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
2017年11月09日

1

発表項目一覧

（1）三止揚による社会的課題の克服の重要性

（2）三止揚を図るための方策：MELT-UPの重要性

（3）社会的課題例「安心・安全な電子メール利用環境」紹介

（4）社会的課題例の克服施策検討プロセスへの
MELTの考え方の適用の試み

（5）おわりに
（試行結果からのMELT-UP方法論確立上の課題）

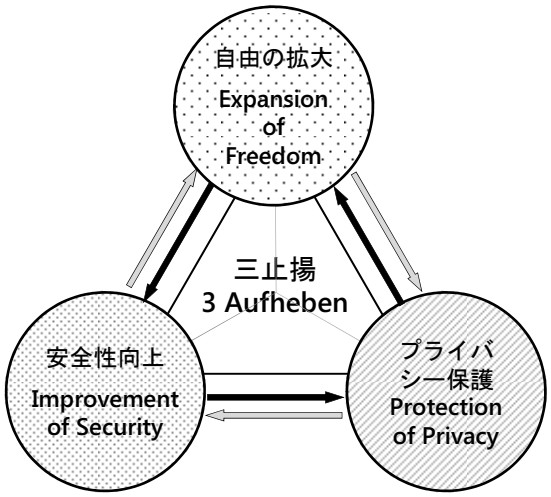
2

歴史とは自由拡大の過程

- ヘーゲル（1770～1831) 曰く
- 「歴史とは、自由拡大の過程であり、
- 自由の拡大に伴って、矛盾も増大する。」

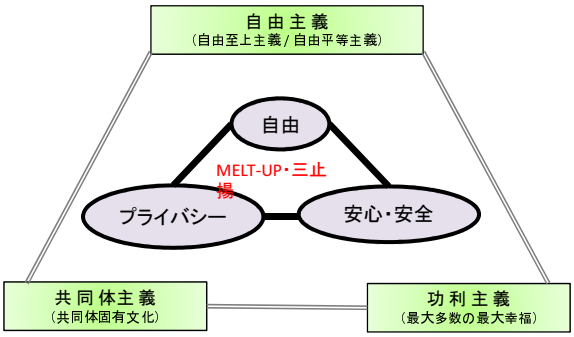
- ネット社会では、誰もが実感
- 例えば、
- 霧の中での顔認識（NEC 先端技術論文賞）
- 交通安全か、 夜霧よ今夜も有難うか

3



4

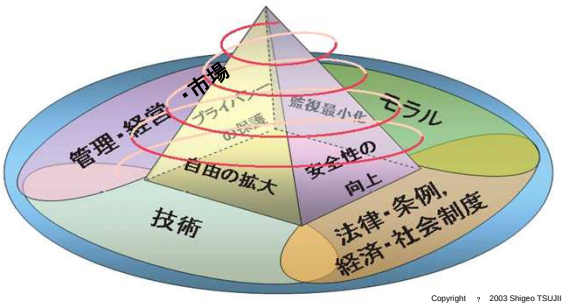
サンデルの体系*と本提案の三止揚の関係



＊ 西垣 通著：ネット社会の「正義」とは何か

5

セキュアな社会基盤の構築



MELT upの概念

6

証拠確保・認証に関する　三止揚・MELTーUP

- 20世紀末から概念提案してきたが、次の4つの課題について、
- 具体的に検討する。本発表では、S/MIME

- 下記の4システムに関するMELTーUP　について、具体的に検討する。

- 1. IoT 認証　　セキュアIoTプラットフォーム協議会（辻井理事長）設立
- 2. 電子メールにおける送信者認証ーS/MIME
- 3. マイナンバーにおける公的個人認証
- 4. 仮想通貨・ブロックチェインにおける所有者認証

