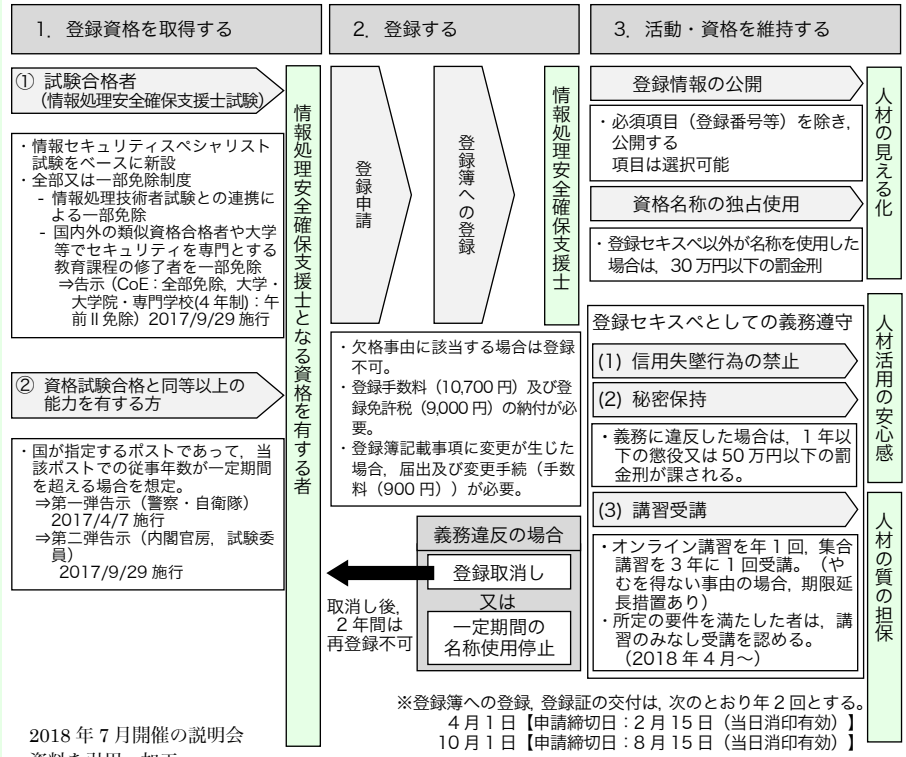
目　次

第３部　午後問題のテーマ別対策と必要知識

2. 人材の見える化
・資格保持者のみ資格名称を使用可能（名称独占資格）
・登録簿の整備，登録情報の公開
3. 人材活用の安心感
・人物として問題ない人材のみを登録・資格継続する規定
- 厳格な秘密保持義務
- 信用失墜行為の禁止義務
- 禁錮以上の刑，またはサイバー犯罪関連の刑に処せられていない方を登録



2018年7月開催の説明会資料を引用・加工

図表 1-1-1　情報処理安全確保支援士制度（登録セキスペ）の全体像

情報処理安全確保支援士の通称名とロゴマーク：

情報処理安全確保支援士が社会全体で活用され，企業等におけるセキュリティ対策を進めるため，法律上の名称に加え，通称名とロゴマークを設けます。

法律名：情報処理安全確保支援士
通称名：登録セキスペ（登録情報セキュリティスペシャリスト）
英語名：RISS（Registered Information Security Specialist）
ロゴマーク：

