暗号文通信システムについての歴史的考察: 古典インド文献にみる原初形態

相場 徹† 山根 信二‡
aiba@vacia.is.tohoku.ac.jp s-yamane@soft.iwate-pu.ac.jp

†東北大学大学院情報科学研究科
‡岩手県立大学ソフトウェア情報学部

概要 暗号の歴史は軍事や外交といった国家レベルの文脈において語られることが多い。しかし、そのような議論は、個人的なレベルでの暗号利用の歴史についての視点を欠落させてしまう。

本発表では、インド古典のカーマスートラ、およびヤショーダラによる注釈文献を取り上げ、そこで述べているとされる暗号の内容および用途についての検討をおこなう。この検討の結果、ヤショーダラ注における暗号は軍事・外交といった国家レベルの用途ばかりを想定していたものではなかったことを示す。そして、前近代において民間レベルでの秘密通信が存在しえたことが、現代においてどのような意義を持つかについて論じる。

キーワード 暗号史, サンスクリット語, カーマスートラ, 換字法暗号

Historical Perspective on the Cryptography Technology: Its Primordial Form in Classical Sanskrit Literature

Tooru Aiba† Shinji Yamane‡
aiba@vacia.is.tohoku.ac.jp s-yamane@soft.iwate-pu.ac.jp

†Graduate School of Information Sciences, Tohoku University
‡Faculty of Software and Information Science, Iwate Prefectural University

Abstract The status of cryptography is often offered as the national security issue. Such viewpoint fails to explain the status and history of non-governmental or personal use of cryptography. Today all Internet users in all countries can access to uniform strong cryptographic technology. It is neither the first time nor the last time. This situation is similar as the cryptography technology in pre-modern.

Reading the description of *Kāmasūtra* and its commentaries, we examine the original form of non-governmental secret writing and the similarities to the 21st century. We also reports the resent studies on the history of cryptography by Sanskrit researchers.

Keywords history of cryptography, Sanskrit, Kāmasūtra, substitution cipher

1 はじめに

暗号は、近代以前においては専ら軍事や外交において用いられていた。しかし近年のパーソナルコンピュータとインターネットの普及によって、一般の人たちも暗号を使うようになってきた — 暗号の歴史は、このような枠組で語られることが多い。たとえば郵政省研究会による「21世紀デジタル社会の暗号政策への提言」[12] もこれと同様の歴史認識を示している。

それに対し、報告者らは、暗号についての歴史的考察である「キーエスクロー以降の通信傍受: 歴史的分析」[11] において、近代以前においても軍事・外交以外の目的での暗号利用の事例があった可能性について言及し、暗号史における民間暗号の位置づけについての再検討を試みた。なかでも古代インドにおけるカーマスートラ *(Kāmasūtra; KS)* での暗号の利用に関する記述が、軍事・外交以外での民間レベルでの暗号の利用例になるであろうことを指摘した。

この報告者らの指摘は、基本的には Kahn[4] に基づいておこなったものであった。しかし、Kahn の古代インドの暗号に関する記述について詳細に検討をおこなおうとした場合、彼自身が古典文化に関する研究者でないことに由来する記述の曖昧さが目立ち、史料としての情報量も不足している。

そこで本発表では、前近代における民間レベルでの暗号利用の一例として *KS* およびそれに対するヤショーダラ (Yaśodhara) による注釈書ジャヤマンガラー (*Jayamaṅgalā*)[1]に注目し、これらの文献中で Kahn が言及した箇所について、その記述内容および背景を Kahn よりもさらに詳しく検討・紹介することとしたい。これにより本発表は、 Kahn による暗号史の補足をおこなうものとなろう。

発表の内容であるが、まず *KS* 本文およびヤショーダラ注の原典を確認するところから始める。次に、ヤショーダラ注で紹介されている暗号アルゴリズム (換字法) の強度についての情報を示したのち、暗号利用がどのような用途を想定したものであったかに関して検討する。そして、ヤショーダラが示した暗号の記述が、暗号史においてどのような位置づけがなされるかについての考察をおこなう。

[1]以後「ヤショーダラ注」と呼ぶ。

2 *KS* と Kahn

KS およびヤショーダラ注の内容についての検証を始める前に、これらのテキストについて、また Kahn がこれらテキストをどのように紹介しているかについて簡単に紹介しておく。

