Chapter 9

著作権とセキュリティー

本章では、情報コンテンツの著作権や悪意のあるソフトウェア（コンピューターウイルス）への対策など、コンピューターを利用する際の一般的な注意事項をご説明します。コンピューターとそれを使用するユーザーは日々、様々な危険に晒されています。コンピューターやそこに保存されたデータを守るためにも、意図せざる法令違反を避けるためにも、ぜひ本章をご一読ください。

※本書に記載の画面は、実際の画面と一部異なる場合がございます。

9.1. 著作権について

近年、多彩な情報コンテンツを取り入れることで、魅力的な教材を作成することが可能となりました。しかし作成にあたっては、著作権について十分に留意する必要があります。教材作成において、情報コンテンツの複製や配布などを行う際には、著作権法上の問題が発生するか否かを事前にご確認ください。ここでは、主に情報コンテンツの著作権について、簡単にご説明します（カッコ内は著作権法における該当条項）。

自分の著作物には自分の著作権が発生します。それを用いて教材等を作成し、配布及びサーバー等にアップロードすることは、著作権者の正当な権利の行使とみなされます。

問題となるのは、他人の著作物を利用する場合です。他人の著作物を利用するには、原則として著作権者もしくは著作権管理団体の許諾を得る必要があります（第63条第2項）。しかし例外的に、教材作成のための複製や授業時間中の提示については、一定の条件を満たす場合に限り、著作権者等の許諾なしに著作物を利用することができます（第35条）。一定の条件とは、次のようなものです。著作権者等の許諾なしに授業のための複製や提示を行うには、これらすべての条件を満たす必要があります。

1. 複製できる人は、「教育を担任する者」と「授業を受ける者」に限ること。
2. 「授業の過程」における利用であること。
3. 「必要と認められる限度」内であること。
4. 既に「公表された著作物」であること。

なお、この例外規定は著作権者の権利を制限する性格のものでもあるため、「ただし、当該著作物の種類及び用途並びにその複製の部数及び様態に照らして著作権者の利益を不当に害することとなる場合は、この限りではない」（第35条）という但し書きを設けて、著作権の保護と著作物の利用との間のバランスをとっています。授業等における複製を、無制限に許容するものではありません。

以下に、情報コンテンツを用いた授業において想定される、「著作権侵害になる例」と「著作権侵害にならない例」をいくつか例示します。

【著作権侵害になる例】

- 購入した DVD をコピーして、他の教師に貸した。
  →著作権者の頒布権の侵害（第 26 条）。
- 教材として販売されている CD を CD-R にコピーして、クラスの学生・生徒に配布した。
  →授業中の利用でも「当該著作物の種類及び用途並びにその複製の部数及び様態に照らして著作権者の利益を不当に害することとなる場合」に該当する可能性がある（第 35 条但し書き）。
- 他人の著作物をサーバーに保存し、授業時間外にも自由に閲覧させてレポートを書かせた。
  →授業時間外にサーバーに残し、受講生以外も閲覧できる状態だと「授業の過程」とは見なされない（第 35 条）。また学外に向けて公開しているサーバーに蓄積すると、著作権者の公衆送信権等の侵害（第 23 条）。

【著作権侵害にならない例】

- 市販のビデオを購入して、授業中にプロジェクタを使って上映した。
  →営利を目的としない上映等に該当（第 38 条第 1 項）。
- 放送されているラジオの番組を録音して、授業中に流した。
  →同上（第 38 条第 3 項）
- 海外ビデオの PAL 方式を、教室備付ビデオデッキで再生できる NTSC 方式にダビングした。
  →授業で上映するための「必要と認められる限度」内での複製と見なされる（第 35 条）。
- 他人の著作物をサーバーに保存し、受講生のみに提示し、授業後にサーバーから削除した。
  →「授業の過程」における利用とみなされる（第 35 条）。

ここに挙げた「著作権侵害にならない例」であっても、著作物の利用状況や条件の微妙な差異によって、著作権侵害とみなされ得る場合があります。情報コンテンツの著作権の取り扱いに関して、ICTサポートでは相談に応じることはできますが、一切責任は負いかねます。明確に許諾の必要がないと判断できない場合には、著作権者、著作隣接権者、著作権管理団体等に直接問い合わせるか、著作権情報センター等の公的機関に問い合わせることをお勧めします。また、著作権に関する法令は随時改正されますので、ご自身でも確認されるようお願いします。

