

名古屋港コンテナターミナルのサイバー攻撃 におけるインシデント対応について

令和 6 年 7 月 2 6 日
国土交通省 最高情報セキュリティアドバイザー
北尾 辰也

2023年7月4日（火）6:30頃より、名古屋港統一コンテナターミナルシステムにおいてサイバー攻撃による障害が発生し、名古屋港全コンテナターミナルの作業停止を余儀なくされた。

障害はランサムウェア攻撃によるものであり、ターミナル関係者が総力をあげて復旧に取り組み、7月6日（木）18:15に全ターミナルの作業を再開した。

名古屋港コンテナターミナルの概要

取扱貨物（令和3年港湾統計より）

総取扱貨物量	1億7,779万トン（平成14年から20年連続日本一）
主な輸出貨物	完成自動車、自動車部品（輸出量の約65%）
主な輸入貨物	LNG（液化天然ガス）、鉄鉱石、原油、石炭の原料（輸入量の約53%）
外貿コンテナ取扱個数	約254万TEUで国内3位。（1TEUは20フィートコンテナ1個換算）

名古屋港は色々な項目で日本一となっている

項目	名古屋港	2位	3位
総取扱貨物量	1億7,779万トン	千葉港	横浜港
輸出額	12兆4,805億円	横浜港	東京港
輸出額から輸入額を差し引いた貿易差引額	7兆1,913億円	神戸港	横浜港
自動車輸出台数	117万台	三河港	横浜港
臨港地区面積（陸域）	4,298ヘクタール	北九州港	横浜港

名古屋港管理組合のWebサイトより

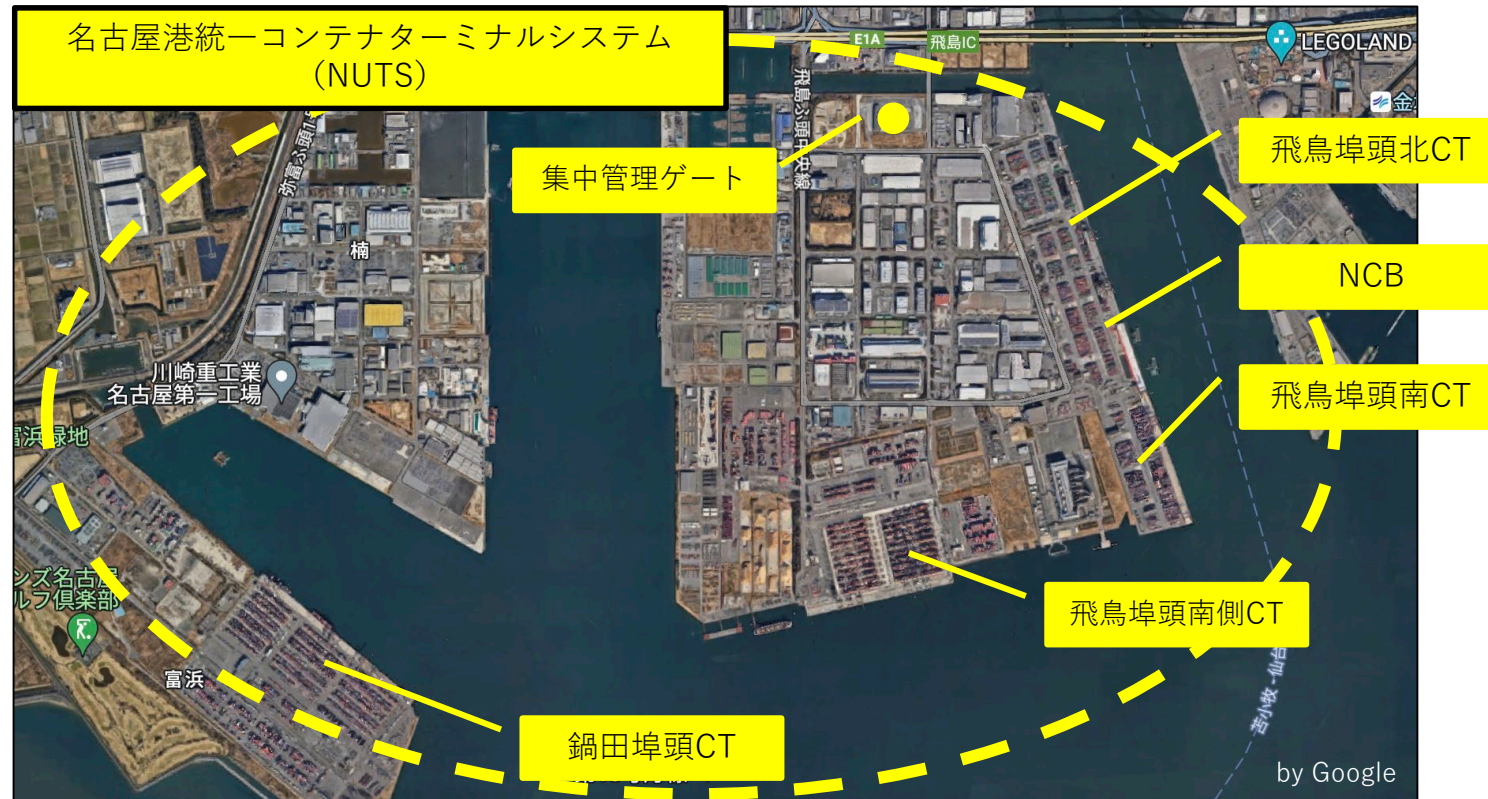
➡ 5つのターミナルで1日約7,500本のコンテナを扱っている（輸出が輸入より若干多い）

