現場レポート

暗号研究から電子政府構築まで

中央大学研究開発機構 教授
辻 井　重 男

NPOデジタル・フォレンジック研究会 コラム　　2010年2月25日号より

現場レポート 暗号研究から電子政府構築まで

辻井重男

目次

Ⅰ部
1. 2010年1月 高松から
2. 暗号の2010年問題とは------朝日新聞記事から
3. 日本発祥の多変数公開鍵暗号の研究現場から
4. 国際会議PQCrypto 2010から――量子コンピュータ時代の暗号
5. 創る人と批判する人
   5.1 哲学の場合
   5.2 暗号の安全性検証
6. ヒルベルト的世界観からゲーデル・ブラウアー的世界観へ

Ⅱ部 (未完)
7. 電子政府の構築へ向けて
8. 矛盾の超克――国民安心
   番号とプライバシー
9. 2010年4月韓国の電子政府を訪ねて
10. 2010年5月19日 韓国の先進事例に学ぶシンポジウムから
11. 文理軸―理念・現実軸の平面上で考える人材育成

1　SCIS 2010 高松から

図1　SCIS 2010 (高松)の発表論文　分野別件数

Table 1. Classification of MPKC by Ding et. al [DWY07]

Mixed-field (or "Big Field")	MIA	Matsumoto-Imai Scheme A or C* Matsumoto, Imai et. al 1983~88
	HFE	Hidden Field Equation Patarin 1996
Single-Field (or "True")	UOV	Unbalanced Oil and Vinegar Kipnis, Patarin, Goubin 1997~99
	STS	Stepwise Triangular System Tsujii et. al 1985~89 (In Japanese) Shamir 1993

2010 年 2月 – 6月	会場		投稿締切	採否通知	カメラレディ	会議
	開催地	開催国				
FSE 2010 (International Workshop on Fast Software Encryption)	Seoul	Korea	–	–	–	2/7 – 10
TCC 2010 (Theory of Cryptography Conference)	Zurich	Switzerland	–	–	–	2/9 – 11
CT-RSA 2010 (RSA Cryptographers' Track)	San Francisco, California	USA	–	–	–	3/1 – 5
WISTP 2010 (Workshop in Information Security Theory and Practice)	Passau	Germany	–	–	–	4/12 – 14
AFRICACRYPT 2010	Stellenbosch	South Africa	–	2/19	2/28	5/3 – 6
PQCrypto 2010 (International Workshop on Post-Quantum Cryptography)	Darmstadt	Germany	–	–	2/28	5/25 – 28
PKC 2010 (International Conference on Practice and Theory in Public Key Cryptography)	Paris	France	–	–	3/12	5/26 – 28
EUROCRYPT 2010	Nice	France	–	–	2/26	5/30 – 6/3
ACNS 2010 (International Conference on Applied Cryptography and Network Security)	Beijing	China	–	3/31	4/20	6/22 – 25
Workshop on Tools for Cryptanalysis 2010	Egham	UK	4/20	5/20	6/10	6/22 – 23
SCC 2010 (International Conference on Symbolic Computation and Cryptography)	Egham	UK	3/14	4/11		6/23 – 25

2010 年 7月 – 9月	会場		投稿締切	採否通知	カメラレディ	会議
	開催地	開催国				
ACISP 2010 (Australasian Conference on Information Security and Privacy)	Sydney	Australia	2/16	4/13	4/26	7/5 – 7
SECRYPT 2010 (International Conference on Security and Cryptography)	Athens	Greece	2/26	4/8	4/22	7/26 – 28
JWIS 2010 (Joint Workshop on Information Security)	Guangzhou	China	5/14	6/21	7/8	8/5 – 6
LatinCrypt 2010 (international conference on cryptology and Information security)	Puebla	Mexico	3/15	5/14	6/7	8/8 – 11
SAC 2010 (Selected Areas in Cryptography)	Waterloo, Ontario	Canada	5/17	7/6	7/20	8/12 – 13
CRYPTO 2010	Santa Barbara, California	USA	2/18	4/30	5/28	8/15 – 19
CHES 2010 (Workshop on Cryptographic Hardware and Embedded Systems)	Santa Barbara, California	USA	3/1	4/30	5/26	8/18 – 20
WISA 2010 (International Workshop on Information Security Applications)	Jeju Island	Korea	6/11	7/9	7/31, 9/18	8/24 – 26
SCN 2010 (7th Conference on Security and Cryptography for Networks)	Amalfi	Italy	4/5	5/28	6/18	9/13 – 15

