問 1 正解 完璧 直前チェック

Webのショッピングサイトを安全に利用するため，WebサイトのSSL証明書を表示して内容を確認する。Webサイトが，EV SSL証明書を採用している場合，存在するサブジェクトフィールドのOrganization Nameに記載されているものはどれか。

ア　Webサイトの運営団体の組織名
イ　証明書の登録業務を行う機関（RA）の組織名
ウ　証明書の発行業務を行う機関（CA）の組織名
エ　ドメイン名の登録申請を受け付ける機関（レジストラ）の組織名

問 2 正解 完璧 直前チェック

IEEE 802.1Xで使われるEAP-TLSによって実現される認証はどれか。

ア　CHAPを用いたチャレンジレスポンスによる利用者認証
イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証
ウ　ディジタル証明書による認証サーバとクライアントの相互認証
エ　利用者IDとパスワードによる利用者認証

問 3 正解 完璧 直前チェック

RLO（Right-to-Left Override）を利用した手口の説明はどれか。

ア　“コンピュータウイルスに感染している”といった偽の警告を出して利用者を脅し，ウイルス対策ソフトの購入などを迫る。
イ　脆弱性があるホストやシステムをあえて公開し，攻撃の内容を観察する。
ウ　ネットワーク機器のMIB情報のうち監視項目の値の変化を感知し，セキュリティに関するイベントをSNMPマネージャに通知するように動作させる。
エ　文字の表示順を変える制御文字を利用し，ファイル名の拡張子を偽装する。

春

問1　ア

解説 **EV SSL証明書**は，企業の実在性確認などの認証方法を厳格にし，業界内で統一基準を設けたSSLサーバ証明書である。**Organization Name**は，Webサイトを運営している団体の組織名称となる。具体的には，企業Aのホームページであれば，Organization Nameは企業Aを指す。

問2　ウ

解説 **IEEE 802.1X**は，クライアントPCと，無線のアクセスポイントやスイッチングハブとの間で利用される，ディジタル証明書による認証プロトコルである。鍵交換により共有された鍵を用いて，クライアントPCと接続先との暗号化通信を行う。

IEEE 802.1Xでは，EAP-TLSやEAP-PEAPなどの認証方式が使用される。

EAP-TLS（Extensible Authentication Protocol - Transport Layer Security）：EAPは，サーバとクライアント間の認証プロトコルである。TLSは，電子証明書を利用して認証を行う方式である。

EAP-PEAP（Extensible Authentication Protocol - Protected Extensible Authentication Protocol）：EAPは，サーバとクライアント間の認証プロトコルである。PEAPは，パスワード入力によって認証を行う方式である。

問3　エ

解説 **RLO**：Unicodeで定義されている制御文字の流れを，右から左に変更することで，ウイルスがファイル名の拡張子を偽造する。

ア：「偽セキュリティ対策ソフト型」ウイルスの説明である。
イ：ハニーポットの説明である。

問 4 正解 完璧 直前チェック

VA（Validation Authority）の役割はどれか。

ア　ディジタル証明書の失効状態についての問合せに応答する。
イ　ディジタル証明書を作成するためにディジタル署名する。
ウ　認証局に代わって属性証明書を発行する。
エ　本人確認を行い，ディジタル証明書の発行を指示する。

問 5 正解 完璧 直前チェック

サイドチャネル攻撃の説明はどれか。

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量（処理時間や消費電流など）やエラーメッセージから，攻撃対象の機密情報を得る。
イ　企業などの機密情報を詐取するソーシャルエンジニアリングの手法の一つであり，不用意に捨てられた機密情報の印刷物をオフィスの紙ゴミの中から探し出す。
ウ　通信を行う2者間に割り込んで，両者が交換する情報を自分のものとすり替えることによって，気付かれることなく盗聴する。
エ　データベースを利用するWebサイトに入力パラメタとしてSQL文の断片を与えることによって，データベースを改ざんする。

問 6 正解 完璧 直前チェック

X.509におけるCRL（Certificate Revocation List）についての説明のうち，適切なものはどれか。

ア　PKIの利用者は，認証局の公開鍵がWebブラウザに組み込まれていれば，CRLを参照しなくてもよい。
イ　認証局は，発行した全てのディジタル証明書の有効期限をCRLに登録する。
ウ　認証局は，発行したディジタル証明書のうち，失効したものは，失効後1年間CRLに登録するよう義務付けられている。
エ　認証局は，有効期限内のディジタル証明書をCRLに登録することがある。

