第一部

招待講演１
暗号研究者から見た言語・論理と
デジタルフォレンジック

辻井　重男

中央大学研究開発機構　機構教授

／一般財団法人マルチメディア振興センター　理事長

／一般財団法人放送セキュリティセンター　理事長

第6回産業日本語研究会・シンポジウム

辻井重男

暗号研究者から見た言語・論理とデジタルフォレンジック

概要

古典暗号時代に、暗号解読とその誤訳などが第1次・第2次大戦の勃発
に及ぼした深刻な影響について触れた後、
現代暗号研究者から視た組織通信における
言語と論理の役割を多角的に考察する。

特に、現代暗号の安全性証明における論理的証明、
クラウド環境下における秘匿検索・暗号化状態処理のための
自然言語処理と論理学の活用、
デジタルフオレンジックや公共情報コモンズ（災害情報伝達システム、Lアラート）
における 言語翻訳課題の緊急性について考察する。

2014年7月辻井企画講演会の動機

法令工学　北陸先端科学技術大学院大学(JAIST)　21世紀COE

- 論理学と日本語の両面から
- 法律と論理学・言語処理　学際的総合研究

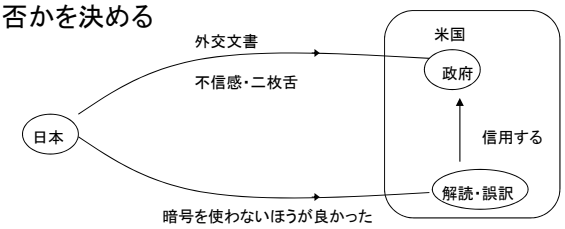
デジタルフォレンジック　武田薬品　80億円　殆ど翻訳料

- 公共情報コモンズ（マルチメディア振興センター）
- 避難情報のリアルタイム多言語化
- イギリス　17世紀の英語改革　外山滋比古
-

- 個人的研究動機
- 論理学暗号方式の創始
- 放送通信の4類型と組織通信ー情報セキュリティ概念の高度化

誤訳
御前会議　　Meeting in the Morning
天聴ニ達セラレアリ（難解な表現、文語調）
甚タ恐懼ニ堪エサルモ（天皇に対し出すぎたようで恐縮である）
誤訳　　⇓
重大な懸念を抱いている（政治家自身が）

最新＝最後 ⟶ 最終通告
（電文簡単化）
日米戦争回避条件の一つ
米独開戦時　日独伊三国同盟
↓
日本　自主的に参戦か否かを決める
⇓
Automatically　と誤訳



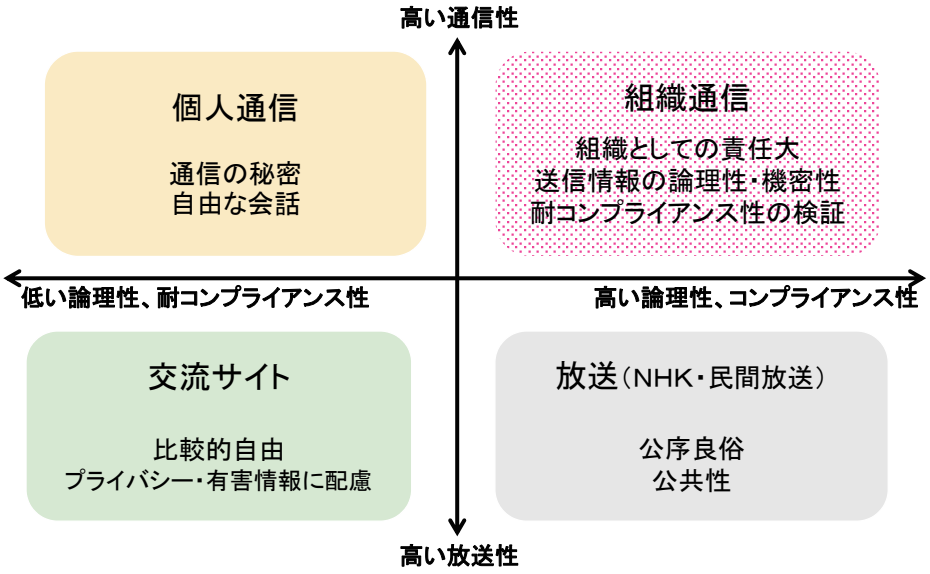
議論の流れ

- １．情報伝送・暗号理論研究の立場から
- ２．デジタルフォレンジクと日本語の課題
- ３．日本語の論理性に対する私見
- ４．言語と論理に関する課題

- 付録　１．放送・通信の４類型と情報セキュリティ概念の高度化－第２報
- 　　－組織通信と公共情報コモンズ（Lアラート）
- 　　２．尸位素餐（しいそさん）とは？

1. 情報伝送・暗号理論研究の立場から

放送・通信の4類型と組織通信



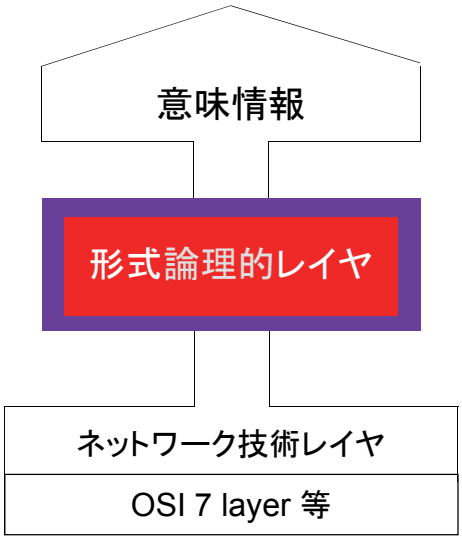
組織間通信における機密通信の必要性

- 情報量の爆発的増大、組織の複雑化、
- 関与者（Multi-Stake Holder）の拡大を背景に
- 企業、自治体、医療・介護ネットワークなどの
- 組織間における高度な機密通信の必要性増大

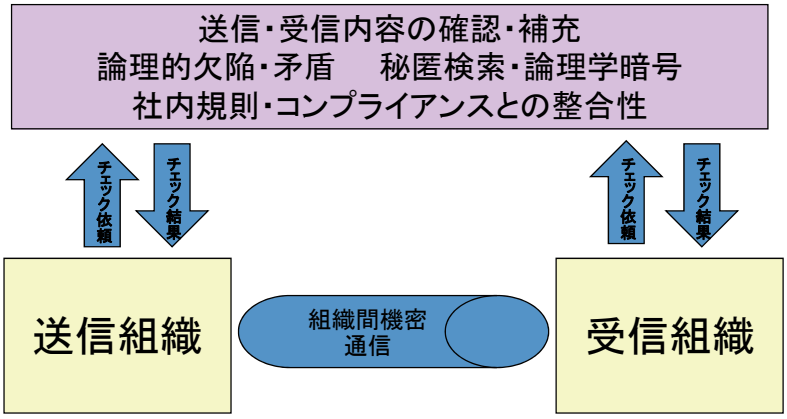
例：My Number、税と社会保障、収入・資産
全自治体（居住区域外）に跨る個人情報把握の必要性。
プライバシー保護のため、必要な個人情報のみ把握。

7

情報通信の新階層



Open data, Cloud, Big data, My number環境下での
情報通信・セキュリティ概念の高度化への対応



9

組織間機密通信

- 従来は自治体や病院などの単独組織内で、
  情報を共有・処理することが多かった。

- ネットワーク化、OCBM環境化、関与者の増大

例えば、医療・介護組織間の連携・業務指示
- 事業所単位での活動から連携へ
- 作業指示書などが書類でなく情報通信で

① 機密・プライバシーを保護し、

② 情報の論理性・耐コンプライアンス性を高めつつ、
複数組織間や民間・行政間での情報交換の増大

10

組織通信に要求される機能

正確性、信頼性、緊急性、迅速性、証拠性（デジタルフォレンジック）

機密性（組織暗号、構造化言語による秘匿検索）

情報限定性、 論理的無矛盾性、

法的整合性（耐コンプライアンス性）

多言語性　　（赤字は、本委託研究で実施中）

法令工学

JAIST　21世紀COE　法令工学の提案　片山 卓也

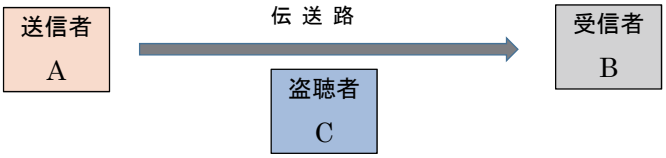
- 「法令工学とは、法令が
- 1） 制定目的にそって適切に作られ、
- 2） 論理的矛盾や文書的問題がなく、
- 3）関連法令との整合性がとれていることを検査・検証し、
- 4）法令の改訂に対しては、矛盾なく変更や追加削除が行われること
- を情報科学的手法によって支援することを目的とする学問分野である」

