txt030422 アクセス制御

①　ネットワークへの不正侵入

ⓐ　インターネット社会の特性

㋐　ネットワーク上で個人はＩＤとパスワードによって識別される。他人のＩＤとパスワードを使用してなりすますことも可能である。
㋑　不特定多数の人に情報を伝達したり、逆に電子メールを受け取ることもできる。
㋒　時間的、地理的な制約がなく、広範囲なコミュニケーションが可能である。
㋓　ネットワーク上では物理的な場所は必要がない。
㋔　電子データは瞬時に抹消できる。

ⓑ　不正侵入とは

不正侵入は権限のないものがコンピュータシステムへ侵入する行為のことである。他人のＩＤやパスワード、システム上の弱点を悪用して不正にサーバにアクセスする。侵入されると、機密情報を盗まれたり、データを改ざん・消去されたり、別のコンピュータへの不正侵入の踏み台になったりする。ネットワークの利用の広範囲化と高度化に伴って、セキュリティが重要視されるようになり、ネットワークへの不正侵入が問題になっている。侵入検知ツールは不正な侵入を見つけた場合、管理者にアラームを発し、アクセスの遮断やシステムの復旧、侵入者の作業を記録するバックトレースを行う。

ⓒ　代表的なネットワークへの不正侵入の方法

㋐　他人へのなりすましの侵入

相手認証をパスワードで行う方式では、他人のパスワードを使用すると簡単になりすましによる侵入が可能となる。パスワードの類推、ソシアルエンジニアリング手法の利用によるシステム管理者へのなりすましによりパスワードの入手が可能になる。

㋑　セキュリティホールを利用した侵入

開発時のテストに利用した機能が残存した場合、管理者権限を使用して遠隔からプログラムの立ち上げが可能になる。セキュリティホールはプログラムの不具合によるセキュリティ上の弱点である。

㋒　外部からの攻撃

大量のデータを攻撃対象のサーバに送り込んで、正当な利用者にシステムを使わせなくする方法である。システムの機能を停止させてしまう。

ⓓ　不正アクセス対処法

㋐　パスワードを簡単に類推できないものにする。
㋑　ＩＤカードとパスワードを同時に使用する。
㋒　サーバプログラムをセキュリティホール対策済みのものを使用する。
㋓　ファイアウォールを設置する。
㋔　セキュリティ監視により、不正アクセスの兆候を早期に把握し、予防する。
㋕　暗号化によりデータを保護する。

②　アクセス管理

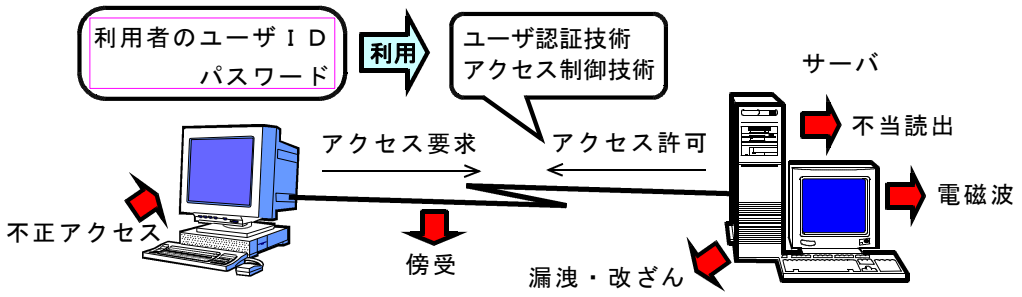
ⓐ　アクセス管理とは

アクセス管理はファイルやネットワークなどへのアクセスに関して、ユーザごとにアクセス権を与え、アクセス状況を管理することである。暗号化と並んで、情報への不当なアクセスを防止する直接的な対策である。システムの不正利用のリスクやユーザの誤操作によって発生するデータ消失などのリスクを防ぐために実施する。

アクセス管理を適切に行うためには、ユーザ認証技術、アクセス制御技術の二つの技術が必要である。ユーザ認証技術は、名乗ったユーザが本人であることを証明する本人確認技術である。アクセス制御は共有資源の利用を管理・制御する機能であり、アクセス制御技術は、それぞれのユーザがあらかじめ許可された権利以上のアクセスを防止する技術である。

