問2　社内認証システムの統合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 700 名の業務用ソフトウェアパッケージの開発販売会社である。都心に本社を構える A 社は，営業部，人事部，経理部，総務部，情報システム部，製品サポート部，製品開発部及び研究部から構成されている。

A 社は，長らくソフトウェアパッケージの販売を事業の中心としてきたが，最近刷新された経営陣の決定によって，SaaS（Software as a Service）型のインターネットサービスの提供及び関連 SI 事業（以下，SaaS 型サービス事業という）を立ち上げる計画を開始した。

〔A 社の情報システム〕

A 社における社内向けの情報システムは，表に示すように分類される。このうち，社内の情報技術基盤となる情報システム群（以下，インフラ系という）及び基幹業務に関する情報システム群（以下，基幹業務系という）は，情報システム部の所管である。インフラ系には，Web アプリケーション（以下，Web アプリという）向けに A 社が独自に開発したシングルサインオン（以下，A-SSO という）システムが含まれている。他方，製品サポート部，製品開発部及び研究部が，部署ごとに導入して運用管理をしている情報システム群（以下，部署運用系という）があり，それらの一部は，認証に A-SSO システムを採用している Web アプリ（以下，A-Web アプリという）である。

表　A 社における社内向けの情報システムの分類

分類	所管部門	含まれるシステム名	備考
インフラ系	情報システム部	プロキシ，電子メール，A-SSO，NTP（Network Time Protocol）など	・インフラ系のサーバマシン群のベンダサポートは 2012 年末に終了する(1)。 ・電子メールは UNIX OS 上で稼働
基幹業務系	情報システム部	財務会計，勤怠管理，人事管理，施設予約，経費精算など	勤怠管理と施設予約は A-SSO システムで認証
部署運用系	製品サポート部	顧客管理，製品管理など	顧客管理と製品管理は A-SSO システムで認証
	製品開発部	グループウェア，e ラーニングなど	グループウェアと e ラーニングは A-SSO システムで認証
	研究部	研究サーバ，ナレッジベースなど	・研究サーバは UNIX OS 上で稼働 ・ナレッジベースは A-SSO システムで認証

注(1)　A 社では，ベンダのサポートが終了する前に，情報システムをリプレースすることになっている。

〔認証統合プロジェクトの発足〕

A 社では，社内に A-SSO システムを含む複数の認証システムが混在しており，システム監査において，図 1 に示す課題が指摘されていた。ここで，認証システムとは，アカウント情報の管理，利用者の認証及びアクセス許可を行うシステムのことをいう。

(1) 情報システム全体では 3 種類の利用者 ID が使用されており，使い分けが面倒との利用者の声が多くある。
(2) 情報システムごとにパスワードルールが異なるので，同じレベルのパスワードの強度が確保されていない。
(3) 認証システムを管理する部署が複数に分かれているので，アカウントの運用及び認証システムの運用管理に関しても，同じレベルのセキュリティが確保されていない。
(4) アカウント情報を管理するディレクトリ間の反映が一部手動で行われており，過去，アカウント情報を誤って削除するなどのトラブルが発生した。これに対する防止対策が必要である。
(5) 緊急に対処すべき課題とまでは言えないが，セキュリティ管理の現状を踏まえると，A-SSOシステムには脆(ぜい)弱性がある。

図 1　A 社の認証システムに関して指摘されていた課題

そこで，認証システムを統合することになり，情報システム部を中心とした社内プロジェクトチーム（以下，S チームという）が発足した。また，経営陣から，当該プロジェクトは，SaaS 型サービス事業に活用できる成果を出すようにという指示があった。この指示を考慮し，プロジェクトの開始に先立ち，認証システムの統合の基本方針を図 2 にまとめた。

(1) アカウント情報の一元化によって，認証の利便性を向上させる。
(2) 認証システムの運用コストを削減する。
(3) 新たに導入する認証システムは，将来にわたって継続的に利用できるものにする。
(4) 情報システムのセキュリティを向上させる。
(5) 認証システム自体のセキュリティを向上させる。
(6) 各部署が独自に情報システムを導入し，運用管理も独自に実施する方針を継続する。
(7) 上記(1)～(6)を妨げない程度で，SaaS 型サービス事業で用いる新技術を積極的に取り入れる。