春

問4　ア

解説　**VA**：ディジタル証明書の失効リスト（CRL）を管理する機関である。VAは，認証局（CA）とは別に，失効リスト（CRL）の有効性のみを管理するため名称が異なる。
イ：認証局（CA）の役割である。
ウ，エ：失効リスト（CRL）の管理のみであるため，誤りである。

問5　ア

解説　**サイドチャネル攻撃**は，暗号を解読するための攻撃手法の一つである。暗号化や復号をする際に発生する電磁波，熱，演算処理時間など暗号化を直接解読するのではなく，外部からの観測といった二次的要素から解読を行う手法である。
イ：**スキャベジング**の説明である。
ウ：**中間者攻撃**（man in the middle attack）の説明である。
エ：**SQL インジェクション攻撃**の説明である。

問6　エ

解説　**CRL**は，有効期間中に失効した公開鍵証明書を記載したリストで，認証局から発行される。公開鍵証明書の検証時の公開鍵証明書失効確認に使用するため，常に参照される。
　公開鍵証明書の有効期間中に秘密鍵の紛失や漏えいが発生した場合には，該当する証明書の廃棄手続きが行われ，公開鍵証明書のシリアル番号がCRLに記載される。
ア：CRLは常に参照される。
イ：ディジタル証明書の有効期限内に失効したものを登録する。
ウ：有効期限内に失効したリストであるため，有効期限が切れるまで失効リストに登録される。

問 7

正解 □ 完璧 □ 直前チェック □

JVN（Japan Vulnerability Notes）などの脆弱性対策ポータルサイトで採用されているCVE（Common Vulnerabilities and Exposures）識別子の説明はどれか。

ア　コンピュータで必要なセキュリティ設定項目を識別するための識別子である。
イ　脆弱性が利用されて改ざんされたWebサイトのスクリーンショットを識別するための識別子である。
ウ　製品に含まれる脆弱性を識別するための識別子である。
エ　セキュリティ製品を識別するための識別子である。

問 8

正解 □ 完璧 □ 直前チェック □

総務省及び経済産業省が策定した“電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）”を構成する暗号リストの説明のうち，適切なものはどれか。

ア　推奨候補暗号リストとは，CRYPTRECによって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。
イ　推奨候補暗号リストとは，候補段階に格下げされ，互換性維持目的で利用する暗号技術のリストである。
ウ　電子政府推奨暗号リストとは，CRYPTRECによって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。
エ　電子政府推奨暗号リストとは，推奨段階に格下げされ，互換性維持目的で利用する暗号技術のリストである。

春

問7　ウ

解説　**JVN**は，日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し，情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトである。JPCERTコーディネーションセンター（JPCERT/CC）と，独立行政法人情報処理推進機構（IPA）が共同運営している。

CVEは，脆弱性を識別するための識別子である。

問8　ウ

解説　CRYPTREC暗号リストの**電子政府推奨暗号リスト**とは，暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された暗号技術について，市場における利用実績が十分であり今後の普及が見込まれると判断された当該技術の利用を推奨するもののリストである。

推奨候補暗号リストとは，CRYPTRECにより安全性及び実装性能が確認され，今後，電子政府推奨暗号リストに掲載される可能性のある暗号技術のリストである。

ア：電子政府推奨暗号リストの説明である。
イ，エ：格下げされた暗号技術のリストではない。

問 9 正解 完璧 直前チェック

IPsecに関する記述のうち，適切なものはどれか。

ア　IKEはIPsecの鍵交換のためのプロトコルであり，ポート番号80が使用される。
イ　暗号化アルゴリズムとして，HMAC-SHA1が使用される。
ウ　トンネルモードを使用すると，エンドツーエンドの通信で用いるIPのヘッダまで含めて暗号化される。
エ　ホストAとホストBとの間でIPsecによる通信を行う場合，認証や暗号化アルゴリズムを両者で決めるためにESPヘッダではなくAHヘッダを使用する。

問 10 正解 完璧 直前チェック

NTPを使った増幅型のDDoS攻撃に対して，NTPサーバが踏み台にされることを防止する対策として，適切なものはどれか。

ア　NTPサーバの設定変更によって，NTPサーバの状態確認機能（monlist）を無効にする。
イ　NTPサーバの設定変更によって，自ネットワーク外のNTPサーバへの時刻問合せができないようにする。
ウ　ファイアウォールの設定変更によって，NTPサーバが存在する自ネットワークのブロードキャストアドレス宛てのパケットを拒否する。
エ　ファイアウォールの設定変更によって，自ネットワーク外からの，NTP以外のUDPサービスへのアクセスを拒否する。

