はじめに

情報社会と呼ばれる現在では、サイバー攻撃による脅威が増大し、セキュリティという言葉が特別なものではなくなっています。特に、最近は、ネットワーク化の進展に伴い不正アクセスによるデータの漏えいや改ざん、コンピュータウイルスによる被害が急速に増えています。

少し紹介すると、ネットワークを通じて他人のコンピュータに不正に侵入し、操作して情報を破壊したり、盗み出したりする不正行為をクラッキングと呼びます。また、コンピュータウイルスのうち自分自身を増殖させることができるものをワーム、コンピュータに感染しネットワーク（インターネット）を通じて外部から操ることを目的として作られたものをボットと呼びます。

スパイウェアとは、有用なプログラムやツールを装うことで、ユーザに気付かれないようにコンピュータに侵入し、不正に個人情報等を収集するプログラムのことで、代表的なスパイウェアにトロイの木馬があります。

他にも様々な脅威がありますが、これらに対して情報セキュリティ対策があり、利用者 ID やパスワード、シングルサインオン、ワンタイムパスワードなど、銀行での認証やネットバンキング等日常で利用されています。

上記のように、巧妙化する攻撃手法に対して、企業や組織の対策は勿論ですが、IT を利用する方が日常の業務や生活において情報セキュリティの知識を身に付ける必要があります。

このような中、平成 28 年 4 月（春期）から国家試験「情報処理技術者試験」の新たな試験区分として、「情報セキュリティマネジメント試験」が創設されました。

本試験の午前では、情報セキュリティ全般に関する知識をはじめ、CSIST などの情報セキュリティ管理、不正アクセスや情報漏えいなどへの情報セキュリティ対策などに関する論点が問われます。また、本試験の午後では、内部不正の防止や標準型攻撃への対策など身近な事例に即した内容が問われるとされています。

そこで、本書では、公開されたシラバスやサンプル問題を分析し、IT パスポートをはじめ、基本情報技術者試験や応用情報技術者試験、情報セキュリティスペシャリスト試験などの本試験で過去に出題された問題から、情報セキュリティマネジメント試験の分野に関する出題をテーマ（項目）別に収録しました。合格に向けて、テーマ（項目）ごとに繰返し学習していただき、情報セキュリティに関する知識を基礎から応用まで幅広く学習して本試験に臨んで頂ければ幸いです。

なお、情報処理技術者試験センターが発表した情報セキュリティマネジメント試験の概要や「公式サンプル問題」も収録しましたので、是非、試験概要の理解に活用してください。

資格の大原 情報処理講座の教職員一同、皆様の本試験合格を心より祈念しております。

資格の大原　情報処理講座

目　次

セキュリティ 編

Part１．情報セキュリティ

Part２．情報セキュリティ管理

Part3. セキュリティ技術評価

Part4. 情報セキュリティ対策

Part5. セキュリティ実装技術

法務 編

Part1. 知的財産権

Part2. セキュリティ関連法規

Part3. 労働関連・取引関連法規

Part４．その他の法律・ガイドライン・技術者倫理

Part５．標準化関連

情報セキュリティマネジメント試験の概要

この欄に掲載する資料は、2015 年 10 月に発表された独立行政法人 情報処理推進機構「情報セキュリティマネジメント試験 紹介ページ」より抜粋したものです。

情報セキュリティマネジメント試験の創設について

IT の高度化やインターネットの普及が社会に様々な恩恵をもたらす一方、サイバー攻撃の手口はますます巧妙化・複雑化し、社会全体に対する非常に大きな脅威となっています。

「情報セキュリティをいかに確保するか」は今や組織にとって大きな経営課題ですが、標的型攻撃、内部不正などの多種多様な脅威は、「IT による対策（技術面の対策）」だけではなく、適切な情報管理、業務フローの見直し、組織内規程順守のための従業員の意識向上といった、「人による対策（管理面の対策）」についてもしっかりとした取組みが重要です。

そのための情報セキュリティマネジメントを担う人材の育成をいかに推進していくかが、社会全体での課題であると言えます。

「情報セキュリティマネジメント試験」は、このような社会ニーズの高まりを背景に、政府の『「日本再興戦略」改訂 2015』（平成 27 年 6 月閣議決定）や経済産業省 産業構造審議会で示された方向性を踏まえて、国家試験「情報処理技術者試験」の新たな試験区分として創設されました（平成 28 年度春期から試験開始。春期（4 月）、秋期（10 月）の年 2 回実施）。

情報セキュリティマネジメント試験は、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験です。〈共通キャリア・スキルフレームワーク（CCSF）レベル 2 相当〉

- **部門全体の情報セキュリティ意識を高め、組織における情報漏えいリスクを低減する！**
- **万が一トラブルが発生しても、適切な事後対応によって、被害を最小限に食い止める！**
- **情報セキュリティを確保することで、より安全で積極的な IT 利活用を実現する！**

試験の対象者

組織作りに欠かせない情報セキュリティマネジメント人材は、業種、職種を問わず、また、営業・企画・製造・総務・人事・経理などの部門を問わず、多くの現場で強く必要とされています。

- 業務で個人情報を取り扱う全ての方
- 業務部門・管理部門で情報管理を担当する全ての方
- 外部委託先に対する情報セキュリティ評価・確認を行う全ての方
- 情報セキュリティ管理の知識・スキルを身に付けたい全ての方
- ｉパス（IT パスポート試験）合格から、さらにステップアップしたい全ての方

試験時間と出題形式

時間区分	午前	午後
試験時間	90 分	90 分
出題形式	多肢選択式（四肢択一）	多肢選択式
出題数／解答数	50 問／50 問	3 問／3 問
基準点	60 点（100 点満点）	60 点（100 点満点）

採点方式については、素点方式です。合格基準は、各時間区分（午前、午後）の得点が全て基準点以上の場合に合格です。

出題内容

■午前の出題内容

情報セキュリティの考え方をはじめ、情報セキュリティ管理の実践規範、各種対策、情報セキュリティ関連法規などに加えて、

ネットワーク、システム監査、経営管理などの関連分野の知識を問います。

重点分野	**情報セキュリティ全般**	機密性・完全性・可用性、脅威、脆弱性、サイバー攻撃手法、暗号、認証 など
	情報セキュリティ管理	情報資産、リスク、ISMS、インシデント管理などの各種管理策、CSIRT など
	情報セキュリティ対策	マルウェア対策、不正アクセス対策、情報漏えい対策、アクセス管理、情報セキュリティ啓発 など
	情報セキュリティ関連法規	サイバーセキュリティ基本法、個人情報保護法、不正アクセス禁止法など
関連分野	**テクノロジ**	ネットワーク、データベース、システム構成要素
	マネジメント	システム監査、サービスマネジメント、プロジェクトマネジメント
	ストラテジ	経営管理、システム戦略、システム企画

■午後の出題内容

業務の現場における情報セキュリティ管理の具体的な取組みである情報資産管理、リスクアセスメント、IT 利用における情報セキュリティ確保、 委託先管理、情報セキュリティ教育・訓練などのケーススタディによる出題を通して、情報セキュリティ管理の実践力を問います。

出題の特色

- **身近な事例をベースにした実践的な出題！**
- **国際・国内標準や公的なガイドラインに基づく出題！**

サンプル問題

午前　問題　　https://www.jitec.ipa.go.jp/sg/sample.html より

問１　情報セキュリティにおいて，業務で利用しているシステムに影響を与える事象 a～d のうち，脅威によって直接的に引き起こされたものだけを全て挙げたものはどれか。

a　CD-ROM の劣化によって，保存しておいた顧客リストが利用できなくなる。
b　自然災害による停電や断水によって，システムが利用できなくなる。
c　定期的なメンテナンスによって，メンテナンス期間中はシステムが利用できなくなる。
d　メールサーバの設定ミスによって，メールサーバと連携して動作する自動問合せ業務システムが利用できなくなる。

ア　a，b　　イ　a，b，d　　ウ　b，c　　エ　c，d

問２　ディジタルフォレンジックスの活動に含まれるものはどれか。

ア　インシデントの原因究明に必要となるデータの収集と保全
イ　自社システムを攻撃して不正侵入を試みるテストの実施
ウ　定期的なウイルスチェック
エ　パスワード認証方式からバイオメトリクス認証方式への切替え

問３　電子的な文書ファイルの機密性を維持するために使用するセキュリティ対策技術として，適切なものはどれか。

ア　アクセス制御　　イ　タイムスタンプ
ウ　ディジタル署名　　エ　ホットスタンバイ

午前　解答・解説

問１　解答－イ

脅威は、情報資産や組織に損失や損害をもたらす要因で、不測の事態において発生し、潜在的に存在するもので、事故、災害などの物理的脅威、コンピュータ技術に起因する技術的脅威、誤操作や紛失など人的ミスによる人的脅威に分けられます。

a　技術的脅威に該当します。

b　物理的脅威に該当します。

c　脅威ではありません。

d　人的脅威に該当します。

問２　解答－ア

ディジタルフォレンジックスは、コンピュータ犯罪の被害に備えて、不正アクセスなどのコンピュータに関する犯罪の法的な証拠を明らかにするために、原因究明に必要な情報を収集して分析するための手段や技術です。

問３　解答－ア

アクセス制御は、「need-to-know（最小権限）」の原則に従って、利用者ごとに文書ファイルに対するアクセス権を設定することで、文書ファイルの機密性を維持する仕組みです。

イ　タイムスタンプ（時刻認証）は、データが存在していた日時を記録した情報です。

ウ　ディジタル署名（電子署名）は、公開鍵暗号方式を利用して、データが正当な送り手からのものであることを証明すると同時に、改ざんされていないことを証明する方法です。

エ　ホットスタンバイは、現用系と待機（予備）系の２台のコンピュータを用意し、現用系に障害が発生した場合に備えて、待機系ではOSだけを起動させて業務システムは起動させずに待機させておく方法です。

