技術報告

海洋情報部研究報告 第 60 号 令和 4 年 3 月 18 日
REPORT OF HYDROGRAPHIC AND OCEANOGRAPHIC RESEARCHES No.60 March 2022

新旧の IHO のデータ保護スキームの概要†

梶村　徹*1，服部友則*2

Overview of the old and new IHO Data Protection Schemes†

Toru KAJIMURA*1 and Tomonori HATTORI*2

Abstract

IHO S-63“IHO Data Protection Scheme”is the standard for protecting S-57 ENCs from piracy and unauthorized use. It has been used worldwide. Part 15 of the IHO S-100“Universal Hydrographic Data Model”is the upgraded version of S-63 and will be used for S-100 products, not only for ENCs, in the near future. This article gives comparisons between them and offers some considerations.

1　はじめに

S-63「データ保護スキーム」は，従来地域電子海図調整センター（RENC）である PRIMAR によって S-57「デジタル水路データの転送基準」に基づく航海用電子海図（S-57 ENC）の複製頒布に採用されていたデータ保護スキームを，国際水路機関（IHO）の推奨するデータ保護スキームとして採用したものであり，2003 年の Edition 1.0 以後，2020 年刊行の Edition 1.2.1 までに小規模な修正が加えられてきた．この間，国際海事機関（IMO）においても海運へのサイバー攻撃対策の重要性が認識されてきており，現在，S-57 ENC を S-63 のスキームで保護することが，世界の ENC の流通において，一般的になっている．

一方，S-100「ユニバーサル水路データモデル」は，水路データ全般の基準として開発されてきており，S-101「次世代電子海図製品仕様」で作製された ENC（S-101 ENC）のみでなく，他の水路情報も，これを基に作製されることとされている．S-100 を基に作製された製品（S-100 製品）のデータ保護スキームは 2018 年刊行の Edition 4.0.0 で Part 15 として初めて S-100 中に記述されたが，これは，S-63 を基に開発されたものである．S-100 は 2022 年中に Edition 5.0.0 として刊行される予定となっており，データ保護スキームを記述している Part 15 にも若干の修正（本稿執筆時点で，5.3 節で後述するデュアルフュエル ECDIS に対応するために，ディレクトリ構造に関する記述の追加などが議論されている）が期待され，それが実用版の S-100 製品の保護に用いられると考えられる．

本稿では，S-63（以下，特記しない限り Edition 1.2.1 について）と S-100（以下，特記しない限り Edition 4.0.0 について）Part 15 の概要

† Received September 15, 2021; Accepted October 28, 2021
＊1　技術・国際課　Technology Planning and International Affairs Division
＊2　技術・国際課　海洋研究室　Ocean Research Laboratory, Technology Planning and International Affairs Division

を述べ，これらを比較し，さらに考察を行う．

2　データ保護の基本

2.1　データ保護の目的

S-63 と S-100 Part 15 はどちらも次の 3 点の確保を目的とする；

・不正使用防止：情報を暗号化することによりデータの不正使用を防止する
・選択的アクセス：顧客が許可された情報のみにアクセスできるよう制限する
・真正性：データの出所が認められた情報源からであることを確認する

2.2　データ保護の手法

S-63 と S-100 Part 15 はデータセキュリティの入門書に書かれているような基本的なデータ保護の手法を用いている．以下に簡単に説明する．

2.2.1　暗号化／復号

元に戻すことを前提に，情報を一見無意味な情報に変換し，元の情報を読み取れないようにすることを暗号化といい，暗号化された情報を元に戻すことを復号という．また，暗号化と復号の変換規則の情報を鍵という．鍵には，暗号化と復号で同じ鍵を使用する共通鍵と，1 組の別の鍵を使用する非対称鍵があり，非対称鍵の一方を公開鍵，もう一方を秘密鍵という．3 章で後述する M_KEY，HW_ID，製品キーは共通鍵である．

2.2.2　電子署名

あるデータにハッシュアルゴリズムを利用すると，そのハッシュ値が得られる．元のデータが 1 bit でも異なると，ハッシュ値は大きく変化し，異なるデータから同じハッシュ値が得られることは極まれにしか起こらない．また，ハッシュ値から元のデータを推測することは不可能である．これらの性質を利用し，転送中にデータが改ざんされていないことを次のように確認することができる．

