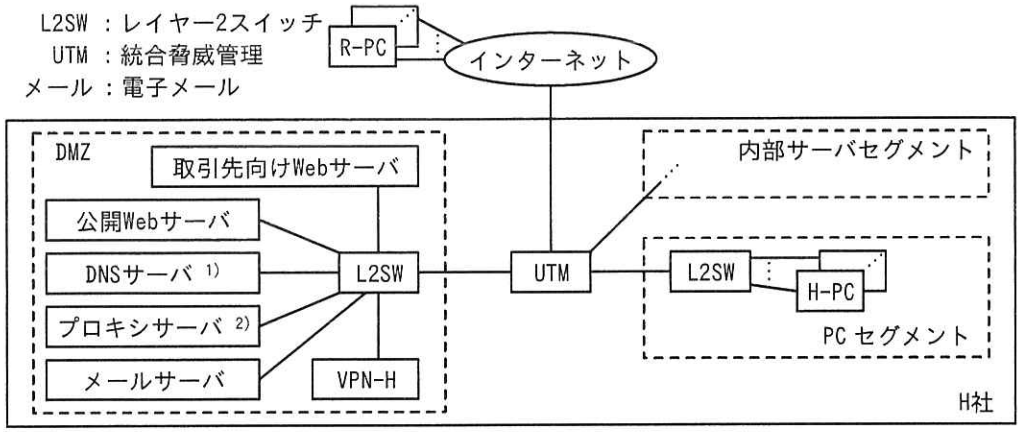
問２　サイバー攻撃への対策に関する次の記述を読んで，設問に答えよ。

H 社は，従業員 3,000 名の製造業であり，H 社製品の部品を製造する約 500 社と取引を行っている。取引先は，H 社に設置された取引先向け Web サーバに HTTPS でアクセスし，利用者 ID とパスワードでログインした後，H社との取引業務を行っている。また，公開 Web サーバでは，H 社製品の紹介に加え，問合せや要望の受付を行っている。いずれの Web サーバが停止しても，業務に支障が出る。

H 社では，社内に設置している PC（以下，H-PC という）とは別に，一部の従業員に対して，VPN クライアントソフトウェアを導入したリモート接続用 PC（以下，リモート接続用 PC を R-PC という）を貸与し，リモートワークを実現している。R-PC と H 社との間の VPN 通信には，VPN ゲートウェイ（以下，VPN ゲートウェイを VPN-GW といい，H 社が使用している VPN-GW を VPN-H という）を使用している。

H 社のネットワークは，情報システム部の L 部長と T 主任を含む 6 名で運用している。H 社のネットワーク構成を図 1 に示す。



注 1)　H 社ドメインの権威 DNS サーバと再帰的な名前解決を行うフルサービスリゾルバを兼ねる。
注 2)　H-PC からインターネットへの HTTP 及び HTTPS 通信を中継する。

図 1　H 社のネットワーク構成

UTM の機能概要及び設定を表 1 に，VPN-H の機能概要及び設定を表 2 に示す。

表 1　UTM の機能概要及び設定

機能名	機能概要	設定
ファイアウォール機能	ステートフルパケットインスペクション型であり，送信元の IP アドレスとポート番号，宛先の IP アドレスとポート番号の組合せによる通信の許可と拒否のルールによって通信を制御する。	有効
NAT 機能	（省略）	有効
IPS 機能	不正アクセスの検知方法は，次の 2 通りを設定できる。 アノマリ型　：あらかじめ登録したしきい値を超えた通信を異常として検知する。 シグネチャ型：あらかじめ登録したシグネチャと一致した通信を異常として検知する。	無効
WAF 機能	不正アクセスの検知方法は，IPS 機能と同様に，アノマリ型とシグネチャ型を設定できる。	無効