午後　問題　　https://www.jitec.ipa.go.jp/sg/sample.html より

問１　内部不正防止のためのログのレビューに関する次の記述を読んで，設問 1～6 に答えよ。

A 社は，高級化粧品を個人に販売しており，従業員は 100 人である。A 社は総務部，情報システム部，購買部，営業部から成り，営業部には 60 人の従業員が属している。営業部は企画課，営業 1 課～4 課から構成される。営業部の IT 環境は次のとおりである。

・営業部員は全員 A 社所有のノート PC を使用している。
・社内ネットワークに接続された，スキャナ用の共用 PC が 1 台設置されている。
・営業部員は，社外から社内のシステムを使用する際には，ノート PC をインターネット経由で A 社の VPN サーバに接続して使用している。

なお，A 社では，インターネットの使用を広く認めており，Web メールやファイル共有サービスなどを含め，サービスの使用を制限していない。

A 社では，顧客情報などの機密情報の漏えいを防ぐ目的で，退職後も一定期間有効な損害賠償条項を含む機密保持契約を全従業員と締結している。

A 社では，営業部員が表計算ソフトを使用してノート PC で顧客情報を管理していたが，顧客管理パッケージ（以下，B システムという）を社内に導入し，そこで集約して管理することを決定した。B システムに関する方針は次のとおり定めた。

・B システムの主管部門は営業部である。
・B システムを使用するのは営業部だけである。
・見込み客の登録から販売後のフォローアップまでを一貫して B システムによって管理する。
・B システムの導入及び運用は A 社の情報システム部が行う。
・B システムは 2 か月後から使用開始する。
・表計算ソフトを使用して管理していた顧客情報は B システムに移行後，ノート PC から削除する。

情報システム部は，B システムに関して，利用者 ID の管理，データのバックアップ取得，ログの記録などに関する要件について営業部との間で合意した。B システムは顧客情報を取り扱うシステムなので，内部不正による顧客情報の漏えいを防止するため，採取するログの保存方法や，レビュー方法（誰がいつ，どのように）について C 君が検討を開始した。

〔ログのレビュー方法の検討〕

営業部の企画課に所属する C 君は，営業部の情報セキュリティリーダを兼ねている。C 君は B システムのログの仕様を確認しようと思い，情報システム部担当者の D 君にログの仕様の調査を依頼した。そこで D 君は，B システムのログのサンプルを提示した（表 1）。ログイン及びログアウトのログはサーバ X で，それ以外のログはサーバ Y で記録されるが，表 1 は，情報システム部でツールを用いてそれらのログを同じ形式に整え，表計算ソフトを使用して時系列順に並び替えたもの（以下，加工済みログという）とのことであった。

表 1　B システムの加工済みログ（抜粋）

日時	利用者のIP アドレス	利用者ID	操作	顧客ID
2015/03/10 15:30:10	10.0.0.5	1013	LOGIN	0
2015/03/10 15:40:03	10.0.0.5	1013	READ	10023
2015/03/10 15:40:10	10.0.0.5	1013	READ	10025
2015/03/10 15:40:15	10.0.0.5	1013	READ	10102
2015/03/10 15:45:20	10.0.0.5	1013	UPDATE	10102
2015/03/10 15:50:16	10.0.0.5	1013	DELETE	10023
2015/03/10 16:03:10	10.0.0.8	1002	LOGIN	0
2015/03/10 16:15:03	10.0.0.8	1002	READ	10105
2015/03/10 16:16:10	10.0.0.8	1002	READ	10321
2015/03/10 16:16:15	10.0.0.8	1002	READ	10222
2015/03/10 16:20:12	10.0.0.5	1013	LOGOUT	0
2015/03/10 16:25:19	10.0.0.8	1002	LOGOUT	0

注記　顧客 ID の 0 は，顧客情報に関係しない操作であることを意味する。

D 君は，B システムでは，次の対策を実施することを C 君に説明した。

・加工済みログの順番が，実際に営業部員が B システムに対して実施した操作の順番どおりになるよう，［　a　］を行う。

・ログが故意に消されてしまうことがないように［　b　］を行う。

営業部では，顧客ごとに担当営業を決めているが，担当営業が休みの際のサポートなどが必要なので，B システムでは，全営業部員が全顧客情報にアクセスできるようにする。

最近，同業他社で，従業員が，共有ファイルサーバにある全ての顧客情報を USB メモリにコピーして持ち出し，転職先で使ったという事件が発生した。そこで営業部長は，C 君に図 1 の要件を伝え，対策の検討を指示した。

・顧客情報への業務目的外のアクセスをログのレビューによって検出したい。ログのレビュー手順は，まずログの内容を確認し，もし業務目的外と思われる顧客情報へのアクセスログがあった場合は，遅滞なく営業部長に報告の上，そのログが示す操作を行った営業部員がなぜその操作を行ったかを適切な方法で確認する。

・万が一問題が発生したときに備えて，後からでもどの営業部員がどの顧客情報にアクセスしたか特定できるようにしておきたい。

図 1　営業部長が伝えた要件

営業部長は，①リスクを更に低減させるために，営業部員が退職する際に新たな手続を実施することとした。

②C 君は，営業部長が伝えた要件を基に，どのような立場の人がどの程度の頻度でレビューをすべきかを検討した。③さらに C 君は，ログの長期的な保存方法についても検討を行った。C 君が，検討結果を営業部長に説明したところ，営業部長もこれに同意した。

情報システム部による B システムの導入完了後，各営業部員は，表計算ソフトを使用して管理していた顧客情報を B システムに移行し，ノート PC から削除した。移行完了後，営業部では B システムの使用を開始した。

〔ログのレビュー開始〕

Bシステムの使用を開始して1か月が経過し，ログのレビューが開始された。Bシステムには約4,000人の顧客情報が保管されている。ログの生成件数を考えると，30日間で100人分以上の顧客情報にアクセスした営業部員のログに限定してレビューを行うべきだということになった。そこで，④C君は，過去30日間に発生したREADのログからレビュー対象のログを抽出する条件を示してD君にログの抽出を依頼した。抽出されたログを見たC君は，ある営業部員が1,000人分の顧客情報にアクセスしたことを示すログを発見した。そこで，C君はすぐに営業部長に報告し，その営業部員の上長の課長に確認した。その結果，その課長の指示でダイレクトメールを送付していたことが分かり，問題はないことが確認できた。

営業部長とC君で相談した結果，レビューを行う人，及び頻度は検討結果のとおりとし，抽出条件に基づいて抽出したログだけをレビュー対象とすることとした。

営業部長は，ログをレビューするに当たり，次のことを指示した。

・全ての営業部員に対し，ログをレビューすることを伝えること。ただし，ログのレビューを回避されないように，抽出条件を営業部員には伝えないこと。
・ログがレビューされていることを営業部員に印象付けるために，ログに記録されているアクセスについて定期的に必ず営業部員にアクセスの目的を確認すること。

〔課題の発見とリスクの更なる低減〕

C君は，職場内でBシステムが適切に使用されているかどうかを観察していたところ，いくつかの事象が目に留まり，このままでは，⑤ログのレビューを適切に実施したとしても，図1の要件が実現できないことに気付いた。そこでC君は，営業部長に相談の上，各課長に改善を依頼した。

Bシステムの使用開始から1年間が経過した。ログのレビューによって営業部全体の情報セキュリティ意識が高まり，営業部長のC君に対する評価は大きく高まった。

設問１　本文中の［　a　］と［　b　］に入れる組合せとして正しい答えを，解答群の中から選べ。

a，b に関する解答群

	a	b
ア	サーバの時刻同期	ログの WORM メディアへの記録
イ	サーバの時刻同期	ログの暗号化
ウ	ログの WORM メディアへの記録	サーバの時刻同期
エ	ログの WORM メディアへの記録	ログの暗号化
オ	ログの暗号化	サーバの時刻同期

注記　WORM：Write Once Read Many

設問２　本文中の下線①で実施することになった手続はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　退職する営業部員が担当していた顧客情報を，他の営業部員に引き継ぐ。

イ　退職する営業部員が担当していた顧客情報を，B システムから完全に消去する。

ウ　退職する営業部員に，その営業部員と締結した機密保持契約書を見せ，その営業部員がアクセスした顧客情報がログに記録されていることを説明する。

エ　退職する営業部員の PC のハードディスクは再利用せず，完全に物理破壊する。

設問３　本文中の下線②における，C 君の検討結果はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　営業部の各課長が，情報システム部担当者の依頼があった都度，ログをレビューする。

イ　営業部の各課長が，毎週，ログをレビューする。

ウ　情報システム部担当者が，営業部長が指定した頻度でログをレビューする。

エ　情報システム部担当者が，毎週，ログをレビューする。

設問４　本文中の下線③においてC君が検討したログの保存方法はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　情報システム部が全てのログを 10 年間保存する。

