# 2023年度 国際港湾協会日本セミナー

# 港湾デジタル化について

## 2023　IAPH世界港湾会議より

2024年1月26日（金）

名古屋港管理組合
建設部事業推進課　課長補佐
水野 信一

写真はカリファ港（アブダビ）

# 目次

１．2023年世界港湾会議　港湾デジタル化のセッション紹介

２．米国ロサンゼルス港のサイバーセキュリティ対策

３．日本の港湾のサイバーセキュリティ対策

４．考察

# 1．港湾デジタル化のセッション　概要

- 港湾デジタル化に関しては、2024年よりMaritime Single Window（日本ではいわゆる港湾EDI）の導入が義務化されることに伴う港湾の入出港手続きの取組に留まらずターミナル・オペレーションさらにはサプライチェーンに関わるあらゆる分野のデジタル化の促進について議論された。
- 特に、デジタル化が進めば進むほど重要性が高まるサイバーセキュリティに関して多くの参加者の興味を集めた。

| DX関連講演タイトル | 主な内容 | 主な登壇者 |
|---|---|---|
| ①寄港最適化プロジェクト<br>Port call optimization | 入出港手続きの効率化事例 | シンガポール海事港湾庁（MPA）　副センター長<br>ハンブルグ港港湾局　グローバル戦略官<br>寄港最適化国際委員長 |
| ②港湾と港湾都市におけるデジタルツイン<br>Digital Twin Projects in Ports and Port Cities | デジタルツインの作成方法、計画立案 | アントワープ港　デジタル部門チーフ<br>アブダビ港　情報部門　CTO |
| ③DXを可能にする経営の変革<br>Change Management to Enable Digital Transformation | デジタル化に伴う関係者間の合意形成 | ジブチ港湾コミュニティシステム常務<br>ハンブルグ港湾局　港湾プロセスソリューション部門長 |
| ④海上貨物サプライチェーンにおけるデータ協調<br>Panel: Data Collaboration in Maritime Cargo Supply Chains | 港湾が港湾関係者間の効率的なデータ交換を行うために必要な仕組みづくりについて | ハンブルグ港港湾局長<br>LA港　最高情報責任者（CIO）<br>アブダビ港　情報部門　CEO |
| ⑤港湾に対するサイバー攻撃の脅威<br>Cyber Threats to Ports - Review of Recent Cases | 港湾へのサイバー攻撃への対処事例 | LA港　最高情報セキュリティ責任者<br>ソハール港　IT責任者 |

# 1．セッション紹介①

○議題　寄港最適化-最初のパイロットプロジェクトの結果

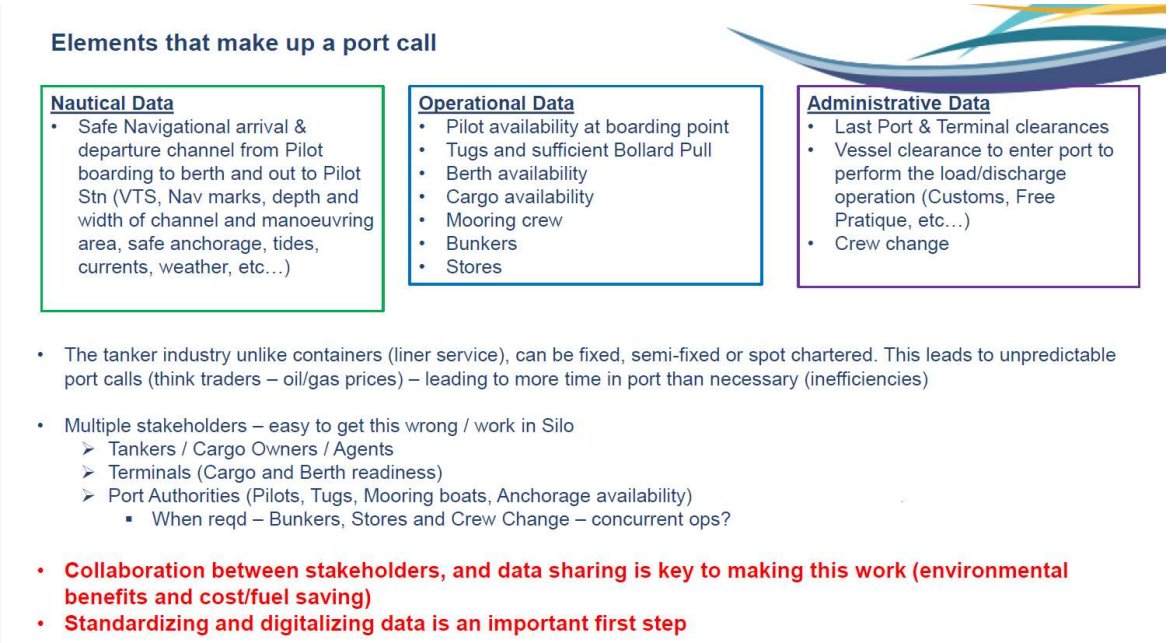
Port Call Optimisation - Results from the First Pilot Projects