データの転送元が，そのデータのハッシュ値に秘密鍵を掛けたものをそのデータの電子署名という．データの転送先は，データと共にその電子署名を入手し，電子署名を転送元の公開鍵で復号してハッシュ値を得ると同時に，データからもハッシュ値を得て，これらのハッシュ値を比較し，一致していれば，データは転送中に書き換えられていないことが確認できる．

2.2.3　電子証明書

データの転送中に，データとその電子署名及び転送元の公開鍵をそっくり入れ替えられると，なりすましが成功してしまう．これを防ぐために，データの転送元の公開鍵に第三者機関（認証局）が電子署名することにより，データの転送元を認証することができる．これを電子証明書という．

3　保護スキーム参加者の役割と許可証（パーミット）

保護スキーム中で，参加者の役割とやりとりされる各種情報は以下のとおり．これらを図で表したものが Fig. 1 である．

3.1　スキーム管理者（SA）

スキーム管理者（Scheme Administrator：SA）はスキーム全体の管理者であり，IHO がその役を担う．SA はスキームに参加する表示装置製造業者（Original Equipment Manufacturer：OEM）やデータ提供者（Data Server：DS）からの申請により，OEM には OEM の固有番号（M_ID）と鍵（M_KEY）の組を，DS にはさらに電子証明書を発行し，認証局の役も担っている．

3.2　表示装置製造業者（OEM）

OEM はスキーム参加を SA に申請し，M_ID と M_KEY の組を受け取る．また，表示装置に固有の番号（HW_ID，実は鍵）を付与し，これらを元にユーザパーミット（3.5 節で後述）を作製する．

