平成１９年度　秋期　情報セキュリティアドミニストレータ　午後Ｉ問題

問１　VPN の導入に関する次の記述を読んで，設問 1～4 に答えよ。

E 大学は，都市近郊にある総合大学である。7 学部が四つのキャンパスに散在しており，昨年，あるビルの 1 フロアを借りて，期間限定のキャンパス（以下，サテライトキャンパスという）をオープンさせた。サテライトキャンパスは，講義だけでなく様々なイベントを開催するなど，広告塔的な役割を担っている。サテライトキャンパスの各部屋には，インターネット回線が設置された。

〔VPN 導入対象のネットワーク構成〕

U 教授の研究グループでは，今年度，2 週間の予定で，サテライトキャンパスで研究成果をデモンストレーションすることになった。その期間，U 教授の研究グループ専用に用意された部屋（以下，デモルームという）と，ほかのキャンパスにある U 教授の研究室（以下，U 研究室という）との間に，新たに VPN を独自に導入することにした。

U 研究室内の LAN は，ファイアウォール兼ルータ（以下，FWR という）を経由してインターネットへ接続しており，不要なトラフィックはすべて遮断している。U 研究室には，PC，Web サーバ，SSH サーバ，ファイルサーバ，メールサーバ，イメージスキャナ及びプリンタがあり，これらは大学院生の S 君が管理している。SSH サーバは，インターネットからの接続も可能としている。また，FWR は DHCP サーバも兼ねており，PC を LAN に接続するだけで LAN を利用できるようになっている。U 研究室とデモルームのネットワーク構成は，図のとおりである。FWR1 は U 教授の研究グループの所有であるが，FWR2 は，ほかの研究グループから一時的に借りてきて，デモルームの LAN を構築した。

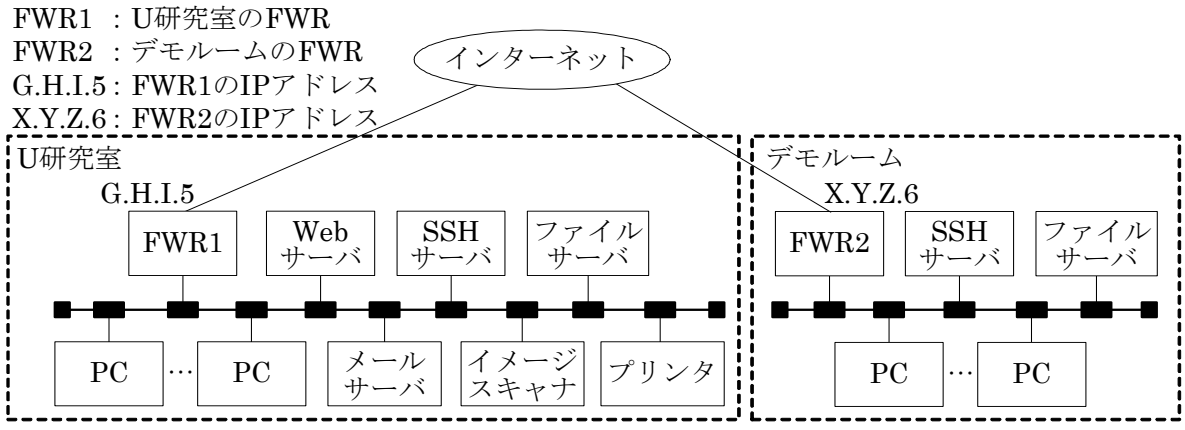

図　ネットワーク構成

〔VPN 方式の選定〕

U 教授は S 君に対し，VPN 方式を選定するように伝えた。特に，U 教授は PC を携帯してデモルームと U 研究室を行き来するので，デモルームでも U 研究室のサーバ類を利用できることと，機密データを大量に扱うので，必要なセキュリティを確保できることを条件とした。S 君は，既に稼働中の FWR

がもつ IPsec-VPN 機能を含めて，導入可能な 3 方式を表 1 にまとめ，VPN 導入を手伝うことになった O 君と，比較・検討した。

表１　VPN 方式の比較（抜粋）

比較項目	方式 1	方式 2	方式 3
方式概要	IPsec-VPN 機能を利用	SSL-VPN ソフトを利用	SSH ソフトを利用
VPN 通信区間	ルータ間	PC と SSL サーバ間	PC と SSH サーバ間
PC ユーザ認証方式	不要	公開鍵証明書を利用	公開鍵暗号又はパスワードを利用
転送対象プロトコル	IP	TCP	SMTP，POP などのプロトコル
個別 PC の設定	省略		
VPN 導入の容易さ	省略		

次は，VPN 方式の選定に関する O 君と S 君の会話である。

O 君：基本的なことですが，これらの VPN を用いる意義は何ですか。例えば，AES といった共通鍵暗号化方式で暗号化したファイルを転送すれば，VPN は必要ないと思います。

S 君：そうとは言い切れないよ。ファイル転送の際暗号化によって盗聴は防げるが，暗号化だけでは，［　ア　］や［　イ　］の脅威を防ぐことはできない。方式 1～3 による VPN を適切に用いれば，それらの脅威に対処できる。また，暗号鍵は接続ごとに更新することが望ましいので，そのための仕組みもこれらの VPN では利用できる。

