高校２年次「社会と情報」の課題について

令和２年４月 28 日
情報科

「社会と情報」の授業については，授業が開始された後にオリエンテーションを実施します。授業を受けるための心構えや学習方法について，そのオリエンテーションの中で伝えます。

ただ，このような状況ですので，今できることは，まず皆さんには教科書を開いてもらうことと考えました。次のページからの課題に取り組んでください。取り組み方については，次のとおりです。

【取り組み方】

1　課題をダウンロードする。（この次のページからの部分です。）
　紙の形にした方が取り組みやすいかもしれませんが，その必要はありません。

2　解答用紙のファイルをダウンロードする。（この PDF とは別の Word 形式のファイルです。）
　これも，紙の形にする必要はありません。

3　課題を読み，教科書の対象ページを読んで考える，答えを探る。

4　次のいずれかの方法で解答を作る。

(1)　解答用紙のファイルに入力して保存する。
　Word 形式のファイルなので，コンピュータや携帯端末で直接入力・編集することができます。それに入力して保存をしてください。

(2)　紙の形の方がよい場合は，印刷して書き込む方法でも構いません。

(3)　(1)(2)のいずれも難しい場合は，答えにあたる教科書の部分をマーカー等でチェックするだけでも後で楽かもしれません。

5　解答用紙を提出する。

(1)解答用紙のファイルとして保存した場合は，次のいずれかで提出する。
　USB に保存して，最初の授業に USB を持参する。携帯端末への保存はできているが，USB への移動が難しいという場合は，最初の授業の際に申し出てください。

(2)紙の形にした場合は，最初の授業で提出する。

(3)最初の授業で課題と解答用紙を受け取り，２回目の授業で提出する。

世の中の状況によっては，再度課題に取り組んでもらうことがあるかもしれません。早めに取り組んでおいてください。それから，取り組んだ結果としてのファイルは削除したり紛失したりしないように，取扱いには注意をしてください。

【　社会と情報サイト用 課題 No.01　　3 章　情報安全　】

1　個人による安全対策　教科書▶P.60〜P.61

確認問題

1　情報セキュリティ

（1　　）とは，情報の盗聴（盗み見）や，改竄，破壊などの（2　　）や不慮の事故に対して，個人的，組織的，技術的な（3　　）を講じることである。

2　パスワードの管理

コンピュータやネットワークの利用を開始することを（1　　）といい，一般に個人を識別するための（2　　）と本人であることを確認するための（3　　）の入力が求められる。また，(2)と（3）を合わせて（4　　）といい，これがコンピュータやネットワークを利用する権利になる。

3　マルウェアとその対策

コンピュータのシステムやソフトウェアに，何らかの危害を加える悪質なプログラムのことを総称して（1　　）という。このうち，ほかのファイルやシステムに寄生・感染する機能があるプログラムのことを（2　　）といい，この感染経路は Web ページの閲覧，OS やソフトウェアの（3　　）から侵入するなどいろいろな場合がある。

その対策は，（4　　）ソフトウェアの利用が一般的であるが，このソフトウェアは，ウイルスだけでなく情報を勝手に送信してしまう（5　　）や意図しない広告を表示する（6　　）など，（1）の対策になる場合が多い。

4　不正アクセスの制限

利用する権限をもっていないコンピュータやネットワークに入り込むことを（1　　）という。これに対して，外部から侵入されるのを防ぐ技術に（2　　）があり，第三者が侵入しないように，外部とのやり取りを監視し，不正なアクセスを検出して遮断（しゃだん）する機能をもつ。

練習問題

5　パスワードの注意点　次の(1)〜(5)のパスワードは，5 月 12 日生まれの高校生である佐藤一郎君の考えたものである。これらのうち適切なものに〇，適切でないものに×を記入しなさい。また，×の場合はその理由を書きなさい。

