安心・安全電子メール利用基盤SSMAX
（Secure and Safe eMAil eXchange framework)

2018年6月27日
才所敏明
中央大学研究開発機構
（（株）IT企画）

略歴

1970年　東京大学・工学部・計数工学科卒業
1970年～1994年　本社情報システム部門
東芝社内技術部門・研究部門向け
計算機利用環境の整備・高度化を担当。
EWS（SUN）の全社導入・活用推進、
社内インターネット網・UNIXメール網の構築・活用推進。
1995年～2007年　セキュリティ技術研究開発部門
セキュリティ技術の研究開発および事業支援活動を指揮しつつ、
我が国としてのセキュリティ研究開発課題を
中央省庁へ多数提案し受託・研究開発指揮。
2007年～　（株）IT企画
大学向けの講義・講演（九大、慶応、秋田大、日大、法政大等）
IT企業向けコンサル活動
2014年～　中央大学研究開発機構（研究員）
研究対象分野：サイバーセキュリティ、IoT、ビッグデータ、FinTech

説明項目

（1）電子メール利用環境のリスク

（2）現状の対策とその限界

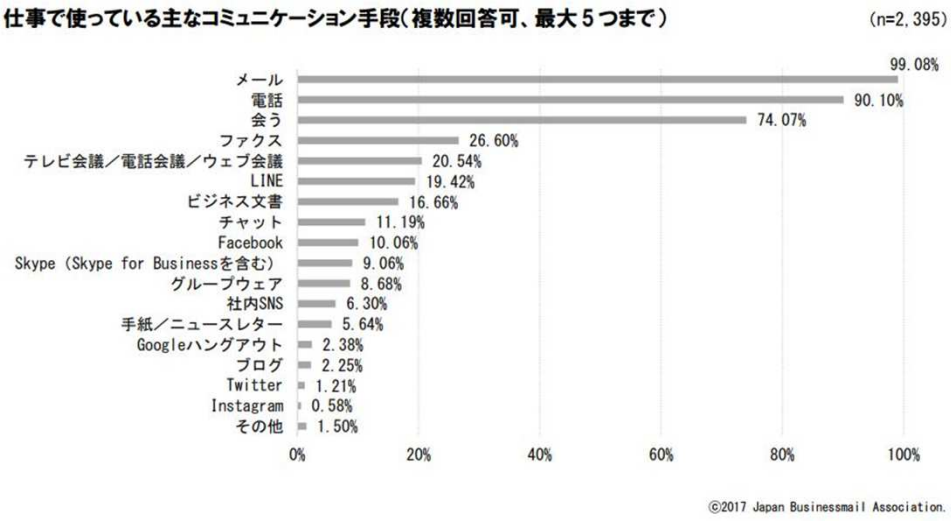
（3）セキュアメール標準S/MIMEの有効性と限界

（4）安心・安全電子メール利用基盤SSMAX

（5）今後の課題

（1）電子メール利用環境のリスク

電子メールがネット経由の通信手段の主役



「ビジネスメール実態調査 2017」（2017年6月2日に一般社団法人日本ビジネスメール協会発表）

電子メールがネット経由の通信手段の主役だからこそ
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）

情報セキュリティ10大脅威2018（IPA発表）

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報等の不正利用	1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ランク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃	4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	6位	ウェブサービスからの個人情報の窃取	3位
8位	情報モラル欠如に伴う犯罪の低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10位	IoT機器の不適切な管理	9位	サービス妨害攻撃によるサービスの停止	4位
ランク外	偽警告によるインターネット詐欺	10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