表 2　VPN-H の機能概要及び設定（抜粋）

機能名	機能概要	設定
VPN 通信機能	VPN クライアントソフトウェアを導入した PC との間で VPN 通信を行う。VPN 接続時の認証方式は，VPN クライアントソフトウェア起動時に表示されるダイアログボックス（以下，VPN ダイアログという）に，利用者 ID とパスワードを入力させる方式である。	有効
多要素認証機能	利用者 ID とパスワードによる認証方式に次のいずれかの認証方式を組み合わせた多要素認証を行う。 （ア）スマートフォンに SMS でセキュリティコードを送り，その入力を確認する方式 [1)] （イ）デジタル証明書によってクライアント認証を行う方式 （ウ）スマートフォンに承認要求のプッシュ通知を送り，その通知の承認を確認することで認証を行う方式	無効

注 [1)]　VPN ダイアログに利用者 ID とパスワードを入力し，その認証が完了すると，セキュリティコード入力画面が表示され，SMS でセキュリティコードがスマートフォンに送信される。送信されたセキュリティコードを，セキュリティコード入力画面に入力することで認証される。

最近，同業他社でサイバー攻撃による被害が 2 件立て続けに発生したという報道があった。1 件は，VPN-GW が攻撃を受け，社内ネットワークに侵入されて情報漏えいが発生した事案である。もう 1 件は，DDoS 攻撃による被害が発生した事案である。

H 社でも同様な事案が発生する可能性について，L 部長と T 主任が調査することにした。

〔VPN-GW への攻撃に対する調査〕

T 主任は，VPN-GW への攻撃方法を次のようにまとめた。

方法 1：VPN-GW の認証情報を推測し，社内ネットワークに侵入する。

方法 2：VPN-GW の製品名や型番を調査した上で，社内ネットワークへの侵入が可能になる脆弱性を調べる。もし，脆弱性が存在すればその脆弱性を悪用し，社内ネットワークに侵入する。

T 主任は，方法 1 については，VPN-H の認証強化を検討することにした。また，方法 2 については，VPN-H の脆弱性対策と，VPN-H へのポートスキャンに対する応答を返さないようにする方法（以下，ステルス化という）を検討することにした。方法 1 と方法 2 について T 主任がまとめた対策案を表 3 に示す。

表 3　方法 1 と方法 2 について T 主任がまとめた対策案

攻撃方法	対策	対策名	内容
方法 1	V-1	VPN-H の認証強化	インターネットから VPN-H へのアクセス時は，多要素認証を用いる。
方法 2	V-2	VPN-H の脆弱性対策	（省略）
	V-3	ステルス化	VPN-H のポートを通常は応答を返さないように設定しておく。H 社が許可した PC からのアクセス時だけ，接続を許可する。

〔DDoS 攻撃に対する調査〕

次に，T 主任は，DDoS に関連する攻撃について調査し，H 社で未対策のものを表 4 にまとめた。

表 4　H 社で未対策の DDoS に関連する攻撃

項番	攻撃	例
1	UDP Flood 攻撃	公開 Web サーバ，DNS サーバを攻撃対象に，偽の送信元 IP アドレスとランダムな宛先ポート番号を設定した UDP データグラムを大量に送り付ける。
2	SYN Flood 攻撃	（省略）
3	DNS リフレクション攻撃の踏み台にされる	（省略）
4	HTTP GET Flood 攻撃	a

次は，表 4 についての T 主任と L 部長の会話である。

T 主任 ：項番 1，2，4 の DDoS 攻撃のサーバへの影響は，UTM の IPS 機能と WAF 機能で軽減することができます。

L 部長 ：そうか。機能の設定に関する注意点はあるのかな。

T 主任 ：例えば，アノマリ型 IPS 機能で，トラフィック量について，しきい値が高すぎる場合にも，①しきい値が低すぎる場合にも弊害が発生するので，しきい値の設定には注意するようにします。また，項番 3 の対策として，現在の DNS サーバを廃止して，権威 DNS サーバの機能をもつサーバ（以下，DNS-K という）とフルサービスリゾルバの機能をもつサーバ（以下，DNS-F という）を社内に新設します。インターネットから社内への DNS 通信は b への通信だけを許可し，社内からインターネットへの DNS 通信は c からの通信だけを許可します。

