

次の問 1 は必須問題です。必ず解答してください。

問 1 クラウドサービスの利用者認証に関する次の記述を読んで、設問 1, 2 に答えよ。

A 社では現在、Web ベースの業務システムが複数稼働しており、それぞれが稼働するサーバ（以下、業務システムサーバという）を社内 LAN に設置している。A 社のネットワーク構成を、図 1 に示す。

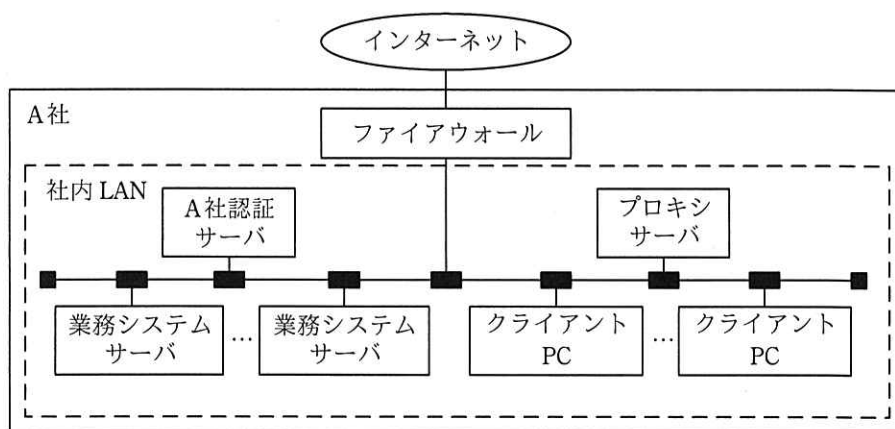


図 1 A 社のネットワーク構成

利用者は、業務システムを、社内 LAN に設置されたクライアント PC の Web ブラウザから利用する。社外から社内 LAN へのリモートアクセスは禁止されている。業務システムの利用者認証は、A 社認証サーバでの利用者 ID とパスワード（以下、この二つを併せて利用者認証情報という）の検証によって行っており、シングルサインオンを実現している。

社内 LAN からインターネットを介した社外への通信は、クライアント PC からプロキシサーバを経由した、HTTP over TLS（以下、HTTPS という）による通信だけが、ファイアウォールによって許可されている。社外からインターネットを介した社内 LAN への通信は、全てファイアウォールによって禁止されている。ファイアウォールの設定は、A 社のセキュリティポリシーに基づき変更しないものとする。

[クラウドサービスの利用者認証]

このたび A 社は、業務システムの一つである販売管理システムを、B 社がインターネットを介して提供する販売管理サービス（以下、B 社クラウドサービスという）に移行することにした。利用者認証に関しては、A 社認証サーバと B 社クラウドサービスを連携し、次の(1)～(3)を実現することにした。

- (1) B 社クラウドサービスをシングルサインオンの対象とする。
- (2) A 社の利用者認証は、B 社クラウドサービスについても、A 社認証サーバで行う。
- (3) 利用者が本人であることを確認するために A 社認証サーバで用いる a は、B 社クラウドサービスには送信しない。

(1)～(3)を実現するために、A 社は、利用者認証を仲介する ID プロバイダ（以下、IdP という）を社内 LAN に設置することにした。IdP は、認証結果、認証有効期限及び利用者 ID（以下、これら三つを併せて認証済情報という）にデジタル署名を付加してから、Web ブラウザを介して、B 社クラウドサービスに送信する。B 社クラウドサービスは、付加されているデジタル署名を使って、受信した認証済情報に b がないことを検証する。このために、IdP の c を B 社クラウドサービスに登録しておく。

Web ブラウザと B 社クラウドサービスとの間、及び Web ブラウザと IdP との間の通信には、HTTPS を用いる。IdP と A 社認証サーバとの間の通信には LDAP を用いる。

[B 社クラウドサービスが利用可能になるまでの処理の手順]

A 社の利用者が、利用者認証されていない状態で、B 社クラウドサービスを利用しようとした場合に、利用可能になるまでの処理の手順を次の①～⑩に示す。

- ① 利用者は、Web ブラウザから B 社クラウドサービスにアクセスの要求を送信する。
- ② B 社クラウドサービスは、アクセスの要求を IdP に転送する指示（以下、転送指示という）を、Web ブラウザに返信する。

