第三者調査委員会報告書

令和４年７月 11 日

市橋克哉、中村素典、井戸清隆

目次

1. 事案の経緯（事実）

1-1. 事案の発生

花園大学拈花館（ねんげかん）講師控室に、社会福祉学部児童福祉学科Ｘ准教授の送受信メールの一覧表と推測される印刷物（別添資料１、以下「一覧表」という。）が放置されていた。

① 発見日：2021 年 11 月 15 日（月）8 時頃

② 発見者：児童福祉学科Ｙ教授

③ 状況：Ｘ准教授によりＸ准教授本人の送受信メール一覧であることが確認された。
但し、Ｘ准教授には一覧表を印刷した覚えがなく、不正操作が疑われることとなった。

④ 申告：Ｙ教授より、磯田学長に対して本件が報告されるとともに本件に対して調査依頼があった。

1-2. 大学の対応

（１）調査の開始

2021 年 11 月 15 日 16 時 45 分　学長より情報システムセンターへ、状況の保全と事実確認（不正アクセスの有無)、必要ならば至急適切な処置をとるよう指示が出された。

（２）調査の経過

情報システムセンターよりネットワーク保守管理を委託している京都電子計算機株式会社（以下「Kip」という。）に調査を依頼。

複合機（リコー製）の調査は Kip と総務課庶務管理担当佐藤誠係長がリコージャパンと連携して調査を行う。

Kip より「出所不明な印刷物に関する調査報告」（別添資料２）が提出された。

（３）2021 年 11 月 29 日学長への報告

① Kip は、ログ（記録）の調査が可能だった hunet（花園大学学術情報ネットワーク）のファイヤーウォールの解析と、過去 10 週間（2021 年 9 月 12 日～11 月 16 日）のメールサーバー（PO）と Active!Mail のログ解析を行ったが、学内及び学外からの不正アクセスは確認できなかった。

② 一覧表の出力については次のような理由から調査できなかった。

ⅰ）プリンターサーバー（RIN３）のログは、初期値が記録機能〈無効〉となっていた。

ⅱ）拈花館講師控室のリコー複合機のログは、時間、枚数のみの 20 件の出力記録で、出力マシンやユーザー名の紐づけもなかった。調査の指示を受け、11 月 15 日 18 時 31 分の時点で確認したが、同日 15 時 00 分の使用ログが最も古いものであり、それ以前のログはシステム上削除されていた。

ⅲ）講師控室設置のパソコン（HN20897）のイベントログでは、ログイン履歴はあったが、印刷履歴はなかった。

③　Ｘ准教授が確認したところ、数件本人以外のメールもあるが、2019 年 10 月 27 日～2020 年 3 月末ごろのものと推測されるとのこと。

（４）2021 年 12 月 9 日学長への報告

①　上記３）①のファイヤーウォールの調査を 2018 年 10 月まで、メールサーバーの調査を 2020 年 9 月までさかのぼったが、不正アクセスは確認できなかった。

④　　これ以上の検証はできない。

1-3. 関係教員からの申立書の提出

（１）2022 年 1 月 12 日付で児童福祉学科Ｙ教授及びＸ准教授から「申立書―大学メールアカウントへの学内における不正アクセス事件について」（別添資料３省略）が学長宛提出される。申立書では、次の 3 点が要求された。

①　2019 年度に遡ったログ解析

②　当該文書を作成した犯人の特定

③　①、②を含む大学による安全配慮義務の遂行

（２）2022 年 2 月 14 日、ハラスメント相談員の福富昌城教授及び秦美香子教授がＹ教授及びＸ准教授と面談したところ、本件に関して大学に次のような対応を求めるとの要求があった。なお、その際、その他 2 件の事案についても要求があった。

①　2020 年 12 月 25 日に遡った再調査（ログ解析）を求めたい。

②　当該不正アクセスを行った者の特定を求めたい。

③　Ｘ准教授について、大学側に安全配慮義務の履行を求めたい。

④　大学が推奨するメールシステムについて、システム利用者の通信内容に関する秘匿性を担保する安全配慮義務の遂行を求めたい。

1-4. 第三者調査委員会の設置

2022 年 4 月 4 日、市橋克哉（名古屋経済大学法学部特任教授、行政法）、中村素典（京都大学学術情報メディアセンター教授、情報通信）及び井戸清隆（元文部科学省私学部学校法人経営指導室長）で構成される第三者調査委員会を設置、次の事項について調査を依頼した。

①　Ｘ准教授の大学メールアカウントが不正アクセスされ、送信内容が読み取られたと疑われる事案について調査しその結果を報告すること。

②　本件事案から大学が学ぶべきことを報告すること。

1-5. 第 3 者調査委員会の活動の経緯

4 月 25 日（月）16：00～18：00　第 1 回委員会開催（於：裁松館応接室）
5 月 9 日（月）15：00～17：00　第 2 回委員会開催（於：裁松館応接室）
5 月 16 日（月）16：30～19：00 中村教授による検証（於：拈花館講師控室）
5 月 27 日（金）16：00～17：00 中村教授による追加検証（於：拈花館講師控室）
5 月 31 日（火）16：00～18：00　第 3 回委員会開催（於：裁松館応接室）
6 月 14 日（火）17：00～19：00　第 4 回委員会開催（於：裁松館応接室）
7 月　　日　　　　　　　　　　　　中村教授による追加検証
7 月　　日　報告書を磯田学長に提出

2. 第三者調査委員会による調査

今回の事案は、特定の者しか知り得ないはずのメールのサブジェクト（件名）および、そのメールに付随する添付ファイルの名前から構成される 1 枚の「一覧表」が印刷された状態で残されていた、というものである。この印刷物について、どのような方法をとれば印刷することができるのか、という点について、不正アクセスの可能性も含め調査・検討を行い以下のように整理する。なお、以下の整理では、この印刷物から遡ってたどるため、実際の手順とは時間順序的に逆に記載している。（具体的な検証方法は、「○付録 第三者調査委員会による検証の実施とその結果について」を参照のこと。）

2-1. 印刷物の作成方法について

講師控室の複合機に 1 枚の印刷物である「一覧表」が残されていたが、この印刷物には、「花園大学」の表示がない。複合機で複写を行った場合は「花園大学」の文字が印字される仕様となっており、複合機をプリンターとして PC 等から印刷を行った場合には「花園大学」の文字は印字されない。このことから、この印刷物は PC 等から印刷されたものであると考えられる。印刷済みのものが外部から持ち込まれた可能性は否定できないが、そのような可能性は低い。

学内の大学管理の PC においては、印刷の出力先を選択することで、当該複合機をプリンターとして使用することが可能となっている。学内に設置された大学管理の PC であれば、どこからでも印刷することが可能である。また、複合機の IP アドレスを知ることができれば、大学管理でない私物等の PC を大学に持ち込んでプリンターの設定を行うことで印刷することも可能である。なお、私物等の PC から複合機に対して印刷できる条件は、Windows であること（提供されている Mac 用のドライバは古いため、最近の Mac にはインストールが不可）と、学内の有線ネットワークに接続していること（学外や無線ネットワークからは印刷不可）、である。

