データ保護・誤送信防止の
メール技術とは？

アジェンダ

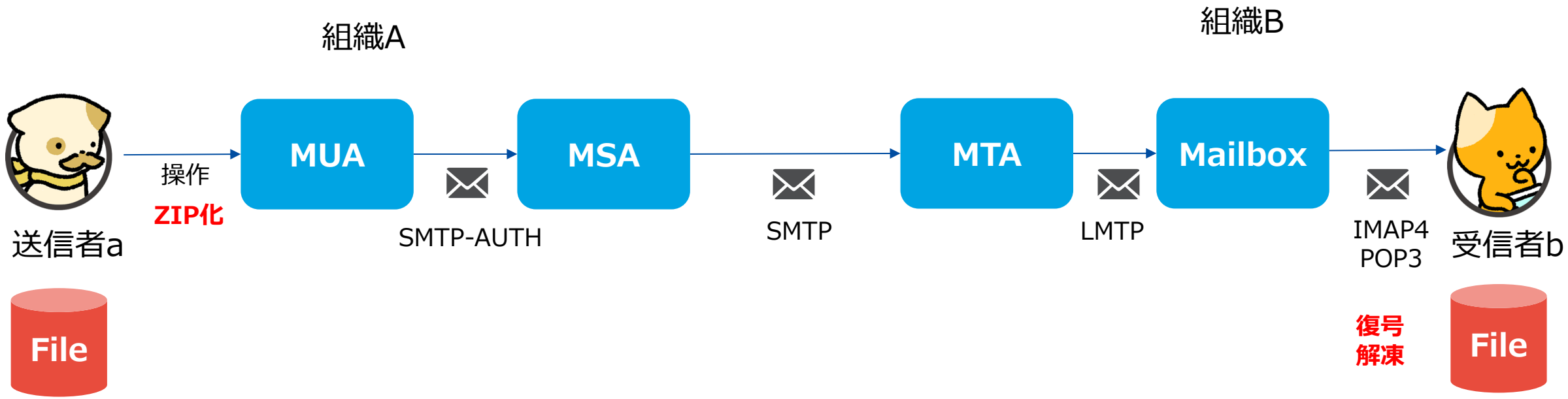
- セキュリティインシデントの 8 パターン
- それぞれのパターンを防御する 10 つの手段
- それぞれの防御方法の課題
- STARTTLS / MTA-STS / DANE
- モバイルでのデータ保護

