標的型メール攻撃に対抗する「組織通信向けS/MIME」

2016年9月23日
才所 敏明
中央大学研究開発機構
toshiaki.saisho@advanced-it.co.jp

自己紹介

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門
＊本社情報システム部門に所属 、東芝Gの技術部門・研究部門の
研究開発活動環境の整備・高度化を推進

1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門
＊東芝のセキュリティ技術センター発足と同時にセンター長就任
＊その後、東芝Gのセキュリティ技術開発・事業支援活動を推進

2007年10月～　(株)IT企画を設立
＊情報技術および情報セキュリティ技術分野の研究開発や
その応用事業に対するプロフェッショナルサービスを開始
＊法政大学、日本大学で情報セキュリティに関する講義担当

2013年5月～　中央大学研究開発機構
＊国立研究開発法人情報通信研究機構（NICT）より受託した
「組織間機密通信のための公開鍵システムの研究開発」PJより
研究員として参加

本日のお話

（1）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
（2）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
（3）標的型メール攻撃対策の現状とその課題
人的対策と技術的対策
（4）暗号メール標準S/MIMEの可能性と課題
提供機能・実現方式とその普及上の課題
（5）組織通信向けS/MIMEの可能性
提供機能・特徴、S/MIMEの課題の克服方策

（1）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＞

標的型攻撃の手順

(1)事前調査

不正侵入に有益な、攻撃対象とした組織やシステムの情報を調査する。

(2)不正侵入

事前調査で得た情報を利用し、攻撃対象組織の内部へウイルス等のマルウェアを送り込む。

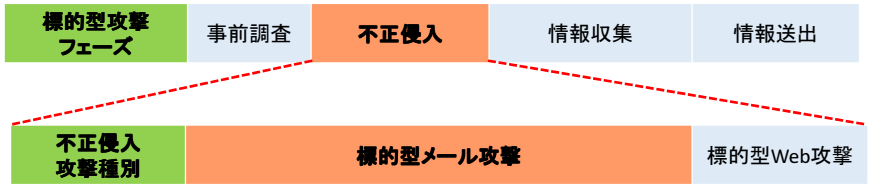
(3)情報収集

侵入に成功したマルウェアが、組織ネットワーク内の情報を探索し収集する。

(4)情報送出

収集した情報を攻撃者へ届けるべく、組織外へ送出する。

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）

2015 年に公表された
主な情報窃取サイバー攻撃事例とその内容

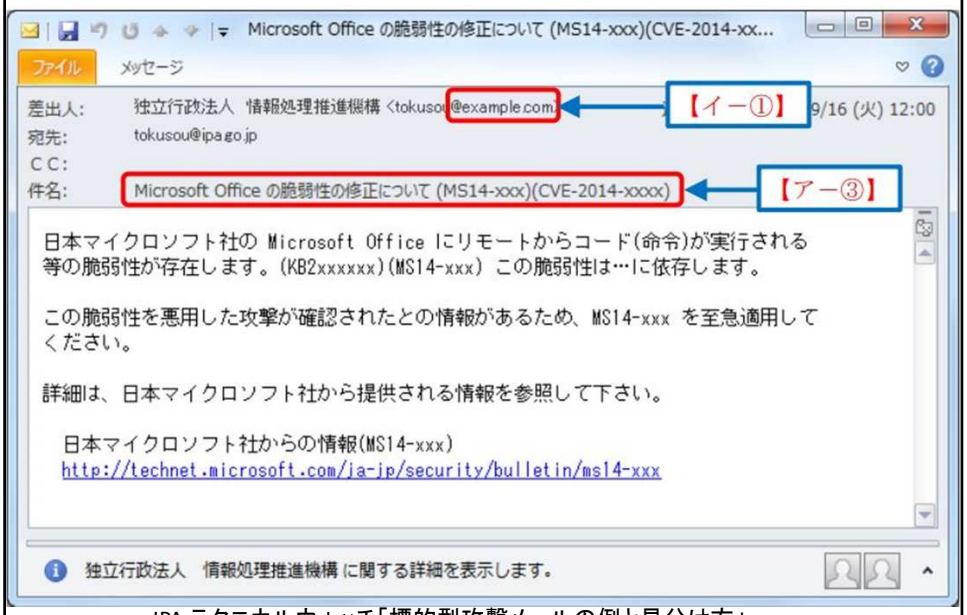
標的型攻撃メールによる侵入！

23件のうち、15件が

No.	発覚/公表日	被害組織	発覚原因	侵入経路	情報流出被害
1	1月9日	商社	外部からの指摘	標的型メール	400 件の個人情報
2	1月16日	新聞社	不審通信調査	不明	電子メール、社内文書などが流出
3	6月1日	年金事業	外部からの指摘	標的型メール	101 万件の個人情報