(1) satoichi　　(2) ichi512　　(3) 7alw3g6_　　(4) dreamcometrue　　(5) apple123

6　マルウェアとその対策　次のア～オのウイルス対策のうち，誤っているものをすべて選びなさい。

ア．メールの添付ファイルは急ぎの用事が多いので，すぐ開いてみてからウイルスチェックをする。
イ．ウイルス対策ソフトウェアを活用し，定義ファイルの更新を常に行う。
ウ．OS にセキュリティホールがあると表示されたので，パッチをインストールした。
エ．電子メールから感染することがあるので，常に最新の電子メールソフトウェアに更新しておく。
オ．インターネットに接続していないパソコンなので，ウイルス対策ソフトウェアはインストールしておく必要がない。

7　不正アクセスの制限　不正アクセス行為は，「なりすまし行為（A）」，「攻撃する行為（B）」，「助長する行為（C）」の 3 つに分けることができる。これらに関して次の問いに答えなさい。

(1) 次のア～カの行為は，上記の不正アクセス行為Ａ～Ｃのどれに該当するか答えなさい。
　ア．OS のセキュリティホールからネットワークに侵入した。
　イ．コンピュータのディスプレイに貼ってあるメモに書いてあった他人のユーザ ID とパスワードを使い，ネットワークにログインした。
　ウ．会社の同僚のユーザ ID とパスワードを無断で他人に教えた。
　エ．他人のユーザ ID を使い，ためしにパスワードをユーザ ID と同じにして入力したらネットワークにログインできた。
　オ．他人のユーザ ID とパスワードを掲示板に書き込んだ。
　カ．コンピュータウイルスを使い，ネットワークに侵入した。
(2) (1)のア～カの行為の中で，ファイアウォールで防ぐことができるものをすべて選びなさい。
(3) (1)のア～カの行為の中で，ファイアウォールで防ぐことができないものを１つあげ，不正アクセス行為を防止する対策としてどのようなことが考えられるか書きなさい。

2　組織による安全対策　教科書▶P.62～P.63

確認問題

1　情報セキュリティポリシーの策定

（1　　）とは，組織全体の情報セキュリティに関する基本方針である。ファイルの利用制限やネットワークの構築方法，暗号化による盗聴対策，（2　　）対策，不正侵入対策，機密漏洩（ろうえい）対策，（3　　）時の対応計画，実施手順などの方針を定めたものである。

2　アクセス制御

フォルダやファイルなどを利用する権限を（1　　）という。複数の利用者がコンピュータを共有している時，フォルダやファイルなどに（1）を設定して，特定の利用者だけがこれらを扱えるようにすることを（2　　）という。ファイルやフォルダを利用するためには，各ユーザがコンピュータ

に自分のアカウントでログインし, 各アカウントに与えられた(1) を利用する。(1) には「(3　　)」や「(4　　)」などの権限があり，その制御として「(5　　)」や「(6　　)」などがある。複数設定された（1）限が競合した場合は「（6）」が「（5）」に優先される。なお，（1）は個人だけでなくグループにも設定でき，グループに与えられた権限は，そのメンバー全員に反映される。また，管理者（（7　　））は，すべてのフォルダやファイルに対して，（1）を設定できる権限がある。

3　VLAN の構築

（1　　）とは，物理的な接続に依存せず仮想的にグループを作ってそれぞれ分離された別々の LAN を構築する手法である。例えば，同じグループ内でのみ通信を可能にし，異なるグループ間の通信は遮断したいことがある。（2　　）の中には（1）の機能をもっているものがあるので，これを用いることで，ポートごとに仮想的なグループを構成することができる。（1）では，物理的なグループ単位での（3　　）を行うが，利用者単位の場合は，フォルダやファイルに
（4　　）の設定をする必要がある。

練習問題

4　組織による安全対策　次の(1)～(4)の文章は, 組織による安全対策に関することについて説明したものである。

該当する用語を下の語群から選び，記号で答えなさい。
(1) アクセス権の設定の権限をもっている管理者
(2) 物理的な接続に依存せず，仮想的なグループを作り，分離された別々の構内通信網を構築する手法
(3) 組織全体の情報セキュリティに関する基本方針
(4) フォルダやファイルなどにアクセス権を設定すること
＜語群＞……

