同志社大学の全構成員の皆さまへ
To all members of
Doshisha University

2024年度版
2024 Edition

自分は大丈夫だと思っていませんか？

Do you think you are safe?

ネットワークトラブルから自分を守る、一人ひとりの意識と行動が大事です。
Protect yourself from network troubles. The key is individual awareness and behavior.

Check List

情報セキュリティ対策、正しくできていますか？

- ☐ パスワードを簡単な文字列にしていませんか？
- ☐ パソコンのウイルスチェックを定期的に行っていますか？
- ☐ USB メモリーやモバイルパソコンに、重要な情報を大量に保存していませんか？
- ☐ 甘い誘いや緊急を装うメールの内容をよく確認せず、メール中のリンクをクリックしたことがありませんか？
- ☐ SNS に投稿する時に、個人情報や位置情報を公開していませんか？

Are your information security measures correct ?

- ☐ Is your password a simple character string?
- ☐ Do you regularly run the virus check on your computer?
- ☐ Are you storing a large amount of important information on a USB flash drive or laptop?
- ☐ Have you ever clicked on a link in an e-mail that pretended to be a sweet invitation or emergency without carefully checking the content?
- ☐ When posting to social media , do you disclose your personal information and location information?

詳しくは次のページ
Check inside for more information!

情報セキュリティを維持するために…
To protect information security

1. パスワードの取り扱いについて

パスワードは、ユーザIDの利用者が本人かどうかを確認するためのもので、コンピュータやネットワークを利用する上で非常に重要です。パスワードは大切な個人情報として、しっかりと各自で管理しましょう。パスワードの管理を疎かにすると、自分自身のプライバシーが侵害されるだけでなく、自分のユーザIDとパスワードが不正利用され、大きな被害になることもあります。

同志社大学では、各種情報サービスの利用にはユーザ ID・パスワードに加えて多要素認証が必要です。多要素認証は複数の要素を用いて本人確認を行う仕組みで、セキュリティを高めることができます。

パスワード取り扱いの注意点

- 他人に推測されやすいパスワードは設定しない。（自分の生年月日や電話番号・名前 など）
- 同じパスワードを使い回さない。
- パスワードを入力しているところを他人に見られないようにする。
- パスワードをメモして持ち歩かないようにする。

Password management

The password authenticates the user of the UserID, and is very important in using computers and networks. You should manage your password properly as your personal information. If you do not manage your password properly, it may cause not only violation of your own privacy, but also unauthorized use of your UserID and password, which can cause serious damage.

At Doshisha University, Multi-Factor Authentication is required to use various information services in addition to a UserID and password. Multi-Factor Authentication is a system that uses multiple factors to verify the identity of the user to increase security.

Tips for password management

- Do not use a password that can be easily guessed by others. (e.g. Your birthday, phone number, name, etc.)
- Do not reuse the same password.
- Keep others from seeing your password.
- Do not write down your password and carry it with you.

2. 機密情報の取り扱いについて

個人情報や機密情報をUSBメモリーやモバイルパソコンに保存して、持ち歩かないようにしましょう。USBメモリーやモバイルパソコンは、携帯が容易なため、紛失や盗難の被害にあう可能性が高くなります。機密情報の漏洩に繋がりますので十分に注意してください。

データ保存の際は、同志社大学が提供しているクラウドストレージサービスも活用しましょう。学生の方は OneDrive、教職員の方は OneDrive および Webdisk を利用できます。また、学外のクラウドサービスを利用する際は、信頼できるサービスの提供元であることを十分に確認してください。

メール送信の宛先 To、Cc、Bcc の違いを知っていますか？

メールアドレスも個人情報です。Bcc にすべきところを To で送信してしまうと、他の受信者にメールアドレスが漏洩してしまいます。使い分けには注意しましょう。

- To　直接内容を伝えたい相手
- Cc　直接の宛先ではないが、内容を伝えておきたい相手
- Bcc　内容を伝えておきたいが、他の受信者に名前やメールアドレスを知られたくない相手

Handling of confidential information

Do not store and carry around your personal and confidential information on a USB flash drive or laptop. USB flash drives and laptops are easy to carry around, so they are more likey to be lost or stolen. Please be careful as it will lead to the leakage of confidential information.

For saving data, please use cloud storage service offered by Doshisha University. Students can use Microsoft OneDrive cloud storage service and faculty members can use OneDrive and Webdisk. When using any other cloud service, please make sure that it is provided by a reliable provider.

Do you know the difference between the e-mail destinations To, Cc, and Bcc?

E-mail address is personal information. If you send an e-mail using "To" when it should be "Bcc", the e-mail address will be leaked to other recipients. Use To, Cc, and Bcc correctly.

