問２　情報セキュリティ対策の強化に関する次の記述を読んで，設問1～7に答えよ。

A社は，従業員数200名の金型加工業者である。新潟市内の同じ敷地に本社と工場が，大阪市に営業拠点がある。本社には，管理部，設計部及び製造部がある。管理部には，総務係，営業係及びシステム係がある。営業係は，営業拠点を管理する。製造部は，工場を管理する。

A社の金型加工技術は，評価が高く，大企業から金型加工を請け負うことがある。請け負うときは，金型加工に必要な情報を収めたファイル（以下，設計情報ファイルという）を，DVD-R又は電子メール（以下，メールという）を使って，発注元との間でやり取りする。

A社では，最新技術の情報収集を目的として，取引先が参加している複数のメーリングリストに，営業係員及び設計部員が参加している。

〔営業秘密の取扱い〕

A社では，自社の営業秘密が不正競争防止法で保護されるようにするために，不正競争防止法及び経済産業省が公表している営業秘密管理指針（平成27年1月28日全部改訂）を参考にして，表1に示す営業秘密に関する管理規則を定めている。

表1　営業秘密に関する管理規則（概要）

要件名	管理規則（概要）
[a]性	・営業秘密を含む文書は，全てのページにA社秘密情報と記載すること ・閲覧できる者を，A社の業務上必要な従業員に制限すること
[b]性	・A社で開発し，A社の事業に必要な金型加工技術の情報を，営業秘密とすること
[c]性	・営業秘密は，一般的に知られた状態にならないように，業界誌などの刊行物に掲載しないこと

〔A社のネットワーク構成〕

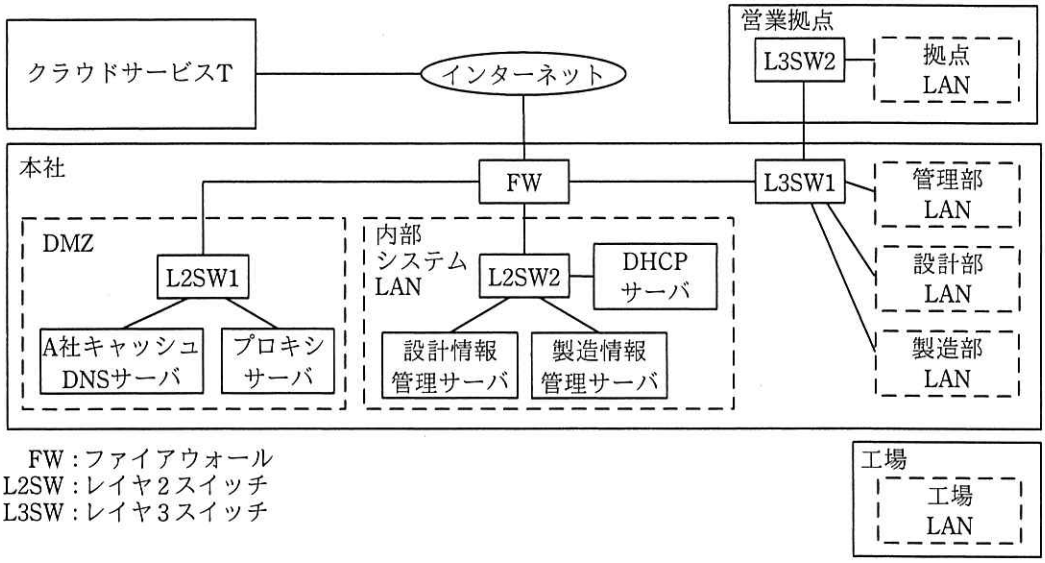
A社では，デスクトップPC（以下，DPCという）を，全ての従業員に貸与している。DPCの社外への持出しは，禁止されている。

