情報処理工学 第14回

藤田 一寿

公立小松大学保健医療学部臨床工学科

殆どの図はIPAセキュリティ10大脅威より

情報漏えい

故意ではない情報漏洩

- 忘れ物
  - ノートパソコン，USBフラッシュメモリ，書類.
- ファイル交換ソフト
  - ウイルスに感染することで機密ファイルが共有され全世界にばら撒かれる.
- メールの送信先の間違い
- インターネットサービスの設定ミス
  - パスワードを掛けるべきところをかけていなかった.
- 公開してはいけないファイルを公開する.
  - 2015年FRBが誤って内部資料を公開 (https://www.nikkei.com/article/DGXLASGM25H21_V20C15A7NNE000/)
  - 2018年Amazonが誤ってメールアドレスを公開
  - 2018年経産省が入札情報を誤って公開

故意ではない情報漏洩

- パスワードが簡単すぎ不正アクセスされ情報漏洩
- ハードディスクの捨てる際，OSのゴミ箱フォルダに機密ファイルを移し削除する．
  - OS上では消えたように見えても，データはハードディスク上に残ったまま．データ復旧ソフトを用いると，消したデータをもとに戻せることがある．
  - 確実に削除するには，ディスクを破壊するかディスクを何度か乱数などで上書きする必要がある．

  - 事例
    - 2019年HDDの処理を委託されたブロードリンクの社員が，そのHDD持ち出しをオークションサイトで転売した．そのHDDは神奈川県のPCから取り出されたもので，落札者がデータ復旧ソフトを用いると神奈川県の公文書がそのHDDから見つかった．

意図的な情報漏洩

- 従業員が故意に内部情報を外部に漏洩させる
  - 処遇の不満などによるストレスの発散
  - 借金返済のため情報を売る

- 事例
  - 2014年ベネッセの顧客情報が漏洩していることが発覚.
    - システム開発・運用を行っていた子会社のシンフォームに再委託先企業の社員が顧客情報を持ち出し，250万で売却.

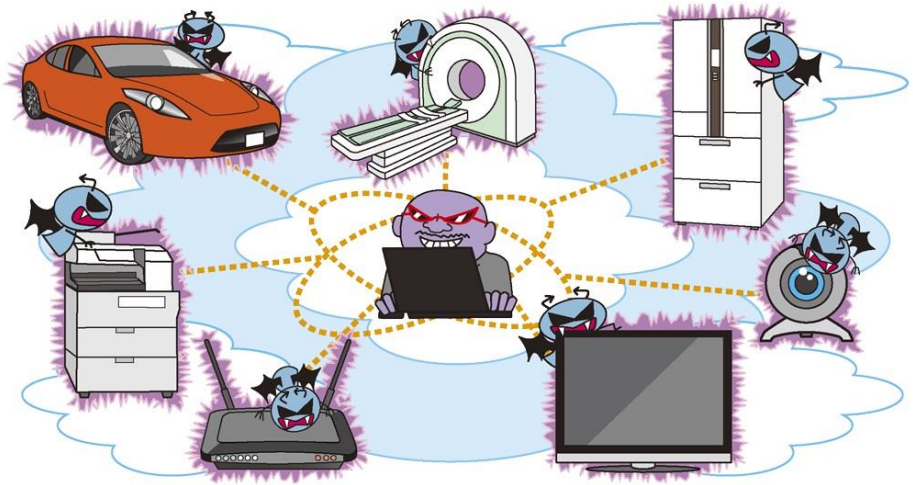
IoT機器のセキュリティー

IoT機器

- **IoT (Internet of Things)とはモノのインターネットとも呼ばれ，あらゆるモノがインターネットにつながる社会やその様子を表す.**
- 現在でも，パソコンやスマートフォンだけではなく，テレビ，スマートスピーカー，車，監視カメラ，電子レンジなどもインターネットに繋がっている場合がある.
- IoT機器とは，インターネットに繋がるあらゆるモノのことで，特にパソコンやスマートフォンのような以前からインターネットにつながっていたIT機器以外を指すことが多い.
- IoT機器は，見た目がパソコンやスマートフォン (IT機器)に見えないため，一般ユーザだけではなくメーカーもセキュリティに対する意識が低くなる.
- **IoT機器はIT機器と同等の機能を有するため（LinuxなどのOSが入っている），IT機器と同等のセキュリティ対策をする必要がある.**

IoTのセキュリティ問題

- IoT機器にマルウェアを感染させ，マルウェアをばらまく．
- IoT機器マルウェアを感染させ，DDoS攻撃を行う．
- IoT機器から機密情報を窃取する．
- IoT機器を遠隔制御する．



なぜ問題が起こるのか

- IoT機器に対するセキュリティに対する意識の低さ
- 例
  - 管理者権限のIDとパスワードがadmin：1234など典型的なものに設定されている.
  - しかも，その設定をユーザが変更できないように作られている機器がある.

