【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： ネットワークとネットワークを接続する機器は？ 正解はエ
ア リピータハブ イ スイッチングハブ ウ モデム エ ルータ
p.259 9-10-2 TCP／IP の続きから
・NTP＝ネットワーク・タイム・プロトコル：インターネットに接続しているノードの時計合わせ
・PPP＝ポイント・ツー・ポイントプロトコル：２点間接続用、コンピュータとネットワークなど
・【補足】ポート番号：サービス識別番号で、アドレスと合わせて「どのサーバのどのサービス宛か」を示すために用いる。基本的な番号は固定で、SMTPは２５番。
p.260 9-11-1 ネットワーク応用
・【補足】IPアドレス：３２ビットなのはIPv4（バージョン４）のアドレスで、現在IPv6（p.264）に移行中。どちらもネットワークとノード（ホスト）の情報を持つので、離れたネットワークにあるノードとの通信にも利用できる
・ICANN=インターネット・コーポレーション（組織）フォー・アサインド（引き当てた）ネーム（名前）＆ナンバー（番号）：グロバールIPアドレスが世界で１つだけの番号であること、これに付随するドメイン名（例： tku.ac.jp）が世界的に重複しないことを保証する。
・NIC＝ネットワーク・インフォメーション・センター：国や地域ごとにあるICANNの下部組織。日本はJPNIC。
・【補足】プライベートIPアドレス：IPアドレスの範囲の一部で、LANにおいて自由に利用できる番号帯。
・【補足】アドレスクラス：IPアドレスのネットワーク部分とノード（ホスト）部分の切れ目を定めるルールで主にABCの３種類（DEは特殊用途）。ノード数を多くしたい場合はA、ネットワークを細かく分けたい場合はCを用いる。
・NAT=ネットワーク・アドレス・トランスレーション（変換）：LANにあるプライベートIPアドレスのノードが、インターネット上のノード（サーバ）と通信できるように、グローバルIPアドレスに変換する仕組み。
・NAPT＝ネットワーク・アドレス＆ポート番号・トランスレーション：NATでは世界中のノードの通信には足りないので、アドレス（約４２億）とポート番号（約6万）の組み合わせで変換するように改良したもの。現在の主流。
・DHCP=ダイナミック（動的）ホスト（ノード）コンフィグレーション（設定）プロトコル：主にプライベートIPアドレスの自動設定をしてくれる仕組み。通常、サーバがルータや無線アクセスポイントにあり、PCやゲーム機などがクライアントとしてサービスを要求する。
・【補足】デフォルトゲートウェイ：LAN上にない相手へのパケットの出入り口となるノードのIPアドレス。主に、ルータが担う。既定の出入り口の意味。主に、DHCPで設定される。
・DNS=ドメインネーム（ドメイン名）システム：IPアドレスでの通信は不便で管理しづらいので、ドメイン名という名前をつけ、IPアドレス⇔ドメイン名の変換を行う仕組み
・URL＝ユニフォーム（単一形式）リソース（ネットワーク上の資源）ロケータ（位置情報）：プロ

トコル名、サーバ(ホスト)名、ドメイン名、ディレクトリ名をつないだ文字列で、インターネット上の住所を示すもの。
・IPv6:IPv4のIPアドレスの不足(枯渇)やセキュリティの向上のための新バージョン。アドレスが32ビットから128ビットになり、世界中のノードに割り振ることが可能。IPv4と混在できるので、ゆっくりと移行中。
・IPsec:IPに含まれるパケットの暗号化機能。IPv6では標準。
p.265 9-11-2 インターネットのサービス
・WWW=ワールドワイド(世界的な広さの)ウェブ(くもの巣):迂回が可能なネットワークを世界的につないだもの。データの配信や閲覧などのサービスを提供。
・RSS=リソース(ネットワーク上の資源)ディスクプリションフレームワーク(記述のための枠組み)サイトサマリー(サイト情報の要約用)。ニュースサイトやブログなどが提供する要約。
・【補足】電子メールのBcc:ブラインド(見えない)カーボンコピー(写し)の略で、通常、メールに記述した宛先(TOまたはCC)は受信者全員に見えるが、Bccを使うと見えなくできる。よって、相互にアドレスを知らせたくない複数の相手に同報メールを送る場合に便利。
※ TOとCCは動作は同じだが、TOには主たる受信者を指定する。
・MIME=マルチパーパス(多目的)インターネットメール・エクステンション(拡張):本来は文字列しか送れないインターネットメールにおいて、画像などのファイルを添付できるようにした仕組み。
