CSS2017

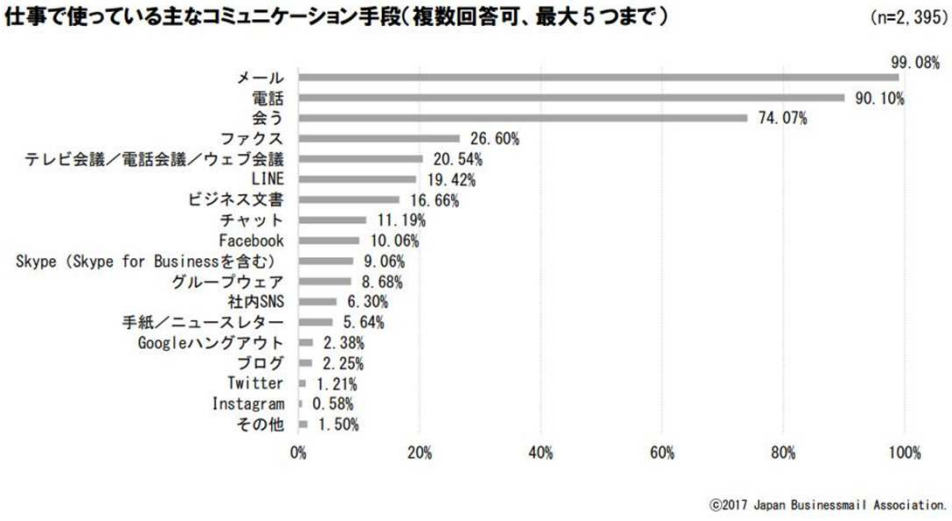
安心・安全電子メール利用基盤（SSMAX）

2017年10月24日

才所 敏明　五太子 政史　辻井 重男
中央大学研究開発機構

1

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）

3

安心・安全電子メール利用基盤（SSMAX）が目指す世界は・・・

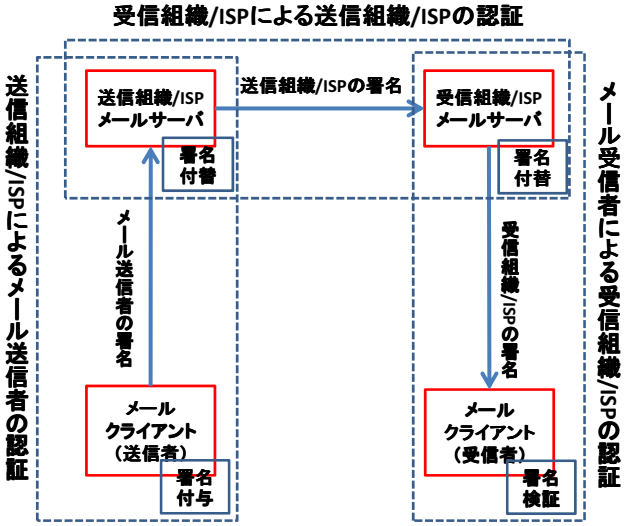
（1）サイバー攻撃に利用されない電子メール！

（2）電子メールが安心して活発に利用されるように！
　サイバー攻撃メールだけでなく、いじめや脅迫等の
　悪意のあるメールの氾濫を防ぎ、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
　（1984年日本でのインターネットの歴史が始まって以来、
　電子メールの産業界での活用を推進してきた一員としては
　現在はちょっと悲しい状況）

（3）安心・安全電子メール利用基盤（SSMAX）の実現により、
　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基盤を確立したい！

