マルチメディア通信と分散処理 30－5
（1986. 7. 25）

暗号関連技術の標準化動向

白石 旭
NTT 電気通信研究所

本稿では、TC97／SC20及びTC68／SC2において検討されている、暗号技術や暗号を利用したメッセージ認証技術、デジタル署名技術等の暗号関連技術の標準化動向、及び、TC97／SC21／WG1において検討されている、OSI（開放型システム間相互接続）環境におけるセキュリティ・アーキテクチャの標準化動向について述べる。更に、暗号関連技術の標準化に絡む安全性問題を中心とした標準化経緯とTC97を中心する最近の動きについて紹介する。

The trend of the standardization for cryptographic techniques

Akira SHIRAISHI
NTT Electrical Communication Labolatories
Yokosuka Post Office.box 8,238 JAPAN

This paper introduces the activities of the standardization for cryptographic techniqes on ISO (INTERNATIONAL ORGANISATION FOR STANDARDIZATION). The encipherment and digital-signature algorithms are investigated in TC97/SC20 ,and message-authentication algorithm is in TC97/SC20 and TC68/SC2. The security architecture in OSI (Open Systems Interconnection) environment is investigated in TC97/SC21/WG1. Furthermore ,this paper presents the problems of safety in standardization for cryptographic techniqes and current activities about it on TC97.

１．はじめに

暗号関連技術としては、情報を隠蔽できる暗号技術以外に、それを応用して、情報の内容が改ざんされていないかを確認できるメッセージ認証（データ完全性）や情報の作成元（署名者）を確認できるデジタル署名などの技術がある。本論では、国際標準化機構（ＩＳＯ）におけるＴＣ９７／ＳＣ２０での活動を中心として、これらの技術に関する標準化動向について述べる。

２．標準化の背景

暗号関連技術は、コンピュータやネットワーク（回線）に存在する情報を、盗聴／改ざんあるいは不正情報の混入などの不正なアクセスから保護するのに有効である。これらの保護機能は、ネットワークに接続された端末や計算機等の装置（ノード）相互間で合意した同様の処理機構（例えば、暗号化機能では鍵配送手順と暗号アルゴリズム等）を具備することによって実現される。（不特定を含めた）多数のノードで構成されるコンピュータ・ネットワークシステムにおいては、ノード毎に保護機能が異なると、各ノードは相手ノード毎の保護機能を必要とするため、開発や運用費の面でその実現が困難となる。従って、各ノードが保護機能を安い費用で容易に実現できるように、これらの技術を標準化する必要がある。

暗号における従来の技術は、暗号アルゴリズムが秘密であったことから、その標準化が不可能であった。しかし、アルゴリズム公開形暗号方式の開発によって米国内で標準化が図り得たこと、また一方で、国際的ネットワークにおけるセキュリティの重要性の認識が世界的に高揚してきたことなどを契機に、暗号関連技術の国際標準化の動きが活発化してきた。

３．暗号関連技術の国際標準化機構（ＩＳＯ）

ＩＳＯでは、現在３つの機関で暗号関連技術の標準化を進めている（図１）。

機関名	検討内容
ＩＳＯ／ＴＣ９７／ＳＣ２０	暗号関連アルゴリズム 暗号関連技術のＯＳＩへの適用
ＩＳＯ／ＴＣ９７／ＳＣ２１／ＷＧ１	セキュリティ・アーキテクチャ （各レイヤのセキュリティサービス）
ＩＳＯ／ＴＣ６８／ＳＣ２／ＷＧ２	銀行システムのメッセージ認証

図１　暗号関連技術の国際標準化機関と検討内容

情報処理システムの標準化を担当するＩＳＯ／ＴＣ（Technical Committee）９７では、当初はＴＣ９７のＷＧ（Working Groop）１で暗号アルゴリズムの検討を進めてきたが、その後、暗号技術を応用したセキュリティ技術であるデータ

完全性やデジタル署名等の検討項目が新たに追加され、1984年からはＳＣ（Sub Committee）２０としてその組織が強化された。また、情報処理システム間の相互接続に必要なネットワーク・アーキテクチャの標準化を担当するＳＣ２１では、ＯＳＩ（開放形システム間相互接続）基本参照モデルの中にセキュリティアーキテクチャを追加するために、1983年からその検討を進めている。

一方、最もセキュリティ対策が重要と思われる銀行システムの標準化を担当するＩＳＯ／ＴＣ６８では、情報の完全性を確認できるメセージ認証技術の標準化を進めており、最近になってＴＣ９７とのリエゾンを図るようになってきた。

