

# 認証システム

問 2

Check

【2010年秋期 基本 問4】

認証システムに関する次の記述を読んで、設問に答えよ。

複数のクライアントと複数のアプリケーションサーバ（以下、APサーバという）が接続されているネットワークにおいて、単純な認証システムを利用する場合について、ここでは二つの問題点を取り上げる。

- ① 利用者は、使用するクライアントから各 AP サーバにログインするごとに、利用者 ID とパスワードの入力操作を行わなければならない。
- ② クライアントと AP サーバとの間の通信データの横取りと偽造によって、AP サーバのサービスが不正に利用される危険性がある。

ここで、これらの問題を改善するための認証システム（以下、新認証システムという）を考える。

なお、ここでは、これらの問題に直接関連しない仕様については、その記述を省略する。

[新認証システムによる問題点の解消]

問題点①に対しては、利用者が一度、利用者 ID とパスワードをクライアントに入力して認証を受ければ、そのクライアントと各 AP サーバ間での認証は、利用者を介さないで済むように改善する。

このために、チケットと呼ぶ認証データを用いる。チケットは、クライアントに対して発行され、そのクライアントは、AP サーバの認証を得るとき、発行されたチケットを AP サーバに送信する。

問題点②に対しては、AP サーバに送信されたチケットが、チケットの発行を受けたクライアントから送られてきたものであることを、AP サーバが確認できるよう、チケットとは別に認証子と呼ぶ認証データを用いる。

図 1 に新認証システムの構成を示す。

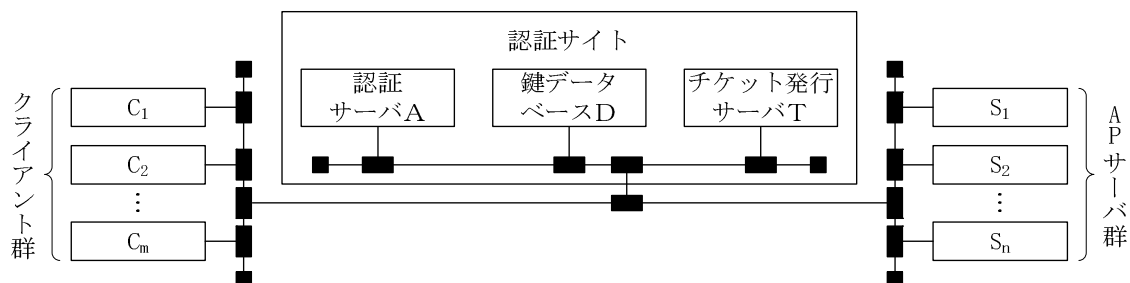


図 1 新認証システムの構成

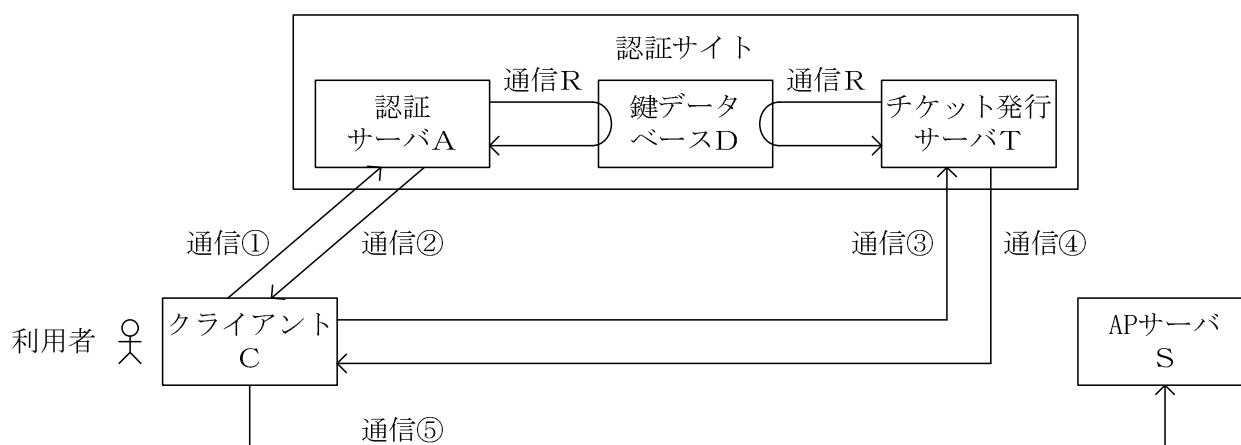
# 1 情報セキュリティ

[新認証システムの構成と方式についての説明]

- (1) 新認証システムでは、共通鍵暗号方式によって、通信データを暗号化する。以下、共通鍵を鍵という。
- (2) 認証サイトは、認証サーバ、鍵データベース及びチケット発行サーバで構成する。
- (3) チケット発行サーバの鍵は、チケット発行サーバ自体と鍵データベースに登録されている。
- (4) 各 AP サーバの鍵は、それぞれの AP サーバ自体と鍵データベースに登録されている。
- (5) 利用者の鍵は、利用者のパスワードから計算して決められ、鍵データベースに登録されている。クライアントには、利用者が入力したパスワードから計算した鍵が、利用者がクライアントの利用を終了するまで、一時的に保持される。

[認証のための通信の例]