○登壇者　ハンブルグ港湾局　グローバル・ストラテジックネットワーク部長　イングリッド・ボケ・サルトレ氏

シンガポール港　海事港湾局（MPA）　副センター長　ギャビン・ヨウ氏

国際寄港最適化タスクフォース　議長　ベン・ファン・シェルペンゼール氏

国際石油会社海洋フォーラム　航海アドバイザー　ケビン・コエーリョ氏




○主な内容

・船舶の寄港に必要な海事情報を船側と港側でやり取りする際の効率化は、寄港プロセスの最適化に不可欠

・特にタンカーなどの不定期船においては、目的地や寄港地の頻繁な変更があり、より一層重要なもの。

・港と船社間の海事情報共有プラットフォームの整備が必要とされており、ロッテルダム港、シンガポール港を中心として、国際タスクフォースにて、そのシステム構築の検討が進められている。

# 1．セッション紹介②

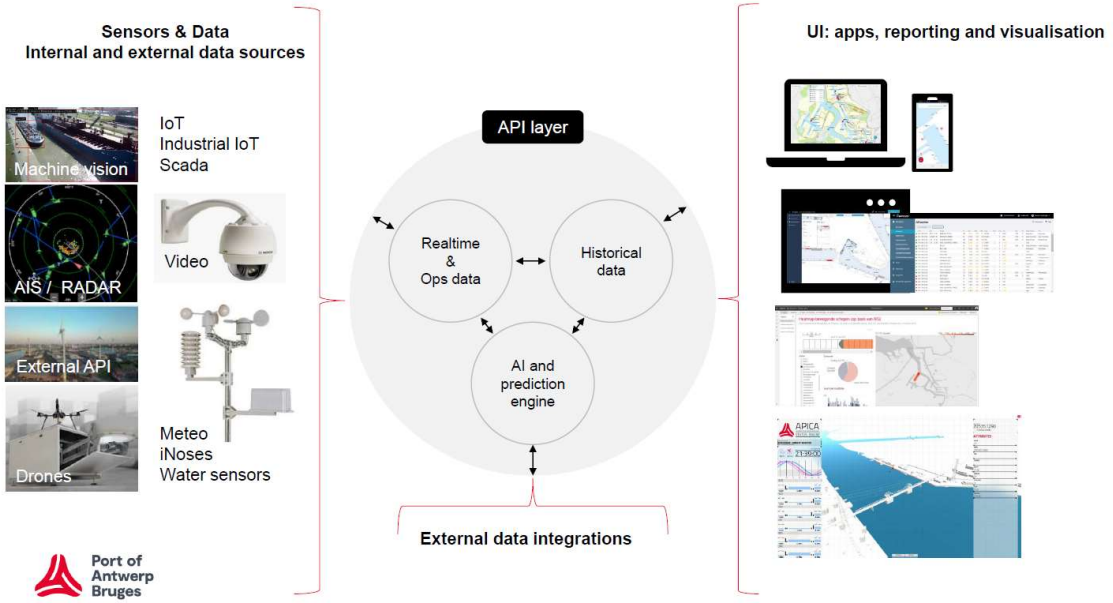
〇議題　港湾と港湾都市におけるデジタルツイン

Digital Twin Projects in Ports and Port Cities

〇登壇者　アントワープ港　デジタル＆イノベーション部長　エルヴィン・フェルストラーレン氏

アブダビADポートグループ　デジタルクラスタ最高技術責任者　ユセフ・アル・リヤミ氏

S＆Pグローバル　Journal of Commerce 技術担当　エリック・ジョンソン氏（コーディネーター）




アントワープ港のデジタルツイン計画の概念

〇主な内容

・デジタルツインを活用した港湾と港湾都市の開発とレジリエンス強化について、アントワープ港、アブダビの港湾開発のデジタル化などが紹介された。

・アントワープ港では、スマートポート計画としてデジタルツインを推進しており、港内に設置した多数のセンサー、カメラ、ドローンを活用して港内の情報収集を行い、港の安全確保と円滑な交通の実現に寄与している。

