＜問2＞ ネットワークのセキュリティ対策

●設問 1

[試験センターによる解答例]

(1)　A 社公開 Web サーバの名前解決ができなくなる。(23 字)
(2)　DNS リフレクション攻撃（12 字）
(3)　a：ア
　　b：イ
(4)　c：A
(5)　d：ランダム化（5 字）
(6)　e：DNSSEC（6 字）
(7)　f：オ
　　g：カ
　　＊f と g は順不同。

＜解説＞

(1)　表 1 にあるように、A 社の外部 DNS サーバは A 社ドメインの権威 DNS サーバ及び再帰的な名前解決を行うフルサービスリゾルバとして使用されている。また、表 1 の注 2)にあるように、同サーバをフルサービスリゾルバとして使用しているのはプロキシサーバとメールサーバである。このように、外部 DNS サーバは、A 社公開 Web サーバに対するアクセス要求があった際に、権威 DNS サーバとして名前解決をする役割を担っている。したがって、外部 DNS サーバのサービスが停止した場合には、A 社公開 Web サーバの名前解決ができなくなるという影響が及ぶことになる。

(2)　下線②のような手法で DNS サーバを悪用し、第三者のサーバに DoS 攻撃を行うのは、DNS リフレクション攻撃（「DNS amp 攻撃」「DNS リフレクター攻撃」とも呼ばれる）である。DNS リフレクション攻撃への対策としては、DNS サーバを権威 DNS サーバとフルサービスリゾルバの機能に分離し、フルサービスリゾルバはインターネット側からのリクエストには応じないようにするのが有効である。

(3)　表 3 の項番 5 は宛先がインターネットとなっており、サービスが DNS であるから、送信元に入るのはフルサービスリゾルバの機能を持つ DNS-F である。一方、項番 6 は送信元がインターネットでサービスが DNS なので、宛先に入るのは権威 DNS サーバの機能を持つ DNS-K である。

(4)　DNS のリソースレコードにおいて、サーバ等のホスト名に対する IP アドレス情報を登録しているのは A レコードであり、メールサーバのホスト名（FQDN）は MX レコードに登録する。DNS キャッシュポイズニング攻撃は、あるホストの FQDN に対する IP アドレス情報を不正に書き換えるので、 c には“A”が入る。

DNS キャッシュポイズニング攻撃とは、フルサービスリゾルバである DNS サーバから権威 DNS サーバへの名前解決要求に対し、悪意ある DNS サーバが、正当な権威 DNS サーバからの応答が返る前に、悪意あるサイトに誘導するための不正な名前解決情報を返すことで、フルサービスリゾルバの DNS サーバのキャッシュに登録させる攻撃である。そのようにしてキャッシュが汚染された DNS サーバを利用したユーザが悪意あるサイトに誘導され、機密情報が盗まれるなどの被害を受ける。
この攻撃を成立させるためには、次の条件を満たす必要がある。

① 標的となる DNS サーバのキャッシュに登録されていない名前解決要求であること
② 標的となる DNS サーバが上位サーバに問合せた際の送信元ポート番号あてに応答を返すこと
③ 標的となる DNS サーバが上位サーバに問合せた際のトランザクション ID（DNS のリクエストを一意に識別するための ID）と応答の ID を合致させること
④ 正当な上位サーバからの応答よりも早く応答を返すこと

上記②については、標準的に 53 番固定としている DNS サーバが多数存在すること、③については、ID が 16 ビット（最大 65,536 通り）であることが攻撃を容易にさせる要因となっている。

(5)　上述のように、送信元ポート番号を 53 番固定としている DNS サーバの存在が DNS キャッシュポイズニング攻撃を容易にさせる要因となっている。したがって、対策として DNS の送信元ポート番号を固定とせず、ランダム化するのが有効である。

