SC

平成26年度　秋期
情報セキュリティスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を○印で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　利用者 ID 管理システム及び認証システムの設計に関する次の記述を読んで，設問 1～6 に答えよ。

N 社は，従業員数 20,000 名の大手金融機関である。N 社はこれまで，日本の顧客企業の海外展開に合わせて海外にも支店を設け，顧客企業の現地法人及びその従業員向けの金融サービスを提供することによって，海外での取引を急速に拡大させてきた。N 社は現在，日本，欧米，アジアという地域ごとに業務を行っており，システムも地域ごとに構築している。N 社の正社員の人事管理も地域ごとに人事システムで行っているが，契約社員は，支店ごとに契約社員を管理する者（以下，管理者という）が人事システムを使わずに管理している。

N 社は，より広い範囲の顧客企業及び個人顧客に世界共通の金融サービスを提供するための第一歩として，各地域の情報系システム（以下，社内システムという）のうち，機能面で共通性の高いものを，全地域から利用できる共通のシステム（以下，G システムという）として一本化し，各地域の社内システムの利用者全員に，G システムと，利用者が所属する地域の社内システムを併用させることにした。また，地域によって異なっている利用者 ID（以下，ID という）管理及び利用者認証の方式と運用を統一し，セキュリティ管理の一元化及び効率向上を実現することにした。N 社の各地域における利用者認証方式の概要を表 1 に示す。

表 1　N 社の各地域における利用者認証方式の概要

種別＼地域	日本	欧米地域	アジア地域
PC における利用者認証	IC カードによる利用者認証（ディレクトリサーバ製品 Q を利用）	ID，パスワードによる利用者認証（ディレクトリサーバ製品 Q を利用）	
社内システムにおける利用者認証	エージェント型の認証サーバを開発して利用	リバースプロキシ型の認証サーバ製品 P を利用	
PC と社内システムにおけるシングルサインオン	SPNEGO プロトコル[1] によって実現		実現されていない

注[1]　RFC 4178 The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism

〔日本における ID 管理・認証の方式〕

日本の N 社では，利用者が日本の PC（以下，日本 PC という）に接続された IC カードリーダに IC カードを差し込むと，IC カードから ID とディジタル証明書（以下，証明書という）が読み取られ，ディレクトリサーバ製品 Q を用いた日本のディレクト

リサーバ（以下，ディレクトリサーバを DS という）において利用者認証が行われる。日本の DS（以下，日本 DS という）は，PC における利用者認証が成功すると，日本 PC に当該利用者のチケット認可チケット（以下，TGT という）を発行する。日本 PC は N 社が一括調達したものであり，IC カードリーダは，日本 PC 専用に開発されたものである。

利用者が日本 PC のブラウザを起動すると，ブラウザは，ホームページとして設定された日本の認証サーバ（以下，日本認証サーバという）にアクセスする。日本認証サーバは，認証していないブラウザからの HTTP 要求に対して，HTTP ステータスコード 401，Negotiate の値をもつ WWW-Authenticate ヘッダ，並びに ID 及びパスワードの入力画面を含む HTTP 応答を返す。そうすると，ブラウザは，日本認証サーバのアクセスに必要なサービスチケット（以下，ST という）の提示，又はフォーム認証による ID とパスワードの入力のどちらかを行う。日本 PC のブラウザは，SPNEGO によるシングルサインオン（以下，SSO という）を利用する設定が行われており，前述の HTTP 応答を受信すると，日本 DS に TGT を提示して ST を受け取り，その ST を日本認証サーバに提示して日本の社内システム（以下，日本社内システムという）における利用者認証が成功する。ST には暗号化された ID が含まれており，ST を受け取ったサーバは，復号処理によって ID を得ることができる。

日本認証サーバは，利用者認証が成功すると，認証 Cookie を発行し，認証成功を示すメッセージと日本のポータルサーバ（以下，日本ポータルという）へのリンクをブラウザに表示する。利用者がそのリンクをクリックすると，日本ポータルは，認証 Cookie の検証を行う。検証が成功すると，当該利用者がアクセス可能な日本社内システムへのリンクが並んだポータル画面をブラウザに表示する。

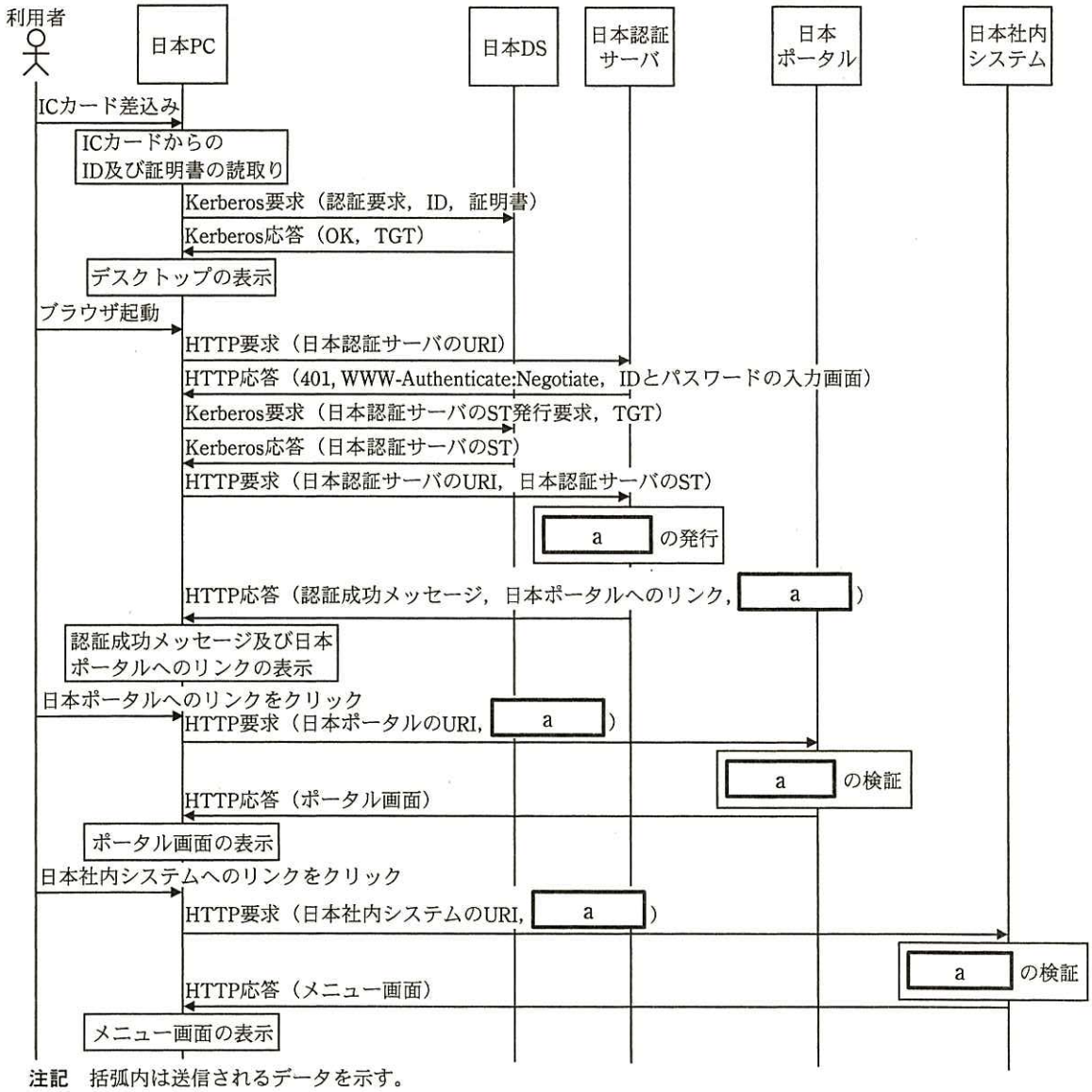
利用者が日本社内システムにアクセスすると，日本社内システムは，認証 Cookie の検証を行った後，メニュー画面をブラウザに表示する。日本ポータル及び日本社内システムでの認証 Cookie の検証では，日本認証サーバと併せて開発された，エージェントと呼ばれる Java プログラムがアプリケーションプログラムからメソッドとして呼び出される。

