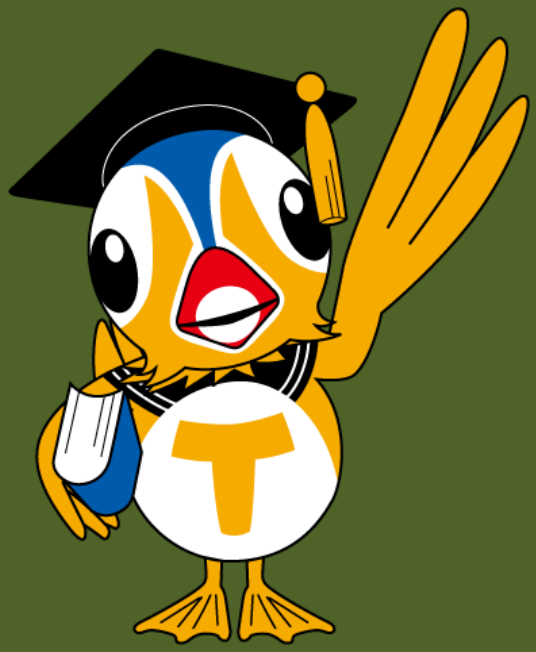
情報セキュリティ対策
これだけは守りましょう！！
Let’s Ensure Information Security



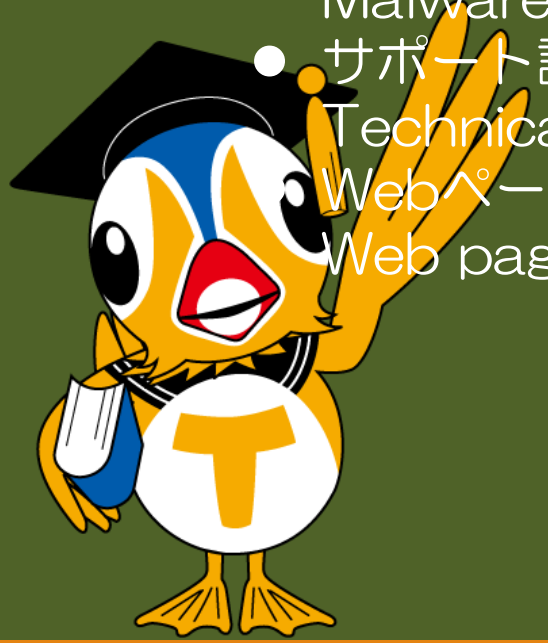
鳥取大学　情報戦略機構

Organization for Information Strategy and Management (OISM),Tottori University

鳥取大学
Tottori University

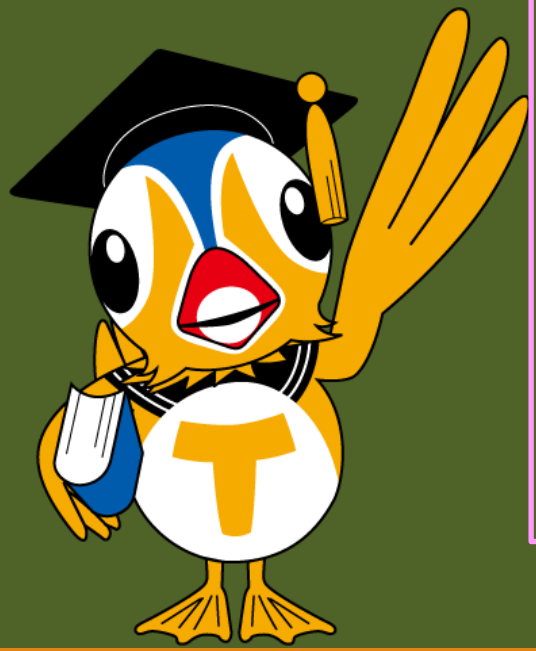
これまでに鳥取大学で発生した主な情報セキュリティインシデント
Information Security Incidents in Tottori University

- 個人情報が記録されたUSBメモリの紛失
  Lost USB flash drives storing personal information
- フィッシングによる情報の漏洩
  Information breaches by phishing
- メールの添付ファイルからマルウェア感染
  Malware infections via files attached to emails
- フリーソフトウェアインストールに伴うマルウェア感染
  Malware infections followed by installations of free software
- サポート詐欺
  Technical support scam
- Webページの改ざん
  Web pages defaced



鳥取大学
Tottori University

マルウェアに感染したら…
When malware infects your computer…



業務上の重要なファイルの破壊や消失
Destruction or loss of an important files
他人への被害の拡散
Expansion of damage to others
マルウェアの駆除と対応に費やされる時間と労力
Consumed time and effort on handling malware

大規模な情報漏洩を起こせば…
If massive information leakage happens…

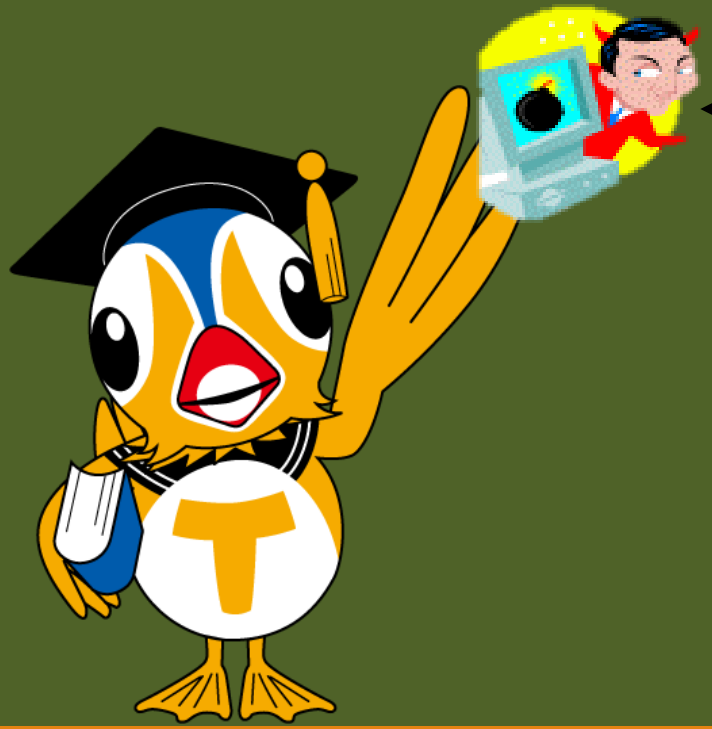
信用失墜、高額な損害賠償
Lost trust in societies, expensive compensation
大学経営にも影響が出る
Bad effect on university management

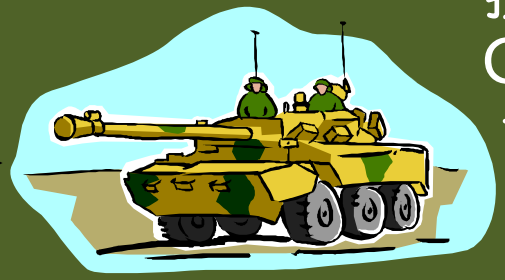
鳥取大学
Tottori University

情報セキュリティを維持するために
In Order to Ensure Information Security

制度・規則・ガイドライン
Social system, rules, guidelines

脅威
Threat



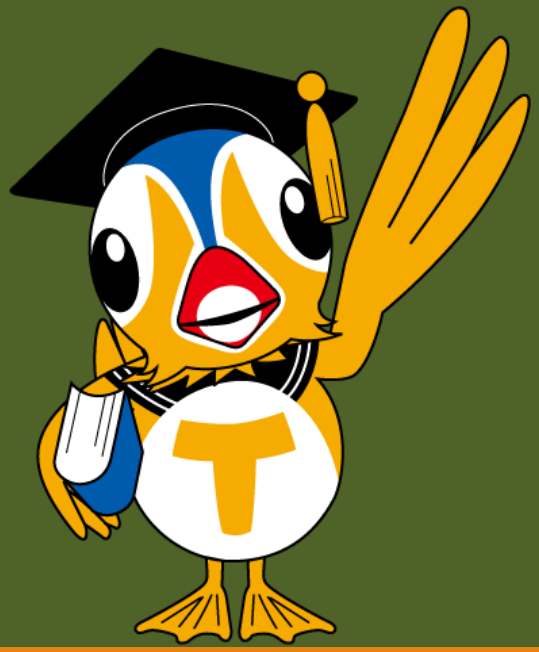


技術・装置による対応
Countermeasures by technology and devices

利用者自身の対応
Self defense by users
- モラル moral
- 注意 awareness

鳥取大学
Tottori University

鳥取大学の情報セキュリティポリシー
Information Security Policy of Tottori University



情報セキュリティポリシーとは、企業や組織において情報セキュリティを維持するための行動指針や規則のことです。
Information security policy is behavioral guideline or rules to ensure information security in a company or an organization.

本学においては、平成24年に「鳥取大学情報セキュリティ基本方針に関する規則」が制定され、以後各種の規程やガイドラインが制定されています。
In Tottori University, Information Security Basic Policy Act was enacted in 2012. Since then, related rules and guidelines have been enacted.

鳥取大学 Tottori University

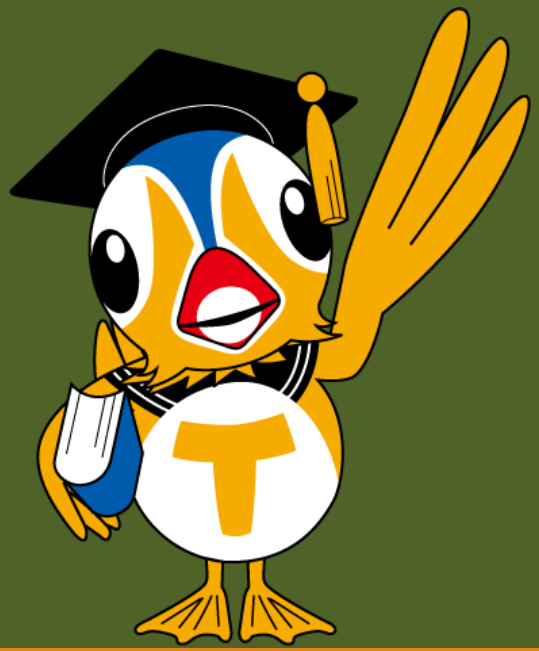
本学の情報セキュリティポリシーの体系
Information Security Policy System

