コンピュータ演習

```
AIリテラシー 08講 データ・AIにまつわるセキュリティ
```

目次

第08講 データ・AIにまつわるセキュリティ

情報セキュリティの基礎

セキュリティとは

> 経営資源を脅威から守り、安全に経営を行うための活動全般

簡単に言えば

> 大事なものを害になるものから守り、安心して暮らしていくためのあれこれ

情報セキュリティと言うと、コンピュータに関連した狭い分野の話題と誤解しがちだが、大事な情報が**紙の書類**から漏れることもたくさんある。

セキュリティでは「リスク」に注目

> 安全(セキュリティ)はつかみどころがないが、危険(リスク)は具体的で把握しやすい

セキュリティを守る=リスクをなくす

経営資源(情報資産)、脅威、脆弱性

リスク(危険)を分類してみる

- 経営資源(情報資産)...もれなく把握する
- 脅威...脅威を洗い出す(ハードディスクの故障など)
- 脆弱性...脅威に対して持っている弱点

脆弱性の例としては「火事に対して消化器がない」「泥棒に対して鍵をかけ忘れた」「マルウェアに対してセキュリティ対策ソフトがない」等

リスクの顕在化

教科書では以下のように書かれています。

> 経営資源(情報資産)、脅威、脆弱性の3つが重なってしまったときにリスクの度合いがとても大きくなることが知られています。これを**リスクの顕在化**と言います。

一方

> **顕在リスク**とは、言葉のとおり「顕在している＝明らかになっている」リスクのことをいいます。

とする説もあります。こちらの解釈で言えば、リスクを明らかにすることが**リスクの顕在化**となります。

- 【危機管理を知ろう】顕在リスクと潜在リスク 2つのリスクを理解しよう

リスクを減らすためには

経営資源(情報資産)、脅威、脆弱性の3つのリスク要因のうち、対応できる可能性が高いものは

- 脆弱性

となります。

セキュリティ対策の手順と受容水準

セキュリティ対策とはほとんどの場合、脆弱性をなくしていく活動です。手順は以下のようになります。

1. 識別：もれなく脅威を見つけ出す
2. 評価：脅威に順番や点数をつけること
3. 対応：

脅威がどのくらいまずいのかを点数化した上で、対応できるものから対応していきます。

災害時、医療現場ではトリアージ(重症度によって治療の優先順位を決めること)が行われていますが、それと同じことです。

受容水準

リスクをゼロにすることはできません。

組織としてリスクを許容できない・許容できるの線があり、これを**受容水準**と言います。

リスクへの対応方法

リスクの対応方法は大きく分けて4つ

- リスク回避
- リスク移転
- リスク低減
- リスク保有

リスクの発生可能性・リスク発生の際の損害の大きさによってどう対応するかが決まります。

- リスク対応（Risk Treatment）

リスク回避・リスク移転

リスク回避

被害が大きく、頻度も高いリスクに対して選択される。リスクの元を絶ってしまう発想だが、高い効果の反面、副作用が大きい。

例：会社が倒産するのが怖いから、会社の経営を辞めてしまおう

リスク移転

被害額が大きいけれども、頻度は低いリスクへの対応。

例：自動車事故のような大損害を出したときに、保険会社がお金を肩代わりしてくれるが、そのために普段から保険料を支払う。

リスク低減・リスク保有

リスク低減

被害額は小さいけれども頻度が大きいリスクへの対応。

例：大事なファイルのバックアップにより、復元可能としておく

リスク保有

被害額も小さく頻度も低いリスクに対しての方法。

例：損害が軽微なので、損害額より対策費の方が大きくなってしまうケース

情報のCIA

機密性、完全性、可用性

情報分野のセキュリティを考えたとき、「情報が脅威から守られて安全な状態」とは

- 機密性(Confidentiality：許可されたものだけにアクセスことができる)
- 完全性(Integrity：不正に書き換えられたり毛さりたりしていないこと)
- 可用性(Availability：いつでも使える状態にあること)

が維持されていることで、頭文字を取って**情報のCIA**と呼びます。

多要素認証

機密性を守る手段としてパスワードがありますが、過信しないようにしましょう。

- 生体認証(指紋・顔認証)に置き換える
- 多要素認証(パスワードとスマホの両方が必要など)

の方法がとられるようになっている

認証に用いる情報の種類

知識情報

パスワード・PINコード・秘密の質問

所持情報

スマホ・USB・ICカード・HSM(電子証明書)

生体情報

指紋・顔・声紋・静脈

- 静脈認証とは？指紋認証との違いについても解説

多要素認証ではない例

- 第一パスワードと第二パスワードを入れさせるような仕組み
- PPAP

暗号化と匿名加工情報

暗号化とは

インターネットのような共有回線では、機密性や完全性を維持するのは大変。どこで誰が受信しているかわからないため。

専用線をひくのも大変。

そのために、**暗号化**の技術が重要となる。誰かが**盗聴**したときにも**解読**できなければ意味のある情報を取り出せない。

WebではHTTPS(HyperText Transform Protocol Secured)が利用され、暗号化が当たり前になっている。

暗号の仕組み

元の情報を**平分**といい、暗号化手順(暗号アルゴリズム)と鍵(暗号を作ったり、元に戻したりするための情報)によって暗号文にする。

暗号化手順・鍵を知っている人は**複合**して元の平分を扱うことができる。

そのため、盗聴しても安心という仕組み。

個人情報の保護と匿名加工情報

AIやデータサイエンスで重要視されるセキュリティ要素として

- 個人情報の保護
- 匿名加工情報

が重要。(04講の4-1でも触れてる)

漏洩のリスクなしにデータを活用することができる。

今までは活用が困難だったデータも使われやすくなり、社会が活性化したり、イノベーション(技術革新)が怒ったりするかもしれない。