原著論文

学術情報処理研究 No.24
JACN 2020年
DOI:10.24669/jacn.24.1_48

徳島大学におけるクライアントOSのサポートライフサイクル管理

A management of the support life cycle for client operating systems in Tokushima University

板東 孝文，竹内 寛典，上田 哲史，松浦 健二

Takafumi BANDO, Hironori TAKEUCHI, Tetsushi UETA, Kenji MATSUURA

{bandou.takafumi, takeuchi.hironori, ueta, ma2}@tokushima-u.ac.jp

徳島大学 情報センター
Center for Administration of Information Technology, Tokushima University

概要

大学など研究機関は，常にサイバー攻撃の脅威にさらされており，水際である PC，および搭載 OS のセキュリティ対策の需要が高まっている．本学では，構成員が使用しているクライアント機器の OS について，新たな方針の策定と，既存の情報システムを利用した OS 更新の促進のための施策を実施した．これら施策は，大学組織の構成員の多様性を考慮して設計されている．学内の認証基盤の網羅性に着目し，そのログを用いて利用者と利用 OS を推定，対象となる OS の利用者に対しては個別メールによる OS 更新の周知促進を行った．本論文では，その実践事例と効果，今後の課題について述べる．

キーワード

OS, Windows, macOS, Shibboleth

1 はじめに

昨今，IT 技術の発展と社会的な浸透によって，さらなる情報化の推進が進んでいる．また，情報や技術をただ蓄積するだけではなく，どのように共有・展開し，変革を行っていくのか，といった観点から，Society 5.0 や，Digital Transformation といった概念が注目されている．

教育現場にも同様の傾向が見られ，大学法人においても，学生の PC 必携化 [1]，書類の電子化 [2] などの前衛的な施策が行われており，教育・研究のみならず，一般的事務作業においても，情報技術の重要性が増している．こういった状況から，大学の構成員の PC の利用率は高く，特定のクライアント機器を個人が占有して使用する傾向がある．また，組織の情報資産と構成員を紐付けるデバイスであるという点から，クライアント機器は情報セキュリティの観点からも重要である．情報セキュリティ 10 大脅威 [3] においても，個人が使用するクライアント機器が起点となる事象が上位に挙げられている他，過去の他大学の報告 [4] では，学内の機器を集計した結果，27%の機器が適切なセキュリティ対策が行われていない機器として検出された．こういった背景から，クライアント機器の情報セキュリティ対策は必要不可欠であると言える．つまり，大学法人における情報セキュリティを担当する部門は，クライアント機器と，それを使用する構成員に対し，環境の多様性を考慮したうえで，適切な情報セキュリティ対策に取組まなければならない．大学法人におけるセキュリティ対策としては，他大学から，サーバ脆弱性診断と，その結果を考慮した効果的なセキュリティマネジメント手法が提案されている [5][6]．しかし，それらの手法は主にサーバとその管理者を対象としたものであり，クライアント機器へ

のセキュリティ対策としては，必ずしも親和性が高いわけではない．一般的にクライアント機器の利用環境は，サーバ機器よりも多岐にわたり，それを配慮した上での取組みが必要である．また，機器を利用する利用者に着目すると，大学の構成員は，教員，職員，学生に大別されるが，クライアント機器の使用状況も異なり，情報スキルの習熟レベルや遵守すべきセキュリティレベルにも大きな差異がある．情報セキュリティの確保という点において，こういった環境に対する大学法人として一貫性のある網羅的な対応を行う必要がある．そのためには，組織内で使用されるクライアント機器について，一元的かつ恒久的な運用環境の実装が必要である．

一方，2019 年度には，Microsoft 社が提供する OS，Windows 7 のサポートが終了した．本学における Windows 7 のシェア，また脆弱な OS が学内で使用されることで発生するリスクを考慮すると，当該 OS のサポート終了が与える影響は大きいと考えられた．また，シェアの高い OS としては，macOS も挙げられる．macOS に関しては，毎年最新のバージョンがリリースされることが慣例となっており，バージョンの管理については，個人の運用コストが高く，不適切な運用がセキュリティリスクとなる可能性がある．情報セキュリティの担保のためには，全学的な指針が必要である．

そこで，情報センターでは，一定の情報セキュリティ水準を確保するため，学内で使用されるクライアント機器の OS に関する方針を提案した．本学におけるクライアント機器は，各部局の責任者の管理の下で利用されているが，その詳細な管理方法に関しては部局の裁量で行われており，全学的には一元管理されていない．他大学では，IT 資産管理システムを利用した情報資産の管理手法 [7] が提案されており，本学においても一部のクライアント機器について，同様の資産管理システムが導入されている．しかし，全学的に同様の手段で資産管理を行うためには，費用的にも人的にも大きなコストが必要となる可能性が高く，また，即効性が低いため，期日を要する本取組には適さない．

一方，他大学において，認証ログを利用した情報システム [8] が開発されており，認証ログを情報元として構成員の情報を収集することについては，一定の成果が挙がっている．これは認証ログの継続性，網羅性の高さによるもので，本学においても，全学的に利用されている認証システムのログを利用することにより，クライアント機器の利用状況を集約的に取得できる可能性がある．