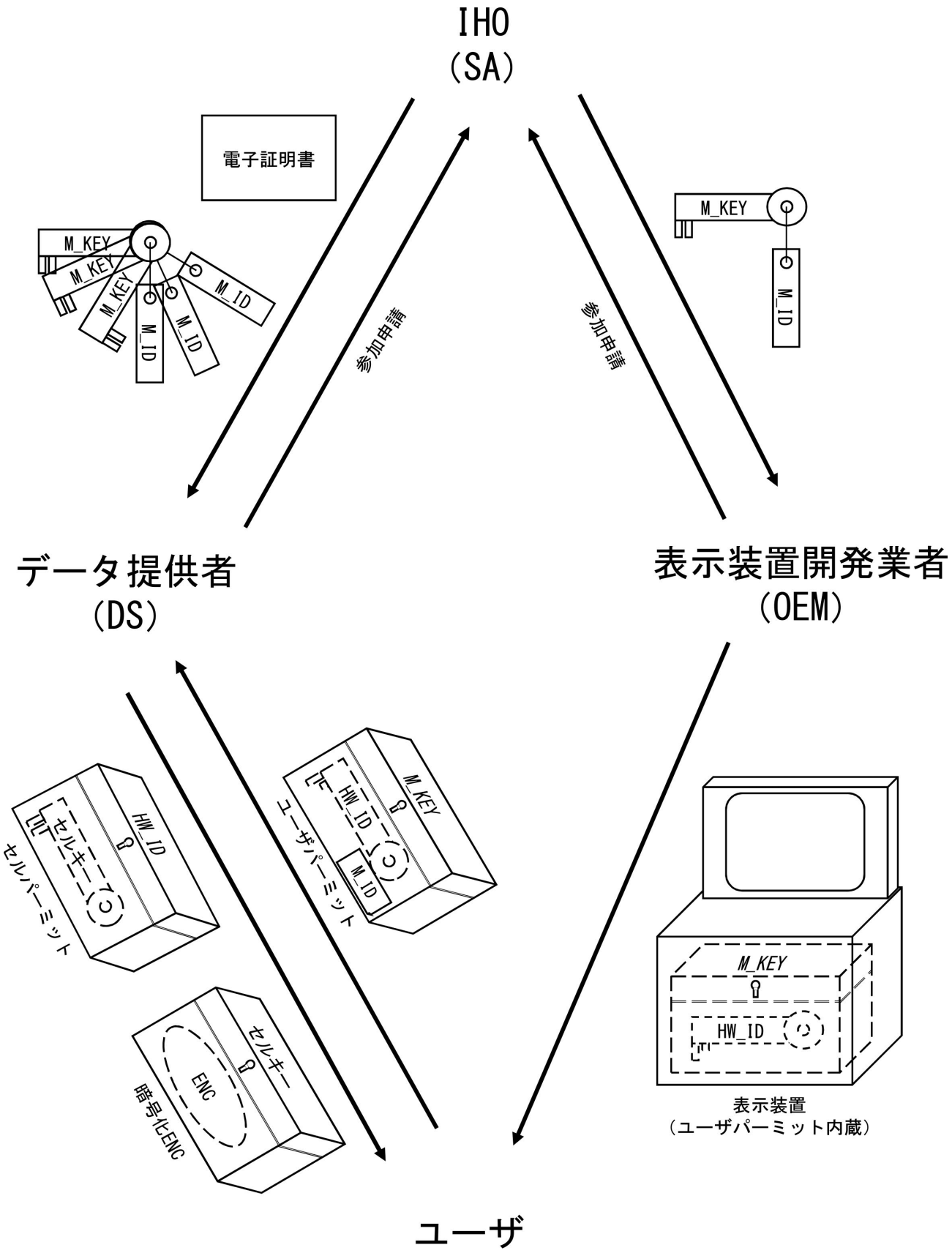


Fig. 1. Data flow among players in data protection scheme.
図 1. データ保護スキーム参加者間のデータフロー.

3.3 データ提供者（DS）

DS は RENC，水路機関などがその役を担い，我が国では複製頒布者である．DS は，スキーム参加を SA に申請し，M_ID と M_KEY の組の表（スキームに参加している OEM にどの M_ID と M_KEY を割り当てたかを示したもの，M_ID と M_KEY は 1 対 1 対応であり，ユーザパーミット（3.5 節で後述）から HW_ID を取り出す際に，使用する M_KEY をこの表から特定する）及びその DS の電子証明書を受け取る．DS は，データセット（製品）を製品キー（S-63 ではセルキーと呼ぶ）で暗号化し，これを磁気媒体や通信などで顧客に提供する．また，別途，顧客から契約する製品の情報とユーザパーミットを受け取り，これを元にデータパーミット（3.6 節で後述）を作製し，顧客に提供する．

3.4 顧客

データセットの利用者である顧客は必要な製品の情報とユーザパーミットを DS に送り，データパーミットを受け取る．データセットの復号や改ざんされていないことの確認は表示装置が自動的に行うため，顧客がこれらで使用する鍵を意識することはない．顧客の表示装置は，HW_ID を使ってデータパーミットから製品キーを復号し，製品キーからデータセットを復号する．また，復号されたデータセットは，表示装置の内部形式に変換されたもの（ENC では SENC）のみが記録され，復号された製品キーと共にただちに消去される．

3.5 ユーザパーミット

ユーザパーミットは，HW_ID を M_KEY で暗号化し，M_ID を付加したものであり，顧客固有である．

3.6 データパーミット（セルパーミット）

S-63 では，暗号化の対象が ENC だけであったため，データの許可証をセルパーミットと呼んでいるが，S-100 では他の製品も暗号化の対象となり得るため，セルパーミットと呼び続けるのは不適切であり，データパーミットと呼ぶ．データパーミットは，製品キーを HW_ID で暗号化したものに，有効期限を付加したもの．顧客固有である（DS は，M_ID と M_KEY の組の表を利用し，ユーザパーミットから HW_ID を取り出す）ことから，他の顧客と使い回すことができない．このため，DS は顧客毎に製品を暗号化することをせず，暗号化された製品を大量に複製することができる．

4 S-63 から S-100 Part 15 への変更点

これまで述べてきたように，S-100 Part 15 は S-63 を基本的に踏襲しているが，細部に変更を加えている．以下に変更点を述べる．諸元の比較は Table 1 のとおり．