A社は，クラウドサービスTを利用している。クラウドサービスTの機能とA社での利用方法の概要を表2に示す。

表2　クラウドサービスTの機能とA社での利用方法の概要（抜粋）

サービス名	IPアドレス	機能名	機能と利用方法の概要
権威 DNS サービス	x2.y2.z2.2, x2.y2.z3.4	ドメイン名登録及び提供機能	・インターネット向けのA社ドメイン名の情報を登録し，提供する。
キャッシュ DNS サービス	x2.y2.z2.3	DNS キャッシュ機能	・インターネット上のドメイン名の名前解決を行う。 ・オープンリゾルバ対策として，クラウドサービスT上のサーバからの名前解決だけを許可する。
メールサービス	x2.y2.z2.17	メール転送機能	・SMTP を使用し，インターネットとの間でメールを転送する。 ・迷惑メールの踏み台として使われないよう，[d] 対策として，インターネットから転送されてきたメールのうち，宛先メールアドレスのドメイン名がA社ドメイン名のメールだけを受信する。
		マルウェア対策機能	・送受信時にメールのマルウェアスキャンを行い，マルウェアが検知されたメールを隔離する。
		Web メール機能	・DPC とメールサービスとの間は，HTTP over TLS を使用する。
		Web メール接続元制限機能	・A社のネットワークからの利用だけが可能となるよう，①特定のネットワークからの接続だけを許可している。

A社のネットワーク構成を図1に，A社のネットワーク一覧を表3に示す。



FW：ファイアウォール
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ

注記1　工場 LAN は，閉じたネットワークである。

注記2　工場 LAN に接続されている工作機械及び管理サーバの記載は省略している。

注記3　拠点 LAN，管理部 LAN，設計部 LAN 及び製造部 LAN に接続されている DPC の記載は省略している。

注記4　内部システム LAN 上のサーバ及び DPC からのインターネットアクセスは，プロキシサーバ経由で行われる。

図1　A社のネットワーク構成

表3　A社のネットワーク一覧

ネットワーク名	ネットワークアドレス
DMZ	x1.y1.z1.16/29
内部システム LAN	192.168.1.0/24
管理部 LAN	192.168.16.0/24
設計部 LAN	192.168.19.0/24
製造部 LAN	192.168.21.0/24
工場 LAN	192.168.32.0/24
拠点 LAN	192.168.64.0/24

〔A社の情報システム〕

DMZ 上のサーバには，グローバル IP アドレスを割り当てている。DMZ 上のサーバの概要を表4に示す。

表4　DMZ上のサーバの概要（抜粋）

サーバ名	IPアドレス	機能名	機能と利用方法の概要
A社キャッシュDNSサーバ	x1.y1.z1.17	DNSキャッシュ機能	・インターネット上のドメイン名の名前解決を行う。 ・オープンリゾルバ対策として［　e　］からの名前解決だけを許可する。
		時刻同期機能	・国立研究開発法人情報通信研究機構がインターネット上で公開している［　f　］サーバと時刻同期を行う。
プロキシサーバ	x1.y1.z1.18	URLフィルタリング機能	・接続元IPアドレスごとに，接続できるURLを制限する。

内部システムLAN上のサーバの概要を表5に示す。

表5　内部システムLAN上のサーバの概要（抜粋）

サーバ名	IPアドレス	機能名	機能と利用方法の概要
DHCPサーバ	192.168.1.2	DHCP機能	・IPアドレスを割り当てるDPCのMACアドレスをあらかじめ登録しておく。 ・登録済みMACアドレスのDPCにIPアドレスを割り当てる。
設計情報管理サーバ	192.168.1.3	設計情報管理機能	・利用者は，Webインタフェースを用いて，設計情報ファイルのアップロード，ダウンロード及び検索を行うことができる。 ・利用者IDとパスワードで利用者認証を行う。 ・パスワードは10字以上とし，英数字及び記号を使用できる。 ・設計部のサーバ管理者が，利用者IDと初期パスワードを登録する。 ・フォルダごとにアクセス権限を設定できる。現在は，利用者IDごとに割り当てられたフォルダ配下のファイルにアクセスできる。
		アクセス制限機能	・接続元のIPアドレスによってアクセスを制限する。アクセスを許可するIPアドレスには，A社で利用するプライベートIPアドレスを登録する。
製造情報管理サーバ	192.168.1.4	製造情報管理機能	（省略）

A社では，全ての従業員に個別のメールアドレスを割り当てており，従業員は，メールサービスを用いてメールを送受信している。

従業員のメールアドレス以外に同報用のメールアドレスがあり，このアドレスに届いたメールは，登録された従業員のメールアドレスに同報される。

従業員は，第三者に秘匿したい電子ファイルをメールに添付し，金型加工の発注元との間で送受信する場合には，ZIP 形式で圧縮している。メール添付する際の圧縮ファイルの取扱いについては，次のルールを定めている。