鳥取大学情報セキュリティ基本方針に関する規則（平成24年学長裁定）

鳥取大学情報システム運用基本規程

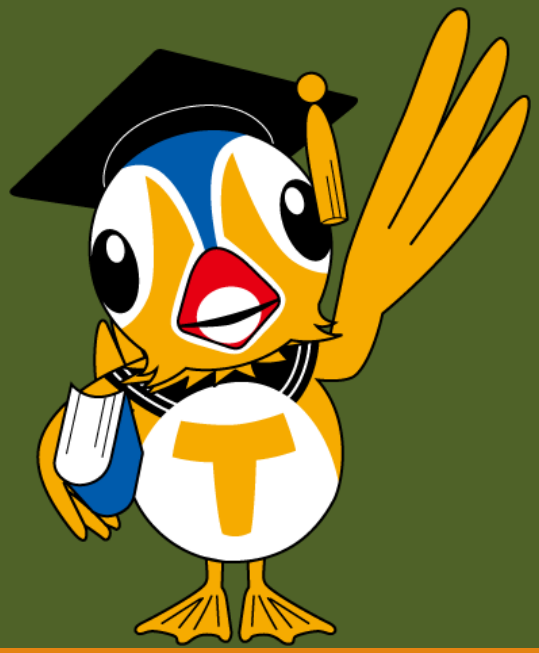
鳥取大学情報システム運用管理要項

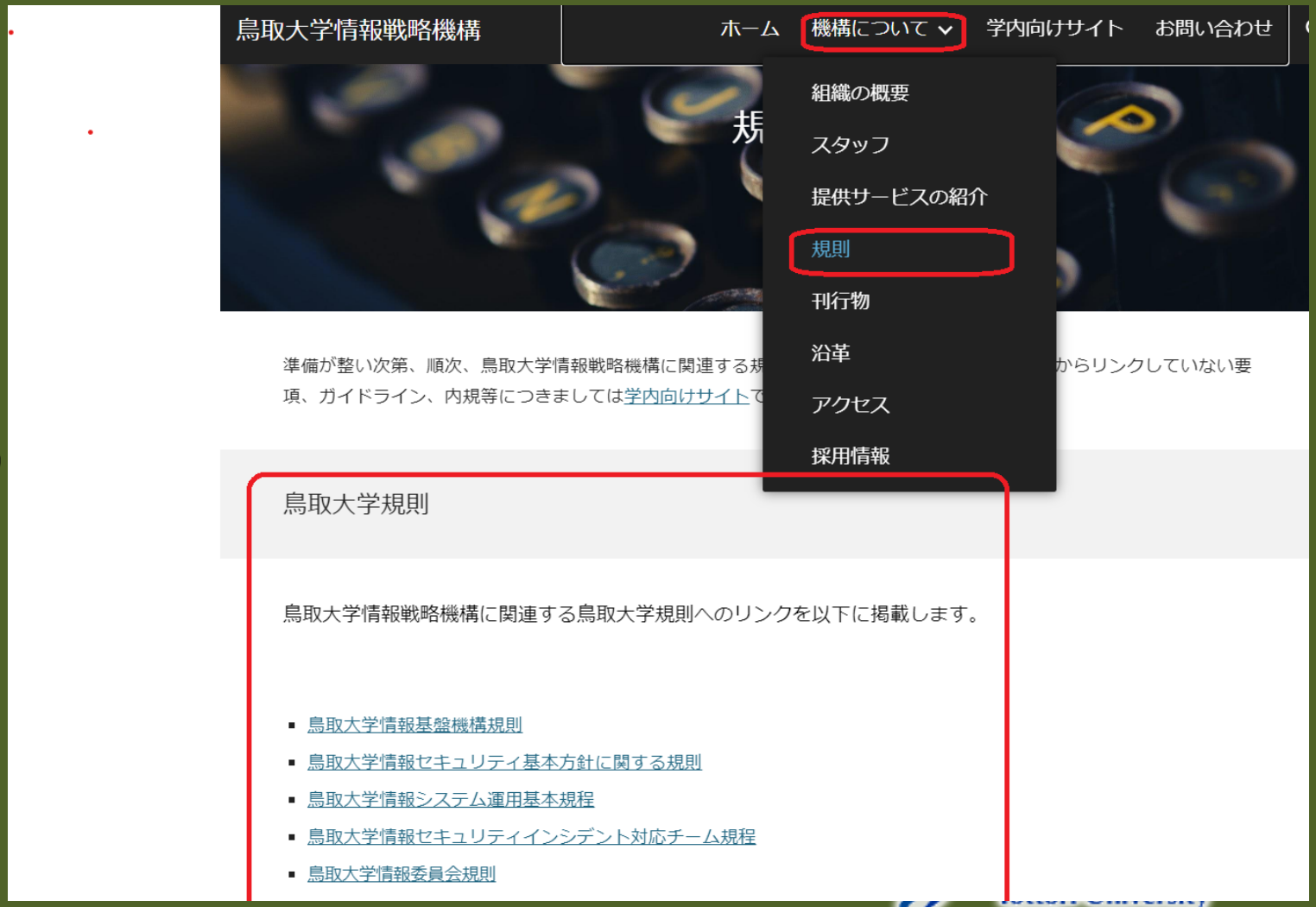
- サーバ運用管理ガイドライン
- 監査要綱
- インシデント対応ガイドライン
- 情報の格付け基準
- パスワードガイドライン
- Webブラウザ利用ガイドライン
- 電子メール利用ガイドライン
- 情報機器取扱ガイドライン
- 無線LANアクセスポイント設置ガイドライン
- 外部委託ガイドライン



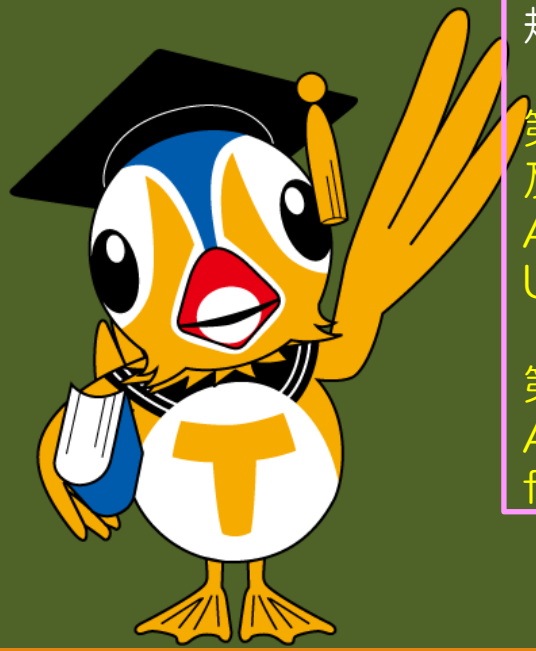
鳥取大学
Tottori University

情報セキュリティポリシーは情報戦略機構Webページに掲載しています
Information Security Policy Documents (only in Japanese) on OISM Web





鳥取大学情報セキュリティ基本方針に関する規則
Tottori University Information Security Basic Policy Act

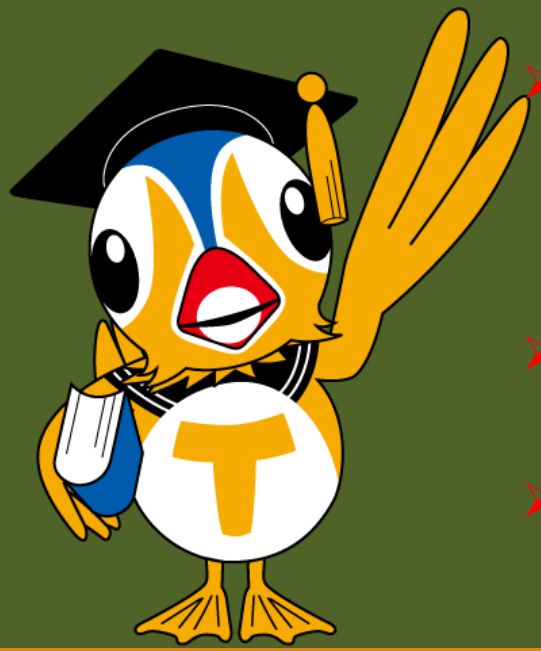


（趣旨）
第１条　この規則は、 鳥取大学（以下「本学」という。）における情報システム及び情報セキュリティに関し必要な事項を定めるものとする。
（目的）
第２条　本学情報システム及び情報セキュリティは、本学のすべての教育・研究活動及び運営を、安定的かつ効率的に行うための基盤として設置運用する。
（運用の基本方針）
第３条　本学のすべての教職員、学生等に情報の保護の必要性と責任について理解を深めることにより、情報の損失等による社会的信用の失墜、教育・研究・医療活動の中断等を未然に防ぐため、別に定める運用と利用に関する各種規定により、優れた秩序と安全性をもって安定的かつ効率に運用する。
（利用者の義務）
第４条　本学情報システムを利用する者や運用の業務に携わる者は、この規則及び別に定める運用と利用に関する各種規定を遵守しなければならない。
Article 4. users and operators of information systems in Tottori University must comply with associated rules separately stipulated.
（利用の制限）
第５条　前条に違反した者は、本学情報システムの利用を制限することがある。
Article 5. those who violates the previous article may be restricted from using information systems.

鳥取大学 Tottori University

1．マルウェアに感染したと思ったら…
If Malware Probably Infects with Your Computer…

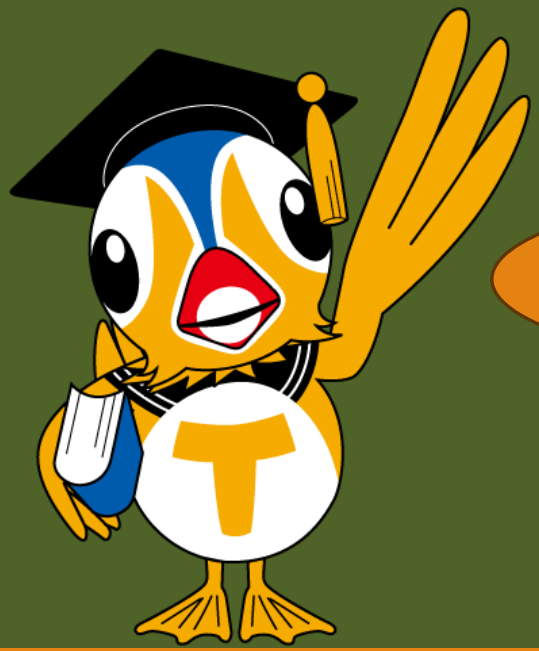
マルウェア（ウイルスなどの悪意のあるプログラム）に感染したら初動対応が重要です。
On a possible infection of malware (malicious software such as computer virus), the initial response is important.