正社員が入社すると，人事管理手続に基づき，正社員情報の確認と登録の承認が行われた後，人事システムに登録される。人事システムに新しい正社員情報が登録されると，情報システム部は，当該正社員の証明書を発行し，ID と証明書を日本 DS に登録し，ID と証明書を格納した IC カードを当該正社員に貸与する。

契約社員が日本社内システムにアクセスする必要がある場合，管理者が所属長に対して当該契約社員のシステム利用申請を行い，承認を得る。その後，日本の情報システム部は，当該契約社員の証明書を発行し，ID と証明書を日本 DS に登録し，ID と証明書を格納した IC カードを管理者経由で当該契約社員に貸与する。

ID の先頭 2 桁は，正社員では AA，契約社員では本店・支店の識別番号であり，後続 6 桁は，正社員では社員番号，契約社員では管理者が採番した番号である。

日本における利用者認証の通信シーケンスを図 1 に示す。



注記　括弧内は送信されるデータを示す。

図 1　日本における利用者認証の通信シーケンス（概要）

〔欧米地域におけるID管理・認証の方式〕

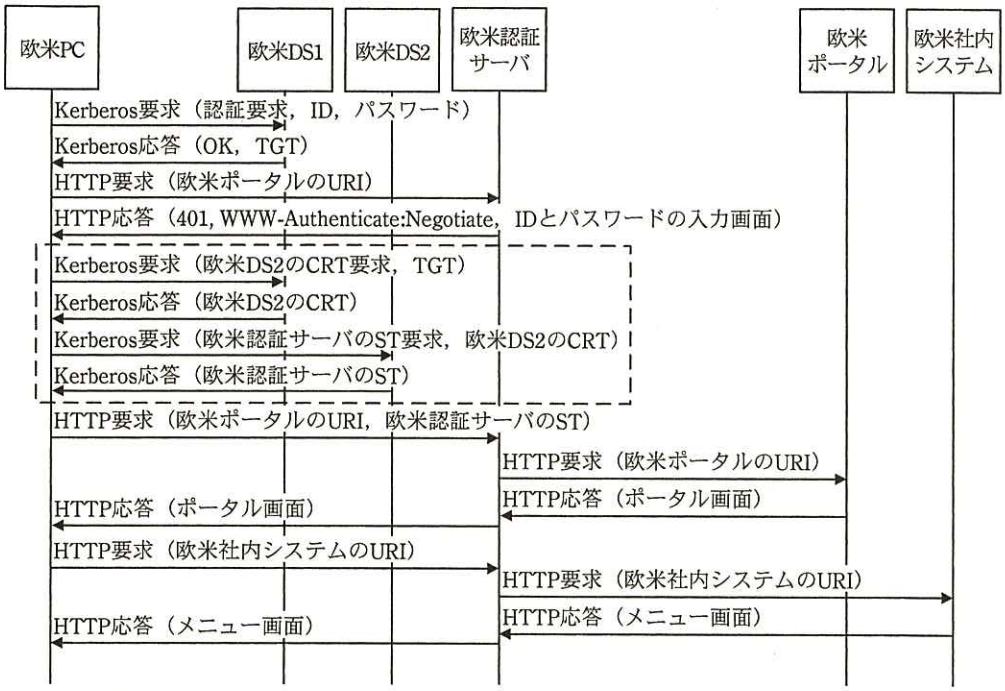
20年前から支店を設けている欧米地域では，N社は，ブラウザ，製品Qを用いた欧米地域のDS1（以下，欧米DS1という）及び欧米地域のDS2（以下，欧米DS2という）並びにリバースプロキシ型の認証サーバ製品Pを用いた欧米地域の認証サーバ（以下，欧米認証サーバという）を組み合わせて，SPNEGOによるSSOを実現している。製品Pは，SPNEGOによるSSOを利用するように設定されると，認証されていないブラウザからのHTTP要求に対して，日本認証サーバと同じ動作をしてSPNEGOによる利用者認証を行う。欧米地域のPC（以下，欧米PCという）のブラウザ及び欧米認証サーバは，SPNEGOによるSSOを利用するように設定されている。

欧米DS1には欧米PCのコンピュータ名及び欧米地域のIDが，欧米DS2には欧米地域の各サーバのコンピュータ名が，それぞれ登録されている。欧米DS1及び欧米DS2には，お互いを信頼するという設定が行われている（以下，信頼関係が結ばれているという）。現在，N社の中のDS間で信頼関係が結ばれているのは，欧米DS1と欧米DS2間だけである。

利用者が，欧米PCにログオンして，ブラウザを立ち上げると，ブラウザは，ホームページとして設定された欧米地域のポータルサーバ（以下，欧米ポータルという）にアクセスしようとする。

欧米地域におけるID管理の手続は，日本と同様である。欧米地域の情報システム部は，新しい正社員又は契約社員のIDと初期パスワードを欧米DS1に登録し，当該正社員又は管理者に通知する。IDの体系は日本と同じであり，日本と重複しているIDがある。