・発注元ごとの打合せで取り決めた，12 字以上の英数字及び記号で構成されるランダムな文字列から成るパスワードから生成した鍵を用いて暗号化する。

・暗号化アルゴリズムは，[g] を用いる。[g] は，[h] が選定した，電子政府における調達のために参照すべき暗号リスト（平成 30 年 3 月 29 日版）でも利用が推奨されている共通鍵暗号である。[h] は，暗号技術の適切な実装法や運用法の調査及び検討を行う国内のプロジェクトである 。

設計情報管理サーバの利用者は，設計部員及び製造部員である。利用者 ID は，利用者のメールアドレスである。初期パスワードには，メールアドレスと同じ文字列を登録し，利用者に通知する。利用者は，自身でパスワードを変更することができる。

FW，プロキシサーバ，内部システム LAN 上のサーバ，及び全ての DPC は，A 社キャッシュ DNS サーバとの間で [f] を用いて時刻同期を行っている。

DPC の IP アドレスは，DHCP サーバの DHCP 機能及び L3SW の DHCP リレーエージェント機能によって，動的に割り当てられる。

A 社では，DMZ 上及び内部システム LAN 上にあるサーバの名称と IP アドレスの対応を DPC の hosts ファイルに設定している。

DPC，DMZ 上のサーバ及び内部システム LAN 上のサーバは，導入時に，OS，アプリケーションソフトウェア及びマルウェア対策ソフト（以下，これらを併せてA社標準ソフトという）に脆弱(ぜい)性修正プログラムを適用し，マルウェア対策ソフトはマルウェア定義ファイルを導入時点での最新版に更新している。

導入後は，プロキシサーバ経由でA社標準ソフトの各ベンダのサイトに毎月末に自動で接続し，それぞれの脆弱性修正プログラムを適用している。

DPC 及びサーバ上のマルウェア対策ソフトは，起動時及び起動後 2 時間おきにプロキシサーバ経由でマルウェア対策ソフトベンダのサイトからマルウェア定義ファ

イルをダウンロードし，更新している。マルウェア対策ソフトでは，ファイルを読み書きするときにマルウェアスキャンする機能（以下，リアルタイムスキャンという）を有効にするとともに，全てのファイルをマルウェアスキャンする機能（以下，フルスキャンという）を，毎週火曜日 12 時に実行している。フルスキャン実行時，CPU の負荷を減らすために，圧縮ファイルは対象外としている。

〔情報漏えいの発生〕

6 月 7 日，金型加工業者 B 社の L 氏から，設計情報管理サーバの管理者である設計部の J さんに，A 社の情報が漏えいしているおそれがあると連絡があった。J さんは，設計部長及び管理部の E 部長に報告した。J さんの報告内容を，次に示す。

・L 氏が，検索サイトで金型技術情報を検索したところ，A 社と B 社が共同で展示会に出品する金型（以下，共同出品金型という）の設計情報ファイル（以下，ファイル S という）と同じ名称のファイルが，ある Web ページに掲載されていることを発見した。

・ファイル S は，DVD-R に保存し，6 月 1 日に J さんから L 氏に手渡している。（以下，当該 DVD-R を DVDS という）

・L 氏が，掲載されていた Web ページを確認したところ，ファイル S と同じ名称をもつファイルの更新日付は 6 月 4 日と表示されていた。

・L 氏は，掲載されていたファイルがファイル S と同一であるかどうかの確認及び B 社における設計情報ファイルの管理状況の調査を，B 社のセキュリティ担当者に依頼した。

・B 社のセキュリティ担当者は，同一ファイルであることを確認するためファイルの［　i　］を調べた。その結果，DVDS 中のファイル S の［　i　］と同じであったので，同一ファイルであることが確認された。

・B 社では，全ての設計情報ファイルを，設計室の閉じたネットワークにだけ接続された PC 及びサーバで利用しており，インターネットに漏えいする可能性は低い。

・B 社では，DVD-R などの外部記録媒体の持込み，持出し及び使用を管理している。管理記録によれば，DVDS に関する記録は，設計室内への持込み及び設計室内での使用だけであった。

・L 氏は，A 社から漏えいした可能性があるとして，A 社に調査を求めてきた。

E部長は事態を重くみて，ファイルSの漏えいについての調査，及び必要であればその対処，並びにA社全体としての情報セキュリティ対策強化案の検討をシステム係のFさんに指示した。さらに，A社の情報システムの導入及び運用を支援しているシステム会社と一緒に調査することにし，システム会社のG氏が協力することになった。

