English version follows.

2021 年 12 月 24 日

情報・システム研究機構
構成員各位

情報・システム研究機構
最高情報セキュリティ責任者（CISO）
椿　広計

年末年始休暇中における情報セキュリティ対策について
Information security measures during the New Year's holidays

各研究所・施設等構成員各位におかれては、日頃から情報セキュリティの確保について、御協力いただき有り難うございます。

長期休暇中は、業務システムの担当者や管理者、外部委託の業者等が長期に渡って不在になることが想定され、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったりするなど、情報セキュリティインシデント（以下「インシデント」という。）発生に気がつきにくく、発見が遅れる可能性があります。有事の際の対応において予期しない問題が生じることが懸念されます。

特に、新型コロナウィルス感染症への対応のための在宅勤務が年末年始休暇と重なり長期間出勤できないことも想定されます。

ついては、在宅勤務や休暇期間中及びその前後におけるインシデント発生の防止、インシデントの際の対応等について別紙の対策を実施してください。

【本件問い合わせ先】
本部事務部総務課情報基盤係
E-mail: rois_network@rois.ac.jp
TEL: 03-6402-6225

【機密性１情報】

別紙

在宅勤務時の対策

長期休暇への対応に加えて以下の対策を実施してください。

1. 在宅勤務に当たって

在宅勤務者は、お使いのテレワーク環境に関して所属先が定めた規程やルールをよく理解し、それに従ってください。

不明な点等がある場合は自分で判断せず、まずは所属先のシステム管理者等に相談をしてください。

規程やルールとあわせて、お使いのパソコン等に対して、修正プログラムの適用、セキュリティソフトの導入および定義ファイルの最新化、パスワードの適切な設定と管理、不審なメールに注意するなど、日常における情報セキュリティ対策[1]を実施してください。

2. 在宅勤務を始める前に

テレワークで使用するパソコン等は、できる限り他人と共有して使わないようにしてください。共有で使わざるを得ない場合は、業務用のユーザーアカウントを別途作成してください。

ウェブ会議のサービス等を新たに使い始める際は、事前にそのサービス等の初期設定の内容を確認してください。特にセキュリティ機能は積極的に活用してください。

3. 自宅ルータ

自宅のルータは、メーカーのサイトを確認のうえ、最新のファームウェアを適用（ソフトウェア更新）してください。

休暇前の対策

1. インシデント発生時における連絡・報告先の確認

各機関におけるインシデント発生時における連絡・報告先や対応手順等を確認してください。夜間、休日の対応についても念のため確認してください。

2. 機器やデータの持ち出しルールの確認と遵守

長期休暇中に所外での対応が必要となるなどパソコン等の機器やデータ等の情報を持ち出す場合は、各機関の持ち出しルールを事前に確認し遵守してください。

3. 所内ネットワークへの機器接続ルールの確認と遵守

ウイルス感染したパソコンや外部媒体等を所内ネットワークに接続することで、ウイ

---

[1] 日常における情報セキュリティ対策
https://www.ipa.go.jp/security/measures/everyday.html#section3
（2019 年 4 月 2 日、独立行政法人情報処理推進機構セキュリティセンター）

ルスをネットワーク内に拡散してしまう恐れがあります。長期休暇中に、所内ネットワークへ機器を接続する予定がある場合は、各機関の機器接続ルールを事前に確認し遵守してください。

4. パスワード使い回しの確認

業務で使用している ID やパスワードを他の私的な利用を含めた Web サービスでも使い回していないか再度確認してください。使い回している場合には、速やかに業務で使用しているパスワードを各機関のルールに則って変更してください。

5. 使用しない機器の電源 OFF

長期休暇中に使用しない機器は電源を OFF にしてください。

休暇中の対策

1. 持ち出し機器やデータの厳重な管理

持ち出しルールに則り自宅等に持ち出したパソコン等の機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう、厳重に管理してください。

