【講義メモ】 担当：平野正喜（ひらのまさき）
この講座ではプロジェクタに講義メモを書きながら進めます。この文字サイズの読める席にお座りください。
18:15～20:45（途中休憩有）。受講者数は１３人です。
この講義メモは講義終了と同時に下記のサイトにPDFで掲載し、ダウンロード可能にします。ご利用ください。次回予告も掲載します。質問やコメントが送信可能です。
https://tkuip.rundog.org
前回の１問：侵入検知システムは？ 正解はイ
ア DMZ（p.277） イ IDS（p.278） ウ XSS（p.272） エ CSRF（p.272）
次回予告：p.282「物理的なセキュリティ対策」から再開しテキストを終え、直前答練（過去問演習）を行います。利用する問題文プリントは講師が当日配布しますが、解説が（初日に配布した）問題集に収録されていますので、活用をお勧めします（持参するかどうかは自由です）。

p.282 9-14-2 物理的なセキュリティ対策
・【補足】アンチパスバック：入室制限において１人の認識で他者を一緒に通してしまう「友連れ」を防止するために、入室記録のない者の退室を認めない仕掛け。
p.283 9-14-3 暗号技術
・【補足】暗号化アルゴリズムと鍵のイメージ：例えば「N文字ずらす」という暗号化アルゴリズム、N＝2という鍵があれば、元の文章（平文）「TKU」から暗号文「VMW」を生成できる
・【補足】共通鍵暗号方式：暗号化用の鍵と復号（平文に戻す）ための鍵が同一であるシンプルな暗号化方式。暗号化・復号が高速だが、送信先ごとに異なる鍵をあらかじめ配布しておく必要がある。また不特定多数との暗号化通信は不可。
・【補足】公開鍵暗号化方式：事前に専用のソフトウエアにより暗号化用の鍵と復号用の鍵を生成する暗号化方式。暗号化用の鍵を公開したり、アプリケーションに与えておくことにより、送信者の誰でも暗号化が可能になる。復号は受信者が持つ復号鍵のみで可能なので、手間なく、不特定多数とも暗号化通信が可能。しかし、仕組みが複雑なので暗号化・復号が低速。
・AES=アドバンスド（進化した）エンクリプション（暗号化）スタンダード（標準）：共通鍵暗号化方式の国際標準。
・DES=データ・エンクリプション（暗号化）スタンダード（標準）：AESの基になった初期の法式で、暗号化の強度が弱い（短時間で解読できてしまう）ので、現在は利用されない
・RSA：公開鍵暗号方式の国際標準
・SSL＝セキュア（安全、暗号化された）ソケット（接続）レイア（層）：WebブラウザとWebサーバの間で暗号化通信を行うプロトコル。これを用いるのがHTTPS（p.258,285）
・【補足】ディジタル証明書：公開鍵の電子証明書データで、公開鍵の正当性を第三者が認めていることを示す
・【補足】ワンタイムパスワード：使い捨てパスワードともいい、専用のデバイスやスマートフォンに時間ごとに表示される数字列をパスワードとして用いる方式。一定時間で無効になるので詐取されても被害が起こらない。
・【補足】 生体認証の2タイプ：身体的特徴（指紋、静脈、網膜など）と、行動的特徴（筆跡など）。どちらも、本人拒否率と他人受入率を同時に下げるには工夫が必要

