Response examples by type of information incident

This section explains the appropriate response to take according to the type of information incident. Incidents which require a more rapid response are noted with the icon Initial Response. When an information incident occurs, carry out the initial response before contacting the Information Security Incident Emergency Contact Desk.

Responding to malware infections

Malware infections are a type of information incident which often go unnoticed by users and are instead discovered and pointed out by others. In some cases, such as ransomware, users directly realize the damage when a message demanding the payment of a ransom is displayed or their files become locked. The damage caused by a malware infection can rapidly spread and has a significant scope of impact, so quickly take the following actions.

Response

1 Disconnect from the network Initial Response

Remote operation, unauthorized transfers of money to online banks, external cyber attacks, proliferation to peripheral devices, and other forms of secondary damage spread through the network. Therefore, to prevent the damage from spreading, disconnect the infected device from the network by unplugging the LAN cable for a wired connection and turning off the physical switch (or turning off the OS settings if there is no switch) for the wireless LAN (Wi-Fi) for a wireless connection.

2 Backups

The information stored on an infected device may be infected by the malware, so caution is required when handling such information. If you must make a backup of the information, backup the data to external media.

3 Recovering an infected device

To use an infected device once again, perform a clean install of the OS or restore the device to the factory settings before use.

Responding to ID and password theft

Even if unauthorized access occurs as a result of ID and password theft, in many cases the users do not realize what has happened. Depending on the service, the theft may become apparent through change notification emails that they know nothing about, unauthorized login warning notifications, and by checking the login history. In some cases, a user may be contacted about a possible ID and password leak due to an information incident caused by another person.

If your ID and password are stolen, promptly take the following actions.

Response

1 Change your password Initial Response

Change your password so that the damage does not spread.

If your password has been changed and you cannot access the account, contact your system provider (Administrator) to ask for support.

2 Check the service settings

If your ID and password are stolen and an attacker fraudulently logs into your account, the service settings may be changed in a malicious way, so check the service settings.

If your university ID and password are stolen, check the email system and other service settings which use the university ID (in the case of the email system, the settings may be changed to forward messages to the attacker's email address).

Responding to mobile devices or external media loss, information missending and unintentional information sharing

If you lose a smartphone, notebook PC, or other mobile device and it is found by a malicious person, the personal information on the mobile device may be stolen or the person may gain unauthorized access to websites using IDs and passwords saved on the device.
If USB memory, an external hard disk drive, or other storage media is lost, there is also a risk that the information stored on the lost external media may be leaked.
Sending an email in error or publishing information due to incorrectly configuring the scope of sharing in online storage, etc. may also lead to an information leak.

Take the following actions for information incidents which involve the risks of such "information leaks."

Response

1 (For mobile devices) Delete the information or lock the device

Initial Response

If you configured the remote wipe feature as discussed in Countermeasures 7-1 "Take steps so that information is not accessed if a device is stolen or lost," run the feature right away.

Furthermore, if you lost a smartphone or other mobile device with a service subscription, contact the mobile carrier and consult with them about taking the following actions.

- Search for the general location
- Lock the device
- Temporarily suspend the line service

2 Check the stored information

Clarify the confidentiality of the stored information as well as the scope and extent of the impact if the information were leaked.

3 Report the occurrence of an information incident

If the device contained highly confidential information such as personal information, promptly notify all parties which may be affected by that information (faculty members should contact their supervisor).