

平成28年度後期 情報検定

<実施 平成29年2月12日（日）>

システムデザインスキル

（説明時間 14：30～14：40）

（試験時間 14：40～16：10）

- ・試験問題は試験開始の合図があるまで開かないでください。
- ・解答用紙（マークシート）への必要事項の記入は、試験開始の合図と同時に行いますので、それまで伏せておいてください。
- ・試験開始の合図の後、次のページを開いてください。＜受験上の注意＞が記載されています。必ず目を通してから解答を始めてください。
- ・試験問題は、すべてマークシート方式です。正解と思われるものを1つ選び、解答欄の○をHBの黒鉛筆でぬりつぶしてください。2つ以上ぬりつぶすと、不正解になります。
- ・辞書、参考書類の使用および筆記用具の貸し借りは一切禁止です。
- ・電卓の使用が認められます。ただし、下記の機種については使用が認められません。

<使用を認めない電卓>

1. 電池式（太陽電池を含む）以外の電卓
2. 文字表示領域が複数行ある電卓（計算状態表示の一行は含まない）
3. プログラムを組み込む機能がある電卓
4. 電卓が主たる機能ではないもの
 - *パソコン（電子メール専用機等を含む）、携帯電話（PHS）、スマートフォン、タブレット、電子手帳、電子メモ、電子辞書、翻訳機能付き電卓、音声応答のある電卓、電卓付き腕時計、時計型ウェアラブル端末等
5. その他試験監督者が不適切と認めるもの

＜受験上の注意＞

1. この試験問題は14ページあります。ページ数を確認してください。
乱丁等がある場合は、手をあげて試験監督者に合図してください。
※問題を読みやすくするために空白ページを設けている場合があります。
2. 解答用紙（マークシート）に、受験者氏名・受験番号を記入し、受験番号下欄の数字をぬりつぶしてください。正しく記入されていない場合は、採点されませんので十分注意してください。
3. 試験問題についての質問には、一切答えられません。自分で判断して解答してください。
4. 試験中の筆記用具の貸し借りは一切禁止します。筆記用具が破損等により使用不能となった場合は、手をあげて試験監督者に合図してください。
5. 試験を開始してから30分以内は途中退出できません。30分経過後退出する場合は、もう一度、受験番号・マーク・氏名が記載されているか確認して退出してください。なお、試験終了5分前の合図以降は退出できません。試験問題は各自お持ち帰りください。
6. 試験後にお知らせする合否結果（合否通知）、および合格者に交付する「合格証・認定証」はすべて、Webページ（PC、モバイル）での認証によるデジタル「合否通知」、デジタル「合格証・認定証」に移行しました。
 - ①団体宛にはこれまでと同様に合否結果一覧ほか、試験結果資料一式を送付します。
 - ②合否等の結果についての電話・手紙等でのお問い合わせには、一切応じられませんので、ご了承ください。

問題を読みやすくするために、
このページは空白にしてあります。

問題 1 次の経営戦略に関する各設問に答えよ。

<設問 1> 次の PPM に関する記述中の に入れるべき適切な字句を解答群から選べ。

PPM (Product Portfolio Management) とは、自社の事業を市場の成長率 (以下, 成長率) と相対的な市場の占有率 (以下, シェア) により「花形」, 「金のなる木」, 「問題児」, 「負け犬」に分類し、今後の投資戦略をどうするかなどを検討する。

J 社は国内向けの家電製品を製造しており、次の 4 つの製品を分析した。

表 製品の分析

製品	分析結果
LED 照明機器	従来の電球や蛍光灯に比べて高価ながらも寿命が長く電力消費量が少ないことから普及が進んで成長率が高くなっている。J 社の販売戦略が成功したため、J 社のシェアは高くなった。
液晶テレビ	大画面化・高画質化が進んでいるが、国内販売数は減少し、成長率は低いと言える。海外の安い製品などにシェアを奪われつつあり、J 社のシェアは低い。
ヘッドフォン	スマートフォンなどの携帯情報端末を所有する人が増えており、音楽プレイヤーとして利用する人も多い。成長率は高いと思われるが、J 社の認知度が低いことが影響して J 社のシェアは低い。
愛玩ロボット	コンピュータを内蔵した動物型のロボットである。他社でも同種の製品が販売されてブームを作ったが、最近は業界全体で販売数が横ばいである。撤退する企業が相次いでいるが、J 社の製品は販売量が安定しており、シェアは高い位置をキープしている。