図 2　A 社の認証システムの統合の基本方針

〔認証システムの洗い出し〕

S チームは，A 社で利用している認証システムについて精査する必要があると判断し，まず，他社製の認証システムに関して，仕様を詳しく調査することにした。

A 社は，PC 端末，ファイルサーバ及び一部の Web アプリにおける認証の仕組み，並びにディレクトリとして，C 社製ディレクトリシステム（以下，C-DIR という）を，導入している。C-DIR では，利用者，PC 端末，プリンタ及びサーバから構成されるド

メインという管理単位を定め，ドメインコントローラ（以下，DC という）によって管理する。また，DC では，C-DIR のディレクトリに保持されるアカウント情報を用いて認証を行う。認証には，C 社独自仕様のチャレンジレスポンス認証（以下，C-CR 認証という），又は Kerberos 認証を利用することが可能である。

C-CR 認証では，図 3 に示すプロトコルの (b)-1～(b)-4 において，①DC が生成した疑似乱数をチャレンジとし，それを受信したクライアントで，利用者 ID，パスワード及びチャレンジの連結をハッシュ化したレスポンスを DC に返信し，アクセス許可を受ける。

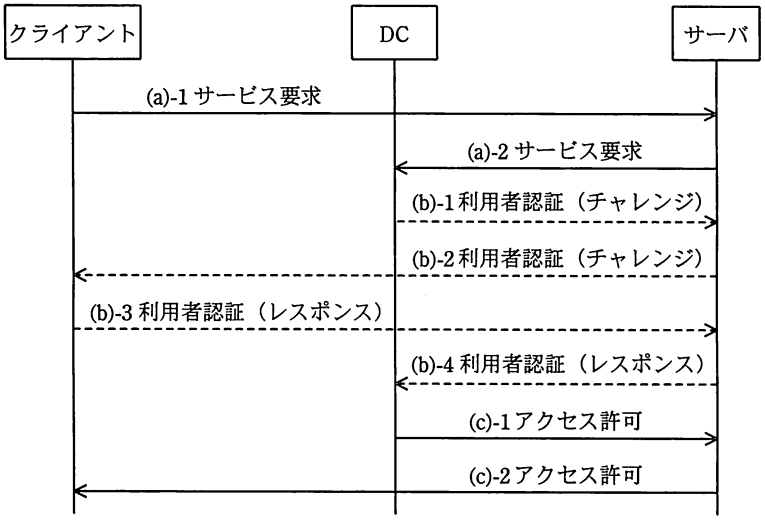


図 3　C-CR 認証のプロトコル

他方，Kerberos 認証では，図 4 に示すように，クライアントが，DC における認証後，有効期限付のチケットが発行され，それをサーバに提示し，アクセス許可を受ける。

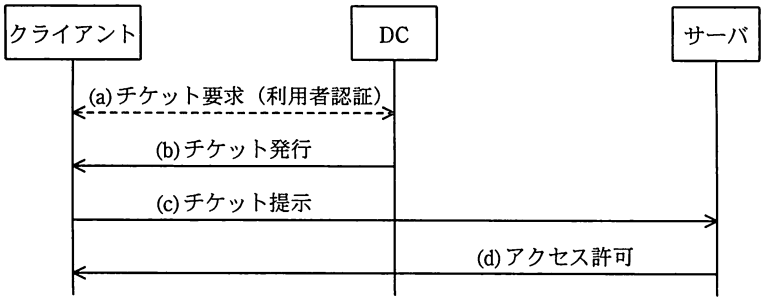


図 4　Kerberos 認証のプロトコル

C-CR 認証の場合，クライアントはサーバへの接続のたびに DC において認証を行う必要があるが，Kerberos 認証の場合，有効期限内であればチケットをサーバに提示するだけでサービスを受けられる。A 社では，トラフィックが少なくなるなどのメリットが多い Kerberos 認証だけを利用している。また，Kerberos 認証において，②有効期限切れのチケットが悪用されないように，DC とサーバを [a] させて運用している。

研究サーバ用及び電子メール用のサーバマシンでは，UNIX OS が稼働しており，利用者認証のために，NIS（Network Information Service）が導入されている。ここで，NIS とは，NIS ドメインと呼ばれる管理単位において，UNIX OS が稼働するマシン間で，利用者のアカウント情報を共有するための仕組みである。

社外から社内 LAN へのアクセスのための SSL-VPN での認証，及び社内の無線 LAN での認証には，RADIUS が使用されている。ここで，RADIUS とは，サーバにおいて，利用者の認証及びアカウンティングを実現するための仕組みである。