2010 年 10月 - 12月	会場		投稿締切	採否通知	カメラレディ	会議
	開催地	開催国				
ProvSec 2010 (International Conference on Provable Security)	Malacca	Malaysia	4/16	6/11	6/30	10/13 – 15
ISITA 2010 (International Symposium on Information Theory and its Applications)	Taichung	Taiwan	3/15	5/31	7/7	10/17 – 20
ICTCI 2010 (International Conference on Trusted Cloud Infrastructure)	Shanghai	China	5/15	7/15	8/15	10/18 – 20
ISC 2010 (Information Security Conference)	Boca Raton, Florida	USA	6/15	7/30	8/15	10/25 – 28
IWSEC 2010 (International Workshop on Security)	神戸	日本	4/30	7/9		11/22 – 24
ICISC 2010 (Annual International Conference on Information Security and Cryptology)	Seoul	Korea	8/31	10/19	11/1	12/ 1 – 3
ASIACRYPT 2010	Singapore		5/20	8/17	9/10	12/5 – 9
GLOBECOM 2010 (IEEE Global Communications Conference)	Miami, Florida	USA	3/15	7/1	8/1	12/6 – 10
Indocrypt 2010 (International Conference on Cryptology in India)	Hyderabad	India	7/30	9/17	9/24	12/12 – 15
Pairing 2010 (International Conference on Pairing-based Cryptography)	山中温泉	日本	6/11	8/19	9/13	12/13 – 15

表3　The Third International Workshop on Post-Quantum Cryptography (PQCrypto 2010)

分野	総数	上:方式提案型 下:解読・解析型	国別件数					
			日本	中国	US	ドイツ	フランス	オランダ
多変数 公開鍵暗号	8	3	1*	0	1	1	0	0
		5	0	2	3	0	0	0
誤り訂正符号 応用暗号	7	2	0	0	0	1	1	0
		5	0	0	1	3	0	1
その他 (格子に基づく署名・ 非可換歪多項式 に基づく鍵交換)	2	2	0	0	0	1	1	0
		0	0	0	0	0	0	0
全分野	17	7	1	2	5	6	2	1
		10						

* S. Tsujii, M. Gotaishi, K. Tadaki, and R. Fujita, "Proposal of a Signature Scheme based on STS Trapdoor,"

５　創る人と批判する人

西田幾多郎の日記から
「私の論理と云うのは学界からは理解されない。否、
一顧も与えられてないと云ってよいのである。・・・」
西田幾多郎の悲哀に満ちた人生を象徴にするような話

「善の研究」より
「幅の無い線、厚さのない面　などというものは存在しない・・・」
「意識現象こそ実在」？
楕円暗号の立場；　数学的実在は物理的実在を超越して
社会的実在となって、ICカードに宿る

高木貞治　vs　ヒルベルト
多変数公開鍵に関するある論文の中で、J. Ding 等は，下記のように述べている：
“We stress that it is still an original sin that no list of possible attacks can be exhaustive”

（1）自分の生んだ子は可愛い。

たとえ、医者が見離したとしても、

何とか育てたいと思って提案者は夜半目覚めても考え続ける。

解読者は、同じ仲間でも、提案された方式に、それほど愛着は感じないから、

解読した後、考え続けないことが多い。

（2）暗号の分野でも、創るのが好きで得意な人と、

批判し、解読するのが性に合っている人に分かれる傾向がある。

両方に能力のある研究者も勿論いるが、

そのような人も、提案する時と解読する時とで、（1）のように心理状態が異なる。

表4　電子政府に関する日韓の比較

韓国	
人口	4700万人
電子証明	1999年導入。2004年からは銀行を通じて IC カードにも発行。
発行枚数	1,380万枚（2006年10月 非 IC カードタイプも含む）
署名/認証	署名用、認証用の2種類
国民 ID	有
用途	電子申請、申告、インターネットバンキング、オンラインショッピング等

日本	
人口	1億2700万人
電子証明	2004年1月導入。IC カードに格納する方式。 全国民が対象。電子証明書は住基カード（IC カード）に格納する方式。
発行枚数	118万枚（2009年11月）
署名/認証	署名用のみ
国民 ID	無（基本 4 情報（住所・氏名・性別・生年月日）により代替）
用途	電子申請、自治体独自利用