7

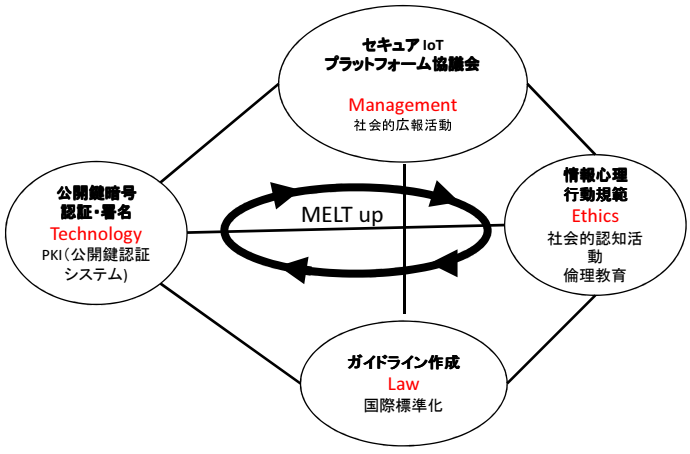


図　セキュア IoT プラットフォーム構築に向けての MELT up 活動

8

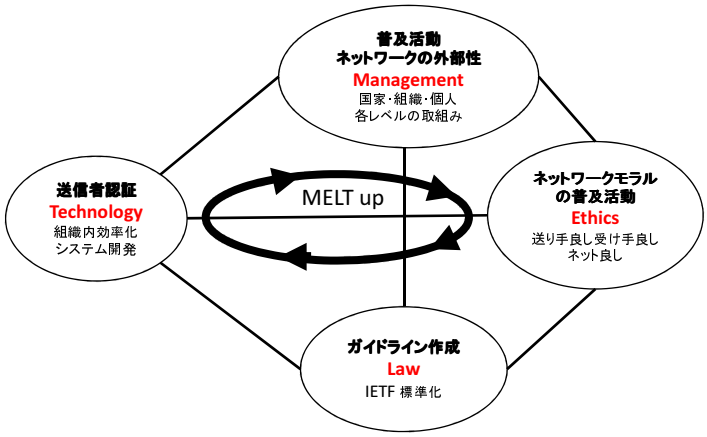


図　IoT を含む S/MIME の普及へ向けての MELT up 活動

9

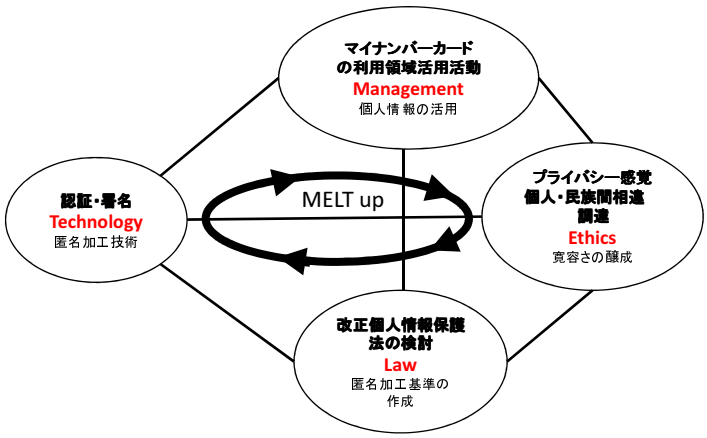


図　マイナンバーの利用拡大に向けての MELT up 活動

10

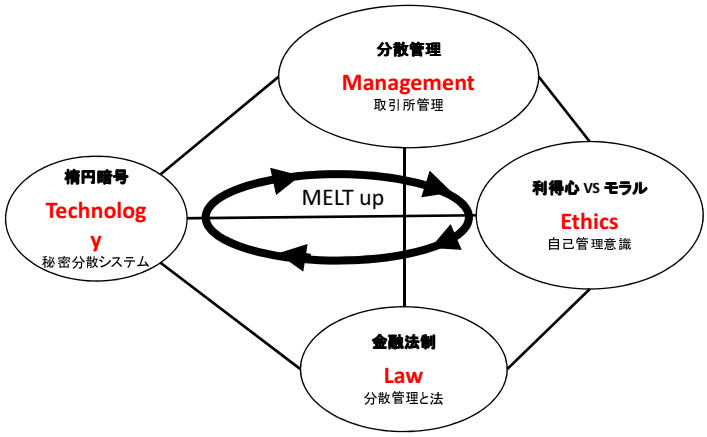


図　暗号通貨（ビットコイン）・ブロックチェインの高信頼化へ向けての MELT up 活動

11

三止揚による社会的課題の克服（1）

人類の歴史は技術開発の歴史
　新たな技術の開発
　人類の制約や課題を克服
　人類は新たな自由を得，社会は発展

一方、新たな技術開発の成果の普及は，
　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も多い

12

三止揚による社会的課題の克服（2）

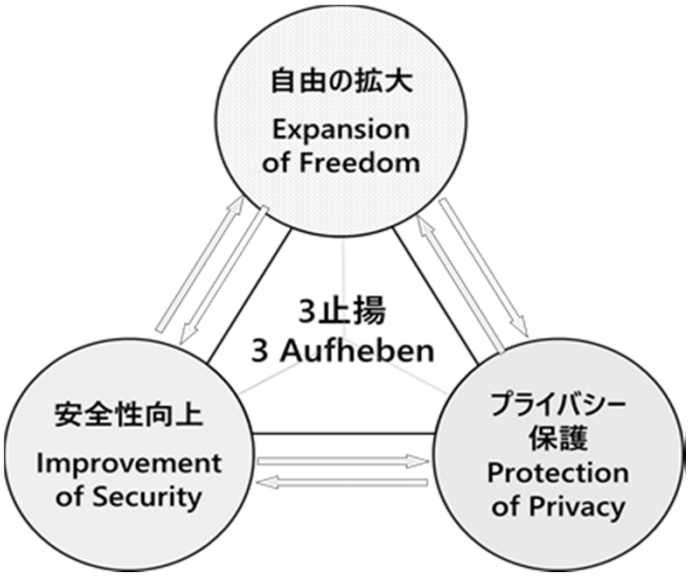
人類の根源的欲求である，

　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）ことが必要

13

三止揚による社会的課題の克服（3）



14

発表項目一覧

（1）三止揚による社会的課題の克服の重要性

（2）三止揚を図るための方策：MELT-UPの重要性

（3）社会的課題例「安心・安全な電子メール利用環境」紹介

（4）社会的課題例の克服施策検討プロセスへの
MELTの考え方の適用の試み

（5）おわりに
（試行結果からのMELT-UP方法論確立上の課題）

15

三止揚を図るための方策：MELT-UP（1）

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

16

三止揚を図るための方策：MELT-UP（２）

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，

①その技術成果が
社会で持続的に活用される仕組み
②その仕組みの適切な運用を支える
法制度・ガイドライン
③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．

17

三止揚を図るための方策：MELT-UP（３）

高度情報化社会においては，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

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
その仕組みの適切な運用を支える法制度・ガイドライン
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．