〔対策 V-1 についての検討〕

次は，対策 V-1 についてのL部長とT主任の会話である。

L部長 ：対策 V-1 での注意点はあるのかな。

T主任 ：最近は，多要素認証の利用が多くなってきたこともあり，多要素認証を狙った攻撃が発生しています。多要素認証を狙った攻撃例を表5に示します。

表5　多要素認証を狙った攻撃例

攻撃例	概要
攻撃例1	表2（ア）と組み合わせた多要素認証を突破するフィッシング攻撃であり，次の手順で行われる。 (1)　攻撃者が，フィッシングメールを使って，VPN ダイアログの画面を装った罠（わな）の Web サイトに正規利用者を誘導し，正規利用者に利用者 ID とパスワードを入力させる。 (2)　[d] (3)　[e] (4)　攻撃者が，社内ネットワークに不正に接続する。
攻撃例2	表2（ウ）と組み合わせた多要素認証を突破する多要素認証疲労攻撃であり，次の手順で行われる。 （省略）

L部長 ：攻撃例1については，不正なリモート接続を阻止するために，メールで受信したメッセージ内の URL リンクを安易にクリックしないよう注意喚起する必要があるな。

T主任 ：はい。しかし，当社では，業務の手続の督促などで従業員に URL リンクが含まれるメールを送っているので，URL リンクのクリックを禁止することはできません。不審な URL かどうかを見極めさせることは難しいでしょう。そこで，②たとえ罠の Web サイトへの URL リンクをクリックしてしまっても，不正なリモート接続をされないように，従業員全員が理解できる内容を，注意喚起する必要があります。

〔対策 V-3 についての検討〕

次は，対策 V-3 についての L 部長と T 主任の会話である。

L 部長 ：対策 V-3 について説明してほしい。

T 主任 ：VPN-H には，どのような通信要求に対しても応答しない“Deny-All”を設定した上で，あらかじめ設定されている順番にポートに通信要求した場合だけ所定のポートへの接続を許可するという設定（以下，設定 P という）があります。

L 部長 ：設定 P の注意点はあるのかな。

T 主任 ：設定されている順番を攻撃者が知らなくても，③攻撃者が何らかの方法でパケットを盗聴できた場合，設定 P を突破されてしまいます。

L 部長 ：設定 P とは別の方法はあるのかな。

T 主任 ：VPN-H の機能にはありませんが，SPA（Single Packet Authorization）というプロトコルがあります。SPA の主な仕様を表 6 に示します。

表 6　SPA の主な仕様

項番	内容
1	TCP の SYN パケット又は UDP の最初のパケット（以下，SPA パケットという）には，HMAC ベースのワンタイムパスワードが含まれており，送信元の真正性を送信先が検証できる。検証に成功すれば，以降の通信のパケットは許可される。検証に失敗すれば，以降の通信のパケットは破棄される。
2	SPA パケットにはランダムデータが含まれており，送信先で検証される。以前受信したものと同じランダムデータをもつ SPA パケットを受信した場合は，破棄される。
3	SPA パケットの最後尾フィールドには先行フィールドのハッシュ値が格納されている。送信先では，この値を検証し，検証に失敗すれば，そのパケットは破棄される。
4	送信先では，検証した結果は，送信元に返さない。

T 主任 ：SPA なら，④攻撃者が何らかの方法でパケットを盗聴できたとしても，突破はされません。

L 部長 ：そうか。VPN 通信機能と同様の機能をもち，SPA を採用している製品があるかどうか，ベンダーに相談してみよう。

L 部長がベンダーに相談したところ，S 社が提供しているアプライアンス（以下，S-APPL という）の紹介があった。L 部長と T 主任は，S-APPL の導入検討を進めた。

〔S-APPL の導入検討〕

S-APPL は，VPN 通信機能，SPA パケットを検証する機能などをもつ。S-APPL と接続するためには，S-APPL のエージェントソフトウェア（以下，S ソフトという）を接続元の PC に導入し，接続元の PC ごとの ID と秘密情報を，S-APPL と接続元の PC それぞれに設定する必要がある。なお，秘密情報は，SPA パケットの HMAC ベースのワンタイムパスワードの生成などに使われる。S-APPL と S ソフトの主な機能を表 7 に示す。