＊5＊

（2）現状の対策とその限界

技術的対策（SPF、DKIM）
人的対策

標的型メール攻撃対策

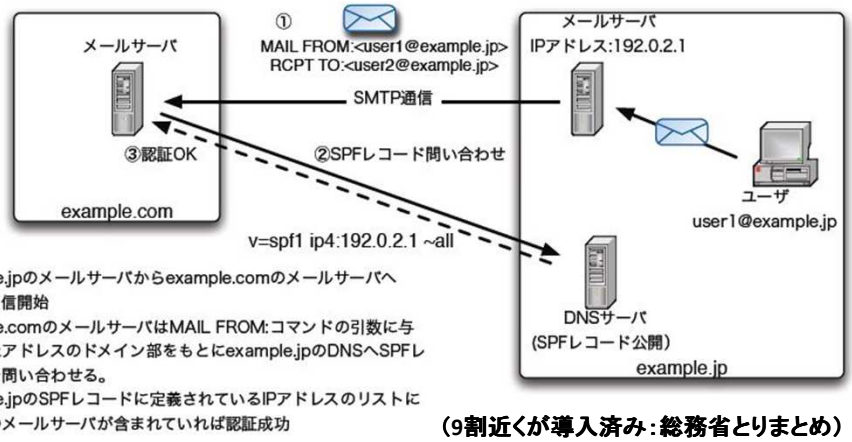
技術的対策

標的型メールかどうかをメールシステムにて確認し、直接排除またはメール受信者への注意喚起等により、標的型攻撃メールの被害回避を目指した対策

人的対策

教育・訓練により、メール受信者（社員・職員）の標的型攻撃メールを見極める能力を高め、標的型メールかどうかを受信者本人に確認させ、標的型攻撃メールの被害回避を目指した対策

現在の技術的対策（1）
SPF（Sender Policy Framework）

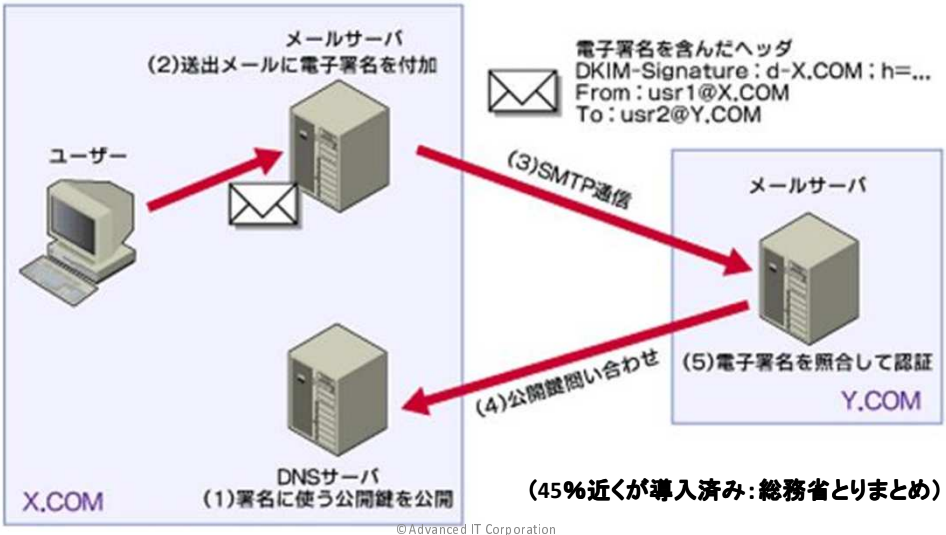


① example.jpのメールサーバからexample.comのメールサーバへSMTP通信開始
② example.comのメールサーバはMAIL FROM:コマンドの引数に与えられたアドレスのドメイン部をもとにexample.jpのDNSへSPFレコードを問い合わせる。
③ example.jpのSPFレコードに定義されているIPアドレスのリストに送信側のメールサーバが含まれていれば認証成功

（9割近くが導入済み：総務省とりまとめ）

http://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/spf/#30

現在の技術的対策（2）
DKIM（Domainkeys Identified Mail ）



（45%近くが導入済み：総務省とりまとめ）

http://www.atmarkit.co.jp/ait/articles/0602/16/news114.html

現在の技術的対策の課題

なりすましメールを防ぐには、
より確実なメール送信者の認証が必要！

標的型攻撃メールの多くは送信元アドレスの詐称！

詐称元は、企業、官公庁が7割超

（「標的型攻撃メールの傾向と事例分析＜2013年＞」IPAの資料より）

SPF,DKIM共にドメイン（メールサーバ）認証技術

ドメインの詐称は検知可能だが・・・

＝＞攻撃者が独自ドメインを取得しメールサーバを運用した場合は、対応不可！

＝＞ドメインの正規のメールサーバが（不正に）利用された場合は、検出不可！

＊メール送信用のSMTPプロトコルには、メール送信者認証機能無し
メールサーバを利用し、なりすましメールを送信することは容易

＊SMTP auth（RFC2554）は、パスワードによるメール送信者の認証機能有り
パスワードベースのメール送信者認証の場合でも
0.2～0.3%のID/PWDが盗まれている（調査結果あり）