- 速やかにコンピュータを学内ネットから切り離す（感染拡大防止）
  Immediately disconnect your computer from the network (prevention of the spread of infection)
- 直ちに、鳥取大学情報セキュリティインシデント対応チーム（TU-CSIRT）に連絡する
  Immediately contact TU-CSIRT
  TU-CISRT: csirt@tottori-u.ac.jp
- コンピュータの電源は切らない
  Do not power off your computer
- セキュリティソフトでスキャンを行わない
  Do not scan your computer with Security Software

鳥取大学 Tottori University

パソコンを学内ネットワークから切り離す
How to disconnect your computer from the network



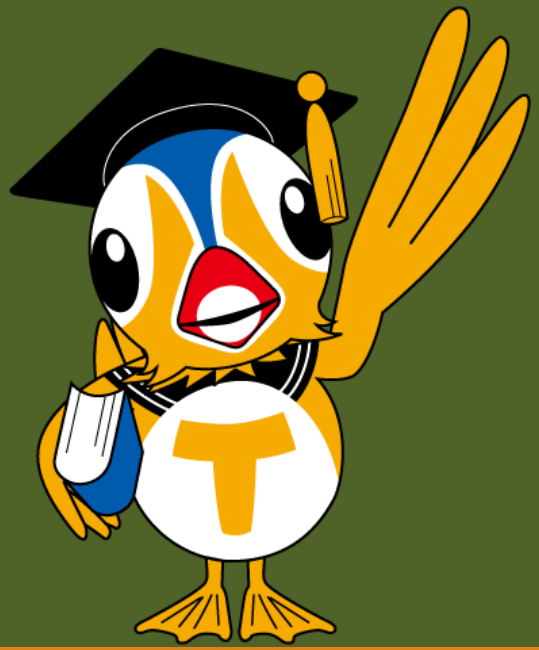
1. LANケーブルを探す
Find the LAN cable

2. LANケーブルを抜く
Plug off the LAN cable

無線LAN (Wi-Fi) はオフにする
Disable wireless LAN (Wi-FI)

鳥取大学
Tottori University

2．OSとアプリは常に最新版に
Keep your OS and Apps Updated

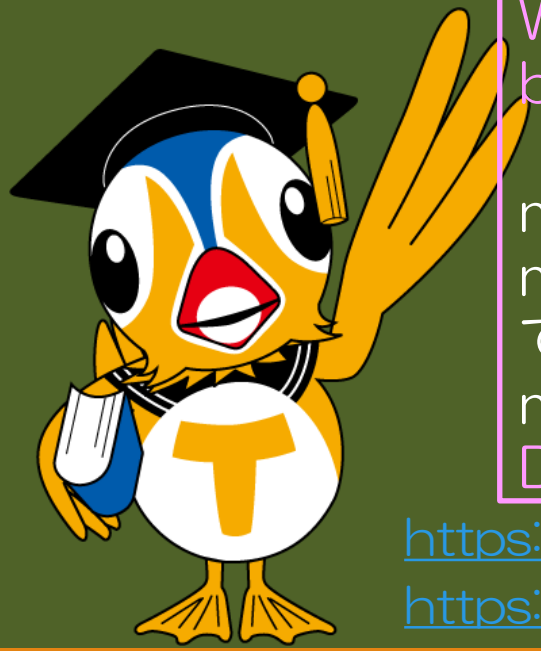


OSおよびアプリケーションソフトから脆弱性が見つかることがあります。
これらの脆弱性をそのままにしていると、マルウェア感染の危険性が高まります。OSおよびアプリケーションソフトを自動的に最新版に更新して脆弱性への対応をしてください。
Vulnerabilities can be found on OS or applications.
If vulnerabilities are not fixed, risks of malware infections increase.
Keep OS and applications updated automatically and fix vulnerabilities.

サポートの切れたOSやアプリケーションソフトをインストールしたパソコンをインターネットに繋げることはセキュリティ上非常に危険です。
It is very dangerous to connect a computer to a network whose OS and applications are outdated.

鳥取大学
Tottori University

2．OSとアプリは常に最新版に
Keep your OS and Apps Updated



Windows OSについてはWindows8.1以前はサポートが終了しています。Microsoft Officeについては2013以前のOfficeはサポートが終了しています。Windows 10，Office 2019も2025年10月14日にサポート終了予定です。
サポートの切れたOSまたはアプリケーションソフトをインストールしたパソコンを学内LANへ接続することはできません。
You cannot connect a computer with outdated OS and/or applications to a network.
Windows 8.1 or before and Microsoft Office 2013 or before finished receiving any supports.

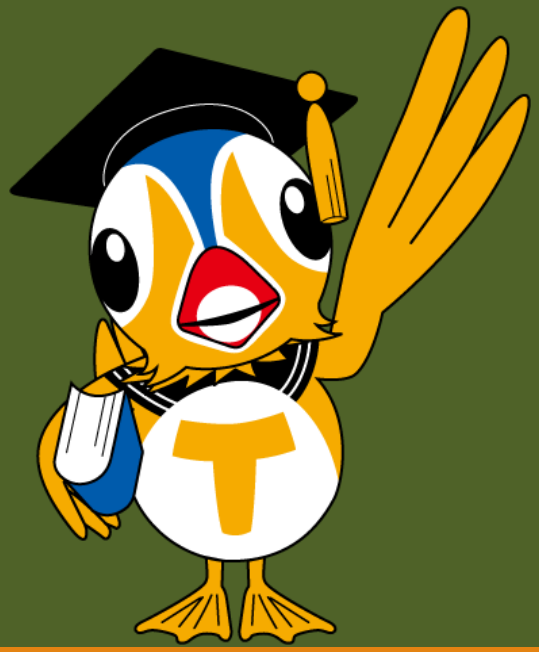
macOSは2世代前までがサポート対象と考えられます。
macOS 11 Big Sur 以前のバージョンは使用しないようにしてください。
macOS might be supported up to two generations.
Do not use 11 Big Sur or before.

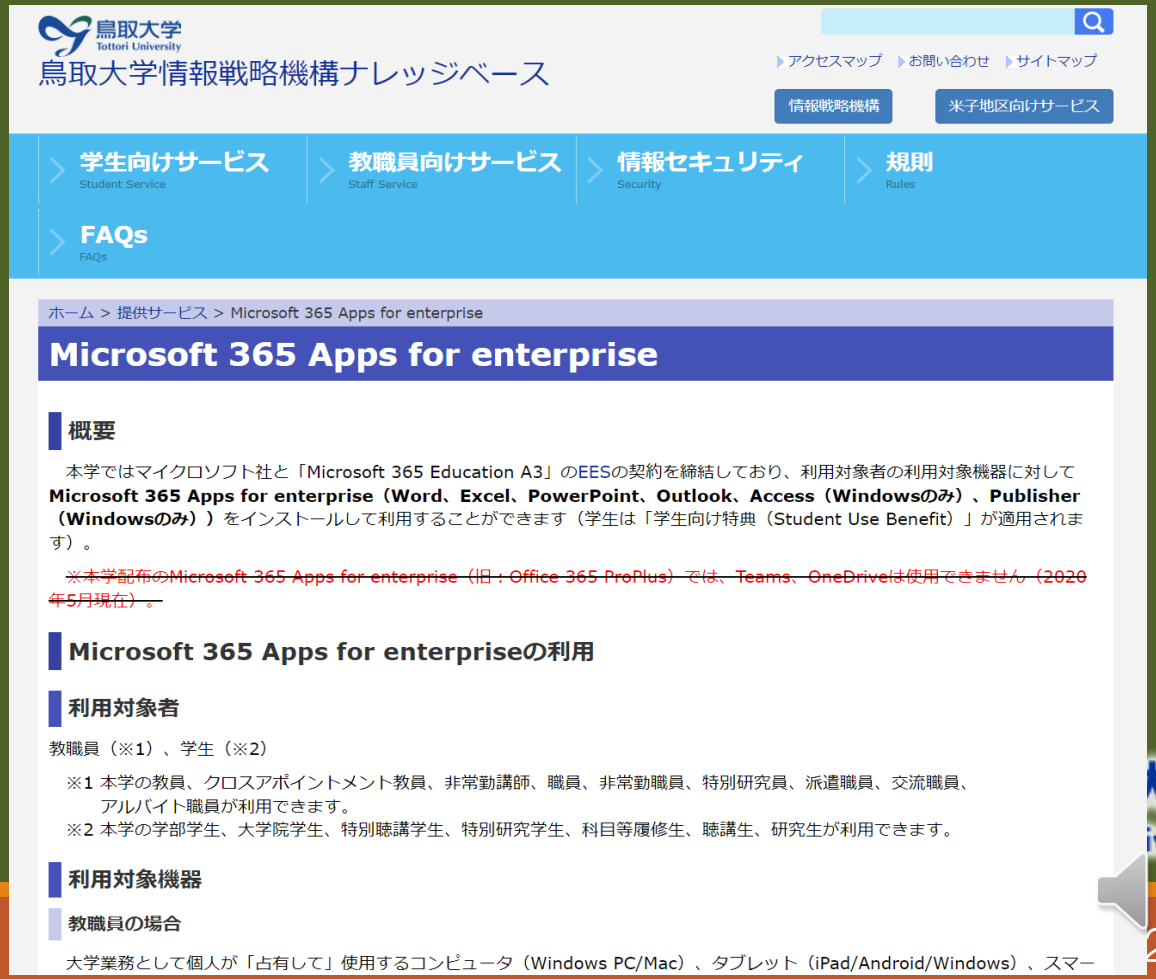
https://learn.microsoft.com/lifecycle/
https://support.apple.com/HT201222

鳥取大学 Tottori University

常に最新のOfficeソフトが使えます
You Can Always Use the Latest Microsoft Office Software

本学はMicrosoft社とMicrosoft 365の契約を行っており、常に最新のOfficeソフトが使えます。
Tottori University has Microsoft 365 agreement, and all members can use the latest Office software.





鳥取大学 Tottori University
鳥取大学情報戦略機構ナレッジベース

アクセスマップ | お問い合わせ | サイトマップ

情報戦略機構 | 米子地区向けサービス

学生向けサービス Student Service | 教職員向けサービス Staff Service | 情報セキュリティ Security | 規則 Rules | FAQs FAQs

ホーム > 提供サービス > Microsoft 365 Apps for enterprise

Microsoft 365 Apps for enterprise

概要

本学ではマイクロソフト社と「Microsoft 365 Education A3」のEESの契約を締結しており、利用対象者の利用対象機器に対して**Microsoft 365 Apps for enterprise（Word、Excel、PowerPoint、Outlook、Access（Windowsのみ）、Publisher（Windowsのみ））**をインストールして利用することができます（学生は「学生向け特典（Student Use Benefit）」が適用されます）。

~~※本学配布のMicrosoft 365 Apps for enterprise（旧：Office 365 ProPlus）では、Teams、OneDriveは使用できません（2020年5月現在）。~~