表 7　S-APPL と S ソフトの主な機能

項番	機能名	機能概要
1	SPA 機能	SPA パケットを用いて送信元の真正性を S-APPL が検証する。
2	VPN 通信機能	S-APPL と S ソフトを導入した PC との間で VPN を確立する。
3	多要素認証機能	VPN-H の多要素認証機能と同じ機能をもつ。
4	接続サーバ許可機能	VPN 確立後にアクセス可能なサーバを PC ごとに設定する。

T 主任は，対策 V-1～3 について，次のように考えた。

・対策 V-1 については，表 7 項番 3 の機能で対応する。方式は，表 2（イ）の方式を採用する。

・対策 V-2 については，S-APPL の脆弱性情報を収集し，脆弱性修正プログラムが公開されたら，それを適用する。

・対策 V-3 については，表 7 項番 1 の機能で対応する。

T 主任は，対策 V-3 のための H 社のネットワーク構成の変更案を作成した。なお，変更する際は，次の対応が必要になる。

(1)　VPN-H を S-APPL に置き換える。R-PC には，S ソフトを導入する。

(2)　R-PC ごとの ID と秘密情報を，S-APPL と R-PC それぞれに設定する。

(3)　VPN-H に付与していた IP アドレスを S-APPL に付与する。

(4)　S-APPL の FQDN を DNS サーバに登録する。

T 主任は，S-APPL の導入によって VPN-GW への攻撃の対策が可能であることを L 部長に説明した。L 部長は，効果とリスクを検討した上で，S-APPL を導入することを決めた。

〔DDoS 攻撃に対する具体的対策の検討〕

T 主任は，表 4 の項番 3 以外に対する具体的対策の検討に着手した。

まず，通信回線については，DDoS 攻撃で大量のトラフィックが発生すると，使えなくなる。これについては，通信回線の帯域を大きくするという方法のほか，⑤外部のサービスを利用するという方法があることが分かった。

次に，サーバへの影響は，これまでに検討した UTM の IPS 機能と WAF 機能を有効化することで軽減できることが分かっている。加えて，取引先向け Web サーバについては，次の対応によって，⑥更に DDoS 攻撃の影響を軽減できることが分かった。

・取引先には，H 社との取引専用の PC（以下，取引専用 PC という）を貸与する。取引専用 PC には，S ソフトを導入する。
・取引専用 PC ごとの ID と秘密情報を，S-APPL と取引専用 PC それぞれに設定する。
・S-APPL に，取引専用 PC が VPN 確立後にアクセス可能なサーバとして，取引先向け Web サーバだけを設定する。
・UTM のファイアウォール機能で，インターネットから取引先向け Web サーバへの通信を拒否するように設定する。

その後，H 社では，S-APPL の導入，UTM の設定変更，DNS サーバの変更などを行い，新たな運用を開始した。

設問１　〔DDoS 攻撃に対する調査〕について答えよ。

(1)　表 4 中の［　a　］に入れる攻撃の例を，H 社での攻撃対象を示して具体的に答えよ。

(2)　本文中の下線①の場合に発生する弊害を，25 字以内で答えよ。

(3)　本文中の［　b　］，［　c　］に入れる適切な字句を，“DNS-F”又は“DNS-K”から選び答えよ。

設問２　〔対策 V-1 についての検討〕について答えよ。

(1)　表 5 中の［　d　］，［　e　］に入れる，不正な接続までの攻撃手順を，具体的に答えよ。

(2)　本文中の下線②について，注意喚起の内容を，具体的に答えよ。

設問３　〔対策 V-3 についての検討〕について答えよ。

(1)　本文中の下線③について，設定 P を突破する方法を，30 字以内で答えよ。

(2)　本文中の下線④について，突破されないのはなぜか。40 字以内で答えよ。

設問４　〔DDoS 攻撃に対する具体的対策の検討〕について答えよ。

(1)　本文中の下線⑤について，利用する外部のサービスを，20 字以内で具体的に答えよ。

(2)　本文中の下線⑥について，軽減できる理由を，40 字以内で答えよ。