問２　クラウドセキュリティに関する次の記述を読んで，設問1～6に答えよ。

C社は，従業員150名の個人向けの投資コンサルティング会社である。金融商品や不動産投資に詳しいファイナンシャルプランナ60名からなる事業部，50名の営業部，20名の企画部，20名の経営管理部がある。顧客の投資診断や運用の提案を行うロボットアドバイザサービスが好調で，創立5年目で売上高が30億円を超える会社に成長を遂げた。

CEOは，顧客満足度と従業員満足度の向上を目指して，次期ITに関して次のような方針を示している。

次期ITの方針1：サービスを更に向上させるために積極的にITを活用する。特にSaaSを活用する。

次期ITの方針2：働き方改革及びパンデミック対策の観点から，テレワーク環境を整備する。

C社では，経営管理部内の総務グループ（以下，総務Gという）の5名が情報システムの管理を担当している。

C社の現在の情報システム概要は，図1のとおりである。

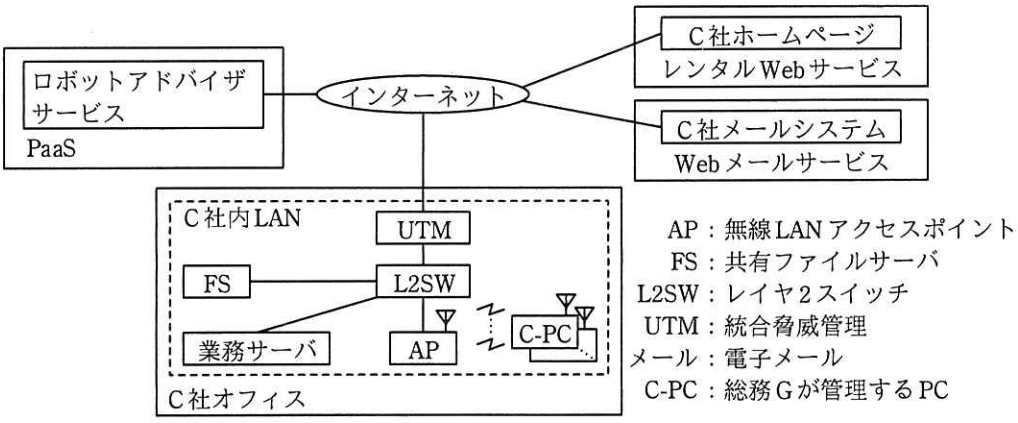


図1　C社の現在の情報システム概要

UTM は，ステートフルパケットインスペクション型ファイアウォールに複数のセキュリティ機能を統合したものである。DHCP サーバの機能も備えており，AP に接続する機器に 192.168.1.20～192.168.1.240 の範囲の IP アドレスを配布している。

C 社内 LAN のネットワークセグメントは一つだけである。有線で L2SW に接続している機器には固定の IP アドレスを割り当てている。無線 LAN は WPA2 パーソナルで運用しており，SSID 及び事前共有鍵を従業員に開示している。

C 社は，従業員に 1 人 1 台の C-PC を貸与している。OS のドメインコントローラは導入しておらず，従業員は貸与された C-PC にローカルログインする。C-PC は AP に接続し，インターネットへのアクセスが可能である。事業部及び企画部では，顧客への提案や企画の立案時にインターネット上にある多くの情報を収集，取捨選択，加工することによって付加価値を生み出すことが不可欠であると認識している。その他の部門では，取引先などの企業情報検索と出張先への経路の検索にインターネットを利用している。

PC，スマートフォンなどの個人所有の機器（以下，個人所有機器という）の C 社内 LAN への接続は統制しておらず，多くの従業員は，個人所有機器を AP に接続して使用している。また，業務で新たに SaaS を利用する際，会社で統一された承認ルールはなく，各部の判断で SaaS の利用契約を締結している。

〔一つ目のトラブル〕

新入社員が配属されたある日，C-PC で障害が発生しているという連絡が総務 G に入った。総務 G の A さんが調査したところ，次のような状況であった。

・朝の時点では，C-PC や個人所有機器の利用について特に異常を感じた従業員はいなかった。

・営業部の U さんが 13 時に出張から戻り C-PC を起動したところ，C-PC へのローカルログインはできたが，業務サーバにアクセスできず，メールの送受信もインターネット上の Web サイトの閲覧もできなかった。

