船舶のサイバーリスク管理のための モニタリング技術について

2021年12月2・3日

株式会社MTI　船舶物流技術グループ
若海伽奈

船舶の機器とセキュリティ三大要素

✓船舶の機器のデジタル化が進むにつれ、サイバー攻撃のリスクが増加している。

サイバーセキュリティ3大要素	IT (Information Technology) メールPC　プリンタ　電話	OT (Operation Technology) 航海・機関機器　制御ネットワーク
機密性 権限保持者のみ情報にアクセス出来るようにする	• **情報漏洩防止**	• データ漏洩の影響度は低い
完全性 情報が正確で完全であることを維持する	• **運航や貨物情報等の改ざん防止** • 情報整合性の保持	• **運航機器の正常動作** • **運航の安全性確保**
可用性(継続性) 必要時に常に情報にアクセスが出来るようにする	• システムの一時的な停止が運用要件により容認できる	• **運航機能の継続稼働性確保**
侵害の影響	一般には人命や安全を脅かさない**経営や非物理的影響**	船舶、船員、貨物、環境等**人命や安全が脅かされる**

船舶のOT機器へのサイバー攻撃

船舶のOT機器への攻撃源	船舶への攻撃	船舶の被害
• **USBポート**からの感染 • **メール添付**からの感染 • **不正URL**からの感染	• GPS信号成りすまし • AIS信号成りすまし • OT機器の制御乗っ取り • データ破壊、改ざん	• **安全運航**が脅かされる。

※OT機器を守る＝”乗っ取り“や”運航不能“を防止し、船の運航に関する各機能の正常動作を維持する

各国船級のガイドラインでの対応

- IACS(International Association of Classification Societies:国際船級協会連合) No.166 Recommendation on Cyber Resilienceでは、

  船舶のOT機器・システムのモニタリングについて既に推奨している。

6.4 Detect (D):

Functional requirements

OTシステムの通常運用を監視する手段の提供

D1) Means for the monitoring of normal operations of OT systems should be provided, based on continuous and/or on-demand self-diagnostics and connection quality and/or network performance monitoring tools should be available at least on networks connecting OT systems of Category II and III and on networks connecting IT systems to OT systems of Category II and III.

現在Recommendation(推奨)だが、今後**Unified Requirement (UR:強制)**になることが見込まれる。

⇒船舶の**OT機器のモニタリング**が今後要求されるようになってくる。

他業界で使用されている OT機器のモニタリングツールの比較

ベンダ	海事業界の知見	特徴・導入事例	監視体制（SOC）
A社	○ スマートポートで事例有り	AIにより正常動作を学習し、脅威を検出	△ A社からのSOCサービスの提供は無いが、他社と組み合わせた監視レポートサービス有り
B社	×	石油、ガス、航空などのOT脅威監視	×
C社	○	交通、石油等のOT向け脅威監視、資産管理、構成管理	△ C社からのSOCサービスの提供は無いが、他社からの提供有り

C社のツールで船舶のOT機器のモニタリング検証を行った。

SOC＝Security Operation Center

船舶のOT機器のモニタリング技術検証 実施概要

検証ツール

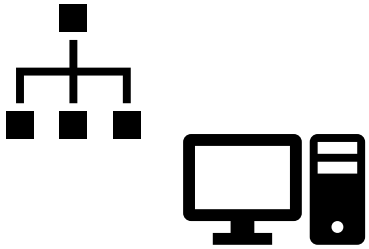
検証に用いたツール	C社のツール
ツール概要	PLC等のOTプロトコルに対応するセキュリティモニタリングサービス
主要機能	1. アセット管理 2. NWマップの自動生成 3. ポリシーの設定・イベント検知・通知 4. 通信状況の可視化 5. モニタリング結果を統括したセキュリティレポート作成

※PLC＝Programmable logic controller、機器の制御に使われるコントローラー

検証概要

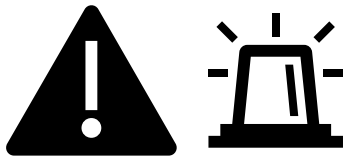
検証対象	船舶の操船系機器を模擬した環境
検証方法	検証環境にモニタリングツールを接続し、通信されるパケットをキャプチャ・自動解析を行った。

