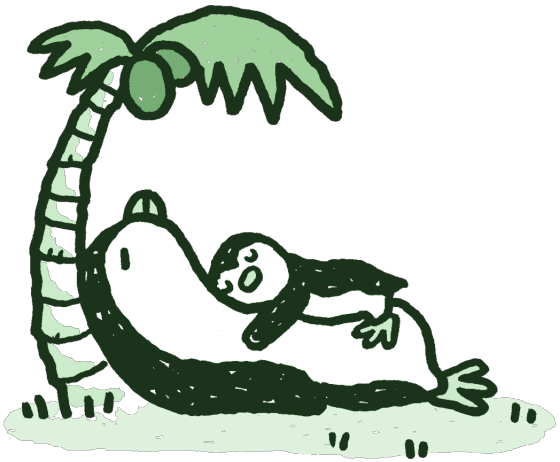
セキュリティ



★ ★ ★

9-1 情報セキュリティ

●情報セキュリティとは

アドレス帳に登録された連絡先のデータや、Webサイトにログインしたときのパスワード、ネットショッピングをするときに入力したクレジットカードのデータなど、これらのデータはすべて、大事な**情報資産**であり、なくしてしまったり、盗まれて悪用されたりすると大変です。そのため、さまざまな対策をして守らなければなりません。これを**情報セキュリティ**といいます。情報セキュリティとは、情報資産の**機密性**、**完全性**、**可用性**を維持することです。

●機密性

情報を不正アクセスから守り、第三者への情報漏えいをなくすことです。データの暗号化などの技術により向上させることができます。

●完全性

情報が作られたときから、書き換えられたり欠けていない、完全で正しいことです。ディジタル署名などの技術により向上させることができます。

●可用性

利用者が必要なときに情報資産を使えることです。定期バックアップなどで向上させることができます。

電子透かし

画像、音声、動画等のディジタルコンテンツに情報を埋め込む技術です。作者名、課金情報、コピー可能回数といった情報を埋め込むことにより、不正コピーやデータの改ざんを判別することができます。

平成26年春試験から、午前試験では情報セキュリティ分野の出題比率が高くなりました。また午後試験では同分野が選択問題から必須問題に変更になっています。

●情報資産における脅威（きょうい）

情報セキュリティ対策を行うには、まず情報資産が、どのような脅威にさらされているのかをきちんと把握する必要があります。情報がさらされている脅威には、**技術的脅威**、**人的（じんてき）脅威**、**物理的脅威**の３種類があります。

●技術的脅威

コンピュータ技術を使った脅威を**技術的脅威**といいます。技術的脅威は、不正アクセスやコンピュータウイルスをはじめ、さまざまな手口や攻撃があります。

・フィッシング

銀行などを装った偽（にせ）のWebサイトを作り、URLを載せた電子メールを送り、ユーザにアクセスさせて暗証番号やパスワードをだまし取ることを**フィッシング**といいます。

・DNSキャッシュポイズニング

PCが参照するDNSサーバに誤ったドメイン管理情報を覚え込ませて、偽のサーバに誘導する攻撃を**DNSキャッシュポイズニング**といいます。

・SQLインジェクション

Webアプリケーション上で悪意のある問合せや操作を行う命令文を入力して，データベースのデータを改ざんしたり不正に取得したりする攻撃を**SQLインジェクション**といいます。この攻撃を防ぐためには、入力中の文字が、データベースへの問合せや操作において特別な意味をもつ文字として解釈されないように無効化します。

・**DoS（ドス）攻撃**

サーバに大量のデータを送信し、サーバの機能を停止させる攻撃をDoS攻撃といいます。

・**ディレクトリトラバーサル攻撃**

管理者が意図していないパスでWebサーバ内のファイルを指定し、許可されていないファイルを不正に閲覧する攻撃をディレクトリトラバーサル攻撃といいます。

・**Webビーコン**

Web ページなどに小さい画像を埋め込み、ユーザのアクセス動向などの情報を収集する仕組みのことを、Webビーコンといいます。

・**キーロガーの悪用**

キーロガーは、もともと利用者をサポートするために、キーボード入力を監視して記録するソフトウェアです。こっそりパソコンに仕掛けて、ネットバンキング利用時に、利用者が入力したパスワードを収集するなど悪用の手口として使われます。

用語

[電子透かし]：情報を埋め込むことにより、不正コピーやデータの改ざんを判別する
[フィッシング]：偽のサイトにアクセスさせて情報を盗む
[DNSキャッシュポイズニング]：DNSサーバに誤ったドメイン管理情報を覚え込ませて偽サーバに誘導
[SQLインジェクション]：Webアプリケーション上で悪意のあるSQL文を入力してデータベースのデータを改ざん、不正に取得
[DoS攻撃]：大量のデータを送りつけてサーバの機能を停止させる
[ディレクトリトラバーサル攻撃]：管理者が許可していないパスで、Webサーバ内のファイルに不正アクセス
[Webビーコン]：小さい画像を埋め込み、アクセス動向を収集する