イ　情報システム部が営業部員ごとにログを仕分けして，各営業部員が自分の分を保存する。

ウ　レビュー後のログは保存せず，情報システム部担当者が速やかに削除する。

エ　レビューで不審であると判断したログだけを情報システム部が 10 年間保存する。

設問５　本文中の下線④で C 君が D 君に示した抽出条件を，解答群の中から選べ。

解答群

ア　アクセスしたユニークな顧客 ID 数が 100 以上の営業部員のログ

イ　アクセスしたユニークな顧客 ID 数が 100 以上の日のログ

ウ　ログ件数が 100 以上の営業部員のログ

エ　ログ件数が 100 以上の日のログ

設問６　C 君が観察した次の(ⅰ)～(ⅳ)の事象のうち，本文中の下線⑤の原因となるものを全て挙げた組合せを，解答群の中から選べ。

（ⅰ） B システムで表示した顧客情報をコピーし，表計算ソフトにペーストした上で A 社の共有ファイルサーバに置いて共有している。

（ⅱ） B システムの使用申請をしてから，営業部長が承認するまでに 2 週間掛かっている。

（ⅲ） ある営業部員が共用 PC から B システムにログインし，ログインしたままその PC で他の営業部員が B システムを使っている。

（ⅳ） ある営業部員が頻繁に B システムにログイン，ログアウトを繰り返している。

解答群

ア （ⅰ），（ⅱ）　　イ （ⅰ），（ⅱ），（ⅳ）　　ウ （ⅰ），（ⅲ）

エ （ⅰ），（ⅳ）　　オ （ⅱ），（ⅲ）　　カ （ⅱ），（ⅲ），（ⅳ）

キ （ⅱ），（ⅳ）　　ク （ⅲ），（ⅳ）

午後　解答・解説

■解答

設問１	ア
設問２	ウ
設問３	イ
設問４	ア
設問５	ア
設問６	ウ

■解説

設問１

問題文に「加工済みログの順番が，実際に営業部員が B システムに対して実施した操作の順番になるよう」と記述されているので、時間順という意味で、空欄 a には「サーバの時刻同期」が入ります。また、「ログが故意に消されてしまうころがないように」と記述されているので、空欄 b には 1 回だけ書き込めるが消すことができない WORM メディアにログを記録する「ログの WORM メディアへの記録」が入ります。

設問２

通常、機密保持契約書には、機密情報を漏えいした場合の罰則が記載されています。退職する営業部員に、その営業部員が締結した機密保持契約書を見せることで、機密漏えいを抑止します。また、その営業部員がアクセスした顧客情報がログに記録されていることを説明し、機密保持契約の対象に顧客情報が含まれることを認識させて、顧客情報の漏えいを抑止します。

設問３

「図１　営業部長が伝えた要件」に、「・顧客情報への業務目的外のアクセスをログのレビューによって検出したい。～（省略）～遅滞なく営業部長に報告の上」と記述されているので、業務が分かる管理職が遅滞なく営業部長に報告する「営業部の各課長が，毎週，ログをレビューする」ことになります。

設問４

イ　「各営業部員が自分の分を保存する」場合には、不正を行った営業部員が証拠を消すことが可能です。

ウ　「レビュー後のログは保存せず」ということは、「ログの長期的な保存方法についても検討」という趣旨に反します。

エ　「レビューで不審であると判断したログだけを～（省略）～保存する」場合には、ログに記録されていない顧客情報の漏えいがあった場合に、担当した営業部員を把握することができません。

設問５

〔ログのレビュー開始〕の２行目に、「ログの生成件数を考えると，30 日間で 100 人分以上の顧客情報にアクセスした営業部員のログに限定してレビューを行う」と記述されています。

顧客 ID は顧客を特定するための情報です。したがって、100 人以上の顧客情報にアクセスした営業部員のログなので、「アクセスしたユニークな顧客 ID 数が 100 以上の営業部員のログ」を抽出します。

設問６

「図１　営業部長が伝えた要件」に、「・万が一問題が発生したときに備えて，後からでもどの営業部員がどの顧客情報にアクセスしたか特定できるようにしておきたい。」と記述されています。

「(ｉ) B システムで～（省略）～A 社の共有ファイルサーバに置いて共有している。」と「どの営業部員がどの顧客情報にアクセスしたか特定」できません。

また、「(iii) ある営業部員が共有 PC からＢシステムにログインし，ログインしたままその PC で他の営業部員がＢシステムを使っている。」という場合においても、「どの営業部員がどの顧客情報にアクセスしたか特定」できません。

テキスト

セキュリティ

Ｃｏｎｔｅｎｔｓ

1．情報セキュリティ

01　情報セキュリティの目的と考え方

1．情報セキュリティの概念

JIS Q 27001:2006 では、情報セキュリティを「情報の機密性（Confidentiality）、完全性（Integrity）及び可用性（Availability）を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。」と定義しています。

機密性	許可された者だけが許可された方法でのみ情報にアクセスできるようにすることで、不正アクセスや情報漏洩から情報資産を守ること
完全性	情報や情報の処理方法が正確で完全であるようにすることで、許可されていない者によって情報が改ざんされたり、破壊されたりしないこと
可用性	許可された者が、必要なときに情報にアクセスできることを確実にすることで、正規の利用者が情報を利用しようとしたときには、いつでも情報にアクセスすることができること

なお、これら３つの要素（機密性、完全性、可用性）から残り４つの特性（真正性、責任追跡性、否認防止、信頼性）を導くことができます。

例題 1-1　　ITパスポート　平成 24 年秋　問 83

ａ～ｃは情報セキュリティ事故の説明である。ａ～ｃに直接関連する情報セキュリティの三大要素の組合せとして，適切なものはどれか。

ａ　営業情報の検索システムが停止し，目的とする情報にアクセスすることができなかった。
ｂ　重要な顧客情報が，競合他社へ漏れた。
ｃ　新製品の設計情報が，改ざんされていた。

	ａ	ｂ	ｃ
ア	可用性	完全性	機密性
イ	可用性	機密性	完全性
ウ	完全性	可用性	機密性
エ	完全性	機密性	可用性

解答－イ

ａは、正規の利用者が情報を利用しようとしたときに利用できなかったのですから、「可用性」が守れなかったことになります。

ｂは、情報漏えいから情報資産を守れなかったのですから、「機密性」が守れなかったことになります。

ｃは、情報が改ざんされていたのですから、「完全性」が守れなかったことになります。

ここで演習 1-1～1-4 を解いて下さい

２．OECD セキュリティガイドライン

OECD セキュリティガイドラインは、OECD（経済協力開発機構）が、各国における情報システム及びネットワークのセキュリティ確保のための枠組み作りの指針として採択したガイドラインで、次の９つの原則から構成されています。

①認識（Awareness）の原則

参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。

②責任（Responsibility）の原則

すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。

③対応（Response）の原則

参加者は、セキュリティの事件に対する予防、検出及び対応のために、時宜を得たかつ協力的な方法で行動すべきである。

④倫理（Ethics）の原則

参加者は、他者の正当な利益を尊重するべきである。

⑤民主主義（Democracy）の原則

情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである。

⑥リスクアセスメント（Risk assessment）の原則

参加者は、リスクアセスメントを行うべきである。リスクアセスメントとは、セキュリティ上の脅威と脆弱性を識別し、リスクの許容できるレベルの決定やリスクを管理するための措置の選択を支援するもの。

⑦セキュリティの設計及び実装（Security design and implementation）の原則

参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。

⑧セキュリティマネジメント（Security management）の原則

参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。

⑨再評価（Reassessment）の原則

参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

02 情報セキュリティの重要性

社会のネットワーク化に伴い、企業にとって情報セキュリティの水準の高さが企業評価の向上につながり、情報システム関連の事故が事業の存続を脅かすことになります。

なお、情報システム関連の事故は、情報資産（後述）に脅威と脆弱性が組み合わさることで発生します。

1．脅威

脅威は、情報資産や組織に損失や損害をもたらす要因で、不測の事態において発生し、潜在的に存在するものです。

1）脅威の種類

内閣府の情報セキュリティ対策推進会議が公表する「情報セキュリティポリシーに関するガイドライン」では、物理的脅威、技術的脅威、人的脅威に大別しています。

①物理的脅威

物理的脅威には、事故、災害、故障、破壊、盗難、不正侵入などがあります。

②技術的脅威

技術的脅威には、不正アクセス、盗聴、マルウェア、なりすまし、改ざん、エラーなどがあります。なお、悪意をもってコンピュータに不正侵入しデータを盗み見たり破壊などを行う**クラッキング**も技術的脅威に該当します。また、受信者の承諾なしに無差別に送付される SPAM（迷惑メール）や、インターネットを介して不特定多数の者とファイルのやり取りを行うための**ファイル共有ソフト**も技術的脅威に該当します。

③人的脅威

人的脅威には、誤操作、紛失、破損、不正利用などがあります。なお、本人を装って電話をかけてパスワードを聞き出す、パスワードを入力しているところを後ろから近づいて覗き見る、ゴミ箱に捨てられた資料から IP アドレスの一覧や利用者名、パスワードといった情報を探すなどの、電子的な方法を用いないで組織内部の人間からパスワードや機密情報などを不正に入手する**ソーシャルエンジニアリング**も人的脅威に該当します。

例題 1-2　　**基本情報　平成 26 年秋　問 36**

ソーシャルエンジニアリングに分類される手口はどれか。

ア　ウイルス感染で自動作成されたバックドアからシステムに侵入する。
イ　システム管理者などを装い，利用者に問い合わせてパスワードを取得する。
ウ　総当たり攻撃ツールを用いてパスワードを解析する。
エ　バッファオーバフローなどのソフトウェアの脆弱性を利用してシステムに侵入する。

解答－イ
ア　不正アクセスの手段などに関する記述です。
ウ　ブルートフォース攻撃に関する記述です。
エ　バッファオーバフロー攻撃に関する記述です。

ここで演習 1-5～1-11 を解いて下さい

2）マルウェア

マルウェア（malicious software）とは、コンピュータウイルス（computer virus）やスパイウェア（Spyware）、ランサムウェア、キーロガーなどの不正プログラムの総称です。

①コンピュータウイルス

コンピュータウイルスは、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す。

代表的なコンピュータウイルス	説明
ワーム（worm）	コンピュータウイルスのうちコンピュータシステム又はネットワークを介して自分自身を繁殖させることができるもの
ボット（bot）	ネットワーク（インターネット）を介して感染したコンピュータを外部から操ることを目的として作成されたもの
マクロウイルス（macro virus）	マクロと呼ばれる簡易プログラムで作成されたウイルスで、ワープロソフトの文書ファイルや表計算ソフトのワークシートに潜伏し、ファイルを開いたときに他の同一形式のファイルに感染するもの