O 君：なるほど。VPN で総合的なセキュリティを確保できるということですね。方式 2 を採用するというのはどうでしょうか。

S 君：方式 2 は，サーバ用ソフトと公開鍵証明書の管理ツールを必要とする。また，公開されて日が浅いソフトウェアなので，未知の脆弱性に関して不安がある。方式 2 より方式 3 の方がいいかな。

O 君：しかし，方式 3 では転送対象プロトコルに関する問題はないですか。

S 君：そうなんだ。方式 3 では，利用可能なアプリケーションが限定され，駄目だな。U 教授の希望をかなえるためには，採用した経験はないけど方式 1 がいいかな。

O 君：方式 2 でも転送対象プロトコルの問題はないですし，設定も簡単そうですよ。

S 君：確かにそうだが，①VPN 導入後，利用者の手間がかからないというメリットも大きいので，方式 1 にしよう。

S 君たちは方式 1 を採用することに決め，U 教授の許可を得て，設定作業に入った。

〔FWR の概要と設定〕

FWR の IPsec の鍵管理には，事前共有鍵を利用する IKE（Internet Key Exchange）方式（以下，事前共有鍵 IKE 方式という），公開鍵証明書を利用する IKE 方式（以下，公開鍵証明書 IKE 方式という），及び IKE を用いずに事前共有鍵を手動で共有する方式（以下，手動鍵管理方式という）の 3 方式がある。IKE のフェーズ 1 では，“鍵管理方式”の選択のほかに“DH グループ”及び”暗号化とハッシュのアルゴリズム”の組合せから構成される 24 組の暗号スイートのうちの 4 組を，フェーズ 2 における通信用に提案するように設定できる。また，フェーズ 2 でも同様に，IPsec プロトコル用に暗号スイートを 4 組設定できる。

S 君は，一時的に借りた FWR2 の暗号スイートに関する設定は変更せず，FWR1 の設定を行った。IPsec-VPN に関する主な設定は，表 2 のとおりである。ただし，IPsec プロトコルとして，［ a ］と ESP があるが，今回は ESP を利用する。

表２　FWR1 と FWR2 の IPsec-VPN に関する主な設定

		FWR1	FWR2
接続先 IP アドレス		X.Y.Z.6	G.H.I.5
鍵管理方式		事前共有鍵 IKE 方式	事前共有鍵 IKE 方式
暗号スイート	フェーズ 1	g2:3des:sha	g2:des:sha
		g2:3des:md5	g2:des:md5
		g1:des:sha	g2:aes128:sha
		g1:des:md5	g2:aes128:md5
	フェーズ 2	g2:3des:sha	g2:des:sha
		g2:3des:md5	g2:des:md5
		g2:aes128:sha	g2:aes128:sha
		g2:aes128:md5	g2:aes128:md5

O 君：事前共有鍵 IKE 方式を設定していますが，“IKE”とは何ですか。
S 君：IPsec 通信に先立ち，［ b ］と同時に［ c ］を行うプロトコルだよ。また，セッションごとに暗号鍵を生成する機能を提供している。
O 君：それと，“DH グループ”とは何ですか。
S 君：IKE で利用する DH という［ c ］プロトコルのパラメタの一つだよ。FWR では 2 種類選べるが，2 点間で同じ値にする必要がある。
O 君：FWR には，［ d ］として AES，DES，3DES の三つがあり，［ e ］として MD5，SHA-1 を利用できますよね。
S 君：実際には，それらの組合せを一つの暗号スイートとして扱う。例えば，g2:des:sha という暗号スイートは，DH グループが 2，［ d ］が DES，［ e ］が SHA-1 であることを表している。
O 君：暗号スイートをなぜ 4 組も選ぶのですか。
S 君：一方が提案した暗号スイートを，他方が受け入れないとき，ほかの暗号スイートを利用できるようにするためだよ。また，暗号スイートの利用に関して，各 FWR の優先順位の提案もできるということだね。

〔VPN の稼働〕

後日，二人で各機器を設置した後，②デモルーム側の PC から U 研究室のサーバへの VPN 接続を試みたが，接続できなかった。表 3 に示す各 FWR のログを調べたところ，設定ミスがあることが分かった。それ以外のルーティングを含むネットワーク上の設定は間違っていなかった。設定を修正した結果，無事，VPN 接続ができた。

表３　FWR1 と FWR2 の IPsec-VPN に関するログ（抜粋）

FWR1		
日付	時刻	メッセージ
2007-09-11	18:17:04	VPN configuration saved by admin
2007-09-13	13:49:14	IKE<X.Y.Z.6> Phase1：Responder started negotiations
2007-09-13	13:49:14	Rejected an IKE packet on WAN from <X.Y.Z.6>:500 to <G.H.I.5>:500, since there were no acceptable Phase l proposals
2007-09-13	13:49:18	IKE<X.Y.Z.6> Phase 1:Discarded an initial packet
2007-09-13	13:49:22	IKE<X.Y.Z.6> Phase 1:Responder started negotiations
2007-09-13	13:49:22	Rejected an IKE packet on WAN from<X.Y.Z.6>:500 to <G.H.I.5>:500,since there were no acceptable Phase 1 proposals
2007-09-13	13:49:26	IKE<X.Y.Z.6> Phase 1:Discarded an initial packet
2007-09-13	13:49:30	IKE<X.Y.Z.6> Phase 1:Responder started negotiations
2007-09-13	13:49:30	Rejected an IKE packet on WAN from<X.Y.Z.6>:500 to <G.H.I.5>:500,since there were no acceptable Phase 1 proposals
2007-09-13	13:49:34	IKE<X.Y.Z.6> Phase 1:Discarded an initial packet
FWR2		
日付	時刻	メッセージ
2007-09-13	13:48:42	VPN configuration saved by admin
2007-09-13	13:49:13	IKE<X.Y.Z.6> - > <G.H.I.5> Phase 1: Initiated negotiations
2007-09-13	13:50:02	IKE <G.H.I.5> Phase 1: Retransmission limit, connection failure

