

パスワードの使用に関する意識調査

—— 定期的な変更に関する考察 ——

八 城 年 伸

A Consciousness Survey of the use of Passwords: A Study of Regular Change

Toshinobu YASHIRO

はじめに

ユーザ認証に用いられるパスワードは、受け取ったら速やかに変更する、定期的に変更する、他人に推測されにくいものにするなど、それらを支援するための様々な試みがなされてきた。しかしながら入学から間もない大学生を対象にパスワードに関する意識調査を行ったところ、自ら作成したパスワードは身近な記憶へ関連づけている傾向が見られた。このことは、頻繁な変更には耐えられない、多種多様なパスワードの作成と使い分けができない、他人から推測されやすいことを示している。こうした傾向が情報教育の程度に依存するものであるかを検討するために、異なるカリキュラムにより情報教育を受けたグループを加えて継続調査を行ってきた。

I. 調査に至る経緯と問題点の整理

パスワードは古くから定期的に変更するものであるとされており、それを支援するための様々な試みがなされてきた。Microsoft Windowsにおいて、システム管理者が定めた期間を経過してなおパスワードが変更されない場合に、強制的にパスワードを変更させるための仕組みが備わっているのは、その一端であると言える。

しかしながら定期的なパスワードの変更は、情報産業に従事する者であっても容易なものではない。マイクロソフトの情報システム部門であるMicrosoft IT Japanの荒瀬達也氏が「情報セキュリティ管理実践セミナー」において、8文字以上、有効期限70日、履歴を管理して循環使用を認めない、24時間以内の再変更は不可、という同社のパスワードに関するポリシーを明らかにした。その際に、パスワードのリセット依頼が社内ヘルプデスクへの問い合わせ上位10件に必ず入っているとされていたが、これもパスワードの定期的な変更が容易ではないことの一端を表していると言えよう¹⁾。

マイクロソフトのポリシーは厳し過ぎるケースであると思われるが、教育の現場においてもパ

1) 「多くの失敗を経験しながら改善を進めてきた…マイクロソフトが自社のセキュリティ対策を披露」,
(<http://itpro.nikkeibp.co.jp/article/NEWS/20080226/294794/>, 2008/2/26現在, 2009/09/14再確認)

パスワードを定期的に変更させる試みは古くから行われてきた。筆者の前任校である広島大学においても、90日間パスワードが変更されない場合に変更を促すメールが送信されるシステムが導入されていた²⁾。当時、部局の情報システム担当者であった筆者は、ユーザからの問い合わせやクレームに対処する立場にあったが、そこで目撃したユーザの行動はシステムの実効性を根底から揺るがすものであった。すなわち、システムにおいてパスワードの循環使用制限と再変更までの時間制限が設けられてなかったため、パスワード変更を2回繰り返すことで元のパスワードを使い続ける、変更は促されても強制力がないことが知れ渡ると無視をするユーザが増加していったなどである。また、変更したパスワードを忘れた、憶えられないためにメモをとるなど、パスワードを管理する上で好ましからぬ事態も散見されている。

後に安田女子大学・安田女子短期大学に転じたところ、前任校とは異なる幾つかの事象に気がついた。イントラネットに近い情報システム環境のためか、学生の情報セキュリティに関する意識が比較的希薄のように感じられたのである。パスワードに関する意識も同様で、情報科目においてはパソコンへのログイン情報を出席確認に用いる教員が多いことから、友人のパソコンまでログインを済ませる（＝代返を行う）グループが存在していた。友人同士におけるパスワードの教え合い行為は、代返という実利が見込める学内情報サービスに留まらず、就職情報サイトなどの学外サービスにも及んでおり、パスワードを忘れた際に思い出すためのヒントを友人に聞いていたケースも目撃した。

これらのことから筆者が導き出したのが、パスワードを直接教え合うには至らなくとも友人間で共有するレベルの情報を基にパスワードを作成しているケースが多いのではないかと、セキュアなパスワードを作成するには手法の教授が必要ではないかと、という仮説である。仮説の検証の手始めとして、情報の基礎科目においてパスワード作成ソフトを用いたパスワードの作成と変更方法の説明を行ったが、それに対する学生の反応は意外なものであった。代表的な意見としては「せっかく憶えたのだから変えたくない」というものである。