ⓑ　アクセス権

アクセス権は、ユーザがコンピュータのファイルやネットワークなどの共有資源を利用するための権利のことであり、アクセスの禁止や読み取りの許可、書換・削除の許可など、ユーザごとに権利の設定を行う。アクセス制御は他人への成りすまし対策やセキュリティホール対策には無力である。



③　アクセス制御技術

ⓐ　アクセスのブロックする部位による分類

㋐　サブネットワークの入り口でのブロック

ファイアウォール技術で特定のネットワークへの不当な侵入を防止する。企業情報ネットワークとインターネットを接続し、その間で選択的にデータのやり取りを行う。

㋑　コンピュータの入り口でのブロック

不当な相手がコンピュータに入れなくするためのものである。相手からかかってきた通信を最初に一度切ってから、コールバックする方式である。

㋒　ファイルの入り口でのブロック

ファイルにアクセスできなくするためのものである。ファイル取り扱いの権利を設定し、その設定により権利のない主体の不正アクセスを制御することができる。

ⓑ　アクセスマトリックス

ユーザがあるファイルに対するアクセス要求を出すと、ＯＳはアクセスマトリックスを参照してそのアクセスが許されているか否かを調べる。許されているならばそのアクセスを実行させ、許されていないならばそのアクセスを行えないようにする。

ⓒ　アクセスマトリックスの設定・変更のやり方

㋐　任意アクセス制御

ユーザにアクセスマトリックスの任意の設定・変更を許す。

㋑　強制アクセス制御

ユーザにアクセスマトリックスの変更を許さない。システムが最初に決定したセキュリティ方針を守らせる。アクセスマトリックスを改ざんされにくいので、セキュリティレベルは高い。あらかじめ正しくアクセスマトリックスができていることが不可欠である。

④　オレンジブック

ⓐ　オレンジブックとは

オレンジブックはアクセス制御の機能レベルなどに関連するセキュリティの要求レベルを規準化したものである。米国の軍や政府が民間から製品を調達するために使用している。

ⓑ　セキュリティレベル

Ｄクラスは、セキュリティ機能がないシステムである。Ｃクラスは、任意アクセス制御の機能があるものが対応し、Ｃ１は正規のユーザかどうかが区別できるものであり、Ｃ２は個々の

ユーザを区別し、アクセス制御が個々のユーザに対して可能なものである。通常のオフィスで使用するシステムはＣクラスである。Ｂクラスは、強制アクセス制御が可能なものである。Ｂ１、Ｂ２、Ｂ３の３クラスからなり、後のものほどセキュリティレベルが高い。Ａクラスは、最もセキュリティレベルが高く、セキュリティ方針とシステムの設計が合致していることを数学的に証明する必要がある。

⑤　ユーザ管理

ⓐ　ユーザ管理とは

ユーザ管理は情報システムの利用者をユーザＩＤなどの識別子を用いて、ユーザの資源利用の実態把握やユーザの不当アクセス防止などの管理を行うことである。ユーザ管理を利用して、ユーザごとにファイルなどの共有資源へのアクセス権を設定し、管理する。障害時に影響されるユーザの迅速な把握、的確な情報提供を行うユーザ支援もユーザ管理の重要な一面である。

ユーザ管理を実施することにより、情報処理システムの信頼性、安全性、効率性および有用性を高め、設備計画の方向性の明確化、セキュリティ面の強化、障害対策の迅速化などの効果が期待される。

ⓑ　ユーザ管理の目的

㋐　資源利用の把握に活用し、合わせて発生する費用の配賦に使用する。
㋑　資源の将来的な設備増強など設備計画に活用する。
㋒　障害発生時に影響の及ぶユーザへ迅速な連絡に活用する。
㋓　利用権を持たない利用者を制限し、情報処理システムの安全性や、信頼性、性能維持の確保に利用する。
㋔　ユーザ支援の一貫として、情報処理システム広報作業など効率性向上のために利用する。