(6)　問題文で解説されている技術は DNSSEC（DNS Security Extensions）である。
DNSSEC は、名前解決要求に対して応答を返す DNS サーバが、自身の秘密鍵を用いて応答レコードにディジタル署名を付加して送信する。応答を受け取った側は、応答を返した DNS サーバの公開鍵を用いてディジタル署名を検証することで、応答レコードの正当性、完全性を確認する。

(7)　DNS over TLS は、クライアントであるスタブリゾルバが、フルサービスリゾルバである DNS サーバとの間で行う通信を TLS によって暗号化する技術である。した

がって [f] にはオ、[g] にはカが入る（f と g は順不同）。なお、スタブリゾルバとは、一般的な PC の OS 等に搭載されている機能であり、フルサービスリゾルバに対して要求を出し、その結果を受け取ることによって名前解決をする。

●設問２

[試験センターによる解答例]

(1)　権威 DNS サーバがサービス停止になるリスク（21 字）
(2)　h：カ
　　i：ク
(3)　j：拒否
　　k：許可
　　l：拒否
　　m：拒否
(4)　n：オ
　　o：ア
　　p：カ
　　※ n と p は順不同。

＜解説＞

(1)　従前の DNS サーバの構成では、外部 DNS サーバの権威 DNS サーバの機能をバックアップする仕組みがなかったため、同サーバの障害により権威 DNS サーバがサービス停止になるリスクがあった。DNS-S がセカンダリの権威 DNS サーバとなることにより、このリスクを低減することができる。

(2)　h：DNS サーバの NS レコードには DNS サーバの FQDN を登録する。[h] の上の行でプライマリの権威サーバである DNS-K の FQDN が登録されているので、[h] に登録するのはセカンダリの権威 DNS サーバである DNS-S の FQDN である。DNS-S は X 社のホスティングサービス上にあるので、ドメイン名は“x-sha.co.jp”となる。したがって、[h] にはカの“dns-s.x-sha.co.jp.”が入る。

　i：DNS サーバの MX レコードにはメールサーバの FQDN を登録する。A 社のメールサーバのホスト名は“mail”であり、自社ネットワーク内にあるので、ドメイン名は“a-sha.co.jp”となる。したがって、[i] にはクの“mail.a-sha.co.jp.”が入る。

(3)　ゾーン転送は、セカンダリの権威 DNS サーバである DNS-S がプライマリの権威 DNS サーバである DNS-K に対して要求する。ゾーン情報が流出するのを防ぐため、上記以外のゾーン転送要求は拒否する必要がある。したがって、表 4 ではゾーン転送要求元が DNS-S で、ゾーン転送要求先が DNS-K である [k] のみが“許可”で、それ以外は全て“拒否”となる。

(4)　表 1 の注 2)にあるように、A 社のフルサービスリゾルバはプロキシサーバとメールサーバが使用している。フルサービスリゾルバの機能を X 社ホスティングサービス上の DNS-HF に移行することにより、プロキシサーバ及びメールサーバから DNS-HF への DNS 通信を許可するよう FW のフィルタリングルールを変更する必要がある。したがって、[o] にはアの“DNS-HF”が入り、[n] [p] にはオの“プロキシサーバ”とカの“メールサーバ”が入る。(順不同)

＜問3＞ セキュリティ運用

●設問 1

[試験センターによる解答例]

a：PC の動作に問題がないこと（13 字）

＜解説＞

検証 LAN の PC に先行してセキュリティパッチ（パッチ）を適用し、社内で利用しているアプリケーションプログラムを 2 日間動作させるのは、パッチの適用によって PC の動作に問題がないことを確認するためである。

●設問 2

[試験センターによる解答例]

L2SW1

＜解説＞

表 1 の FW の概要にあるように、G 社でインターネットとの間の通信を許可しているのは DMZ だけである。マルウェア感染が DMZ 又はどの LAN で起きたとしても、マルウェアからインターネットへの通信が通過することになる L2SW であるから、図 4 の中で該当するのは DMZ にある L2SW1 である。