Microsoft 365 Apps for enterpriseの利用

利用対象者

教職員（※1）、学生（※2）

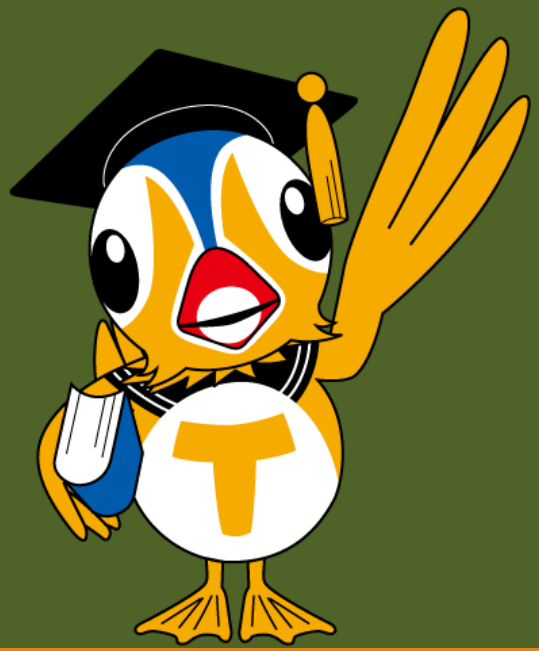
※1 本学の教員、クロスアポイントメント教員、非常勤講師、職員、非常勤職員、特別研究員、派遣職員、交流職員、アルバイト職員が利用できます。
※2 本学の学部学生、大学院学生、特別聴講学生、特別研究学生、科目等履修生、聴講生、研究生が利用できます。

利用対象機器

教職員の場合

大学業務として個人が「占有して」使用するコンピュータ（Windows PC/Mac）、タブレット（iPad/Android/Windows）、スマー

3．セキュリティソフト（ウイルス対策ソフト）の導入
Installation of Security Software (Anti-Virus Software)

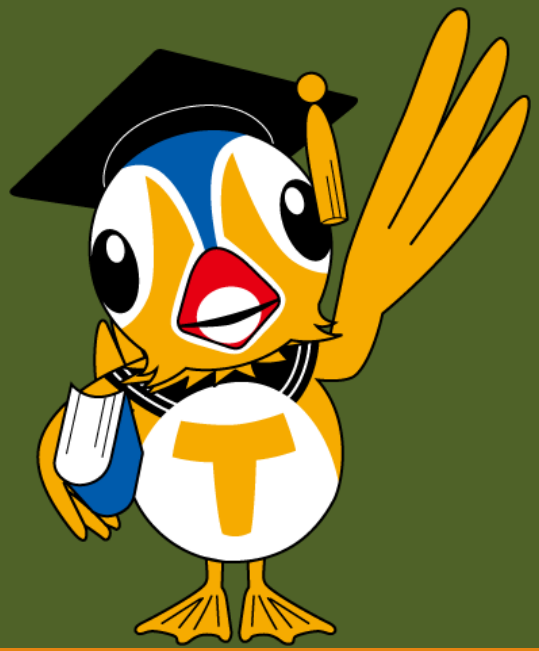


WindowsパソコンとMacを学内LANに接続する際にはセキュリティソフトをインストールするよう決められています。
ウイルス対策ソフトがインストールされていないWindowsパソコン又はMacを学内LANに接続することはできません。
You must install security software into your Windows or Mac computer when connecting them to the campus network.

WidowsにはWidows Defenderが最初からインストールされていますが、業務で利用するPCにはMicrosoft Defender for Endpointを導入してください。
Install Microsoft Defender for Endpoint to your business use computer even though Windows Defender is already installed by default.

鳥取大学
Tottori University

4．メールを利用する際の注意点
Notes on Using Emails

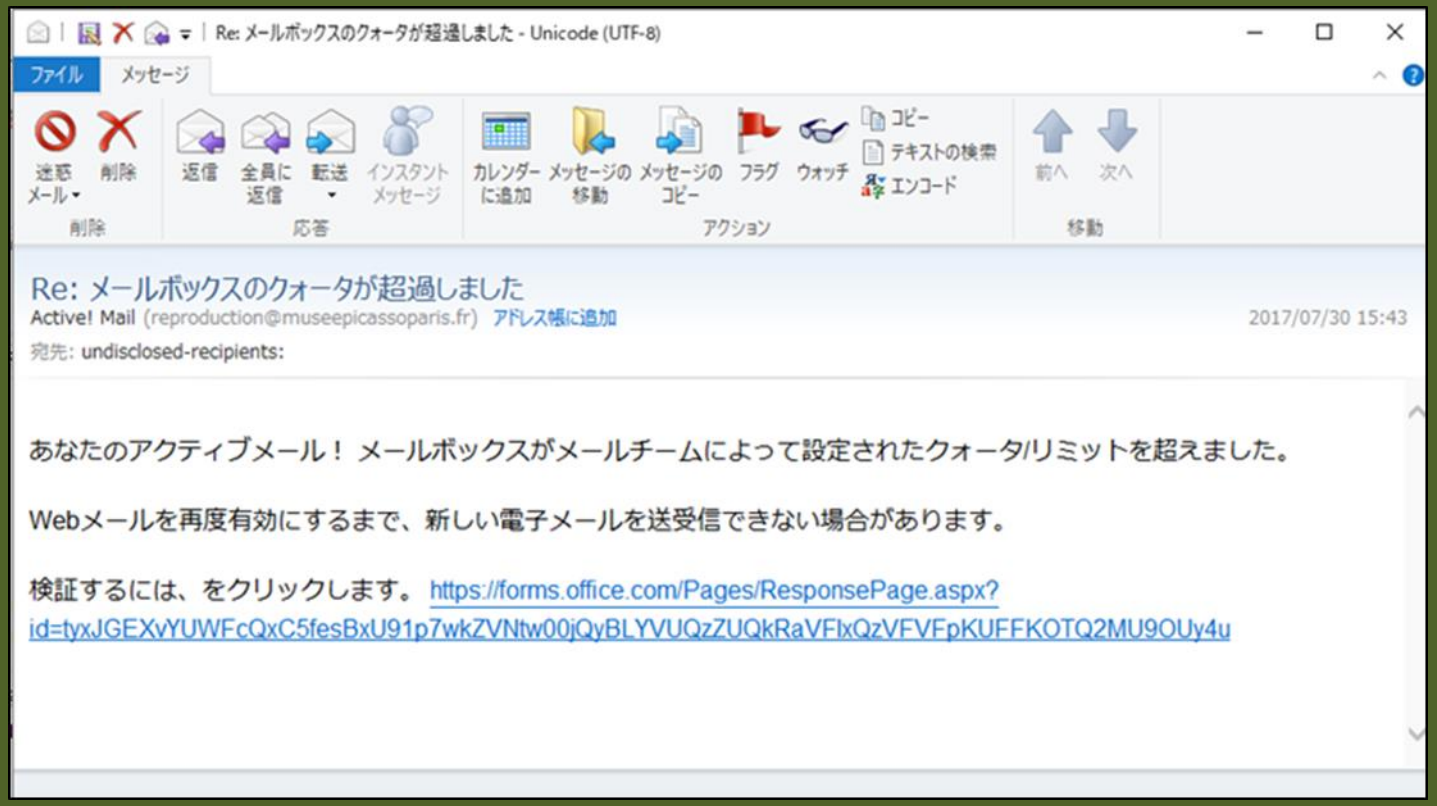


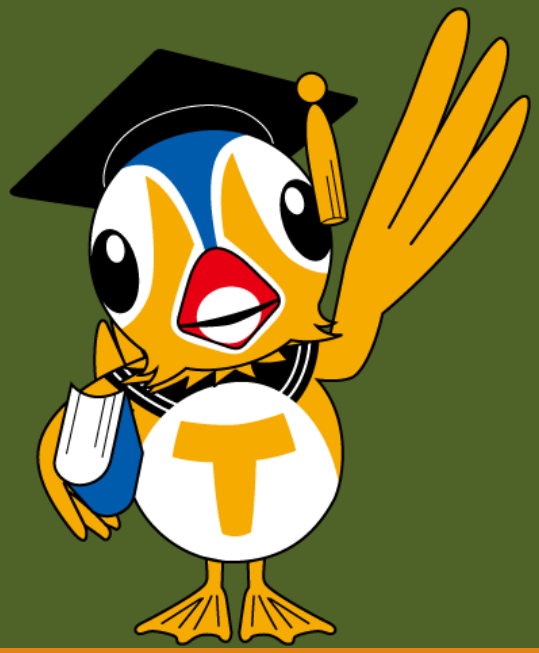
マルウェア感染の主要な経路の一つは電子メールの添付ファイルです。
不審な添付ファイルは開かないようにしましょう。
Do not open attached suspicious files because the primary cause of malware infection is email.

また、メール文中のリンクをクリックさせて本物そっくりの偽サイトに誘導し重要情報を盗み取るフィッシング詐欺も多発していますので注意をしてください。
Be careful of phishing that defrauds you of confidential information by navigating to a fake site, which almost perfectly copies the original site, via a link in an email.

鳥取大学 Tottori University

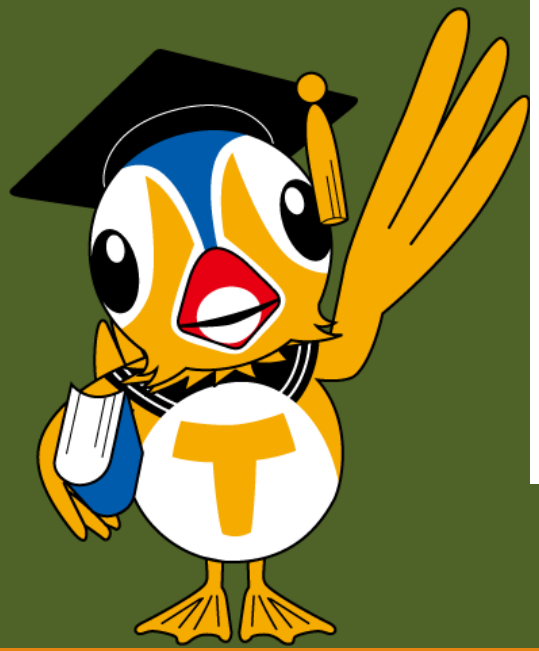
フィッシングメールの例
Examples of Phishing Emails





鳥取大学
Tottori University

フィッシングメールの例（つづき）
Examples of Phishing Emails (continued)



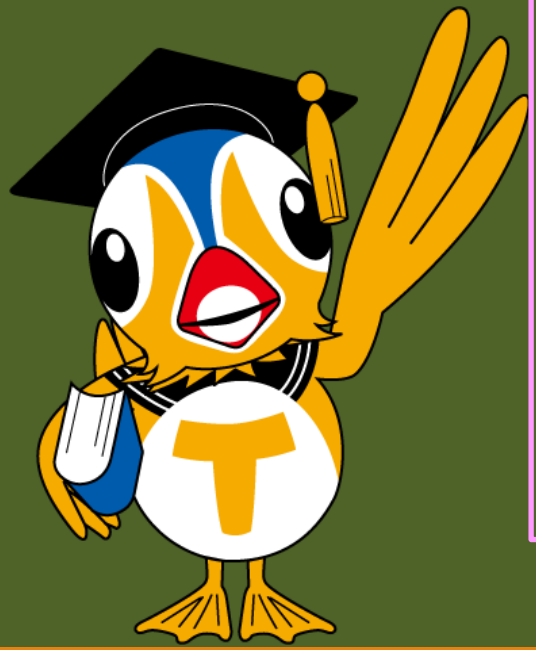
鳥取大学
Tottori University

標的型攻撃
Targeted Attacks

無差別ではなく、特定の組織や個人を標的として、マルウェアや偽サイトへのリンクを含んだメールを送付する攻撃。
Attacks sending emails containing malware or links to malicious sites to targeted specific organizations or individuals.

