Microsoft Defender for Endpoint を用いた OS 更新状況可視化システムの構築

掛井 将平 [1)]，守屋 賢知 [2)]，齋藤 彰一 [1)]，松尾 啓志 [2)]

1) 名古屋工業大学 サイバーセキュリティセンター
2) 名古屋工業大学 情報基盤センター

kakei.shohei@nitech.ac.jp

Constructing an OS Update Status Visualisation System using Microsoft Defender for Endpoint

Shohei Kakei[1)], Masanori Moriya[2)], Shoichi Saito[1)], Hiroshi Matsuo[2)]

1) Cybersecurity Center, Nagoya Institute of Technology
2) Information Technology Center, Nagoya Institute of Technology

概要

名古屋工業大学サイバーセキュリティセンターでは，センターの実務者が学内計算機の OS 更新状況を確認する手段と，計算機の利用者・管理者が OS 更新の要否を確認する手段を提供するために OS 更新状況可視化システムを構築した．構築したシステムを利用して OS 更新状況の傾向を分析したところ，新しいバージョンのリリースにあわせて比較的速やかに OS が更新されている様子が確認できた．一方で，本学の OS 更新の目安である二か月よりも古いバージョンの OS を利用している計算機が 140 台前後を推移している様子も確認できた．

1 はじめに

Windows や macOS，Linux などの基本ソフトウェア（Operating Systems, OS）はハードウェアの抽象化やハードウェア資源のアクセス制御などの計算機の基本的な機能を担っている．計算機上で実行されるアプリケーションは OS を介してハードウェアの資源を利用しており，マルウェアや不正アクセスから計算機を保護するには OS のセキュリティ対策が重要である．例えば，2022 年 3 月ごろに観測された学術機関を標的とした攻撃の事例では，Windows のリモートコード実行可能な脆弱性である MS13-098/CVE-2013-3900 の利用が観測されている[*1]．

IPA が公開する「情報セキュリティ 10 大脅威 2023」の組織向け脅威の 8 位に「脆弱性対策情報の公開に伴う悪用増加」が挙げられている．いわゆる，N デイ脆弱性と呼ばれる脆弱性を悪用した攻撃であり，セキュリティパッチ（修正プログラム）や回避策が公開されてから利用者が対策を講じるまでの期間（N 日）に実施される攻撃である．セキュリティパッチの公開により，脆弱性の存在を利用者に知らせることでソフトウェアの更新を促すことができるが，同時に攻撃者にも脆弱性の存在が知られることとなる．Windows では，Windows Update を通してセキュリティパッチが提供されており，2023 年上半期には 600 件以上の脆弱性が修正[*2]されている．これら全ての脆弱性が必ずしもすぐに悪用されるわけではないが，脆弱性が公開されている状況を鑑みると可能な限り迅速にセキュリティパッチを適用することが望ましい．しかしながら，河田らによる企業・団体勤めの Windows 利用者を対象としたアンケート調査 [1] によると，約 41% の利用者が Windows Update の適用を後回しにしており，その主な理由は「業務が忙しい」であった．

名古屋工業大学サイバーセキュリティセンターでは，計算機のセキュリティのチェックに Microsoft Defender for Endpoint（MDE）を利用しており，日々の CSIRT 活動に活用している．MDE はマルウェアなどによる脅威の検出や調査を支援するシステムであり，MDE がインストールされた計算機の情報を収集することもできる．サイバーセキュリティセンターで

[*1] https://www.trendmicro.com/ja_jp/research/23/a/targeted-attack-campaign-earth-yako.html

[*2] https://msrc.microsoft.com/update-guide/vulnerability

はこれまで，MDE がインストールされた計算機の OS の更新状況を実務者が確認し，更新が必要な計算機の管理者にメールで連絡を行っていた．しかし，OS 更新状況の集計は手作業であったため月に一回の頻度でしか作業できず，更新が必要な計算機の存在を迅速に知らせることができなかった．また，日ごとの更新状況を記録できず，OS の更新を依頼後に状況が改善していることを確認できなかった．そこで本稿では，一連の作業を自動化することを目的に開発した OS 更新状況可視化システムを説明し，本システムを用いて調査した OS 更新状況の結果について報告する．OS 更新状況可視化システムにより，計算機の管理者は自身が管理している計算機の OS の更新の要否を，実務者は全体の OS 更新状況を確認することができる．

2 関連システム

本章では，構築した OS 更新状況可視化システムに関係する三つのシステムについて説明する．これら三つのシステムが持つ情報を連携することで，どの計算機が，どのバージョンの OS を利用し，誰が管理しているかが分かる．