用 語

［キーロガー］：パソコンに仕掛けて入力パスワードを収集し悪用

●人的脅威

「人」が原因である脅威を**人的脅威**といいます。コンピュータの置き忘れや操作ミスなど、情報のもち主のうっかりミスによるものや、内部関係者が意図的に情報を漏えいしたりすることがこれに当たります。

・ソーシャルエンジニアリング

システム管理者などを装って、利用者に問い合わせてパスワードを聞き出したり、緊急事態を装って組織内部の機密情報を聞き出したりするなど、人間の心理の隙をついて情報を盗む行為を**ソーシャルエンジニアリング**といいます。

・なりすまし

盗んだIDやパスワードなどを使い、ネットワーク上でその人のふりをすることを**なりすまし**といいます。なりすましによって、情報を盗んだり、他人に迷惑な行動をしたりします。

・サラミ法

不正行為が表面化しない程度に、多数の資産から少しずつ詐取する方法を**サラミ法**といいます。

●物理的脅威

大雨や地震、落雷などの災害、またはコンピュータの故障など、コンピュータが物理的に損害を受けて情報を失う脅威を**物理的脅威**といいます。空き巣によるコンピュータの盗難や破壊などもこれに当たります。

用 語

［ソーシャルエンジニアリング］：人間の心理の隙をついて機密情報を聞き出す

［サラミ法］：表面化しない程度に、多数の資産から少しずつ詐取

●リスクアセスメント

これまで説明してきたようなさまざまな脅威が発生する可能性のことを、**リスク**といいます。情報資産に対するリスクを洗い出し、リスクによって発生する可能性のある損害を明らかにした上でリスク対応を策定する一連のプロセスを**リスクアセスメント**といいます。分析によって得られた損失額と発生確率から、リスク発生時の被害の大きさを評価し、優先度をつけて対応を検討します。

リスク対策には、次のような対応方法があります。

〈リスク対策の種類〉

種別	内容	例
リスク回避	リスクの原因を排除すること。損失額が大きく発生率の高いリスクに対して行う対策	個人情報の破棄、Web公開の停止など
リスク移転（リスク共有）	リスクを他者に肩代わりしてもらうこと。損失額が大きく発生率の低いリスクに対して行う対策	保険への加入など
リスク軽減	リスクによる損失を許容範囲内に軽減させること。損失額が小さく発生率は高いリスクに対して行う対策	情報の暗号化など
リスク保有	対策を講じないでリスクをそのままにしておくこと。損失額も発生率も小さいリスクに対して行う対策	

用語

［リスクアセスメント］：予測リスクを洗い出し評価・分析。損失額と発生確率に応じて、対応を優先順位付け

スキル

→リスクの種別とそれぞれの事例について、答えられるようにしておこう。

●情報セキュリティマネジメントシステム

情報セキュリティを維持するためには、企業などが情報を適切に管理し、機密を守るための仕組みを確立し、継続的な改善をしていくことが必要です。この仕組みを、**情報セキュリティマネジメントシステム**または**ISMS**（Information Security Management System）といいます。

ISMS確立の手順は、おおよそ次のような流れで行います。

①リスクの分析と評価

②リスク対応のための管理目的および管理策の選択

③適用宣言書の作成

スキル

→ISMS確立の手順について、分析→評価→対応策の決定→宣言というおおまかな流れを覚えておこう。

●情報漏えいを防ぐ方法

情報漏えいを防ぐためには、機密情報を適切に取り扱う必要があります。具体的な対策として、次のような方法があります。

●機密ファイルをノート型PCに入れて持ち歩く場合

機密ファイルをノート型PCに入れて持ち歩く場合、盗難や紛失のリスクがあるため、ハードディスクの内容を暗号化することで情報漏えいを防ぎます。

●機密ファイルを廃棄する場合

機密ファイルが保存されたパソコンを産業廃棄物処理業者に引き渡して廃棄する場合、磁気ディスクの全領域を複数回上書きするなど、データを完全に消去する必要があります。

●機密ファイルをメールで送信する場合

機密ファイルにパスワードを設定してメール添付する場合、パスワードはそのメールには記載せず、別の手段で相手に伝えるようにします。宛先を間違えて機密ファイルが誤送信された場合にも、情報漏えいを防ぐことができます。