・この後に起動した C-PC や接続しようとした個人所有機器の多くで同様の障害が発生していたが，何台かの C-PC や個人所有機器では障害が発生していなかった。障害が発生していたものと発生していなかったものとで，障害原因になるような違いは見当たらなかった。

Aさんは，障害が発生していたC-PCのネットワーク設定を調べたところ，①上位2オクテットが169.254に設定されたIPアドレスで動作していることに気付いた。C社は雑居ビルの中にあって誰でもC社オフィスに近づくことが可能なので，偽のDHCPサーバが立ち上げられたなど，何らかのサイバー攻撃を受けているのではないかと心配になり，経営管理部のE部長に報告した。E部長は，専門家の助言が必要と考え，C社内LANの構築で支援を受けたD社に依頼した。

D社のセキュリティコンサルタントである情報処理安全確保支援士（登録セキスペ）のKさんは，Aさんから説明を受け，次のようにコメントした。

コメント1：障害が発生したC-PCのIPアドレスは，DHCPサーバが正常に動作していない場合にしばしば確認される。偽のDHCPサーバの設置ではなく，②C社内LANでの個人所有機器の利用が原因で問題が引き起こされた結果である。個人所有機器の利用が原因であれば，DHCPサーバの設定変更で当面の障害に対処し，C社内での個人所有機器の利用を見直していくのがよい。

コメント2：念のために，③UTM以外にDHCPサーバが稼働しているかどうかも調査するとよい。

コメントを受け，Aさんが調査したところ，UTM以外にDHCPサーバは確認できなかった。このことから，サイバー攻撃を受けているわけではないと判断し，DHCPサーバの設定を変更した。

〔二つ目のトラブル〕

DHCPサーバに起因するトラブル（以下，トラブル1という）が解決した直後，企画部が最近利用し始めたビジネスチャットサービスR（以下，サービスRという）という無料のSaaSにおいて，別のトラブル（以下，トラブル2という）が発生した。

トラブル2の報告を受けたAさんが調査したところ，次のような状況であった。

状況1：企画部の部員がサービスRに開設したチャットエリアにおいて，模造サングラス販売の不正サイトに誘導するチャットが，部員のVさんのアカウントから連続して書き込まれた。Vさん本人は，身に覚えがないとのことだった。

状況2：企画部では，以前からサービスWというSNSを使って公開情報を発信して

いる。Vさんを含む部員の数名は，会社のメールアドレスをサービスRとサービスWの利用者IDとして登録し，両方のサービスで同じパスワードを設定していた。サービスWでは，パスワード漏えいの事故があり，企画部の部員は全員がサービスWのパスワードを変更したが，誰もサービスRのパスワードは変更しなかった。

状況3：外部の何者かがサービスR内の情報に不正にアクセスし情報を持ち出していないかを調査するため，サービスRの提供会社にアクセスログを提供してもらえないかと問い合わせたが，無料のサービスについては提供できないという回答だった。

状況1～3から，Aさんは，サービスRのアカウントが乗っ取られている可能性が高いので全員のパスワードをすぐに変更すべきであることと，サービスRでどのような情報にアクセスされたかはログが入手できないので調査が困難であることをE部長に報告した。E部長は，状況3について，仮に情報漏えいがあった場合，最大でどの程度の被害となり得るかを判断するために，④アクセスログの調査以外に実施できる調査を指示した。Aさんは，総務Gのほかの部員にも協力を仰ぎ，指示された調査を実施して結果をまとめた。

E部長は，調査の結果を確認し，今回は大きな被害はなかったと判断したが，情報セキュリティ対策の強化が急務であると感じた。そこで，業務における個人所有機器及びSaaSの利用を統制すべきとCEOに提言した。CEOは，統制の必要性に合意したが，一方で，過剰に統制すると従業員のビジネスマインドを阻害しかねないので，統制レベルを慎重に検討するよう指示した。