参考　電子政府ガイドライン作成検討会セキュリティ分科会報告書

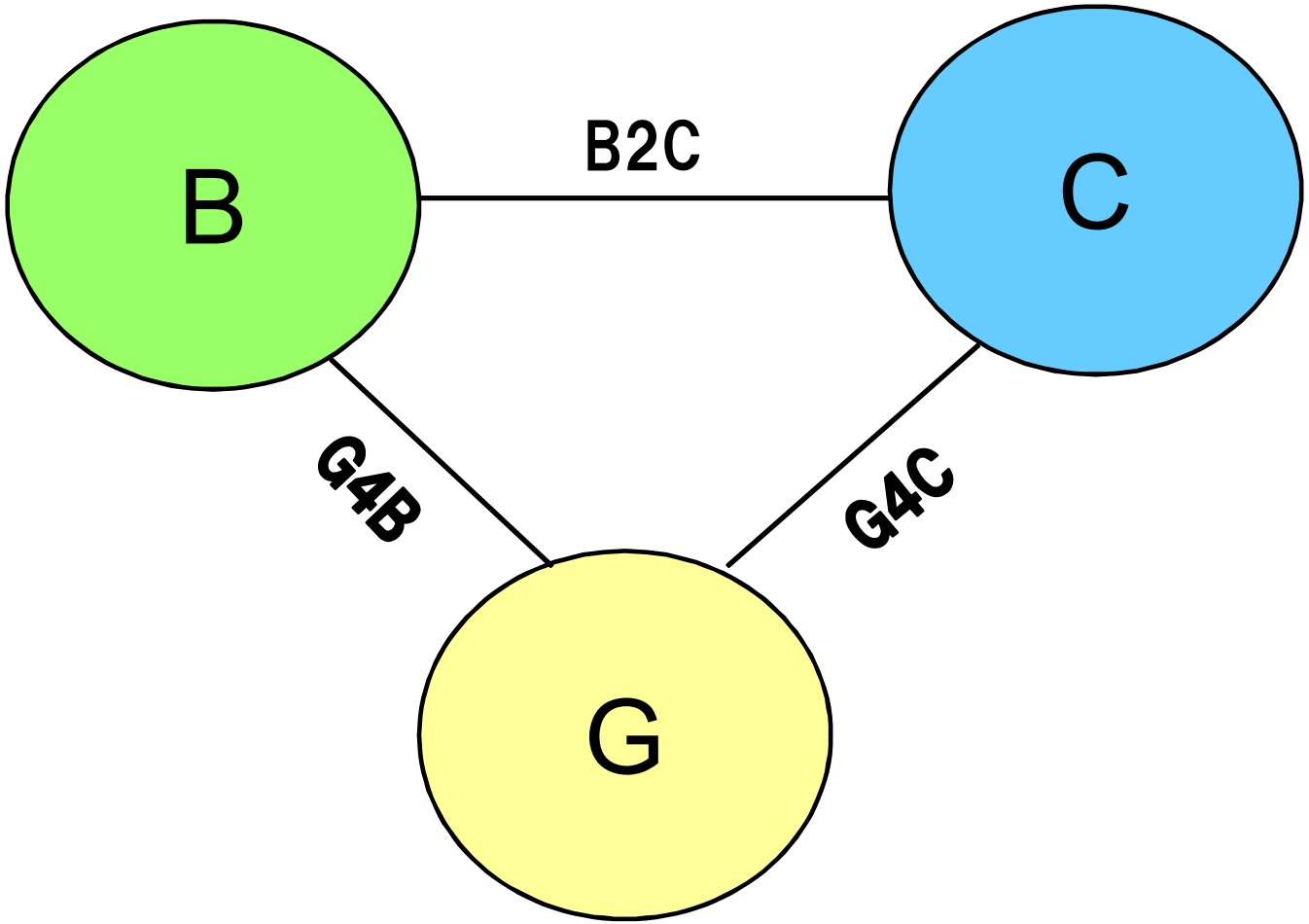
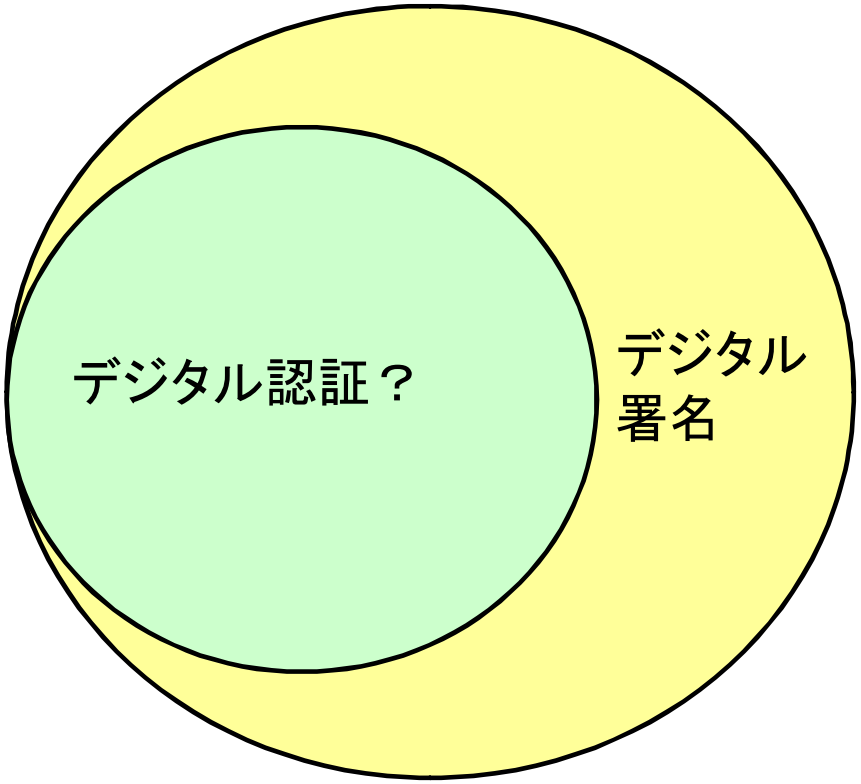