上述のように、講師控室の複合機をプリンターとして利用することは、学内からであれば可能である。しかしながら、「一覧表」が後述 2-2 の記載の方法で作成されたものであるならば、印刷物は複数ページであった可能性が高く、講師控室内で設置 PC あるいは持ち込み PC を使用して印刷し、最終ページのみ回収し忘れたと考えるのが自然である。（もちろん、意図的に最終ページのみが印刷された可能性は否定できない。）

また、2-2 の記載の方法で作成された「一覧表」を印刷する方法としては、Mozilla Thunderbird から直接印刷する方法と、一旦 PDF として（印刷先をファイルとして）保存したものを印刷する方法とが考えられる。しかしながら、そのようにして印刷されたことを裏付ける証拠（複合機に対する印刷記録や、私物 PC をネットワークに接続した記録等）は確認されていない。

2-2. 「一覧表」の電磁的作成の方法について

印刷物の内容がメールに関するものであることから、メールを扱うアプリケーションの印刷機能について調査を行った。その結果、あくまでも可能性の一つに過ぎないが、用いられた手順の例が判明した。

1. Gmail の Web サイト上、または Mac のメールアプリで、一覧表にあったいくつかのメールが選択され、それらを添付ファイルとする 1 つの転送メールにまとめられた。(以下、「添付ファイルつき転送メール」)
2. 上記の添付ファイルつき転送メールを Mozilla Thunderbird で読み込み、印刷機能を用いて転送メールが印刷された。(読み込む方法としては、メールサーバー経由、あるいはダウンロードされたファイル経由の 2 通りが考えられる。)

一般に、メールをファイルとして保存すると、拡張子 eml をもつファイル(以下、「eml 形式ファイル」)として扱われることが多く、メールに添付されるファイルの形式もこの状態となる。eml 形式ファイルが添付された添付ファイルつき転送メールを Thunderbird から印刷すると、転送メール自体の本文だけでなく、添付されているメールの内容も本文に続けて順次出力される仕様となっている。添付ファイルつき転送メール 1 件の印刷を行うことにより、それに添付されている全てのメールの内容が順に印刷され、最後に添付ファイル一覧が付加される。

この最後に付加される添付ファイル一覧が、問題となっている「一覧表」の形式に酷似している。「一覧表」は A4 用紙横置きの 2 段組であるが、印刷時に 2 ページ分を A4 用紙 1 枚に収める指定を行うことで、印刷形式を合わせることが可能である。印刷例を図 1 に示す。

もし、このような手順で「一覧表」が印刷されたのであるならば、この「一覧表」は最終ページにあたり、それより前のページとしてメールの本文が存在していたと考えられる。従って、一連のページが印刷されたのであれば、最終ページ以外は残されていなかったことから、印刷物を回収するために講師控室内で印刷操作が行われた可能性が高い。

ただし、大学管理の PC には Thunderbird はインストールされておらず、一般ユーザーの権限では Thunderbird をインストールすることができない(正確には、インストールできても、アンインストールすることができない)ことから、Thunderbird がインストールされた私物の PC が利用された可能性が高いと考えられる。なお、Thunderbird は申立人の PC では使用されていないことを確認している。

Subject: Gmailによる転送
From: 中村素典 <[redacted]@kyoto-u.ac.jp>
Date: 2022/04/04 10:06
To: Motonori Nakamura <[redacted]@gmail.com>

—テストメール.eml—

Subject: テストメール
From: Motonori Nakamura <[redacted]@kyoto-u.ac.jp>
Date: 2022/04/04 9:50
To: [redacted]@gmail.com

１通目

—Re: テストメール.eml—

Subject: Re: テストメール
From: Motonori Nakamura <[redacted]@gmail.com>
Date: 2022/04/04 9:51
To: Motonori Nakamura <[redacted]@kyoto-u.ac.jp>

２通目（１通目への返信）

—Re: テストメール.eml—

Subject: Re: テストメール
From: Motonori Nakamura <[redacted]@kyoto-u.ac.jp>
Date: 2022/04/04 9:51
To: Motonori Nakamura <[redacted]@gmail.com>
BCC: [redacted]@kyoto-u.ac.jp

３通目（２通目への返信）

—添付ファイル:—

テストメール.eml	880 バイト
Re: テストメール.eml	5.5 KB
Re: テストメール.eml	1.1 KB

図 1 Thunderbird による印刷例

2-3. 添付ファイルつき転送メールの作成

「一覧表」では、添付ファイルつき転送メールの添付ファイル一覧として、添付されているメールの件名が列挙されているように見えるが、正確には、件名に基づき自動生成される添付ファイルのファイル名の列挙であり、元のメールに最初から添付されていたファイル

のファイル名も一覧に含まれている。このような、メールを転送する際に用いられるファイル名の自動生成方法は、メールの添付操作を行うメールアプリによって異なる。思い付く一般的なアプリについて調査した結果、次のことがわかった。

a. 大学が提供する Active!Mail
   - 添付ファイル形式でのメールの転送に対応しないため該当しない。
b. Windows 標準搭載のメールアプリ（Outlook でない方）
   - 添付ファイル形式でのメールの転送に対応しないため該当しない。
c. Microsoft Outlook
   - 転送メールの添付ファイル名が ForwardedMessage.eml となるため該当しない。
d. Mac 標準搭載のメールアプリ
   - 添付ファイル形式でのメールの転送が**可能**（Google をメールサーバーとして設定し確認）。添付ファイル名の形式も一致する。
e. Gmail (Web ブラウザからの利用)
   - 添付ファイル形式でのメールの転送が**可能**。添付ファイル名の形式も一致する。
f. Thunderbird
   - 添付ファイル形式でのメールの転送が可能。ただし、添付メールの件名の先頭に「Re:」があった場合に、添付ファイルに自動的につけられるファイル名に「Re:」の部分が含まれない。しかし、「一覧表」には返信メールであることを示す「Re:」の記載が含まれている。従って、Thunderbird はこの処理において該当しない。

以上のことから、上記の中では、Mac 標準搭載のメールアプリ、または、Gmail を利用して添付ファイルつき転送メールが作成された可能性が高い。

2-4. 大学のメールサーバーへの不正アクセスの可能性について

大学のメールシステムは、メールボックスを保持するメールサーバーと、ウェブブラウザからメールを閲覧するための Active!Mail サーバーの 2 台構成となっている。それぞれのサーバーに対して試みうる不正アクセスと、その可能性について検討した結果を以下に示す。