休暇明けの対策

1. 修正プログラムの適用

長期休暇中に Windows や Mac 等の OS（オペレーティングシステム）や MS Office、セキュリティソフトやブラウザ等の各種ソフトウェアの修正プログラムが公開されている場合があります。修正プログラムの有無を確認し、必要な修正プログラムを適用してください。なお、修正プログラムの適用については、システム管理者の指示に従ってください。

2. 定義ファイルの更新

長期休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイル（パターンファイル）が古い状態のままになっています。電子メールの送受信やウェブサイトの閲覧等を行う前に定義ファイルを更新し、最新の状態にしてください。さらに、ハードディスクのフルスキャンも実行してください。

3. 持ち出し機器のウイルスチェック

持ち出しルールに則り長期休暇中に持ち出していたパソコンや、データを保存していた USB メモリ等の外部記憶媒体にウイルスが感染していないか、所内で利用する前にセキュリティソフトでウイルススキャンを行ってください。

4. フィッシングメールに注意

Amazon、メルカリ、三井住友カード、楽天、ETC 利用照会サービス等を騙るフィッシングメールが増えています。記載されている URL にアクセスすると本物そっくりな偽サ

イトに誘導され、利用しているサービスのアカウント情報（ID／パスワード）の入力や、偽アプリケーションのインストールが求められ、これらを実行して、アカウントを窃取されたり、サービスを乗っ取られるという被害が発生しています。

　これらのメッセージには十分な注意を払い、不審と思われるメッセージが届いた場合は、記載されている URL を開いたり、アカウント情報や個人情報等を入力したりしないでください。

【参考】

○　年末年始における情報セキュリティに関する注意喚起
https://www.ipa.go.jp/security/topics/alert20211216.html
（2021 年 12 月 16 日、独立行政法人情報処理推進機構セキュリティセンター）

○　テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html
（2021 年 7 月 20 日更新、独立行政法人情報処理推進機構セキュリティセンター）

○　夏季休暇等に伴うセキュリティ上の留意点について
https://www.nisc.go.jp/active/infra/pdf/summer20210721.pdf
（2021 年 7 月 21 日、内閣サイバーセキュリティセンター）

○　長期休暇に備えて 2020/04(情報更新)
https://www.jpcert.or.jp/newsflash/2020041401.html
（2020 年 4 月 16 日、一般社団法人 JPCERT コーディネーションセンター）

○　Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends
https://www.cisa.gov/uscert/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats
(2021 年 11 月 22 日、米国 CISA)

December 24th, 2021

To all the staff members

Research Organization of Information and Systems
Chief Information Security Officer（CISO）
Hiroe Tsubaki

Information security measures during the New Year’s holidays

I would like to show my gratitude to all the staff members at each research institute and facility and so on for your continuous cooperation for ensuring information security.

As it is assumed that during the long vacation, persons in charge of the business system, administrators and outsourced business operators will be absent over a long period time, the occurrence of information security incidents (hereinafter called “incidents”) may be hard to notice and their discoveries may be delayed, including delays in dealing with the occurrence of computer virus infection and unauthorized accesses.

When responding to an emergency, it is feared that unexpected problems may occur.

In particular, there will be New Year's holidays while working from home due to COVID-19 measures, and it is assumed that you will not be able to come to work for a long period of time.

That being so, regarding the prevention of the occurrence of the incidents and the measures to be taken in time of incidents, before, during, and after working from home and the vacation, carry out the measures described in the attached document.

【Contact】
Information Technology Section,
General Affairs Division,
Central Administration Department
E-mail: rois_network@rois.ac.jp
TEL: 03-6402-6225

[Confidentiality 1]

Attachment

Measures for working from home

In addition to dealing with the long vacation, carry out the following measures.

1. For working from home

   People working from home should understand the regulations and rules regarding your telework environment stipulated by your department and follow them.

   If you have questions or concerns, do not judge by yourself but contact the system administrators and the like of your department.

   Along with regulations and rules, implement everyday information security measures[2] for your PCs such as applying correction programs, introducing security software, updating definition files, setting and managing passwords properly, looking out for suspicious e-mails, and so on.

2. Before starting working from home

   Do not share the PC and the like that you use for teleworking with others as much as possible. If you have no other choice, create a user account for business use separately.