設問１　本文中の［　a　］～［　e　］に入れる適切な字句を解説群の中から選び，記号で答えよ。

解答群

ア　AH　　イ　DSA　　ウ　SPI　　エ　暗号化アルゴリズム　　オ　鍵交換
カ　認証　　キ　ハッシュアルゴリズム　　ク　呼出し　　ケ　ルーティング

設問２　本文中の［　ア　］，［　イ　］に入れる適切な字句を，それぞれ 15 字以内で答えよ。ただし，［　ア　］には真正性について，［　イ　］にはデータの完全性について答えよ。

設問３　本文中の下線②の VPN 接続失敗の原因を踏まえて，表 2 中の FWR の設定をどのように修正すればよいか。45 字以内で述べよ。

設問４　O 君と S 君の会話を踏まえ，VPN の導入について，(1)，(2) に答えよ。

(1) 本文中の下線①に示した方式 1 のメリットを，表 1 に基づき，60 字以内で述べよ。

(2) 事前共有鍵 IKE 方式を設定する運用管理上のメリットを，公開鍵証明書 IKE 方式及び手動鍵管理方式と比較して，それぞれ 40 字以内で述べよ。

問２　情報の取扱いに関する次の記述を読んで，設問 1～4 に答えよ。

L 社は，地方都市を中心に不動産管理業を営む，社員数 100 名ほどの企業である。都市部にある本社のほか，近郊の市町村にある 10 か所の営業所を拠点として事業を展開している。本社と営業所間及び営業所相互間では，取り扱う不動産物件に関する情報（以下，物件情報という）や，借主，貸主などの顧客に関する情報（以下，顧客情報という）を日常的にやり取りしている。

本社と営業所間及び営業所相互間での取扱いに慎重を要する物件情報や顧客情報の移送手段（以下，移送手段という）は，営業所の設備，物件情報や顧客情報のボリューム・形態，及び移送の距離や求められる迅速さに応じて，図 1 の中から選択することにしている。

1. 物件情報や顧客情報が記録されている電子ファイルは，社員に割り当てられた PC を用い，電子メール（以下，メールという）に添付して送受信する。
2. 電子化されていない，紙媒体の物件情報や顧客情報は，ファックスで送受信する。
3. 大量の電子ファイルを一括して運搬する場合には，USB メモリに電子ファイルを書き込み，宅配便や書留郵便で送付する。ただし，急ぎの場合には，社員がかばんに入れて直接届ける。

図１　移送手段

〔誤送信事故の発生〕

ある日，L 社の顧客である M 氏から，L 社社員によるファックスの誤送信によって，L 社に預けていた M 氏の個人情報が第三者に送付されてしまったという苦情があった。ファックスを受信した第三者が M 氏に連絡したことから，誤送信が発覚した。

L 社の経営陣は，この誤送信事故を契機として，それまで散発的に実施してきた情報セキュリティ対策を問題視し，情報セキュリティ委員会を設置して総合的な対策の検討を開始することになった。

その第一段階として，情報セキュリティ委員会の事務局を担当する情報システム部の C 主任が，本社と各営業所を回って L 社の日常業務における移送手段について調査し，L 社の現状を把握した。図 2 は，その結果をまとめたものである。

1. 外部記憶媒体を用いた情報の取扱い
(1) 外部記憶媒体に関しては，会社保有の USB メモリだけを日常業務に利用しており，私物を利用している者はいない。
(2) 運搬前後の USB メモリの管理は，取り扱う社員の責任であり，各自が自分の机の引き出しやキャビネットに入れて施錠保管している。
(3) USB メモリへの電子ファイルの書込み，USB メモリからの電子ファイルの読出しは，各自の PC を用いて行っている。
(4) 電子ファイルは，ファイル暗号化ソフトで暗号化してから USB メモリに書き込んでいる。
(5) USB メモリは，急ぎの場合を除き，宅配便や書留郵便で送付している。

2. ファックスを用いた情報の取扱い
(1) ファックスで送信する場合は，送信者がファックス送信前に名あて人に対して，ファックス装置から出

力された印刷物を直ちに回収するように電話で依頼している。
(2) ファックスの受信に関しては，最終退出者がファックス装置から出力された印刷物の有無を確認し，印刷物が放置されていた場合には，翌営業日までキャビネットに施錠保管している。

3. メールを用いた情報の取扱い
(1) メールサーバとメールを読み書きする PC は，ウイルス対策ソフトを導入し，適切に運用している。
(2) メールを読み書きする PC は，適切な ID とパスワードでアクセス制御している。
(3) 会社あてのメールを自宅など社外へ自動転送することは，禁止している。
(4) 後日の確認に備え，メールサーバでメールの内容を記録し，保管している。