欧米地域における利用者認証の通信シーケンスを図2に示す。



CRT：相互レルムチケット

欧米社内システム：欧米地域の社内システム

注記1　括弧内は送信されるデータを示す。

注記2　破線の枠内の機能が正しく動作するためには，次の二つの条件が必要である。

・欧米DS1及び欧米DS2の間で信頼関係が結ばれていること

・欧米DS1及び欧米DS2がもつドメイン名，登録されているID及びコンピュータ名が重複していないこと

図2　欧米地域における利用者認証の通信シーケンス（概要）

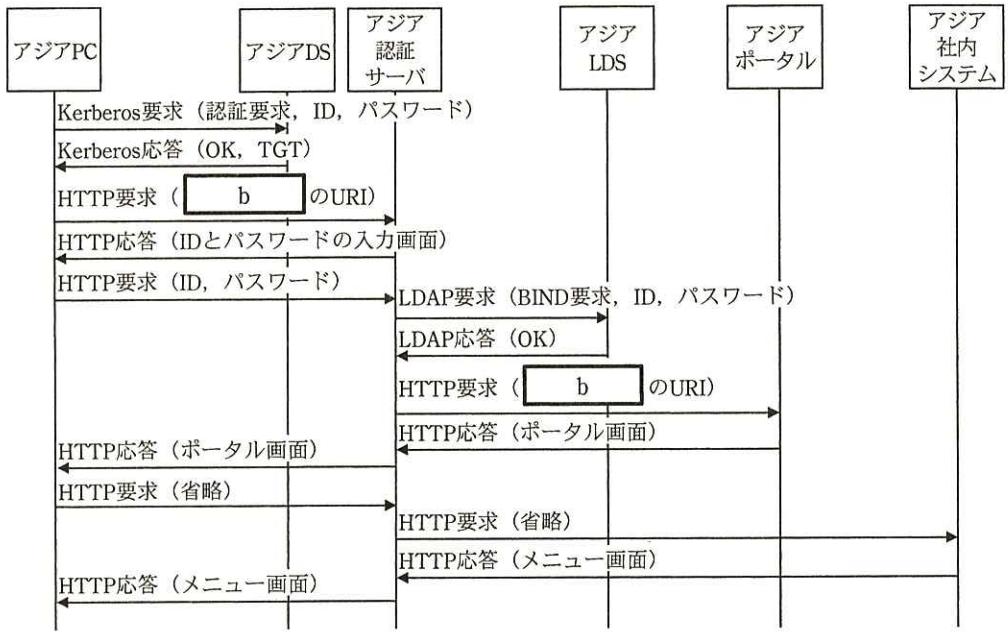
〔アジア地域におけるID管理・認証の方式〕

支店網を急拡大してきたアジア地域において，N社は，製品Pを用いたアジア地域の認証サーバ（以下，アジア認証サーバという）に，LDAPサーバ製品Rを用いたアジア地域のLDAPサーバ（以下，アジアLDSという）を組み合わせて，SSOを短期間で実現した。ただし，アジア認証サーバは，SPNEGOではなくフォーム認証を利用しており，アジア地域のPC（以下，アジアPCという）にSPNEGOの設定はされていない。SSOの対象は，アジア地域のポータルサーバ（以下，アジアポータルという）と，アジア地域の社内システム（以下，アジア社内システムという）である。

利用者が，アジアPCにログオンして，ブラウザを立ち上げると，ブラウザは，ホームページとして設定されたアジアポータルにアクセスしようとする。その際，アジア認証サーバは，アジアLDSを参照し，IDとパスワードによる利用者認証を行う。

アジア地域の全ての正社員及び契約社員は，入社時にアジア PC が利用できるように製品 Q を用いたアジア地域の DS（以下，アジア DS という）に ID が登録される。しかし，アジア LDS への ID 登録や削除は人事システムと連携していない。そのため，正社員及び契約社員は，アジア社内システムにアクセスする必要が生じた際に，自ら ID とパスワードの登録をアジア地域の情報システム部に依頼している。情報システム部は，依頼内容に沿ってアジア LDS に ID とパスワードを登録する。他の地域と重複している ID はない。

アジア地域における利用者認証の通信シーケンスを図 3 に示す。



注記　括弧内は送信されるデータを示す。

図 3　アジア地域における利用者認証の通信シーケンス（概要）

〔G システムにおける ID 管理・認証の設計〕

日本の情報システム部の X 部長は，部下の Y さんに，G システムにおける ID 管理，SSO 及びアクセス制御を行うグローバル ID・アクセス管理システム（以下，GIAM システムという）を設計し，情報セキュリティスペシャリストの Z 主任のレビューを受けるように指示した。Y さんは，認証サブシステム，ID 管理サブシステム，ポータルサブシステム（以下，G ポータルという）から成る GIAM システムを設計した。それ

ぞれのサブシステムの概要は次のとおりである。

・認証サブシステム

製品 P を用いた認証サーバ（以下，認証サブシステムの認証サーバを G 認証サーバという）と製品 R を用いた LDAP サーバ（以下，認証サブシステムの LDAP サーバを GLDS という）から成り，G ポータル及び G システムへのアクセスにおいて，N 社全体で一意となる ID（以下，GID という）とパスワードによる利用者認証及び SSO を実現する。利用者認証が成功すると，HTTP ヘッダに GID を埋め込んで G ポータル及び G システムに送信する。

・ID 管理サブシステム

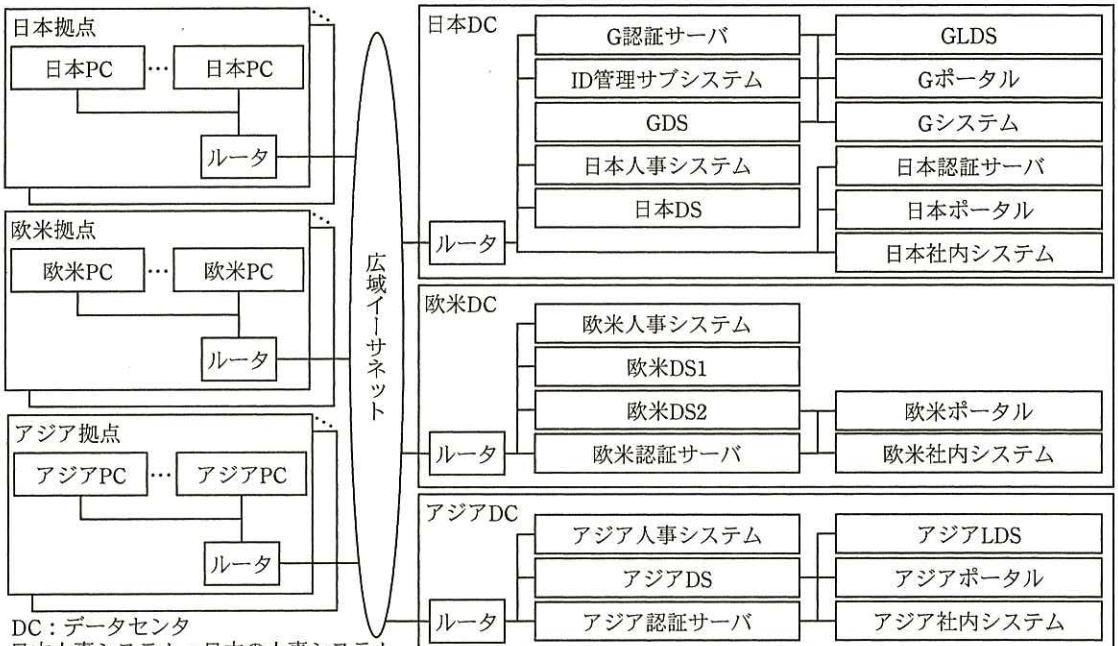
日次で各地域の人事システムから正社員の利用者情報を収集し，新たに登録された正社員に対して，GID と初期パスワードを生成して GLDS に登録する。

・G ポータル

G 認証サーバから渡された GID 及び GLDS に登録された利用者属性に基づいてポータル画面を生成し，G システム及び当該利用者が所属する地域のポータルサーバへのリンクを表示する。全地域の PC ではブラウザに G ポータルをホームページとして設定し，ブラウザが立ち上がると G ポータルのポータル画面が表示されるようにする。

Y さんが設計した，GIAM システム及び関連システムの論理構成を図 4 に，GIAM システムにおける利用者認証の通信シーケンスを図 5 に，それぞれ示す。

なお，図 4 において，グローバル DS（以下，GDS という）には，製品 Q が用いられ，認証サブシステム，ID 管理サブシステム及び G ポータルの各サーバのコンピュータ名が登録される。



DC：データセンタ
日本人事システム：日本の人事システム
欧米人事システム：欧米地域の人事システム
アジア人事システム：アジア地域の人事システム

図4　GIAM システム及び関連システムの論理構成

注記1　括弧内は送信されるデータを示す。
注記2　破線部分については後述する。

図5　GIAM システムにおける利用者認証の通信シーケンス（概要）

Yさんは，GIAMシステムの設計について，Z主任のレビューを受けた。Z主任は，Yさんに，図5中の破線の部分にアジア地域の認証方式を採用した理由を質問した。Yさんは，次の2点を説明した。

・①エージェント型の認証サーバを採用した場合，Gポータルや Gシステムに市販のパッケージ製品を採用する際に大きなカスタマイズが必要となる。

・SPNEGOによるSSOを実現するためには，②GDSと各地域のDSに関する変更と③ID体系に関する変更が必要になり，地域間調整が必要である。

Z主任は，認証サブシステムの設計を了承した。

次にZ主任は，④ID管理サブシステムの設計に不十分な点があることを指摘し，各地域の人事システムとは別のサーバから利用者情報を収集する必要があると助言した。

さらに，Z主任は，⑤一部の地域で，Gポータルのポータル画面中のリンクから地域のポータルサーバへのアクセスが失敗することを指摘し，Gポータルのポータル画面に載せるリンクを修正する必要があると助言した。

YさんはZ主任の助言を反映し，GIAMシステムの設計についてX部長の承認を得た。

〔欧米地域からの要望への対応〕

X部長は，Yさんと Z主任に対して，GIAMシステムの設計内容について，各地域の情報システム部及び利用者の代表者に説明するよう指示した。Yさんと Z主任が欧米地域に出張して GIAMシステムの設計内容を説明したところ，次の要望が挙がった。

要望1.

