成員に対して無償で提供してきた．

1.3 BYOD

九州大学では，国立の総合大学として初めて 2013 年度の新入生から PC 必携化（BYOD：Bring Your Own Device）を実施し，2018 年度には 6 年制の医歯薬系学生も含めてすべての学部生が自分自身の PC を使って学習する体制を実現できている．これにより，PC ルームのコスト削減だけでなく，利用者の声を活かしたインフラの整備と教材コンテンツの充実を図り，学生が，何時でも，何処でも，自由に，自分のペースで，より自発的に学習できる環境の整備を推進している．

BYOD を進めるにあたり，全学生の ICT を活用する学習環境を揃え，円滑に学習を開始できるように，毎年 4 月に全新入生を対象とした PC 講習会を開催している．この PC 講習会の際に，セキュリティ対策ソフトのインストールも行っており，85%を超える学生がキャンパスライセンスのセキュリティ対策ソフトをインストールしている状態である．

2. 切り替えに向けて

2.1 切り替えに至る経緯

シマンテック社より，2017 年 6 月～2018 年 5 月の契約を最後に，これまで契約していたアカデミックサブスクリプションを廃止する旨の事前連絡が 2017 年 2 月にあり，2017 年 6 月 2 日付で正式にサービス終了の通知があった．

これを受けて，情報統括本部内で代替サービスの検討を進めることとなった．代替サービスを検討するにあたって

†1 九州大学
Kyushu University
a) ueda.masatsugu.371@m.kyushu-u.ac.jp

は，特に以下の要件に重点を置いて検討を進めた．

- 人数（FTE）契約が可能なこと
  → ソフトウェアの著作権保護に関するコンプライアンス体制の確率が可能
- 学生の個人 PC にインストール可能なこと
  → BYOD には必須
  → 学生を含めた全学的セキュリティの確保が可能
  → 学生の経済的支援につながる

2.2 ソフトウェアの選定

上記の要件を踏まえて検討したうえで，第 3 者評価の結果（Gartner / AV-Test）及び価格等を考慮した結果，トレンドマイクロ社のキャンパスアグリーメント（以下,「トレンドマイクロ」と呼ぶ）を採用 することとした．各ソフトウェアの検討状況を表 1 に，学内における承認プロセスを図 2 に示す．

表 1　各ソフトウェア検討状況

製品名	FTE	学生 PC	価格
S	○	―	―
E	○	○	△
F	○	○	△
M	―	―	―
トレンドマイクロ キャンパスアグリーメント	○	○	○

情報統括本部内承認
　2017/7/26　情報環境整備推進室連絡会議
　　情報統括本部運営会議
全学委員会承認
　2017/9/6　情報政策委員会
　2017/9/11　役員協議会
　2017/9/19　部局長会議等・教育研究評議会

図 2　学内承認プロセス

2.3 トレンドマイクロキャンパスアグリーメント

トレンドマイクロキャンパスアグリーメントの概要は以下のとおりである．

- 契約方式
  → 人数（FTE 数）契約（教職員・学生・名誉教授）
- 対象
  → 大学所有パソコン
  → 構成員が大学に持ち込む可能性がある端末（1 人当たり Windows，Mac，モバイル端末計 3 台まで）

キャンパスアグリーメントで利用可能なトレンドマイクロ社製のソフトウェア一覧を表 2 に示す．

表 2　利用可能なソフトウェア一覧

対象	ソフトウェア
Windows	ウイルスバスター Corp XG （以下,「ウイルスバスターCorp」という．）
Mac	Trend Micro Security for Mac （以下,「TMSM」という．）
Linux	Server Security for Linux
他	Server Protec for Windows Control Manager Mobile Security

3. 切り替え作業

3.1 スケジュール

利用者の移行期間をできるだけ長く確保するために，トレンドマイクロの提供開始を 2017 年 12 月 18 日とした．しかしながら開始の通知を部局宛に通知した直後に，準備した管理サーバの設定では問題が発生することが明らかになり，これへの対応を考慮して，管理サーバの運用方法を変更するなど，対応に時間を取られ，最終的には提供開始を 2018 年 1 月 11 日に延期した．そのため切替期間が若干短くなった．