1-2　登録について

(1)　資格登録について

平成 29 年（2017 年度）春期試験から開始された「情報処理安全確保支援士試験」の合格者は，登録セキスペの登録資格を有します。

(2)　登録日について

登録セキスペの登録申請は随時受け付けていますが，登録日は次のとおり年に 2 回です。

4 月 1 日（申請の受付期限：2 月 15 日（当日消印有効））
10 月 1 日（申請の受付期限：8 月 15 日（当日消印有効））

(3)　登録内容の公開について

登録セキスペについての，次の情報をホームページにて公開します。なおこれ以外の情報については，登録申請の際に提出する「登録事項等公開届書」に基づいて公開します。

① 登録番号
② 登録年月日
③ 情報処理安全確保支援士試験に合格した年月
④ 講習の修了年月日

問題	解答
ディジタル署名の仕組み（5）	① 本文＋ハッシュ関数＝メッセージダイジェスト作成 ② 自分の秘密鍵で暗号化 ③ 対になる公開鍵で復号 ④ 本文＋ハッシュ関数＝メッセージダイジェスト作成 ⑤ ③と④を比較
ＰＫＩの仕組み－１．申請（3）	① 鍵ペアを生成 ② CSR を作成し，CA に申請 ③ CA がディジタル証明書を発行
ＰＫＩの仕組み－２．確認（2）	① CA の公開鍵で CA のディジタル署名を検証 ② ディジタル証明書内の，発行元の公開鍵を使って発行元のディジタル署名を検証
ＰＫＩ（4）	① CA（認証局），RA（登録局）と IA（発行局） ② ディジタル証明書 ③ CSR ④ CP/CPS
ディジタル証明書の形式（3）	① X.509 ② PKCS#7（複数の証明書）＋データ OK ③ PKCS#12（秘密鍵）
ディジタル証明書のチェック方法（5）	① CA，発行元のディジタル署名を検証 ② 証明書内の有効期限をチェック ③ CRL，OCSP で失効情報をチェック ④ ルート CA の確認 ⑤ アドレスバーの赤，緑をチェック
SSL/TLS のバージョン（4）	① SSL3.0 ② TLS1.0～TLS1.1 ③ TLS1.2（現在 OK） ④ TLS1.3（2018 年 8 月 RFC8446）
SSL/TLS の通信手順（4）	① 使用可能な暗号化等を決定する ② サーバから ディジタル証明書を送信する

図表 1-2-2　暗記事項を瞬時にイメージ

このような暗記事項が頭に入っていて，瞬時にイメージできる。

ちなみに，ここで連想できるぐらいに暗記して理解できても，そうした知識すなわち勉強して得た知識が，必ずしも設問になるとは限りません。むしろ設問にならないことの方が多いかもしれません。設問を解くためではなく，問題文を読解するためや，問題ない運用だということを判断するために必要な知識だということにもなります。そういう意味で，幅広い知識が必要になると考えておきましょう。広く，少しだけ深い知識が必要になります。そこが他の試験区分にはない，情報処理安全確保支援士試験の最大の特徴でしょう。

■　もう一つの過去問題の活用術　■

■知識を補充することが目的

過去問題を利用して得点力をアップさせる方法は，この章の「4.午後Ⅰ・午後Ⅱ対策」で説明しましたが，もう一つ，過去問題を使いながら，知識を増やしていく方法があります。過去問題を“知識の補充”教材に特化して活用するのです。情報処理安全確保支援士試験となっても“知識の補充”は変わることはありません。ポイントは，次のようになります。

- 練習は，過去問題を，時間を計測して解く必要はない。解答例にある解答を問題文と一緒に見ながら，読み進めていくだけでいい。
- できる限り数多くの問題に触れる方がいい（読むだけなら可能）。
- 解説はなくてもいいので，IPA の過去問題と解答例を使える。そうなると，平成 16 年以後全問題が活用できるため，古い過去問題集が入手できないという問題もなくなる。
- 3〜5 年前の過去問題を中心に古い問題の方が有益である。もちろん，法制度で変更があったところや技術転換した部分は除くが，そういう問題は少ない。
- 知識がないときの方が効果的（当たり前だけど）

以上の点を踏まえて，第 3 部の各章の「2. 学習方法」では，「時間を計測して解いた方がいい」，「解かなくてもいい。読むだけでいい」というような形で問題を推奨しています。

■原則，午後Ⅰは解く，午後Ⅱは読む

午後Ⅰの問題は，時間を計測して解いてみて解答手順の改善に活用するのがいいでしょう。一方，午後Ⅱの問題は“知識の補充”を目的に読み進めていけばいいと考えています。午後Ⅰの解答速度で処理できれば，午後Ⅱは十分時間内に解答できるからです。それに，午後Ⅱの問題は「解く練習をしてみて解説を読んで……」ということをすると時間がすごくかかりますが，“読むだけ”なら，同じ時間でより多くの問題を読むことができますよね。午後Ⅱは良い教科書なので，少しでも多くの問題に触れておいた方がいいのは間違いありません。

■IPA の過去問題をフル活用した者が勝つ！

「（知識の補充目的の）過去問題を読むだけの学習」であれば，解説に頼る必要がないので，IPA の過去問題をフル活用できます。数多くの問題に触れて理解を深めた人は，筆者の周囲でも，確実に合格を手にしていますからね。