スキル

→情報漏えいを防ぐための具体的な方法を覚えておこう。

試験にチャレンジ

基本情報技術者試験　平成27年春

SQLインジェクション攻撃の説明はどれか。

ア：Webアプリケーションに問題があるとき、悪意のある問合せや操作を行う命令文を入力して、データベースのデータを不正に取得したり改ざんしたりする攻撃

イ：悪意のあるスクリプトを埋め込んだWebページを訪問者に閲覧させて、別のWebサイトで、その訪問者が意図しない操作を行わせる攻撃

ウ：市販されているDBMSの脆弱性を利用することによって、宿主となるデータベースサーバを探して自己伝染を繰り返し、インターネットのトラフィックを急増させる攻撃

エ：訪問者の入力データをそのまま画面に表示するWebサイトに対して、悪意のあるスクリプトを埋め込んだ入力データを送ることによって、訪問者のブラウザで実行させる攻撃

解説　SQLインジェクションは、Webアプリケーション上で悪意のあるSQL文を入力してデータベースのデータを改ざん、不正に取得する攻撃です。　解答：ア

試験にチャレンジ

基本情報技術者試験　平成26年春

情報セキュリティにおける“完全性”を脅かす攻撃はどれか。

ア：Webページの改ざん

イ：システム内に保管されているデータの不正コピー

ウ：システムを過負荷状態にするDoS攻撃

エ：通信内容の盗聴

解説　完全性とは、情報が書き換えられたり欠けていない状態です。Webページの改ざんは、完全性を脅かす攻撃です。　解答：ア

試験にチャレンジ

基本情報技術者試験　平成25年秋

リスク共有（リスク移転）に該当するものはどれか。

ア：損失の発生率を低下させること
イ：保険への加入などで、他者との間でリスクを分散すること
ウ：リスクの原因を除去すること
エ：リスクを扱いやすい単位に分解するか集約すること

解説 リスク共有は、リスクを他者と共有し分散することです。

解答：イ

試験にチャレンジ

基本情報技術者試験　平成26年秋

情報漏えい対策に該当するものはどれか。

ア：送信するデータにチェックサムを付加する。
イ：データが保存されるハードディスクをミラーリングする。
ウ：データのバックアップ媒体のコピーを遠隔地に保管する。
エ：ノート型 PC のハードディスクの内容を暗号化する。

解説 ノート型PCは盗難や紛失のリスクが高いため、ハードディスクの内容を暗号化することで情報漏えいを防ぎます。

解答：エ

★ ★ ★

9-2 コンピュータウイルス

●コンピュータウイルスとは

コンピュータウイルスは、経済産業省が定めた**コンピュータウイルス対策基準**において、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を１つ以上有するもの」と定義されています。

〈コンピュータウイルスの３機能〉

①自分自身をほかのプログラムにコピーし伝染させる「自己伝染機能」
②特定の日時や処理回数に至るまで症状を出さない「潜伏機能」
③ファイルの破壊や、設計者の意図しない動作をする「発病機能」

マルウェア
近年では、この定義に当てはまらないさまざまな種類のウイルスが増えてきたため、悪意のあるソフトウェア全般を**マルウェア**と呼びます。

●コンピュータウイルスの種類

コンピュータウイルスには、次のようなものがあります。

〈コンピュータウイルスの種類〉

種類	特徴
マクロ型ウイルス	ワープロソフトや表計算ソフトなどのマクロ機能を使って感染するウイルス。ファイルを開くだけで感染
ファイル感染型ウイルス	拡張子com、exe、sysなどの実行型ファイルに感染するウイルス。感染プログラムを実行することで感染
システム領域感染型ウイルス	コンピュータ起動時、最初に読み込まれるシステム領域（ブートセクタなど）に感染するウイルス。コンピュータを起動することで感染

種類	特徴
トロイの木馬	何も問題のない普通のソフトを装ってコンピュータに侵入し、データの破壊や改ざん、ファイルの外部流出などを行うウイルス。自己増殖することはない
ワーム型ウイルス	単独で動作し、ネットワーク経由で他のコンピュータに入り込んで自己増殖していくウイルス

用語

［トロイの木馬］：普通のソフトを装ってコンピュータに侵入。データの破壊や改ざんなどを行う

●コンピュータウイルスへの対策

コンピュータウイルスに対する予防･検知･感染後の対応についても､「コンピュータウイルス対策基準」にまとめられています。

●ウイルスの予防

ウイルスの感染源は、主に電子メールとWebサイトです。電子メールによる感染を防ぐには、知らない人から送られてきた添付ファイルをむやみに開かないことが重要です。Webサイトの閲覧による感染を防ぐには、ブラウザに怪しいWebサイトは表示しない設定をしておくなどの対策方法があります。また、PCの脆弱(ぜい)性を突いて感染しないように、OSやアプリケーションの修正パッチを適切に適用します。

