平成29年度
情報セキュリティに関する自己診断結果

回答まとめ（2018.3）

実施日：2018/2/9～3/7

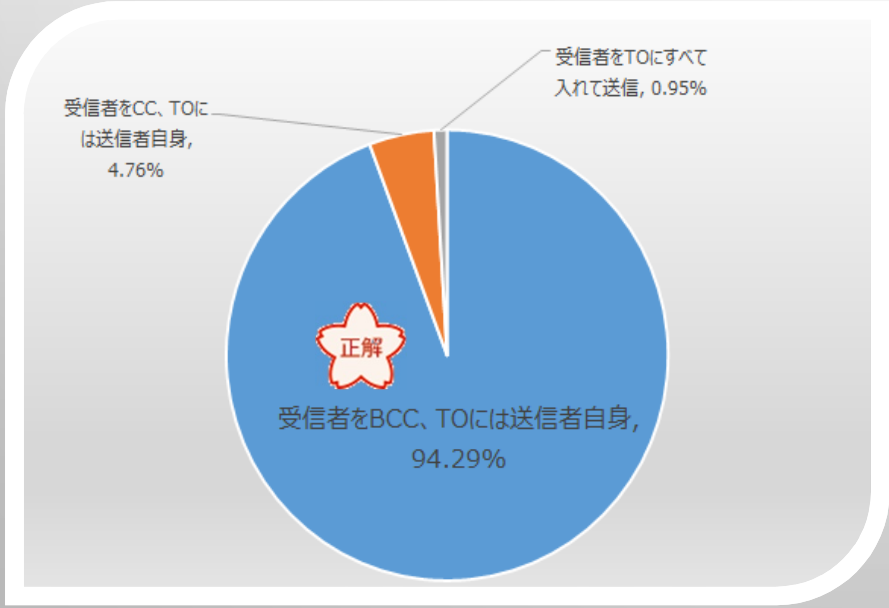
回答数：105人　回答割合19.8%

（役職員数　2/28現在：531人）

（※学生、非常勤講師除く）

1. 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？

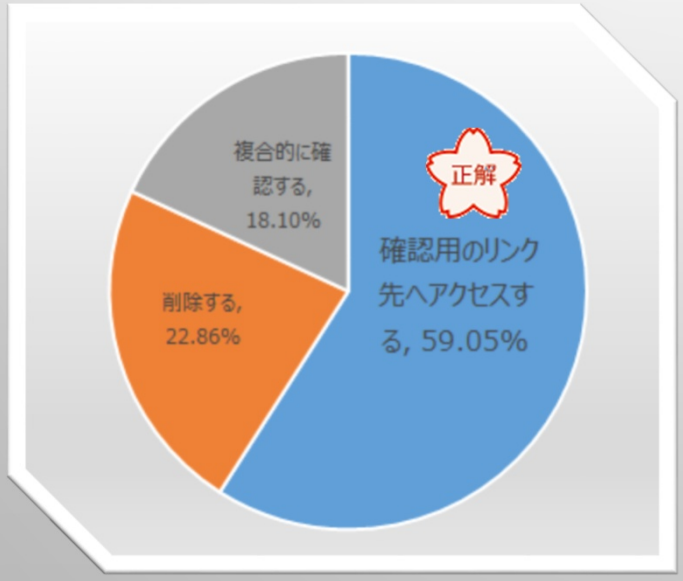
Answer Choices	Responses	
正解 受信者をBCC（ブラインドカーボンコピー）に入れ、TO（あて先）には送信者自身のアドレスを入れて送信する	94.29%	99
受信者をCC（カーボンコピー）に入れ、TO（あて先）には送信者自身のアドレスを入れて送信する	4.76%	5
受信者をTO（あて先）にすべて入れて送信する	0.95%	1
	Answered	**105**
	Skipped	**0**



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。

2. 件名や本文に心当たりのないメールが届きました。大手通販サイトの引き落としに関する具体的な内容が書かれていて、確認用のリンク先（URL）が示されていました。このようなメールを受信した場合の対応方法として不適切なものはどれですか？