・デジタルによる状況把握により、港湾や都市開発におけるさまざまな経営判断が助けられ、港湾施設管理やセキュリティ確保にとって有益なものとなり得る

# １．セッション紹介③

〇議題　DXを可能にする経営の変革

Change Management to Enable Digital Transformation

〇登壇者　ハンブルグ港湾局　ポートプロセスソリューション部長　ファンティアン・ズエソンダム氏

ジブチ港湾コミュニティシステム（DPCS）常務　ワルサマ・ギレ氏

国際港湾共同体協会（IPCSA）総長　ニコ・デ・カウワー氏

マリタイムストリート代表取締役社長／IAPHデータ協調委員長　パスカル・オリヴィエ氏

港湾関係者とのデータ協調に必要な５つの概念

〇主な内容

・今後世界中で進むポートコミュニティシステムやシングルウインドウ化の導入にあたって、港湾関係者と互いにデータ共有するにあたっての考え方などについて議論を行った。

・ジブチ港や、ハンブルグ港では、ポートコミュニティシステム導入に非常に困難を極めたが、関係者にデータ共有の重要性の理解を得て導入された事例の紹介がされた。

・技術的な情報技術の確立とともに、マネジメントの変革が重要であり、各港それぞれの状況にあわせ、変化し続けていく必要がある。

# 1．セッション紹介④

○議題　海上貨物サプライチェーンにおけるデータ協調

Panel: Data Collaboration in Maritime Cargo Supply Chains

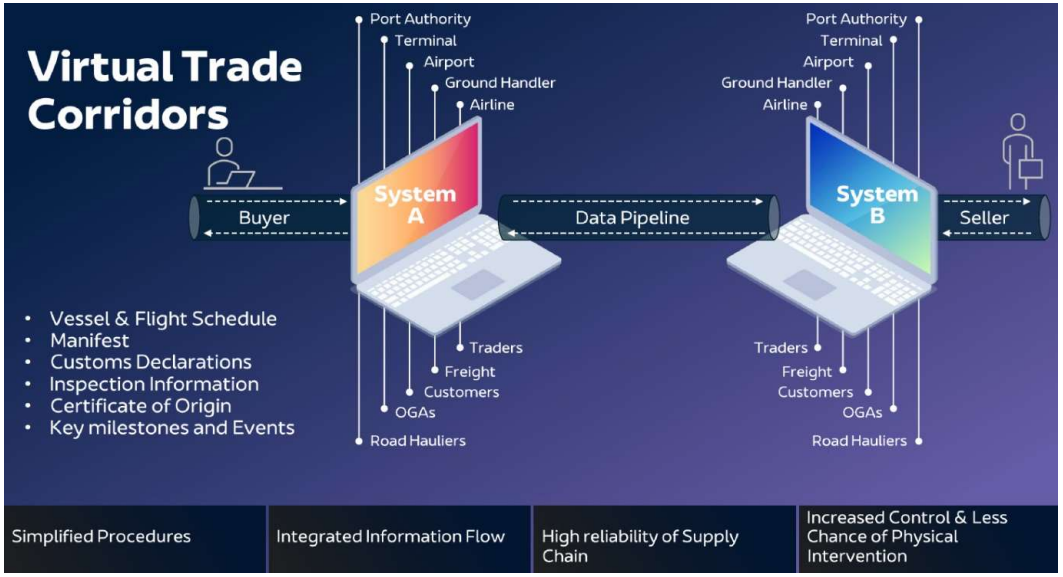
○登壇者　ハンブルグ港湾局長　イエンス・マイヤー氏

ロサンゼルス港　最高情報責任者　シーバ・バルゲーゼ氏

世界銀行　世界貿易・地域統合ユニット長　セバスチャン・デサス氏

アブダビADポートグループ　デジタルクラスタグループ　ノウラ・アル・ダヘリ氏

S＆Pグローバル　Journal of Commerce 技術担当　エリック・ジョンソン氏（コーディネーター）




アブダビのコミュニティシステムの概念

○主な内容

・LA港やハンブルグ港、アブダビで導入されたポートコミュニティシステムの概要や、導入に向けての過程などを紹介

・コミュニティシステムの整備は、利用者への適切な情報提供が可能になるほか、円滑なCOVIT19などの混乱状況下でも弾力性を持てた。

・導入されたシステムに対する攻撃も増え、安全でセキュアなシステムが求められており、LA港では最善の攻撃はレジリエンスとしてとらえ、継続的で大規模な投資が行われている。

# １．セッション紹介⑤

〇議題　港湾に対するサイバー攻撃の脅威について
　　Cyber Threats to Ports - Review of Recent Cases

〇登壇者　ソハール港（オマーン）IT責任者　バーデル・アル・ガイディ氏
　　ロサンゼルス港港湾局　情報技術部門　最高情報セキュリティ責任者　トニー・チョン氏
　　S＆Pグローバル　Journal of Commerce 技術担当　エリック・ジョンソン氏（コーディネーター）

〇主な内容

・最近のサイバー攻撃の事例や対処について、LA港のセキュリティ対策事例を中心に紹介

・LA港では、近年サイバー攻撃が飛躍的に増えており、港湾を自主防衛するための対策を港湾局を中心に実施している。

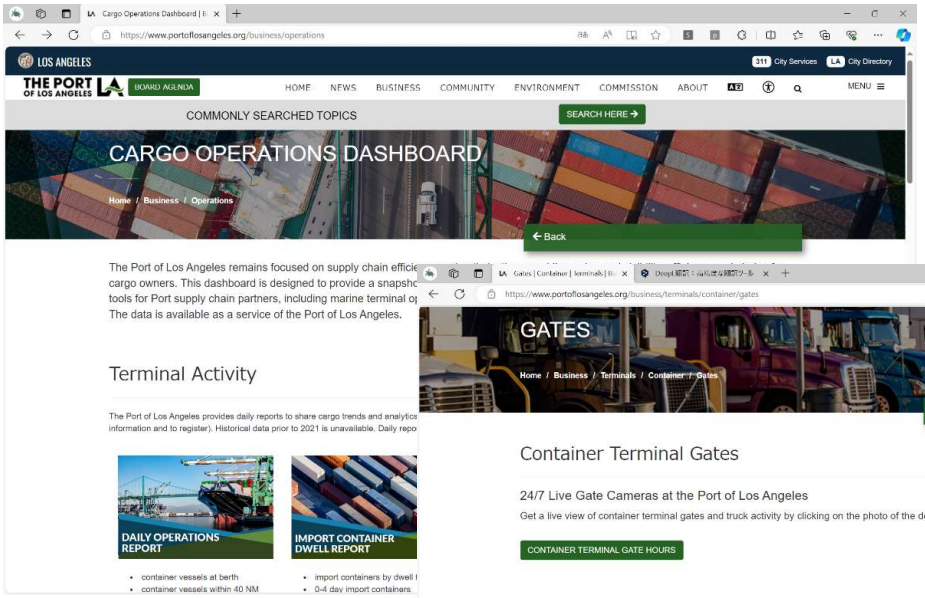
・その仕組みとして、港湾局自体のセキュリティ強化（CSOC）とともに、LA港湾利用者相互の安全確保のための仕組み（CRC）を導入