4	6月9日	業界団体	外部からの指摘	標的型メール	2 万 7 千件の個人情報
5	6月10日	商工会議所	外部からの指摘	標的型メール	1 万 2139 件の個人情報
6	6月13日	医療保険事業	外部からの指摘	不明	不明
7	6月16日	地方自治体	外部からの指摘	標的型メール	不明
8	6月16日	海外協力事業	外部からの指摘	標的型メール	不明
9	6月17日	医療保険事業	外部からの指摘	不明	個人情報（規模不明）
10	6月17日	施設管理事業	外部からの指摘	標的型メール	不明
11	6月17日	公共施設	外部からの指摘	標的型メール	不明
12	6月17日	海外協力事業	不明	標的型メール	個人情報（規模不明）
13	6月19日	医療機関	外部からの指摘	標的型メール	250 件の個人情報
14	6月19日	宿泊施設	外部からの指摘	標的型メール	個人情報（規模不明）
15	6月19日	医療機関	外部からの指摘	標的型メール	不明
16	6月22日	教育機関	外部からの指摘	標的型メール	3308 件の個人情報
17	6月25日	官公庁	外部からの指摘	不明	不明
18	7月10日	官公庁	外部からの指摘	水飲み場型	不明
19	7月16日	教育機関	内部異常調査	標的型メール	3 万 6300 件の個人情報
20	7月17日	政府機関	不審通信調査	不明	不明
21	7月20日	地方自治体	外部からの指摘	水飲み場型	2700 件の個人情報
22	8月7日	研究開発法人	不明	水飲み場型	215 件の個人情報
23	8月28日	交通機関	外部からの指摘	標的型メール	不明

TrendLabs 2015年 年間セキュリティラウンドアップより

標的型攻撃メールの例



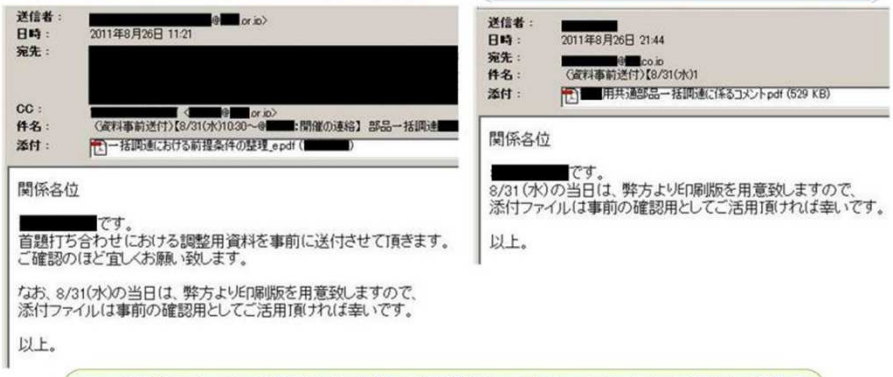
IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」

標的型メール攻撃事例

～社団法人に所属するＡ氏になりすました標的型メール～

社団法人のＡ氏が甲社職員等に送付した実際のメール

社団法人のＡ氏になりすまし乙社職員等に送付された標的型メール



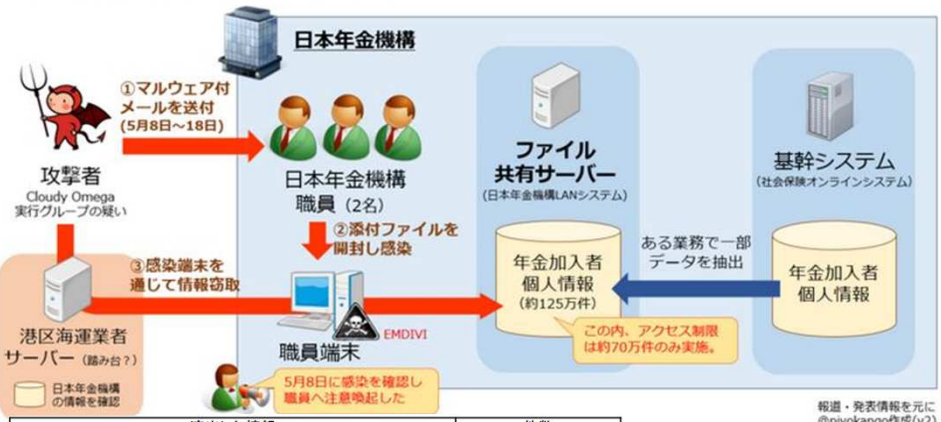
- 実際のメールが送付された約10時間後に、同メールの本文をほとんどそのまま引用した標的型メールが送付
- 社団法人のA氏が実際のメールを送付した際に、参考送付していた同社団法人のB氏のPCがのっとられ、メールの情報が窃取されていた模様

警察庁のHPより　https://www.npa.go.jp/keibi/biki7/231014shiryou.pdf

日本年金機構の情報漏えい事件（2015年5月）

標的型攻撃メールに端を発した情報漏えい事件！

日本年金機構 情報漏えいの概要イメージ



流出した情報	件数
二情報（基礎年金番号、氏名）	約3．1万件
三情報（基礎年金番号、氏名、生年月日）	約116．7万件
四情報（基礎年金番号、氏名、生年月日、住所）	約5．2万件
合計	約125．0万件

