次の問1は必須問題です。必ず解答してください。

問1　DNSのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

R社は，Webサイト向けソフトウェアの開発を主業務とする，従業員約50名の企業である。R社の会社概要や事業内容などをR社のWebサイト（以下，R社サイトという）に掲示している。

R社内からインターネットへのアクセスは，R社が使用するデータセンタを経由して行われている。データセンタのDMZには，R社のWebサーバ，権威DNSサーバ，キャッシュDNSサーバなどが設置されている。DMZは，ファイアウォール（以下，FWという）を介して，インターネットとR社社内LANの両方に接続している。データセンタ内のR社のネットワーク構成の一部を図1に示す。

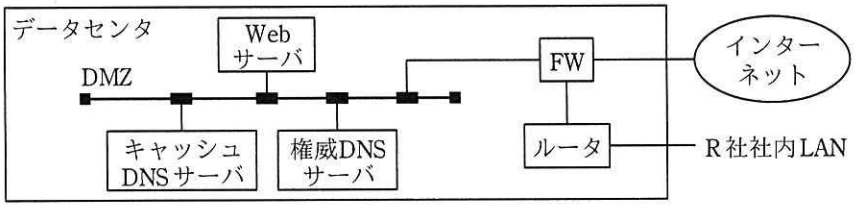

図1　データセンタ内のR社のネットワーク構成（一部）

R社サイトは，データセンタ内のWebサーバで運用され，インターネットからR社サイトへは，HTTP Over TLS（以下，HTTPSという）によるアクセスだけが許されている。

〔インシデントの発生〕

ある日，R社の顧客であるY社の担当者から，“社員のPCが，R社サイトに埋め込まれていたリンクからマルウェアに感染したと思われる”との連絡を受けた。Y社は，Y社が契約しているISPであるZ社のDNSサーバを利用していた。

R社情報システム部のS部長は，部員のTさんに，R社のネットワークのインターネット接続を一時的に切断し，マルウェア感染の状況について調査するように指示した。Tさんが調査した結果，R社の権威DNSサーバ上の，R社のWebサーバのAレコードが別のサイトのIPアドレスに改ざんされていることが分かった。R社のキャッシュDNSサーバとWebサーバには，侵入や改ざんされた形跡はなかった。

Tさんから報告を受けたS部長は，①Y社のPCがR社の偽サイトに誘導され，マルウェアに感染した可能性が高いと判断した。

〔当該インシデントの原因調査〕

S部長は，当該インシデントの原因調査のために，R社の権威DNSサーバ，キャッシュDNSサーバ及びWebサーバの脆弱性診断及びログ解析を実施するよう，Tさんに指示した。Tさんは外部のセキュリティ会社の協力を受けて，脆弱性診断とログ解析を実施した。診断結果の一部を表1に示す。

表1　R社サーバの脆弱性診断及びログ解析の結果（一部）

診断対象	脆弱性診断結果	ログ解析結果
権威DNSサーバ	・OSは最新であったが，DNSソフトウェアのバージョンが古く，［　a　］を奪取されるおそれがあった。 ・インターネットから権威DNSサーバへのアクセスはDNSプロトコルだけに制限されていた。	業務時間外にログインされた形跡が残っていた。
キャッシュDNSサーバ	・OS及びDNSソフトウェアは最新であった。 ・インターネットからキャッシュDNSサーバへのアクセスはDNSプロトコルだけに制限されていた。	不審なアクセスの形跡は確認されなかった。
Webサーバ	・OS及びWebサーバのソフトウェアは最新であった。 ・インターネットからWebサーバへのアクセスはHTTPSだけに制限されていた。	Y社のPCがマルウェア感染した時期に②R社サイトへのアクセスがほとんどなかった。

診断結果を確認したS部長は，R社の権威DNSサーバのDNSソフトウェアの脆弱性を悪用した攻撃によって［　a　］が奪取された可能性が高いと考え，早急にその脆弱性への対応を行うようにTさんに指示した。