➡ 1ターミナルあたり1日約1,500本のコンテナを処理 ➡ 凡そ3本／分の処理能力が必要

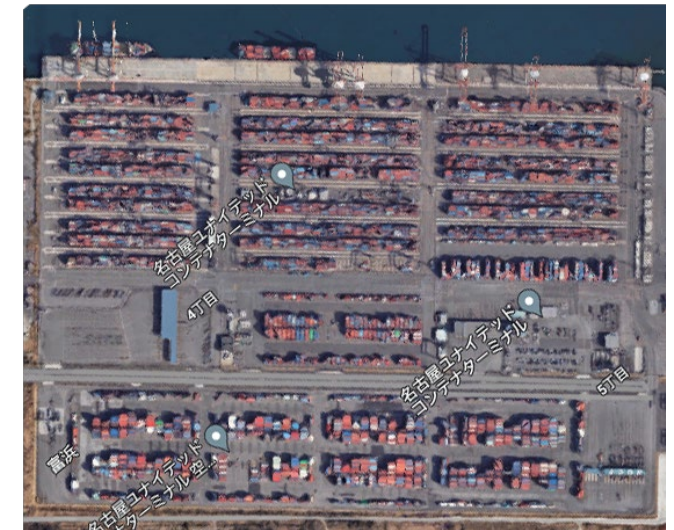
名古屋港統一コンテナターミナルシステム (NUTS)

名古屋港の5つのコンテナターミナルおよび集中管理ゲート（日本で唯一）が統一のコンピュータシステムで運用されている。2007年に現在の姿の基となるシステムがスタートし、機能を拡大しながら今日に至っている。