以上の認証システム以外に，LDAP を用いて，パスワード認証を行う情報システムがある。

〔A-SSO システムの仕様の確認〕

S チームは，次に，A 社が独自に開発した A-SSO システムの仕様を確認した。

A-SSO システムは，A-SSO サーバ及び A-SSO 用のディレクトリで構成される。A-SSO サーバは，A-Web アプリの利用者を認証するために，A-SSO 用のディレクトリに保持されるアカウント情報を用いる。認証には，図 5 に示すプロトコルを利用する。

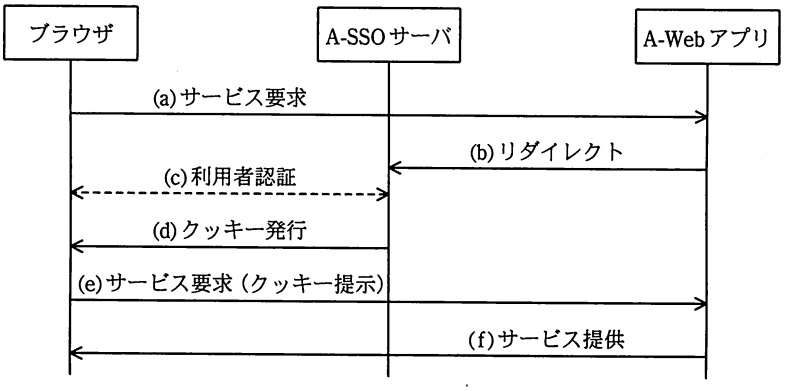


図 5　A-SSO システムのプロトコル

次は，A-SSO システムのプロトコルの動作概要である。

(a) 利用者のブラウザは，A-Web アプリにサービスを要求する際，A-SSO 用のクッキーがあれば，それを A-Web アプリに提示する。その場合には (f) に進む。

(b) A-Web アプリは，サービス要求を A-SSO サーバにリダイレクトする。

(c) 利用者は，利用者 ID とパスワードを入力し，認証を受ける。

(d) A-SSO サーバは，認証が成功すれば A-SSO 用のクッキーを発行する。

(e) ブラウザは，クッキーを A-Web アプリに提示し，サービスを要求する。

(f) A-Web アプリは，クッキーを検証し，有効ならば，サービスを提供する。

ここで，A-SSO 用のクッキーには，セッション ID やクッキーの発行日時などが設定されており，トリプル DES を用いて暗号化されている。また，すべての A-Web アプリには，クッキーを復号するために暗号化鍵を配布している。ブラウザは，一度，クッキーの発行を受けると，有効期間内であれば，(b)〜(e) の手続なしに，すべての A-Web アプリにアクセスできる。

〔A 社のアカウント情報の反映のフロー〕

A 社で利用している認証システムの仕様の確認後，S チームは，アカウント情報の反映のフローを確認した。

図 6 は，認証システム間で，アカウント情報をどのように反映しているかのフローを示している。まず，人事マスタデータベース（以下，人事マスタという）から CSV 形式のファイル（以下，人事マスタファイルという）を手動で，適時，出力しておく。アカウント作成の際，人事マスタファイルを基に，利用者 ID，パスワードなどのアカウント情報を，アカウント情報を管理する LDAP サーバのデータベース（以下，LDAP マスタという）に追加する。併せて，C-DIR のディレクトリにも追加する。さらに，LDAP マスタから，LDAP 1 には即時に，LDAP 2 には日次で，データ転送される。ここで，LDAP 1 は A-SSO サーバから参照され，LDAP 2 はそれ以外の LDAP を利用する認証システムから参照される。NIS と RADIUS のアカウント情報については，利用者からの申請後，手入力で NIS に追加する。その後，RADIUS に，即時，データ転送される。