現在の技術的対策の課題

電子メールシステムの脆弱性に基づく課題を、
電子メールシステムそのものには手を付けず、
周辺ソフト・技術による現在の対策には限界！

現行の電子メールシステムの仕様との整合性には
配慮しつつも、悪意のあるメールが流通・氾濫する
時代に対応できる仕組みの考案・導入が不可欠！

人的対策の現状・課題

府省庁の標的型メール攻撃に対する職員の教育・訓練報告

平成24年度　19府省庁　約12万人
開封率：1回目14.6%　2回目10.6%
平成25年度　18府省庁　約18万人
開封率：1回目10.1%　2回目16.3%

➔標的型メールを見分ける能力の醸成は必要だが、効果は限定的
（5%の開封率でも、組織内の100人に標的型メールが送られれば
99%以上の確率で開封され、組織は被害に遭うことになる。）

組織への不正侵入を防げるか（効果？）

電子メールの利用状況

日本:

企業のホワイトカラーのメール受信数　39通/日
メール送信数　12通/日
＜ビジネスメール実態調査2017より＞

メール処理時間は1日2.27時間
（業務従事時間の約1/3はメール処理）
＜JUAS Advanced研究会の2015年報告より＞

米国:

典型的ビジネスユーザのメール処理時間146分/日
（電話:54分、IM:23分、SM:18分）
＜2010年5月のOsterman Research Surveyより＞

典型的ビジネスユーザのメール送受信数　133～160通/日
＜2009年のWall Street Research Reportより＞

人的対策の現状・課題

99%以上のビジネスマンがメールを主たる通信手段
12通のメール送信、39通のメール受信（1日平均）
「ビジネスメール実態調査 2017」

標的型攻撃メールかどうかの確認ポイントは多数！
場合によっては差出人に確認、専門家へ相談も必要

府省庁の教育・訓練受講者18万人が、39通の受信メールの標的型攻撃メールかどうかの判断に、仮に1日あたり15分～30分、人的対策遂行のため時間がかかったとすると・・・

➔　年間270億～540億の費用負担に相当

このような人的対策の費用負担は問題では？

人的対策の現状・課題
費用負担の試算例

[人的対策充当時間]
社員・職員が標的型攻撃メールかどうかの判断ために
新たに必要となる時間　15分～30分/1日

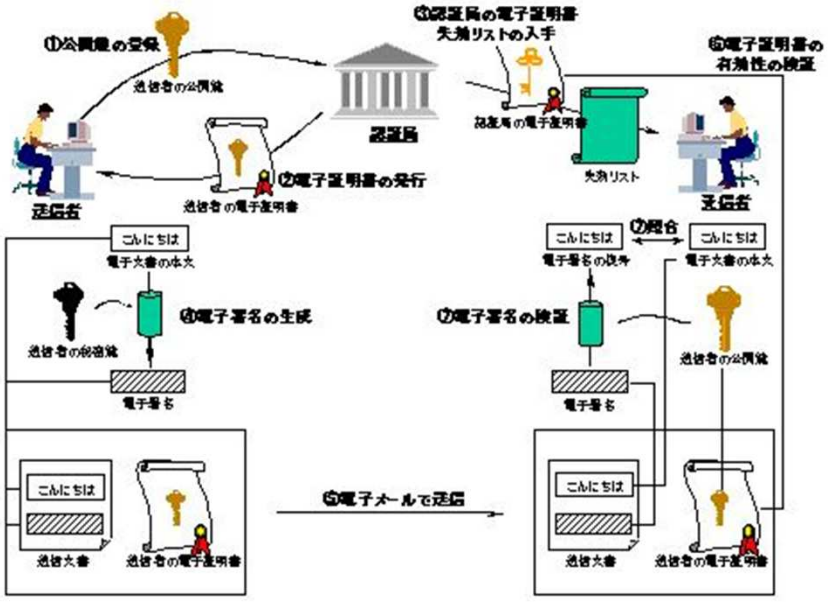
[対象とする公務員数・給与]
国家公務員　60万人（一般職34万人）　給与41万円
地方公務員　280万人（一般職90万人）　給与38万円
1か月あたりの見えない人的対策費用
≒34万人＊41万円＊（15分/8時間）　・・・　国家公務員
＋90万人＊38万円＊（15分/8時間）・・・　地方公務員
≒約150億/月　（年間1800億！）

[日本社会としての負担は莫大]
民間社員（300人以上の事業所）　約1800万人

➔人的負担軽減のため、より効果的な抜本的な
技術的対策の開発・導入に注力すべき！

（3）セキュアメール標準
S/MIMEの有効性と限界

S/MIMEとは



S/MIMEを利用した電子メールの例（https://www.ipa.go.jp/security/enc/digitalsignature/01_ML.htm）

