1994･TS-Tokyo-Tech-EEIC-Engrg.

辻井重男　「デジタルセキュリティ総合科学の構築 ―DX 社会基盤の創設に向けて」

TSUJII　Shigeo　“ Construction of Integrated Security for Digital Transformation”

略歴：

1933 年 9 月 13 日生　1958 年 東京工業大学卒業、1970 年 工学博士
1979 年　東京工業大学教授、1994 年 中央大学教授、
1996 年　電子情報通信学会　会長
1999 年　中央大学研究開発機構　機構長
2003 年　日本学術会議 会員
2004 年　情報セキュリティ大学院大学初代学長
2004 年　中央大学研究開発機構教授
2007 年　日本ペンクラブ会員
2010 年　（一財）マルチメディア振興センター理事長
2013 年　（一財）放送セキュリティセンター理事長
2017 年　（一社）セキュア IoT プラットフォーム協議会理事長
瑞宝中綬章、NHK 放送文化賞、C＆C 賞、高柳記念賞、電子情報通信学会功績賞、
IEEE 第三千年記 記念賞、発明表彰等
郵政省 電波監理審議会会長、総務省・内閣等の諸官庁における、電子署名法、
住民基本台帳法等の多くの法制度創設に関する委員会委員長を歴任。
デジタル信号処理、現代暗号理論に関する学術論文発表・デジタルセキュリティ
総合科学構築・三止揚―MELT-UP の提案、及び、光輝会（シニア研究者から
成るグループ）の設立等、現在まで研究・人材育成活動を続けて来た。

研究成果の学術的・社会的インパクト

（1） 社会的背景と研究経路 60 余年

60 余年に及ぶ、研究・教育生活を振り返るとき、当然ながら、社会の変化、人との出会い等が、私の小さな研究成果に強く影響していたことが思い出される。最近、話題となっている DX (Digital Transformation), 即ち、デジタル技術による社会変革は、１９５８年、日本電気（NEC）株式会社に入社した頃から始まっていた。１９６０年前後、NEC は電電公社（当時）の傘下にあってアナログ伝送方式からデジタル伝送方式への変換を進めていた。その中で、辻井は日本初のデジタル伝送方式（PCM２４CH 方式）を開発し、また、カラーテレビの時代を予想して雑音抑止のデジタル化に関する特許を取得し、発明表彰を受けた。

その後、大学に転職した後、アナログ処理に代るデジタル信号処理の研究を先導した。

２０２０年、コロナ禍の中で、テレワークが広がり、電子ハンコが話題となっている。電子ハンコとは、公開鍵暗号の秘密鍵による電子認証・署名のことである。印鑑登録証明が利用されない欧米諸国では、デジタル化の進展にとなって、手書き署名が出来なくなったらどうするかが深刻な課題となり、１９７０年代後半、Digital Signature の為に、公開鍵暗号という、数千年に及ぶ暗号の歴史上、画期的な方式が創造されたのである（その数年前、英国の諜報機関で、鍵配送の為、公開鍵暗号が発明されていたが、秘密にされていた)。暗号といえば、情報秘匿が連想されるが、公開鍵暗号の主用途は、本人認証・署名であり、IoT も含めた真正性保証なのである。筆者は、１９９０年代、日独国際会議の招待講演で、日本には印鑑登録証明という制度があると紹介し、ドイツ人たちを驚かせたことがあった。しかし、認証・署名の電子化では、諸外国に大きく遅れてしまった。筆者は、公開鍵暗号の数学的構造の美しさに魅せられて、１９８０年初頭から暗号理論研究を始め、現在、話題となっている耐量子コンピュータ暗号の一つである多変数公開鍵暗号方式を提案した。当時は、セキュリティに対する社会的意識は低く、暗号は、「軍事外交だけでなく、情報社会にも必要なのか」という意識で話題を呼んだ。その後、社会基盤の底に沈み、社会的関心は薄れたが、最近、ブロックチェインや暗号資産等で、再び関心が高まってきたようである。

