KAIRIKI GROUP
2025 年 12 月 23 日

海力株式会社
〒101-0032 東京都千代田区岩本町 2-1-17 鈴与日本橋ビル 7 階
Tel: 03-5846-9515　Fax: 03-5846-9516
Mail: info@kairiki-ships.com　URL: http://kairiki-ships.com/

ISO27001

KC No. 008

各位

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24, Change 1 の改正発行について

USCG より、2025 年 11 月 12 日に NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24, Change 1(NVIC 02-24, CH 1)が改正発行されました。
このガイダンスは、海上輸送保安法（MTSA）の規制対象事業体および海洋輸送システム（MTS）関係者に対し、増大するサイバー脅威を含むセキュリティリスクへの対応を強化し、報告要件への遵守を目的としています。

【主な目的と背景】

■　目的：
セキュリティ侵害（BOS）、不審な活動（SA）、輸送セキュリティ事案（TSI）、サイバーインシデント、および報告対象のサイバーインシデント(RCI)の報告要件を遵守するためのガイダンスを提供すること。

■　背景：
2024 年 2 月 21 日の大統領令により、33 CFR Part 6 が改正され、「サイバーインシデント」の定義が追加され、実際のまたは脅威となるサイバーインシデントの即時報告が義務付けられました。2025 年 7 月 16 日には、USCG が海上セキュリティ規則を更新し、「報告対象のサイバーインシデント（RCI）」の定義を追加し、33 CFR Part 6 の対象外の事業体（OCS 施設など）に国家対応センター（NRC）への報告を義務付けられました。

【報告が必要なセキュリティ・サイバー事案と報告先】

1.　サイバーインシデント

- 対象：MTSA規制対象事業体およびMTS関係者（船舶、港湾、ウォーターフロント施設など）
- 報告内容：妨害行為、破壊的活動、またはデジタルインフラを含む施設を危うくする実際のまたは脅威となるサイバーインシデントの証拠
- 報告先：NRCへの遅滞ない通知が強く推奨されています。これによりUSCGの港湾管理責任者（COTP）への通知要件が満たされます。さらに、NRCへの通知はFBIのCyWatchに直ちに転送され、FBIへの報告要件も満たされることとなります。また、サイバーインシデントの場合、アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）にも別途報告を行う必要があります。

海力株式会社
〒101-0032 東京都千代田区岩本町 2-1-17 鈴与日本橋ビル 7 階
Tel: 03-5846-9515　Fax: 03-5846-9516
Mail: info@kairiki-ships.com　URL: http://kairiki-ships.com/

2.　対象のサイバーインシデント（RCI）

- 対象：33 CFR Part 6の対象ではない規制対象事業体（例：大陸棚（OCS）施設）
- 報告内容：すべてのRCI
- 報告先：NRCへ遅滞なく報告が必要です。

3.　セキュリティ侵害（BOS）と不審な活動（SA）

- 対象：MTSA規制対象事業体
- 報告内容：BOS（セキュリティ対策が回避または違反された事案で、TSIに至っていないもの）またはSA（TSIにつながる可能性のある活動）があった場合
- 報告先：NRCへ遅滞なく報告することが義務付けられています。地元の港湾管理責任者（COTP）に直接報告することも可能ですが、NRCへの通知義務は免除されません。

4.　輸送セキュリティ事案（TSI）

- 対象：MTSA規制対象事業体
- 報告内容：重大な人命の損失、環境被害、輸送システムの混乱、または特定の地域での経済的混乱をもたらすセキュリティ事案が発生した場合
- 報告先：　COTPへ遅滞なく報告し、その後、セキュリティ計画に定められた手順に従って対応を開始します（これにはNRCへの連絡が含まれる場合があります）。

【サイバー事案報告の具体例】

サイバーインシデントおよび RCI として報告が求められるのは、以下のいずれかにつながる、または合理的にその可能性がある事案です：

- 情報システム、ネットワーク、またはOT（オペレーショナル・テクノロジー）システムの機密性、完全性、可用性の実質的損失
- 事業運営や物品・サービスの提供能力における混乱または重大な悪影響（公衆衛生や安全に重大な影響を与える可能性のあるものを含む）
- 多数の個人の非公開の個人情報の開示または不正アクセス
- 重要インフラシステムまたは資産へのその他の潜在的な運用の混乱

（通常の迷惑メールやフィッシングの試み、標準的なアンチウイルスプログラムで対処されるような悪意のある低レベルと見なされる事象は、サイバーインシデントとは見なされません。）

海力株式会社
〒101-0032 東京都千代田区岩本町 2-1-17 鈴与日本橋ビル 7 階
Tel: 03-5846-9515　Fax: 03-5846-9516
Mail: info@kairiki-ships.com　URL: http://kairiki-ships.com/

【問い合わせ先】

質問等があれば、USCG の港湾・施設コンプライアンス室（CG-FAC）MTSCyberRule@uscg.mil に直接問い合わせが可能です。

【昨年発行された NVIC 02-24 からの変更点】

1. 報告対象サイバーインシデント（RCI）の組み込み

- RCIの報告要件に関するガイダンスが追加されました。
- RCIは、OCS施設など、サイバーインシデント報告の対象外の事業体に適用されます。

2. サイバーインシデント報告手続きの簡素化と整合性

- 海上輸送システム（MTS）関係者に適用される「サイバーインシデント」の定義と、MTSA規制対象事業者に適用される「報告対象のサイバーインシデント（RCI）」の定義との間の重複に対処し、報告基準の整合性が図られました。
- OCS施設がサイバーインシデント報告の対象外であること、およびRCIの報告義務が33 CFR Part 6の対象外の事業体にのみ適用されることが明確化されました。

3. FBIへの報告の簡素化
NRC に通知することで、FBI CyWatch への報告要件も満たされることが明確化されました。これにより、報告プロセスが合理化されました。

4. 規制変更への対応

- 2024年2月21日の大統領令14116号（米国船舶、港湾、港、および沿岸施設等の保全に関する規則の改正）、および2025年7月16日の沿岸警備隊による海上保安規制の更新（33 CFR Part 101、104、105、106へのサイバーセキュリティ要件の追加）に対応したガイダンスが提供されました。
- 大統領令14116号により、33 CFR Part 6が改正され、「サイバーインシデント」の定義が追加され、サイバーインシデントの証拠をFBI、CISA、およびCOTPに直ちに報告する要件が追加されました。

原文はこちら
United States Coast Guard (USCG)
NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24, Change 1(NVIC 02-24, CH 1)

本件に関するお問い合わせがございましたら、弊社までお気軽にご相談ください。