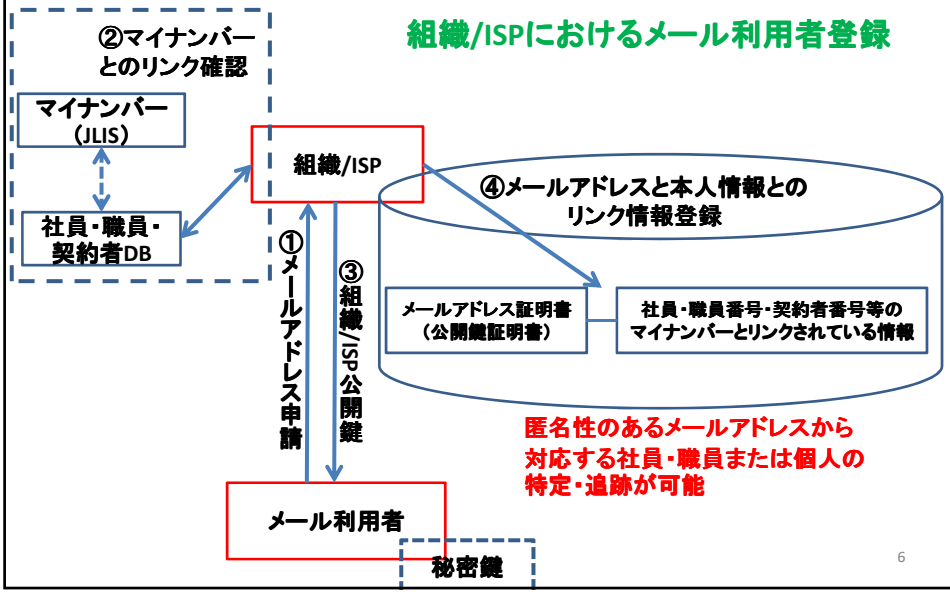
4

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）



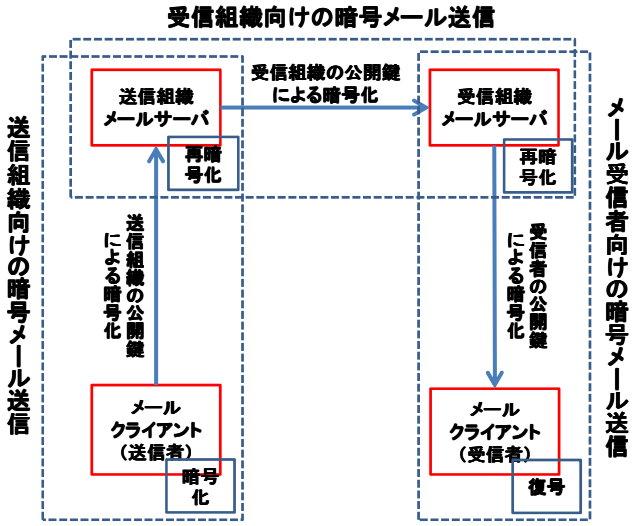
5

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



6

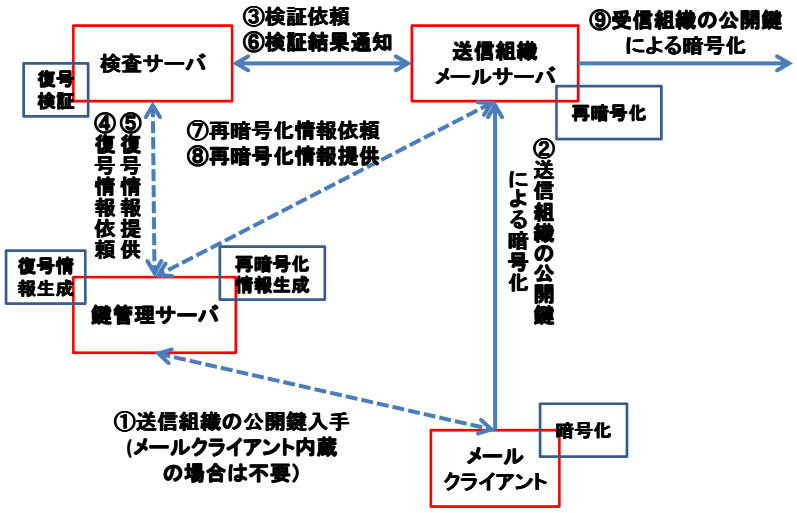
メール内容の秘匿（漏洩防止）



暗号化の連鎖

7

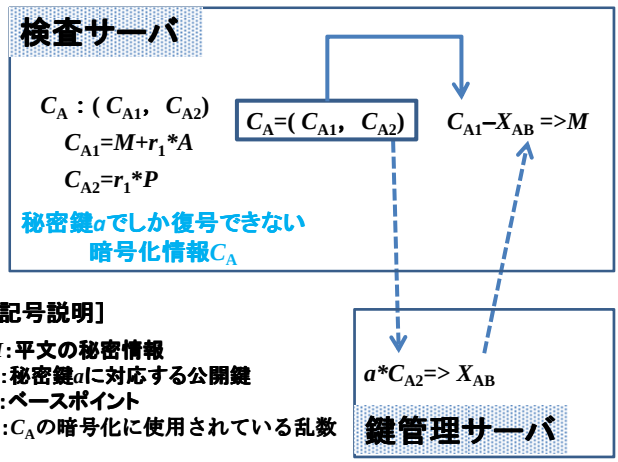