これらから、「花形」となる製品は (1) , 「金のなる木」となる製品は (2) , 「問題児」となる製品は (3) , 「負け犬」となる製品は (4) である。
PPM では、 (5) で得た利益を (6) に投資してその事業を成長させる。

(1) ~ (4) の解答群

- | | |
|-------------|-----------|
| ア. LED 照明機器 | イ. 愛玩ロボット |
| ウ. 液晶テレビ | エ. ヘッドフォン |

(5) の解答群

- | | | | |
|----------|-------|--------|--------|
| ア. 金のなる木 | イ. 花形 | ウ. 負け犬 | エ. 問題児 |
|----------|-------|--------|--------|

(6) の解答群

- | | | |
|-----------|-----------|------------|
| ア. 花形や負け犬 | イ. 花形や問題児 | ウ. 負け犬や問題児 |
|-----------|-----------|------------|

<設問 2 > 次の SWOT 分析に関する記述中の [] に入れるべき適切な字句を解答群から選べ。

SWOT 分析とは、内部環境における強みと弱み、外部環境における機会と脅威の 4 つのカテゴリで分析し、事業戦略を考えるためのフレームワークである。

IT 企業の P 社で行った SWOT 分析は、表のようになった。

表 SWOT 分析

強み (Strengths)	機会 (Opportunities)
<ul style="list-style-type: none">・ネットワーク技術に高い評価を得ている・ホスティングのシェアが高い	<ul style="list-style-type: none">・クラウド環境への関心が高い・世界中が市場になっている
弱み (Weaknesses)	脅威 (Threats)
<ul style="list-style-type: none">・営業力が弱い・社内で統一した意思を決定するのに時間がかかる	<ul style="list-style-type: none">・海外からの参入企業が増えている・新規システム開発の需要が低い

この分析をもとに、強み、機会、弱み、脅威を組み合わせる戦略を考える。

例えば、「レンタルサーバの技術を応用してクラウドビジネスを世界中に展開する」という戦略は [(7)] を組み合わせたものであり、「元々持っている技術力をさらに高めて海外からの参入に対抗する」という戦略は [(8)] の組合せになる。

(7) , (8) の解答群

ア. 強みと機会

イ. 強みと脅威

ウ. 弱みと機会

エ. 弱みと脅威

問題2 次のオブジェクト指向設計に関する記述中の [] に入れるべき適切な字句を解答群から選べ。

オブジェクト指向とは、データと [(1)] (操作) を一つにまとめて扱うことにより、再利用性の高い設計や開発を行う考え方であり、オブジェクト指向設計という。

データと操作を一体化したものをオブジェクト、または、クラスと呼び、外部から直接参照されないように隠蔽することを [(2)] と呼ぶ。これにより、オブジェクトの独立性を高めることができ、また、オブジェクトの中身を知らなくても必要な操作ができるようになる。これらのオブジェクト間でやりとりされる情報は [(3)] と呼ばれる。