監視カメラの事例

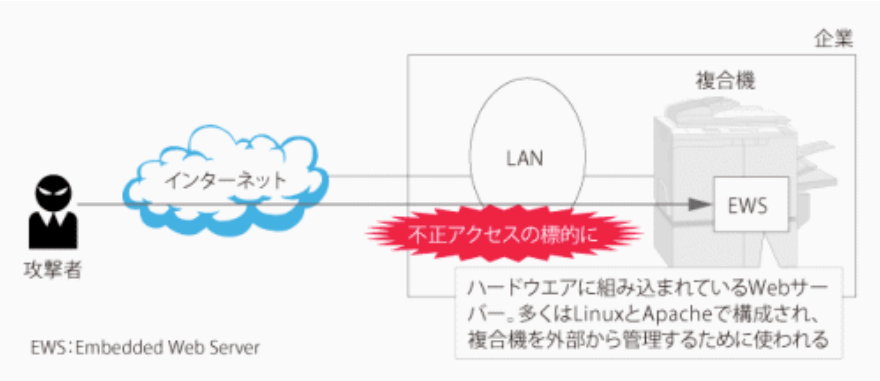
- 監視カメラはインターネットから動画の視聴，カメラの向きの制御などが行えるものがある．

- 監視カメラの画像の流出
  - 監視カメラの中には，画像がインターネットに公開される設定になっているものがある．世界中の監視カメラ画像を見られるサイトも存在する．
- 監視カメラの乗っ取り
  - 2018年上尾市の河川監視カメラに不正アクセスがあり，「I’m hacked. bye2」と監視カメラの画像に表示された．さらに，パスワードが変更され，制御不可能になった (https://www.sankei.com/region/news/180428/rgn1804280045-n1.htm, https://scan.netsecurity.ne.jp/article/2018/05/01/40886.html)

プリンタと複合機の事例

- プリンタや複合機はインターネットから印刷，スキャンされた資料の閲覧，設定の変更などが行えるものがある．

- 2013年複数の大学等で，複合機で読み取った情報がインターネット上で閲覧できる状態となっていたことが判明した．



日経新聞

テスラモデルSの遠隔操作

- テスラ車の通信機能に存在した脆弱な仕様をついて車載情報端末用の車内ネットワークに侵入
- 車載情報端末のWebブラウザーに存在した脆弱性を攻撃して、任意のコードを実行可能に
- 車載情報端末のLinuxカーネルに存在した脆弱性を攻撃して、ルート権限を取得
- 情報端末用の車内ネットワークと、制御系ネットワーク（CAN）とをつなぐ「コントローラー」を攻撃して、コントローラーのファームウエアを書き換え
- コントローラーから電子制御ユニット（ECU）に偽のコマンドを送り自動車を遠隔操作

http://business.nikkeibp.co.jp/atcl/report/15/061700004/072800212/

IoT機器のセキュリティ対策

- IoT機器は一見すると機能が限定され安全に見えるが，中身はパソコンと同じであると考えて，パソコンやネットワーク機器と同様のセキュリティ対策を行う．

- ソフトウェアを最新のものにする．
- 初期設定を使わず，よりセキュリティの高い設定にする．
  - ID，パスワードだけではなく，ネットワークの設定も．

全般的な対策

- すべてのソフトを常に最新の状態にしておく.
- ウイルス対策ソフトの導入する.
  - しかし，全てのウイルスを検知できるわけではない.
- 簡単なパスワードにしない.
- セキュリティの高い設定にする.
- 機密情報を持ち出さない.
- メールに添付されているファイルを安易に開かない.
- ITセキュリティに関わる事案が起こった後のことを考えておく.

その他

ユーザ認証とアクセス管理

- 情報セキュリティ管理のためには，個々の利用者ごとに適切な権限を設定する必要がある.
- 最低限必要な利用者にのみ必要最低限のアクセスを許可することが大切.