- 法令工学でいう法令とは、法律のみでなく、都道府県の条令や、企業の社内規則なども対象にしている。

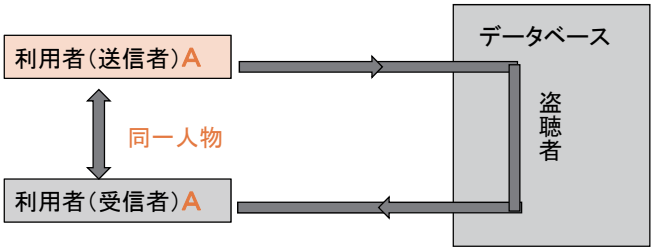
- 論理学と自然言語処理の相性を両側から高める研究が重要

3. 研究開発内容　3.2　情報通信・セキュリティ概念の高度化への対応

秘密通信と秘匿検索



(a) 秘密通信の場合



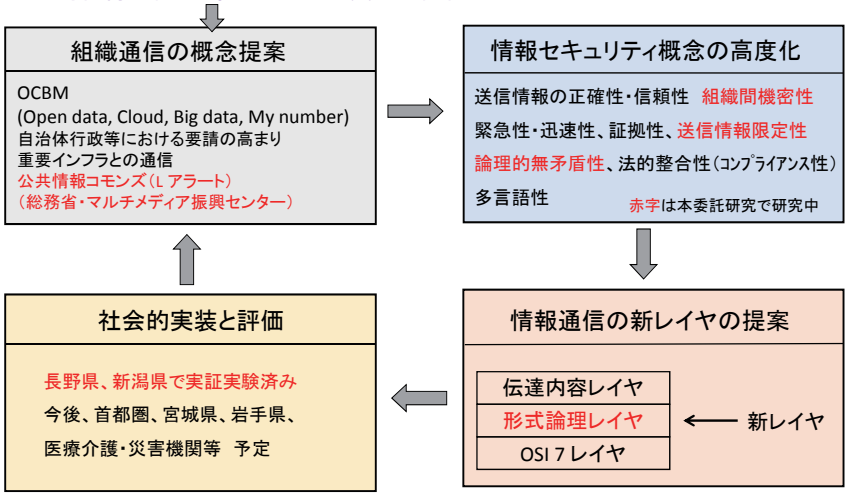
(b) 秘匿検索の場合

自然言語から論理式への変換(暗号化)については伝達に必要はない

13

組織通信概念の提案とその実現に向けて

IEEE等国際会議・総務省シンポで賛同的評価



通信の意義
高速大容量→信を通わす

- OCBM時代　Open,Cloud,Big data,My number
- ビジネス、法令、科学技術文書などの論理性
- 送信内容の論理的欠陥・矛盾の検出　　CIA概念の拡大

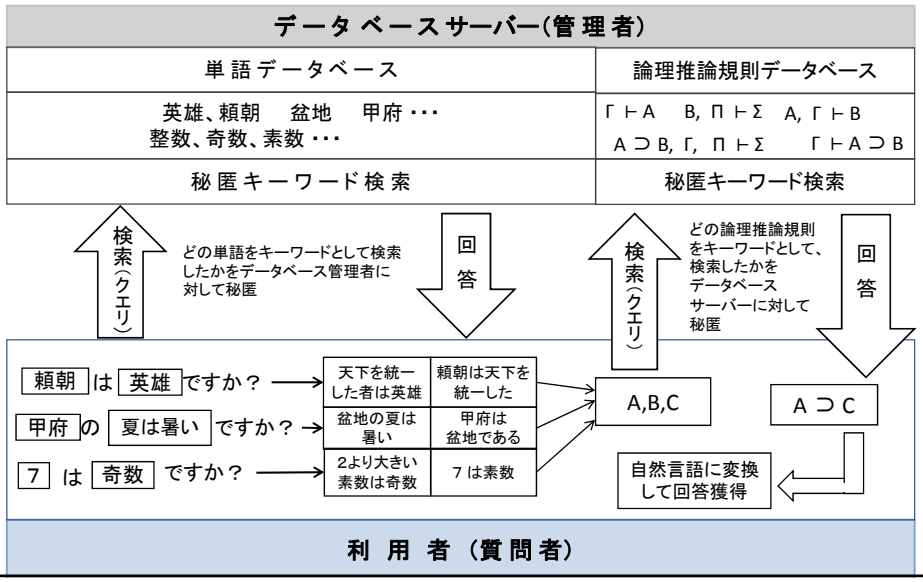
- 質問・回答　　証拠の論理的保全・開示
- 暗号化　平文を論理式に直接暗号化

- 現代論理学を利用　　古典論理を超えて

- 6月2日　日経朝刊　　米国での訴訟和解　　深刻な課題
- デジタル・フォレンジック　　証拠の保全・開示
- 武田薬品工業　80億　殆どが　翻訳料

3. 研究開発内容　3.2　情報通信・セキュリティ概念の高度化への対応

現代論理学暗号に基づく
秘匿検索・回答文作成システム



アリストテレスの三段論法のモデルの例

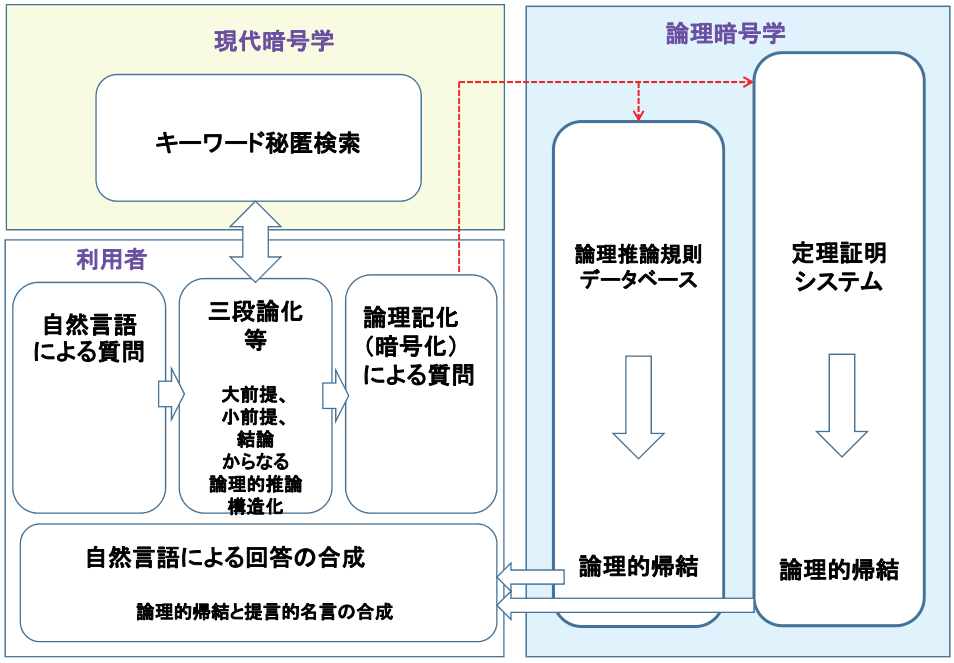
- 言い換えれば，モデルが開示されなければ，何を推論しているのかわからない．日常言語と導出規則2（A⊃B, B⊃C ⊢ A⊃C）は，多から1への写像である．
- 多から1への写像を説明する「導出規則2 A⊃B, B⊃C ⊢ A⊃Cに対応する日常言語を使った別のモデルによる三段論法」には次のようなものが考えられる．

  甲府は(A)，盆地である(B)
  盆地は(B)，夏暑い(C)
  ゆえに，甲府は(A)，夏暑い(C)

  2 より大きい素数は(A)，
  2 より大きい奇数である(B)
  2より大きい奇数は(B)，7である(C)
  ゆえに，2 より大きい素数は(A)，7 である(C)

- このように，導出規則2 A⊃B, B⊃C ⊢ A⊃C に意味を与えるモデルと導出規則自体を分離して考えることが，情報セキュリティにおける「他者からの隠ぺい概念」に結びつく．

17



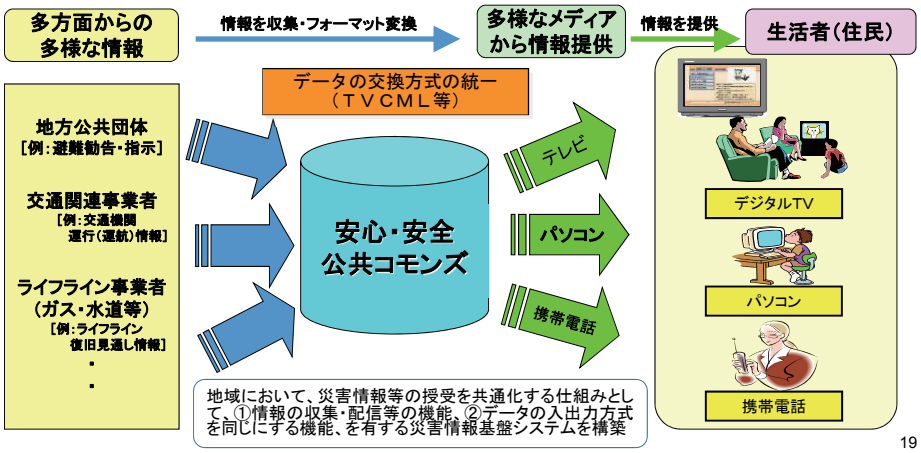
現代暗号と論理学暗号の融合による秘匿問合せ/回答システム

総務省「地域の安心・安全情報基盤に関する研究会」報告書（平成20年7月2日）より抜粋

『安心・安全公共コモンズ』のコンセプト （FMMC吉田部長）

多様なメディアを活用して、高齢者をはじめ誰もが、いつでもどこでも、分かりやすい形式で地域の安心・安全に係るきめの細かい情報を迅速に入手できるようにするための具体的な仕組みを、早急に構築することが喫緊の課題