4.1 暗号化アルゴリズム

S-63 と S-100 Part 15 のどちらも暗号化前にデータセットを ZIP 圧縮する．

S-63 では製品の暗号化に blowfish というアルゴリズムを用いているが，S-100 Part 15 では AES（Advanced Encryption Standard）というアルゴリズムを用いる．どちらも，データセット（任意長）を固定長のかたまり（ブロック）に分割（それぞれ 8 bytes と 16 bytes），次々と変換し，連結していく．データセットがこの固定長の整数倍でない場合，最後のかたまりに対するダミーの詰め物によって整数倍化される．この詰め物は復号された後，取り除かれる．

4.2 鍵の長さ

暗号化に用いる各鍵の長さは，S-63 では 40 bits だったが，S-100 Part 15 では 128 bits である．

4.3 パーミット

4.3.1 ユーザパーミット

S-63 では，M_KEY を鍵として，40 bits の HW_ID を blowfish アルゴリズムで暗号化（結果は 8 bytes になる），暗号化された HW_ID の

Table 1. Parameter comparison between S-63 and S-100 Part 15.
表 1. S-63 と S-100 Part 15 の諸元の比較.

	S-63 Ed1.2.1	S-100 Ed4.0.0 Part15
暗号化アルゴリズム	blowfish	AES
暗号化ブロックの長さ	8 bytes	16 bytes
製品キー(セルキー)の長さ	40 bits	128 bits
M_KEYの長さ	40 bits	128 bits
HW_IDの長さ	40 bits	128 bits
暗号化されたHW_IDの長さ	16進16桁	16進32桁
暗号化された製品キーの長さ	16進16桁	16進32桁
M_IDの長さ	16進4桁	16進6桁
暗号化の対象ファイル	データセットファイル	製品仕様で定める
データパーミットのファイル形式	TXT	XML
公開鍵・秘密鍵の長さ	512 bits	1024 bits
ハッシュ生成アルゴリズム	SHA-1	SHA-256
ハッシュ値の長さ	160 bits	256 bits
電子署名生成アルゴリズム	DSA	DSA
電子署名の対象ファイル	データセットファイル	交換セット中の全てのファイル
電子署名の所在	署名ファイル	カタログファイル中
電子証明書の所在	最上位フォルダ	カタログファイル中

チェックサム（4 bytes）を計算し，M_ID（2 bytes）を付加する．結果を 16 進 28 桁で表記する．

S-100 Part 15 では，M_KEY を鍵として，128 bits の HW_ID を AES アルゴリズムで暗号化（結果は 16 bytes になる），暗号化された HW_ID のチェックサム（4 bytes）を計算し，M_ID（3 bytes）を付加する．結果を 16 進 46 桁で表記する．

S-63 及び S-100 Part 15 中のユーザパーミットの例示を各要素に分解すると Fig. 2 のようになる．

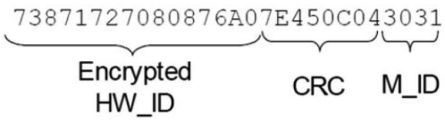
4.3.2　データパーミット（セルパーミット）

データパーミットは，S-63 では TXT 形式，S-100 では XML 形式である．

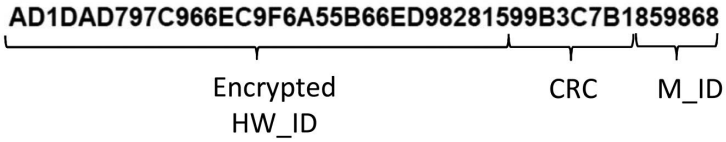
S-63 では，まず，ヘッダーが 2 行あり，その後にセルパーミットの内容が続く．これは，セル名 8 文字，有効期限年月日 8 文字，HW_ID で暗号化されたセルキー 1（現在使用中）及びセルキー 2（将来予定）がそれぞれ 16 進 16 桁，HW_ID で暗号化されたチェックサム 16 進 16 桁から成り，さらに，コンマ区切りの管理情報が続く．

S-100 では，まず，ヘッダー部があり，その後にデータパーミットの内容が続き，最後にデータパーミット全体に対する電子署名が付く．データパーミットの内容は，製品毎にまとめられ，また，ファイル毎に，ファイル名，製品の版番号，有効期限年月日，HW_ID で暗号化された製品キーが 16 進 32 桁から成る．S-63 のセルパーミットと異なり，情報は XML タグで区切られ，製品キーは 1 つだけであり，チェックサムは付いてい