5 脅威

情報を詐取したり，改ざんや破壊したりする目的で，システムに対する攻撃が行われます。マルウェア，不正アクセス，盗聴，なりすまし，サービス不能攻撃，アプリケーションへの攻撃など。個々の攻撃手法には，独特の名称が付けられているので，それを覚えていきましょう。

(1) マルウェア（malware）

悪意のコード（malicious code），又は悪意のソフトウェア（malicious software）の総称。コンピュータウイルス（ワーム，トロイの木馬，ボット等）に加えて，バックドアやルートキット，キーロガーなどの攻撃ツール，スパイウェアなども含んだ概念になります。

代表的なマルウェア		概要
ウイルス		自己伝染機能，潜伏機能，発病機能のいずれか一つ以上を有するもの（経済産業省：コンピュータウイルス基準より）。
	ワーム	ネットワークを通じてほかのコンピュータに拡散することを目的とした不正プログラム。
	トロイの木馬	増殖が主目的ではなく，ひっそりと常駐し，特定の日時や外部からの指示で破壊活動を開始する。
	ボット	コンピュータウイルスやワームの一種。語源はロボット。ボットを仕掛けた攻撃者は，遠隔操作によって，その端末から迷惑メールを送信したり，他のコンピュータを攻撃したりする。同一の指令サーバ配下のボットで形成されたネットワークをボットネットという。
攻撃ツール	バックドア	裏口。ハッキング成功時に，次回からアクセスや操作をしやすいように常駐させておくプログラムなど。
	ルートキット（rootkit）	様々なハッキングツールをまとめてキット状にしたもの。不正プログラムそのものや，バックドアの設置，ログの改ざんなど，標的サーバに不正侵入した後に使うツールなどをまとめたもの。
	キーロガー	打鍵したキーの使用を記録するソフト。
スパイウェア		利用者のコンピュータ内部の情報（環境設定情報，アクセス履歴など）を外部に自動的に通知する目的で常駐するプログラム（ソフトウェア）。

暗記事項

暗記事項をまとめました。しっかりと暗記してください。

問題	解答
1．情報セキュリティの概念	
三大要素（3）	① 情報資産 ② 脅威 ③ 脆弱性
情報セキュリティ確保の手順（4）	① 基本方針，情報セキュリティ委員会設置 ② 情報セキュリティポリシの作成 ③ セキュリティ教育，周知活動 ④ 定期的に評価・監査，必要に応じて見直し
情報セキュリティ対策（4）	① 抑止効果を狙う ② 予防的対策 ③ 事後対策（検知，復旧） ④ 再発防止策
情報セキュリティの三要素（3）	① Confidentiality；機密性 ② Integrity；完全性 ③ Availability；可用性
2．国の動向	
重要な動き（5）	① サイバーセキュリティ基本法 ② サイバーセキュリティ戦略 ③ サイバーセキュリティ経営ガイドライン（Ver2.0） ④ 中小企業の情報セキュリティ対策ガイドライン　第3版 ⑤ 割賦販売法の改正
サイバーセキュリティ基本法（3）	① サイバーセキュリティ戦略本部を設置 ② NISC（内閣サイバーセキュリティセンター）に改組 ③ サイバーセキュリティ戦略の作成及び実施（3年ごと）
割賦販売法の改正（4）	① カード情報の非保持化 ② PCIDSS 準拠（カード情報を保持する場合） ③ 加盟店の信用照会端末は IC カード決済対応を義務化 ④ EC サイトはリスクに応じた多面的・重層的な不正使用対策の導入（パスワードによる本人認証，属性・行動分析等）
3．情報セキュリティマネジメント	
制度（6）	① 情報セキュリティマネジメント試験 ② ISMS 適合性評価制度 ③ システム監査制度 ④ 情報セキュリティ監査制度 ⑤ プライバシーマーク制度 ⑥ 内部統制制度

Part 3　Chapter 2

第2章 PKI

PKI をメインテーマにした問題はそれほど多くはありません。しかし，設問単位ではコンスタントに出題されていましたし，問題文にキーワードが登場するケースも多く，「本当に，よく見かけるな」という印象があります。実際の開発現場でも，普通に“SSL/TLS”，“https”，“ディジタル証明書（公開鍵証明書，電子証明書)”という用語を用いますよね。

