

VDESを使ったAIS認証のしくみ

海のデジタル安全を守る「次世代の身元確認システム」を分かりやすく解説します。

(株) スターヌラ・ジャパン 渡部 浩章 (わたなべ ひろあき)

 所要時間: 15分

 対象: 海事関係者の皆様

 VDES / AIS / 電子署名

1. 認証の基本コンセプト

「認証（Authentication）」とは何か？

認証とは一言でいうと、相手に対し「本当に本人（本物）ですか？」を確認し証明する手続きのことです。

身近な例①：対面での本人確認

- マイナンバーカードやパスポートを提示
- 顔写真と実際の本人の顔を見比べる
- 「この人は間違いなく本人だ」と判断する

身近な例②：ネットショッピング

- アドレスバーに表示される「鍵マーク」
- 偽物の詐欺サイトではなく「本物の銀行や通信サイト」であることを裏で自動検証している

2. AISの抱えるリスク

なぜ今、AISに「認証」が必要なのか？

⚠ 現状のAISには「認証の仕組み」が存在しません

現在のAIS信号は「誰でも自由に同じ形式で電波を出せる」ため、善意を前提とした無防備な状態です。

 **ゴースト船**
(成りすまし)

存在しない架空の船をECDIS
画面等に表示させる

+

 **位置・データ改ざん**

他船の位置や名称、針路を嘘
の情報に書き換える

→

 **ECDISの混乱**

航行安全・衝突防止への
甚大な脅威

3. デジタル認証の仕組み

デジタル認証のキホン：「電子証明書」と「鍵」

デジタル世界では「非対称暗号（公開鍵・秘密鍵）」という技術を使って成りすましを防ぎます。

1. 秘密鍵（実印・ハンコ）

- ・ 送信者（自船のAIS機器内）だけが厳重保管
- ・ 誰にも絶対渡さない秘密の情報
- ・ これを使ってデータに**電子署名**を付与

2. 公開鍵・証明書（印鑑証明書）

- ・ 受信者（他船や海上保安庁など）に配布
- ・ 「信頼できる第三者機関(PKI/CA)」がお墨付き
- ・ 誰でも取得して使用可能

4. 既存AISの限界

既存AISだけでは認証データを送れない「2つの壁」

壁①：メッセージ構造が固定

AISのデータ形式は国際規格で厳密に定められています。世界中の全船舶に普及しているため、今から「電子署名用の枠」を拡張できません。

[位置] [針路] [速力] → 余白一切なし！

壁②：電波帯域（通信量）が限界

東京湾や関門海峡などの主要港湾・狭水道では、すでにAISの送信に使っている電波（VHF帯）は過密状態にあります。さらに電子署名データを載せると通信障害を引き起こします。

現在の利用率：ほぼ100%過密状態

5. 解決策（本題）

VDESを使った Dual Channel 構想

ここで登場するのが VDES（VHF Data Exchange System）です。大容量のVDEチャンネルを組み合わせて解決します。



6. 認証方式の詳細 (IALA G1192 Ed2.0)

方式①：後追い署名方式 (Scheme 1)

✓ 特徴：既存の古いAIS受信機への影響ゼロ（上位互換）

① まず通常通り AIS メッセージを送信

AISチャンネルを使用。従来の既存AIS機器でも問題なく受信・画面表示が可能。

② 直後に VDE チャンネルで「後追い情報 (Follow-on)」を送信

直前に送ったAISメッセージの「電子署名」を、VDESの回線で追撃送信する。

③ 受信側のアプリケーション（ECDIS等）で署名検証

届いたAISメッセージと後追い署名を検証し、「**本物マーク**（認証済アイコン）」を表示する。

方式②：一体型署名方式 (Scheme 2)

⚡ 特徴：VDE Signed Segment によるダイレクト送信

【送信】VDES通信包（パケット）

📦 [メッセージ本体 (AIS)]
+ [電子署名 (Signed Segment)]

最初から1つのワンセットにしてVDEで送信



【受信】VDES対応端末

無線機本体の内部で直接署名を即座に検証。
署名検証に成功すれば「AIS送信元は本物
（例えば本物の仮想標識・AtoN）」として
ECDIS海図上に表示。

8. 方式の比較

2つの認証方式の使い分けまとめ

項目	方式①：後追い署名 (Scheme 1)	方式②：一体型署名 (Scheme 2)
使用チャンネル	AIS (データ) + VDE (署名)	VDE (データ + 署名)
既存AIS機器との互換性	✅ 完全互換 (受信・表示可能)	⚠️ VDE認証対応機が必要
署名検証を行う場所	外部アプリ (ECDIS等)	VDES無線機本体
主な用途	一般船舶の位置報告・動静通知	仮想航路標識 (Virtual AtoN) 等

9. 導入に向けた課題

本格普及に向けた実用上のチャレンジ



1. 計算負荷と電波の消費

全メッセージに個別に署名をつけると通信容量を消費するため、一括認証技術（TESLA方式等）が検討されています。



2. 数万隻の「鍵・証明書」管理

世界中の船舶へ安全に証明書を発行・更新するPKIインフラ（公開鍵基盤）の国際的運用ルールの策定が必要です。



3. 「元データ（GPS等）」の正しさは別問題

AIS認証は「送信者が本物か」を証明しますが、GPS信号自体が偽造（スプーフィング）された場合は防げません。GNSS認証技術等との多層的な防御が必要となります。

10. まとめ

安全な海上交通の実現に向けて

AIS認証は「VDES」の登場でいよいよ現実的に

従来AISの帯域・メッセージ構造の限界を、VDESの大容量通信が打ち破りました。

将来的なSOLAS条約等での義務化トレンド

国際海事機関(IMO)やIALAにおいて、VDES規格および認証機能の国際標準化が進んでいます。

「VDES対応」を見据えた機器更新計画を

新造船や定期機器更新時には、将来の認証拡張に対応可能な「VDES対応端末」への切り替えが推奨されます。

ご清聴ありがとうございました。