〔次期ITのセキュリティ要件〕

E部長は，トラブル1及びトラブル2の再発防止策，並びに次期ITの方針を踏まえて，統制の実現に向けた次期ITのセキュリティ要件を表1のように整理した。

表1　次期ITのセキュリティ要件

要件	内容
要件1	APには，C-PCだけを接続できるようにする。
要件2	業務での個人所有機器の利用を禁止する。テレワークに必要なPCは貸与する。
要件3	パスワードの使い回しを防ぎ，従業員がパスワードを管理する負担を軽減するため，SaaSへのログインを統合する。
要件4	業務で利用するSaaSは，総務Gが契約したSaaSだけに制限する。また，業務に不要なWebサイトへのアクセスを制限する。ただし，業務での情報収集は妨げないようにする。
要件5	総務Gが契約したSaaSには，総務Gが管理するアカウントでアクセスする。C-PCからは，従業員が個人で管理するアカウントでのアクセスができないようにする。
要件6	業務で利用するSaaSは，その安全性を総務Gが判断した上で契約する。
要件7	業務で利用するSaaSからの情報漏えいを防ぐための技術的対策を導入する。

〔要件1の検討〕

APへの接続方式をWPA2エンタープライズにし，APへの接続時にIEEE 802.1X（以下，802.1Xという）でのディジタル証明書による認証を行う。

802.1Xのシーケンスを図2に示す。

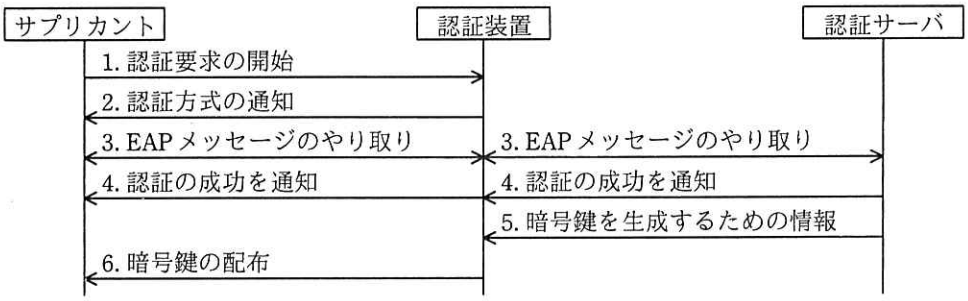


図2　802.1Xのシーケンス（概要）

図2中のサプリカントには図1中の［　a　］が，図2中の認証装置には図1中の［　b　］が該当する。C-PCのIPアドレスは，図2中の［　c　］，DHCPサーバから割り当てられる。

〔要件2及び3の検討〕

要件2については，業務で利用するC社の情報システムやSaaSへのアクセスの際，機器をクライアント認証することにした。また，要件3については，SaaSへのアク

セスにおける認証と認可に，インターネット上の認証サービスである IDaaS を利用することにした。

代表的な IDaaS であるサービス Q について調査した。サービス Q の概要を表 2 に示す。

表 2　サービス Q の概要

番号	分類	内容
1	提供形態	クラウドサービスとして機能を提供している。
2	接続元の認証	次の方式又はその組合せで認証することができる。 - 利用者 ID 及びパスワード - ディジタル証明書による TLS クライアント認証 [1)] - ワンタイムパスワードデバイス又は SMS を使ったワンタイムパスワード - 生体認証
3	SaaS との連携	SAML を採用している SaaS と連携できる。連携した SaaS にはシングルサインオンできる。

注 [1)]　ディジタル証明書は，クレデンシャルとともに検証する。

C 社の各部と議論を重ねた結果，幾つかの SaaS を総務 G で契約し，管理して提供すれば，ほとんどの業務が行えることが分かった。これらの SaaS は全て SAML 認証に対応しており，サービス Q と連携できることも確認できた。また，ディジタル証明書だけで認証することもでき，従業員がパスワードを管理する負担の軽減につながるので，サービス Q を採用することにした。

C 社オフィス外での業務については，モバイル PC を追加で購入し，モバイル PC を持ち出し用の C-PC（以下，持出 C-PC という）として貸与することにした。

〔要件 4 及び 5 の検討〕

要件 4 を満たすためには，総務 G が契約した SaaS へのアクセスについてサービス Q での認証を必須にするだけでなく，総務 G が契約していない SaaS やインターネット上の様々な Web サイトへのアクセスも制御する必要がある。しかし，総務 G が契約した SaaS，企業情報検索，出張先への経路検索及び C 社の情報システムへのアクセスだけを許可し，それ以外へのアクセスを全て遮断すると，⑤支障が出る業務がある。