ア．セキュリティポリシー　　イ．アクセス制御　　ウ．VLAN
エ．アドミニストレータ　　オ．VPN

5　アクセス制御　ある会社の営業部の正社員である A, 営業部のアルバイトの B, 営業部長の C, 社長の D は,

あるファイルに対して下記のような権限をもっていた。4 人それぞれのアクセス権の設定を①～④から選びなさい。ただし営業部に対しては，このファイルのアクセス権の設定は読み取り・書き込みとも許可になっているものとする。

＜あるファイルに対する権限＞
・正社員 A は，読み取りができるが，書き込みはできなかった。
・アルバイト B は，読み取りも書き込みもできなかった。
・営業部長 C と社長 D は，読み取りも書き込みもできた。

＜アクセス権の設定＞

	読み取り		書き込み	
	許可	拒否	許可	拒否
①		●		●
②				

③	●		●	
④				●

●は，その権限が設定されていることを意味する。

6　VLAN の構築　スイッチやハブは，集線装置と呼ばれているもので，LAN の構築には必要な装置の１つである。次の問いに答えなさい。

(1) 次の①，②の説明は，スイッチ，ハブのどちらの説明か答えなさい。

① コンピュータから送られてきたデータをすべてのコンピュータに対して送信し，データの取捨選択はコンピュータが行う。

② コンピュータから送られてきたデータを解析して宛先を検出し，送り先のコンピュータのみにデータを送信する。

(2) (1)より，スイッチを用いることは，ネットワーク全体に対してどのようなメリットがあると考えられるか書きなさい。

3　安全のための情報技術　教科書▶P.64～P.65

確認問題

1　暗号化

データの盗聴などの不正行為を防ぐ対策として，第三者が見ても意味がわからないようにすることを（1　　）といい，この処理をする前のデータを（2　　），処理した後のデータを（3　　）という。また，（3）を（2）に戻すことを（4　　）といい，これらの処理に必要な情報を（5　）という。（1）にはさまざまな方法があるが，Web ページ上で情報をやり取りする際に用いられる暗号化技術に（6　　）がある。

2　有害情報への対処

インターネット上の誹謗（ひぼう）・中傷（ちゅうしょう）などの有害情報に対処するには，情報の受信の際に必要な情報のみを選別する（1　　）という方法がある。その方式として，不適切な Web ページのリストを作成し，それを閲覧できなくする（2　　）方式や，有益な Web ページのリストを作成し，それだけが閲覧できる（3　　）方式などがある。

3　電子すかし

Web ページに掲載された画像などのデータは，簡単に（1　　）することができるため，権利者の了解なく流用されないよう，著作権等の侵害を防ぐための技術として（2　　）がある。

4　誤り検出符号（パリティビット）

データを送受信する際に，通信回線の（1　　）の影響を受け，データの０と１が入れ替わってしまう

と，送ったデータと受け取ったデータが異なることとなり，不都合が生じる。このデータの変化（誤り）を検出するために，各ビットが変化したかどうかを確認するためのデータを，（2　　）データに加えることによって，誤りを検出する方法がある。この時の付加データを（3　　）という。また，この付加データが，あるビット数のデータの中にある「1」の個数が偶数個になるように付加されている場合を（4　　），奇数個になるように付加されている場合を（5　　）という。

練習問題

5　暗号化　次の(1)～(5)の文章は，暗号に関することについて説明したものである。該当する用語を下の語群から選び，記号で答えなさい。

(1) 暗号化されたデータを元に戻すこと
(2) 暗号化する前のデータ
(3) 暗号化する際に必要な情報
(4) 元のデータに戻す際に必要な情報
(5) Web ページで情報をやり取りする際の暗号化技術

＜語群＞……

ア．暗号化鍵　　イ．平文　　ウ．復号　　エ．SSL　　オ．復号鍵

6　有害情報への対処　次の(1)～(3)の文章は，コンテンツフィルタリングのブラックリスト方式やホワイトリスト方式の問題点について説明したものである。それぞれに該当する方式の名称を書きなさい。