したがって，（メインテーマでの出題や，設問単位での出題，キーワードのみの出現などすべてを含めて)問題文に出現する可能性はとても高いと考えて，早い段階でしっかりと学習しておきましょう。問題を解くときに PKI 関連の用語に即座に反応できるようになれば，問題文を短時間で正確に理解することができますからね。

●学習目標　（次の知識が，瞬時に“アウトプット”できるようになる）

(1)　ディジタル証明書（概要）
(2)　PKI の運用環境（CA，RA，IA）
(3)　PKI の仕組み（一連の手順，CSR，CP/CPS）
(4)　ディジタル証明書のチェック方法
(5)　SSL／TLS
(6)　HSTS（HTTP Strict Transport Security）
(7)　時刻認証

２．学習方法

本章の具体的な学習方法と学習手順を下記①～⑥に，また，③，④，⑤で使用する過去問題を図表 3-2-1 に，それぞれまとめました。

試験区分	出題年度 期	問	タイトル	キーワード	本書掲載
(SW) AP	平成16年春	午後Ⅰ問1	リモートアクセスによるセキュリティの確保	公開鍵暗号，電子署名基礎	DL(※)
	平成17年秋	午後Ⅰ問3	SSL暗号化通信	SSL通信シーケンス	DL(※)
	平成21年秋	午後　問9	公開鍵基盤を用いた社員認証システム	ICカードへの組込み	DL(※)
	平成25年秋	午後　問8	Webサイトのセキュリティ強化策	リバースプロキシサーバ，WAF	DL(※)
	平成26年春	午後　問1	営業支援サーバへのSSLの導入	SSL全般	DL(※)
	平成19年春	午後Ⅰ問3	電子データによる文書の保管	ディジタルタイムスタンプの手順	DL(※)
SU	平成17年秋	午後Ⅰ問4	SSLを利用したWebシステム	PKI，SSL	DL(※)
	平成17年秋	午後Ⅱ問1	電子文書の保存	時刻認証全般	DL(※)
SC	平成21年春	午後Ⅱ問1	公開鍵基盤の構築	公開鍵基盤	DL(※)
	平成23年秋	午後Ⅰ問3	プロキシ経由のWebアクセス	プロキシによるSSLの内容検査	DL(※)
	平成26年秋	午後Ⅰ問2	代理店販売支援システム	暗号技術（安全性）	DL(※)
	平成28年春	午後Ⅰ問3	スマートフォンアプリケーションの試験	HTTPS，サーバ証明書，コモンネーム	DL(※)
	平成28年秋	午後Ⅱ問1	ICカードを用いた認証システム	PKI，ICカード，暗号化などの複合問題	P.230
	平成29年秋	午後Ⅰ問3	SSL/TLSを用いたサーバの設定と運用	SSL/TLSのバージョン，POODLE攻撃	P.216

(※)＝https://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_mondai.html からダウンロード