2.1 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint（MDE）は，エンドポイントで動作するセンサを用いて，リスクベースの脆弱性検出や修復機能などを提供するセキュリティソリューションである．エンドポイントにインストールされたセンサが侵害の検出，イベントの調査，セキュリティ分析のための情報などのセキュリティ関連情報を収集し，その情報を組織のテナントに送信する．テナントへのアクセスは Microsoft 365 Defender（M365 Defender）ポータルを使用し，ここからエンドポイントのセキュリティを管理できる．例えば，検知された侵害の一覧やエンドポイントで発生したイベントのタイムラインを確認できる．

MDE の特筆すべき機能の一つとして，Advanced Hunting が挙げられる．Advanced Hunting を利用することで，定期的に収集されているエンドポイントの各種情報（OS や OS バージョン，IP アドレス，MAC アドレス，セキュリティアラートなど）を過去 30 日に遡って検索できる．これらの情報はいくつかのテーブルで管理されており，Kusto Query Language（KQL）を用いて検索できる．今回構築したシステムでは，Advanced Hunting を用いて学内の計算機の各種情報（MAC アドレス，IP アドレス，OS，OS バージョン）を収集している．

2.2 MAINS データベース

名古屋工業大学情報基盤センターでは，学内ネットワーク（LAN）としてキャンパス情報ネットワーク（MAINS）を構築し，その運用，保守を行っている．MAINS には研究室や個人の PC，スマートフォンなどが接続され，教育や研究，事務などに活用されている．MAINS に接続して，MAINS 内のリソースやインターネットを利用するには計算機の認証が必要であり，有線接続の場合は MAC アドレス認証，無線接続の場合は IEEE 802.1X 認証が適用される．MAINS データベースは MAC アドレス認証で MAINS に接続する計算機を管理するデータベースであり，MAC アドレスを MAINS データベースに登録することで，明示的な認証なしに MAINS に接続できる．学内に常設される計算機や毎日持参する計算機など，日々の活動で利用される計算機が登録されている．

MAINS データベースに MAC アドレスを登録する際に，当該計算機の利用者情報を登録する必要がある．計算機が登録されると，固定 IP アドレスが割り当てられ，MAINS データベース上で MAC アドレス，IP アドレス，利用者情報を確認できるようになる．今回構築したシステムでは，MDE から取得した OS の情報と利用者情報を MAC アドレスと IP アドレスで対応付けている．

2.3 統一データベース

MAINS データベースと同様に，本学情報基盤センターでは，教職員と学生の氏名や ID，メールアドレス，所属，指導教員などの情報を管理する統一データベースを構築し，その運用，保守を行っている．統一データベースは，本学構成員に関する情報を統一的に管理する基盤であり，その情報は学内システムへのシングルサインオンにも利用されている．今回構築したシステムでは，計算機の利用者への連絡のためのメールアドレスの取得や，利用者が学生の場合にその指導教員を検索するために利用している．

3 OS 更新状況可視化システムの構築

3.1 設計方針

N デイ脆弱性の脅威を踏まえると，可能な限り最新のバージョンの OS を利用することが望ましい．しかし，個々の計算機の管理者に OS の更新を逐一依頼することは作業コストの観点から現実的でなく，管理者が主体的に OS 更新の要否を確認できる環境を用意することが望ましい．その上で，一定期間対応されていない計算機について，その管理者にサイバーセキュ

リティセンターから連絡することで，管理者と協働で計算機のセキュリティを確保できる体制の整備を目指す．以上を踏まえて，以下の二つの方針をたてる．

- 方針 1：計算機の管理者が OS の更新の要否を確認できること
- 方針 2：一定期間更新されていない計算機の管理者に OS の更新を依頼できること

方針 1 について，学内の計算機の情報が登録されている MAINS データベースに OS の更新の要否を載せることで，管理者による確認ができる．方針 2 について，OS のバージョンのリリース日と更新状況のチェック日の差から，一定期間以上の古いバージョンの計算機をリストアップし，その管理者に連絡を行う．計算機の利用者が教職員の場合は，その教職員を管理者とし，計算機の利用者が学生の場合は，その学生を監督する立場のある主指導教員と副指導教員を管理者として連絡する．連絡先は，統一データベースの情報を参照することで取得できる．

また，実際に OS が更新されたかどうかを把握するには，連絡後に実務者が継続的に OS の更新状況を確認する必要がある．そこで，以下の方針を追加する．

- 方針 3：日ごとの OS の更新状況を時系列で確認できること

方針 3 について，方針 1 で MAINS データベースに掲載した情報を日ごとのバックアップを記録しておくことで，OS の更新状況を時系列で確認できる．以上，三つの方針に従って OS 更新状況可視化システムを構築する．