住民への情報提供が容易な『安心・安全公共コモンズ』の構築が必要



地域において、災害情報等の授受を共通化する仕組みとして、①情報の収集・配信等の機能、②データの入出力方式を同じにする機能、を有する災害情報基盤システムを構築

19

2．デジタルフォレンジック ―国際訴訟と翻訳の課題

参考

- 1） 守本正宏著「カルテル・PL訴訟・特許訴訟」ディスカバリ
- （企業家大学出版2012年3月）

- 2） 改訂版 デジタルフォンレジック事典
- デジタルフォンレジック研究会編（日科技連）
- 辻井；日本語の論理性向上のための論理学・自然言語処理
- ・機械翻訳（第10章 10．1）

米国における 民事訴訟ーPretrial

- 6月2日 日経朝刊 米国での訴訟和解 深刻な課題
- デジタル・フォレンジック 証拠の保全・開示
- 武田薬品工業 80億 殆どが 翻訳料
- ーーーーーーーーーーーーーーーーーーーーーーーーーーーー

- 日本企業 不必要な資料まで翻訳 情報漏洩

e ディスカバリの流れ

- １．　特定（identification)　　データなどの具体的確認
- ２．　データの保全（Preservation)
- 3.　データの収集（Collection)
- 4.　データプロセス（Processing)
- 5.　分析（Analysis)　　翻訳の絞込み
- 6.　証拠閲覧（Review)
- 7.　提出ドキュメントの作成（Production)

「ディスカバリ」 守本 正宏著

１０周年記念　表彰普及・啓発賞

- 日米民事訴訟比較　　米国文化　当事者主義；
- プリトライアルの段階で、被告と原告双方が、徹底的に「証拠開示（ディスカバリ」する。
- デジタル署名・公開鍵暗号の役割
- 余談；池上 彬番組　エニグマ機 出演　しかし・・・
- 相手側が提供した情報の中から証拠を見つけ出す。

- 日本本社の在米国子会社が訴訟にあった場合の
- 翻訳の費用は莫大。
- 機械翻訳・自然言語処理、現代論理学の導入

3．日本語の論理性に対する私見

- 尸位素餐（しいそさん）とは？
- ―ビッグデータ時代の日本語の論理性と国際性
- 付録参照

日本語と日本人のDNA

- 長いトンネルを抜けると雪国であった　　川端康成
- The train came out of the long tunnel into the snow country
  サイデンスティッカー
  その列車が、その長いトンネルを抜けると、その雪国に入った
  再日本語訳

主体ー客体？　　純粋経験　　主語・定冠詞　不要？
自他一体の境地

フランスの2歳の子供でも（写真）

西田幾多郎著 「日本文化の問題」（1940年、昭和15年）

- 「私は日本文化の特色と云うのは・・・どこまでも自己自身を否定して
- 物となる、物となって見、物となって行うと云うにあるのではないかと思う。己を空うして物を見る、自己が物の中に没する、・・・
- 日本精神の真髄は、物に於て、事に於て一になると云うことでなければならない。」

- 自己を否定し、私を排し、無心になって、対象と自己を一体化する。
- （佐伯啓思著　西田幾多郎　無私の思想と日本人）

日本語、途方もなく自由だった？

日本語が持つ「途方もない融通無碍な自由さ」だ。「非論理的なものも『てにをは』がつなげてしまうなど意味を超えて感情を喚起する、ある種の分泌性がある」。そして日本語を操る我々にも「つじつまが合わないものを受け入れ、そこに美や叙情を感じる性質がある」というのだ。

（赤田 泰和）

朝日新聞 2013年4月30日 夕刊掲載記事より

結構ですね。

日本語の課題

- 揺れ動く感情を連綿と綴る
  湿度100%の演歌？（広田）

- 外山 滋比古
- 150年振りに改革必要
- イギリス　17世紀　大改革
- 情緒・感覚→明晰な論理表現へ

イギリス・ロイヤルアカデミーの英語改革

『今の英語』

◎詩、文学など
情緒・感情を中心とした
曖昧模糊たる表現が多い

◎これではイギリス人の新しい
考え方を十分に表現できない

英語改革

『改革した英語』

◎科学文章など、科学的、論理的、
思考的な表現に重点を置く

◎これなら、イギリス人の納得いく
内容を明晰に表現できる

The History of the Royal-Society of London
for the Improvement of Natural Knowledge

イギリス・ロイヤルアカデミー

トーマス・スプラット
(1635-1713)

4. 言語と論理に関する課題

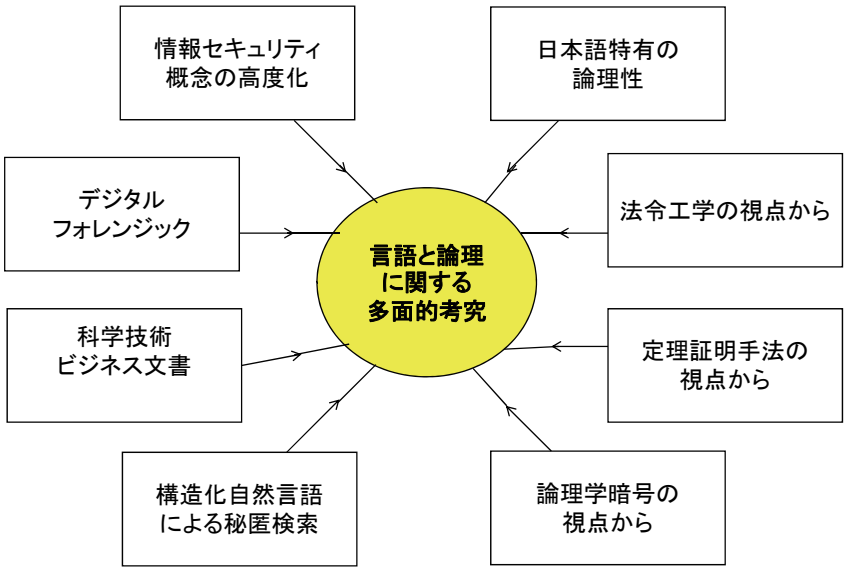


図　言語と論理に関する多面的考究の必要性

自然言語から人工言語へ

与謝野晶子は与謝野鉄幹を愛している。
与謝野鉄幹は与謝野晶子に愛されている。　OK

皆は誰かを愛している。→　誰かは皆に愛されている。　OK？

「いかなる行為にも、その究極的目的がある」→
「ひとつの究極的目的を目指して、全ての行為がなされる」　OK？
アリストテレス　ニコマコス倫理学

「感覚的な事物の存在は、全て何らかの精神に依存している」→
「ある精神が、全ての感覚的な事物の存在に不可欠である」　バークレー　OK？

自然言語では隠されている構造→論理形式が記号表現の表面に現れている言語

命題論理から述語論理へ

- 命題論理（文を単位とする推論）やアリストテレスの三段論法では、主語・述語の関連が消えてしまって、推論の正当化が出来ない。

- アリストテレスの方法
- 「全てのAはBである。」 項に一定の記号を与える。
- 「全ての」とか「ある」の部分はそのまま温存。

- 正当化には　文を構成する要素部分の取り扱いと普遍量化子・存在量化子の導入が不可欠
- →　述語論理

述語論理　項からモノ（変数）へ

・　パンダは笹を食べ、コアラはユーカリを食べる。
• パンダもコアラも動物である。
• 笹もユーカリも植物である。
• ――――――――――――――――――――――

• 質問；それならパンダもコアラも草食動物ですか。

記号表現

F(x); x はパンダである。　　G(x); x はコアラである。
H(z);　z は笹である。　　F_1(x);　x はユーカリである。
G_1 (x,z);　xはzを食べる。

• ∀ x (F(x)　⊃　∃ z (G_1(x.z) ∧ H(z)))
•　　∧ ∀ y (G(y) ⊃ Ez_1 (G_1 (y,z_1)
•　　∧ F_1 (z_1)))