4. その他の取扱い
(1) 情報の取扱いに関する規則を定め，違反者には罰則を科している。
(2) 情報の取扱いを徹底するために，定期的な社員教育を実施している。
(3) 本社と営業所において，PC の持込みと持出しは行われていない。
(4) 本社と営業所のネットワークは，ファイアウォールなどでセキュリティ上の脅威から適切に保護されている。
(5) 無線通信（無線 LAN）を設置・利用している者はいない。

図２　移送手段の調査結果

C 主任は，上司である情報セキュリティアドミニストレータの D 課長に，調査結果を報告した。D 課長は，L 社の現状を踏まえた上で，情報の取扱方法ごとに，想定されるリスクと，そのリスクを低減するための情報セキュリティ対策の検討を C 主任に指示した。次は，検討の進め方に関する C 主任と D 課長の会話である。

C 主任：情報セキュリティ対策を検討するには，どのような観点で整理するのがよいでしょうか。
D 課長：そうだな。例えば，リスクを低減するための情報セキュリティ対策を，抑止，予防，検知，回復の四つの観点から検討するという考え方がある。
C 主任：すみませんが，抑止，予防，検知，回復について，もう少し詳しく教えていただけないでしょうか。
D 課長：抑止とは，リスクを［ a ］に発現させようとする者に対して，そうした行為を［ b ］し，思いとどまらせるために実施する対策をいう。予防とは，［ a ］であるか，［ c ］であるかにかかわらず，リスクが発現する原因を取り除くために実施する対策をいう。さらに，検知とは，発現したリスクを早期に発見するために実施する対策であり，回復は，損害を局所化し，原状への復帰を図るために実施する対策をいう。
C 主任：リスクの要素には，［ d ］と［ e ］が含まれているという話を聞いたことがあるのですが，それらとの関係はどう考えればよいのでしょうか。
D 課長：抑止は人的な［ d ］の発生を減少させるためのもの，予防は［ d ］に付け込まれる［ e ］を減少させるためのものと考えれば分かりやすい。
C 主任：分かりました。早速，検討を始めます。

C 主任は，D 課長の説明を踏まえて対策を検討し，その結果を D 課長に報告した。表は，報告のために C 主任が整理した，情報の取扱方法ごとの情報セキュリティ対策である。

表　情報の取扱方法ごとの情報セキュリティ対策

情報の取扱方法	想定されるリスク	情報セキュリティ対策			
		抑止	予防	検知	回復
1. 外部記憶媒体を用いた情報の取扱い	運搬中の USB メモリからの情報漏えい	(略)	①電子ファイルを暗号化してから書き込む。	ア	(略)
	運搬中の USB メモリの紛失	(略)	②かばんに入れて施錠し，直接届ける。	③USB メモリの所在を運搬後に確認する。	(略)
	保管中の USB メモリの紛失	(略)	④キャビネットに施錠保管する。	⑤USB メモリの所在を定期的に確認する。	(略)
2. ファックスを用いた情報の取扱い	誤送信によるファックス送信情報の社外への漏えい	(略)	⑥登録済の短縮番号を用いて送信する。	イ	(略)
	送信したファックスの名あて人への未着	(略)	(略)	⑦名あて人に連絡して到着を確認する。	⑧未着時には再送する。
	受信したファックスの置忘れによる紛失	(略)	ウ	エ	(略)
3. メールを用いた情報の取扱い	メールによる情報の漏えい	オ	⑨電子ファイルを暗号化してから添付する。	⑩メールの内容を記録し，必要に応じて確認する。	(略)
	送信したメールの名あて人への未着	(略)	(略)	⑪名あて人に連絡して到着を確認する。	⑫未着時には再送する。
4. その他の取扱い	(略)	(略)	(略)	(略)	(略)

注　表中の下線は，実施済の対策を表す。

D 課長は，表の内容について C 主任と協議し，必要な修正を加えた上で，情報セキュリティ委員会に対策の実施を上申した。その結果，情報セキュリティ委員会での審議を経て表の情報セキュリティ対策は承認され，規程の整備と，未実施の対策の実施が直ちに進められた。

設問１　本文中の［ a ］～［ e ］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　意図的　　イ　可用性　　ウ　看過　　エ　完全性　　オ　機密性
カ　脅威　　キ　偶発的　　ク　継続的　　ケ　けん制　　コ　資産価値
サ　脆弱性

設問２　図２に示した調査結果を踏まえ，表中の［　ア　］～［　オ　］に入れる適切な追加の対策を，それぞれ35字以内で述べよ。

設問３　L社における情報の取扱いについて，(1)，(2)に答えよ。

(1) 表に示した①～⑫の対策のうち，相互に矛盾を生じて支障を来す可能性のある対策はどれとどれか。①～⑫の中から二つ選び，記号で答えよ。

(2) (1)で挙げた矛盾する対策によって，どのような支障を来すか。30字以内で述べよ。

設問４　リスクへの対応に際しては，リスクの低減だけでなく，リスクの回避を検討する場合がある。本社と営業所間及び営業所相互間でのファックスを用いた情報の送受信におけるリスクを回避するため，あなたが情報セキュリティアドミニストレータであったら，どのような対策を提言するか。L社における情報の取扱方法を踏まえ，USBメモリとファックスを用いない代替策を，50字以内で具体的に述べよ。

