

歴史を変え、情報社会を拓いた暗号

ーテクノロジーと数学のかかわりの歴史を鳥瞰し、
暗号技術の将来を考えるー

2007年7月14日

笠原 正雄

E-mail: kasahara@utc.osaka-gu.ac.jp

本講義のポイント




- 数学とテクノロジーのかかわりの歴史を鳥瞰し、暗号技術、そしてより広く情報技術、情報通信技術への「数学」の貢献について考察し、このことを踏まえて将来を展望する。
- 上記を講術するにあたって、“基本を大切に”ということを中心に掛ける。
- 安全、安心の保証された情報社会を構築するため数学、テクノロジーを強化することが必要であることを述べる。

問1:テクノロジーとは

テクノロジー = テクネー + ロゴス (ギリシャ語)
技術 術 理

ロゴスは多義語。言語, 理, 意味, 調和, 理性などの意味がある。動詞形レーゲンは数える, 集める, の意味。

私のコメント: テクノロジーは歴史的には,

テクネー  テクノロジー  テクネー  テクノロジー
と変遷していると思われる。再びテクネーとなるのか？

テクノロジーと呼ばれるにふさわしい姿勢で技術を追求することが私達に望まれている。

問2: 日本語の「技術」とは。テクネーとは。

にしあまね

(I) 西周『百学連環』:

Mechanical Art → 器械技。技は“手足を働かす”の意。→手足を働かせて機械を働かすこと。技術と訳すべし。

(II) ハイデッガー:

テクネーは「蔽いをとって表わす働き。すなわち真理の自己顯示。」ここに真理とは、アレーティアすなわち蔽われていないこと。

(III) 笠原:

テクノロジーはせめて技術道と訳すべきであった。

(1) www.klnet.pref.kanagawa.jp

(2) 本多修郎: 技術の人間学

(3) 笠原正雄: “情報技術の倫理. その基本の基本”

電子情報通信学会「技術と社会. 倫理研究会」(2007-12)予定

テクノロジーの変遷 I

・人間の生の技術の根本は「測る技術」である。
バビロニアの占星術に由来する「測る神」への信仰。
(神は世界に数的比例調和を与えた。)

・ギリシャの「ロゴス思想」は普遍的な形, あるいは
数的比例調和を世界の根本と見る。
自然哲学(数学特に数論)が自由人の中で発展。
・テクノロジーはロゴスが抜けたまま奴隷の世界へ
(プラトンのテクネーの分類参照)

本多修郎『技術の人間学』朝倉書店(1975-04) より ©

プラトンによるテクネーの分類

| テクネー | |
|----------------------------------|--------------------------------|
| 獲得術 | 制作術 |
| 学習術, 知識獲得術 金利獲得術, 闘争術, 狩猟術 | ・ 実物制作術(農耕術, 医術, 建築術, 道具技術) |
| | ・ 影像制作術(類似像制作術, 幻像制作術) |

本多修郎『技術の人間学』朝倉書店(1975-04) より ©

ギリシャの「数学」. その一つの側面

ピュータゴラス (BC570-497) は数学者であり, また宗教家でもあった. 神秘宗教教団を創設したが教団員は輪廻転生を信じていた. ピュータゴラス派の「数学」は数論, 音楽, 天文学, 幾何学であった. 音楽・天文・幾何など, 宇宙に現れる善で公正な配分の妙 (調和均衡) を知ることによって魂が浄められ, より良く生まれ変わると信じていたと云われている.

「数学」とアイデア思想

数学的完全な円はアイデア界にのみ存在する。人によって描かれる円はアイデアとしての円の“写し”である。地上にある事物は全て、アイデア界にある事物の“写し”である。

・・・地上にある事物を描く画家は“写し”の“写し”を作る者に過ぎない。プラトンはこのような立場から絵画、詩作を評価した。

古代音程理論の数比

音程の近親度は振動数(弦長)の比で与えられる。

数比の単純さが協和度の判定規準。

協和するのは,

1:2のオクターブ

2:3の5度, クインテ

3:4の4度, クワルテ

ロゴスは社会に如何なる影響を及ぼしたか

- ロゴスは社会には直接的貢献をしなかった.
- テクネーの発展とバランスをとって余りある古代ギリシャの詩人*, 思想家の哲学, プラトン, アリストテレス等々の偉大な「技術哲学」が存在.