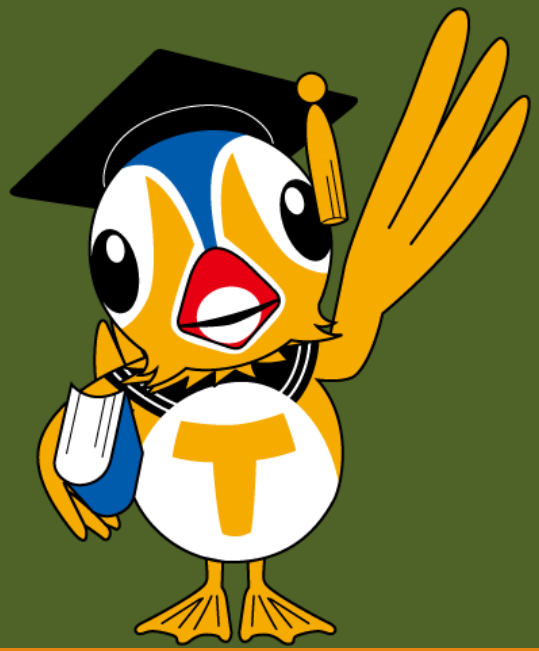
主な目的は情報の詐取である。
A main purpose is to steal information.

- 関係者しか知らない言葉やフレーズで信用させる
  make you trust using only words known to friends or acquaintance
- 添付ファイル付き偽装メール fake email attached file
- 偽ホームページへの誘導 navigating to phishing site



鳥取大学
Tottori University

科学研究費を騙った標的型攻撃
Targeted Attack Mimicking KAKENHI (Japanese Research Budget)



件名：　【H29科研費】繰越申請について
添付ファイル：　【H29科研費】繰越申請について.zip

お世話になっております。
今年度の科学研究費助成事業（科学研究費補助金）の
繰越についてお知らせいたします。
翌年度に繰り越すことができるのは、計画の変更等に伴い当該年度中に使用することができなかった科研費です。例えば、研究計画の終了後に余った科研費は、繰越の対象にはなりません。
■申請の有無についての回答期限
平成２９年１月２６日（木）　１２時【厳守】
■○○係提出期限
平成２９年２月２日（木）　１２時【厳守】

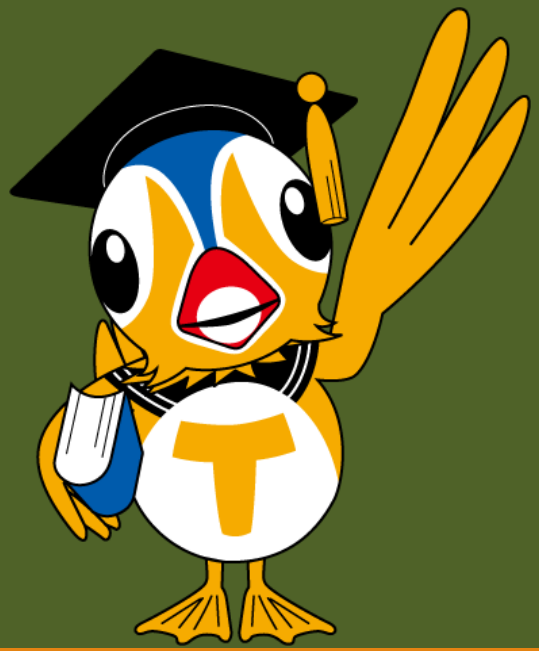
鳥取大学
Tottori University

情報戦略機構が
行っている技術的対応

Technical Countermeasures Implemented by OISM

鳥取大学
Tottori University

多要素認証システム
Multi-Factor Authentication



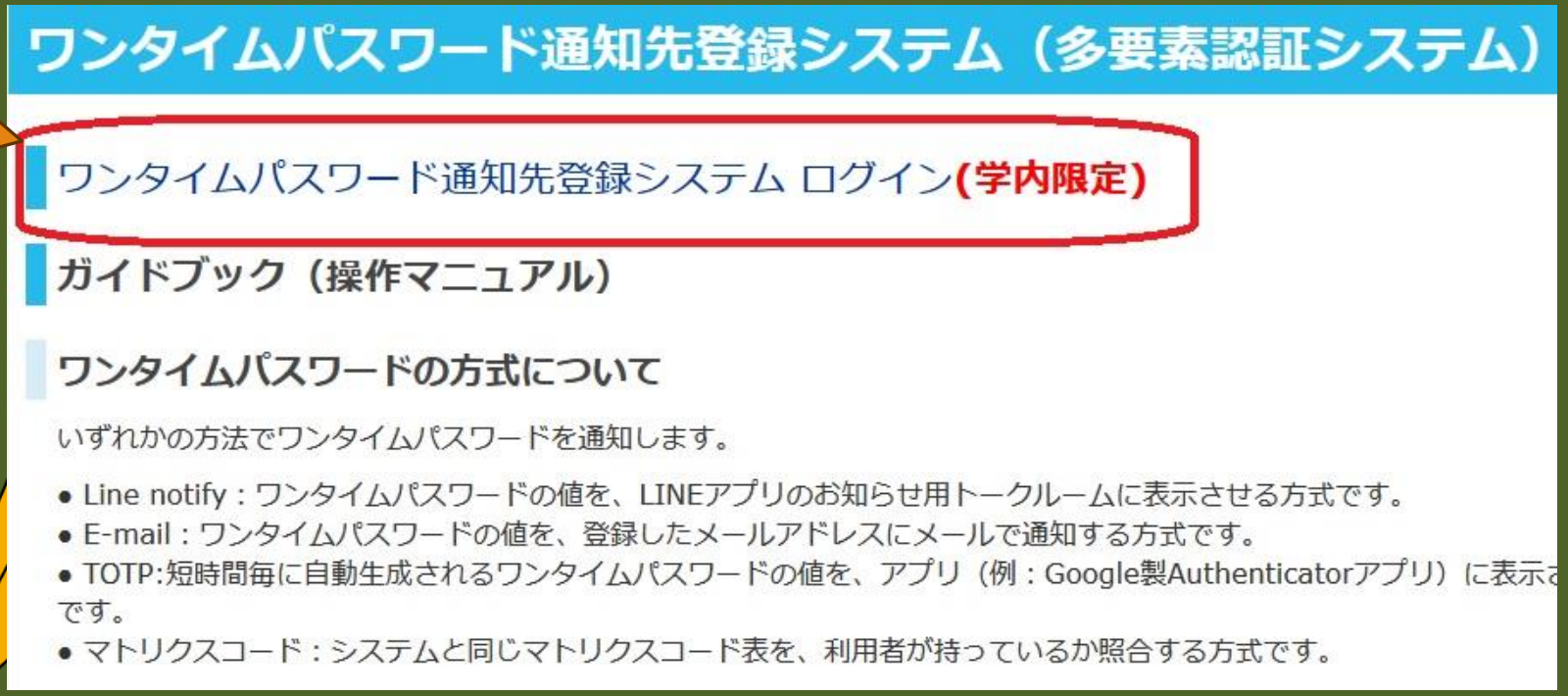
ユーザ名とパスワードに加えて、使い捨てのワンタイムパスワードを認証に用いるシステムです。メールなどを学外から利用する場合にワインタイムパスワードが必要になります。
Multi-factor authentication requires additional One-Time Password (OTP) for authentication in addition to a username and a password.
One time password is always required when you access to information systems off campus.

セキュリティを高めるため、学内から利用する時もワンタイムパスワードを必須にすることができます。
Multi-factor authentication can be enabled even on campus for more security.

事前に各自「ワンタイムパスワード通知先登録システム」に登録する必要があります。
You must register on OTP registration system in advance.

多要素認証システム（登録）
Multi-Factor Authentication（How to register）

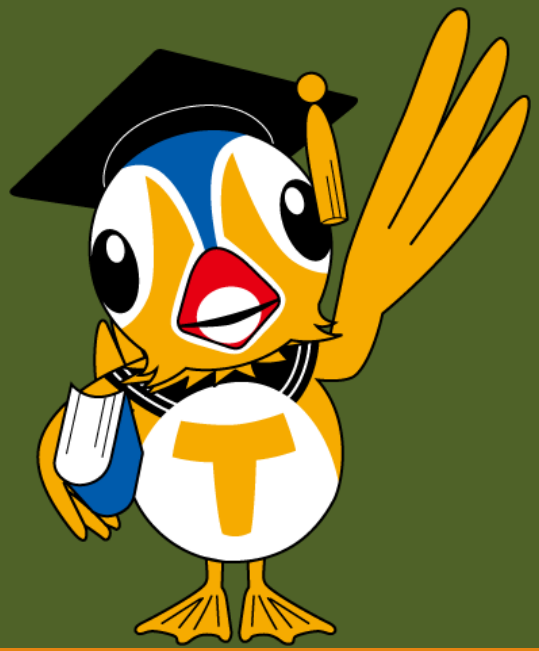
Access to OISM page, and click here.



You can register the following OTP generation methods:
Line notify, alternative email, TOTP, matrix code.