４．各標準化機関での標準化内容と状況

（１）ＴＣ９７／ＳＣ２０

本機関では、「データ暗号技術」（暗号アルゴリズムとその利用）と題して、３つのＷＧが以下のような内容を分担している（表１）。

①ＷＧ１：秘密鍵暗号とその利用
②ＷＧ２：公開鍵暗号とその利用
③ＷＧ３：通信アーキテクチャにおける暗号の利用

表１　ＳＣ２０の課題と標準化段階

WG	課　題	段階	記　事
WG１	ＤＥＡ１（ＤＥＳ）	ＩＳ	ISO8227(61.5)（独、仏反対）
	ＦＥＡＬ（ＮＴＴ開発暗号）	WD	ｱﾙｺﾞﾘｽﾞﾑの形式検査中
	６４ビット暗号利用モード	ＩＳ	ISO8372(61.5)（独、仏、ｵｰｽﾄﾘｱ反対）
	Ｎビット暗号利用モード	WD待ち	WD：Working Draft
	相手認証（秘密鍵系）	WD待ち	
	データ完全性（秘密鍵系）	WD待ち	
WG２	ＤＥＡ２（ＲＳＡ法）	ＤＰ	DP9307(61.5)
	公開鍵系標準化調査	注１	注１：技術調査報告('86.7予定)
	相手認証とデータ完全性（公開鍵系）	WD待ち	
	デジタル署名	WD待ち	
WG３	ＯＳＩレイヤ１への適用法	ＤＰ	DP9160(61.1)１ビットＣＦＢモード
	ＯＳＩレイヤ３への適用法	WD待ち	
	ＯＳＩレイヤ４への適用法	WD	ＡＮＳＩ規格(ﾚｲﾔ4の暗号:X3T1-85-50.3、ﾚｲﾔ6の暗号/ﾒｯｾｰｼﾞ認証/相手認証:X3T1-81-106.19)資料を叩き台
	ＯＳＩレイヤ６への適用法	WD	

現在、ＷＧ１で２件の国際規格（ＩＳ：International Standard）化とＷＧ２およびＷＧ３で各１件の草案（ＤＰ：Draft Proposal）化がなされている。

・ＩＳ０８２２７：ブロック暗号アルゴリズムに関する規格であり、ＤＥＳ（Data Encryption Standard：米国ＮＢＳ標準）に準じた暗号アルゴリズム（ＤＥＡ１：Data Encryption Algorithm No１）を規格化している。

・ＩＳ０８３７２：64ビット暗号アルゴリズムの利用モードに関する規格であり、ＮＢＳ標準の４種モード（ＥＣＢ：Electronic Codebook、ＣＢＣ：cipher block chaining、ＣＦＢ：cipher feedback、ＯＦＢ：output feedback）にほぼ等しい内容を規格化している。

・ＤＰ９１６０　：ＯＳＩにおける物理レイヤでの暗号利用に関する規格であり、ＤＴＥ－ＤＣＥ間に接続する暗号装置（但し、暗号機能がＤＴＥ、ＤＣＥに含まれる場合を含む）の採用暗号アルゴリズムと利用モード、回線インタフェース（Ｖ．24、Ｘ．20他）バイパス（暗号機能切り離し）制御法等を規格化している。

・ＤＰ９３０７　：公開鍵暗号アルゴリズムであるＲＳＡ（開発者の頭文字）をＤＥＡ２として規格化している。

なお、後述する様に、暗号アルゴリズムの標準化に対する否定論の動きが最近活発化したため、標準化作業は現在中断している。

（２）ＴＣ９７／ＳＣ２１／ＷＧ１

本機関ではＯＳＩ基本参照モデルを審議しており、そのAd Hocグループの検討によって、基本参照モデルにセキュリティ関連アーキテクチャが追加（1984.10）され（表２）、ＩＳ０７４９８（ＯＳＩ基本参照モデルの国際規格）の補遺（パート２）としてＤＰ化されている。

表２　暗号関連セキュリティサービスとメカニズムとの対応及びレイヤの位置

Service \ Mechanism	Encipherment	Digital Signature	Data Integrity
Peer Entity Authentication	[3,4,6]	[3,4,6]	－
Data Confidentiality	1,2,3,4,6	－	－
Data Integrity	[3,4,6]	[3,4,6]	3,4,6
Data Origin Authentication	[3,4,6]	[3,4,6]	[3,4,6]
Non-repudiation	－	[6]	[6]