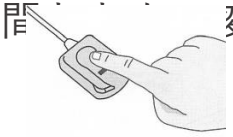
- 利用者が誰なのかを確認することを，ユーザ認証という.

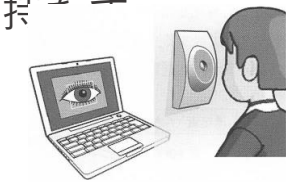
- ユーザ認証をパスしてシステムを利用できる状態にすることをログイン（ログオン），システムの利用を終了してログイン状態を断ち切ることをログアウト（ログオフ）という.

認証方式の種類と特徴

- ユーザIDとパスワードによる認証
  - ユーザIDとパスワードの組み合わせを使って個人を識別する認証方法.
- ２段階認証(2要素認証)
  - IDとパスワードに加え，さらにもう一つの認証方法を増やし安全性を高めた認証方法.

- ICカード認証
  - ICチップの埋め込まれたカードを用いた認証方式.
- 生体認証（バイオメトリクス認証）
  - 指紋，虹彩，静脈などの身体的特徴を用い認証する方法.
  - 用いる身体的特徴には，誰でも持っており（普遍性）本人以外同じ特徴を持たず（唯一性）時間[illegible]変化しない（永続性）ことが必要.



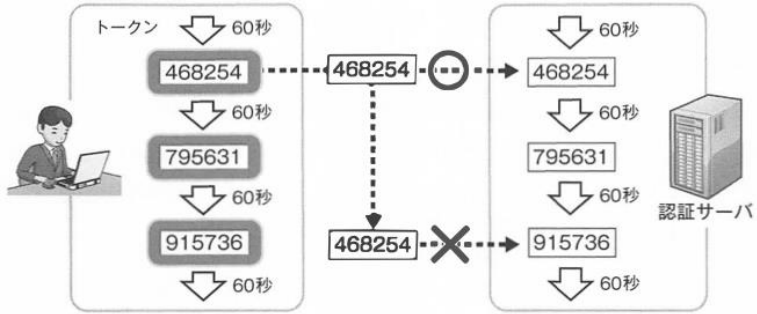


認証方式の種類と特徴

- ワンタイムパスワード
  - 一度限り有効という，使い捨てのパスワードを用いる認証方法.
  - 認証を行うたびに毎回異なるパスワードを使用するため，たとえパスワードが盗まれたとしてもそのパスワードはすぐに使えなくなる．そのため，安全性が高い.
  - パスワードはトークンにより生成される.
  - トークンはハードウェアのものとソフトウェアのものがある.
  - 携帯電話のSMS（ショートメッセージサービス）でパスワードを送る場合もある.
  - 2段階認証にも使われる.

（ソニー銀行）

(スクエアエニックス)



暗号化技術とデジタル署名

- インターネット上では様々な情報が，様々なコンピュータを介して運ばれている．
  - インターネット上の情報伝達は，複数の小さな紙に書かれた情報がバケツリレーで運ばれているようなもの．
- インターネット上で運ばれる情報にはユーザ名とパスワード，クレジットカード情報，銀行口座情報など他の人に見られたくないが含まれる．
- 情報が運ばれる際，情報は盗み見られる可能性がある．
  - バケツリレーで運ばれる紙の情報は，運んでいる人に見られる可能性がある感じ．

インターネット上での情報通信における危険性

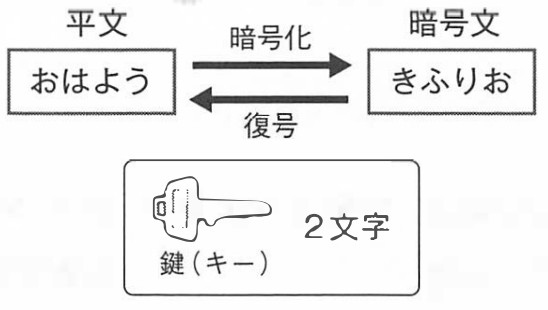
- 盗聴
  - 情報のやり取りは正常に行われるが，情報のやり取りの途中で第三者に情報を見られる．
  - 暗号化で防ぐ．
- 改ざん
  - 情報のやり取りは一見正常に行われているように見えるが，途中で第三者がその情報の内容を書き換える．
  - ディジタル署名で防ぐ．
- なりすまし
  - 第三者が別人になりすまし，情報のやり取りを行う
  - 認証局（CA）を用い防ぐ．

暗号化と復号

- インターネット上での情報のやり取りは必ず盗み見られる可能性がある.