法に抵触する可能性のある録画や複製のために、マルチメディアLABの機材を利用することはできません。また、コピーガード仕様で録画されたVHSやDVD等の複製は法律上、禁じられています（第30条第1項第2号）。マルチメディアLABでも、そのような作業の支援はお断りしております。

参考文献：

- 著作権法令研究会編著『実務者のための著作権ハンドブック』（第9版）
  公益社団法人著作権情報センター発行， 2014年
- コンピュータソフトウェア著作権協会編著『図解わかる著作権―クリエイティブ×ビジネスの基礎知識―』
  ワークスコーポレーション， 2010年

9.1.1. オンライン・オンデマンド授業における著作物の配布について

「授業目的公衆送信補償金制度」の施行にともない、教育機関の設置者が補償金を支払うことで、著作者の許諾を得ることなく、インターネットを介して（＝クラウドストレージやメールなどのサービスを利用して）教員が生徒に他者の著作物を公衆送信することが可能となりました。

ただし、必要と認められる限度を超えて複製物を配布した場合や、授業の開講期間を超えて長期間にわたる資料の共有をおこなった場合など、この制度の適用外と判断されうる事例はさまざまに想定されます。運用にあたっては下記参考サイト（とくに、「改正著作権法第35条運用指針（令和3（2021）年度版）」に記載の想定される事例集）を確認のうえ、細心の注意を払ってください。

また、市販のブルーレイディスクやDVDを動画データなどに変換して送信する場合、動画データの作成過程で著作権法を侵害（第30条第1項第2号）している可能性が濃厚です。おやめください。

- ◆ 授業目的公衆送信補償金制度の早期施行について
  https://www.bunka.go.jp/seisaku/chosakuken/92169601.html
- ◆ 授業目的公衆送信補償金制度とは
  https://sartras.or.jp/seido/
- ◆ 改正著作権法第35条運用指針（令和3（2021）年度版）
  https://sartras.or.jp/wp-content/uploads/unyoshishin_20201221.pdf

9.2. セキュリティー対策について

近年、情報通信技術の発達に伴いコンピューターやネットワークの利用が一般化したことにより、それにまつわる厄介な問題も出現してきました。利用者が意図しないうちに、大切な情報が破壊されたり、秘匿情報が盗用されたりといった問題が、コンピューター利用の規模の大小にかかわらず発生しています。本節では、そうした問題に遭わないための初歩的な対策を記します。

本節を読み進める前に、すぐにでも始められるセキュリティー対策として、コンピューター利用の様々な場面で必要となる「パスワード」の管理について、今一度ご確認ください。パスワードが他人に知られてしまうと、悪意ある人間にとっての便利な「魔法の鍵」になってしまいます。なお、GCS26マシンのパスワード変更方法については、「1.4.1. パスワードの変更の仕方」をご覧ください。

9.2.1. 悪意のあるソフトウェア(コンピューターウイルス)の脅威

9.2.1.(a) 悪意のあるソフトウェアの種類と被害

コンピューターの内部に存在する有害なソフトのことを「マルウェア(malware)」と言います。マルウェアは、悪意ある人間が悪意ある目的(もしくは興味本位)で作成したプログラムで、コンピューターに保存されているデータを破壊したり、コンピューターに保存されているデータを詐取したりします。マルウェアは、単体のファイルとしてコンピューター内部に存在することもあれば、正常なファイルに寄生して存在するものもあります。こうした正常なファイルに寄生し増殖し、さらに他のファイルにも寄生を拡大するようプログラムされたものを、特に「コンピューターウイルス」と呼びます(ただし、最近では悪意のあるソフトウェア全般を総称的に「コンピューターウイルス」と呼ぶこともあります)。

有害性の有無にかかわらず、広告などを画面上に表示するソフトのことを「アドウェア(adware)」と言います。アドウェア自体にはデータの破壊や詐取を行う能力はありませんが、インターネット・ブラウザーのホームページ(起動時に表示するページ)を勝手に書き換えたり、画面上に不意に広告を表示したりして、コンピューターの通常の利用を妨害する場合があります。