3.2 構築したシステムの構成

構築したシステムの構成を図 1 に示す．本システムは三つのモジュールから構成される．

セキュリティ情報作成モジュール 本モジュールは，MDE のインストール状況と OS の更新状況を表す情報（セキュリティ情報）を作成する．M365 Defender の Advanced Hunting を利用して，計算機ごとにその計算機の「MDE のインストールの有無」，「OS のバージョン情報」を取得する．取得した情報は，当該バージョンのリリース日から判定された OS 更新の要否と合わせて MAINS データベースに記録される．セキュリティ情報の作成は一日一回行われ，その作成日と当該バージョンのリリース日の差が二か月以内であれば OS 更新状況を Pass（更新不要）と判定し，そうでなければ Error（要更新）と判定する．また，作成されたセキュリティ情報は後述する OS 更新状況可視化モジュールで利用するために，セキュリティ情報履歴データベースに日ごとに記録される．計算機の管理者と利用者は自身の計算機のセキュリティ情報を MAINS データベースから確認できる（図 2）．

OS 更新通知モジュール 本モジュールは，MAIS データベースに記録されているセキュリティ情報を用いて，MDE がインストール済みかつ OS の更新が必要な計算機の管理者に OS 更新通知をメールで送信する．MAINS データベースには，計算機の情報とその利用者の情報が格納されているが，利用者が学生の場合もある．そのときは，統一データベースから主指導教員と副指導教員の情報を取得し，これらを管理者とする．なお，利用者が教職員の場合は，その者を管理者とする．管理者と通知対象の計算機の関連付けができたら，統一データベースから取得した管理者の連絡先に OS 更新通知メールを送信する．

OS 更新状況可視化モジュール 本モジュールは，セキュリティ情報を日ごとに集計し，各種集計値の推移や割合をグラフで可視化する．例として，「OS のバージョンごとの計算機の台数の推移」や「OS 更新状況が Error となっている計算機の台数の推移」，「OS 更新状況が Error となっている計算機のバージョンの内訳」などを集計している．

3.3 構築したシステムの実装と処理の流れ

Ubuntu 22.04 の計算機上に，OS 更新状況可視化システムを構築した．各モジュールを Ruby 3.2.2 で実装し，OS 更新状況可視化モジュールの OS 更新状況の可視化部分を Ruby on Rails 7.0.8 による Web アプリケーションとして実装した．セキュリティ情報履歴データベースには Postgresql 15.3 を使っている．

3.3.1 セキュリティ情報の作成

本処理では，M365 Defender から各計算機の OS のバージョンを取得し，OS 更新の要否を判定し，その結果をセキュリティ情報として MAINS データベースに記録する．まず初めに，セキュリティ情報作成モジュールが Advanced Hunting により M365 Defender の DeviceInfo テーブルと DeviceNetworkInfo テーブルから必要な情報を取得する（Phase A-1）．DeviceInfo テーブルからは，OS やそのバージョン情