* 例えば三大悲劇詩人の一人, アイスキュロスの『縛られたプロメテウス』などの思想...

テクノロジーの変遷Ⅱ

- ・中世. テクノロジーは停滞. 牧歌的平和な時代.
- ・ルネサンス以降, アグリコラの鉱山技術, フランシス・ベーコンの技術哲学, ガリレオ, デカルトの哲学・数学, ニュートンの物理学, により, ロゴスを伴ったテクノロジーが復活, 発展.

- ・古代ローマの建築学者ウィトルー・ウィウスの著書:
『ウィトルー・ウィウスの建築書』
- ・ドイツルネサンス時代の鉱山学者アグリコラの著書:
『デ・レ・メタリカ(金属について)』

の思想はテクネー＋ロゴス＝テクノロジーへの復活を強力に主張した。
ウィトルー・ウィウス, アグリコラは技術史に残る2大巨星である。

科学と芸術

- ・ 科学と技術とは密接に関連しあうが、歴史的には別の道を歩んで発展してきた。科学は長い間、実際的应用については無関心を通してきた。一方技術は科学の成果を利用できるときにも、科学からの助けをあざ笑うようなことが再三あった。
- ・ 科学と技術の協力が可能であり、望ましいという主張は17世紀初頭頃より、イギリスのフランシス・ベーコン、フランスのルネ・デカルト、オランダのシモン・ステヴィンによって主張されたが、それが実行に移されたのは18世紀のことである。

(以上フォーブス・ディクステルホイス『科学と技術の歴史』
みすず書房(1977-09) 序, p2より)

我が国のセキュリティ上の最大の問題

- ・明治維新以降、我が国にはロゴスが抜けたままの西洋技術がテクネーの形で直輸入されつづけている。
- ・ロゴスが未成熟なまま今もテクネーが輸入されていないか「個人情報保護」等々の法律、ガイドラインは十分なロゴスを伴って受け入れているか。

我が国の技術はロゴスが欠落。これが最大のセキュリティ上の問題。

因みに自然に対する技術支配の思想を確立したフランシス・ベーコンの有名な言葉

“Nature obeyed and conquered”

は我が国において理解されているか。

ロゴスの欠落が我が国を環境公害最先進国にしたのではなかったか。ロゴスの欠落が、社会システムに脆弱さを日増しに大きく生み出しているのではないか。我が国はロゴス欠落最先進国になるのではないか。

Nature obeyed and conquered 自然はそれに従うことによってのみ征服される

人間は自然を征服し、制御し、利用することが可能であるが、そうするためには人間は自然の法則に従わねばならない。そうするためには自然の研究をとおして自然のもろもろの法則を学ぶのでなければできないことじゃない。ひらたく言えば技術はその基礎として科学をもたねばならず、科学は技術を可能とする。

ギリシャの「数学」とは

古代ギリシャの「数学」は以下の分野から成る.

- 1. 数論
- 1. 天文学
- 1. 幾何学
- 1. 音楽

ギリシャの幾何学はエジプトの「測地術」に由来する.
しかしプラトンは

“Geometria (測地術)は滑稽なもの”

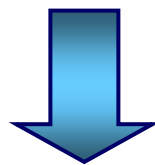
と評した.