⑥　ユーザＩＤ

ⓐ　ユーザＩＤの付け方

㋐　英数字の組合せで構成されたものが一般的である。
㋑　個人単位のユーザに付与する。ユーザがどのような利用者であるかも体系づける。
㋒　先頭に利用者の作業内容を示す英字を付ける。
㋓　ユーザＩＤによるアクセス権を設定する。

ⓑ　ユーザＩＤの発行・停止

ユーザＩＤの発行・停止はシステム運用管理者によって管理される。ユーザＩＤは、ユーザからの申請に基づき、ＩＤを初期パスワードとセットで発行する。同時に、ユーザのアクセス権も要件に応じて設定される。ユーザは、システム管理者が発行した初期パスワードを独自のパスワードに変更する。

ⓒ　設定・発行・停止時の作業

㋐　ユーザＩＤ発行時のユーザ要件の確認
㋑　人事異動による利用制限の見直し
㋒　退職に伴う利用停止
㋓　定期的な利用状況の確認
㋔　ユーザへの使用指導

ⓓ　ユーザＩＤ発行時の確認項目

㋐　申請者の会社名・所属・氏名・連絡先・プロジェクト名
㋑　利用時間帯
㋒　利用目的
㋓　利用資源、使用量

ⓔ　承認・却下の決定

運用担当者が受付し、システム運用管理者が内容を確認し、承認・却下などを決定する。

ⓕ　ＩＤ発行の可否を決定する審査のポイント

㋐　申請者が以前にも登録申請を行っていないか。(二重登録の禁止)。
㋑　申請者が以前に不正使用などによるＩＤ抹消などの措置を受けていないか。
㋒　利用目的と利用資源が適合しているか(不要箇所へのアクセス禁止)
㋓　利用目的、ＩＤ利用者(責任者)が明確になっているか。
㋔　プロジェクト、組織単位で複数のＩＤ申請を提出した場合、複数申請の理由、利用方法、管理者が明確になっているか。

ⓖ　ユーザＩＤの管理

システム管理者は発行後もユーザＩＤの管理が必要となる。定期的にユーザＩＤの有効性管理を実施する必要がある。過去に情報処理システムを利用していたユーザが過去使用していたユーザＩＤを利用してアクセスすることが考えられる。

ユーザＩＤの管理内容は次の通りである。

㋐　ユーザＩＤの利用期限の設定

利用期限を設定し、期限切れの場合は再度利用申請を行わせる規定を設ける。１年間程度の有効期限を設定し定期更新と併せて更新申請を受け付ける。

㋑　一定期間未使用ユーザのアクセス権停止

一定期間、一度も情報処理システムへアクセスしていないユーザに利用停止措置を行う。利用停止措置を受けたユーザは新たにユーザＩＤの利用承認を受けることとする。

㋒　認証エラーの回数によるアクセス権停止

ユーザが情報処理システムを利用する場合、ユーザＩＤの他にパスワードを入力し、ユーザ認証を行う。このとき何度もパスワードを間違えるということは、ユーザ以外の人間による不正アクセスと考えられるので、一定回数以上の認証エラーの検出をしたユーザＩＤへは停止措置を行う。この保護対策は銀行などの現金自動支払機（ＣＤ）システムなどで利用されている。

⑦　パスワード

ⓐ　パスワードとは

パスワードはコンピュータで利用者の認証を行うために利用される数字や文字列である。利用制限を行っているコンピュータや共有資源では、ユーザＩＤとパスワードによって利用者であることを認証する。ユーザＩＤの保有者自身が実際にアクセスしているかどうかを確認するために利用する。正当な利用者以外にパスワードを漏洩したり、推測しやすいパスワードを設定すると、悪意ある第三者による不正利用の恐れがある。パスワードの発行はユーザＩＤの発行手続きと同様な方法をとる。

