電子情報通信学会技術研究報告原稿用紙
一般(様式 1)
社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

社会的課題「安心・安全な電子メール利用環境の実現」のための三止揚・MELT-UP の試み

才所 敏明† 辻井 重男‡

†‡：中央大学研究開発機構 〒112-8551 東京都文京区春日 1-13-27
E-mail: †toshiaki.saisho@advanced-it.co.jp, ‡tsujii@tamacc.chuo-u.ac.jp

あらまし 社会的課題解決（克服）における三止揚という考え方，三止揚を目指した社会的課題克服のための施策検討における MELT-UP という考え方の重要性は，報告者の一人である辻井が二十数年来提唱してきた理念である．現社会が直面する社会的課題「安心・安全な電子メール利用環境の実現」を例題とし，その社会的課題克服のための施策検討プロセスへ MELT-UP の考え方の適用を試みた．結果として，社会的課題「安心・安全な電子メール利用環境の実現」について具体的な克服施策を導出でき，MELT-UP の考え方の有効性を実感できた．一方，MELT-UP による施策検討プロセスは検討を担当する人の知識・見識・能力に強く依存するであろうこともわかった．本稿では，今回 MELT-UP の考え方を適用した社会的課題克服施策検討プロセスを具体的に報告すると共に，検討プロセスからの属人性の完全な排除は難しいが，MELT-UP の考え方による社会的課題克服施策検討プロセスの客観性を高めるための検討課題を指摘する．

キーワード 三止揚，MELT-UP，電子メール，社会的課題，安心・安全電子メール利用環境，社会的課題克服策検討方法論

Attempt to apply 3-Aufheben・MELT-UP for social issues “Realization of Safe and Secure E-mail Exchange Framework”

Toshiaki SAISHO† and Shigeo TSUJII‡

†‡:Research and Development Initiative, Chuo University 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan
E-mail: †toshiaki.saisho@advanced-it.co.jp, ‡tsujii@tamacc.chuo-u.ac.jp

Abstract The importance of "3-Shiyou(3-Aufheben)" on solving social problems (overcome), and the importance of the idea of MELT-UP in discussing measures for overcoming social problems are what Tsujii has adovocated for over 20 years. We took the example of "realizing a safe and secure e-mail use environment" as an example of social issues faced by the present society and we tried attempt to apply the MELT-UP concept to the policy planning and review process to derive the measures for overcoming. As a result, we were able to derive concrete overcoming measures on social issues "realization of secure and secure e-mail usage environment" and realized the effectiveness of MELT-UP's way of thinking. On the other hand, we also found that the policy planning and review process by MELT-UP will depend strongly on the knowledge, insight and ability of the person in charge of planning and review. In this paper, we concretely report the process of overcoming social issues applying the MELT-UP concept. And we propose the issues to be considered for enhancing the objectivity of the overcoming policy planning and review process based on the MELT-UP concept though complete elimination of genus from the planning and review process is difficult.

Keywords 3-shiyou, 3-Aufheben, MELT-UP, E-mail, Social Issues, Safe-and-Secure-E-mail-Exchange-Framework, SSMAX, Methodology-to-consider-overcoming-social-issues

1. はじめに

社会的課題の克服には三止揚という考え方が重要であること，三止揚を目指した社会的課題克服施策の検討にあたっては MELT-UP という考え方が重要であることは，報告者の一人である辻井が長年提唱してきた理念である．

我々は，三止揚を目指した社会的課題克服のための，MELT-UP という考え方に基づく施策検討の具体的な進め方などを MELT-UP 方法論として整理することを目指し，今回，社会が実際に直面している課題の一つ

である,「安心・安全な電子メール利用環境の実現」を対象に，その検討プロセスへの MELT-UP の適用を試みた．本件が，MELT-UP を社会的課題克服策検討プロセスへ効果的に適用した最初の事例となることを期待している．

本稿では，まず三止揚および MELT-UP の考え方を紹介，次に MELT-UP 適用対象として選定した社会的課題「安心・安全な電子メール利用環境の実現」を紹介した上で，その課題克服施策検討プロセスへの MELT-UP 適用の試みを具体的に紹介する．その後に，今回の適用の試みについての評価および MELT-UP の方法論としての整理の可能性と課題などを報告する．