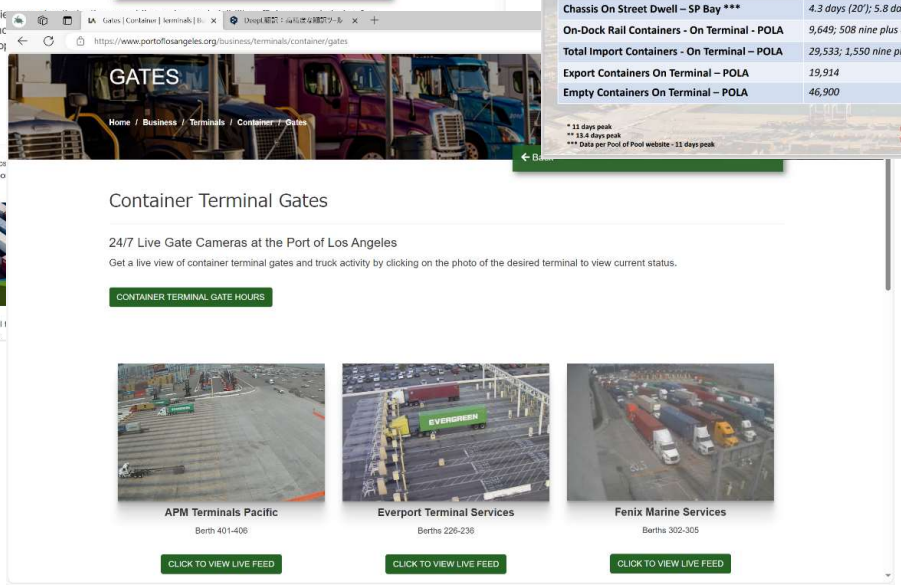
・公益確保のため両システムともLA港湾局で整備・運用され、維持管理費でそれぞれ年間150万ドルの維持費がかかるが、多発する攻撃に対する費用として不可欠なもの

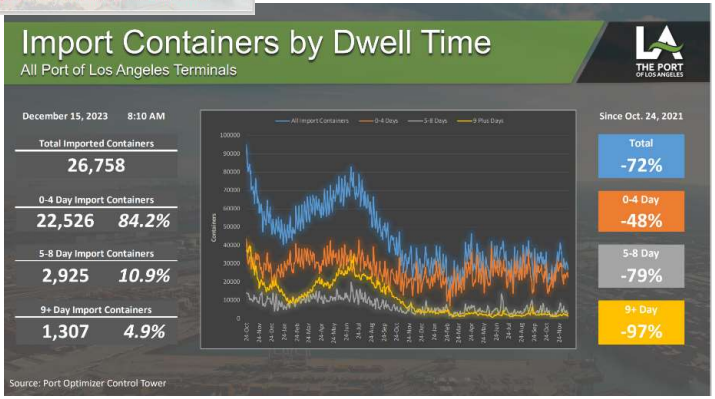
・港湾は物流情報の拠点であり、サイバーテロに狙われやすい。港湾局が公益性を持ち、ポートコミュニティシステムや港湾関係者を守ることが必要。

# 2．LA港のポートコミュニティシステム

- LA港港湾局では、ポートコミュニティの構築に注力しており、その一環としてポートオプティマイザーを導入し、各ターミナルの個別のシステム上にある情報を港湾全体で統合するプラットホームとなっている。
- 船舶の「運行状況」、「コンテナ搬出入許可状況」、「コンテナの滞留状況」、「ゲートの混雑状況」等の情報を各ターミナルのシステムから自動で収集し、HPからリアルタイムに可視化するものとなっている。






（出典）POLA　HP

# ２．サイバーセキュリティオペレーションセンター（CSOC）

- LA港港湾局の内部システム保護のため、2014年にサイバーセキュリティオペレーションセンター（CSOC）を開設。CSOCは、サイバーインシデントを防止および検出するための一元化されたハブとして機能。2019年には、このシステムをアップデートし、G2 CSOCとしている。
- 開設当時は月間500万件の攻撃だったが、現在では、月間6,000万件（１秒で2,000件）の攻撃があり、より頻繁で巧妙で損害を与える攻撃から港を保護している。リアルタイムモニタでどんな攻撃を受けているかなど把握できる。
- セキュリティセンターの整備には7-800万ドルを要し、年間維持費は150万ドルである。バックアップシステムは災害に備え、遠隔地（以前はコロラドだったが、現在は州内）に設置。