ⓑ　パスワード設定上の留意点

㋐　パスワード入力の際にパスワード自体の表示や印字を抑止する。
㋑　パスワードの有効期限を設定する。
㋒　利用者が自分のパスワードをいつでも自由に変更できるようにする。
㋓　パスワードを暗号化してファイル上に格納する。
㋔　パスワードを保存するパスワードファイルのアクセスを制限する。
㋕　高度パスワードを適用し、類推できるようなパスワードの使用を制限する。
㋖　初期パスワードの設定をする。
㋗　初期パスワードは、初回だけ仮パスワードで情報処理システムへアクセスを許し、ファイルアクセス前にユーザ側で正式のパスワードに変更しなければならない方法にする。

⑧　ユーザＩＤとパスワードの管理機能

ⓐ　セキュリティ監視

ユーザＩＤとパスワードの管理の機能を利用して、システム運用管理者はユーザの認証などセキュリティ監視を強化する。ユーザＩＤとパスワードのセキュリティ管理プログラムを作成し、管理する仕組みを作り上げることが必要となる。

ⓑ　セキュリティ管理プログラムの機能

㋐　ユーザＩＤの登録／削除機能
㋑　ユーザＩＤに対する認証情報の管理機能
**　　ユーザ名、所属部署、連絡先、有効期限など**
㋒　ユーザＩＤに対する認証チェック機能
㋓　パスワードの登録／変更機能
㋔　パスワードに対する認証チェック機能
㋕　最終アクセス日時の管理機能

例題演習

インターネット利用時のセキュリティ確保に関する記述のうち，適切なものはどれか。

ア　インターネットを経由してデータベースサーバを利用する場合，データベースへの不正アクセスやデータの改ざんを防止する対策も必要となる。
イ　インターネットを利用して電子メールを送る場合，暗号化を行えば，電子メールの到達確認ができる。
ウ　インターネットを利用するには，利用者認証システムに登録する必要がある。
エ　社内電子メールシステムをインターネットで社外と接続しても，ファイアウォールを導入すれば，社内からの重要情報の流出は自動的に防止できる。

解答解説

インターネットのセキュリティに関する問題である。

アのデータベースサーバを利用する場合に不正アクセスの防止やデータの改ざん対策が必要になる。求める答えはアとなる。

イの暗号化は、第三者へ内容が漏洩しないようにするために、ある一定の規則に従ってデータを変換することである。暗号化は電子メールの到達確認とは異なる。

ウの利用者認証システムは、ネットワーク経由でコンピュータにアクセスしてくるユーザーが登録済みか否かを信頼できる方法で確認するソフトウエアである。中心部分は認証サーバと呼ぶソフトウエアで、ユーザーの名前やパスワードなどを一括管理する。インターネットを利用するためには必ずしも必要としない。個人ユーザがプロバイダーと契約してインターネット

を利用する場合には、プロバイダーのシステムを経由するために認証が必要になるだけである。

エのファイアウォールは、インターネットとＬＡＮとの間に置くことでデータ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを守る仕組みである。ファイアウォールを設置しても社内からの重要情報の流出を自動的に防止できない。

例題演習

コンピュータシステムに対する利用者の利用資格の正当性チェックと利用状況の把握を行う目的で，利用者に付与される情報を表す用語として，適切なものはどれか。

ア　ＩＰアドレス　　イ　アクセス権
ウ　パスワード　　エ　ユーザＩＤ

解答解説

ユーザＩＤに関する問題である。

アのＩＰアドレスは、ＴＣＰ／ＩＰで通信する場合、通信元や通信先を識別するためのアドレスである。

イのアクセス権はデータやプログラムを読み書きし、利用することを認めた権利である。

ウのパスワードは正当なユーザ本人かどうかを確認するための合い言葉である。

エのユーザＩＤはコンピュータの利用時に許可されているユーザを認識するために個々のユーザに与えられた番号であり、英字と数字が用いられる。システムへのアクセス権を判断するのに利用したり、使用実績の把握に用いる。求める答えはエとなる。