なお、クラスを具体的なデータ値や操作で表したものを [(4)] と呼ぶ。

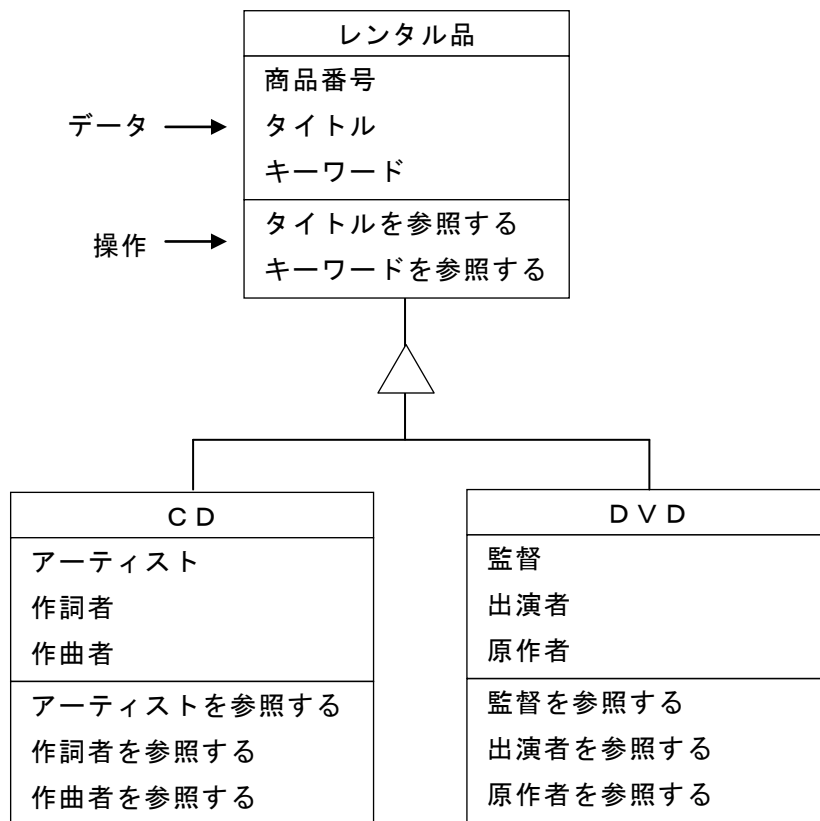


図 クラスの階層構造

クラスを階層化したときの上位のクラスを [(5)]、下位のクラスを [(6)] と呼び、上位のクラスで定義されたデータや操作を下位のクラスに引き継ぐことができる。これを [(7)] と呼ぶ。共通部分は上位クラスから引き継ぎ、下位のクラスで個別に定義しなければならない部分のみ定義することにより、生産性を向上させている。

上位クラスと下位クラスの間にはいくつかの種類があるが、図のレンタル品クラスと CD クラスの関係は、 [(8)] 関係となる。

(1) ~ (4) の解答群

ア. イベント	イ. インスタンス	ウ. カプセル化
エ. コンポーネント	オ. プロパティ	カ. メソッド
キ. メッセージ	ク. ユースケース	

(5) ~ (7) の解答群

ア. インナークラス	イ. インヘリタンス	ウ. オーバライド
エ. サブクラス	オ. スーパクラス	カ. デリゲーション
キ. ポリモフィズム	ク. メンバークラス	

(8) の解答群

ア. 依存	イ. 集約／分解	ウ. 特化／汎化
-------	----------	----------

問題3 次のネットワークに関する各設問に答えよ。

<設問1> 次のIPアドレスに関する記述中の に入れるべき適切な字句を解答群から選べ。

ネットワーク上でTCP/IPを利用した通信を行う場合、通信機器はIPアドレスを使用する。

IPアドレスは、ネットワークアドレスとホストアドレスで構成されており、IPv4では32ビットで表される。ここで、先頭から何ビットまでをネットワークアドレスとするかを表しているのがサブネットマスクである。サブネットマスクは、ネットワークアドレス部をすべて「1」、ホストアドレス部をすべて「0」で表したビット列で、通常のIPアドレスと同様に、8ビットごとに10進数に変換し、ピリオドで区切って表記する。

また、IPアドレスには、ネットワークアドレスのビット数と先頭ビットの値により分けられたクラス方式と、ネットワークアドレスのビット数を必要な分だけで設定するクラスレス方式がある。クラス方式におけるクラスA~Cのネットワークアドレスと標準サブネットマスクを表1に、ネットワークアドレスの範囲を表2に示す。