以上のことを踏まえて入学から間もない1年次生を対象に意識調査を行ったところ、自分で作成したパスワードは身近な事柄に結びつけて記憶しているために変更したくない、システム管理者が考えているほど重要なものとは認識していない、という傾向がうかがえる結果が得られている³⁾。この傾向が情報教育の程度に依存するものであるかを検討するために、異なるカリキュラムによる情報教育を受けたグループを加えて継続調査を行い、その結果を公表してきた⁴⁾⁵⁾。

過去の公表においては紙面や発表時間の制約もあり、継続的な調査に対する分析が手薄になっていたことは否めない。本稿においては、継続的な調査の部分において、パスワードを定期的かつ強制的に変更させられることへの意識について、更なる調査と分析を行うものである。

2) 岸場清悟他、「利用者パスワード変更促進手法と評価」、情報処理学会研究報告DSM 2001 (80), pp.57-61, 社団法人情報処理学会

3) 八城年伸、「パスワードに関する意識調査と考察」、平成18年度情報教育研究集会講演論文集, pp.588-591, 2006

4) 八城年伸、「パスワードに関する継続的な意識調査と考察」、平成19年度情報教育研究集会論文集, pp.463-466, 2007

5) 八城年伸、「パスワードに関する教育と意識調査」、平成20年度情報教育研究集会論文集, pp.37-40, 2008

II. 調査方法

調査においては、パスワードに関する基本的な認識や意識を調べるため、情報に関する専門教育を受けていない1年次生を主な対象とした。また、変化を調べるために同一の集団に対して継続調査も行っている。表1のG1～G4の記号が継続調査の各グループを示す。

表1) 調査の実施時期と対象学科・学年

	時期	回収率	有効 回答	有効 回答率	現ビ		短大		共通	
					対象	継続	対象	継続	対象	継続
第1回	2006年7月	92.4%	184	88.0%	1年	G1	1年	G3		
第2回	2007年1月	91.6%	194	96.4%	1年	G1	2年		1年	G4
第3回	2007年12月	92.4%	158	91.3%	1・2年	G1/G2	2年	G3	1年	G4
第4回	2008年7月	91.2%	292	96.9%	1～3年	G1/G2			1・2年	G4
第5回	2008年12月	84.3%	98	89.7%	1年				1年	G4
第6回	2009年1月	92.7%	89	N/A	1年				1年	G4

調査は八城が担当している講義において実施した。対象の学生のうち、安田女子大学現代ビジネス学部（現ビと略記）と安田女子短期大学秘書科（短大と略記）は、いずれも情報関連科目のウェイトが高い学科であるが、まったくの初心者から意識の高い学生まで混在している。安田女子大学の共通教育（共通と略記）においては習熟度別クラス編成となっているが、担当クラスの習熟度はまちまちであり、こちらも初心者から意識の高い学生まで混在している。以下の分析において、習熟度との関連性が認められる場合には、その旨を明記する。

調査項目については定期的な見直しを行っているが、見直し前後の調査と相互に比較が行えるよう、設問や選択肢を揃えるようにした。設問の中にはプライベートに関する事項と受け取られるものも含まれることから、単なる未回答と回答拒否とを区別するため、「この設問には回答したくない」という選択肢を設けた。各回における設問の違いについて、主だった点について表2にまとめる他、第3回の調査に用いた調査紙を本稿末尾に縮小添付する⁶⁾。