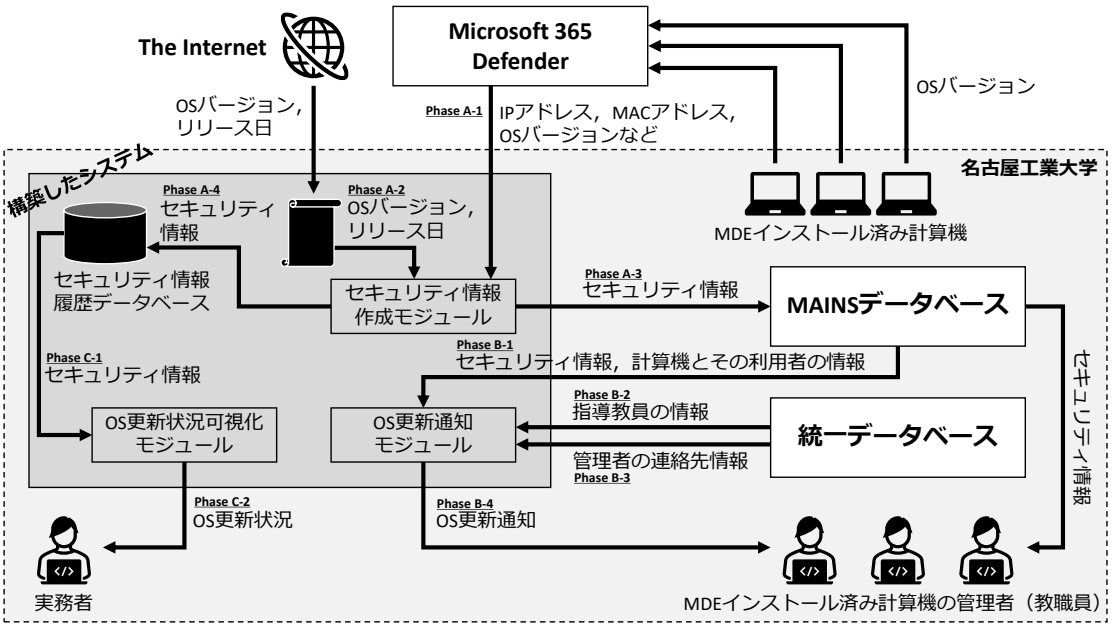

図 1　構築した OS 更新状況可視化システムの全体像

図 2　MAINS データベースの画面（OS が要更新の例）

報，MDE のインストール状態などを取得する．図 3 に，DeviceInfo テーブルから必要な情報を取得する KQL を示す．DeviceInfo テーブルには，DeviceId ごとの最新の情報が記録されているわけではなく，各計算機から収集された情報が履歴データとして記録されている．そこで，DeviceId ごとに最新の行のみを抽出するようにしている．次に，DeviceNetworkInfo テーブルからは，MAC アドレスと IP アドレスの情報を取得する．図 4 に，DeviceNetworkInfo テーブルから必要な情報を取得する KQL を示す．DeviceNetworkInfo テーブルも DeviceInfo テーブルと同様に，最新の情報だけが記録されているわけではない．そのため，DeviceId ごとに最新の行のみを抽出するようにしている．また，異なる DeviceId に同じ IP アドレスが紐づいている場合があるため，IP アドレスごとに最新の行のみを抽出するようにしている．以上の操作により取得した両テーブルを DeviceId をキーに結合することで，どの計算機がどのバージョンの OS を利用しているかが分かる．

次に，OS バージョンファイルを用いて，Phase A-1 で取得した各計算機の OS のバージョンのリリース日を調べる（Phase A-2）．セキュリティ情報作成モジュールの実行日とリリース日の差が二か月以内であれば OS 更新状況を Pass と判定し，そうでなければ Error と判定する．

次に，MAC アドレス，IP アドレス，OS，OS バージョン，OS 更新状況を MAINS データベースに保存する（Phase A-3）．

最後に，セキュリティ情報作成モジュールの実行日を名前としてセキュリティ情報履歴データベースにテーブルを作成し，Phase A-3 で記録したデータと同じデータを本テーブルに記録する（Phase A-4）．

```
DeviceInfo | where isnotempty(OSPlatform) | where isempty(MergedToDeviceId)
    | summarize arg_max(Timestamp, *) by DeviceId // Select latest rows per DeviceId
    | project DeviceId, DeviceName, OSPlatform, OSDistribution,
      OSVersion, OSVersionInfo, OnboardingStatus
```

図 3　DeviceInfo から OS やそのバージョンの情報，MDE のインストール状態などを取得する KQL

```
DeviceNetworkInfo | where isnotempty(IPAddresses) and isnotempty(MacAddress)
    | mv-expand parse_json(IPAddresses)
    | extend IPAddress = tostring(IPAddresses.IPAddress)
    | where has_any_ipv4_prefix(IPAddress, '133.68.', '10.')
    | distinct Timestamp, DeviceId, DeviceName, IPAddress, MacAddress
    | summarize arg_max(Timestamp, *) by DeviceId  // Select latest rows per DeviceId
    | summarize arg_max(Timestamp, *) by IPAddress // Select latest rows per IPAddress
    | join (DeviceInfo | summarize arg_max(Timestamp, *) by DeviceId
      | project DeviceId, MergedToDeviceId) on DeviceId
    | where isempty(MergedToDeviceId)
    | project DeviceId, DeviceName, IPAddress, MacAddress
```

図 4　DeviceNetworkInfo から MAC アドレスと IP アドレスを取得する KQL

表 1　調査における基礎情報

項目	数値
MDE インストール済み計算機の台数	1,970
Windows11	924
Windows10	958
macOS	88
教職員の人数	1,130
研究室配属済み学生の人数	2,631