表1 ネットワークアドレスと標準サブネットマスク

クラス	ネットワークアドレス	標準サブネットマスク
A	先頭が0で始まる8ビット	255.0.0.0
B	先頭が10で始まる16ビット	255.255.0.0
C	先頭が110で始まる24ビット	255.255.255.0

表2 ネットワークアドレスの範囲

クラス	最小値 (2進数)	最大値 (2進数)
A	0000 0000	0111 1111
B	1000 0000 0000 0000	1011 1111 1111 1111
C	1100 0000 0000 0000 0000 0000	1101 1111 1111 1111 1111 1111

ここで、ネットワークアドレスの範囲内でも特定の用途に使用され、ネットワーク機器に割り当てることができないIPアドレスがいくつか存在する。例えば、クラスAの「127.0.0.1」は (1) アドレスと呼ばれ、このIPアドレスを宛先に指定して送信すると自分に宛てたものとして戻ってくることから、自分がネットワークに提供しているソフトウェアのテストや、機器が正常に稼動しているかどうかを確認するために使用される。

(1) の解答群

- ア. コールバック
- ウ. ユニキャスト

- イ. マルチキャスト
- エ. ループバック

<設問 2> 次のプライベート IP アドレスに関する記述中の [] に入れるべき適切な字句を解答群から選べ。

プライベート IP アドレスは、LAN を管理するネットワーク管理者により自由に割り当て可能であり、LAN 内だけ有効でインターネット上では通信できない IP アドレスである。このため LAN 内の機器がインターネットにアクセスする場合は、 [(2)] などの技術によりインターネット上のグローバル IP アドレスに変換するか、グローバル IP アドレスが割り当てられた [(3)] サーバ（代理サーバ）を経由してアクセスすることになる。

なお、表 3 に示すように、プライベート IP アドレスもクラスごとに使用できるアドレスの範囲が規定されている。

表 3 プライベート IP アドレスの範囲と標準サブネットマスク

クラス	プライベート IP アドレスの範囲	標準サブネットマスク
A	[(4)]. 0. 0. 0 ~ [(4)]. 255. 255. 255	255. 0. 0. 0
B	172. 16. 0. 0 ~ 172. 31. 255. 255	255. 255. 0. 0
C	[(5)]. 0. 0 ~ [(5)]. 255. 255	[(6)]

(2) , (3) の解答群

- ア. DHCP
- イ. DNS
- ウ. NAT
- エ. ファイル
- オ. プロキシ
- カ. メール

(4) の解答群

- ア. 0
- イ. 1
- ウ. 10
- エ. 20

(5) の解答群

- ア. 182. 168
- イ. 192. 168
- ウ. 202. 168
- エ. 212. 168

(6) の解答群

- ア. 255. 0. 0. 0
- イ. 255. 240. 0. 0
- ウ. 255. 255. 0. 0
- エ. 255. 255. 255. 0

<設問3> 次のサブネット化に関する記述中の に入れるべき適切な字句を解答群から選べ。

クラス方式のホストアドレス部の一部をネットワークアドレスとして利用し、複数のサブネットワークを構築することをサブネット化という。このとき、サブネットマスクは、標準のネットワークアドレス部にサブネットワーク部を含めてネットワークアドレスとして指定する。

例えば、クラスCのIPアドレスに対して、サブネットマスクを「255.255.255.240」と指定した場合、一つのサブネットワーク内には (7) 個のホストアドレスを設定できる。このとき、設定可能なサブネットワークすべてを利用するネットワーク全体では (8) 個のホストアドレスを設定できる。ただし、すべてのビットが「0」とすべてのビットが「1」の値は、サブネットワークのアドレスに設定できるが、ホストアドレスには設定できないものとする。