S/MIME
Secure/Multipurpose Internet Mail Extensions

電子メールへ電子署名や暗号化の機能を付加する規格。

1995年に最初の版が開発され、1998年にIETFへセキュリティ標準の一つとして提案され、以来、IETFにて仕様が検討され標準化が進められてきた。

最新版Version3.2の仕様は、RFC5750、RFC5751(2010年1月）として発行されている。

S/MIMEの利用により、「間違いなく本物の送信者からのメールであること」を受信者が確認できる（メール送信者の確実な認証が可能）。

➔ **送信者のなりすましによる標的型メール攻撃の無効化が可能！**

「サイバーセキュリティ2013」（平成25年6月　情報セキュリティ政策会議）でも、
“DKIMやS/MIMEのように暗号技術を利用した対策の導入を推進”という方針が記載され、
「標的型攻撃に対抗するための通信規格の標準化に関する調査結果」
（平成25年3月　総務省情報通信国際戦略局通信規格課）でも、
“電子メールによるなりすまし被害の防止対策の1つである、S/MIME”と記載され
S/MIMEの導入方法が説明されている。

しかし、現実にはあまり活用されていない！

S/MIME普及の課題・方式の限界

(1)メールアドレス証明書（電子証明書）
が必要であり費用負担が発生（年間数千円）

(2)通信相手のメールアドレス証明書の更新・管理が必要
通信相手それぞれのメールアドレス証明書
（自分自身の秘密鍵の安全な管理も必要）

(3)自らのS/MIME導入努力・投資だけでは効果無し
社会基盤として普及させることが必要

(4)機密情報の不正流出を防げない
暗号化ファイルのコンテンツ検査が困難

(5)ウイルス等のマルウェアの流入を防げない
暗号化ファイルのセキュリティ検査が困難

＊20＊

（4）安心・安全電子メール利用基盤 SSMAX

（Secure and Safe eMAil eXchange framework)

悪意のあるメールの流通・氾濫を防ぐ！

悪意のあるメール発信の可能性の無い組織
であることを確認の上、メールを受信

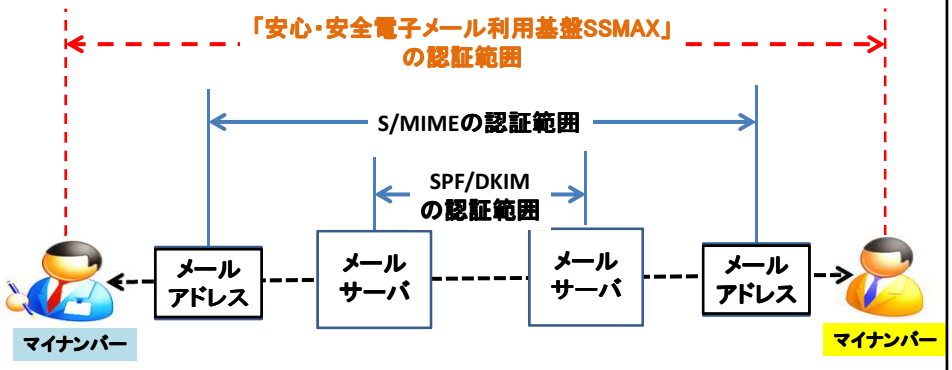
➔受信者に悪意のあるメールが到達できないように！
（悪意のあるメール発信の可能性の低い組織かどうか
によりメール受信の是非を判断）