１９９０年代は、情報セキュリティ＝暗号　という雰囲気であったが、暗号だけで情報セキュリティが確保できる筈はないと思い、テレビジョン学会（現在、映像情報メディア学会）の招待論文で、情報セキュリティ総合科学を構築の必要性を訴えた。

その後、２０００年前後から、デジタルセキュリティを理念と現実という視点から考察し、自由の拡大、公共性確保、個人の権利・プライバシィの三者を理念と定め、それらの矛盾相克しがちな三理念を可能な限り高度に達成すべく、管理・経営（Management），倫理（Ethics），法制度（Law），技術（Technology）を実現手段とする方策を、三止揚・MELT-UP と称することとし、内外の学会などで提唱して来た（図１参照)。

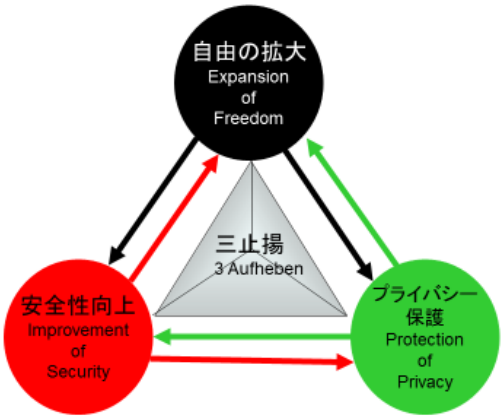

図１　三止揚

２００４年、中央大学を定年退職し、情報セキュリティ大学院大学の初代学長に就任した際、大学の理念として、三止揚・MELT-UP を掲げ、技術のみでなく、法制、管理経営などの分野からも一流の人材を教授として招いた。情報セキュリティ大学院大学は、社会人学生が多いが、技術系出身の社員が、法制度を学習するケースも多く、人材育成に貢献している。また、電子情報通信学会倫理研究会（現在、技術と社会・倫理研究会）の創設に尽力した。

中央大学では、１９９９年、外部資金により運営する研究開発機構が設置され、辻井は初代機構長に任命され、定年退職後、現在に至るまで、プロジェクト研究資金を獲得し機構教授を続けて来た。その間、ポスドクと合わせて、定年退職後も研究意欲旺盛な約１０名のシニア研究者が筆者のグループに加わり、セキュリティを初め、ブロックチェインやデジタル通貨などの分野で多くの成果を挙げている。

（２）　研究成果の概要

Ⅰ．１９５８年（昭和３３年）～１９６５年（昭和４０年）日本電気（株）勤務

① 日本初のデジタル伝送方式（PCM２４チャンネル方式）の開発

② 世界初のテレビ信号のデジタル方式の開発。

カラーテレビのデジタル化で特許取得・発明表彰

説明：

当時、カラーテレビは実用化されていなかった。私は、白黒テレビでデジタル化の実験を行っていた際、これが、カラーテレビ信号なら、デジタル化された画面に大きな雑音が発生することになるのではないかと想像し、それを防ぐ為、標本化周波数を NTSC 信号の３倍とするデジタル化方式を提案した。

後に、「放送事業部が今日あるのは、あの特許のお陰だ」と言われたそうである。

Ⅱ．１９６５年（昭和４０年）～２００４年（平成１６年）　山梨大・東工大・中央大勤務

③ デジタルネットワークのグラフ理論的研究。電子情報通信学会 論文賞受賞

④ デジタル信号処理の先導的研究開始。電子情報通信学会 論文賞２件受賞

１９８０年頃から現代暗号の研究を開始。

⑤ １９８５年　順序解法による多変数公開鍵暗号方式の提案。

多変数公開鍵暗号は、現在、米国の NIST において、耐量子公開鍵暗号の候補となっている日本発の公開鍵暗号である。松本・今井による MI 暗号に続き、１９８５年、辻井は、回路網構成からヒントを得て、順序解法型多変数公開鍵暗号を提案した。１９８０年代、多変数公開鍵暗号の研究を行っていたのは日本のみである。１９９４年、若し、量子コンピュータが実用化された場合、現在、利用されている、RSA 暗号や楕円曲線暗号が解読されることが理論的に明らかにされるに及んで、海外でも、多変数公開鍵暗号などの耐量子暗号の研究が盛んになり現在に至っている次第である。