(7) の解答群

ア. 14 イ. 16 ウ. 30 エ. 32

(8) の解答群

ア. 196 イ. 224 ウ. 254 エ. 256

問題4 次のデータベースに関する記述を読み、各設問に答えよ。

J社は雑貨の間屋であり、リレーショナルデータベースを使用し、販売管理を行っているが、社員管理等にも利用したいと考えている。

手始めに、今まで手作業で行っていた出張手当の精算処理をシステム化することになり、データベースのテーブル設計を行うことにした。次の図1は、出張手当の申請書例である。テーブル設計に関する仕様の一部を次に示す。

- ・申請番号は、出張手当申請書ごとに付与される一意の番号である。
- ・所属は、所属している課名を記入するが、課には一意の番号が付与されている。
- ・社員番号は、入社時に付与される一意の番号である。
- ・明細番号は、出張手当申請書内の詳細に記入した順番に付与される番号である。
- ・種別は、金額が発生した内容であり、あらかじめ決められている名称を記入する。
- ・金額には、日当は一日ごと、宿泊は一泊ごとに記入する。宿泊の場合、宿泊場所を出発地に記入する。

出張手当申請書						
申請番号 12345			申請日 20XX年 2月 3日			
所 属 販売課						
社員番号 9876						
社員名 J 検一郎						
明細番号	日付	取引先	種別	出発地(宿泊地)	到着地	金額
1	20XX-01-05	渡辺商店	新幹線・片道	東京	岩手県盛岡市	17,200
2			バス・往復	岩手県盛岡市	岩手県宮古市	4,060
3			宿泊	岩手県宮古市		12,000
4			日当			3,000
5	20XX-01-07	橘屋	飛行機	羽田	福岡	26,590
6			タクシー	福岡空港	宇美町	2,440
:	:	:	:	:	:	:
						84,600

図1 出張手当申請書の例

<設問1> データベースの正規化に関する次の記述中の [] に入れるべき適切な字句を解答群から選べ。

図1の帳票より各項目を取り出し、 [(1)] を排除し、 [(2)] の形にした。次に「申請書」テーブルと「申請明細」テーブルの二つのテーブルを作成した(図2)。下線が引いてある項目は主キーである。

[申請書]

申請番号	申請日	所属	社員番号	社員名
------	-----	----	------	-----

[申請明細]

申請番号	明細番号	日付	取引先	種別	出発地	到着地	金額
------	------	----	-----	----	-----	-----	----

図2 申請書テーブルと申請明細テーブル

さらに、「申請書」テーブルを「申請書」テーブル、「社員」テーブル、「課」テーブルの三つのテーブルに分割した(図3)。これは、(3)以外の項目に従属している項目を別テーブルにしているため、(4)である。これにより、例えば“社員の配属がまだ決まっていない新設の課”の(5)が可能となる。

[申請書]

申請番号	申請日	所属課番号	社員番号
------	-----	-------	------

[社員]

社員番号	社員名	課番号
------	-----	-----

[課]

課番号	課名
-----	----

図3 申請書テーブル分割後のテーブル

また、「申請明細」テーブルを「申請明細」テーブルと「種別」テーブル、「取引先」テーブルの三つのテーブルに分割した(図4)。

[申請明細]

申請番号	明細番号	日付	取引先番号	種別番号	出発地	到着地	金額
------	------	----	-------	------	-----	-----	----

[種別]

種別番号	種別内容
------	------

[取引先]

取引先番号	取引先名
-------	------

図4 申請明細テーブル分割後のテーブル

(1) , (3) の解答群

- ア. 外部キー
- イ. 繰り返し項目
- ウ. 候補キー
- エ. 主キー

(2) , (4) の解答群

- ア. 非正規形
- イ. 第1正規形
- ウ. 第2正規形
- エ. 第3正規形

(5) の解答群

- ア. 関係喪失
- イ. 事前登録
- ウ. 排他制御

<設問2> 次の出張手当種別計を求める SQL 文の に入れるべき適切な字句を解答群から選べ。

課ごとの1ヶ月間の出張手当の種別ごとの集計をすることになった。なお、出張手当種別計は、課番号、種別番号の昇順に表示し、社員が申請時に所属していた課を基準に行う。また、月の開始日、終了日はホスト変数“:月開始日”、“:月終了日”に格納されているものとする。

```
SELECT 申請書.所属課番号, 課.課名, 申請書.種別番号, 種別.種別内容,  
       SUM(申請明細.金額) AS 出張手当種別計  
FROM 申請書, 課, 申請明細, 種別  
WHERE  (6)  
      AND 日付 BETWEEN :月開始日 AND :月終了日  
GROUP BY 申請書.所属課番号, 課.課名, 申請書.種別番号, 種別.種別内容  
ORDER BY  (7)
```