・【補足】リスクベース認証の例：ふだん使っていないPCやブラウザやスマートフォンや所在地からのアクセス時に、通常とは異なる確認メッセージが表示されたり、２要素認証（PCとスマートフォン両方での入力）が求められる仕組み
・SSO=シングル（１度の）サインオン（認証）：あるシステムへのログインを、他のシステムが信用する方式と、認証専用のシステムへのログインを他のシステムが確認する方式がある
・CAPTCHA＝人間には文字列が識別できるが、システムでの文字列解析ができないような絵による「利用者が人間である（自動化されたシステムではない）」ことの証明手段
・【補足】デジタル署名：公開鍵暗号方式を逆向きに使い、作成者が自分の鍵で暗号化した文書を相手に渡すと、相手は誰でも作成者の公開鍵で復号できる。これにより、作成者が本人であること、途中で改ざんされていないことを確認するのが目的。暗号化の意味はない。
・【補足】ハッシュ：デジタル署名には公開鍵暗号方式を用いるので低速で、大きなファイルでは時間がかかる。そこで、元の文書から機械的な方式で文字列を生成して用いる。この方式をハッシュ関数、文字列をハッシュ値という。元の文書が異なればハッシュ値も違うものになるようにハッシュ関数は工夫されている。よって、ディジタル署名では、ハッシュ値を暗号化して用いる。
① 送信者は文書からハッシュ値①を得る
② ハッシュ値を自分の鍵を用いて暗号化する
③ ハッシュ値の暗号化結果と、文書を相手に送る（公開してもOK）
④ 受信者は受け取ったハッシュ値を送信者の公開鍵で復号して元のハッシュ値①を得る
※得られれば送信者は本人だとわかる
⑤ 受信者も文書からハッシュ値②を得る
⑥ ①と②が同じであれば、改ざんされていない
・CA＝サーティフィケーション（認証）エージェンシー（局、第三者）：公開鍵の正当性を認証しディジタル証明書を発行する機関や会社。証明書も暗号化されており、CAの公開鍵で復号できることで、証明書の正当性を確認できる
・PKI＝パブリックキー（公開鍵）インフラストラクチャ（基盤）：公開鍵暗号化方式を用いることで、社会的な暗号化通信の基盤を構築すること。なお、公開鍵暗号化方式だけでは低速であることから、共通鍵方式との併用（ハイブリット方式）が活用されている。
① 共通鍵を用意して、これで文書を暗号化する（共通鍵方式なので高速）
② 共通鍵自体を相手の公開鍵で暗号化する（短い文字列なので時間がかからない）
③ 相手に①と②を送る
④ 受信者は自分の復号鍵で②を復号して、共通鍵を得る
⑤ 受信者は④で得た共通鍵で①を復号する（共通鍵方式なので高速）

＜直前答練＞
R7公開問題から頻出問題をピックアップして時間内に解答・解説を行います。
【ストラテジ系】
問1：正解はウ
請負契約は p.43、偽装請負は請負契約でありながら派遣契約（p.42）と同じ状態になっていること。ポイントは指揮命令関係で、請負業者Bが指揮命令を行わなず、派遣先Aに従ってしまうと、請負にならないので違法。
問7：正解はイ。四択から該当しない3つを除くことで消去法で正解を得るパターン。