S-63のユーザパーミット



S-101のユーザパーミット



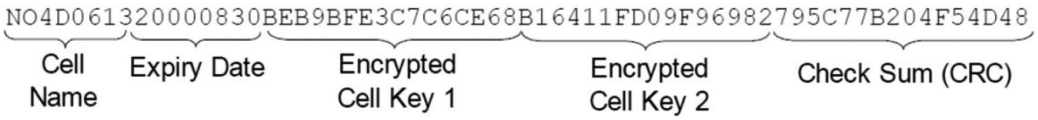
S-63のセルパーミット（ヘッダー部分）

```
:DATE 20080809 11:11
:VERSION 2
```

S-100のデータパーミット（ヘッダー部分）

```
<header>
    <date>20180607 14:11:59</date>
    <dataserver>primar</dataserver>
    <version>1.0.0</version>
    <userpermit>80352805938502220302542</userpermit>
</header>
```

S-63のセルパーミット（フィールド部分）



S-100のデータパーミット（フィールド部分）

```
<permit>
    <filename>101GB40079ABCDEF.000</filename>
    <editionNumber>10</editionNumber>
    <expiry>20183112</expiry>
    <encryptedKey>2011AA840D5C2204</encryptedKey>
</permit>
```

Fig. 2. Examples of permits and their components.
図 2. パーミットの例とその要素.

ない.

4.4 電子署名

S-63 ではハッシュ生成アルゴリズムにハッシュ関数の 1 種である SHA-1 を利用しているが，S-100 Part 15 では，SHA-2 の一種である SHA-256 を利用する（SHA-1 は弱点が発見されたため，暗号の事実上の世界標準である NIST（National Institute of Standard and Technology：アメリカ国立標準技術研究所）Special Publication 800-131A 中で，新規採用を行ってはならないとされている）.

S-63 では，ひとつのデータセットファイルがひとつの電子署名ファイルを持ち，交換セット中の他のファイルは電子署名を持たないとされている（このため，データセット中に含めることが適当ではない，長文の文字情報や説明図などを，サポートファイルと呼ぶ別ファイルとしておき，データセット中から参照することにしているが，これらは電子署名の対象ではない）. また，電子署名ファイルのファイル名は対応するデータセットファイルの航海目的を表す数字（ファイル名の

3 文字目）の 1 ～ 6 をアルファベットの I ～ N に置き換えたものとし，電子署名ファイルはデータセットファイルと同じディレクトリに置かなければならないと定めている．

S-100 では，S-100 交換セット中のファイルは，その種類毎にカタログファイル中の所定のメタデータ中に（データセットファイルであれば S100_DataSetDiscoveryMetadata に，サポートファイルであれば S100_SupportFileDiscoveryMetadata に）情報を記載することとされており，全てのファイルに対し電子署名を記載しなければならないとされている．S-100 の電子署名メカニズムは，データセットのみでなく，地物カタログや描画カタログにも用いられる．

4.5 カタログファイル

カタログファイルは，ファイルの所在情報ほかを記述したファイルであり，その内容は大まかに基準（S-57 または S-100 Part 4a）中で定められ，さらに各製品仕様で制限がかけられる．カタログファイルは，S-57 では ISO8211 で，S-100 では XML でエンコードされる．

S-57 ではカタログファイルに，全てのファイルのフルパス，セルの範囲，チェックサム，コメント程度しか記載できず，データ管理に十分な情報をこれに記載することができなかったため，S-63 中で，その他の管理ファイル（4.6 節で後述）を作り，それに情報を記載するよう定めていた．また，S-57 ENC は逐次更新方式を採用しており，これは，海図としての情報全体を含むベースファイルに対し，補正部分のみを含む差分ファイルを適用することでなされる．改版されると，版番号（EDTN）が 1 つ大きくなり，それまでの補正情報は全て含まれたと見なされ，また，差分ファイルは更新番号（UPDN）が付され，その番号順に適用されなければならず，途中を飛ばしたり，遡ったりすることはできない．EDTN や UPDN は最新維持上重要な情報であるが，S-57 ENC の製品仕様では，これらは，データセットファイル中に記載されるだけで，カタログファイル中に記載されることにはなっていない．そこで，S-63 で，これらの情報をその日付と共にカタログファイルのコメントサブフィールドに記載することとし，データセットの復号前にこれらの情報を得られることで，最新維持の際の表示装置の負荷を減らしている．

