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

辻井 重男[†1]　才所 敏明[†1]　山澤 昌夫[†1]　佐藤 直[†1]

概要：
情報セキュリティ総合科学の視点から，筆頭著者（辻井）が永年，主張してきた，「自由，安心・安全，プライバシーという，相互に矛盾しがちな三者に対する三止揚を情報社会の価値観とし，これを実現するために，Management(経営・管理，市場), Ethics(倫理，心理，行動規範), Law (法制度), Technology (技術)を密結合・強連結させること(MELT-UPと呼ぶ)により住み易い情報社会の実現を目指す」という視座の中で，人，物，通貨，組織など，あらゆるモノがネットに繋がる，広義の IoT，即ち，IoE(Internet of Everything) 環境におけるデジタルフォレンジックの社会基盤的役割について考察する．

キーワード：三止揚，Management，Ethics，Law，Technology，MELT-UP，IoT，IoE，デジタルフォレンジック

3-Aufheben・MELT-UP Sociological Study of Digital Forensic Activities

Shigeo Tsujii[†1]　Toshiaki Saisho[†1]　Masao Yamasawa[†1]　Naoshi Sato[†1]

Abstract:
The first author (Tsujii) has emphasized for a long time that "Aufheben of the three: freedom, security, and privacy, which tend to contradict each other, shall be the value of information society and the information society good to live in shall be realized by closely connecting and strongly linking Management, Ethics, Law, and Technology, (MELT-UP)" from the aspect of "Information Security as a Comprehensive Science." On the other hand, current society is in the IoT environment in a broad sense or IoE (Internet of Everything) environment, where people, things, currencies, and organizations, etc. are connected to networks. Based on the standpoint described above, the role of digital forensics as a social infrastructure is discussed.

Keywords: Three-Aufheben, Management, Ethics, Law, Technology, IoT, IoE, DigitalForensic

1. 序論　集合知—知のフラット化

１８世紀以降，カント，ルソーなどにより，多くの思想が生まれた背景には，王政から，民政へ変わる時代の流れと合わせて，ニュートンの万有引力の法則に見られるように，自然界が美しく描けるのなら，「人間・社会も」と言うことで，社会の構成要素である人間を理想化したこともあるのではないだろうか．ニュートンが生まれた時，カントは３歳．ニュートンを尊敬し，天文学の論文なども書いているそうである．自然科学の影響もあり，几帳面な性格もあって，定言命法のような厳格な思想が生まれたように思われる．

ルソーの一般意思などは，個人を理想化し過ぎて，現実離れした結論を導いているように思われる．しかし，ビッグデータの時代には，集合知が把握し易くなり，知のフラット化が進んでいることから，東浩紀は，一般意思 2.0 を提案し，ルソー・フロイトとグーグルを結びつけている（一般意思 2.0—ルソー，フロイト，グーグル，２０１１年）．

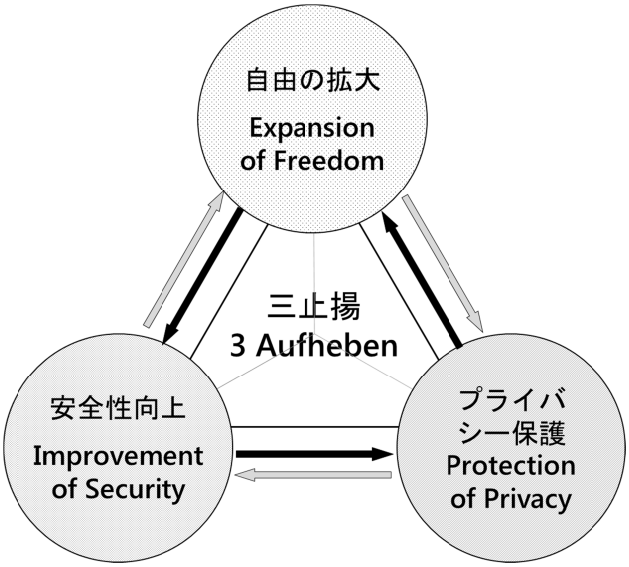
このように，IoT, BigData, AI 環境の中では，これまで，教養のレベル，或いは，理学的であった，思想・哲学が，実用のレベル・工学に近づいてきたようである．