コンピューターの動作(操作)情報を盗み出すことを目的にしたソフトのことを「スパイウェア(spyware)」と言います。盗み出す情報は、Webページの閲覧履歴からキーボードの入力履歴まで様々です。特に、キーボードの入力履歴を盗み出すタイプのスパイウェア(キーロガー)は、様々なIDやパスワードの盗用、クレジットカード番号の盗用など、コンピューター利用とは直接関係しない場面にまで被害が及ぶことがあります。

9.2.1.(b) 悪意のあるソフトウェアの侵入経路と対策

近年、インターネット利用がより身近なものとなったことで、悪意のあるソフトウェアの被害が拡大しやすくなっています。しかし、実際に悪意のあるソフトウェアの侵入を許してしまうかどうかは、コンピューター利用者の備えと判断に依存する部分もあります。悪意のあるソフトウェアの被害に遭わないための一般的な注意点を、以下に記しますのでご確認ください。

◆ ウイルス対策ソフトをインストールし最新の状態に保つ

コンピューターにはウイルス対策ソフトを導入し、定義データベースの自動更新を有効にするとともに、その保護が常時有効な状態でご利用ください。学内のすべてのGCS26マシンには、ウイルス対策

ソフトが導入されています。導入時の設定のままでネットワーク接続をしている状態であれば、定義データベースの自動更新と保護が、常時有効となっています。

◆ 不審な Web サイトにはアクセスしない

悪意のあるWebサイトにアクセスすると、自動的に悪意のあるソフトウェアのダウンロードが開始されるようプログラムされているページがあります。インターネットを利用する際には、不審なWebサイト（アダルトサイト、あり得ない低価格を謳う通販サイト、有名企業や公的機関を詐称した偽のサイトなど）にはアクセスしないようご注意ください。偽サイトの手口は年々巧妙化しており、サイトの見た目や機能だけでは真偽の判断がむずかしい場合もあります。そのようなときは、サイトのURLを確認し、不審な文字列になっていないかどうかを確認してください。

◆ 安易に無償ソフトをダウンロードおよびインストールしない

無償提供されるソフトウェア（フリーソフト）の一部には、悪意のある仕掛けが仕組まれているものもあります。無償だからと安易にダウンロードするのではなく、開発者や提供者の信頼性を確認することをお勧めします（悪評の高いソフトフェアであれば、ソフト名をインターネットで検索すれば危険性について知ることができます）。また、信頼できるソフトウェアのインストールに際しても、安易に不必要なオプションをインストールしないようご注意ください。

◆ 不審な差出人からのメールおよびその添付ファイルを開かない

電子メールも、悪意のあるソフトウェアの侵入経路のひとつです。悪意のあるソフトウェアを含んだメールには、興味を引くような文面が織り込まれており、それに誘導されて添付ファイルを開いてしまう（実行してしまう）ことで悪意のあるソフトウェアが侵入します。心当たりのない差出人からのメールを開かない、安易に添付ファイルを開かないといったことにご留意ください。また、メールの差出人情報（氏名やメールアドレスなど）は容易に詐称することが可能です。差出人のみならず、件名や文面等も含めて総合的に判断し、少しでも不審な点があれば、電話等で事実関係の確認を行ってください。

また、メールを経由して侵入する悪意のあるソフトウェアの中には、侵入したコンピューターのメールソフトを悪用して、無差別に悪意のあるソフトウェアを添付したメールを送信してしまうものもあります（差出人を意図的に詐称するため、実際には何の関係もないはずの人が悪意のあるソフトウェアを含んだメールの差出人として表示されてしまいます）。この場合、悪意のあるソフトウェアの被害者が悪意のあるソフトウェアの被害を拡大させてしまうことになります。

◆ USBメモリもこまめにウイルスチェックを行う

USBメモリを介して悪意のあるソフトウェアが侵入することもあります。不特定多数が使用できるコンピューター（学会会場やホテル等）でUSBメモリを使用する際は、十分ご注意ください。また、ウイルス対策ソフトでUSBメモリや外付けハードディスクを対象とした検査（スキャン）を定期的に行うことをお勧めします。