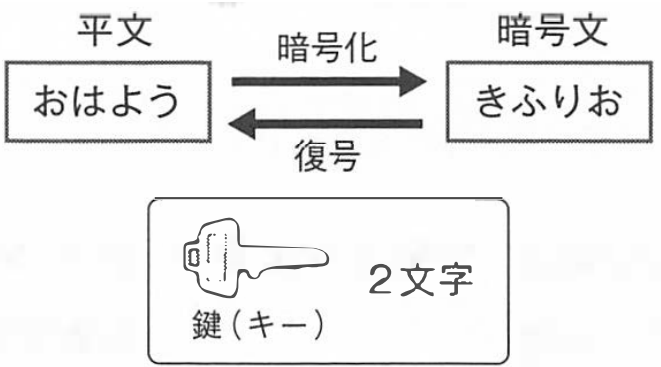
- 情報をやり取りしている当事者同士しかわからないルールで，情報を変換してしまえば，第三者には読み取れない.

  - 情報を第三者にわからないように変換することを暗号化という.
  - 暗号化された情報をもとに戻すことを復号という.



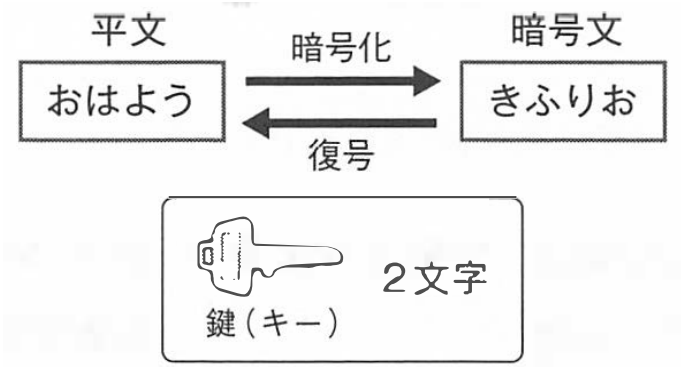
共通鍵暗号方式

- 暗号化前の情報を平文（ひらぶん），暗号化後の情報を暗号文という．
- 情報を暗号化・復号するため用いるデータを鍵という．
- 情報の送り手と受け手が同じ鍵を用いる方式を，共通鍵暗号方式（秘密鍵暗号方式）という．
- 鍵が第三者に知られると暗号化の意味はなくなる．



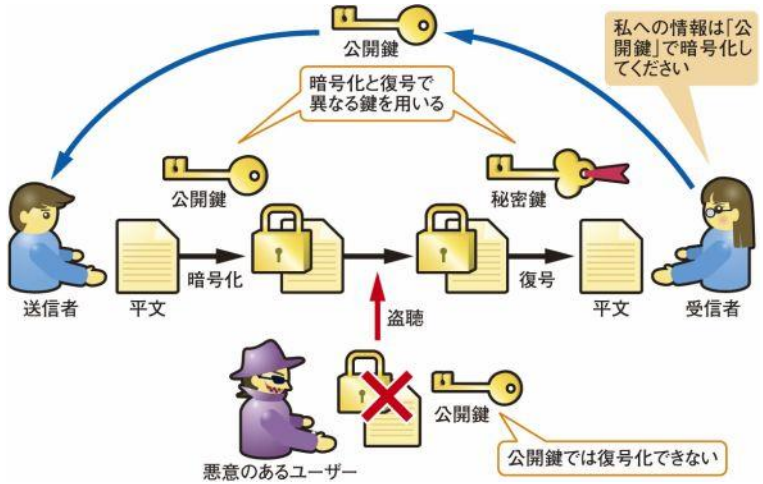
共通鍵暗号方式の問題

- 共通鍵暗号方式は，通信する相手同士で鍵を持つ必要がある．
  - 人図が増えれば増えるほど鍵の数が増える．例えば，４人でお互い通信しようとすると６個鍵が必要．
  - 通信相手に鍵を安全に送る必要がある．
    - 鍵が安全に送れるのなら，暗号化する必要はないのでは？