自然言語と論理学の相性は悪いか？

- 富美子は物理の得意な女性だ。
- 富美子は女性だが、物理が得意だ。
- 富美子は女性のくせに、物理が得意だ。

- 論理学は　ニュアンス・感情表現は苦手？
- 科学技術、法律、ビジネス等に限れば
- 可なり相性を良く出来る。

今後の展開　多様な論理学の導入が必要

1階述語論理・古典論理から多様な論理へ

神の視点（古典論理）；有罪か無罪かは決まっている？
判決の前に死亡するかも？

人間の視点；法律や医療の相談では、直観主義論理、様相論理

など多様な論理学を導入する必要がある。logics

数学においてすら、構成主義、直観主義の立場がある（π＝３．１４・・・・）

暗号の安全性証明　IND-CCA等では専ら古典論理（背理法）だが。

親が叱らない　と　子供は勉強しない→子供が勉強する　と　親は叱る？

古典論理・命題論理から非古典論理・述語論理へ

- 2重否定＝肯定　を認めない
- ×　排中率、背理、対偶、含意、ド・モルガンの一部
-
- Q　華子さん　好きですか？　　A　好きでないことはありません
- Q　それでは好きなのですね　　A　？

- 親が叱らない→子供は勉強しない　子供が勉強する→親が叱る？

多値論理、直観主義論理、様相論理・・・
JAIST　21世紀COE　法令工学　Davidsonian style

フレーゲ（1848－1925）の命題観

- 「伊藤 邦武著；物語　哲学の歴史」 より

- 命題とは関係を表現する関数が、その定項や変項として個別的な対象を含むものであり、それに加えて、それらの対象についての量的表記を行う「量化子」を加えたものである。
- 例；師弟　という関数が　ソクラテス、プラトンという値をとる。

- 新しい論理学は主語ー述語の命題形式を廃棄することで、
- 命題同志の演繹的な関係の推論の力を飛躍的に増大。

- → 形而上学の大きな変革へ（意識の哲学から言語哲学へ）

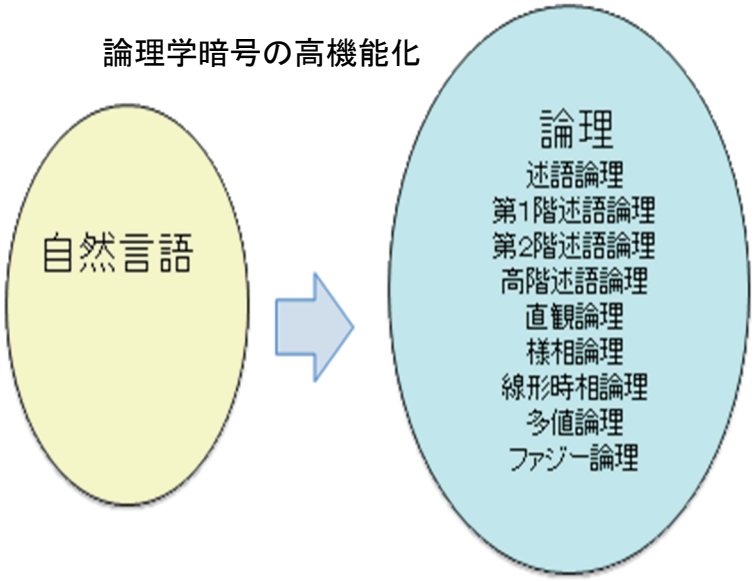
古典論理から非古典論理へ

- 古典論理＝神の論理　nearly ＝数学の世界
- 排中律　２重否定＝肯定
- 真か偽か　善か悪か　好きか嫌いか　有罪か無罪か
- 人間世界　好きでないことはない＝好き？

非古典論理

- 直観主義論理　×　排中律、２重否定＝肯定
- 田中角栄　有罪？
- 様相論理　知識、信念、自覚　例；医師　薬１００mg　communication
-

論理学暗号の高機能化



長期的重要課題

- **―日本語文の論理性向上のための論理学・自然言語処理・機械翻訳―**
- （辻井；IDF事典原稿―将来の課題より抜粋　）
- （1）　日本語の論理性を高めること
- （2）　現代論理学と日本語を含む
- 　　自然言語処理の親和性を高めること

付録１

SCIS 2015 The 32nd Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 20 - 23, 2015
The Institute of Electronics, Information and Communication Engineers

放送・通信の４類型と情報セキュリティ概念の高度化—第２報 —組織通信と公共情報コモンズ（Ｌアラート）

Advanced Concept of Information Security in 4 Categories of Communication and Broadcast — 2 nd Report — Public Disaster Proof System (L-Alert)

辻井 重男 * 吉田 正彦 † 柴崎 哲也 ‡ 小林 正幸 ‡
Shigeo Tsujii Masahiko Yoshida Tetsuya Shibasaki Masayuki Kobayashi
川喜多 孝之 ‡
Takayuki Kawakita

あらまし Open data, Cloud, Big data の普及や，2016 年 1 月から予定されている My number の導入，即ち，OCBM の進展に伴い，従来の紙の文書に代わり，大量の電子化された文書が，組織間で通信される状況に変わろうとしている．本文では，（個人）通信，放送，交流サイトに，組織通信を加えて放送・通信分野を 4 分野に類型化し，その中で，組織通信のあり方を考察する．組織間の通信では，個人間の自由な会話と異なり，伝達情報の正確性，信頼性，迅速性，緊急性，機密性，送信情報限定性，論理的無矛盾性，各組織が公表している個人情報保護規定との整合性などのコンプライアンス性，或いは，多言語性などが厳しく求められる場合が多い． 現在，C・I・A，即ち，機密性（Confidentiality），完全性（Integrity），利用可能性（Availability）が，情報セキュリティの３要素とされているが，本文では，組織通信における情報セキュリティ概念を上記のように高度化して考察することとする．組織通信の例として，現在，総務省と一般財団法人 マルチメディア振興センターが協力して，全国的展開を推進している公共情報コモンズ（Ｌアラート）について考察する．

キーワード 放送，通信，交流サイト，組織通信，情報セキュリティ，公共情報コモンズ，Ｌアラート，組織暗号

1 放送通信の４類型—公共放送，個人放送，公共通信，個人通信

20 世紀末までは，情報伝達は，放送と通信に大別され，放送は公序良俗，通信は憲法で保証された個人間通信の秘密を守るという別々の価値観の下に共存していた．

公共放送については，NHK も民間放送も，有害情報や個人情報保護に配慮するなど，法的・倫理的な面や論理的整合性など様々な面からチェックがなされている．放送業界は，自ら放送倫理・番組向上機構を設け，外部評価を受け入れている．

他方，今世紀に入り，フェイスブックやツイッターなど様々な SNS が生まれている．SNS は，誰でも自由に，いわば個人放送局を開設して表現の自由を楽しむことが出来るようになっている．だが，比較的自由な世界であるだけに，名誉毀損，プライバシー侵害，あるいは児童ポルノなどの問題を生じている．児童ポルノの問題では，表現の自由と倫理との相克が深刻な課題となっており，緊急避難法理により，実在児童が被害を受けないよう規制されている．

1900 年頃，哲学者ヘーゲルは，「歴史とは，自由拡大のプロセスであり，自由の拡大に伴って矛盾も拡大する」と述べているが，最近の IT ，特にビッグデータの浸透などを見るとき，ヘーゲルの歴史の法則の妥当性を実感させられる．

このような複雑な様相を帯びた SNS は，個人放送局の集合体と見ることも出来るので，放送を，公共放送と個人放送という対立概念で捉えることも出来る．

放送の世界と対称的に，通信の世界では，通信傍受法

* 中央大学研究開発機構，〒 112–8551 東京都文京区春日 1–13–27, Research and Development Initiative, Chuo University, Kasuga 1–13–27, Bunkyo-ku, Tokyo, 112–8551 Japan
† 総務省
‡ （一財）マルチメディア振興センター

に抵触するような犯罪に関わる会話は別として，これまでは，殆ど制約の無い世界であった．しかし，今後は，Open data, Cloud, Big data の普及や，2016 年 1 月から予定されている My number の導入，即ち，OCBM の進展に伴い，従来の紙の文書に代わり，大量の電子化された文書が，組織間で通信される状況に変わろうとしている．即ち，個人通信とは異なる通信の世界として，今後，組織通信が広がろうとしている．

個人通信の場合，通信の秘密が憲法によって保証される中で，通信相手以外の他者に対しては，責任を強く意識することなく，比較的自由に会話が出来る状況にあるが，今後，自治体，企業，医療・介護ネットワークなどの間の組織通信においては，組織体としての，正確性，信頼性，確実性，迅速性，送信情報の限定性，耐コンプライアンス性，論理的無矛盾性や，多言語性などが求められるようになる．即ち，組織通信は，いわば公共通信という性格を帯びてくると言える．

以上を要約すると，やや割り切った分類にはなるが，21 世紀に入って以降，図 1 に示すように，放送の分野では，公共放送に対応して，個人放送が生まれ，通信分野では，個人通信に対して，公共通信が拓けようとしていると言える．