Tさんは，R社の権威DNSサーバのDNSソフトウェアの脆弱性は，ソフトウェアベンダが提供する最新版のソフトウェアで対応可能であることを確認し，当該ソフトウェアをアップデートしたことをS部長に報告した。S部長はTさんに，R社の権威DNSサーバ上のR社のWebサーバのAレコードを正しいIPアドレスに戻し，R社のネットワークのインターネット接続を再開させたが，Y社のPCからR社サイトに正しくアクセスできるようになるまで，③しばらく時間が掛かった。R社は，Y社に謝罪するとともに，当該インシデントについて経緯などをとりまとめて，R社サイトなどを通じて，顧客を含む関係者に周知した。

〔セキュリティ対策の検討〕

S 部長は，R 社の権威 DNS サーバに対する④同様なインシデントの再発防止に有効な対策と，R 社のキャッシュ DNS サーバ及び Web サーバに対するセキュリティ対策の強化を検討するように，T さんに指示した。

T さんは，R 社の Web サーバが使用しているディジタル証明書が，ドメイン名の所有者であることが確認できる DV（Domain Validation）証明書であることが問題と考えた。そこで T さんは，EV（Extended Validation）証明書を導入することを提案した。R 社の Web サーバに EV 証明書を導入し，Web ブラウザで R 社サイトに HTTPS でアクセスすると，R 社の［ b ］を確認できる。

また T さんは，⑤R 社のキャッシュ DNS サーバがインターネットから問合せ可能であることも問題だと考えた。その対策として，FW の設定を修正して R 社社内 LAN からだけ問合せ可能とすることを提案した。また，R 社のキャッシュ DNS サーバに，偽の DNS 応答がキャッシュされ，R 社の社内 LAN 上の PC がインターネット上の偽サイトに誘導されてしまう，［ c ］の脅威があると考えた。DNS ソフトウェアの最新版を確認したところ，ソースポートのランダム化などに対応していることから，この脅威については対応済みとして報告した。

設問 1　本文中の下線①で，Y 社の PC が R 社の偽サイトに誘導された際に，Y 社の PC に偽の IP アドレスを返した可能性のある DNS サーバを，解答群の中から全て選び，記号で答えよ。

解答群

ア　DNS ルートサーバ　　イ　R 社のキャッシュ DNS サーバ

ウ　R 社の権威 DNS サーバ　　エ　Z 社の DNS サーバ

設問 2　〔当該インシデントの原因調査〕について，(1)～(3)に答えよ。

(1)　表 1 及び本文中の［ a ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　管理者権限　　イ　シリアル番号

ウ　ディジタル証明書　　エ　利用者パスワード

(2) 表 1 中の下線②で，R 社サイトへのアクセスがほとんどなかった理由を 20 字以内で述べよ。

(3) 本文中の下線③で，Y 社の PC が正しい R 社サイトにアクセスできるようになるまで，しばらく時間が掛かった理由は，どの DNS サーバにキャッシュが残っていたからか，解答群の中から選び，記号で答えよ。

解答群

ア DNS ルートサーバ　　イ R 社のキャッシュ DNS サーバ

ウ R 社の権威 DNS サーバ　　エ Z 社の DNS サーバ

設問3 〔セキュリティ対策の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線④で，同様なインシデントの再発防止に有効な対策として，R 社の権威 DNS サーバに実施すべきものを，解答群の中から選び，記号で答えよ。

解答群

ア 逆引き DNS レコードを設定する。

イ シリアル番号の桁数を増やす。

ウ ゾーン転送を禁止する。

エ 定期的に脆弱性検査と対策を実施する。

(2) 本文中の［ b ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア 会社名　　イ 担当者の電子メールアドレス

ウ 担当者の電話番号　　エ ディジタル証明書の所有者

(3) 本文中の下線⑤で，R 社のキャッシュ DNS サーバがインターネットから問合せ可能な状態であることによって発生する可能性のあるサイバー攻撃を，解答群の中から選び，記号で答えよ。

解答群

ア DDoS 攻撃　　イ SQL インジェクション攻撃

ウ パスワードリスト攻撃　　エ 水飲み場攻撃

(4) 本文中の［ c ］に入れるサイバー攻撃手法の名称を，15 字以内で答えよ。