【H19 春-SV 午後Ⅱ問２の問題】

社内システムのセキュリティ対策に関する次の記述を読んで，設問 1～5 に答えよ。

A 社は，東京に本社があり，関東に工場や営業所をもつ従業員数 5,000 名の製造業者である。A 社では，数年前から社内業務の電子化を推進しており，従業員の日常業務に活用させるため，昨年までに各部署に必要台数分のノート PC が配布されている。また，本社と，工場及び営業所（以下，これらを拠点という）に業務サーバを設置している。本社から接続されたインターネットを利用して，電子メール（以下，メールという）の送受信や，Web サーバによる情報発信を行っている。本社には情報システム部門があり，社内ネットワーク及び情報システム（以下，社内システムという）を管理している。図1に，A 社の社内システム構成を示す。

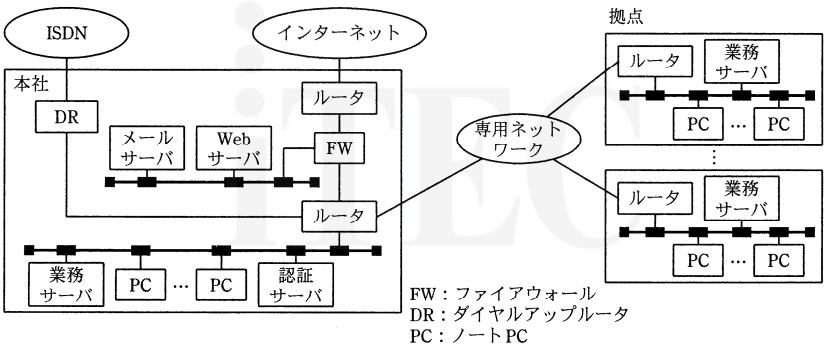

図１　A 社の社内システム構成

外出することが多い営業部員を中心とする 50 名の従業員（以下，利用者という）は，外出先からメールサーバや各自の拠点の業務サーバを利用するために，会社から貸与されたノート PC を社外に持ち出し，PHS サービスを介してリモートアクセスを行っている。利用者は，ダイヤルアップルータ（DR）を介して社内システムにアクセスする。その際，メール送受信には，SMTP と POP を使用している。また，業務サーバへのアクセスには，TCP/IP 上の独自プロトコルが使われている。A 社では，事業拡大に伴って海外にある委託業者への出張が増加していること，及びより高速な回線を用いて社外から業務サーバにアクセスしたいという要望があることの 2 点を考慮して，リモートアクセスシステムをインターネット経由に構築し直すことにした。

iTEC
Copyrights by ITEC,Inc. 2022

一方，A 社の経営陣は，情報漏えいが頻発している社会的背景を踏まえて，情報統括役員（CIO）を中心としたプロジェクトチームを組織し，社内システム全体のセキュリティ対策の見直しを行うことを指示した。コンサルタント会社によるセキュリティ診断の結果，1）リモートアクセスシステムにおける利用者認証，2）ノート PC に保存されているデータに関するセキュリティ対策，3）ウイルス感染に関するセキュリティ対策，の三つの問題点が指摘された。

そこで，情報システム部門の B 君は，プロジェクトチームの作業の一環として，指摘された三つの問題点に関する対策を含め，上司の C 氏と共同でリモートアクセスシステムの再構築を検討することになった。

〔既存のリモートアクセスシステムにおける利用者認証〕

まず，B 君は C 氏とともに，既存のリモートアクセスシステムに関して指摘された問題点の精査を行うことにした。次は，そのときの B 君と C 氏の会話である。

C 氏：既存のリモートアクセスシステムに関するセキュリティ診断の結果を確認しよう。

B 君：不正侵入の防止策として，利用者認証を実施していますが，運用面での問題点が指摘されています。

C 氏：なるほど。それでは，利用者の認証方式について，具体的に説明してくれ。

B 君：利用者を認証するために，認証サーバを設置して，DR への接続時に利用者 ID とパスワードのチェックを行います。また，PHS 端末を用いたアクセスなので，念のため DR は発信者番号に基づいた接続制限を行っています。