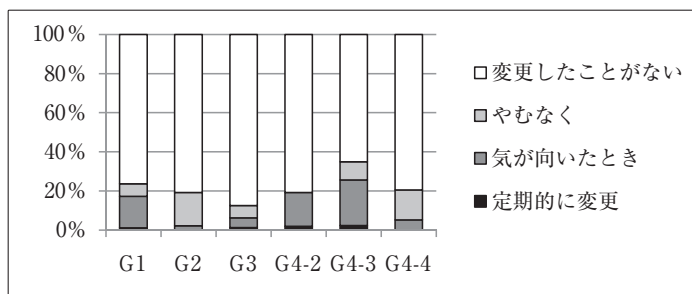
表2) 調査ごとの主な変更点

	設問数	直前回との変更点
第1回	6	
第2回	6	設問の順の見なおし、選択の少なかった選択肢の廃止
第3回	12	記憶に関する設問と、守ることのできるポリシーに関する設問の追加
第4回	12	第3回と同じ
第5回	14	記憶に関する設問の廃止と、パスワードの強度判定に関する設問の追加
第6回	14	第5回と同じ

6) 本来の調査紙は、A4版、横位置、両面刷りである。

Ⅲ. パスワード変更の有無と変更頻度

システム管理に携わる者であれば、パスワードを定期的に変更しているか否か、変更しないのであれば理由が何であるかは関心事である。電子メールや「mixi」などのネットワーク・サービス全般について、もっともよく変更するパスワードを対象として、パスワード変更の有無について尋ねた。継続調査を行ったG1～G4の各グループにおいて、初回の調査時におけるパスワード変更の有無をまとめたものがグラフ3である。G4のグループにおいては第2回目から第4回目の調査についてそれぞれ、G4-2のような枝番号を振ってある。



グラフ3) パスワードの変更の有無

パスワードを変更した経験がないとの回答は、もっとも多いG3のグループで87.5%、最も少ないG4-3のグループでも65.1%であった。「やむなく変更した」との回答は、授業等で半ば強制的に変更させられた、仮パスワード発行方式のサービスのために正式利用には変更することが必要であった、などが理由であり、実質的には変更したことがないと同列に扱っても差し支えないと考えられる。

G4-3は習熟度が「高」のグループであるが、グループごとの回答の傾向に有意差はなく、調査の時期においても回答の傾向に有意差はなかった。さらに学内情報サービスを利用するための初期パスワードを変更した経験についても尋ねた結果をまとめたのが表4である。

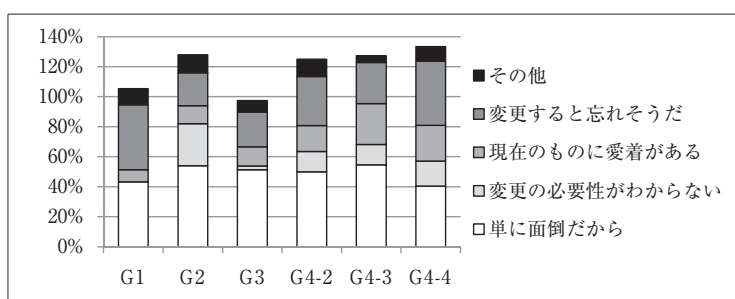
表4) 学内情報サービスのパスワード変更の有無

	G2	G4-3	G4-4
自分で変更した	1.9%	10.9%	0.0%
授業で変更した	1.9%	0.0%	11.9%
変更していない	96.3%	89.1%	88.1%

以上のことから、情報科目の習熟度の違い、情報教育に関するカリキュラムの違い、調査の実施時期の違い（前期と後期の授業の違い）セキュリティに関する意識の程度に関係なく、パスワードを変更する習慣や意識そのものがないと考えることができる。定期的に変更していると回答した場合でも、その頻度は毎月から年に2回までとまちまちであり、特に傾向はなかった。なお、回答の傾向に差異が見られないことから、第5回目以降の調査においては調査項目そのものを廃止した。

IV. パスワードを変更しない理由

パスワード変更の有無の設問に対し「定期的に変更してない」との回答に着目し、変更しない理由についてまとめたものがグラフ5である。複数回答可のため、合計は100%とはならない。第1回調査の対象であったG1とG3のグループの回答傾向と、それ以外のグループの回答傾向とは有意差があった。そこで、G1とG3以外のグループの複数回答の状況についてまとめたものが表6である。