(6) の解答群

- ア. 申請書.所属課番号 = 課.課番号
AND 申請明細.種別番号 = 種別.種別番号
- イ. 申請書.所属課番号 = 課.課番号
AND 申請書.申請番号 = 申請明細.申請番号
- ウ. 申請書.所属課番号 = 課.課番号
AND 申請書.申請番号 = 申請明細.明細番号
AND 申請明細.種別番号 = 種別.種別番号
- エ. 申請書.所属課番号 = 課.課番号
AND 申請書.申請番号 = 申請明細.申請番号
AND 申請明細.種別番号 = 種別.種別番号

(7) の解答群

- ア. 申請書.種別番号, 申請書.所属課番号
- イ. 申請書.種別番号 DESC, 申請書.所属課番号 DESC
- ウ. 申請書.所属課番号, 申請書.種別番号
- エ. 申請書.所属課番号 DESC, 申請書.種別番号 DESC

<設問3> 次の1ヶ月間に申請された宿泊費の平均を求め、その平均金額を超えている宿泊日、宿泊地、金額を求める SQL 文の に入れるべき適切な字句を解答群から選べ。

宿泊費が宿泊地によって差が出ているようだということなので、検証することになった。1ヶ月間に申請された宿泊費の平均を求め、その平均金額を超えている宿泊日、宿泊地、金額を表示する。なお、宿泊の種別番号、月の開始日、終了日はホスト変数":宿泊", ":月開始日", ":月終了日"に格納されているものとする。

```
SELECT 申請明細.日付 AS 宿泊日, 申請明細.出発地 AS 宿泊地, 申請明細.金額
FROM 申請明細
WHERE 申請明細.日付 BETWEEN :月開始日 AND :月終了日
AND 申請明細.種別番号 = :宿泊
AND 申請明細.金額 >  (8)
```

(8) の解答群

- ア. (SELECT AVG(申請明細.金額) FROM 申請明細)
- イ. (SELECT AVG(申請明細.金額) FROM 申請明細
WHERE 申請明細.種別番号 = :宿泊)
- ウ. (SELECT AVG(申請明細.金額) FROM 申請明細
WHERE 申請明細.日付 BETWEEN :月開始日 AND :月終了日
AND 申請明細.種別番号 = :宿泊)
- エ. (SELECT AVG(申請明細.金額) FROM 申請明細
WHERE 申請明細.日付 BETWEEN :月開始日 AND :月終了日
AND 申請明細.種別番号 = :宿泊
GROUP BY 申請明細.宿泊地)

問題5 次のセキュリティ技術に関する各設問に答えよ。

<設問1> 次の暗号化方式に関する記述中の□に入れるべき適切な字句を解答群から選べ。

データを暗号化して通信を行う方法の代表的なものとして共通鍵暗号方式と公開鍵暗号方式がある。

共通鍵暗号方式は暗号化と復号に同じ鍵を使い、公開鍵暗号方式は暗号化と復号で異なる一組の鍵を使用し、一方を一般に公開するので公開鍵と呼び、もう一方の鍵は作成した本人だけが使用するので秘密鍵と呼ぶ。この二つの方式を、暗号化と復号に要する時間で比較すると、□(1)。

また、図1のように5台のコンピュータが相互に暗号化したデータを送受信する場合、共通鍵暗号方式のみで行う場合に必要になる鍵の数は□(2)個になり、公開鍵暗号方式のみで行う場合に必要になる鍵の組数は□(3)組である。通信相手が多くなるほど鍵の数や鍵の漏えいに対する点から□(4)の方が鍵の管理が容易である。