C 氏：利用者がノート PC や PHS 端末を紛失したときの対応はどうなっているのか，説明してくれ。

B 君：紛失した利用者から，紛失した場所と時刻，最後にリモートアクセスした時刻を電話で連絡してもらい，その利用者のアカウントの［ a ］措置を行い，DR の［ b ］を見て，不審なリモートアクセスがないか確認しています。

C 氏：認証に使用するパスワードはどのように管理されているのかね。

B 君：リモートアクセスに使用するパスワードには有効期限を設け，利用者に対して，1 か月ごとに更新するように義務付けています。有効期限までにパスワー

iTEC
Copyrights by ITEC,Inc. 2022

ドを更新しないと，アクセスできなくなるので，そのときはパスワードの初期化が必要となります。パスワードが失効した利用者や，パスワードを忘れた利用者からは，メールでパスワード初期化の依頼があります。情報システム部門でパスワードの初期化を行い，初期化によって設定された暫定パスワードをメールで返信し，直ちにパスワードを変更するようにお願いしています。

C氏：パスワード管理について問題点が指摘されているということだったが。

B君：はい。緊急の場合には，外出先からの電話による問合せに対し，①利用者IDだけを聞いて暫定パスワードを教えてしまうこともあります。また，パスワードの更新に当たっては，過去に使用したことのあるパスワードと新しいパスワードを照合し，同一であれば別のパスワードを設定するように指示します。同じパスワードを再使用できないので，パスワードを覚えることが利用者にとって負担になっているようです。中には，付せんに書き留めて，ノートPCに張り付けている利用者もいるようです。

C氏：それは問題だな。リモートアクセスシステムの再構築を機に，問題解決を図ることにしよう。

〔リモートアクセス方式の変更〕

B君とC氏は，現在のDR経由のリモートアクセスをインターネット経由に切り替えることにした。利用者は，公衆無線LANサービスや，インターネットサービスプロバイダが提供する動的IP割当てによるインターネットアクセスサービスを利用し，リモートアクセスシステムを介して社内システムにアクセスする。図2に，A社の新しい社内システム構成案を示す。

iTEC
Copyrights by ITEC,Inc. 2022

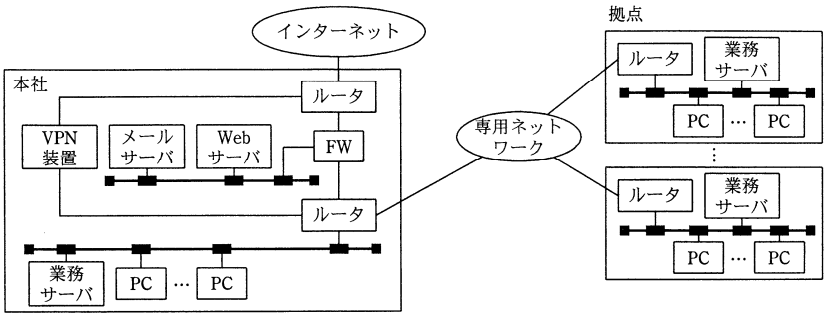

図２　A 社の新しい社内システム構成案

C 氏：それでは，リモートアクセス方式について検討しよう。インターネット上で VPN を構成する手段として，IPsec を用いる方法（以下，IPsec-VPN という）があるが，IPsec-VPN について少し説明してくれないか。

B 君：はい。IPsec-VPN では，暗号通信に先立ち，暗号方式の決定や鍵の交換，相互認証のためのプロトコルとして［　c　］を使用します。［　c　］によって生成された共有鍵は，［　d　］という IP パケットのフォーマット仕様に従って送受信するデータの暗号化に使用されます。

C 氏：相互認証はどのような方式にするのかね。

B 君：事前共有鍵を用いた方式にしようと思います。［　c　］のフェーズ 1 には，メインモードとアグレッシブモードがあり，リモートアクセスの利用形態に依存してどちらかを使います。メインモードでは，端末の IP アドレスを ID とし，それに事前共有鍵を割り当てます。一方，アグレッシブモードでは，利用者 ID など運用者が独自に設定した ID に対して事前共有鍵を割り当てます。