3.3.2　OS 更新通知の送信

本処理では，OS 更新通知モジュールが OS の更新が必要な計算機の管理者に OS の更新を依頼するメールを送信する．まず初めに，MAINS データベースに記録されている計算機のうち，OS 更新状況が Error の計算機とその利用者の情報を抽出する（Phase B-1）．利用者が学生の場合は，その主指導教員と副指導教員を統一データベースから検索する（Phase B-2）．最後に，管理者のメールアドレスを統一データベースから取得し（Phase B-3），管理者に OS 更新通知を送信する（Phase B-4）．

3.3.3　OS 更新状況の表示

本処理では，OS 更新状況可視化モジュールがセキュリティ情報履歴データベースに記録された日ごとのセキュリティ情報を取り出し（Phase C-1），日ごとに集計した結果を実務者に提示する（Phase C-2）．集計結果は，後述する 4 章の図 5 や図 8 などのグラフの形式で提示される．

4　OS 更新状況の調査

4.1　概要

3 章で説明したシステムを導入し，MDE インストール済み計算機を対象に OS の更新状況の調査を行った．なお，MDE インストール済み計算機の台数（教育用 PC や事務用シンクラ等の情報基盤センター管理端末を除く），教職員の人数と学生（研究室配属済み）の人数は表 1 の通りである．

OS 更新状況可視化システムのリリース後のタイムラインを表 2 に示す．6/2 に本システムをリリースし，セキュリティ情報が MAINS データベースに追加されたことを業務掲示板に掲示した．その後，更新状況の調査用の機能の実装を進めて，8/18 から日ごとの OS 更新状況の記録を開始した．9/11 には，OS の更新を促すために，セキュリティ情報を確認することと更新依頼メールを受信した際には OS の更新を行うことを業務掲示板にてアナウンスした．そして，9/19 にその時点で OS が二か月以内に更新されていない計算機の管理者宛てにメールによる更新の依頼を行った．このとき，対象となった計算機の台数は 172 台で，管理者の人数は 88 人であった．

4.2　調査結果

本節では，OS 更新状況可視化システムで得られた日ごとのセキュリティ情報を用いて，8/18 以降の OS 更新状況の調査結果を説明する．

まず，OS のバージョンごとの利用台数の推移を示す．本学で利用されている様々な計算機のうち，比較的利用台数が多い Windows11 22H2（OS build 22621），Windows10 22H2（OS build 19045），macOS 13 Ventura の結果について，それぞれ図 5，図 6，図 7 に示す．なお，実線は執筆時点でリリースから二か月以内のバージョンを，破線は執筆時点でリリースから二か月以上経過しているバージョンをそれぞれ表し，凡例のカッコ内の数字は当該バージョンのリリース日を表している．また，観測されたバージョンのうち，直近にリリースされた八つのバージョンのみを示している．全体的な傾向として，いずれも特定のタイミ

表 2　OS 更新状況可視化システムのリリース後のタイムライン

日付	内容
2023-06-02	MAINS データベースにセキュリティ情報の掲載を開始を業務掲示板にてアナウンス
2023-08-18	OS 更新状況の記録を開始
2023-09-11	セキュリティ情報の定期的な確認と OS 更新依頼メールを受信した際の OS の更新を業務掲示板にて依頼
2023-09-19	OS が二か月以内に更新されていない計算機（172 台）の管理者（88 人）にメールで OS の更新を依頼

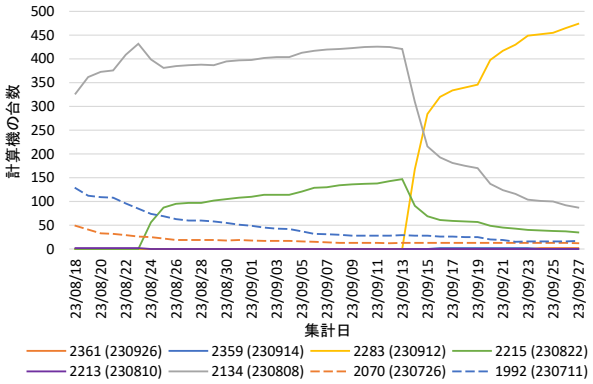

図 5　Windows11 22H2（OS build 22621）のバージョンごとの推移

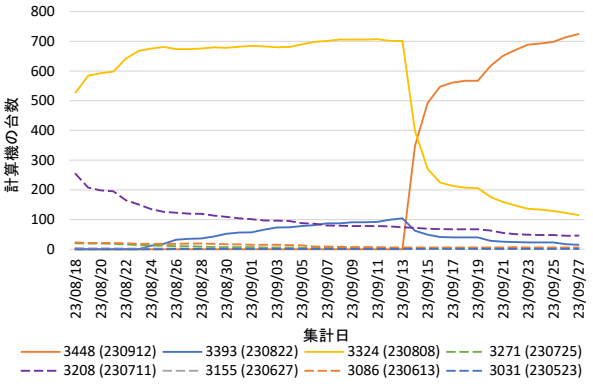

図 6　Windows10 22H2（OS build 19045）のバージョンごとの推移

ングを境に比較的速やかにより新しいバージョンへの入れ替わりが発生している様子を確認できた．また，Windows に関しては，入れ替わり発生後，一度そのスピードが鈍化した後に，再度入れ替わりが進んでいる様子を確認できた．