幾何学が数論に組み入れられたことの影響とは

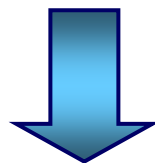
幾何学は測地術どころか、空間的形象の学でさえない



イデア思想への帰結



中世キリスト教世界に前向きに受け入れられる



ガリレオの「科学革命」の精神的よりどころ

ガリレオの科学革命

ガリレオが、“科学革命”で対峙したのは、彼よりも、2,000年以上も前に生きたアリストテレスである。より厳密には、アリストテレスの宇宙論、運動論を善しとするキリスト教会（特にイエズス会）と対峙したのであった。

革命には多くの場合、“復古の御旗”が振られるといわれている。ガリレオの場合もまた、例外ではない。実際、彼は著書『儀金鑑識官』において、「哲学は、宇宙という壮大な書物の中に書かれている。そしてこの宇宙は、常に目の前に開示されて存在する。けれど、書かれている文字が読めなければ、この宇宙なる書物の理解は不可能である。この書物は数学の言葉で書かれており、その文字は、三角形、円等々の幾何学的図形である。これらの文字がなければ、この物語は、一語たりとも理解できない。人はただ迷宮の中をさまよい歩くばかりである」と述べている。

“数”の原理性・規則性が世界の秩序を成すと受け取られていた古代ギリシャの、とりわけプラトンに代表される伝統的な世界観に立ち返ることを、自らが遂行する科学革命の精神的よりどころとしていたように思われる。

（以上 笠原正雄：情報技術の人間学，電子情報通信学会，コロナ社(2007-02)より）

ガウス, フェルマー, オイラーの数論研究の モチベーションを探る

バビロニアの数神秘思想, ピュータゴラスの宇宙は数であるという考え, プラトンのイデア思想, そして古代ギリシャから受けつがれてきた「数」の世界が持つ神秘性, 際限もない奥の深さが, 数論研究への強いモチベーションであったことがガリレオの言葉から推定される.

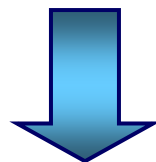
肥大化した18~20世紀のアナログ的科学技術が上記のモチベーションをおおい隠し, “数論は女王のように美しいが役に立たない”と揶揄された時期があった.

21世紀サイバー社会を可能にするもの

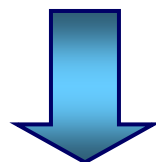
- バビロニアーギリシャの数神秘思想こそが17～20世紀、数論の成長をもたらした.
- 20世紀の科学技術を力強く支えたさまざまな“役立つ数学”の影で“数論は女王のように美しいが役には立たない”と^{やゆ}揶揄された.
- 21世紀サイバー社会の構築を可能とする現代情報技術を根底から支えている「数論」を軽視し、テクネーにのみ走ることは大きな危険と隣り合わせ.
- 「数論」重視の姿勢が必要.

数学と暗号技術の将来(1)

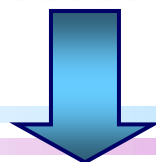
(Ⅰ) 数論を重視する姿勢こそがサイバー社会を構築するための基本姿勢. 将来信じ難いレベルの技術を数論は将来も創出するであろう.



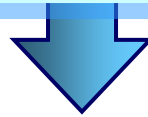
(Ⅱ) にも拘わらず数論とその応用研究者の貢献は残念なことにサイバー社会の喧騒の中で忘却されるであろうか.



(Ⅲ) そうであれば私達は何のモチベーションで研究するのか.

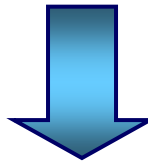


数学と暗号技術の将来(2)



(Ⅳ) 古代ローマ時代の建築家ウィトルウィウスしゅろの言葉に耳を傾けよう

“古代ギリシャの昔、オリンピックの勝者は棕櫚の冠をかむり四頭馬車で凱旋し、終身年金を受ける。しかるにピュータゴラス、デーモクリトウス、プラトー、アリストテレースは何も受けていない。(神のような知恵と意志によって世界を支配し、勇気でもって敵をことごとく打ち破るインペラートル。カエサルよ。)これらの人々に名誉が与えられて然るべきことを私は告白したい。



(Ⅴ)ピュータゴラス、デーモクリトウス、プラトー、アリストテレスは情報学者である私の拙著にすら登場する。現在、さまざまな分野で広く知られ深く尊敬されている。(Ⅱ)の私の危惧はあたらぬであろう。