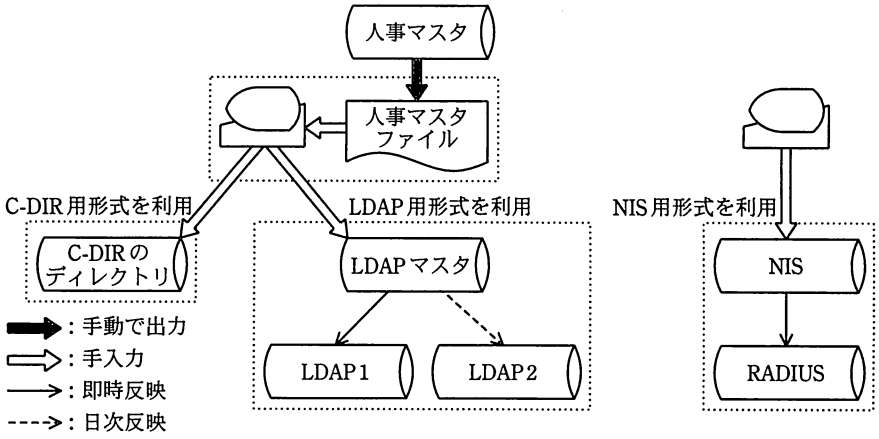


図6　アカウント情報の反映のフロー

A 社では，アカウント情報に関して，C-DIR 用，LDAP 用及び NIS 用の 3 種類のデータ形式を用いている。LDAP のアカウント情報では，inetOrgPerson といったオブジェクトクラスによって組織の利用者の情報を管理する標準的な [b] を用いている。例えば，製品開発部のスズキタロウ氏が社内で利用する LDAP 用のアカウント情報を [c] によってテキスト形式で示すと，図 7 となる。

```
dn: uid=suzuki, ou=seihin-kaihatsu, dc=a-company, dc=com
cn: Taro Suzuki
sn: Suzuki
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
ou: 製品開発部
telephonenumber: 03-xxxx-5555
```

図7　LDAP におけるスズキタロウ氏のアカウント情報（抜粋）

〔統合認証システムの基本設計〕

社内の認証システムの仕様を洗い出した後，S チームでは，図 8 に示すとおり，新たに導入する認証システム（以下，統合認証システムという）の基本設計を行った。

アカウント情報は，エントリの属性を定義する [b] を拡張して，A 社で必要とする利用者 ID，パスワード，所属，電話番号などの属性を管理できるようにした。また，統合認証システムではアカウント情報を一元的に管理することとした。

アカウント情報のシステム間の反映に関しては，人事マスタから ID 管理サーバ（以下，IDM という）にアカウント情報を日次で反映し，IDM のディレクトリ（以下，

IDM マスタという）で保持し，変換後，IDM から C-DIR のディレクトリ及び LDAP にアカウント情報を即時反映する方式を採用した。LDAP は，シングルサインオンシステム及び RADIUS での認証に利用される。NIS は DC と連携することができる。

利用者がパスワードを変更したい場合は，IDM の Web インタフェースを通して，利用者が自ら変更することが可能で，C-DIR 又は LDAP サーバなどに，即時反映される仕組みとした。

A-SSO システムには，図 1 の (5) の指摘があることに加え，③A-SSO 用のクッキーの利用が原因となり，A-SSO サーバと A-Web アプリが同じインターネットドメイン上にないとシングルサインオンを実現できないという技術的課題があった。社内ドメインだけでの運用では問題はないが，SaaS 型サービス事業を展開する上で，事業形態の制約となるので，製品開発部と研究部との検討の結果，統合認証システムでは，SAML（Security Assertion Markup Language）に準拠したシングルサインオン（以下，SAML 型 SSO という）システムを採用することにした。

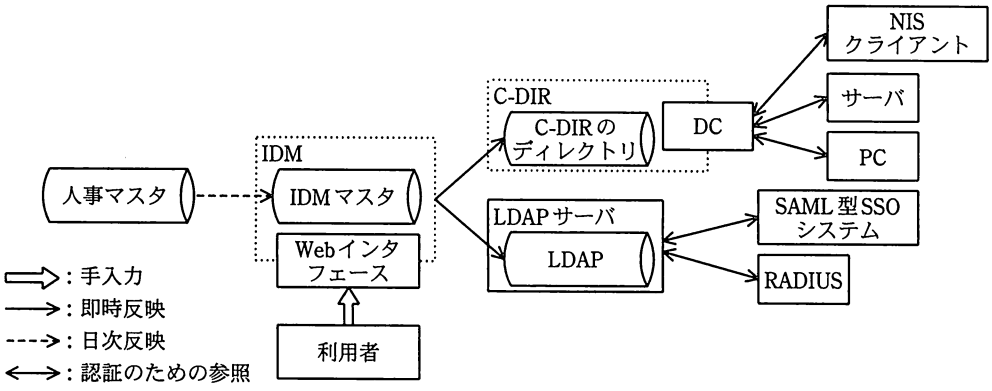


図 8　統合認証システムの基本設計概念

SAML とは，記述言語として [d] を用いて，認証及び [e] に関する情報を交換するための標準規格である。今回，A 社で採用した SAML 型 SSO システムにおける認証及び [e] を実現するプロトコルは，図 9 のとおりである。Web アプリ上には，SP（サービスプロバイダ）と呼ばれるモジュールが稼働しており，IdP（Id プロバイダ）と呼ばれる Web アプリと連携して，利用者認証を行う。IdP においては，様々な認証方式を採用できるが，A 社では，入力フォームを活用した，利用者 ID とパスワードを用いる方式を採用し，図 8 の統合認証システムにおける LDAP サーバと連携させることにした。

