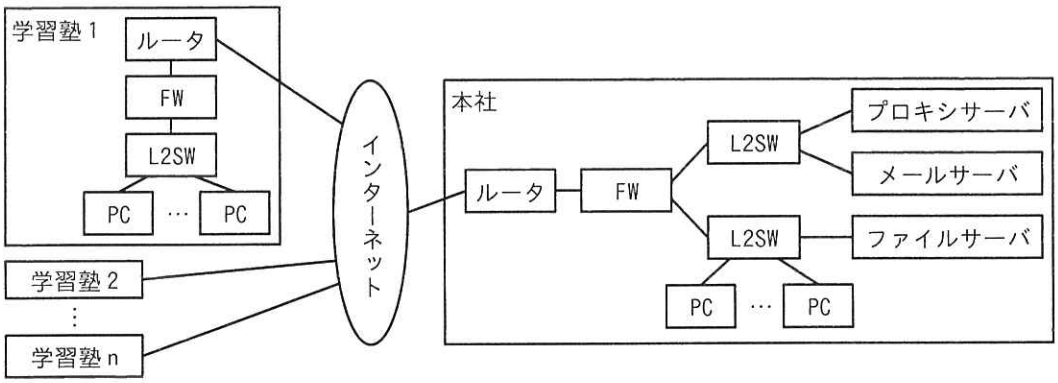
次の問１は必須問題です。必ず解答してください。

問１　リモート環境のセキュリティ対策に関する次の記述を読んで，設問に答えよ。

Q 社は，首都圏で複数の学習塾を経営する会社であり，各学習塾で対面授業を行っている。生徒及び生徒の保護者からはリモートでも受講が可能なハイブリッド型授業の導入要望があり，Q 社の従業員からはテレワーク勤務の導入要望がある。

〔Q 社の現状のネットワーク構成〕

Q 社のネットワーク構成（抜粋）を図１に示す。



FW：ファイアウォール　　L2SW：レイヤー２スイッチ
注記　学習塾２～学習塾ｎは学習塾１と同様の構成である。

図１　Q 社のネットワーク構成（抜粋）

〔Q 社の現状のセキュリティ対策〕

Q 社のセキュリティ対策は次のとおりである。

・パケットフィルタリングポリシーに従った通信だけを FW で許可し，その他の通信を遮断している。
・業務上必要なサイトの URL 情報を基に，URL フィルタリングを行うソフトウェアをプロキシサーバに導入して，業務上不要なサイトへの接続を禁止している。
・PC 及びサーバ機器には，外部媒体の使用ができない設定をした上で，マルウェア対策ソフトを導入して，マルウェア感染対策を行っている。
・PC，ネットワーク機器及びサーバ機器には，脆弱(ぜい)性に対応する修正プログラム（以下，セキュリティパッチという）を定期的に確認した後，適用する方法で，脆弱性対策を行っている。

〔Q社の現状のセキュリティ対策に関する課題〕

・ネットワーク機器及びサーバ機器のEOL（End Of Life）時期が近づいており，機器の更新が必要である。

・セキュリティパッチが提供されているかの調査及び適用してよいかの判断に時間が掛かることがある。

・ルータとFWを利用した①境界型防御によるセキュリティ対策では，防御しきれない攻撃がある。

・セキュリティインシデントの発生を，迅速に検知する仕組みがない。

Q社では，ハイブリッド型授業とテレワーク勤務が行えるリモート環境を実現し，Q社のセキュリティに関する課題を解決する新たな環境を，クラウドサービスを利用して構築することになり，情報システム部のR課長が担当することになった。

〔リモート環境の構築方針〕

R課長は，境界型防御の環境に代えて，いかなる通信も信頼しないという［ a ］の考え方に基づくリモート環境を構築することにした。

R課長は，リモート環境について次の構築方針を立てた。

・クラウドサービスへの移行に伴い，ネットワーク機器及びサーバ機器は廃棄し，今後のQ社としてのEOL対応を不要とする。

・②課題となっている作業を不要にするために，クラウドサービスはSaaS型を利用する。

・セキュリティインシデントの発生を迅速に検知する仕組みを導入する。

・従業員にモバイルルータとセキュリティ対策を実施したノートPC（以下，貸与PCという）を貸与する。今後は，本社，学習塾及びテレワークでの全ての業務において，貸与PCとモバイルルータを使用してクラウドサービスを利用する。

・貸与PCから業務上不要なサイトへの接続は禁止とする。

・生徒は，自宅などのPC（以下，自宅PCという）からクラウドサービスを利用してリモートでも授業を受講できる。

〔リモート環境構築案の検討〕

R課長はリモート環境の構築方針を部下のS君に説明し，構築する環境の検討を指

示した。

S 君はリモート環境構築案を検討した。

・リモート環境の構築には，T 社クラウドサービスを利用する。

・貸与 PC から Web サイトを閲覧する際は，③プロキシを経由する。

・貸与 PC からインターネットを経由して接続する Web 会議，オンラインストレージ及び電子メール（以下，メールという）を利用することで，Q 社の業務及びリモートでの授業を行う。