送信組織における暗号化送信メールの検査方式



秘密情報の不正な持出の検知・防止方式

8

検査サーバにおける復号手順

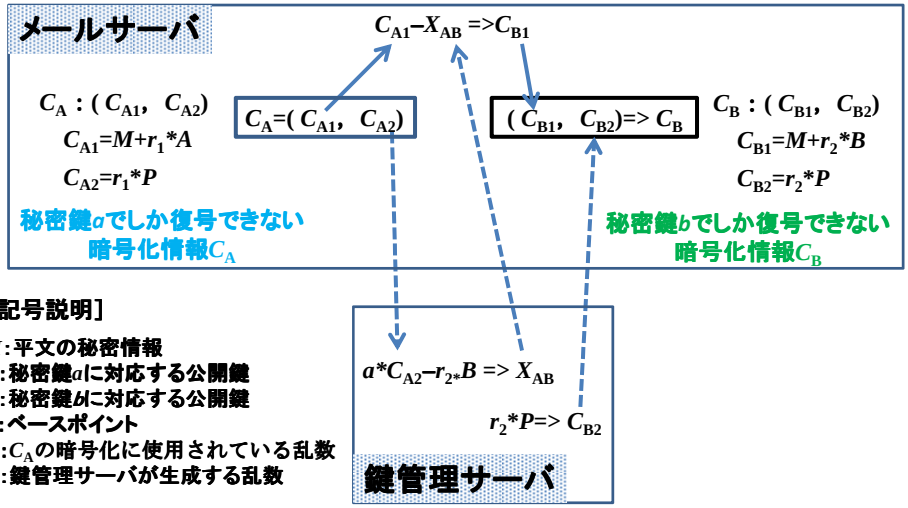


［記号説明］

M:平文の秘密情報
A:秘密鍵aに対応する公開鍵
P:ベースポイント
r_1:C_Aの暗号化に使用されている乱数

9

メールサーバにおける再暗号化手順

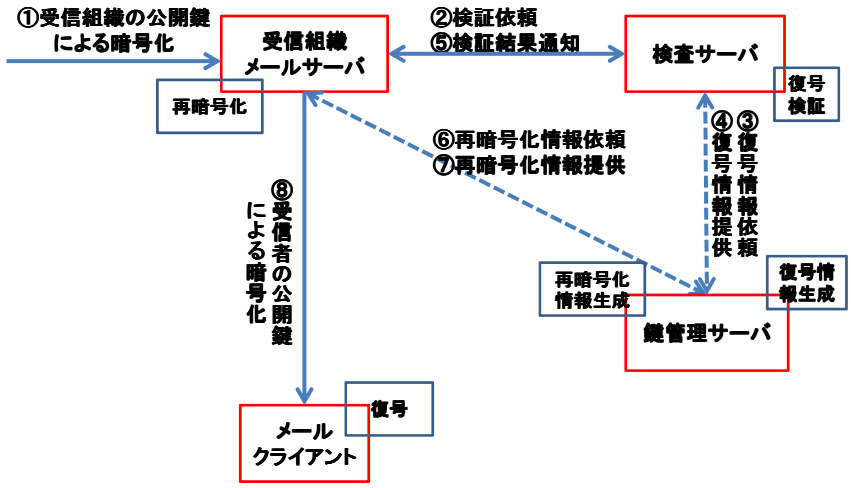


［記号説明］

M:平文の秘密情報
A:秘密鍵aに対応する公開鍵
B:秘密鍵bに対応する公開鍵
P:ベースポイント
r_1:C_Aの暗号化に使用されている乱数
r_2:鍵管理サーバが生成する乱数