2. 三止揚および MELT-UP について

人類の歴史は技術開発の歴史でもある．新たな技術の開発により，人類の制約や課題が克服され，人類は新たな自由を得，社会の発展を促してきた．しかし，新たな技術開発の成果は，安全性やプライバシー侵害への不安など負の側面を伴うものである．技術開発がもたらす自由の拡大は人類の根源的欲求の一つではあるが，安全性を脅かす新たなリスクを生むことにもなり，同様に人類の根源的欲求の一つである安全性向上とは相反する場合も多く，また自由の拡大は新たなプライバシー侵害のリスク生むことにもなり，同様に人類の根源的欲求の一つであるプライバシー保護とは相反する場合も多い．

このように人類の根源的欲求である，自由の拡大，安全性向上，プライバシー保護の追求はお互いに矛盾する面も多い．人類にとってより良い社会の実現を目指すには，それぞれの根源的欲求をできる限り追求しつつ，相互に発生する矛盾を克服する（超克し高度均衡を図る：三止揚）必要がある．辻井は，この三止揚の重要性を二十数年来提唱してきた（図 1）．

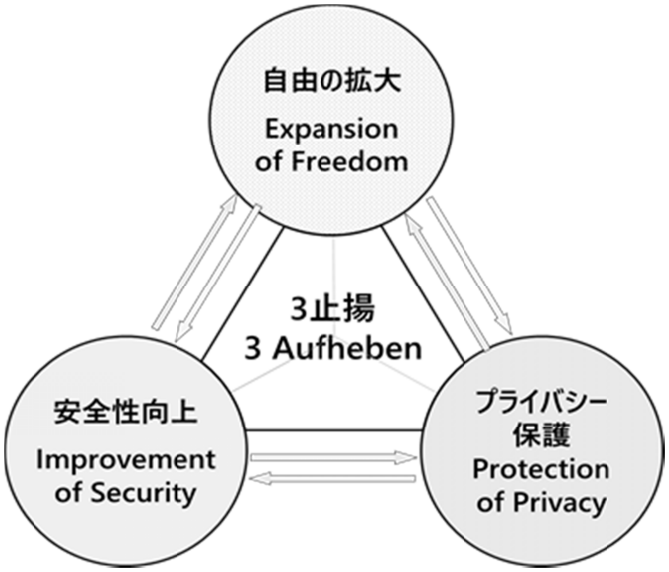

図 1　三止揚

また，この三止揚を図るための方策として，辻井は MELT-UP を提唱してきた．MELT-UP とは，社会的課題の克服においては，経営・管理（Management），倫理・行動規範（Ethics），法制度・標準化（Law），技術（Technology）の四つの観点から，三止揚を目指すという方策である（図 2）．

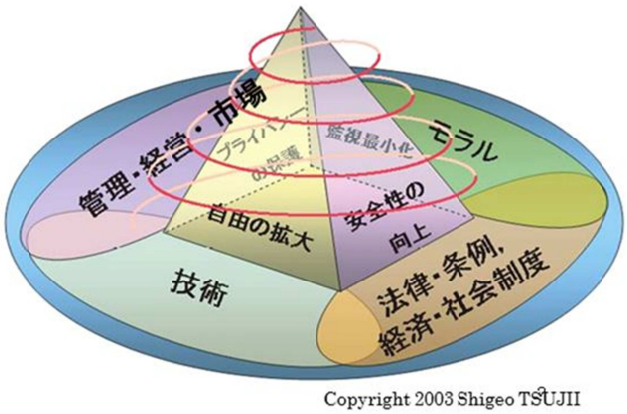

図 2　MELT-UP

技術者・研究者は往々にして，社会的課題の克服を目指す際，技術開発を先行させ，その技術成果が社会で持続的に活用される仕組みやその仕組みの適切な運用を支える法制度・ガイドラインの検討，更には利用者が適切な利用を心がけるベースとなる倫理や行動規範の醸成の検討をおろそかにする傾向にある．最近の技術開発，特に IT 分野の技術開発の進歩は目覚ましく，産官学の社会活動や国民の生活活動の隅々まで IT に支えられるようになってきた高度情報化社会（ネットワーク社会）においては，新たな IT 分野の技術開発成果の社会実装が社会活動や個人活動に直接的に影響を与えることが多く，技術開発成果が社会に受け入れられるためのハードルは高くなってきたといえる．

今後更に高度情報化・ネットワーク化が進展するのは必至，このような社会における新たな社会的課題の克服を目指す際は，技術開発だけを先行させるのではなく，社会実装を念頭に置き，社会実装がスムーズに進むよう，その技術成果が社会で持続的に活用される仕組みやその仕組みの適切な運用を支える法制度・ガイドラインの検討と共に，利用者が適切な利用を心がけるベースとなる倫理や行動規範の醸成を並行し推進し，社会的課題克服策の社会受容性を高める必要があろう．