9.2.1.(c) 悪意のあるソフトウェアが侵入してしまった場合の対処

悪意のあるソフトウェアの侵入を防ぐために適切な対策をしていたとしても、すべての悪意のあるソフトウェアの侵入を完全に防止することは不可能です。運悪くコンピューターに悪意のあるソフトウェアが侵入してしまった(いわゆるコンピューターウイルスに感染してしまった)場合には、そのコンピューターに保存されていたデータをすべて消去してOSの再インストール(リカバリー、初期化)を行うといったことまでを視野に入れた、大がかりな復旧処置が必要になります。コンピューター内に悪意のあるソフトウェアが侵入してしまった場合(それが疑われる場合を含む)、ICTサポートまでお電話ください。ICTサポートの閉室時間であった場合は以下をご対応いただき、ICTサポートまでメールにてご連絡ください。

(1) コンピューターをネットワークから切断する。
コンピューターに接続されているLANケーブルを抜いたり、Wi-Fiを切断します。データの流出や別のコンピューターへの侵入(感染)などの二次被害を防止するためです。

(2) ウイルス対策ソフトで検査する。
ウイルス対策ソフトを起動して、コンピューター全体を検査(スキャン)します。悪意のあるソフトウェアが侵入した際にコンピューターに接続していた外付けの記憶媒体(USBメモリ、外付けハードディスク、SDカード等)も検査対象に含めます。

9.2.2. 悪意のあるソフトウェアに限らない脅威

コンピューターは、インターネット等を利用して外部と通信を行っている限り、悪意のあるソフトウェア以外にも様々な脅威に晒されることになります。しかし、コンピューター利用者が適切な知識を持ち、適切な対処をすれば、比較的安全にコンピューターやインターネットを利用することができます。

9.2.2.(a) インターネットやメールを通じた詐欺

金融機関やショッピングサイトからのメールやWebサイトを装い、キャッシュカードの暗証番号やクレジットカード番号などの個人情報を詐取する「**フィッシング詐欺**」と呼ばれる被害が発生しています。偽のメールや偽のWebサイトに誘導されて表示される入力フォームに、コンピューター利用者自身が個人情報や各種カード番号などを書き込んでしまうことにより、個人情報が盗み取られたり、キャッシュカードやクレジットカードのコピーが不正に作られてしまったりといった被害が発生します。また、インターネット利用者に特定のリンクをクリックさせ、差し迫った期限や脅迫的な文言を用いることで、現金を振り込ませるよう誘導する「**ワンクリック詐欺**」と呼ばれる被害も発生しています。

これらの詐欺は、偽メールや偽Webサイトを用いる点では悪意のあるソフトウェアの侵入と類似していますが、コンピューターやそのデータに対しては具体的な被害を与えることなく、コンピューター利用者に金銭的な被害をもたらす点が特徴といえます。プログラム上の処理によってではなく、あくまでもコンピューター利用者本人が偽の入力フォームに個人情報を入力したり、表示されている口座宛に実際に現金を送金してしまったりすることで被害が発生します。

「**フィッシング詐欺**」も「**ワンクリック詐欺**」も、基本的には無視していれば実害はありません。気になる場合には、警察もしくは消費生活センターが問い合わせの窓口となります。Webサイトの管理者やメールの差出人に直接連絡を取ることは危険です。自分の個人情報が相手に伝わってしまう場合や、新たな詐欺や脅迫の被害に遭う可能性があります。

近年販売されているウイルス対策ソフトの中には、「フィッシング詐欺」や「ワンクリック詐欺」に誘導するWebサイトにアクセスしようとすると、自動的にそのWebサイトを表示しないように動作するものもあります。必要に応じて、そうした機能を利用することもお勧めします。

9.2.2.(b) ソフトウェアの脆弱性を狙った攻撃

コンピューターのソフトウェアは、未知のプログラムの不具合(「バグ(bug)」と呼ぶ)などにより、情報セキュリティー上の弱点を抱えたまま製品として出荷されてしまうことがあります。こうした情報セキュリティー上の弱点を「脆弱性(vulnerability)」と呼びます。脆弱性が残された状態でコンピューターを利用していると、悪意のあるソフトウェアの侵入経路となり得るだけでなく、不正アクセス(本来は利用権限のない者が、コンピューターを不正に操作したり、ネットワークを不正に利用したりする犯罪行為)を許す隙を与えてしまう場合があります。