10

受信組織における
暗号化受信メールの検査方式



マルウェア検知・流入防止方式

11

メール送受信者が組織に所属しない
個人の場合のメール内容の秘匿方式

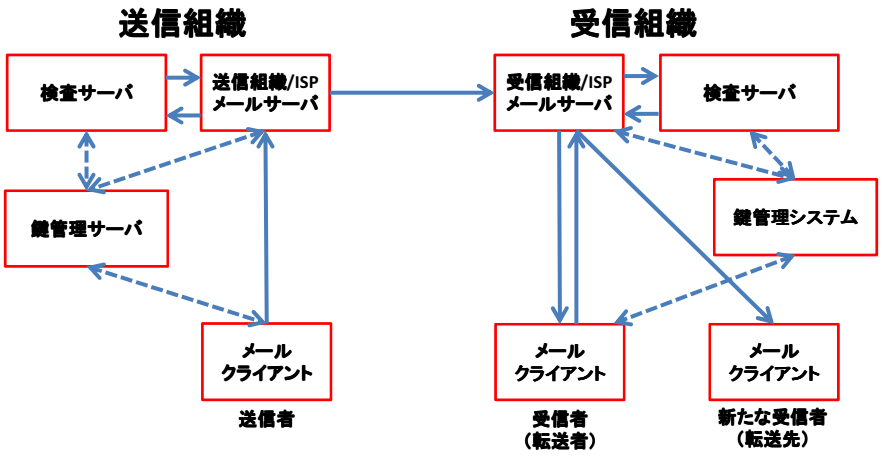
個人情報・プライバシー情報保護の観点から

暗号化送信メールの復号しての検査
および、暗号化受信メールの復号しての検査は、
原則行わない。

但し、メール利用者の同意（希望）があれば、実施。

12

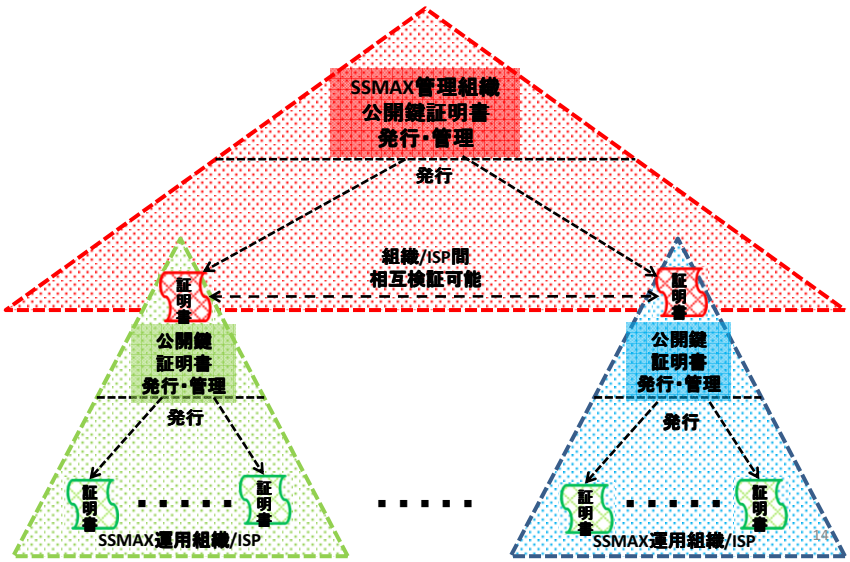
安心・安全電子メール利用基盤（SSMAX）



SSMAXシステム構成

13

SSMAXにおけるPKIの階層



14

SSMAX利用者（メール送受信者）

（1）メール利用申請手続き
本人確認情報、特定・追跡のための情報送付
メールアドレス、所有者名の情報、自身の公開鍵送付
所属する組織/ISPの公開鍵証明書、
自身の公開鍵証明書の入手・管理
（2）メール送信手続き
所属する組織/ISPの公開鍵による暗号化
自身の秘密鍵による署名付与
（3）メール受信手続き
所属する組織/ISPの公開鍵による署名検証
自身の秘密鍵による復号
（4）維持・管理が必要な情報
自身の秘密鍵、公開鍵（証明書）
所属する組織/ISPの公開鍵（証明書）

15

送信（受信）組織/ISP

（1）メール利用者登録手続き
本人確認、特定・追跡性確認
申請者のメールアドレス（公開鍵）証明書発行・送付、自組織/ISPの公開鍵証明書送付
メールアドレス証明書、特定・追跡のための情報の登録・管理
（2）メールサーバ、検査サーバ登録手続き
メールサーバ、検査サーバの公開鍵証明書発行・送付・管理
（3）SSMAX管理組織へ参加・継続申請手続き
SSMAX運用体制等を示す書類、自組織/ISPの公開鍵
（4）送信メール処理手続き
メールサーバは、検査サーバへ転送し検査を依頼
検査サーバは、鍵管理サーバの支援を受け復号し検査、検査結果をメールサーバへ通知
メールサーバは、鍵管理サーバの支援を受け、宛先組織/ISP（受信者）向けに再暗号化し送信
（5）SSMAX管理組織対応処理手続き
（悪意のあるメールを受信した場合、SSMAX管理組織経由、送信組織/ISPへ対応依頼）
悪意のあるメール送信の連絡を受けた場合、該当するメール利用者に対応依頼
（6）維持・管理が必要な情報
鍵管理サーバ：自組織の秘密鍵、公開鍵証明書、通信相手組織/ISPの公開鍵証明書
利用者のメールアドレス証明書、特定・追跡のための情報
メールサーバ、検査サーバの公開鍵証明書
メールサーバ、検査サーバ：自身の秘密鍵、公開鍵（証明書）、組織/ISPの公開鍵証明書