哲学者，サンデルは，社会の価値観を，功利主義，自由主義，共同体主義の３つに分類しているが，これらの思想を，現実社会に当て嵌めようとすれば，どれか一つの思想を実現すれば済むと言うわけにはいかず，それらをどう，組み合わせるかが課題となろう（西垣　通著，２１世紀の「正義」とは何か．２０１７年）．

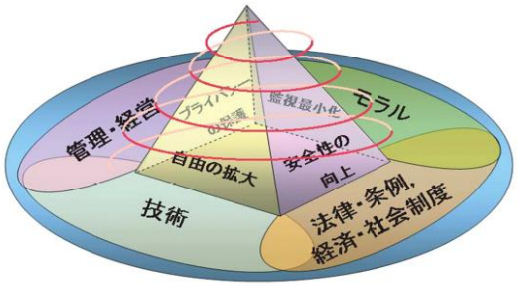
2. 三止揚—MELT-UP と真正性証明

筆者は，前世紀末から，情報セキュリティ総合科学の視野の中で，自由の拡大，安心・安全の向上，プライバシィ保護を３つの価値に着目し，これらの矛盾相剋し勝ちな三者をどのように止揚するかを考えてきた．安心・安全性の向上と，プライバシィ保護は，両立する場合も多いが，相克する場合も少なくない．東日本大震災の際，入院患者情報を，プライバシィ保護を理由に，家族に知らせなかったことは記憶に新しい．最近，NEC(株)は，霧を取り除いて，人や物体の輪郭をはっきりさせる画像処理技術を開発し，ある先端論文賞を受賞した．「夜霧よ，今夜も有難う」（石原裕次郎）ではないが，プライバシィ保護の点で如何かという見方もあるが，車の衝突防止などの安全性向上の効果

が大きいであろう．



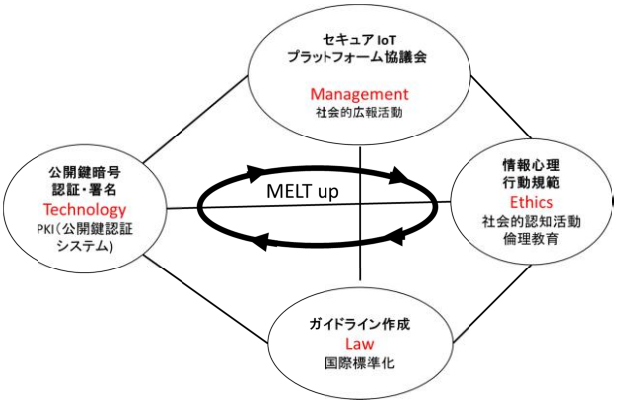
相反し勝ちな３つの価値を，可能な限り高度均衡させることを，三止揚と名付け，そのためには，Management, Ethics, law and Technology の４分野を強連結・密結合させて，PDCA サイクルのように，回していくことが，有効ではないかと考えて来た．この方法論を MELT-UP と名付けている．



具体的には，現在，次の４つのシステムにおける真正性証明について，中央大学研究開発グループが中心となり，検討を進めている．

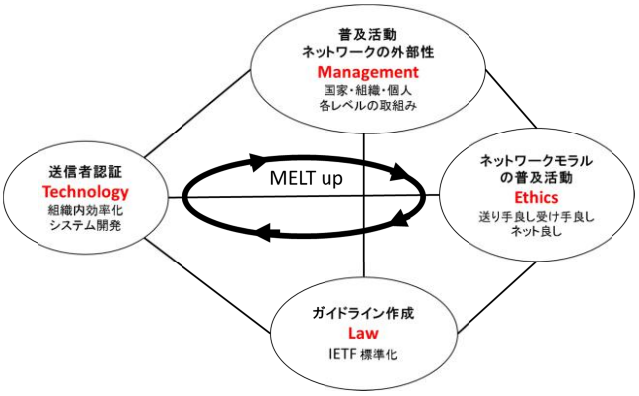
Ⅰ．IoT における発信物の真正性証明のガイドライン・国際標準作成
Ⅱ．S/MIME(Secure/Multi-purpose Internet Mail Extensions)の普及・拡大
Ⅲ．マイナンバーカードの利用拡大
Ⅳ．ブロックチェイン