Fさん及びG氏は，まず，情報漏えいの調査及び一時的な対処を実施し，その後に，A社全体としての情報セキュリティ対策強化案を検討することにした。

〔情報漏えいの調査及び一時的な対処〕

FさんはG氏の協力を受けて，FW，DMZ上のサーバ及び内部システムLAN上のサーバの調査を開始した。FさんとG氏は，設計情報管理サーバからファイルSが取り出された可能性が高いと考え，設計情報管理サーバのアクセスログを調査した。その結果，ファイルSを作成するためにJさんが設計情報管理サーバに登録した利用者ID kyoudou@a-sha.co.jp（以下，ID-Kという）による不審なアクセスが6月1日に発生していたことが判明した。設計情報管理サーバの6月1日のアクセスログのうち，利用者IDがID-Kのものを表6に示す。

表6　設計情報管理サーバのアクセスログ

項番	接続元IPアドレス	日時	利用者ID	ログ項目
1	192.168.19.8	6/1 11:40:30	kyoudou@a-sha.co.jp	ログイン成功
2	192.168.19.8	6/1 11:41:40	kyoudou@a-sha.co.jp	kyoudousyuppin.zipをアップロード
3	192.168.19.8	6/1 11:42:50	kyoudou@a-sha.co.jp	ログアウト
4	192.168.64.3	6/1 16:50:00	kyoudou@a-sha.co.jp	ログイン失敗
5	192.168.64.3	6/1 16:50:05	kyoudou@a-sha.co.jp	ログイン失敗
6	192.168.64.3	6/1 16:50:09	kyoudou@a-sha.co.jp	ログイン失敗
7	192.168.64.3	6/1 16:50:13	kyoudou@a-sha.co.jp	ログイン成功
8	192.168.64.3	6/1 16:50:20	kyoudou@a-sha.co.jp	ファイルの一覧表示
9	192.168.64.3	6/1 16:51:30	kyoudou@a-sha.co.jp	kyoudousyuppin.zipをダウンロード

Fさんが，ID-KについてJさんに確認したところ，ID-Kは，共同出品金型の設計に携わっているJさん及び2名の設計部員（以下，3名を併せて，共同出品担当メンバという）が利用していた。

さらに，表6の接続元IPアドレスに記録されたDPCを特定するために，DHCPサーバのログを調査することにした。DHCPサーバの6月1日のIPアドレス割当ログのうち，割り当てたIPアドレスが192.168.19.8又は192.168.64.3であるものを表7に示す。

表7　DHCPサーバのIPアドレス割当ログ

項番	対象DPC	日時	ログ項目
1	Jさんの DPC	6/1 08:30:00	IPアドレス192.168.19.8を割り当てた。
2	営業係Kさんの DPC	6/1 11:30:00	IPアドレス192.168.64.3を割り当てた。
3	Jさんの DPC	6/1 11:50:30	IPアドレス192.168.19.8を解放した。
4	営業係Kさんの DPC	6/1 17:30:20	IPアドレス192.168.64.3を解放した。

Fさんは，②サーバのログの調査だけでは操作者を特定するには不十分なので，当事者へのヒアリング及び DPC の動作ログの調査が必要であると判断した。ヒアリング及び調査の結果を図2に示す。

(1) 共同出品担当メンバへのヒアリング及び調査の結果

・6月1日の行動

08:30 3人とも，出勤し，DPCを起動した。

08:35 共同出品金型の設計をJさんが始めた。

11:40 設計を終え，設計情報管理サーバにID-Kでログインし，ファイルSをアップロードした。アップロード後，ログアウトした。

11:45 ファイルSをDVDSに保存した。

11:50 3人とも，DPCをシャットダウンした。

13:00 B社との打合せ及びDVDSの手渡しのために，3人でB社に向かった。

13:30 3人とも，B社に到着し，L氏にDVDSを手渡し，打合せを始めた。

17:30 3人とも，打合せを終え，B社から直接帰宅した。

・6月4日の行動

3人とも，社外の研修に終日参加していた。

(2) Kさんへのヒアリング及び調査の結果

・6月1日の行動

11:30 外出先から戻り，DPCを起動した。

11:35 取引先向け資料の作成を始めた。

16:30 取引先向け資料に関する打合せを上司と始めた。

17:30 上司との打合せを終えて，DPCをシャットダウンした。

18:00 帰宅のため会社を出た。

・6月4日の行動

08:30 出勤し，DPCを起動した。

08:35 提案資料の作成を始めた。

17:25 提案資料を保存し，DPCをシャットダウンした。

17:30 帰宅のため会社を出た。

・設計情報管理サーバへのアクセス

Kさんには設計情報管理サーバの利用者IDの割当てはなく，アクセスできない。

図2 ヒアリング及び調査の結果

ヒアリング及び調査の結果，Fさんは，③表6の項番4から項番9のアクセスは，共同出品担当メンバの操作ではなく，Kさんの DPC がマルウェアに感染し，マルウェアによってファイルSが漏えいした可能性があると判断した。Fさんは，E部長に報告するとともに，調査のために，KさんのDPCを回収し，予備のDPCをKさんに貸与した。