16

SSMAX管理組織

（1）組織/ISP登録・継続手続き

SSMAXが適切な運用が

実行される/されているかどうかの判定

組織/ISPの公開鍵証明書発行・送付

（2）悪意のあるメール発生対応手続き

組織/ISP間の通知/回答の確認・記録

17

安心・安全な電子メール利用環境の実現に向けた対策の比較

		現状	既存技術の普及	新技術の開発・普及
対策内容		SPF、DKIMによるメールサーバ認証の仕組み	S/MIMEによるメール送信者認証の仕組み	SSMAXによるメール送信者認証・特定・追跡の仕組み、およびメール内容秘匿の仕組み
対策の特徴	費用	人的対策費用：年間600億 ＊公務員一般職120万人が1日5分人的対策投入時 ＊民間企業の対象社員数は、その10倍以上	パブリック・メールアドレス証明書：年間24億 ＊公務員一般職120万人へ証明書配布 ＊民間企業の対象社員数は、その10倍以上	パブリック・公開鍵証明書：年間2億 ＊官公庁2000組織へ公開鍵証明書配布 ＊民間企業の対象組織数は、その7倍以上 その他のSSMAX運用：年間数億 ＊SSMAX管理組織運営
	手間	組織側：SPF、DKIM導入・運用 社員側：メール受信の都度、 悪意のあるメールかどうかのチェック・判断	組織側：パブリック・メールアドレス証明書発行・更新 社員側：通信相手全てのメールアドレス証明書の入手・管理 通信相手の定期的な更新に対応した更新 （通信する社員全員が対象）	組織側：プライベート・メールアドレス証明書発行・更新 社員側：自分の秘密鍵および所属する組織の公開鍵のみの管理で良い
	プライバシー	メール内容の保護は不可	メール内容の保護は不可 ＊暗号化機能は存在するが、社会実装は不可	メール内容の保護が可能
	その他	メール送信者の認証は不可 悪意のあるメールの氾濫抑止は不可 ＊メール送信者の特定・追跡は不可	悪意のあるメールの氾濫抑止は不可 ＊メール送信者の特定・追跡は不可	悪意のあるメールの氾濫抑止が可能 ＊メール送信者の特定・追跡が可能で、悪意のあるメールの送信停止等の措置可能
対策完了後の姿		悪意のあるメール対策 ＊状況は悪化するばかりで、好転する可能性は無い ＊人的対策に依存し続けざるを得ない メールによるコミュニケーション範囲 ＊個人情報、機密情報を含むコミュニケーションには使用不可	悪意のあるメール対策 ＊対策効果は限定的 ＊人的対策に依存し続けざるを得ない メールによるコミュニケーション範囲 ＊組織の機密情報を含むコミュニケーションには使用不可	悪意のあるメール対策 ＊悪意のあるメールの完全排除は難しいが、発信源からの悪意のあるメールの継続的な発信を止めることは可能 メールによるコミュニケーション範囲 ＊個人情報、組織の機密情報を含むコミュニケーションが可能

「安心・安全電子メール利用基盤（SSMAX）」：ネット依存が高まる現代社会に様々の混乱・不安を与える電子メールのセキュリティ上の課題を抜本的に効率的に克服できる。SSMAXの社会実装により、我が国の産業活動や国民の生活活動を支える安心・安全な基礎的・共通的コミュニケーション基盤の、早期確立を目指したい。

18

SSMAXで実現できること

（1）メール送信者の認証のみならず、特定・追跡が可能
悪意のあるメール発信源を速やかに停止させることが可能
＝＞SSMAX参加組織間では悪意のあるメールの氾濫は無く、
一定レベルの安全性が確保され、安心してメール受信可能

（2）標的型攻撃メールの流通を抑止可能で、リスクを大幅に低減可能

（3）個人・組織を対象とした、
中傷・脅迫・いじめなど、悪意のあるメールの氾濫も抑止可能

（4）メール情報の秘匿も可能で、個人情報・秘密情報に拘らず、
安心して緊密なコミュニケーションが可能

（5）安心・安全電子メール利用基盤により、
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基盤の確立へ

終

ご清聴、ありがとうございました。

20

当日、会場で受けた
主要な質問への回答と今後の課題

（1）組織間のセキュアな電子メール転送に、
なぜSSL/TLSを使用しないのか？
＝＞代替案については未検討と回答したが、
SSL/TLSによる代替は様々の課題が発生するはず。
代替案の可能性・是非についての検討が必要か。

（2）そこまで大きく変えるのなら、
全く違ったコミュニケーション方法を検討しては？
＝＞原則、メールの基本的なプロトコル等は変更しない、
現在の電子メールの枠組で対応可能と説明。
SSMAX実現に必要な追加機能モジュールを整理し、
現在のメールシステムとの関係の説明整理が必要か。