現行システムと同様に，一度PCにログオンすれば，欧米社内システム及びGシステムへのSSOができるようにしてほしい。

要望2.

ワークスタイル変革及び災害対策として，利用者が自宅から，個人所有の PCやタブレット端末（以下，個人所有機器という）を使って欧米社内システムを利用する方法を検討中である。インターネット経由で社内のシンクライアントサーバにアクセスし，仮想デスクトップから欧米社内システム及び Gシステムにアクセスする際においても SSOを実現してほしい。ただし，インターネット経由の仮想デスクト

ップへのアクセスにおいては，二要素認証を実装したい。

要望3.

他地域への出張中でも，仮想デスクトップから，欧米社内システム及びGシステムにアクセスする際においてSSOを実現してほしい。

Yさんは，GIAMシステムに下線②と下線③の変更を行うことにし，欧米地域の三つの要望全てを全地域の利用者に対して実現する拡張GIAMシステムを設計した。

拡張GIAMシステムでは，自宅又は出張先にいる利用者は，個人所有機器から自分が所属する地域のVPNサーバ経由で自分が所属する地域のシンクライアントサーバにアクセスし，Gポータルのポータル画面から，Gシステム，自分が所属する地域のポータルサーバ及び自分が所属する地域の社内システムにアクセスする。

個人所有機器の業務利用を希望する利用者は，個人所有機器の利用申請を行い，所属長に承認されると，VPN接続用のID（以下，VPNIDという）とパスワード（以下，VPNパスワードという）が割り当てられ，ハードウェア型のワンタイムパスワード（以下，OTPという）トークンが貸与される。

拡張GIAMシステム及び関連システムの論理構成を図6に，個人所有機器からシンクライアントサーバへのアクセスの通信シーケンスを図7に，仮想デスクトップからGシステムへのアクセスの通信シーケンスを図8に，それぞれ示す。

Yさんは，利用者が各地域のPCからGシステムにアクセスする場合の通信シーケンスは，図8中の仮想デスクトップを各地域のPCに置き換えたものになると考えた。

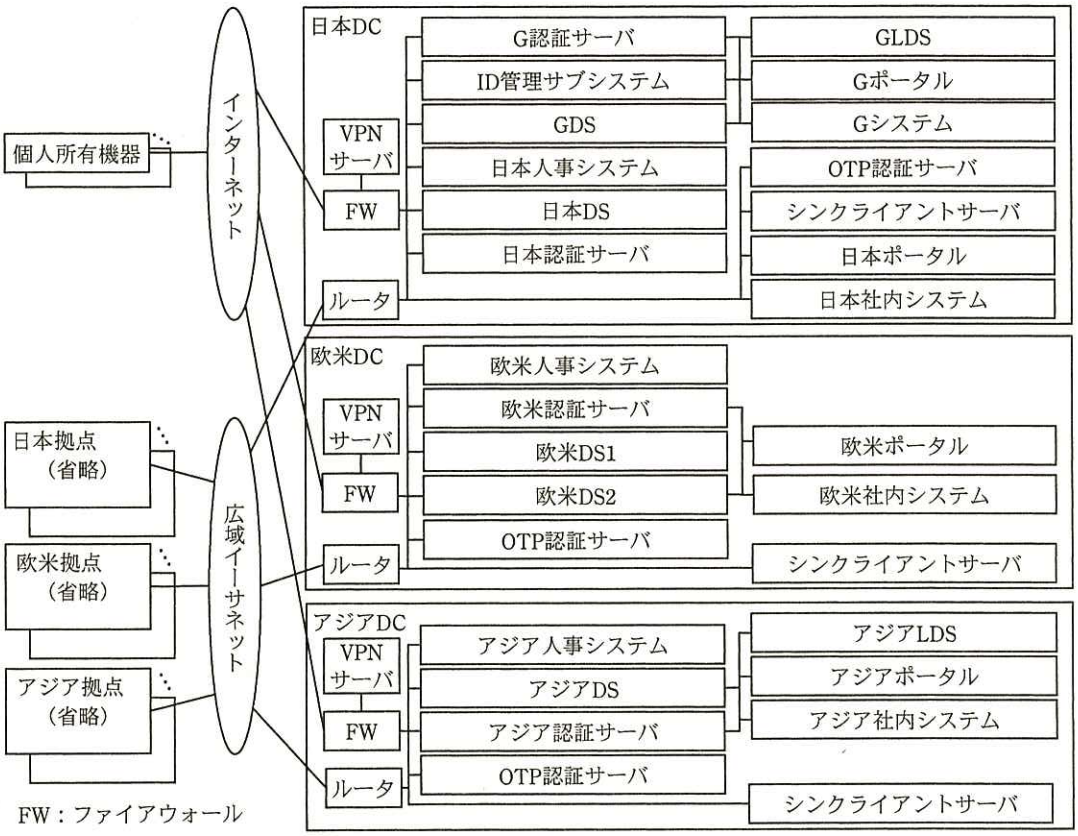
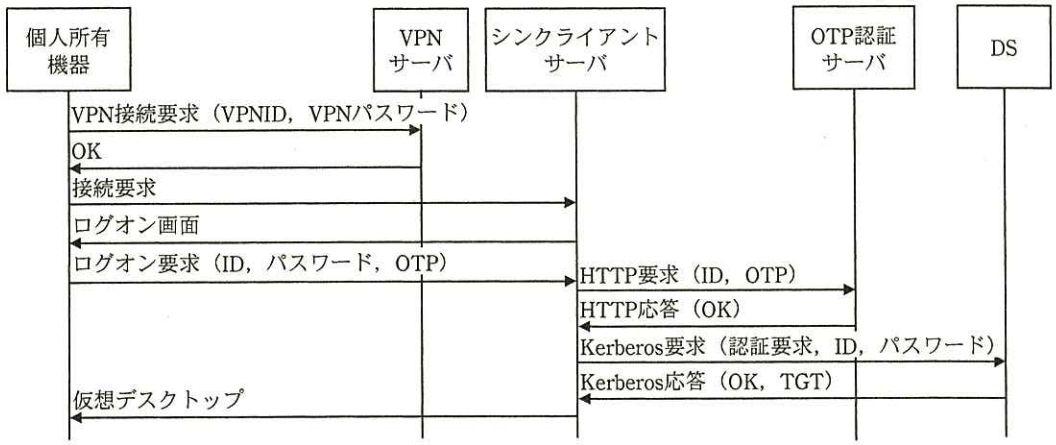
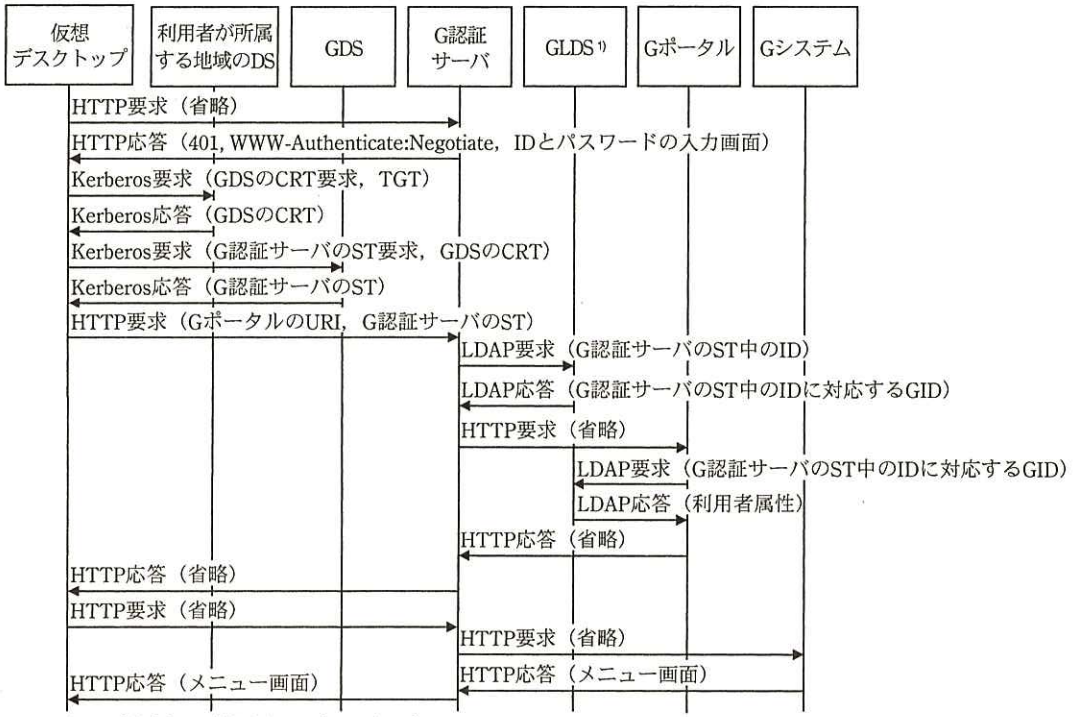