S-100 ではカタログファイル中にこれらの情報を記載できるようになっており，これまでに刊行された S-100 製品仕様中に S-63 で使われたような管理ファイルに関する記述はない．

4.6 S-57 ENC のその他の管理ファイル

S-63 には，複数の DS からのデータ提供や，大容量媒体でのデータ提供を，より管理し易くするために，以下のファイルを DS が交換セット中に置くことが記述されている．これらは，データ保護のためとは言い難いため，これ以上本稿では触れない．

・PRODUCT.TXT
・SERIAL.ENC
・STATUS.LST
・ENC.PMT
・MEDIA.TXT

5 考察

5.1 暗号の強さの向上

暗号が解かれにくいことを暗号の強さといい，鍵の長さを指数として強くなる．暗号を解く方法のひとつに「総当たり攻撃」と呼ばれるものがあり，可能な組み合わせを全て試すという単純な方法で強い暗号でも数学的には解ける（実用的には，膨大な計算機資源が必要とされるため，解けないと見なせる）．仮に，1 秒間に 1 京（10 の 16 乗）通りの組み合わせを試すことができる計算機が 1 台あり，これを総当たり攻撃で製品の暗号解読に用いたとすると，S-63 では約 2 ミリ秒，S-100 Part 15 では約 1000 京年の時間がかかる（人の一生が 100 年程度，宇宙開びゃく以来 200 億年経っていないことと比較しても，後者は現実的な時間ではない）と見込まれる．

5.2 IMO におけるサイバーセキュリティの検討

IMO は，海運へのサイバー攻撃に警戒を強めており，IMO での検討は IHO のデータ保護スキームにも影響するため，注意しておく必要がある．ここで，S-101 ENC の実用化を目前に控え，S-57 ENC を保護の対象とする S-63 に，ECDIS の改修を必要とするような，大規模な改訂は考えにくいものの，全く否定することはできない．一方，実用版の S-100 製品仕様がまだ開発中であることから，S-100 Part 15 には容易に改訂が加えられると考えられる．

5.3 デュアルフュエル ECDIS

IHO は，S-101 ENC が刊行され始めても，ただちに S-57 ENC を廃止することなく，しばらくは両 ENC が共存する期間があるとしており，この期間中は，両 ENC とも読み込める「デュアルフュエル ECDIS」を構想している．DS がどのように，両 ENC，さらに他の S-100 製品を提供していくか，特に関係者の混乱を防ぐかは，IHO 及び関係機関において今後の検討を必要とする．

6 まとめ

S-100 Edition 4 Part 15 に記述されたデータ保護スキームは，基本的に S-63 を踏襲しつつ，細部において必要な変更が加えられているが，S-100 Edition 5 でさらに細部に変更が加えられる可能性がある．また，IHO における S-100 を基にした製品仕様の開発はまだ途上であり，これまでに刊行された試験用の製品仕様には，製品に暗号を掛けるかどうかに関する記述がなされていないものが多い．暗号化を導入するかどうかは実用版の製品仕様（S-100 Edition 5 を基にする）で記述されることになるため，データ保護の実装はこれらを確認する必要がある．

文　献

IHO（2000）S-57 Appendix B.1“ENC Product Specification”Edition 2.0.

IHO（2018）S-100“Universal Hydrographic Data Model”Edition 4.0.0.

IHO（2018）S-101“ENC Product Specification”Edition 1.0.0.

IHO（2020）S-63“IHO Data Protection Scheme”Edition 1.2.1.

要　旨

S-100 製品のためのデータ保護スキームは，S-100 Part 15 として，2018 年刊行の Edition 4 に初めて記述された．これは S-63 を基に開発されたものだが，セキュリティを強化すると同時に，データ管理も改善された．S-100 製品のための実装には，なお細部の検討が必要である．