18

発表項目一覧

（1）三止揚による社会的課題の克服の重要性

（2）三止揚を図るための方策：MELT-UPの重要性

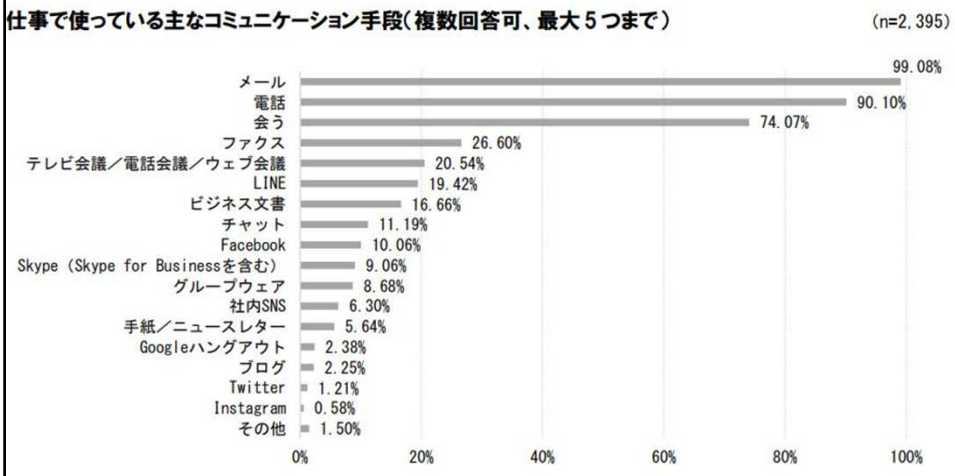
（3）社会的課題例「安心・安全な電子メール利用環境」紹介

（4）社会的課題例の克服施策検討プロセスへの
MELTの考え方の適用の試み

（5）おわりに
（試行結果からのMELT-UP方法論確立上の課題）

19

MELT-UP適用を試みる社会的課題
「安心・安全な電子メール利用環境の実現」



電子メールがネット経由の通信手段の主役

20

標的型攻撃の初期潜入には ほとんど電子メールが利用されている

2016年における標的型サイバー攻撃の公表事例一覧

公表月	組織	侵入発覚理由	侵入経路
6月	旅行会社	自組織の対策により不審な通信を確認し発覚	標的型メール
6月	国立大学	自組織の対策により不審な通信を確認し発覚	標的型メール
7月	国立大学	外部からの不審な通信の指摘	標的型メール
10月	国立大学	外部からの不審な通信の指摘	標的型メール
11月	金融機関	自組織の対策により不正プログラムのダウンロードを確認	標的型メール
11月	経済団体	内部調査の結果不審な通信の存在を確認	不明/未公表
11月	出版社	外部からの不審な通信の指摘	標的型メール

国内標的型サイバー攻撃分析レポート　2017年版（トレンドマイクロ 株式会社）

21

目指すべき 安心・安全な電子メール利用環境

（1）組織対象の標的型攻撃メールの氾濫を防ぐことができる

（2）個人対象のフィッシングメールや、誹謗・中傷、脅迫、いじめなどの悪意のあるメールの氾濫を防ぐことができる

（3）メール内容の保護が保証され、個人情報や機密情報を活用した緊密なコミュニケーションにも使用できる

（4）メールの安全性を高め、その安全性に裏付けられたメールへの安心感を醸成し、安心して活発に利用される電子メール利用環境

（5）我が国の産業活動、国民の生活活動を支える安定した基礎的・共通的コミュニケーションとしての安心・安全な電子メール利用環境

22

発表項目一覧

（1）三止揚による社会的課題の克服の重要性

（2）三止揚を図るための方策：MELT-UPの重要性

（3）社会的課題例「安心・安全な電子メール利用環境」紹介

（4）社会的課題例の克服施策検討プロセスへの MELTの考え方の適用の試み

（5）おわりに
（試行結果からのMELT-UP方法論確立上の課題）

23

安心・安全な電子メール利用環境を目指して 克服すべき課題と克服方針

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

24

課題
克服方針

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

施策案
1

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。

25

施策案
1

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。

課題
1

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．

26

課題
1

①メール送信者が組織に属する場合、所属する組織による不正な秘密情報持出の有無に関する
送信メールの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、所属する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
受信メールの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。

施策案
2

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。

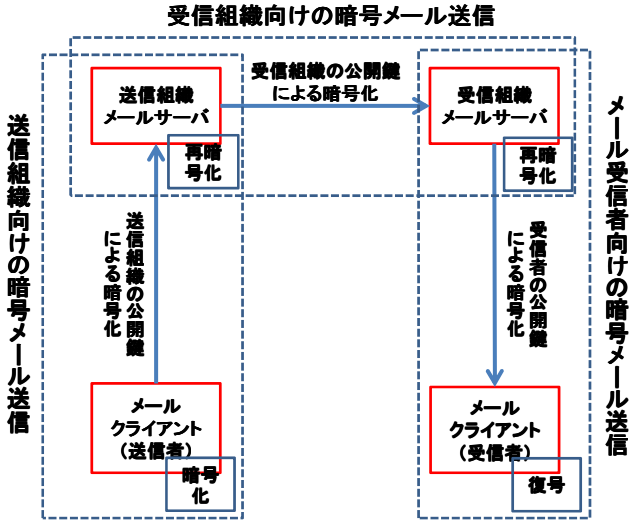
管理・経営(M)

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。

27

メール内容の秘匿(漏洩防止)



暗号化の連鎖

28

施策案2

課題2

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。

①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。
②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。
③一般に、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。

29

課題2

施策案3

①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。
②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。
③一般に、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。