問 11 正解 完璧 直前チェック

マルウェアの活動傾向などを把握するための観測用センサが配備されるダークネットはどれか。

ア　インターネット上で到達可能，かつ，未使用のIPアドレス空間
イ　組織に割り当てられているIPアドレスのうち，コンピュータで使用されているIPアドレス空間
ウ　通信事業者が他の通信事業者などに貸し出す光ファイバ設備
エ　マルウェアに狙われた制御システムのネットワーク

春

問9　ウ

解説　**IPsec**は，インターネットで暗号通信を行うための規格である。IPv6では標準で実装される。

ア：UDPポート番号500が使用される。
イ：IPsecでは鍵交換プロトコルとして**IKE**（Internet Key Exchange）が使用される。HMAC-SHA1は，IPsecのAHヘッダ（認証ヘッダ）などの認証機構に採用されている鍵ハッシュ関数を利用したメッセージ認証方式である。
ウ：IPsecの通信モードには，データ部分のみを認証/暗号化して元のIPヘッダは対象としないトランスポートモードと，IPヘッダも含めて暗号化・カプセル化するトンネルモードの二つがある。トランスポートモードはエンド・ツー・エンドで認証や暗号化を行う場合に使用し，トンネルモードはネットワーク間の通信に対して認証や暗号化を行う場合に使用される。
エ：AHヘッダでは暗号化はできない。

問10　ア

解説　**NTP増幅型攻撃**は，インターネットの時刻動機プロトコルである**NTP**（Network Time Protocol）の弱点を利用して，不正なネットワークトラフィックを発生させ増幅することで攻撃する手法である。

ア：正しい。NTPサーバの状態確認機能を利用して攻撃することが可能であるため，無効にすることで防御できる。
イ，エ：NTPは他のサーバへ時間を合わせにいくため，自ネットワーク外への時刻同期ができないと時刻を合わせることができない。
ウ：ブロードキャストパケットを利用した攻撃ではないため，効果はない。

問11　ア

解説　**ダークネット**とは，インターネット上の未使用のIPアドレス空間のことを示す。ダークネットに到来するパケットを観測することで，インターネットを経由して感染を広めるマルウェアの活動傾向などを把握することができる。

問 12 正解 完璧 直前チェック

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。

問 13 正解 完璧 直前チェック

迷惑メールの検知手法であるベイジアンフィルタリングの説明はどれか。

ア　信頼できるメール送信元を許可リストに登録しておき，許可リストにないメール送信元からの電子メールは迷惑メールと判定する。
イ　電子メールが正規のメールサーバから送信されていることを検証し，迷惑メールであるかどうかを判定する。
ウ　電子メールの第三者中継を許可しているメールサーバを登録したデータベースに掲載されている情報を基に，迷惑メールであるかどうかを判定する。
エ　利用者が振り分けた迷惑メールから特徴を学習し，迷惑メールであるかどうかを統計的に解析して判定する。

問 14 正解 完璧 直前チェック

DNSSECで実現できることはどれか。

ア　DNSキャッシュサーバからの応答中のリソースレコードが，権威DNSサーバで管理されているものであり，改ざんされていないことの検証
イ　権威DNSサーバとDNSキャッシュサーバとの通信を暗号化することによる，ゾーン情報の漏えいの防止
ウ　長音“ー”と漢数字“一”などの似た文字をドメイン名に用いて，正規サイトのように見せかける攻撃の防止
エ　利用者のURLの打ち間違いを悪用して，偽サイトに誘導する攻撃の検知

春

問12　エ

解説　**rootkit**とは，**クラッカ**が**セキュリティホール**などを利用して不正侵入した後に，侵入の隠ぺい，バックドアの確保，踏み台による攻撃などに用いる機能をまとめたツール群のことである。
イ：ウイルス対策ソフトの説明である。
ウ：ポートスキャンツールの説明である。