図 2 は、利用者が、クライアント C から目的の AP サーバ S にアクセスする場合の認証の流れを示す。



注 通信Rは、鍵データベースを参照していることを表す。

図 2 認証の流れの例

認証は、次の3段階で行われる。ここで、 $\text{enc}(x)$  は、 $x$  を暗号化したものを表す。

第1段階は、クライアントCがチケット発行サーバTにチケットを要求するためのチケット（以下、チケット発行サーバT用チケットという）の認証サーバAへの要求（図2中の通信①）と、その発行（図2中の通信②）である。

通信①では、クライアントCは、次のデータを認証サーバAに送信する。

## 認証システム

データ	データの説明
$ID_C$	利用者 ID である。
$ID_T$	チケット発行サーバ T の ID である。

通信②では、認証サーバ A は、次のデータをクライアント C に応答する。

データ	データの暗号化に用いた鍵	データの説明
$enc(KEY_{CT})$	利用者の鍵 $KEY_C$	$KEY_{CT}$ は、クライアント C とチケット発行サーバ T との間（以下、C-T 間という）の通信データの暗号化に用いる鍵であり、C-T 間のセッション鍵という。
$enc(TICKET_{CT})$	<span style="border: 1px solid black; padding: 2px;">a</span>	$TICKET_{CT}$ は、チケット発行サーバ T 用チケットである。 $TICKET_{CT}$ は $KEY_{CT}$ を含む。これによって、チケット発行サーバ T にクライアント C 経由で $KEY_{CT}$ を安全に渡すことができる。

第 2 段階は、クライアント C が AP サーバ S にアクセスするためのチケット（以下、AP サーバ S 用チケットという）のチケット発行サーバ T への要求（図 2 中の通信③）と、その発行（図 2 中の通信④）である。

通信③では、クライアント C は、次のデータをチケット発行サーバ T に送信する。

データ	データの暗号化に用いた鍵	データの説明
$enc(TICKET_{CT})$	<span style="border: 1px solid black; padding: 2px;">a</span>	$enc(TICKET_{CT})$ は、クライアント C では復号できない。クライアント C はチケット発行サーバ T にそのまま送信し、チケット発行サーバ T が復号する。
$enc(AUTH_{C1})$	<span style="border: 1px solid black; padding: 2px;">b</span>	認証子 $AUTH_{C1}$ は、クライアント C が生成する。
$enc(ID_S)$	<span style="border: 1px solid black; padding: 2px;">b</span>	$ID_S$ は、AP サーバ S の ID である。

チケット発行サーバ T は、 $TICKET_{CT}$  を送信したのが間違いなくクライアント C であることを  $TICKET_{CT}$  と  $AUTH_{C1}$  から確認する。確認ができたとき、通信④では、チケット発行サーバ T は、次のデータをクライアント C に応答する。

# 1 情報セキュリティ

データ	データの暗号化に用いた鍵	データの説明
enc(KEY <sub>CS</sub> )	<input type="text" value="b"/>	KEY <sub>CS</sub> は、クライアントCとAPサーバSとの間（以下、C-S間という）の通信データの暗号化に用いる鍵であり、C-S間のセッション鍵という。データの暗号化に用いた鍵は、チケット発行サーバTが、通信③で受け取った enc(TICKET <sub>CT</sub> ) から取り出したものである。
enc(TICKET <sub>CS</sub> )	<input type="text" value="c"/>	TICKET <sub>CS</sub> は、APサーバS用チケットである。TICKET <sub>CS</sub> は、KEY <sub>CS</sub> を含む。これによって、APサーバSにKEY <sub>CS</sub> をクライアントC経由で安全に渡すことができる。

第3段階は、APサーバS用チケットの提示である（図2中の通信⑤）。  
通信⑤では、クライアントCは、次のデータをAPサーバSに送信する。

データ	データの暗号化に用いた鍵	データの説明
enc(TICKET <sub>CS</sub> )	<input type="text" value="c"/>	enc(TICKET <sub>CS</sub> )は、クライアントCでは復号できない。クライアントCはAPサーバSにそのまま送信し、APサーバSが復号する。
enc(AUTH <sub>C2</sub> )	<input type="text" value="d"/>	認証子 AUTH <sub>C2</sub> は、クライアントCが生成する。

APサーバSは、TICKET<sub>CS</sub>を送信したのが間違いなくクライアントCであることを TICKET<sub>CS</sub>と AUTH<sub>C2</sub>から確認する。確認ができたとき、利用者は、クライアントCから、APサーバSへのアクセスが許可される。

設問 本文中の  に入れる正しい答えを、解答群の中から選べ。

aに関する解答群

- ア C-T間のセッション鍵 KEY<sub>CT</sub>
- イ チケット発行サーバTのID ID<sub>T</sub>
- ウ チケット発行サーバTの鍵 KEY<sub>T</sub>
- エ 利用者ID ID<sub>C</sub>

b, cに関する解答群

- ア APサーバSのID ID<sub>S</sub>
- イ APサーバSの鍵 KEY<sub>S</sub>
- ウ C-S間のセッション鍵 KEY<sub>CS</sub>
- エ C-T間のセッション鍵 KEY<sub>CT</sub>
- オ チケット発行サーバTの鍵 KEY<sub>T</sub>

dに関する解答群

- ア APサーバSの鍵 KEY<sub>S</sub>
- イ C-S間のセッション鍵 KEY<sub>CS</sub>
- ウ C-T間のセッション鍵 KEY<sub>CT</sub>
- エ チケット発行サーバTの鍵 KEY<sub>T</sub>