悪意のあるメール送信者の特定・追跡による
悪意のあるメール発信源の除去

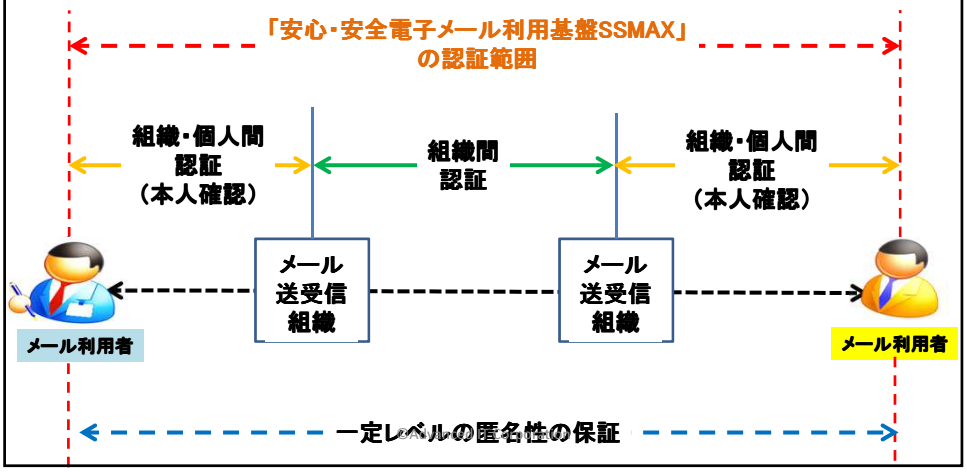
➔メール送信者の端末からのウイルス等の駆除

➔悪意のあるメール送信者の
安心・安全な電子メール利用環境からの排除！

メール送信者の特定・追跡のために



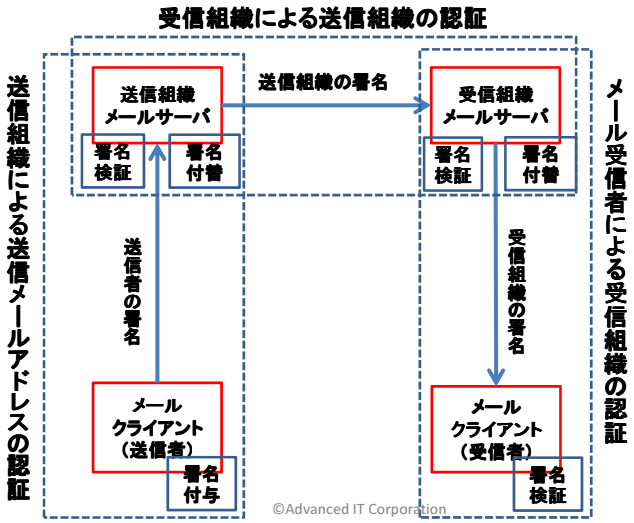
メール送信者の特定・追跡のために



メール送信者の特定・追跡のために
SSMAXで実現する四つの仕組み

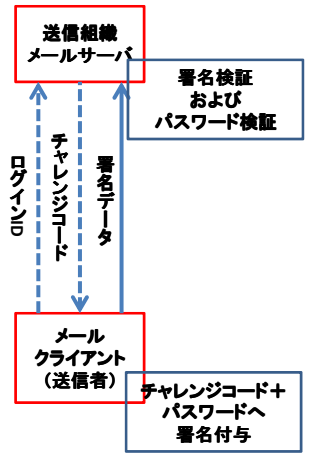
①「送信メールアドレスの認証」に関する仕組み
　メールアドレス証明書記載のメールアドレスから、
　　送信されたメールかどうか
②確実な「送信者の本人確認」に関する仕組み
　メールアドレス証明書の発行を受けた
　　その本人が送信したメールかどうか
③「送信者の特定・追跡性」に関する仕組み
　メールアドレス証明書の発行を受けた
　　その本人を特定・追跡可能なメールかどうか
④「送信組織の信頼性」確認に関する仕組み
　①～③を適切に実施している送信組織かどうか