●ウイルスの検知

コンピュータには、必ずウイルス対策ソフトをインストールしておきます。ウイルス対策ソフトは、既知ウイルスの情報（シグネチャコード）をウイルス定義ファイルとしてもっていて、これと比較してウイルスの検知・駆除(くじょ)を行います。これを、パターンマッチング方式といいます。ウイルスは毎日新しい種類のものが作られているので、最新のウイルスにも対応できるよう、ウイルス定義ファイルは定期的に更新する必要があります。

●感染後の対応

ウイルスに感染してしまったら、コンピュータをすぐにネットワークから切り離すことが重要です。これは、ネットワークを通じてさらに感染を広げてしまうなど、被害の拡大を防ぐためです。

逆アセンブル

新種ウイルスの動作を解明するのに有効な手法として、**逆アセンブル**があります。バイナリコードからソースコードに変換することで、新種ウイルスの動作を解明します。

用語

[パターンマッチング方式]：既知ウイルス情報（シグネチャコード）を使用して、対象ファイルと比較しウイルスを検出

スキル

→ウイルス（マルウェア）対策について、適切な方法を覚えておこう。

試験にチャレンジ

基本情報技術者試験　平成25年秋

クライアントPCで行うマルウェア対策のうち、適切なものはどれか。

ア：PCにおけるウイルスの定期的な手動検査では、ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。

イ：ウイルスが PC の脆弱(ぜいじゃく)性を突いて感染しないように、OS 及びアプリケーションの修正パッチを適切に適用する。

ウ：電子メールに添付されたウイルスに感染しないように、使用しないTCPポート宛ての通信を禁止する。

エ：ワームが侵入しないように、クライアントPCに動的グローバルIPアドレスを付与する。

解説 定義ファイルの更新後は、すべてのファイルをスキャンする必要があるため、アは誤り。使用しないTCPポート宛ての通信を禁止しても、メールの内容をチェックできずウイルス感染を防止できないので、ウも誤り。クライアントPCに動的グローバルIPアドレスを付与しても、ワームの侵入は防止できないためエも誤り。　解答：イ

試験にチャレンジ

基本情報技術者試験　平成20年秋

データの破壊、改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールさせ、実行させるものはどれか。

ア：DoS攻撃
イ：辞書攻撃
ウ：トロイの木馬
エ：バッファオーバフロー攻撃

解説 キーワードは「データの破壊、改ざんなどの不正な機能」「プログラムの一部に組み込んだ」です。　解答：ウ

試験にチャレンジ

基本情報技術者試験　平成26年秋

ウイルス対策ソフトのパターンマッチング方式を説明したものはどれか。

ア：感染前のファイルと感染後のファイルを比較し、ファイルに変更が加わったかどうかを調べてウイルスを検出する。
イ：既知ウイルスのシグネチャと比較して、ウイルスを検出する。
ウ：システム内でのウイルスに起因する異常現象を監視することによって、ウイルスを検出する。
エ：ファイルのチェックサムと照合して、ウイルスを検出する。

解説 パターンマッチング方式は、既知ウイルス情報を使用して、対象のファイルと比較してウイルスを検出します。シグネチャは、コンピュータウイルスの情報やパターンです。　解答：イ

★ ★ ★

9-3 暗号化と認証

●データの暗号化

暗号化とは、その名のとおり、データを第三者には解読できない「暗号文」に変換することです。暗号化することによって、たとえ通信中にデータが他の人に盗まれてしまっても、データの内容を知られることはありません。暗号化したデータを元に戻すことを復号といいます。

暗号化と復号には、それぞれ鍵を使ってデータを変換します。鍵とは、データを変換するための特別なデータです。この鍵の違いによって、さまざまな暗号方式があります。

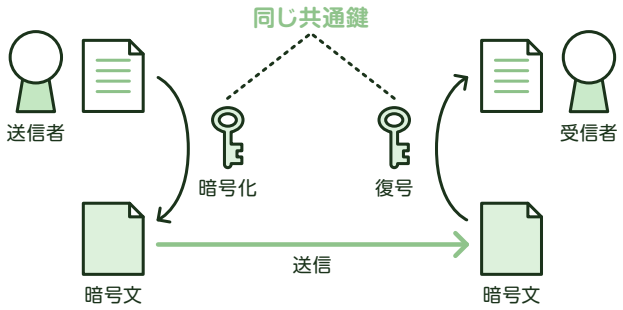
●共通鍵暗号方式

暗号化と復号に同じ鍵を使う暗号方式を共通鍵暗号方式といいます。データの送信者と受信者が同じ共通鍵をもっている必要があります。鍵はあらかじめ送信者から受信者へ配布しておきますが、鍵を盗まれてしまうと誰でも復号できてしまうので、鍵の受け渡しには注意が必要です。

