「安心・安全電子メール利用基盤」構想
Safe and Secure E-mail Exchange Framework (SSMAX)

2017年1月26日

才所 敏明　五太子 政史　辻井 重男
中央大学研究開発機構

toshiaki.saisho@advanced-it.co.jp

（1）電子メールは現在も基本的・共通的コミュニケーション基盤

電子メールの黎明期

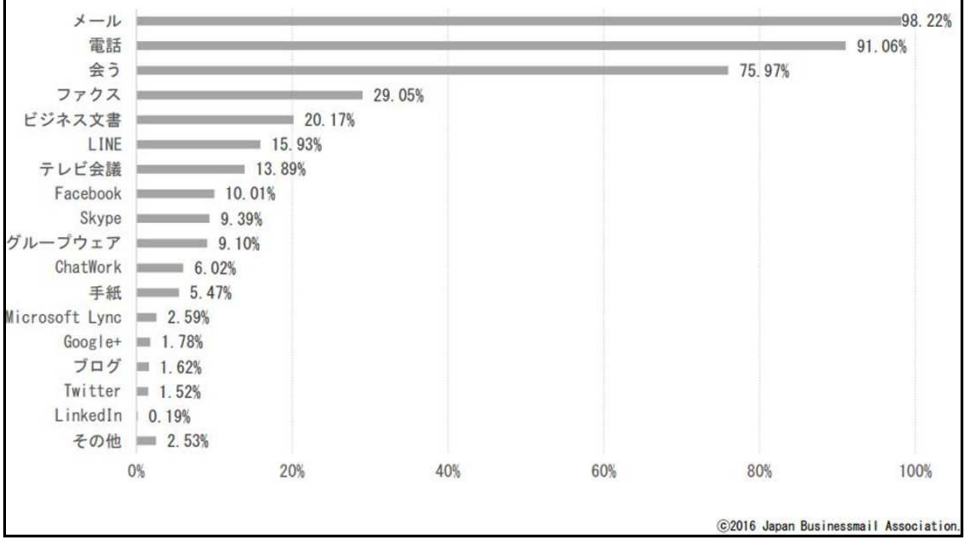
1984年　JUNET実験開始（東芝も参加）

1986年　企業での電子メール利用に関する議論開始
　　５～６社＋大学関係者10名程度の構成

1987年　InetClub発足（企業での電子メール利用実験）

1992年　AT&T Jens（現SpinNet）が日本初の、
　　インターネットイニシアティブ (IIJ) が日本企業初の
　　ISPとしてサービスを開始

電子メール
現在も、組織（業務）通信の主役



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　55通/日
メール送信数　　12通/日
＜JUAS Advanced研究会の2016年報告より＞
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＞

（2）組織を脅かす標的型攻撃

標的型攻撃メールが
標的型攻撃における侵入手段の主役

標的型攻撃の現状

標的型攻撃による情報漏洩等の被害が多発

＊日本年金機構の情報漏洩事件（2015年５月）

機構の公開/非公開メールアドレス宛てに、

業務に関係ありそうな件名のメール送信

約125万件の個人情報の流出の可能性

＊（株）ジェイティービー（JTB）の情報漏洩事件（2016年３月）

実在する取引先企業のメールアドレスになりすまし

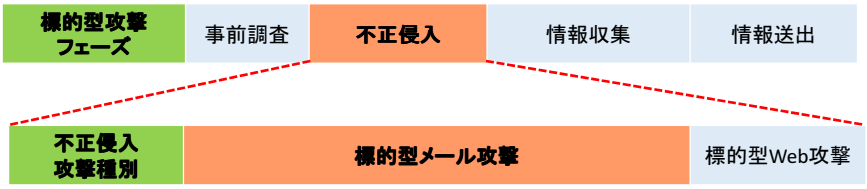
約793万人分の個人情報の流出の可能性

社会的影響が大きかったセキュリティ上の脅威の1位が

「標的型攻撃による情報漏洩」（組織にとっての最大の脅威）

＜「情報セキュリティ10大脅威 2016」（IPA）より＞

標的型攻撃の侵入手段
＜　標的型メールが主役　＞



不正侵入手法の中心は「標的型メール」！
　国内標的型サーバー攻撃分析レポート2015年版（トレンドマイクロ資料）
「標的型メール」は標的型攻撃の不正侵入手法の主役！
　平成27年上半期のサイバー空間をめぐる脅威の情勢について（警察庁資料）