図表 3-2-1　この章のテーマに関連する過去問題（FE，AP，SU，SV，SC）

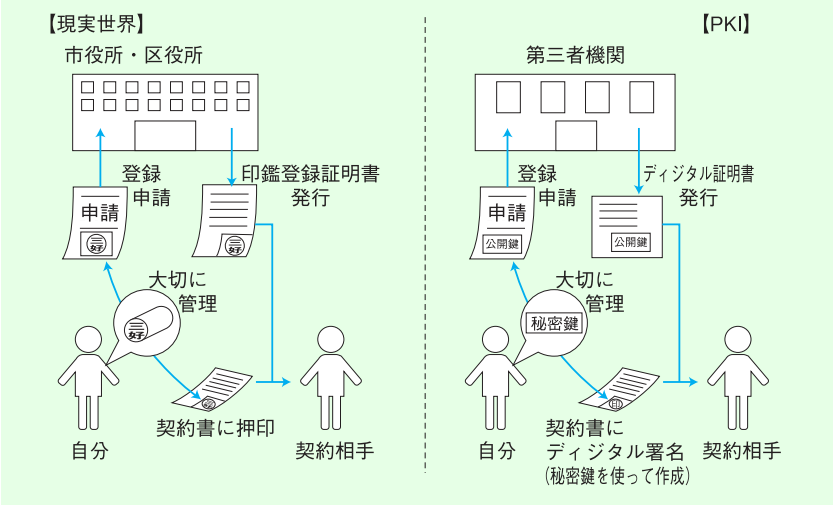
３．暗記事項

暗記事項をまとめました。しっかりと暗記してください。

問題	解答
ディジタル署名の仕組み（５）	① 本文＋ハッシュ関数＝メッセージダイジェスト作成 ② 自分の秘密鍵で暗号化 ③ 対になる公開鍵で復号 ④ 本文＋ハッシュ関数＝メッセージダイジェスト作成 ⑤ ③と④を比較
ＰＫＩの仕組み－１．申請（３）	① 鍵ペアを生成 ② CSR を作成し，CA に申請 ③ CA がディジタル証明書を発行
ＰＫＩの仕組み－２．確認（２）	① CA の公開鍵で CA のディジタル署名を検証 ② ディジタル証明書内の，発行元の公開鍵を使って発行元のディジタル署名を検証
ＰＫＩ（４）	① CA（認証局），RA（登録局）と IA（発行局） ② ディジタル証明書 ③ CSR ④ CP/CPS
ディジタル証明書の形式（３）	① X.509 ② PKCS#7（複数の証明書）＋データ OK ③ PKCS#12（秘密鍵）
ディジタル証明書のチェック方法（５）	① CA，発行元のディジタル署名を検証 ② 証明書内の有効期限をチェック ③ CRL，OCSP で失効情報をチェック ④ ルート CA の確認 ⑤ アドレスバーの赤，緑をチェック
SSL/TLS のバージョン（４）	① SSL3.0 ② TLS1.0～TLS1.1 ③ TLS1.2（現在 OK） ④ TLS1.3（2018 年 8 月 RFC8446）
SSL/TLS の通信手順（４）	① 使用可能な暗号化等を決定する ② サーバからディジタル証明書を送信する ③ クライアントからディジタル証明書を送信する ④ 暗号化通信の開始
SSL/TLS に対する攻撃（４）	① ダウングレード攻撃 ② バージョンロールバック攻撃 ③ BEAST 攻撃 ④ POODLE 攻撃

5．PKI に関する知識の整理

PKI（Public Key Infrastructure）とは，「公開鍵暗号技術を使って，ディジタル署名の正当性を証明するための基盤」のことです。当該ディジタル署名が，間違いなく本人のものであると証明する……それには PKI が必要になるのです。ここでは，そうした PKI に関する知識の整理を目的に，学習目標に準じて説明していきます。



図表 3-2-2　第三者機関の役割

PKI の仕組みは，現実世界の印鑑と印鑑登録，印鑑登録証明書の仕組みと比べてみると理解しやすいですね。現実世界では，重要な契約を締結するとき，契約書には印鑑登録した印鑑で印を押し，役所から発行してもらった印鑑登録証明書を添付して保存しておきます。PKI も同じような仕組みで，次のような対応関係になると考えればいいでしょう。

＜現実世界＞	＜ PKI ＞
市役所・区役所	→ 第三者機関等（登録局（RA）・認証局（CA））
大切に管理する印鑑	→ 大切に管理する秘密鍵
契約書に押印	→ ディジタル署名処理
印影	→ ディジタル署名
印鑑登録証明書	→ ディジタル証明書

6．演習問題　1

(H29秋-SC 午後Ⅰ問3)

SSL/TLSを用いたサーバの設定と運用に関する次の記述を読んで，設問1～3に答えよ。

C社は，衣服のデザイン，製造及び販売を行う中堅の衣料品製造会社である。近年は，C社の複数の販売チャネルのうち，ECモールに出店したオンラインショップでの販売量が増えており，C社の社名も比較的知られるようになった。C社では，事業を更に拡大するために，新たに独自のドメイン名を取得し，C社専用の販売サイト（以下，ECサイトという）を立ち上げることにした。

ECサイトの構築，運用及び管理は，C社のシステム部が担当することになった。システム部は開発会社の協力を得て構築を進め，当初の計画どおり運用が開始された。

〔社外からの通報〕

運用開始から3か月が経過した頃，C社の問合せ窓口に，ECサイトで利用されている一部のサーバ証明書に対応する秘密鍵が，サーバ証明書と一緒に，あるWebサイト（以下，Qサイトという）に掲示されているという通報があった。そこで，システム部のM部長は，ECサイトの管理を担当するBさんに，セキュリティ専門会社であるE社の支援を得て本件を調査し必要な措置を講じるよう指示した。