JTBの情報漏えい事件 （2016年3月19日～24日）

標的型攻撃メールに端を発した情報漏えい事件！

発端：取引先を装ったメールの添付ファイルを開いたこと
（➔JTBの子会社iJTBのパソコンがウイルスに感染）

実在する取引先企業（ANA）のメールアドレスになりすまし、
航空券の偽装PDFファイルをメールで送りつける巧妙なもの

流出の可能性：約793万人分の個人情報
【含まれていた個人情報】
①氏名(漢字、カタカナ、ローマ字)
②性別
③生年月日
④メールアドレス
⑤住所
⑥郵便番号
⑦電話番号
⑧パスポート番号
⑨パスポート取得日

（2）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

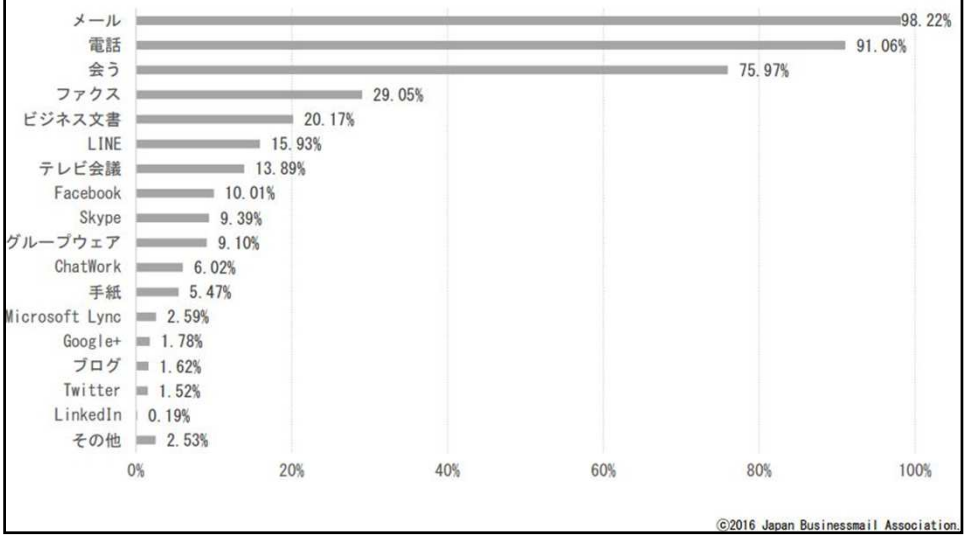
1984年　JUNET実験開始（東芝も研究所が参加）

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＞

（3）標的型メール攻撃対策の現状とその課題

人的対策と技術的対策

標的型メール攻撃対策

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

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、メール受信者へ注意喚起あるいは破棄等により、標的型攻撃メールの被害回避を目指した対策

人的対策の現状・課題
不正侵入防止効果は限定的！

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！
（組織としての開封率＝$1-0.95^{100}$＝0.994079470779666）

人的対策の現状・課題
見えない費用負担は膨大！

98%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、55通のメール受信（1日平均）
「ビジネスメール実態調査 2016」

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、55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・・・