船舶のOT機器のモニタリング技術検証



アセット管理

通信状況の可視化



イベント検出・通知

船舶のOT機器のモニタリング技術検証 －アセット管理－

結果画面イメージ図

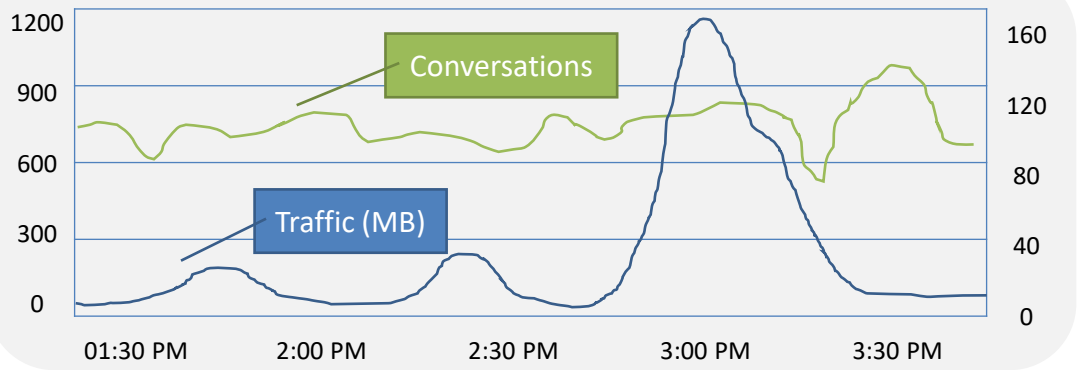
アセット	タイプ	リスクスコア	重要度	IPアドレス	カテゴリ	ベンダ
Endpoint1	Endpoint	14	Low	192.168.0.1	Network Assets	Intel
Laptop1	Laptop	45	Low	192.168.0.2	Network Assets	Buffalo
Endpoint2	Endpoint	25	Low	192.168.0.3	Network Assets	
Laptop2	Laptop	14	Low	192.168.0.4	Network Assets	Intel
:	:	:			:	:

CVEs: Common Vulnerabilities and Exposures: 共通脆弱性識別子

ネットワーク内のアセットの、**IPアドレスや機器情報が自動検出**され、
それぞれの機器の**リスクレベル**が自動的に算出された。

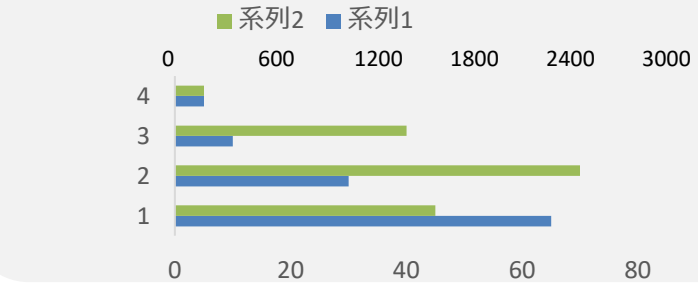
船舶のOT機器のモニタリング技術検証 －通信状況の可視化－

トラフィック結果イメージ

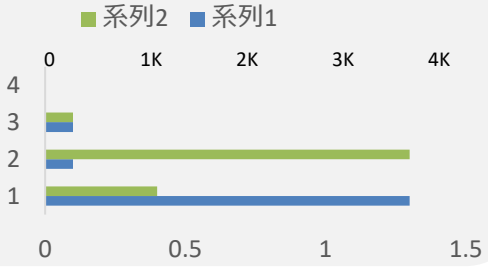


通信状況を
リアルタイムに確認が出来た。

Top5送信元

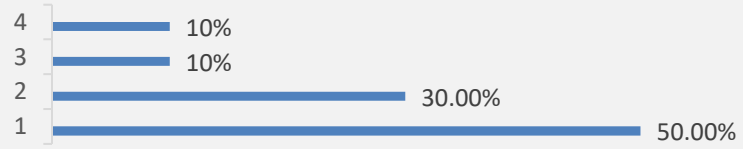


Top5送信先



通信量が多い
送信元・送信先が
明らかになった。

Protocols



通信量の多いプロトコルが明らかになった。

船舶のOT機器のモニタリング技術検証 ーイベント検出・通知ー

イベント通知イメージ

ID	時間	イベント	重要度	アセット	IPアドレス
1	04:55 PM Mar 15, 2021	Unauthorized Conversation	Low	Endpoint1	192.168.0.1
2	04:33 PM Mar 15, 2021	Spike in Network Traffic	Medium	Laptop1	192.168.0.3
3	04:29 PM Mar 15, 2021	New Asset Discovered	Low	Endpoint2	192.168.0.4
4	04:24 PM Mar 15, 2021	Asset not seen for 1 hour	Low	Laptop2	192.168.0.8

イベント情報

- イベント詳細
- トリガーのポリシー
- ステータス（解決済・未解決）
- 本イベントを確認すべき理由
- 推奨対応策

例

イベントを確認するべき理由

通信しているべき端末が通信していない場合、その端末への通信経路が壊れている、またはその端末は到達不可となっている。これは、ネットワークが切断されたり、DoS攻撃が実行され、端末との通信が制限された場合に発生する可能性がある。

- **推奨対応策**

端末へのpingまたはtracerouteを実行し、接続が存在するかどうかを検証し、存在しない場合はどこで失敗するか確認。一度に多くのアセットが消える場合は、障害が発生した可能性のある共通のネットワークコンポーネントがあるかどうか確認。

適用するポリシー・イベントの通知先を設定し、
ポリシーに該当するイベントの通知を受けた。
対処方法が推奨された。

船舶のOT機器のモニタリング技術検証　まとめ

- 船舶の**OT機器のサイバーセキュリティを守る＝安全運航の維持を守る**

- 対策の第一歩は、**アセットや通信の現状を理解する**こと。

- OT機器のモニタリングツールを船舶の模擬環境で検証した結果、
  検出されるべき端末が検出され、端末情報や通信状況が確認できた。
  脅威となる通信・イベントを**タイムリー検出**できた。
  →**モニタリングをしていなかったら気づくことが出来なかった。**

- OT機器のモニタリングは既にIACSのガイドラインでも明示されており、**今後要求されるようになる**ため、準備を進める必要がある。

ご清聴どうもありがとうございました。