港湾システムにおける
現実的な情報セキュリティの在り方

―2022年度IAPH日本セミナー―

クロサカタツヤ（株式会社 企）

2022年7月19日

自己紹介：クロサカタツヤ

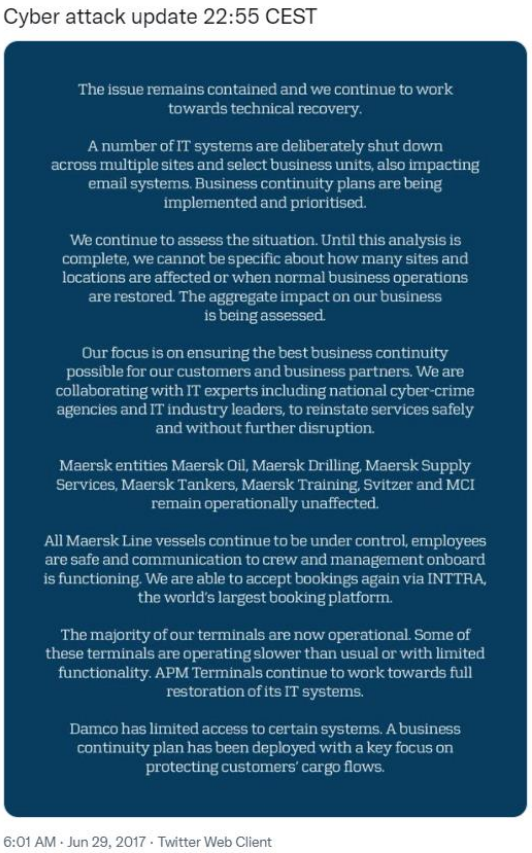
株式会社 企（くわだて）　代表取締役
慶應義塾大学大学院政策・メディア研究科　特任准教授

【略歴】
1999年慶應義塾大学大学院政策・メディア研究科修了。三菱総合研究所を経て、2008年に株式会社企（くわだて）を設立。通信・放送セクターの経営戦略や事業開発などのコンサルティングを行うほか、総務省、経済産業省、OECD（経済協力開発機構）などの政府委員を務め、政策立案を支援。2016年からは慶應義塾大学大学院特任准教授を兼務。近著『5Gでビジネスはどう変わるのか』（日経BP刊）。

【主な役職等】

- 総務省 デジタル時代における放送制度の在り方に関する検討会 小規模中継局等のブロードバンド等による代替に関する作業チーム 構成員（2022年～）
- 公正取引委員会 デジタルスペシャルアドバイザー（2021年～）
- 内閣官房デジタル市場競争本部　Trusted Web推進協議会委員／同TF座長（2020年～）
- 国土交通省 海事産業将来像検討会 委員（2019年～2021年）
- 総務省 ICTサービス安心・安全研究会 消費者保護ルールの検証に関するWG委員（2018年～）
- IoT推進コンソーシアム データ流通促進WG 委員（2018年～）
- インフォメーションバンクコンソーシアム 監事（2018年～）
- OECD WPDGP（データガバナンス及びプライバシー作業部会）日本政府代表団員（2009年～）
  ※WPISP, WPIE, WPSPDEから改組
- 総務省 消費者保護ルール実施状況のモニタリング定期会合（2016年～）
- IPA専門委員（人工知能）、等