* 上記(Ⅳ)のかっこ内の文章は私による補筆。ウィトルーウィウスはオクターヴィアヌスに対し、このような姿勢をもっていた。

梶井剛「電話発明六十周年記念に就て」(1936年)より

ベルの電話に関する発明はラジオ或は国際無線電話或はトーキーとなり社会百般の文化の進運に貢献。

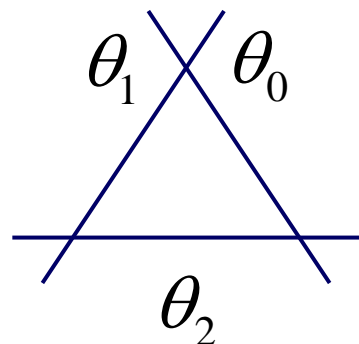
世界に於ける人類間の意思の疎通即ち言葉を換えて申せば世界の和平を増進する上に於て比類なき功績を挙げた。

今日に於ける世界人類の闘争は若し電話の如き国民相互の了解の具なかりせば一層甚だしかるべきことは容易に予想せらるる。

最近科学の進歩が国民として又人類として如何に重要なやを社会に於いても稍認識する様に相成りましたが由来科学者が黙々として其の研究に没頭して功績に報いらるることなくとも天職と信じて生涯を捧ぐる心持は極めて貴いことでありまして後世に於いて初めて其の恩恵をたたえらるることより外報いらるる途のないことは甚だ遺憾と考える。

(後略)

球充てん問題: 2次元の場合



インシデンス行列



$$H = \begin{bmatrix} \theta_1^2 & \theta_1 \cdot \theta_2 \\ \theta_1 \cdot \theta_2 & \theta_2^2 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ 1 & -2 \end{bmatrix}$$

タイプ I_3 の特異ファイバ

— H は2次元平面の球充てんを与えるグラム行列に一致！！

θ_1^2 : 自己交点数は-2回である(交点理論)。

笠原正雄: 格子理論とその応用へのガイダンス, 代数曲線とその応用論文小特集, 電子情報通信学会論文誌, A, (1999-08)より

三角関数と楕円関数の不思議

表1: 三角関数と楕円関数

Table1: Trigonometric function and elliptic function.

| | | |
|--------------------------------------|--|---|
| $\omega_i(u)$ | $\int_0^u \frac{dz}{\sqrt{1-z^2}} = \omega_0(u)$ | $\int_0^u \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}} = \omega_1(u)$ |
| Inverse function of $\omega_i(u)$ | $f(\omega)$ Trigonometric function | $\wp(z) = \frac{1}{z^2} + \sum'_{\omega \in L} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}$ Elliptic function |
| Periodicity of function | Simple periodic function | Doubly periodic function |
| | $f(\omega)^2 + f'(\omega)^2 = 1$ | $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ |
| Domain/Period | Circle | Torus |

笠原正雄: 格子理論とその応用へのガイダンス, 代数曲線とその応用論文小特集,
電子情報通信学会論文誌, A, (1999-08)より

数学と電子情報通信技術のつながり

(Ⅰ) 19世紀～20世紀中頃

数学は主として実験結果の説明役.

例. カーソンのFMの帯域圧縮効果に対する理論的な反証.

(Ⅱ) 20世紀デジタル時代を先駆けた理論

1928年のナイキストの「波形伝送論」そして
シャノンの通信に関わる「数学理論」に代表されるように
数学は将来の技術の可能性を示唆する.

例. ナイキスト理論は高速通信技術, そしてシャノン理論は
誤り制御技術の発展の基盤を構築した.

(Ⅲ) 1960年以降

デジタル通信の技術の発展にうながされて, 数学が技術的手法
を直接創出する役目を担う.

例. ガロア体, モーデルヴェイユ格子
ユークリッド互除法, ヴェイユペアリング
オイラーの定理, 中国人の剰余定理, 因数定理, 等々が暗号技術,
通信技術に直接的に新手法を与えている.

輝かしい未来社会を我が国に実現するための三箇条

- 大学, 企業, 国, 自治体等々の構成メンバーには, それぞれが携わる仕事の中で, 以下の姿勢をとることが希求される.
 1. 仕事に関わる“現状”を正しく把握すること.
 2. 仕事に関わる“普段着の哲学”を持つこと.
 3. 仕事に関わる歴史を知り, これを輝く未来の到来につなげること.