3. 社会的課題「安心・安全な電子メール利用環境の実現」について

インターネットの歴史と共に発展してきた電子メ

ール（以下，メールと略記）は，コミュニケーション手段の多様化が進む中でも基礎的・共通的コミュニケーション基盤として，依然として重要な役割を担っている．「ビジネスメール実態調査 2017」([12])によると，ビジネスマンの業務上の通信手段は，メール 99.08%，電話 90.10%，会う 74.07%などが主要なものであり，LINE19.42%，Facebook10.06%など，最近のツールも使われ始めているが，メールがネット経由の電子的通信手段の主役であるのは間違いない．

しかし，個人対象のフィッシングメールや組織対象の標的型攻撃メール等の悪意のあるメールの流通を安易に許す現在のメールシステムの脆弱性により，メールへの信頼性が失われつつある．今後もメールが我が国の国民の生活活動や産業界の業務活動を支える基礎的・共通的コミュニケーション基盤としての役割を担うのは確実であるがゆえに，悪意のあるメールの流通を安易に許す現在のメールシステムの脆弱性を克服し，更に個人情報や秘密情報の安全な送受信が可能な安心・安全な電子メール利用環境の早期実現は，我が国の大きな社会課題の一つである．安心・安全な電子メール利用環境の実現は，メールシステムの安全性を高め，その安全性に裏付けられたメールへの安心感の醸成により，生活活動や産業活動におけるコミュニケーションの緊密化・効率化・活発化が期待され，安定した基礎的・共通的コミュニケーション基盤の確立は我が国の更なる成長を促す重要な施策である．

4. 「安心・安全な電子メール利用環境の実現」施策検討プロセスへの MELT-UP 適用の試み

4.1 克服すべき課題および克服方針の策定

施策検討の出発点として，「安心・安全な電子メール利用環境の実現」のために，次の二つの具体的な克服すべき課題とその克服方針を策定した．

①悪意のあるメール（標的型攻撃メール，フィッシングメール，いじめ・中傷・脅迫メール等）氾濫の抑止

［克服方針］メール送信者の特定・追跡を可能とし，悪意のあるメール送信者には是正措置あるいはメール利用停止を要請することにより，悪意のあるメールの発信を制御する

②送信者（送信）メールアドレスのなりすまし，メール内容の改ざん・漏洩の抑止

［克服方針］送信メールアドレスおよびメール内容の真正性を確認可能とし，更にメール内容の秘匿性を保証する仕組みを導入する

設定した課題は，我々が定義した「安心・安全な電子メール利用環境」に基づくものであるが，設定した克服方針については，より適切な克服方針が存在する可能性もある．我々が策定した克服方針が最適であることの証明は難しいが，学会発表等を通じ多くの専門家のレビューを受けたことにより，克服方針の妥当性については一定の評価を得たと理解している．今後も機会をとらえ多くの方々のレビューを受ける予定である．

4.2 克服施策案(1)の策定

4.1 の克服方針に基づき，図 3 に示す克服施策案(1)を策定した．本施策案は，技術（T）施策として 2 項目（認証機能，暗号化機能），管理・経営（M）施策として 2 項目（特定機能，追跡機能）の，4 項目から構成されている．本施策案は暗号・認証技術の研究開発やその応用開発に長年従事してきた経験から導出した結果であるが，導出された施策項目は MELT-UP の考え方に即して，経営・管理（M），倫理・行動規範（E），法制度・標準（L），技術（T）の四つに分類した．

技術(T)		
	①	[送信者・内容認証機能] メール送信者は、送信メールアドレスおよびメール内容の真正性を保証するため署名を付与、受信者は付与されたメール送信者の署名を検証する。
	②	[送信内容秘匿機能] メール送信者は受信者の公開鍵を使用し、メール内容を暗号化する。
管理・経営(M)		
	①	[送信者特定機能] メール利用者が使用するメールアドレスは、信頼できる第3者機関がメール利用者の本人確認を行い、パブリックなメールアドレス証明書（公開鍵証明書）の発行を行うものとする。
	②	[送信者追跡機能] メールアドレス証明書を発行する第3者機関は、メール利用者のメールアドレスに対応するマイナンバー（または4情報）を確認し保管するものとする。

図 3　克服施策案(1)