政府機関に対する標的型メール攻撃は、前年度の3倍に急増！
　サイバーセキュリティ政策に係る年次報告（2014年度）
　（平成27年7月サイバーセキュリティ戦略本部）
標的型メール攻撃件数は過去最高！
　平成27年におけるサイバー空間をめぐる脅威の情勢について（警視庁資料）

（3）揺らぐ電子メールへの信頼

我が国の産業・社会活動を支える
「安心・安全電子メール利用基盤」の必要性

我が国の産業・社会活動を支える「安心・安全電子メール利用基盤」構築へ

①電子メールは
　我が国の基礎的・共通的コミュニケーション基盤
　将来にわたっても、その地位は不変
　組織の産業活動、個人の社会・文化活動を支える
　重要なコミュニケーション基盤（重要インフラの一つ？）

②標的型メール/フィッシングメールの氾濫により
　電子メールによるコミュニケーションへの
　信頼感が失われつつある

我が国の産業・社会活動を支える
「安心・安全電子メール利用基盤」（SSMAX）の必要性

「安心・安全電子メール利用基盤」（SSMAX）
で実現を目指すセキュリティ機能

①悪意のある電子メールの氾濫防止

②電子メール情報の漏洩防止

（4）悪意のある電子メールの氾濫防止

送信メールアカウント保有者の
特定・追跡性が重要

悪意のあるメールの氾濫を防ぐには

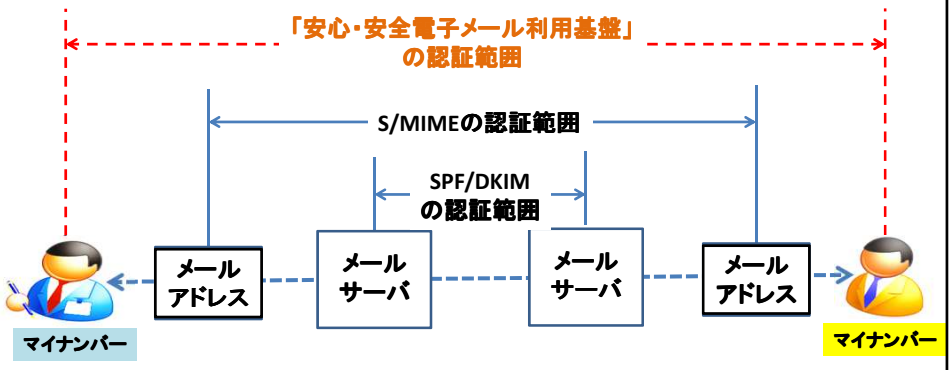
悪意のあるメールの特定・検知による被害回避

➔悪意のある攻撃者の費用対効果を下げ
攻撃意欲をそぐ

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

➔悪意のある攻撃者の
「安心・安全電子メール利用基盤」からの排除

メール送信者の特定・追跡のために



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、被害者では無い！

➔ 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

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

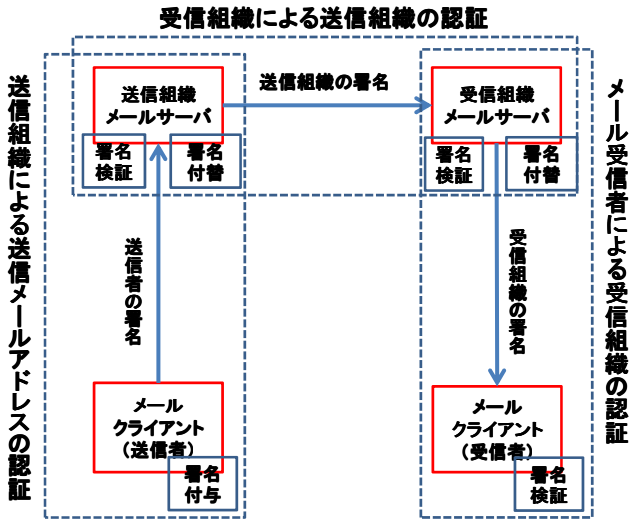
①「送信メールアドレスの認証」に関する仕組み
メールアドレス証明書記載のメールアドレスから、
送信されたメールかどうか

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

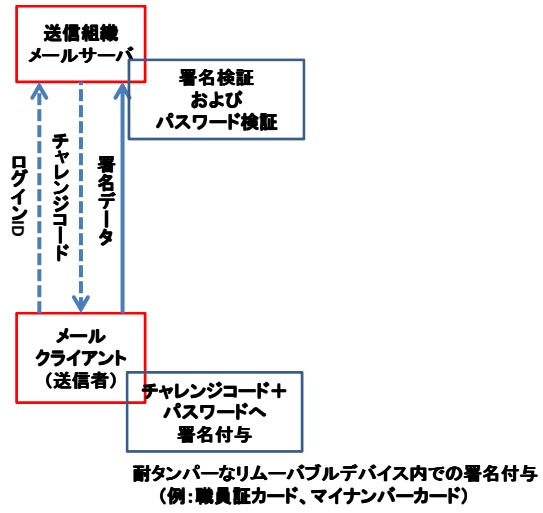
③「送信者の特定・追跡性」に関する仕組み
メールアドレス証明書の発行を受けた
その本人を特定・追跡可能なメールかどうか

