試作問題「旧情報（仮）」の第4問に見る「ネットワークとセキュリティ」問題の工夫

情報処理学会・学会誌「情報処理」
2023年11月6日 09:04

安田　豊 （京都産業大学 情報理工学部）

連載『教科「情報」の入学試験問題って？』，今回は大学入試センターが公開した試作問題のうち「旧情報

（仮）」の第4問をとりあげます．第4問ではネットワークとセキュリティ関連の事項を扱っています．

第4問は9つの小問からなりますが，それらすべてが前文で示される3人の家庭のネットワーク環境（と言っても1つはネットワーク「なし」環境ですが）に関連する形で提示されます（**図-1**）．

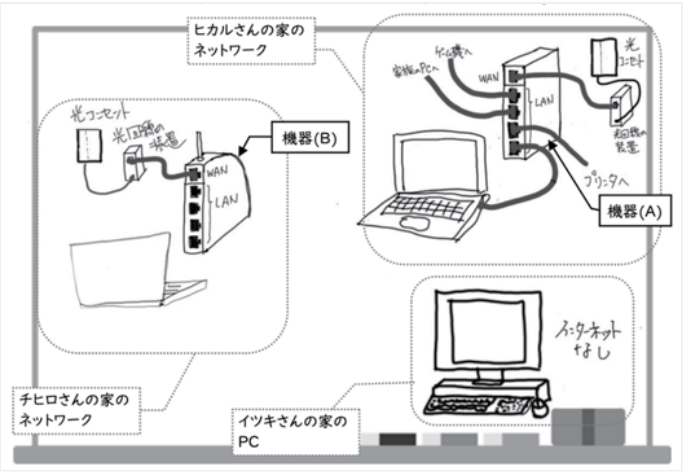

図-1　3人が絵を描いたホワイトボード

実に手描き感あふれる図ですね．こうした具体的なネットワーク環境を起点にさまざまな検討を行い，それぞれの検討で必要となる関連事項に対する理解を問いたかったのだと推測します．本稿ではこの具体的な環境と問いかける内容の関連付けについて見ていきます．

ところでネットワークやセキュリティ関連の問題を作るのはかなり難しい側面があります．後半ではそのことについても少し考察してみようと思います．

表-1に9つの小問の概要を示します．また，各問が主にネットワーク分野とセキュリティ分野のどちらに強く関係しているかを記号「N」「S」でマークしておきます．

問	分野	概要
1	N	機器(A)の名称と役割を確認する
2	N	「SSID」「key」という単語から、その役割を確認する（セキュリティ面ではなくネットワーク面）
3	S	機器(B)によるセキュリティ対策の妥当性を判断する
4	S	家庭用インターネット環境の構築に必要な事項を検討する
5	S	Wi-Fi アクセスポイントの鍵マークの理解を確かめる
6	N	自宅インターネット環境の機器の接続に関する理解を確かめる
7	S	ブルートフォース攻撃(注 1)におけるパスワードの長さと計算量の関係を見る
8	S	ブルートフォース攻撃への有効な対策を選ぶ
9	S	各種のセキュリティ対策と機密性・完全性・可用性との関係を確かめる

表-1　小問の構成

分量としてはセキュリティ分野が多めで，また問題の難易度としてもセキュリティ分野の方が高めに設定されているように思えます．本稿ではそのセキュリティ分野の問題を1つとりあげ，詳しく見てみましょう．

注1） 問題文にそのまま「ブルートフォース（総当たり）攻撃」と出ているのですが，この語は教科「情報」の教科書に登場したことはないと思われます．知らなくても「総当たり」という表現から推定して解くこともできそうですが，少し無理があるかなとも思いました．もちろん試作問題ですから本番ではより洗練されたものが出されると思いますが．

目次

問3「セキュリティ対策として適当なものを2つ選べ」

図-2に問3をそのまま引用します．

問3　機器（B）でできるセキュリティ対策として適当なものを，次の⓪～③のうちから二つ選べ。ただし，解答の順序は問わない。［エ］・［オ］

⓪　機器（B）の機能を設定するために管理者としてログインするときに必要となるパスワードを，初期設定のものから別の推測されにくいものに変更する。
①　Wi-Fiに接続するためのパスワードの長さを，より短いものに変更する。
②　機器（B）の電波が届く場所を広げるために，中継機器を新たに設置する。
③　Wi-Fiを利用する際，より強い暗号化のプロトコルを設定する。

