コンテナターミナルにおける情報セキュリティ対策等検討委員会　中間取りまとめ①

名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策について（概要）

国土交通省

1. はじめに

中間取りまとめ①は、名古屋港における情報セキュリティ事案を受けて設置された「コンテナターミナルにおける情報セキュリティ対策等検討委員会」における議論等を踏まえ、コンテナターミナルにおける情報セキュリティ対策として特に留意すべき点を整理し、緊急に実施すべき対応策を取りまとめたもの

2. 名古屋港事案の検証

【感染経路】
保守用VPNを通じて物理サーバにランサムウェアが侵入し、サーバ情報が暗号化されたものと考えられる一方で、VPN経由以外での侵害の可能性についても精査すべき

【主な問題点】
○ 保守作業に利用する外部接続部分のセキュリティ対策が見落とされていたこと
○ サーバ機器及びネットワーク機器の脆弱性対策が不十分であったこと
○ バックアップの取得対象と保存期間が不十分であったこと
○ システム障害発生時の対応手順が未整備であったこと　等

【主な評価点】
○ 事案発生から丸2日半という短期間で復旧が図られたこと
○ システムを使用せずにマニュアル作業で船舶との間の荷役が継続されたこと　等

3. ターミナルオペレーションシステムに必要な情報セキュリティ対策

○ システムの機器構成、ネットワーク構成、外部との接続状況等の把握
○ サーバやネットワーク機器の外部接続に関する設定の見直し
○ セキュリティ対策ソフトの導入、ソフトウェアの定期的な更新
○ システムログを含むバックアップの取得と適切な取得頻度・保存期間・保存場所の設定
○ 外部委託を行う場合の情報セキュリティの確保　等

4. コンテナターミナルの運用に必要な情報セキュリティ体制

○ 最高情報セキュリティ責任者及び情報セキュリティ担当者の指定
○ セキュリティインシデント対応手順の策定及びセキュリティインシデント対応訓練の実施
○ 情報連絡体制の構築、システム障害を想定した事業継続計画の策定
○ 情報セキュリティに関する情報の収集
○ 関係者の情報セキュリティ意識の向上及び情報セキュリティ教育・訓練等の実施
○ 脆弱性や設定不備の検査及び情報セキュリテイ対策の監査の定期的な実施　等

5. 今後の対応

○ 中間取りまとめ①の周知や説明会の開催により港湾関係者の理解の増進に努める
○ コンテナターミナルの重要性やシステム依存度を踏まえた情報セキュリティ対策のレベルについて整理
○ サイバーセキュリティ政策や経済安全保障政策における港湾の位置付けについて検討
○ 諸外国の事例調査、ガイドラインの策定などを通じた、港湾関係者へ有益な情報の提供に努める