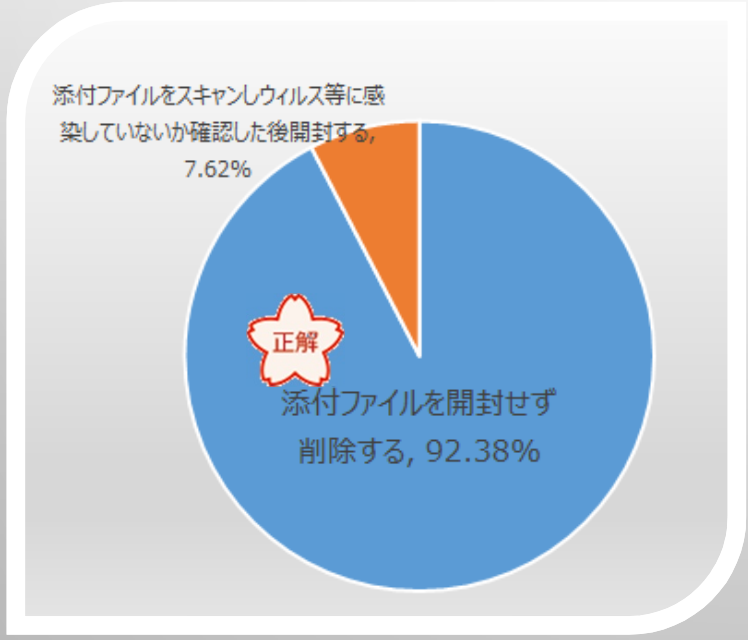
Answer Choices	Responses	
正解 確認用のリンク先へアクセスする	59.05%	62
削除する	22.86%	24
メールのヘッダー情報等を見て正しい送信者からのものか確認する、周囲の人に同様のメールが届いていないか確認する、送信元の通販サイトに不審なメールについてのお知らせが出ていないか確認する等複合的に確認する	18.10%	19
	Answered	**105**
	Skipped	**0**



標的型サイバー攻撃の多くは、このようなメールを起点に発生します。現在は、企業から配信される引き落としやアカウント管理に関するメール等を巧妙に作成し、一見しただけでは見分けが付かない程になっています。このような不審メールは、確認用のリンク先にアクセスするとマルウェアに感染する恐れがありますので、絶対にアクセスしないでください。

3. 添付ファイル付きのメールが届きました。件名や本文に心当たりはありませんが、このような不審なメールを受信した場合、適切な対応方法は次のうちどれでしょうか？

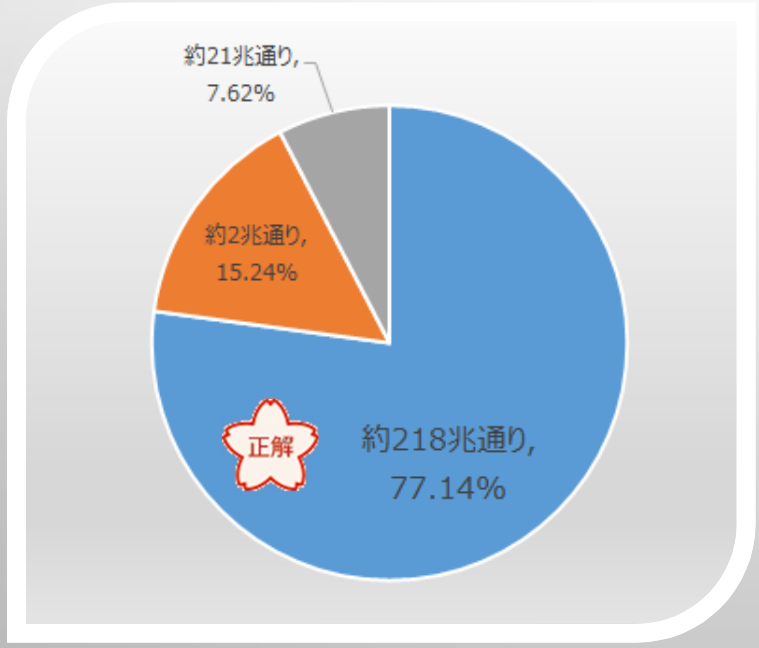
Answer Choices	Responses	
正解 添付ファイルを開封せず削除する	92.38%	97
添付ファイルをスキャンしウィルス等に感染していないか確認した後開封する	7.62%	8
添付ファイルを開封して確認する	0.00%	0
	Answered	**105**
	Skipped	**0**