図 6　拡張 GIAM システム及び関連システムの論理構成



注記 1　括弧内は送信されるデータを示す。
注記 2　各サーバは利用者が所属する地域のサーバである。

図 7　個人所有機器からシンクライアントサーバへのアクセスの通信シーケンス（概要）



注記　括弧内は送信されるデータを示す。
注1)　GLDSでは，IDとGIDの対応付けをもつ。

図8　仮想デスクトップからGシステムへのアクセスの通信シーケンス（概要）

Y さんは，拡張 GIAM システムの設計について，Z 主任のレビューを受けた。Z 主任は，IC カードによる利用者認証の方式を採用しなかった理由を質問した。⑥Y さんは，採用した場合，IC カードリーダの追加導入や持ち運びが必要になる上，テスト工程の期間と工数が大きくなると説明した。次に，Z 主任は，⑦要望 2 を実現する方法としてシンクライアントサーバを各地域の DC に配置し，利用者が自分の所属する地域のシンクライアントサーバにアクセスするようにした理由を質問した。Y さんは，その理由を説明した。

Z 主任は，⑧一部の地域の利用者は，PC における利用者認証の後，G ポータル及び地域のポータルサーバにアクセスしようとしたときに ID とパスワードの再入力が必要であることを指摘し，当該地域におけるシステム設定の変更が必要であると助言した。

Y さんは，Z 主任の助言を反映し，拡張 GIAM システムの設計について X 部長の承認を得た。Y さんと Z 主任は，再度各地域の情報システム部及び利用者の代表者に説明を行い，合意を得た。各地域の情報システム部は，G システム及び拡張 GIAM システムの構築を始めた。

設問1　各地域におけるID管理・認証の方式について，(1)～(3)に答えよ。

(1)　図1中の［　a　］に入れる適切な字句を，本文中の用語を用いて答えよ。

(2)　図3中の［　b　］に入れる適切な字句を，図3中から選び，答えよ。

(3)　アジア地域におけるアジアLDSへの正社員及び契約社員のIDの登録手順について，セキュリティ上の問題点を45字以内で述べよ。

設問2　GIAMシステムにおける利用者認証方式について，(1)～(3)に答えよ。

(1)　本文中の下線①について，必要なカスタマイズの内容を35字以内で述べよ。

(2)　本文中の下線②について，変更の内容を25字以内で述べよ。

(3)　本文中の下線③は，どのような現状の問題を解決するために必要か。30字以内で述べよ。

設問3　本文中の下線④について，(1)，(2)に答えよ。

(1)　ID管理サブシステムの設計における不十分な点を，25字以内で述べよ。

(2)　利用者情報の収集元として適切なサーバ名を，図4中から三つ選び，答えよ。

設問4　本文中の下線⑤について，地域のポータルサーバへのアクセスが失敗する地域を，本文中の用語を用いて答えよ。また，ポータル画面に載せるリンクはどのサーバのURIにすべきか。サーバ名を10字以内で答えよ。

設問5　〔欧米地域からの要望への対応〕について，(1)～(3)に答えよ。

(1)　拡張GIAMシステムの二要素認証において使われる認証要素を二つ挙げ，それぞれ8字以内で答えよ。

(2)　本文中の下線⑥について，Yさんがテスト工程の期間と工数が大きくなると説明したのは，テスト工程でどのような機能検証を行う必要があると考えたからか。25字以内で述べよ。

(3)　本文中の下線⑦について，利用者が他の地域のシンクライアントサーバにアクセスした場合に発生するおそれがある問題を，ネットワークに関連する要因とともに50字以内で述べよ。

設問6　本文中の下線⑧について，(1)，(2)に答えよ。

(1)　IDとパスワードの再入力が必要である地域を，本文中の用語を用いて答えよ。

(2)　SSOを実現するためには，どの構成要素に対して，どのような設定が必要か。設定が必要な構成要素を二つ選び，答えよ。また，それらの設定内容を，それぞれ15字以内で述べよ。

問2　Webサイトのセキュリティに関する次の記述を読んで，設問1～3に答えよ。

A社グループは，サービス業，小売業，ネットビジネス業及び情報サービス業のA社～G社の7社から成る企業グループである。A社を含むグループ各社が運営しているWebサイトは，企業情報サイト，BtoCサービスサイト，BtoBサービスサイト，一時的なキャンペーンサイトなど，様々である。グループ各社及びその情報システム関連部門の概要を，表1に示す。

表1　グループ各社及びその情報システム関連部門の概要

社名	概要	情報システム関連部門の概要
A社	・A社グループの持株会社 ・従業員数は100名	・情報システム部は部員数が20名で，A社グループ共通の情報システムの企画とグループ各社情報システム部の統括を行う。 ・サーバ構築，アプリケーションソフトウェア開発（以下，アプリ開発という）及び情報システムの運用はD社に委託する。
B社	・ホテル，ゴルフ場などの施設を運営するサービス業 ・A社グループの中核企業 ・従業員数は5,000名	・情報システム部は部員数が20名で，B社の情報システムの企画を行う。 ・サーバ構築，アプリ開発及び情報システムの運用はD社に委託する。
C社	・水族館，遊園地，大型商業施設などの施設を運営するサービス業 ・30年前に，A社グループ内に設立 ・従業員数は3,000名	・情報システム部は部員数が10名で，C社の情報システムの企画を行う。 ・サーバ構築，アプリ開発及び情報システムの運用は，D社及びA社グループ外の情報システム会社H社に委託する。
D社	・情報サービス業 ・30年前に，B社から独立 ・従業員数は500名	・情報システム部は部員数が10名で，D社の情報システムの企画を行う。 ・開発部は，主にA社，B社，C社及び自社の情報システムのサーバ構築，アプリ開発を行い，運用部はその運用を行う。
E社	・スーパーマーケットなどの小売業 ・10年前に，A社グループに参加 ・従業員数は10,000名	・情報システム部は部員数が20名で，E社の情報システムの企画を行う。 ・サーバ構築，アプリ開発及び情報システムの運用はG社に委託する。
F社	・ネットビジネス業 ・E社が5年前に設立 ・従業員数は300名 ・ショッピングサイトαなどを運営	・情報システム部は部員数が10名で，F社の情報システムの企画を行う。 ・サーバ構築，アプリ開発及び情報システムの運用は，G社及びA社グループ外の情報システム会社J社に委託する。
G社	・情報サービス業 ・15年前に，E社から独立 ・従業員数は100名	・情報システム部は部員数が10名で，G社の情報システムの企画を行う。 ・開発部は，主にE社，F社及び自社の情報システムのサーバ構築，アプリ開発を行い，運用部はその運用を行う。