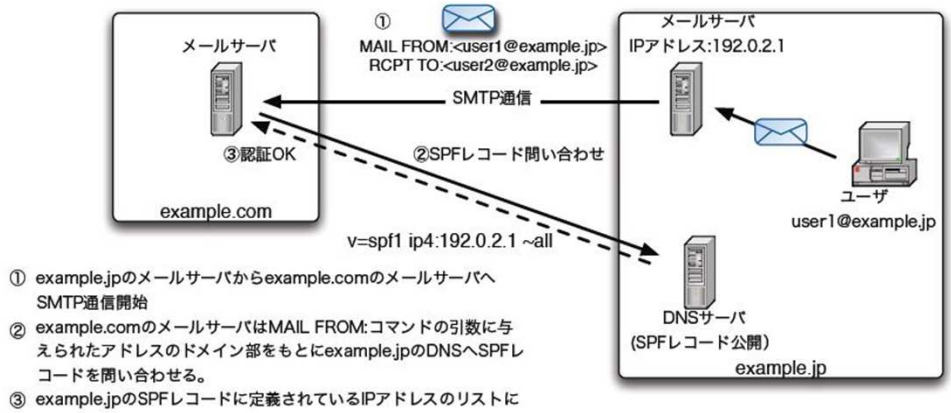
➔ 年間270億～540億の費用負担に相当

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、もっと技術的対策に注力すべき！

現在の技術的対策
SPF（Sender Policy Framework）

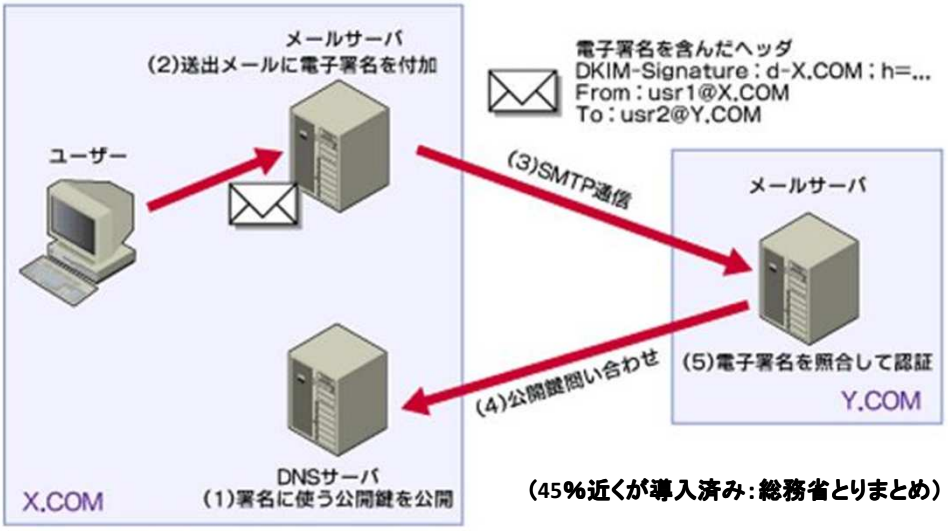


① example.jpのメールサーバからexample.comのメールサーバへSMTP通信開始
② example.comのメールサーバはMAIL FROM:コマンドの引数に与えられたアドレスのドメイン部をもとにexample.jpのDNSへSPFレコードを問い合わせる。
③ example.jpのSPFレコードに定義されているIPアドレスのリストに送信側のメールサーバが含まれていれば認証成功

（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
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