本施策案は，S/MIME そのものを社会実装する案と言える．4.2 で示した克服方針を満足していることは容易に理解できる．

4.3 克服施策案(1)の課題・改良点の検討

克服施策案(1)が克服方針を満足し，その社会実装が進めば「安心・安全な電子メール利用環境の実現」が可能と考えられる．しかし，本施策案の社会実装を進めるにあたり課題や改良点が無いかどうか，MELT-UP の観点から検討を試みた結果，管理・経営（M）の観点から次の 2 点が本施策の社会実装を阻害する課題となることがわかった．この課題は S/MIME が社会で広範に利用されない原因の一つでもあった．

①メール送信者が組織に属する場合，送信メールは全て所属組織による秘密情報の不正な持出の有無に関する検査を受ける必要があるが，メール受信者の公開鍵で暗号化された送信メールの検査は難しい．

②メール受信者が組織に属する場合，受信メールは全て所属組織によるウイルス等の悪意のある内容の有無に関する検査を受ける必要があるが，メール受信者の公開鍵で暗号化された受信メールの検査は難しい．

なお，上記 2 点の課題は，「暗号化状態での秘密情報の有無の検査やウイルス等の悪意の有無の検査」は現状では難しいという判断に基づいているが，将来，このような検査が暗号化状態でも可能となれば，この 2 点の課題は不適当となり，以降の検討プロセスは大きく変わることになる．

4.4 克服施策案(2)の策定

4.3 の検討結果に基づいて，克服施策案(1)の見直しを検討した結果，発見された課題の克服には技術（T）の②の施策項目の見直しが直接的な解となるので，図 4 のように克服施策案(2)を策定した．修正個所は赤枠で囲んだ部分である．

このように，暗号化されたメールも，組織から外部へ発信される前に，また外部から受信されメールも、組織内の受信者へ送信（転送）される前に，一旦は復号され，検査を受ける施策に変更することにより，**4.3** で発見された課題は克服できる．

なお，組織に所属しない個人がメールを送受信する場合，MSP（メールサービスプロバイダ）と契約しサービスを受けることになるが，MSP では個人情報やプライバシー情報保護のため，一旦復号しての不正な秘密情報持出の有無の検査やウイルス等の悪意のある内容の有無の検査は原則行わず，個人の責任で実施するものとする．もちろん，個人の依頼（同意）により，MSP が一旦復号しての何らかの検査を行うことは，想定しておく必要があろう．

技術(T)		
	①	[送信者・内容認証機能] メール送信者は、送信メールアドレスおよびメール内容の真正性を保証するため署名を付与、受信者は付与されたメール送信者の署名を検証する。
	②	[送信内容秘匿機能] メール送信者は所属する組織（送信組織）の公開鍵を使用し、メール内容を暗号化する。送信組織は復号し秘密情報の不正持出の有無の検査実施後、メール受信者が所属する組織（受信組織）の公開鍵を使用し、メール内容を暗号化する。受信組織は復号しウイルス等の検査実施後、メール受信者の公開鍵を使用し、メール内容を暗号化する。 但し、メール送信者がMSPを利用する個人の場合、送信組織での復号してのメール内容の検査は原則行わず、また、メール受信者がMSPを利用する個人の場合、受信組織での復号してのウイルス等の検査は原則行わない。
管理・経営(M)		
	①	[送信者特定機能] メール利用者が使用するメールアドレスは、信頼できる第3者機関がメール利用者の本人確認を行い、パブリックなメールアドレス証明書（公開鍵証明書）の発行を行うものとする。
	②	[送信者追跡機能] メールアドレス証明書を発行する第3者機関は、メール利用者のメールアドレスに対応するマイナンバー（または4情報）を確認し保管するものとする。

図 4　克服施策案(2)

4.5　克服施策案(2)の課題・改良点の検討

克服施策案(2)　の社会実装を進めるにあたり課題や改良点が無いかどうか，MELT-UP の観点から検討を試みた結果，管理・経営（M）の観点から，次の 4 点が本施策案(2)の課題・改良点であることがわかった．

①組織の承認を受けた秘密情報を含むメール送信の場合も復号され検査を受けることになる。その検査処理過程で組織の秘密情報漏洩のリスクが発生する。

②組織に所属するメール送信者およびメール受信者の場合，秘匿機能のために使用する公開鍵（証明書）は，必ずしもパブリックな公開鍵（証明書）である必要は無い．

③認証機能と秘匿機能で使用する鍵のスコープ（有効範囲）が異なると，2 種類の鍵の使い分けが必要となり，利用者，運用する組織の両方の管理負担を増やすことになり，好ましくない．

④一般に，パブリックなメールアドレス証明書を使用する場合，費用負担が大きい．より安価なプライベートなメールアドレス証明書の利用による施策の方が望ましい．認証機能においても秘匿機能と共用可能な公開鍵ペアによる，プライベートなメールアドレス証明書の利用ができないか．

