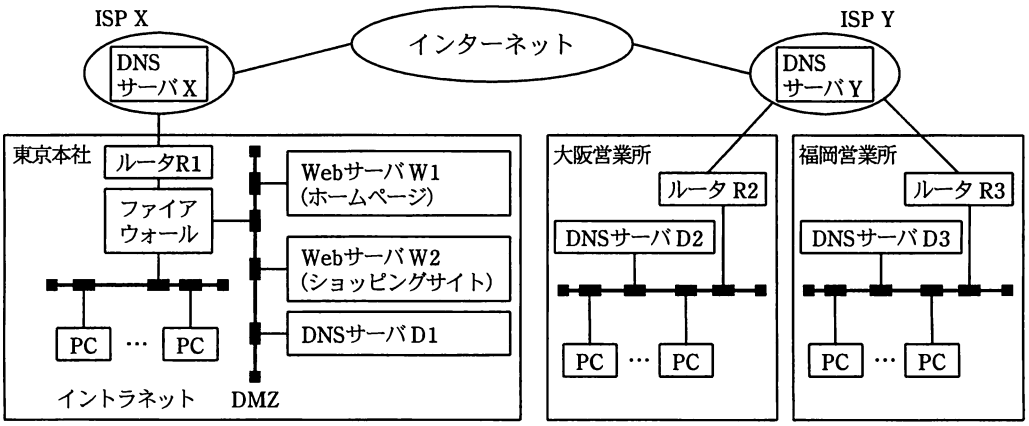
問9　DNS サーバのセキュリティ対策に関する次の記述を読んで，設問 1～4 に答えよ。

M 社は，ある製品の開発，販売を手掛ける企業であり，東京本社のほかに，大阪と福岡に営業所をもっている。自社のホームページは東京本社に設置した Web サーバ W1 で運営しており，自社製品のショッピングサイトは同じく東京本社に設置した別の Web サーバ W2 を使っている。M 社の Web サーバ W1，W2 のホスト名の情報は，東京本社に設置した DNS サーバ D1 で管理している。東京本社はインターネットサービスプロバイダ（以下，ISP という）X と，大阪営業所及び福岡営業所は ISP Y と契約してインターネットに接続している。M 社のネットワーク構成を図に示す。また，M 社の PC に設定されている DNS サーバの情報を表に示す。



注　ルータ R2，R3 には簡易なファイアウォール機能が備わっている。

図　M 社のネットワーク構成

表　M 社の PC に設定されている DNS サーバの情報

PC	DNS サーバの情報
東京本社の PC	DNS サーバ D1
大阪営業所の PC	DNS サーバ D2
福岡営業所の PC	DNS サーバ D3

あるとき，掲載されている商品を確認するために M 社のショッピングサイトにアクセスしていた福岡営業所の社員 A さんから，①「ホームページのリンクをクリックしてショッピングサイトにアクセスしようとしたところ，いつも表示されるショッピン

グサイトとは違うサイトが表示された。」という報告が東京本社に入った。M 社のネットワーク管理者 B さんが，東京本社と大阪営業所に在席する社員に指示し，各自の PC から，A さんの報告と同様の手順でショッピングサイトにアクセスさせてみたところ，A さんの報告のような状態にはならなかった。そこで，原因究明のためにセキュリティ対策会社である N 社に調査と対策の検討を依頼した。

しばらくした後，A さんから②「再度同様の手順でアクセスしたところ，今度は正しいショッピングサイトが表示された。」という報告が入った。

調査を開始した N 社の担当者 C さんは，東京本社に設置されている Web サーバ W1，W2 及び DNS サーバ D1 に改ざんの跡がないかを確認したが，コンテンツの異常や不正アクセスを示す証跡は発見されなかった。大阪営業所及び福岡営業所に設置されている PC のウイルスチェック結果や DNS サーバ D2 と D3 の状態も確認したが，異常は発見されなかった。さらに，ISP X 及び ISP Y にインシデントの発生状況について問い合わせたが，当該期間での発生はないとの回答を受けた。

