問4　ホスト名の衝突（ネットワーク）　(H27春-FE 午後問4)

【解答】

［設問1］　a－ウ，b－エ，c－イ

［設問2］　イ

【解説】

2012年に新gTLD（ジェネリック（汎用）トップレベルドメイン）の申請受付が開始され，多数のgTLDの使用が認められるようになった。これを背景に，以前よりイントラネット上で独自のTLDを運用してきた企業や団体においてホスト名が衝突するリスクが高まっている。本問は，DNSの名前解決の流れを通じてホスト名が衝突する仕組みと発生する問題，そしてこの問題に対する対策がテーマになっている。

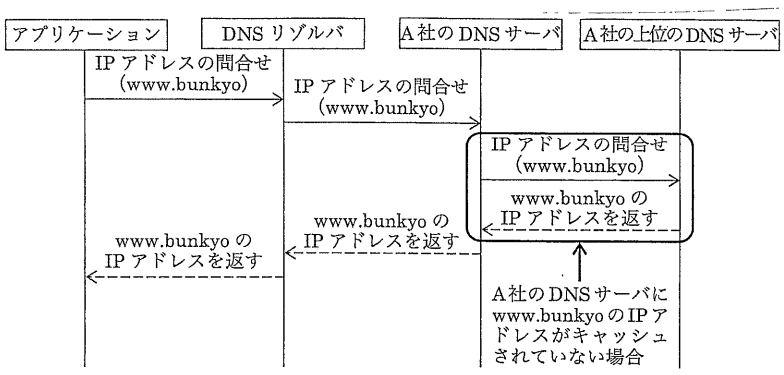
設問1は，独自のTLDを運用しているネットワークにおいて，新しいgTLDの運用が開始された場合に発生する問題とリスクに関する問題である。

設問2は，新しいgTLDが追加されることによって生じる，名前衝突のリスクを低減させる対策を導き出す問題である。

［設問1］

A社では独自のTLDとして“corp”を使っており，A社のDNSサーバで管理しているホスト名は問題文の表1のとおりである。また，A社のドメインである“example.co.jp”を省略しても，ホスト名に対応するIPアドレスを得ることができるよう各端末のDNSリゾルバの設定で“example.co.jp”をサーチリストに登録している。問題文では“www.bunkyo.example.co.jp”のIPアドレスを知るためにホスト名“www.bunkyo”で問い合わせた場合の流れを，①～⑥の解説と図2で説明している。これを踏まえて新しく正式なTLDが追加された場合の動作と問題点を解答していく。

・空欄a：新しく正式なTLDとして“bunkyo”が追加され，“www.bunkyo”のWebサーバの運用が開始された場合に，ホスト名“www.bunkyo”を問い合わせたときの動作について解答する。ホスト名“www.bunkyo”のIPアドレスを問い合わせた場合，図Aのような動作となるため，インターネット上のWebサーバ“www.bunkyo”のIPアドレスが返される。



図A　ホスト名“www.bunkyo”のIPアドレス問合せ

① アプリケーションが，DNSリゾルバにホスト名“www.bunkyo”のIPアドレスを問い合わせる。

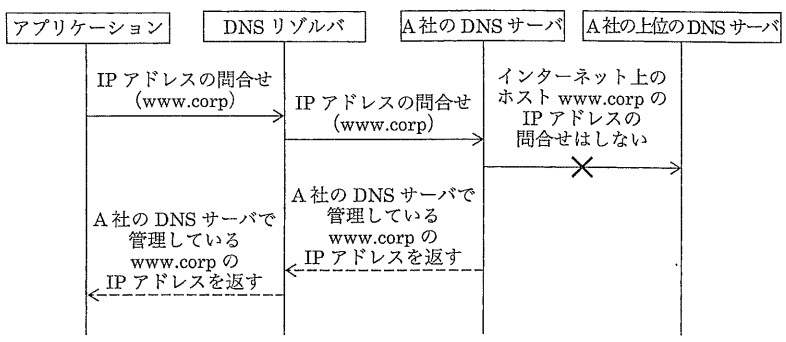
② DNSリゾルバは，A社のDNSサーバにホスト名“www.bunkyo”のIPアドレスを問い合わせる。