4.6　克服施策案(3)の策定

4.5 の検討で発見された課題②～④に対応し，克服施策案(2)の見直しを検討した結果，課題②～④の克服には技術（T）の①の施策項目の見直しが直接的な解となるので，図 5 の克服施策案(2)の技術（T）の施策項目①のように修正した．その結果，組織・MSP 内のメール送信者・内容の認証，送信内容の秘匿については，当該組織・MSP が担当することになるため，経営・管理（M）の施策項目①，②の修正も必要となった．また，当該組織・MSP がその役割を適切に果たしているかどうかが，全体の信頼性のベースになるため，組織・MSP の信頼性を確認できる仕組みが別途必要となり，経営・管理（M）の施策項目③を追加した．修正・追加個所は赤枠で囲んだ部分である．

4.5 の検討で発見された課題①については、「一旦復号して検査する処理過程での高い安全性を実現する対策」が必要となるが、この段階で具体的克服施策へ展開するのは難しく、留意事項とし記録、今後の検討プロセスの適切な段階で、具体的克服施策へ展開することとした。なお、本留意事項については克服施策案の一部として記載し、以降の検討プロセスで漏れないよう配慮すべきだが、本稿の報告範囲では本留意事項にはふれないので省略している。

技術(T)		
	①	[送信者・内容認証機能] メール送信者は、送信メールアドレスおよびメール内容の真正性を保証するため署名を付与する。メール送信者が所属する組織またはMSPでは、署名検証により送信メールアドレス、メール内容の真正性を確認後、メールに付与されている署名をメール送信者の署名からメール送信者が所属する組織またはMSPの署名に変更する。 メール受信者が所属する組織またはMSPでは、署名検証により送信メールアドレス、メール内容の真正性を確認後、メール送信者が所属する組織またはMSPの認証後、メールに付与されている署名をメール送信者が所属する組織またはMSPの署名からメール受信者が所属する組織またはMSPの署名に変更する。 メール受信者は、署名検証により送信メールアドレス、メール内容の真正性を確認する。
	②	[送信内容秘匿機能] メール送信者は所属する組織(送信組織)の公開鍵を使用し、メール内容を暗号化する。送信組織は復号し秘密情報の不正持出の有無の検査実施後、メール受信者が所属する組織(受信組織)の公開鍵を使用し、メール内容を暗号化する。受信組織は復号しウイルス等の検査実施後、メール受信者の公開鍵を使用し、メール内容を暗号化する。 但し、メール送信者がMSPを利用する個人の場合、送信組織での復号してのメール内容の検査は原則行わず、また、メール受信者がMSPを利用する個人の場合、受信組織での復号してのウイルス等の検査は原則行わない。
管理・経営(M)		
	①	[送信者特定機能] メール利用者が使用するメールアドレスに対し、所属する組織またはMSPがメール利用者の本人確認を行い、プライベートなメールアドレス証明書(公開鍵証明書)の発行を行うものとする。
	②	[送信者追跡機能] メールアドレス証明書を発行する組織・MSPは、メール利用者のメールアドレスに対応するマイナンバー(または4情報)を確認し保管するものとする。
	③	[組織・MSP信頼機能] メールアドレス証明書を発行する組織・MSPに対し、信頼できる第3者機関(本施策の管理組織)が本施策に基づくメール利用者の管理を行っていることを確認の上、パブリックな公開鍵証明書の発行を行うものとする。

図 5　克服施策案(3)

4.7　克服施策案(3)の課題・改良点の検討

克服施策案(3)　の社会実装を進めるにあたり課題や改良点が無いかどうか，MELT-UP の観点から検討を試みた結果，法制度・標準（L）の観点から，次の 2 点が本施策案(3)の課題・改良点であることがわかった．

①本施策案は，主に送信組織・MSP に対応（投資）を求めるものであるが，その恩恵を受けるのは，主に受信組織・MSP である．このような性質の対応（通信相手のための投資）を，個々の組織・MSP の経営判断に期待するのは難しい．早期の対応（投資）へ組織・MSP を誘導する施策が必要であろう．

②本施策案に基づき社会実装された安心・安全な電子メール利用環境は，組織・MSP の信頼性に強く依存している．組織・MSP の信頼性は，登録時点の状況確認のみでは不十分で，定期的な確認の仕組みが必要であろう．