共通鍵暗号方式は、暗号化と復号の処理が速いのが特徴です。しかし、データを送る相手の数だけ鍵を作成する必要があるので、不特定多数の人にデータを送るときには不向きです。

代表的な共通鍵暗号方式には、DES（ディーイーエス）やAES（エーイーエス）などがあります。

〈共通鍵暗号方式〉



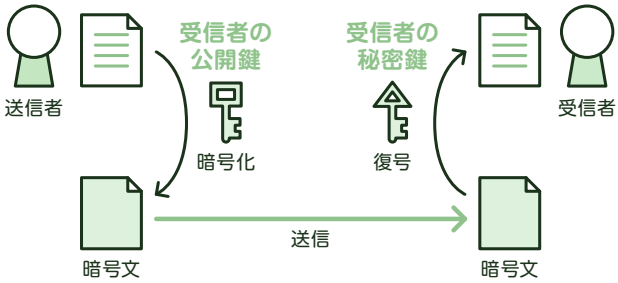
●公開鍵暗号方式

暗号化するときと復号するときに、それぞれ対になる2つの鍵を使う暗号方式を**公開鍵暗号方式**といいます。受信者は、あらかじめ暗号化に使う**公開鍵**をインターネットなどで公開しておき、送信者はその鍵を使ってデータを暗号化します。復号は、受信者がもっている**秘密鍵**で行います。公開鍵は公開してもかまいませんが、秘密鍵は受信者以外には知られないようにしなくてはなりません。

鍵を公開しているので、不特定多数の相手からデータを受け取るのに向いていますが、暗号化と復号の処理に時間がかかるという短所があります。

代表的な公開鍵暗号方式には、巨大な数の素因数分解の困難さを利用したRSA（アールエスエー）や楕円曲線（だえん）暗号などがあります。

〈公開鍵暗号方式〉



試験問題では、暗号化するときに使う鍵を暗号化鍵、復号に使う鍵を復号鍵と表記しています。公開鍵暗号方式では、暗号化鍵＝受信者の公開鍵、復号鍵＝受信者の秘密鍵となります。

用語

［共通鍵暗号方式］：同じ鍵（共通鍵）で暗号化・復号を行う

［公開鍵暗号方式］：受信者の公開鍵で暗号化し、秘密鍵で復号する

［RSA］：巨大な数の素因数分解の困難さを利用した公開鍵暗号方式

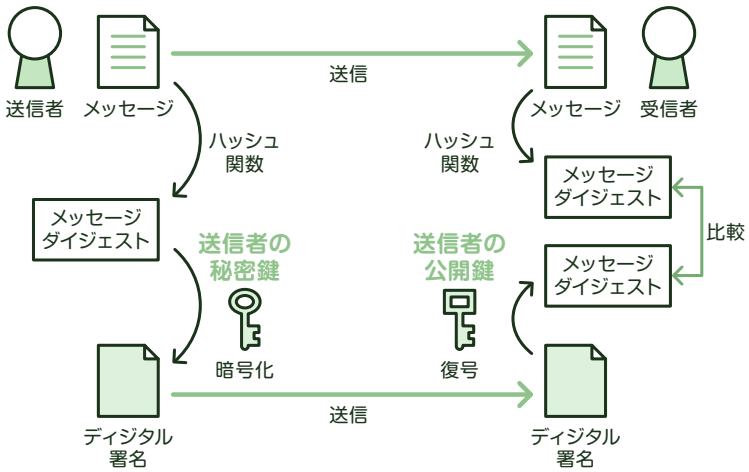
●ディジタル署名

公開鍵暗号方式を応用した技術を用いて、ディジタルデータに、自分が作成したデータであることを証明するために署名を付けることができます。これを**ディジタル署名**といいます。ディジタル署名は、ハッシュ関数（「4-6 探索アルゴリズム」参照）を使って、メッセージからメッセージダイジェストと呼ばれる要約データを作成、さらに自分の秘密鍵を使って暗号化したものです。

受信者は、メッセージとディジタル署名を受け取ります。メッセージはハッシュ関数を使ってメッセージダイジェストを作成、ディジタル署名は送信者の公開鍵で復号することでメッセージダイジェストを作成します。