C 氏：それでは，まずメインモードから説明してくれ。

B 君：図 3 にメインモードの概要を示します。

iTEC
Copyrights by ITEC,Inc. 2022

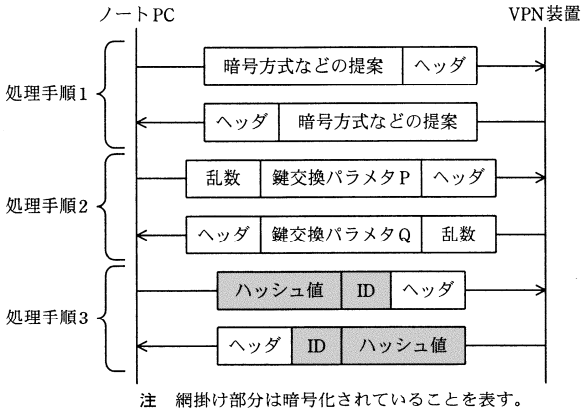

図3　メインモードの概要

B君：処理手順 1 では，使用する暗号方式やハッシュアルゴリズムなどが決定されます。次に，処理手順 2 では，暗号化で用いる共有鍵が生成されます。鍵交換パラメタは，鍵共有アルゴリズムである［　e　］アルゴリズムに使用されます。鍵交換パラメタ P は，ノート PC がランダムに生成した一時鍵情報 p から計算された値で，鍵交換パラメタ Q は，VPN 装置がランダムに生成した一時鍵情報 q から計算された値です。鍵交換パラメタ P，Q からは，一時鍵情報 p，q は計算できません。鍵交換パラメタ Q と一時鍵情報 p を組み合わせて［　e　］アルゴリズムで計算した値は，鍵交換パラメタ P と一時鍵情報 q を組み合わせて［　e　］アルゴリズムで計算した値と一致します。この値を［　e　］アルゴリズムの出力値と呼びます。この出力値を計算すると，ノート PC が保持していた一時鍵情報 p や，VPN 装置が保持していた一時鍵情報 q は，直ちに削除されます。一方，処理手順 2 で交換した乱数と事前共有鍵を利用して，マスタ鍵が生成されます。また，マスタ鍵と［　e　］アルゴリズムの出力値などを使用して，セッション鍵が計算されます。最後に，処理手順 3 では，ID とハッシュ値の交換が行われます。ハッシュ値は，鍵交換パラメタなどを入力として，マスタ鍵を鍵情報として用いた鍵付きハッシュ関数によって計算されます。ノート PC や VPN 装置はハッシュ値を受信すると，その値が正しいかどうかを検証します。

iTEC
Copyrights by ITEC,Inc. 2022

C氏：次に，もう一方のアグレッシブモードについても説明してくれ。

B君：はい。図4にアグレッシブモードの概要を示します。

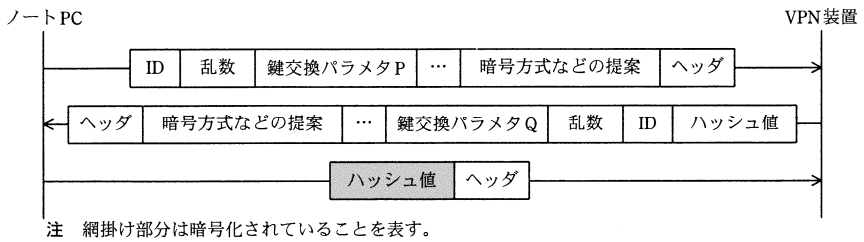

図4　アグレッシブモードの概要

B君：認証手法，セッション鍵の生成方法はメインモードとほぼ同じです。

C氏：使用できるIDに違いがあるようだから，リモートアクセス時のネットワーク環境も考慮して，どちらのモードを採用したらよいか検討してくれ。

B君：はい。分かりました。

〔利用者認証方式の変更〕

C氏：次に，利用者認証の運用面での問題点について検討しよう。現在の利用者認証方式では，パスワード管理を行うために，利用者と運用者双方に負担がかかっている。パスワードが正しく運用されればよいが，現状では困難のようだ。利用者の利便性を考慮して，［ f ］認証の導入を検討してみよう。指紋や虹彩を用いた［ f ］認証は，パスワードを管理する必要がないので有効な方法だと思う。一般に，その認証精度は，［ g ］拒否率と［ h ］受入れ率の組合せで評価される。通常は［ g ］拒否率よりも［ h ］受入れ率が十分に低くなるように設定されているようだ。