p.266 9-11-3 通信サービス
・ISP=インターネット・サービス・プロバイダ(提供業者)
・FTTH=ファイバー(光回線)トゥ・ザ・ホーム(家庭へ)
・VoIP=ボイス(音声)オン・IP:音声⇔パケットの変換技術。IP電話の基礎技術。
・VoIPゲートウェイ:音声電話網とインターネットを接続するゲートウェイ装置
・MNO=モバイル・ネットワーク・オペレータ:移動体通信事業者
・MVNO=モバイル・バーチャル(仮想)ネットワーク・オペレータ:MNOの通信網を使って移動体通信事業を行う
p.268 9-12-1 情報セキュリティの概念
・【補足】情報セキュリティの脅威:人的、技術的、物理的の3種類がある
p.269 9-12-2 脅威と脆弱性
・【補足】脆弱性:システムの欠陥ではなく、セキュリティ上の盲点や通常の利用では発現しないような問題点のこと。
・【補足】ソーシャルエンジニアリング:社会的な手口。技術的攻撃ではない手法で、主に、情報の詐取(盗み取り)を狙う行為。なりすまし、スカベンジング(ゴミ盗み)、盗み見など。
・【補足】不正のトライアングル:通常、不正行為は本人の心的な抵抗にあうが、3要素が揃うと抵抗しくなること。動機、機会、正当化。
p.271 9-12-3 サイバー攻撃の手法
・APT=アドバンスド(進化した)パーシステント(執拗な)スリート(脅威)。標的型攻撃の特徴で、成果が得られるまで周到な準備と調査を行いしつこく攻撃ししてくること。
・【補足】BOF=バッファ(入力データの格納域)オーバーフロー(あふれさせる)攻撃。入力のあるWebやアプリにおいて、入力データの長さのチェックを怠ると、異常な長さの文字列の入力により想定外のダメージや結果になることを狙う攻撃。
・【補足】SQLインジェクション:データベースを用いるアプリなどは、応答をSQLで行うため

に画面などから得たデータを入れたSQLを送信する。例「住所を出せ、対象は□」という意味のSQLの□に埋め込む。よって、画面からSQL文（例：なし＆表を消せ）を含むデータが入ると「住所を出せ、対象はなし＆表を消せ」という意味になってしまう攻撃。アプリ側でSQL文になるような入力を無害化（サニタイジング）すれば対処可能。
・DoS＝デニール（不能化）オブ・サービス：サーバに正当な手段で過剰な負荷を与える攻撃。防御が難しいが、攻撃元を遮断することで対処。
・DDoS=ディストリビューテッド（拡散）DoS：攻撃元を多数化することで、対処を難しくするDoS攻撃。マルウェア（コンピュータウィルス）が感染したPCや、パスワードが管理されていないIoT機器（主に監視カメラ）を乗っ取って悪用することが多い。
・XSS＝クロスサイト（Webサイトをまたがって行う）スクリプティング（スクリプト言語を用いる攻撃）：善意のサイト（脆弱性有り）と悪意のサイトを組み合わることで可能になる攻撃
・CSRF＝クロスサイト（Webサイトをまたがって行う）リクエスト（要求）フォージェリ（偽装）：サービスにログイン中のユーザを悪意のあるページに誘導し、そこでの操作がサービスのページにリクエストされるようにする仕掛け。SNSに悪意のある書き込みをさせたり、個人情報を書き込ませたりするのが目的。
p.273 9-13-1 リスクマネジメント
・【補足】リスク対応の4種：（※出題により表現が異なる場合がある）
① 回避：リスクのある行為を行わない、使わない、取りやめる
② 軽減：リスクによる損害を小さくする
③ 転嫁：金銭などによりリスクを他者にゆだねる。つまり保険を掛けること
④ 受容：何もしない（発生確率が低い、想定損害額が小さい場合）
p.273 9-13-2 情報セキュリティ管理
・【補足】 情報セキュリティ管理の3大コンセプト：機密性（情報がもれない）、完全性（壊されない）、可用性（使いたい時につかえる）
・ISMS＝インフォメーション（情報）セキュリティ・マネジメント（管理）システム
・ISO 27000シリーズ：ISMSの実施基準の国際標準
・JIS Q 27000シリーズ：↑の日本版
・【補足】情報セキュリティポリシー：通常、公開できる基本方針と対策基準までのこと。実施手順は業務情報を含むので非公開。トップダウンで策定するのが基本。
p.275 9-13-3 個人情報保護
・【補足】個人情報保護法：初期は個人情報を一定件数以上保持する事業者のみが対象だったが、現在では個人情報に関わる全ての事業者が対象。