図2　国民基盤としての電子政府

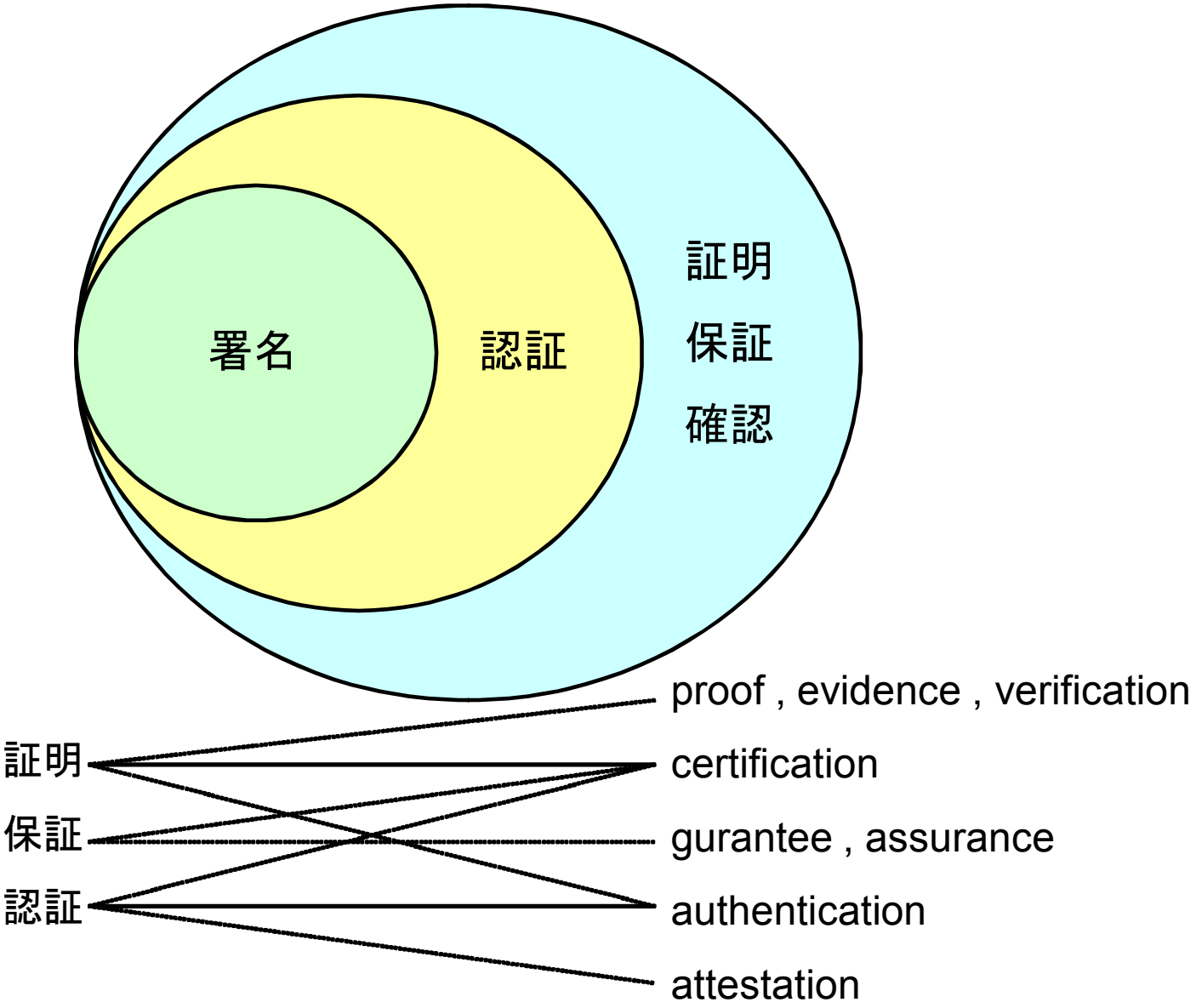
図4　技術的文脈の中での用語

RSA 1978　　Digital Sig.