シマンテック社との契約は 2018 年 5 月末までなっており, それまではトレンドマイクロと SEP を並行運用できる．ただし，できるだけ 2017 年度末までに移行作業を完了したいこと，アナウンスする締め切りまでに切り替えを完了できない利用者（教員は締め切りを過ぎないと作業に取り掛からない者が多い）のことも考慮して，2018 年 3 月 16 日を当面の切り替えの締め切りとした．ただし現実には予想通り，5 月末を過ぎても SEP を使っている PC が残り，それらの駆逐に時間を取られている．

また，2018 年度の新入生に対しては，4 月の PC 講習会の際にトレンドマイクロをインストールさせることとした．

3.2 管理サーバ構築

管理サーバを構築するにあたり，オンプレミスとクラウド利用の比較を行い，コストの面からオンプレミスに環境を構築することとし，想定されるインストール台数等から管理サーバ群の構成を, 管理サーバ 3 台（Windows 用 2 台，Mac 用 1 台）と SPS サーバ 3 台に決定した．管理サーバ群のスペックを表 3 に示す．

当初，すべてのサーバに対して学内からのアクセスのみ許可する方針としていたが, 後述する, Windows Update RS4 対応のために，Mac 用管理サーバを SPS サーバと兼用としたうえで，3 台の管理サーバについては学外からのアクセスを許可することとした．管理サーバ群の構成図を図 3 に示す．

表 3　管理サーバ群スペック

管理サーバ（Win）①・② 管理サーバ（Mac）兼 SPS サーバ④	
CPU	2.1GHz×8 コア
メモリ	16GB
形態	ベアメタル
SPS サーバ①・②・③	
CPU	2.1GHz×2 コア
メモリ	2GB
形態	仮想マシン

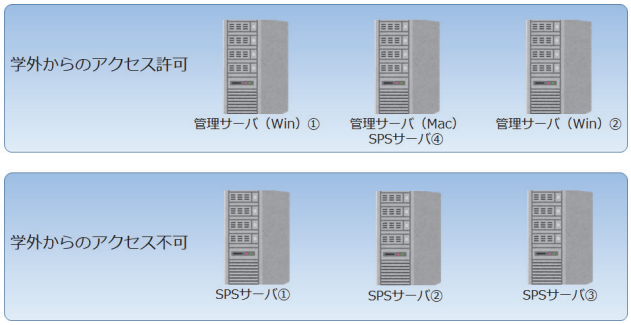

図 3　管理サーバ群構成図

3.3 学内への周知

全学委員会での承認後，各部局に出向き教職員を対象とした部局説明会を行うこととし，2017 年 10 月から 2018 年 1 月にかけて学内 22 部門を対象に実施した結果，合計で 1,163 名が参加した．

他にも，学内全構成員を対象とした各部局長向けの通知を，予告及びシマンテック社サービス終了を含めて，7 回実施した．なお，この通知は学生ポータルにも掲載するとともに，連動して全学生に個別メール配信を行うことで，学生向けの周知を図った．

さらに，周知の徹底を図るため，生協食堂において，卓上 POP の設置，トレイ広告への掲載，生協売店でのポスター掲示を行った．また，情報統括本部が発行する刊行物（IT だより 2018 年 3 月発行）にもセキュリティ対策ソフトの変更に関する記事を掲載した．

4. 問い合わせ対応

4.1 問い合わせの分析

2018 年 1 月 11 日にトレンドマイクロを提供開始した直後から，多くの問い合わせが寄せられた．問い合わせ件数の推移を図 4 に示す．

問い合わせ内容を分析したところ，全体の 70%の問い合わせが，以下の 4 つの分類に入ることが分かったため，重点的に対応を進めることとした．

図 4　問い合わせ件数推移

- ウイルスバスターCorp のインストールに失敗する．
- ウイルスバスターCorp インストール後，動作が不安定になる．
- TMSM (Trend Micro Security for Mac)のインストールに失敗する．
- TMSM インストール後，「保護が無効」のままになる．

4.2 ウイルスバスターCorp のインストール失敗

主な原因は，他のセキュリティ対策ソフト（トレンドマイクロ社の他製品を含む）がインストールされている，またはその残骸が残っているケースであった．

(1) **SEP**

エラーメッセージ

“Office Scan supports automatic uninstallation of Symantec Endpoint Protection XXXX ・・・・”

原因

SEP のアンインストールが不完全

対応

SEP 削除ツールの再実行
レジストリキーの削除

(2) **ウイルスバスタークラウド**

エラーメッセージ

“Unable to automatically uninstall Trend Micro Titanium Maximum Security 2012 x64”

