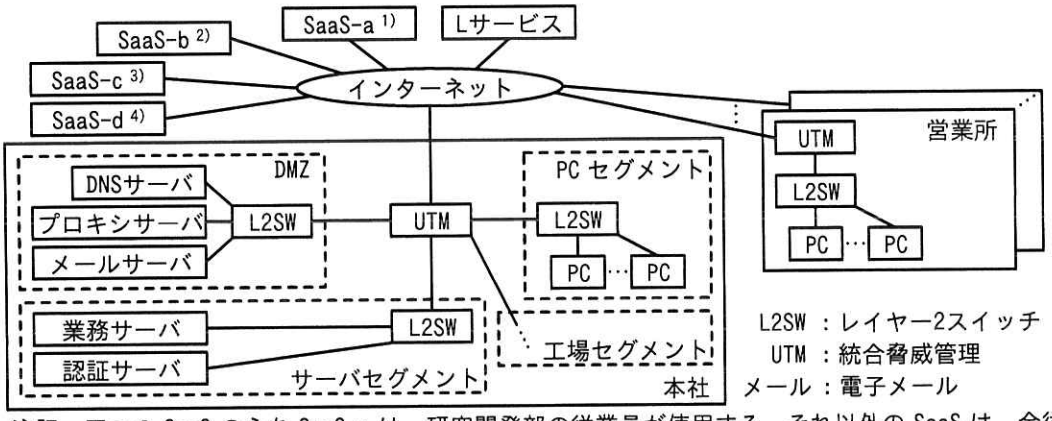
問３　クラウドサービス利用に関する次の記述を読んで，設問に答えよ。

Q 社は，従業員 1,000 名の製造業であり，工場がある本社及び複数の営業所から成る。Q 社には，営業部，研究開発部，製造部，総務部，情報システム部がある。Q 社のネットワークは，情報システム部の K 部長と S 主任を含む 6 名で運用している。

Q 社の従業員には PC 及びスマートフォンが貸与されている。PC の社外持出しは禁止されており，PC の Web ブラウザからインターネットへのアクセスは，本社のプロキシサーバを経由する。Q 社では，業務で SaaS-a，SaaS-b，SaaS-c，SaaS-d という四つの SaaS，及び L サービスという IDaaS を利用している。Q 社のネットワーク構成を図 1 に，図 1 中の主な構成要素並びにその機能概要及び設定を表 1 に示す。



注記　四つの SaaS のうち SaaS-a は，研究開発部の従業員が使用する。それ以外の SaaS は，全従業員が使用する。

注 1)　SaaS-a は，外部ストレージサービスであり，URL は，https://△△△-a.jp/ から始まる。

注 2)　SaaS-b は，営業支援サービスであり，URL は，https://○○○-b.jp/ から始まる。

注 3)　SaaS-c は，経営支援サービスであり，URL は，https://□□□-c.jp/ から始まる。

注 4)　SaaS-d は，Web 会議サービスであり，URL は，https://●●●-d.jp/ から始まる。

図 1　Q 社のネットワーク構成

表 1　図 1 中の主な構成要素並びにその機能概要及び設定

構成要素	機能名	機能概要	設定
認証サーバ	認証機能	従業員が PC にログインする際，利用者 ID とパスワードを用いて従業員を認証する。	有効
プロキシサーバ	プロキシ機能	PC からインターネット上の Web サーバへの HTTP 及び HTTPS 通信を中継する。	有効

表1　図1中の主な構成要素並びにその機能概要及び設定（続き）

構成要素	機能名	機能概要	設定
Lサービス	SaaS連携機能	SAMLで各SaaSと連携する。	有効
	送信元制限機能	契約した顧客が設定したIPアドレス[1)]からのアクセスだけを許可する。それ以外のアクセスの場合，拒否するか，Lサービスの多要素認証機能を動作させるかを選択できる。	有効[2)]
	多要素認証機能	次のいずれかの認証方式を，利用者IDとパスワードによる認証方式と組み合わせる。 （ア）スマートフォンにSMSでワンタイムパスワードを送り，それを入力させる方式 （イ）TLSクライアント認証を行う方式	無効
四つのSaaS	IDaaS連携機能	SAMLでIDaaSと連携する。	有効
UTM	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，IPアドレス，ポート，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[3)]
	NAT機能	（省略）	有効
	VPN機能	IPsecによるインターネットVPN通信を行う。拠点間VPN通信を行うこともできる。	有効[4)]

注[1)]　IPアドレスは，複数設定できる。

注[2)]　本社のUTMのグローバルIPアドレスを送信元IPアドレスとして設定している。設定しているIPアドレス以外からのアクセスは拒否する設定にしている。

注[3)]　インターネットからの通信で許可されているのは，本社のUTMではDMZのサーバへの通信及び営業所からのVPN通信だけであり，各営業所のUTMでは一つも許可していない。