不審なメールに添付されているファイルは開封せずに削除しましょう。スキャンをかけてウィルスが検出されなくても、未知のウィルスに感染している可能性もありますので、スキャンをかけたからと言って安心はできません。

4.【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？

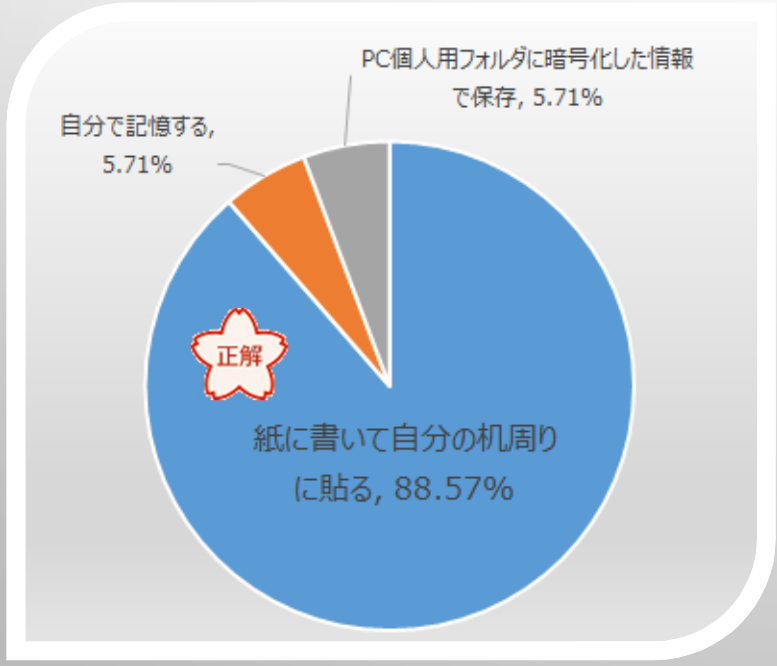
Answer Choices	Responses	
正解 約218兆通り	77.14%	81
約2兆通り	15.24%	16
約21兆通り	7.62%	8
	Answered	**105**
	Skipped	**0**



約218兆どお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。

5. 個人で使用するパスワードの保存方法として、不適切な方法は次のうちどれでしょうか？

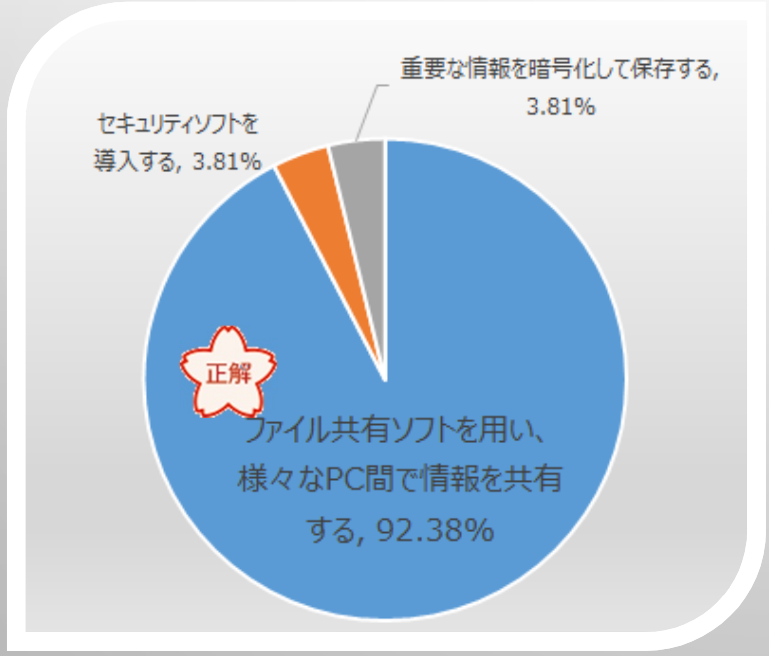
Answer Choices	Responses	
正解 紙に書いて自分の机周りに貼り付けておく	88.57%	93
自分で記憶する	5.71%	6
PC内の個人用のフォルダに暗号化した情報で保存する	5.71%	6
	Answered	**105**
	Skipped	**0**



