問2　社内システムの情報セキュリティ対策強化に関する次の記述を読んで，設問 1～5 に答えよ。

A 社は，従業員数 500 名の金属加工会社である。A 社では，電子メール（以下，メールという）の送受信，Web の閲覧，及び Web サーバによる情報公開にインターネットを利用している。社外に公開するドメイン名として a-sha.co.jp（以下，A 社ドメイン名という），サブドメイン名として cc.a-sha.co.jp（以下，A 社サブドメイン名という）を利用している。

〔メールによる情報交換〕

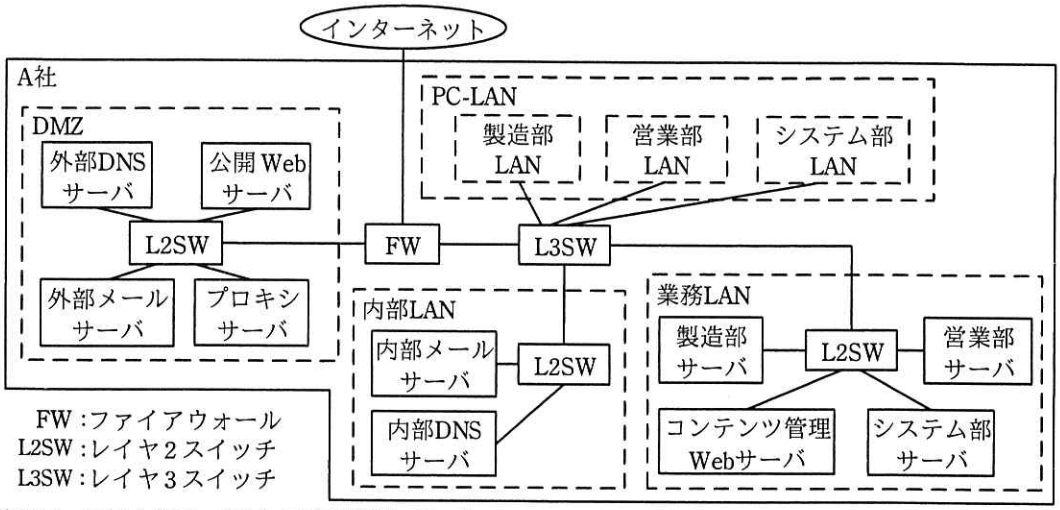
A 社では，業者とデータを交換する場合，ファイルを，あらかじめ取り決めたパスワードで暗号化し，メールに添付して送受信している。さらに，担当者不在の場合でも迅速に対応できるように，担当者が所属するグループの同報用メールアドレスにもメールを送信してもらっている。グループ同報用メールアドレスに届いたメールは，グループに所属する従業員全員のメールアドレスに転送（以下，同報転送という）される。A 社で使用しているメールアドレスの種別を表 1 に示す。

表 1　A 社で使用しているメールアドレスの種別

種別	メールアドレス	概要
従業員用メールアドレス	*user*@a-sha.co.jp	従業員が利用するメールアドレスである。*user* は，従業員ごとに異なる文字列を割り当てる。
グループ同報用メールアドレス	*group*@cc.a-sha.co.jp	同報転送に利用するメールアドレスである。*group* は，グループごとに異なる文字列を割り当てる。
通知用メールアドレス	no-reply@a-sha.co.jp	A 社内のサーバから送信される通知用メールの送信者メールアドレスである。

〔A 社の情報システム〕

A 社の情報システムのネットワーク構成を図 1 に示す。



注記1　PCは全て，PC-LANに接続している。
注記2　PCの記載は省略している。

図1　A社の情報システムのネットワーク構成

DMZの各サーバには，グローバルIPアドレスを割り当てている。L3SW，PC，内部LANのサーバ及び業務LANのサーバには，プライベートIPアドレスを割り当てている。