グラフ5) パスワードを変更しない理由

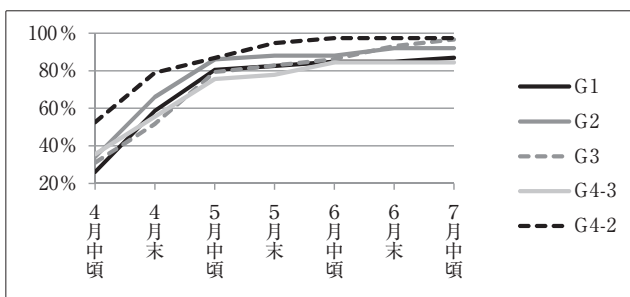
表6) 複数回答の状況

	G2	G4-2	G4-3	G4-4
単に面倒だから	40.0%	36.5%	40.9%	21.4%
面倒+愛着がある	2.0%	3.8%	6.8%	0.0%
面倒+忘れそう	2.0%	3.8%	9.1%	9.5%
面倒+愛着+忘れそう	2.0%	5.8%	2.3%	4.8%

「単に面倒だから」、「変更の必要性がわからない」、「変更方法を知らない」という単純な理由であれば、パスワード変更を促す施策が有効であると思われる。しかしながら、「単に面倒だから」を理由に挙げたのは設問に回答した学生の4割弱に過ぎず、それ以外の学生は別の理由、または複数の理由を挙げている。このことは、単に変更を促すだけでは不十分であり、ユーザが感じている不安を取り除かなければ効果が上がりにくいことを示唆していると考えられる。

V. パスワードの記憶に要する時間

調査の過程で、安田女子大学・安田女子短期大学の学生においては、パスワードの変更経験が少なく、入学時に渡された初期パスワードを使い続ける学生が大多数であることが明らかになった。パスワードを変更しない理由として、「忘れそう（憶えられない）」とする学生が少なからず存在することから、パスワードの記憶には時間を要するものと考えられる。そのため、第3回と第4回の調査において、初期パスワードの記憶に要した期間についての設問を設けた。それをまとめたのがグラフ7である。回答は憶えた時期について半月単位の自己申告によるため、相応の誤差を含んでいる可能性がある。また、憶えた時期を忘れたとする回答があるため、グラフの終点は100%とならない。



グラフ7) 初期パスワードを覚えた時期

G4-2グループのみ他のグループと若干の差異が認められるが有意な違いではない。平均すると66.6%の学生が30日程度で記憶しており、これは授業担当者として観察した学生の行動とほぼ一致する。入学当初の時期は、電子メールを含めた情報システム全般の操作を習得するためのログオン操作が多いことに加え、各種事務手続きでもパスワードを使用しているため、記憶が促進された可能性が考えられる。すなわちログオン操作の回数が相対的に少なくなる上級生においては、記憶に要する時間が長くなることが予想される。

機械的に生成され、連想記憶に頼ることのできない初期パスワードにおいて、記憶に要する時間と忘れやすさは対で考える必要があると思われる。忘れやすさについて調べるため、情報サービスに触れる機会が少なくなる長期休暇、大学においては1年次の夏休みの後でもパスワードを憶えていたかについて2年次以上の学生に尋ねた結果が表8である。

表8) パスワードを忘れていた学生の割合

	共通教育 2007年度入学生	現代ビジネス学部 2007年度入学生	現代ビジネス学部 2006年度入学生
忘れた割合	41.4%	23.0%	19.0%
相関係数	0.27	0.60	0.49

パスワードを忘れた学生の割合について、現代ビジネス学部とその他の学部において95%信頼区間で有意な差が認められた。これは現代ビジネス学部においては貸与ノートパソコンを使用する関係から、長期休暇の期間中においてもパスワードの入力を行う必要性があったこと、入学年次により差が生じた原因については、パソコンを使用する際のログオン先が原因として考えられる。これらの主な相違点について表9にまとめた。

表9) 情報環境の相違点

入学年次	2006年度	2007年度	2008年度	2009年度
貸与パソコン	現代ビジネス学部	現代ビジネス学部		
自己パソコン		薬学部	現代ビジネス学部 薬学部	全学部
ログオン先	Windowsドメイン	Windowsドメイン ・ローカル併用	ローカルログオン	ローカルログオン