(1) 不適切な Web ページであっても，まだリストに登録されていない場合，閲覧できてしまう。
(2) Web ページの遮断効果は確実であるが，リストにある Web ページしか見られないため，インターネット利用の幅をせばめてしまう可能性がある。
(3) Web ページのリストを頻繁に作成する必要がある。

7　電子すかし　電子すかし技術によってできることとして，最も適切なものを次のア～オのうちから 1 つ選びなさい。

ア．著作権情報などを，透けて見える画像として元の画像に重ねて表示することができる。
イ．復号鍵がなければ，データを利用できなくすることができる。
ウ．元のデータからの変化が一見してわからないように，著作権情報などを埋め込むことができる。
エ．データのコピー回数を制限することができる。
オ．データをコピーすることを不可能にすることができる。

8　誤り検出符号（パリティビット）　7 ビットの送信データに，誤り検出符号を 1 ビット付加して 8 ビットとして送信する際，偶数パリティとすることとした。このとき，次の問いに答えなさい。

(1) 次の①，②のようなデータを受信した。このデータの送信において，1 ビットの誤り検出によって誤りがあったといえるかどうか答えなさい。

①受信したデータは，「０１１０１１０１」であった。

②受信したデータは，「１１０００１０１」であった。

(2) 次の①，②のようなデータを送信したい。付加すべき誤り検出符号を「1」または「0」で答えなさい。

①送信したいデータは，「０１０１１１０」である。

②送信したいデータは，「１１０１０００」である。

4　暗号化　教科書▶P.66～P.67

確認問題

1　共通鍵暗号方式

共通鍵暗号方式は1つの鍵でデータの（1　　）と（2　　）を行う。簡単な共通鍵暗号方式の例に，文字を任意の文字数分ずらす（3　　）暗号がある。

2　公開鍵暗号方式

公開鍵暗号方式は，（1　　）になっている異なる（2　　）を利用する。この（2）は，どちらの鍵でも暗号化できるが，暗号化に利用しなかった方の鍵でしか復号できない。また片方の鍵からもう一方の鍵を算出することはできない。このため，一方の鍵を暗号化用として公開し，もう一方を復号するための鍵として（3　　）者が公開しないでもつ。このようにすると，一対の鍵だけで多数を対象に暗号化されたデータを受け取れ，（4　　）鍵を厳重に管理しなくてもよいため，インターネットを利用して不特定多数とやり取りするような場合に向いている。

実際の手順は，まず，（5　　）者はあらかじめ（3）者から送られてきた（4）鍵で平文を暗号化する。次に，暗号文を（3）者に送った後，暗号文を受け取った（3）者は自分しかもっていない（6　　）で復号して元の平文に戻す。

3　SSL

共通鍵暗号方式は，（1　　）方式に比べて処理時間が短いという利点はある。しかし，相手に鍵を安全に送らなければいけないという問題もある。そこで，Web ページで用いられている（2　　）では，共通鍵暗号方式を使って平文の（3　　）・（4　　）を行い，平文に比べてサイズの小さい共通鍵自体は，（1）方式で（3）・（4）を行う二重の暗号化方式を利用している。

4　ディジタル署名

（1　　）方式の手順を逆にすることで，送信者の（2　　）確認ができる。ディジタル署名は，平文からプログラムを利用して作った要約文を送信者の（3　　）鍵で暗号化したものである。これを平文に付加して受信者に送る。受信者は，送信者から送られてきた（4　　）鍵を使ってディジタル署名を復号する。こうして得られた要約文と平文から作成した要約文を比較して一致すれば，これらは送信者本人から送られてきたものであることを確認できると同時に，途中で（5　　）が改竄（かいざん）されていないこともわかる。

練習問題

5　共通鍵暗号方式／公開鍵暗号方式　次の(1)～(5)の文章は，共通鍵暗号方式（A）と公開鍵暗号方式（B）について説明したものである。それぞれに該当する暗号方式を A，B で答えなさい。