ウイルス対策として，サーバ及びPCにW社のウイルス対策ソフトを導入している。サーバ及びPCでは，リアルタイムスキャンを有効にし，さらに，サーバでは毎週土曜日20時に，PCでは毎日12時にフルスキャンを起動している。ウイルス定義ファイルは，サーバ，PCとも，1時間おきに更新している。

A社では，全ての従業員にPCを1台ずつ貸与している。PCのOS及びソフトウエアの脆弱性修正プログラムを，それぞれ毎月1回自動で適用している。

〔DMZのサーバの概要〕

A社は，2年前にDMZへのプロキシサーバ新設に合わせ，DMZの全サーバをリプレースした。DMZのサーバは，システム部が運用している。システム部では，業者に委託して，年1回，DMZのサーバに対するインターネットからの脆弱性検査を実施しており，問題がないことを確認している。また，システム部では，DMZのサーバで使用されているOS及びソフトウェアの脆弱性情報を収集している。DMZのサーバでは，脆弱性修正プログラムがリリースされてから1か月以内に適用するよう

にしている。

DMZ のサーバの機能概要を表 2 に示す。

表 2　DMZ のサーバの機能概要（抜粋）

機器名	概要
外部 DNS サーバ	・DNS コンテンツ機能 - A 社ドメイン名及び A 社サブドメイン名を管理する。 ・DNS キャッシュ機能 - オープンリゾルバ対策が行われており，再帰的な DNS 問合せを許可するのは，公開 Web サーバ，外部メールサーバ，プロキシサーバ及び内部 DNS サーバだけである。 ・ログ取得機能 - DNS 問合せ及びその結果は記録しない。 - DNS サーバプログラムの起動と停止を記録する。
外部メールサーバ	・転送機能 - インターネットと内部メールサーバとの間でメールを転送する。 - サーバ証明書を用いて SMTP 通信をセキュアにした [a] に対応している。 - SMTP の転送元 IP アドレスとエンベロープの宛先メールアドレスのドメイン名の組合せで，メールの転送先を決定する。 ・ログ取得機能 - メールの転送結果，転送元 IP アドレス，転送先 IP アドレス，送信者メールアドレス，宛先メールアドレス及びメールサイズを記録する。 - メールの転送を行う [b] プログラムの起動と停止を記録する。
プロキシサーバ	・プロキシ機能 - PC，内部 LAN のサーバ，及び業務 LAN のサーバから，DMZ，及びインターネット上の Web サーバへの HTTP 通信及び HTTP over TLS 通信を中継する。 ・HTTP ウイルススキャン機能 - HTTP 通信のウイルススキャンを行う。 ・URL フィルタリング機能 - サーバ管理者が登録できる管理者ホワイトリスト及び管理者ブラックリスト，並びにベンダが提供するベンダブラックリストを使う。 - フィルタリングルールは，送信元 IP アドレス単位に設定できる。 ・ログ取得機能 - 送信元 IP アドレス，URL，HTTP ヘッダ情報及び通信データサイズを記録する。 - プロキシサーバプログラムの起動と停止を記録する。

外部メールサーバの転送機能の設定を表 3 に示す。この設定によってオープンリレーが防止されている。

表3　外部メールサーバの転送機能の設定

項番	転送元 IP アドレス	宛先メールアドレスのドメイン名	処理
1	全て	A 社ドメイン名，A 社サブドメイン名	[c] に転送する。
2	[c] の IP アドレス	全て	宛先メールアドレスのドメイン部を基に MX レコードを問い合わせる。MX レコードの FQDN を基に，A レコードを問い合わせ，得られた IP アドレスに転送する。
3	全て	全て	拒否する。

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

〔内部 LAN のサーバ及び業務 LAN のサーバの概要〕

内部 LAN のサーバは，システム部が運用している。内部 LAN のサーバの機能概要を表 4 に，内部メールサーバの転送機能の設定を表 5 に，業務 LAN のサーバの機能概要を表 6 に示す。