例題 1-3　　IT パスポート　平成 23 年春　問 76

多数のコンピュータに感染し，遠隔操作で攻撃者から指令を受けると DDoS 攻撃などを一斉に行う不正プログラムに付けられた呼び名はどれか。

ア　ハニーポット　　イ　ボット
ウ　マクロウイルス　　エ　ワーム

解答－イ

ア　ハニーポットは、不正侵入の手口を研究するために、意図的に設けられたネットワークへの侵入箇所です。

ウ　マクロウイルスは、マクロと呼ばれる簡易プログラムで作成されたウイルスで、ワープロソフトの文書ファイルや表計算ソフトのワークシートに潜伏し、ファイルを開いたときに他の同一形式のファイルに感染するコンピュータウイルスです。

エ　ワームは、コンピュータシステム又はネットワークを介して自分自身を繁殖させることができるコンピュータウイルスです。

②スパイウェア

スパイウェアは、有用なプログラムやツールを装うことで、ユーザに気付かれずにコンピュータに侵入し、不正に個人情報などを収集するプログラムで、代表的なスパイウェアに**トロイの木馬**（Trojan horse）があります。

スパイウェアによる被害を防ぐにはスパイウェア対策ソフトを導入し、怪しいサイトに近づかず、不用意なダウンロードは行わず、添付ファイルは開かないなどの、注意が必要です。

例題 1-4　　**IT パスポート　平成 24 年春　問 54**

不正プログラムの一種であるトロイの木馬の特徴はどれか。

ア　アプリケーションソフトのマクロ機能を利用してデータファイルに感染する。

イ　新種ウイルスの警告メッセージなどの偽りのウイルス情報をチェーンメールで流す。

ウ　ネットワークを利用して，他のコンピュータに自分自身のコピーを送り込んで自己増殖する。

エ　有用なソフトウェアに見せかけて配布された後，システムの破壊や個人情報の詐取など悪意ある動作をする。

解答－エ

ア　マクロウイルスに関する記述です。

イ　デマウイルスに関する記述です。

ウ　ワームに関する記述です。

③ランサムウェア

ランサムウェアは、感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、元に戻すための代金を利用者に要求するプログラムです。

④キーロガー

キーロガーは、キーボードからの入力情報を監視するソフトウェアやハードウェアのことで、単に入力された文字だけでなく、使用したアプリケーションなども記録できるものもあります。

利用者 ID やパスワードなどの情報を不正に入手するために、不特定多数の利用者が利用するパソコンに、秘かにキーロガーを仕掛ける事例が増えています。

例題 1-5　　基本情報　平成 27 年春　問 34

キーロガーの悪用例はどれか。

ア　通信を行う２者間の経路上に割り込み，両者が交換する情報を収集し，改ざんする。
イ　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。
ウ　ブラウザでの動画閲覧時に，利用者の意図しない広告を勝手に表示する。
エ　ブラウザの起動時に，利用者がインストールしていないツールバーを勝手に表示する。

解答ーイ

ア　中間者攻撃（Man-in-the-middle）に関する記述です。
ウ　アドウェアに関する記述です。
エ　ブラウザ・ハイジャッカーに関する記述です。

ここで演習 1-16、1-17 を解いて下さい

⑤ルートキット

ルートキット（rootkit）は、攻撃者が不正侵入後に利用する複数の機能をまとめてパッケージ化したソフトウェアです。不正侵入した痕跡を隠蔽するためにログを改ざんする機能や、OS に不正なプログラムを組み込んで隠蔽する機能などが含まれます。

例題 1-6　　情報セキュリティスペシャリスト　平成 27 年春　午前Ⅱ　問 12

rootkit に含まれる機能はどれか。

ア　OS の中核であるカーネル部分の脆弱性を分析する。
イ　コンピュータがウイルスやワームに感染していないことをチェックする。
ウ　コンピュータやルータのアクセス可能な通信ポートを外部から調査する。
エ　不正侵入して OS などに組み込んだものを隠蔽する。

解答－エ
ア　脆弱性検査ツールに関する記述です。
イ　コンピュータウィルスチェックツールに関する記述です。
ウ　ポートスキャンに関する記述です。

ここで演習 1-18、1-19 を解いて下さい

⑥バックドア
バックドアは、攻撃者が不正な行為に利用するため、企業内情報ネットワークやサーバに設置した通常以外の侵入経路です。

例題 1-7　　基本情報　平成 26 年春　問 43

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

解答－エ
ア　シンクライアントエージェントは、必要最低限の機能だけを備えたシンクライアントシステムで動作する自律的なソフトウェアです。
イ　ストリクトルーティングは、TCP/IPの経路選択において、途中の経路をすべて送信者が指定する方法です。
ウ　ディジタルフォレンジックスは、コンピュータ犯罪の被害に備えて、不正アクセスなどのコンピュータに関する犯罪の法的な証拠を明らかにするために、原因究明に必要な情報を収集して分析するための手段や技術です。

ここで演習 1-20 を解いて下さい

２．脆弱性

脅威の発生を誘発する弱点を情報システムの**脆弱性**と呼びます。具体的には、情報システムの情報セキュリティに関する欠陥、企業、組織、個人に対する行動規範の不徹底、未整備などです。

なお、ハードウェアを含めたシステム全体の欠陥や弱点を脆弱性と呼ぶのに対して、ソフトウェアの**バグ**（欠陥、欠陥が原因となって発生する誤動作）によって発生するセキュリティ上の欠陥や弱点を特に**セキュリティホール**と呼びます。

例題 1-8　　IT パスポート　平成 26 年春　問 58

不正アクセスなどに利用される，コンピュータシステムやネットワークに存在する弱点や欠陥のことを何というか。

ア　インシデント　　イ　セキュリティホール
ウ　ハッキング　　エ　フォレンジック

解答ーイ

ア　インシデントは、システムの脆弱性によって脅威が誘発されて損失が発生している状態です。

ウ　ハッキングは、他人のコンピュータシステムに不正に侵入する行為です。

エ　フォレンジック（ディジタルフォレンジクス）は、コンピュータ犯罪の被害に備えて、不正アクセスなどのコンピュータに関する犯罪の法的な証拠を明らかにするために、原因究明に必要な情報を収集して分析するための手段や技術です。

03 サイバー攻撃

１．不正のメカニズム

不正のメカニズムについて、アメリカの犯罪学者であるドナルド．R．クレッシーは、「不正行為は、機会、動機、正当化の３要素がそろったときに初めて行われる」という「不正のトライアングル（機会、動機、正当化）理論」を唱えました。

機会は、不正行為を容易に実行できる客観的環境です。

動機は、不正行為の実行に対する主観的欲求です。

正当化は、不正行為の実行を肯定する主観的事情です。

例題 1-9　　情報セキュリティスペシャリスト　平成 27 年秋　午前Ⅱ　問 9

不正が発生する際には“不正のトライアングル”の３要素全てが存在すると考えられている。“不正のトライアングル”の構成要素の説明のうち，適切なものはどれか。

ア　“機会”とは，情報システムなどの技術や物理的な環境及び組織のルールなど，内部者による不正行為の実行を可能，又は容易にする環境の存在である。

イ　“情報と伝達”とは，必要な情報が識別，把握及び処理され，組織内外及び関係者相互に正しく伝えられるようにすることである。

ウ　“正当化”とは，ノルマによるプレッシャーなどのことである。

エ　“動機”とは，良心のかしゃくを乗り越える都合の良い解釈や他人への責任転嫁など，内部者が不正行為を自ら納得させるための自分勝手な理由付けである。

解答ーア

イ　“情報と伝達”は３要素ではありません。

ウ　“動機”に関する説明です。

エ　“正当化”に関する説明です。

２．攻撃者の種類

コンピュータやネットワークに関して高度な技術をもつ者をハッカーと呼び、その技術を利用して、コンピュータやネットワークに不正に侵入して破壊・改ざんなど（クラッキング）を行う者をクラッカーと呼びます。

クラッカーは愉快犯である場合が多いですが、クラッキングにより詐欺や恐喝などを行う詐欺犯や故意犯もいます。その中で、ボットを埋め込んだコンピュータで構成されたネットワークである**ボットネット**を指揮して犯罪を行うクラッカーを特に**ボットハーダー**と呼びます。

また、興味本位で他のクラッカーが制作した不正プログラムを利用してクラッキングを行う**スクリプトキディ**と呼ばれる者もいます。

３．攻撃の動機

攻撃には様々な動機がありますが、最も一般的な動機は金銭奪取です。また、社会的・政治的主張が攻撃の動機となる場合もあります。社会的・政治的主張のためにクラッキングを行うことを**ハクティビズム**と呼びます。

なお、国民生活や社会・経済基盤を標的にした大規模なクラッキングを**サイバーテロリズム**と呼びます。

４．サイバー攻撃手法

システムの脆弱性を悪用するサイバー攻撃手法にはさまざま種類があります。

１）不正ログイン

コンピュータやネットワークに不正ログインする代表的な攻撃手法は次のとおりです。

①パスワードクラック

他人のパスワードを見破ることを**パスワードクラック**と呼び、代表的な方法に総当り攻撃と辞書攻撃があります。

総当り攻撃 （**ブルートフォース**）	文字を組み合わせてあらゆるパスワードでログインを何度も試みて、力ずくでパスワードを見破る攻撃手法
辞書攻撃	利用者がパスワードとして使いそうな文字列をあらかじめ辞書ファイルとして登録しておき、その辞書ファイルにある言葉を片っ端から入力し、力ずくでパスワードを見破る攻撃手法