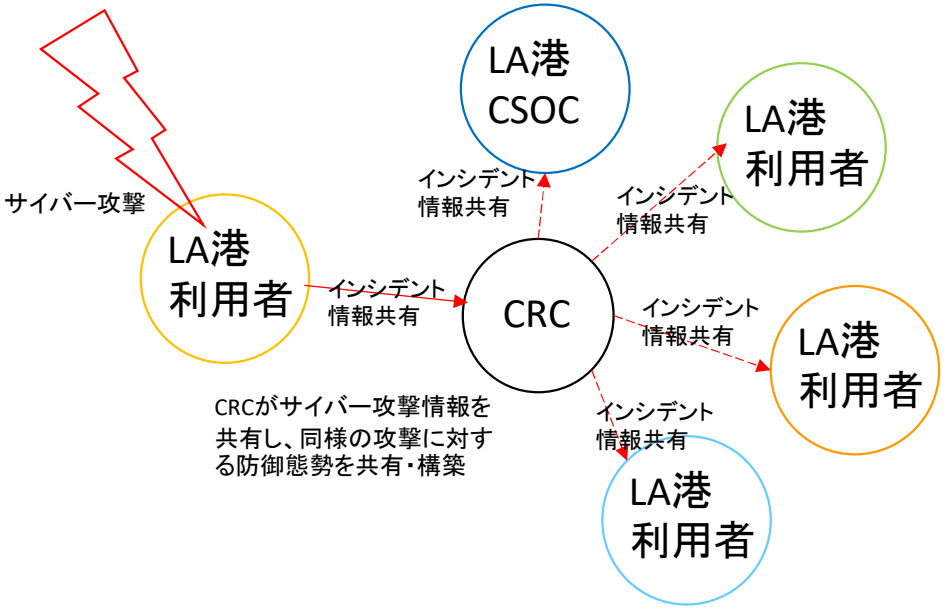
LA港のCSOC（サイバーセキュリティオペレーションセンター）

# 2．サイバーレジリエンスセンター（CRC）

- 2021年には自動化された港湾コミュニティサイバー防御ソリューションであるサイバーレジリエンスセンター(CRC)を設立。CRCは、ロサンゼルス港のサプライチェーン関係者が共同で設計し、IBMが運用。
- LA港の港湾物流関係者を保護する目的で設置され、LA港利用者であれば情報を得ることができる仕組み。
- サイバー攻撃の可能性に対する早期警戒検知器として機能しており、テナントや貨物取扱業者などの参加者が脅威を迅速に共有することで、必要に応じてより適切に防御的対応をとれるようにしている。さらに、攻撃後の業務復旧に対しても、関係者が信頼できる情報資源としての役割も果たしている。