- ➡ 複数のコンテナターミナルを統合管理している港は日本では名古屋港と博多港のみ
- ➡ 名古屋港は日本で最もIT化が進んでいるコンテナターミナル

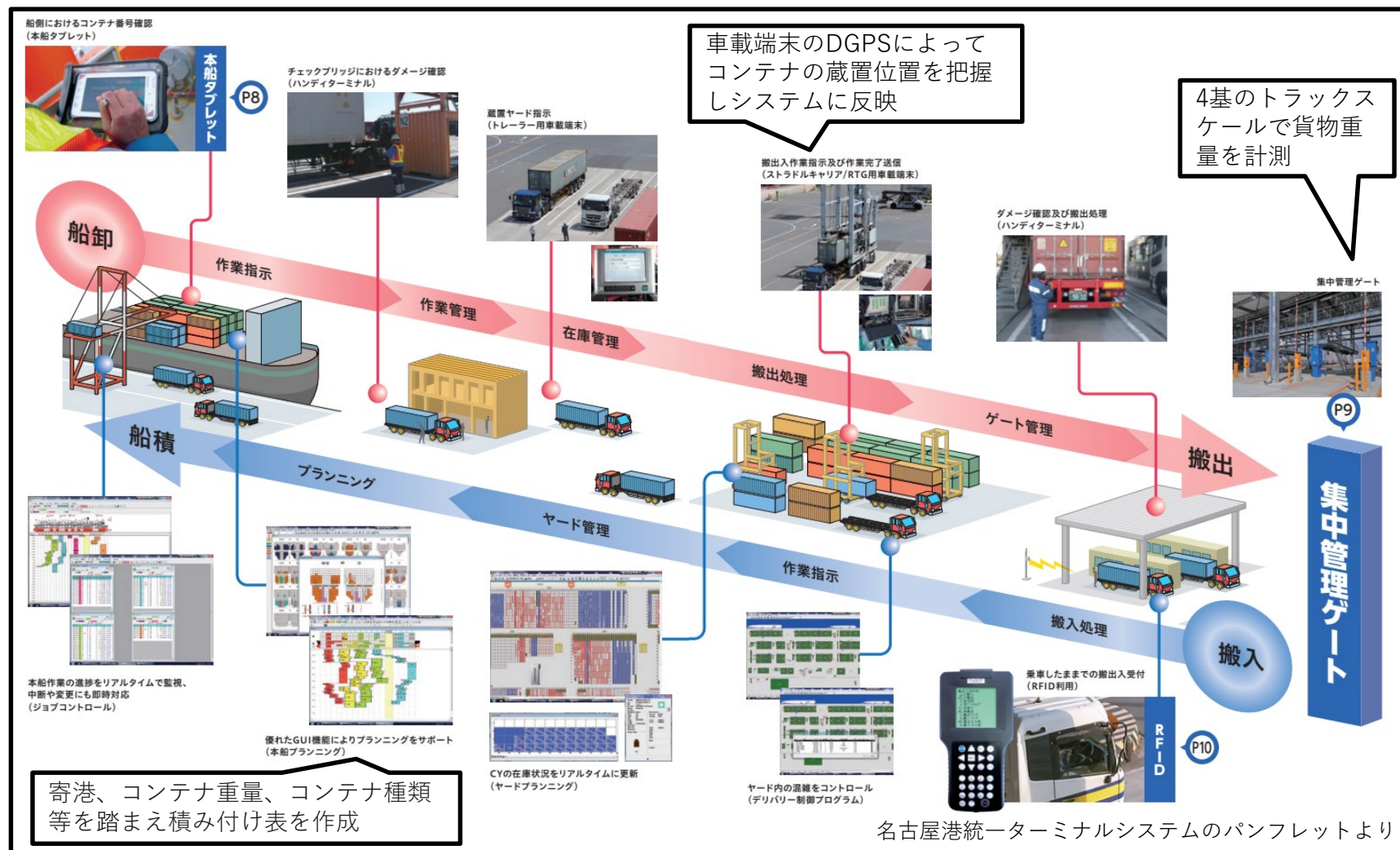


名古屋ユニテッドターミナル（鍋田埠頭ターミナル）



by Google

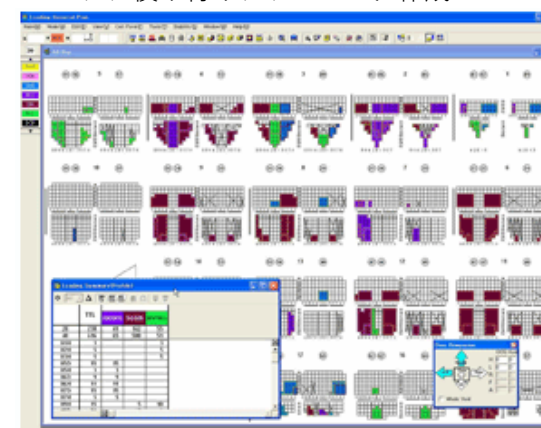
コンテナターミナルにおける全ての作業（コンテナ船積卸作業、プランニング、コンテナ保管管理、コンテナ搬出入管理、ヤード作業管理、保税管理等）が統合管理され、効率的かつ機能的なオペレーションが実現されている。



ヤード (※) 管理
※コンテナを集積・保管・受け渡しを行う場所



コンテナ積み付けプランニング作成



➡ ITの支援によって高効率・高利便性を実現

タイムライン (1日目)

【7月4日（火）】

- 06:30頃 NUTSシステムの作動が停止したことを確認
- 07:15頃 状況確認後、システム保守会社及びシステム開発会社へ調査を依頼
- 07:30頃 システム専用のプリンターからランサムウェアの脅迫文書が大量に印刷される
- 08:15頃 サーバが再起動できないことが判明
 - ➡ システムの担当者では、理解できない状況が発生
 - ➡ 愛知県警察本部サイバー攻撃対策隊（以下「愛知県警」）に連絡
- 09:00頃 愛知県警から、ランサムウェア攻撃の可能性があるとの見解が示される

この時の状況

トラックの待ち行列が伸びていった

朝、一隻が既に着岸しており、昼にも着岸予定あり

- ➡ ターミナルのオペレーションを担う機器に問題はなかったが、システムの支援がないと、通常レベルの運営はできない。
- ➡ バックアップは別の場所にコピーを取得しており、無事であることが確認できた

対応方針

システム復旧を優先させることを判断。復旧までは下記暫定策を実施することとした。

1. 船卸→搬出はマニュアル作業で実施