図-2　問3（全文）

問題中の「機器（B）」とはチヒロさんの家の無線LANアクセスポイント機能付きのブロードバンドルータ（いわゆるWi-Fiルータ）です．

この問題をストレートに解こうとすると，4つの選択肢でそれぞれ指定された操作や処置をしたとき，それがセキュリティ対策としてプラスに働くかマイナスに働くか，あるいはまったく関係ないかを判断することになります．各選択肢について，1つずつそのようにして検討してみます．

選択肢（0）は簡単に言えば「初期パスワードの変更」です．この状況を把握するには，まずWi-Fiルータの設定作業はネットワーク越しに行うものであり，その際に管理者のパスワードが要求される，そしてそのパスワードは初期状態では共通であったり機体ラベルに書かれていたりして危険だ，という3つのことを知っているか，あるいは記述から読み取ることが必要です．それが揃えば初期設定からパスワードを変更することの意味，つまりセキュリテイ対策としての効果について判断できる，というわけです．つまりこの操作はセキュリティ対策的に「プラス」だと判断できます．

選択肢（1）「パスワードを短くする」 についてはWi-Fiルータの設定操作にパスワードがあり，またパスワードの強度（破られにくさ）がその長さに依存していることを理解している必要があります．この2つのことが分かっておれば，パスワードを短くすることはセキュリティ対策的には「マイナス」だと判断できます．

選択肢（2）「中継機器の設置」ですが，そうした機器の存在を知らない受験者も，記述から機能・役割を推定することはできるでしょう．その上で無線LAN接続の範囲が広がった際のセキュリティ的なリスクについて検討することになります．予想外のところから第三者が接続を試みる可能性が上がる点をマイナス評価することはあっても，プラス側の作用はあまり想像できません．もちろんこの中継機器が機器（B）より強い暗号化に対応していたり，MACアドレス認証などの機能を持っていれば話は別ですが，そのような説明は問題文中には登場しないため，セキュリティ対策的には「無関係」「少なくともプラスではない」と判断することになるでしょう．

選択肢（3）「（Wi-Fiに接続する際の）より強い暗号化のプロトコルの設定（注2）」ですが，この状況を把握するには，まずWi-Fiの接続には複数の暗号化プロトコルが用意されていることを知らねばなりません．またそれが通信プロトコルと結びついたものであることを理解していなければ「問題の説明記述がおかしい」といった種類の誤答選択肢である可能性を排除できません．それを把握できれば，この措置がセキュリティ対策的には「プラス」だと判断できるでしょう．

かなり細かく確認しました．断片的な用語の知識ではなく，部品としての機能や役割ではなくシステムの中での動きを理解していることを問おうとする意図が感じられませんか．その目で見ると問3は良い問題です．

しかし一方で「そのような関連事項の理解がなくとも問3は解ける」と思う人が多いでしょう．全体の情況を把握せず，断片的に選択肢の文言からセキュリティ対策的にそれがプラスに働くものを消去法を含めて2つ選べばよい，というアプローチです．実際，（0）初期パスワードの変更，（1）パスワードを短くする，（2）中継機器の設置，（3）強い暗号化のプロトコル，くらいの語句の印象からだけで正解を選べそうです．

ネットワークとセキュリティ分野の問題の（主に作問側の）困難さは実にこれ，つまり「断片的な用語の知識」で短絡的に解くアプローチと闘うことにあります．

注2）問題文からWi-Fiアクセスポイントとの接続，つまりデータリンク層での暗号化であることはおよそ汲み取れます．しかし厳密にはこの記述では，より上位層での（より強い）暗号化プロトコルの導入も含んでしまいます．たとえばWebのアクセスにSSLでなくTLS，それも1.1でなく1.3を利用するといったケースです．するとこ

れは機器（B）での処置ではない，という点で選択肢（3）が「適切」から「不適切」に逆転してしまいます．次節で提案している，「機器（B）の設定を確認し，不要であればより弱い暗号化プロトコルの使用を無効にする」などがよいかもしれません．

ではどのような問い方が可能か

つまりこの問い方ではまだ不十分で，本当はもっと深く問いたいところです．試作問題の作問者にしても，正解である選択肢（0）（3）のそれぞれについて，なぜ，どのようにしてそれがセキュリティ対策としてプラスに働くのかを問いたかったのでは，と思ってしまいます．少しこの場で「もしもう少し深く問うとしたら，どのような問題になるか」を想定してみましょう．