標的型攻撃メールの多くは送信元メールアドレスの詐称！

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）

しかし、メールサーバが（不正に）利用された場合は、検出不可！

メールサーバが不正利用される危険性！

＊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）

∴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！

（4）暗号メール標準S/MIMEの可能性と課題

提供機能・実現方式とその普及上の課題

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」

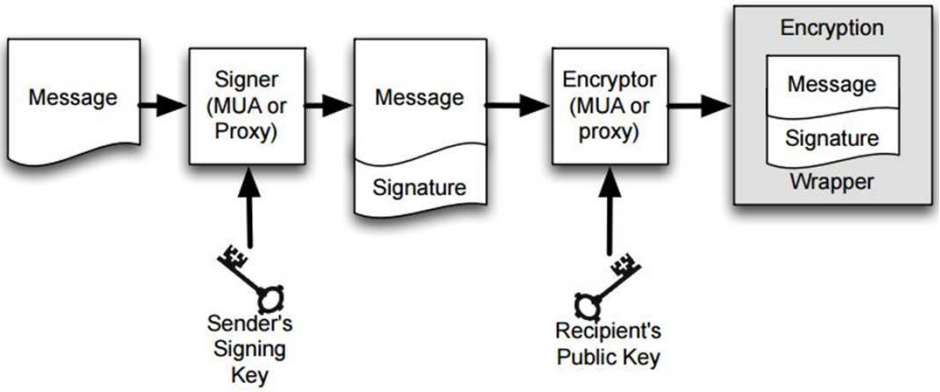
（平成25年3月　総務省情報通信国際戦略局通信規格課）でも、

“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。

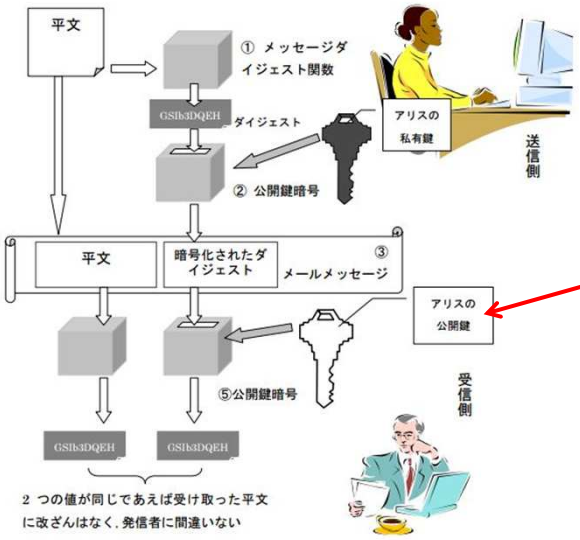
しかし、現実にはほとんど使用されていない！

S/MIME
暗号化と署名付与の方式



SECOND DRAFT NIST Special Publication 800-177“Trustworthy Email”より

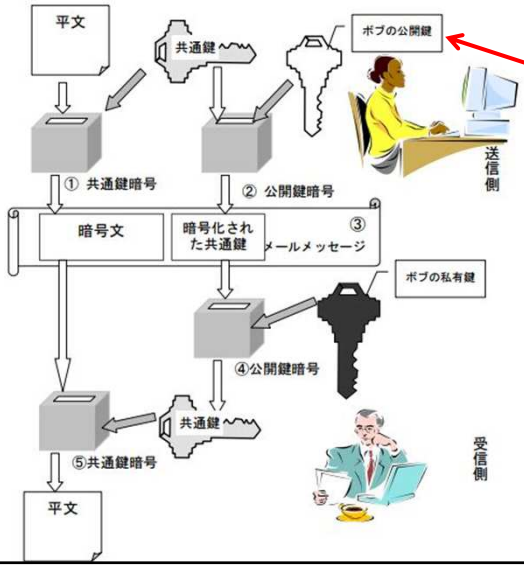
S/MIMEによる署名付与
非改竄性検証および送信者認証



送信者（アリス）の公開鍵が必要

「電子メールのセキュリティ S/MIMEを利用した暗号化と電子署名」（IPA）より

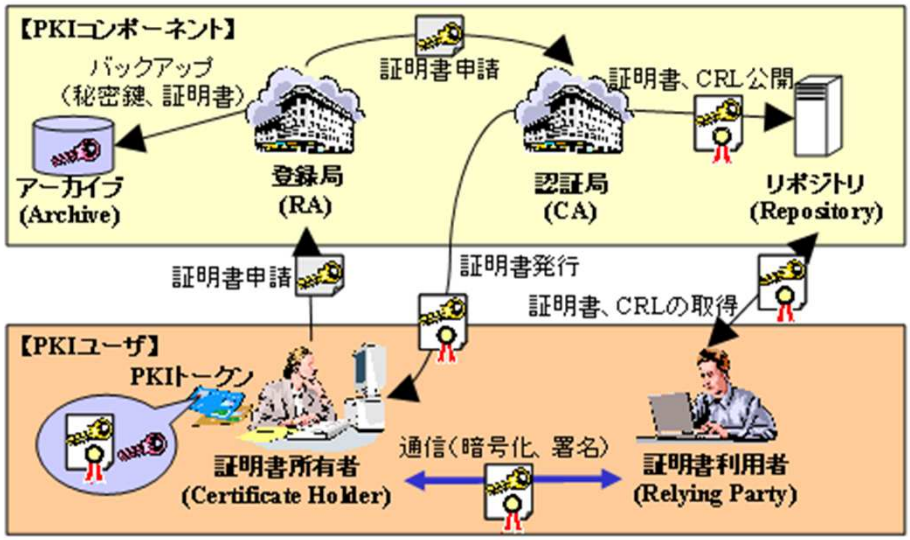
S/MIMEによる暗号化
通信情報の秘匿



受信者（ボブ）の公開鍵が必要

「電子メールのセキュリティ S/MIMEを利用した暗号化と電子署名」（IPA）より

PKI
公開鍵の真正性を確認できる枠組



S/MIME普及の課題

(1)メールアドレスごとに公開鍵との対応を示す証明書
（メールアドレス証明書）が必要であり費用負担（年間数千円）が発生

(2)通信相手のメールアドレス証明書の入手・管理・更新が必要（暗号化）
有効期限（1年～3年）ごとの更新

(3)被害を受ける受信側自らのS/MIME導入努力・投資だけでは効果無し
送信側が署名付与しないと「送信者認証」が不可能
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）
暗号化ファイルのコンテンツ検査が困難

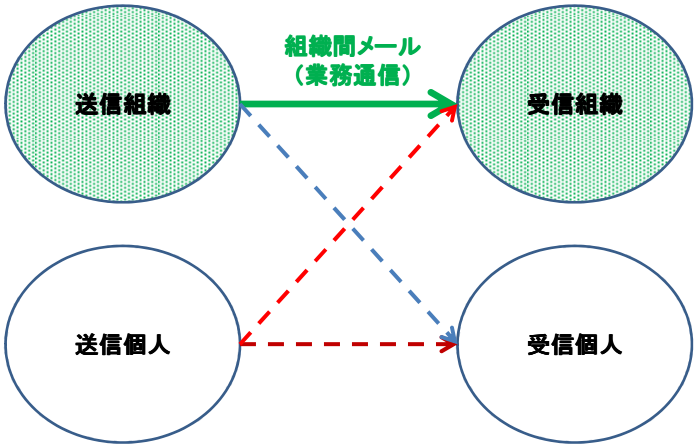
(5)ウイルス等のマルウェアの流入を防げない（暗号化）
暗号化ファイルのセキュリティ検査が困難

(6)暗号化機密情報転送時の不必要な復号により漏洩リスクが増大（暗号化）
暗号化ファイルの暗号化状態での転送が困難

（5）組織通信向けS/MIMEの可能性

提供機能・特徴、
S/MIMEの課題の克服方策

まずは組織通信向けに S/MIMEに準じた仕組みを！



Divide and Conquer!

なぜ、組織通信向け、なのか

★そもそも、標的型メール攻撃の標的は、企業、官公庁（組織）！

★標的型メール攻撃の標的は、非公開（業務通信用）メールアドレス！
業務通信用の非公開メールアドレスに対する攻撃
平成26年年間の全体の7割
平成27年上期は全体の9割
（「サイバー空間をめぐる脅威の情勢について」警察庁の広報資料より）

★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）

➔ 組織通信が、標的型メール攻撃の標的になっている現状

➔ S/MIMEの思想に準じつつも、その課題を克服したシステムにより、
組織通信を対象とした標的型攻撃メールを排除できないか！

➔ 組織通信向けと限定すれば、S/MIMEの普及課題の克服も可能では？

組織通信向けに限定した場合のS/MIME普及課題の克服策

(1)メールアドレス証明書が必要であり費用負担が発生
　　年間数千円 ➔ 所属する組織が発行(個人負担なし、組織の負担も軽微)

(2)メールアドレス証明書および鍵の更新・管理が必要
　　通信相手それぞれのメールアドレス証明書 ➔ 組織の公開鍵証明書
　　自分自身の秘密鍵の安全な管理 ➔ 社員・職員カードの利用