2.1 *KS* とヤショーダラ注

古代インド人においては、ダルマ「法」・アルタ「利」・カーマ「愛」の三つが人間的な努力の目的とされており、この各々について多くの経典が作成された。カーマについても、カーマ・シャーストラ文献と称される多量のテキストが作成されたが、その中でも、現存するものの中では最古で、またおそらく最も有名なものが *KS* である。著者はヴァーツヤーヤナ (Vātsyāyana) とされ、作成年代は一般に 4 世紀頃と考えられており、たとえば岩本 [2] はこの著作の成立年代を西暦 300 年前後と推定している。

また、この *KS* とは別に、*KS* の内容について逐語的に注釈をおこなっている注釈文献が存在している。Kahn や本発表が参照している注釈文献はヤショーダラ作とされるジャヤマンガラーである。彼が活躍した年代について、Renou [7] は 13 世紀としている。この年代推定が正しいとすると、ヤショーダラによる注釈文献が作成されたのは、*KS* が作成されてから 1000 年近くも経過したのちのこととなる。それゆえ、ヤショーダラによる注釈は *KS* 本文の主旨を正しく伝えるものというよりは、彼が活躍していた時代において *KS* の内容がどのように理解されていたかを示すものと考えるべきであろう。

2.2 Kahn にみる *KS*

KS 1.3.16 節には、「女が娘のうちに学ぶべき 64 の技芸 (yoga)」なるものが列挙されており、その 46 番目に “mlecchita-vikalpā” (和訳本で

a	kha	gha	ca	ña	na	ya	ra	la
ka	ga	ṅa	ṭa	ṇa	ma	śa	ṣa	sa

表 1: “mūladevīya” における入替文字一覧

は「言語読解法」[3] あるいは「秘かに申合せた言葉の種々な使い方」[2]) なるものが存在している[2]。Kahn はこれこそが “secret writing” に関する記述であると説明している。

それでは “mlecchita-vikalpā” とはいったい何であるのか。Kahn は、ヤショーダラ注によってそれを説明している。すなわち “mlecchita-vikalpā” には “kauṭilīya” と “mūladevīya” という二つの種類があるが、この後者の “mūladevīya” が換字法暗号であり、表 1 に示す[3]ような換字表が用いられていた。ただし、この換字は単に一部の文字のみを入れ替えているだけで、他の文字については換字操作は一切おこなわれない。“mūladevīya” には、さらに会話レベルのものと、“gūḍhalekhya” と呼ばれる文書レベルのものとが存在している。

また古代インドにおいては、政治関係を主題にした物語などにおいて暗号が利用された場面がほとんど出てこないことから、暗号が広く利用されていたわけではなかったろうと Kahn は指摘している。

3 *KS* と “mlecchitavikalpā”

前節で紹介したような Kahn の紹介はどこまで信用できるものなのであろうか。本節では、実際に原典、とくに *KS* 本文を参照しながら “mlecchita-vikalā” とは何かについての調査をおこなう。

[2]Kahn はこれを 45 番目としており、*KS* 本文とは番号が異なっている。これは、おそらく Kahn が参照した Burton による翻訳の番号が間違っているか、Burton が、我々が用いた校訂本 [8] とは異なる系統の文献を用いていたかのいずれかと思われる。あるいは、*KS* の校訂本 [8] の註部分のナンバリングの間違いを引き継いでしまった可能性も考えられる。この註部分では、*KS* 本文ではそれぞれ 30 番、31 番に割り当てられている durvācakayoga, pustakavācana の両方に 30 番という番号を割り振っており [8, pp.32–33]、それ以後は番号がずれている。

[3]Kahn は “ta” と “pa” も入替文字組として紹介しているが、[8] には該当する記述がないため、ここでは除外している。

3.1 “mlecchita” の語義

“mlecchita-vikalpā” で「暗号」に相当する意味を持ち得るのは “mlecchita” の部分である。この単語は動詞語根 “mlecch” から派生したものであるが、この “mlecch” は “*wälschen, eine unverständliche* oder *fremde Sprache sprachen*” [1], “to speak indistinctly (like a foreigner or barbarian who does not speak Sanskrit)” [6]、すなわち「(外国人や蛮人のように) 意味不明な音声を発する」という意味で用いられるのが一般的なようである。辞書に挙げられている文例を見ても、“na brāhmaṇo mlecchet (バラモンは mlecch すべきでない)” [1] とあり、「バラモンのような高貴で教養の高い人たち」とは対極にある異民族で (古典インド的観点からみて) 教養が低い、何かしら劣った存在と意識されるものが発する、「言語」と呼ぶに値しない意味不明な音声という意味合いが “mlecch” の中に込められていると見てよいであろう。