現代ビジネス学部の2006年度入学生まではパソコンを使用する際の主なログオン先としてWindowsドメインを用いるように指導していたが、2007年度入学生からはパソコンへのローカルログオンを併用するようになり、2008年度以降はローカルログオンのみとなった。2009年度以降は、前期の情報関連科目においてWindowsドメインへのログオンが必須である情報教室を利用しなくなったため、パスワードを使用する機会はさらに減っていると思われる。

また、記憶に要した時間と休み明けに忘れていたかの相関を求めたところ、記憶に時間を要した学生ほど忘れていたとする傾向が現れている。現代ビジネス学部の学生においては99%信頼区間で有意であり、使用頻度の少ない学生ほど忘れるという、ごく当たり前の経験則を裏付ける結果となった。なお、現在は調査時点よりも初期パスワードを使用する機会が減っているため、パスワードを憶えるのに期間を要し、なおかつ忘れやすくなっているものと考えられる。

VIII. 定期的な変更への対応

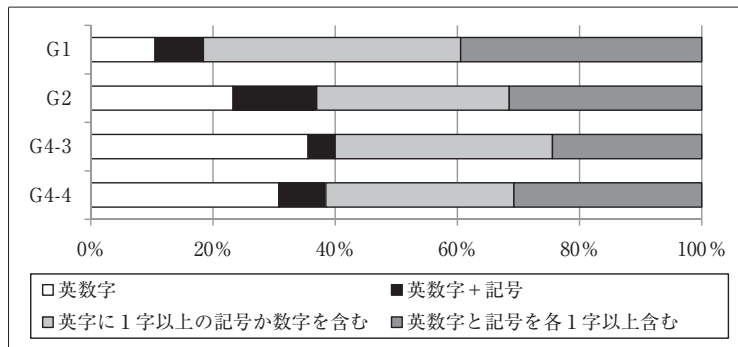
パスワードを定期的に変更するということは、循環使用や使い回しの制限がない場合を除き、新しいパスワードを作成する必要がある。情報サービスにおいては、それぞれの認証システムやセキュリティ・ポリシーに基づいてパスワードに用いる文字種や文字数に基準を設けていることが一般的であり、それらを満たしたパスワードを作成しなければならない。安田女子大学におけるパスワード作成ポリシーは「大小文字、数字、記号を各々1字以上含む6～8字」となっている。ポリシーが複雑であるほど、ポリシーを守りつつ、憶えやすく忘れにくい、新しいパスワードを作ることが困難であることは想像に難くない。パスワード作成ポリシーを表10のような6段階に分類し、どの程度であれば守ることができるかについてまとめたものがグラフ11である。

表10) パスワード作成ポリシーの選択肢

選択肢	例
大文字・小文字・数字が使える	Password
大文字・小文字・数字・記号が使える	Password-
大文字・小文字が使い、1字以上の数字を含むこと	Password1
大文字・小文字が使い、1字以上の記号を含むこと	Password#
大文字・小文字が使い、1字以上の記号と数字を含むこと	Passw0rd&
大文字・小文字・数字・記号がそれぞれ1文字以上あること。	pAs5W-rd

回答は自己申告であるが、自分で作成したことのあるパスワードを同様のポリシーに当てはめた場合との相関係数が0.3～0.6と弱いながらも正の相関関係が見られ、なおかつ99%信頼区間で有意であることから、回答の信頼性はあるものと思われる。

全体の34.8%の学生が安田女子大学におけるポリシーを守って作成することが可能であると回答したが、回答の傾向は調査対象グループにより大きく異なっている。1年次生よりも2年次生、2年次生よりも3年次生と、上級生になるほど複雑なポリシーでも作成可能であるとする回答が増えている。このことは利用する情報サービスが増加するに連れて、様々なポリシーに従ったパスワードを作成する機会が増えること、すなわち「慣れ」によって複雑なパスワードが作成可能になることを示唆していると考えられる。そうであれば定期的なパスワードの変更により作成する機会を増やすことが考えられるが、定期的なパスワードの変更が求められるとして、それが30