〔4年前までのグループ各社の状況〕

4年前まで，グループ各社は，Web サイトのセキュリティ対策に各社それぞれの考えで取り組んでいた。

A 社は，セキュリティ対策や個人情報の保護について，B 社～G 社に対して業界ガイドラインへの準拠をポリシとして求めていたが，具体的な指示も準拠状況の確認も行っていなかった。

〔セキュリティ対策プロジェクトの立上げ〕

その後，セキュリティに詳しい L 氏が A 社の経営陣に加わった。L 氏は，A 社グループ内でセキュリティ事故が発生すれば，A 社グループ全体の信頼を損なうおそれがあると取締役会で問題提起した。取締役会では，セキュリティ対策プロジェクト（以下，プロジェクトという）を立ち上げ，グループ全体のセキュリティ対策を推進することを決定した。

この決定を受けて，プロジェクトの責任者には A 社情報システム部長が，プロジェクトリーダには A 社情報システム部の U 課長がそれぞれ任命された。プロジェクトメンバはグループ各社から数名ずつ選出された。

U 課長は，公開しているグループ各社の Web サイトに脆弱(ぜい)性が潜在していたり，今後作り込まれたりするおそれがあり，次の二つが必要であると考えた。

・脆弱性を作り込まず，Web サイトを安全に構築するための対策を実施する。
・攻撃を受け，セキュリティ事故となった場合に，セキュリティ事故の情報は緊急にグループ各社に展開し，対策を実施する。

そこで，部下の P さんとともに，セキュリティ専門家の支援を受けて，次のセキュリティ対策を推進する計画を立案した。

(1) セキュアサイト構築ガイドラインの制定
(2) セキュアサイト構築ガイドラインを踏まえた，具体的な内容を記載した各社セキュアサイト構築基準の制定及び定期的な見直し
(3) セキュアサイト構築基準に従った，サーバ構築及びアプリ開発
(4) セキュリティ事故が発生した直後の A 社情報システム部への報告

(1)～(4)は，グループ各社の取締役会で承認され，3 か月後，(1) が完了し，(2)～(4) についてもグループ各社に指示が出された。

〔F 社ショッピングサイトαへの攻撃〕

F 社から G 社に運用を委託している，ショッピングサイトα（以下，サイトαという）には，PC サイト，携帯サイト及びスマートフォンサイト（以下，スマホサイトという）があり，それぞれ 30 画面で構成されている。今年になって，サイトαの携帯サイトに不審なアクセスがあった。G 社の運用担当者が週 1 回のメンテナンス中にログインのエラーログを確認したところ，利用者 ID に特殊記号を含んだものを多数発見した。通常の利用では考えられないエラーだったので，F 社のサイトα担当者に報告した。

F 社のサイトα担当者から連絡を受けた F 社情報システム部の N さんは，不正アクセスの可能性があると考え，セキュリティ専門業者の X 社に調査を依頼した。X 社の T 氏が調査した結果，携帯サイトの Web アプリケーションソフトウェア（以下，Web アプリケーションソフトウェアを Web アプリという）が，SQL インジェクション攻撃を受けていたことが分かった。そこで，N さんはサイトα担当者に対し，携帯サイトのサーバをネットワークから切り離すように指示した。

次は，そのときの N さんと T 氏の会話である。

N さん：サイト利用者の情報を読み出されたのでしょうか。

T 氏　：いいえ。携帯サイトのアクセスログと，携帯サイトの Web アプリが記録していた POST データのログを確認しましたが，サイト利用者の情報を読み出すリクエストは受信していませんでした。どうやら，脆弱性を探す目的で攻撃を仕掛けられたようです。

N さん：なるほど。それで，脆弱性はあったのでしょうか。

T 氏　：はい。表 2 に示す，携帯サイトのアクセスログを見てください。Web サーバのアクセスログのうち，前回メンテナンス以降の部分について確認したところ，特定の IP アドレスから 27 画面に対して，SQL インジェクションの代表的なパターンが試行されていました。このうち，ステータスコードが 200 であり，かつ，応答のサイズが通常のアクセス時と比較して［ a ］であ

るアクセスログの番号［ b ］を見つけることができます。このログから，脆弱性があると考えられる URI のパス名は［ c ］であり，クエリ文字列中のパラメタ名は［ d ］であることが分かります。

Nさん：分かりました。攻撃が行われた27画面について，早急に対策を行います。

T氏　：念のために，①それらの画面だけでなく，携帯サイト全体に対して SQL インジェクション対策を行ってください。そのほか，PC サイトとスマホサイトの対策はどのようになっていますか。

Nさん：PC サイトは2年前にリニューアルし，スマホサイトも同時にリニューアルしました。いずれも公開前及びその後の改修時にセキュリティ診断（以下，診断という）をしたので大丈夫だと思います。一方，携帯サイトは 5 年前に公開してから，一度も診断をしていません。アクセスを携帯キャリアのゲートウェイからだけに制限していたので，大丈夫だと思っていました。

T氏　：そうですか。今後は，携帯サイトも診断してください。

Nさん：分かりました。

表2　携帯サイトのアクセスログ（抜粋）

番号	IP アドレス	メソッド	URI のパス名	クエリ文字列 [1)2)]	ステータスコード	応答のサイズ（バイト）
1	ipA	GET	/		200	3,284
2	ipA	POST	/Login		302	0
3	ipA	GET	/top		200	3,165
4	ipA	GET	/Catalog	category=shirt	200	1,840
5	ipA	GET	/Catalog	category=shirt'	200	1,840
6	ipA	GET	/Catalog	category=shirt''	200	1,840
7	ipA	GET	/Catalog	category=shirt' and '1'='1	200	1,840
8	ipA	GET	/GoodsSearch	word=new	200	3,877
9	ipA	GET	/GoodsSearch	word=new'	200	3,877
10	ipA	GET	/GoodsSearch	word=new''	200	3,877
11	ipA	GET	/GoodsSearch	word=new' and '1'='1	200	3,877
12	ipA	GET	/GoodsDetail	goodsNo=10001	200	1,798
13	ipA	GET	/GoodsDetail	goodsNo=10001'	500	527
14	ipA	GET	/GoodsDetail	goodsNo=10001 and 1=1	200	1,806
15	ipA	POST	/CartAdd		200	1,611
16	ipA	POST	/Order		200	2,239
17	ipA	POST	/OrderConfirm		200	1,818

注 1)　クエリ文字列は，URI デコード済みである。

2)　クエリ文字列中の''は，一重引用符（シングルクォーテーション）が二つ連続している。

数日後，N さんは G 社から携帯サイトの対策が完了したという報告を受けた。そこで，N さんは，X 社にソースコードを提示し，脆弱性が修正されていることを確認してもらった。その後，F 社では携帯サイトを再開し，N さんは A 社情報システム部に，F 社でセキュリティ事故が発生したことを報告した。