②パスワードリスト攻撃

パスワードリスト攻撃は、あらかじめ何らかの方法で取得したIDとパスワードをリスト化し、これを用いて不正ログインする攻撃手法です。

なお、ネットワーク上のデータを盗聴してIDやパスワードを不正に取得する方法を**スニッフィング**と呼びます。

例題 1-10　　応用情報　平成 25 年秋　問 44

サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち，適切なものはどれか。

	辞書攻撃	スニッフィング	ブルートフォース攻撃
ア	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。
イ	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。
ウ	ランダムな値でパスワードを設定する。	ログインの試行回数に制限を設ける。	パスワードを平文で送信しない。
エ	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。

解答－イ

辞書攻撃は、利用者がパスワードに使いそうな言葉をあらかじめ登録した辞書ファイルに記載の言葉を先頭から順に入力することでパスワードを探し出そうとするため、パスワードをランダムな文字列で作ることで被害を防ぐことができます。

スニッフィングは、ネットワーク上のデータを盗聴して、IDやパスワードを不正取得するので、データを暗号化することで被害を防ぐことができます。

ブルートフォース攻撃は、適当に文字を組み合わせて作成したパスワードでログインを繰り返すことで、力ずくでパスワードを探し出そうとするため、推測しにくいパスワードを設定する、パスワードを定期的に変更する、ログインの試行回数に制限を設けるなどの方法で被害を防ぐことができます。

２）Web アプリケーションの脆弱性

Web アプリケーションの脆弱性を利用した代表的な攻撃手法は次のとおりです。

①クロスサイトスクリプティング

クロスサイトスクリプティングは、悪意をもったスクリプトを、標的となるサイト経由で利用者のブラウザに送り込み、その標的にアクセスした利用者のクッキー（Cookie）にある個人情報を盗み取る攻撃手法です。

②クロスサイトリクエストフォージェリ

クロスサイトリクエストフォージェリは、Web サイトに不正なスクリプトや HTTP リダイレクト（自動転送）などを埋め込むことで、閲覧者の意図に関わらず別の Web サイトを不正に操作させる攻撃手法です。

③クリックジャッキング

クリックジャッキングは、Web サイトのコンテンツ上に透明化した標的サイトのコンテンツを配置し、利用者が気づかないうちに標的サイト上で意図に反した操作を実行させる攻撃手法です。

④ドライブバイダウンロード

ドライブバイダウンロードは、Web サイトにアクセスした利用者に気付かれないように、自動的にマルウェアなどをダウンロードし実行する攻撃手法です。

⑤SQL インジェクション

SQL インジェクションは、Web ページ上で利用者がデータを入力する欄（入力フォーム）に、SQL 文を閉じる区切り文字と不正なコマンドを埋め込むことで、データベース内のレコードを不正に操作して、レコードに含まれる情報の改ざん、消去、盗聴などを行う攻撃手法です。

⑥ディレクトリトラバーサル

ディレクトリトラバーサルは、ファイルを Web アプリケーションが使用する場合に、相対パス指定を悪用し、サーバ内の想定外のファイル名を直接指定することによって、本来は許されないファイルを不正に閲覧する攻撃手法です。

例題 1-11　　基本情報　平成 27 年春　問 42

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

解答－ア

イ　クロスサイトリクエストフォージェリに関する記述です。

ウ　ワームに関する記述です。

エ　クロスサイトスクリプティングに関する記述です。

ここで演習 1-23～1-25 を解いて下さい

3）ネットワークの脆弱性

ネットワークの脆弱性を利用した代表的な攻撃手法は次のとおりです。

①中間者攻撃

中間者攻撃（Man-in-the-middle attack）は、送信者と受信者の間に介在し、当事者に成りすまして通信内容を横取りする攻撃手法です。

②第三者中継

第三者中継は、自分とは無関係の第三者のメールサーバを不正に中継することで、送信者が身元を偽ってメールを送信する攻撃手法です。

③IP スプーフィング

IP スプーフィングは、偽の IP アドレスを使いファイアウォールを突破してネットワークに侵入する攻撃手法です。

④DNS キャッシュポイズニング

DNS キャッシュポイズニングは、DNS サーバの情報を不正に書き換えることで、インターネットの閲覧者を偽の Web サイトに誘導する攻撃手法です。

⑤セッションハイジャック

セッションハイジャックは、セッション ID やセッションクッキーを盗んで、利用者になりすまして不正アクセスする攻撃手法です。

⑥リプレイ攻撃

リプレイ攻撃は、正当な利用者のログインシーケンスを記録して盗聴することで、利用者になりすまして不正アクセスする攻撃手法です。ログインシーケンスとは、ログインするための一連の手続きを指します。

例題 1-12　　応用情報　平成 27 年春　問 37

DNS キャッシュポイズニングに分類される攻撃内容はどれか。

ア　DNS サーバのソフトのバージョン情報を入手して，DNS サーバのセキュリティホールを特定する。
イ　PC が参照する DNS サーバに誤ったドメイン管理情報を注入して，偽装された Web サーバに PC の利用者を誘導する。
ウ　攻撃対象のサービスを妨害するために，攻撃者が DNS サーバを踏み台に利用して再帰的な問合せを大量に行う。
エ　内部情報を入手するために，DNS サーバが保存するゾーン情報をまとめて転送させる。

解答ーイ

ア　攻撃する前の事前調査であるバナーチェックに関する記述です。
ウ　DDoS攻撃に関する記述です。
エ　ゾーン転送を利用した攻撃をする前の事前調査です。

ここで演習 1-26～1-29 を解いて下さい

4）サービス妨害

CPU やサーバ、ネットワークに過大な負荷をかけることで利用者へのサービスの提供を妨害する代表的な攻撃手法は次のとおりです。

①DoS 攻撃

DoS 攻撃は、攻撃目標のサーバに大量のデータを送信して過大な負荷をかけることで、サービスの低下や停止に追い込む攻撃手法です。

②DDoS 攻撃

DDoS 攻撃は、複数の全く関係のない第三者のコンピュータに攻撃プログラムを仕掛けて踏み台にすることで、標的とするサーバに一斉にデータを送信し、過大な負荷をかけて、サービスの低下や停止に追い込む攻撃手法です。

③メールボム

メールボムは、サイズが大きい電子メールや大量の電子メールを送り付ける攻撃手法です。

例題 1-13　　IT パスポート　平成 25 年春　問 52

DoS（Denial of Service）攻撃の説明として，適切なものはどれか。

ア　他人になりすまして，ネットワーク上のサービスを不正に利用すること
イ　通信経路上で他人のデータを盗み見ること
ウ　電子メールや Web リクエストなどを大量に送りつけて，ネットワーク上のサービスを提供不能にすること
エ　文字の組合せを順に試すことによって，パスワードを解読しようとすること

解答－ウ
ア　なりすましに関する記述です。
イ　盗聴に関する記述です。
エ　ブルートフォース攻撃に関する記述です。

ここで演習 1-30 を解いて下さい

５）標的型攻撃

特定の企業や組織を狙った**標的型攻撃**の代表的な攻撃手法は次のとおりです。

①APT

APT（Advanced Persistent Threats）は、特定の企業や組織に狙いを定め、複数の手段を組み合わせてシステムに侵入・潜伏し、データの盗聴や改ざんなどの攻撃を長期間継続して行う攻撃手法です。

②水飲み場型攻撃

水飲み場型攻撃は、標的となる企業や組織の構成員が頻繁にアクセスする Web サイトを改ざんし、当該構成員がアクセスした時だけマルウェアに感染するようにした攻撃手法です。

例題 1-14　　応用情報　平成 26 年秋　問 37

APT（Advanced Persistent Threats）の説明はどれか。

ア　攻撃者は DoS 攻撃及び DDoS 攻撃を繰り返し組み合わせて，長期間にわたって特定組織の業務を妨害する。
イ　攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す。
ウ　攻撃者は特定の目的をもち，特定組織を標的に複数の手法を組み合わせて気付かれないよう執拗に攻撃を繰り返す。
エ　攻撃者は不特定多数への感染を目的として，複数の攻撃を組み合わせたマルウェアを継続的にばらまく。

解答ーウ

特定の個人や組織に対する攻撃を標的型攻撃と呼びます。その中で、複数の手法を組み合わせて持続的に行われるものは、APT（Advanced Persistent Threats：持続的標的型攻撃）と呼ばれます。

ここで演習 1-31 を解いて下さい

６）近年深刻化する脅威

上記以外に、近年深刻化する脅威には次のようなものがあります。

①フィッシング

偽のメールや Web サイトを用いて、個人情報やクレジットカード番号、パスワードなどの情報を不正に入手する行為を**フィッシング**と呼びます。

代表例	説明
ワンクリック詐欺	メールや Web サイトに記載されている URL を一度クリックしただけで一方的に契約を了承したことにされて代金を請求する手法
スミッシング	携帯電話のショートメッセージサービスを利用したフィッシング

②ゼロデイ攻撃

ゼロデイ攻撃は、セキュリティの脆弱性が公表される（セキュリティパッチが提供される）前にセキュリティホールに対して行われる攻撃手法です。

例題 1-15　　IT パスポート　平成 23 年秋　問 87

フィッシングの説明として，最も適切なものはどれか。

ア　ウイルスに感染したコンピュータを，そのウイルスの機能を利用することによってインターネットなどのネットワークを介して外部から不正に操作する。
イ　偽の電子メールを送信するなどして，受信者を架空の Web サイトや実在している Web サイトの偽サイトに誘導し，情報を不正に取得する。
ウ　利用者が入力したデータをそのままブラウザに表示する機能が Web ページにあるとき，その機能の脆弱性を突いて悪意のあるスクリプトを埋め込み，そのページにアクセスした他の利用者の情報を不正に取得する。
エ　利用者に気づかれないように PC にプログラムを常駐させ，ファイルのデータや PC 操作の情報を不正に取得する。