ログそのように獲得した情報からクライアント OS のサポートライフサイクルへアプローチすることで，全学的な観点から情報セキュリティ環境の向上に貢献することが期待できる．

2　クライアント機器の環境

2.1　セキュリティポリシー

本学では，情報セキュリティ水準の確保と情報セキュリティのマネジメントを目的として，2004 年度にセキュリティポリシーが策定された．その中で，クライアント機器に関する項があり，他の情報機器にアクセスすることで処理を行うものと定義されている．また，大学資産の機器だけではなく，業務もしくは教育・研究の用途で学内に持ち込まれる個人資産の機器についても同様である．本学における，クライアント機器のセキュリティポリシー上の管理体制の概略を図-1 に示す．クライアント機器については，部局情報セキュリティ管理者，もしくはシステム管理者が当該機器の管理者とされる[1]．これら管理者はクライアント機器管理手順にしたがって適正な管理を実施しなければならない．本論文で述べる取組みに関しては，ポリシー上で規定されたクライアント機器とその管理者を対象とする．

2.2　構成

本学におけるネットワークの構成図を図-2 に示す．本学のネットワークは，大きく分類すると，教育系ネットワーク，研究系ネットワーク，事務系ネットワークに分類される．別途，病院系ネットワークが存在するが，これは SINET[9] に接続されておらず，PC やその OS についての厳密な管理体制が構築されているため，本論文で述べる取組みの適用範囲外とする．教育系ネットワークには，各 PC 教室の教育用 PC が接続されている．教育用 PC は，主に学生が講義・演習の用に供しており，管理は情報センターおよび，部局管理者が行う．

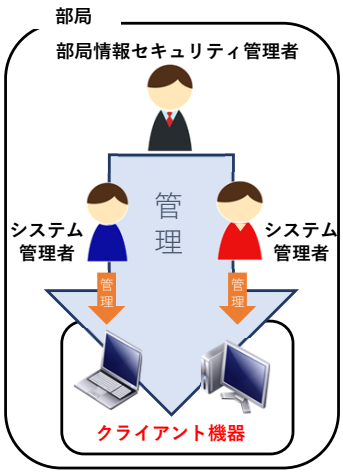

図- 1: 管理体制

[1]部局によっては，別途システム管理者が設定される

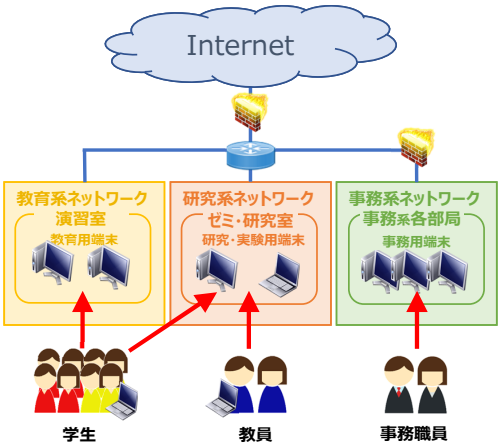

図- 2: ネットワーク構成図

研究系ネットワークは，主に教員とその配下のゼミ・研究室向けに提供されているネットワークで，各部局の責任者が管理している．このネットワークには，基本的には各構成員が必要とするクライアント機器やサーバなどを，部局の判断で接続しており，校費で購入された機器だけではなく，教員が私費で購入した機器や，学生の持込み端末なども接続される．

事務系ネットワークは，事務系職員が利用する業務系ネットワークである．セキュリティ確保のため，他ネットワークとの間には専用のファイアウォール機器が設置されている．また，事務系ネットワークの管理は，本学の事務組織内の担当部局が統括的に行っている．

3　対応の方針

本学は，2019 年度に，学内で利用されるクライアント機器の OS について，サポート期限の観点から基準となる方針を策定した．この方針は，情報センターにおいて学内のクライアント機器の利用状況調査などを経て検討され，本学における情報化施策の意思決定機関である情報戦略室によって策定された．本方針は，本学において，セキュリティポリシーの下，恒常的，普遍的に適用される．

3.1　基本的な考え方

本項で述べる方針は，本学の情報セキュリティを担保するために構成員が使用するクライアント機器について，一定の利用条件を定めるものとする．利用条件についての基本的な考え方を以下に述べる．

- Windows などサポート期間の定めのある OS はサポート期間に含まれているものとする．
- macOS などサポート期間の明示的な定めのない OS は，最新の OS バージョンとする．ただし，原則として，最新から 2 世代前の OS までを本学での利用可能対象とする．
- 評価版・テスト版等は原則として利用を認めない．
- スマートフォンの OS は，提供ベンダのサポート状況に従う．

3.2　クライアント OS 区分

利用条件を基に，より直感的に把握できるよう，クライアント OS の区分を作成した．表-1 に示す．これらのステータスは本学の定義したものであり，利用制限の適用範囲は本学内となる．ここでの学内とは，学外からの学内ネットワーク接続も該当する．例えば，VPN を利用して学内ネットワークに接続する場合は，本方針の適用内となる．原則として，イエローの区分に該当するクライアント機器の利用者には注意喚起を行う．また，レッドの区分に該当するクライアント機器は，本学の情報システムの利用について一部制限をかける．これらの詳細については，次節以降で述べる．