例題演習

コンピュータセキュリティ対策に関する記述のうち，適切なものはどれか。

ア　一時記憶領域に残っている機密データは，ジョブ終了時に確実に消去する。
イ　金利計算処理などで，端数を特定口座に振り込む，いわゆるサラミ技術に対しては，データにチェックディジットを付加する。
ウ　端末から入力された数値データの改ざんに対しては，仮想記憶領域のページ又はセグメント単位に割り付けられた記憶保護キーによって，保護のレベルを変える。
エ　ユーティリティプログラムを使用したデータ改ざんに対しては，そのユーティリティプログラムのバックアップをとっておき，元のプログラムと比較する。

解答解説

コンピュータセキュリティ対策に関する問題である。

アの記憶領域に残っている機密データはジョブ終了時に確実に消去することはセキュリティ対策として重要である。求める答えはアとなる。

イのデータにチェックディジットを付加することは入力データのチェックには役立つがサラミ技術などの犯罪の防止対策にはならない。

ウの仮想記憶領域のページまたはセグメント単位に割り付けられた記憶保護キーの保護レベ

ルの変更は、改ざんは実記憶域の主記憶で行われるためセキュリティ対策にはならない。

エの内容のユーティリティプログラムのバックアップをとっておき、元のプログラムとの変化が分かっても、データの改ざんを防止できることにはならない。

例題演習

ユーザＩＤの管理について、最も適切なものはどれか。

ア　同じプロジェクトに参加している利用者は、みな同じユーザＩＤを用いる。
イ　複数のユーザＩＤをもつ利用者は、すべてのＩＤに対して同じパスワードを設定する。
ウ　ユーザＩＤに権限を設定する場合は、必要最小限なものにする。
エ　ユーザＩＤの抹消は、廃止の届出後、十分な期間をおいてから行う。

解答解説

ユーザＩＤ管理に関する問題である。

アのプロジェクトで皆同じユーザＩＤを用いるのは間違いで、個人単位に付与する。個人の識別子を用いて、ユーザの資源の実態把握と不当アクセス防止などの管理をする。

イの同一人が複数のＩＤカードをもつのは管理上不合理になる。アクセス権の設定もどのユーザＩＤに付与するのか不明確になる。

ウのユーザＩＤの権限を設定する場合、権限は必要最小限のものにし、利用目的、利用期限を明確にする。求める答えはウとなる。

エのユーザＩＤの抹消は、利用目的が完了した時点で直ちに抹消する必要がある。

例題演習

コンピュータシステムにおけるパスワード運用管理方法として、適切なものはどれか。

ア　トラブル処理を迅速化するために、ユーザＩＤとパスワードの一覧表を作成し、管理者しか分からないように隠す。
イ　利用者が自分のパスワードをいつでも自由に変更できるようにする。
ウ　利用者管理作業を簡素化するために、現在使用されていないユーザＩＤとパスワードを再利用する。
エ　利用者登録申請書が届く前に、新任者の人事異動速報を見てユーザＩＤと仮のパスワードを登録する。

解答解説

パスワード運用方法に関する問題である。

アは、パスワードは本人のみが認識でき、変更できるもので、管理者でも、他人のユーザＩＤとパスワードの一覧表を作成し、いつでも確認できるようにすることは誤りである。

イの利用者がいつでも変更できるようにすることは正しい。求める答えはイとなる。

ウの現在利用されていないユーザＩＤとパスワードの再利用は、不正アクセスや情報処理システムの破壊などのトラブルの原因になる。従って、使用停止処理を必ず行う必要がある。

エの利用者登録申請書が到着する前に、ユーザＩＤや仮のパスワードを登録することは間違いである。

例題演習

公衆回線を利用しているコンピュータシステムで、セキュリティの面から適切な運用方法はどれか。

ア　あらかじめ定められたパスワードの変更を禁止する。
イ　接続要求があった場合、特定の電話番号にコールバックして接続する。
ウ　パスワードはユーザが確認できるように、ログイン時に端末に表示する。
エ　パスワードをあらかじめ定めた回数間違えて入力した場合、パスワードを通知する。