B君：そうしますと，認証でのリトライ回数の上限も［ g ］拒否率を考慮して設定した方がよいということですね。IPsec-VPN でのリモートアクセスに対し，［ f ］認証をどのように適用すればよいでしょうか。

C氏：指紋認証デバイス（以下，認証デバイスという）を，リモートアクセスシステムの利用者に配布して，その中に事前共有鍵を格納する方式がよいだろう。認

iTEC
Copyrights by ITEC,Inc. 2022

証デバイスでは，指紋認証に成功しないと，格納されている事前共有鍵を使用できないようにできる。また，認証デバイスは，使用する PC の認証を行うので，会社が貸与したノート PC 以外からのアクセスを制限できるね。

B 君：リモートアクセスシステムは，指紋の照合に成功することと，ノート PC と認証デバイスの組合せが正しいことの 2 点を確認して認証するわけですね。それでは，認証デバイスを利用した方式について検討を進めたいと思います。

C 氏：認証デバイスの配布方法，初期登録方法，及び認証デバイスを紛失した際の運用手順についても検討してくれ。

〔ノート PC に保存されているデータに関するセキュリティ対策〕

次に，B 君と C 氏は，ノート PC に保存されているデータに関するセキュリティ対策を検討することにした。

C 氏：リモートアクセスに使用するノート PC の管理は利用者に任せているが，どのような指導を行っているか確認しよう。

B 君：ノート PC からの機密情報の漏えいを防止するために禁止規定を設けています。具体的には，貸与されたノート PC 以外で業務を行わない，貸与されたノート PC には決められたソフトウェアだけをインストールする，などの事項を厳守するように周知徹底しています。

C 氏：情報漏えいの観点からは，それ以外の対策も考える必要があるね。ノート PC に保存されるデータとしては，業務で使用するファイル（以下，業務データという）とメールの 2 種類がある。そのため，ノート PC や認証デバイスが盗まれた場合の対策が必要だから，対策案を挙げてくれ。

B 君：はい。ノート PC にはなるべくデータを保存しないようにするというのはいかがでしょうか。対策案としては，まず，メールに使用するプロトコルを IMAP に移行してもらいます。また，業務データは業務サーバの個人データ領域に保管し，使用するときに，その都度ノート PC にダウンロードし，使用後は速やかにアップロードして，ノート PC 内の業務データを直ちに削除してもらうようにします。

C 氏：その対策案では，メールや業務データがノート PC に残ってしまう可能性を否

iTEC
Copyrights by ITEC,Inc. 2022

定できない。②ノート PC のハードディスク全体に関する対策も併せて考える必要がある。その際には，認証デバイスも活用してくれ。

B 君：分かりました。ハードディスク全体に関する対策も含めて検討します。

〔ウイルス感染に関するセキュリティ対策〕

最後に，B 君と C 氏は，セキュリティ診断の結果として指摘された，ウイルス感染への対策を行うことにした。A 社では，ノート PC の管理は従業員に任せており，情報システム部門が許可しているウイルスチェックソフトの中から，従業員が選んだウイルスチェックソフトをインストールしていた。その結果，セキュリティ診断によって，ウイルスチェックソフトがインストールされていないノート PC や，ライセンス契約が切れて最新のパターンファイルに更新できなくなったウイルスチェックソフトが発見された。そこで，これまでのウイルス対策に加えて，全社的に統一されたウイルス対策を検討することになった。

幾つかの製品を調査した結果，FW にメールウイルスチェック機能を搭載することにした。この機能には，FW を通過しようとするメールをいったん代理受信し，ウイルスがなければ FW 自身が SMTP を使ってメールサーバへチェック済メールを送信するプロキシモードと，ノート PC とメールサーバ間の SMTP セッションを横取りしてウイルスチェックを行い，ウイルスがなければ送信元 IP アドレスを変更せずにそのまま転送する透過モードがある。B 君は，デフォルト設定であるプロキシモードでメールウイルスチェック機能を使用することにした。また，ウイルスメール発見時には，FW が，社内の送受信者にウイルス警告メールを送信する設定も行い，運用を開始した。

メールウイルスチェック機能導入後，しばらくたってから，A 社からのメールがあて先に届くまでに時間がかかるようになった。A 社のメールサーバは，不正メールの中継を防止するために，SMTP の送信元 IP アドレスを基に A 社のネットワークから送信されたメールだけを転送している。B 君がメールサーバを調べてみると，大量の転送待ちのメールがメールサーバに滞留していることが判明した。これらのメールは，A 社の従業員が送信したものではない不正メールであり，A 社のメールサーバが社外からのスパムメールの中継に利用されていたことが確認された。