さらに，ID-Kは不正ログインに使用されたので，Fさんは，Jさんに，④ID-Kへの一時的な対処を依頼した。

Fさんは，G氏のアドバイスを受けながら，JさんとKさんへの追加のヒアリング及び調査を行った。それらの結果を図3に示す。

(1) Jさんへの追加ヒアリング結果
・4月に，共同出品金型用の同報用メールアドレス kyoudou@a-sha.co.jp を登録してもらった。同報先には，共同出品担当メンバを登録してもらった。
・kyoudou@a-sha.co.jp は，共同出品関係者とのメールのやり取りにおいて Cc の宛先としている。社外のメーリングリスト宛てにメールを送信した時に，kyoudou@a-sha.co.jp を Cc に指定したこともある。
・Jさんがファイル S を作成するために，4月に ID-K を設計情報管理サーバに登録した。
・ID-K のパスワードは，初期パスワードのまま変更していなかった。
(2) Kさんへの追加ヒアリング結果
・5月21日9時，DPC からメールサービスにアクセスした。
・送信者が運送会社のメールアドレスになっており，かつ，ZIP 形式のファイルが添付されたメールが届いた。
・添付ファイルを DPC にダウンロードし，保存した。
・保存した添付ファイルを展開したところ，PDF ファイルがあり，ファイル名が“送付状”であったので開いた。身に覚えがない内容だったので，PDF ファイルを削除した。
・6月5日9時，上記添付ファイルを誤って再び展開したところ，リアルタイムスキャンによって，PDF ファイルがマルウェア X として検知され，PDF ファイルを削除したとのメッセージが DPC に表示された。直ちに，PC 上の上記添付ファイルを削除した。マルウェアの対処は完了したものと判断した。
・6月5日13時，フルスキャンによって別のファイルがマルウェア Y として検知され，削除された。
(3) マルウェア X に関する情報
・ダウンローダ型のマルウェアであり，攻撃者が用意した C&C（Command and Control）サーバの URL が内部に保持されている。C&C サーバからマルウェア Y をダウンロードし実行する。
・PDF 閲覧ソフトの脆弱性を悪用して PC に感染する。5月16日にリリースされた PDF 閲覧ソフトの脆弱性修正プログラムが適用されていれば，マルウェア Y をダウンロードしない。
(4) マルウェア Y に関する情報
・PC の hosts ファイルを用いて，Web サーバを探索する。
・Web サーバが見つかると，C&C サーバから取得した利用者 ID とパスワードのリストを用いてログインを試みる。ログインが成功すると，クローリングしてファイルを一つずつダウンロードし，攻撃者が用意したサーバにアップロードする。
(5) マルウェア対策ソフトベンダの対応
・5月28日10時，マルウェア X に対応したマルウェア定義ファイルをリリースした。
・6月5日10時，マルウェア Y に対応したマルウェア定義ファイルをリリースした。
(6) フルスキャン実施
・6月8日10時，F さんは，マルウェア対策ソフトで圧縮ファイルをフルスキャンの対象とするように一時的に設定を変更した後，最新のマルウェア定義ファイルに更新し，フルスキャンを行うように全ての従業員に指示した。このフルスキャン実施では，マルウェアは検知されなかった。
(7) 他のサーバの調査
・製造情報管理サーバのログを調査したところ，不審なログインの記録はなかった。

図3 追加のヒアリング及び調査の結果

G氏は，図3の(2)について，マルウェア対策ソフトでマルウェアが検知されたにも

かかわらず，報告がなかったので，A 社としての対策がとれなかったことへの改善が必要であると指摘した。F さんは，図 3 及び G 氏の指摘を踏まえ，（あ）～（え）の作業計画を作成した。

