

- サイバーポート(港湾物流)のセキュリティは、「Microsoft Azureのセキュリティ」、「アプリケーション上のセキュリティ」、「外部監査の導入」「運用上のセキュリティ対策」により、対策を講じている。
- 今後もこれらのセキュリティ対策を継続するとともに、新たな脅威等に対しても必要な対策を講じていく。

1. Microsoft Azureのセキュリティ

- 港湾関連データ連携基盤は、クラウドセキュリティ推進協議会によるCSゴールドマークの認証を受けている“Microsoft Azure”のPaaS (Platform as a Service)上に構築している。
- 利用者アカウント管理にはAzure Active Directory B2Cを採用しており、安全性の高いID管理・アクセス管理を実施し、機密性を確保している。
- WebアプリケーションやAPIの公開にあたっては、Azure Front Doorを採用しネットワークレベルのDDoS攻撃に対する保護を行っている。
- 高い可用性(システムが停止することなく稼働し続ける能力)を持つデータベースを使用し、データ保存時の暗号化も実施している。

2. アプリケーション上のセキュリティ

- ユーザーの2段階認証を行うことにより、ユーザーのなりすましや情報漏洩を防止している。
- 事業種別に基づいた帳票APIの権限制御を行うことにより、機密性を確保している。
- 情報更新された情報は、実行者を含めて更新内容を全て保持する仕組みとすることで、意図しない改竄を抑止している。

3. 外部監査の導入

- システム構築・改良のテスト工程において、構築事業者の内部監査を実施するとともに、外部事業者によるセキュリティ監査(システムの脆弱性等のテスト)を行っている。

4. 運用上のセキュリティ対策

- Azureのサービスを利用し、24時間365日ランサムウェア等の不正な挙動が検知可能な監視、データベースやアプリケーションの定期的なバックアップを行っている。
- システム運営者の利用端末等にはセキュリティ製品を導入している。
- システム運営者へは、セキュリティマネジメント講習並びにセキュリティルール遵守点検を定期的実施している。