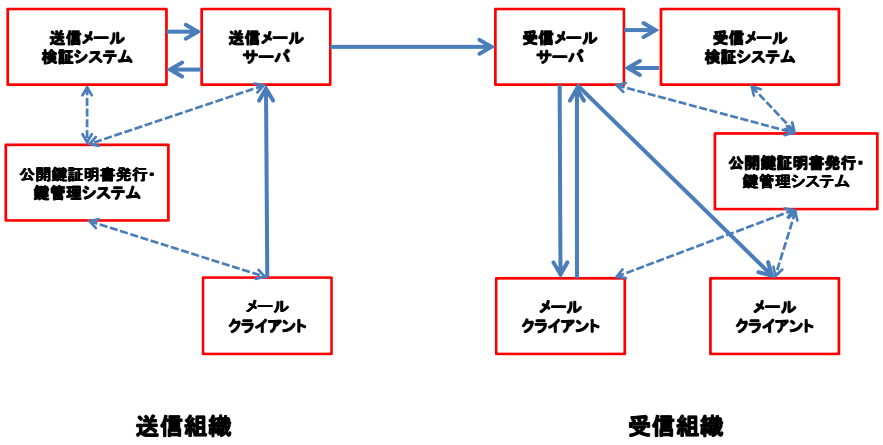
(3)自らの導入努力・投資だけでは効果無し
　　社会基盤として普及させることが必要 ➔ 検討中

(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 ➔ 安全な環境で復号し検査

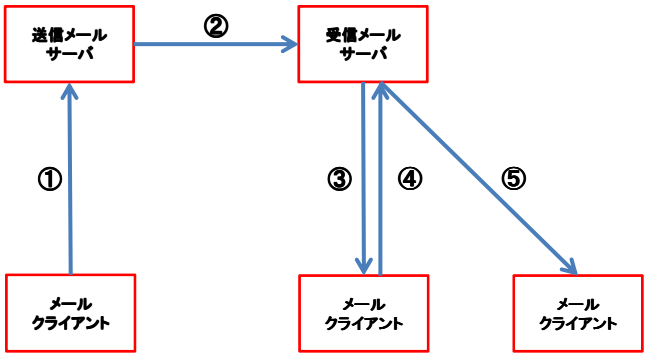
(5)ウイルス等のマルウェアの流入を防げない
　　暗号化ファイルのセキュリティ検査が困難 ➔ 安全な環境で復号し検査

(6)暗号化機密情報転送時の不必要な復号により漏洩リスクが増大
　　暗号化ファイルの暗号化状態での転送が困難 ➔ 組織暗号による暗号化

組織通信向けS/MIME構成

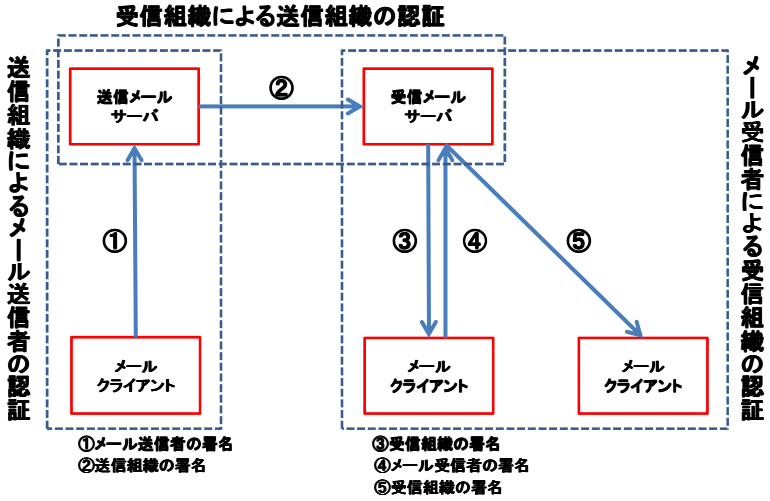


メールに付与される署名の変遷



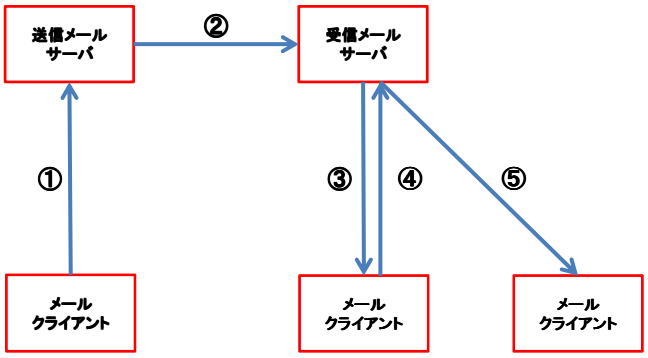
①メール送信者の署名
②送信組織の署名
③受信組織の署名
④メール受信者の署名
⑤受信組織の署名