Tottori University

多要素認証システム（ログイン）
Multi-Factor Authentication（Login Page）



鳥取大学
Tottori University

鳥取大学ログインページ：manaba
サービス

鳥大ID(もしくは鳥大のメールアドレス)と
パスワードを入力し「ログイン」を選択して
ください。

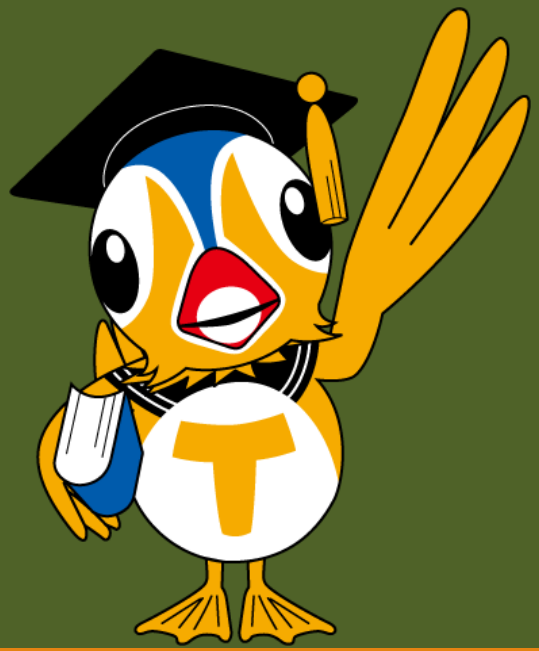
鳥大IDまたはメールアドレス / Toridai ID or E-Mail

パスワード / Password

ログイン / Login

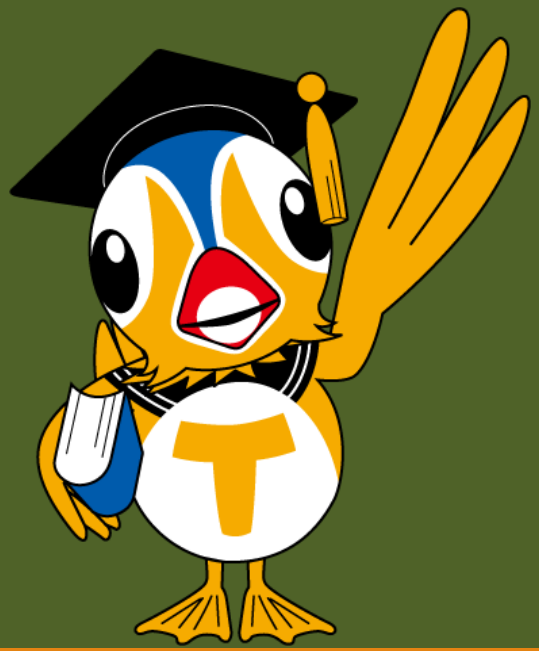
鳥取大学
Tottori University

多要素認証システム（ワンタイムパスワード方式選択）
Multi-Factor Authentication（Multi-factor Selection）



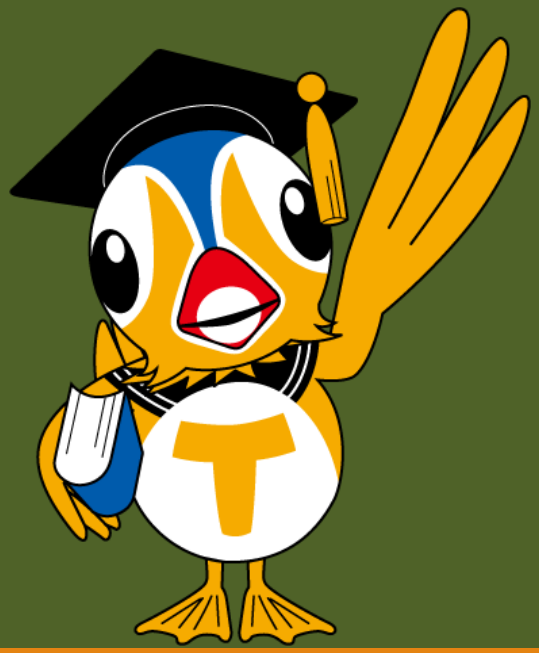
鳥取大学 Tottori University

多要素認証システム（ワンタイムパスワードの入力）
Multi-Factor Authentication（Input OTP）



鳥取大学
Tottori University

多要素認証システム（高セキュリティ設定）
Multi-Factor Authentication (Securer Setting)



マトリクスコード

項目	データ
登録日	2019年12月5日19:01
操作	マトリクスコード削除

信頼できる端末を全て取り消す

端末紛失時や不正アクセスが疑われる時に実行します。
ワンタイムパスワード入力の省略を取り消します。

取り消し

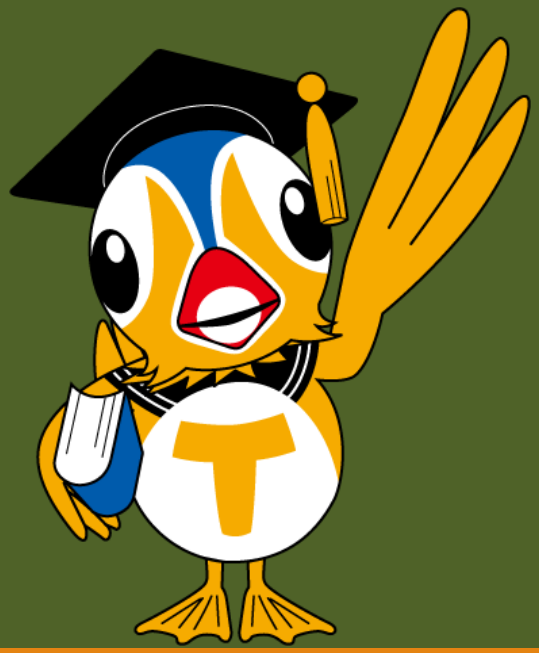
高セキュリティ設定(推奨)

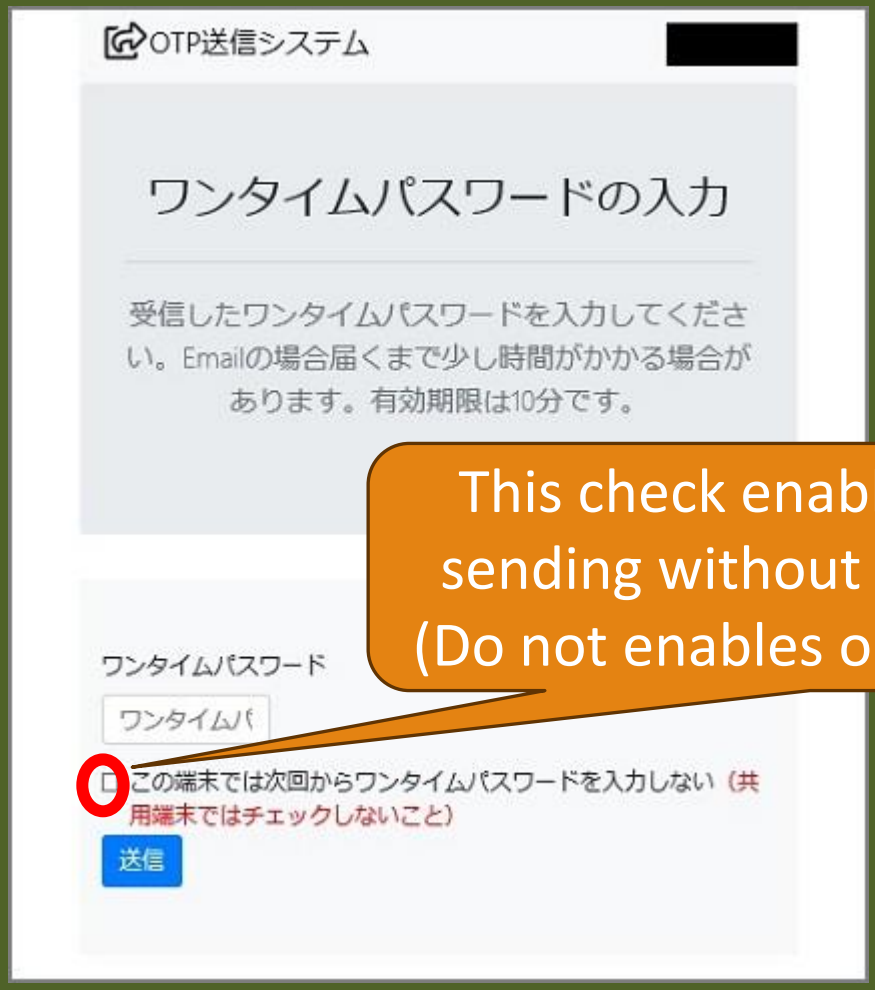
学内から接続した場合でも全てのサーバに対して多要素認証を行います。

高セキュリティ有効化中(無効化する)

鳥取大学
Tottori University

多要素認証システム（ワンタイムパスワード入力省略）
Multi-Factor Authentication (Automatic OTP Sending)





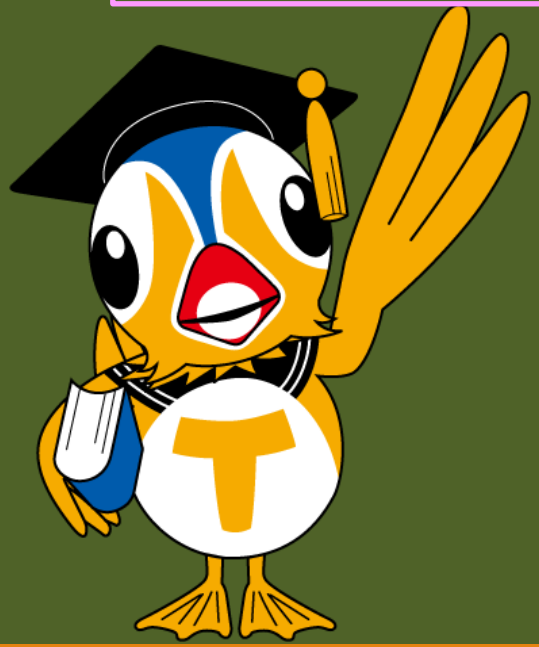
This check enables automatic OTP sending without manual OTP input.
(Do not enables on shared computer)

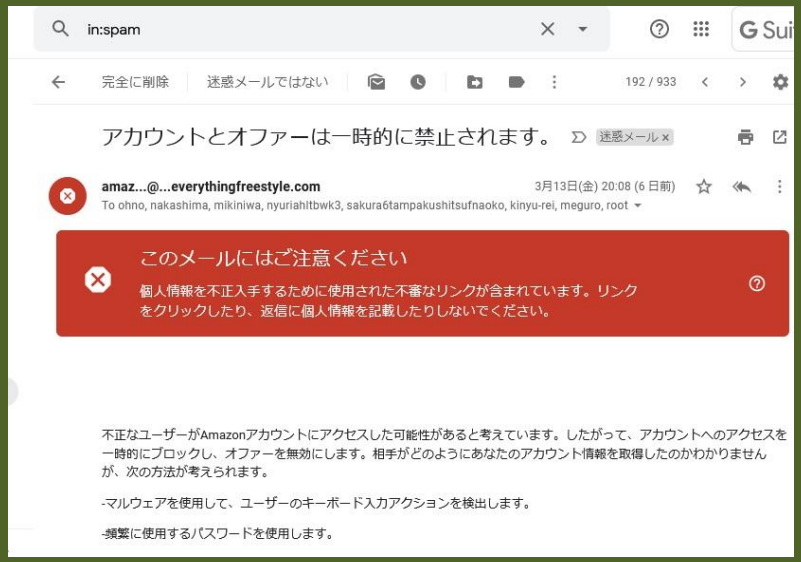
鳥取大学
Tottori University

Gmailの利用（Google Workspace for Educationを契約）
Toridai Gmail (Using Google Workspace for Education)

Webブラウザでメールを利用することを推奨しています。フィッシングや添付ファイルに対する警告が表示されます。
We strongly recommend to use Toridai Gmail with a Web browser which warns phishing and malware.

メールの検索も高速です。また、メールの返信し忘れを注意してくれます。
Toridai Gmail with Web browser can search for mails quickly and remind you of replying a received mail.

