事　務　連　絡
平成２９年　７月２０日

各部局長
事務局各課(室)長 殿
監査室長

情報統括本部長
安浦　寛人

夏季休暇中のインターネット等の利用について（通知）

平素より情報セキュリティの維持につきましては，ご協力いただき御礼申し上げます。
さて，夏季休暇中は通常時とは異なり，管理者不在による異常事態の発見や対処の遅れなどにより，被害が拡大する危険性がございます。今年度は，平成２９年８月１１日（金・祝）から８月１６日（水）まで夏季における業務の一斉休止となり，さらなる注意が必要です。
つきましては，特に以下の点にご注意され，万一問題が発生した場合は，速やかに情報統括本部九大 CSIRT にご連絡くださいますようお願い致します。早期にご連絡いただければ，未然に防げる二次的なトラブルもございますのでよろしくお願い致します。
なお，御家庭におかれましても，パソコンやインターネット等を利用される場合は，職場同様にセキュリティやコンプライアンスに注意され，楽しいはずの休暇が台無しにならないようご注意下さい。

１）休暇中に使用されないパソコン，サーバ，プリンタ，複合機，TV 会議システム等につきましては，電源を必ず切断されますようお願い致します。(節電のためにもご協力をお願い致します。)
なお，休暇明けに作業を開始する時にソフトウェアのアップデートやウイルス対策ソフトウェアのパターンファイルを最新版に更新して下さい。

２）パソコンやスマートフォンの盗難や紛失，及び個人情報等の漏洩にご注意下さい。大学の費用で購入したパソコンやスマートフォン並びに情報の学外への持ち出しは，九州大学や各部局の規程・規則に従って下さい。また，許可を得て持ち出す場合も，パソコン等の内部に保存された情報や使用・作成した情報の漏洩に十分注意して下さい。パソコンであれば，OS の提供する機能(BitLocker 等)を用いて内蔵ドライブを完全に暗号化しておいて下さい。

３）不審メールにご注意下さい。最近のウイルスは、ウイルスチェックで検知されません。メールサブジェクトが「写真」「請求書」などになっている場合でも添付ファイルをすぐに開いたり、URL をクリックせずに，送信元や URL のアドレスなどをよくご確認下さい。特に zip ファイルが添付されている場合は十分に注意して下さい。また，判断がつかない場合は，情報統括本部に御相談下さい。

４）Twitter や Facebook などの SNS への不適切あるいは過度な書き込みにご留意ください。SNS の匿名性に乗じて普段はしないような発言を行った結果，その反動で大学に問い合わせをされたり，自身のプライバシーが不特定多数に公開されたりする事例もあるようです。なお，ほとんどの SNS では，発言者を特定することは可能です。

５）インターネット上での著作権にご留意下さい。インターネットには，著作権を守られるべき，音楽や映画等の情報コンテンツが不法に流通しています。それらの不法コンテンツをインターネット利用により入手し利用することもまた不法であり，行ってはいけません。

６）その他，情報セキュリティ上の問題が発生した場合は，本学の情報セキュリティポリシーに従い，情報統括本部において該当する機器をネットワークから切り離すなどの措置を行ないますのでご了承下さい。

・長期休暇向け情報セキュリティ対策の参考
https://www.ipa.go.jp/security/measures/vacation.html（情報処理推進機構）
http://www.microsoft.com/ja-jp/security/pc-security/vacation.aspx（マイクロソフト）
https://imperia.trendmicro-europe.com/jp/threat/preventing_intrusions/holidays/index.html
（トレンドマイクロ）

≪情報統括本部・九大 CSIRT　連絡先≫
電話（平日時間内）　：092-802-2617
E-mail：sec-incident@iii.kyushu-u.ac.jp
≪情報セキュリティインシデントが生じた場合の連絡・処理フロー≫
https://www.sec.kyushu-u.ac.jp/sec/sec-incident.html

情報統括本部　九大 CSIRT　内線：伊都(90)−2696, 2685, 2686, 2687
E-mail: sec-incident@iii.kyushu-u.ac.jp

July 20,2017

Reminder for computer security in this holiday season

Please pay more attention to your computer security in holiday seasons. In addition, security incidents might get serious due to delays in incident detection and response. Please report to CSIRT as soon as humanly possible if you have any security incident during your vacation.

Guidelines:

1. Make sure to shut down your computers, printers, and electronic devices in your office which you don't use during your vacation. You need to apply security updates for your operating system, applications, and antivirus software firstly after the holiday season.

2. Be particularly wary about loss or theft of your electronic devices and information leakage. Follow applicable regulations when you take out university computers and private data from the university. Please encrypt full disks of the carry-out computers by means of BitLocker and so on.

3. Take extra care about phishing and other suspicious e-mail. DO NOT CLICK on any link without a careful check of the destination URL. DO NOT OPEN suspicious attachments, especially ZIP files. Note that many latest malware can evade detection by anti-virus programs. Please ask to Information Infrastructure Initiative if you can't verify them.

4. Do not post with inappropriate contents on SNS. The university has received some inquiries about posts on SNS.

5. Do not violate copyright. Downloading or sharing infringing contents is a crime.

Reference Links

・Information-technology Promotion Agency, Japan（IPA）
http://www.ipa.go.jp/security/english/index.html

Information Infrastructure Initiative,Kyudai CSIRT
E-mail:sec-incident@iii.kyushu-u.ac.jp