平成30年度
情報セキュリティ自己診断

回答まとめ（2019.4）

実施日：2019/2/22～3/15

回答数：90人　**回答割合**17.48%

（役職員数　2019/2/28**現在：**515**人）**

（※監事、学生、非常勤講師、休職者除く）

■ お互いのアドレスを知らない複数の人へメールを送る場合、次のどの方法で送信することが適切ですか？

回答	回答率	回答数
正解 **受信者をBCC、TOには送信者自身**	**97.78%**	**88**
受信者をCC、TOには送信者自身	2.22%	2
受信者をTOにすべて入れて送信	0.00%	0
合計	100.00%	90

この場合、TOやCCに受信者を入れることは、不要な情報提示となり情報漏えいに繋がりかねません。また、受信者が返信をする場合も、誤送信を引き起こす原因となりますので、この方法での送信はやめましょう。

■ URLの先頭に記載されている「http://」と「https://」の説明で、正しいものは次のうちのどれですか？

回答	回答率	回答数
正解 **HTTPSは、認証局から発行された証明書を設定し通信を暗号化しているが、証明書を発行した認証局等が実在しているものとは限らない。**	**80.00%**	**72**
HTTPSは、認証局から発行された証明書を設定し通信を暗号化しているので、安全なサイトしか存在しない。	20.00%	18
HTTP及びHTTPSの通信は、両方とも暗号化されているので安全である。	0.00%	0
合計	100.00%	90

詐欺サイトや偽サイトでもHTTPSを利用している場合があります。不審に感じたら証明書の内容を確認し、実在する団体であるかを確認することも重要です。

■ 次のうち、一般的にマルウェアではないものはどれでしょうか？

回答	回答率	回答数
コインマイナー	**35.56%**	**32**
ボット	32.22%	29
キーロガー	18.89%	17
スパイウェア	6.67%	6
ランサムウェア	6.67%	6
合計	100.00%	90

「コインマイナー」を無許可で設置することは違法となる可能性がありますが、コインマイナー自体はマルウェアではありません。
キーロガー：感染したデバイスのキーボードで入力したデータをロギングするもの
ボット：第三者に端末を自由に使われてしまう悪意のあるプログラム
スパイウェア：感染したデバイスの個人情報やアクセス履歴などの情報を収集するプログラム
ランサムウェア：感染したデバイスのデータを暗号化し、復号化するために金銭を要求するプログラム

■【数字＋アルファベットの大文字／小文字】で8桁のパスワードを構成した場合、組合せはどのくらいになりますか？

回答	回答率	回答数
約218兆通り	**74.44%**	**67**
約2兆通り	16.67%	15
約21兆通り	8.89%	8
合計	100.00%	90

正解

約218兆通りの組合せとなります。最低でもこの位のボリュームを確保し、かつ一般的な単語や文字列が連想できにくい構成だとパスワードの強度が高くなります。

■ 情報漏えいへの対策として「不適切」なものは次のうちどれでしょうか？

回答	回答率	回答数
正解 **デバイスへのログインIDと、重要な情報へアクセスするためのログインIDを同じものに設定する**	**90.00%**	**81**
重要な情報をクラウドストレージに保存し、ローカルディスクに残さない	4.44%	4
リモート操作で、デバイスのロックや保存データの消去ができるよう設定する	3.33%	3
重要な情報をセキュアな外付けデバイスに保存する	2.22%	2
セキュリティソフトを導入する	0.00%	0
合計	100.00%	90

デバイスのログインID（パスワード含む）と重要な情報へアクセスするためのログインIDを同じにすると、デバイスにログインされただけで重要な情報までたどれてしまう可能性が非常に高くなります。ログインに使用するIDは、目的別に異なるものに設定し、セキュリティ強度を高めるようにしましょう。

■ Windows PCで、スクリーンをロックする場合のショートカットキーは次のうちどれでしょうか？

回答	回答率	回答数
Windowsキー　＋　L	**76.67%**	**69**
Ctrlキー　＋　L	15.56%	14
Fnキー　＋　L	7.78%	7
合計	100.00%	90

