センターより

情報セキュリティ教育の充実のため、情報セキュリティ・情報倫理に関するパンフレットを作成しました。

情報セキュリティ・倫理マニュアル

Saitama University 埼玉大学

安心して情報システムを利用するための10か条

1. OSやソフトウェアは常に最新版にしましょう

PCやスマートフォンの基本ソフトウェア（OS）やアプリケーションソフトウェアを更新して，セキュリティ対策を最新にしましょう。

2. ウイルス対策を徹底しましょう

IDやパスワードを盗んだり，遠隔操作を行ったり，ファイルを勝手に暗号化するウイルスが増えています。
PCやスマートフォンにはウイルス対策ソフトを導入しましょう。

3. ID・パスワードは適切に管理しましょう

IDとパスワードは本人であることを証明する大切な情報です。パスワードは，第三者に「教えない」「知られない」ようにしましょう。容易に推測される誕生日，名前などを使ったり，同じパスワードを使い回したりするのはやめましょう。多要素認証が利用できる場合は有効にしましょう。

4. 不審なメールは無視（削除）しましょう

不審なメールのリンクのクリックや，添付ファイルを開くとウイルスに感染する可能性があります。メールの差出人を確認し，知らない人から届いたメールは無視（削除）しましょう。差出人の「なりすまし」を防ぐため，メールソフトやスマートフォンなどのフィルタ機能を上手に使いましょう。

5. 情報管理に注意しましょう

ウイルス感染やネットワークの侵入，PCやUSBメモリの盗難・紛失により個人情報が漏洩する事件が多発しています。個人情報や機密情報を含む重要なファイルはパスワードでロックして，管理を徹底しましょう。なくなると困る重要なファイルはバックアップを作成して適切に保管しましょう。

6. Webページの通信が暗号化されているか確認しましょう

Webページでパスワードやクレジットカード番号などを入力するときは，盗聴や改ざんを防ぐため通信暗号化を確認しましょう。Webページのアドレス先頭が「https://」となっているか，Webブラウザのアドレス欄に鍵「🔒」マークが表示されていれば通信が暗号化されています。

7. 著作権などの知的財産を侵害してはいけません

著作物やデザインを無断で複製したり，WebページやSNSに掲載したりしてはいけません。
正当なライセンスのないソフトウェアを使用したり，違法ダウンロードしたりしてはいけません。

8. 掲示板やSNSは注意して利用しましょう

現実社会と同様にインターネット上でもルールやマナーを守り，掲示板やSNSで個人等を誹謗中傷してはいけません。書き込みはうのみにせず，デマやフェイクニュースでないか確認しましょう。

9. 個人情報やプライバシー情報を守りましょう

埼玉大学
マスコットキャラクター
メリンちゃん

インターネット上に，安易に個人情報やプライバシー情報を公開することは危険です。
自分や家族，友人の個人情報をSNSに掲載するときは，情報の公開範囲に注意しましょう。
写真を公開するときは、一緒に写った人に事前に許可を取りましょう。