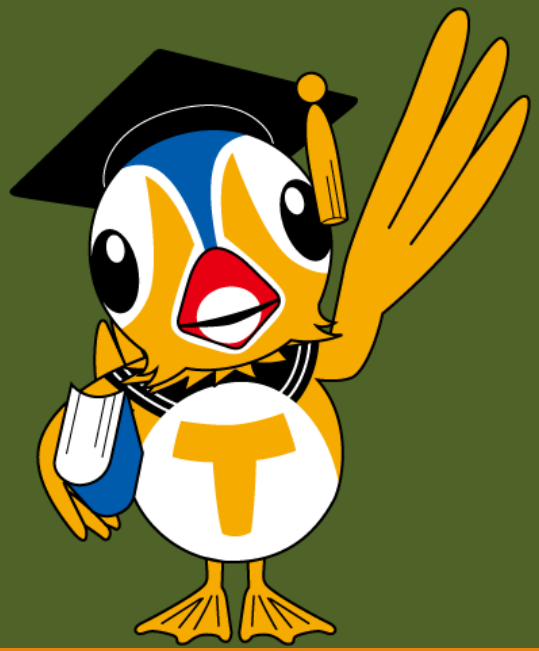




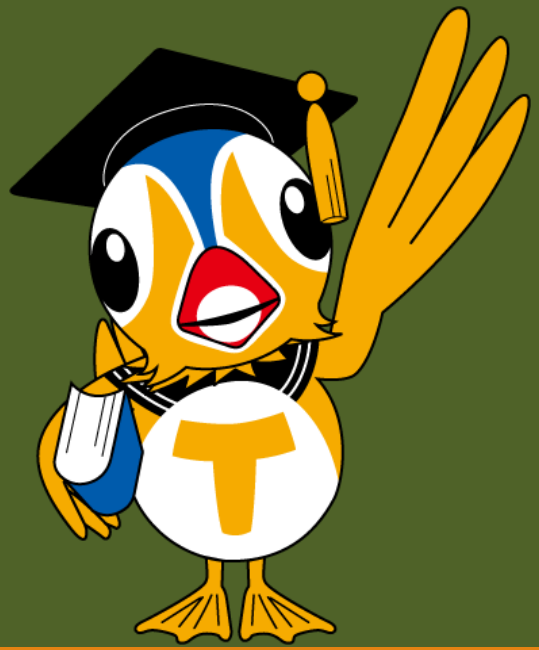
鳥取大学 Tottori University

ファイル受け渡しサービス
File Sharing Service

容量の大きなファイルや実効形式ファイルが受け渡しできます。
File sharing service enables to send a large-size file or executable files.



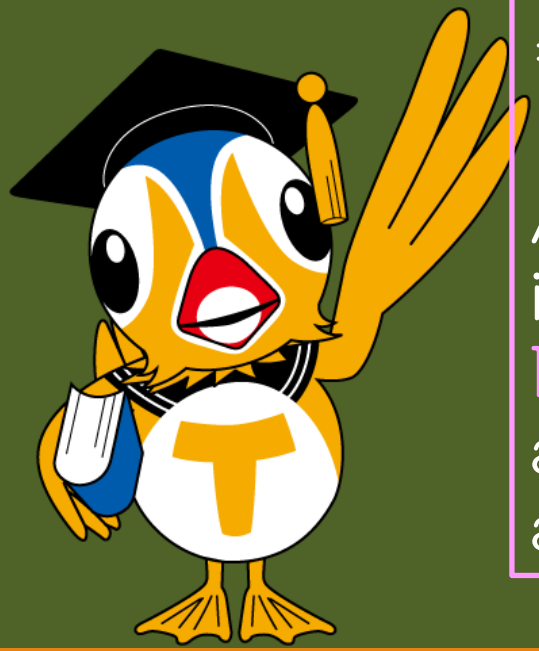
5．出所の定かでないソフトウェアを利用しない
Do not Use Software of Unknown Developer



出所の定かでないフリーソフトの中には、悪意を持って作られた物もあります。このようなソフトをインストールして、情報が盗み取られる被害も発生しています。出所の定かでないソフトウェアを利用しないようにしましょう。
Some of free software of a unknown origin may be developed with malicious intent. There have been some cases where confidential information is leaked by installed such free software.
Do not use software of a unknown developer.

鳥取大学
Tottori University

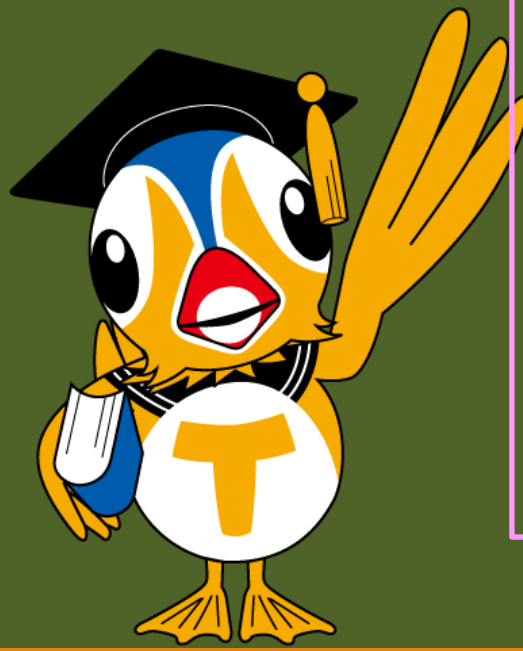
6．パスワードの管理
Password Management



パスワードはあなたの情報を守る重要なものです。他人に容易に推測されないよう、パスワードは英文字、数字を組み合わせた長いもの（12文字以上必須）としましょう。 記号を含めても構いません。複雑なパスワードは手帳に記載するなどしても構いません。

A password is important to secure your information. A password should be long (at least 12 or more characters are required) and a combination of alphabets, numbers, and symbols.

6．パスワードの管理（つづき）
Password Management (continued)



鳥大IDのパスワードを学外の他のサービスで使い回してはいけません。使い回していると、一旦パスワードが漏れれば、同じパスワードを利用しているサービス全てで不正利用される危険性があります。

Do not use your Toridai ID password for other services outside Tottori University.
If the same password is employed and the password is leaked, all services may be accessed without any authorization.

7．パソコンやUSBメモリ等の盗難・紛失に気を付ける
Do not Lose Your Computer and USB Flash Drive

重要情報が保存されたパソコンやUSBメモリーの盗難や紛失が起きれば、皆さん個人の業務に支障が生じるだけでなく、大学の信用問題にも関わります。重要情報が保存されたパソコンやUSBメモリの盗難や紛失には十分注意をお願いします。
事務職員の方が業務で使うUSBメモリは、暗号化機能が付いたものと決められています。教員におかれても暗号化機能が付いたUSBメモリの使用をお勧めいたします。

The theft or loss of a computer or USB flash drive containing important information will not only affect your individual work, but also affect the credibility of the university.
Please be careful against the theft or loss of them.
USB flash drive used by administrative must have an encryption function. Faculty members are also encouraged to use USB flash drives with encryption functions.

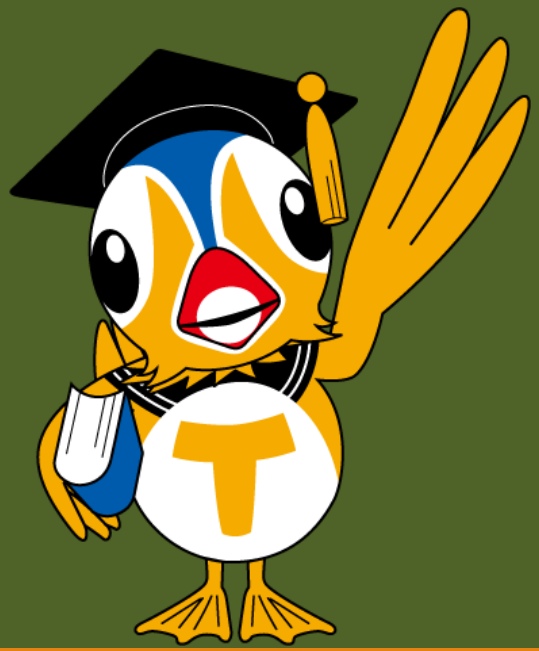
Office製品ファイルの暗号化
Encryptions of Office Files

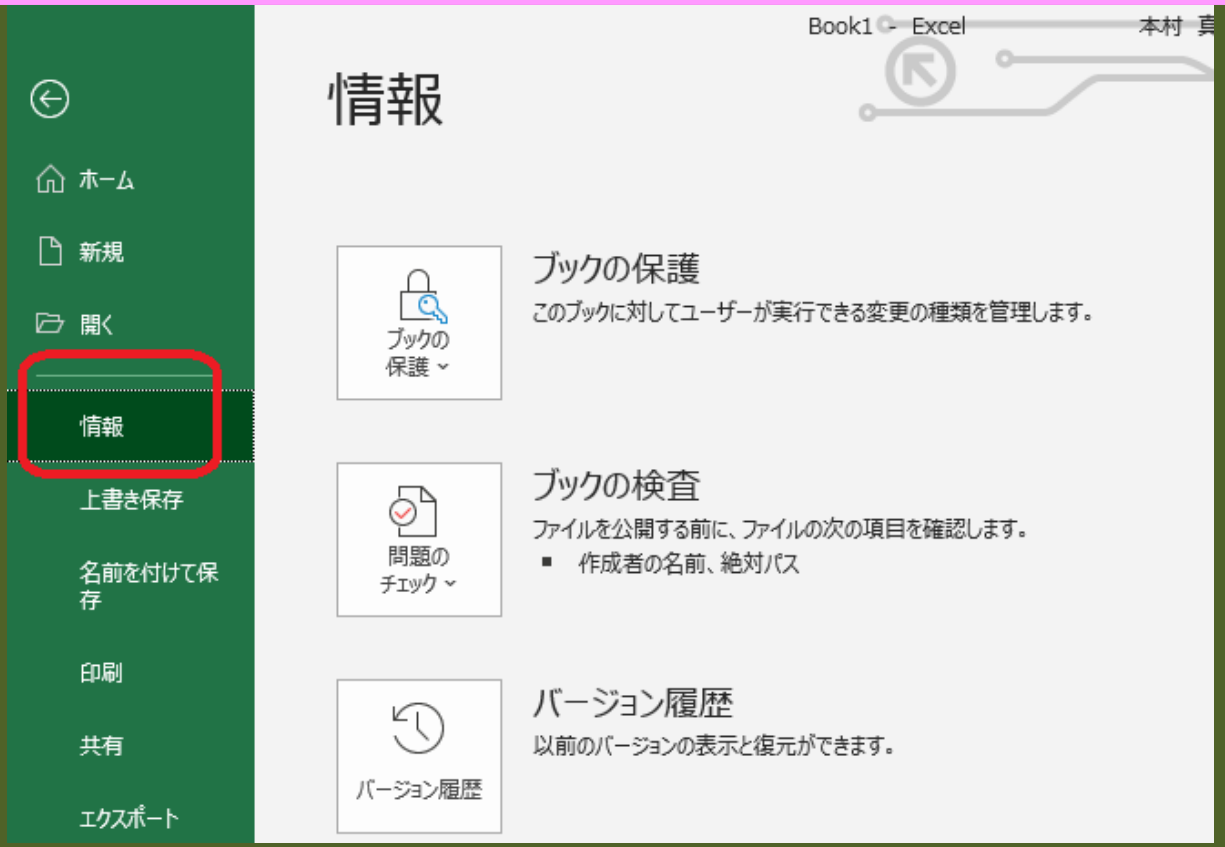
重要な情報はMicrosoft Office製品を用いて作成される場合が多いと思います。
Microsoft Office製品には暗号化が標準機能として備わっています。
次項以降に、Microsoft Excelを例に暗号化手順を説明します。
Wordファイル, Power Pointファイルも同様な手順で暗号化が行えます。

Documents containing Important information are often created using Microsoft Office products.
Microsoft Office products have encryption as standard function.
The following slides will explain how to encrypt a file using Microsoft Excel.
Word and Power Point files can be encrypted by the similar procedures.
Reference: https://support.microsoft.com/office/protect-an-excel-file-7359d4ae-7213-4ac2-b058-f75e9311b599

Microsoft Excel の暗号化
Encryption on Microsoft Excel

（1）「ファイルタブ」から「情報」を選択します。
Select [File] tab, and [Info].