Ⅰ．については，今年４月，サイバートラスト（株）やセコム（株）と共に，一般社団法人セキュア IoT プラットフォーム協議会を設立した（理事長 辻井重男，監事 佐々木良一）．その目的は，デバイス層，ネットワーク層，プラットフォーム層，サービス層の４層を対称として，発信物の真正性証明のガイドライン・国際標準を作成することである．自動運転車が，人身事故などを起こしたとき，車だけの認証ではなく，その部品まで，認証しておかなければ，事故の解明，責任の所在，或いは，e-Discovery には不十分である．そこで，協議会では，先ず，デバイスの耐タンパー領域に，認証機能を埋め込むことに取り掛かっている．

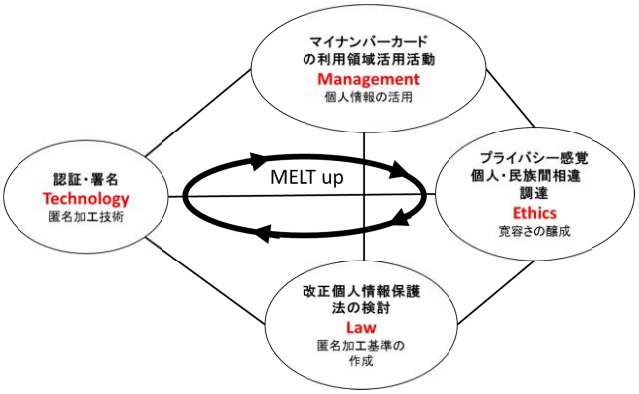


Ⅱ．S/MIME については，組織レベルから，送信者の真正性証明（PKI 認証）の全国的普及を推進することにより，標的型攻撃を激減させることが出来ると考えられる．その普及を妨げているのは，経費と手間が多少かかること，暗号化した場合，安全性確保（マルウエアー対策）とプライバシィ保護の両立が難しいことなどが上げられる．そこで，組織レベルから，段階的に，効率化を進めていくことが望ましい．

基盤となるのは，各組織が，自己防衛・孤塁を守ることのみに腐心せず，「送り手良し，受け手良し，ネット良し」という，互いに相手を思いやるネットワークモラルであろう．

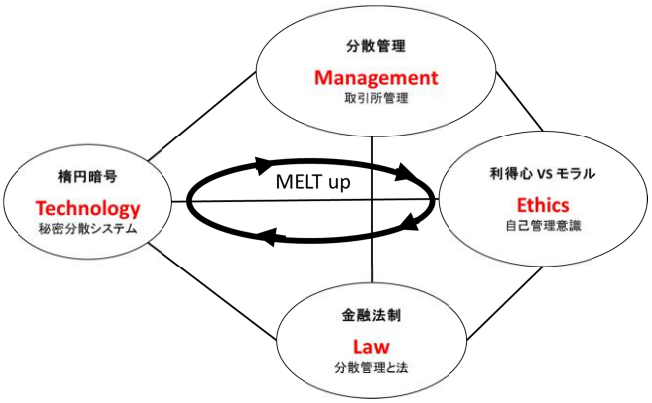


Ⅲ．マイナンバーカードの利用拡大についても，公的個人認証の利用による本人確認システムを普及させることにより，プライバシィを保護しつつ，自由で，安心･安全な情報社会の実現を図るべきであろう．



Ⅳ．ブロックチェインについても，本人確認方式の安全性向上を図るべきである．ビットコインの安全性について，多くの解説書では，「パスワードをキチンと管理しましょう」で済ましているが，より安全性の高い方式を導入すべきである．

暗号通貨はインターネット上のソフトウェアで実現されるが，その利用者，通貨交換業者に始まり，採掘業者や，ソフトウェアの開発集団といった必ずしも目的を共有しない複数集団が暗号通貨サービスの存続を支えている．ビットコインの分裂に見るように，軋轢が発展につながる現象もあり，図のようなＭＥＬＴの相互関係が必至である．それらの発展的構造構築の研究が今後重要になると考える．