- To　The person you want to convey the message directly
- Cc　Not the direct destination, but the person you want to convey the message
- Bcc　The person you want to convey the message but hide the name and address from other recipients.

3. ICカード（学生証 / 社員証・身分証・利用者証）の取り扱いについて

ICカードは重要なカードですので、紛失したり、盗難に遭ったりしないよう、管理に十分注意してください。また、他人に貸与したり、譲渡したりしてはいけません。万一、ICカードを紛失した場合には、速やかに所定の窓口にて利用停止の手続きを行ってください。

IC card management (student ID card and ID card for faculty member)

Please keep your IC card secured to prevent being lost or stolen. Do not lend or transfer it to others. If you have lost your IC card, immediately follow the suspension procedure at the counter.

4. フィッシングメールについて

有名企業やシステム管理者等の名をかたったメールを送信して偽のウェブサイトへ誘導し、IDやパスワード等を詐取するフィッシング詐欺が行われています。Apple ID、Microsoftアカウント等、複数のサービスを利用できる認証情報が狙われる傾向にあり、非常に巧妙な手口でユーザの気を引く傾向も見られますので、十分に注意してください。

もし、フィッシングにひっかかってしまうと、次のような被害が発生します。

- あなたのメールアドレスで、世界中に新たなフィッシングメールが大量に送信されてしまう。
- あなたのメールが第三者に漏洩してしまう。
- 他のシステムへも不正アクセスされてしまう。

同志社大学に限らずその他機関についても、ユーザID・パスワード・暗証番号等をメールで問い合わせることは一般的ではありません。このような問い合わせがあっても回答しないでください。判断に迷う場合は、発行機関に問い合わせましょう。

万一、本学のユーザ ID・パスワードを本学提供システム以外に入力したり、メールに回答した場合は、直ちにパスワードを変更してください。

被害に遭ったときの対処法は、IPA 独立行政法人 情報処理推進機構の Web サイトに紹介されています。

Phishing e-mails

Phishing is a scam in which e-mails with the names of famous companies and system administrators are sent to lead to fake websites and spoof IDs and passwords. Credentials that you can use for multiple services such as Apple ID and Microsoft account tend to be targeted. Be careful as it uses very clever tricks to get your attention.

If you get caught in phishing the following damage may occur.

- A large amount of new phishing e-mails are sent around the world, using your e-mail address.
- Your e-mail leaks to third parties.
- Unauthorized access to your other systems.

It is not common for Doshisha University and other institutions to ask for UserIDs, passwords, etc. by e-mail. Do not respond to such e-mails. If you are not sure, contact the issuing agency.

If you enter your University UserID and password in a system other than the one provided by our University, or If you reply to a suspicious e-mail, please change your password immediately.

The Information-technology Promotion Agency (IPA) website provides information on what to do if you are a victim of this type of attack.

5. スマートフォンの安全な利用について

スマートフォンの普及に伴い、不正アプリによる電話帳データの漏えいやワンクリック詐欺等、スマートフォンの利用者を狙った被害が年々増えており、パソコンと同様のセキュリティ対策が必要になってきています。以下を始めとするセキュリティ対策を行い、安全・快適にスマートフォンを利活用してください。

スマートフォンのセキュリティ対策

- 画面のロックは必ず設定する。
- 信頼できるサイトからアプリをインストールする。
- アプリに許可する権限を確認する。
  ※同志社大学が提供するサービス以外のサービスやアプリで、同志社大学のユーザ ID・パスワードを入力してはいけません。
- セキュリティソフトの導入も検討しましょう。

Safe use of smartphone

With the spread of smartphones, the number of crimes targeting smartphone users, such as malware apps that cause leakage of phonebook data and one-click fraud, is increasing year by year, so the same security measures as PCs are needed. Take the following security measures and use your smartphone safely and comfortably.

Smartphone security measures

- Make sure to lock your screen.
- Install apps from trusted sites.
- Check the permissions you allow for the app.
  ※Do not enter Doshisha University UserID and password in services or apps other than those provided by Doshisha University.
- Consider using security software.

6. SNS 利用上の注意点について

SNSはとても身近で便利なコミュニケーション手段として利用者も多いサービスですが、トラブルも多く発生しています。以下の点に注意して利用してください。

- 情報発信の際は、自分だけでなく、家族や友人等を含めた他者のプライバシーや権利（著作権等の知的財産権、肖像権等）にも十分に配慮してください。
- ソーシャルメディア上の情報は一瞬にして世界中に広まることを意識してください。
- 個人情報・位置情報を公開することにより個人や位置が特定され、危険な目に遭う可能性があります。
- 各SNSの仕様や公開範囲の設定方法を十分に理解した上で、適切に利用してください。

Notes on using social media

Social media are very familiar and convenient communication method with many users, but they also have many troubles. When using, note the following.