2. 既に搬入済みのコンテナはマニュアル作業で船積
3. 新たな搬入は停止

この対応を取り得た要因・背景

- ① バックアップが生きていた
- ② システム化以前のマニュアル作業経験者の存在
➡ ただし、システム障害やサイバー攻撃を想定したBCPは整備されていなかった
- ③ 迅速な意識決定と、関係者（各港湾事業者）の結束
- ④ 攻撃を受けたのはNUTS単独（ベンダーのデータセンター内の専用区画）だったこともあり、資産（システム構成やネットワーク構成）の把握ができていた
➡ 侵入経路や侵入された原因は不明だったが、資産の把握ができていたため、封じ込め（＝攻撃者の影響力排除）ができた
- ⑤ 保守ベンダーとの良好な関係

タイムライン（2日目（前半））

【7月5日（水）】

- 02:00頃 物理サーバ基盤全8台が復旧、仮想サーバ（45台）の復元作業を開始
- 12:00頃 名古屋港運協会より、今回のシステム障害の原因がランサムウェアへの感染であることが判明したこと等をプレス発表

➡ 2日目（7/5）の夕方にはシステムを復旧し、3日目（7/6）の朝から作業を再開する見積もりだった。

令和5年7月5日
12時発表

名古屋港記者クラブ会員 各位
報道 各位

名古屋港運協会
名古屋港コンテナ委員会
ターミナル部会

名古屋港統一ターミナルシステムのシステム障害について

昨日4日（火）、午前6時30分ごろから名古屋港内全てのコンテナターミナル内で運用している名古屋港統一ターミナルシステム（NUTS※）に障害が発生しました。

原因究明にあたって、システムを運用している名古屋港運協会ターミナル部会と愛知県警察本部と打合せを行ったところ、ランサムウェアの感染であることが判明いたしました。

現在、復旧にむけて関係者総力をあげて取り組んでいるところであり、本日（7月5日（水））18時を目処にシステム復旧を図るとともに7月6日（木）8時30分からの作業再開を目指し作業を進めております。