調査結果から，C さんは“DNS キャッシュポイズニング”が今回の現象の原因だろうと判断した。C さんが取りまとめた調査結果の概略は，次のとおりである。

〔調査結果の概略〕

・福岡営業所で発生した現象は，DNS キャッシュポイズニングが原因だと推定される。
・具体的には，［ a ］の DNS キャッシュに偽りの情報が一時的に埋め込まれていたので，A さんからの報告の現象が発生した。
・DNS キャッシュポイズニングの攻撃手法は各種あるが，今回のものは 2008 年に公表されたカミンスキー・アタックである可能性が考えられる。
・［ a ］の DNS ソフトウェアのバージョンが古いので，早急にカミンスキー・アタック対策を施した最新版を導入するべきである。
・DNS キャッシュポイズニングへの根本的な対応策としては，DNS サーバからの応答に公開鍵暗号方式で署名する［ b ］の導入が望まれるが，利用可能になるまでしばらく時間が必要である。現時点では，東京本社，大阪営業所，福岡営業所の PC が参照する DNS サーバに偽りの情報が埋め込まれる可能性を低減する工夫をするべきである。

次は，調査完了後の B さんと C さんの会話である。

〔調査完了後の会話〕

C：今回の福岡営業所で発生した現象は，DNS キャッシュポイズニングが原因だったと思われます。DNS キャッシュポイズニングについては御存じですか。

B：名前は聞いたことがありますが，実際に発生したのを見たのは初めてです。

C：今後の対応策ですが，まずは今回の現象の内容について，M 社全体に知らせた方がよいでしょう。

B：どのような内容を知らせたらよいでしょうか。

C：第一報として，起こった事実を正確に伝えることが大切ですね。［ c ］と，［ d ］の 2 点は，必ず含めるようにしてください。DNS キャッシュポイズニングについては，別途時間を設けて，社員へのセキュリティ教育の一環で解説するのがよいと思います。

B：分かりました。文案を考えて，社内のポータルサイトなどで知らせるように手配します。ところで，福岡営業所の PC の DNS 設定はどうしたらよいでしょうか。ISP Y の DNS サーバ Y に変更すればよいですか。

C：それよりも，大阪営業所と福岡営業所の PC に設定する DNS サーバを，東京本社に設置されている DNS サーバ D1 に変更したらどうでしょう。

B：全社の PC が同じ DNS サーバを利用することで，管理対象の DNS サーバを一元化するわけですね。そうすると，ネットワーク全体の運用管理も単純化できます。

C：イントラネット間は，現在使っているインターネット接続を使って結ぶのが経済的ですね。東京本社と大阪営業所，福岡営業所の間を，［ e ］で結ぶわけです。

B：そうするには，東京本社と大阪営業所，福岡営業所が一つのネットワークになるので，PC に割り当てる［ f ］に重複がないか調査する必要がありますね。早速調べてみることにします。

C：DNS サーバ D1 は，現在 DNS コンテンツサーバの機能（Web サーバなどの情報をインターネットに提供する機能）と DNS キャッシュサーバの機能（社内の PC などからの問合せを中継する機能）を提供しています。DNS キャッシュサーバへの［ g ］からのアクセスを制限するために，DNS コンテンツサーバと DNS キャッシュサーバの機能を分離した方がよいですね。

B：その場合，DNS キャッシュサーバはネットワークのどこに配置すべきでしょうか。

C：今の DNS サーバ D1 と同じ DMZ に置くことも可能ですが，できれば PC などが置かれているイントラネットがよいでしょう。東京本社の PC と同様のセキュリティポリシによって，ファイアウォールで保護するのが適切だと思います。

設問 1　本文中の下線①，②の現象について，(1)，(2)に答えよ。

(1)　①のようにして，目的とは異なる Web サイトに誘導されて，その結果個人情報などを盗まれてしまう脅威の名称を解答群の中から選び，記号で答えよ。

解答群

ア　改ざん　　イ　ソーシャルエンジニアリング

ウ　盗聴　　エ　フィッシング

オ　不正侵入

(2)　①の状態から②の状態に変化した理由を，20 字以内で述べよ。

設問 2　C さんが取りまとめた調査結果の概略について，(1)，(2)に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を図中から選び，その名称を答えよ。

(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　DNSSEC　　イ　IPSEC　　ウ　PKI

エ　SSH　　オ　SSL

設問 3　本文中の［　c　］，［　d　］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　DNS サーバ X に問題があったこと

イ　DNS サーバ Y に問題があったこと

ウ　大阪営業所の PC に問題があったこと

エ　東京本社の各サーバに問題がなかったこと

オ　福岡営業所の DNS サーバ D3 に問題があったこと

カ　福岡営業所の PC に問題があったこと

設問 4　本文中の［　e　］～［　g　］に入れる適切な字句を答えよ。