表-1 の区分を基に決定した 2020 年 7 月現在の代表的なクライアント OS のステータスを表-2 に示す．なお，Windows においては，サポート期間内の OS であっても，サポートが終了している Update バージョンが存在する．これに関してはセキュリティ更新プログラムが適用されないため，利用不可とする．また，表-2 における macOS の利用可能バージョンについては，表-1 での定義より，最新から 2 世代前の 10.13，10.14 が本来の利用可能バージョンであるが，macOS 10.12 も利用可能とし

表- 1: クライアント OS 区分

ステータス名	分類	意味
グリーン	最新バージョン	正式リリース後のメジャーリリースでの最新バージョン
イエロー	旧バージョン	サポート期間の定めのある OS のうちサポート期限内であるもの サポート期間の定めのない OS は，原則として 2 世代前の OS まで
レッド	利用不可	上記いずれにも該当しない古いバージョン．サポート終了の OS リリースプレビュー版，RC 版，評価版，プレリリース版，開発版など

表- 2: クライアント OS ステータス

ステータス名	クライアント OS バージョン	
	Windows	macOS
グリーン	10	10.15
イエロー	8.1	10.12～14
レッド	7 以前	10.11 以前

ている．これは，現時点での学内で利用される macOS 10.12 の台数の多さと，情報センターの対応リソースを考慮し，暫定的に特別対応を行っている．

4　クライアント OS への対応

本節では，前節で述べた方針に基づき行ったクライアント機器に対する OS 更新対応について述べる．2019 年度の対応としては，サポート期限終了日までに学内で利用される Windows 7 を無くすことと，ステータスがレッドの macOS の利用を段階的に削減し，最終的には無くすことを目標として設定した．おおまかな対応フローを図-3 に示す．なお，それぞれの OS に対し，学内への影響に鑑みて，期日を考慮しつつ，異なるスケジュールで並行に対応を進めた．

4.1　スケジュール

対応の大まかなスケジュールを図-4 に示す．Windows 7 はサポート終了日を期日として，各種対応を行った．また，macOS に関しては，各バージョンの学内の検出数から想定される影響範囲を検討し，適時対応を行った．図-4 における横棒線は，当該の期間に継続的に対応を行ったことを表す．また，丸は特定日に対応を行っている事を表している．破線については，継続して利用調査を行っているが，後述する利用制限措置により，実質的には検出されることはないことを表す．

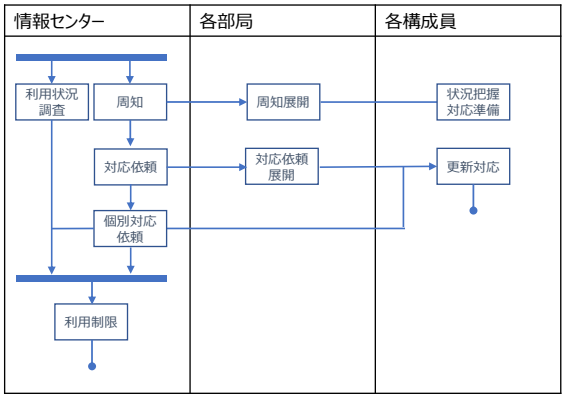

図- 3: 対応フロー

4.2　対応の詳細

4.2.1　利用状況調査

OS 更新対応について，対応ボリュームの推定とスケジュール策定のため，利用状況の調査を行った．まず，包括ライセンスにより全学的に導入されているセキュリティソフトの管理サーバにおけるセキュリティソフトの導入 PC リストから，2019 年 5 月 31 日時点の Windows 7 の台数を取得した．その後，各部局への周知と対応依頼を散発的に行い，再度，2019 年 9 月 16 日に台数を取得した．また，セキュリティソフトが必ずしも全ての機器に導入されていないので，より調査の精度を高めるため，各部局向けに利用状況アンケートを実施した．そこでは，使用している OS と台数について照会するとともに，更新対象となる OS を使用している場合は，今後の対応方針について回答を促した．表-3 に，これらの調査による検出数を示す．

表-3 から分かるように，各部局への周知と対応依頼によって，検出数は減少傾向となった．特に，事務局の機器については，事務組織内の情報担当部局が 2019 年 9 月 16 日以降から 10 月 17 日にかけて，計画的に更新対応を行ったことにより，大きく減少している．しかし，他の部局については，アンケートからの検出数から，セキュリティソフトが未導入の機器が多数存在することが分かる．また，2019 年 5 月 31 日から 9 月 16 日への推移から，減少ペースを上げる必要があると判断した．そのためには，機器の管理者に対して直接的に対応の促進を行わなければならない．そこで，より網羅的な手段を検討した結果，各種情報システム用の認証サーバなどが所有している情報を援用し，情報を補完する対応を行った．なお，本学では全学を対象とした認証機構として，

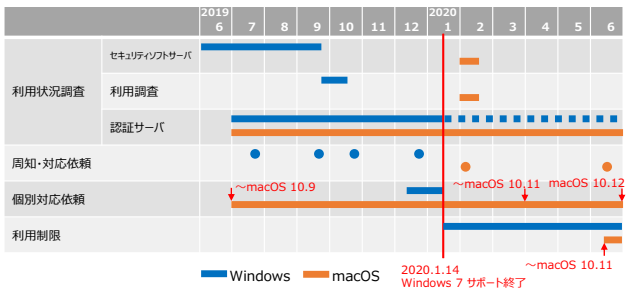

図- 4: 対応スケジュール

表- 3: 各調査による Windows 7 検出数

調査手段	セキュリティソフト		アンケート
調査日	2019/5/31	2019/9/16	2019/10/17
学部系部局	906	610	866
その他部局	173	119	151
事務局	161	161	5