問13　エ

解説　**ベイジアンフィルタリング**は，ベイズ理論を用いた自己学習型スパムメールフィルタである。スパムの要素を示す言葉と特徴のリストを自動生成し，フィルタリングする仕組みである。
　ベイズ理論とは，過去の事象の発生確率から統計的に解析して予測する理論である。提唱者であるトーマス・ベイズ（Thomas Bayes）の名前が付けられている。
ア：メールサーバの**アクセスリスト**による対策の説明である。
イ：**送信ドメイン認証**による対策の説明である。
ウ：**ブラックリスト**を利用した対策の説明である。
エ：**ベイジアンフィルタリング**の説明である。自己学習し統計的に解析する点に注目するのがよい。

問14　ア

解説　**DNSSEC**（Domain Name System Security Extension）：DNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を証明するセキュリティ拡張機能のことである。応答を送信するDNSサーバが秘密鍵を使って応答に署名し，受信する側が公開鍵で検証する。秘密鍵で正しい署名を付けるので，署名の検証によって偽の応答を検知できる。

問 15 正解 完璧 直前チェック

DNSの再帰的な問合せを使ったサービス不能攻撃（DNS amp攻撃）の踏み台にされることを防止する対策はどれか。

ア　DNSキャッシュサーバとコンテンツサーバに分離し，インターネット側からDNSキャッシュサーバに問合せできないようにする。
イ　問合せがあったドメインに関する情報をWhoisデータベースで確認する。
ウ　一つのDNSレコードに複数のサーバのIPアドレスを割り当て，サーバへのアクセスを振り分けて分散させるように設定する。
エ　他のDNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を，ディジタル署名で確認するように設定する。

問 16 正解 完璧 直前チェック

SMTP-AUTHの特徴はどれか。

ア　ISP管理下の動的IPアドレスからの電子メール送信について，管理外ネットワークのメールサーバへのSMTP接続を禁止する。
イ　PCからメールサーバへの電子メール送信時に，ユーザアカウントとパスワードによる利用者認証を行う。
ウ　PCからメールサーバへの電子メール送信は，POP接続で利用者認証済みの場合にだけ許可する。
エ　電子メール送信元のサーバが，送信元ドメインのDNSに登録されていることを確認して，電子メールを受信する。

春

問15　ア

解説　DNSの再帰的な問合せを使ったサービス不能攻撃（**DNS amp**）は**DDoS**（Distributed Denial of Service）の一種である。DNSキャッシュサーバを踏み台とし，送信元を偽装したDNSクエリによりDNSサーバを攻撃する手法である。

対策は，**DNSキャッシュポイズニング**の脆弱性対策を行うことや，通常一つになっているキャッシュサーバの機能とコンテンツサーバの機能を分離して，コンテンツサーバを守ることである。

DNSキャッシュサーバ：DNSの参照に必要な一時的なデータのみを保管する。
DNSコンテンツサーバ：DNSのゾーン情報をもち，恒久的なデータを保管する。

ア：正しい。DNS amp攻撃はキャッシュサーバを狙って攻撃をする。
イ：**Whois**でドメイン情報を検索しても踏み台の防止にはならない。Whoisは，IPアドレスやドメイン名の登録者に関する情報を検索，提供可能とするサービスである。
ウ：**DNSラウンドロビン**の説明である。

問16　イ

解説　**SMTP-AUTH**は，クライアントがメールを送る際，SMTPサーバへのアクセス時にユーザ認証を行い，認証されたクライアントだけに電子メールの送信を許可する方式である。

ア：電子メール広告企業やウイルス感染してボット化したPCなどからのメール発信を阻止するために，管理外のメールサーバへSMTP通信の利用を防止する対策。**OP25B**（Outbound Port 25 Blocking）という。
ウ：**POP before SMTP**の説明。電子メールの送信を行う際のユーザ認証方法の一つである。送信前に指定したPOP3サーバにあらかじめアクセスさせることによって，SMTPサーバの使用許可を与える方式。SMTPが開発された当初は，ユーザ認証機能が実装されていなかったため，管理外のネットワークからSMTPを利用させたい場合に使用してきた。
エ：不正な発信元からの電子メール受信を防ぐための方法の一つ。実在しないドメインから大量の広告電子メールが発信された場合に対する対策である。

問 17 正解 完璧 直前チェック

SQLインジェクション対策について，Webアプリケーションの実装における対策とWebアプリケーションの実装以外の対策として，ともに適切なものはどれか。

	Webアプリケーションの実装における対策	Webアプリケーションの実装以外の対策
ア	Webアプリケーション中でシェルを起動しない。	chroot環境でWebサーバを稼働させる。
イ	セッションIDを乱数で生成する。	TLSによって通信内容を秘匿する。
ウ	パス名やファイル名をパラメタとして受け取らないようにする。	重要なファイルを公開領域に置かない。
エ	プレースホルダを利用する。	データベースのアカウントがもつデータベースアクセス権限を必要最小限にする。