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）

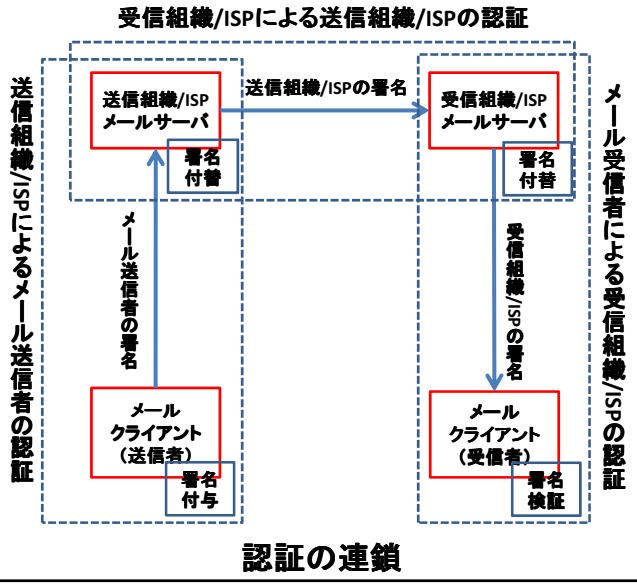
① [送信者特定機能]
メール利用者が使用するメールアドレスに対し、所属する組織またはMSPがメール利用者の本人確認を行い、プライベートなメールアドレス証明書（公開鍵証明書）の発行を行うものとする。

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または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または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。

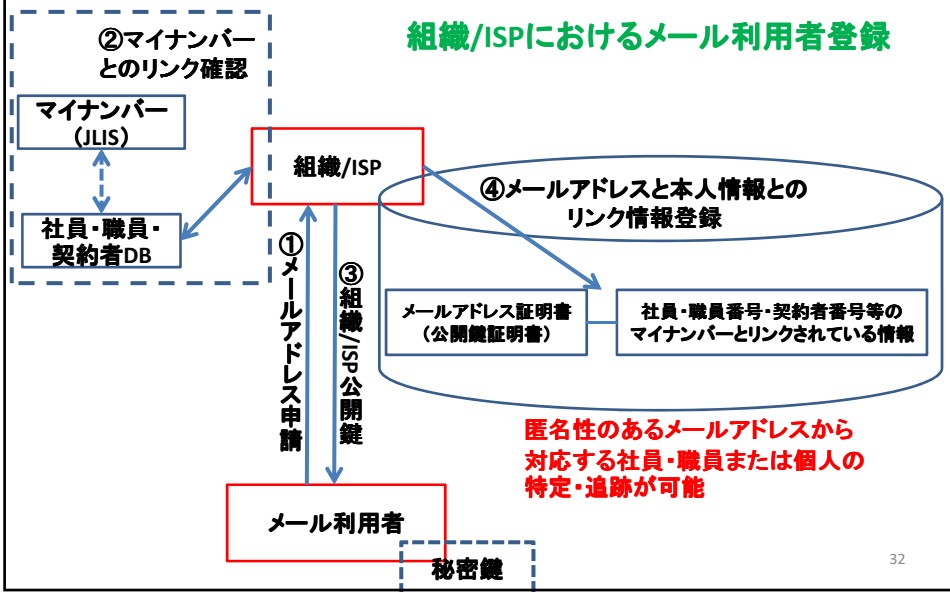
30

メール送信者の認証（なりすまし検出）
送信メッセージの認証（改ざん検出）



31

悪意のあるメール送信者の特定・追跡性とメール送信者の匿名性の両立



32

施策案 3

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または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または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。

課題 3

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．

課題 3

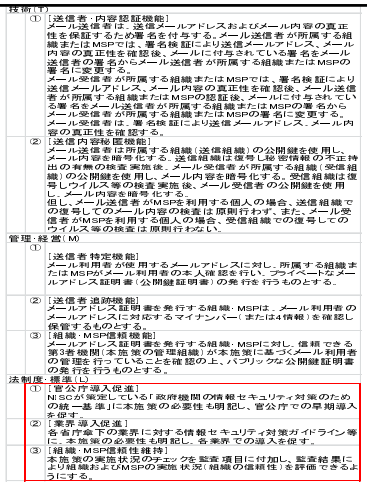
①本施策案は，主に送信組織・MSPに対応（投資）を求めるものであるが，その恩恵を受けるのは，主に受信組織・MSPである．このような性質の対応（通信相手のための投資）を，個々の組織・MSPの経営判断に期待するのは難しい．早期の対応（投資）へ組織・MSPを誘導する施策が必要であろう．
②本施策案に基づき社会実装された安心・安全な電子メール利用環境は，組織・MSPの信頼性に強く依存している．組織・MSPの信頼性は，登録時点の状況確認のみでは不十分で，定期的な確認の仕組みが必要であろう．

施策案 4

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。

施策案 4

課題 4


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。

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．

課題 4

施策案 5

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．

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。

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.