表4　内部 LAN のサーバの機能概要

機器名	概要
内部メールサーバ	・転送機能 - 外部メールサーバとの間でメールを転送する。 - 業務 LAN のサーバからのメールを転送する。 - 宛先メールアドレスのドメイン名が A 社ドメイン名又は A 社サブドメイン名の場合，メールをメールボックスに格納する [d] プログラムを起動する。 - SMTP の転送元 IP アドレスとエンベロープの宛先メールアドレスのドメイン名の組合せで，メールの転送先を決定する。 - 業務 LAN のサーバから送信される通知用メールの宛先メールアドレスは，従業員用メールアドレスだけである。 ・メールアーカイブ機能 - 送信者メールアドレスのドメイン名，宛先メールアドレスのドメイン名のいずれかが，A 社ドメイン名でも A 社サブドメイン名でもないメールを保管する。サーバ管理者は，Web インタフェースを使って，保管したメールを検索できる。 ・PC からのメール転送機能，メールボックス機能及び POP3 機能 ・SMTP ウイルススキャン機能 - SMTP 通信のウイルススキャンを行う。 ・ログ取得機能 - メールの転送結果，転送元 IP アドレス，転送先 IP アドレス，送信者メールアドレス，宛先メールアドレス及びメールサイズを記録する。 - メールの転送を行う [b] プログラム，メールをメールボックスに格納する [d] プログラム，及び POP3 プログラムの起動と停止を記録する。

表 4　内部 LAN のサーバの機能概要（続き）

機器名	概要
内部 DNS サーバ	・DNS コンテンツ機能 - 社内専用のドメイン名を管理する。 ・DNS キャッシュ機能 - 内部 DNS サーバで解決できない DNS 問合せは，外部 DNS サーバに DNS 問合せを送る。 ・ログ取得機能 - DNS 問合せの内容とその結果は記録しない。 - DNS サーバプログラムの起動と停止を記録する。

表 5　内部メールサーバの転送機能の設定

項番	転送元 IP アドレス	宛先メールアドレスのドメイン名	処理
1	全て	A 社ドメイン名	メールをメールボックスに格納する [d] プログラムを起動する。
2	全て	A 社サブドメイン名	同報転送処理を起動する。
3	A 社が利用しているプライベート IP アドレス	全て	外部メールサーバに転送する。
4	全て	全て	拒否する。

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

表 6　業務 LAN のサーバの機能概要（抜粋）

機器名	概要
コンテンツ管理 Web サーバ	・Web サーバ機能 - 公開 Web サーバでの公開前に，表示確認を行うための機能である。 ・コンテンツ管理機能 - 公開 Web サーバで使用するコンテンツのバージョン管理を行う。 - 公開するコンテンツを，コンテンツ管理 Web サーバから公開 Web サーバに，コンテンツ管理者の指示で転送する。 ・ログ取得機能 - 送信元 IP アドレス，URL，HTTP ヘッダ情報及び通信データサイズを記録する。 - Web サーバプログラム及びコンテンツ管理プログラムの起動と停止を記録する。

業務 LAN のサーバ間では，日次でデータの転送がある。業務 LAN のサーバのうちコンテンツ管理 Web サーバは，システム部が運用している。各部のサーバはそれぞれの部で運用している。

内部 LAN のサーバ及び業務 LAN のサーバでは，OS 及びソフトウェアの脆弱性修正

プログラムの適用を年 1 回実施している。直近では，2 か月前の 3 月に実施した。しかし，コンテンツ管理 Web サーバ及び営業部サーバでは，ソフトウェアの動作検証が間に合わず，OS 及びソフトウェアの脆弱性修正プログラムの適用を 8 月に延期した。

〔マルウェア感染と調査〕

5 月 11 日 13 時 10 分に，システム部 Web 管理グループの H さんからシステム部運用グループの E 主任に，“PC のフルスキャン中に PDF ファイルがマルウェア X として検出され，駆除された”との連絡があった。5 月 9 日に，H さんは次の操作を行ったとのことであった。