このような侮蔑的な意味合いは、“mleccha” という別の派生名詞になると一層鮮明になる。この名詞は “a foreigner, barbarian” といった “mlecch” の意味と直接関係している語義以外に、“ein Mann, der Hang zum Bösen hat” [1], “a wicked or bad man, sinner” [6] のように「悪人」という意味も持たされている。このように調査してみると、暗号のように高度な細工を施した文書を “mlecch” という単語で表現するのは、若干の不自然さを感じる。それゆえ “mlecchitavikalpā” は、「暗号読解」というよりは「異民族語の理解」と解釈するのが妥当のように思われる。

単語の意味内容を知るためには、同じ文献の中で同じ単語が使われている箇所を探しだし、その用例を調べるという方法もある。しかし残念なことに、*KS* 全体を通してこの “mlecch” という単語が用いられるのはこの一回のみであるため、実際に *KS* の中で “mlecch” がどのような単語であるかについての、これ以上の手がかりを得ることはできない。

3.2 他の技芸 (yoga) との関連

そこで *KS* で列挙されている「64 の技芸」に含まれる項目間の関係に注目する。すなわち、内容が重複する項目をいくつも立てることはないであろうと仮定し、他の項目で示された内容を調べることによって、“mlecchita-vikalpā” という単語の意味内容の絞り込みをおこなうのである。

まず 45 番目に挙げられている「指文字のような話し方 (akṣara-muṣṭikā-kathana)」という項目である。ヤショーダラ注は、これを “sābhāsā” および “nirābhāsā” という 2 種に分けて、それぞれの内容を紹介しているが、その中に、文中の各単語の最初の一文字のみを並べる手法[4]が紹介されている。このヤショーダラの解釈がどこまで妥当かどうかは定かではないが、「指文字のような」という単語だけで、あらかじめ決められた合言葉・符丁によって意図を相手に伝えるような通信方法であることは明白である。それゆえ、“mlecchita” にはそのような意味が含まれないことが推測される。

そして 47 番目の「地方語に関する知識 (deśa-bhāṣā-vijñāna)」である。この「地方語」が具体的に何を指しているかは定かではないが、岩本 [2, p.318] は *Kathāsaritsāgara* 6.148 節に「サンスクリット語、プラークリット語及びデーシァ・バーシャーが人間の間に用いられる三つの言語である」とあることを指摘し[5]、地方語とは「文学用語としてのサンスクリット並びにプラークリット以外の凡ての口語方言を指したものと考えられる」と述べている。もし、非インド系の言語も全部「地方語」に含まれるのであれば、“mlecchita-vikalpā” が「外国語」と解釈される可能性が排除されることになる。すると “mlecchita” とは、外国語でもなく、特殊な合言葉・符帳を用いた通信でもない意味不明な言語となり、ヤショーダラが述べているような「文面に細工をした文書」である可能性は高くなってくる。

しかし現状ではまだ、ここで示した以上の判断材料を用意するには至っておらず、*KS* 本文における “mlecchitavikalpā” が暗号であったか否かについての明確な判断をくだすには至っていない。ただ、“mlecchita” の一般的な意味から考えると、それが暗号である可能性は小さいと考えざるを得ない。

4 ヤショーダラ注における暗号

前節では、Kahn が暗号利用の事例として紹介している *KS* の “mlecchitavikalpā” についての調査を試みた。しかし *KS* の “mlecchitavikalpā” が暗号であるという確証は得られなかった。

そこで本節では、ヤショーダラ注を中心として、ヤショーダラが紹介している暗号の内容について、またヤショーダラはその暗号がどのような用途において用いられると考えていたかについて、順に述べていくこととする。これらの作業は、Kahn の暗号史に対する補足の役割を果たすことになるであろう。

4.1 暗号の強度

ヤショーダラは “mlecchita” について「音節の交換 (akṣara-vyatyāsa) によって意味がわからないものにすること」 [8, p.34] と明確に定義している。そしてその実例として、Kahn も紹介しているような暗号化の手法が、具体的には、以下のように示されている。

> **a-kau kha-gau gha-ṅau** ca-eva **ca-ṭau ña-ṇau na-mau** / **ya-śau ra-ṣau la-sau** ca-iti mūladevīyam-ucyate[6][8, p. 35]