インターネットイニシアティブ
櫻庭　秀次

ソフトバンク
北崎　恵凡

TwoFive
加瀬　正樹

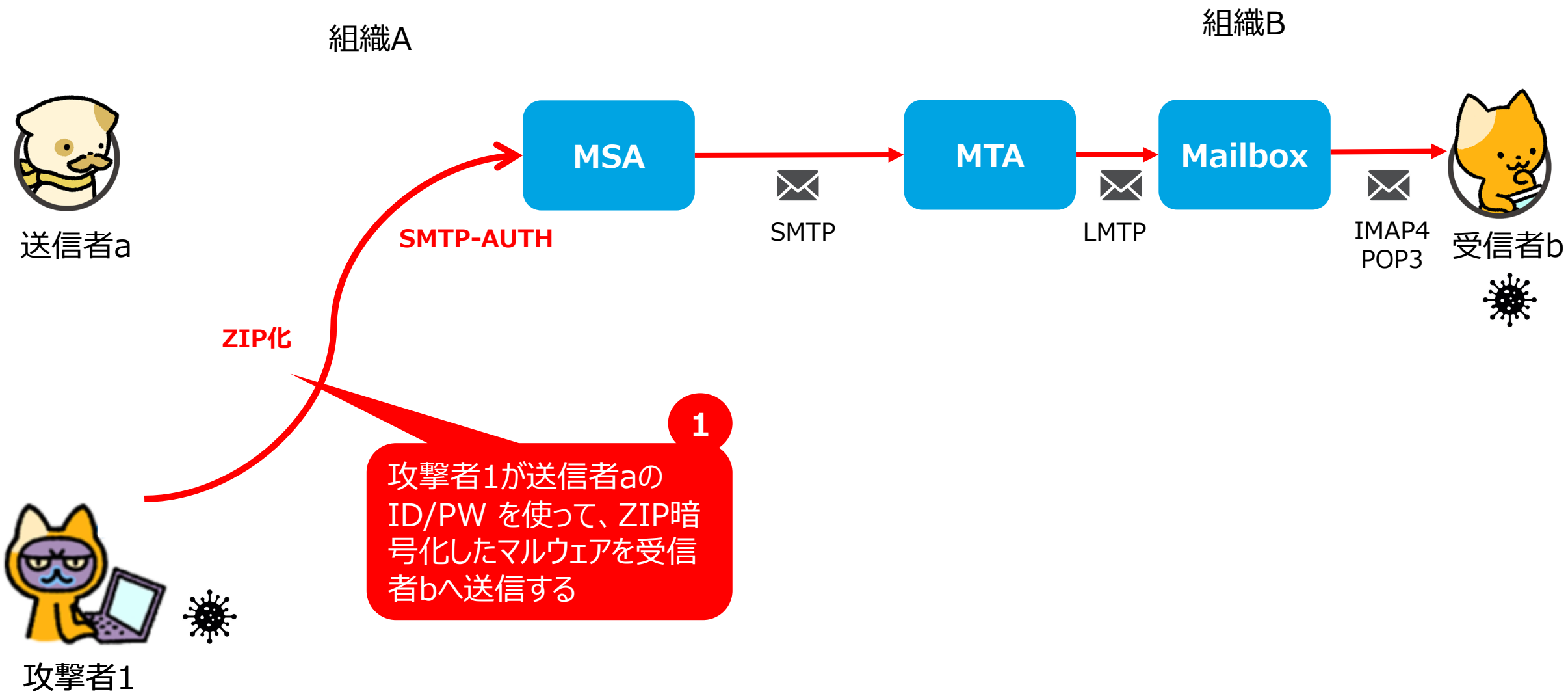
”暗号化 ZIP” 添付ファイルの流れ



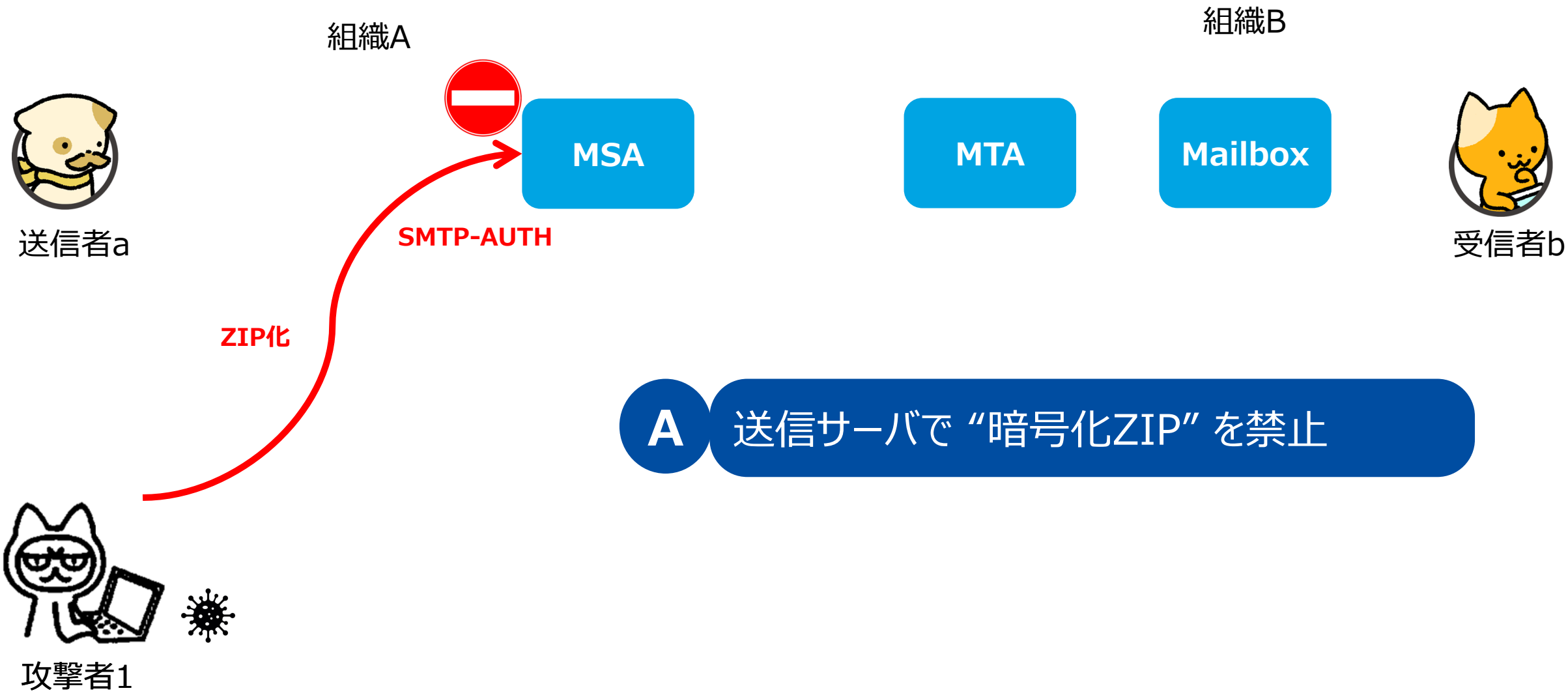
前提：

- 端末を盗んだり、不在の時に端末を悪用するなどはスコープ外とする
- メール送信時には必ず SMTP-AUTH を適用する
- ゲートウェイでアンチマルウェアを適用した場合に、ある程度有効に動作する
- 攻撃者は暗号化ZIPを開錠できる