解答ーイ
ア　ボットに関する記述です。
ウ　クロスサイトスクリプティングに関する記述です。
エ　スパイウェアに関する記述です。

ここで演習 1-32、1-33 を解いて下さい

04 情報セキュリティ技術（暗号技術）

1．CRYPTREC 暗号リスト（電子政府推奨暗号リスト）

CRYPTREC 暗号リストは、総務省と経済産業省が共同で運営する暗号技術検討会及び関連委員会（CRYPTREC）が、安全性と実装性能が確認された暗号技術のうち、電子政府の調達時に利用することを推奨する暗号技術のリストです。

後述する AES や RSA の一種や、SHA-246 などがリストに掲載されています。

例題 1-16　　情報セキュリティスペシャリスト　平成 26 年秋　午前Ⅱ　問 8

CRYPTREC の活動内容はどれか。

ア　暗号技術の安全性，実装性及び利用実績の評価・検討を行う。
イ　情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ政策の推進に係る企画などを行う。
ウ　組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。
エ　認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。

解答ーア

イ　内閣官房情報セキュリティセンタに関する記述です。
ウ　情報マネジメントシステム推進センタに関する記述です。
エ　JCMVP（Japan Cryptographic Module Validation Program）に関する記述です。

２．暗号方式

データを権限なしの照会や使用から保護する方法に、暗号化技術があります。通信データの漏えいや改ざんといった犯罪を防止するためには暗号化は欠かせません。

暗号化とは、データを第三者が解読できないように一定のルールで変換することで、暗号化する前のデータを平文（Plane Text）、暗号化されたデータを暗号文（Cipher Text）と呼びます。また、暗号文を平文に戻すことを**復号**といいます。

暗号化の代表的な方法には、共通鍵（秘密鍵）暗号方式と公開鍵暗号方式があります。

例題 1-17　　IT パスポート　平成 21 年秋　問 62

小文字の英字からなる文字列の暗号化を考える。次表で英字を文字番号に変換し，変換後の文字番号について１文字目分には１を，２文字目分には２を，…，ｎ文字目分にはｎを加える。それぞれの数を 26 で割った余りを新たに文字番号とみなし，表から対応する英字に変換する。

例　fax　→　6, 1, 24　→　6+1, 1+2, 24+3　→　7, 3, 27　→　7, 3, 1　→　gca

この手続きで暗号化した結果が“tmb”であるとき，元の文字列はどれか。

文字番号	1	2	3	4	5	6	7	8	9	10	11	12	13
英字	a	b	c	d	e	f	g	h	i	j	k	l	m

文字番号	14	15	16	17	18	19	20	21	22	23	24	25	26
英字	n	o	p	q	r	s	t	u	v	w	x	y	z

ア　she　　イ　shy　　ウ　ski　　エ　sky

解答－エ

例のように記述すると次のようになります。

???　→　?, ?, ?　→　?+1, ?+2, ?+3　→　?, ?, ?　→　?, ?, ?　→　tmb

結果の“tmb”をそれぞれ文字番号にすると次のようになります。

???→?, ?, ?→?+1, ?+2, ?+3→?, ?, ?→ 20, 13, 2→tmb

この値は 26 で割った余りですから、26 で割る前の数字と異なる場合があります。

ｎ文字目の文字番号にｎの値を加えているので、３文字目には３を加えているのですが、３文字目に対応する数値が４よりも小さいため、余りの値になっていることが分かります。つまり、１段階前は次のようになります。

???　→　?, ?, ?　→　?+1, ?+2, ?+3　→　20, 13, 28　→　20, 13, 2　→　tmb

残りの数値を逆算すると、全体は次のようになります。

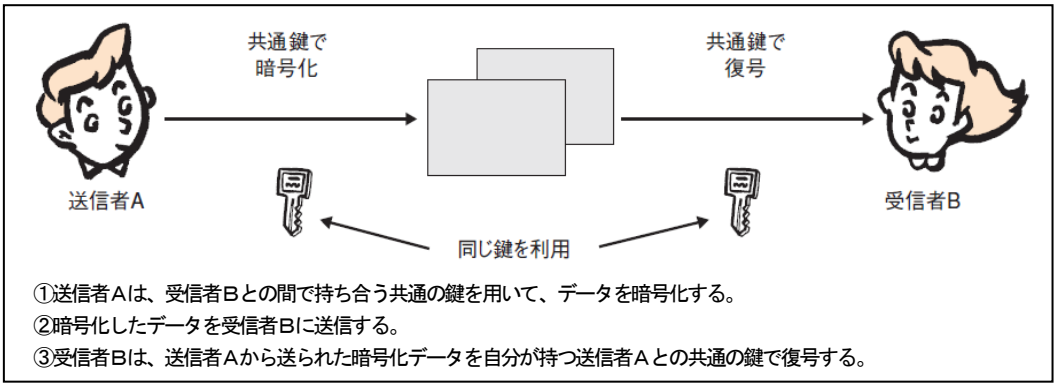
sky　→　19, 11, 25　→　19+1, 11+2, 25+3　→　20, 13, 28　→　20, 13, 2　→　tmb

ここで演習 1-34、1-35 を解いて下さい

３．共通鍵暗号方式

共通鍵暗号方式は、暗号化も復号も共通の鍵を用いる方式です。そのため、鍵情報は公開せずに秘密にします。この方式では、仮にN人の相手とデータのやり取りをする場合にはN個の鍵を必要とするため、鍵の管理が問題となります。また、鍵情報を安全に相手方に渡す方法を工夫する必要があります。

代表的な暗号化アルゴリズムに、**AES** があります。



共通鍵暗号方式

例題 1-18　　情報セキュリティスペシャリスト　平成 25 年秋　午前Ⅱ　問 3

共通鍵暗号方式で，100 人の送受信者のそれぞれが，相互に暗号化通信を行うときに必要な共通鍵の総数は幾つか。

ア　200　　イ　4,950　　ウ　9,900　　エ　10,000

解答－イ

共通鍵暗号方式では、平分を暗号化、暗号文を復号するために、同一の鍵を使用します。

例えば、３人のグループ（A、B、C）で共通鍵暗号方式を採用した場合、AはBとCに対し、別々の鍵を渡すことで「AとB」「AとC」の送受信を行うことになります。また、同様にBとCに関しても、自分以外のメンバ分だけ異なる鍵を渡す必要があります。

つまり、各人が持っている鍵の総和は「（人数－１）×人数」となります。ただし、鍵の種類で考えると、Aが渡したBの共通鍵と、BのAに対する鍵は同一のものとなるため、共通鍵の総数としては「（人数－１）×人数÷２」となります。

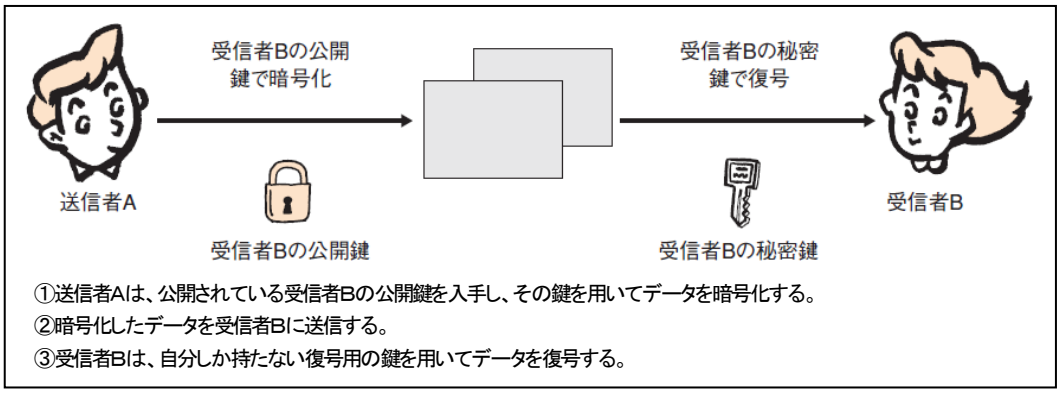
したがって、必要な鍵の個数は「（100－１）×100÷２＝4,950 個」となります。

ここで演習 1-36、1-37 を解いて下さい

４．公開鍵暗号方式

公開鍵暗号方式は、データ受信者の**公開鍵**（暗号化のための鍵情報と暗号化アルゴリズムを不特定多数の者に公開）を使ってデータを暗号化する方式です。暗号化と復号のための鍵情報は共通でなく、復号のための鍵情報は**秘密鍵**としては公開しません。暗号文の受信者は、公開鍵と対の秘密鍵で復号します。この方式は、暗号化に使う鍵を公開できるため、不特定多数との通信に向いています。ただし、一方の公開している鍵から、秘密にしている鍵を割り出せることがあるため、共通鍵暗号方式に比べて、鍵情報を複雑にする必要があり、暗号化に多くの時間が必要となります。

代表的な暗号化アルゴリズムに、開発者の頭文字（Rivest、Shamir、Adleman）を取って命名された**RSA** があります。



公開鍵暗号方式

例題 1-19　　基本情報　平成 27 年秋　問 38

Ｘさんは，Ｙさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので，公開鍵暗号方式を用いて暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

ア　Ｘさんの公開鍵　　イ　Ｘさんの秘密鍵
ウ　Ｙさんの公開鍵　　エ　Ｙさんの秘密鍵

解答－ウ

公開鍵暗号方式は、暗号化鍵と復号鍵に異なる鍵を用い、暗号化鍵を公開して、復号鍵を秘密にしておく方式です。

この方式を使って通信する場合には、公開されている相手（受信者）の公開鍵を使って平文を暗号化して送信します。その暗号化情報を受信して、正しく復号できるのは受信者の秘密鍵であり、受信者は公開鍵と対をなす秘密鍵を使用して、元のメッセージに復号します。

ここで演習 1-38～1-41 を解いて下さい

５．ハイブリッド暗号方式

共通鍵暗号方式と公開鍵暗号方式は相反する性質をもっており、これらを組み合わせることで互いの問題点を解決したのが、ハイブリッド暗号方式です。

暗号方式	性質
共通鍵暗号方式	公開鍵暗号方式に比べ処理は高速ですが、鍵情報を安全に配布することが難しい。
公開鍵暗号方式	鍵情報の管理は容易ですが、処理に時間がかかる