4.8　克服施策案(4)の策定

4.7 の検討結果に基づいて，克服施策案(3)の見直しを検討した結果，発見された課題①については，官公庁での先行導入，業界に対する導入の動機づけ，課題②については，監査制度との連携による本施策案の持続性，により克服を目指し，法制度・標準（L）の施策項目①～③の追加を行った．以上の検討プロセスにより，克服施策案(4)を策定した．追加した施策項目は，赤枠で囲んだ部分である．

技術(T)		
	①	[送信者・内容認証機能] メール送信者は、送信メールアドレスおよびメール内容の真正性を保証するため署名を付与する。メール送信者が所属する組織またはMSPでは、署名検証により送信メールアドレス、メール内容の真正性を確認後、メールに付与されている署名をメール送信者の署名からメール送信者が所属する組織またはMSPの署名に変更する。 メール受信者が所属する組織またはMSPでは、署名検証により送信メールアドレス、メール内容の真正性を確認後、メール送信者が所属する組織またはMSPの認証後、メールに付与されている署名をメール送信者が所属する組織またはMSPの署名からメール受信者が所属する組織またはMSPの署名に変更する。 メール受信者は、署名検証により送信メールアドレス、メール内容の真正性を確認する。
	②	[送信内容秘匿機能] メール送信者は所属する組織(送信組織)の公開鍵を使用し、メール内容を暗号化する。送信組織は復号し秘密情報の不正持出の有無の検査実施後、メール受信者が所属する組織(受信組織)の公開鍵を使用し、メール内容を暗号化する。受信組織は復号しウイルス等の検査実施後、メール受信者の公開鍵を使用し、メール内容を暗号化する。 但し、メール送信者がMSPを利用する個人の場合、送信組織での復号してのメール内容の検査は原則行わず、また、メール受信者がMSPを利用する個人の場合、受信組織での復号してのウイルス等の検査は原則行わない。
管理・経営(M)		
	①	[送信者特定機能] メール利用者が使用するメールアドレスに対し、所属する組織またはMSPがメール利用者の本人確認を行い、プライベートなメールアドレス証明書(公開鍵証明書)の発行を行うものとする。
	②	[送信者追跡機能] メールアドレス証明書を発行する組織・MSPは、メール利用者のメールアドレスに対応するマイナンバー(または4情報)を確認し保管するものとする。
	③	[組織・MSP信頼機能] メールアドレス証明書を発行する組織・MSPに対し、信頼できる第3者機関(本施策の管理組織)が本施策に基づくメール利用者の管理を行っていることを確認の上、パブリックな公開鍵証明書の発行を行うものとする。
法制度・標準(L)		
	①	[官公庁導入促進] NISCが策定している「政府機関の情報セキュリティ対策のための統一基準」に本施策の必要性も明記し、官公庁での早期導入を促す。
	②	[業界導入促進] 各省庁傘下の業界に対する情報セキュリティ対策ガイドライン等に、本施策の必要性も明記し、各業界での導入を促す。
	③	[組織・MSP信頼性維持] 本施策の実施状況のチェックを監査項目に付加し、監査結果により組織およびMSPの実施状況(組織の信頼性)を評価できるようにする。

図 6　克服施策案(4)

4.9 克服施策案(4)の課題・改良点の検討

克服施策案(4)　の社会実装を進めるにあたり課題や改良点が無いかどうか，MELT-UP の観点から検討を試みた結果，倫理・行動規範（E）の観点から以下の 3 点の利用者個人に関する課題があることがわかった．

①追跡機能のために組織・MSP で保管されるメール利用者の情報として，マイナンバー（または 4 情報）が保管されるのは不安を感じるのではないか．

②メールアドレス証明書の利用が，個人情報の漏洩に繋がりはしないかという不安を感じるのではないか．

③メール送信者の特定・追跡性に不安を感じるのではないか．

4.10 克服施策案(5)の策定

4.9 の検討結果に基づいて，克服施策案(4)について以下のように見直しを検討し，図 7 に示す克服施策案(5)を策定した．

利用者個人に関する課題①については，マイナンバー（あるいは 4 情報）とのリンクが確認でき，組織・MSP が追跡機能に支障をきたさない情報の利用も可能とし，管理・経営（M）の施策項目②を修正した．

課題②については，メールアドレス証明書のメールアドレス所有者名としてニックネーム等，本人を直接特定できない名前の利用を可能とすることにより克服を目指し，管理・経営（M）の施策項目①を修正した．