メッセージダイジェストを比較し一致すれば、メッセージの内容が送信中に改ざんされておらず、送信者本人が作成したものであることが証明できます。

〈ディジタル署名〉



これも知っとこ

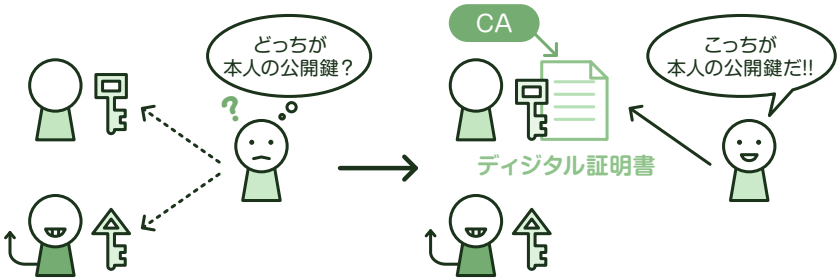
ディジタル証明書をスマートフォンに導入

社員が利用するスマートフォンにディジタル証明書を導入することで、社内システムへアクセスするとき、そのスマートフォンがアクセスを許可されたデバイスであることを確認できます。

●認証局（CA）

公開鍵が本当に本人のものであるか、その正当性を証明するための第三者機関を認証局（CA：Certification Authority）といいます。認証局は、通信相手からの申請に基づいてディジタル証明書を発行し、公開鍵が本人のものであることを証明します。

〈認証局(CA)〉



●SSL

SSL（Secure Socket Layer）は、インターネット上でセキュリティを確保するために、Webサーバとクライアント間の通信を暗号化するプロトコルです。公開鍵暗号方式や共通鍵暗号方式などのセキュリティ技術を使って、データの盗聴や改ざんを防ぎます。Webブラウザに標準搭載され、インターネット上で安全にデータをやりとりするための業界標準となっています。

IPsecとS/MIME

IPsecは、インターネットで暗号通信を行うための規格です。IPパケットを暗号化して送受信することでセキュリティを高めることができます。

S/MIME（Secure/Multipurpose Internet Mail Extensions）は、電子メールの公開鍵暗号方式による暗号化とディジタル署名について定めた標準規格です。

用語

［ディジタル署名］：データ送信者の証明と改ざんされていないかどうかを確認する技術

［CA］：公開鍵の正当性を証明する第三者機関

［SSL］：インターネット上でデータを安全にやりとりする業界標準プロトコル

スキル

→公開鍵暗号方式やディジタル署名においてデータを暗号化、復号する際に、誰のどの鍵を使うかを理解しておこう。

試験にチャレンジ

基本情報技術者試験　平成23年特別

非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。

ア：AES　　イ：DSA　　ウ：IDEA　　エ：RSA

解説 RSA暗号を解読するには、非常に大きな数を素因数分解する必要があります。　　解答：エ

試験にチャレンジ

基本情報技術者試験　平成24年春

文書の内容を秘匿して送受信する場合の公開鍵暗号方式における鍵と暗号化アルゴリズムの取扱いのうち、適切なものはどれか。

ア：暗号化鍵と復号鍵は公開するが、暗号化アルゴリズムは秘密にしなければならない。

イ：暗号化鍵は公開するが、復号鍵と暗号化アルゴリズムは秘密にしなければならない。

ウ：暗号化鍵と暗号化アルゴリズムは公開するが、復号鍵は秘密にしなければならない。

エ：復号鍵と暗号化アルゴリズムは公開するが、暗号化鍵は秘密にしなければならない。

解説　公開鍵暗号方式では、暗号化鍵と暗号化アルゴリズムは公開されますが、復号鍵は秘密にしておかなければなりません。　解答：ウ

試験にチャレンジ

基本情報技術者試験　平成26年秋

ディジタル証明書をもつA氏が、B商店に対して電子メールを使って商品の注文を行うときに、A氏は自分の秘密鍵を用いてディジタル署名を行い、B商店はA氏の公開鍵を用いて署名を確認する。この手法によって実現できることはどれか。ここで、A氏の秘密鍵はA氏だけが使用できるものとする。

ア：A氏からB商店に送られた注文の内容は、第三者に漏れないようにできる。

イ：A氏から発信された注文は、B商店に届くようにできる。

ウ：B商店に届いた注文は、A氏からの注文であることを確認できる。

エ：B商店は、A氏に商品を売ることが許可されていることを確認できる。

解説　ディジタル署名によって実現できるのは、送信者であるA氏本人の注文であることです。また、A氏の注文が改ざんされていないことも確認できます。　解答：ウ

9-4 ネットワークセキュリティ

★ ★ ★

●ネットワークセキュリティ技術

コンピュータをネットワークに接続すると、ネットワークを介して他のコンピュータにアクセスできるので便利ですが、逆に他のコンピュータから不正にアクセスされてしまう危険性もあります。そのため、ネットワークを介した不正なアクセスを防止するためのさまざまな技術があります。