A）学内でログアウト操作を失念し放置されてしまった共用 PC にアクセスされた可能性
⇒Active!Mail にアクセスするためのパスワードはブラウザには保存せず毎回入力していたとのことから、Active!Mail には容易にはアクセスできないと考えられる。

B）メールサーバーに POP/IMAP で不正アクセスが行われた可能性
⇒パスワードは初期設定のまま用いられていたものの、ログが残る期間において不審なアクセスは認められておらず（本人によるアクセス時間の照合を含む）可能性は低い。

なお、POP/IMAP は学外からアクセス不可である。

C) Active!Mail サーバーに不正アクセスが行われた可能性
⇒パスワードは初期設定のまま用いられていたものの、ログが残る期間において不審なアクセスは認められておらず（本人によるアクセス時間の照合を含む）可能性は低い。

D) メールの転送設定が不正に書き換えられていた可能性
⇒後述のように申立人は大学に届いたメールを Gmail に転送する設定を行っているが、メールの転送先は複数設定できないことからこの可能性は低い。もし発覚すれば転送先が知られることとなり不正アクセスの証拠となることからも、この可能性は低い。

E) 大学の PC に不正アクセスが行われた可能性
⇒Web ブラウザ経由での Active!Mail へのアクセスでしかメールを扱っておらず、PC 自体にはメールのデータは残らないため、メールの入手は困難である。

F) 大学の PC を踏み台にしてメールに不正アクセスが行われた可能性
⇒ブラウザには Active!Mail サーバーにアクセスするためのパスワードが保存されていないことから可能性は低い。PC ではウイルス感染も確認されておらず、この PC へのリモートデスクトップも使用できない設定となっている。

G) 大学の PC の停止中に同じ IP アドレスを設定した PC が接続され不正アクセスが行われた可能性
⇒同一 IP アドレスは設定可能ではあるが、ログが残る期間において不審なアクセスは認められておらず（本人によるアクセス時間の照合を含む）可能性は低い。

H) メールサーバーに管理者権限で不正アクセスが行われた可能性
⇒管理者アカウントは適切に管理され、不審なアクセスも確認されていない。

I) Active!Mail サーバーに管理者権限で不正アクセスが行われた可能性
⇒管理者アカウントは適切に管理され、不審なアクセスも確認されていない。

2-5. 申立人の自宅の PC 等への不正アクセスの可能性について

申立人は自宅の PC からも大学の Active!Mail を利用している。また、大学のメールサーバーに届いたメールは、すべて Gmail に転送されるように設定しており、Gmail も Web ブラウザを用いてアクセスしている。このような状況において、試みうる不正アクセスと、その可能性について検討した結果を以下に示す。

J) 学内でログアウト操作を失念し放置されてしまった共用 PC にアクセスされた可能性
⇒Gmail にアクセスするためのパスワードはブラウザに保存していたとのことから、容易にメールを閲覧・送信することが可能である。メールボックスに保存されているメールをいくつか選択し、添付ファイル形式で転送を行うことも容易である。個人利用の Gmail についてはメールの送信ログを確認することができないため、送信済みメールの

フォルダに送信したメールが残されていなければ、送信履歴を確認することができない。（不審なメールは送信済みメールのフォルダには見当たらないとのことである。）

K）Gmail に Web ブラウザから不正アクセスが行われた可能性

⇒Gmail のパスワードは推測が難しいものが使用されており、不審なログインについての Google からの通知も届いていない。（通知が削除された可能性は残る。）なお、二要素認証を使用する設定にはなっていないため、パスワードがわかればログイン可能ではあった。

L）Gmail に POP/IMAP で不正アクセスが行われた可能性

⇒パスワードは推測が難しく、不審なログインについての Google からの通知も届いていない。（通知が削除された可能性は残る。）

M）Gmail の転送設定が不正に設定されていた可能性

⇒Gmail にアクセスできている時点で目的は達成されているため、転送の必要性がない。発覚すれば不正アクセスの証拠となることからも、この可能性は低い。

N）自宅の PC に不正アクセスが行われた可能性

⇒PC には推測が難しいログオンパスワードが設定されており、ウイルスバスターもインストールされているため可能性は低い。

O）自宅の PC を踏み台にしてメールに不正アクセスが行われた可能性

⇒ブラウザやメールアプリにパスワードが保存されていることから、PC に不正アクセスできれば、メールへのアクセスは容易である。PC には推測が難しいログオンパスワードが設定されており、ウイルスバスターもインストールされているため可能性は低い。

P）自宅の無線 LAN に不正に接続された PC から本人になりすまして不正アクセスが行われた可能性

⇒WPA2 パーソナルで暗号化されており、接続には推測が難しい 12 文字のパスワードが必要であり、不正アクセスの可能性は低い。

3.　不正アクセスの可能性等に関する判断

第三者調査委員会は、先に記した「1. 事案の経緯」および「2. 第三者調査委員会による調査」を踏まえて、不正アクセスの可能性等に関して、以下のように判断した。

3-1. 講師控室の複合機による「一覧表」の作成に関する判断

①　「一覧表」には「花園大学」の印字は入っていない。講師控室の複合機による複写であれば「一覧表」に「花園大学」の印字が入る。したがって、「花園大学」の印字が入っていない「一覧表」は、複合機をプリンターとして使用する方法で、PC 等から印刷されたものであると、第三者調査委員会は判断した。

②　学内の大学管理の PC を使用すれば、複合機のプリンター機能を用いて「一覧表」を印刷できる。なお、私物の PC であっても、Windows で学内優先ネットワークに接続した PC であり、かつ、複合機の IP アドレスが分かれば、私物の PC で複合機のプリンター設定を行うことで、「一覧表」の印刷ができる。したがって、大学管理の PC、または、上記の諸条件を満たす場合は私物の PC によって、「一覧表」が複合機のプリンター機能を用いて印刷されたと、第三者調査委員会は判断した。

③　ただし、後述の 3-3 で解明されたように、大学管理の PC には、Thunderbird をインストールすることができないため、Thunderbird をインストールした私物の PC によって印刷された蓋然性が高いと、第三者調査委員会は判断した。

④　「一覧表」を複合機のプリンター機能を用いて印刷する場合、Thunderbird から直接印刷する方法および PDF に保存したものを印刷する方法という二つの方法がある。しかし、複合機の印刷記録または私物の PC をネットワークに接続した記録等の証拠は保存されていない。したがって、第三者調査委員会は、上記の二つの方法のうちどちらの方法で印刷したかを特定することはできなかった。

3-2. 講師控室の複合機による「一覧表」以外の「印刷物」の作成に関する判断

①　「一覧表」は、後述の３－３で解明した方法により作成した蓋然性がきわめて高いと、第三者調査委員会は判断した。この方法で「一覧表」が作成される場合、「印刷物」の最後の頁となる「一覧表」の前に、相当頁にのぼるメールそれぞれの内容を盛り込んだ「印刷物」が講師控室の複合機のプリンター機能を用いて印刷されていたと、第三者調査委員会は判断している。