1. 送信者(SMTP-AUTH)を乗っ取りマルウェア送信

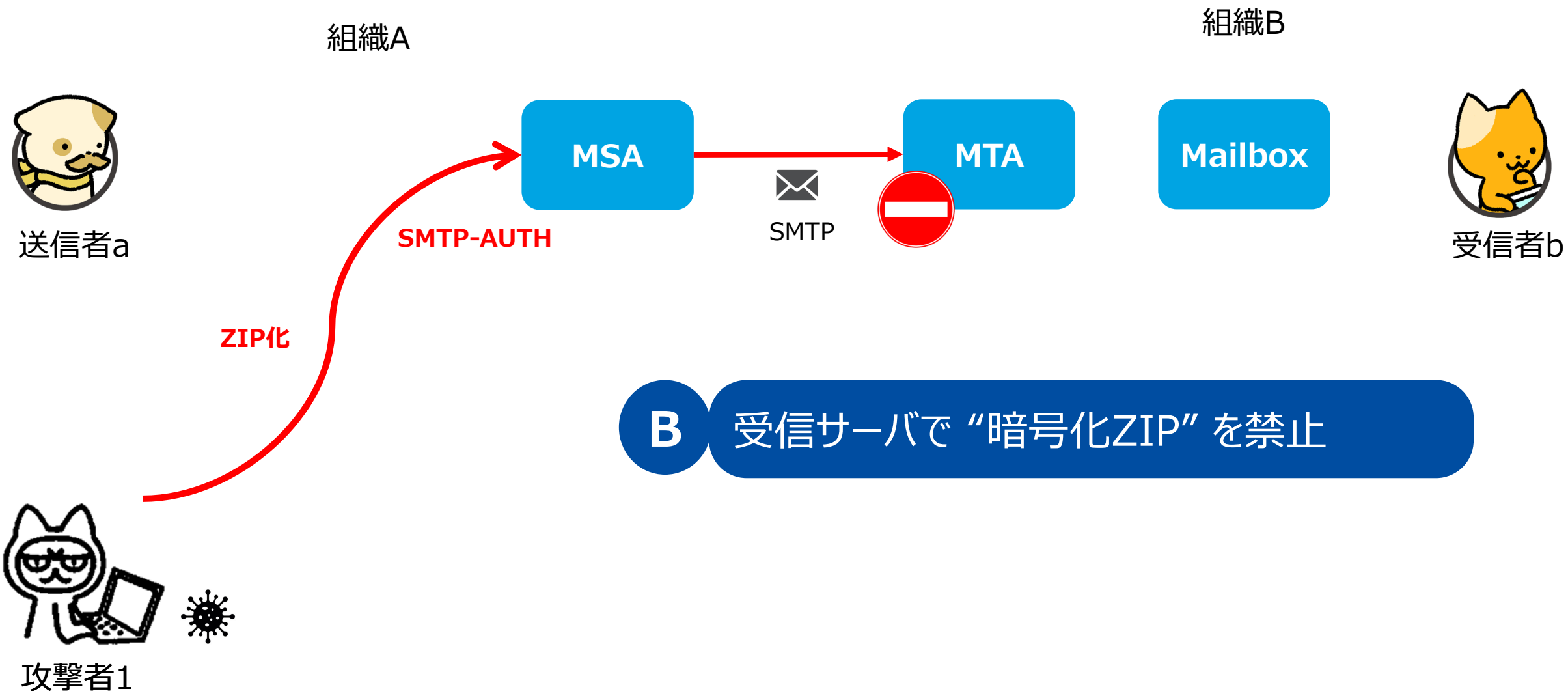


1. 送信者(SMTP-AUTH)を乗っ取りマルウェア送信



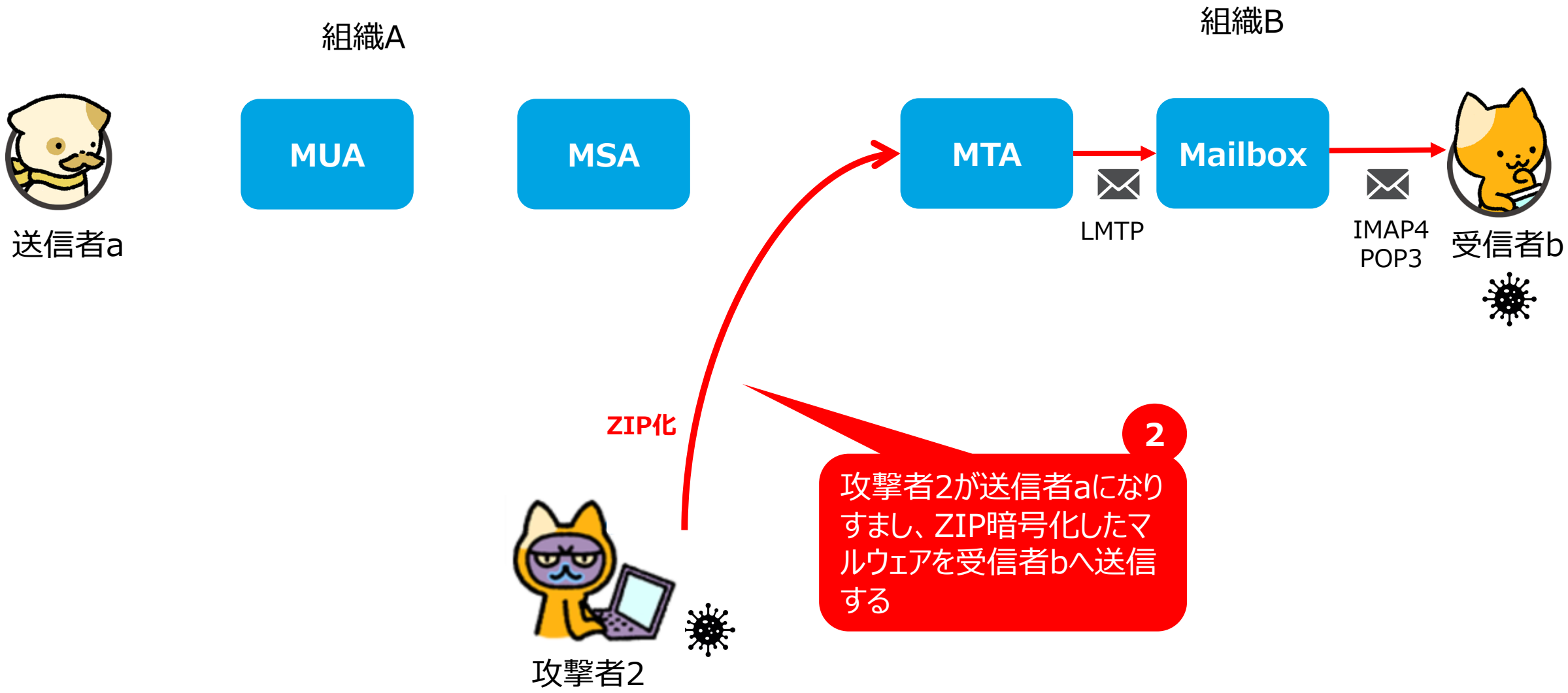
A 送信サーバで“暗号化ZIP”を禁止