原因

ウイルスバスタークラウド（ほとんどの場合体験版）がインストールされている

対応

ウイルスバスタークラウドのアンインストール

(3) **ビジネスセキュリティクライアント**

エラーメッセージ

“ウイルスバスター Corp. クライアントをバージョン

Vol.2018-IOT-43 No.16
Vol.2018-SPT-30 No.16
2018/9/28

アップできません．・・・”

原因

ウイルスバスタービジネスセキュリティクライアントがインストールされている

対応

ウイルスバスタービジネスセキュリティクライアントのアンインストール

(4) **ウイルスバスターCorp**

エラーメッセージ

“すでにインストールされています．・・・”

原因

ウイルスバスターCorp のアンインストールが不完全

→ 後述するインストール後の動作が不安定なケースで，再インストールを繰り返す際に，アンインストール後再起動を実施しなかった等

対応

レジストリキーの削除

(2)及び(3)は，エラーメッセージから当該ソフトウェアを特定することが難しかったため，解決までに時間を要した．また，特に(4)に関しては，複数のレジストリキーの削除等複雑な作業が必要であったため，削除ツールを別途準備することとした．

4.3 ウイルスバスターCorp インストール後，動作が不安定になる

他のセキュリティ対策ソフトとの競合が主な原因であった．ソフトウェアとしては，McAfee LiveSafe，Intel Security Assist，ESET 等があった．対応策として，Windows をセーフモードで起動しウイルスバスターCorp をアンインストールした後，競合ソフトウェアのアンインストールを行った．

この中で，McAfee LiveSafe については，生協が販売する新入生向けの推奨 PC にプリインストールされていることが判明し，このままでは PC 講習会で大きな混乱が生じる可能性が高いことがわかった．このため，直ちにトレンドマイクロ社と対応を協議し，2018 年 3 月 16 日に修正パッチが提供され，McAfee LiveSafe がインストールされている状態では，ウイルスバスターCorp のインストールができないようにした．

ほとんどの場合，SEP 利用時には問題なく動作しており，他のセキュリティ対策ソフトとの競合を考慮しなかったため，ソフトウェアの特定に時間を要した．最終的には，インストールされているソフトウェアの一覧を取得するスクリプトを作成し，その実行結果を確認することで，競合ソフトウェアを特定した．

4.4 TMSM のインストール失敗

4.2，4.3 と同じく他のセキュリティ対策ソフトとの競合が主な原因であった．ソフトウェアとしては，ウイルスバスタークラウド（体験版を含む），SEP，McAfee LiveSafe，ClamXAV，MacKeeper 等があった．

TMSM はインストール失敗時に「ソフトウェアの製造元に問い合わせてください．」と表示されるだけであり，原因の特定が困難であった．そこで，トレンドマイクロ社と協議の上，ウイルスバスタークラウド体験版のインストールを試すことで，競合ソフトウェアを特定することとした．TMSM インストール失敗時のエラーメッセージを図 5 に，ウイルスバスタークラウド体験版インストール時のメッセージを図 6 に示す．図 6 では，問題になったセキュリティ対策ソフトウェアの名称が表示されていることがわかる．

図 5　TMSM インストール失敗時のメッセージ

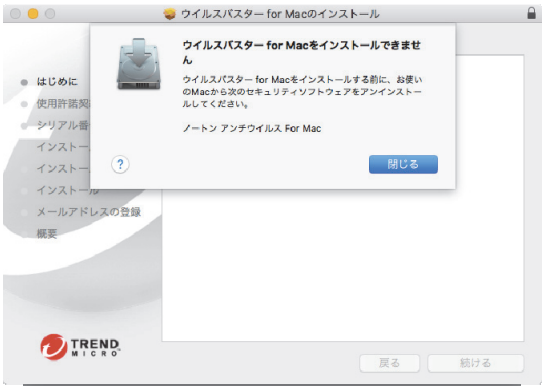

図 6　ウイルスバスタークラウド体験版
インストール失敗時のメッセージ

4.5 TMSM で「保護が無効」となる

当初，インストールは完了したが「保護が無効」となるとの問い合わせが数多くあった．調査の結果，TMSM が利用するポートを部局のファイアウォールで遮断しているこ

とが原因であった．

この影響で，2018 年 1 月 23 日から 3 月 1 日かけて，TMSM の提供を中断することとなり，TMSM に関しては，切り替えの締め切りを，3 月 26 日に延期することとなった．