②　「1. 事実の経緯」によれば、講師控室の複合機周辺には、「一覧表」のみが放置されており、最後の頁である「一覧表」以外の「印刷物」はなかった。したがって、「印刷を行った者」は、誤って最後の頁である「一覧表」を回収しなかったため、「一覧表」が複合機周辺に放置された蓋然性が高いと、第三者調査委員会は判断した。

③　論理的には、「印刷を行った者」が故意に「一覧表」だけを複合機で印刷したという可能性についても、第三者調査委員会は排除するものではない。しかし、たとえ特定の者を威嚇する意図があったとしても、多数の者が日常的に利用する講師控室に故意に「一覧表」だけを放置するという行為は合理的なものではないため、この可能性は低いと判断した。

④　第三者調査委員会は、「一覧表」に加えて相当頁にのぼるメールそれぞれの内容を盛り込んだ「印刷物」が講師控室の複合機のプリンター機能を用いて、「申立人以外の者」によって印刷されたと判断している。「一覧表」もメールそれぞれの内容も、個人情報保護法が定める個人情報、すなわち、個人識別情報にあたる（個人情報保護法 2 条 1 項 1 号)。そして、これらの個人情報のなかに学術研究目的で取扱う個人情報が含まれている場合は、学術研究機関である大学は、この法律の規定を遵守するとともに、その適正を確保するために必要な措置を自ら講じなければならないと定められている（個人情報保護法 59 条)。第三者調査委員会は、印刷されたメールに含まれる個人情報の内容を調査する任務を有するものではないが、個人情報保護法の遵守という観点に立ったこれらのメールの内容（学生および研究対象の者の個人情報（答案・成績、家庭・健康状況等）の有無）の確認についても、大学には求めるものである。

3-3.　「一覧表」の電磁的作成方法に関する判断

①　「2. 第三者調査委員会による調査」によると、eml 形式によりファイルされた相当数のメールから構成された添付ファイルが添付された転送メールについて、これを Thunderbird を用いて印刷すると、(1) 転送メールそれ自身の本文が印刷されるのに加えて、(2) 添付ファイルを構成する相当数のメールそれぞれの内容も順次印刷される、そして、(3) 最後の頁として、添付ファイルの「一覧表」が印刷される。

②　①の「2. 第三者調査委員会による調査」が試した方法で印刷した添付ファイルの「一覧表」の形式は、複合機周辺に放置されていた「一覧表」のそれに酷似していることが分かった。そして、後者の「一覧表」は A4 横書き 2 段組であるが、前者の「一覧表」も、印刷時に A4 一枚につき 2 頁という指定を行えば、後者の「一覧表」と同一の形式となることも分かった。

③　したがって、複合機周辺に放置された「一覧表」は、①および②による電磁的作成方法でつくられた蓋然性がきわめて高いと、第三者調査委員会は判断した。

④　大学管理の PC には Thunderbird はインストールされていない。また、一般ユーザーには、Thunderbird をインストールする権限はない。したがって、複合機周辺に放置された「一覧表」は、Thunderbird をインストールした私物の PC によって、講師控室の複合機の印刷機能を用いて印刷された蓋然性が高いと、第三者調査委員会は判断した。

3-4.　添付ファイルつき転送メールの作成に関する判断

①　「2. 第三者調査委員会による調査」によると、「一覧表」は、それぞれのメールの件名および添付ファイル名に基づいて自動作成されるものである。この「一覧表」の自動作成方法は、メールの添付操作を行うメールアプリごとに異なる。

②　「2. 第三者調査委員会による調査」は、6 通りの自動作成方法について調べている。その結果、Mac 標準搭載のメールアプリ、または、Gmail を利用して、添付ファイルつき転送メールの作成が行われた可能性が高いと結論づけており、第三者調査委員会も、この結論を自らの判断とした。

3-5. 大学のメールサーバーに対する不正アクセスに関する判断

①　「2. 第三者調査委員会による調査」は、大学のメールシステムであるメールボックスをもつメールサーバーおよびウェブブラウザからメールを閲覧するための Active!Mail サーバーの二つのサーバーに対する不正アクセスの可能性について、個別具体的かつ詳細な調査を行った。

②　この調査によると、A)からＩ）まで、9 通りにもわたる不正アクセスの可能性について、それぞれ検討を行っている。これらの検討の結果は、いずれの不正アクセスの可能性についても、ログが残る期間が限定されていたり、管理者アカウントの管理に不適切な点は見つからず、不審なアクセスも確認されていなかったりで、現時点では特定の方法で行われたと判断することはできないとするものであった。

③　この「2. 第三者調査委員会による調査」による大学のメールサーバーに対する不正アクセスに関する判断を受けて、第三者調査委員会としては、残念ではあるが、大学のメールサーバーに対する不正アクセスの特定は、現時点ではできないと判断せざるをえなかった。

3-6. 申立人の自宅の PC 等に対する不正アクセスに関する判断

①　「2. 第三者調査委員会による調査」は、申立人の自宅 PC からの Active!Mail へのアクセスが Gmail を用いて行っていることから、Gmail および自宅 PC に対する不正アクセスの可能性について、個別具体的かつ詳細な調査を行った。

②　メールを eml 形式によりファイルすることは、Gmail または Thunderbird を用いた場合に限られる。大学では Gmail を業務に使用しておらず、また大学管理の PC には Thunderbird がインストールされていないことに鑑みると、申立人が個人的に使用する Gmail に不正アクセスが行われた可能性の方が高いと、第三者調査委員会は判断した。

③　この調査によると、J)から P）まで、7 通りの不正アクセスの可能性について、それぞれ検討が行われている。検討の結果は、いずれの不正アクセスの可能性についても、推測困難なパスワードが用いられていたり、ログが残る期間が限定されていたりするため、現時点では、不正アクセスの方法を特定できないとするものであった。

④　この「2. 第三者調査委員会による調査」による申立人の自宅の PC 等に対する不正アクセスに関する判断を受けて、第三者調査委員会としては、この問題についても残念ではあるが、申立人の自宅の PC 等に対する不正アクセスの特定は、現時点ではできないと判断せざるをえなかった。

3-7.　まとめ

①　第三者調査委員会は、「1. 事実の経緯」および「2. 第三者調査委員会による調査」を踏まえて、不正アクセスの可能性等に関して判断した。

②　講師控室の複合機周辺に放置された「一覧表」を証拠として保全したことから、第三者調査委員会は、講師控室の複合機による「一覧表」の作成方法、講師控室の複合機による「一覧表」以外の「印刷物」の作成方法、　「一覧表」の電磁的作成方法、および、添付ファイルつき転送メールの作成方法については、どのような方法がそれぞれ用いられたかについて、一定の解明を行うことができた。