個人で使用するパスワードは第三者の目に触れない形で保存しておくことが重要です。個人用のフォルダにパスワードを記録した情報を保存しても、不正アクセスによって第三者に盗み見られる恐れがあるので、この場合は暗号化して保存しましょう。

6. 情報が漏えいしないために日頃から注意すべき行動として、不適切なものは次のうちどれでしょうか？

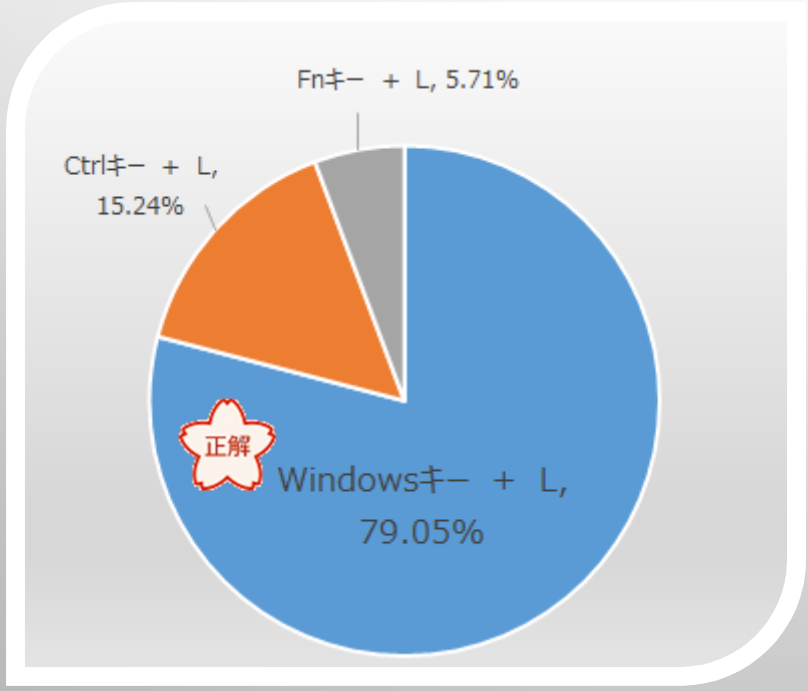
Answer Choices	Responses	
正解 ファイル共有ソフトを用い、様々なPC間で情報を共有する	92.38%	97
セキュリティソフトを導入する	3.81%	4
重要な情報を暗号化して保存する	3.81%	4
	Answered	**105**
	Skipped	**0**



ファイル共有ソフトを使用して不特定多数のPCとファイルの共有・交換を行うと、利用者の操作ミスや設定の誤り、ウィルス感染等により情報漏えいの危険が高まります。

7. 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？

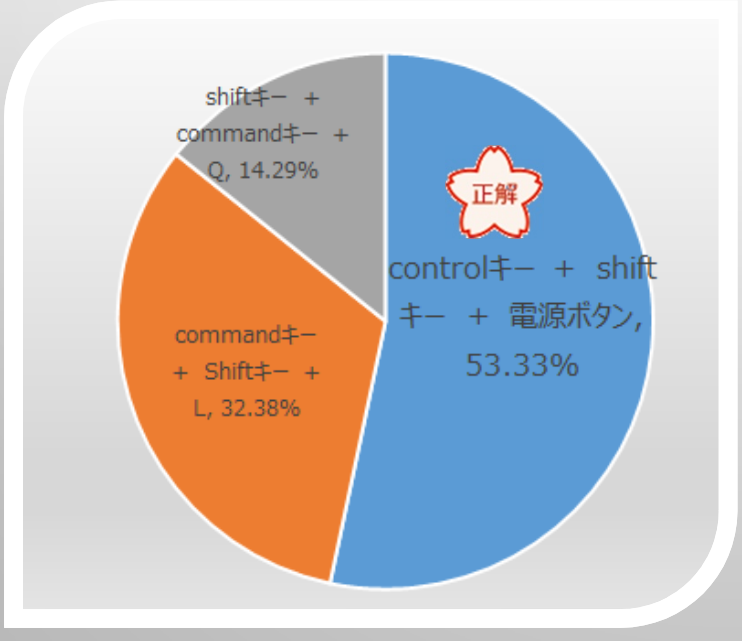
	Answer Choices	Responses	
正解	Windowsキー ＋ L	79.05%	83
	Ctrlキー ＋ L	15.24%	16
	Fnキー ＋ L	5.71%	6
		Answered	**105**
		Skipped	**0**