1. 送信者(SMTP-AUTH)を乗っ取りマルウェア送信

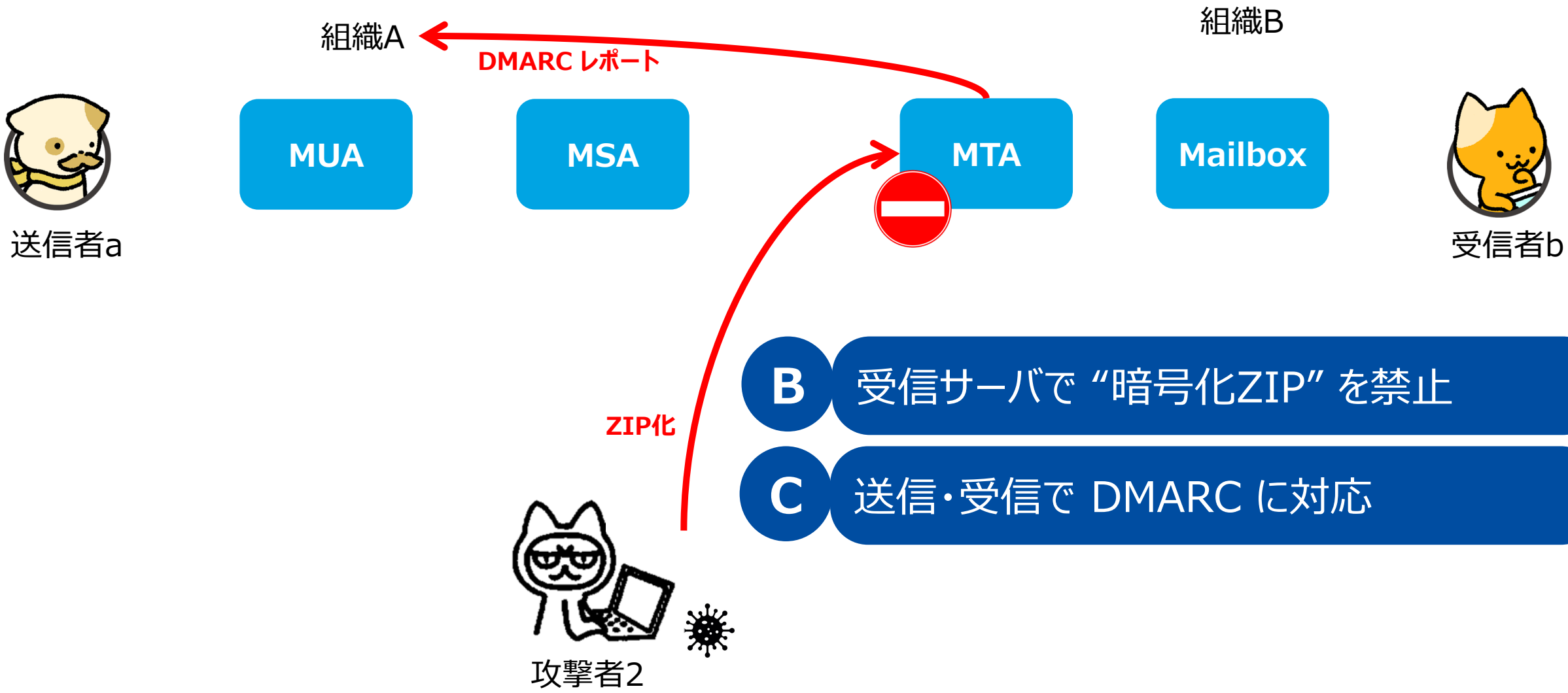


B 受信サーバで“暗号化ZIP”を禁止

2. 外部攻撃者のなりすましマルウェア送信

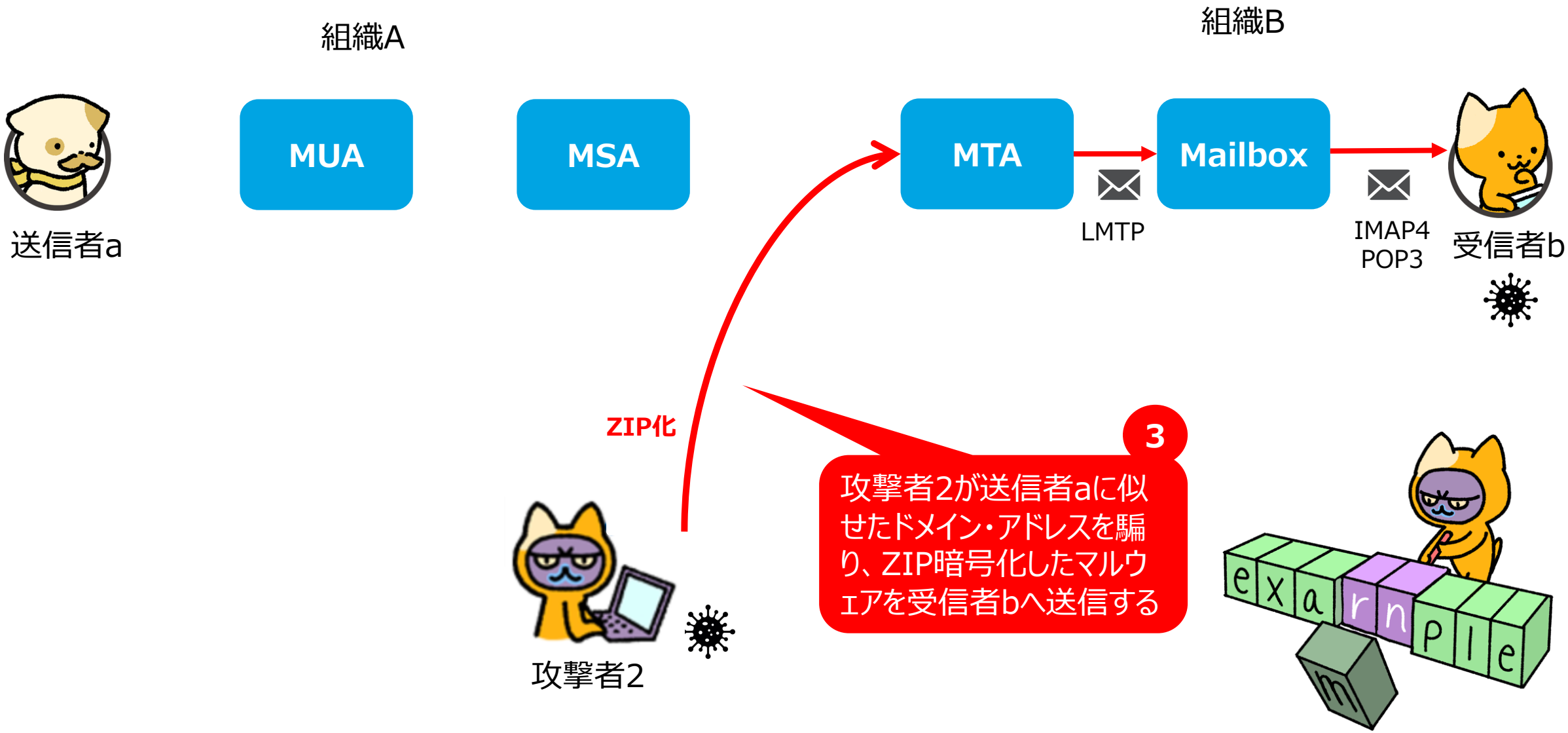


2. 外部攻撃者のなりすましマルウェア送信