（あ）設計部長に報告するために，情報漏えいの経緯をまとめる。

（い）類似のマルウェア感染を防止する対策を検討する。

（う）設計情報管理サーバへの不正ログイン対策を検討する。

（え）サーバ及び DPC それぞれの，マルウェア対策ソフトの状態と脆弱性修正プログラムの適用状況を集中管理する仕組みを導入する。

F さんは，（あ）～（え）の作業計画を E 部長に報告し，実施についての了承を得た。

（あ）について，F さんは，情報漏えいの経緯をまとめ，E 部長が設計部長に報告した。

（い）について，F さんは，類似のマルウェア感染を防止する対策として，今回の感染の経緯と類似のマルウェアへの注意点を社内に周知した。

さらに，圧縮ファイル中のマルウェアが検知されなかったことについて，F さんは，平常時も圧縮ファイルをフルスキャンの対象とすべきかを G 氏に相談した。G 氏は，平常時の運用では，圧縮ファイルをフルスキャンの対象にしなくても DPC がマルウェアに感染するリスクは変わらないと答え，⑤その理由を F さんに説明した。F さんは，圧縮ファイルをフルスキャンの対象外とするという設定は変えないことにした。

〔設計情報管理サーバへの不正ログイン対策の検討〕

（う）について，F さんは，設計情報管理サーバへの不正なログインの経緯及び設計情報管理サーバの利用状況を踏まえ，⑥設計情報管理サーバへのアクセスを制限する設定変更案及び⑦パスワードに関する運用方法の見直し案を作成し，J さんに提案した。J さんは，F さんの提案どおりに設定の変更及び運用方法の見直しを実施することにした。

さらに，F さんと G 氏は，ID-K のように利用者 ID を共用する限り，パスワードの管理は不十分になると考えた。そこで，利用者 ID の共用は全て禁止し，フォルダへのアクセス権限を利用者 ID ごとに設定する案を作成した。

Fさんは，検討結果をE部長に説明し，了承を得てJさんに実施を依頼した。

〔集中管理の仕組みの導入〕

（え）について，Fさんは，次の機能を備えた集中管理サーバの導入案を作成した。

・マルウェア定義ファイルを配信し，配信状況を管理する機能

・マルウェアの検知を［ j ］する機能

・脆弱性修正プログラムを配信し，配信状況を管理する機能

Fさんは集中管理サーバの導入案を，E部長に説明した。E部長は，役員会で集中管理サーバの導入を提案し，集中管理サーバの導入費用が次年度の設備導入予算に組み込まれることになった。E部長は，一連の対処及び施策を設計部長に報告した。

設問1　表1中の［ a ］～［ c ］に入れる適切な字句をそれぞれ5字以内で答えよ。

設問2　〔A社のネットワーク構成〕について，(1)，(2)に答えよ。

(1)　表2中の［ d ］に入れる適切な字句を10字以内で答えよ。

(2)　表2中の下線①について，接続を許可するネットワークアドレスを答えよ。

設問3　〔A社の情報システム〕について，(1)～(4)に答えよ。

(1)　表4中の［ e ］に入れる適切なIPアドレスを答えよ。

(2)　表4及び本文中の［ f ］に入れる適切なプロトコル名を英字5字以内で答えよ。

(3)　本文中の［ 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　AES　　イ　DES　　ウ　HMAC　　エ　MD5　　オ　ZipCrypto

(4)　本文中の［ h ］に入れる適切な字句を英字10字以内で答えよ。

設問4　本文中の［ i ］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　サイズ　　イ　作成者の利用者ID　　ウ　作成日時　　エ　ハッシュ値

設問５　〔情報漏えいの調査及び一時的な対処〕について，(1)～(5)に答えよ。

(1)　本文中の下線②について，不十分な理由を 55 字以内で述べよ。

(2)　本文中の下線③のように判断した根拠を 50 字以内で具体的に述べよ。

(3)　本文中の下線④について，一時的な対処を 15 字以内で答えよ。

(4)　図 3 中の(6)について，フルスキャンを実施した目的は何か。40 字以内で述べよ。

(5)　本文中の下線⑤について，理由を 50 字以内で述べよ。

設問６　〔設計情報管理サーバへの不正ログイン対策の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑥について，設定変更の内容を 50 字以内で具体的に述べよ。

(2)　本文中の下線⑦について，見直し後の運用方法を 40 字以内で具体的に述べよ。

設問７　本文中の［　j　］に入れる適切な字句を 10 字以内で答えよ。