Shibboleth[10] による統合認証サービスを導入している．

表-4 に，統合認証サービスを経由する主な情報システムを示す．表中の○は利用が必須，△は一部もしくは要望に応じて利用可，×は利用不可を表している．また，表以外にも，他部局が管理する全学的，もしくは特定部局で利用される情報システムに対して，希望を募り認証源として提供している．このように，統合認証サービスは非常に用途が幅広い認証基盤であり，網羅的な情報取得の機会を与える．

そこでの認証ログから，対象となる OS と利用者 ID をひも付けたデータを作成し，個別の対応依頼を行った．その手順を，図-5 に示し，各手順の詳細について述べる．

(1) 専用ログファイル作成

統合認証サービスの認証ログから必要な情報のみを抽出した専用のログファイルを作成する．前述したとおり，統合認証サービスは Shibboleth を利用して構築されており，Shibboleth が出力する `idp-audit.log` を抽出元とした．デフォルトの設定では，`idp-audit.log` にはクライアントの IP アドレス，およびユーザエージェントは出力されない．そのため，これらを出力するための設定を追記した．また，抽出処理を容易に行えるよう，区切り文字，利用者 ID，IP アドレス，ユーザエージェントを `idp-audit.log` の末尾にまとめて出力した．

(2) ログメール送信

ログ管理ツールの機能により，ログ受信用メールアドレス宛に，専用ログファイルの内容が毎日送信される．本処理も定期実行される自動処理である．

(3) 集計用ワークシート編集

利用状況について統括的に管理するため，集計用ワークシートを利用する．この集計用ワークシートについて，図-6 に示す．ワークシートは，利用者 ID ごとに利用日時，OS が一覧化されている統括管理用シートと，認証ログが蓄積されている日次データ用シートで構成されている．ログ受信用メールアドレス宛に届いた専用ログファイルの内容を日次データ用シートに追記することにより，統括管理用シートが自動的に構成される．担当者は日次の業務として，毎朝日次データ用シートを更新する．その際の所要時間はおおよそ 5 分程度である．統括管理用シートは一覧性が高く，後述する個別対応などの取組みにおいて完全性の高い管理ができる．

(4) 個別対応依頼メール送信

作成された集計用ワークシートのデータを元に，個別の対応依頼メールを送信する．集計用ワークシートに実装されたスクリプト処理により，動的に抽出された対象者を宛先，規定の文章を本文としたメールを自動で新規作成する．メールソフトと連

表- 4: 主な統合認証利用サービス一覧

システム名称	利用対象	
	教職員	学生
VPN・無線 LAN 利用申請システム	△	△
マイページシステム	△	○
総合ポータルシステム	△	△
ソフトウエアダウンロードシステム	△	△
ファイル転送サービス	△	△
情報倫理学習システム	○	△
文書共有システム	△	×

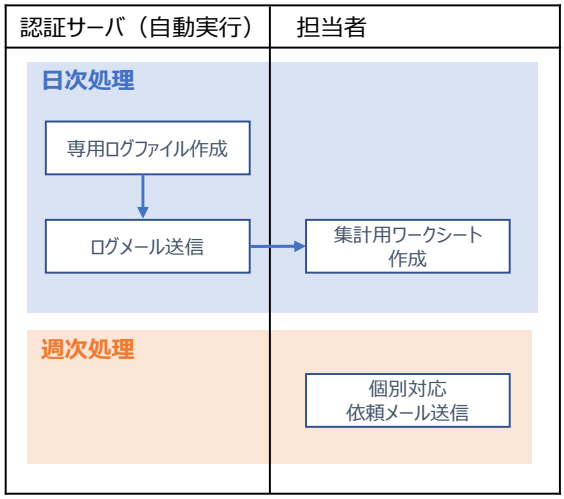

図- 5: 対応手順

図- 6: 集計用ワークシート

携することにより，そのまま自動送信することも可能だが，1 件ずつ確認し，内容を編集することもできる．担当者は，週次の業務として本処理を実施する．本作業の所与時間は，確認も含めて 20 分程度となる．

4.2.2 周知・対応依頼

本対応に関して，情報センターから各部局に対して，複数回の周知を行った．Windows 7 対応に関しては，2019 年 7 月に初回の周知を行った．目的は，各セキュリティ管理者を対象に，Windows 7 のサポート期限が 2020 年 1 月で終了することの初報と，今後の調査や各種対応への協力の依頼であった．2 回目は，2019 年 9 月に行った．これは各部局宛の利用状況調査の実施の案内と，協力の依頼が目的であった．調査の依頼を通し，セキュリティ管理者に部局内の状況を把握させつつ，システム管理者への周知と対応を促進した．3 回目の通知は後述する延長サポートの周知と，募集を目的とした．最後の通知はサポート期限が迫った 2019 年 12 月に実施した．ここでは，期日までの対応の再度の催促と，期日までに利用が確認できた Windows 7 の利用者 ID に対して，当該の OS の利用がある限り，個別メールによる注意喚起を行うことを予告した．

macOS に関する周知としては，2020 年 2 月 5 日に利用状況調査の実施案内を行った．また，2020 年 6 月 5 日には，利用制限措置の実施についての周知を行った．