③　しかし、大学のメールサーバーに対する不正アクセスの方法、および、申立人の自宅の PC 等に対する不正アクセスの方法については、数多くの可能性に関する個別具体的で詳細な調査を第三者調査委員会は行ったものの、残念ながら、証拠となる種々のログが残っていなかったり、管理者アカウントの管理に不適切な点は見つからず、不審なアクセスも確認されていなかったりなどで、その解明を阻む制約となった。

4. 今後の再発防止と情報管理の改善のための課題について

4-1 情報システム運用の改善

（1）電子メールサービスの管理

Active!Mail は多くの大学等で利用されているソフトウエアであり、それ自体には問題はないと考えるが、その運用にあたっては、いくつかの考慮すべき点があるように見受けられる。

① メールサーバーにアクセスする際のセキュリティ設定
パスワードが平文でネットワークを流れると、盗聴によるなりすましを招きかねないため、パスワードによる認証が必ず暗号通信の中で行われる運用が求められる。Web メールを HTTPS で暗号化するように、POP・IMAP・SMTP についても TLS（それぞれ、POPS、IMAPS、SMTPS）で暗号化する等の対応が望まれる。POP・IMAP 等への学外からのアクセスは不可となっているようだが、学内からのアクセスについても暗号化設定を必須とすることが望ましいと考える。すでにそのような運用になっている可能性もあるが、そのことを確認、把握しておくことが大切である。

② 電子メールの自動転送
大学のメールサーバーから学外の（個人契約の）メールサーバーへの自動転送は必ずしも禁止する必要はないが、大学の機密情報が意図せずメールから漏えいしてしまわないよう、転送先となるメールサービスの管理（パスワード管理、不正アクセス対策等）は転送を行う利用者（教職員）の責任において行うべきものであることを周知しておく必要があると考える。
また、電子メールは情報漏えいが発生しやすい通信手段であるという前提のもと、重要な情報は添付ファイルとして送信するのではなく、受信者本人であることを確認した上でダウンロードしてもらうような方法など、確実に受信者本人のみが受け取ることができる手段を利用することが望まれる。

参考：高等教育機関の情報セキュリティ対策のためのサンプル規程集
（https://www.nii.ac.jp/service/sp/）
D3252 電子メール、メッセージング利用ガイドライン

（2）パスワード管理

① 初期パスワードの変更

アカウントの発行を受けたら、すぐに初期パスワードを変更することが求められる。初期パスワードは印刷され複数の人の手を介すること多いため漏えいする可能性が高く、関係者が不必要に疑われたりしないように、また初期パスワードが漏えいしたとしても問題とならないようにするためにも、利用開始時のパスワード変更は不可欠である。(パスワードを変更しなければ利用が開始できないようになっていることが理想である。)

一方、パスワードの定期的な変更は、現在は必ずしも必要とはされていない。定期的な変更より、他のシステムでも利用しているパスワードの使いまわしを避ける方が重要である。

② パスワードの文字列

パスワードは漏えいしなかったとしても、計算機による総当たり解読攻撃(ブルートフォースアタック)への耐性が求められる。計算機の能力の向上により、現在では8文字でも十分安全とは言えないとされている。

参考:(同) D3255 認証情報管理ガイドライン

③ ブラウザへのパスワード保存に対する配慮

最近のブラウザは、ログインした際にパスワードを記憶する機能がある。パスワードを記憶させておくと煩わしいパスワード入力作業を省略することができる。しかし、ブラウザに不正アクセスされた場合に、パスワード自体が表示されることがないとしても、容易にログインを許してしまうことになるため、ブラウザへのパスワードの保存には注意が必要である。

キオスク端末ではパスワードを入力しないように注意することは当然として、他人が容易に触れることが可能な場所で使用するノート PC や共用 PC においては、安全なログインパスワードが設定されていることを確認するとともに、離席時にログアウトやスクリーンロックされていることを確認することが重要である。

また、盗難・紛失時の情報漏えい対策として、ハードディスクの暗号化を行っておくことを推奨する。

(3) ログ管理

① ログの保存期間

アクセス記録(利用記録)の保存はセキュリティ対策の上で重要な事項の一つである。様々なインシデントの発生に備え、どのような内容のログが保存されるかについて把握しておくことが大切である。また、ログの保存期間についても確認しておく必要がある。以前は、最低3ヶ月分の記録を保存すべきとされることが一般的であったが、インシデントの発

生が発覚した際にそれでは保存期間が不足している事例が多いことから最近では 1 年分の記録の保存が一般的になりつつある。今回の場合、メールの送受信記録、端末へのログイン記録、PC のネットワークへの接続記録、プリンターへの印刷記録などの確認が必要であったが、これらについて必要な情報が必要な期間保存されるかどうかについての見直しを推奨する。

参考：(同）D2101 情報セキュリティ対策基準

② ログの保存範囲

ログはインシデント対応のためのみでなく、運用しているシステムの更新等の際に、個々の設備の利用率等を把握して改善につなげるための重要な情報源となる。例えば、プリンター利用についても、だれがいつどの程度の印刷を行ったかを把握しておくことは、コスト削減や設備増強を検討する上でも重要であろうと考える。

（４）情報システムの利用方針の明確化

① 情報格付けに基づく情報の適切な取り扱い

情報システムで扱う情報について、機密性・完全性・可用性のそれぞれの観点においてレベル分けを行うとともに、情報漏えいすると支障がある要機密情報（機密性２情報、機密性３情報）については、その扱い方を定め、情報を受け渡す際に明記するといった対応が望ましいとされている。

参考：(同）D2102 情報格付け基準、D3102 情報格付け取扱手順

② 大学の資産としての情報システムの運用方針

大学により提供される情報システムにおいて扱われる情報については、その適正な管理に責任を負う大学として把握・確認しなければならない場合がある。大学は利用規程を定めて、大学が当該情報を把握・確認することができる場合について、個別具体的に明記する。

サンプル規定において運用方針を明確化することについても言及がある。

参考：(同）D3252 電子メール、メッセージング利用ガイドライン

4-2. 情報システム運用の改善に実効性を持たせるための対応

① システム運用に関する学内規則の整備

大学管理下にあるシステムに関して、システム管理者がログ管理を行うこと、必要に応じて電子メールのモニタリング等が行われること、システム運用に関して問題生じた場合迅速な対応（原因の調査、その後の対処等）が可能となるよう責任と権限を明確化すること、などを学内規則上明記する。特に、個人メールのモニタリングについては、個人情報に配慮しつつも、システム管理者の権限と責任において、適切な条件および手続きに基づいて実施されるべきものであり、速やかに整備が必要である。