組織通信（公共通信）においては，従来，1 つの病院内で処理していた患者の情報も，ケアマネージャ，介護士，看護士やヘルパーなど，様々な方々からなる医療・介護ネットワークに流されるようになりつつあり，各職種の人に見せる患者情報を制限や個人情報保護法への配慮が必要なケースも生じている．

現在，中央大学研究開発機構では，独立行政法人 情報通信研究機構（NICT）からの委託研究を受け，組織通信という概念を提唱すると共に，その一つの特性として組織暗号と名付ける方式を開発し，長野県や新潟県において，実証実験を行っている．組織暗号とは，組織通信において，暗号文を平文に戻す機会を最小限に抑える機密通信方式である．今，県庁や市町村，或いは病院など異なる組織間で，送信側組織の担当者が，ある文書をある組織に送る場合，受信側担当者が不明な場合，受信側組織の代表者（庶務課長，事務局長等）に，暗号化された文書と，その平文のラベルを送り，受信側組織の代表者は，原則として，暗号文を復号することなく，ラベルにより，適切な担当者に再送信する方式である．暗号方式としては，楕円暗号や多変数公開鍵暗号が考えられるが，現在，楕円エルガマル暗号により鍵管理が安全に行える，

図 2 に示すような方式を開発し，自治体を対象に実証実験を行い，関係者から好評を得ている．

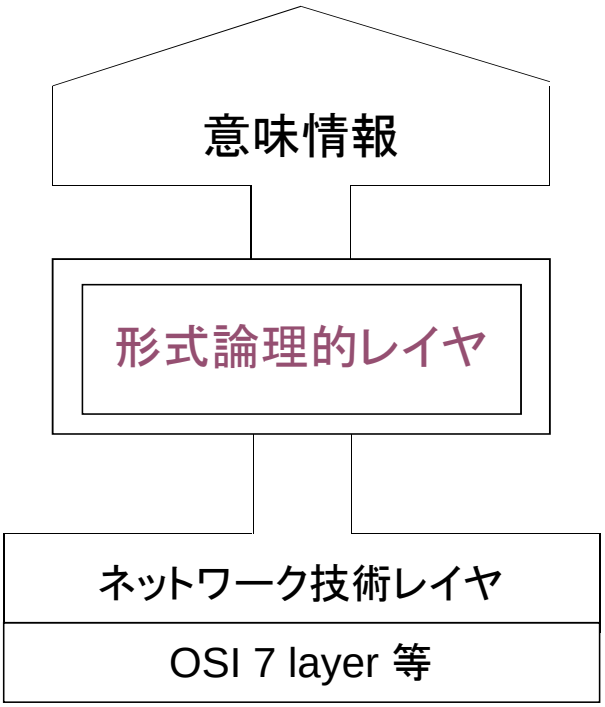


図 3: 情報通信の新階層

2　公共情報コモンズ（Ｌアラート）

（一財）マルチメディア振興センター（理事長　辻井重男）では，公益目的事業として，総務省と協力して，公共情報コモンズというプロジェクトを全国的に展開している．このプロジェクトは，災害発生時などに各自治体や消防庁などから，ばらばらに発信されていた情報を，データ形式などを統一し，放送メディアなどに伝達する社会システムを構築しようと言うプロジェクトであり，平成 19 年 7 月の新潟県中越沖地震を発端として，検討が始められたものであるが，東日本大震災以降，日本各地の自治体との連携が急速に進められている．この際，発信者側では，情報の正確性をよくチェックした上で，公共情報コモンズを通して放送メディアなどに向けて情報発信することが必須である．公共情報コモンズは，送信側組織としての各地域の自治体，国土交通省の組織，消防庁，気象庁，ライフライン系組織（電力，ガス，水道，交通機関など）と，受信側組織としての NHK・民間放送，ヤフーなどのメディアとの間の組織通信である．

2014 年 11 月現在，運用を開始した都道府県の数は 22，準備中のものを含めると 35 に達しており，順調に利用・運用が進んでいる．2014 年度に公共情報コモンズへ発信された避難勧告の件数は，2014 年 10 月末までの時点で約 2600 件と，2013 年度の 4 倍を超えている．

以下，図 5，図 6，図 7，図 8，図 9，図 10 に公共情報コモンズの概念，システム構成，運用状況などを示し

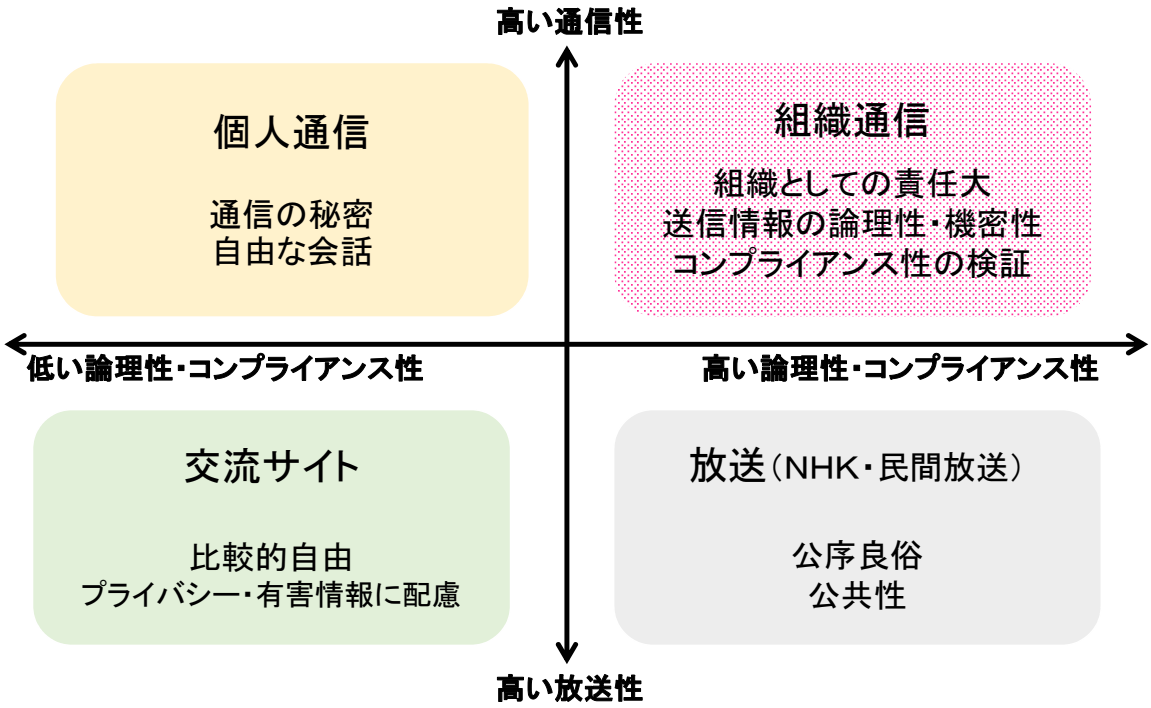


図 1: 放送・通信の 4 類型と組織通信

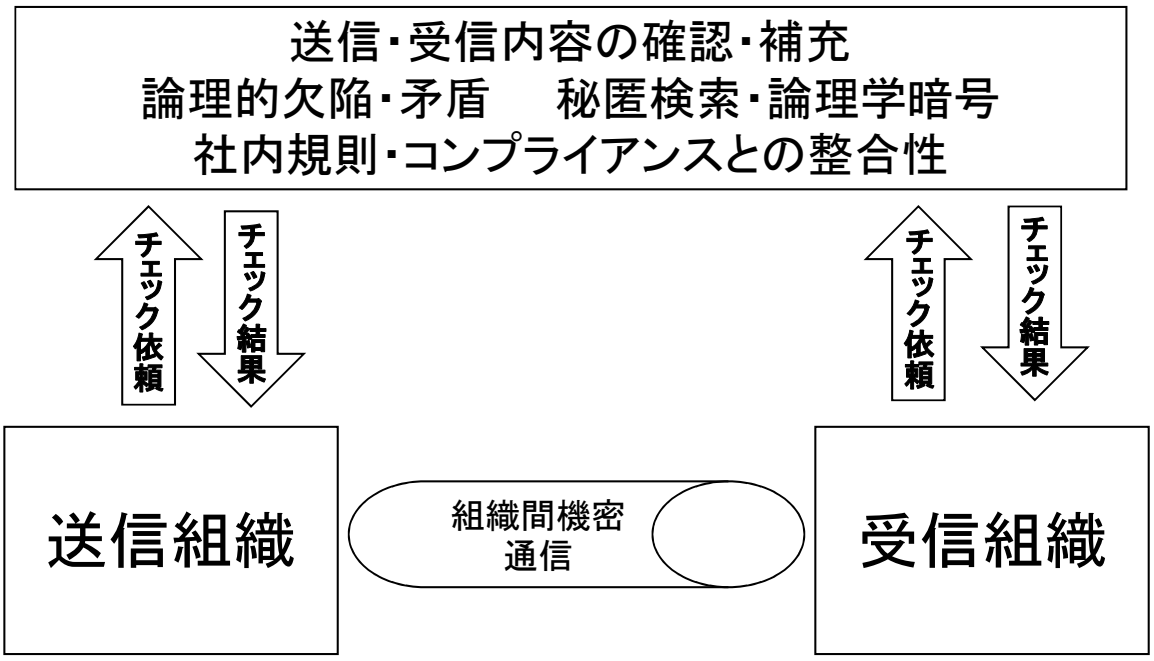


図 2: OCBM（Open data, Cloud, Big data, My number）環境下での情報通信・セキュリティ概念の高度化への対応

ておく．

謝辞

本研究は，独立行政法人 情報通信研究機構（NICT）の委託研究「組織間機密通信のための公開鍵システムの研究開発—クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて」の一環として行ったものである．公共情報コモンズ（L アラート）の推進に尽力しておられる総務省，並びに（一財）マルチメディア振興センターの関係各位に謝意を表する．また，本論