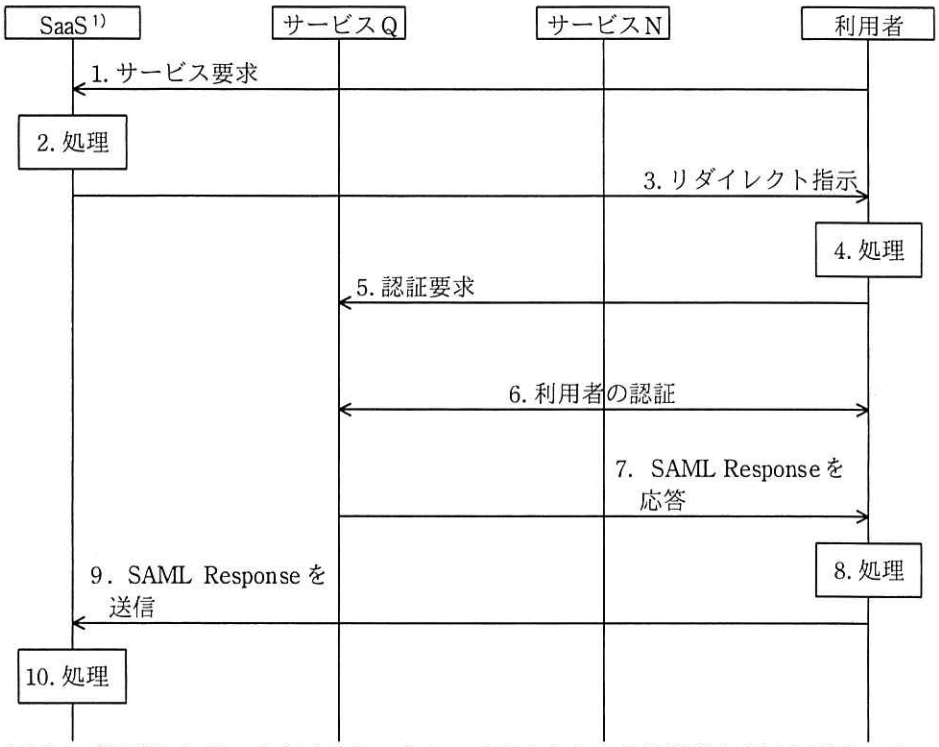
調査を更に進めた結果，要件4及び5の実現に利用できそうなサービスがあることが分かった。機器からインターネットへの通信を中継するプロキシ型のクラウドサービスである。その一つにサービスNがある。サービスNを利用するには，機器からインターネットへの通信を全てサービスN経由で行うなどの制御を行う端末制御エージェントソフトウェア（以下，Pソフトという）を機器に導入する必要がある。管理者は，Pソフトを，一般利用者権限では動作の停止やアンインストールができないように設定することができる。

サービスNの機能を表3に示す。

表3　サービスNの機能（抜粋）

番号	機能名	内容
1	利用者IDによるフィルタリング機能	・Pソフトで，SaaSへのログイン時に，許可された利用者IDの場合だけ通信を許可し，その他の利用者IDの場合は通信を遮断する。 ・許可する利用者IDは，管理者がSaaSごとに設定できる。
2	URLフィルタリング機能	・サービスNが中継する際に，アクセス可能なURLを制限する。 ・制限するURLのリストはベンダから提供され，例えば，“ショッピング”，“犯罪・暴力”，“金融・経済”などWebサイトの内容による分類や，“オンラインストレージ”，“アップローダ”などのWebサービスの機能による分類がされており，管理者が選択できる。 ・制限するURLは，管理者が追加及び削除できる。
3	可視化機能	・中継する通信を監視し，統計情報をログとして提供する。 ・一部のSaaSについては，そのSaaSが提供するAPIを使って，アクセスログを収集できる。
4	保管時の自動暗号化機能	・一部のSaaSに対し，そのSaaSが提供するAPIを使って，特定フォルダに保管するファイルを自動的に暗号化することができる。 ・暗号鍵は，利用者ごと又は社内共通にすることができる。