参考：「個人情報の保護に関する法律についてのガイドライン」 に関するＱ＆Ａ
令和４年５月26日、個人情報保護委員会（令和４年６月18日確認）
（従業者の監督）
Ｑ５－７ 従業者に対する監督の一環として、個人データを取り扱う従業者を対象とするビデオやオンライン等による監視（モニタリング）を実施する際の留意点について教えてください。
Ａ５－７ 個人データの取扱いに関する従業者の監督、その他安全管理措置の一環として 従業者を対象とするビデオ及びオンラインによるモニタリングを実施する場合は、次のような点に留意することが考えられます。なお、モニタリングに関して、個人情報の取扱いに係る重要事項等を定めるときは、あらかじめ労働組合等に通知し必要に応じて協議を行うことが望ましく、また、その重要事項等を定めたときは、従業者に周知することが望ましいと考えられます。
○モニタリングの目的をあらかじめ特定した上で、社内規程等に定め、従業者に明示すること
○モニタリングの実施に関する責任者及びその権限を定めること
○あらかじめモニタリングの実施に関するルールを策定し、その内容を運用者に徹底すること
○モニタリングがあらかじめ定めたルールに従って適正に行われているか、確認を行うこと

② 説明会の実施

①を整備したのち、すべての構成員を対象として情報システム及び個人情報保護に関する説明会を実施し十分に周知する。

③ サポート体制の強化

財政的な制約はあるが、情報システムの運用体制及び問題対処への実務を担う部門の強化を行う。

○　付録 第三者調査委員会による検証の実施とその結果について

大学における情報環境として、どのようなサービスが提供され、どのような操作が可能となっているかという点について、講師控室を訪問し実際に操作を行ってみた。前述のとおり、添付ファイル形式でメールが扱われた可能性が高いこと、印刷形式の作成に Mozilla Thunderbird が使用された可能性が高いことから、そのような操作に関連する次の 3 つの操作シナリオについて検証を行った。

1. Active!Mail によるメール転送操作の挙動
2. Mac のメールアプリと Thunderbird との組み合わせによる挙動
3. Gmail と Thunderbird との組み合わせによる挙動

■シナリオ 1：Active!Mail によるメール転送操作の挙動

大学が提供する Active!Mail（Web ブラウザからの利用）において、一覧表の元データとなる添付ファイル形式のメールが作成された可能性について検証する。

手順

1. 検証用のアカウントを大学にてご用意頂く。
2. 適当なサブジェクトのテストメールを自分宛に送信する。
3. 前項のテストメールに対して返信する（サブジェクトに Re:がつく）。
4. 前項の返信メールに対して返信する（サブジェクトが前項と同じになる）。
5. 新たなメールを作成し、項番 1、2、3 のテストメールを添付して、自分宛に返信する。
6. 届いたメールの添付ファイル名を調べて、項番 1、2、3 のサブジェクトがそのまま添付ファイル名になっているかどうか確認する。

結果

- 大学で提供されている Active!Mail では、メール作成時にメールボックスに保存されているメールを直接添付することができず、メールを一旦ファイルに保存した上で、そのファイルを指定する形で添付操作を行う必要があることが確認された。このため、添付ファイル形式のメールを含む転送メールを Active!Mail を用いて作成することは容易ではない（非常に煩雑であり現実的ではない）ことを確認した。

■シナリオ 2：Mac のメールアプリと Thunderbird との組み合わせによる挙動

このシナリオでは、メールサーバーにアクセスする PC として Mac が用いられた可能性について検証する。メールサーバーに対して（Mac にインストールされた）Thunderbird からもアクセスする方法と、Thunderbird は印刷形式を作成するためだけに使用する（メールサーバーへのアクセスには使用しない）方法が考えられるため、2 つの手順について検証する。

準備

（シナリオ 1 の手順 1〜4 と同じもの。Active!Mail にて準備。）
1. 検証用のアカウントを大学にてご用意頂く。
2. 適当なサブジェクトのテストメールを自分宛に送信する。
3. 前項のテストメールに対して返信する（サブジェクトに Re:がつく）。
4. 前項の返信メールに対して返信する（サブジェクトが前項と同じになる）。

（Mac に対する準備）
5. Mac を大学（講師控室）のネットワークに接続できるように準備する。
6. Mac から講師控室のプリンター（複合機）に印刷できるように設定する。
7. Mac のメールアプリから、大学のメールサーバーにアクセスできるように設定を行う。

手順 1　（Thunderbird からメールサーバーに直接アクセスしない場合）

8. Mac のメールアプリで、新たなメールを作成し、項番 2、3、4 のテストメールを添付して、下書きとして保存する。
9. 保存した下書きをファイルとして保存する。
10. 保存したファイルを Thunderbird で開く。
11. 講師控室のプリンタ（複合機）に印刷する。（一旦 PDF として保存し、それを印刷する方法もある。）

結果

- Mac から講師控室のプリンター（Ricoh imagio MP C5000）に印刷するためにはプリンタドライバのインストールが必要であるが、メーカから提供されているプリンタドライバは MacOS 10 用（最終更新 2006 年 2 月）であり、その対応 OS は MacOS 10.5（2007 年 10 月リリース、PowerPC 版 Mac 最終バージョン、2011 年頃サポート終了）までである。最近の MacOS には対応していないため（MacOS 12.3 へのインストール

を試みたが印刷できず)、約 10 年前の古い Mac を利用しない限り Mac から直接印刷することは不可能であると考えられる。(MP C5000 の後継機種については最近の MacOS 用のドライバが提供されているが、そのようなドライバを用いたとしても、MP C5000 に印刷することはできなかった。)

- Mac のメールアプリから大学のメールサーバーにアクセスできるように設定を試みたが、設定を完了することができなかった。このような方法は不可能である、とまでは言い切れないが、容易ではないと思われる。

手順 2 (Thunderbird からメールサーバーに直接アクセスする場合)

12. Thunderbird から、大学のメールサーバーにアクセスできるように設定を行う。
13. Thunderbird を利用して項番 8 で保存した下書きファイルを開く。(項番 8 のメールが送信され、それを受信して開いたものでも可。この場合、項番 12 は大学のメールサーバーでなくても良い。)
14. 講師控室のプリンタ(複合機)に印刷する。(一旦 PDF として保存し、それを印刷する方法もある。)

結果

- Mac にインストールした Thunderbird からは大学のメールサーバーにアクセスできるよう設定することができた。
- 項番 8 が実施できていないため、項番 13 は確認できず。
- 手順 1 の結果の通り、Mac からの印刷はできなかった。講師控室の PC からであれば、一旦 PDF にしたものを印刷することが可能であることを確認した。

■シナリオ 3:Gmail と Thunderbird との組み合わせによる挙動

このシナリオでは、Gmail (Web ブラウザによる利用)が用いられた可能性について検証する。Gmail に対して Thunderbird からもアクセスする方法と、Thunderbird は印刷形式を作成するためだけに使用する(メールサーバーへのアクセスには使用しない)方法が考えられるため、2 つの手順について検証する。