③ ホスト名“www.bunkyo”のIPアドレスがA社のDNSサーバにキャッシュされていない場合は，更に上位のDNSサーバに“www.bunkyo”を問い合わせ，インターネット上のWebサーバ“www.bunkyo”のIPアドレスをDNSリゾルバに返す。キャッシュされている場合は，キャッシュされているインターネット上のWebサーバ“www.bunkyo”のIPアドレスをDNSリゾルバに返す。

④ DNSリゾルバは，A社のDNSサーバから返されたインターネット上のWebサーバ“www.bunkyo”のIPアドレスをアプリケーションに返す。

したがって，（ウ）が正解である。

・空欄b：新しく正式なTLDとして，“corp”が追加され，インターネット上でホスト名“www.corp”のWebサーバの運用が開始されたとき，A社のDNSサーバでは既にホスト名“www.corp”が管理されており，図Bのような動作となるため，インターネット上のWebサーバ“www.corp”のIPアドレスを得ることができなくなってしまう。



図B　ホスト名“www.corp”のIPアドレス問合せ

① アプリケーションが，DNSリゾルバにホスト名“www.corp”のIPアドレスを問い合わせる。

② DNSリゾルバは，A社のDNSサーバにホスト名“www.corp”のIPアドレスを問い合わせる。

③ ホスト名“www.corp”がA社のDNSサーバに自社で管理しているホスト名となっているため，A社で管理している“www.corp”のIPアドレスを返す。

④ DNSリゾルバは，A社のDNSサーバから返されたA社で管理しているホスト名“www.corp”のIPアドレスをアプリケーションに返す。

したがって，（エ）が正解である。

・空欄c：空欄aや空欄bの説明のとおり，新しく正式なTLDが追加され，独自のTLDと名前の衝突が起こることによって，これまで内部のホストである“www.bunkyo.example.co.jp”へのアクセスを“www.bunkyo”で行えていたが，意図せずインターネット上のWebサーバ“www.bunkyo”にアクセスしてしまうことになり，情報漏えいなどのセキュリティ上のリスクが高まる。したがって，（イ）が正解である。

なお，その他の選択肢には次のようなリスクがある。ただし，名前の衝突とは無関係であり，利用者が，意図せず別のサーバに接続してしまうリスクとは関係がないといえる。

ア：ウイルス対策ソフトの未使用や使用不備によるリスクといえる。

ウ：内部犯行によるリスクといえる。

エ：ファイアウォールの設定不備や脆弱性によるリスクといえる。

［設問2］

名前が衝突するリスクを低減させる対策として有効なものと，そうでないものを選別する。

（ア）は，独自のTLDの利用を停止することで，名前の衝突が無くなるため有効である。

（イ）は，外部のDNSサーバとの通信を遮断することで，名前の衝突は回避できるが，外部のホストのIPアドレスの問合せができなくなるという根本的な問題が発生するため有効ではない。

（ウ）は，サーチリストの利用をやめることで，“www.bunkyo.example.co.jp”を“www.bunkyo”で問い合わせることができなくなり，名前の衝突の可能性が低くなるため有効である。

この問題では，名前が衝突するリスクを低減させる対策として適切でないものを問うている。したがって，（イ）が正解である。

なお，この問題は，リスクをあくまでも「低減」するものとそうでないものを選択する形式になっている。つまり，（ア）の対策で名前の衝突が無くなっても，サーチリストを利用している限り，省略したホスト名での問合せか，省略をしていないホスト名での問合せかをDNSリゾルバが区別できないリスクが残る。一方，（ウ）の対策でサーチリストの利用をやめても，独自のTLDの利用を続ける限りは，インターネット上の新たにできた正式なTLDに対する問合せか，独自のTLDに対する問合せかをDNSリゾルバが区別できないリスクが残る。このため，（ア）と（ウ）両方の対策をとることで，リスクを「低減」ではなく，「回避」することができる。