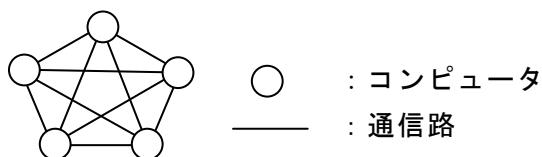


図1 ネットワークの図

(1) の解答群

- ア. 共通鍵暗号方式の方が長い
- イ. 共通鍵暗号方式の方が短い
- ウ. どちらも同じである

(2) ~ (4) の解答群

- ア. 1 イ. 4 ウ. 5 エ. 10 オ. 20
- カ. 共通鍵暗号方式 キ. 公開鍵暗号方式

<設問 2> 次のメッセージダイジェストに関する記述中の に入れるべき適切な字句を解答群から選べ。

ハッシュ関数は、任意の長さの入力データに対して固定長のハッシュ値を返すものである。また、ハッシュ値から元の入力データに戻すことができないという性質を持っている。

メッセージダイジェストとは、送信データ(平文のメッセージ)にハッシュ関数を施して得られるハッシュ値のことである。メッセージダイジェストを利用した通信を行うことで通信の途中で改ざんが行われていないことを証明できる(図2)。送信者は、平文のメッセージとメッセージダイジェストを一緒に送信し、受信者は、平文のメッセージに同じハッシュ関数を施してメッセージダイジェストを生成し、受信したメッセージダイジェストと照合して一致すれば平文のメッセージが改ざんされていないことを確認できる。

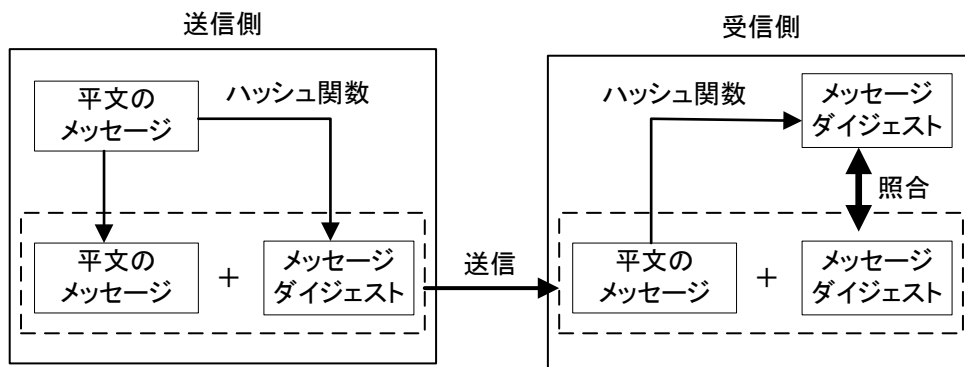


図2 メッセージダイジェストを利用した通信

また、送信者の正当性を受信者が確認する技術に、公開鍵暗号化方式を利用した (5) がある。これは任意の文字列を (6) で暗号化したものをデータに添付して送信し、受信者は添付された任意の文字列を (7) で復号するものである。この任意の文字列にメッセージダイジェストを利用することで、送信者の正当性だけでなく改ざんの有無も確認できる。ただし、これだけでは鍵の正当性が確認できないので、 (8) が発行するデジタル証明書を利用することで、より送信者の正当性が保証される。

(5) , (8) の解答群

- | | |
|----------------|--------------|
| ア. 検証局 | イ. セッションキー |
| ウ. チャレンジ/レスポンス | エ. デジタル署名 |
| オ. 認証局 | カ. プリシェアードキー |

(6) , (7) の解答群

- | | |
|------------|------------|
| ア. 受信者の公開鍵 | イ. 受信者の秘密鍵 |
| ウ. 送信者の公開鍵 | エ. 送信者の秘密鍵 |

<メモ欄>

<メモ欄>

<メモ欄>