グラフ11) 守ることのできるポリシー

日ごとの場合と90日ごとの場合で、守ることのできるポリシーが変わるかを尋ねたところ興味深い結果が出た。

30日ごとの変更を仮定すると、65%の学生が「より簡単なルールでないと守ることができない」と回答した。初期パスワードの記憶に要する時間においても30日程度で記憶できる学生の割合が66.6%でしかないことを考えると、30日ごとの変更は非現実的であると言わざるを得ない。90日ごとの変更を仮定しても、31%の学生が「より簡単なルールでないと守ることができない」と回答している。複雑なポリシーを守らせつつ、定期的な変更を求めることは、ユーザに少なからぬ負担を強いることであると言えよう。

IX. ま と め

初期パスワードのように機械的に生成され、一見すると無意味な文字列は、連想に頼る記憶ができないために憶えるのに相応の時間を要し、なおかつ忘れやすいものであるとの経験則が裏付けられた。対して自分で作成したパスワードにおいては記憶のしやすさが異なると思われるが、記憶のしやすさを優先して友人レベルで共有する情報から推測可能であるとの結果も得られている³⁾⁴⁾。ポリシーを簡単にすれば安易なパスワードを増やしかねず、厳しいポリシーを維持しようとするれば必然的にメモ等に頼ることになり、いずれも好ましくない状況を誘発するであろう。

以上のことを踏まえてパスワードの定期的な変更を求めるのであれば、調査対象の2/3の学生が対処可能な90日に多少の余裕を加えて120日程度、現実的には学期の開始時期に合わせて年に2回程度が望ましいと考えるものである。この程度の間隔であれば、情報システムの利用頻度の低い上級生であっても対応可能であり、さらには変更しないことに対してアカウント停止などのペナルティを課すことも現実的な選択肢となり得るであろう。

なお、今回の結論は女子学生という偏った集団におけるものであり、普遍的な結果を得るためには調査対象に男子学生を加え、性別による違いが見られるものなのかを検討する必要があると考える。また、現状は自己申告を基にした調査であるが、作成したパスワードを自ら検証することができるシステムの構築についても今後の課題としたい。

付録) 第3回調査の調査紙

パスワードに関する意識調査

このアンケートはパスワードの管理について、皆さんがどのような意識を持っているかを調査するものです。回答は統計的な処理のみを行い、個々の内容を公表することはありません。成績とも関係ありません。率直に回答してください。なお、回答したくない項目については、未記入ではなく「回答したくない」という選択肢を選んでください。

問1 あなたはパスワードが必要な情報サービス(電子メールやミクシィなど)をいくつ利用していますか? 今は利用していても退会などの廃止手続きをしていないものも1つと数えて、当てはまるものに○印をつけてください。

選択肢

1~3種類のサービス
4~7種類のサービス
8種類以上のサービス
この設問には回答したくない

問2 あなたは現在、何通りのパスワードを使い分けていますか? 当てはまるものに○印をつけてください。

選択肢

できるだけ揃えているが、やむを得ないものは別れている
2~3種類を使い分けている
4~5種類を使い分けている
できるだけ別々にしているが、同じになっているものもある
この設問には回答したくない

問3 あなたが自分で決めたパスワードについてお尋ねします。そのパスワードがわかるとしたら怖だと思えますか。もともと当てはまるものに○印をつけてください。複数のパスワードがある場合は、もっともよく使用するパスワードについて答えてください。

選択肢

自分で決めたパスワードはない
家族には教えている
家族なら推測できると思う
親しい友人なら推測できると思う
趣味や性格が同じ人なら推測できると思う
推測はできないと思うが辞書に載っている言葉を使っている
普通では推測できないと思う
この設問には回答したくない

問4 問3で思い浮かべたパスワードについてお尋ねします。そのパスワードを決めた際に参考にしたもの(由来)は何ですか? 当てはまるものすべてに○印をつけてください。