・貸与 PC から T 社クラウドサービスへのログインは，ログインを集約管理するクラウドサービスである IDaaS（Identity as a Service）を利用する。従業員は ID とパスワードを用いてシングルサインオンで接続してクラウドサービスを利用する。

・④SIEM（Security Information and Event Management）の導入と，アラート発生時に対応する体制の構築を行う。

・貸与 PC には，マルウェア対策ソフトを導入し，外部媒体が使用できない設定を行う。また，⑤紛失時の情報漏えいリスクを低減する対策をとる。

・生徒は，自宅 PC からインターネット経由で，Web 会議に接続して，リモートで授業を受講できる。

S 君が検討したリモート環境構築案（抜粋）を図 2 に示す。

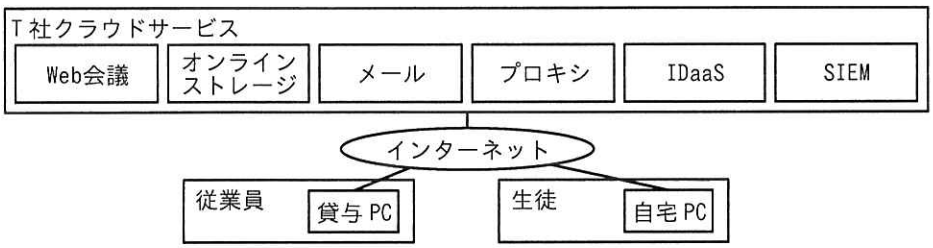


図 2　リモート環境構築案（抜粋）

〔構築案への指摘と追加対策の検討〕

S 君は検討した構築案について R 課長に説明した。すると，セキュリティ対策の不足に起因するセキュリティインシデントの発生を懸念した R 課長は，“ a ”では，クラウドサービスにアクセスする通信を信頼せずセキュリティ対策を行う必要があるので，エンドポイントである貸与 PC と自宅 PC に対する攻撃への対策及びクラウドサービスのユーザー認証を強化する対策が必要である。追加の対策を検討するよう

に。”と指摘した。

R 課長が懸念したセキュリティインシデント（抜粋）を表 1 に示す。

表 1　R 課長が懸念したセキュリティインシデント（抜粋）

項番	分類	セキュリティインシデント
1	貸与 PC	ゼロデイ攻撃によるマルウェア感染
2		ファイルレスマルウェア攻撃によるマルウェア感染
3	自宅 PC	マルウェア感染した自宅 PC から Web 会議への不正アクセス
4	クラウドサービスのユーザー認証	不正ログインによる情報漏えい

S 君は，R 課長の指摘に対して，表 1 のセキュリティインシデントに対応した次の対策を追加することにした。

・項番 1，2 の対策として，貸与 PC に⑥EDR（Endpoint Detection and Response）ソフトを導入する。

・項番 3 の対策として，T 社クラウドサービスは不正アクセス及びマルウェア感染の対策がとられていることを確認した。

・項番 4 の対策として，知識情報である ID とパスワードによる認証に加えて，所持情報である従業員のスマートフォンにインストールしたアプリケーションソフトウェアに送信されるワンタイムパスワードを組み合わせて認証を行う，［　b　］を採用する。

S 君は，これらの対策を追加した構築案を R 課長に報告し，構築案は了承された。

設問 1　本文中の下線①について，防御できる攻撃を解答群の中から選び，記号で答えよ。

解答群

ア　システム管理者による内部犯行

イ　パケットフィルタリングのポリシーで許可していない通信による，内部ネットワークへの侵入

ウ　標的型メール攻撃での，添付ファイル開封による未知のマルウェア感染

エ　ルータの脆弱性を利用した，インターネット接続の切断

設問２　〔リモート環境の構築方針〕について答えよ。

(1)　本文中の［　a　］に入れる適切な字句を６字で答えよ。

(2)　本文中の下線②について，課題となっている作業を 25 字以内で答えよ。

設問３　〔リモート環境構築案の検討〕について答えよ。

(1)　本文中の下線③で実現すべきセキュリティ対策を，本文中の字句を用いて 15 字以内で答えよ。

(2)　本文中の下線④を導入した目的を，〔Q 社の現状のセキュリティ対策に関する課題〕と〔リモート環境の構築方針〕とを考慮して 30 字以内で答えよ。

(3)　本文中の下線⑤について，対策として適切なものを解答群の中から全て選び，記号で答えよ。

解答群

ア　貸与 PC のストレージ全体を暗号化する。

イ　貸与 PC のモニターにのぞき見防止フィルムを貼付する。

ウ　リモートロック及びリモートワイプの機能を導入する。

設問４　〔構築案への指摘と追加対策の検討〕について答えよ。

(1)　本文中の下線⑥について，表１の項番１，２のセキュリティインシデントが発生した場合の EDR ソフトの動作として適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　貸与 PC をネットワークから遮断し，不審なプロセスを終了する。

イ　登録された振る舞いを行うマルウェアの侵入を防御する。

ウ　登録した機密情報の外部へのデータ送信をブロックする。

エ　パターン情報に登録されているマルウェアの侵入を防御する。

(2)　本文中の［　b　］に入れる適切な字句を５字で答えよ。