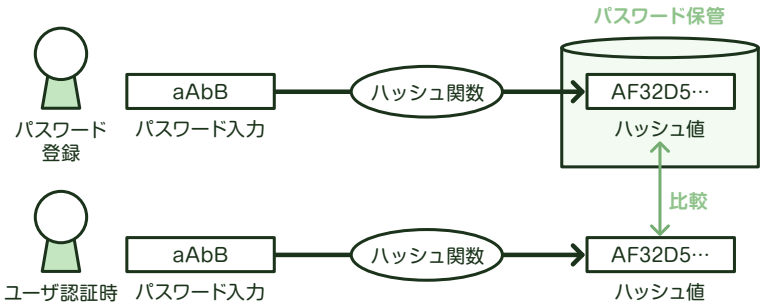
●ユーザ認証

データにアクセスするときにID（アイディー）とパスワードの入力を求め、ユーザ本人によるアクセスであることを確かめます。これを**ユーザ認証**といいます。ただしIDとパスワードを盗まれると、本人以外でもアクセスできてしまうため、パスワードは定期的に変更するなどの配慮（はいりょ）が必要です。

●パスワードのハッシュ化

パスワードを保管する際は、パスワードそのものではなくハッシュ関数で変換したハッシュ値を登録します。これをハッシュ化といいます。認証時も同様に入力パスワードをハッシュ化し、ハッシュ値で比較する方法がとられます。万が一ハッシュ値が流出しても、パスワードそのものを得ることができないため、よく用いられている方法です。

〈パスワードのハッシュ化〉



ハッシュ値を使ったコンテンツ改ざん検知

ハッシュ値は、Webサーバなどのコンテンツ改ざんの検知にも利用されます。Webサーバのコンテンツの各ファイルのハッシュ値を保管しておき、定期的に各ファイルからハッシュ値を生成し比較することで、コンテンツが改ざんされていないかチェックします。

●RADIUS（ラディウス）

RADIUS（Remote Authentication Dial In User Service）は、ネットワークにアクセスしてきた利用者を認証サーバを使って認証するシステムです。無線 LAN や VPN 接続などで使われます。

●バイオメトリクス認証

文字や数字を入力するパスワードではなく、人間の指紋や目の虹彩（こうさい）などの身体的特徴によって認証を行うのが、**バイオメトリクス認証**（生体認証）です。バイオメトリクス認証には、身体的特徴を抽出して認証する方式のほかに、署名するときの速度や筆圧から行動的特徴を抽出して認証する方式もあります。IDやパスワードに比べて、なりすましの危険性が少なく、高い信頼性と利便性を備えていますが、一方で装置の調整には、本人を誤って拒否する確率と他人を誤って許可する確率の双方を考慮に入れる必要があります。

虹彩認証

バイオメトリクス認証の一種で、瞳孔の外側にある虹彩と呼ばれる環状部分のパターンで本人確認を行う認証方式を**虹彩認証**といいます。大人は虹彩が変化しないので、認証デバイスでのパターン更新がほとんど不要です。

用語

［RADIUS］：無線LANやVPN接続などで使用される利用者認証システム

用語

[バイオメトリクス認証]：人間の指紋や虹彩など身体的特徴によって認証。筆記速度や筆圧など行動的特徴により認証する方式もある

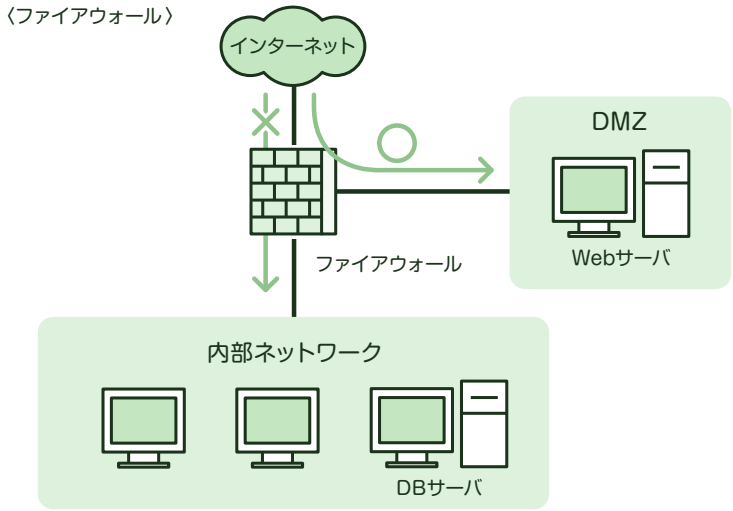
スキル

→バイオメトリクス認証において、身体的特徴と行動的特徴を抽出して認証する方式には具体的にどんなものがあるか理解しておこう。

●ファイアウォール

LAN（ラン）などの内部ネットワークとインターネットなどの外部ネットワークの間に配置し、LANへ不正なアクセスができないようにするシステムを**ファイアウォール**といいます。