〔グループ各社の管理強化〕

F 社から報告を受けた U 課長は，F 社のセキュリティ事故を分析し，次のような施策案を考えた。

(1) 今回の携帯サイトの脆弱性を含め，脆弱性の多くは診断によって発見できるので，Web サイトの公開前の診断を義務付ける。また，稼働中の全 Web サイトに対しては，優先順位を決めて，順次診断をしていく。

(2) Web サイトによってリスクが異なるので，実施すべき対策を Web サイトごとに各社で決める。

(3) 対策の実施状況と併せて，グループ各社のセキュアサイト構築基準の制定状況と定期的な見直し状況を調査し，問題があれば改善を指示する。

次は，上記の施策案の具体的な進め方に関する，U 課長と部下の P さんの会話である。

U 課長：インターネットに公開している Web サイトでは診断を必須とするが，インターネットに公開していない社内用 Web サイトでは診断はどうしたらいいだろうか。

P さん：グループ各社に任せるにしても判断に困るでしょうね。

U 課長：それなら，基準を統一するために診断ガイドラインを作成しよう。また，グループ各社の Web サイトについて，診断履歴の調査はもちろん必要だが，サイトについてもっと詳しく情報を収集した上で，診断していない Web サイトについて，診断の優先順位を整理してほしい。

P さん：Web サイトの情報収集は調査票を用意して，グループ各社の情報システム部に回答してもらいます。

U 課長：しかし，情報システム部で Web サイトをよく把握していない場合もあるな。

P さん：そうですね。そのような場合の情報システム部への指示方法も検討します。

U課長：セキュアサイト構築基準についても，制定状況及び見直し状況について調査票に回答してもらえばよいだろう。

Pさん：分かりました。

〔診断ガイドラインの制定〕

U課長は，セキュリティ専門家の協力を得て診断ガイドラインを作成するようPさんに指示した。1か月後，図1に示す診断ガイドライン案が作成された。

1. 診断の種類
   - 診断には，プラットフォーム診断とWebアプリ診断の2種類がある。
   - プラットフォーム診断では，OS，ミドルウェア及びネットワーク機器の脆弱性を検出する。ただし，ネットワーク機器では，不要なサービスが稼働していないかを確認する。
   - Webアプリ診断では，Webアプリの脆弱性を検出する。
2. 診断の実施時期
   - 対象Webサイトの公開前に，プラットフォーム診断及びWebアプリ診断を行う。
   - 対象Webサイトの公開後，1年ごとに，プラットフォーム診断及びWebアプリ診断を行う。
3. 診断の実施方法
   - 社内ネットワークからの攻撃を想定する場合，ファイアウォールの内側から診断する。
   - インターネットからの攻撃を想定する場合，ファイアウォールの内側又は外側のいずれかから診断する。
   - IPS，WAFなどによって，［ e ］からの通信が遮断されると，対象Webサイトの脆弱性を検出できないので，［ e ］からの通信は遮断しないように設定した上で診断する。IPS，WAFなどの制約によって，これができない場合は，IPS，WAFなどの内側から診断する。
   - PCサイト，携帯サイト及びスマホサイトのそれぞれについて診断する。ただし，動的ページのプログラムが同じソースコードのプログラムであれば，いずれか一つのサイトについて診断すればよい。
   - ASPサービス及びパブリッククラウドサービスは，サービス提供事業者の許可を得た上で診断する。ただし，サービス提供事業者が診断を許可しない場合は，セキュリティ対策についてサービス提供事業者に説明を求め，確認する。（省略）
4. Webサイトの特徴に応じた診断項目
   - Webサイトが次のいずれかに該当する場合は，詳細な診断を行う。そうでない場合は簡易な診断を行う。
     - インターネットに公開しているWebサイト
     - 決済機能をもつWebサイト
     - 個人情報を扱うWebサイト
5. 診断項目

（省略）

6. 診断実施後の対応
   - 検出された脆弱性については，リスクの大きさによって修正の要否を検討し，対策を行う。
   - ファイアウォールの内側から行った診断で検出された脆弱性のうち［ f ］については，深刻な脆弱性であっても，対策の優先順位を下げてよい。
   - ②脆弱性の修正完了後，公開前にプラットフォーム診断及びWebアプリ診断を再度行う。

（以下，省略）

図1　診断ガイドライン案

U 課長は，診断ガイドライン案を確認するとともに，それをグループ各社へ展開することについて A 社取締役会で承認を得た。その後，グループ各社の Web サイトについて診断ガイドラインに沿って診断を進めるよう指示した。

〔新技術によって生じる脆弱性への対応〕

グループ各社のセキュアサイト構築基準について調査した結果，制定はしているが，見直しをしていないことが分かった。

U 課長は，最近の脆弱性への対応に加え，今後 Web サイトに新技術を採用した場合の対応も必要になると考えた。そこで，グループ各社の情報システムで今後採用する可能性がある技術を調査した上で，その技術を使った場合に考えられる脆弱性について，セキュリティ専門家に調査を依頼した。

セキュリティ専門家の調査結果によると，セキュアサイト構築ガイドラインに追加が必要な項目は次の三つであった。

(Ⅰ) DOM（Document Object Model）ベースの XSS（クロスサイトスクリプティング）の対策

(Ⅱ) クリックジャッキングの対策

(Ⅲ) HSTS（HTTP Strict Transport Security）の使用

(Ⅰ) DOM ベースの XSS の対策

JavaScript による Web ページ操作に問題がある場合に起きる XSS は，DOM ベースの XSS と呼ばれている。JavaScript を利用する場合は，注意が必要である。

例えば，図 2 に示す HTML（http://www.example.jp/domxss.html）があった場合に，図 3 に示す URI にブラウザからアクセスすると，“1” という警告ダイアログが表示される。

```
<html>
<body>
<script>
 document.write(decodeURIComponent(location.hash));
</script>
</body>
</html>
```

図 2　HTML（http://www.example.jp/domxss.html）

```
http://www.example.jp/domxss.html [ g ] <script>alert(1) [ h ]
```

図3　警告ダイアログが表示されるURI

反射型（reflected 型，non-persistent 型）の XSS と違って，DOM ベースの XSS では攻撃者が注入するデータが Web サイトからの応答中に出力されない。ブラウザ上の HTML データに入力データを動的に挿入するような JavaScript が応答中に含まれていると，入力データにスクリプトが含まれていたときに，そのスクリプトがブラウザ上で実行されてしまう。そのため，DOM ベースの XSS は，③反射型の XSS とは診断方法が異なる。

DOM ベースの XSS の対策のためには，“document.write”，“innerHTML” などの，動的にブラウザ上の HTML データを操作するメソッドやプロパティを使用するのではなく，“createElement” などの DOM 操作用のメソッドやプロパティを使用して，ブラウザ上の HTML データを構築することが必要である。

(Ⅱ)　クリックジャッキングの対策

クリックジャッキングの対策には，④HTTP 応答ヘッダで “X-FRAME-OPTIONS” に DENY を指定することによって，自サイトをフレーム内で表示させないようにする方法がある。近年，クリックジャッキングによると思われる事件が発生しており，この応答ヘッダに対応したブラウザが増えている。

(Ⅲ)　HSTS の使用

HSTS とは，Web サイトが HTTPS の使用をブラウザに強制させる機能である。HSTS がブラウザで有効となるまでの通信の流れを，図 4 に示す。また，HSTS が有効になったブラウザのアドレスバーに “http://www.example.jp/” を入力した場合のブラウザの挙動を，図 5 に示す。HSTS は，HTTPS 応答のヘッダに [i] を指定することによって有効となる。