ソフトウェアに脆弱性が発見されると、サポート期間内であれば、多くの場合、開発したメーカーから更新プログラムが提供されます。脆弱性に対応した更新プログラムの導入は、早めに行うことが大切です(詳しくは「9.3. ソフトウェアの更新について」をご覧ください)。サポートが終了したソフトウェアは、脆弱性が発見されても修正・更新されませんので、ご利用を中止することをお勧めします。

なお、近年は「ゼロデイ攻撃」と呼ばれる、ソフトウェアに対する脆弱性が発見されたと同時に、メーカーが更新プログラムを配布するまでの間に、その脆弱性を利用して行われる攻撃が発生しています。コンピューター利用者は、指摘された脆弱性の内容を確認し、危険となる行為を行わないなど、更新プログラムを適用するまでの間は十分に注意する必要があります。

9.2.2.(c) 複合化・巧妙化するコンピューター関連の犯罪

昨今、ここまでに挙げた悪意のあるソフトウェアの脅威やそれ以外の脅威は、コンピューター利用者にとって複合的な脅威となる場合があります。例えば、脆弱性を狙った攻撃により不正アクセスを許してしまったことで自分のコンピューターが悪意のあるソフトウェアを拡散する中継点にされてしまうことや、アドウェアの侵入によりそれに誘導されることで「フィッシング詐欺」の被害に遭ってしまうことなどが起こり得ます。

とはいえ、悪意のあるソフトウェアやその他の脅威への適切な対策を行っていれば、必ずしも悪意ある者の意のままに悪意のあるソフトウェアを動かしたり不正アクセスをしたりすることはなく、どこかの段階で被害を食い止められる確率は高まります。そのためにも、各々の脅威への備えを確実に行うことが重要です。

9.2.3. GCS26マシンでのセキュリティー対策

すべてのGCS26マシンには、ウイルス対策ソフトが導入されており、悪意のあるソフトウェアが持ち込まれそうになった場合には、リアルタイムで検出・駆除することができます。

GCS26環境では、インターネット上からの悪意のあるソフトウェアの侵入や不正な通信を防ぐ設備を導入しており、Webサイト閲覧時の安全性を確保しています。また、総合的なメールセキュリティーシステムを導入しています（詳しくは「5.1. メールのセキュリティー対策」をご覧ください）。これにより、悪意のあるソフトウェアが添付されたメールを受信した場合、その悪意のあるソフトウェアを削除するとともに、当該メールの受信者には、悪意のあるソフトウェアが添付されていた旨のメッセージを送付します。なお、当該メールの送信者には何も通知されません。

このように、学習院では個々のコンピューター、インターネット、メールのそれぞれについて、セキュリティー対策がなされておりますが、もしも未知（新種）の悪意のあるソフトウェアが侵入しようとした場合には、その侵入を完全に防止することはできません。未知のものと疑われるものは、その性質等を分析したうえで駆除すべきもののリスト（「定義データベース」と言う）に加えられるためです。そのため、「出所が不明なファイルを開かない」、「不審なWebサイトにアクセスしない」、「たとえ知人からのメールであっても不用意に添付ファイルを開かない」といった自己防衛も大切です。

9.2.4. GCS26マシン以外でのセキュリティー対策

学習院のネットワークに接続するすべてのコンピューターには、ウイルス対策ソフトがインストールされている必要があります。また、そのウイルス対策ソフトをアクティベーション（有効化）したうえで、ウイルス定義データベースを常に最新状態にしておく必要があります。

Windows 10以降のWindows機には、購入（インストール）時点からOS標準のウイルス対策機能「Microsoft Defender」が備わっています。Microsoft Defenderを最新の状態に保っていれば、基本的なウイルス対策はできています。

さらに強固なセキュリティーが必要となる場合は、有償のウイルス対策ソフトの導入を検討してください。購入当初からウイルス対策ソフトがインストールされていることを謳っているコンピューターもありますが、多くの場合、購入時にインストールされているウイルス対策ソフトは「プリインストール版」と呼ばれるもので、ライセンス期限が短く設定されています（2～3か月程度のものが多い）。期限が切れる前に、更新版を購入するか、別のウイルス対策ソフトを導入する必要があります。OS標準のウイルス対策で十分だと判断した場合でも、プリインストールされた対策ソフトをアンインストールし、Microsoft Defenderを有効化する手順が必要です。ライセンス期間が切れたままPCを使い続けないでください。