CRM＝カスタマ（顧客）リレーションシップ（関係）マネジメント（管理）：p.65
PoC=プルーフ（検証）オブ・コンセプト（概念）
RAS＝リモート（外部）アクセス・サーバ：
SLA＝サービスレベル・アグリメント（合意書）：p.126
問13：正解はウ。「技術情報の提供を依頼」に着目する
EDI＝エレクトロニック（電子）データ・インターチェンジ（交換）：p.67
KPI＝キー（重要）パフィーマンス（業績）インジケータ（指針）：p.64
RFI＝リクエスト（依頼）フォー・インフォメーション（情報）：p.93
RFP＝リクエスト（依頼）フォー・プロポーザル（提案）：p.93
問15：正解はア。「事業領域ごとに独立した組織」がカンパニーと呼ばれる
カンパニ制組織、機能別組織、マトリックス組織は p.14
プロジェクト（組織）は p.116
問16：正解はイ。「不正なアクセス」の禁止法ではないので注意。
不正アクセス禁止法は p.38。IDとパスワードの無断利用（c）と、その助長行為（a）を禁止している。IDとパスワードに関連していてもマルウェアの作成行為は対象外。
問18：正解はア。アクセシビリティは p.232
イはCRM（顧客関係管理）など。ウはUX（p.60）。エはアクセス権（p.204）
問19：正解はア。
VR＝ヴァーチャル（仮想）リアリティ（現実）。p.239。アが該当
AR＝オーギュメンテッド（拡張）リアリティ（現実）。p.239。イウエが該当
【マネジメント系】
問37：正解はエ。（IT）サービスマネジメント、SLA、SLMは p.126
SLA＝サービスレベル・アグリメント（合意書）
SLM＝サービスレベル・マネジメント（管理）
NDA＝ノン（非）ディスクロージャ（公開）アグリメント（合意書）。p.43
SCM＝サプライ（供給）チェーン（連鎖）マネジメント（管理）。p.65
問38：正解はエ。情報セキュリティ監査は p.130
アはシステム監査（p.129）
イはセキュリティワイヤ（p.282）などが該当
ウはITガバナンス（p.131）
問39：正解はア。アジャイルは p.105。ウォーターフォールモデルは p.104。
アジャイル（迅速）はウォータフォール（滝）モデルの改善であり、「特徴を継承」しているわけではない。
「開発工程を順に実施」はウォータフォールモデルの特徴。
問44：正解はエ。「確認用のソフトウェア」が試作品（プロトタイプ）を表している
アジャイルは p.105。ウォーターフォール、スパイラル、プロトタイピングは p.104。
問49：正解はウ。クラウドサービスは p.87（クラウドコンピューティング）。サービスデスク、チャットボットは p.127。
FAQ＝フレクエント（頻繁に）アスクド（尋ねられた）クエッション（質問）。よくある質問と回答集。サイト上に置くことで誰でも利用できる。チャットボットの基データになるが、チャットボットを導入しても内容が充実することはあまりない。
なお、オペレータのチャットや電話のスキルと、AIであるチャットボットは無関係

問50：正解はア。チャットボットは p.127。
イはIoT（p.74）。
ウは産業用ロボットなど。
エはRPA＝ロボティック（ソフトウェアによるロボットのような仕掛けによる）プロセス（手順）オートメーション（自動化）。p.84
【テクノロジ系】
問57：正解はイ。
プロキシサーバは代理アクセスをするサーバ機能 p.278。HTTPプロキシサーバは、主にLAN内のWebブラウザからのリクエスト（要求）を受け取って、代わりにインターネット上のWebサーバとの送受信を行うサーバ。
問58：正解はウ
DNSは p.263。ドメインネーム（ドメイン名）システム。www.tku.ac.jp のようなドメイン名と、これに対応する 220.220.1.1 のようなIPアドレスとの相互変換をしてくれるシステム。
アはDHCP＝ダイナミック（動的）ホスト（PCなどのノード）コンフィグレーション（設定）プロトコル、p.263
イはHTTPS＝ハイパテキスト（HTMLなどで書かれた制御情報を持つ文書）トランスファー（転送）プロトコル・セキュア（暗号化）、p.285
エのMACアドレスはネットワークインターフェイスごとの番号で、ホストやドメインには対応付けられない（1対多になる）
問60：正解はエ。
TCP／IPは p.257、FTPは p.258、ファイル・トランスファ（転送）プロトコル。
アはNTP＝ネットワークタイム（時刻合わせ）プロトコル p.259
イはSMTP＝シンプル・メール・トランスファ（転送）プロトコル p.258
ウはDHCP＝ダイナミック（動的）ホスト（PCなどのノード）コンフィグレーション（設定）プロトコル、p.263
問61：正解はウ。DBMS＝データベースマネジメント（管理）システム。p.240。
トランザクションは一連の更新のこと p.248。
変更結果の確定をコミット、処理前に戻すことをロールバックという。
アはレプリケーション p.196
イはログファイル p.249
エはインデックス（索引）の機能
今日の一問はR7公開問題の問64とします。
回答と解説は模擬試験とその解説の後の、要点整理で行います。

次回予告： 6号館F505教室で模擬試験を行います。いつもの教室ではありませんので、ご注意ください。
※模擬試験終了時に、問題・解説のプリントをお渡しします
※模試を欠席される方には、来週金曜日からの模擬試験解説で問題・解説のプリントをお渡ししますので、講師までお知らせください。
※今回、欠席された方には、来週金曜日からの模擬試験解説でR7公開問題のプリントをお渡ししますので、講師までお知らせください。