・JIPDEC：プライバシーマーク（個人情報を適切に扱っている事業者の認定制度）の運用団体
p.276 9-13-4 情報セキュリティ組織・機関
・CSIRT＝コンピューター・セキュリティ・インシデント（サービス低下現象）レスポンス（対応）チーム
・SOC＝セキュリティ・オペレーション・センター：主にインシデントの検知を担う監視部門で、CSIRTへの通報と対応協力を行う
p.277 9-14-1 さまざまなセキュリティ対策
・【補足】コールバック：元は電話のかけ戻しで通話相手の確認用。ネットワークにおいても、接続要求をそのまま受けずに、逆向きに要求することで、接続相手の確認を行うこと。

・【補足】ファイアウォール：主に内側から外側への通信とその返事のみ許可する仕掛け。加えてパケットのヘッダにあるアドレス情報やポート番号などもチェックして、不適切なパケットは通過させない（パケットフィルタリング）機能を持つ
・DMZ＝デ（非）ミニタライズド（武装）ゾーン（地帯）：内部と外部の間に置くゾーンのことで、インターネットにおいては内部・外部の両方から用いるようなサーバを配置するセグメント（ネットワーク部分）。メールサーバ、Webサーバ、DNSサーバ等が対象。主に2台のファイアウォールで実現するが、1台のファイアウォールに3本のネットワークを接続する形式もある
・【補足】Proxy：代理人の意味で、NATやNAPT、ファイアウォールが、内部からの通信を受けとって、外部へのアクセスを代わりに行ってくれることの総称。
・IDS＝イントルージョン（侵入）デテクション（検知）システム：外部からの不正なパケットによる侵入行為を検知して、管理者に通知する
・IPS＝イントルージョン（侵入）プリベンション（防止）システム：外部からの不正なパケットによる侵入行為を防止するために、通信を遮断する。設定が難しいが自動化が可能。
・WAF＝Webアプリケーション・ファイアウォール：Webサーバ上で動作するアプリケーション専用のファイアウオール。Webアプリに特化した攻撃の防御が行える。
・【補足】コンテンツフィルタ：パケットフィルタリングではパケットの内容は評価できない（バラバラに切られているので）。そこで、パケットを集めて、元の通信データに戻してからチェックすること。スパムメールや情報漏えい、マルウェアを含むメールなどをチェックできるが、負荷が高く、通信速度の低下を起こしやすい。
・ペネトレーション（侵入）テスト：敢えてシステムへの侵入を行うことで、欠陥や脆弱性の有無を確認すること
・デジタル・フォレンジックス（証拠保全）：日常状態の記録（ログファイル）を保存しておくことで、比較により異状を検知すること。そのための活動。
・VPN＝ヴァーチャル（仮想）プライベート（私設）ネットワーク：「まるで自分専用のネットワークであるかのうように」利用できること。具体的には入り口での暗号化と出口での復号（元に戻すこと）を自動化したもの。インターネットなどの共有回線でも情報漏えいを懸念せずに通信できる。
・【補足】検疫ネットワーク：主に持ち歩きPCやBYOD（個人所有の端末）を社内ネットワークに接続した時、悪影響の波及を避けるために、チェック専用のネットワークに接続させる仕組み。入出国における検疫に似ている。OSや主要アプリやセキュリティのチェックや更新後、問題がなければ自動的に社内ネットワークに接続される。
・DLP＝データロス（情報漏えい）プリベンテーション（防止・監視）：主に重要情報の送信やコピーを制限する仕組み。データの動きを監視するのが特徴。
・【補足】ウイルス定義ファイル：マルウェアのパターンファイルともいい、監視ソフトウェアがマルウェア（悪意のあるソフト）の判定に用いるデータ。常に最新化する必要がある。
・IPA＝経済産業省の関連団体でITパスポート試験などの実施、セキュリティ情報の収集と分析などを行う。マルウェア感染時はIPAに届け出る義務がある
・JVN＝ジャパン・ヴァルヌラビリティ（脆弱性）ノート：国内の脆弱性情報の収集と分析を行い提供するサイト。IPAとJPCERTが運営
・JPCERT：情報セキュリティに関する情報の収集・分析・公開や啓もうを行う団体。
・【補足】パッチファイル：元はあて布の意味で、ソフトウェアの一部を差し替えることで更新・改良・不具合解消を行うためのファイル。

本日の1問：侵入検知システムは？
ア DMZ イ IDS ウ XSS エ CSRF
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