ウイルス対策ソフトには、無償提供されるものから有償提供されるものまで様々なものがあります。現在、多くの有償ウイルス対策ソフトは、特定の種類の悪意のあるソフトウェアに備えるものというよりは、コンピューターの健全性を保つための総合的なセキュリティーソフトウェアが主流となっています。悪意のあるソフトウェアの検出能力、インターネットやメールの利用者保護、ファイアウォール（不正アクセス対策）、ライセンス形態、価格などがそれぞれ異なります。ご自身のコンピューター利用状況にあったものをお選びください。有償のものでも、期間を限定した試用版が提供されている場合がありますので、それを実際にご自身のコンピューターにインストールして使用感を試すことができます。ウイルス対策ソフトの機能や性能を比較したい場合は、より中立的で複数の検証に基づいて評価されているものを参照することをお勧めします（その一例を「9.4. 最新のセキュリティー情報の入手方法」に示しています）。

なお、ウイルス対策ソフト（特に無償提供されるもの）の中には、ソフトウェアの使用許諾上、その利用をホー

ムユース(家庭での利用)に限定しているものがあります。そのようなウイルス対策ソフトは、学部・学科で購入されたコンピューター、各種研究費で購入されたコンピューターなどには、導入することができませんのでご注意ください。

> 偽ウイルス対策ソフトにご用心:
> 無償のウイルス対策ソフトを装って、悪意のあるソフトウェアやその他の脅威をコンピューターに引き起こすような悪質なソフトウェアがインターネット上で公開されています。こうしたソフトは、悪意のあるソフトウェアが検出されたことを装い、その駆除のためと称して、別の悪意のあるソフトウェアをダウンロードさせたり、有料版の購入が必要だと偽ってクレジットカード番号を入力させたりします(フィッシング詐欺の一種)。

9.3. ソフトウェアの更新について

インターネットを積極的に利用するソフトウェア(ブラウザー、メールソフトなど)は、その脆弱性を突かれ、悪意のあるソフトウェアの侵入や不正アクセスなどの攻撃に晒される危険が高いといえます。そのため、メーカーは頻繁に更新プログラムを提供します。コンピューター利用者が最新の更新プログラムをインストールすることは、重要なセキュリティー対策のひとつといえます。もちろん、更新プログラムのインストールによって、セキュリティー面の改善だけではなく、動作不良やエラー終了などのソフトウェアの不具合が改善される場合もあります。

特に、ソフトウェアをパッケージで購入してインストールしたものや、スキャナー等の機器に付属しているソフトウェアは、その製造元のWebサイトに更新版が公開されている場合があります。多くのメーカーのWebサイトには、「サポート」、「ダウンロード」、「アップデート」といったリンクが用意されています。メーカーの対応状況は、そのソフトウェア・メーカーによって異なりますので、詳しくは各ソフトウェアの説明書またはヘルプファイル等でご確認ください。

なお、Windowsのシステムファイルや Microsoft Office 製品(Word, Excel, PowerPoint, Access, Publisher)の更新に関しては、「9.3.1. Windows Update」をご覧ください。

9.3.1. Windows Update

GCS26マシンでは、Microsoft WindowsおよびOfficeのアップデートが管理されているため、次のようになります。いずれも手動での更新作業は不要です