要件4及び5は，サービスQとサービスNを組み合わせて実現する。サービスQとサービスNを利用した場合の動作の概要を図3に示す。



注記1　図中の“処理”には，先行するシーケンスを入力とした条件判断などの処理と，そのまま次のシーケンスにリダイレクトする処理がある。

注記2　サービスNの処理などは記述を省略している。

注 1)　総務Gが契約しているSaaSである。

図3　サービスQとサービスNを利用した場合の動作の概要

図3において，⑥総務Gが管理していない機器からのサービス要求があった場合は，シーケンスが途中で遮断される。

調査の結果，サービスQとサービスNを利用することで要件4及び5を実現できると判断し，サービスNを採用することにした。

〔要件6及び7の検討〕

要件6については，C社では，SaaSを契約するに当たって，⑦SaaS又はSaaS事業者が何らかのセキュリティ規格に準拠していることの第三者による認証を確認するか，SaaS事業者が自ら発行するホワイトペーパを確認することにした。

要件7については，SaaSで重要な情報を扱う場合，当該SaaSで利用可能ならば表3中の番号［　d　］の機能を利用する。それによって，サービスNを経由しない

不正アクセスによる SaaS からの情報漏えいを防ぐことで，要件 7 に対応することにした。

〔次期 IT への移行〕

C-PC は管理者権限による管理を総務 G が行い，従業員には一般利用者権限だけを与えることにした。また，⑧持出 C-PC は，セキュリティ設定とソフトウェアなどの導入を行ってから従業員に貸与することにした。

検討を進めた次期 IT への移行計画は承認され，C 社の情報システムは次期 IT に移行された。

設問 1　〔一つ目のトラブル〕について，(1)～(3)に答えよ。

(1) 本文中の下線①は何と呼ばれているか。解答群の中から選び，記号で答えよ。

解答群

ア　グローバルアドレス　　イ　プライベートアドレス

ウ　ブロードキャストアドレス　　エ　マルチキャストアドレス

オ　リンクローカルアドレス　　カ　ループバックアドレス

(2) 本文中の下線②について，C 社内 LAN での個人所有機器のどのような利用状況によって，どのような問題が引き起こされたか。60 字以内で具体的に述べよ。

(3) 本文中の下線③について，UTM 以外に DHCP サーバが稼働しているかどうかをどのように調査するのか。UTM の DHCP サーバを稼働させたまま行う方法と停止させて行う方法を，それぞれ 55 字以内で具体的に述べよ。

設問 2　本文中の下線④について，アクセスログ以外に何を調査すべきか。調査すべきものを 40 字以内で述べよ。

設問 3　〔要件 1 の検討〕について，(1)，(2)に答えよ。

(1) 本文中の［　a　］，［　b　］に入れる適切な字句を，図 1 中の用語で答えよ。

(2) 本文中の［　c　］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　“1.”より前に　　イ　“3.”と同時に

ウ　“6.”と同時に　　エ　“6.”より後に

設問4　〔要件4及び5の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線⑤で示した，C社において支障が出る業務とは何か。一つ挙げ25字以内で述べよ。

(2) 要件4は，表3中のどの機能で実現できるか。表3中の番号で一つ答えよ。

(3) 要件5は，表3中のどの機能で実現できるか。表3中の番号で一つ答えよ。

(4) 本文中の下線⑥について，図3中のどの段階で遮断されるかを，解答群から選び，記号で答えよ。また，総務Gが管理していない機器かどうかはどのような方法で判定するか。判定の方法を30字以内で具体的に述べよ。

解答群

ア　1.～2.　　イ　3.～4.　　ウ　5.～6.

エ　7.～8.　　オ　9.～10.

設問5　〔要件6及び7の検討〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑦について，規格又は認証の例を20字以内で答えよ。

(2) 本文中の［　d　］に入れる適切な番号を，表3中の番号で一つ答えよ。

設問6　〔次期ITへの移行〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑧について，要件2を満たし，そのセキュリティ設定が従業員によって無効にされないためには，どのように設定する必要があるか。30字以内で述べよ。

(2) 本文中の下線⑧について，要件4及び5を満たし，それを維持するためには，どのソフトウェアをどのように設定する必要があるか。40字以内で述べよ。