以上のような具体例を総括して，デジタル・フォレンジックにおける MELT-UP について考えてみよう．

M (Management)

Management については，国際レベル，国家レベル，捜査機関レベル，裁判所レベル，企業レベル，個人レベルなどの各レベルから，技術，法制度，監査，倫理・行動規範などを総合した対応を考えねばならない．日本では，個人認証に対して，公的個人認証と電子署名法の 2 本立てになっている例からも推察されるように，国としての旗振り役が，定まっていないことが，上記の S/MIME の普及を遅滞させるのではないかと危惧される．

E (Ethics)

上に紹介した，サンデルの共同体主義は，世界各地の従来の文化をベースに思考しているようである．文化とは，ある組織や地域・国家などに固有な， 価値観，正義感，美意識，行動規範などの総体を意味するのであろうが，これからのネットワーク社会では，

第 1 層： 世界共通レーヤ
第 2 層： 各文化圏レーヤ

の 2 層に分けて考えることが必要ではないか，筆者は考えている．

世界共通レーヤでは，これまでの各文化圏の美意識や正義感に拘らず，ネットワークへの全参加者にとって住み良い情報社会に求められるモラルを普及させねばならない．ネット社会に共通する世界的モラルとは，先ずは，人に迷惑をかけないこと，更に進んで，自分ファーストに留まらず，社会貢献に努めることではないだろうか．江戸時代，近江商人は「売り手良し，買い手良し，世間良し」と言ったそうである．S/MIME について，「送り手良し，受け手良し，ネット良し」と上述したのは，近江商人から借用した文句である．また，アダム・スミスの国富論・道徳感情論に先立って，石田梅岩は，石門心学を拓いたが，それは，山鹿素行から「商人共は，右から左に物を流すだけで，儲けている」と非難されたことも一つの動機になったと伝えられている．商人のモラルは，第 1 層の世界共通レーヤ，武士道は美学であり，第 2 層に相当するのではないだろうか．

L (Law System)

改めて書くまでもなく，刑法・刑事訴訟法，民法・民事訴訟法，通信の秘密，不正アクセス禁止法，プロバイダ責任制限法，迷惑メール防止法，特定電子メール送信適正化法，e-文書法，著作権法，公益通信者保護法，個人情報保護法，電気通信事業法，行政機関の保有する情報の公開に関する法律，電子記録債権法，電子消費者契約法，電子署名及び認証業務に関する法律，番号制度，等，多数の法律が，デジタル・フォンレジックスに絡んでおり，その適用に当っては，不正行為の摘発とプライバシィの相克など，悩ましい課題が少なくない．

T (Technology)

これも，今更言うまでもないが，コンピュータ基礎技術，暗号技術，画像処理技術，自然言語処理技術など，一般的な技術をベースに，ハードディスクドライブの消去・復元技術，証拠保全・収集・分析技術，e-ディスカバリー対応技術，訴訟に備える技術などが用いられる．

分散処理環境の広がりなどにより，デジタル・フォンレジックスの利用範囲は広がっており，常に，MELT-UP を回転させることが要請される状況である．

3. デジタルﾌｫﾝﾚｼﾞｯｸの課題――日本語の論理性と法令工学との連携

高デジタルﾌｫﾝﾚｼﾞｯｸの課題は山積しているが，ここでは，日本語の論理性と法令工学の視点から考えてみよう．

米国に子会社を持つ日本企業が，米国で，訴訟に巻き込まれた際，日本語で書かれた証拠書類を英語に訳さなければならない．例えば，ある製薬会社は，米国での pre-trial の為に約８０億円を費やしたが，その内の大半は，翻訳に要したとのことであった（2013 年６月２日，日本経済新聞）．今後，益々，文書やデータ量が増大していく中で，日本語から英語への機械翻訳の効率化が課題となっている．

「川端康成は，雪国でノーベル賞を取った」とコンピュータに教えておいて,「雪国を書いたのは誰？」と質問しても，答えられないそうである（国立情報学研究所，新井紀子）．