問 18 正解 完璧 直前チェック

TCPヘッダに含まれる情報はどれか。

ア　宛先ポート番号　　イ　送信元IPアドレス
ウ　パケット生存時間（TTL）　　エ　プロトコル番号

問 19 正解 完璧 直前チェック

192.168.1.0/24のネットワークアドレスを，16個のサブネットに分割したときのサブネットマスクはどれか。

ア　255.255.255.192　　イ　255.255.255.224
ウ　255.255.255.240　　エ　255.255.255.248

問17　エ

解説 **SQLインジェクション**は，アプリケーションの想定しないSQL文を実行することでデータベースシステムを不正に操作し，データの取得や書き換えなどを可能にする攻撃のことである。対策としては，プレースホルダを利用する。プレースホルダは，「$1」や「?」のように，SQL文の中で入力された文字列を他の文字列に置換する代替する変数である。

また，データベースのアカウントのもつアクセス権を必要最小限にして，最低限な機能のみを実行可能としておくことも必要である。

問18　ア

解説 TCPヘッダは下記のような構造となっている。

<table>
<tr><td colspan="6">送信元ポート番号</td><td colspan="2">宛先ポート番号</td></tr>
<tr><td colspan="8">シーケンス番号</td></tr>
<tr><td colspan="8">ACK番号</td></tr>
<tr><td>データオフセット</td><td>予約領域</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>ウィンドウサイズ</td></tr>
<tr><td colspan="6">チェックサム</td><td colspan="2">緊急ポインタ</td></tr>
</table>

問19　ウ

解説 **サブネットマスク**：ネットワークの識別に利用されるネットワークアドレス部を定義する32ビットの数値。サブネットマスク値とIPアドレスのビットの論理積を計算することによりIPアドレスのネットワークアドレス部を取得できる。

192.168.1.0/24のアドレスで，サブネットマスクが255.255.255.0であるから，左から24ビットがネットワーク部，残り8ビットがホスト部である。ネットワーク自体やブロードキャストアドレスを含めて2^8=256台のホストの割当てができる。選択肢のサブネットマスクのホスト数から，分割するサブネット数は下記になる。

選択肢	サブネットマスク	第4オクテットの計算	ホスト数	サブネット数
ア	255.255.255.192	256 − 192 = 64	64個	256/64 = 4
イ	255.255.255.224	256 − 224 = 32	32個	256/32 = 8
ウ	255.255.255.240	256 − 240 = 16	16個	256/16 = 16
エ	255.255.255.248	256 − 248 = 8	8個	256/8 = 32

問 20 正解 完璧 直前チェック

HTTPのヘッダ部で指定するものはどれか。

ア　HTMLバージョン情報（DOCTYPE宣言）
イ　POSTリクエストのエンティティボディ（POSTデータ）
ウ　WebサーバとWebブラウザ間の状態を管理するクッキー（Cookie）
エ　Webページのタイトル（＜TITLE＞タグ）

問 21 正解 完璧 直前チェック

分散トランザクション処理で利用される2相コミットプロトコルでは，コミット処理を開始する調停者（coordinator）と，調停者からの指示を受信してから必要なアクションを開始する参加者（participant）がいる。この2相コミットプロトコルに関する記述のうち，適切なものはどれか。

ア　参加者は，フェーズ1で調停者にコミット了承の応答を返してしまえば，フェーズ2のコミット要求を受信していなくても，ローカルにコミット処理が進められる。
イ　調停者に障害が発生するタイミングによっては，その回復処理が終わらない限り，参加者全員がコミットもロールバックも行えない事態が起こる。
ウ　一つの分散トランザクションに複数の調停者及び参加者が存在し得る。例えば，5個のシステム（プログラム）が関与している場合，調停者の数が2，参加者の数が3となり得る。
エ　フェーズ1で応答のない参加者が存在しても，調停者は強制的にそのトランザクションをコミットすることができる。

問 22 正解 完璧 直前チェック

共通フレームによれば，システム要件の評価タスクにおいて見極めることはどれか。

ア　システム要件とシステム方式との間に一貫性があるかどうか。
イ　システム要件とシステム方式との関連が追跡できるかどうか。
ウ　システム要件を満たすシステム方式設計が実現可能かどうか。
エ　ソフトウェア品目が割り当てられたシステム要件を満たすかどうか。