4.2.3 個別の対応依頼

後述する利用制限措置を行う前の最終的な通告として，認証サーバのログから抽出したデータを元に，各利用者個人宛に対応依頼のメールを一斉送信した．Windows 7 については，サポート終了日のおよそ 1 か月前である 2019 年 12 月 20 日に，過去 1 か月半の認証サーバログから抽出された利用者へメールを送信した．また，サポート終了日の 1 週間前より，前日の利用者宛にメールを送信した．その際の送信件数を表-5 に示す．

表- 5: Windows 7 個別メール送信件数

送信日時	検出期間	送信数	
		教職員	学生
2019/12/20	2019/11/01～2019/12/15	149	155
2020/01/06	2019/12/16～2020/01/05	52	73
2020/01/07	2020/01/06	10	5
2020/01/08	2020/01/07	7	13
2020/01/09	2020/01/08	6	16
2020/01/10	2020/01/09	6	5
2020/01/13	2020/01/10～2020/1/12	12	14

対応スケジュールや業務日の関係から，1 回のメール送信にあたる対象の検出期間は一定ではないが，メールの送信件数は，検出期間の長さと正比例にはならなかった．これは，何らかの理由で OS の更新を行わず，検出され続けているユーザが一定数存在している可能性が高い．全体的な検出数には減少傾向が見られるが，個別メールが有効ではないユーザが一定数存在すると考えられる．

macOS については，認証ログを収集し始めた 2019 年 7 月より，macOS 10.9 以前の OS の利用者に対してメールを送信した．2020 年の 3 月からは，macOS 10.10，10.11 を対象に加えた．この際の送信件数を表-6 に示す．

表-6 からは，年度始の機器利用の増加とみられる一部の期間を除き，減少傾向が見られた．また，Windows 7 の場合と比較すると，学生の割合が低い．検出対象となる OS のバージョンうち，最新である macOS 10.11 のリリースが 2015 年であり，入学年度の関係から，それ以前に購入した macOS を利用し続けている学生が比較的少数であることが考えられる．

4.2.4 更新対応

本学における Windows の更新対応は，セキュリティポリシーによれば，原則としてクライアント機器の管理者である部局情報セキュリティ管理者の下，各システム管理者が行うこととなっている．技術的なサポートが必要な場合は，適時，情報センターのスタッフがフォローした．

表- 6: macOS 個別メール送信件数

送信日時	検出期間	送信数	
		教職員	学生
2020/03/05	2020/02/27～2020/03/04	84	27
2020/03/12	2020/03/05～2020/03/11	28	10
2020/03/19	2020/03/12～2020/03/18	12	4
2020/03/26	2020/03/19～2020/03/25	22	3
2020/04/09	2020/03/26～2020/04/08	39	4
2020/04/16	2020/04/09～2020/04/15	47	8
2020/04/23	2020/04/16～2020/04/22	44	8
2020/04/30	2020/04/23～2020/04/29	42	6
2020/05/07	2020/04/30～2020/05/06	48	9
2020/05/14	2020/05/07～2020/05/13	32	6
2020/05/21	2020/05/14～2020/05/20	32	5
2020/05/28	2020/05/21～2020/05/27	30	6
2020/06/04	2020/05/28～2020/06/03	24	4
2020/06/11	2020/06/04～2020/06/10	27	4
2020/06/18	2020/06/11～2020/06/17	23	2
2020/06/25	2020/06/18～2020/06/24	16	2

4.2.5 利用制限

Windows 7 に関する対応の最終段階として，サポート終了日である 2020 年 1 月 14 日より，統合認証サービスの利用制限措置を行った．利用制限措置として，認証画面の表示に際し，接続元クライアント機器のユーザエージェント情報を取得，Windows 7 をはじめとするサポートが終了した OS が発見された場合，エラー画面へと自動的に遷移することにより，認証を行わせない．その際のエラー画面を，図-7 に示す．なお，図-7 の画面への遷移に関しては，Web サーバソフトウエアのログにより，接続元の IP アドレスが自動的に記録されている．

利用制限措置により，統合認証を経由する各情報サービスがアクセス不可となることによる学内活動への支障が生じ得る．これら影響を極力低減するための方策として，教育用 PC を代替利用させつつ，その間に当該の機器の OS を更新することを促した．教育用 PC はキャンパスの各所に設置されており，原則，本学の全構成員が利用できる．そのため，統合認証を経由する各サービスの利用という点においては，一定のフォローが実現できた．

4.3 Windows 7 拡張セキュリティ更新プログラム

先に述べたとおり，Windows 7 のサポート期限は 2020 年 1 月 14 日とされていた．しかし，2019 年 10 月，Microsoft 社より，有償での 1 年間有効な拡張セキュリティ更新プログラム（ESU）が公表された．この ESU は，最長で 3 回受けられるため，3 年間は延長サポートを受けることができる．また，ESU の購入は組織単位の一括購入であり，必要数を決定した上で導入する必要があった．