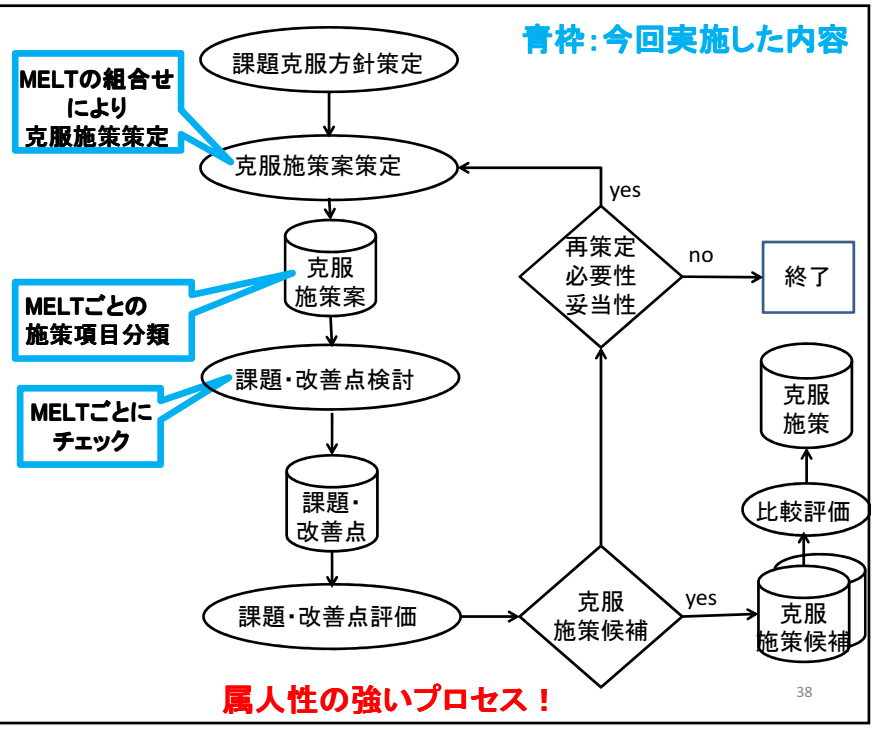
以降も，数多くの課題・改善点を検討しつつ、施策の見直し・詳細化を継続することになる。