SCIS 2010　2010.1.19 ~ 22
高松　　600名以上参加
　　300件以上の論文発表
署名 ≫ 認証

図5　社会的文脈の中での用語



11　人材育成

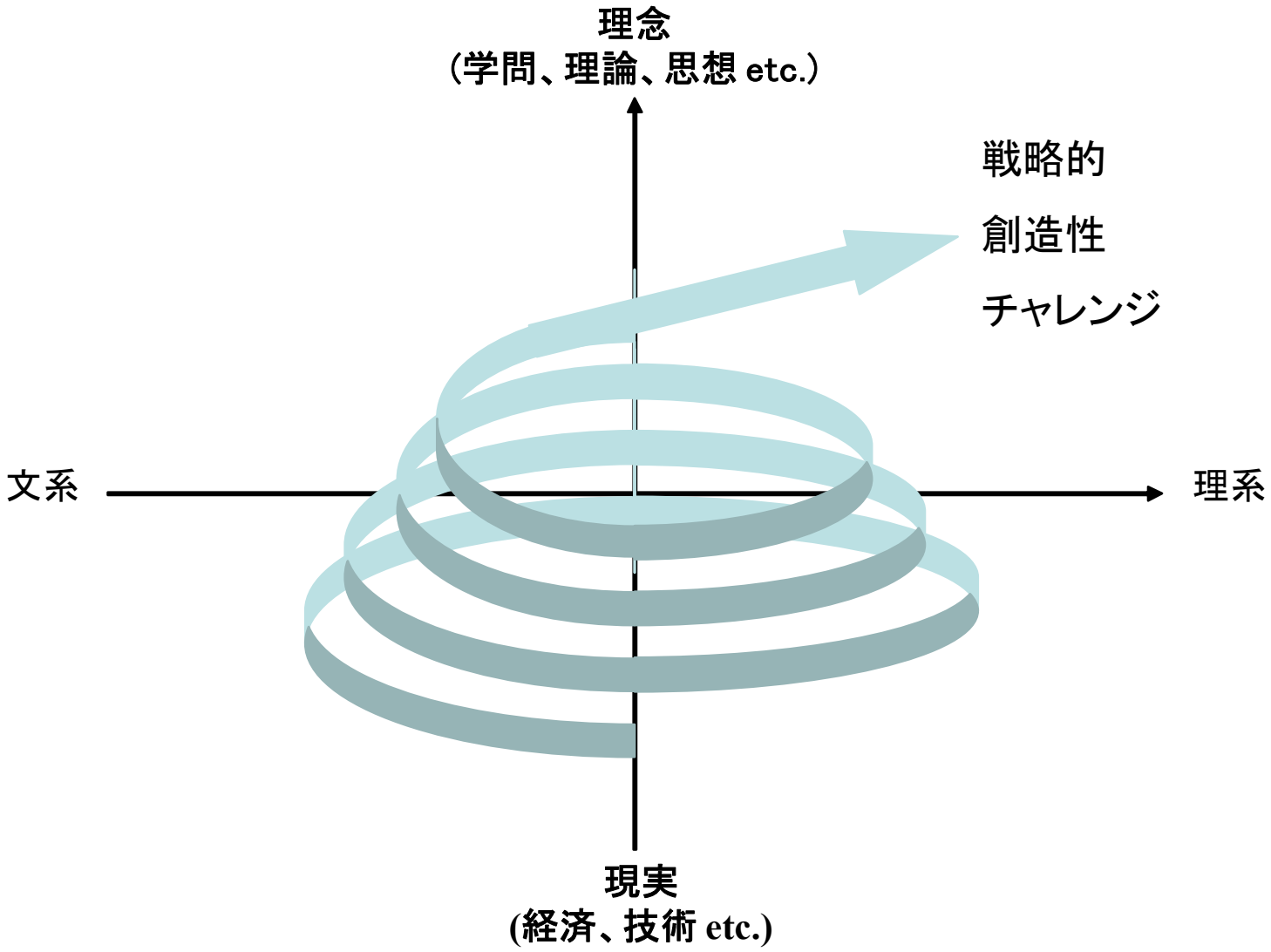


図6　求められる人材像