本学の基本的な方針として Windows 7 の更新を促していたが，再調査の結果，どうしても必要という回答が少なからずあった．そのため，ESU を導入する必要があると判断した．改めて，導入のための申請を全学的に募った結果，6 部局から，合計 19 台の機器について申請があった．申請理由について，以下にまとめる．

- 導入ソフトウエアの更新不可

  機器に導入されているソフトウエアが，更新後の最新の OS に対応しておらず，利用できなくなるケースで，8 件確認できた．このパターンで申請された機器は全て，研究・実験用途で専門性が高いソフトウエアが利用されているものであった．

- 予算不足

  OS 更新のためには機器もしくはソフトウエアライセンスの購入を行う必要があり，その予算が確保できていなかったケースで，4 件の申請がこのケースであった．

- 期間限定の利用希望

  近い将来，Windows 7 で利用しているシステムに関する更新の予定があるが，サポート終了に間に合わないため，ESU を利用申請するケースがあった．全て同一の部局から合計 7 件の申請があった．

ESU は年度更新となっているため，今年度も継続の意見調査を行う予定である．また，ESU を導入した機器への利用制限措置について，ESU 導入機器の管理者に対して問い合わせを行い，統合認証の利用は必要ないことを確認している．そのため，利用制限措置については特別な対応を行っていない．

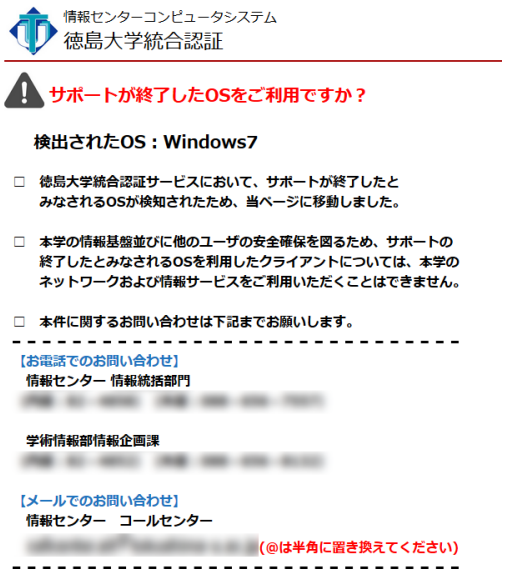

図- 7: 統合認証サービス エラー

5 検証

5.1 考察

本節では，認証サーバでの認証ユーザ数の推移を元に，取組みの効果と今後の課題について考察する．また，認証ログを用いた OS 更新の促進の取組みについての問題点について述べる．

5.1.1 Windows 7

図-8 に，日ごとの Windows 7 の認証ユーザ数の週当たりの合計数の推移を示す．図示した期間は，認証サーバのログの取得を開始してから，サポート期間の終了に伴う利用制限措置を行うまでである．

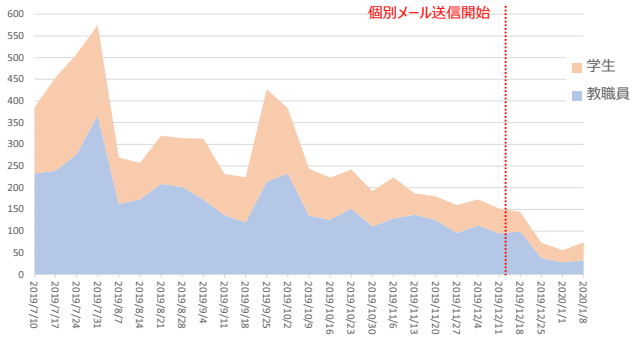

図- 8: Windows 7 認証ユーザ数推移

全体的な傾向としては，Windows 7 の認証ユーザ数は減少傾向にあり，本論文で述べた対応の成果が現れているといえる．しかし，増減率については，9 月下旬と 1 月初旬において，大きな増加率が検出されていた．これは，どちらも長期休暇が終了するタイミングであることから，直前週である長期休暇中の機器の利用数が減少していることと，大学の再開を翌週に控えた当該週の機器の利用数の増加によるものと推測される．また，長期休暇の終了直前に，帰省先などから普段利用しないクライアント機器からアクセスを行ったことなども考えられる．

全体的な増減率の推移に関しては，ある程度一定の割合で減少していることを期待したが，前週と比較した際に減少がみられた週は全体の 65.4%にとどまった．これは，取組みそのものに改善の余地があることを考慮しても，大学という組織において，利用されるクライアント機器に対し，網羅的な対応を行うことが容易ではないことを表している．今後の Windows OS のサポート終了の際にも，同様の事象が発生することが考えられるため，クライアント機器に対する統括的な管理策など，抜本的な観点からの対応を考慮していく必要がある．また，観測期間内で特に高い増加率が検出された長期休暇のタイミングに関しては，メール送信のスパンを短縮するなど，集中的な特別対応を行うことを検討したい．