公開鍵暗号方式

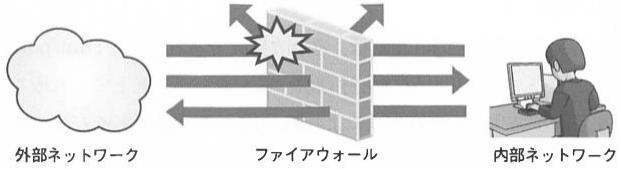
- 情報の受信者は公開鍵と秘密鍵と呼ばれる２つのペアの鍵を作成する.
- 情報の送信者は，公開鍵を使い暗号化する.
- 受信者は秘密鍵を用い復号にする.
- 公開鍵で暗号された情報は秘密鍵でしか復号できない.
  - 公開鍵は不特定多数に知られても問題ない.
- 受信者は鍵のペアを１つ作れば良い.
  - 通信相手ごとに鍵を作る必要がない.



(http://ascii.jp/elem/000/000/431/431308/index-2.html)

ファイヤウォール

- LANの中と外とを区切る壁として働くシステムをファイアウォールという.



- パケットフィルタリング
  - 予め指定されたルールに則ってパケット（情報）を通過させる.
  - 例：IPアドレス，ポート番号など

- アプリケーションゲートウェイ（プロクシサーバ）
  - LAN内のコンピュータはアプリケーションゲートウェイを通じ外へつながる.
  - 外からはアプリケーションゲートウェイしか見えないため，LAN内のコンピュータが不正アクセスの標的になることを防ぐことができる.

コンピュータウイルス関連の用語

- マルウェア
  - 不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアの総称．(wikipedia)
- コンピュータウイルス
  - コンピュータに感染して破壊活動を行ったりトラブルを引き起こしたりするプログラム．(IT用語辞典)
  - マルウェアの一種で，自立せず，動的に活動せずプログラムファイルからプログラムファイルへと静的に感染するもの．感染先のプログラムの一部を書き換え，自分のコピーを追加し，宿主が実行された時に自分自身をコピーするコードを実行させることで増殖する．(wikipedia)
- トロイの木馬
  - 有用なプログラムあるいはデータファイルのように偽装されていながら，その中にマルウェアを隠し持っているファイル．(wikipedia)

演習

演習

- コンピュータセキュリティに対する脅威で，ゼロデイ(zero-day)攻撃の説明はどれか．ME2種43回

1. コンピュータに保存されてあるファイルを暗号化し，復元の見返りとして身代金を要求する．
2. 本物のサイトに偽装したウェブサイトにメールなどで誘導し，アカウント情報やクレジットカード番号等の個人情報を詐取する．
3. 攻撃対象がよく利用するウェブサイトを改ざんし，アクセスした際にウイルスを感染させる．
4. 極めて多量のアクセスを集中させて，相手のシステムを正常に稼働できない状態におちいらせる．
5. ソフトウェアの脆弱性が見つかってから，その対策が行われるまでの間に，脆弱性を利用して攻撃を行う．

演習

- コンピュータセキュリティに対する脅威で，ゼロデイ(zero-day)攻撃の説明はどれか．ME2種 43回

1. コンピュータに保存されてあるファイルを暗号化し，復元の見返りとして身代金を要求する．
   ランサムウェアです．
2. 本物のサイトに偽装したウェブサイトにメールなどで誘導し，アカウント情報やクレジットカード番号等の個人情報を詐取する．
   フィッシング詐欺です．
3. 攻撃対象がよく利用するウェブサイトを改ざんし，アクセスした際にウイルスを感染させる．
4. 極めて多量のアクセスを集中させて，相手のシステムを正常に稼働できない状態におちいらせる．
   DoS攻撃です．
5. **ソフトウェアの脆弱性が見つかってから，その対策が行われるまでの間に，脆弱性を利用して攻撃を行う．**

演習

- 標的型攻撃メールの特徴について誤っているのはどれか．第34回臨床工学技士国家試験

1. 特定の組織（官公庁，企業，医療機関など）の機密情報の窃取を目的とする．
2. 件名，本文，添付ファイル名を業務に関連したものに偽装する．
3. 本文や添付ファイルに記載したリンク先にウイルスを仕込む．
4. 組織が頻繁に利用するウェブサイトを改ざんしウイルスを仕込む．
5. 大量のスパムメールを不特定多数に送信する．