・この PDF ファイルは，公開 Web サーバで公開するコンテンツの一部であり，暗号化された形でコンテンツ作成業者 B 社の J 氏からメールで送信されたファイルの一つである。送信されたファイルを，一旦，PC 上で復号し，展開した。
・復号し，展開したファイルをコンテンツ管理 Web サーバにアップロードした。
・コンテンツ管理 Web サーバでコンテンツの内容を確認した。

E 主任は，念のために，各部のサーバ管理者にサーバのフルスキャンを依頼した。フルスキャンの結果，コンテンツ管理 Web サーバではマルウェア X 及びマルウェア Y が，営業部サーバではマルウェア Y が検出され，駆除された。E 主任は，上司の D 部長に一報するとともに，部下の F さんに調査を指示した。

F さんが行った調査の結果と感染への対処を図 2 に示す。

(1) H さんへのヒアリング結果
・5 月 9 日 8 時 30 分，PC 上のメールソフトでメールを受信した。
・5 月 9 日 8 時 40 分，Web 管理グループの同報用メールアドレス宛てに J 氏から送信されたメールを開き，あらかじめ取り決めてあったパスワードを用いて，メールに添付された暗号化圧縮ファイルを復号し，展開した。
・5 月 9 日 8 時 50 分，展開したファイルをコンテンツ管理 Web サーバにアップロードした。
・5 月 9 日 9 時，サーバ室に出向き，コンテンツ管理 Web サーバの設定を変更するために，管理者 ID でログインした。設定変更後，コンテンツ管理 Web サーバで，コンテンツの内容を確認した。
・5 月 11 日 13 時，PC のフルスキャンで，PDF ファイルがマルウェア X として検出され，駆除されたとのメッセージが表示された。
・コンテンツは公開 Web サーバには転送していない。

図 2　調査結果と感染への対処

(2) マルウェアXに関する情報
- ダウンロード型のマルウェアであり，内部に C&C（Command and Control）サーバの URL が保持されている。C&C サーバからマルウェアYをダウンロードする。
- PDF 閲覧ソフトの脆弱性を悪用して PC を感染させる。2 月にリリースされた PDF 閲覧ソフトの脆弱性修正プログラムを適用していれば，マルウェアYをダウンロードしない。

(3) マルウェアYに関する情報
- OS のバッファオーバフローの脆弱性を悪用して，ネットワーク経由で感染を広げる。2 月にリリースされた OS の脆弱性修正プログラムを適用していれば，ネットワーク経由では感染しない。
- マルウェア中に多数の FQDN が保持されている。
- OS の設定で指定された DNS サーバに対して，マルウェアに保持された FQDN の全ての TXT レコードを問い合わせ，得られた文字列を指示として解釈し，動作する。
- メール送信機能があり，インストールされているメールソフトに設定されているメールサーバの情報を用いてメールを送信する。その際，送信者メールアドレスは，メールソフトに設定された送信者メールアドレスを用いる。

(4) W社の対応
- 5 月 11 日 3 時，W社は，マルウェアX及びマルウェアYに対応したウイルス定義ファイルをリリースした。

(5) コンテンツ管理 Web サーバの調査
- OS のバッファオーバフローの脆弱性を悪用され，マルウェアYに感染したと考えられる。
- 内部メールサーバへの通知用メールの送信テストを目的に，H さんが，メールソフトをインストールしていた。

(6) 内部メールサーバの調査
- 5 月 9 日 10 時，コンテンツ管理 Web サーバが転送元で，メールサイズが 1k バイトのメールが 10 通，転送された。送信者メールアドレスは，コンテンツ管理 Web サーバのメールソフトに設定されているメールアドレスであり，宛先メールアドレスはインターネット上のメールアドレスであった。メールアーカイブ機能を用いて調査した結果，J 氏からメールで受け取ったファイル名の一覧が送信されていた。