問３　電子文書の安全な管理に関する次の記述を読んで，設問 1～5 に答えよ。

P 社は，従業員数 800 名の医薬品会社であり，医薬品の研究開発から製造，販売まで行っている。経営組織としては，事業部制を採用しており，大阪本社のほか，近県に研究センタをはじめ工場や事務所がある。

社内には，新薬研究データや医薬品情報などが電子文書として多数存在する。各事業部では情報の有効活用を図るために，検索対象となる電子文書をあらかじめ走査して索引を作っておく索引型の全文検索によって，高速な検索を可能にしている。

P 社では，情報セキュリティ対策に早くから取り組んでおり，5 年前にはセキュリティポリシを策定し，電子文書取扱規程を定めた。各事業部には，機密文書の指定権者を置いて，電子文書が機密扱いに該当するか否かの判定を行っている。また，ほかの研究機関との共同研究プロジェクトには特に留意し，共同研究過程で利用される機密文書に対しては，期間を限定したアクセスだけ許可することを規定している。

機密文書として指定された電子文書は，閲覧用の PDF ファイルに変換される。閲覧用の PDF ファイルは，印刷，変更，及びクリップボードへのコピーが一切できないように設定されて，ファイルサーバ上の閲覧用フォルダに格納される。一方，元のワープロ文書は，ファイルサーバ上で，特定の従業員だけがアクセスできるフォルダに格納される。従業員の認証情報は一元化されており，閲覧用フォルダ及び特定の従業員だけがアクセスできるフォルダに対しては，認証情報に基づいたアクセス制御を行っている。

〔セキュリティ対策の見直し〕

先月，ある医療機関の PC が盗難に遭って，大量の個人情報が漏えいし，新聞に大きく取り上げられた。これまで P 社では，幸いにして大きな情報漏えい事故は起きていないが，この新聞報道もあって，情報システム部の B 部長は，P 社における機密文書の取扱いについて実態調査を行った。その結果，次の問題が浮上した。

(1) システム的な情報漏えい防止策が，フォルダのアクセス制御に依存しているので，フォルダから取り出したファイルを制御する手立てがなく，情報が第三者に流出するおそれがある。

(2) 設定誤りを検知する仕組みがないので，文書を作成した従業員が電子文書取扱規程に従わずに，変更可能な PDF ファイルを閲覧用フォルダに格納していることが見過ごされ，機密情報の信憑性の低下が懸念される。

(3) 共同研究過程で利用された機密文書が PC に保存され，許可された期間を過ぎても操作可能になっている状況が見られた。

そのほかに，印刷や変更などの操作権限の設定が画一的なので，業務遂行上で必要な操作に支障を来しており，業務効率の低下が見られるという指摘もあった。

B 部長は，これらの問題を重く受け止め，情報セキュリティアドミニストレータの N 主任に，機密文書のセキュリティ対策を見直すよう命じた。

N 主任は，直ちに検討を行い，PDF ファイルに変換する必要がなく，しかも運用が容易な，表に示す電子文書管理システムの導入を提案した。B 部長は，この提案を具体的に進めるよう指示した。

表　電子文書管理システム（骨子）

項目	説明
方式	操作権限管理方式
操作制限の方法	アクセスが許可された者の操作権限を，電子文書ごとにサーバで管理し，操作権限に応じて電子文書の操作を可能にする。電子文書は暗号化され，アクセスが許可されていない者は一切操作できない。
電子文書作成時の作業	[a] の原則にのっとって，アクセスが許可された者，操作権限，アクセス許可期間などを，電子文書ごとに登録する。
印刷やコピー	操作権限の範囲で，各自の PC で行う。

〔電子文書管理システムの導入検討〕

図は，電子文書管理システムの概要である。電子文書管理システムは，アクセスが許可された者のリスト（以下，AL という）や操作権限などを管理する RM サーバ，RM サーバと連携して電子文書に対する操作を行う RM クライアント，及びファイルサーバから構成される。RM クライアントは，ワープロ機能をもち，全従業員に配布される。電子文書管理システムに登録された電子文書は，RM クライアントを使用しない限り中身が読めないように制限されている。RM サーバと RM クライアントの間は，データを公開鍵暗号方式で暗号化して送受信する。このとき用いる公開鍵証明書は，人事データベースなどと連動して，従業員，派遣社員，共同研究プロジェクトの研究者などに一人 1 枚ずつ発行され，従業員の出向や退職派遣契約の終了，共同研究プロジェクトの終了などによって [b] する。

RM サーバは，電子文書の管理単位に配置することとし，当面は事業部ごとに 1 台ずつ配置する。各事業部の機密文書の指定権者は，電子文書管理システムに登録される電子文書の文書管理者となる。文書作成者は，適切な AL や操作権限を電子文書の属性として設定するとともに，電子文書取扱規程に従ったアクセス許可期間を設定する。