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。

8. Mac OS 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？（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。）

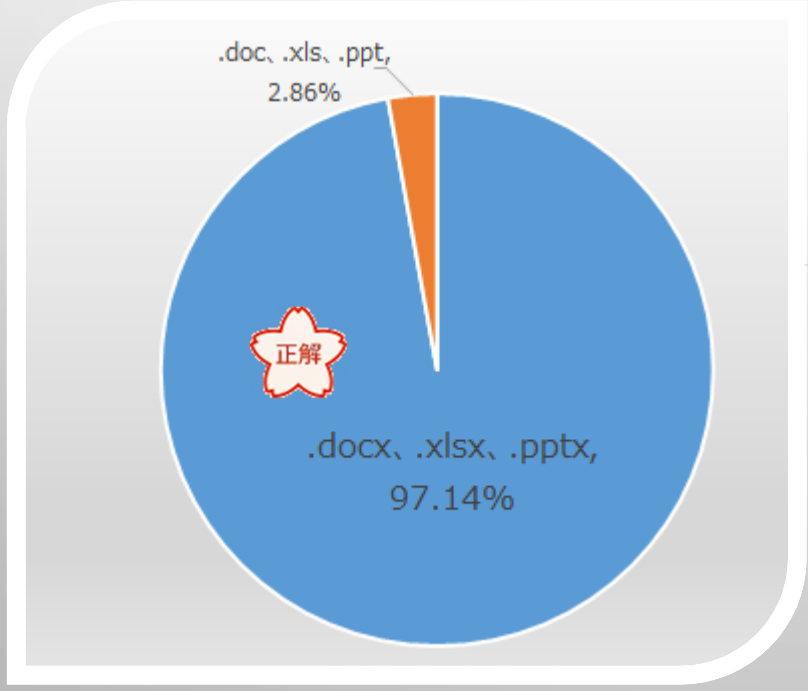
Answer Choices	Responses	
正解 controlキー ＋ shiftキー ＋ 電源ボタン	53.33%	56
commandキー ＋ Shiftキー ＋ L	32.38%	34
shiftキー ＋ commandキー ＋ Q	14.29%	15
	Answered	**105**
	Skipped	**0**



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。

9. Microsoft Office最新版で使用される拡張子で正しいものはどれでしょうか？

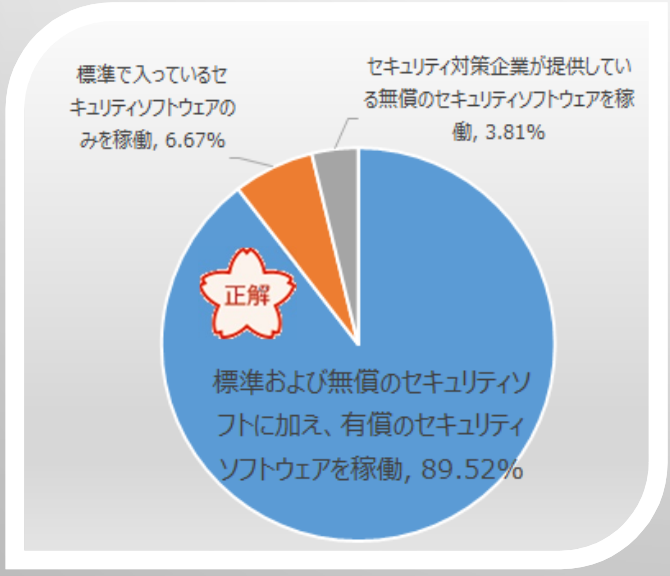
Answer Choices	Responses	
正解 .docx、.xlsx、.pptx	97.14%	102
.doc、.xls、.ppt	2.86%	3
.odt、.ods、.odp	0.00%	0
	Answered	**105**
	Skipped	**0**



MS Office 2007以降、新しいファイル形式（XML形式）になっています。セキュリティの面でも機能が改善されていますので、最新のファイル形式で運用してください。