普段着の哲学:

- ・湯川秀樹: 新生の科学日本に寄せる, 科学朝日(1945-10)
- ・笠原正雄: 情報技術の人間学, 電子情報通信学会, コロナ社(2007-02)

普段着の哲学で私が、今、気にしていること

「情報」、「インフォメーション」、「技術」、「テクノロジー」、「情報技術」、「IT」、「倫理」、「モラル」等々のキーワードが我が国では曖昧に定義されているのでは？

このように非常に大切な部分が漠としたままで思想が述べられ、議論が展開されているのではないか。

笠原正雄：“情報技術の倫理. その基本の基本”

電子情報通信学会「技術と社会. 倫理研究会」(2007-12)予定

例えば情報とは？

小学館発行の日本国語大辞典によれば“情報”とは、以下のようである。

- (1) 事柄の内容, ようす. またはその知らせ.
- (2) 状況に関する知識.

では, 情報の“情”とはどういう意味であろうか？ 同辞典によると“情”の意味は次のように五通りに分けられるが, 情報の情は, 第四番目の意味であると記述されている。

- (1) 心に感じて動くはたらき. 感情, 情緒等.
- (2) いつくしみの心. 愛情, 厚情等.
- (3) 異性を思う心. 恋情, 情事等.
- (4) ありさま, ようす. 状況, 国情, 情報等.
- (5) おもむき, あじわい. 詩情, 旅情等.

情報とは“ありのままの知らせ”である。

そしてインフォメーションとは？

- ・ ドイツの哲学者ハイデッガーは「Information」について、「Informationはインフォームする. すなわち情報は、報道と同時に形成し、整列させ、整頓させる...」という興味深い内容の解釈を与えている. しかし、私見ではあるがインフォメーションには、in(内部, 心に), form(形づくる)というニュアンスが感じられ、いくぶん干渉的である.

秋富克哉:テクノロジー論 I, 京都工芸繊維大学講義資料

笠原正雄:情報技術の人間学, 電子情報通信学会, コロナ社(2007-02)

インフォメーション車と情報車

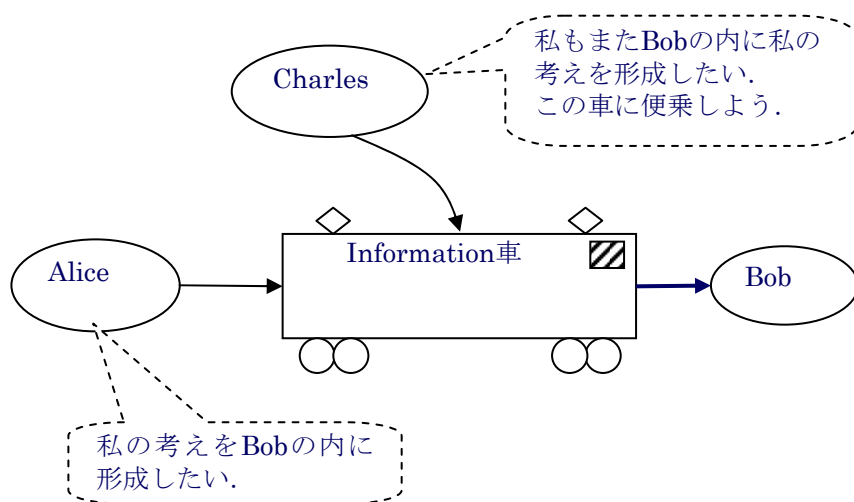


図1 (a)