Windows11 に関して，9/13 にバージョンの入れ替わりが開始した．22621.2283 が増加した一方で，22621.2215 と 22621.2134 が減少した様子が図 5 から確認できる．2283 は 9/12 にリリースされたバージョンであり，リリースと同時に 2215 と 2134 から同バージョンへの入れ替わりが始まったと思われる．9/16 ごろに入れ替わりの速度が鈍化した後，9/19 に 2134 からの入れ替わりが再度進んだ様子が確認できる．表

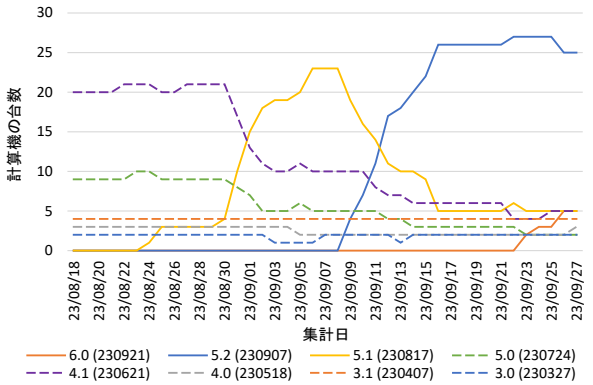

図 7　macOS 13 Ventura のバージョンごとの推移

2 に示したように，9/19 は OS の更新を依頼したタイミングであったが，2134 は 9/19 の時点でリリースから二か月以内のバージョンであったため，連絡の対象に含まれていなかった．その他の要因として，9/19 は週明けのタイミングであり，計算機の再起動により OS の更新が進んだと考えられる．

Windows10 に関して，Windows11 と同様に 9/13 にバージョンの入れ替わりが開始した．19045.3448 が増加した一方で，19045.3393 と 19045.3324 が減少した様子が図 6 から確認できる．3448 は 9/12 にリリースされたバージョンであり，リリースと同時に 3393 と 3324 から同バージョンへの入れ替わりが始まったと思われる．入れ替わりの速度の鈍化も Windows11 と同様に 9/16 から確認でき，その後，9/19 に 3324 からの入れ替わりが進んだ様子が確認できる．3324 は 9/19 の時点でリリースから二か月以内のバージョンであり，連絡の対象に含まれていなかったため，週明けのタイミングによる計算機の再起動により OS の更新が進んだと考えられる．

macOS に関して，9/8 にバージョンの入れ替わりが開始した．13.5.2 が増加した一方で，13.5.1 が減少した様子が図 7 から確認できる．13.5.2 は 9/7 にリリースされたバージョンであり，リリースと同時に同バージョンへの入れ替わりが始まったと考えられる．