選択肢

携帯電話やキャッシュカードなどの暗証番号
誕生日(自分・家族・友人・ペットなど)
住所や番地、電話番号(自分・家族・友人など)
ニックネーム(自分・友人・ペットなど)
有名な人やアーティストなど
自分の持ち物(自動車・ブランド品など)
好きな言葉やスラーズ、ことわざなど
この設問には回答したくない
その他(差し支えない範囲内で記入してください)

問5 パスワードを定期的に変更していますか? もっとも当てはまるものに○印をつけてください。変更の頻度がはばらばらな場合は、もっともよく変更するパスワードについて答えてください。

選択肢

年に何回か変更している(回数を数字で記入してください)
決まったときだけ変更している
やむを得ず変更したことがある
変更していない
この設問には回答したくない

問6 パスワードを変更していない、あるいは変更したくないとしたら、その理由について当てはまるもの全てに○印をつけてください。

選択肢

パスワードを変更する必要性がわからない
現在のパスワードに愛着(なしみ)がある
新しいパスワードを覚えられる(忘れそう)
殆ど揃えているので一つだけ変更できない
単に面倒だから
変更する方法を知らない(方法を忘れた)
この設問には回答したくない

裏面へ続きます。

問7 学校のパスワードについてお尋ねします。入学時に渡されたパスワードは変更しましたか?

選択肢

自分で変えた
授業の中で変えた
変更していない

問8 学校のパスワードについてお尋ねします。入学時に渡されたパスワードを覚えるのに、どのくらいの日数がかかりましたか? だいたいの日数で答えてください。

選択肢

4月中旬までに覚えた(入学から1週間・情報の授業3回程度)
5Wまでに覚えた(入学から3週間・情報の授業7回程度)
5月中旬までに覚えた(入学から1月半・情報の授業10回程度)
5月下旬までに覚えた(入学から2月・情報の授業15回程度)
6月中旬までに覚えた(入学から2月半・情報の授業20回程度)
6月下旬までに覚えた(入学から3月・情報の授業25回程度)
7月中旬までに覚えた(入学から3月半・情報の授業30回程度)
変更した時点で学校のパスワードは覚えなかった
今でも覚えていない
いつか覚えたのか分らない

問9 学校のパスワードについてお尋ねします。夏休みが終わった後で情報教室を使う際もパスワードを覚えていましたか?

選択肢

きちんと覚えていた
覚えていたが入力間違えてしまった
忘れかけていたが、すぐに思い出した
覚えていなかった

問10 学校のパスワードには文字数や使える文字などにルールがあります。今の安田のルールは選択肢の1番下のものですが、あなたが自分でパスワードを作らなくてはならなくなった時に、自分で守ることのできるルールを全て選んでください。なお、作ったパスワードはメモをなくしても憶えられて書籍から使えるもので、文字数は6文字以上8文字以下とします。

○印欄	選択肢	例
	大文字・小文字・数字が使える	Password
	大文字・小文字・数字・記号が使える	Password!
	大文字・小文字が使える、1字以上の数字を含むこと	Password1
	大文字・小文字が使える、1字以上の記号を含むこと	Password!
	大文字・小文字が使える、1字以上の記号と数字を含むこと	Password\$
	大文字・小文字・数字・記号がそれぞれ1文字以上あること	pa5\$mk-rd

問11 定期的にパスワードの変更が求められるとしたら、問10の守れるルールは変わりますか。30日ごと、90日ごとに新しくパスワードを作らないとならなして、どうなると思うか当てはまるものに印をつけてください。

選択肢

30日ごと	90日ごと	より簡単なルールでないと守れないと思う
		守れるルールは変わらないと思う
		より複雑なルールでも守れると思う

問12 表面の問3で思い浮かべたパスワードについてお尋ねします。そのパスワードが満たしているルールを選んでください。

○印欄	選択肢	例
	大文字・小文字・数字が使える	Password
	大文字・小文字・数字・記号が使える	Password!
	大文字・小文字が使える、1字以上の数字を含むこと	Password1
	大文字・小文字が使える、1字以上の記号を含むこと	Password!
	大文字・小文字・数字・記号がそれぞれ1文字以上あること	pa5\$mk-rd
	上記よりも複雑なルール	

ご協力、ありがとうございました。