ハイブリッド暗号方式では、通信したいデータの暗号化には、処理が高速な共通鍵暗号方式を用います。そして、その共通鍵を相手に渡す手段として公開鍵暗号方式を用いる方式です。まずデータを共通鍵で暗号化します。次に、受信者の公開鍵でデータを暗号化するために使った鍵情報（共通鍵）を暗号化し、暗号化したデータとともに受信者に送信します。受信者は、送信者から送られてきた鍵情報（共通鍵）を自分の秘密鍵を用いて復号し、復号された共通鍵を使って暗号化されたデータを復号します。

例題 1-20　　基本情報　平成 22 年秋　問 41

手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。

[手順]
⑴　送信者は，電子メールの本文を共通鍵暗号方式で暗号化し（暗号文），その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する。（共通鍵の暗号化データ）
⑵　送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。
⑶　受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号化方式で復号し，得た共通鍵で暗号文を復号する。

ア　送信者による電子メールの送達確認
イ　送信者のなりすましの検出
ウ　電子メールの本文の改ざんの有無の検出
エ　電子メールの本文の内容の漏えいの防止

解答－エ

データの暗号化と復号に共通鍵暗号方式を用い、その際の共通鍵を公開鍵暗号方式で暗号化して相手に送る方法を、ハイブリッド暗号方式と呼びます。
ア　電子メールの送達の確認は、受信者側から受信の旨を返信してもらうことで確認します。
イ　送信者のなりすましの検出には、公開鍵暗号方式を応用したディジタル署名を用います。
ウ　電子メール本文の改ざんの有無を検出するには、メッセージ認証符号を用います。

ここで演習 1-42 を解いて下さい

６．ハッシュ関数

データ（メッセージ）をそのサイズに関わらず 128 から 512 ビット程度の一定のサイズに変換する関数を**ハッシュ関数**と呼び、ハッシュ関数によって演算した結果をハッシュ値（**メッセージダイジェスト**）と呼びます。ハッシュ関数から得られたハッシュ値は、異なるデータが同じ値になることがほとんどありません。

代表的なハッシュ関数に、可変長のデータから 256 ビットのハッシュ値を生成する **SHA-256** があります。

例題 1-21　　基本情報　平成 27 年春　問 43

Web サーバのコンテンツの改ざんを検知する方法のうち，最も有効なものはどれか。

ア　Web サーバのコンテンツの各ファイルの更新日を保管しておき，定期的に各ファイルの更新日と比較する。
イ　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生成したハッシュ値と比較する。
ウ　Web サーバのメモリ使用率を定期的に確認し，バッファオーバフローが発生していないことを確認する。
エ　Web サーバへの通信を監視し，HTTP，HTTPS 以外の通信がないことを確認する。

解答ーイ

保管していたハッシュ値と比較して値が異なれば改ざんされたことになります。

ア　更新日を改ざんすることもできます。
ウ　バッファオーバフロー攻撃は、特定のサーバに大量のデータを送信してメモリ領域をあふれ（オーバフロー）させて、システムを停止させる行為や、あふれ出たデータを実行させる行為で、改ざんとは関係ありません。
エ　HTTP、HTTPS 以外の通信がなくても、SQL インジェクション攻撃などによりコンテンツが改ざんされることがあります。

ここで演習 1-43 を解いて下さい

７．S/MIME

S/MIME（Secure MIME）は、画像や音声などのマルチメディアデータをメールで送信するためのプロトコルである MIME に暗号化機能を加えたプロトコルです。

S/MIME を使ってメッセージを送信することで、盗聴、改ざんを防ぐことができます。

なお S/MIME では、メッセージ本文の暗号化に共通鍵暗号方式を用い、共通鍵の受渡しには公開鍵暗号方式を用いるので、受信者はあらかじめ自身の公開鍵が本物であることを証明する公開鍵証明書を取得しておく必要があります。

例題 1-22　　IT パスポート　平成 24 年秋　問 56

ＡさんがＢさんに暗号化メールを送信したい。S/MIME（Secure/Multipurpose Internet Mail Extensions）を利用して暗号化したメールを送信する場合の条件のうち，適切なものはどれか。

ア　Ａさん，Ｂさんともに，あらかじめ，自身の公開鍵証明書の発行を受けておく必要がある。

イ　Ａさん，Ｂさんともに，同一の ISP（Internet Service Provider）に属している必要がある。

ウ　Ａさんが属している ISP が S/MIME に対応している必要がある。

エ　Ｂさんはあらかじめ，自身の公開鍵証明書の発行を受けておく必要があるが，Ａさんはその必要はない。

解答－エ

Ａさんは、まず、メール本文を共通鍵で暗号化し、共通鍵をＢさんの公開鍵を使用して暗号化して暗号化したメール本文と一緒にＢさんに送信します。このときＡさんは、Ｂさんの公開鍵が本物であるかどうかを判断するために、Ｂさんの公開鍵証明書を確認します。

Ｂさんは、Ａさんから送られた暗号化された共通鍵を自分のもつ秘密鍵で復号し、その共通鍵を用いて暗号化されたメール本文を復号します。

ここで演習 1-44、1-45 を解いて下さい

８．PGP

PGP（Pretty Good Privacy）は、S/MIME と同様に、メッセージ本文の暗号化に共通鍵暗号方式を用い、共通鍵の受渡しには公開鍵暗号方式を用いる暗号方式ですが、事前に当事者間で公開鍵を交換することを前提としているため、公開鍵の所有者を保証する仕組みは必要としません。また、入手した公開鍵が有効性を確認する仕組みもありません。

９．危殆化

危殆化とは、「危険な状態になる」という意味で、コンピュータの処理能力の向上や暗号解読技術の進歩は、既存の暗号化技術の危殆化を招いています。

例題 1-23　　応用情報　平成 25 年春　問 37

暗号アルゴリズムの危殆化を説明したものはどれか。

ア　外国の輸出規制によって十分な強度を持つ暗号アルゴリズムを実装した製品が利用できなくなること
イ　鍵の不適切な管理によって，鍵が漏えいする危険性が増すこと
ウ　計算能力の向上などによって，鍵の推定が可能となり，暗号の安全性が低下すること
エ　最高性能のコンピュータを用い，膨大な時間やコストを掛けて暗号強度をより確実なものとすること

解答－ウ

危殆化（Compromise）とは、セキュリティ上の安全が脅かされ得る状態になることをいいます。コンピュータの計算能力の向上などにより、暗号化アルゴリズムのうちいくつかは安全性が低下しつつあります。

05 情報セキュリティ技術（認証技術）

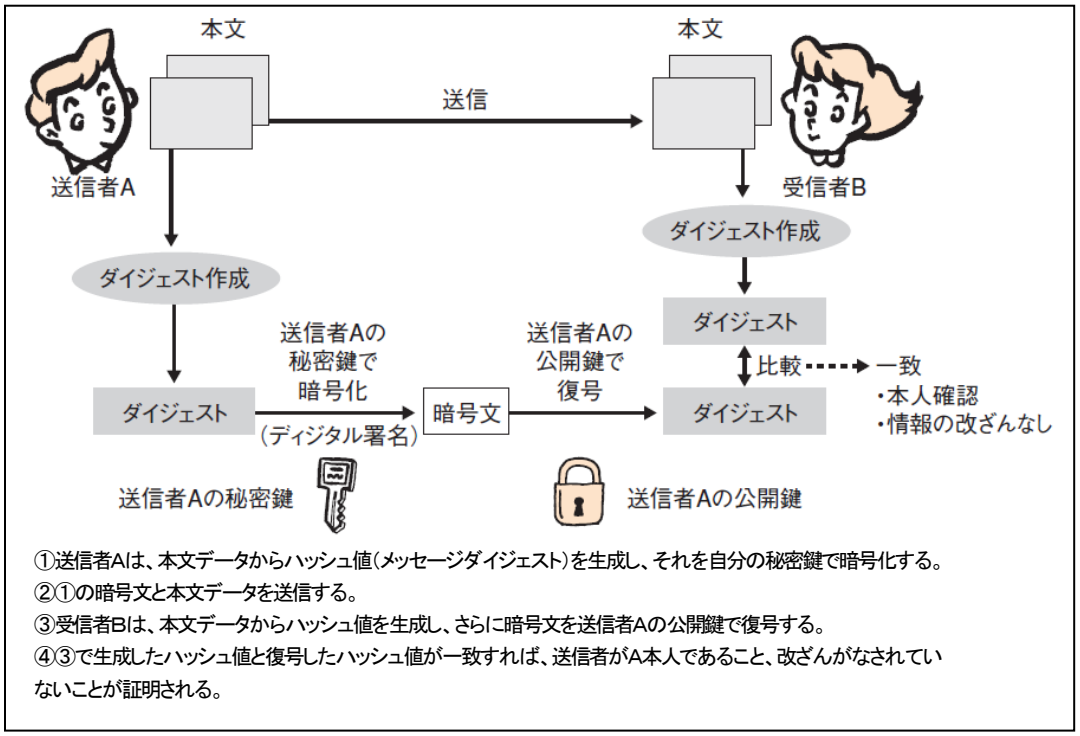
対象物の正当性を証明する方法を認証技術と呼びます。

代表的な認証技術に、ディジタル署名、タイムスタンプ、メッセージ認証、チャレンジレスポンス認証があります。

1．ディジタル署名

ディジタル署名（電子署名）は、データが正当な送り手からのものであることを証明する（送信者認証）と同時に、改ざんされていないことを証明する（メッセージ認証）方法です。