4.6 研究室訪問

メールや電話では対応が難しい案件があり，問い合わせ対応の一環として，トレンドマイクロ社のスタッフとソフトウェア事業室のメンバーが，不具合の起こっている利用者の研究室（合計 30 ヶ所）に出向き，直接 PC を確認し，改善及びログの収集作業等を実施した（表 4）．

表 4　研究室訪問状況

日付	キャンパス	件数
2 月 16 日	伊都	2
2 月 20 日	伊都	5
2 月 26 日	馬出	3
	箱崎	1
2 月 28 日	伊都	2
	馬出	2
3 月 8 日	馬出	2
3 月 13 日	伊都	1
3 月 15 日	伊都	1
3 月 16 日	伊都	2
3 月 23 日	伊都	1
3 月 26 日	馬出	2
3 月 29 日	馬出	2
5 月 24 日	箱崎	1
7 月 4 日	箱崎	2
7 月 19 日	伊都	1

※下線はトレンドマイクロ社が同行

また，上記以外に新入生 PC 講習会（4 月 2 日，4 月 3 日開催）の際にも，トレンドマイクロ社の技術者に講習会会場に待機してもらい，その場でトラブル対応を行った．

4.7 TMSM 予約検索

TMSM の予約検索は，管理サーバにおいて一括管理され，各端末で個別に予約検索のタイミングを設定できないため，使い勝手の悪い仕様となっている．

本件に関して，トレンドマイクロ社より TMSM で手動検索を実行するコマンドの情報を入手し，これを crontab に登録することで予約検索に近いことを実現できることがわかった．しかしながら，Mac 利用者にとって crontab の編集は，ハードルが高いケースもあると考え，GUI ベースで編集できるツールを開発・公開することとした．GUI ツールの画面を図 7 に示す．

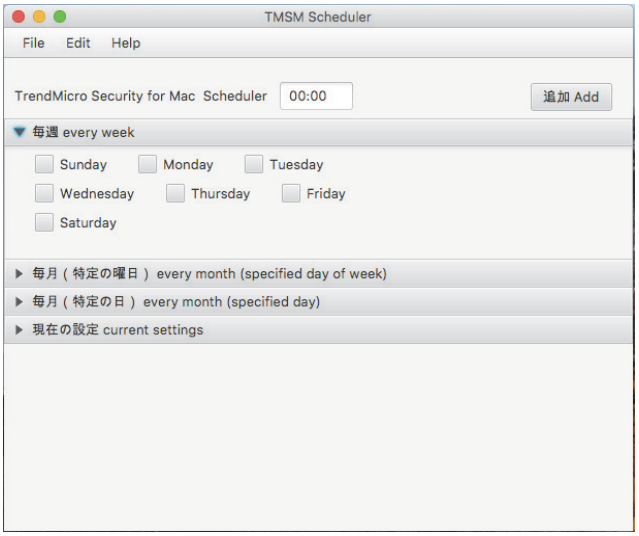

図 7　TMSM 予約検索 GUI ツール

5. Windows 10 RS4 対応

5.1 ウイルスバスターCorp の Windows10 RS4 対応

2018 年 5 月末の SEP の契約期限に向けて切り替え作業を進めている中で，4 月末に Windows 10 RS4 の提供が開始され，5 月 25 日ごろから Windows Update が本格化した．一方，ウイルスバスターCorp の RS4 への対応は，当初は 5 月中旬の予定となっていたが，予定が遅れ，最終的に 6 月 12 日に RS4 対応のウイルスバスターCorp がリリースされた．その結果，　ウイルスバスターCorp の RS4 対応が Windows Update の本格化に間に合わなかったため，結果的に，動作が不安定になるだけでなく，OS の再インストールが必要となるケースも含めて，多くの利用者が多大な影響を受けた．

こうしたトラブルに不満を抱いた利用者が新聞社にトラブルについての情報提供をしたために本件が新聞記事になった．その結果，大学のセキュリティレベルが低下していることが外部に対して周知の事実となり，悪意のある攻撃者に絶好の機会と捉えられた可能性があること，また報道機関への対応などのために，本来はセキュリティ対策ソフトウェアの問題対応に投入すべき人的資源をメディア対応に取られて，悪影響が出た．

5.2 ソフトウェア事業室の対応

ソフトウェア事業室では，5 月 2 日の段階で，ウイルスバスターCorp が RS4 に対応していない旨を，Web ページに掲載した．しかしながら，Windows Update の本格化後に問い合わせが急増したため，緊急対応として 5 月 30，31 日に，学内の全構成員に対して一斉メールで依頼した．その際，依頼した緊急対応は以下のとおりである．