1. RM サーバ
(a) 電子文書ごとの属性（作成者，AL の名前，操作権限，アクセス許可期間など），電子文書を暗号化するための電子文書ごとに一意な共通鍵及び AL に関する情報を管理する。操作権限は，AL ごとに設定できる。
(b) 文書作成者からの要求に従って，電子文書ごとの属性の登録，変更，取消し及び表示に必要な処理を行う。登録時は，登録番号を発行する。文書作成者からの要求のうち，本人が作成した文書に対する要求だけを受け付ける。
(c) 文書管理者からの要求に従って，登録されている電子文書の属性一覧の表示を行う。
(d) アクセスが許可された者からの要求に従って，アクセス許可期間内であることを確認の上，電子文書の属性に応じた利用許可証を発行する。

2. RM クライアント
(a) 電子文書の作成・編集及び電子文書に対する操作を行う。
(b) 電子文書の作成・編集後に，RM サーバに対してその電子文書の属性の登録を要求し，発行された登録番号を電子文書に付けて，ファイルサーバに格納する。また，必要に応じて，登録されている電子文書の属性の変更，取消し及び表示を要求する。
(c) ファイルサーバから登録番号付き暗号化ファイルを取り出し，登録番号を抽出して RM サーバに送り，

利用許可証の発行を要求する。利用許可証を受け取ると，暗号化ファイルを復号するとともに，操作権限に従って閲覧や印刷を行う。

3. ファイルサーバ

(a) 全文検索用索引データを抽出するとともに，登録番号付き暗号化ファイルを格納しておく。

4. 処理概要

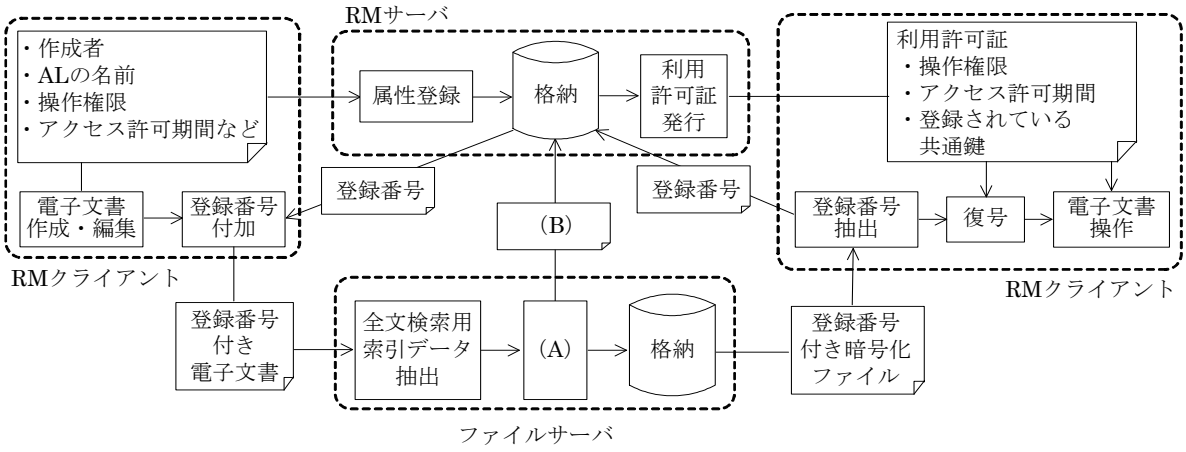

図　電子文書管理システムの概要

次は，電子文書管理システムの運用に関するB部長とN主任の会話である。

B部長：電子文書を利用できない期間があるという事態は許されないので，将来，事業部の統合が起きた場合でも，迅速に対応しなければならないが，運用面で問題はないか。

N主任：事業部の統合に当たって，統合が行われる前に準備が可能な作業や，統合が行われた後の作業はあらかじめ洗い出してあります。これらの作業を確実に行うことで，遅滞なく対応可能です。

この計画は，情報セキュリティ委員会に諮られ，操作権限の設定が適切に行われていないことによって機密情報の流出や信憑性の低下が見過ごされる問題を，①電子文書管理システムを活用した運用方法によって解決できることが評価され，承認された。

電子文書管理システムは，その後，無事に試行段階に入った。また，②共同研究過程で利用された機密文書に対する許可期間限定アクセスも，電子文書管理システムで徹底できるようになった。

設問１　表中の［　a　］及び本文中の［　b　］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　失効　　イ　信頼　　ウ　必要　　エ　変更

設問２　本文中の下線②に関して，電子文書管理システムを用いると，共同研究過程で利用される機密文書に対する許可期間限定アクセスをなぜ徹底することができるのか。30 字以内で具体的に述べよ。

設問３　事業部が統合される場合に，電子文書管理システムを統合後の事業部に対応させるための作業を二つ挙げ，それぞれ 30 字以内で述べよ。

設問４　本文中の下線①で示した運用方法を，40 字以内で具体的に述べよ。

設問５　操作権限管理方式による電子文書管理システムを実現するために必要な，図中 4. 処理概要の（A）の処理内容と（B）の通知内容を，それぞれ二つずつ挙げ，10 字以内で答えよ。

問４　情報セキュリティの継続的改善に関する次の記述を読んで，設問 1～4 に答えよ。

W 社は，正社員数 500 名の電子部品メーカである。都心の本社ビルに総務部，システム部，営業部があり，郊外の工場に設計部，製造部がある。本社ビルには 150 名が勤務しており，そのうちの 90 名が営業部員である。一方，工場には 350 名が勤務しており，その半数が製造部員である。営業部，製造部では，正社員以外に派遣社員及びアルバイトが業務に従事しており，各部署の課ごとに課長が管理している。特に製造部では，頻繁に入れ替わる多数のアルバイトが業務に従事している。