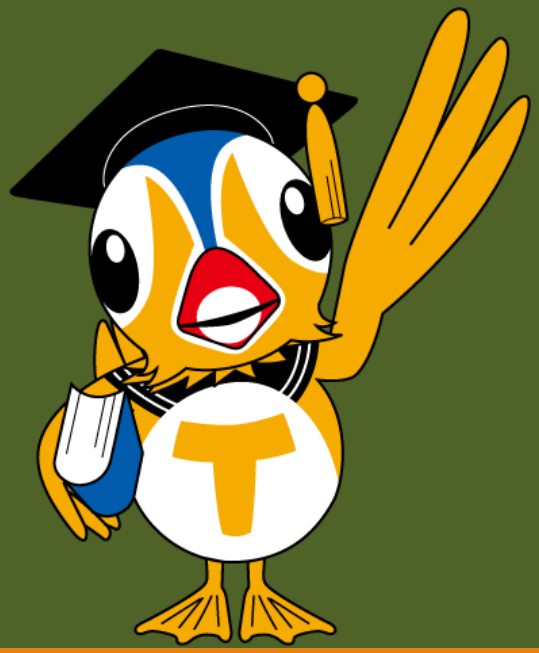


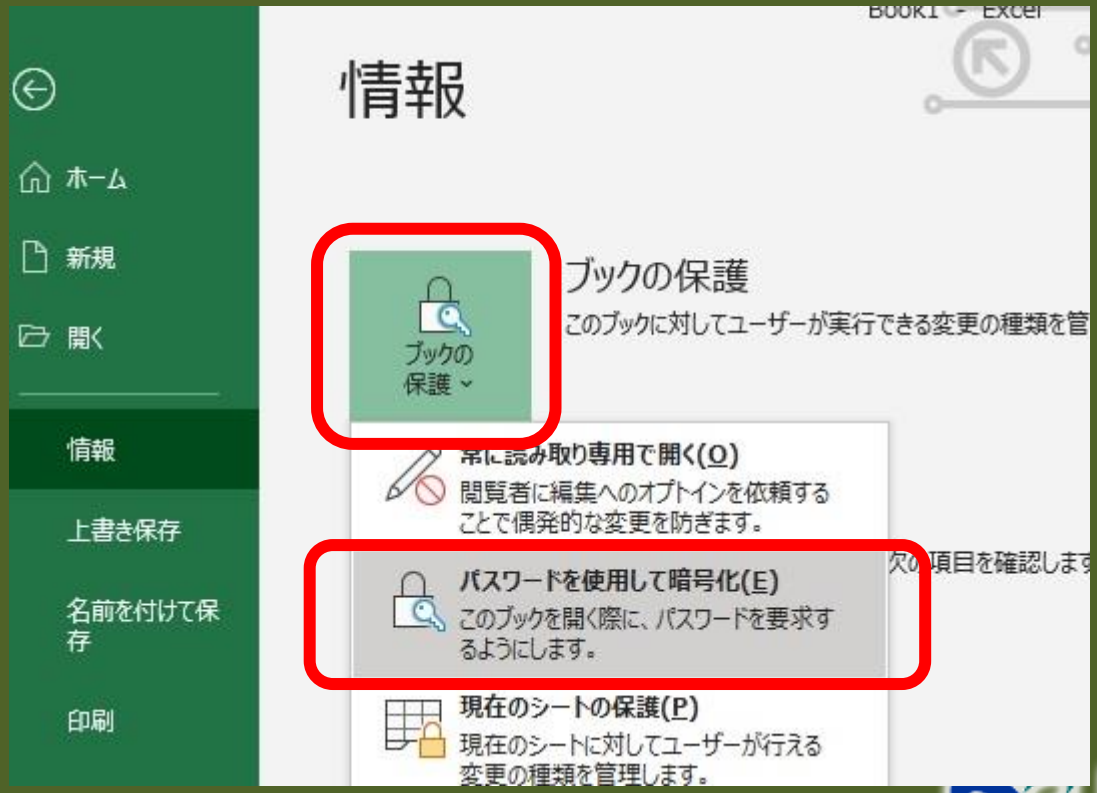


鳥取大学 Tottori University

Microsoft Excel の暗号化
Encryption on Microsoft Excel

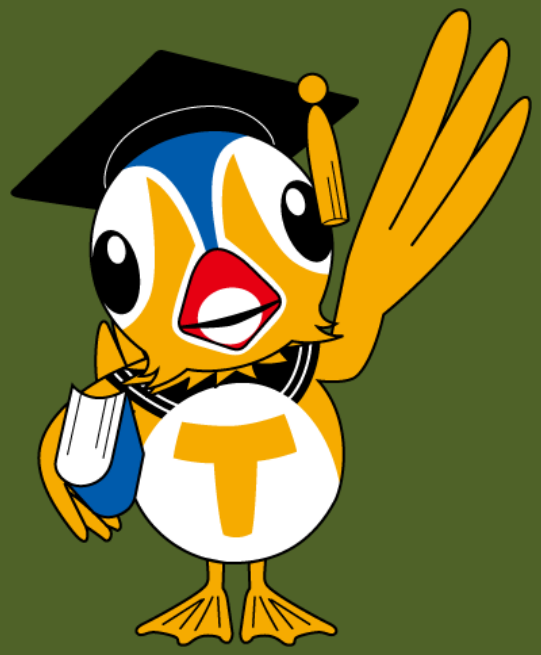
（2）「ブックの保護」から「パスワードを利用して暗号化」を選択。
Select [Protect Workbook] and choose [Encrypt with password].





鳥取大学
Tottori University

怪しい・危ない・しまったと思ったら、直ちにTU-SCIRTへ
Immediately Contact TU-CSIRT if Suspicious, Dangerous or Done



- コンピュータウイルスに感染したかも？
  Infected with a computer virus?
- フィッシング詐欺に引っかかったかも？
  Defrauded by Phishing?
- 重要な情報が漏えいしたかも？
  Confidential Important Information is leaked?
- USBメモリを無くしたかも？
  Lost USB flash drive?

→こんな時は直ちにTU-CSIRTへ連絡してください。
Immediately contact TU-CSIRT in above cases.

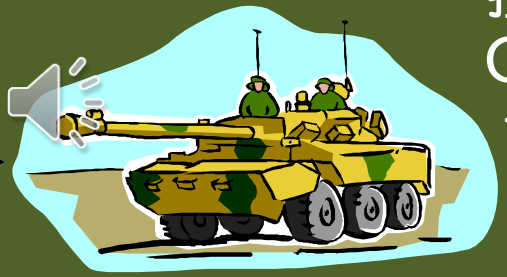
TU-CSIRT（鳥取大学情報セキュリティインシデント対応チーム）は、部局を問わず情報セキュリティインシデントに対応する組織です。
Email：csirt@tottori-u.ac.jp

CSIRT：Computer Security Incident Response Team

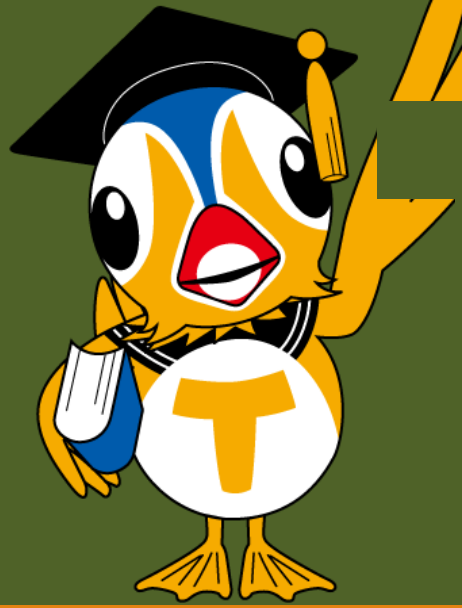
何よりも大切なのは利用者の対応
The Most Important is a User Response

制度・規則・ガイドライン
Social system, rules, guidelines

脅威
Threat



技術・装置による対応
Countermeasures by technology and devices

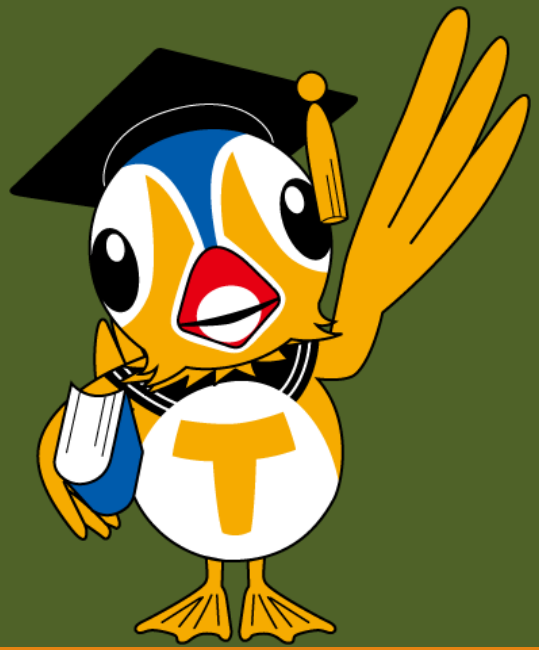


利用者自身の対応
Self defense by users
- モラル moral
- 注意 awareness

鳥取大学
Tottori University

本学の情報セキュリティの維持に
ご協力下さいますようお願い致します。

Thank you for your cooperation
to ensure information security.



鳥取大学
Tottori University