注[4)]　本社のUTMと各営業所のUTMとの間でVPN通信する設定にしている。そのほかのVPN通信の設定はしていない。

〔Lサービスの動作確認〕

Q社のPCがSaaS-aにアクセスするときの，SP-Initiated方式のSAML認証の流れを図2に示す。

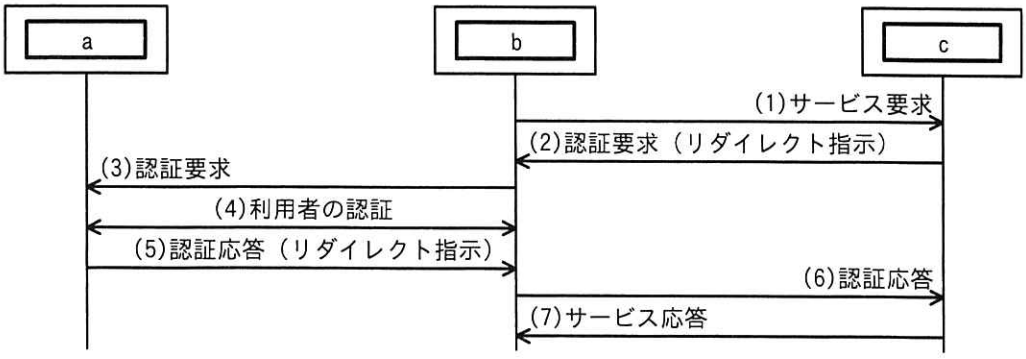


図2　SAML認証の流れ

ある日，同業他社の J 社において，SaaS-a の偽サイトに誘導されるというフィッシング詐欺にあった結果，SaaS-a に不正アクセスされるという被害があったと報道された。しかし，Q 社の設定では，仮に，同様のフィッシング詐欺のメールを受けて SaaS-a の偽サイトに L サービスの利用者 ID とパスワードを入力してしまう従業員がいたとしても，①攻撃者がその利用者 ID とパスワードを使って社外から L サービスを利用することはできない。したがって，S 主任は，報道と同様の被害に Q 社があうおそれは低いと考えた。

〔在宅勤務導入における課題〕

Q 社は，全従業員を対象に在宅勤務を導入することになった。そこで，リモート接続用 PC（以下，R-PC という）を貸与し，各従業員宅のネットワークから本社のサーバにアクセスしてもらうことにした。しかし，在宅勤務導入によって新たなセキュリティリスクが生じること，また，本社への通信が増えて本社のインターネット回線がひっ迫することが懸念された。そこで，K 部長は，ネットワーク構成を見直すことにし，その要件を表 2 にまとめた。

表 2　ネットワーク構成の見直しの要件

要件	内容
要件 1	本社のインターネット回線をひっ迫させない。
要件 2	L サービスに接続できる PC を，本社と営業所の PC 及び R-PC に制限する。なお，従業員宅のネットワークについて，前提を置かない。
要件 3	R-PC から本社のサーバにアクセスできるようにする。ただし，UTM のファイアウォール機能には，インターネットからの通信を許可するルールを追加しない。
要件 4	HTTPS 通信の内容をマルウェアスキャンする。
要件 5	SaaS-a 以外の外部ストレージサービスへのアクセスは禁止とする。また，SaaS-a へのアクセスは業務で必要な最小限の利用者に限定する。

K 部長がベンダーに相談したところ，R-PC，社内，クラウドサービスの間の通信を中継する P 社のクラウドサービス（以下，P サービスという）の紹介があった。P サービスには，次のいずれかの方法で接続する。

・IPsec に対応した機器を介して接続する方法

・P サービスのエージェントソフトウェアを R-PC に導入し，当該ソフトウェアによ

って接続する方法

P サービスの主な機能を表 3 に示す。

表 3　P サービスの主な機能

項番	機能名	機能概要
1	L サービス連携機能	・R-PC から P サービスを経由してアクセスする SaaS での認証を，L サービスの SaaS 連携機能及び多要素認証機能を用いて行うことができる。 ・L サービスの送信元制限機能には，P サービスに接続してきた送信元の IP アドレスが通知される。
2	マルウェアスキャン機能	・送信元からの TLS 通信を終端し，復号してマルウェアスキャンを行う。マルウェアスキャンの完了後，再暗号化して送信先に送信する。これを実現するために，［　d　］を発行する［　e　］を，［　f　］として，PC にインストールする。
3	URL カテゴリ単位フィルタリング機能	・アクセス先の URL カテゴリと利用者 ID との組みによって，“許可”又は“禁止”のアクションを適用する。 ・URL カテゴリには，ニュース，ゲーム，外部ストレージサービスなどがある。 ・各 URL カテゴリに含まれる URL のリストは，P 社が設定する。
4	URL 単位フィルタリング機能	・アクセス先の URL のスキームからホストまでの部分 [1]と利用者 ID との組みによって，“許可”又は“禁止”のアクションを適用する。
5	通信可視化機能	・中継する通信のログを基に，クラウドサービスの利用状況の可視化を行う。本機能は，［　g　］の機能の一つである。
6	リモートアクセス機能	・P コネクタ [2]を社内に導入することによって，社内と社外の境界にあるファイアウォールの設定を変更せずに社外から社内にアクセスできる。