①「送信メールアドレスの認証」に関する仕組み



＊AE＊

②確実な「送信者の本人確認」に関する仕組み（2Way認証の例）

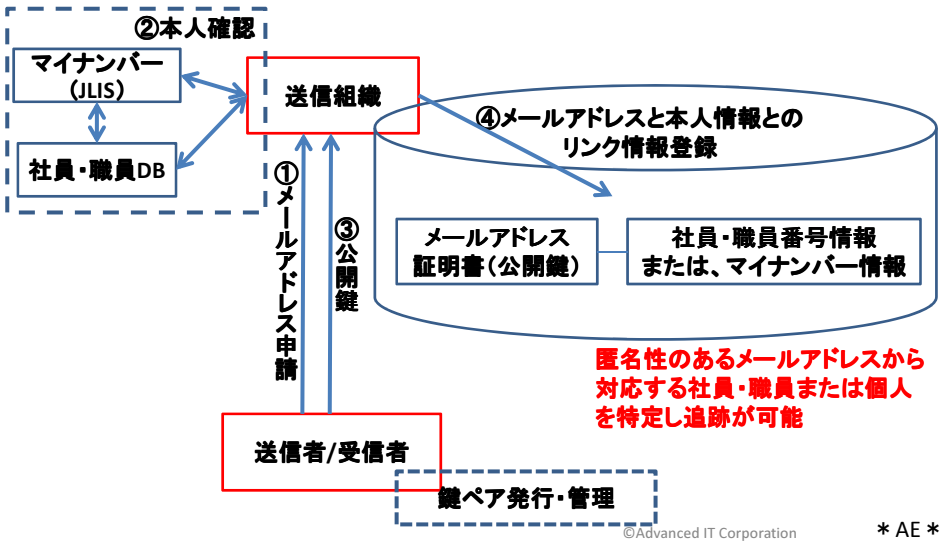


耐タンパーなリムーバブルデバイス内での署名付与
（例：職員証カード、マイナンバーカード）

©Advanced IT Corporation

＊AE＊

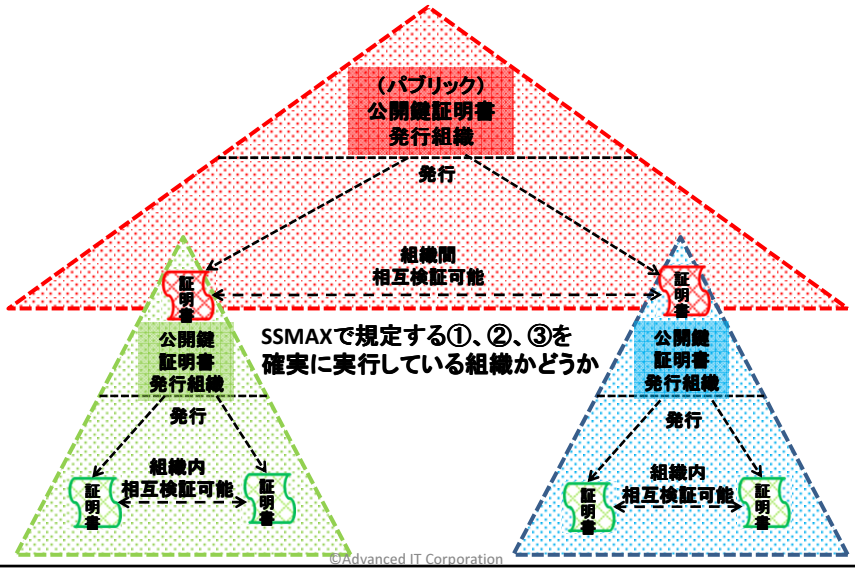
③「送信者の特定・追跡性」に関する仕組み



＊AE＊

＊AE＊

④「送信組織の信頼性」確認に関する仕組み



＊30＊

電子メール利用者/組織の社会的責任

なりすましされた電子メール利用者/組織は、被害者では無い！

➔ なりすましを許す状況を放置していたのは、加害者の攻撃を助長する行為！

“OECD情報セキュリティ・ガイドライン（2002年8月発表）の「責任の原則」”
すべての参加者は、情報システム及びネットワークの
セキュリティに責任を負う。

メールアドレスが悪用された電子メールサービス事業者（組織）は、
社会的責任を負うべきである！

➔ 悪意のあるメール送信に利用された場合、
メールアドレス利用者の特定・追跡および是正要請・排除等の
対応措置の責任を負うべきである！

“OECD情報セキュリティ・ガイドライン（2002年8月発表）の「対応の原則」”
参加者は、セキュリティの事件に対する予防、
検出及び対応のために、時宜を得たかつ協力的な方法で
行動すべきである。

https://www.ipa.go.jp/security/fy14/reports/oecd/handout.pdf

「安心・安全電子メール利用基盤」

Secure and Safe eMAil eXchange framework(SSMAX)

（1）送信者の特定・追跡が可能な電子メール利用基盤
悪意のある電子メールの流通・氾濫を抑止可能！

（2）送信情報の保護が可能な電子メール利用基盤
個人情報・秘密情報の送信にも利用可能！

（６）安心・安全な
インターネット社会に向けて

（１）まずは、電子メール利用リテラシーを！

（２）次に、現時点で利用可能なS/MIMEの普及を！

＊費用負担、手間、組織の場合は暗号化

（３）抜本的には、SSMAXの開発・普及を！

＊試作・評価・実証実験

＊国民的合意形成

＊強力な政策による社会実装推進

（４）更に、メール以外のコミュニケーション基盤への
SSMAX思想の展開を！

（５）更に、情報を発するIoT機器についても、
SSMAX思想の展開を（＝＞SSIoT）！

終

SSMAXについての詳細は・・・

情報処理学会　論文誌　2018年9月号
「超スマート社会を支えるコンピュータセキュリティ技術」 特集

「安心・安全電子メール利用基盤（SSMAX）」
悪意のあるメールの根絶とメール内容の確実な保護を目指して