- **B** 受信サーバで “暗号化ZIP” を禁止
- **C** 送信・受信で DMARC に対応

3. ホモグラフドメインからマルウェア送信



3. ホモグラフドメインからマルウェア送信

組織A

組織B

送信者a

MUA

MSA

MTA

Mailbox

受信者b

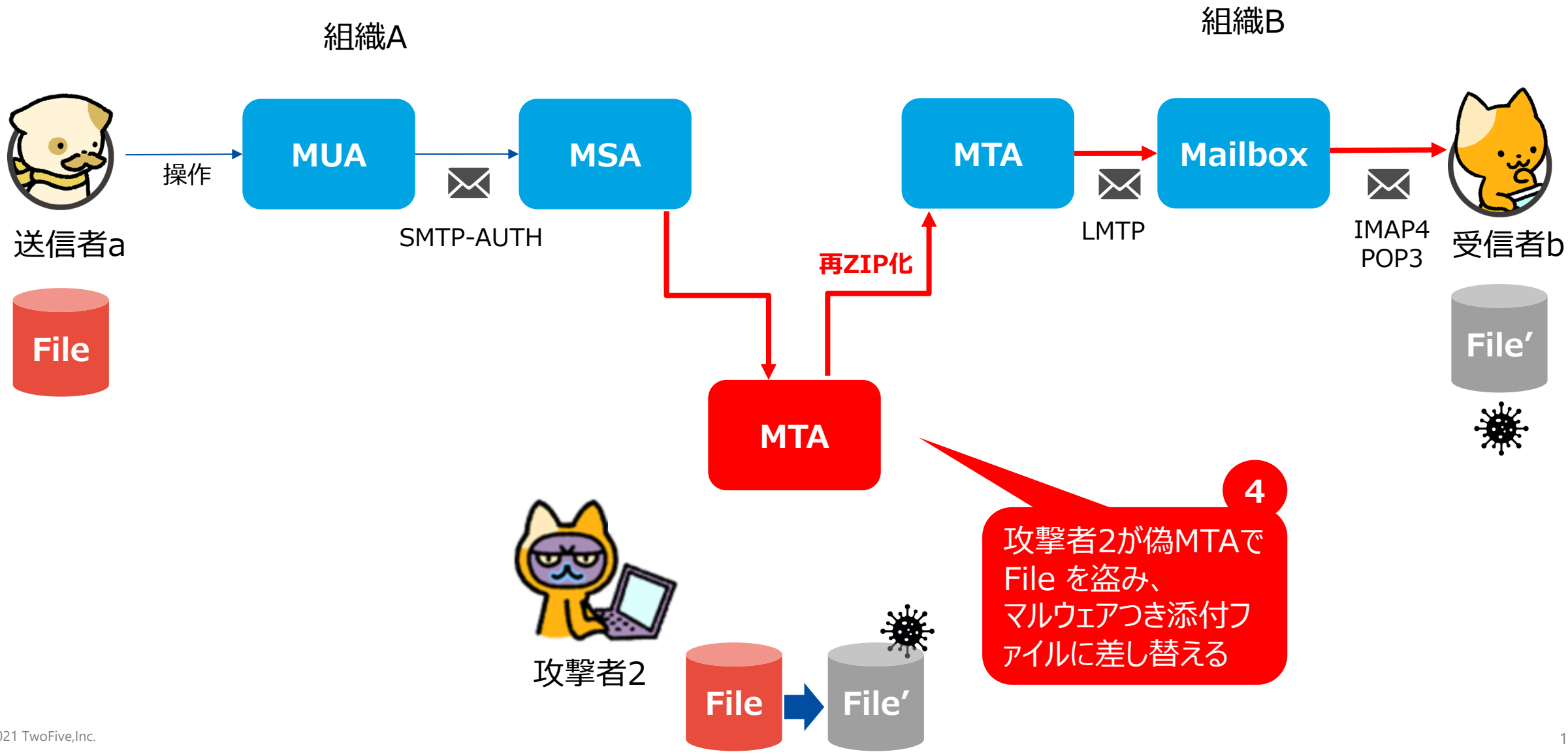