(7) 営業部サーバの調査
- OS のバッファオーバフローの脆弱性を悪用され，ネットワーク経由でマルウェアYに感染したと考えられる。

(8) Hさん及び営業部への依頼事項
（省略）

図2　調査結果と感染への対処（続き）

E 主任と F さんは図 2 について D 部長に報告した。複数のサーバでマルウェアが検出されたことから，D 部長は，セキュリティ対策の見直しが必要と判断し，セキュリティ専門業者の C 社に助言を求めることにした。C 社の P 氏が担当することになった。

F さんと P 氏は，図 2 を精査した。P 氏は，追加の調査事項として，次の 2 項目を挙げた。

・マルウェア X に感染したサーバから C&C サーバへの HTTP 通信及び HTTP over TLS 通信の有無を確認するために，[e] のログから [f] という条件に合致するログを抽出する。

・[g] のログから，マルウェア Y によって送信されたメールが [h] という条件に合致するログを抽出する。

F さんは，P 氏が挙げた調査を実施した。

続いて，F さんと P 氏は，マルウェア Y への対策について検討した。次は，その際の会話である。

P 氏　：マルウェア Y は，C&C サーバから指示を受け取ります。マルウェア Y と同様のタイプのマルウェアに感染した場合に備えて，①外部 DNS サーバと内部 DNS サーバの DNS 問合せに関する設定を変更してください。

F さん：はい，分かりました。

P 氏　：さらに，内部 DNS サーバで，DNS 問合せの内容とその結果をログに記録すると，マルウェア Y と同様のタイプのマルウェアの検出に役立ちます。

F さん：マルウェア中に多数の FQDN があり，それぞれの FQDN に合致するログを抽出するのは時間が掛かりそうです。効率よく抽出するにはどうしたらいいでしょうか。

P 氏　：内部 DNS サーバのログから [i] という条件に合致するログを抽出する方法はどうですか。

F さん：それならば，すぐにできます。

F さんと P 氏は，検討した結果を運用手順としてまとめた。

〔ウイルス対策の強化の検討〕

F さんと P 氏は，図 2 を基にし，ウイルス対策の強化について検討することにした。P 氏は，問題点として，次の 5 点を挙げた。

(あ) SMTP ウイルススキャンでは，暗号化されたファイルについてウイルス検出ができないこと

(い) PC 利用者からのマルウェア感染の申告をきっかけにして，調査及び対処に着手しているが，マルウェア感染の影響を最小限にするためには，遅過ぎること

(う) 図2中の(6)にあるようなメール送信を防止するための対策が不十分であること

(え) 業務 LAN のサーバから C&C サーバへの通信を遮断するための対策が不十分であること

(お) 業務 LAN のサーバ間のマルウェア感染を防止するための対策が不十分であること

問題点(あ)について，P 氏は，コンテンツ作成業者との間でファイルをやり取りするためにデータ交換サーバを DMZ に導入すること，及びメールへのファイル添付を禁止することを，F さんに提案した。データ交換サーバの機能を図3に示す。

(1) アップロード，ダウンロード及び削除機能
・Web インタフェースを使って，ファイルのアップロード，ダウンロード及び削除を行う。
(2) 認証機能
・利用者 ID 及びパスワードを使って認証する。
(3) アクセス制限機能
・フォルダ及びファイルごとに，アクセス可能な利用者 ID を設定する。
・あらかじめ登録された IP アドレスからの接続だけを許可する。
(4) ウイルススキャン機能
・ファイルのアップロード及びダウンロード時にウイルススキャンを行う。
(5) 通信の暗号化機能
・HTTP over TLS を用いて通信を暗号化する。
(6) 利用者管理機能
（省略）

図3　データ交換サーバの機能

さらに，P 氏は，②図 3 中の(4)のウイルススキャン機能を有効なものとするためのアップロード時の注意点を説明した。

問題点(い)について，F さんと P 氏は検討の結果，サーバ用及び PC 用の③ウイルス対策集中管理ソフトをインストールしたウイルス対策管理サーバの導入を提案することにした。