たとえば元の選択肢（0）が示した「Wi-Fiルータの初期設定パスワードを変更すべき」なのはなぜか，そうしないとどんな問題が生じるかを問うことが考えられます．その選択肢の中に「初期状態で共通のパスワードが設定されている」ために「予期せず電波到達範囲から第三者にWi-Fiネットワークに接続」される可能性があること，またパスワードが破られたとき，「契約者以外のISP利用（盗用）」や「盗聴による機密情報の漏洩」の問題，あるいはHTTPS接続による暗号化によって機密情報が保護されていたとしても「アクセス先が判明することによるプライバシ問題」があり得ることが認識できるかどうかを確認する問いなり選択肢なりを散りばめることになるでしょう．

また，通常はその製品が扱える最も強い暗号化のプロトコルがはじめから動作するよう設定されているはずですから，「（現在）より強い暗号化のプロトコルを設定する」ような状況設定はできません．ただしその逆，つまり侵入口となり得る「より弱い暗号化のプロトコルを無効に設定する」，またそのために「弱い暗号化プロトコルにしか対応していない（恐らくは古い）機器を更新する」ことの妥当性は普通に問えるでしょう．

しかし難易度をそれほど高めることもできませんし，かなり長い説明記述を加えることになるでしょうから，上に示したアイディアを実際に「良い」問題として完成させるのは簡単ではなさそうです．

ネットワークとセキュリティ分野の作問の難しさ

セキュリティ的な意味での攻撃とは，対象となる（それなりに複雑な）システムに対して想定外の，つまり設計者の意図しない操作やアクセスをすることで行われます．そして脆弱性はシステムのあちこちに散在しています．「正常なシステムに関する理解」を下敷きにしない限り，脅威に対抗するセキュリティ対策もまた断片的なものになってしまいます．

そしてもちろん「情報」の問題は知識の断片でなく，大学入試センターが示し続けているように「知識の質を問う」，また「思考力・判断力・表現力等を発揮できる」ものであるべきです．冒頭に述べたように，この試作

問題「旧情報（仮）」の第4問ですべての小問を，最初に提示した具体的なネットワーク環境（図1）に関連付けた形にしたのは，その現れだと筆者は考えています．つまり単純な用語知識などでなく，システム及び関連事項の理解を下敷きにした検討・判断をさせる方向に押しているように思うのです（注3）．

また，たとえば問7のような良い問題もあります．これはブルートフォース攻撃でのパスワードの長さと計算量の関係を見るもので，用語の知識だけでやり過ごすことのできない，計算機科学の側面を取り入れたものです．

ともすれば単純な用語知識で解けるものになりがちなネットワークとセキュリティ分野の問題ですが，今後もこうした工夫が重ねられていくでしょう．教科「情報」はもちろん「用語の意味」や「断片的な対処法」を教えるものではなく，むしろそれらを関連づけることができる基礎的な情報処理システムに関する理解を目指すものと思います．

受験する人はこのことを意識して，ネットワークとセキュリティ分野に対しては，ぜひ全体的なシステムの動きを想像しながら問題を解いてもらいたいと思います．

注3） もちろんネットワーク機器の呼称の曖昧さによる問題を避けたかった面もあるでしょう．たとえば「ブロードバンドルータ」などはWi-Fiアクセスポイントから NATやファイアウォールまで多様な機能を組み合わせた製品で，「その役割は＊＊である」といった問いが困難です．

参考文献

1）大学入試センター：令和7年度試験の問題作成の方向性，試作問題等
https://www.dnc.ac.jp/kyotsu/shiken_jouhou/r7/r7_kentoujoukyou/r7mondai.html

（2023年9月19日受付）
（2023年11月6日note公開）

■**安田　豊**（正会員）
京都産業大学情報理工学部准教授．IPSJMooc（https://sites.google.com/a.ipsj.or.jp/mooc/）第4章作成に携わった．SDN などに興味を持つ．

情報処理学会ジュニア会員へのお誘い

小中高校生，高専生本科～専攻科1年，大学学部１～3年生の皆さんは，情報処理学会に**無料で入会**できます．**会**

員になると有料記事の閲覧，情報処理を学べるさまざまなイベントにお得に参加できる等のメリットがあります．ぜひ，入会をご検討ください．入会は**こちら**から！