# アクセンチュア出前授業

4I24 中川寛之

## 「セキュリティとは〇〇である。」の〇〇に当てはまる語句を自分で考えよ。

私は、「セキュリティとは**被害を最小限に抑えること**である。」と考えます。
理由は、大きく3つあります。

> 1つ目：情報セキュリティの授業

情報セキュリティ基礎の授業において、セキュリティ対策の目的は完全に攻撃を防ぐことではなく、発生した際の被害を最小限に抑えることであることを学んだからです。

> 2つ目：コストとセキュリティのバランス

「セキュリティは**コスト**である」とアクセンチュアの方がおっしゃった通り、サービスや企業を運用するにあたって、セキュリティは必要不可欠な要素です。しかし、セキュリティ対策は企業が投入できるコストとの折衷案であり、無限にリソースを投入できるわけではありません。コストをかければかけるほど堅牢な仕組みを構築できることは理解できますが、予算の制約により妥協せざるを得ない部分が必ず存在します。そのため、各企業が自社の状況に応じて実現可能な対策を講じ、万が一の際の被害を最小限に抑える意識が重要だと考えます。

> 3つ目：完璧なものは存在しない

セキュリティは完璧ではないと私は考えます。授業で箕浦先生がおっしゃった「セキュリティは**人**である」という言葉にも通じますが、人間は楽をしようとする意識により不完全であり、必ずミスを起こします。そのような状況下で、いかに被害を抑えるかという視点が重要です。
また、ゼロデイ攻撃の存在や昨今のAIを悪用した攻撃手法の進化を踏まえると、すべての攻撃を防ぐという意識ではなく、攻撃を受けた場合でも被害を最小限に抑える意識が現実的かつ効果的なアプローチだと感じます。

## セキュリティ人材不足の現状について調査してまとめよ。

日本国内のサイバーセキュリティ人材は約11万人不足しており、世界全体でも約400万人が不足している状況です。

興味深いのは、日本のセキュリティ従事者数が前年比で23.8%増加しているにもかかわらず、人材不足が解消されていない点です。これは、企業のDX推進やクラウド導入、サイバー攻撃の高度化によって、人材が増えるペース以上に業務需要が急増しているためだそうです。

また、日本特有の問題として、米国では1割未満の企業しか人材不足を感じていないのに対し、日本では9割以上の組織が不足を実感しています。特に中小企業では約70%がセキュリティ専門の体制を持たず、基礎的な教育も不十分な状態です。高度な専門資格である「情報処理安全確保支援士（登録セキスペ）」の保有者も約2.4万人（2025年4月時点）にとどまっており、11万人の不足を補うには程遠い状況となっています。

参考資料_経済産業省
参考資料_東洋経済

## nmapを使ったポートスキャンをどのようにセキュリティ対策に役立てることができるか説明せよ。

> 公開する必要のないポートは閉じる

一般的に、Webサーバであれば80番や443番のポートは公開する必要がありますが、そのほかのポートは必要最低限のポートのみ公開するようにし、できるだけアクセスできる範囲を限定することで安全性を高めることができます。Nmapなどのポートスキャナを利用し、どのポートが開いているのかを把握し、公開しなくても良いポートであれば閉じます。

> 不要なサービスは停止する

起動する必要のないサービスは停止させておくことも対策の一つです。ポートスキャンにより、不要なサービスが稼働していることが判明してしまえば、そのサービスの脆弱性を突かれて攻撃を受ける可能性があります。

定期的にどのサービスが稼働しているのかを確認し、意図していないサービスが稼働していれば停止させることも必要です。

> WAFを導入する

WAF（Web Application Firewall）は、HTTPやHTTPSを解釈して、各種の攻撃からWebサーバを守ってくれる装置のことです。ファイアウォールや、IDS/IPSで検知できないような攻撃にもWAFであれば検知できる場面も多いとされています。

引用資料_エンベーダー

# アプリケーションの許可/拒否リストを設定することは，どのようにセキュリティ対策となるか説明せよ。

## 許可リスト

**許可されたもの以外はすべて実行させない**という、強力なセキュリティ対策。

- 仕組み（Default Deny）:
  システム管理者が事前に「安全である」と確認したアプリケーションだけをリストに登録します。リストに載っていないプログラムは、たとえ無害なものであっても一切起動しません。
    - セキュリティ効果:
      未知のウイルス（ゼロデイ攻撃）を防ぐ: 新種のランサムウェアやウイルスが侵入しても、そのプログラムは「許可リスト」に載っていないため、実行（発病）することができません。従来型ウイルス対策ソフトが検知できない脅威に極めて有効です。
    - シャドーITの防止:
      社員が勝手に業務に関係のないソフトや、セキュリティリスクのあるフリーソフトをインストールして使うことを物理的に防ぎます。

## 拒否リスト

**禁止されたもの以外はすべて実行させる**という、従来型のセキュリティ対策です。

- 仕組み（Default Allow）:
  「動作させてはいけない危険なアプリケーション」や「業務に不要なソフト」をリストに登録し、それらの実行をブロックします。

- セキュリティ効果:
  既知の脅威を防ぐ: 過去に特定されたマルウェアや、脆弱性があることが分かっている特定のソフトウェアの起動を阻止します。

- 特定の行動制限:
  業務時間中のゲームアプリや、情報漏洩のリスクがあるファイル共有ソフトなど、具体的な「使わせたくないソフト」をピンポイントで止めるのに役立ちます。

| 特徴 | 許可リスト方式 | 拒否リスト方式 |
|---|---|---|
| **基本動作** | 許可したもの以外<br>すべて拒否 | 禁止したもの以外<br>すべて許可 |
| **未知の脅威** | 防げる<br>(リストにないため起動しない) | 防げない<br>(リストにないため起動してしまう) |
| **運用負荷** | 高い<br>(新しいアプリを使うたびに登録が必要) | 低い<br>(禁止したい時だけ登録すればよい) |
| **セキュリティ強度** | 極めて高い | 普通<br>(すり抜けのリスクあり) |

## 授業を通して学んだこと，感想など

今回のアクセンチュアの出前授業を通して、サイバーセキュリティ人材の重要性と必要性を強く実感しました。

インターネットが誕生してから長い年月が経ち、サイバー攻撃の手法はより高度化・巧妙化してきています。ランサムウェアやゼロデイ攻撃、最近ではAIを悪用した攻撃など、従来の対策では防げない新たな脅威が次々と生まれています。それに対抗するために、ポートスキャンによる脆弱性の把握、WAFの導入、アプリケーションの許可リスト方式など、攻撃の進化に合わせて防御技術も進化し続けていることを理解しました。

特に印象に残ったのは、最後のQ&Aセッションです。アクセンチュアがセキュリティをビジネスとして展開する企業としての姿勢や、クライアント企業に対してどのようにセキュリティの価値を提供しているのかについて深く理解することができました。「セキュリティはコストである」という言葉の通り、現実のビジネスではコストと効果のバランスを取りながら、最適な対策を選択していく必要があることを学びました。

日本国内で約11万人ものセキュリティ人材が不足している現状を知り、今後の社会においてセキュリティ人材がますます重要になっていくことを実感しました。就職活動の選択肢としてセキュリティという分野も選んでみても面白いなと思いました。