02 プロキシサーバ

出題ナビ

もともとはWebページの閲覧性の向上を目的に導入されるサーバで，まさにプロキシ＝代理として，クライアントの代わりにWebサーバへアクセスを行います。近年ではセキュリティ装置としての出題が増加。クライアントとWebサーバに直接通信させない効果があることに注意。

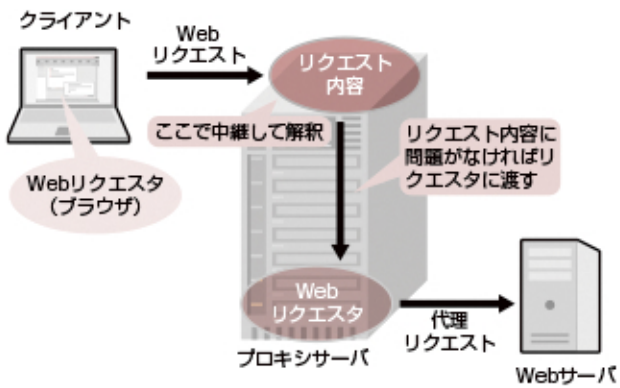
プロキシサーバ

自社のクライアントが同じサーバへ何度も通信する場合，最初のアクセス時にコンテンツをプロキシサーバにキャッシュしておけば，2度目以降のアクセスではわざわざWebサーバまでコンテンツをもらいにいかなくても，プロキシサーバが返信すればよいわけです。

合格のツボ

プロキシサーバを利用すると，

→ **通信速度の向上が期待できる**
→ **WAN回線の契約によっては，トラフィック減によるコスト削減も可能**



プロキシサーバは万能ですね。もうWebサーバにアクセスする必要はないんじゃないですか？

オリジナルはあくまでWebサーバです。Webサーバの情報が更新された場合，プロキシサーバは古い情報をキャッシュしていることになります。キャッシュの有効期限は本試験の頻出項目です。

● プロキシサーバのセキュリティ装置的な運用

プロキシサーバの主要な役割は上記のとおりですが，それに加えてセキュリティ装置としても使われることが増えました。個々のクライアントを直接Webサーバと通信させず，プロキシサーバを介するわけです。

合格のツボ

プロキシサーバでは
- **クライアントのIPアドレスがWebサーバに漏れない**
- **個々のクライアントPCに，設定漏れ，利用者が勝手に設定を書き換えていた，などの脆弱性があっても，プロキシサーバに通信を集約することで管理できる**

リバースプロキシとシングルサインオン

シングルサインオンの出題増に絡んで，リバースプロキシの出題も増加しています。ここで一緒に覚えてしまいましょう。

シングルサインオンとは，複数のサーバにログイン（サインオン）する必要があるときに，どこか1つにログインできれば後は自動的にログインできるようにしようというしくみです。

3ステップで覚える！

リバースプロキシ

① 複数のサーバのユーザIDとパスワードを覚えるのが面倒！
② ログイン自体も面倒！
③ その解決策として登場。実装技術はリバースプロキシ，クッキー，SAML

リバースプロキシは，まさにプロキシサーバを通常と逆に配置する方法です。一般的なプロキシはクライアント側に配置して，クライアントの通信を集約する形になりますが，リバースプロキシはサーバ側に配置して，クライアント側から見ると，プロキシサーバに集まった通信を各サーバに振り分けるような形です。

覚えにくいを覚えやすく

プロキシサーバとリバースプロキシ

	プロキシ	リバースプロキシ
配置	クライアント側	サーバ側
目的	コンテンツ高速化	シングルサインオン

SAML認証

XMLベースのマークアップ言語であるSAMLを使って認証に関する情報（アサーション）をやり取りするしくみです。クッキーやリバースプロキシと異なり，異なるドメイン間でも運用できるのがポイントで，伝送プロトコルとしてはHTTPやSOAPが使われます。

アサーションは3種類あります。

属性ステートメント	ユーザの情報
認証ステートメント	認証を行ったサーバの情報
認可ステートメント	サブジェクトに何を許可したかの情報

サブジェクトとは認証を受ける対象で，ユーザやクライアントマシンなどです。サブジェクトはまず**アイデンティティプロバイダ**（**IdP**：認証サーバ）にアクセスして認証してもらいます。そこで発行された認証情報を**サービスプロバイダ**（**SP**：Webサーバなど）に送ればシングルサインオンが実現するというわけです。