ディジタル署名は、公開鍵暗号方式を応用した方法で、公開鍵暗号方式が受信者の公開鍵で暗号化するのに対して、ディジタル署名は送信者の秘密鍵で暗号化する点が異なります。これは、「送信者の秘密鍵で暗号化したデータは、送信者の公開鍵のみで復号できる」ということから、データの送り手を証明するものです。なお、送信者の秘密鍵を**署名鍵**、送信者の公開鍵を**検証鍵**と呼ぶことがあります。



①送信者Aは、本文データからハッシュ値（メッセージダイジェスト）を生成し、それを自分の秘密鍵で暗号化する。
②①の暗号文と本文データを送信する。
③受信者Bは、本文データからハッシュ値を生成し、さらに暗号文を送信者Aの公開鍵で復号する。
④③で生成したハッシュ値と復号したハッシュ値が一致すれば、送信者がA本人であること、改ざんがなされていないことが証明される。

ディジタル署名

例題 1-24　　基本情報　平成 27 年春　問 38

ディジタル署名における署名鍵の用い方と、ディジタル署名を行う目的のうち、適切なものはどれか。

ア　受信者が署名鍵を使って、暗号文を元のメッセージに戻すことができるようにする。
イ　送信者が固定文字列を付加したメッセージを、署名鍵を使って暗号化することによって、受信者がメッセージの改ざん部位を特定できるようにする。
ウ　送信者が署名鍵を使って署名を作成し、それをメッセージに付加することによって、受信者が送信者を確認できるようにする。
エ　送信者が署名鍵を使ってメッセージを暗号化することによって、メッセージの内容を関係者以外に分からないようにする。

解答－ウ

ディジタル署名は、メッセージが正当な送り手からのものであることを証明すると同時に、改ざんされていないことを証明する方法で、具体的な手順は次の通りです。

① 送信者は一定の手順でメッセージのハッシュ値を生成し、それを送信者自身の秘密鍵で暗号化し、本文データと共に送信します。秘密鍵を署名鍵と呼びます。
② 受信者は受け取った本文データから同一の手順でハッシュ値を生成します。同時に受け取った暗号化されたハッシュ値を送信者の公開鍵で復号します。公開鍵を検証鍵と呼びます。
③ 受信者が生成したハッシュ値と復号したハッシュ値が一致すれば、正当な送り手からのデータであり、改ざんされていないことが証明されます。

ここで演習 1-46、1-47 を解いて下さい

2．タイムスタンプ

タイムスタンプ（時刻認証）は、データが存在していた日時を記録した情報です。第三者機関（タイプスタンプ機関）がタイムスタンプを付与したデータにディジタル署名することで、タイムスタンプの正当性と完全性を保証します。

ディジタル署名されたデータを公開する場合、タイムスタンプを利用すると、公開されたデータがまさしく本人のものであることと同時に、公開以前にデータが存在していたことを示し、データの作成を否認することを防ぎます。

例題 1-25　システム監査　平成 23 年春　午前Ⅱ　問 20

手順に示す処理を行ったとき，検証できることはどれか。

[手順]
⑴　送信者Ａはファイルハッシュ値を計算して，信頼できる第三者機関に送信する。
⑵　第三者機関は，信頼できる日時を保持しており，受診したハッシュ値とその受信日時を結合し（結合データ），そのディジタル署名を生成し，ディジタル署名と結合データの組（ディジタル署名済みの結合データ）を送信者Ａに返信する。
⑶　送信者Ａはファイルと第三者機関から送られてきたディジタル署名済みの結合データを受信者Ｂに送信する。
⑷　受信者Ｂは第三者機関のディジタル署名を確認し，ファイルから計算したハッシュ値と，ディジタル署名済みの結合データから取り出されたハッシュ値を照合する。そして，結合データから取り出された日時を確認する。

ア　当該日時でのファイルの存在と，それ以降にファイルが改ざんされていないこと
イ　当該日時に受信者Ｂにファイルが到達したこと
ウ　当該日時に送信者Ａが受信者Ｂにファイルを送信したこと
エ　当該日時にファイルが作成されたこと

解答ーア

この問題はタイプスタンプ付与の手順を示しています。

ファイルから計算したハッシュ値と、ディジタル署名済みの結合データから取り出されたハッシュ値が一致すれば、受信日時にファイルが存在していたことと、ファイルは改ざんされていないことが証明されます。

ここで演習 1-48 を解いて下さい

３．メッセージ認証

メッセージ認証は、受け取ったデータ（メッセージ）が改ざんされていないことを確認する方法です。

ハッシュ値は、異なるデータが同じ値になることがほとんどありません。そのため、送信者はデータと共にそのハッシュ値を送信し、受信者は受け取ったデータからハッシュ値を生成し、これと送信者から受け取ったハッシュ値との一致を確認することで、データが改ざんされていないことを確認できます。

例題 1-26　　基本情報　平成 24 年春問 40

送信者からメール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者がメール本文から求めたハッシュ値とを比較することで実現できることはどれか。ここで，受信者が送信者から受け取るハッシュ値は正しいものとする。

ア　電子メールの送達の確認
イ　電子メール本文の改ざんの有無の検出
ウ　電子メール本文の盗聴の防止
エ　なりすましの防止

解答ーイ

ア　電子メールの送達の確認は、受信者側から受信の旨を返信してもらうことで確認します。
ウ　電子メール本文の盗聴の防止は、暗号化によって行います。
エ　送信者へのなりすましの防止は、送信者が自身の情報を認証機関に登録し、受信者がこれを利用することで行います。

ここで演習 1-49 を解いて下さい

４．メッセージ認証符号

メッセージ認証符号（**MAC**：Message Authentication Code）は、送信データに共通鍵をつけてハッシュ化したデータ（メッセージダイジェスト）です。

送信者はデータ（メッセージ）とともにメッセージ認証符号を送信し、受信者は受け取ったデータからメッセージ認証符号を作成し、これと送信者から受け取ったメッセージ認証符号との一致を確認することによって、データの正当性を証明します（メッセージ認証）。

例題 1-27　　基本情報　平成 26 年春問 36

メッセージ認証符号におけるメッセージダイジェストの利用目的はどれか。

ア　メッセージが改ざんされていないことを確認する。
イ　メッセージの暗号化方式を確認する。
ウ　メッセージの概要を確認する。
エ　メッセージの秘匿性を確保する。

解答－ア

受信者は、送信者から受け取ったメッセージ（データ）から作成したメッセージダイジェストと、送信者から受け取ったメッセージダイジェストが一致すれば、メッセージが改ざんされていないことを確認できます。

ここで演習 1-50 を解いて下さい

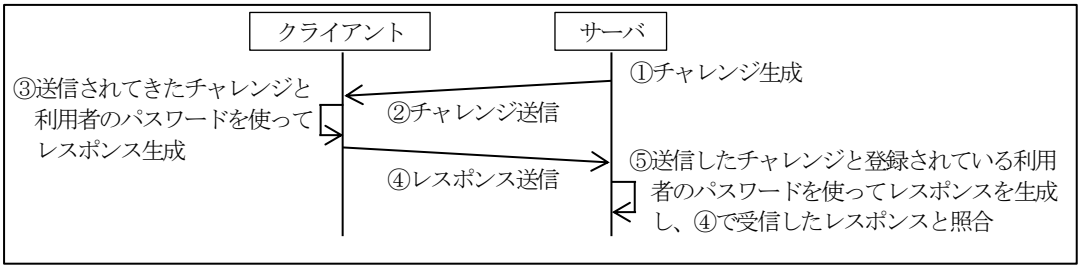
５．チャレンジレスポンス認証

チャレンジレスポンス認証方式は、ネットワークにおける利用者認証の方式です。

クライアントは、利用者が入力したパスワードと、サーバから送られてきたランダムなデータであるチャレンジからレスポンスと呼ばれるデータを生成し、サーバに送り返します。

サーバは送信したチャレンジと利用者があらかじめ登録したパスワードからレスポンスを生成し、利用者から送られてきたレスポンスと照合します。両者の一致を確認することで利用者の正当性を確認します。

なお、チャレンジレスポンス認証を用いることで、パスワード自体が通信されないため、ネットワーク上でのパスワードの漏えいと、リプレイ攻撃を防ぐことができます。



例題 1-28　応用情報　平成 24 年春　問 39

手順に示すクライアントとサーバの処理と通信で可能になることはどれか。

[手順]
(1)　サーバはクライアントから要求があるたびに異なる予測困難な値（チャレンジ）を生成して保持するとともに，クライアントへ送る。
(2)　クライアントは利用者が入力したパスワードのメッセージダイジェストを計算し，(1)でサーバから送られた“チャレンジ”と合わせたものから，さらに，メッセージダイジェスト（レスポンス）を計算する。この“レスポンス”と利用者が入力した利用者 ID をサーバに送る。
(3)　サーバは，クライアントから受け取った利用者 ID で利用者情報を検索して，取り出したパスワードのメッセージダイジェストと(1)で保持していた“チャレンジ”を合わせたものから，メッセージダイジェストを計算する（レスポンス照合データ）。この“レスポンス照合データ”とクライアントから受け取った“レスポンス”とを比較する。

ア　伝送上で発生したパスワードのビット誤りのサーバでの訂正
イ　伝送上で発生した利用者 ID のビット誤りのサーバでの訂正
ウ　ネットワーク上でのパスワードの，漏えい防止とリプレイ攻撃の防御
エ　ネットワーク上での利用者 ID の，漏えい防止とリプレイ攻撃の防御

解答－ウ
〔手順〕(2)に記述されているように、利用者が入力したパスワードは、「予測困難な値（チャレンジ）」を用いて変換されてからサーバに送られるため、パスワードが盗まれることはありません。また、チャレンジは、〔手順〕(1)に記述されているように、クライアントから要求があるたび生成されるので、リプレイ攻撃を防ぐことができます。

ここで演習 1-51 を解いて下さい