文例を沢山，教え込めば，AI は，答えられるようになるとは，予想されるが．

「雪国」の良く知られた書き出し，「トンネルを抜けると雪国であった」を英訳すれば

「The train came out of the long tunnel into the snow country」（サイデン　スッテカー訳）のように，主語も定冠詞も付されるが，日本人は，そんなことは，気にしない．日本語は，感情伝達言語であり，西欧語は，情報伝達言語であるというのは極論であるが，そのような傾向があることは否めない．

「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,「てにおは」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，そこに美や情緒を感じる性質があると言うのだ.（赤田泰和,「日本語，途方もなく自由だった」，朝日新聞，２０１３年４月３０日）

このように日本語賛美論もある反面，「日本語は，揺れる感情を連綿として綴るのに適した湿度 100 パーセントの膠着語である」との批判も見受けられる．

筆者は，個人的には湿度の高い日本語に愛着を持っているが，分野によっては,１７世紀，英国のロイヤルアカデミイーが旗を振って，明晰で論理性の高い英語に換えたように（外山滋比彦「知識と思考」，学士会会報，No.8832010―Ⅳ），論理性を高める時期ではないだろうか．

例えば，法令爆発と言われるように，法律，条令，ガイドラインなどが激増する中で，法令の論理性と機械処理能力を高めておくことが急務である．法令工学は社会のソフトウェアであるという理念に基づいて，法令間の論理的整合性などを向上させるべく，１０年近く前，北陸先端科学技術大学院大学（JAIST）では，片山卓也学長（当時）が代表者となって，文部科学省ＣＯＥ(Center Of Excellence)研究プロジェクトで，法令工学の研究を展開した．現在，中央大学研究開発機構では,福原前学長をユニット長とし，角田篤泰教授，片山教授等により法令工学研究が推進されている．角田らが構築した，条例データベースは，全国自治体の約２分の１で，活用されている．角田は,「法令の要件に結び付く証拠が何になるかを機械的に察知し，それらを自動的に保全できるようにする技術などが，デジタル・フォレンジックスに有効ではないか．そのためには，コンピュータに理解し易い事務処理用日本文の標準化を促進してはどうだろうか」と述べている．情報処理学会でもこのような標準化の検討は既に始めていると聞いているが，一般化・普及を推進することを期待したい．

参考文献

[1] 辻井重男：“展望―情報でキュリティ総合科学の確立を”，テレビジョン学会誌　(現在の映像情報メディア学会誌) Vol.47 No.2 pp.12-15,1993 年 2 月．

[2] 辻井重男：“２１世紀ＣＯＥプログラム―中央大学「電子社会の信頼性向上と情報セキュリティ」，電子情報通信学会誌 Vol.86. No.11, PP.900-905, 2003 年 11 月．

[3] 辻井重男：“組織通信・S/MIM 普及戦略―自由・安全・プラバシィの三止揚を目指して”,日本計画行政学会 通巻 129 号, 2016 年 12 月．

[4] 辻井重男，“ディジタル技術による社会的矛盾の拡大と超克-情報セキュリティの視点から-”,内部統制，No.5，pp.3-14, 2013 年 3 月．

[5] 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・組織通信の枠組の中で～”，民放経営四季報，No.101, pp.8-11，2013 年 9 月．

[6] 辻井重男,才所敏明,五太子政史：“標的型攻撃抑止の為の拡張 S/MIME の普及戦略―国際・国家・組織・個人・IoT の視点から”,電子情報通信学会 暗号と情報セキュリティシンポジウム SCIS2017, 2017 年 2 月．

[7] 辻井重男，五太子政史，才所敏明：”標的型攻撃・サイバー戦争から日本を守るには”, 日本セキュリティマネジメント学会 (JSSM) 第 30 回全国大会， 2016 年 6 月．

[8] 才所敏明，五太子政史，辻井重男：”標的型メール攻撃に対抗する「組織通信向け S/MIME」”，情報処理学会 コンピュータセキュリティシンポジューム CSS2016, 2016 年 10 月．

[9] 才所 敏明，五太子 政史，辻井 重男：”「安心・安全電子メール利用基盤（SSMAX)」構想”，電子情報通信学会 暗号と情報セキュリティシンポジウム SCIS2017, 2017 年 2 月．