図 1 に，W 社本社ビルの情報システムの構成を示す。W 社では，外出先からインターネット経由で行う営業支援システムへのリモートアクセスを，派遣社員を含む営業部員に許可している。営業支援システムは，営業支援 Web サーバと営業情報 DB サーバによって構成されている。外出先から，ノート PC を使って営業支援システムにリモートアクセスする際は，VPN ゲートウェイサーバをプロキシサーバとして動作させ，LAN2 の営業支援 Web サーバにアクセスする。VPN ゲートウェイサーバからの接続は，営業支援システムに限定されている。

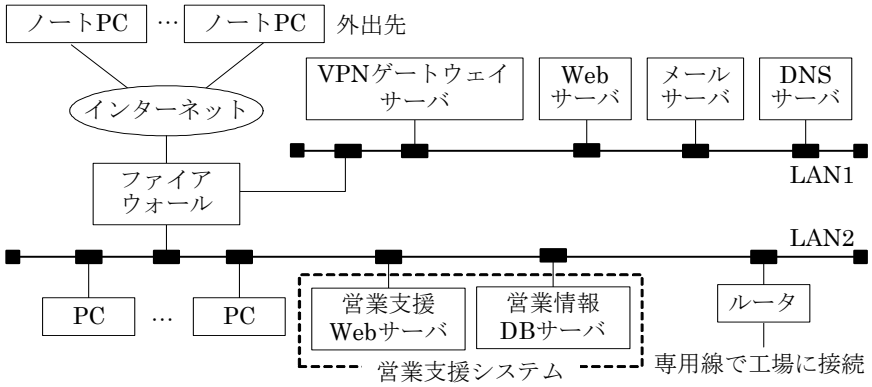

図１　W社本社ビルの情報システムの構成

W 社の全サーバは，ID とパスワードによるアクセス制御が行われており，アカウントの登録及び削除の管理は，サーバごとに任命されたサーバ管理者が行っている。アカウントの付与は，各課の課長が作成するアカウント付与依頼書に基づいて行う。正社員にアカウントを付与する場合は，アカウント付与依頼書に各部署の部長の承認が必要であり，正社員以外の場合には総務部長の承認が必要である。アカウントの削除は，総務部が作成するアカウント削除依頼書に基づいて行う。総務部は，退職した正社員・アルバイト及び派遣契約の終了した派遣社員（以下，退職者という）に関する情報を基にアカウント削除依頼書を作成し，全サーバ管理者に配布する。サーバ管理者は，サーバに登録されたアカウントと対象者を対比して，該当アカウントを削除する。

〔セキュリティインシデントの発見と対応〕

VPN ゲートウェイサーバの管理者であるシステム部の F 君が，ある日，営業部からの問合せによって，現在は業務に従事していない元営業部所属の派遣社員 A 氏のリモートアクセス用アカウントが利用されていることを発見した。そこで，F 君は A 氏のアカウントを削除するとともに，営業支援システムを所管している営業部に対して状況を確認したが，営業支援 Web サーバにおいては A 氏のアカウント

はアカウント削除依頼書に基づいて削除されており，利用できない状態だった。F 君はこの結果を受けて，同様の不正利用を防止するために，VPN ゲートウェイサーバのアカウントに対して①応急対応策を実施した。

その後の調査において，VPN ゲートウェイサーバから A 氏のアカウントが削除されていなかった原因は，アカウント削除依頼書に記載された削除対象者を F 君が見過ごしたことによる，単純な作業ミスであることが判明した。また，この調査の際に，A 氏のアカウント付与依頼書には承認印がなかったこと，及び正社員以外の未承認アカウントが製造部のサーバに登録されていた事例が多数あることも確認された。この件は，セキュリティインシデントとして，経営会議に報告された。

〔セキュリティ対策の見直し〕

W 社では，サーバのアカウント管理のために各種の社内規程を作成し，その遵守についてサーバ管理者に周知徹底を促していた。特に，正社員以外のアカウントの付与については，承認者を総務部長に一元化することによって管理の徹底を図っていた。

しかし，総務部を経由するアカウント付与依頼書の事務処理に時間を要し，派遣社員及びアルバイトの増加に伴って，更に時間がかかることへの不満が多くなり，実際には総務部長の承認前に承認を見越してアカウント登録を行っており，承認後にアカウント登録を行うという運用は徹底されていなかった。また，経営会議において，セキュリティインシデントに関する報告が定性的であり，改善の費用対効果を判断できないことも問題となった。これらの問題を踏まえて，サーバのアカウント管理の実態を定量的に分析し，これを基に課題の優先度を明確にして改善策を具体的に検討することが経営会議において決定され，システム部に対して実態分析と改善策立案の指示が出された。

経営会議での決定を受けて，システム部長は，情報セキュリティアドミニストレータの G 君に，サーバのアカウント管理の現状調査，定量分析，改善策をまとめるように指示した。部長から指示を受けた G 君は，まず定量分析手法を確立する必要があると考え，アカウントの不正利用に関する想定脅威及び分析対象とするサーバのアカウント管理に関する社内規程を明らかにし，これに対応する評価指標を検討して，表 1 を作成した。