ファイアウォールを設置すると、内部ネットワークと外部ネットワークの間に、どちらからも隔離された区域ができます。これを**DMZ**（ディーエムゼット）（非武装地帯）といいます。例えば、WebサーバとDBサーバで構成された利用者向けのサービスをインターネットに公開する場合、以下のようにサーバを設置することが一般的です。インターネットへ情報を公開するWebサーバはDMZに置き、重要なデータを持つDBサーバは不正アクセスを防ぐため内部ネットワークに配置します。



WAF

Webアプリケーションのやりとりを管理することによって不正侵入を防御することのできるファイアウォールを**WAF**（Web Application Firewall）といいます。Webサーバに渡される入力内容などをチェックし、SQLインジェクションなどの攻撃や不正と見なされたアクセス要求を遮断します。

●パケットフィルタリング

パケットのあて先IPアドレスや送信元IPアドレス、ポート番号を判別して、ネットワークへの通過を許可したり、遮断したりする技術を**パケットフィルタリング**といいます。これによって不正侵入を試みるパケットを排除します。ルータやファイアウォールに実装されています。

ARPを利用した通信可否判定

ARPは、IPアドレスからMACアドレスを動的に取得するプロトコルです。この仕組みを利用することで、PCのMACアドレスを確認し、事前に登録されているMACアドレスをもつ場合だけ通信を許可することができます。無線LANのクライアント認証などで使われています。

●プロキシ

内部ネットワークにあるコンピュータのアクセスを中継し、代理でインターネットへ接続を行うコンピュータを、**プロキシ**といいます。接続先にはプロキシがアクセスした履歴しか残らないため、内部ネットワークのIPアドレスを隠すことができます。

●ペネトレーションテスト

コンピュータやネットワークのセキュリティ上の弱点を発見するために、システムを実際に攻撃して侵入を試みるテストを**ペネトレーションテスト**といいます。定期的にテストをすることで、新たなセキュリティホールや設定ミスを発見し、シス

テムの安全性を確保します。

●侵入検知システム

侵入検知システムは、**IDS**（アイディーエス）（Intrusion Detection System）ともいい、コンピュータやネットワークに対する不正行為を検出し、通知するためのシステムです。ネットワーク上の通信を解析し、侵入手口のパターンと一致した場合や、異常を検出した場合には管理者へ通知します。

バックドア

通常の経路以外から不正に侵入するために、侵入者がサーバに仕掛けた裏の侵入経路を**バックドア**といいます。侵入や攻撃を受けたサーバにはバックドアが仕掛けられた可能性が高いため、ディスクのフォーマットやOSの再インストールが必要です。

用語

［ファイアウォール］：内部ネットワークを外部攻撃から守るもの
［DMZ］：外部と内部のネットワークの間にある地帯
［パケットフィルタリング］：IPやポート番号を識別し、通過させるパケットを制限
［プロキシ］：代理でインターネットへ接続し内部ネットワークを隠す
［WAF］：Webアプリケーションの脆弱性への外部攻撃から守るもの
［ペネトレーションテスト］：システムを実際に攻撃して侵入を試みるテスト
［バックドア］：侵入者が通常の経路以外から不正侵入するために仕掛けた裏経路

試験にチャレンジ

基本情報技術者試験　平成26年秋

WAF（Web Application Firewall）を利用する目的はどれか。

ア：Webサーバ及びWebアプリケーションに起因する脆弱性への攻撃を遮断する。

イ：Webサーバ内でワームの侵入を検知し、ワームの自動駆除を行う。

ウ：Webサーバのコンテンツ開発の結合テスト時にWebアプリケーションの脆弱性や不整合を検知する。

エ：Webサーバのセキュリティホールを発見し、OSのセキュリティパッチを適用する。

解説　WAFは、Webアプリケーションのやり取りを管理することによって、SQLインジェクションなどの攻撃や不正と見なされたアクセス要求を遮断します。

解答：ア

試験にチャレンジ

基本情報技術者試験　平成27年春

バイオメトリクス認証には、身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

ア：血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。

イ：署名するときの速度や筆圧から特徴を抽出して認証する。

ウ：瞳孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。

エ：隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証する。

解説　筆記時の速度や筆圧は、個人の行動的特徴です。

解答：イ

試験にチャレンジ

基本情報技術者試験　平成26年春

企業内ネットワークやサーバに侵入するために攻撃者が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：ディジタルフォレンジックス
エ：バックドア

解説 通常の経路以外から不正侵入するために、攻撃者はバックドアを組み込みます。

解答：エ