次に，OS の更新状況が Error の計算機の台数の推移を図 8 に示す．これは，最低でも二か月の間 OS が

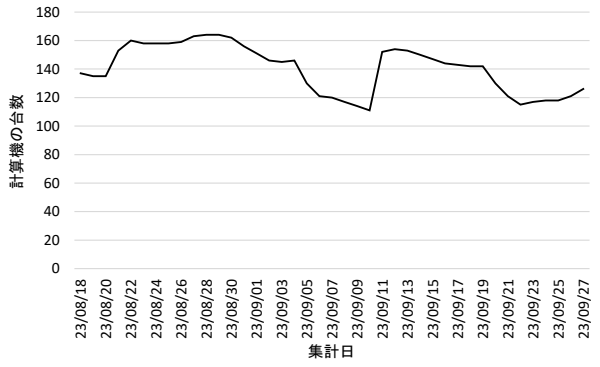

図 8　OS の更新状況が Error の計算機の台数の推移

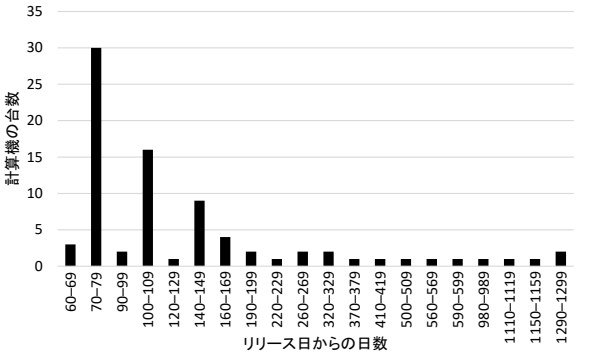

図 9　OS 更新状況が Error の計算機の OS のリリース日からの経過日数の内訳

更新されていない計算機の台数の推移を表す．全体的に緩やかに減少しつつも特定のタイミングでの急増減が見られる．調査期間内おける急増は 8/21 と 9/11 の二回，急減は 9/4 直後と 9/19 直後の二回であった．急増の二回はどちらも特定の OS のバージョンがリリースから二か月経過したタイミング[*3]であり，日常的に OS が更新されていなかった計算機の存在が原因であったと考えられる．急減の二回について，後者はメールによる OS の更新を依頼したタイミングであり，その効果によるものと思われる．一方，前者について，直接的な要因は分からないが，9/2 と 9/3 に一部の棟で計画停電があったため，それによる計算機の再起動が理由の一つとして考えられる．

最後に，OS の更新状況が Error の計算機がどの程度古いバージョンを利用しているかをリリース日からの経過日数ごとに集計した結果を図 9 に示す．最も割合が多かった日数が「70–79 日間」で，次いで「100–109 日間」，「140–149 日間」であった．この結果から，OS の更新を忘れて Error と判定されたが，その後 OS の更新が実施されて，Error が解消されている様子が確認できる．一方で，1 年以上前にリリースされたバージョンを利用している計算機が 10 台見つかった．このような長期間 OS が更新されていない計算機に関しては，利用しているソフトウェアの関係で更新ができていない可能性が考えられる．

5　今後の課題

4.2 節で示したように，OS の更新状況が Error の計算機の台数が 140 台（MDE インストール済み計算機の約 7%）前後を推移していることが本調査で分かった．なんらかの理由で，OS が更新されていない計算機が一定数存在しているものと思われる．今回の調査では計算機に注目して分析を行ったが，各計算機の OS の更新は管理者の責任のもとで行われることを考慮すると，管理者ごとに OS 更新状況の傾向を分析することが望ましい．その際，情報セキュリティの問題は人の心理が大きく関与することから，管理者の属性や性格などの要因によって更新状況の傾向に違いが表れることに注意が必要である．

情報セキュリティ対策において，計算機の利用者の心理的な側面に焦点をあてた研究が行われている．諏訪ら [2] は，利用者のセキュリティ行動に影響を与える要因を知識，態度，行動を三つのグループに分類し，それら要因から構成される情報セキュリティ行動モデルを構築している．20 代から 50 代までの 400 人を対象とした質問紙調査によりモデルを分析した結果，貢献感と無効感による情報セキュリティ対策における社会的ジレンマの存在を指摘している．社会的ジレンマを抱える利用者は，情報セキュリティ対策に対する重要性を認識しているものの，自分一人だけが対策を実施してもセキュリティ事故の防止や緩和に繋がるわけではないと考える傾向がある．また，セキュリティ行動の阻害要因とコスト感の影響の分析において，セキュリティ知識が高まるほどセキュリティ対策として実施しなければならないことが増えて，コスト感が上昇することも指摘している．そのため，セキュリティ知識を高めるだけでなく，具体的な対策手順や実施方法も併せて伝えることが重要と結論付けている．

佐野ら [3] は，行動経済学で用いられている行動変容ステージモデルを参考に，利用者のセキュリティ対策への意識や実施状況に基づき，利用者を「無関心期」，「関心期」，「準備期」，「実行期」，「維持期」の五つのステージに分類するセキュリティ行動変容ステージモデルを提案している．15 歳から 69 歳までのパソコン利用者 1,748 人を対象とした質問紙調査によるモデ

[*3] 8/21 は macOS の 13.4.1.0 が 16 台，12.6.7.0 と 11.7.8.0 が 1 台ずつあり，9/11 は Windows10 の 19045.3208 が 30 台，Windows11 の 22621.1992 が 14 台，22000.2176 が 2 台あった．