この記述から、先に表 1 に示したような換字表が作成できる。

サンスクリット語において用いられる子音の一覧を表 2 に示す。サンスクリット語には、この

[4] “mūdhasabāsuśakanidhakaāvyāḥ” という文は “mū-dha-sa-bā-su-śa-ka-ni-dha-ka-ā-vya” と分解され、この各要素は “**mū**rti-**dha**na-**sa**haja-**bā**ndhava-**su**ta-**śa**tru-**ka**latra-**ni**dhana-**dha**rma-**ka**rma-**ā**ya-**vya**yā” を意味する、という記述がある。[8]

[5] この原典については発表者らは未確認。

[6] (和訳)「a と ka、kha と ga、gha と ṅa . . . la と sa [の換字をおこなう]、これが mūladevīya と呼ばれる」

	無声		有声		
	無気	有気	無気	有気	鼻音
喉音	k	kh	g	gh	ṅ
口蓋音	c	ch	j	jh	ñ
反舌音	ṭ	ṭh	ḍ	ḍh	ṇ
歯音	t	th	d	dh	n
唇音	p	ph	b	bh	m

	半母音	歯擦音
口蓋音	y	ś
反舌音	r	ṣ
歯音	l	s
唇音	v	
気音	h	

表 2: サンスクリット語の子音

ように 33 個の子音[7]が存在している。ヤショーダラの換字表では換字には母音 “a” も用いられているため、交換対象となる音は 34 個になる。そのうえで表 1 および表 2 を対照させてみると、換字の組み合わせについては、「表 2 において、なるべく隣の文字と組をつくる」以上の特段の法則性を見つけることができない。それゆえ、ヤショーダラはおそらく換字表がランダムに作成され得ることを認めており、彼が示したのは単にそのランダムな換字表の一例にすぎないと見てよいのではないか。この解釈が正しいとするなら、ヤショーダラにおける換字の組みあわせは 34! 個の順列、すなわち、およそ 3.0×10^{38} 個の順列となる。これでは単純な方法での解読は不可能となる。

4.2 暗号の用途

ヤショーダラが述べる暗号は、どのような状況における利用を想定していたものなのか。この点を明らかにするためには、“mlecchitavikalpā” をその一項目として含んでいる「女が娘のうちに学ぶべき 64 の技芸 (yoga)」なるものが、どのような意味で「学ぶべき」とされていたかの調査が必要である。

まず、これらの技芸は「女が娘のうちに学ぶべき 64 の技芸 (yoga)」として紹介されているのであるが、別の箇所には「(男も) これら技芸の習得により、幸福 (saubhāgya) が生じる」(*KS* 1.3.25) と書かれており、これらは決して女性のみに限定された美徳ではないことがわかる。また「これら (64 の技芸) によって価値を上げた遊女は、品性・美貌・美徳を備えており、人の集まりにおいてガニカーという称号と地位とを獲得する」(*KS* 1.3.20) とある。ガニカーとは、遊女の中でも最高級の地位にある者たちへの尊称であり、彼女たちは「つねに王に尊敬され、美徳ある人々に称賛され、[多くの人々から交際を] 求められ、訪問され、[女たちの] 目標の存在 (lakṣyabhūtā) となる」(*KS* 1.3.20) ような存在であった。ガニカーに対する周囲の扱いからは、*KS* で説かれている 64 の技芸とは、俗世間における自分の価値を高めるための、男女を問わない、一般的に持っていることが望ましい特技のことではなかったかと考えられる。

実際、*KS* と同様にカーマ (愛) を主題としている諸テキスト、たとえば *Ratirahasya*, *Anaṅgaraṅga* 等には「64 の技芸」と類似した記述がないことからも、これらの技芸がとくにカーマ (愛) と特別な関連を持っているものではないことが言えそうである。

これらのことから、ヤショーダラは、暗号を、それを知っていると一般社会において自分の価値が上がるもの、すなわち、民間の範疇に属する技術として捕らえていたと考えることができる。

5 考察

ヤショーダラ注が示す “mlecchita-vikalpā” の解釈は、二つの意味で非常に特異なものである。

まず、古典インドにおける特異性である。Kahn は *KS* の記述にも関わらず、古典インドの政治劇の中に暗号が利用されている場面が見掛けられないことから、古代インドにおいて暗号は広く用いられていなかったのではないかと推測している。そのような中で、暗号化のアルゴリズムを直接的に提示しているヤショーダラ注は非常に特異な存在といえる。