演習

- 標的型攻撃メールの特徴について誤っているのはどれか．第34回臨床工学技士国家試験

1. 特定の組織（官公庁，企業，医療機関など）の機密情報の窃取を目的とする．
2. 件名，本文，添付ファイル名を業務に関連したものに偽装する．
3. 本文や添付ファイルに記載したリンク先にウイルスを仕込む．
4. 組織が頻繁に利用するウェブサイトを改ざんしウイルスを仕込む．
5. **大量のスパムメールを不特定多数に送信する．**

   不特定多数を対象としたフィッシング詐欺です．

演習

- Webサイトに短時間に大量にアクセスし，過負荷を与えることでサービスを停止させるのはどれか．（臨床工学技士国家試験36）

1. DoS攻撃
2. ランサムウェア
3. フィッシング詐欺
4. インジェクション攻撃
5. 標的型攻撃

演習

- Webサイトに短時間に大量にアクセスし，過負荷を与えることでサービスを停止させるのはどれか．（臨床工学技士国家試験36）

1. **DoS攻撃**
2. ランサムウェア
3. フィッシング詐欺
4. インジェクション攻撃
5. 標的型攻撃

演習

- セキュリティの向上に直接関係するのはどれか．第27回臨床工学技士国家試験

a. オープンソース

b. スパイウェア

c. 電子署名

d. 公開鍵

e. プロキシサーバ

演習

- セキュリティの向上に直接関係するのはどれか．第27回臨床工学技士国家試験

a. オープンソース

ソースコードが公開されているソフト

b. スパイウェア

コンピュータの情報を盗み取るマルウェア

c. 電子署名

電磁的記録に付ける電子的な署名．捏造，改ざんの防止に使われる．

d. 公開鍵

公開鍵暗号方式で使われる鍵．

e. プロキシサーバ

外部のウェブサイトを代理で取得するサーバ．直接外部のウェブサイトに接続しないためセキュリティの向上が期待できる．

演習

- コンピュータセキュリティについて誤っているものはどれか．第34回ME2種

1. ワクチンソフトには侵入したウイルスを駆除する機能がある．
2. コンピュータウイルスに感染しても直ちに症状が出るとは限らない．
3. 「トロイの木馬」に感染すると攻撃者にパソコンを遠隔操作される恐れがある．
4. ファイアウォールとはコンピュータ・ネットワークと外部との通信を制限する．
5. スパイウエアとは不正アクセスを監視するものである．

演習

- コンピュータセキュリティについて誤っているものはどれか．第34回ME2種

1. ワクチンソフトには侵入したウイルスを駆除する機能がある．
2. コンピュータウイルスに感染しても直ちに症状が出るとは限らない．
3. 「トロイの木馬」に感染すると攻撃者にパソコンを遠隔操作される恐れがある．
4. ファイアウォールとはコンピュータ・ネットワークと外部との通信を制限する．
5. **スパイウエアとは不正アクセスを監視するものである．**

   スパイウェアはコンピュータの情報を盗み出すマルウェア．

演習

- 差出人を偽装した電子メールを送って不正なウェブサイトに誘導するなどして，インターネットユーザからアカウント情報やクレジット番号などの個人情報を詐取する行為を何と呼ぶか．（第41回ME2種）

1. フィッシング
2. スパイウェア
3. ランサムウェア
4. DOS攻撃
5. 標的型攻撃

演習

- 差出人を偽装した電子メールを送って不正なウェブサイトに誘導するなどして，インターネットユーザからアカウント情報やクレジット番号などの個人情報を詐取する行為を何と呼ぶか．（第41回ME2種）