解答解説

ユーザ認証の問題である。

アのパスワードの変更は、有効期限を設定し、絶えず変更する必要がある。

イのコールバックは本人であるかどうかの認証方法の一つて、折り返し電話をすることで本人確認をする方法である。ユーザ認証の１つの方法である。求める答えはイとなる。

ウのユーザがパスワードを確認できるように端末に表示するのは誤りで、パスワードの表示や印字は行ってはならない。

エの一定回数間違ったからといって、親切に相手に通知するのは誤りである。

例題演習

ディレクトリに，読取り，更新，配下のファイル作成のアクセス権を設定できるＯＳがある。この３種類のアクセス権は，それぞれに１ビットを使って許可，不許可を設定する。この３ビットを８進数表現０～７の数字で設定するとき，次の試行結果から考えて，適切な記述はどれか。

〔試行結果〕
①　０を設定したら，一切のアクセスができなくなってしまった。
②　３を設定したら，読取りと更新はできたが，作成ができなかった。
③　７を設定したら，すべてのアクセスができるようになった。

ア　２を設定すると，読取りと作成ができる。
イ　４を設定すると，作成だけができる。
ウ　５を設定すると，更新だけができる。
エ　６を設定すると，読取りと更新ができる。

解答解説

アクセス権設定に関する問題である。

３ビットで読取り、更新、作成のアクセス権を設定する。

① ０００はすべてのアクセス権を許可しない。
② ０１１は読取り、更新ができ、作成ができない。
③ １１１はすべてのアクセスが可能になる。
④ 以上の内容からアクセス権の設定は、作成・読取り・更新、または作成・更新・読取りになる。

アは、０１０となり、作成はできない。
イは、１００となり、作成だけができる。求める答えはイとなる。
ウは、１０１となり、作成と更新、または作成と読取りになる。
エは、１１０となり、作成と更新、または作成と読取りになる。

例題演習

画像などのディジタルコンテンツが，不正にコピーされて転売されたものであるかを判別できる対策はどれか。

ア　タイムスタンプ　　イ　電子透かし
ウ　電子保存　　エ　配達証明

解答解説

電子透かしに関する問題である。
アのタイムスタンプは、ファイルなどの電子データにおいて、その作成や更新などが行われた日時を示す情報である。
イの電子透かしは、音声や画像などの電子化されたコンテンツに対して、品質を落とさず利用者に分からない方法で著作権情報を記録する仕組みである。求める答えはイとなる。
ウの電子保存は、情報を電子媒体に保存することである。
エの配達証明は、一般書留とした郵便物や荷物を配達した事実を証明するサービスである。

例題演習

複数の業務システムがある場合のアクセス管理の方法として，最も適切なものはどれか。

ア　業務の担当変更に迅速に対応するために，業務グループごとに共通の利用者ＩＤを使用する。
イ　人事異動が頻繁に発生する場合には，年初にまとめてアクセス権限の変更を行う。
ウ　新入社員の名簿に基づいて，あらかじめ全業務システムに全員の利用者登録を実施しておく。
エ　利用者の職位権限にかかわらず，業務システムごとに適切なアクセス権限の設定を行う。

解答解説

アクセス管理に関する問題である。
アの利用者ＩＤは利用者個人に対して発行するものである。
イのアクセス権の設定は人事異動など必要が発生する度に変更し、発行するものである。

ウの利用者ＩＤの発行は本人の申請に基づいて、担当の業務に関連して発行する。

エの利用者の職務権限に関係なく、業務システムごとにアクセス権を設定するは適切である。求める答えはエとなる。

例題演習

企業内ネットワークやサーバにおいて，侵入者が通常のアクセス経路以外で侵入するために組み込むものはどれか。

ア　シンクライアントエージェント　　イ　ストリクトルーティング
ウ　バックドア　　エ　フォレンジック

解答解説

バックドアに関する問題である。

アのシンクライアントエージェントは、機能を絞ったクライアント用コンピュータのことで、サーバ側でアプリケーションソフトやファイルなどの資源を管理するシステムである。

イのストリクトルーティングは、送信元からあて先までに経由するルーターのＩＰアドレス・リストを，送信元のルーターがすべて指定し，その順番通りにパケットを送信することである。