課題③については，メール利用者の特定・追跡のための情報は暗号化する等，その保護には組織・MSP 共に十分配慮するものとし，また，メール送信者の特定・追跡機能が利用されるのは，メール送信者が悪意のあるメールを送信した場合やその結果として被害を受けた場合に限るものとし，そのための手順・ルールを明確にしておく．社会的に合意がとれる範囲でのみ，特定・追跡が実施されるものとした．結果として，管理・経営（M）の施策項目②を修正した．

更に，個人情報が管理され保護されていることと同時に，悪意のあるメールの送信者には特定・追跡機能が利用され何らかの対応が要請されること，メール送信者には送信内容に対する社会的責任が伴うことを，メール利用者個人には理解いただく必要がある．結果として，倫理・行動規範（E）に施策項目を追加した．

克服施策案(5)の赤枠で囲んだ部分が，修正・追加した施策項目である．

技術(T)		
	①	[送信者・内容認証機能] メール送信者は、送信メールアドレスおよびメール内容の真正性を保証するため署名を付与する。メール送信者が所属する組織またはMSPでは、署名検証により送信メールアドレス、メール内容の真正性を確認後、メールに付与されている署名をメール送信者の署名からメール送信者が所属する組織またはMSPの署名に変更する。 メール受信者が所属する組織またはMSPでは、署名検証により送信メールアドレス、メール内容の真正性を確認後、メール送信者が所属する組織またはMSPの認証後、メールに付与されている署名をメール送信者が所属する組織またはMSPの署名からメール受信者が所属する組織またはMSPの署名に変更する。 メール受信者は、署名検証により送信メールアドレス、メール内容の真正性を確認する。
	②	[送信内容秘匿機能] メール送信者は所属する組織（送信組織）の公開鍵を使用し、メール内容を暗号化する。送信組織は復号し秘密情報の不正持出の有無の検査実施後、メール受信者が所属する組織（受信組織）の公開鍵を使用し、メール内容を暗号化する。受信組織は復号しウイルス等の検査実施後、メール受信者の公開鍵を使用し、メール内容を暗号化する。 但し、メール送信者がMSPを利用する個人の場合、送信組織での復号してのメール内容の検査は原則行わず、また、メール受信者がMSPを利用する個人の場合、受信組織での復号してのウイルス等の検査は原則行わない。
管理・経営(M)		
	①	[送信者特定機能] メール利用者が使用するメールアドレスに対し、所属する組織またはMSPがメール利用者の本人確認を行い、プライベートなメールアドレス証明書（公開鍵証明書）の発行を行うものとする。 メールアドレス証明書へ記載するメール利用者名として直接本人を特定できないニックネーム等も使用可能とする。
	②	[送信者追跡機能] メールアドレス証明書を発行する組織・MSPは、メール利用者のマイナンバー（または4情報）あるいはマイナンバーとのリンクが確認されている情報を確認し、メールアドレス/メール利用者名との対応（個人情報）を保管するものとする。 保管する個人情報は暗号化等により保護するものとする。 悪意のあるメールを受信した場合やその結果として被害を受けた場合に限り、メール送信者の特定・追跡が行われるものとし、そのための手順・ルールを明確にするものとする。（特定・追跡は、社会的に合意のとれる範囲でのみ、実施されるものとする。）
	③	[組織・MSP信頼機能] メールアドレス証明書を発行する組織・MSPに対し、信頼できる第3者機関（本施策の管理組織）が本施策に基づくメール利用者の管理を行っていることを確認の上、パブリックな公開鍵証明書の発行を行うものとする。
法制度・標準(L)		
	①	[官公庁導入促進] NISCが策定している「政府機関の情報セキュリティ対策のための統一基準」に本施策の必要性も明記し、官公庁での早期導入を促す。
	②	[業界導入促進] 各省庁傘下の業界に対する情報セキュリティ対策ガイドライン等に、本施策の必要性も明記し、各業界での導入を促す。
	③	[組織・MSP信頼性維持] 本施策の実施状況のチェックを監査項目に付加し、監査結果により組織およびMSPの実施状況（組織の信頼性）を評価できるようにする。
倫理・行動規範(E)		
	①	[特定・追跡性限定] 悪意のあるメールによる被害の実態を紹介、メール送信者の特定・追跡性の必要性を説明すると共にメールによる情報発信者としての責任を理解いただく。一方、そのような状況にならない限り、特定・追跡のための情報は開示されないことを理解いただく。

図 7　克服施策案(5)

4.11 以降の課題検討･施策案見直し

克服施策案(5)が最終施策では無い．以降も，数多くの課題・改善点が考えられる．大きな課題としては国際展開が考えられ，また改善点あるいは施策項目の詳細定義が必要な点としては組織・MSP の信頼性維持の仕組みが考えられる．