⑥　楕円曲線暗号における理念と現実の完全な一致 ―　新プラトン主義的確認

２６００年程前、ギリシャのタレスは、幅の無い線という理念（イデア）を提案した。明治４０年代、哲学者 西田幾多郎は「物理学者の言う如き、幅の無い線、厚さの無い面などと言うものは実在するものではない。・・・」と述べている。さて、現在、最も普及している公開鍵暗号は、RSA 暗号であり円に対応する。RSA に遅れて、1985 年頃、提案された楕

円曲線暗号は楕円に対応する。鍵長 2048 ビットの RSA 暗号と同じ性能・安全性を有する楕円曲線暗号は鍵長 約 200 ビットで構成できる。それなら、限りなく円に近い（例えば、地球位の大きい円に対して、1 ミリだけ横幅を広げた楕円）に対応する楕円曲線暗号はどうだろうか。理論的には、これも楕円の筈だが、1 万本位の楕円曲線に対してシミュレーション実験を行い、そのことを確認した。新プラトン主義的に言えば、イデアの世界から現実世界に、全く汚れなく降りて来て、IC カードやスマホに入る稀な例であり、加藤尚武 哲学会元会長に、大変興味を持たれた。これは、現代暗号が、大小性・連続性を捨象した有限体上で構築されているからである（図 2 参照)。

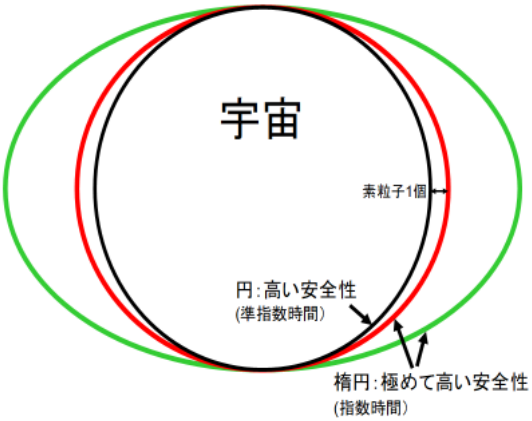

図 2　楕円曲線暗号の安全性

Ⅲ．情報セキュリティ大学院大学初代学長、政府系機関等の理事長として

⑦　デジタルセキュリティ総合科学構築と三止揚―MELT-UP

デジタルセキュリティは、暗号理論のような数学的理論から、人間・社会に直接かかわる管理・経営、倫理、法制度に至るまで、幅の広い分野である。(1)に述べたように、１９９３年、管理・経営、倫理、法制度、技術から成るデジタルセキュリティ総合科学構築を痛感し(文献(9))、その構築を、理念とその具現化の面から検討を続けている ((文献(3)) 等)。住み良い社会・人々を幸せにする理念は何か。それは、時代の価値観等によっても変わり、一意的な回答はないが、数理的世界と異なり、複数の理念の共存となる。例えば、フランス革命では、自由、平等、博愛が掲げられている。最近では、サンデルが、自由主義、共同体主義、功利主義を掲げている。辻井は、20 世紀末から、セキュリティを対象として、自由、公共性（安全性等)、個人の権利（プライバシー等）の三理念を提唱している。これらは相互に矛盾・相克するが、可能な限り高度均衡を図るべく、三止揚―MELT-UP を提唱し、このような理念に基づいて、情報セキュリティ大学院大学を設立して、人材育成に当たり、また、多くのシンポジウムを主催し、DX 社会変革に貢献して来た。