E社のセキュリティコンサルタントであるH氏のアドバイスを受けてBさんが確かめたところ，Qサイトに掲示された秘密鍵は自社のものと一致していた。Bさんは鍵が危たい化したと判断した。

次は，H氏とBさんの会話である。

H氏　：サーバ証明書に対応する秘密鍵が公開された影響について，順に説明していきましょう。サーバ証明書は認証局サービス事業者から発行されます。サーバ証明書には，サーバのFQDNと公開鍵が記載されます。サーバ証明書の作成とその検証には公開鍵暗号方式を利用した［　a　］技術を利用します。サーバ証明書はSSL/TLSで利用されます。SSL/TLSは複数の暗号技術を用います。データの送受信時は，暗号化と復号のために［　b　］を利用します。また，データの送信者と受信者が［　b　］で使用する鍵

〔解答用紙〕

コピーして活用してください。また，アイテックホームページ https://www.itec.co.jp/ からダウンロードすることもできます（P.74 参照）。

設問1	(1)	a					b					c					
		d															
	(2)																
	(3)																
設問2	(1)	ア						イ									
	(2) ①																
	(2) ②																
	(3)	e															
設問3	(1)																
	(2)																
	(3)																
	(4)																

50点満点	（IPA公表の配点比率に基づきアイテックで設問ごとに予想）
設問1	(1)：4×2 点　(2)：6 点　(3)：2 点
設問2	(1)：2×2 点　(2)：2×4 点　(3)：3 点
設問3	(1)：6 点　(2)：2×2 点　(3)：3 点　(4)：6 点

〔解説〕

問題のテーマはSSL/TLSを用いたサーバの設定と運用ですが，出題内容は，サーバ証明書の検証などを中心とした問題です。また，POODLE攻撃や，PFS（Perfect Forward Secrecy）とは何か，ドメイン認証証明書とEV証明書の違いなどをしっかりと把握していれば，解答を作成しやすいといえます。

［設問1］

(1) 空欄aは，H氏の「サーバ証明書の作成とその検証には公開鍵暗号方式を利用した［ a ］技術を利用します」という発言の中にあります。サーバ証明書を作成するためには，CA（Certification Authority；認証局）がRSAなどの公開鍵暗号方式を使ってディジタル署名を付与します。そして，サーバ証明書を検証するには，ディジタル署名を付与したCAの公開鍵を使ってサーバ証明書の検証を行います。したがって，空欄aにはディジタル署名（コ）が入ります。

空欄b，cは，同じH氏の「SSL/TLSは複数の暗号技術を用います。データの送受信時は，暗号化と復号のために［ b ］を利用します。また，データの送信者と受信者が［ b ］で使用する鍵を共有するために，公開鍵暗号方式を用いて［ c ］を行います」という発言の中にあります。SSL/TLSでは，データの送受信時は，処理速度の関係からデータの暗号化と復号には共通鍵暗号方式を使用します。そして，共通鍵暗号方式で使用する鍵をデータの送信者と受信者が共有するために，RSAなどの公開鍵暗号方式を用いて鍵交換を行います。したがって，空欄b，cには，それぞれ共通鍵暗号（カ），鍵交換（オ）が入ります。

ちなみに，SSL/TLSの鍵交換（鍵共有ともいう）のプロセスは，次のように行われます。SSL/TLSのハンドシェイクプロトコルでは，ClientHelloメッセージとServerHelloメッセージによって，最初にクライアントとサーバで使用する暗号スイートなどを折衝します。暗号スイートの例は，図2（H氏による調査の結果（抜粋））の中で記載されていますが，その意味は，図3（暗号スイートの名前の構成（概要））で説明されています。TLS_RSA_WITH_AES_128_CBC_SHAの例では，RSAが認証及び鍵交換のアルゴリズムとして使用されることを示します。このため，ハンドシェイクプロトコルにおいて，サーバからサーバ証明書が送られてくると，クライアントはサーバ証明書にあるCAのディジタル署名を用いてサーバを認証し，クライアントとサーバで行うSSL/TLS通信に必要な共通鍵を作成します。共通鍵を作成することが鍵交換のプロセスに当たりますが，まず，クラ