このような克服施策案の課題検討・施策案見直しのサイクルは際限なく続く可能性があるが，現実的な克服施策に到達した段階で，社会実装のためのプロモーション活動を展開しつつ，更に施策の改良・具体化の検討を進める必要があろう．MELT-UP の適用の試みの対象とした社会的課題「安心・安全な電子メール利用環境の実現」についても，我々は克服施策案(5)にて現実的な克服施策を導出できたと判断し，その実装方式の詳細検討を継続すると共に、早期の社会実装に向けたプロモーション活動にも注力しているところである．

5. 社会的課題克服施策検討プロセスへの MELT-UP の適用に関する考察

社会的課題「安心・安全な電子メール利用環境の実現」のための施策検討プロセスへの MELT-UP 適用の試みは，その検討プロセスを **4.** にて報告した通り，ステップごとの課題・改善点の発掘において，MELT（管理・経営，倫理・行動規範，法制度・標準，技術）のそれぞれの観点，四つの観点からの検討が大変有効であった．また，発掘した課題・改善点の克服施策検討にあたっても，四つの観点からの検討は有効であった．

確定的・トップダウン的な施策策定が困難な社会的課題については，図 8 の黒色実線で示したフローのように，施策案策定後に課題発掘およびその課題を克服可能な新たな施策案策定というプロセスを繰り返し行うことになろう．

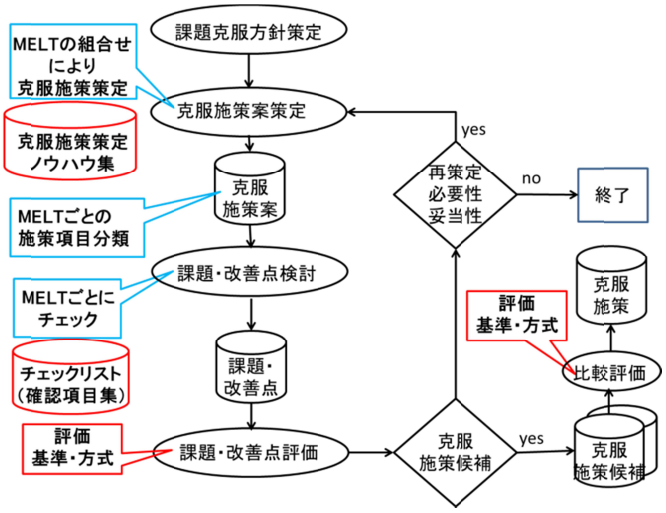

図 8　社会的課題克服施策検討プロセス

今回の MELT-UP 適用の試みでは，このような検討プロセスに対し，図 8 の青枠部分で MELT-UP の考え方を適用した．上述のようにその効果は実感できたが，克服施策案の策定や克服施策案の課題・改良点の発掘は属人性の強いプロセスとなっていた．

今後，MELT-UP の考え方が，社会的課題克服施策検討における客観的な方法論として確立させるには，克服施策案の策定や克服施策案の課題・改良点の発掘における属人性を弱めるため，ガイドライン・検討項目リスト・チェックリスト等の整備が必要であろう．また，一般に社会的課題克服施策は複数存在するなかで，最も適切な施策選定のためには，評価基準や評価方式の検討も必要であろう．図 8 中の赤枠で今後整備・準備が必要と思われる項目を示している．

6. おわりに

今回の MELT-UP 適用の経験から，社会的課題克服施策検討プロセスへの MELT-UP 適用の有用性・有効性については実感したものの，客観的で汎用的な方法論にはまだまだ検討課題が多いことを痛感した．

我々は，様々の社会的課題の克服施策検討プロセスへの MELT-UP 適用を試み，経験を通じて得た知識・ノウハウの整理・検討等を通じ，MELT-UP 方法論の確立を目指したい．

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，Feb. 2003.

[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，Nov. 2003.

[3] 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，Mar. 2013.

[4] 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，Sep. 2013.

[5] 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，Jun. 2016.

[6] 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，　Dec. 2016.

[7] 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，　Feb. 2017.

[8] 辻井重男，才所敏明，山澤昌夫，佐藤直，：“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”, コンピュータセキュリティシンポジューム CSS2017, Oct.2017.

[9] 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, Oct. 2016.

[10] 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, Feb. 2017.

[11] 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）”, コンピュータセキュリティシンポジューム CSS2017, Oct. 2017.

[12] “ビジネスメール実態調査 2017”, http://www.sc-p.jp/news/pdf/170602PR.pdf (参照 2017-07-31).