表１　Ｇ君が作成した評価指標

評価対象・指標 ／ 想定脅威	評価対象とする社内規程（抜粋）	評価指標
権限をもたない利用者による，情報の不正利用	正社員にアカウントを付与する場合には，各部署の部長の承認を得ること	正社員の未承認アカウントの存在率
	正社員以外にアカウントを付与する場合には，総務部長の承認を得ること	正社員以外の未承認アカウントの存在率
退職者による，アカウントの不正利用	アカウントを利用する必要がなくなった場合には，速やかに削除すること	退職者のアカウントの存在率
a	アカウントの付与は特定の個人を対象とし，共用を禁止すること	共用アカウントの存在率
b	パスワードは，定期的に変更することとし，類推が困難な文字列を採用すること	半年以内にパスワード変更がなかったアカウントの存在率

注　アカウントの存在率（%）＝ 該当するアカウント数／全登録アカウント数×100

〔アカウント管理の調査・分析〕

次にG君は，各部署の所管サーバを対象とする調査用紙を作成し，サーバ管理者に対してサーバの調査を依頼した。その後，回収した調査用紙に記載された数値を基に評価値を算出した。評価値は，サーバ所管部ごとに集計し，表2にまとめた。

表２　Ｇ君が算出した，各部署の所管サーバの評価値

単位 %

サーバ所管部署 / 評価指標	総務部	システム部	営業部	設計部	製造部
正社員の未承認アカウントの存在率	0.0	0.0	0.0	1.2	0.0
正社員以外の未承認アカウントの存在率	2.5	1.3	0.0	2.3	31.1
退職者のアカウントの存在率	0.0	0.0	0.0	0.0	2.5
共用アカウントの存在率	0.0	0.0	0.0	0.0	2.8
半年以内にパスワード変更がなかったアカウントの存在率	0.0	0.0	0.0	0.0	2.4

G君はこの評価値を見て，営業部は社内規程の遵守が徹底されているが，営業部以外では社内規程の遵守の徹底に問題があると推測した。特に製造部では，アルバイトが業務に多数従事しており，このことが社内規程遵守の不徹底の原因ではないかと推測した。その後，G 君は，②すべての部署に対して，所管サーバのアカウント管理状況について聞取り調査を実施した。その結果，製造部では，アルバイトへのアカウント付与を早く実施してほしいという各課の課長からの要望が強く，アカウント付与依頼書への総務部長の承認を待たずにサーバ管理者にアカウントを登録させていることが判明した。一方，営業部では，サーバ管理者の作業ミスを防止するために，サーバ管理者以外の者がアカウントの定期点検を実施していることが分かった。

〔アカウント管理の調査結果報告と現状の改善〕

G君は，図2の改善案を作成し，サーバのアカウント管理の実態評価方法とともに，システム部長に検討結果を報告した。

社内規程への追加・修正事項などの改善案

(1) 各部署において，アカウント点検者を新たに任命する。

(2) アカウント点検者は，サーバに登録されているアカウントを毎月点検して，次の事項を確認する。

①正社員のすべてのアカウントが，各部署の部長の承認済であること

②正社員以外のすべてのアカウントが，総務部長の承認済であること

③退職者のアカウントが，アカウント削除依頼書の記載どおりに削除されていること

④共用アカウントが存在しないこと

(3) サーバ管理者は，半年間変更履歴のないパスワードを強制変更する。

(4) アカウント点検者は，パスワードの変更状況を定期的に確認する。

図２　Ｇ君が作成した改善案

システム部長は，アカウント管理状況の定量化の目的は，改善結果を客観的に把握することであると考えていた。G 君が選定した評価指標は定量化の目的に合致したものであり，改善の度合いも定量的に評価できると判断した。また，G 君が作成した改善案は追加投資が不要であり，費用対効果が高いと判断した。しかし，この改善案では，すべての問題を解決するには至らないと判断し，製造部の現状を考慮した上で③アカウント付与に関する社内規程を遵守しやすい内容にするための修正を改善案に追加するよう，G 君に指示した。

その後，システム部長の指示を反映した改善案が経営会議で承認され，社内で実行に移された。この改善策が効を奏し，半年後の調査では，製造部のアカウント管理についても改善が確認された。

設問１　表 1 中の［　a　］，［　b　］に入れる想定脅威を評価対象とする社内規程を参考に，それぞれ 25 字以内で述べよ。

設問２　本文中の下線①について，実施した応急対応策を，25 字以内で述べよ。

設問３　本文中の下線②の聞取り調査について，(1) ～ (3) に答えよ。

(1) 各部署の所管サーバの評価値の精度を確保するために，聞取り調査時に確認すべきことを，25 字以内で述べよ。

(2) 社内規程が遵守されていないと思われる部署において，聞取り調査をする目的は何か。G 君の現状調査の手順を踏まえて，30 字以内で述べよ。

(3) 社内規程が遵守されていると思われる部署において，聞取り調査をする目的は何か。G 君の今回の調査における成果を踏まえて，30 字以内で述べよ。

設問４　本文中の下線③の修正について，(1)，(2) に答えよ。

(1) システム部長は，アカウント付与に関する社内規程を修正することによって，原因となっているどのような状況を改善できると考えているか。その原因を 30 字以内で述べよ。

(2) システム部長の指示に対して，どのような修正が考えられるか。45 字以内で述べよ。