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

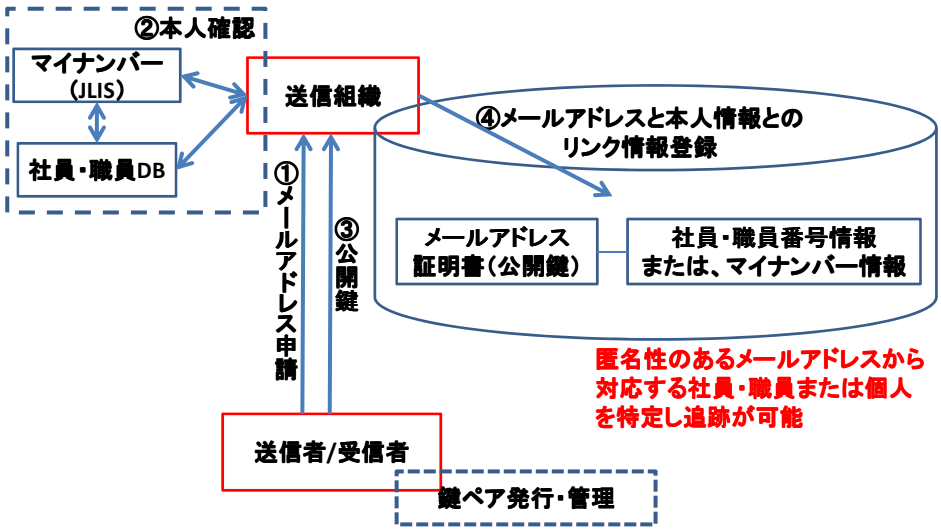
①「送信メールアドレスの認証」に関する仕組み



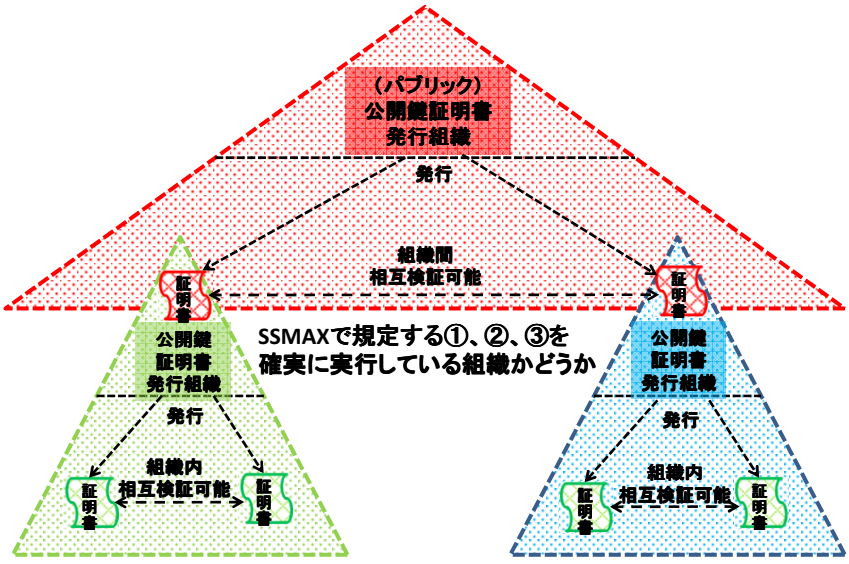
②確実な「送信者の本人確認」に関する仕組み（2Way認証の例）



③「送信者の特定・追跡性」に関する仕組み



④「送信組織の信頼性」確認に関する仕組み



（5）電子メール情報の漏洩防止

組織として導入可能な
暗号利用方式が重要

暗号化の両刃的性質

暗号化のメリット：
　電子メール情報の漏洩防止が可能

暗号化のデメリット：
　①送信電子メールによる
　　機密情報の不正な持出の検知・防止が困難
　②受信電子メール内の
　　マルウェア等の検知・除去が困難

暗号メールと言えども、
　　組織としての責任を果たすためには
　　一旦復号しての検査機能は不可欠

電子メール情報の漏洩防止のために SSMAXで実現する二つの仕組み

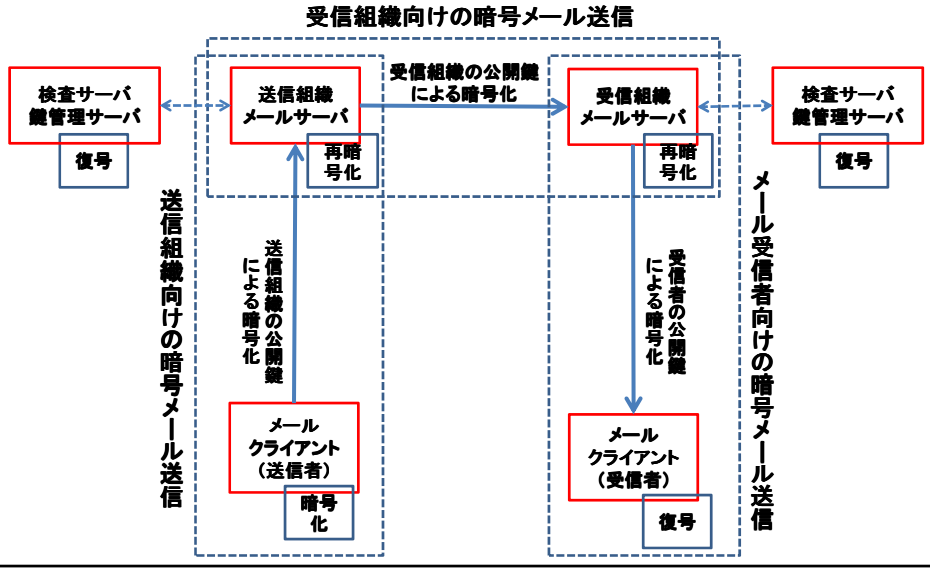
①送信組織での機密情報の不正持出有無検証の仕組み

送信組織が外部にメールを送信する際に、
検証サーバで機密情報の不正持出の有無を検証
検証サーバは鍵管理サーバの支援により復号し検証
検証結果はメールサーバへ通知