⑧　究極の本人確認の為の 3 層型公開鍵暗号の提案

公開鍵暗号は、公開鍵の中に秘密鍵が埋め込まれた 2 階層構造であるが、今後の DX 社会では、本人確認の成否が、生命財産に関わるケースも起こり得る。そこで、辻井等は、マイナンバー、及び、STR(Short Tandem Repeat，プライバシー情報を含まず、DNA，何兆人に 1 人でも同定可能な DNA 情報）を秘密鍵の中に秘密に埋め込む 3 階層公開鍵暗号方式を提案した[図 3 、文献(1)]

文献

(1) 辻井他「究極の本人確認のための 3 層型公開鍵暗号の提案－マイナンバー・STR の秘密鍵への埋め込みとその利用に向けて－第 2 報」2020 年 1 月 電子情報通信学会 SCIS

(2) 辻井、藤田、五太子「多素数法に基づく多変数公開鍵暗号方式（MPKC）の提案 －耐量子コンピュータ暗号の実現に向けて－第 2 報」2019 年 11 月　電子情報通信学会 ISEC

(3) 辻井、才所、山澤、佐藤「三止揚・MELT-UP の視座からのデジタルフォレンジックに関する考察」2017 年 10 月　情報処理学会 CSS 2017

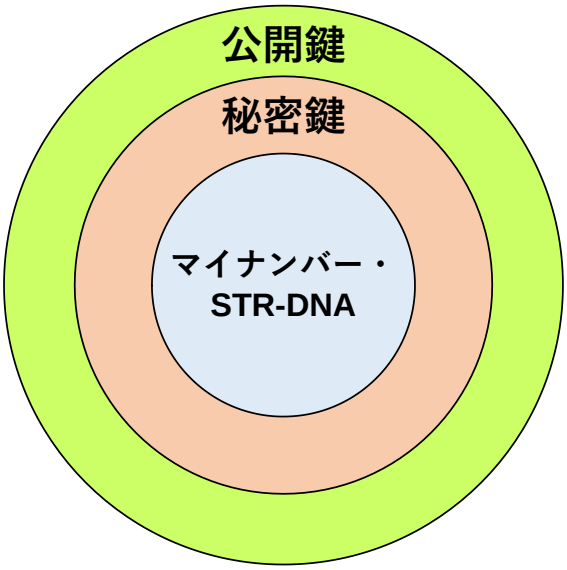

図 3　3 階層公開鍵暗号

(4) 辻井重男「サイバー攻撃・情報漏洩に備えて MELT up 止揚－東工大には総合的止揚力のある人材育成を期待する」2015 年 10 月　蔵前ジャーナル（東工大同窓会誌）

(5) 辻井重男「放送・通信の 4 類型と組織通信・組織暗号 ― 情報セキュリティ概念の高度化に向けて」2013 年 11 月　第 287 号コラム、デジタル・フォレンジック研究会

(6) 加藤尚武編「辻井重男情報哲学入門」2013 年　ホモコントリビューエンス研究会

(7) S. TSUJII「Information Society,Security and Ethics」2011 年 8 月　2011 IEEE International Conference on Peer-to-Peer Computing (IEEE P2P 2011)

(8) 辻井重男「情報セキュリティと信頼性の総合科学」2008 年　日本情報経営学会

(9) 辻井重男「展望―情報セキュリティ総合科学の確立を」1993 年　テレビジョン学会誌（現在、映像情報メディア学会）Vol.47 No.2

著書

暗号―情報セキュリティの技術と歴史　講談社学術文庫（２０１２年６月）

情報社会・セキュリティ・倫理　電子情報通信学会編　コロナ社出版（２０１２年３月）等共編著書

暗号理論と楕円曲線―数学的土壌の上に花開く暗号技術　　森北出版（２００８年９月）

特許

色彩テレビジョン符号変調方式の発明　1978 年（関東地方発明表彰）

((2021-2-15　辻井重男談)