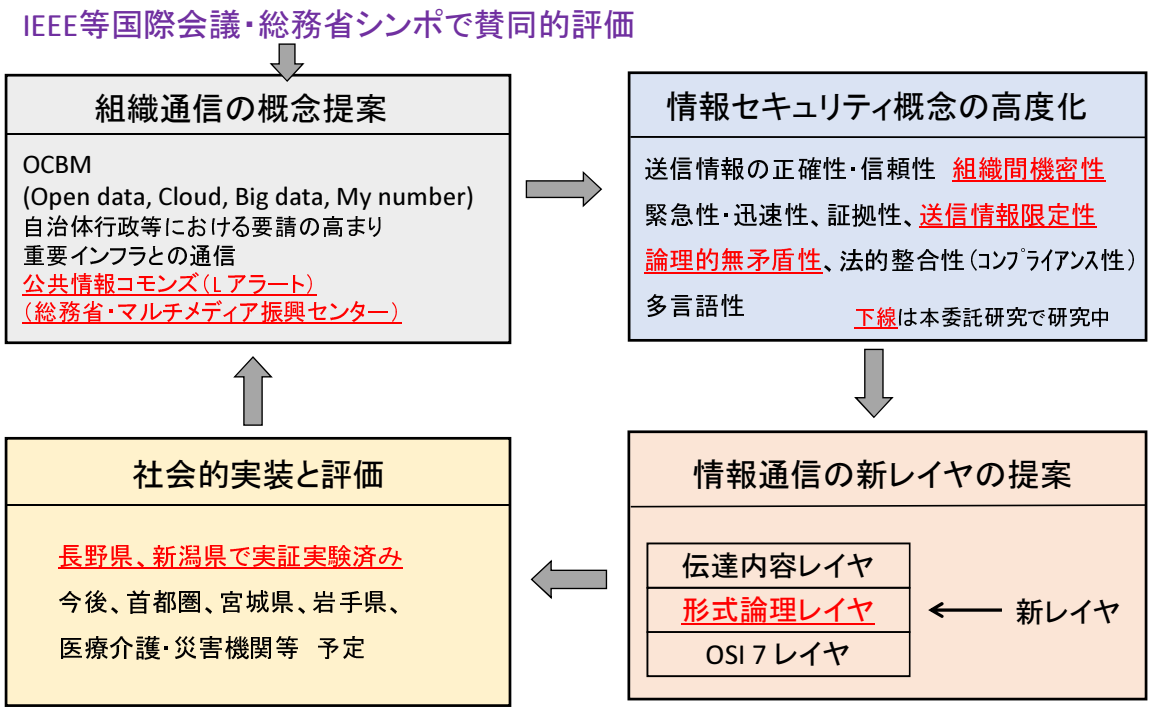


図 4: 組織通信概念の提案とその実現に向けて

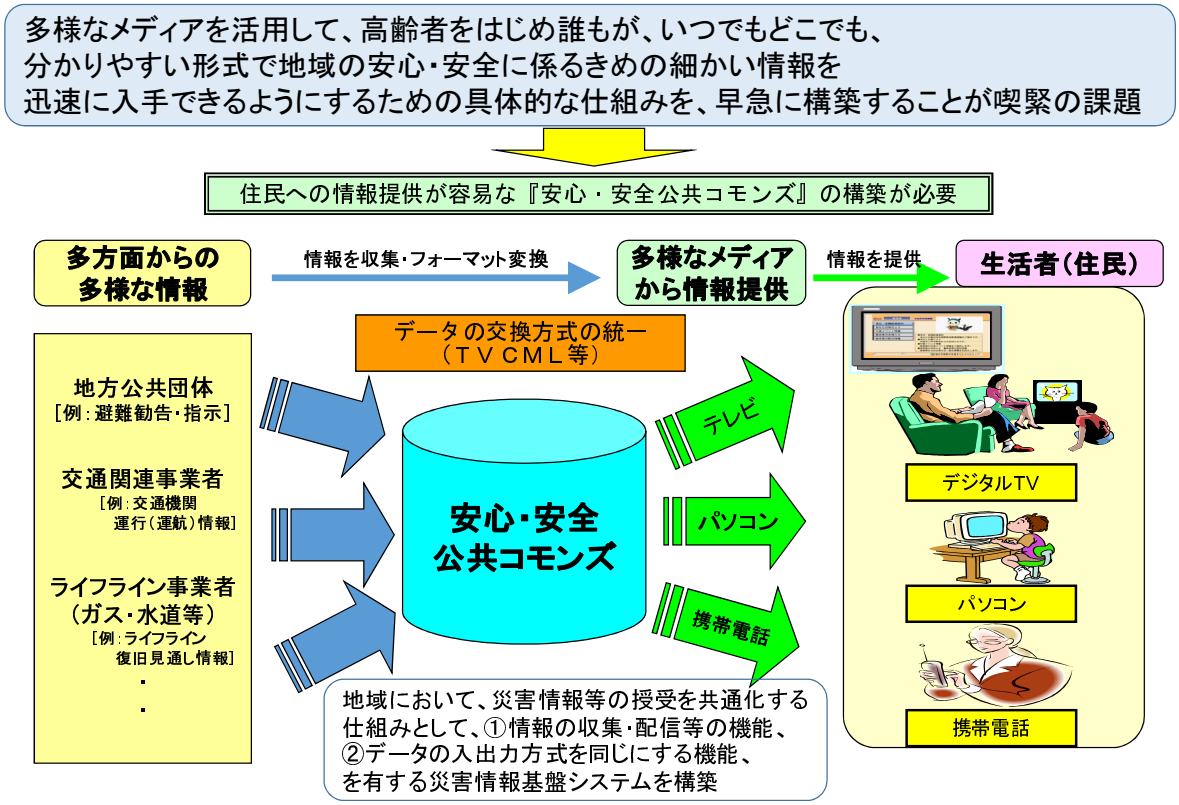


図 5: 『安心・安全公共コモンズ』の構築（総務省「地域の安心・安全情報基盤に関する研究会」報告（2008 年 7 月））

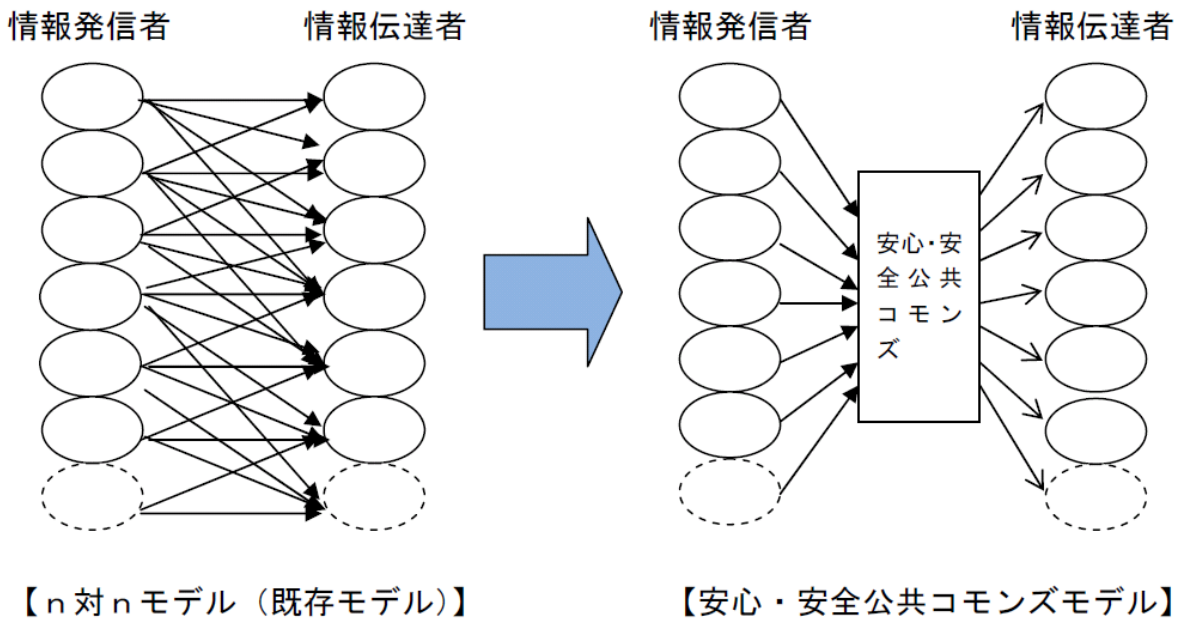


図 6: 「N 対 N モデル」と「安心・安全公共コモンズモデル」（文献 [8] P7 より）

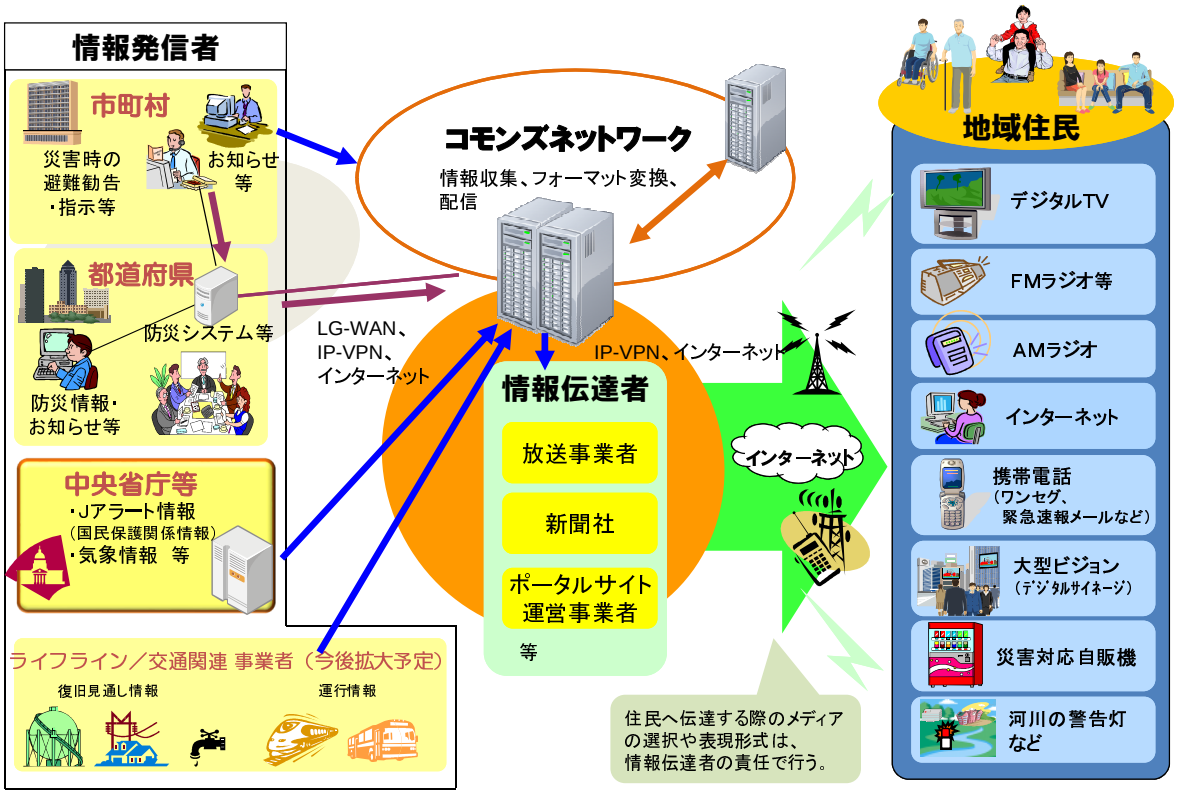


図 7: 公共情報コモンズの利用イメージ

文の編集に協力頂いた藤田 亮 中央大学研究開発機構専任研究員・助教に感謝する．

参考文献

[1] 辻井重男, “放送・通信の４類型と情報セキュリティ概念の高度化 — 組織通信・組織暗号の普及に向

情報種別	サービス開始時点	平成25年6月3日～	平成26年6月16日～
気象警報・注意報※	○	○	○
気象特別警報・警報・注意報※		※	○
指定河川洪水予報	○	○	○
土砂災害警戒警報	○	○	○
記録的短時間大雨情報		○	○
竜巻注意報		○	○
震度速報		○	○
震源に関する情報		○	○
顕著な地震の震源要素更新のお知らせ		○	○
地震回数に関する情報		○	○
地震の活動状況等に関する情報		○	○
震源・深度に関する情報		○	○
津波情報		○	○
津波警報・注意報・予報		○	○
沖合の津波観測に関する情報		○	○
噴火警報・予報			○