ZIP化

攻撃者2

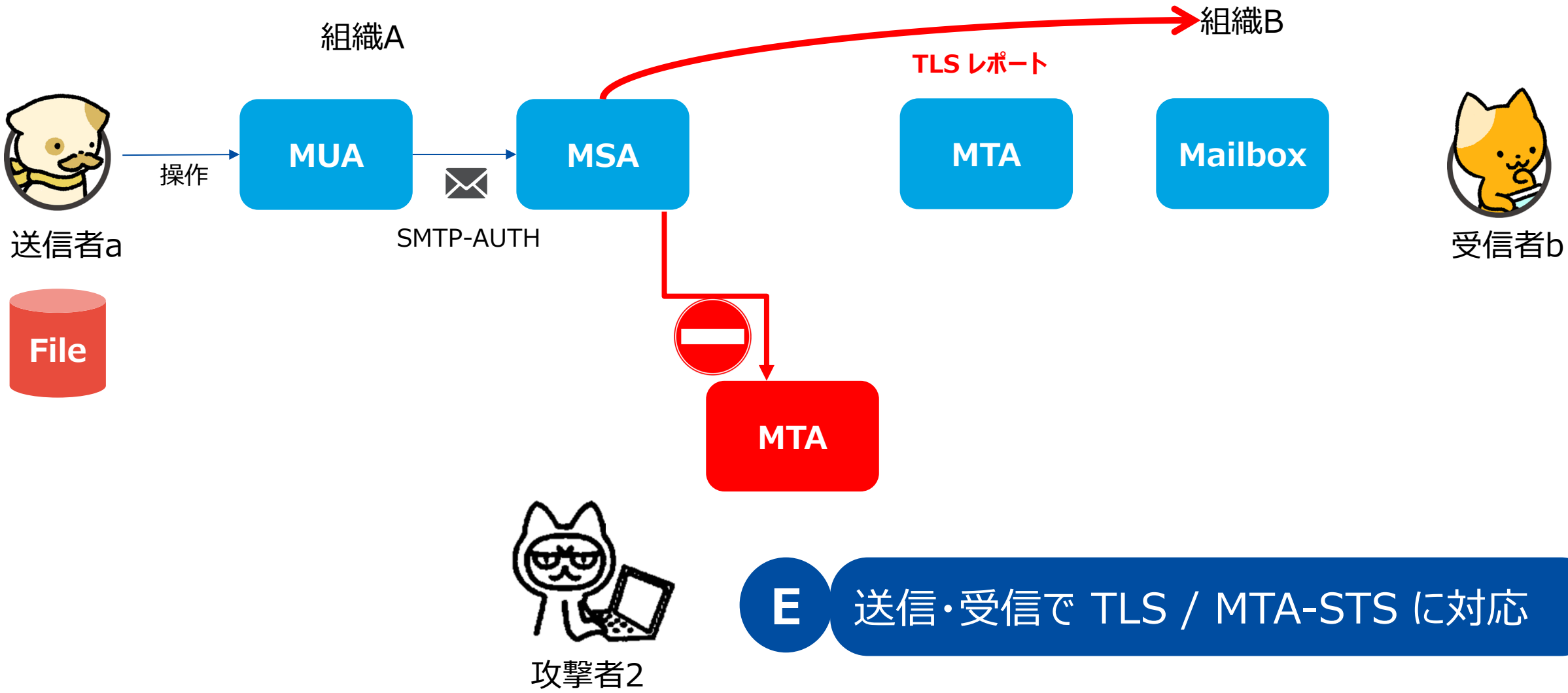
B 受信サーバで “暗号化ZIP” を禁止

D ドメインレピュテーション

4. 中間者攻撃によるデータ漏洩+データ改竄



4. 中間者攻撃によるデータ漏洩+データ改竄



E 送信・受信で TLS / MTA-STS に対応