LA港のサイバーレジリエンスセンター

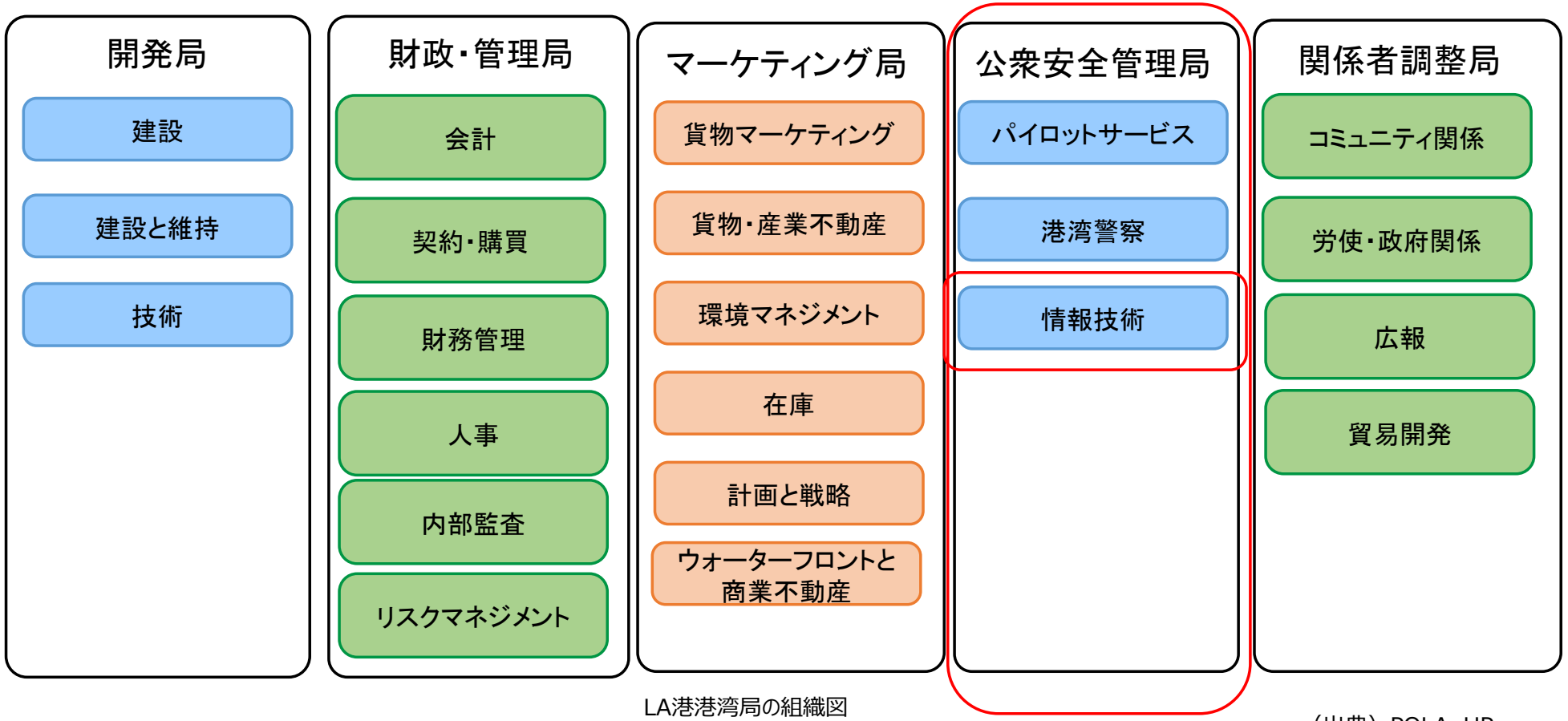
（出典）2023世界港湾会議資料




CRCの概念図

# 2．サイバーセキュリティの実施組織

- CSOC、CRCそれぞれの業務は、LA港港湾局内の公衆安全管理局の情報技術部門が実施。同局内に港湾警察（Port police）も所管




LA港港湾局の組織図

（出典）POLA HP

# 2．米国政府による港湾の保安確保への助成制度

- 米国運輸省海上保安部は、米国の海上輸送システム、米国商船、および米国の海事産業に対し、海賊、テロ、犯罪行為、サイバー攻撃などの海上安全保障上の脅威から米国市民及び海洋権益を保護するための効果的な海上安全保障政策、手順、慣行、法令及び訓練の策定及び実施を促進
- 港湾部門の施策のひとつとして、米国連邦緊急事態管理庁(FEMA)管轄下の国土安全保障省（DHS）とともに、港湾保安助成金制度(Port Security Grant Program)を実施。

- 港湾保安助成制度は、重要な港湾インフラをテロ行為から守るための資金として、州、地方、および民間部門に年100億ドル（約１兆5000億円）が提供。
- 海上サイバーセキュリティの強化、港湾全体の海上安全保障リスク管理、海域認識の強化、海上安全保障の訓練と演習の支援、港湾の回復と強靭化能力を支援する海上安全保障緩和プロトコルの維持または再確立などが対象で、総費用の75%を助成。
- 2023年はLA港湾局へは２０９万ドル（約３億円）が助成

- 参考　日本の予算（令和５年度）

  国土交通省　港湾局　約2600億円

  警察庁　約3200億円

（出典）令和６年度港湾局関係予算決定概要　R5.12　国土交通省港湾局
令和６年度予算のポイント　経済産業、環境、司法・警察係予算　R5.12財務省

## Port Security Grant Program

Funding Totals　NOFOs & Documents

This grant provides funding to state, local and private-sector partners to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities.

**Preparedness Grants Manual**
Recipients seeking guidance on policies and procedures for managing preparedness grants should reference this manual for program-specific information as well as overall guidance on rules and regulations.

FY 2023

Total funding available for fiscal year 2023: **$100 million**

Show 10 entries　Search:

| State | Port Area | Entity Name | FY 2023 PSGP Allocation |
|---|---|---|---|
| NY | New York | New York City Fire Department | $3,981,425 |
| NY | New York | New York City Police Department | $3,462,192 |
| CA | Los Angeles-Long Beach | City of Long Beach Harbor Department | $2,722,875 |
| NY | New York | Nassau Co. Police Department | $2,383,070 |
| TX | Corpus Christi | Port of Corpus Christi Authority | $2,312,500 |
| LA | New Orleans | Plaquemines Port, Harbor and Terminal District | $2,304,825 |
| TX | Sabine-Neches River | Port of Port Arthur Navigation District | $2,183,164 |
| NJ | New York | New Jersey Dept. of Law & Public Safety | $2,139,749 |
| CA | Los Angeles-Long Beach | City of Los Angeles Harbor Department | $2,093,901 |
| TX | Houston-Galveston | City of Houston | $1,827,339 |

Showing 1 to 10 of 229 entries

Previous　1　2　3　4　5　…　23　Next

（出典）FEMA HP
https://www.fema.gov/grants/preparedness/port-security

# ２．米国政府による港湾の保安確保への助成制度

- 2023年の港湾保安助成金のうち、LA港湾局へは、約209万ドルが助成されており、LA港湾危機管理局管轄のCRCやCSOCの設備の改修費やシステムメンテナンス費等に充当されている。
- 総費用の７５%が助成され、港湾局負担分は２５%の約７０万ドル（約１億円）

2023年のLA港の港湾保安助成金の内訳

| | 助成金 | 負担金（25%） | 費用総額 |
|---|---|---|---|
| セキュリティシステムのメンテナンス ※1 | $1,000,000 | $333,333 | $1,333,333 |
| サイバー脅威対策ソフトウェア等 ※2 | $1,000,000 | $333,333 | $1,333,333 |
| 潜水器具等 ※3 | $93,901 | $31,301 | $125,202 |
| 合計 | $2,093,091 | $697,967 | $2,791,868 |