- Windows10 Pro/Education 利用者
  - •Windows Update の延期

- ウイルスバスターCorp のアンインストール及び Windows Defender の利用

- Windows10 Home 利用者
  - Windows10 Education へのアップデート後，Windows Update の延期
  - ウイルスバスターCorp のアンインストール及び Windows Defender の利用

Windows のバージョンに応じて，Windows Update を延期可能なものは延期をし，延期できなものはウイルスバスターCorp の代わりに Windows Defender を利用してもらうということである. なお, Windows Defender を利用するには，ウイルスバスターCorp のアンインストール後，レジストリキーの削除も必要であったため，その情報も併せて提供した.

その後，6 月 12 日に RS4 対応のウイルスバスターCorp が提供されるにあたり，学外の PC にも早急にパッチを配布・適用する必要があると判断し，管理サーバの学外からのアクセス制限を解除した.

5.3 対応遅延に伴う影響拡大の原因

今回，ウイルスバスターCorp の RS4 対応が遅れたことによる影響は，一部の PC では OS の再インストールが必要になるものが出るなど，甚大であったが，その原因は以下の 3 点であると考えており，特に事業室としては利用者向けの情報発信について，さらに積極的に行っていく必要があると考えている.

- ウイルスバスターCorp の RS4 対応遅れ

トレンドマイクロは当初は 5 月 12 日に RS4 対応版を提供する予定であったが，その直前にマイクロソフトが Windows 10 の大幅な仕様変更を行なった．クラウド版と Mac 版はこの仕様変更の影響が少なく予定通りの出荷となったが，コーポレートエディション版では仕様変更への対応に手間取った．他のセキュリティ対策会社はこの仕様変更に対して，「機能制限あり」という形で見切り発車をしたようであるが，トレンドマイクロは RS4 に完全に対応してから提供しようとした．そのために RS4 対応版の出荷が 6 月 12 日に延びた.

- Windows10 Home Edition の Windows Update 機能への認識不足

Windows 10 には Home, Enterprise, Education といくつかの種類がある．Window Update の機能について見ると，Home では利用者が Windows Update の更新時期を制御できず，マイクロソフトの意向に従って自動的に Windows Update が行われる．Home を除く Windows 10 では Windows Update の実行を利用者が制御でき，特に Creators Update については 180 日間停止できる．ウイルスバスターCorp を利用している企業は通常 Windows10 Home でなく，Windows 10 Enterprise を利用しており，組織としては統制も取れているので，一括して Windows Update の延期を行える.

一方，大学では価格の都合などで，Windows 10 Home を使用する利用者が多く，Windows Update の実行を延期できない状況であった．これをトレンドマイクロも大学自身も明確に認識していなかった．そうした中で，ウイルスバスターCorp が RS4 に対応できていないにも関わらず，Windows 10 Home ではこの Windows Update がマイクロソフトの制御の下で自動的かつ強制的に行われた．これによって毎日一定数の PC にトラブルが発生することになった.

- ソフトウェア事業室の情報発信が不十分

問題を把握した後でも，その影響を正しく想像できなかったために，Windows Update を止められない Windows 10 Home から Windows Update を延期できる Windows 10 Education へ，包括契約を利用して切り替えるように迅速に指示できなかった．またウイルスバスターCorp の代わりとして Windows の Defender で良いという判断も当初は自信がなく，決断が遅くなった.

6. SEP への対応

2018 年 5 月末で SEP の契約が終了することから，全ての SEP の利用を停止する必要がある．そのために切り替え依頼の通知などを鋭意行って来たが，予想通り，トレンドマイクロ等に切り替えてもらえない例が多々あった. そこで，毎週 3 日間の SEP の管理サーバへのアクセスログから SEP をアンインストールしていない PC（正確には IP アドレス）を調べて，支線 LAN 管理者を通じて，対応を依頼する措置を取った.

当初は対応が順調に進んでいたが，ある時期からなかなか SEP のアンインストールが進捗しなくなって来た．原因は，利用者が日々使用している PC については順調に切り替えが進むが，日頃直接操作していない PC については誰もその存在さえ意識していないために，対象として誰も気にしていないものが残っているらしいことが判明した．例えば各種情報システムの無人で稼働している管理サーバ，さらにそれらのバックアップサーバ，ファイルの自動バックアップサーバなどである.