   In newly starting to use services of online meetings, confirm the contents of the initial setting of the services in advance. In particular, actively utilize the security functions.

3. Router for domestic use

   Regarding a router for domestic use, confirm the website of the manufacturer and applythe updated firmware (update software).

Measures before the holiday

1. Confirmation of contact and reporting addresses in time of incidents

   Confirm contact and reporting addresses and corresponding procedures in time of incidents of each institution. Confirm how to respond during the nighttime and holiday Just in case.

2. Confirmation and observance of the take-out rules of devices and data

   In case you take devices including a PC and information of data outside the workplace for necessary responses during the long holiday, confirm the take-out rules of each institution and observe them.

3. Confirmation and observance of the device connection rules for the in-house network

   There is a risk of spreading computer viruses in the network by connecting a PC or external media infected by computer viruses to the in-house network. In case you are planning to connect devices to the in-house network during the long holiday, confirm the device connection rules of each institution in advance and observe them.

4. Confirmation of your passwords

---

[2] 日常における情報セキュリティ対策（in Japanese）

https://www.ipa.go.jp/security/measures/everyday.html#section3
（2019 年 4 月 2 日、独立行政法人情報処理推進機構セキュリティセンター）

Confirm again your ID and password used for your business to see whether or not you are using the same one for Web services including other private uses. If so, change the ID and/or password you are using for business immediately in accordance with the rules of each institution.

5. Shut off the power of the devices when not in use

   Shut off the power of the devices when not in use during the long holiday.

Measures during the holiday

1. Strict management of take-out devices and data

   Strictly manage the devices such as a PC and data taken out to your house and so on in accordance with the take-out rules in order to prevent damages such as information leak and so on by virus infection, loss, theft, etc.

Measures after the holiday

1. Application of correction programs

   During the long holiday, there may be cases where correction programs of software such as the operating systems (OS) of Windows and Mac, MS Office, security software, and browsers have been released.

   Make sure if there are correction programs and, if any, apply necessary correction programs. Regarding the application of correction programs, follow the instructions of system managers.

2. Updating of definition files

   Definition files (Pattern files) of security software of PCs whose power was off during the long holiday remain old. Update the definition files before sending and receiving e-mails and browsing websites. Also, do a full scan of hard disks.

3. Virus check for take-out devices

   With security software, run a virus scan program for PCs and external storage media such as USB memory taken out during the long holiday in accordance with the take-out rules to see if they are infected by viruses before using them in-house.

4. Beware of phishing e-mails

   There has been an increase in the number of phishing e-mails from companies such as Amazon, Mercari, Sumitomo Mitsui Card, Rakuten, and ETC inquiry service. If you access the URL, you will be directed to a fake website that looks just like the real one, and you will be asked to enter your account information (ID and password) or install a fake application, resulting in theft of your account or hijacking of your services.

   Be careful of these messages, and if you receive a message that seems suspicious, do not open the URL or enter your account information or personal information.

Thank you.

【Reference】

○ 年末年始における情報セキュリティに関する注意喚起（in Japanese）
https://www.ipa.go.jp/security/topics/alert20211216.html
（2021 年 12 月 16 日、独立行政法人情報処理推進機構セキュリティセンター）

○ テレワークを行う際のセキュリティ上の注意事項（in Japanese）
https://www.ipa.go.jp/security/announce/telework.html
（2021 年 7 月 20 日更新、独立行政法人情報処理推進機構セキュリティセンター）

○ 夏季休暇等に伴うセキュリティ上の留意点について（in Japanese）
https://www.nisc.go.jp/active/infra/pdf/summer20210721.pdf
（2021 年 7 月 21 日、内閣サイバーセキュリティセンター）

○ 長期休暇に備えて 2020/04(情報更新) （in Japanese）
https://www.jpcert.or.jp/newsflash/2020041401.html
（2020 年 4 月 16 日、一般社団法人 JPCERT コーディネーションセンター）

○ Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends
https://www.cisa.gov/uscert/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats
(2021 年 11 月 22 日、米国 CISA)