※１　CRCやCSOCのセキュリティシステムを維持し、港のセキュリティプログラムの継続的な有効性を確保するために必要な、継続的なメンテナンスと修理費用

※２　港のセキュリティプログラムにおける潜在的な弱点からの保護のため、マルウェア保護ソフトウェアと拡張安全データ・ストレージ・サーバーの購入費用

※３　港湾警察の潜水機材導入費用

（出典）2023年LA港港湾局港湾委員会資料より作成

# ３．名古屋港統一ターミナルシステム（NUTS）のシステム障害について

- NUTS概要

名古屋港のコンテナターミナルの効率的、先進的な運用を実現するため、各港湾運送事業者が独自に利用していたシステムを民間主導で統一し、平成１１年に導入したシステム。名古屋港運協会が開発・運営。コンテナターミナルで必要とされる積降作業、保管管理、搬出入管理等について、効率的かつ機能的なオペレーションを実施

- NUTSシステムの障害

令和５年７月４日午前６時３０分頃、障害が発生

７月６日午前７時３０分システム復旧、１５時頃順次作業開始

- システム障害による影響（7/4～7/6）

トレーラーによる搬出入貨物　平均7,500本/日

積降ろしの影響を受けたコンテナ船　37隻

利用者がHP経由で行う各種手続きが利用不可

- システム障害の原因

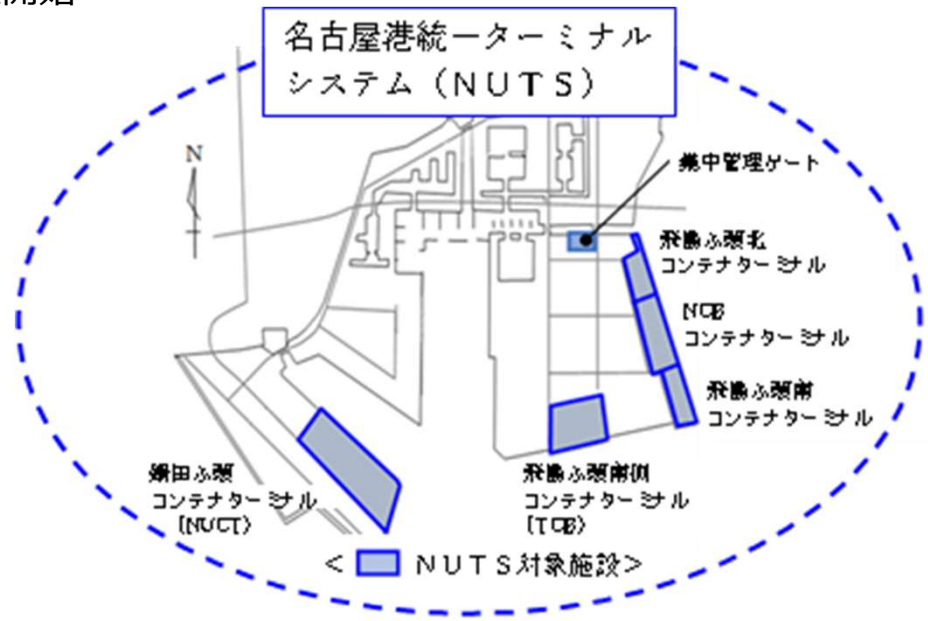
ランサムウェアの感染

- 捜査

愛知県警察が感染経路などを解析しているが犯人特定に至っていない。

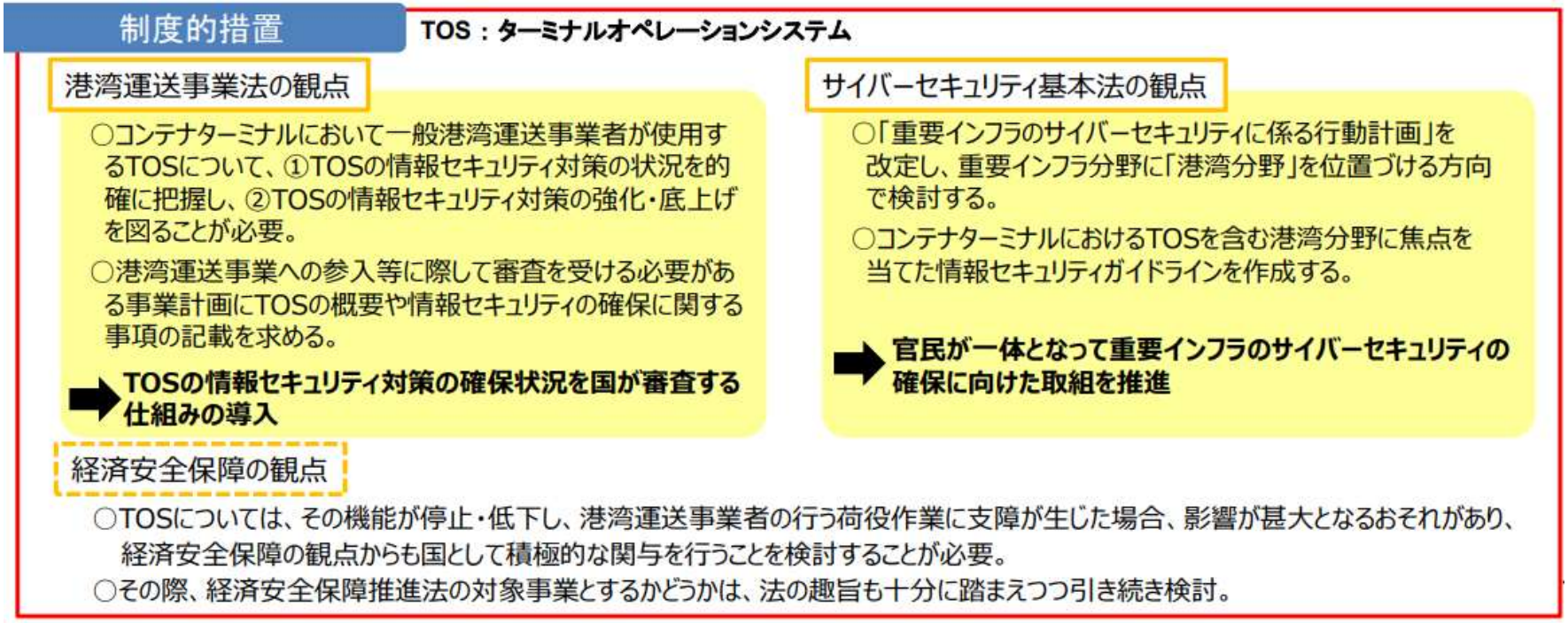
- 復旧、システム強化に向けた財政支援

名古屋港管理組合が実施



# ３．国土交通省によるコンテナターミナルの情報セキュリティ対策の検討について

- 名古屋港の事案を踏まえ、国土交通省では、コンテナターミナルの運営に関する基幹的な情報システムに必要な情報セキュリティ対策について、サイバーセキュリティ政策及び経済安全保障政策における港湾の位置付け等の整理・検討を実施
- ターミナルオペレーションシステムの情報セキュリティ対策を国が審査する仕組みなど、官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取り組みを推進することなどを検討
- サイバーセキュリティ基本法における重要インフラに、港湾分野の位置付けるほか、経済安全保障推進法に基づき国が重要インフラを手掛ける企業を事前に審査する仕組みである基幹インフラに、港湾運送事業の追加を求める方針




（出典）国土交通省港湾局　第3回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

# ３．警察のサイバーセキュリティ対策について

- 日本の警察においては、警察庁においてサイバー警察局を設置し、サイバー事案の捜査等を実施している。
- 重大サイバー事案（警察法第５条第４項第６号ハ※）への対処については、特別捜査隊が設置され、外国捜査機関等と連携し、高度な技術を要する事案や海外からのサイバー攻撃集団による攻撃に対処している。