注 [1]　https://▲▲▲.■■■/ のように，“ https:// ”から最初の“ / ”までを示す。
注 [2]　P 社が提供する通信機器である。P コネクタと P サービスとの通信は，P コネクタから P サービスに接続を開始する。

K 部長は，P サービスの導入によって表 2 の要件を満たすネットワーク構成が可能かどうかを検討するように S 主任に指示した。

〔ネットワーク構成の見直し〕

S 主任は，P サービスを導入する場合の Q 社のネットワーク構成を図 3 に，表 2 の要件を満たすためのネットワーク構成の見直し案を表 4 にまとめて，表 2 の要件を満たすネットワーク構成が可能であることを K 部長に説明した。

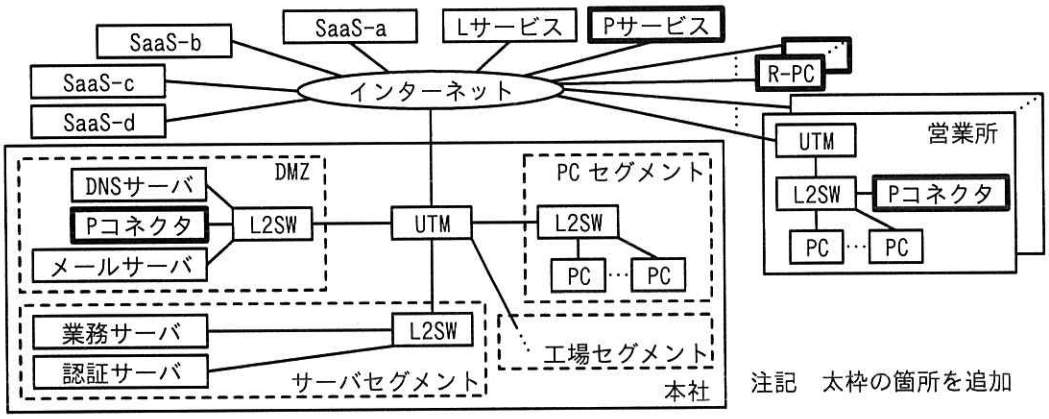


図3　P サービスを導入する場合の Q 社のネットワーク構成

表4　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件1	・②営業所からインターネットへのアクセス方法を見直す。 ・L サービスでの送信元制限機能は有効にしたまま，③営業所から L サービスにアクセスできるように設定を追加する。
要件2	・表3の項番1の機能を使う。 ・L サービスでの送信元制限機能において，Q 社が設定した IP アドレス以外からのアクセスに対する設定を変更する。さらに，多要素認証機能を有効にして，④方式を選択する。
要件3	・表3の項番 h の機能を使う。
要件4	・表3の項番 i の機能を使う。
要件5	・表3の項番3及び項番4の機能を使って，表5に示す設定を行う。

表5　要件5に対する設定

番号	表3の項番	URL カテゴリ又は URL	利用者 ID	アクション
1	あ	j	k の利用者 ID	l
2	い	m	n の利用者 ID	o

注記　番号の小さい順に最初に一致したルールが適用される。

その後，表4のネットワーク構成の見直し案が上層部に承認され，P サービスの導入と新しいネットワーク構成への変更が行われ，6か月後に在宅勤務が開始された。

設問１　〔L サービスの動作確認〕について答えよ。

(1)　図 2 中の［　a　］～［　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　L サービス　　イ　PC の Web ブラウザ　　ウ　SaaS-a

(2)　本文中の下線①について，利用できない理由を，40 字以内で具体的に答えよ。

設問２　〔在宅勤務導入における課題〕について答えよ。

(1)　表 3 中の［　d　］～［　f　］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　P サービスのサーバ証明書　　イ　信頼されたルート証明書

ウ　認証局の証明書

(2)　表 3 中の［　g　］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　CAPTCHA　　イ　CASB　　ウ　CHAP

エ　CVSS　　オ　クラウド WAF

設問３　〔ネットワーク構成の見直し〕について答えよ。

(1)　表 4 中の下線②について，見直し前と見直し後のアクセス方法の違いを，30 字以内で答えよ。

(2)　表 4 中の下線③について，L サービスに追加する設定を，40 字以内で答えよ。

(3)　表 4 中の下線④について，選択する方式を，表 1 中の（ア），（イ）から選び，記号で答えよ。

(4)　表 4 中の［　h　］，［　i　］に入れる適切な数字を答えよ。

(5)　表 5 中の［　あ　］，［　い　］に入れる適切な数字，［　j　］～［　o　］に入れる適切な字句を答えよ。