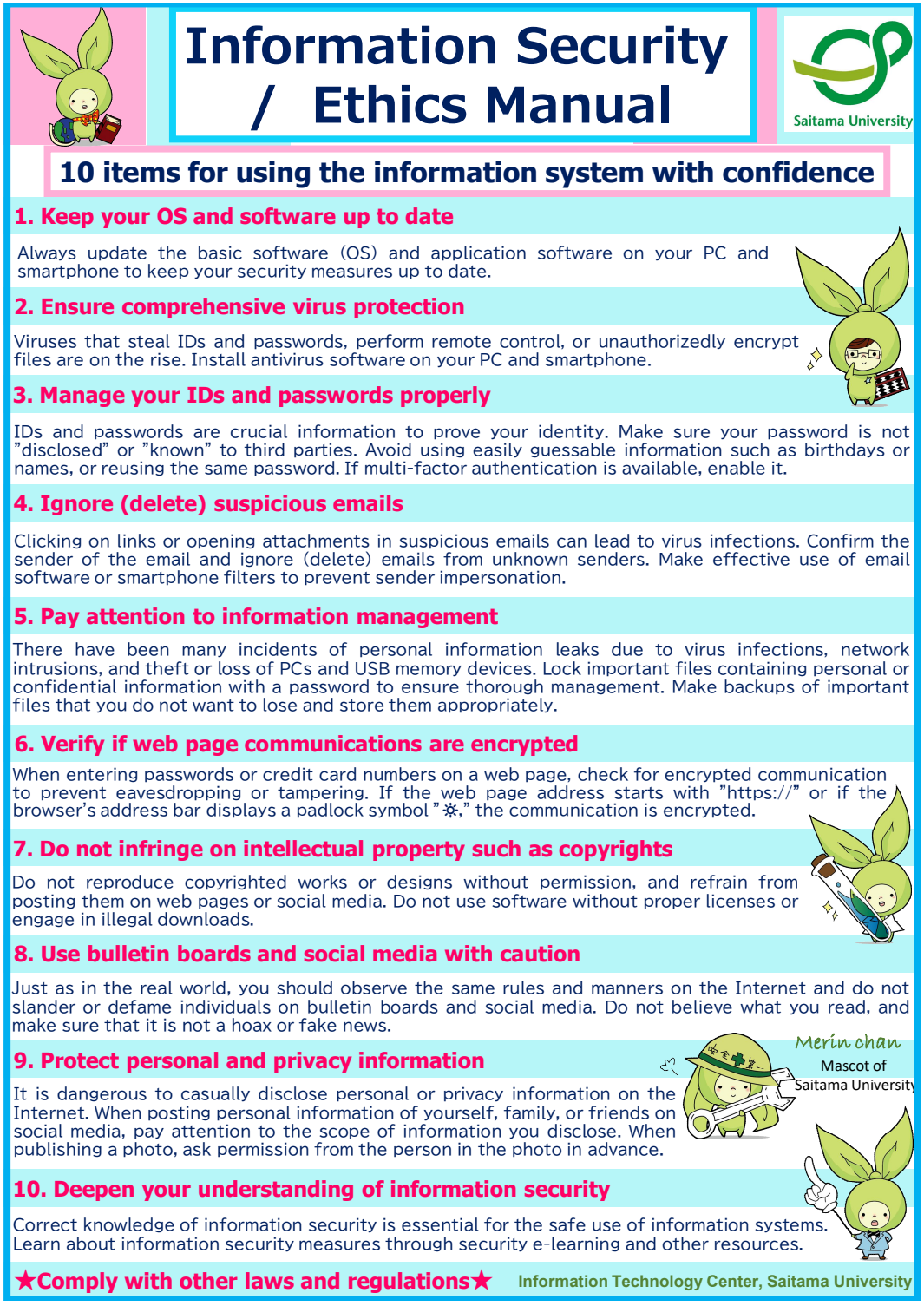
10. 情報セキュリティに関する理解を深めましょう

情報システムの安全な利用には情報セキュリティに関する正しい知識が大切です。
情報セキュリティeラーニングの受講などによって、情報セキュリティ対策を学びましょう。

★その他法令を遵守しましょう★

埼玉大学情報メディア基盤センター

情報機器やネットワークを利用する上で情報セキュリティと情報倫理について注意すべき10項目を挙げ、多様な留学生が在学することに配慮し、日本語のほかに英語のバージョンを作成、ポスターサイズに印刷したものを学内各所に掲示しています。



Information Security / Ethics Manual

Saitama University

10 items for using the information system with confidence

1. Keep your OS and software up to date

Always update the basic software (OS) and application software on your PC and smartphone to keep your security measures up to date.

2. Ensure comprehensive virus protection

Viruses that steal IDs and passwords, perform remote control, or unauthorizedly encrypt files are on the rise. Install antivirus software on your PC and smartphone.

3. Manage your IDs and passwords properly

IDs and passwords are crucial information to prove your identity. Make sure your password is not "disclosed" or "known" to third parties. Avoid using easily guessable information such as birthdays or names, or reusing the same password. If multi-factor authentication is available, enable it.

4. Ignore (delete) suspicious emails

Clicking on links or opening attachments in suspicious emails can lead to virus infections. Confirm the sender of the email and ignore (delete) emails from unknown senders. Make effective use of email software or smartphone filters to prevent sender impersonation.

5. Pay attention to information management

There have been many incidents of personal information leaks due to virus infections, network intrusions, and theft or loss of PCs and USB memory devices. Lock important files containing personal or confidential information with a password to ensure thorough management. Make backups of important files that you do not want to lose and store them appropriately.

6. Verify if web page communications are encrypted

When entering passwords or credit card numbers on a web page, check for encrypted communication to prevent eavesdropping or tampering. If the web page address starts with "https://" or if the browser's address bar displays a padlock symbol "☼," the communication is encrypted.

7. Do not infringe on intellectual property such as copyrights

Do not reproduce copyrighted works or designs without permission, and refrain from posting them on web pages or social media. Do not use software without proper licenses or engage in illegal downloads.

8. Use bulletin boards and social media with caution

Just as in the real world, you should observe the same rules and manners on the Internet and do not slander or defame individuals on bulletin boards and social media. Do not believe what you read, and make sure that it is not a hoax or fake news.