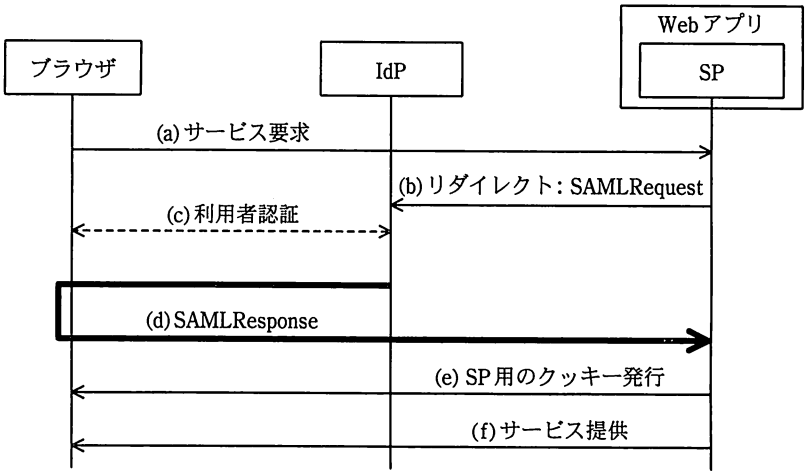


図9　SAML型SSOシステムのプロトコル

次は，A社で採用したSAML型SSOシステムのプロトコルの動作概要である。ここで，各主体は，ほかの主体の公開鍵証明書を保持しているとする。

(a) 利用者のブラウザは，Webアプリにサービスを要求する際，SP用のクッキーがあれば，それを提示する。提示したクッキーが有効であることが検証された場合は(f)に進む。

(b) SPは，SAMLRequestメッセージをエンコーディングした上でURIに含め，サービス要求をIdPにリダイレクトする。

(c) 利用者は，利用者IDとパスワードを入力し，認証を受ける。

(d) IdPは，利用者IDなどの属性を暗号化及びディジタル署名したSAMLResponseメッセージを発行し，ブラウザ上のJavaScriptを用いて，それをSPに転送する。

(e) SPは，SAMLResponseメッセージのディジタル署名などを検証し，有効であれば，SP用のクッキーを発行する。

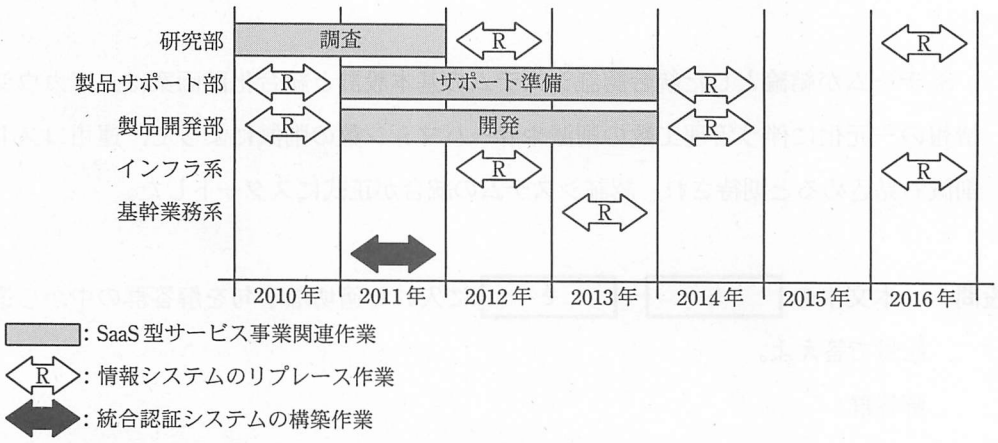
(f) SPが稼働するWebアプリは，該当するサービスを提供する。

Sチームは，SaaS型サービス事業への展開を視野に入れ，SAML型SSOを複数のIdPでも適用できるように設計した。SAML型SSOシステムの導入によってA-SSOシステムの課題に対処できるので，SAML非対応の既存のWebアプリを，情報システムのリプレース時に，SAMLに対応するように改修を行うことにした。将来的には，全社でSAML型SSOシステムを採用することにし，統合認証システムの導入後，適切なタイミングでA-SSOシステムを廃止することを決定した。