(1) 対になっている異なる２つの鍵を利用する。
(2) １つの鍵でデータの暗号化と復号を行う。
(3) 処理時間が短いという利点がある。
(4) インターネットを利用して不特定多数とやり取りする場合に適している。
(5) SSL では，平文の暗号化・復号をこの方式で行っている。

6　公開鍵暗号方式／SSL　次の各図の(1)～(6)に当てはまる用語を，下の語群から選び，記号で答えなさい。ただし，複数回選んでもよいものとする。

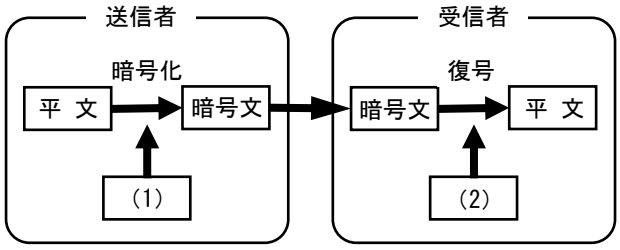


図１　公開鍵暗号方式

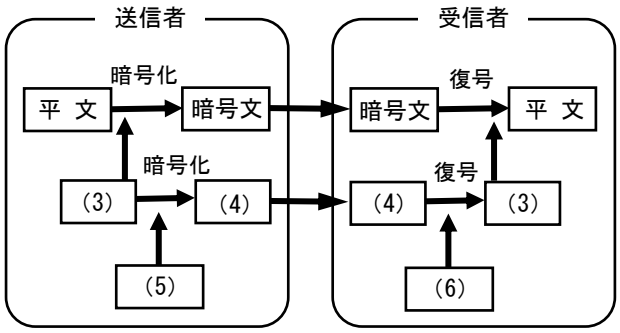


図２　SSL の仕組み（クライアントからサーバに送る場合）

＜語群＞……

ア．送信者の公開鍵　　イ．送信者の共通鍵　　ウ．送信者の秘密鍵
エ．受信者の公開鍵　　オ．受信者の共通鍵　　カ．受信者の秘密鍵
キ．暗号化された秘密鍵　　ク．暗号化された共通鍵

7　ディジタル署名　ディジタル署名に関する次の(1)～(4)の文章のうち，適切なものに○，適切でないものに×を記入しなさい。

(1) ディジタル署名は，データが途中で改竄されていないことを保証できる。
(2) ディジタル署名は，なりすましを防ぐことができる。

(3) ディジタル署名の要約文から平文に戻すことは，可能である。
(4) ディジタル署名の本人性を保証するサービスを電子認証という。

Supplement PLUS 暗号化の仕組み 教科書▶P.68～P.69

確認問題

1 RSA 暗号

2 つの素数の積を求めるのは簡単であるが,積から元の素数に戻す（1　　）は時間がかかる。桁数の大きな素数だと高性能なコンピュータでも膨大な時間がかかる。この困難な（1）を利用した暗号を（2　　）といい,「すべての数は,それをべき乗してから素数の積で割った余りと等しくなるようなべき乗数と素数の積が必ず存在する」という数学的な性質を利用している。

2 RSA 暗号の例

2 つの素数である 5 と 11 で（1　　）鍵と（2　　）鍵を作り,平文である 2 を暗号化・復号する手順は以下のようになる。

⑴ 鍵の作り方

暗号化に用いる鍵を E，復号に用いる鍵を D とし，暗号化と復号の両方に用いる鍵を N とする。RSA 暗号では，暗号化には N と E，復号には N と D が必要である。鍵の作り方は次のようになる。

①暗号化と復号に用いる N の作り方

無作為に大きな素数 P，Q を選び，その積を N（=P×Q）とする。

ここでは，P や Q に大きな素数ではなく小さな素数として P=5，Q=11 を選ぶと，N=（3　　）となる。

②暗号化に用いる E と復号に用いる D の作り方

L を（P－1）と（Q－1）の最小公倍数とし，n を 0 または任意の正の整数とすると，すべての数が自分自身に戻るためのべき乗数は，nL+1 と表すことができる。