準備(シナリオ 1 の手順 1～4 と同じもの。Active!Mail から Gmail への転送設定を行った上で Active!Mail で実施するのが望ましいが、Gmail 上で実施しても構わない。)

1. 検証用のアカウントを大学にてご用意頂く。(Gmail を含む。)

2. 適当なサブジェクトのテストメールを自分宛に送信する。
3. 前項のテストメールに対して返信する（サブジェクトに Re:がつく）。
4. 前項の返信メールに対して返信する（サブジェクトは前項と同じになる）。

手順 1　（Thunderbird からメールサーバーに直接アクセスしない場合）

5. （Gmail 上で）新たなメールを作成し、項番 2、3、4 のテストメールを添付して、下書きとして保存する。
6. 保存した下書きを、USB メモリにファイルとして保存する。
7. Thunderbird がインストールされた PC で、USB メモリのファイルを開く。
8. Thunderbird で印刷し、出力を PDF として保存する。
9. 講師控室の PC で USB に保存した PDF ファイルをプリンタ（複合機）で印刷する。

結果

- Gmail では、下書きとして保存されたメールはダウンロードすることができない。（下書き状態のメールは、他のフォルダに移動させても下書きとして扱われ、ダウンロードできない。）一旦自分宛に送信されたメールであれば、受信箱からダウンロードして USB メモリにファイルとして保存することができた。
- 講師控室の PC には Thunderbird はインストールされていないが、利用者権限にて Thunderbird がインストールできることが確認された（管理者権限が要求されたが、認証をキャンセルするとインストールを進めることができた）。ただし、アンインストールには管理者権限が必要であった。調査の段階でインストールはされていなかったため、講師控室の PC で Thunderbird が利用された可能性は否定できる。（なお、大学は設定に不備があることを認識しており、インストールができないように順次設定変更作業を行っていたが、設定が完了していない端末として残されていた、とのことである。）
- 他の PC にインストールされている Thunderbird で PDF に変換したファイルを USB メモリに保存し、そのファイルを講師控室の PC からプリンターで印刷することができた。
- Gmail で作成しメールを添付した転送メールを Thunderbird で開いて印刷することで、問題となっている一覧表の形式が得られることを確認した。
- Thunderbird がインストールされた PC が Windows であれば、大学のネットワークに有線で接続し、プリンタドライバをインストールすることで、一旦 PDF に保存することなく、PC から直接大学のプリンターに印刷することも可能であった。（無線接続の場合や、学外からは印刷不可とのこと。）

手順 2　(Thunderbird からメールサーバーに直接アクセスする場合)

10. Thunderbird がインストールされた PC から、Gmail にアクセスできるように設定を行う。
11. Thunderbird で項番 5 により保存した下書きファイルを開く。(項番 5 のメールが送信され、それを受信して開いたものでも可。この場合、項番 10 のアクセス先は Gmail でなくても良い。)
12. Thunderbird で印刷し、出力を PDF として保存する。
13. 講師控室の PC で USB に保存した PDF ファイルをプリンタ(複合機)で印刷する。

結果

- Thunderbird から Gmail にアクセスすれば、下書きとして保存されたメールを参照することができる。(講師控室に持ち込んだ PC から Thunderbird で Gmail に接続できることは確認できた。)
- PDF ファイルにして印刷可能であることは手順 1 で検証済み。
- Thunderbird がインストールされた PC が Windows であれば、大学のネットワークに有線で接続し、プリンタドライバをインストールすることで、一旦 PDF に保存することなく、PC から直接大学のプリンタに印刷することも可能であった。(無線接続の場合や、学外からは印刷不可とのこと。)

花園大学

別添資料 1

Re: お願い.eml	16.9 KB
Re: お願い.eml	4.2 KB
お願い.eml	1.9 KB
Re: 学科会議のお願い.eml	5.4 KB
学科会議のお願い.eml	3.8 KB
Re: 名簿について.eml	8.9 KB
Re: 名簿について.eml	7.2 KB
Re: 名簿について.eml	5.1 KB
Re: 名簿について.eml	13.6 KB
Re: 名簿について.eml	2.8 KB
Re: 2020年度学科会議4/1教授会終了後、共同研究室.eml	6.8 KB
Re: 実習について.eml	4.2 KB
Re: 実習について.eml	6.8 KB
Re: 事後報告で申し訳ありません。.eml	3.6 KB
Re: 明日の検討会議.eml	2.0 KB
学科開講科目表.eml	77.5 KB
(12[redacted]学科2015～.xlsx	55.5 KB
業務説明書の作成（依頼）.eml	277 KB
2019[redacted]学科担当一覧.pdf	120 KB
記入例：業務説明書（入試委員会）.pdf	80.1 KB
Re: 進路データ提出（就職課）.eml	7.7 KB
Re: お願い.eml	1.3 KB
Re: おはようございます。[redacted]です。.eml	5.0 KB
《ご相談》せんみつの授業担当と「研究業績」との関係について.eml	4.9 KB
Re: [redacted]eml	14.4 KB
[redacted]です.eml	1.4 KB
シラバス第三者チェックのお願い.eml	2.1 KB
Re: [redacted]です。.eml	4.3 KB
Re: [redacted]です.eml	2.3 KB

《重要「文書」》[redacted]学科主任版「五箇条のご誓文」(2019年10月27日).eml	167 KB
お願い.pdf	117 KB
Re: シラバス、他について.eml	17.2 KB
Re: [redacted]です.eml	2.8 KB
Re: 《重要》面談のお願い!!.eml	4.8 KB
[redacted]です.eml	1.6 KB
返信が遅くなり失礼致しました [redacted] .eml	3.9 KB
[redacted]の教員数の件.eml	1.7 KB
[redacted]の専任教員について.eml	1.0 KB
Re: お礼[redacted].eml	2.1 KB
《重要》2020年1月27日(月)の将来構想検討会議への参加について.eml	6.7 KB
Re: 本年もよろしくお願いいたします [redacted].eml	2.6 KB
Re: お願いの件です[redacted]eml	3.0 KB

別添資料２

令和 3 年 11 月 19 日

花園大学
情報システムセンター　御中

京都電子計算株式会社
ネットワーク部
NW1 課　課長　山田恵一

出所不明な印刷物に関する調査報告

平素より格段のご愛顧を賜り、厚く御礼申し上げます。
さて、令和 3 年 11 月 15 日(月)に発生しました出所不明な印刷物に関する調査につきまして、下記のとおり報告申し上げます。

敬具

記

1. 事象の概要
11 月 15 日(月)9:00 頃、拈花館 3F 講師控室内のプリンタに、出所不明の印刷物が放置されていた。印刷物の内容から類推された持ち主に印刷した覚えが無いため、不正操作を疑われた。