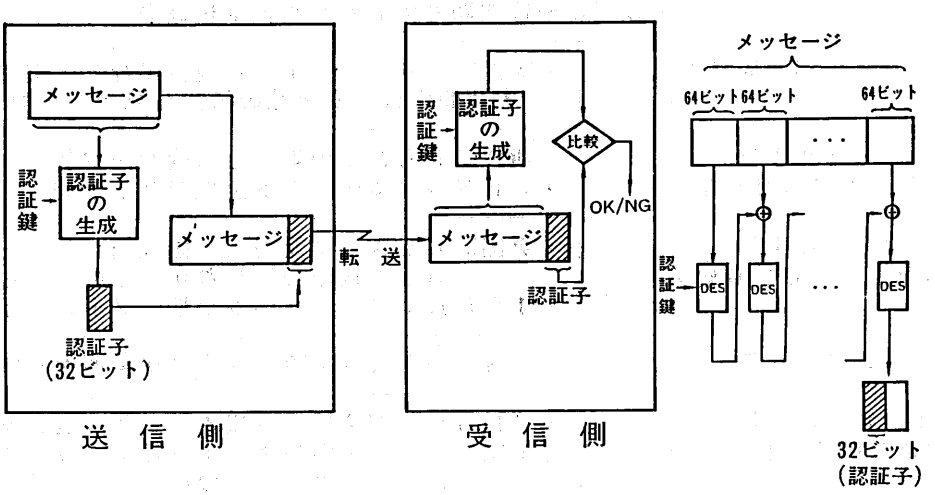
（凡例）　数：ﾚｲﾔ番号（[]無し：適切なﾒｶﾆｽﾞﾑ、[]有り：何れかが適切なﾒｶﾆｽﾞﾑ）

・ＩＳＯ7498／ＤＰ　Part2　：ＯＳＩにおけるセキュリティサービスを６分類（Peer Entity Authentication、Data Confidentiality、Data Integrity、Data Origin Authentication、Access Control、Non-repudiation）の１４項目から整理し、各サービスの実現に適用するメカニズム（暗号、デジタル署名等）や各ＯＳＩレイヤにおいて提供するサービス等の対応を規格化している。

なお、各サービスを実現するメカニズムである暗号およびデジタル署名等のアルゴリズムに関する規格化はＳＣ２０に委ねている。

（３）ＴＣ６８／ＳＣ２／ＷＧ２

本機関では、銀行システムにおけるメッセージ認証（Message Authentication）を検討しており、現在では秘密鍵暗号の適用を前提としたメッセージ認証（図２）に関する１件のＩＳＯ化と３件のＤＩＳ化及び１件のＤＰ化がなされている。



(a) 手　順　　(b) 認証子生成部

図２　メッセージ認証方式

・ＤＩＳ８７３０：メッセージ認証標準化への要求内容として、認証手順（認証子送受信や照合等）、認証子構成要素（認証子生成日付け、メッセージＩＤ等）とフォーマット等を規格化している。
・ＩＳＯ８７３１（パート１）：暗号アルゴリズム（ＤＥＡ１）を用いたメッセージ認証アルゴリズムを規格化している。
・ＤＩＳ８７３１（パート２）：英国提案のメッセージ認証アルゴリズム（ＭＡＡ：Message Authentication Algorithm）を規格化している。
・ＤＰ８７３１（パート３）：独国提案のメッセージ認証アルゴリズム（ＤＳＡ：Decimal Shift and Add）を規格化している。
・ＤＩＳ８７３２：メッセージ認証用の鍵管理方式（鍵の安全保管／手作業または自動配送等）を規格化している。

なお、各認証アルゴリズムの安全性検証は、リエゾンにあるＳＣ２０のＷＧ１において実施された。

５．暗号化関連技術の標準化に対する問題点と最近の動き

暗号技術を標準化するにはそのアルゴリズムを公開する必要があり、公開すれば暗号破りの攻撃の的になる恐れがある。このために、標準化されたアルゴリズムの安全性に寿命を定めて定期的に更改するとすれば、標準化に馴染みにくい。このように、暗号関連技術（特に暗号アルゴリズム）の標準化には、安全性の絶対的保障が困難であるという宿命からくる、セキュリティ特有の問題がある。

また、暗号技術は国家の政策が絡む機密領域の問題であるとして、標準活動を行う幾つかのメンバ国の活動には政府機関が介入しているため（現在では米国が顕著である）、規格化賛否への真の理由には政策的な配慮が絡んでいる感がある。

このらの問題は、標準化作業を進めて行く段階で次第に議論の的となってきた。以下では、安全性問題を中心としたＳＣ２０での標準化経緯と最近の動きについて述べる（表３）。