サイバー警察局組織図　　サイバー警察局のシンボルマーク

サイバー特別捜査隊のシンボルマーク

※警察法第5条第４項

ハ　サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）が害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案（以下この号及び第二十五条第一号において「サイバー事案」という。）のうち次のいずれかに該当するもの（第十六号及び第六十一条の三において「重大サイバー事案」という。）

（１）　次に掲げる事務又は事業の実施に重大な支障が生じ、又は生ずるおそれのある事案

（ｉ）　国又は地方公共団体の重要な情報の管理又は重要な情報システムの運用に関する事務

（ｉｉ）　国民生活及び経済活動の基盤であつて、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業

（２）　高度な技術的手法が用いられる事案その他のその対処に高度な技術を要する事案

（３）　国外に所在する者であつてサイバー事案を生じさせる不正な活動を行うものが関与する事案

（出典）警察庁　サイバー警察局HP

# ４．考察　日米のサイバーセキュリティ対策の国際比較

- 米国LA港では、港湾局が警察組織を持ち、自衛組織としてサイバーセキュリティ対策を実施。港湾局内部システムの保護のためのCSOCの他、港湾内の関連事業者間の監視システムとなるCRCをあわせて運用。その整備費用の多くは米国政府からの助成金制度により支援されている。助成制度は港湾局だけでなく民間企業のセキュリティ対策でも利用可能なものとなっている。
- 日本の港湾は、それぞれ独自に内部システム保護のためのサイバーセキュリティ対策を実施。各ターミナルにおいて運用されるシステムのセキュリティ対策について、経済安全保障推進法に基づき、今後はターミナルのシステムのセキュリティ対策を国が審査する仕組みが導入される。警察法に基づき、捜査等は港湾局とは別組織の警察が行う。

日米の港湾のサイバーセキュリティ体制の主な相違点

| | 米国（LA港） | 日本（名古屋） |
|---|---|---|
| サイバーセキュリティの実施主体 | 各システム管理者及び<br>港湾局が全体を統括（CRC） | 各システム管理者<br>（国の審査体制を検討中） |
| サイバー事案の捜査 | 港湾警察<br>（港湾局内部組織） | 警察<br>（港湾管理者とは別組織） |
| 設備等の費用の政府の支援 | 港湾保安助成金による支援 | なし |

・LA港の体制は、米国の歴史的な考え方から、港湾の自治自衛に対する大きな責任から生まれる施策
・中央政府からの助成金も十分に実施され対策を後押し。民間企業へも助成金がある。
・日本は対策が各システム管理者の実施と偏りがあったが、システムの国の事前審査が検討されており、今後は体制が強化される。

・今後は港湾のサイバーセキュリティ対策が港湾競争力の重要な要素となる。
・日本も政府や警察、民間企業と連携し、対策を進める必要がある。