JPAAWG 2026 / LIGHTNING TALK

遠隔解析議論から再考する S/MIME の暗号化メカニズム

メールの本文・鍵・署名は、どう包まれているのか

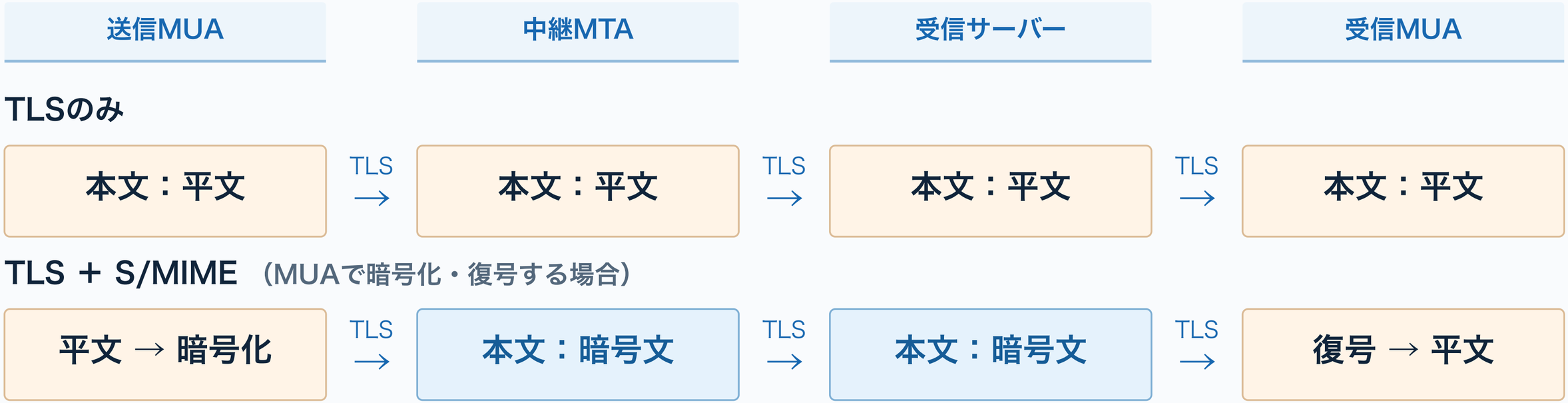
> **端末の「遠隔解析」：導入提言から、改正法案の委員会付託へ**
>
> 警察庁「匿名・流動型犯罪グループによる犯罪被害対策のための技術的措置に関する有識者検討会」が2026年9月に提言。
>
> 10月16日：警察官職務執行法の改正案を閣議決定・国会提出。
>
> 10月30日：衆議院内閣委員会へ付託。

出典：検討会提言（本文p.6） ／ 10月16日 国家公安委員会委員長会見 ／ 国会提出法案 ／ 審議経過（2026年11月4日確認）

01 / PROTECTION BOUNDARY

メールは、どこで平文になる？

TLSは接続ごと。S/MIMEはMIMEデータ自体を保護する。



サーバー内の保存時暗号化は別の保護。図はメール処理時の本文の状態を示す。

保護の境界は 暗号化する場所から、復号する場所まで。端末の平文は別。

RFC 3207 §6 ／ RFC 8551 §3.3　※ 配送・アクセス経路は簡略化。

本文は一度暗号化し、鍵を受信者ごとに包む

CEK = Content-Encryption Key（本文用の共通鍵）　|　例：RSA鍵配送

① メッセージごとに ランダムなCEK を生成

MIMEデータ　＋ CEK →　**共通の暗号文**

② 同じCEKを、それぞれの受信者の公開鍵で暗号化

Aの公開鍵 →	Bの公開鍵 →
暗号化CEK A	**暗号化CEK B**
RecipientInfo A	RecipientInfo B

受信者：自分の秘密鍵でCEKを回復 → 本文を復号

ASN.1の骨格（抜粋・省略あり）

```
EnvelopedData ::= SEQUENCE {
  version CMSVersion,
  ...
  recipientInfos
    RecipientInfos,
  encryptedContentInfo
    EncryptedContentInfo,
  ...
}
RecipientInfos ::=
  SET SIZE (1..MAX) OF RecipientInfo
```

同じ暗号文 ＋ 宛先ごとの鍵情報 を、ひとつのCMSオブジェクトに。

鍵共有方式では、共有秘密から鍵暗号化鍵を導出してCEKを包む。
認証付き暗号にはAuthEnvelopedDataを使う。

RFC 5652 §§6–6.2 ／ RFC 8551 §2.4.4　※ 同一内容・同一暗号方式で複数宛先に送る例。

03 / SIGN THEN ENCRYPT

署名したMIMEデータを、暗号化で包む

内側の署名は内容を検証し、外側の暗号化は署名情報も隠す。

外側：暗号化コンテナ

```
application/pkcs7-mime;
smime-type=enveloped-data
```

↓ 復号すると現れる構造

```
multipart/signed;
protocol="application/pkcs7-signature"
```

本文・添付	分離署名
MIME entity	application/pkcs7-signature

構造の概略。boundary・micalg等は省略。

① 署名対象は、暗号化前の内容

復号したMIMEデータと署名を検証する。
暗号文への署名とは意味が違う。

② 署名の情報も暗号文の内側

署名値や、署名に含めた証明書を
配送経路上に露出させない。

図は分離署名の例。
署名対象をSignedData内に含める形式もある。

ヘッダーのFromなどは別の層。署名情報の秘匿 ≠ 送信者の匿名化

RFC 8551 §3.7：S/MIME 4.0の仕様 ／ RFC 9787 §5.2：2025年公開の実装指針（Informational）
参考：RFC 8551の改訂作業も進行中（draft-ietf-lamps-rfc8551bis-00、2026年7月、未確定）。

04 / LIMITS & OPERATIONS

構造を見れば、保護の限界も分かる

本文を暗号化できても、メタデータ・長期鍵・鍵の入手は別に考える。

01

外側の情報

HEADER / ENVELOPE

本文だけを保護する構成では、外側のSubject等は平文。

ヘッダ保護はRFC 9788で拡張。SMTPの配送先情報まで秘匿するものではない。

02

長期鍵への依存

FORWARD SECRECY

長期の復号鍵が漏れると、その鍵で開ける過去メールも危険。

CEKを毎回変えても、通常の鍵配送・鍵共有では前方秘匿性は得られない。

03

受信者の証明書

KEY DISCOVERY

送信前に、相手の暗号化用証明書を入手・検証する必要。

署名付きメール、ディレクトリ、DNSSECを使うSMIMEA（RFC 8162・Experimental）など。

RFC 9788 ／ RFC 9787 Appendix A.10 ／ RFC 8551 §4.4 ／ RFC 8162

05 / TAKEAWAYS

S/MIMEを「包み方」で理解する

01 **本文の暗号文と、宛先ごとの鍵情報**

EnvelopedData / RecipientInfo が複数受信者への暗号化を支える。

02 **内容に署名し、その全体を暗号化**

MIMEの入れ子によって、署名対象と署名情報の見え方が決まる。

03 **メタデータの秘匿・長期秘密鍵の管理・端末の保護も必要**

ヘッダ保護、長期鍵の管理、証明書の取得、端末の保護も必要。

本文・鍵・署名が、どの境界の内側にあるか。