【品質更新プログラム】

毎月リリースされるセキュリティーや障害修正のアップデートは、Microsoft社からの配信後、数日遅れて自動的に適用されます。

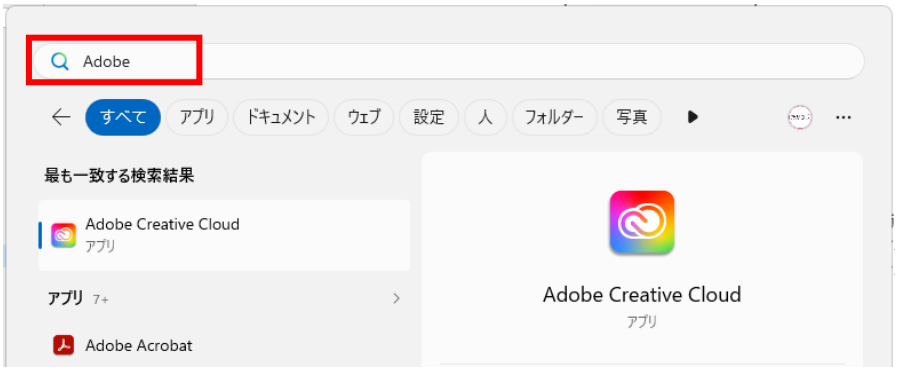
【機能更新プログラム】

年に1から2回リリースされる大型のアップデートは、GCS26マシンにおける不具合の有無を確認後に適用します。そのため数か月遅れで配信されます。なお、GCS26マシンへの適用において問題があると判断された場合は配信しないこともあり得ます。

9.3.2. Adobe 製品の更新

Adobe Acrobatやその他のAdobe製品を更新する場合は、以下の方法で行います。

スタートメニューを開き、「Adobe Creative Cloud」（以下、Adobe CC）を起動します。アプリケーションがみつからない場合は、検索欄に「Adobe」と入力すると、候補アプリの一覧が表示されます。

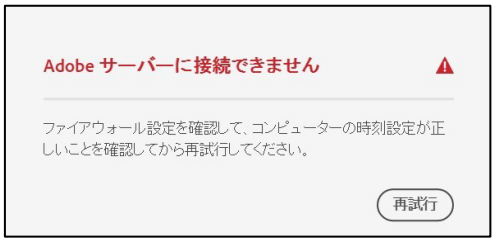


起動後、ログイン画面が表示されるので、メールアドレス（教職員番号@gakushuin.ac.jp）を入力してください。入力後、学習院のログイン画面に遷移しますので、教職員アカウントでログインします。

「Adobe CC」上から、[**アップデート**]メニューを開くと、更新可能なアプリケーションの一覧が表示されます。右上の[**すべてをアップデート**]から、一括で更新することもできます。

【Adobe Creative Cloud にログインできない場合】

「Adobe CC」を起動しても「*Adobe サーバーに接続できません*」とエラーが表示される場合があります。



このような場合、「メニュ」-->「ヘルプ」-->「ブラウザからログイン」を試したり、一旦「Adobe CC」を終了し、任意のAdobe製アプリケーション（Acrobat ProやPhotoshopなど）を起動し、起動したアプリケーション上でログインをしてください。アプリケーションでのログインに成功したら、再度「Adobe CC」を起動します。自動的に「Adobe CC」にもログインされた状態になっているので、アップデートをすすめてください。

9.4. 最新のセキュリティー情報の入手方法

セキュリティー関連の情報は、最近では新聞や TV 等でも取り上げられており、書籍でも情報を入手できますが、Web で調べれば最新の詳細情報をいち早く入手できます。以下、関連する Web サイトをご紹介（例示）します（2026 年 4 月 1 日現在）。

【セキュリティー関連情報公開 Web サイト（公的機関、Windows 販売元による情報）】

- サイバー警察局（警察庁）
  https://www.npa.go.jp/bureau/cyber/index.html
- 独立行政法人 情報処理推進機構（IPA）：情報セキュリティー
  https://www.ipa.go.jp/security/
- マイクロソフト社：Microsoft Security
  https://www.microsoft.com/ja-jp/security/

【セキュリティー関連情報公開 Web サイト（コンピューターセキュリティー企業による情報）】

- Symantec 社：セキュリティセンター
  https://www.symantec.com/ja/jp/security-center/
- Trellix 社:脅威センター（旧マカフィー株式会社：セキュリティー解析センター）
  https://www.trellix.com/ja-jp/threat-center.html
- トレンドマイクロ社：セキュリティーニュース
  https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

【ウイルス対策ソフトに関する Web サイト】

- Cybereason
  https://www.cybereason.co.jp/
- ESET（Windows・Mac・Android 向け）
  https://eset-info.canon-its.jp/
- ノートン セキュリティー（Windows・Mac・Android 向け）
  https://jp.norton.com/
- ClamAV/ ClamXav
  https://www.clamav.net/（Windows 向け） https://www.clamxav.com/（Mac 向け）