9. Protect personal and privacy information

It is dangerous to casually disclose personal or privacy information on the Internet. When posting personal information of yourself, family, or friends on social media, pay attention to the scope of information you disclose. When publishing a photo, ask permission from the person in the photo in advance.

Merin chan
Mascot of
Saitama University

10. Deepen your understanding of information security

Correct knowledge of information security is essential for the safe use of information systems. Learn about information security measures through security e-learning and other resources.

★Comply with other laws and regulations★

Information Technology Center, Saitama University

情報メディア基盤センター教職員名簿

(令和7年3月時点)

【情報メディア基盤センター】

センター長

吉　浦　　紀　晃	教授（併任） (理工学研究科数理電子情報部門)	

専任教員

松　永　　康　佑	准　教　授	～令和6年3月
土　方　　泰　斗	准　教　授	
松　田　　哲　直	准　教　授	令和6年4月～

【総務部情報基盤課】

課　　長

南　雲　　浩　二	

課長代理

菅　間　　保　則	～令和6年3月

技術職員

齋　藤　　広　宣	主任技師	
天　野　　直　子	技　　師（併任）	
青　木　　拓　也	技　　師	～令和7年1月
東　　宏　樹	専門技術員（併任）	
渋　谷　　大　智	専門技術員（併任）	令和6年12月～
倉　永　　直　樹	派遣職員	

事務職員

原　口　　史　之	主　　査	
佐　藤　　泰　弘	主　　査	
杉　田　　吉　弘	主　　任	令和6年4月～
髙　橋　　正　子	事務補佐員	～令和6年3月
村　松　　美由起	事務補佐員	
中　村　　由紀子	事務補佐員	
小　峰　　麻貴子	事務補佐員	
中　村　　美　樹	事務補佐員	令和6年4月～

埼玉大学情報メディア基盤センター規程は、下記を参照してください。(学内限定)
http://www.saitama-u.ac.jp/houki/houki-n/reg-n/2-2-20.pdf

編　集　後　記

埼玉大学 情報メディア基盤センター年報『さいたま』Vol.31 をお届けいたします。昨年度は年報発行に至らず、そのため今号は令和 5 年度・6 年度合併号として 2 年分の報告を掲載しています。本年報作成にご協力くださいました皆さまには、この場をお借りして深く御礼申し上げます。

昨今、ますます情報セキュリティの向上が叫ばれています。当センターでも徐々にではありますが、セキュリティの向上に向けて対応を行っています。例えば令和 5 年度には、Microsoft365 を A3 からより高度なセキュリティ機能を有する A5 プランに変更したほか、セキュリティポリシーの改正を実施、令和 6 年度には「情報セキュリティと情報倫理に関する e ラーニング」の受講義務化を行っています。

また令和 6 年度は、当センターにおいては認証基盤システムの更新が、学内の他部局においても教務システムの更新があり、これを機に各システムのユーザ認証に多要素認証の導入が進みました。

本学で多要素認証を導入したのは令和 3 年 3 月、学生の Microsoft365 のユーザ認証が最初でした。続けて同年 5 月には教職員の Microsoft365 に導入し、その後も SSL-VPN 接続へ導入したほか、ユーザ認証を必要とするサーバに多要素認証を必須化するなど、その対象を拡充しています。

さて、導入した当時こそ「これはなに？」という問い合わせの多かった多要素認証ですが、導入から早 4 年、多要素認証そのものに関する質問はほぼなくなりました。その一方でスマートフォンの機種変更等により認証の手段を失った、との相談が増えており、これは多要素認証リセット申請数に直結しています。学外で Microsoft365 を利用すると、否応なく多要素認証を求められます。画面の指示に従って一度は設定して利用するものの、設定内容のメンテナンスは疎かになっているようで、登録デバイスの変更まで思い至らずに機種変更をしてしまうケースが多いようです。

そしてちらほら聞こえてくるのは「いちいち認証を行うのが面倒」という声です。正直、その気持ちは分からなくもありません。ですがパスワードの流出が増えている今日、自らの情報を守る盾がパスワードだけではなんとも心細い！セキュリティと利便性の相性の悪さは今に始まったことではありませんが、ちょっとした面倒と引き換えに、安心を確保しているのだと思っていただきたいものです。

とはいえ、煩雑すぎる手続きは敬遠されるもの。より安全でより簡便なセキュリティを提供すること、リスクを正しく認識してセキュリティの必要性を知ることができれば、機種変更に起因する多要素認証リセットも減るのではないかと思う今日この頃です。

埼玉大学情報メディア基盤センター年報
『 さいたま 』
Vol.31　2025.7（令和 7 年）

発行者　埼玉大学情報メディア基盤センター
〒338-8570　　さいたま市桜区下大久保 255
電話　　048-858-3674