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。

一般に、基本施策の見通しが立った時点で、施策の詳細化・具体化と並行し、社会実装のための準備活動を展開することになろう。

37

社会的課題克服施策検討プロセス



38

発表項目一覧

（1）三止揚による社会的課題の克服の重要性

（2）三止揚を図るための方策：MELT-UPの重要性

（3）社会的課題例「安心・安全な電子メール利用環境」紹介

（4）社会的課題例の克服施策検討プロセスへの
MELTの考え方の適用の試み

（5）おわりに
（試行結果からのMELT-UP方法論確立上の課題）

39

おわりに

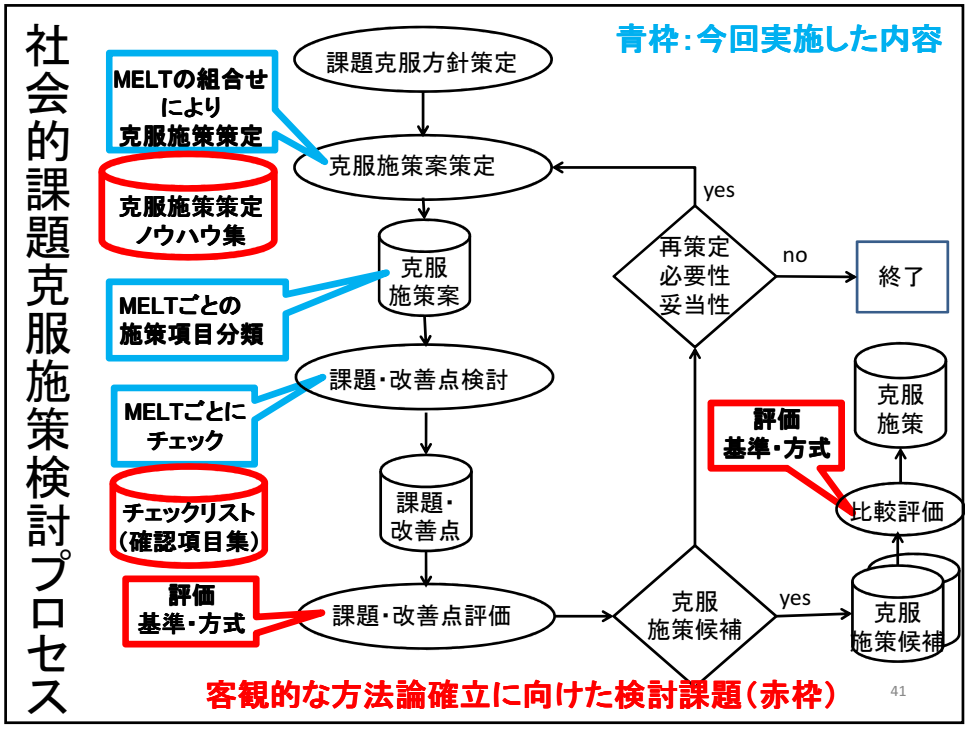
今回の試行では、策定された克服施策案に対し、MELTの視点からの課題を検討・抽出し、抽出された課題をMELTの視点から適切な改訂案を検討し、新たな克服施策案を策定する、という段階的ブラッシュアップ手順を実施

社会的課題克服施策の策定において、MELT-UPの考え方に基づく検討の有用性は実感（技術面だけでなく、管理・経営、法制度・標準、倫理・行動規範面からの検討も並行し実施することの有用性）

しかし、克服施策案に対するMELTの視点からの課題検討・抽出、およびMELTの視点からの克服策改定案の検討は、このままでは極めて属人性が強いプロセスとならざるを得ない

克服施策案の課題克服のためのノウハウ集、克服施策案の課題抽出のためのチェックリスト（確認項目一覧）などの整備や克服施策案の評価方式の確立が必要となろう

40



MELT-UP方法論の確立のために 今後の検討課題

（1）多くの社会的課題への適用
によるノウハウの蓄積・整理
例：暗号通貨、マイナンバーカード、IoT

（2）過去の社会的課題克服策検証
によるノウハウの抽出・整理

（3）これまで提案されている問題解決方法論
の社会的課題克服施策検討への応用検討・整理
例：How to Solve It（1945Polya）

42

終

43

社会的課題とは

定義１：
社会の欠陥や不合理から生まれている問題で、
実際に社会で生活していく上で
支障をきたすレベルの大きな問題

定義２：
世に知れ渡っている解決すべき問題
（誰かが必ず解決しなければならない課題）

44

対象とする社会的課題

「安全・安心を脅かす要因の整理」
（科学技術・学術審議会（第12回（平成16年））配付資料より）

大分類：＊犯罪＊事故＊自然災害＊戦争**＊サイバー空間の問題**＊健康問題＊食品問題＊社会生活上の問題＊経済問題＊政治・行政の問題＊環境・エネルギー問題

サイバー空間の問題

コンピュータ犯罪：*＊不正アクセス、なりすまし＊サイバーテロ＊情報漏洩＊ウィルスによる攻撃＊情報の改ざん＊情報の破壊、消去＊サービス妨害＊情報の不正取得＊不正取引、不正請求＊悪徳商法＊誹謗中傷、脅迫*

大規模なコンピュータ障害：＊システム障害＊情報消失＊通信障害

45

How to Solve It

George Polya（1887年～1985年）
ハンガリー出身のアメリカの数学者
1914年～1940年チューリッヒ工科大学の数学教授
1940年～1953年スタンフォード大学の数学教授

How to Solve It: A New Aspect of Mathematical Method
Published September 25th 2015 by Princeton University Press (first published November 30th 1944)

46

4つの原則

1：Understand the problem

2：Devise a plan

3：Carry out the plan

4：Review/extend

47

Heuristics

Analogy
Generalization
Induction
Variation of the problem
Auxiliary problem
Related and solved problem
Specialization
Decomposing and recombining
Working backward
Draw a figure
Auxiliary elements

48