こんな問題が出る！

シングルサインオンの実装方式の一つであるSAML認証の特徴はどれか。

ア　IdP（Identity Provider）がSP（Service Provider）の認証要求によって利用者認証を行い，認証成功後に発行されるアサーションをSPが検証し，問題がなければクライアントがSPにアクセスする。

イ　Webサーバに導入されたエージェントが認証サーバと連携して利用者認証を行い，クライアントは認証成功後に利用者に発行されるcookieを使用してSPにアクセスする。

ウ　認証サーバはKerberosプロトコルを使って利用者認証を行い，クライアントは認証成功後に発行されるチケットを使用してSPにアクセスする。

エ　リバースプロキシで利用者認証が行われ，クライアントは認証成功後にリバースプロキシ経由でSPにアクセスする。

解説　ドメインをまたいだ認証を実現する技術です。利用者，SP，IdPが登場するのが特徴で，IdPが利用者の認証を，SPがサービスの提供を行います。

解答：ア

こんな問題が出る！

リスクベース認証に該当するものはどれか。

ア　インターネットからの全てのアクセスに対し，トークンで生成されたワンタイムパスワードで認証する。
イ　インターネットバンキングでの連続する取引において，取引の都度，乱数表の指定したマス目にある英数字を入力させて認証する。
ウ　利用者のIPアドレスなどの環境を分析し，いつもと異なるネットワークからのアクセスに対して追加の認証を行う。
エ　利用者の記憶，持ち物，身体の特徴のうち，必ず二つ以上の方式を組み合わせて認証する。

解答：ウ

● 耐タンパ性

耐タンパ性とは，外部機器から組織内の情報を読まれたり書き換えられたりすることにどれだけ耐えられるかを表す指標です。tamperは改ざんや干渉のことです。過去の本試験では，読み出し用の機器が接続されたことを検出すると，チップ内の情報が消去される事例が出題されました。

● TPM (Trusted Platform Module)

TPMはコンピュータの基板上に実装するセキュリティチップです。暗号化や復号，ハッシュ値の計算，デジタル署名，暗号鍵の保存などを行います。ソフトウェアでこれらを実現する方式に比べると耐タンパ性を高めることができます。

● RFID

RFIDは，ID情報を記載した無線対応チップです。人や商品の識別，管理，追跡などに使われます。バーコードで商品を識別する方法に比べると，処理効率やトレーサビリティの点で優れています。

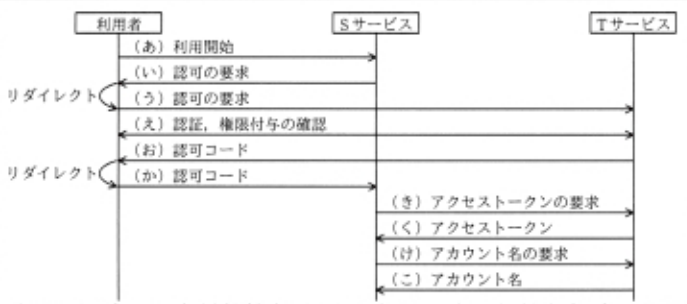
午後問題はこう出る！

今回の改修では，OAuthのAuthorization Code Grantを採用する。OAuthは，認証認可提供SNSと認可情報を送受信するためのプロトコルの一つである。OAuthを用いた認可における三つの主体の説明を図1に，認可のシーケンスを図2に示す。

利用者	：Tサービスのアカウントをもち，S会員の登録を希望する者（以下，S会員登録希望者という）及び登録されたS会員である。
Sサービス	：Tサービスでのアカウント名を要求する。
Tサービス	：認証認可提供SNSである。図3に示す権限を提供する。

注記　Tサービスのアカウント名は変更できない。

図1　OAuthを用いた認可における三つの主体の説明



注記　Sサービスは，S会員登録希望者による利用の初回に，S会員登録希望者がログイン中のTサービスから取得したアカウント名（以下，T-IDという）をSサービス内に登録する。Tサービスにログインしていない場合はログインが促される。2回目以降のSサービスの利用の場合，初回に登録されたT-IDを確認する。

図2　OAuthを用いた認可のシーケンス

解説

OAuthなどの単語が分からなくても萎縮しないでください。本試験では「出題することで広めたい，ここで説明したい」といった問題があります。その場合，細かな部分は問題文が解説してくれます。もちろん，OAuthがサービス連携のための標準規格であることを知っていればより有利に解答できますが，事前知識がなくても食らいついていけます。図1，図2から，三者が登場するよくあるタイプの連携プロトコルで，SサービスからTサービスを呼び出したいこと，そのために利用者から権限をもらって，Tサービスに要求を行うことが読み取れれば十分です。