〔内部 LAN のサーバに関する見直し〕

問題点(う)について，F さんと P 氏は内部メールサーバの設定を見直すことにした。次は，その際の会話である。

F さん ：内部 DNS サーバ及び業務 LAN のサーバから内部メールサーバに転送されるインターネット宛てのメールを拒否する方法はありますか。

P 氏　 ：表 5 を見直し，表 7 のとおりに変更すれば，拒否できます。

F さん ：はい，分かりました。表 7 のとおり，設定変更を提案します。

表 7　見直し後の内部メールサーバの転送機能の設定

項番	転送元 IP アドレス	宛先メールアドレスのドメイン名	処理
1	全て	A 社ドメイン名	メールをメールボックスに格納する [d] プログラムを起動する。
2	[j] の IP アドレス，外部メールサーバの IP アドレス	A 社サブドメイン名	同報転送処理を起動する。
3	[j] の IP アドレス	全て	外部メールサーバに転送する。
4	全て	全て	拒否する。

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

引き続き，内部 DNS サーバの設定を見直し，問題がないことを確認した。

〔業務 LAN のサーバに関する見直し〕

問題点(え)について，F さんと P 氏は，検討の結果，業務 LAN のサーバからインターネットへの通信として，OS 及びソフトウェアの脆弱性修正プログラムのダウンロード，並びにウイルス定義ファイルのダウンロードだけを許可するように，プロキシサーバの設定変更を提案することにした。

問題点(お)に起因するマルウェア感染によって，万が一，業務 LAN のサーバが 1 台でも停止すると，A 社の業務に著しい支障が発生する。しかし，脆弱性修正プログラムがリリースされたとしても，業務 LAN のサーバでは，動作検証に時間を要し，すぐに適用できないこともある。そこで，P 氏は，④業務 LAN のサーバ間の必要な

通信を維持しながら業務 LAN のサーバ間のマルウェア感染を防止するセキュリティ強化案を提案した。

Fさんと P 氏がまとめた提案内容は，D 部長の承認を得た。一部の対策は即時実施され，ウイルス対策管理サーバ及びデータ交換サーバの導入，並びにセキュリティ強化案については，今年度末に予定されている内部 LAN のサーバ及び業務 LAN のサーバのリプレース計画に反映され，実施されることになった。

設問1　A 社のサーバについて，(1)～(3)に答えよ。

(1)　表 2 中の [a] に入れる適切な字句を，英字で答えよ。

(2)　表 2 中及び表 4 中の [b]，表 4 中，表 5 中及び表 7 中の [d] 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　MDA（Mail Delivery Agent）　　イ　MSA（Mail Submission Agent）

ウ　MTA（Mail Transfer Agent）　　エ　MUA（Mail User Agent）

(3)　表 3 中の [c] に入れる適切な字句を，図 1 中の構成要素から選び，答えよ。

設問2　〔マルウェア感染と調査〕について，(1)～(4)に答えよ。

(1)　本文中の [e] に入れる適切な字句を，図 1 中の構成要素から選び，答えよ。また，本文中の [f] に入れる抽出条件を，30 字以内で述べよ。

(2)　本文中の [g] に入れる適切な字句を，図 1 中の構成要素から選び，答えよ。また，本文中の [h] に入れる抽出条件を，25 字以内で述べよ。

(3)　本文中の下線①について，外部 DNS サーバと内部 DNS サーバの DNS 問合せに関する設定変更の内容を，それぞれ 35 字以内で述べよ。

(4)　本文中の [i] に入れる抽出条件を，30 字以内で述べよ。

設問3　〔ウイルス対策の強化の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線②について，注意点とは何か。20 字以内で述べよ。

(2)　本文中の下線③について，調査及び対処の着手の早期化を期待してウイルス対策集中管理ソフトを導入する場合，A 社がウイルス対策集中管理ソフトに求める機能はどのようなものか。40 字以内で述べよ。

設問4　表 7 中の [j] に入れる適切な字句を，図 1 中の構成要素から選び，答

えよ。

設問5　本文中の下線④について，P 氏が提案したセキュリティ強化案を，35 字以内で具体的に述べよ。