なお、復旧状況につきましては、随時公表する予定としております。

このシステム障害により、本日のターミナルへのトレーラーによるコンテナ搬出入作業は中止し、入港コンテナ船の積み卸し作業につきましては元請港運会社にご確認願います。

※ NUTS (Nagoya United Terminal System)

タイムライン (2日目 (後半) ・ 3日目)

【7月5日 (水)】

- 12:00頃 仮想サーバの復元完了、ウイルスチェックを開始
- 21:00頃 復元した仮想サーバからウイルスが検知され、ウイルス駆除の必要があると判断

【7月6日 (木)】

- 02:00頃 ウイルスチェック終了、最終的に約130個のマルウェアを検知、ウイルス駆除を開始
- 07:15頃 ウイルス駆除終了、バックアップデータから復元が完了したが連携に障害が発生
- 14:15頃 連携障害が解消、データと実在庫情報の整合性の確認を開始

15:00～18:15 各コンテナターミナル、順次作業再開

➡ 想定外の事態が発生するも、迅速に対応し、当初の見積もりからは遅れるも3日目の夜に作業を再開

令和5年7月6日
7時45分発表

名古屋港記者クラブ会員 各位

名古屋港運協会
名古屋港コンテナ委員会
ターミナル部会

名古屋港統一ターミナルシステムのシステム障害について (3)

名古屋港統一ターミナルのシステム障害に関しましてはご利用者の皆様に多大なるご迷惑をおかけしておりますことをお詫び申し上げます。
昨日18時に発表致しました上記につきまして、復旧にむけて関係者総力をあげて取り組み、7月6日(木)07時30分にシステム復旧致しました。
なお、7月6日(木)8時30分からの作業再開につきましてはシステム復旧の遅延によりまして、本日午後からの開始予定となっております。
開始時間の詳細につきましては別途ご案内させていただきます。

名古屋港統一ターミナルシステムのシステム障害について (4)

名古屋港統一ターミナルのシステム障害に関しましてはご利用者の皆様に多大なるご迷惑をおかけしておりますことをお詫び申し上げます。
本日7時45分に発表致しました上記につきまして、本日の作業開始時間を午後からの開始予定としておりましたが以下の開始時間(見込み)と致しますのでお知らせします。

※

作業再開時間: TCB 15:00～

NUCT 17:30～(見込み)

飛島東側(3ターミナル) 18:30～(見込み)

1. ログの保全

原因を分析するためのログ（システムログ、アクセスログ）がバックアップ対象となっておらず暗号化被害によって原因分析ができなかった。また、復旧対応によるログの消失も発生しており、証拠保全を考慮したログの保存やインシデント対応手順を整備することが望ましい。

2. 運用再開時のセキュリティ対策状況の確認

運用再開時にシステムの面での確認のみを行い、適切なセキュリティ対策が取られている状態であるかどうかの確認・評価が行われていなかった。

3. 専門家への相談

愛知県警へ迅速に相談してはいるものの、初動対応時や原因究明、運用再開時においてサイバーセキュリティ専門家への相談を行っていない。事案発生時に専門家へ直ちに相談できるよう、日頃から関係を構築しておくことが望ましい。

令和5年7月7日

関係各位

名古屋港運協会
名古屋港コンテナ委員会
ターミナル部会

（お知らせ）名古屋港統一ターミナルシステムのシステム障害について

名古屋港統一ターミナルシステムのシステム障害に関しましてはご利用者の皆様に多大なるご迷惑をおかけ致しましたこと改めましてお詫び申し上げます。

名古屋港統一ターミナルシステムにつきましては、6日(木) 7時30分のシステム復旧以降、順次ターミナル業務を再開し、同日18時15分の飛島東側3ターミナルの作業再開をもって、名古屋港の全てのターミナル(5ターミナル)におきまして通常の業務体制となりましたのでお知らせします。

引き続き、名古屋港のコンテナ物流の安定に努めて参りますので今後とも名古屋港をご利用下さいますようよろしくお願い致します。