M S S A

一般社団法人　宮城県警備業協会
〒981-3105　仙台市泉区天神沢一丁目４番 11 号
℡　022-371-0310　FAX　022-773-6466
info@mssa.jp
http;//www.mssa.jp

令和５年８月７日

会員の皆様へ

テロ対策総合パートナーシップみやぎからの協力要請（ご連絡）
～港湾施設のシステムがサイバー攻撃を受け活動停止に～

テロ対策総合パートナーシップみやぎ（事務局：宮城県警察本部）から別添のとおり資料の送付を受けました。
先般発生した、名古屋港ターミナルの運用がサイバー攻撃を受けて一時停止になった事案の概要等について協力要請がありましたのでご連絡いたします。

港湾施設のみならず、あらゆる業種にも起こりうる事案ですので、情報共有とともに不審情報がありましたら宮城県警察本部までご連絡をお願いいたします。

一般社団法人宮城県警備業協会
専務理事　　高橋　直嗣

別添

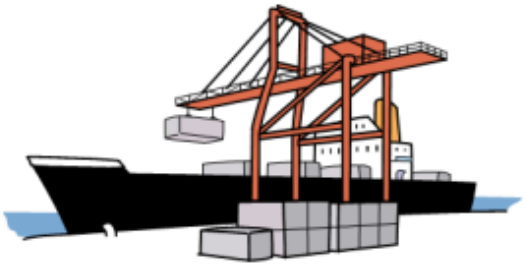
ランサムウェア攻撃により名古屋港は活動停止
～ 事件概要とサイバーセキュリティ対策について ～

令和５年８月２日
ﾊﾟｰﾄﾅｰｼｯﾌﾟみやぎ事務局
（宮城県警察本部外事課）

ターミナルで搬出入作業停止

７月４日午前6時半ころ、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）の全サーバがランサムウェア（身代金要求型マルウェア）感染により暗号化され、全ターミナルの作業が停止する事案が発生しました。

バックアップデータから復元を試み、７月６日午後6時15分にターミナルの作業を再開するまでの間、トレーラーを使ったコンテナ搬出入作業が停止しました。



事案の影響は・・・

日本政府が「重要インフラのサイバーセキュリティに係る行動計画」で定める重要インフラサービス14分野には、港湾運送業を含む「物流」がありますが、「港湾」は含まれておりません。本事案では、重要インフラ事業者が直接的に攻撃を受けたとはいえませんが、周辺の物流事業者にも影響が及んだことから、日本の重要インフラに対するサイバー攻撃であったとの見方もあります。

ランサムウェア攻撃の傾向と特徴

ランサムウェアは、マルウェアの一種で、感染したコンピュータをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、身代金を要求するメッセージを表示するものです。

ランサムウェア攻撃は、サイバー攻撃者による単純な「ばらまき」型のほか、近年は、攻撃実行までにいくつかの操作ステップを踏む、ネットワーク侵入を前提とした「Human-Operated(人による操作)」型が主流となっており、増加傾向にあります。

ランサムウェアに対するサイバーセキュリティ対策

一般的な対策となりますが、

- ○ VPN機器等のぜい弱性対策（セキュリティパッチの適用等）
- ○ セキュリティソフト等の導入
- ○ メールサーバにおける不審メール検出機能の導入

などを見直していただき、ランサムウェア攻撃に備えて下さい。

一方で、サイバー攻撃を完全に防ぐことは極めて困難ですので、万が一侵入された場合の対応・体制を確立していくことが重要とされています。

また、警察庁ウェブサイト上で、各種プログラムのぜい弱性や不正プログラムに関する情報等を公開していますので、御活用下さい。

Windows Server 2012のサポート終了

2023年10月10日、Windows Server 2012, Windows Server 2012 R2のサポートが終了します。

これらのOSをお使いの場合は、サポートが終了する前に最新のOSへ移行しなければ、サポート終了後はMicrosoftから新規のセキュリティパッチが提供されなくなり、ぜい弱性を狙った攻撃を防ぐことが難しくなります。

～「何か変？」 知らせる勇気 テロ防ぐ ～