SaaS 型サービス事業への展開としては，A 社のソフトウェアパッケージを SP と連携するように改修し，Web アプリとして A 社のデータセンタに配備し，サービスを提供する予定である。このサービスを導入する企業は，自社のイントラネットに IdP を用意すれば，導入する企業のイントラネットにある PC 端末からインターネット経由で，A 社のデータセンタに配備された SaaS 型サービス事業の Web アプリを利用することが可能となる。導入する企業は，Web アプリの運用を A 社に委託できるので，自社内での運用に比べてコストの削減が期待できる一方で，④A 社にとっても，IdP を顧客のイントラネットに構築することは運用管理上のメリットがある。

〔移行計画の策定と実施〕

基本設計に続き，S チームは，図 10 のとおり，情報システムのリプレース及び認証システムの統合化計画案を策定した。



注　矢印は，左端が作業を開始する時期で，右端が本稼働の開始時期を示す。

図 10　情報システムのリプレース及び認証システムの統合化計画案

A 社は，情報システムをリース契約で導入しており，4 年ごとにリプレースを実施している。2012 年にはインフラ系のリプレースが予定されており，2013 年には基幹業務系のリプレースが予定されている。いずれの作業も，情報システム部が行う。他方，部署運用系のリプレース作業については，所管部門がそれぞれ行うことになっており，現在，製品サポート部及び製品開発部所管の情報システムのリプレース作業を行っている。また，2012 年に，研究部所管の情報システムのリプレースを実施する予定である。

なお，A 社では，ハードウェアの故障などのトラブルの発生が増えるのを避けるため，リース契約の延長は行わない。

図 10 の計画案の策定では，このような前提の下，認証システムの統合のスケジュールを検討し，次の 3 点を決定した。

・SaaS 型サービス事業は最優先であり，さらに，引き続きソフトウェアパッケージの開発及びサポート業務もあるので，製品サポート部，製品開発部及び研究部所管の情報システムのリプレースの時期は変更しない。

・統合認証システムの構築作業を 2011 年に実施する。

・A-SSO システムのリプレースは，インフラ系のほかの情報システム群のリプレースとともに予定どおり行う。A-SSO システムの廃止が可能になるのは，早くても，[f] 年の末である。それまでは，継続利用しようと考えたが，[g] という理由から，次回のインフラ系のリプレース時に，A-SSO システムも，ほかのインフラ系の情報システム群と併せてリプレースしておく必要があると判断した。

S チームが結論とした統合認証システムの基本設計と統合化計画案は，アカウント情報の一元化に伴う管理工数の削減やサーバマシン数の削減によって，運用コストの削減も見込めると期待され，認証システムの統合が正式にスタートした。

設問 1　本文中の [b] ～ [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　ELF　　イ　LDIF　　ウ　XML　　エ　構成管理

オ　スキーマ　　カ　認可　　キ　パスワード

ク　パスワードファイル

設問 2　C-DIR で用いられている認証について，(1)，(2)に答えよ。

(1)　本文中の下線①の疑似乱数の生成方法に問題があり，同じ乱数が生成される場合，どのような脅威が考えられるか。攻撃の手順とともに，50 字以内で具体的に述べよ。

(2)　本文中の下線②を実現するために，[a] に入れる適切な字句を 10 字以内で答えよ。

設問3　シングルサインオンシステムについて，(1)，(2)に答えよ。

(1)　図1中の(5)の脆弱性とは何か。セキュリティ管理の現状とA-SSOシステムの仕様から判断して，45字以内で述べよ。

(2)　本文中の下線③の技術的課題に，SAML型SSOシステムではどのように対処しているか。図9中の字句を用いて，70字以内で具体的に述べよ。

設問4　統合認証システムについて，(1)，(2)に答えよ。

(1)　統合認証システムにおいて，図1中の(2)の指摘にどのように対処しているか。60字以内で述べよ。

(2)　本文中の下線④にあるA社にとっての運用管理上のメリットとは何か。SAML型SSOシステムの特徴に基づいて60字以内で述べよ。

設問5　移行計画について，(1)，(2)に答えよ。ここで，リプレースされた情報システムは，本稼働後から利用可能とする。

(1)　本文中の［　f　］に入れる適切な年を答えよ。また，Sチームがそのように判断する理由を40字以内で具体的に述べよ。

(2)　本文中の［　g　］に入れる適切な理由を45字以内で具体的に述べよ。