春

問20　ウ

解説
ア：**DOCTYPE宣言**は，HTTPリクエストで指定され，ヘッダ部よりも手前に記載する。
イ：**POSTデータ**は，HTTPヘッダ部の後のBody部に記載する。
ウ：**Cookie**は，HTTPリクエストヘッダに含まれる。
エ：**TITLEタグ**は，HTMLのなかで指定される。
本問は，HTTP通信時のヘッダ部分を指しているため，HTML文のなかで記載するヘッダ部分とは異なることに注意が必要である。

問21　イ

解説 分散トランザクション処理で用いられる2相コミットプロトコルでは，フェーズ2で調停者が参加者に対してコミット/ロールバック要求を出す。このときに通信障害が発生すると，調停者の回復処理が終わらない限り，参加者全員がコミットもロールバックも行えない事態が起きる。
ア：他の参加者がコミットNGの場合もあるから，ローカルにコミット処理はできない。
ウ：全参加者のコミット可否を把握するため，複数の調停者はあり得ない。
エ：フェーズ1で障害が発生したと考えられる場合には，コミットしない。

問22　ウ

解説 システム要件の評価は，システム方式設計においてシステム要件が具体的に実現可能であるかを見極める必要がある。また，システムの運用，保守が可能であるかどうかも合わせて見極める必要がある。
ア，イ，エ：システム方式の評価項目である。

問 23 正解 完璧 直前チェック

マッシュアップを利用してWebコンテンツを表示している例として，最も適切なものはどれか。

ア　Webブラウザにプラグインを組み込み，動画やアニメーションを表示する。
イ　地図上のカーソル移動に伴い，Webページを切り替えずにスクロール表示する。
ウ　鉄道経路の探索結果上に，各鉄道会社のWebページへのリンクを表示する。
エ　店舗案内のWebページ上に，他のサイトが提供する地図検索機能を利用して出力された情報を表示する。

問 24 正解 完璧 直前チェック

データセンタにおけるコールドアイルの説明として，適切なものはどれか。

ア　IT機器の冷却を妨げる熱気をラックの前面（吸気面）に回り込ませないための板であり，IT機器がマウントされていないラックの空き部分に取り付ける。
イ　寒冷な外気をデータセンタ内に直接導入してIT機器を冷却するときの，データセンタへの外気の吸い込み口である。
ウ　空調機からの冷気とIT機器からの熱排気を分離するために，ラックの前面（吸気面）同士を対向配置したときの，ラックの前面同士に挟まれた冷気の通る部分である。
エ　発熱量が多い特定の領域に対して，全体空調とは別に個別空調装置を設置するときの，個別空調用の冷媒を通すパイプである。

問 25 正解 完璧 直前チェック

入出金管理システムから出力された入金データファイルを，売掛金管理システムが読み込んでマスタファイルを更新する。入出金管理システムから売掛金管理システムへのデータ受渡しの正確性及び網羅性を確保するコントロールはどれか。

ア　売掛金管理システムにおける入力データと出力結果とのランツーランコントロール
イ　売掛金管理システムのマスタファイル更新におけるタイムスタンプ機能
ウ　入金額及び入金データ件数のコントロールトータルのチェック
エ　入出金管理システムへの入力のエディットバリデーションチェック

春

問23　エ

解説　**マッシュアップ**とは，Web上に提供されている情報やサービスなどを組み合わせて新しいWebサービスやデータベース，ソフトウェアを開発・提供することである。

マッシュアップをしやすいように，企業のWebサービスを利用するためのAPIを公開・提供するケースが増えている。インターネット上の地図サイトなど各種サービスがある。

問24　ウ

解説　**コールドアイル**や**ホットアイル**は，データセンタ内のラックを配置する際の並べ方のことである。コールドアイルは，ラックの前面を指しサーバやストレージ装置が吸気する際に冷たい空気を供給するためのスペースとなる。

逆にホットアイルは，ラックの背面を指し，サーバやストレージ装置の廃熱されるスペースとなる。

問25　ウ

解説　入金額と入金データ件数をチェックすることで，データが欠けたり誤っていないことが検証できる。

ア，エ：データの正確性はチェックできるが，受渡しが正確に行われたかをチェックすることはできない。
イ：マスタファイル更新のタイムスタンプだけでは，データ受渡しが全て行われたか，正しく行われたかを確認できない。