また，図-8 における赤破線は，表-5 に記載した個別の対応依頼の開始を表している．個別の対応依頼の開始直後は，増減率が –49.3 %と，検出数が半減する結果となった．この数値は，2019 年 8 月初旬に –53.0 %に次いで，観測期間において 2 番目に高い減少率であり，その翌週に関しても，検出数は減少している．翌々週については，検出数が増加しているが，これは年始の大学の業務開始週だったことによる影響と考えられ，個別の対応依頼の開始時と比較すると，検出数は 10 %以下となっており，サポート期間終了の直前ということでのユーザの関心の高まりを考慮しても，個別の対応依頼が効果的であると言える．

図-8 で示した期間以降の Windows 7 の認証ユーザ数は，4.2.5 節で述べた対応により，0 件となっている．学内における Windows 7 の機器としては，4.3 節で述べた ESU を導入した機器が残っているが，事前の調査の結果，当該機器からの統合認証の利用は無いとの報告があったため，今後も Windows 7 での認証ユーザは検出されない見込みである．

5.1.2 macOS

図-9 に，macOS 10.9 以前，macOS 10.10，macOS 10.11 の認証ユーザ数の週当たりの合計数の推移を示す．図示した期間は，認証サーバのログの取得を開始してから，サポート期間の終了に伴う利用制限措置を行うまでである．まず，全体的な利用数としては，新しい OS ほど多い傾向にある．個別の対応依頼の開始後の検出数の動向に注目すると，macOS 10.9 については，減少傾向となり，対応依頼の効果が認められるといえる．macOS 10.10，macOS 10.11 について，個別の対応依頼の開始直後に大きな増加が見られる．これについては，直前の 2 月下旬から 3 月下旬にかけての減少傾向と同様に，大学の年間スケジュールにおける繁忙・閑散に同期しているものと推測される．その後の 4 月下旬から，利用制限措置が開始される 7 月初頭にかけて大きく減少していることから，個別の対応依頼は有効であるといえる．また，macOS のバージョンについて，バージョンごとに特定の傾向は見られなかった．

5.1.3 対応スケジュール

本対応については，利用状況の調査結果を元に，スケジュールを策定し，実対応を行っている．まず，Windows 7 については，おおよそサポート終了の 1ヶ月前から，個別の対応依頼を行った．これは，管理者の対応猶予や情報センターのリソース，年末年始の休業期間などを考慮し，集中的に対応を行うためには 1ヶ月程度必要と判断したためである．5.1.1 節でも述べたように，この

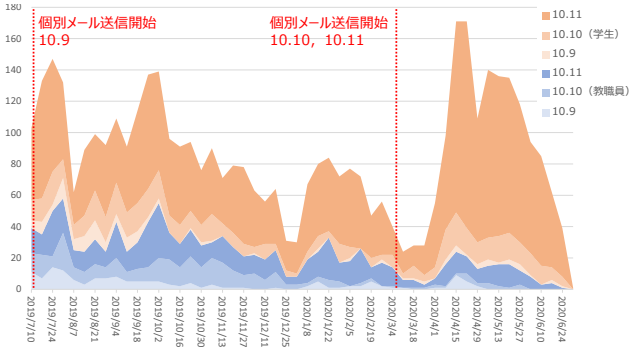

図- 9: macOS 10.9～10.11 認証ユーザ数推移

1ヶ月で 90%程度の削減が実現できたため，スケジュール設定としては有効であったといえる．

また，macOS については，個別の対応依頼を開始してからの検出数の減少を観察し，適当なタイミングで利用制限措置を実施している．macOS においては過去の慣例からも，毎年最新バージョンがリリースされることが予想されるので，サポート期間が終了したとみなされるバージョンの更新を促進するためには，今後は年間を通じた一貫した対応を行う事が必要と考える．

5.1.4 認証ログから抽出されたデータの信頼性

4.2.1 節で述べたとおり，本論文での各対応策においては，認証ログからのマイニングによりデータを抽出しており，その中でも，利用 OS の推定に使用しているユーザエージェントは，重要な情報といえる．しかし，これは，クライアント機器側で生成されるリクエストヘッダ内に存在する文字列をそのまま取得しており，サーバ側で処理され出力されている認証時刻や利用者 ID と比較すると，真正性は担保できていない．すなわち，悪意のあるユーザにとって，リクエストヘッダ内のユーザエージェントを詐称することは比較的容易であり，また，認証側でその改ざんを検出することは困難であることから，認証ログを利用した手段は完全とは言えない．しかし，大学という組織における構成員に対する啓発活動という点では，一定の効果があり，従来困難であった網羅的で一元的な対応が可能となったことには大きなメリットがあったと考えられる．

5.2 今後の課題

本論文で述べた各対応は，特定の OS を対象にしたものであるが，3 節で前述したとおり，本学において普遍的かつ恒久的に行われなければならない．そのために改善が求められるいくつかの課題について，以下に述べる．

(1) 個別メール送信の自動化

4.2.1 節において，認証サーバのログから OS とその利用者のデータを抽出し，管理用ファイルを作成する手順について述べた．これについては，日次の作業として情報センターのスタッフが対応しているため，作業コストが大きい．その後の個別メール送信処理も含めてこの処理を自動化することができれば，作業コストの大幅な削減が期待できる．例えば利用の頻度や，利用システム，大学を取り巻く状況などを考慮したうえで，総合的な判断でメールが自動送信されることが望ましい．処理のロジック策定は，慎重に検討される必要がある．