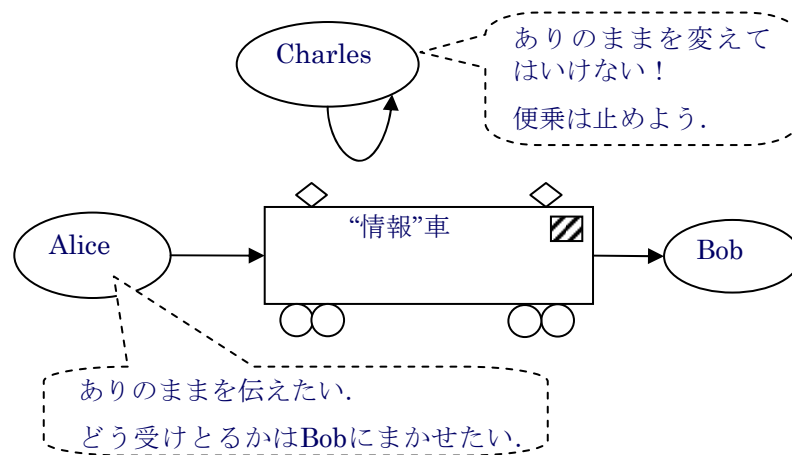


図1 (b)

インフォメーション車は相乗りOK？

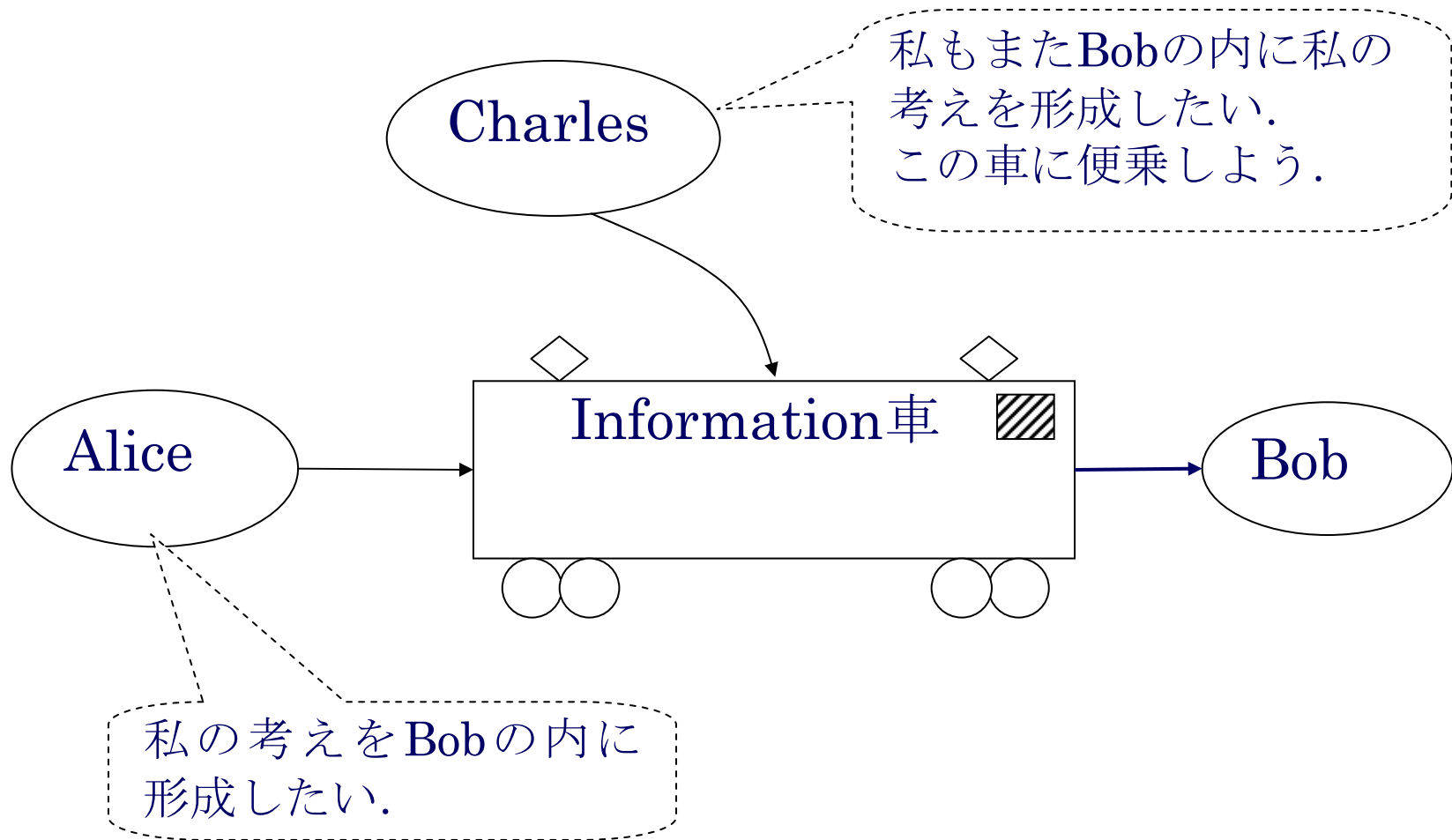


図1(a)