表３　安全性問題を中心とした標準化経歴

１９８１年（ＷＧ１）	・英国⇨ＤＥＡ１をＩＳＯ規格候補として提案 （本期間中は、安全性の議論は見当たらない）
１９８４年１月 （第１回ＳＣ２０総会）	・西独⇨ＤＥＡ１の安全性に疑問を提起 ・ＣＥＳＧ（英国）に安全性テスト依頼
１９８５年１月 （第２回ＳＣ２０総会）	・英国⇨ＤＥＡ１に反対（米国政府がＤＥＳ製品をＢＴへ輸出許可しなかったのが理由） ・１０月迄でＣＥＳＧの安全性テストの中止を決定
１９８５年５月	・ＮＳＡ→ＡＮＳＩ書簡（安全保障期間1988年迄）
１９８６年１月 （第３回ＳＣ２０総会）	・ＣＥＳＧの安全性調査報告（15年程度は安全） ・米国⇨ＤＥＡ１のＤＩＳ化を保留（ＮＳＡ方針によりＡＮＳＩ内の反対派が急増？） ・仏国⇨ＤＥＡ１に反対(NSA/CESG内容矛盾を理由)
１９８６年５月 （ＴＣ９７会議）	・米国⇨暗号アルゴリズム標準化中止を提案 ・ＩＳＯ理事会へ判断を委任

（１）安全性問題を中心とした標準化経緯

第１回ＳＣ２０総会（1984.1）において、ＤＥＡ１の規格化は、その安全性テストをＣＥＳＧ（British Communication and Electronics Security Group）に一年の期限で依頼し、その報告を待って進めることとした。しかし、第２回総会では、テストの見通しが得られず継続しても意味が無いとの判断からその作業を1985年10月で終了し、暗号アルゴリズムの安全性対するＳＣ２０の姿勢を以下の様に定めて、規格化の作業を開始することが決議された。

①国際的な場に公開されて３年以上経過したアルゴリズムをＩＳ化する。

②安全性は、ＳＣ２０では保障せず、ユーザの選択に委ねる。

この間に、ＤＥＳを開発し且つ国内標準化を行った米国が、これまでの規格化賛成から保留の姿勢に転じた。また、仏国も、米国国家安全保障局（ＮＳＡ）の表明書簡（図３）を理由とした規格化反対を行った。

ＮＳＡ書簡（ＡＮＳＩ議長へ）	ＡＮＳＩ議長見解
＊現在でも安全であるが、公表１０年以上経過している。従って、１９８８年まで安全性を保証するが、次期見直し期間（～１９９３年）までの延長は出出来ない。 ＊幾つかのアルゴリズムを開発している（未公表）が、ＮＳＡが進めているＣＣＥＰ（商用コンピュータ安全保証計画）の参加者は、確認書による了解のもとに知る事ができ、さらにＣＣＥＰが認証したデバイスを使用出来る。また、その輸出は米国の国際企業が使うためにのみ許可される。	＊新しい暗号アルゴリズムへの秩序ある移行計画を持つ必要がある。 ＊ＮＳＡの安全保証が得られなくても、ＤＥＳ製品の使用は、政府や民間機関でしばらくの間は続くと予想される。

図３　ＮＳＡ書簡とそれに対するＡＮＳＩ議長見解

（２）ＴＣ９７における最新の動き

暗号アルゴリズムの標準化に反対の立場をとるＮＳＡの意向を受けた米国代表（ＡＮＳＩ所属）は、ＴＣ９７会議（1986.5）において、

①ＳＣ２０は暗号アルゴリズムの標準化は行わない
②ＳＣ２０は暗号アルゴリズムの登録制度を審議する
③暗号アルゴリズムの規格化の扱いは中断する

こと、を提案した。

本会議では、上記提案の判断は非技術的問題であるとして、ＩＳＯ理事会に委ねることが採決された。したがって、ＳＣ２０議長は、当面のＳＣ２０の作業方針を以下のように示した。

①ＳＣ２０／ＷＧ１では、当面暗号アルゴリズムの登録制度について審議することとし、暗号アルゴリズム自体の規格化を一時中断する
②また、ＴＣ９７の決議に基づき、ＳＣ２０／ＳＣ６／ＳＣ２１間の作業課題の分担を見直しする（1986.9迄）ため、従来ＷＧ３で分担していた「ＯＳＩレイヤへの適用法（具体的にはプロトコル）」の作業を一時中断する

５．おわり

以上の様に、ＳＣ２０の標準化活動は、最近に至って全面見直しの様相を呈してきている。これは、各国におけるセキュリティの重要性が高まるにつれて、セキュリティはその内容自体の秘密がセキュリティであるという、標準化にそぐわない困難な問題を有していることを認識しだしたからであろう。ＩＳＯ理事会の判断を見守る必要があるが、今後は、暗号アルゴリズムの登録制度や（アクセス制御を含めた）セキュリティサービス関連プロトコルの検討が標準化活動の中心になるものと思われる。