メールサーバのログを分析したところ，メールウイルスチェック機能の設定に起因

iTEC
Copyrights by ITEC,Inc. 2022

することが判明した。B 君は，FW のメールウイルスチェック機能を透過モードで動作するように設定変更を行い，不正メールの転送に利用されてしまう問題を解決した。

その後，ある従業員のノート PC から大量のウイルスメールが送信されているという報告があった。B 君が調査した結果，③その従業員は，図 5 に示すウイルス警告メールの指示どおりに対策を実施したためにウイルスに感染したことが分かった。

ウイルス警告

ファイアウォールのウイルスチェック機能が，あなたの送信メールからウイルスを検知しました。このウイルスは，メールを介して拡散する最新のウイルスで，PC のウイルスチェックソフトでは駆除できません。次の対策を実施してください。

(1) あなたの PC のウイルスを駆除するために，次のソフトウェアをダウンロードして実行してください。

http://example.com/tool/Remove-XY9998-x86.exe

(2) 実行後に，必ず PC の再起動を行ってください。

ウイルスチェックサービス

図 5 従業員あてに通知されたウイルス警告メールの本文

B 君は，全従業員に，④この事例から学ぶべき注意事項について厳守するように周知徹底した。また，業務用ソフトウェアに対するセキュリティパッチや修正プログラムを保管し，従業員がそれらをダウンロードできるパッチサーバを社内ネットワークに設置した。さらに，多様化するウイルスの脅威に対抗するために，ノート PC に対しても統一したウイルス対策が必要であると判断し，すべてのノート PC に対して，同一のウイルスチェックソフトを導入することにした。

B 君と C 氏はその後も検討を重ね，リモートアクセスシステムの再構築と社内システム全体のセキュリティ対策を完了させることができた。

iTEC
Copyrights by ITEC,Inc. 2022

設問 1　既存のリモートアクセスシステムの検証について，(1)，(2) に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な字句を答えよ。

(2) 本文中の下線①の対応の問題点を，30 字以内で述べよ。

設問 2　IPsec-VPN の導入について，(1) ～ (4) に答えよ。

(1) 本文中の［ c ］～［ e ］に入れる適切な字句を答えよ。

(2) 図 3 及び図 4 のハッシュ値を検証する目的は何か。25 字以内で述べよ。

(3) 攻撃者は，フェーズ 1 終了後に事前共有鍵と送受信されたすべてのデータを入手できたとしても，セッション鍵を計算できない。その理由を 35 字以内で述べよ。

(4) B 君はメインモードとアグレッシブモードのどちらを採用すべきか。採用すべきモードを答えよ。また，採用理由を，ネットワーク環境に着目して 40 字以内で述べよ。

設問 3　利用者認証方式について，(1)，(2) に答えよ。

(1) 本文中の［ f ］～［ h ］に入れる適切な字句を答えよ。

(2) 認証デバイスを紛失した際に，直ちに VPN 装置で実施すべき事項を 20 字以内で述べよ。

設問 4　ノート PC に保存されているデータに関するセキュリティ対策について，(1)，(2) に答えよ。

(1) C 氏が指摘した以外に，ネットワーク接続環境の観点から，B 君が述べた対策案だけを実施した場合に生じるデータ可用性に関する問題点を，35 字以内で述べよ。

(2) 本文中の下線②に関して，ノート PC のハードディスクに施すべきセキュリティ対策を，認証デバイスの活用法も含めて 45 字以内で述べよ。

設問 5　ウイルス感染に関するセキュリティ対策について，(1) ～ (3) に答えよ。

(1) メールサーバがスパムメールの中継に利用された理由を，メールサーバの設定内容に着目して 55 字以内で述べよ。

(2) 本文中の下線③について，ウイルスに感染してしまった原因を 55 字以内で述べよ。また，FW がウイルスを検知できなかった理由を 40 字以内で述べよ。

(3) 本文中の下線④について，パッチ適用に関して周知徹底すべき注意事項を，45 字以内で述べよ。

iTEC
Copyrights by ITEC,Inc. 2022