問4　Webサイトにおけるセッション管理（ネットワーク）（H27秋-FE 午後問4）

【解答】

［設問1］　a－エ
［設問2］　ウ
［設問3］　b－ウ
［設問4］　c－ウ，d－ア

【解説】

ショッピングサイトを事例として，Webサイト内の閲覧動向をセッション管理の仕組みを使って把握する方法を主題に，セッションIDを利用する上でのセキュリティ面の配慮，具体的なセッション管理の実現方法としてクッキーを利用する方法について出題されている。

設問1は，セッションIDの生成から破棄までの期間，設問2は，セキュリティ面に配慮したセッションIDの採番方法について問われている。設問3は，セッションIDの送受信の方法とその特徴，設問4は，クッキーをドメイン指定で利用した場合にどの範囲のドメインにクッキーが送受信されるかを解答する。

［設問1］

ショッピングサイトAにおける商品購入の流れが図1に示されている。セッションIDの生成から破棄のライフサイクルはWebサイトによって考え方が異なる。問題文の冒頭の例では，「ログインからログアウトまで同じ一つのセッションである」として管理するとあるが，Webサイトの閲覧動向を把握するため閲覧を開始したときにセッションIDを生成することもある。

図1に示されたショッピングサイトAの商品購入の流れにおいては，ログアウト時にセッションIDを破棄することから，ログインに成功したときにセッションIDを生成すると考えるのが自然である。したがって，（エ）の「ログインに成功したとき」が正解である。

［設問2］

セッションIDの利用に際してはセキュリティ面に配慮する必要がある。問題文にもあるようにセッションIDを推測しにくい文字列にすることが重要である。推測が容易なセッションIDを利用すると悪意のある第三者にセッションが乗っ取られてしまう可能性がある（セッションハイジャック）。このような攻撃を防ぐためにも，セッションIDとしては推測が困難になる「十分に長いランダムな文字列」を使うことが好ましい。したがって，（ウ）が正解である。

ア，イ，エ：会員IDや通し番号など，一定のルールに基づいて採番されるものをセッションIDとして利用すると，他者による推測が容易になるため，セッションIDには適さない。

［設問3］

セッションIDの送受信の方法として問題文に三つ挙げられている。

(1)　クッキーの値としてセッションIDを記載する。
(2)　URLの中にセッションIDを埋め込む。
(3)　HTML中のフォームでフィールドhiddenにセッションIDを埋め込む。

これらの方法と特徴の組合せを解答群から選ぶ。

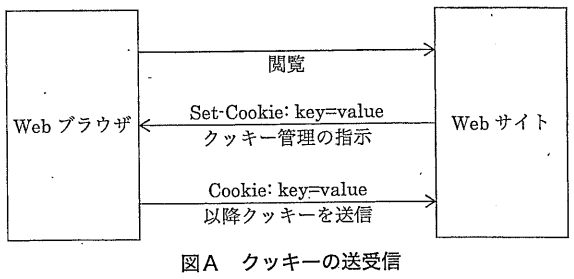
(A)は「Webブラウザのアドレスバーに表示されるURLの中にセッションIDが含まれる」とあるので，(2)の特徴である。

次に(B)は「Webブラウザの設定次第で利用できないことがある」とあるが，問題文にあるようにWebブラウザでクッキーの管理が有効になっていなければ利用できないので，(1)の特徴である。

最後に(C)は「タグ<a>で指定されたリンクのクリックではセッションIDが送信されない」とある。<a>で指定されたリンクがクリックされた際にWebブラウザはHTTPプロトコルのGETメソッドを利用してWebサーバにアクセスする。この点が問題になり得る方法，つまりPOSTメソッドを使ってセッションIDを送信する方法を示している，POSTメソッドはHTMLフォームを使って送信する方法になるので，(3)の特徴である。したがって，（ウ）が正しい組合せとなる。

［設問4］

セッションIDの送受信の方法として挙げられた(1)のクッキーを利用する方法について掘り下げた問題である。クッキーは図Aのように，Webブラウザを利用してWebサイトを閲覧し，Webサイトが Webブラウザにクッキーを管理させたい場合に，クッキーを記載してレスポンスを返し，その後，クッキーの有効期限が切れるか Webサイト側でクッキーの削除をするまで，Webブラウザは Webサイトへクッキーを送信するようになる。



図A　クッキーの送受信

Webサイト側でクッキーの送受信範囲を指示することができる。具体的にはドメイン名やパスを指示することができるが，本問ではドメイン名を指定した場合について問われている。ドメイン名を指示した場合は，ドメイン名が等しいか，より下位ドメインのホスト名宛ての HTTP 要求を送信する際にクッキーを付与することになる。http://www.foo.example.com/index.html にアクセスし，表1に示されたクッキーの名前と送信先ドメイン名の指示があった場合，www.example.com と www.bar.example.com の二つの送信先ドメインの指定はアクセスしたドメイン名の www.foo.example.com に後方一致しないため無効なクッキーとして Web ブラウザで管理されない。したがって，空欄cがある記述は「このうちの3（ウ）個のクッキーを管理する」となる。

この直後に http://www.bar.example.com/index.html にアクセスするときには，www.bar.example.com に後方一致する example.com が送信先ドメイン名で指示された c1 だけが Web ブラウザから送信される。したがって，空欄dには（ア）の「c1」が入る。