署名による認証の連鎖



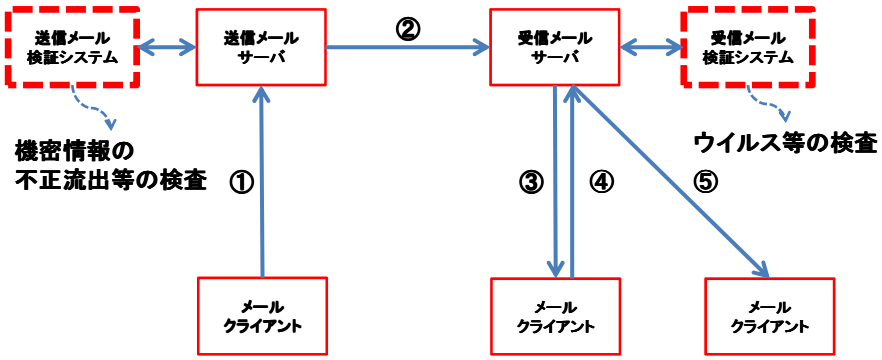
➔㋐メール受信者は、メール送信者の特定・追跡性を確認可能
➔㋑メールアドレス証明書の費用負担削減(1)
（組織内ではプライベートメールアドレス証明書の利用）

暗号化に使用される公開鍵の変遷



①送信組織の公開鍵
②受信組織の公開鍵
③メール受信者の公開鍵
④受信組織の公開鍵
⑤新たなメール受信者の公開鍵

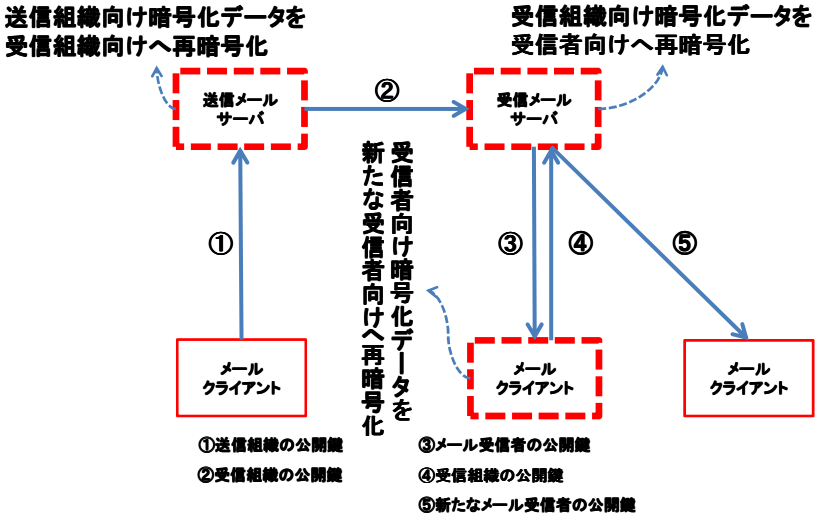
組織暗号による再暗号化の連鎖（1）



①送信組織の公開鍵
②受信組織の公開鍵
③メール受信者の公開鍵
④受信組織の公開鍵
⑤新たなメール受信者の公開鍵

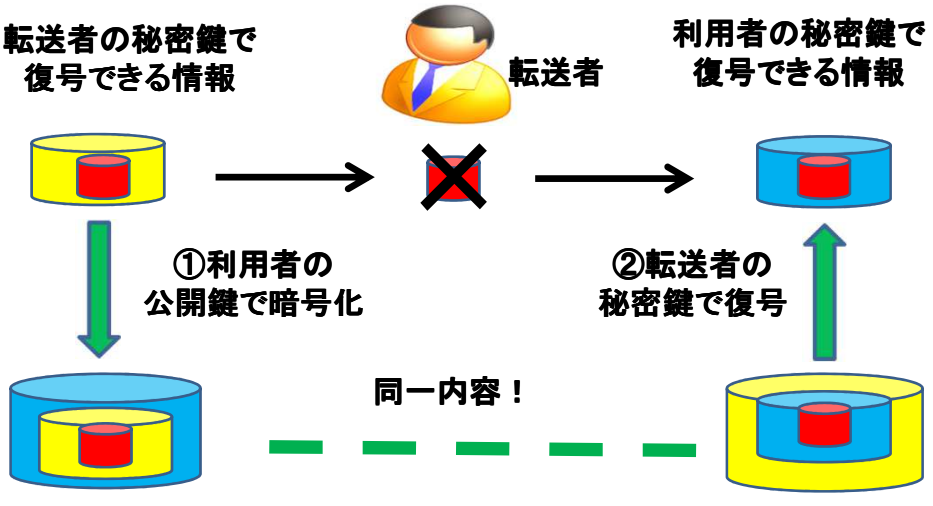
➔㋐メール受信者の公開鍵の管理が不要(2)
➔㋑送信組織の機密情報漏洩等の検査が可能(4)
➔㋒受信組織のウイルスチェック等の検査が可能(5)