- ③ Web ブラウザは、②の転送指示に従い、IdP にアクセスの要求を送信する。
- ④ IdP は、利用者認証情報の入力画面を Web ブラウザに返信する。
- ⑤ 利用者は、Web ブラウザで利用者認証情報を入力する。Web ブラウザは、入力された利用者認証情報を IdP に送信する。
- ⑥ IdP は、利用者認証情報を A 社認証サーバに送信する。
- ⑦ A 社認証サーバは、利用者認証情報を検証し、認証結果を IdP に返信する。
- ⑧ IdP は、認証結果が成功の場合に、認証済情報を発行し、当該情報の B 社クラウドサービスへの転送指示とともに、Web ブラウザに返信する。
- ⑨ Web ブラウザは、⑧の転送指示に従い、認証済情報を B 社クラウドサービスに送信する。
- ⑩ B 社クラウドサービスは、認証済情報に基づいて、B 社クラウドサービスの利用を許可し、操作画面を Web ブラウザに返信する。

B 社クラウドサービスが利用可能になるまでの処理の流れを、図 2 に示す。図 2 中の①～⑩は、処理の手順の①～⑩と対応している。

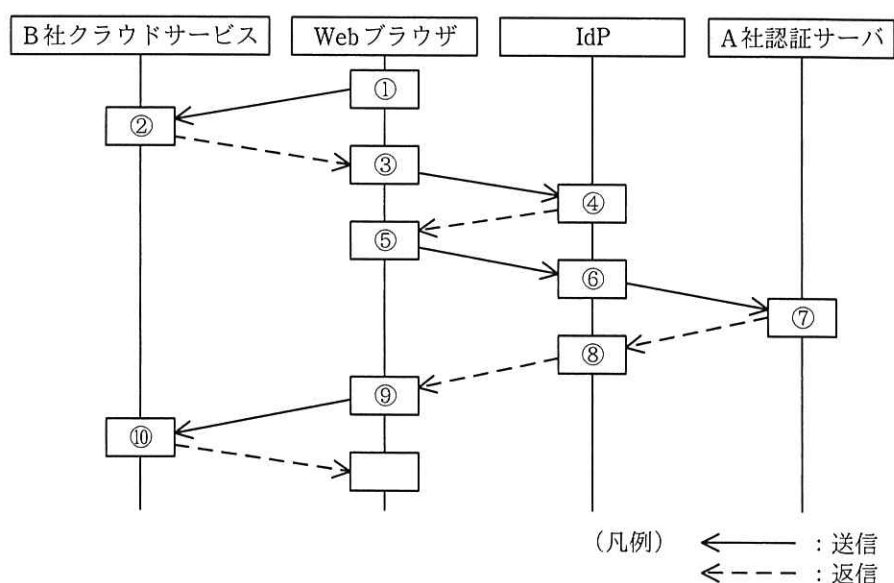


図 2 B 社クラウドサービスが利用可能になるまでの処理の流れ

設問 1 本文中の に入れる適切な答えを，解答群の中から選べ。

a～c に関する解答群

- | | | |
|----------|----------|---------|
| ア PKI | イ 改ざん | ウ 公開鍵 |
| エ サービス妨害 | オ 生体情報 | カ パスワード |
| キ 秘密鍵 | ク 利用者 ID | ケ 漏えい |

設問 2 次の記述中の に入れる適切な答えを，解答群の中から選べ。

B 社クラウドサービスでは，接続元の IP アドレスを A 社のものに限定する機能は提供されていない。しかし，他の業務システムと同様に，B 社クラウドサービスを，社内 LAN からの利用に限定できる。

この理由は， d が必要であるが，IdP を社内 LAN に設置するので，社外から B 社クラウドサービスを利用しようとしても，図 2 中の e の送信で失敗し，利用者認証されないからである。

d に関する解答群

- ア B 社クラウドサービスが，IdP と直接通信する
- イ B 社クラウドサービスが，利用者認証情報を検証し，Web ブラウザに返信する
- ウ IdP が，利用者に代わって，利用者認証情報を B 社クラウドサービスに送信する
- エ Web ブラウザが，IdP と通信する

e に関する解答群

- | | | | | |
|-----|-----|-----|-----|-----|
| ア ① | イ ③ | ウ ⑤ | エ ⑥ | オ ⑨ |
|-----|-----|-----|-----|-----|