- When sending information, give due consideration to the privacy and rights (portrait rights and intellectual property rights such as copyrights) of not only yourself but also others, including family and friends.
- Be aware that the information on social media will spread all over the world in an instant.
- By disclosing personal information and location information, individuals and locations are identified, and there is a risk of becoming a target of crime.
- Fully understand the specifications of each social media and how to set the disclosure range, and use them appropriately.

情報セキュリティ教育
Information Security Education

Check!

学生の皆さんへ　～「ネットワーク利用資格認定試験」受験について～

本学の様々な情報教育環境を安全に利用するにあたり、利用者が最低限身につけておくべき知識やモラルについて確認するため、e-Learningで「ネットワーク利用資格認定試験」を実施しています。新入生の皆さんは、必ず受験し合格しましょう。詳細は、入学時にお渡ししている「ネットワーク利用資格認定試験受験案内」を確認してください。在学生の皆さんや教職員の方も自主学習ツールとして利用できます。ぜひご活用ください。

To students

For the safe use of the information education environment of the University, we conduct the "Network User Certification Examination" on e-Learning to ensure the users have the basic knowledge and morals. All new undergraduate and graduate students must take and pass this examination. For more information, please refer to the "Network User Certification Examination Guide" you received at the time of admission. Other students and faculty members are also encouraged to use this as a self-learnig tool.

教職員の方へ　～「教職員のための情報倫理とセキュリティ」受講について～

2021年度より、e -Learning教材「教職員のための情報倫理とセキュリティ」を導入しました。教職員として押さえておくべきポイントを法律や事例を交えながら解説しています。
本学のユーザ ID をもつ教職員の方が受講することができます。毎年コンテンツを見直し、最新のトピックスを盛り込んでいますので、必ず
年に一度の受講をお願いします。

※本教材は英語版にも対応しています。
※Web シングルサインオンからログインし、「同志社大学ポータル」のタイトルを押下し、画面右下の「クイックリンク」より「情報倫理・ネットワーク利用資格認定試験・コンプライアンス教育」を選択して受講ください。

To faculty members

In 2021, we introduced the "Information Ethics and Safety for Faculty Members" on e-Learning to provide the information on the law and cases that the faculty members should know. It is available to the faculty members with the University UserID. We review the content every year and incorporate the latest topics, so please be sure to take the course once a year.

※ This course is also available in English.
※ To start the course, please log in from the Web Single Sign-on, press on the title of "Doshisha University Portal", and select " 情報倫理・ネットワーク利用資格認定試験・コンプライアンス教育 " from the [クイックリンク] at the bottom right of the screen.

同志社大学
情報セキュリティポリシー

近年の教育研究活動ならびに事務処理における情報化の進展とともに、情報セキュリティを確保することが重要になってきました。これに伴い、本学の保有する各種情報をより有効に、かつ安全に利用するためには、組織の構成員全てが情報セキュリティの重要性を認識するとともに、情報セキュリティの確保にあたっては個別の判断ではなく、広く一般的な手法を用いることが求められます。このため、本学ではこれらに対応するべく「同志社大学情報セキュリティポリシー」を制定しています。詳細は、大学ホームページに掲載しています。

Doshisha University
Information Security Policy

With the progress of computerization in recent educational and research activities and business processing, information security has become important. In order to use the various information held by the University more effectively and safely, all members of the organization must recognize the importance of information security. To ensure information security, it is necessary to use a wide-ranging and general method rather than individual judgement. "Doshisha University Information Security Policy" has been established to respond to these needs. More information is posted on the University website.

IT サポートオフィスホームページ

「ニュース&アラート」では、情報セキュリティ・ウイルス情報や、システム・ネットワークのメンテナンス関連情報、ICT サービスに関するお知らせを掲載しています。
また、情報教育環境の利用に関する情報、PC コーナーの開室時間、各種申請書やマニュアルも掲載しています。
各種案内は、「同志社大学ポータル」でもお知らせします。

IT Support Office Website

"NEWS&ALERTS" posts information security and virus information, system and network maintenance announcements and ICT service information. It also posts information regarding usage of Information Education Environment, PC corner open hours, application forms and manuals. These announcement and information can also be found on the "Doshisha University Portal".

お問い合わせ先 Contact Information

IT サポートオフィス IT Support Office

Tel ： 075-251-4567
Mail ： support@mail.doshisha.ac.jp
HP ： https://it.doshisha.ac.jp/it/