②受信組織でのマルウェア等の悪意の有無検証の仕組み

受信組織が内部にメールを配信する際に、
検証サーバでウイルス等の悪意の有無を検証
検証サーバは鍵管理サーバの支援により復号し検証
検証結果はメールサーバへ通知

暗号化の連鎖による情報漏洩防止と 機密情報不正持出・マルウェア流入防止



（６）「安心・安全電子メール利用基盤」

Safe and Secure E-mail
Exchange Framework　(SSMAX)

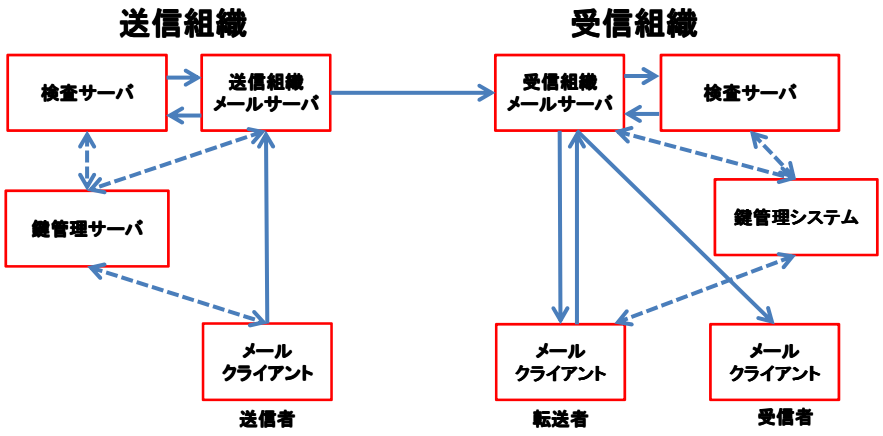
「安心・安全電子メール利用基盤」

Safe and Secure E-mail 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

（２）送信情報の保護が可能な
電子メール利用基盤

SSMAXの全体構成



（7）今後の課題

安心・安全な情報交換・共有が可能な
サイバー空間の実現を目指して

今後の課題

①SSMAXの社会実装
- ＊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

②相互運用性のための国内・国際標準化
- ＊データ形式・プロトコル仕様
- ＊組織認証のための検証項目・評価基準・評価証明書
- ＊事故・事件発生時の運用手順

③他の情報交換・共有基盤への適用
- ＊Webベース情報交換・共有
- ＊SNSベース情報交換・共有

終