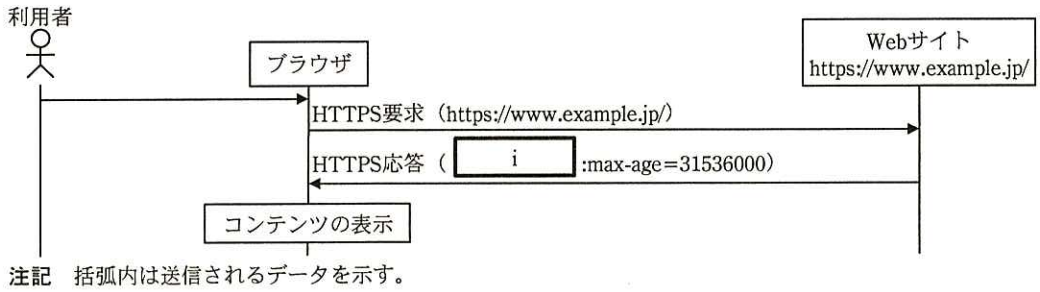


図4　HSTS がブラウザで有効となるまでの通信の流れ

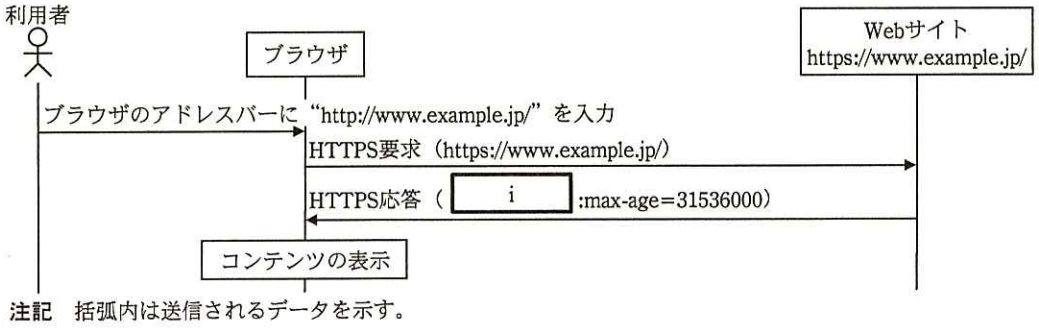


図5　HSTS が有効になったブラウザの挙動

正規の Web サイトで HSTS が有効になるように設定していない場合，正規の Web サイトが HTTPS 通信だけを受け付けるように構成していても，中間者攻撃が行われると，⑤ブラウザが HTTP 通信で接続してしまい，中間者によって通信を盗聴されてしまう。

利用者は毎回［ j ］ことでこの攻撃を受けても気付くことができる。しかし，［ j ］ことを利用者に徹底させるのは難しいので，HSTS のプロトコルが開発され，2012 年に RFC 6797 として公開された。その後，この機能に対応するブラウザが増えている。

P さんは，グループ各社の Web サイトにおける(Ⅰ)～(Ⅲ)の取組状況を Web サイトの概要と併せて調査した。調査結果を表 3 に示す。

なお，クリックジャッキングについては，フレーム内での表示有無だけでなく，クリックジャッキングによって被害を受けるおそれについても整理している。

表3　グループ各社のWebサイトの調査結果（抜粋）

調査項目＼サイト名	サイト1	サイト2	サイト3	サイト4	サイト5	サイト6
運営会社	A社	A社	B社	C社	E社	F社
サイトの種別	企業紹介	ポータル	ホテル予約	レジャー施設入場券販売	ショッピング	ショッピング
機能の概要	検索	ログイン 予定表 資料集 掲示板	会員登録 ログイン 会員ページ 空室検索 宿泊予約 問合せ	会員登録 ログイン 会員ページ 入場券購入 メールマガジン 問合せ	会員登録 ログイン 会員ページ 商品検索 商品購入 問合せ	会員登録 ログイン 会員ページ 商品検索 商品購入 問合せ
JavaScriptの利用	なし	なし	あり	あり	あり	あり
DOMベースのXSS脆弱性	なし	なし	なし	なし	あり	あり
フレーム内での表示の有無	なし	なし	なし	なし	あり （同じドメインページ内で表示）	あり （同じドメインページ内で表示）
対策なしの場合にクリックジャッキングによって被害を受けるおそれ	なし	あり	あり	あり	あり	あり
クリックジャッキング対策の有無	対象外	なし	なし	あり	なし	なし
HTTPSの利用	なし	なし	あり	あり	あり	あり
HSTS対応の有無	対象外	対象外	なし	あり	なし	なし

表3の調査結果から，対応の必要なWebサイトがあることが分かったので，U課長は，セキュアサイト構築ガイドラインに項目(Ⅰ)～(Ⅲ)を追加した上でグループ各社に伝え，さらに，各Webサイトでの対策を検討するよう指示した。

以上の対策によって，グループ各社のWebサイトのセキュリティが強化された。

設問1　〔F社ショッピングサイトαへの攻撃〕について，(1)～(4)に答えよ。

(1) 本文中の［　a　］，［　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　6%未満　　イ　45～55%　　ウ　95～105%　　エ　200%以上

オ　2　　カ　7　　キ　11　　ク　14

(2) 本文中の［ c ］に入れる URI のパス名と，本文中の［ d ］に入れるパラメタ名を，それぞれ 15 字以内で答えよ。

(3) 本文中の下線①について，T 氏が携帯サイト全体に対して対策を行うべきであると考えた理由を，40 字以内で述べよ。

(4) 事故発生後の N さんの対応について，改善すべき点を 30 字以内で述べよ。

設問 2 〔診断ガイドラインの制定〕について，(1)～(3)に答えよ。

(1) 図 1 中の［ e ］に入れる適切な字句を 15 字以内で答えよ。

(2) 図 1 中の［ f ］に入れる適切な内容を，“ファイアウォール”と“ポート”の二つの用語を用いて 40 字以内で述べよ。

(3) 図 1 中の下線②の診断は，検出された脆弱性が適切に修正されたこと以外に何を確認することを目的としているか。30 字以内で述べよ。

設問 3 〔新技術によって生じる脆弱性への対応〕について，(1)～(6)に答えよ。

(1) 図 3 中の［ g ］，［ h ］に入れる適切な文字列を答えよ。

(2) 本文中の下線③について，反射型の XSS の診断方法を 65 字以内で述べよ。また，その診断方法では DOM ベースの XSS を発見できない理由を 35 字以内で述べよ。

(3) 本文中の下線④の対策を行うと，正規の利用において不具合が発生するサイトを，表 3 の中から選び，全て答えよ。また，不具合が起こらないようにするためには，下線④の対策をどのように変更すればよいか。45 字以内で述べよ。

(4) 本文中，図 4 中及び図 5 中の［ i ］に入れる適切な応答ヘッダフィールド名を解答群の中から選び，記号で答えよ。

解答群

ア Content-Disposition　　イ Content-Security-Policy

ウ Strict-Transport-Security　　エ X-Content-Type-Options

オ X-XSS-Protection

(5) 本文中の［ j ］に入れる，利用者のすべきことを，40 字以内で具体的に述べよ。

(6) Web サイトで HSTS が有効になるよう設定している場合でも，本文中の下線⑤の事象が起きる場合がある。HSTS の有効期限が切れた場合以外に，どのような場合に起きるのか。35 字以内で述べよ。

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，次のものに限ります。
   なお，会場での貸出しは行っていません。
   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。