1. フィッシング
2. スパイウェア
3. ランサムウェア
4. DOS攻撃
5. 標的型攻撃

演習

- バイオメトリクス認証はどれか．第35回臨床工学技士国家試験

a. 指紋で認証する．

b. ワンタイムパスワードで認証する．

c. 画面に表示された9点の一部を一筆書きで結ぶ．

d. 「秘密の質問」に答える．

e. 虹彩パターンで認証する．

演習

- バイオメトリクス認証はどれか．第35回臨床工学技士国家試験

a. 指紋で認証する．

b. ワンタイムパスワードで認証する．

2要素認証によく用いられる．

c. 画面に表示された9点の一部を一筆書きで結ぶ．

スマホなどで使われる．

d. 「秘密の質問」に答える．

2要素認証やパスワードを忘れたときに使われる．

e. 虹彩パターンで認証する．

演習

- 施設内でUSBメモリを使用する際のリスクに該当しないのはどれか．第35回臨床工学技士国家試験

1. 紛失
2. 情報の不正持出し
3. 故障による情報消失
4. 不正ソフトウェアの持ち込み
5. フィッシングによる情報漏えい

演習

- 施設内でUSBメモリを使用する際のリスクに該当しないのはどれか．第35回臨床工学技士国家試験

1. 紛失

   USBメモリはなくすと情報漏えい等の危険性があります．

2. 情報の不正持出し

   不正持出しを意図しないでもUSBメモリは小さいため意図せず持ち出す可能性があります．

3. 故障による情報消失

   何でも故障します．バックアップを取りましょう．

4. 不正ソフトウェアの持ち込み

5. **フィッシングによる情報漏えい**

   USBとは関係ありません．

演習

- 使用しているパソコンで，コンピュータウイルス等の不正なソフトウェアが動作していると考えられる．使用しているパソコンの初動対応として最も適切なのはどれか．第29回臨床工学技士国家試験

1. パスワードを変更する．
2. ネットワークから切断する．
3. USBメモリにファイルをバックアップする．
4. システム・ソフトウェアのアップデートを行う．
5. ウイルス対策ソフトを用いてシステムのスキャンを行う．

演習

- 使用しているパソコンで，コンピュータウイルス等の不正なソフトウェアが動作していると考えられる．使用しているパソコンの初動対応として最も適切なのはどれか．第29回臨床工学技士国家試験

1. パスワードを変更する．
   パスワードを変えてもマルウェアが動き続けるので不適切です．
2. **ネットワークから切断する．**
   被害を広げないので初動として良い行動です．
3. USBメモリにファイルをバックアップする．
   マルウェアに感染しているPCにUSBフラッシュメモリを指すのは危険です．
4. システム・ソフトウェアのアップデートを行う．
   アップデートしてもマルウェアは消えません．
5. ウイルス対策ソフトを用いてシステムのスキャンを行う．
   マルウェアの対策としては良い行動です．しかし，2よりも優先度が下がります．

演習

- 正しいのはどれか。 第33回臨床工学技士国家試験

1. データのバックアップは情報漏洩の防止に役立つ。
2. 共通鍵暗号方式では鍵が漏れてもセキュリティ上問題ない。
3. 情報セキュリティにおける完全性とは、情報が正確で改ざんされていないことをいう。
4. オープンソースソフトウェアは、セキュリティ確保のためには使用すべきではない。
5. 院内ネットワークにファイアウォールが導入されていれば、個人の PC を自由に接続してよい。

演習

- 正しいのはどれか。 第33回臨床工学技士国家試験

1. データのバックアップは情報漏洩の防止に役立つ。
   バックアップはデータ消失を防ぎます.
2. 共通鍵暗号方式では鍵が漏れてもセキュリティ上問題ない。
   公開鍵は漏れても問題ないですが，秘密鍵が漏れると暗号が解かれます.
3. **情報セキュリティにおける完全性とは、情報が正確で改ざんされていないことをいう。**
4. オープンソースソフトウェアは、セキュリティ確保のためには使用すべきで はない。
   オープンソースだからといってセキュリティが低いとは限りません.
5. 院内ネットワークにファイアウォールが導入されていれば、個人の PC を自 由に接続してよい。
   個人PCを接続するときは許可を取りましょう.

演習

- 情報セキュリティ対策に使われるファイアウォールの機能はどれか．（臨床工学技士国家試験36）

1. 外部ネットワークと内部ネットワーク間で特定の通信だけを許可する．
2. 脆弱性が発見された内部システムのソフトウェアを自動更新する．
3. 内部ネットワークへの接続時にパスワードを要求する．
4. 通信パケットに含まれるウイルスを駆除する．
5. 暗号化された通信だけを許可する．

演習

- 情報セキュリティ対策に使われるファイアウォールの機能はどれか．（臨床工学技士国家試験36）

1. **外部ネットワークと内部ネットワーク間で特定の通信だけを許可する．**
2. 脆弱性が発見された内部システムのソフトウェアを自動更新する．
3. 内部ネットワークへの接続時にパスワードを要求する．
4. 通信パケットに含まれるウイルスを駆除する．
5. 暗号化された通信だけを許可する．