ルの検証を行い，パソコン利用者は無効感の一因子に負の相関があり，貢献感とセキュリティ対策に対する関心の二因子がステージに正の相関があると分析している．特に，関心とステージ間に強い相関があることを指摘しており，セキュリティ対策への関心を高めるようなアプローチがステージの向上に効果的であると結論付けている．また，文献 [4] において，Windows Update の実施を促すメッセージの文面やユーザインタフェース（UI），配信タイミングが利用者の実際の行動を後押しするかどうかをセキュリティ行動変容ステージごとに調査している．その結果，ステージの向上には UI デザインの工夫が，ステージの維持には文面の工夫が必要であることを指摘している．

セキュリティ対策ソリューションの適切な利用や安全なパスワードの運用をはじめとした規約の遵守など，複雑化するセキュリティ対策に情報システム利用者が疲弊してしまう状態を「情報セキュリティ疲れ」と呼ぶ．さらにこれが悪化することで，情報セキュリティ対策を実施しなくなる「情報セキュリティバーンアウト」状態に陥ることが知られている．その場合, 情報セキュリティ対策の施策に対する効果が得られなくなるため，情報セキュリティ疲れ状態の把握が重要であると指摘されている [5]．畑島ら [6] は，情報セキュリティ疲れの度合いを測定する「情報セキュリティ疲労度測定尺度」を開発し，本尺度を用いて情報セキュリティ対策を実施することによる疲弊の測定が可能であることを示している．

上記既存研究より，利用者の特性によって効果的な情報セキュリティ対策の傾向は異なり，それぞれに適したアプローチをとることが望ましい．このとき，単に情報セキュリティ対策を指示するだけでなく，情報セキュリティ疲れの悪化に注意して，具体的かつ簡単に実行可能な手順を提示することが望ましい．上記で挙げた既存研究の知見などを参考に，本学構成員の特性の把握やその特性に応じた OS 更新状況の提示や更新依頼の方法の検討が今後の課題の一つである．

OS 更新の実効性を高める方法を検討する一方で，OS 更新状況データの活用も課題である．例えば，4.2 節で述べたように，計算機の OS 更新状況の変化が配置場所に起因する可能性がある．そのため，計算機の配置場所と OS 更新状況データを組み合わせた分析ができることが望ましい．また，今回構築したシステムは可視化の機能に限定して独自の Web アプリケーションとして実装したため，BI ツールなどを活用した可視化データの解析が今後の課題である．

6 おわりに

本稿では，MDE と MAINS データベースと統一データベースを組み合わせて構築した OS 更新状況可視化システムの説明と，本システムを使った OS 更新状況の調査について報告した．本システムの導入により，OS の更新が必要な計算機の管理者のみに一か月に一回の頻度で提供していた OS 更新状況を，全ての利用者と管理者が任意のタイミングで確認できるようになった．

構築したシステムを利用して OS 更新状況の傾向を分析したところ，新しいバージョンの OS に比較的速やかに移行している様子が確認できた．一方で，調査できた計算機のうち，二か月以内に OS が更新されていない計算機が約 7% 存在していることが確認できた．今後は，OS 更新の実効性を高める方法の検討と可視化データのさらなる分析を進めて，OS が未更新の計算機の台数をより低い水準に抑える．

参考文献

[1] 河田 真由子，古川 和快，角尾 幸保，“Windows Update に関するユーザの行動傾向と環境・心理学的要因の関係の調査”，研究報告セキュリティ心理学とトラスト（SPT），vol. 2021-SPT-43，no. 23，pp. 1–8.

[2] 諏訪 博彦，原 賢，関 良明，“情報セキュリティ行動モデルの構築―人はなぜセキュリティ行動をしないのか”，情報処理学会論文誌，vol. 53，no. 9，pp. 2204–2212，Sep. 2012.

[3] 佐野 絢音，澤谷 雪子，山田 明，窪田 歩，“セキュリティ行動変容ステージモデルの提案とユーザ要因の関係性の分析”，情報処理学会論文誌，vol. 63，no. 9，pp. 1458–1472，Sep. 2022.

[4] 佐野 絢音，澤谷 雪子，山田 明，窪田 歩，磯原 隆将，西垣 正勝，“OS 更新の促進手法に関する実証実験評価”，情報処理学会論文誌，vol. 64，no. 9，pp. 1330–1348，Sep. 2023.

[5] 畑島 隆，永井 啓太，谷本茂明，金井敦，“大学生の情報セキュリティ疲れの可視化に関する一考察”，コンピュータセキュリティシンポジウム 2017 論文集，vol. 2017，no. 2，Oct. 2017.

[6] 畑島 隆，谷本 茂明，金井 敦，“情報セキュリティ疲労度測定尺度 SFS-9 の開発と信頼性・妥当性の検討”，情報処理学会論文誌，vol. 61，no. 9，pp. 1472–1485，Sep. 2020.