ウのバックドアは、ＩＤやパスワードを使って通信を制限したり、使用権を確認するコンピュータの機能を無許可で利用するために、コンピュータ内に設けられた通信接続の機能を指す。バックドアには、設計・開発段階で盛り込まれるものや稼動中のコンピュータに存在するセキュリティホールを使って送り込まれたソフトウェアである。求める答えはウである。

エのフォレンジックは、証拠として使えるように，コンピュータ内やネットワーク上にあるディジタル・データを収集・分析・保存することである。

例題演習

利用者認証に用いられるＩＣカードの適切な運用はどれか。

ア　ＩＣカードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通なＰＩＮを設定する。
イ　ＩＣカードの表面に刻印してある数字情報を組み合わせて，ＰＩＮを設定する。
ウ　ＩＣカード紛失時には，新たなＩＣカードを発行し，ＰＩＮを設定した後で，紛失したＩＣカードの失効処理を行う。
エ　ＩＣカードを配送する場合には，ＰＩＮを同封せず，別経路で利用者に知らせる。

解答解説

ＩＣカードの暗証番号に関する問題である。

利用者認証を行うには、ＩＣカードのユーザＩＤとそのカードを使用しているのが本人であることを確認する暗証番号が必要である。

ＰＩＮコードは、クレジットカードやキャッシュカードの利用に際し持ち主の本人確認のた

めに使われる、秘密の識別番号である。カードを提示した人物が所有者本人であることを確認するために照合される番号で、他人に知られると成りすまして悪用される恐れがあるため、秘密にして暗誦しなければならない。銀行のキャッシュカードなど、多くの場合に４桁の番号が使われる。

アの共通な暗証番号の設定では本人確認は不可能である。

イのＩＣカードの表面に印字している数字情報を組み合わせて暗証番号を作成すると、第三者が推測可能な番号となり、本人確認の機能にはならない。

ウの失効処理の順序が逆である。

エのＩＣカードを配送する場合には暗証番号は同封しない。暗証番号の配送が必要な場合は別経路で配送する。求める答えはエとなる。

例題演習

パスワードを用いて利用者を認証する方法のうち，適切なものはどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

イ　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。

ウ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。

解答解説

パスワードを用いた利用者認証に関する問題である。

利用者認証は、相手が本当の相手であることを確認する手段であり、単純な方式では、利用者ＩＤとパスワードを組み合わせて利用する。その際、パスワードの盗難防止の目的で、パスワードをハッシュ値に変化して使用する。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して登録し、認証時に入力されたパスワードをハッシュ関数で変換して比較しても利用者認証にはならない。

イの利用者ＩＤをハッシュ関数で変換して登録し、認証時に入力された利用者ＩＤをハッシュ関数で変換しても、本人の確認は不十分である。

ウのパスワードをハッシュ関数で変換して登録し、認証時に入力されたパスワードをハッシュ関数で変換し、比較すると本人の確認は可能である。求める答えはウとなる。

エのパスワードをハッシュ関数で変換して登録し、認証時に入力された利用者ＩＤをハッシ

ュ関数で変換しても、本人の確認は不十分である。

例題演習

入力パスワードと登録パスワードを用いて利用者を認証する方法において，パスワードファイルへの不正アクセスによる登録パスワードの盗用防止策はどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して参照した登録パスワードと入力パスワードを比較する。
イ　パスワードをそのまま登録したファイルを圧縮しておき，認証時に復元して，入力されたパスワードと比較する。
ウ　パスワードをそのまま登録しておき，認証時に入力されたパスワードと登録内容をともにハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

解答解説

パスワードの盗難防止に関する問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して、登録パスワードをそのまま保管していると、盗難時には、パスワードがそのまま使用されることになる。

イのパスワードファイルを圧縮して保管していても、復元すればパスワードを知ることができるため無意味である。

ウのパスワードをそのまま登録していると、ファイルの盗難時にパスワードの内容がそのまま相手に知られてしまう。

エのパスワードをハッシュ関数を使用して、ハッシュ値を求めていると、ファイルを盗まれても直ちに内容が相手に分かることがない。