2. 調査内容

No	日時	場所	調査対象	内容
1	11/16 17:45	拈花館 3F 講師控室	印刷物確認	印刷内容を確認した。
2	11/16 18:26	リモート	プリンタサーバ(RIN3)	Windows イベントログにて印刷履歴を調査した。 →印刷履歴の記録機能が無効（デフォルト値）であり調査不可であった。
3	11/16 18:31	リモート	プリンタ（複合機）	Web UI にて印刷履歴を確認した。 →11/15　15:00 頃のログが最も古く、確認不可であった。
4	11/16 18:48 頃	リモート	メールサーバ(PO)	POP/IMAP アクセスログを調査した。 過去 10 週間にアクセス記録はなかった。 →ActiveMail 以外でメール参照されていない、と判断。
5	11/16 18:55 頃	リモート	ActiveMail	認証ログを調査した。接続元の IP アドレスは HN[redacted]（[redacted]）と[redacted]保有の IP アドレスであった。 →持ち主と思われる教員に割当られた PC と、その教員が契約する ISP[1]であり、本人のアクセスと判断。
6	11/16 18:55 頃	拈花館 3F 講師控室	教育系クライアント（HN[redacted]）	Windows イベントログにて印刷履歴を調査した。 →印刷履歴の記録機能が無効（デフォルト値）であり調査不可であった。

[1] インターネットサービスプロバイダ

別添資料２

7	11/16 19:20 頃	拈花館 3F 講師控室	教育系クライアント （HN[redacted]）	Windows イベントログにてログイン履歴を調査した。 →確認内容は以下の通りである。 [redacted] 2021/11/13(土)10:38～10:57 ※印刷履歴は無し。
8	11/17 10:45	栽松館 [redacted]F [redacted] 室	教育系クライアント （HN[redacted]）	コントロールパネルの「プログラムと機能の 確認」にてインストールされたプログラムを確認した。 →不審なプログラムがインストールされた形跡はなかった。
9	11/17 11:00	栽松館 [redacted]F [redacted] 室	教育系クライアント （HN[redacted]）	サービスにて起動されているサービスを確認 した。 →不審なサービスは存在しなかった。
10	11/17 14:00	拈花館 3F 講師控室	教育系クライアント （HN[redacted]）	Windows イベントログにてログイン履歴を調査した。 →確認内容は以下の通りである。 [redacted] 2021/10/26(火)13:58～14:02 [redacted] 2021/10/27(水)9:38～9:40 [redacted] 2021/10/27(水)10:58～11:04 [redacted] 2021/10/28(木)8:53～8:58 [redacted] 2021/11/13(土)10:38～10:57 ※印刷履歴は無し。

3. 印刷物の元データについて
あるユーザーの受信メールの件名が表形式で記載されたものです。ユーザーのメールアドレスより、関連する PC を特定しました。

4. メールの不正ログインの有無について
11/16 の調査時から過去 10 週間分（2021/9/12～2021/11/16）のアクセスログを確認したところ、学内の特定クライアント PC と、特定プロバイダからのアクセスに限られていました。学内 PC はメールアドレスの利用者の PC であり、特定プロバイダは 1 社で、その利用者が契約するプロバイダであることを確認しました。
以上の事から、学内・学外で不正ユーザーによるログインは存在しないと判断しております。

5. プリンタサーバで印刷履歴の記録機能が無効であった点について
本機能は資産管理システム等で印刷履歴を管理する際に利用することが多いです。貴学では資産管理システムのご利用が無いため、デフォルト値の無効状態で運用しております。

以上

別添資料２

別紙）ネットワークセキュリティについて

1.　インターネットへの通信について

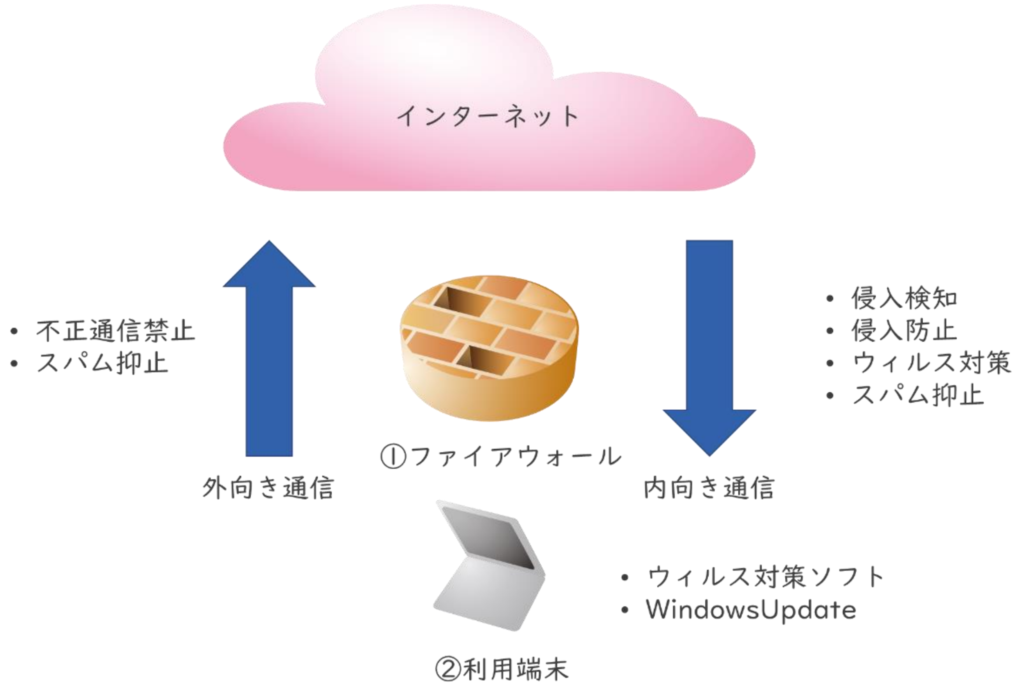

図 1

　学内ネットワークとインターネットの境界にファイアウォール（図 1 の①）を配置しています。学内ネットワークから見て外向きの通信と内向きの通信の際、ファイアウォールの通過時に通信パケットの検査を行い、不正な通信を抑止しています。

　不正な通信抑止の例）
（↑）外向き通信
　　　不正操作の踏み台サーバ（C&C サーバ）への通信を抑止する
　　　スパムメールの発信を抑止する
（↓）内向き通信
　　　侵入を試みる通信を検知し抑止する
　　　ウィルスを含む通信を抑止する
　　　スパム受信を抑止する

2.　端末へのログイン認証について

　統合認証基盤によりユーザーアカウントとパスワードを一括管理しています。管理対象となるシステムは次の通りです。

① PC 利用時のユーザーアカウント
② Web メール
③ 無線 LAN

3.　端末のウィルス対策について
　ウィルス対策ソフトはトレンドマイクロ社のウィルスバスターをインストールしています。