演習

- コンピュータセキュリティ対策であるファイアウォールの機能として正しいのはどれか．第32回ME2種

1. PCの起動時にパスワードを要求する．
2. 送受信データを暗号化する．
3. 複数のハードディスクに同じデータを保存する．
4. 内部ネットワークと外部ネットワークの不正通信を遮断する．
5. コンピュータウイルスを検出，除去する．

演習

- コンピュータセキュリティ対策であるファイアウォールの機能として正しいのはどれか．第32回ME2種

1. PCの起動時にパスワードを要求する．
   ユーザー認証
2. 送受信データを暗号化する．
3. 複数のハードディスクに同じデータを保存する．
   バックアップ．データ消失対策に有効．
4. **内部ネットワークと外部ネットワークの不正通信を遮断する．**
5. コンピュータウイルスを検出，除去する．
   アンチウイルスソフト

問題

- ソフトウェアについて正しいのはどれか.

1. 組み込みソフトウェアは電気機器に内蔵される.
2. ミドルウェアはハードウェアを管理・制御する.
3. 応用ソフトウェアはOSとアプリケーションを仲介する.
4. DBMS(Data Base Management System)は入出力機器を制御する.
5. OSはデータベースを管理する.

問題

- ソフトウェアについて正しいのはどれか.

1. **組み込みソフトウェアは電気機器に内蔵される.**
2. ミドルウェアはハードウェアを管理・制御する.
   ミドルウェアはOSと応用ソフトの間を仲介する.
3. 応用ソフトウェアはOSとアプリケーションを仲介する.
   ミドルウェアのこと.
4. DBMS(Data Base Management System)は入出力機器を制御する.
   DBMSはデータベースの管理システムである.
5. OSはデータベースを管理する.
   OSはハードウェアの管理・制御，ソフトウェアのタスク管理などを行う.

問題

- SaaS(Software as a Service)型ME危機管理システムの利用開始に伴い，医療施設内で必須となるのはどれか.

1. クライアント端末の準備
2. システム専用サーバの設置
3. サーバアプリケーションのインストール
4. バックアップ用記憶装置の設置
5. インターネットに接続できる環境の設備

問題

- SaaS(Software as a Service)型ME危機管理システムの利用開始に伴い，医療施設内で必須となるのはどれか.

SaaSはSoftware as a Serviceの略で，クラウドサービスの一種です．選択肢からクラウドサービスの特徴を選べば良いです.

a. **クライアント端末の準備**
   クラウドサービスを使う端末が必要です.

b. システム専用サーバの設置
   クラウドなので施設内に専用のサーバが必要ありません.

c. サーバアプリケーションのインストール
   クラウドなのでネットワーク越しにインストール済みのアプリケーションを使用します.

d. バックアップ用記憶装置の設置
   クラウドなので自動でバックアップされます.

e. **インターネットに接続できる環境の設備**
   クラウドサービスを使うためのインターネット環境が必要です.

問題

- 無線LANについて正しいのはどれか.

a. 通信規格はIEEE802.11シリーズで規定される.
b. 同じ周波数帯域を使用する電波利用機器である.
c. 各チャネルの中心周波数は同じである.
d. 一つのアクセスポイントに接続できる無線通信端末は１台である.
e. 暗号化方式としてWPA(Wi-Fi Protected Access)がある.

問題

- 無線LANについて正しいのはどれか.

a. 通信規格はIEEE802.11シリーズで規定される.

b. 同じ周波数帯域を使用する電波利用機器である.
   規格により周波数帯域が違う気はする.

c. 各チャネルの中心周波数は同じである.
   すべてのチャネルの中心周波数が同じと読み取ると，この分は間違いである.
   各チャネルごとの中心周波数はいつも同じだと解釈すると正しい.

d. 一つのアクセスポイントに接続できる無線通信端末は１台である
   複数台繋げられます.

e. 暗号化方式としてWPA(Wi-Fi Protected Access)がある.

期末試験

- 第15回（1月30日）講義の後半に実施
- 時間は30分
- 範囲は第8回（ハードウェア）から第14回（セキュリティ）の講義で取り扱った内容
- 国家試験，ME2種の過去問を改変したものを出題
- 筆記用具，スマホ or PCのみ持ち込み可能

- 不合格となった学生がいた場合は，再試の連絡を掲示板する．
- 定期試験ができると国家試験もできるようになるので頑張ろう．

講義アンケートをユニバーサルパスポート上で行う．