情報車は相乗りNo！

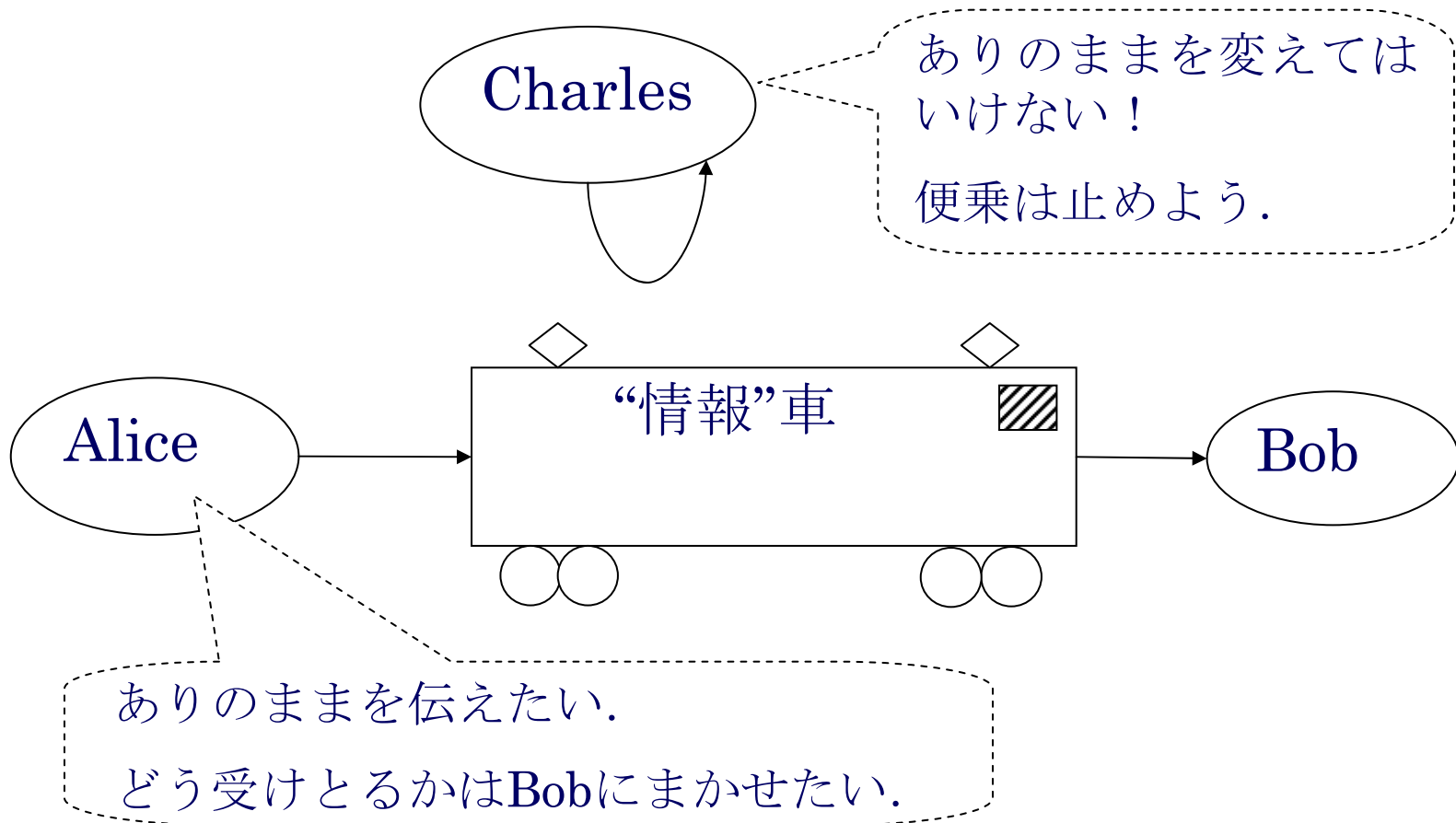


図1 (b)

情報技術とは？

「情報技術」という言葉は、技術史の中にしっかり軸足を置いて考えてみると

- ・演算技術(信号処理技術を含む)
- ・記録技術
- ・通信技術

を中心とする技術とその応用技術であることが明らかである。周知のように上記三つの技術のことごとくが1960年前後より指数関数的成長を続けている。

このことこそが世の中を急速に変革していく非常に大きなエネルギーとなっている。社会を支えるこれらの基幹的な技術が半世紀もの間恒常的に爆発的成長をつづけるといった事態は、技術史上全く未経験のことであった。上記三つの技術の発展こそが結果的に今日のサイバー社会をもたらした最大の原因である。

「情報技術」という言葉の有する真の意味を技術史の視点からしっかり理解する必要がある。

ITとは？

ITとはこれら三つの技術とその関連応用技術であって、サイバー社会で展開するビジネスのために情報をやりとりする技術ではない。

にもかかわらず我が国のマスコミ等で使われているITはInternet Technology, あるいはインターネットを利用するビジネスを意味する場合が多いように思われる。ITは本来、前述のような純粋に工学的に定義される“情報技術”であって、Internet Technologyとは厳密に区別されなければならない。

あいまいな用語の使用は様々な混乱(誤った政策等)を招いており深く憂慮すべきことである。

笠原正雄: 情報技術の人間学, 電子情報通信学会, コロナ社(2007-02)

将来、暗号技術を大きく拓かせるポイント

- ① 「数学」を最重要視し、研究、教育態勢を充実させること