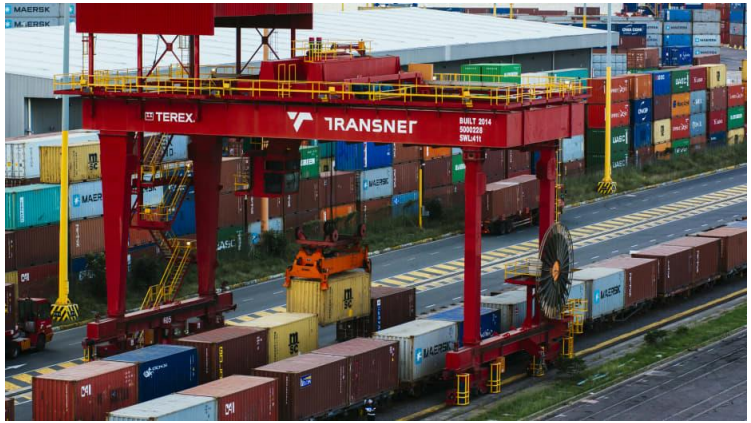
拡大・多様化する海運分野へのサイバー攻撃



- 2017年6月に発生したMaerskの大規模インシデント
  - 発端は、ウクライナ・オデッサのMaerskオフィスにあったPCの会計ソフトM.E.Doc、その外部サーバにマルウェアが仕組まれていた
  - ウィルス発動後、即座にデンマークの本社システムに感染が広がり、そのわずか7分後には世界130カ国のオフィスで不具合発生
  - データ汚染はもちろん、5万台近いPC、サーバ、プリンタ等の周辺機器が破壊、またスマートフォン等にも障害が及んで通信が断絶
  - 業務が全面的に停止し、結果として3億米ドル相当の実害が発生
  - ナイジェリアの同社オフィスで停電が発生したことで、感染から「偶然」免れたデータを物理的にコピーし、デンマークへ輸送することで、10日間程度で業務プロセスと情報システムを復旧
  - これがなかったら、Maerskの業務は6か月停止し、我が国を含む世界の海運にとって悪夢となった可能性もあった

出所　インシデント発生直後のMaersk社ツイート

海運・港湾を狙った「標的型攻撃」も増加



- 海運業界を狙った標的型攻撃（主にランサムウェア）の例
  - 2020年4月：スイス・イタリアMSCがネットワーク停止
  - 2020年5月：豪Tollが巨大な取引データ窃取
  - 2020年9月：フランスCMA-CGMが顧客データ流出
  - 2020年9-10月：国際海事機関（IMO）が業務を一時停止

- 港湾を狙った標的型攻撃の例
  - 2021年7月、南アフリカ国営物流会社TRANSNET社の同国主要港湾ターミナルが7月22日に大規模なサイバー攻撃を受け、同社の通常操業機能が中断し不可抗力宣言が発表
  - コンテナターミナルの出荷システムは手動に切り替えられ、ケープタウン港、ポートエリザベス港、グクラ港、ダーバン港等、南アの主要な港湾の操業が大幅に中断

出所　South Africa port operations halted and workers reportedly put on leave after major cyberattack (CNBC)
https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in-south-africa-after-major-cyberattack.html

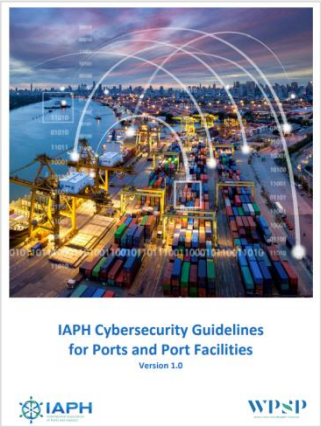
海運が標的になる理由と港湾固有のリスク

- 海運業界が狙われる理由
  - ボトルネックが発生・特定されやすい
  - 当事者が限定的
  - 情報化が発展途上
  - ITとOTの混在による被害拡大リスク

- 港湾のリスク・脆弱性
  - 港湾はボトルネックになりやすい
  - 港湾はステークホルダが多様で複雑
  - 港湾事業者だけでのセキュリティ対策に限界
  - 港湾設備の特殊性
  - 港湾業務の繁忙による対策の劣後

出所　東京都港湾局ツイッター　https://twitter.com/tocho_kouwan/status/773436899876806656/photo/2