組織暗号による再暗号化の連鎖（2）

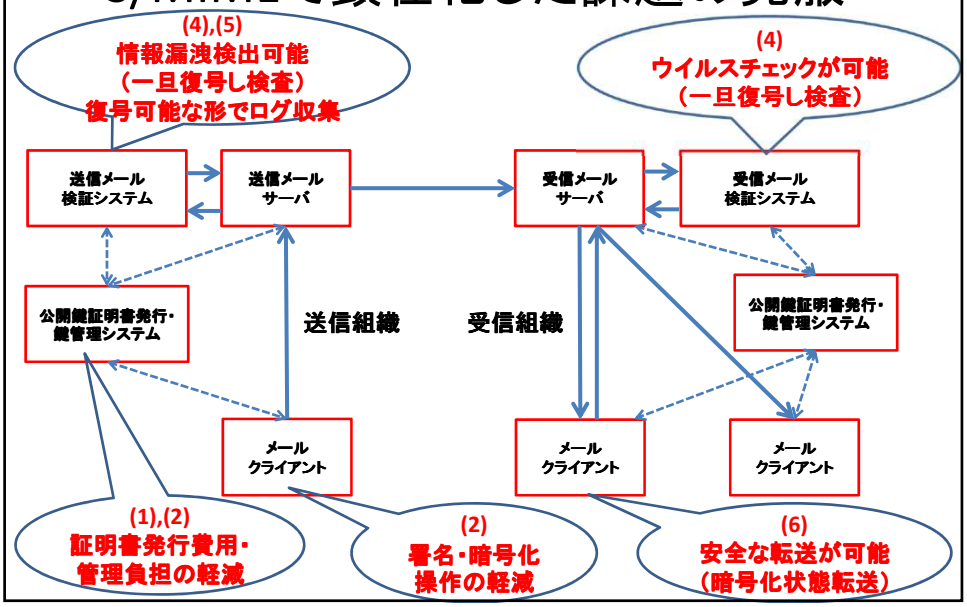


➔㋐新たなメール受信者の公開鍵の管理が不要(2)
➔㋑転送時の機密情報の安全性向上(6)

組織暗号では、なぜ安全に転送が可能なのか？



組織通信向けS/MIME構成による S/MIMEで顕在化した課題の克服



組織通信向けS/MIME

課題(3)社会基盤として普及させるためには

政府主導の対応が不可欠！

（1）我が国の次世代電子メール利用基盤として開発推進

（2）社会実装の目標・スケジュールを策定し推進

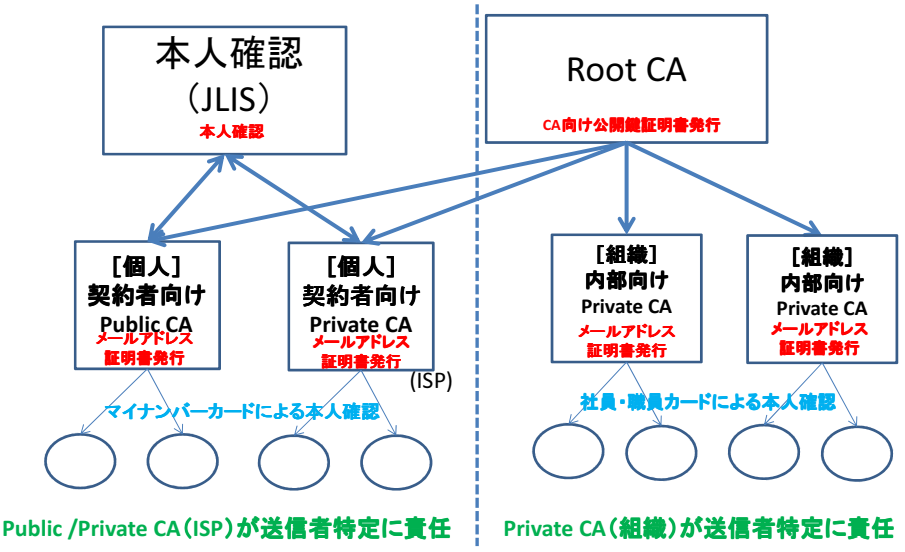
（3）府省庁が率先し導入・活用推進

（4）産業界の導入に対する支援（税制等）

安心・安全な次世代電子メール利用基盤

SSMAX（Safe and Secure MAil eXchange infrastructure)

個人を含めたメール送信者特定のための公開鍵証明書発行方式



まとめ

（1）電子メールは今後も
　　基本的・共通的なコミュニケーション基盤
（2）標的型攻撃の侵入を防ぐ入り口対策の重要性
　　標的型メール攻撃対策もっと重視すべき
（3）現状の標的型メール攻撃対策は非効率的で効果も限定的
（4）「組織通信向けS/MIME」構想の提案
　　送信者の認証・追跡性の重視
　　犯罪抑止力
　　通信情報の秘匿性の重視
　　組織活動へ安心して利用できる安全なメール
（5）我が国の高度情報化社会の更なる発展には
　　「安心・安全な電子メール利用基盤」の整備が必要
（6）具現化のための活動が必要
　　社会のコンセンサス醸成と政府への政策提言

（ご参考）MELTupフォーラム（2016年6月6日）実施報告

ＩｏＴ環境におけるサイバーセキュリティ

―重要インフラ・組織に対する標的型サイバー攻撃に備えて―


ＩｏＴ環境におけるサイバーセキュリティ
―重要インフラ・組織に対する標的型サイバー攻撃に備えて―

参加者数：145名

アンケート結果：（回答数：104）

98%が、標的型メール攻撃を
身近な問題/社会問題と認識

87%が、組織通信型S/MIMEが
標的型メール攻撃に有効と認識
（56%が普及が課題と認識）

66%が、標的型メール攻撃対策の
研究開発・社会実装を検討する
フォーラムへ参加希望

終

ご清聴、ありがとうございました。