- ② 行政の中にプロ中のプロを作ること
- ③ 普段着の哲学(ものの見方、考え方)をしっかり持つこと
- ④ 技術史の中で現在の状況を考え、将来を展望すること. そして現状から目をそらさぬこと

数学, 科学, 技術の順に大切

坂本昂は電子通信学会雑誌(1988-09)においてアメリカの Popular Computing誌(1984年頃)に寄せられた同誌編集者ワットの以下のような興味深い文章をその論文の冒頭で紹介している。

コンピュータリテラシーの推進者たちは、我が国は、ハイテク生産性レースで、日本と西ドイツに負けつつあると論じている。かつての1950年代、ソ連が最初の人工衛星スプートニクを打上げたときを思い出し、推進者たちの説き口は、アメリカが貧しい第三世界に入るのを防ぐため、数学、科学、技術に新たな重点を置くことを要求している。

サイバー社会の構築を可能にするもの

20世紀中頃より指数関数的成長を開始した情報技術の基盤を数論が構築した。

誤り制御技術, 暗号技術の飛躍的發展を数論が支え, サイバー社会の構築を可能としている。

例. ガロア体, モーデルヴェイユ格子
ユークリッド互除法, ヴェイユペアリング
オイラーの定理, 中国人の剰余定理, 因数定理, 等々が暗号技術,
通信技術に直接的に新手法を与えている。

私の大きな期待—むすびにかえて—

中央大学研究開発機構「情報セキュリティ・情報保証人材育成拠点」，“暗号講座”が半年間にわたって開催予定。

多数の参加者，講演者を集めて充実したカリキュラムのもと講義（14コマ）が行われる．当該分野の知識だけでなく，現代では人類が直面している大きな変革の時期であることを肌で感じ，この分野の底辺の拡大が力強くなされることを期待したい．