ガイドラインが整備されはじめている



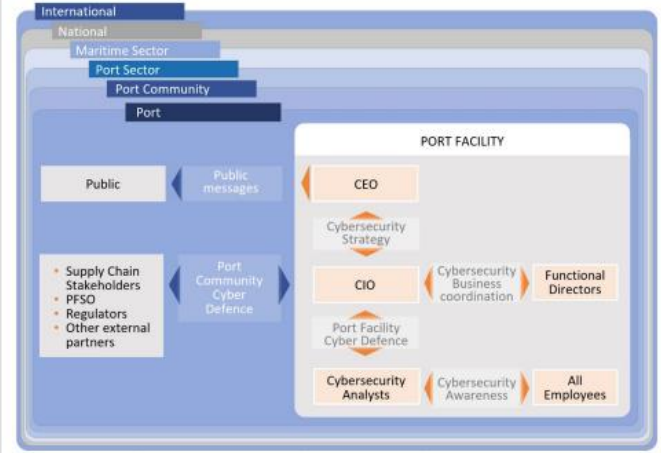
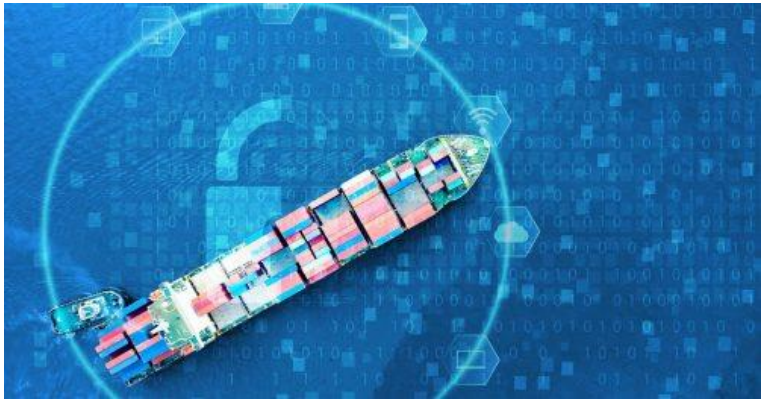


Figure 14 - Cyber information sharing model for ports and port facilities

- IMO：「サイバーリスクマネジメントを安全管理システムに統合するためのガイドライン」(Res. MSC. 428(98))
- **IAPH：港湾及び港湾施設のためのサイバーセキュリティガイドライン**
  - リスク管理業務
  - サイバーセキュリティとリスク管理
  - 海事分野のサイバー脅威と結果
  - 組織のサイバー回向システム
  - リスクと脆弱性の評価
  - 保護、検知、緩和の指標
  - 状況共有、連絡、調整
  - トレーニング
  - インシデント対応と復旧
  - 継続的な改善とサイバーセキュリティの成熟

出所　東京都港湾局ツイッター　https://twitter.com/tocho_kouwan/status/773436899876806656/photo/2

現実的な港湾セキュリティの考え方



- 基本的なスタンス
  - 完璧を求めない
  - できるだけ早く直す
  - 守る対象（モノ・コト・資産）を特定する
- ハード（設備）
  - 汎用化、多重化、冗長化
    - ✓ 特殊な専用設備ほど復旧が遅くなる
- ソフト（運用）
  - 責任追及ではなく原因究明
    - ✓ 現場を委縮させないことが「早く直す」の要諦
- プロの支援を受ける
  - もはや[
  - 敵方」はプロの犯罪者
    - ✓ さらに言えば「正規の軍隊」（cf. ウクライナ戦争）

出所 Cyber security threats to the maritime industry, Marine Industry News, https://marineindustrynews.co.uk/cyber-security-threats-to-the-maritime-industry/

「壁」をどう乗り越えるか

- 内発的な取組の難しさ
  - 危機が起きてから、という「後手」の対応になりやすい
  - 課題が顕在化しないと「予算化」しづらい
  - でも、起きてからでは遅い
- 「日常的な感覚」を活かす
  - 実は日本人は「個人として」すでにDXを実現している
  - 日常感覚を業務にどう取り込むかがカギ
  - 特別なことをしようとせず、日常感覚・日常業務の一歩だけ先にセキュリティがある、という理解の醸成が必要
- たとえば…
  - プライベートでの、ちょっとしたサイバー空間上のトラブルや炎上体験を共有する「雑談」から始める