10.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？

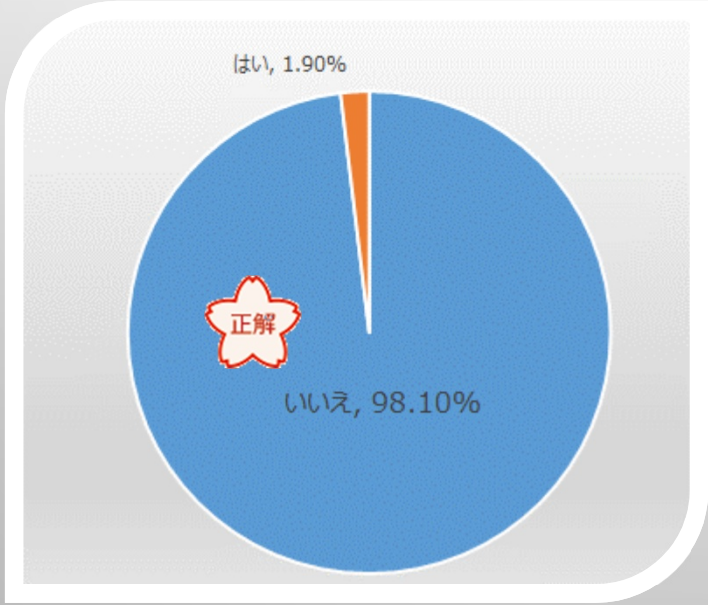
Answer Choices	Responses	
正解 上記に加え、セキュリティ対策企業が提供している有償のセキュリティソフトウェアを稼働させる	89.52%	94
OS等に標準で入っているセキュリティソフトウェアのみを稼働させる	6.67%	7
セキュリティ対策企業が提供している無償のセキュリティソフトウェアを稼働させる	3.81%	4
	Answered	**105**
	Skipped	**0**



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。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。

11.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？

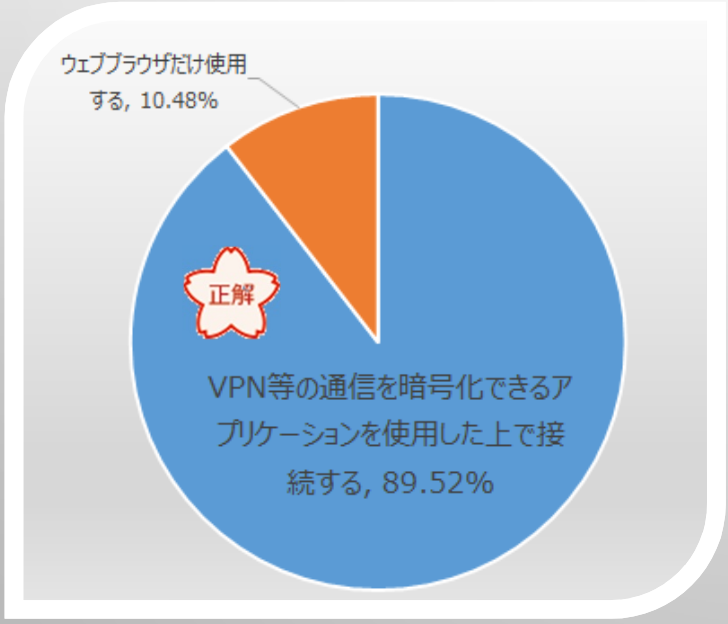
Answer Choices	Responses	
正解 いいえ	98.10%	103
はい	1.90%	2
	Answered	**105**
	Skipped	**0**



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高いです。不正使用を防止するためにも初期値から変更しましょう。

12.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？

Answer Choices	Responses	
正解 VPN等の通信を暗号化できるアプリケーションを使用した上で接続する	89.52%	94
ウェブブラウザだけ使用する	10.48%	11
そのまま接続する	0.00%	0
	Answered	**105**
	Skipped	**0**



公衆無線LANは、通信の暗号化等のセキュリティ対策が行われていない場合があり、第三者により通信情報を盗聴されることがあります。利用の際、特に個人情報が含まれる場合は、通信が暗号化されているか、Wi-Fiに接続しているデバイス同士が通信できないようになっているか等を確認してください。その上で必要に応じ、通信の暗号化ができるアプリケーション（VPNアプリ等）を使用する、ブラウザではURLが「https」で始まるサイトだけ利用する等の注意が必要です。