※　特別警報については、既存の気象警報・注意報においても、見出し文のようなところに、“【特別警報（大雨、暴風、波浪、高潮）】”などと追記

図 8: 防災気象情報（気象情報・注意報など）の対応状況

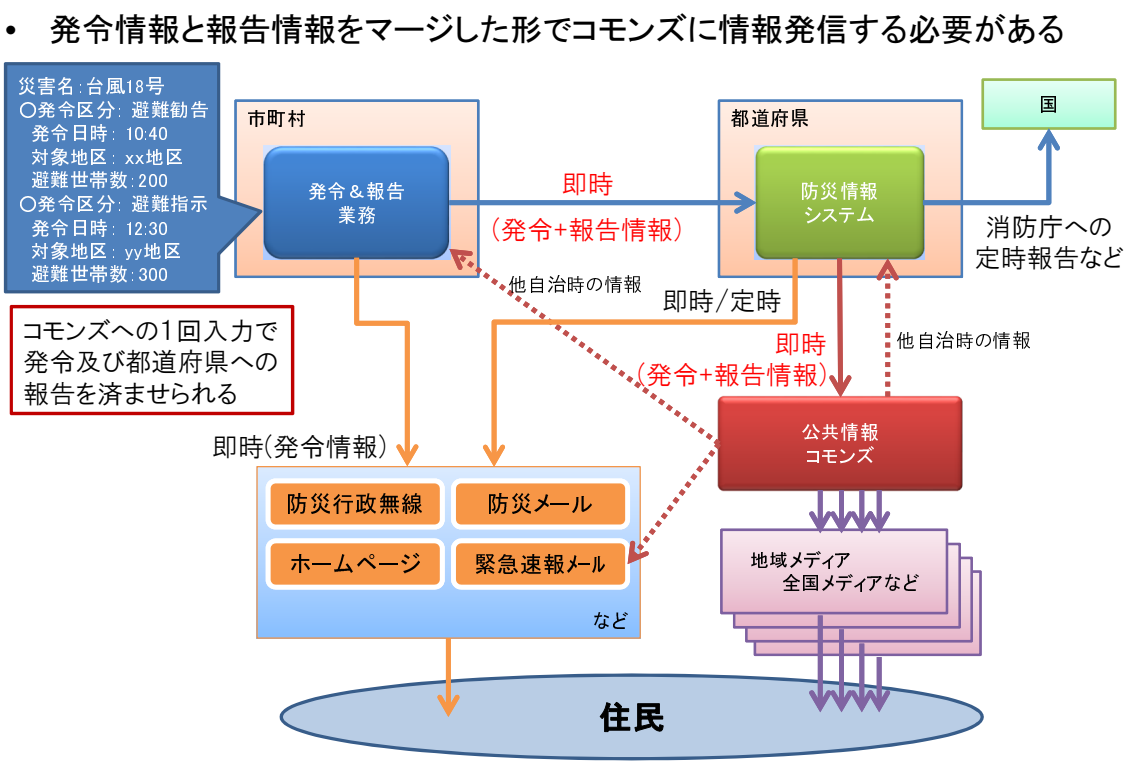


図 9: コモンズ連携後の情報の流れ

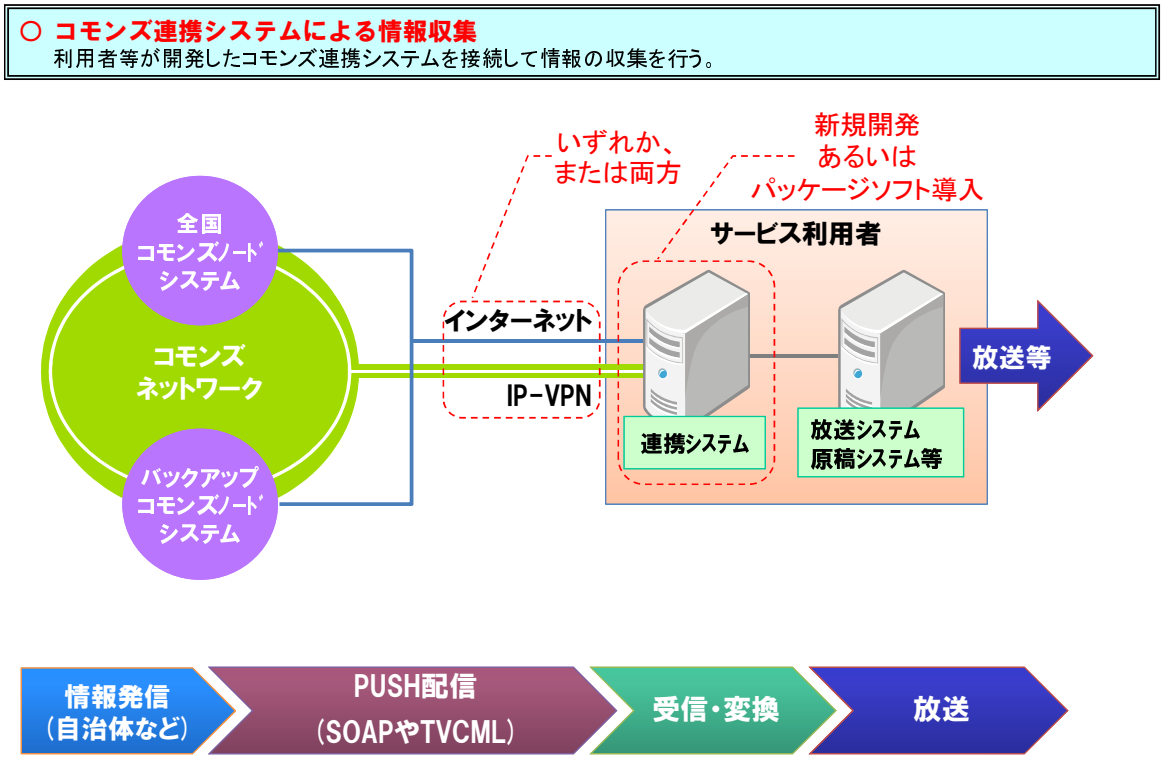


図 10: 公共情報コモンズの情報閲覧（自動連携）

けて —," *Proc. SCIS2014*, 2C4-4, January 2014.

[2] 辻井重男，“自由，安心，プライバシーと三止揚 — MELT up — 放送・交流サイト・個人通信・組織通信の枠組みの中で —，” 民放 経営四季報，No. 101 (2013.9)，日本民間放送連盟 研究所.

[3] Shigeo Tsujii, Hiroshi Yamaguchi, and Masahito Gotaishi, “Advanced Concept of Information Security as a Comprehensive Science,” Transdisciplinary Journal for Engineering and Science, Vol. 5, pp. 14-32, December, 2014.

[4] Hiroshi Yamaguchi, “Secure and Privacy Preserving Data Services in Cloud, —Cryptosystem for Inter-Organizational Communications—,” The SDPS (Society for Design & Process Science) -2013, San Paul, Brazil

[5] Hiroshi Yamaguchi, “Inter-Organizational Communication and Advanced Communication,” The ATLAS (The Academy of Transdisciplinary Learning and Studies) -2014, Asia University, Taichung, Taiwan, June 8, 2014.

[6] 辻井重男, “組織間コミュニケーションの展望と課題,” 日本計画行政学会 第 37 回全国大会ワークショップ, 2014 年 9 月 13 日.

[7] 吉田正彦, “公共情報コモンズ（Ｌアラート）の展望と課題 — 組織間通信の文脈で —,” 日本計画行政学会 第 37 回全国大会ワークショップ, 2014 年 9 月 13 日.

[8] 総務省, “「災害時等の情報伝達の共通基盤の在り方に関する研究会」報告書,” 2014 年 8 月.

[9] （一財）マルチメディア振興センター, “公共情報コモンズの概要と運用について— 地域の安心と安全のために—,” 2014 年 8 月 22 日.

付録２.

ＩＤＦコラム

2015-2-24　　辻井 重男

尸位素餐（しいそさん）とは？
―ビッグデータ時代の日本語の論理性と国際性

このところ、ＮＨＫから「第２次大戦と暗号」について取材を受けている。我々、暗号研究者は、１９７０年代以降の、情報社会の基盤としての暗号を現代暗号と呼び、２０世紀前半までの軍事・外交用暗号を古典暗号と呼んで区別している。

２０１６年からマイ・ナンバーの使用も始まり、本人確認やデジタル署名の基盤性は増すばかりだから、公開鍵暗号を初めとする現代暗号についても、メディアの関心を期待したいのだが、そうはいかないのが悩ましいところだ。

それはさておき、改めて古典暗号関連の資料を読み直してみると、それはそれで、これからの日本再生に向けて考えさせられることも多い。

冒頭にあげた「尸位素餐」という言葉をご存知だろうか。私も最近、小松啓一郎著「暗号名はマジック―太平洋戦争が起こった本当の理由」で初めて知ったのだが、「尸位素餐」とは、「高い官位にありながら、満足に職責を果たさず、給料だけを貰っていること」だそうである。

