情報セキュリティ対策 これだけは守りましょう!!

マルウェアに感染したと思ったら…

マルウェア（ウイルスなどの悪意のあるプログラム）に感染したと思ったら、すぐに機器をネットワークから切り離して、下記相談窓口に連絡する。

OS・アプリ

OSとアプリは常に最新版にアップデートする。

セキュリティソフト

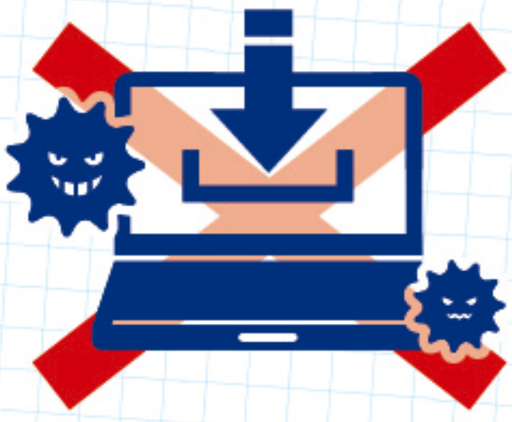
セキュリティソフト（ウイルス対策ソフト）を導入してパターンファイルを最新に保つ。

電子メール

メールの添付ファイルやリンクをクリックするときはマルウェア感染やフィッシングの脅威があるので注意する。

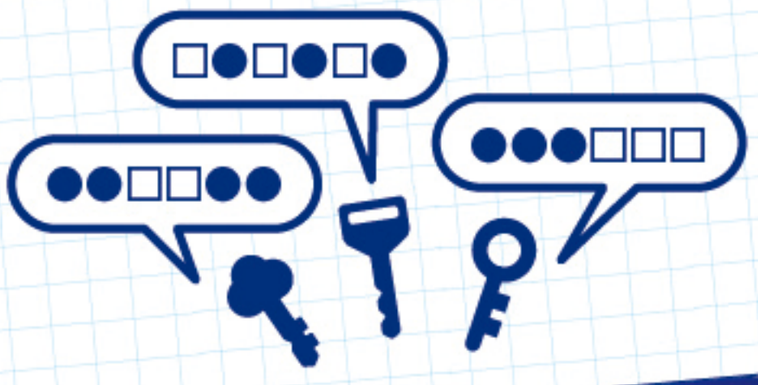
ソフトウェアのインストール

出所の定かでないソフトウェアをインストールしない。



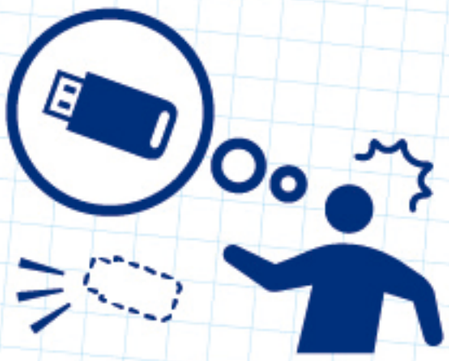
パスワード

パスワードはシステム毎に違うものを使い他人に知られないように気をつける。



盗難・紛失

パソコンやUSBメモリ等の盗難・紛失に気をつける。



2304

相談窓口

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）

各項目の詳しい説明はこちらから

https://kb.oism.tottori-u.ac.jp/security/

E-Mail ／ csirt@tottori-u.ac.jp

What you should do to keep information security.

On a possible malware infection...

You should disconnect your computer or mobile device from the Internet as soon as possible when you suspect it has been infected by malicious software (malware), e.g. a computer virus. Afterwards, contact the inquiry counter as shown below.

Operating system and application

OS and application software should always be up to date.

Security software

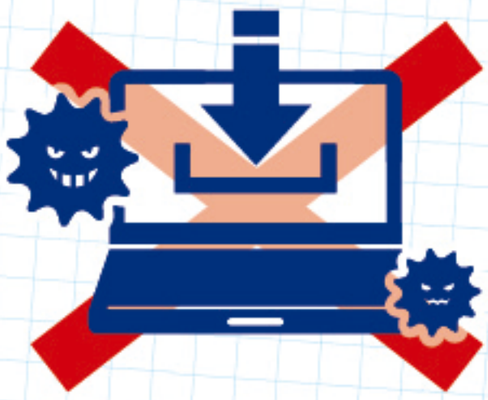
You should install security software (antivirus software) on your computer or mobile device, and keep its pattern file up to date.

E-mail

You should consider the risk of infecting your computer with malware or phishing when you click an attached file or link in an e-mail.

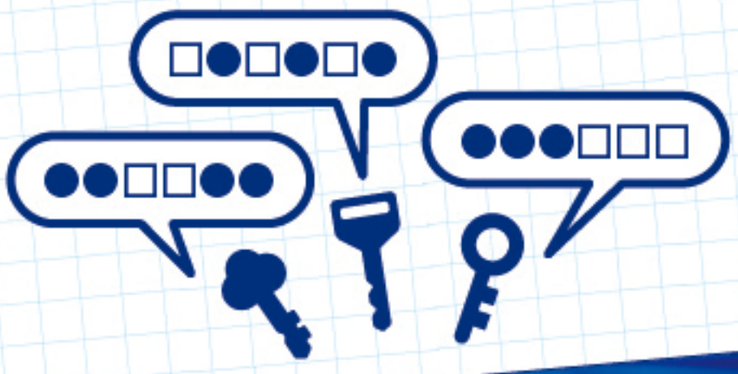
Software installation

You may not install software whose author or source is unknown.



Password

You may not use the same password for different computer systems and services, and never leak your passwords to others.



Lost and Stolen

You should never leave your computer, USB memory stick or other devices unattended. Protect them from theft.

2304

Inquiry counter

Tottori University Computer Security Incident Response Team (TU-CSIRT)

Find out more

https://kb.oism.tottori-u.ac.jp/security/

E-Mail ／ csirt@tottori-u.ac.jp