研究室などでは無線 LAN を使うための DHCP ルータが設置され，これの配下に多くの PC が接続されている．この DHCP サーバの下に接続されている PC で SEP が使用されていると，事業室からの連絡は DHCP サーバの IP アドレスを連絡することになるために，その配下の PC のどれ

が切り替え未完了のものかを判断することが容易ではない．そのため支線 LAN 管理者から追加の情報を請求される例があるが，それでも台数が多い場合には支線 LAN 管理者の負担が大きくなった．

図 8 に切り替えが完了していない PC の台数の推移を示す．当初の SEP 利用台数の 1 %弱であるが，次第に減少しながらもなかなかゼロにならないことがわかる．SEP のパターンファイルの更新は 6 月最初からできないようにしており，PC の画面に警告が表示されているはずであるが，なかなか進捗しない状況が続いている．

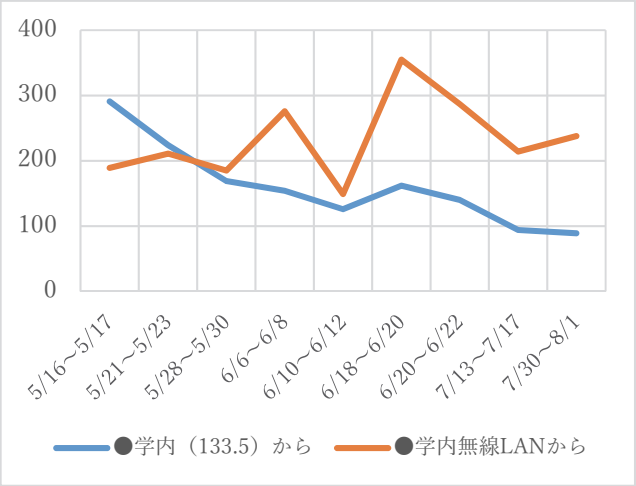

図８　SEP 未切り替え台数の推移

7. おわりに

本稿では，九州大学におけるセキュリティ対策ソフトの切り替えと遭遇した問題点について報告している．多くのトラブルが発生したが，8 月 31 日現在，Windows と Mac を合わせて約 2 万 3 千台の PC にウイルスバスターはインストールされており，九州大学のセキュリティレベルの維持・向上に寄与しているものと考えている．またこの切り替え作業を通じて，利用者自身もセキュリティに関連する意識が向上したと考えている．

通常はこうした大学全体で包括契約をして採用しているセキュリティ対策ソフトウェアを変更することは少ないと思うが，今回はセキュリティ対策ソフトウェア会社の都合で，止むを得ず切り替えを行った．同様のことが他大学においても起こっているのであれば，本稿が今後セキュリティ対策ソフトの導入・切り替えを検討している各機関の参考となれば幸いである．

今後の対応として，以下のような点を考えている．

- 利用者対応としては Windows Update を延期できるように，Windows 10 Home から Windows 10 Education へのライセンスの切り替えを促進する．
- 万が一，Windows の大幅な仕様変更が発生する時の初動をよくするために，Windows Update へのトレンドマイクロの対応状況を確実に把握できる連絡体制を実現する．
- トレンドマイクロ社とマイクロソフト社の間で情報共有や意思の疎通が円滑に行えるような体制の実現を要望し，同様の問題が発生しないような体制の構築に貢献する．

謝辞　セキュリティ対策ソフトの切り替え作業に際し，多大なご協力をいただいたトレンドマイクロ社の関係者に，謹んで感謝の意を表する．また様々なトラブルに遭遇し，その結果，手間のかかる作業を辛抱強く行っていただいた利用者にも感謝します．

参考文献

[1] Naomi Fujimura, Itsuo Omagari, Masatsugu Ueda, and Keiichi Irie : Experience with Software Blanket Contract in Kyushu University, Proc. of SIGUCCS 2008 (Poster Session), pp.307-310, Oct. 2008.
[2] 藤村直美 大曲五男 上田将嗣 入江啓一，九州大学におけるソフトウェア一括契約と運用上の問題，情報処理学会研究報告インターネットと運用技術(IOT) 2008(15(2008-DSM-048)), 67-72, 2008-03-07
[3] 入江啓一 藤村直美 渡部善隆 富山実 三浦誠 上田将嗣 高木早智子 仲田奈理子 酒井健禎，コンピュータソフトウェアのキャンパスライセンス化による経費削減効果について，情報教育研究集会講演論文集 2008 年度, 583-586, 2008