昭和１６年（１９４１年）１２月８日の真珠湾攻撃に始まる日米開戦を回避すべくアメリカとの折衝に当たっていた、野村吉三郎駐米大使は、遅々として進展しない外交交渉に失望し、「このまま、成果が挙がらないのに、給料を貰い続けるのは、心苦しいので、辞任したい」という気持ちを「尸位素餐」の四文字に託して、米国から日本に向けて暗号電文で送信したのである。この電文を傍受した、米国の暗号解読者は、日本人でも分からない漢語が分かる筈もなく、別の意味にすりかえて、米国政府に報告したのである。

これは一例であるが、暗号解読はできても、その翻訳ができず、好戦的に解釈された事例が多かったようである。こうした誤訳の積み重ねがなければ、日米開戦は避けられたかも知れないと、上記の著者は述べている。

古い話を持ち出したが、現在でも翻訳は難しい問題を孕んで

いる。例えば、情報通信分野の国際標準を日本語に、ニュアンスが正確に伝わるように翻訳するのも難しい作業である。

最近の流行語とも言えるビッグデータの正確な定義はないようであるが、多様で膨大な非定型なデータをさすことが多い。従って、文学・小説などは別として、産業、科学技術、法令などの多岐に亘る分野で、日本語で書かれた多くの文書も広い意味ではビッグデータと見なければならない。この場合、日本語の論理性と国際性が問題となる。

日本語の論理性が低いかどうかは、形態素解析（単語レベル）、構文解析（文法レベル）、意味解析、文脈解析という言語解析の４段階のどのレベルで考えるかによる。機械翻訳の場合は、形態素解析、構文解析の論理性が高い方が処理し易い。人間は、意味解析のレベルで理解できることが多いが、構文解析レベルでの論理性を高めないと誤解を招く可能性も生じる。

「赤いお墓の彼岸花」と聞けば、赤いのは、「お墓」でなく「彼岸花」だと理解できるが、

「眠れる森の美女」で、寝ているのは？と聞けば、「美女」と答える人が多い。だが、フランス語では、文法的に明確に「森」を指している。このような誤解を避ける上からも、形態素解析、構文解析レベルでの日本語の論理性を高める必要がありそうである。

イギリスでは、１７世紀末、シェークスピアから１００年近く経った頃、「我々は、このような情緒的で感覚的な言語を使っていて良いのか」と言う反省が起こり、言語の大改革を実行したそうである。

日本語の場合、平安時代は、和歌などが中心で、論理性よりも情緒性が重視されたが、鎌倉時代になると、事務処理も増え、論理性が高まったようである。近代に入り、明治の開国期、そして、第２次大戦後と言語の改革が進められたが、現在、改めて、言語について考える時期を迎えているように思われる。

尤も、これからは、ビジネス言語は英語で書かれるようになるだろうという意見も多いが、そういうケースが増えるにせよ、日本語について考える必要性が高まっていることは否定できない。

デジタルフォレンジックについては、米国における訴訟で、日本語文書の翻訳文を証拠書類として提出する際の、労力、コスト、時間が大きな問題となっており、法令や社内規則などの機械翻訳も要請されよう。ここで、法令分野について考えてみよう。

憲法のように理念を掲げる場合は別として、一般の法律や条

令などは、論理的に明解でなければならない。北陸先端科学技術大学院大学では、片山卓也前学長が研究リーダーとして推進した２１世紀ＣＯＥ以降、法令工学プロジェクトを進めている。法令工学とは、法令を社会のソフトウェアーと考えて、法令間の矛盾、たとえば、法律と条例との矛盾の検証や、法令文自体の論理性のチェック等の情報処理を進める学問である。法令工学では、日本語の論理性を高める研究、及び、自然言語処理に適するように、直観主義論理や様相論理などを用いて、論理学を多様化・高度化する研究という両面からのアプローチによる考察を深めている。

私も、２年ほど前から、暗号文を論理式で表すと言う発想で、研究を開始した関係で、論理学を俄か勉強していることもあって、法令工学の動向を興味深く見守っている。

いずれにしても、ビッグデータ時代には、日本語の論理性と国際性を高める研究は不可欠であろう。