そして、本発表においてより重要な点として、暗号史における特異性があげられる。*KS* にお

[7]正確には、これに “ḥ”(visarga) と “ṃ”(anusvāra) を加えて 35 個になる。

ける「64 の技芸」の位置づけから考えるに、ヤショーダラ注で述べられる暗号は軍事的・外交的な目的に完全に包接されてしまうものでないことは明白である。20 世紀後半に書かれた暗号史の多くは、シーザー暗号をはじめとする軍事技術との関連で暗号を説き起こしている。軍事・外交目的 (あるいは宗教上の目的) に限らない民間利用目的から暗号を位置づけ、それが一般社会において有効であることを示しているヤショーダラ注は、この流れの中において特異な存在となっている。

それと同時に、前近代において民間レベルでの暗号利用の効用を説くヤショーダラ注の存在は、現在の状況を理解する上でも貴重な示唆を与えると考えられる。現在、暗号は武器輸出規制に代表される政府の規制から自由化への方向へと向かっている。だが、市民が自由に暗号を使える現状は人類が初めて迎える事態ではないし、将来また国家機関が暗号規制をおこなう流れになる可能性もある。すなわち、暗号技術そのものは革新を続けているが、社会が暗号を管理すべき武器として位置づけるか、あるいは一般市民が学ぶべき技芸として位置づけるかは時代の条件と共に変化し、その位置づけは簡単に逆転しうることを歴史は示している。それゆえ暗号の歴史をたどることは未来について考えることにつながる。現在そして今後における暗号利用のありかたについて考えるためには、暗号が持つ技術的側面に目を向けるだけではなく、社会がどのように暗号を利用しようとしているかに関する考察を欠かすことはできない。

6　今後の課題

近年になって、若干ではあるが、インドにおける暗号利用に関する研究がおこなわれているようである。アメリカ議会図書館の Thrasher[9] は、インドにおける暗号利用について書かれている関係書目を作成中であり、近い将来にはその成果を INDOLOGY Website [10] にて公開することを予告している。また古典からは離れるが、Metzger[5] は、いまだ未発表ではあるが、17–18 世紀のラジャスタン地方におけるヒンディー語およびラジャスタン語の外交文書中の暗号についての研究をおこなっているようである。

それゆえ、彼らの研究の推移にも注意を払いながら、今後さらに古典インドにおける用例を含む、民間暗号の歴史についての調査を続けていきたいと考えている。

謝辞

東北大学大学院文学研究科博士後期課程に在学中の笠松直さんには、史料について多くの有益な助言を頂いた。しかしながら、本発表における誤りはあくまで本発表の著者に帰属する。

参考文献

[1] O. Böhtlingk and R. Roth. *Sanskrit-Wörterbuch*. St. Petersburg, 1855–1875 (Reprint in Tokyo, 1976).

[2] 岩本裕 訳著. 完訳 カーマスートラ. 杜陵出版, 1949.

[3] 印度学会 訳編. 印度古典 カーマスートラ (性愛の学). 大谷大学内印度学会, 1923.

[4] David Kahn. *The Codebreakers: The Story of Secret Writing*. Scribner, Revised edition (1996), Originally appeared in 1967.

[5] Mathias Metzger. Re: codes. E-Mail via Indology-ML <INDOLOGY@listserv.liv.ac.uk>, Dec. 21, 2000.
Message-ID: <b4.efb80c6.27735b93@aol.com>.

[6] Sir Monier Monier-Williams. *Sanskrit-Engilish Dictionary*. Oxford, new edition, 1899.

[7] Louis Renou. *Litérature Sanskrite*, Vol. 5 of *Glossaires de l'Hindouisme*. Paris, 1945.

[8] G. D. Shastri. *Kāmasūtra by SrīVātsyāyana Muni, with the commentary Jayamangala of Yashodhar*. No. 29 in Kāshi Sanskrit Series. Benares, 1929.

[9] Allen W Thrasher. Re: codes. E-Mail via Indology-ML <INDOLOGY@listserv.liv.ac.uk>, Dec. 20, 2000. Message-ID: <sa40d643.029@loc.gov>.

[10] D. Wujastyk. INDOLOGY – Internet Resources for Indological Scholarship. WWW. (since Nov. 12, 1999) URL: <http://www.ucl.ac.uk/~ucgadkw/indology.html>.

[11] 山根信二, 相場徹, 村山優子. キーエスクロー以降の通信傍受: 歴史的分析. 電子情報通信学会技術研究報告, Vol. 100, pp. 57–62 (ISEC2000–31), 2000.

[12] 郵政省. 21 世紀デジタル社会の暗号政策への提言. URL: http://www.mpt.go.jp/policyreports/japanese/group/internet/ninshou/ (June 1999).