また，ED=nL+1 が成り立つように，L との最大公約数が 1 で，L より小さい 2 つの正の整数として E と D を適当に選ぶ（ただし E≠D）。このようにすると，L=（4 と 10 の最小公倍数）=（4　　）
となり，L と E の最大公約数が 1 で，L より小さい正の整数として E=7 を選ぶと，n=1 の場合に 7D=21
から D=（5　　）となる（ED=21）。

⑵ 暗号化の手順

（1）鍵に N と E を用い，それらを受信者から送信者にあらかじめ送っておく。平文を M，暗号文を C とし，暗号文を送信者から受信者に送信する。平文 M（=2）の E（=7）乗を素数の積 N（=（3））で割った余りを暗号文 C（=（6　　））にする。

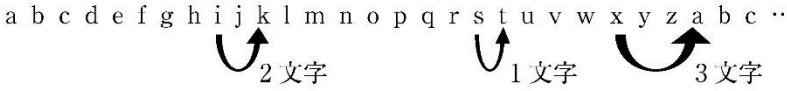
⑶ 復号の手順

（2）鍵に N と D を用いる。D は受信者だけがもっている。復号文を M’とし，暗号文を C とする。そこで，暗号文 C（=（6））の D（=（5））乗を素数の積 N（=（3））で割った余りを復号文 M’（=（7　　））にする。このようにすると，M’=M となり，復号文 M’は平文 M に戻る。

練習問題

3　暗号化の方法　次のように，英文字からなる文字列を暗号化する方法を考えた。これについて，下の問いに答えなさい。

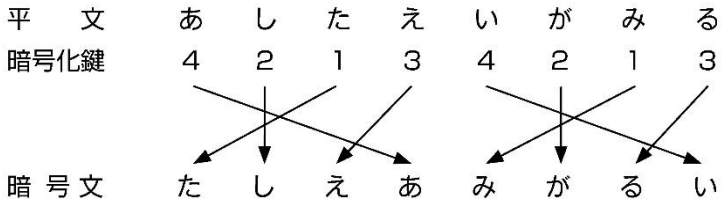
＜暗号化の方法＞
① 文字列の各文字の位置を数え，n 文字目の場合にはそのアルファベットを n 文字後にずらす。
② もし z を超えるときは，その後 abc…と繰り返されるものと考える。
例 平文が「six」のとき
s の 1 文字後は t，i の 2 文字後は k，x の 3 文字後は a である。
よって暗号文は「tka」となる。



(1)「bit」を暗号化しなさい。
(2)「lgb」を復号しなさい。

4　暗号化の方法　次のように，数桁の整数を鍵として，ひらがなの日本文を暗号化する方法を考えた。これについて，下の問いに答えなさい。

＜暗号化の方法＞
平文は「あしたえいがみる」（明日映画観る）であるとし，4 桁の整数を暗号化の鍵とする。
① 1 から 4 までの数字を並べ替え，鍵とする（例 4213）。
② 平文を 4 文字ずつに区切り，鍵の数字を 1 桁ずつ対応させる。
③ 4 文字のひらがなを，1 から 4 の数字の順番に並べ替え，できたものを暗号文とする。



(1) 鍵を 4 桁の整数 2431 とする。「きのうねぼうした」を暗号化しなさい。
(2) 4 桁の整数を鍵にする場合，何通りの鍵を作ることができるか答えなさい。ただし，「1234」では並べ替えが起こらないので除く。
(3) 5 桁の整数を鍵にした場合，復号鍵を 1 つずつ作って復号を試みると最大でも何回で復号が可能か答えなさい。ただし，「12345」の鍵は使用していないものとする。
(4) 復号鍵を 1 つずつ作って復号を試みるとき，4 桁の整数の鍵を使用した場合と比べ，5 桁の整数の鍵の場合では，復号が何倍困難であるか答えなさい。なお，計算は小数第 2 位を四捨五入して求めなさい。