正解

PCからアクセスできる情報を第三者から保護するためにも、離席する際はロックすることを習慣づけましょう。

■ MacOS PCでスクリーンをスリープ（ロック）状態にさせる場合のショートカットキーは次のうちどれでしょうか？（事前にシステム環境設定の『セキュリティとプライバシー』で、『スリープ解除／スクリーンセーバー解除にパスワードを要求』に設定する必要があります。）

回答	回答率	回答数
commandキー　+　shiftキー　+　L	38.89%	35
正解 **controlキー　+　shiftキー　+　電源ボタン**	**37.78%**	**34**
shiftキー　+　commandキー　+　Q	23.33%	21
合計	100.00%	90

PCからアクセスできる情報を第三者から保護するためにも、離席する際はロックすることを習慣づけましょう。電源ボタンは最後に押すタイミングで入力すると、コマンドが正しく実行できます。

■ 学内LANに接続するPCのセキュリティ対策として一番適切なものはどれでしょうか？

回答	回答率	回答数
f）eに加え、OSのアップデートを行い、最新状態に保つ。	**86.67%**	**78**
e）大学やセキュリティ対策企業が提供している有償のセキュリティソフトウェアを稼働させる	8.89%	8
b）aに加え、OSのアップデートを行い、最新状態に保つ。	2.22%	2
d）cに加え、OSのアップデートを行い、最新状態に保つ。	2.22%	2
c）セキュリティ対策企業が提供している無償のセキュリティソフトウェアを稼働させる	0.00%	0
a）OS等に標準で入っているセキュリティソフトウェアのみを稼働させる	0.00%	0
合計	100.00%	90

正解

OSに標準で入っているものや無償で利用できるセキュリティソフトは、検出・保護機能はあっても検疫機能がないものやランサムウェアには対応していないもの等、セキュリティ機能が制限されている場合があります。情報処理センターから配付されているセキュリティソフトや有償で製品化されているセキュリティソフトを導入することを推奨します。

■ 無線LANルータの管理画面にログインするための認証用ID/パスワードは、セキュリティの観点から変更しない方が良いでしょうか？

回答	回答率	回答数
いいえ	**100.00%**	**90**
はい	0.00%	0
合計	100.00%	90

正解

このような認証用IDは初期値が一律で決まっている場合があり、そのまま使用していると第三者に使用される危険性が非常に高いです。
不正な使用、意図しない使用を防止するためにも初期値から変更しましょう。

■ 公衆無線LANを利用する場合、適切な方法はどれでしょうか？

回答	回答率	回答数
通信が暗号化されていても、暗号化キーが公開されている場合、通信内容を盗聴し復号化される恐れがあるので使用には注意する	**100.00%**	**90**
デバイスに入っているアプリケーションだけ使用する	0.00%	0
そのまま接続する	0.00%	0
合計	100.00%	90

正解

公衆無線LANは、接続するための暗号化キーを公表しているケースが多く見受けられます。
この暗号化キーを悪用すると、暗号化された通信を盗聴し復号化できてしまいます。
このような公衆無線LAN環境は極力使用しないことを推奨します。

■ 今年度自己診断に関するまとめ

昨年度に引き続き、今年度も情報セキュリティ自己診断を実施しました。

今年度の診断結果で目立った点としては、「無線LANルータの管理画面にログインするためのID/パスワードは、セキュリティの観点から変更しない方が良いでしょうか？」？という設問について、回答者全員が正解の「いいえ」を回答した点です。実際に学内で無線LANルータを運用する場合にも、管理用ID/パスワードの変更を実践していただきたいと思います。

次に、「公衆無線LANを利用する場合、適切な方法はどれでしょうか？」という設問についても、回答者全員が正解の「通信が暗号化されていても、暗号化キーが公開されている場合、通信内容を盗聴し復号化される恐れがあるので使用には注意する」を回答した点です。学外でも業務のために無線LANを利用する機会があるかと思いますが、特に暗号化キーが公開されているような公衆無線LANについては、極力利用を控えるようにしていただきたいと思います。

情報セキュリティに関しまして、引き続き御協力をよろしくお願いいたします。

学内専用　情報セキュリティのページ：
https://www.nagaokaut.ac.jp/gakunai/designated/security-top/security-top.html