(2) クライアント機器の管理体制の強化

5.1 節で述べたとおり，利用者への個別メールによる対応の催促は，ある程度の効果が期待できるが，一定の期間を要する．より対策の即応性を高めるためには，全学的な部門である情報センターより，各部局が直接取り組める仕組みが構築されていることが望ましい．しかし，現状，セキュリティ管理者が参照できる共通のプラットフォームは未整備であるため，直接的に対応することは困難である．現実的な施策としては，例えば，認証ログによるクライアント機器の利用状況について，各部局のセキュリティ管理者が自部局の構成員に関して確認できる仕組みを構築することが考えられる．これら仕組みの導入により，より現場に近い立場からの注意喚起が迅速に行われることが期待できる．

(3) 統合認証を利用しない機器の検出

個別のメールの送信は認証サーバのログを基に行っているため，統合認証を利用しない機器とその利用者に関しては，学内ネットワークに接続されていたとしても検知することができない．検出の網羅性の向上のためには，別のアプローチが必要であり，一案として，認証プロキシの導入が考えられる．現状，本学ではプロキシサーバが導入済みであるが，認証は課しておらず，認証の導入のためには認証源となるデータの連携の設計が必要である．また，プロキシサーバの利用に関しては，セキュリティポリシー上でも規定されておらず，一部を除いて利用は義務化されていない．よって，認証プロキシの導入のためには，技術的な改修と，制度的な整備が必要であり，導入効果なども検証した上で，今後検討したい．

(4) Windows の Update バージョンへの対応

3.2 節で述べたように，Windows はサポート期間内のバージョンであっても，その Update バージョンについてはサポートが終了しているものが存在する．本論文にて延べたユーザエージェントから OS のバージョンを取得する方法では，Update バージョンを取得することはできないため，図-6 の集計用ワークシート上で識別することはできない．よって，別途資産管理システムの導入や，Update バージョン収集用バッチの配布など，クライアント側での対応を検討する必要がある．これらの対応は，クライアント機器 1 台ずつに行う必要があるため，導入コストが大きい事が予測される．リスクを受容する事も視野に入れた上で，実現の可能性を検討したい．

6 むすび

本論文では，学内で利用されるクライアント機器のOS についての方針を定め，それに則って行ったOS の更新対応とその結果について述べた．認証データを用いてクライアント機器の利用状況を取得することにより，全学に対してある程度網羅的な対応を行うことができた．また，それは既存のシステムのデータを流用したため，低い導入コストで実現できた．今後もクライアント機器のOS に関する対応は，運用面と，そこからもたらされる効果に関して，いくつかの課題がある．これらの課題に関して，情報センターからのみならず，全学的な観点から検討していきたい．

謝辞

本対応にあたり，徳島大学情報センターの元スタッフの森智彦氏には多大なご助言，ご助力を頂きました．深く感謝申し上げます．

参考文献

[1] 森 祥寛, 佐藤 正英, 大野 浩之, 笠原 禎也, 井町 智彦, 高田 良宏, 東 昭孝, 二木 恵, Nakasan Chawanat, “金沢大学における携帯型パソコン必携化に関する 12 年間の取組,” 学術情報処理研究, No. 23, pp.29–42, 2019.

[2] 東北大学，東北大学オンライン事務化宣言—New Normal 時代でのワークスタイルの変革， 2020, https://www.tohoku.ac.jp/japanese/2020/05/press20200528-01-online.html（最終閲覧日：2020 年 8 月 3 日）

[3] 情報処理推進機構， 情報セキュリティ10 大脅威， https://www.ipa.go.jp/security/vuln/10threats2020.html（最終閲覧日：2020 年 8 月 3 日）

[4] 石坂 徹, 石田 純一, 高木 稔, 若杉 清仁, 松前 薫, “PC のセキュリティ状況からみた学内LAN 運用に関する考察,” 情報処理学会 全国大会講演論文集, pp.577–579, 2012.

[5] 沖野 浩二, 金森 浩治, 山下 和也, “脆弱性調査によるセキュリティコントロール,” 学術情報処理研究, No. 23, pp.76–84, 2019.

[6] 田島 浩一, 岸場 清悟, 近堂 徹, 渡邉 英伸, 岩田 則和, 西村 浩二, 相原 玲二, “脆弱性診断で収集されるサーバ情報のセキュリティ対策への応用,” 学術情報処理研究, No. 23, pp.122–127, 2019.

[7] 今井 美香, 伊藤 稔, 中村 文, 不破 泰, “大学におけるソフトウェア資産管理システムの構築と運用,” 第 18 回学術情報処理研究集会 発表論文集, pp.27–31, 2014.

[8] 森田 拓哉, アサノ デービッド, 鈴木 彦文, 岡崎 裕之, “認証ログをライフログとして用いた安否確認システムの開発,” 電子情報通信学会 技術研究報告 No. 119（70）, ICSS2019-6, pp.27–30, 2019.

[9] 国立情報学研究所, 学術情報ネットワークとは, https://www.sinet.ad.jp/aboutsinet（最終閲覧日：2020 年 8 月 3 日）

[10] Shibboleth, https://www.shibboleth.net/（最終閲覧日：2020 年 8 月 3 日）