4. 中間者攻撃によるデータ漏洩+データ改竄

送信者a

操作

MUA

SMTP-AUTH

MSA

組織A

DMARC レポート

組織B

MTA

Mailbox

受信者b

再ZIP化

File

MTA

B 受信サーバで “暗号化ZIP” を禁止

C 送信・受信で DMARC に対応

D ドメインレピュテーション

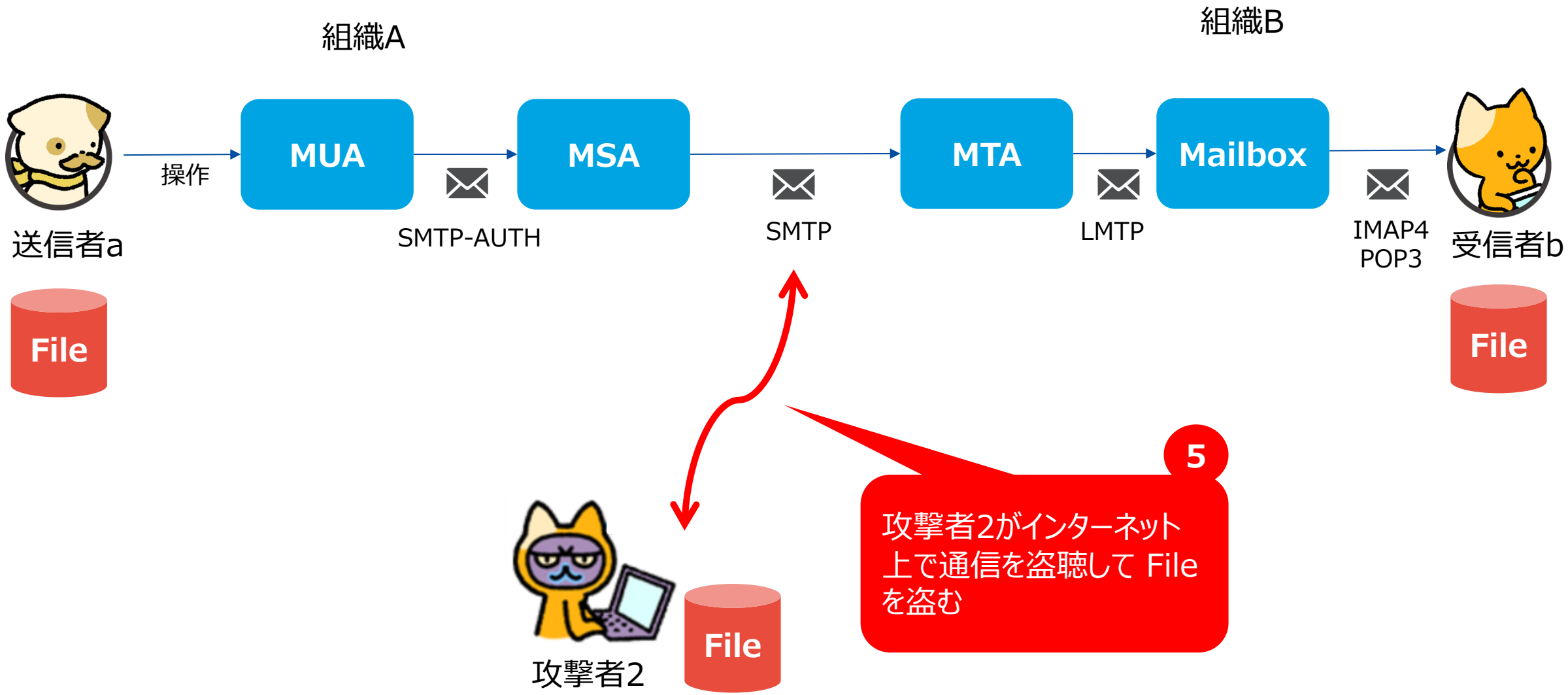
File
盗めたぞ

攻撃者2

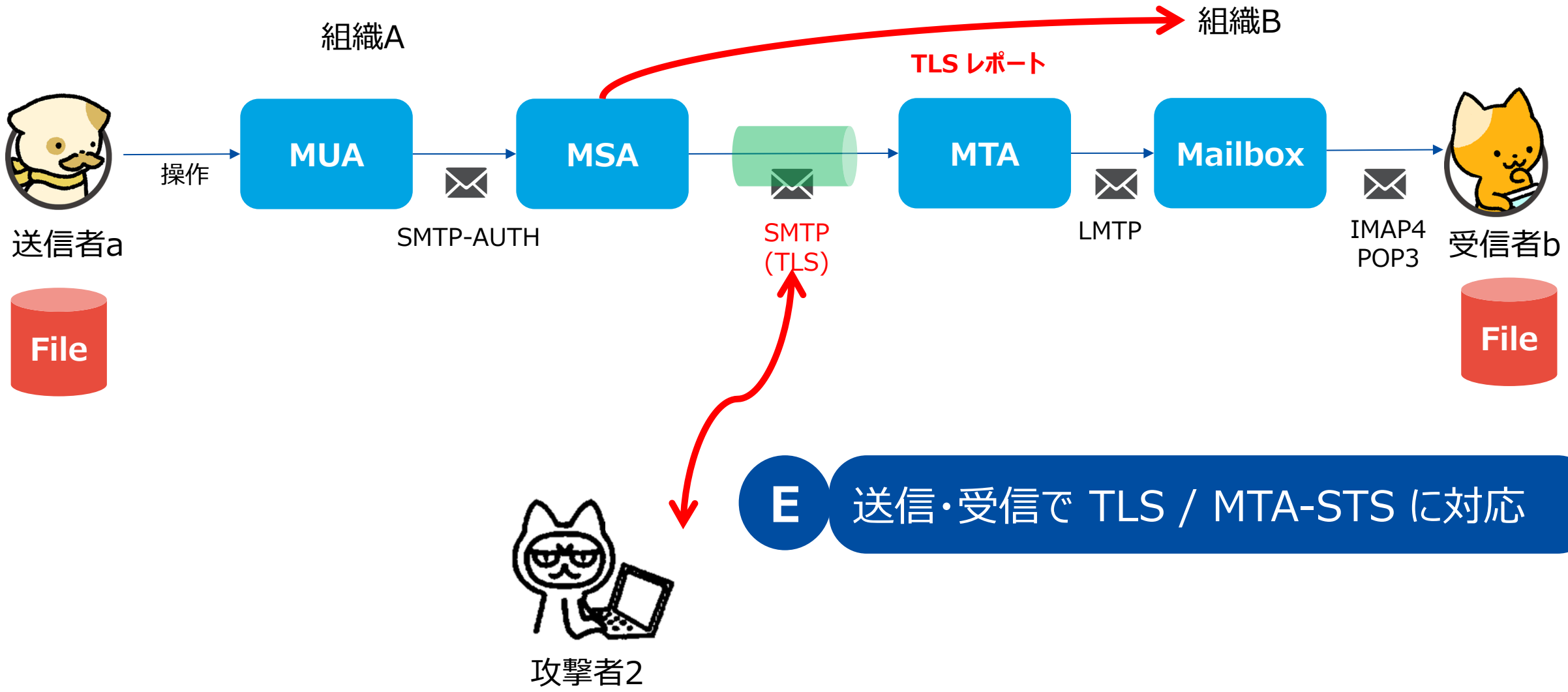
File

File’

5. 盗聴によるデータ漏洩

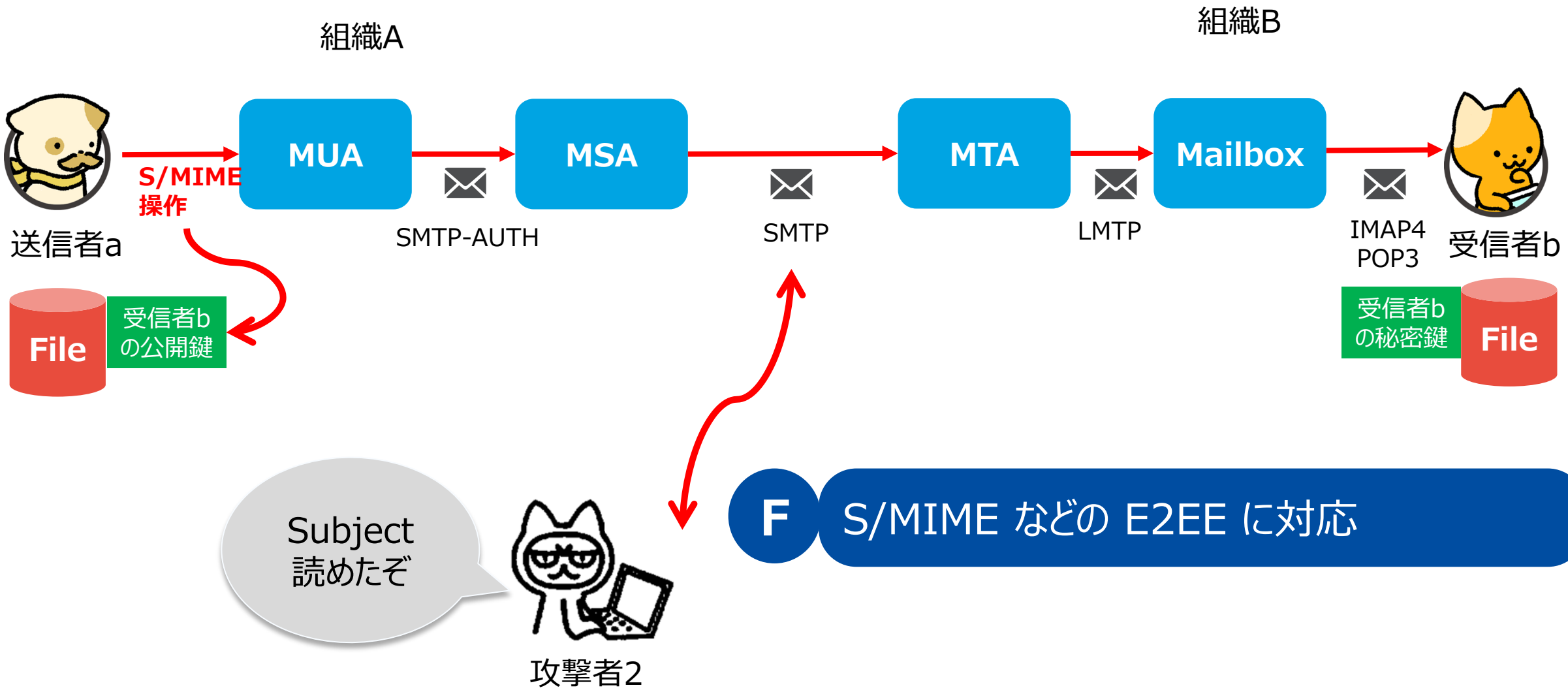


5. 盗聴によるデータ漏洩



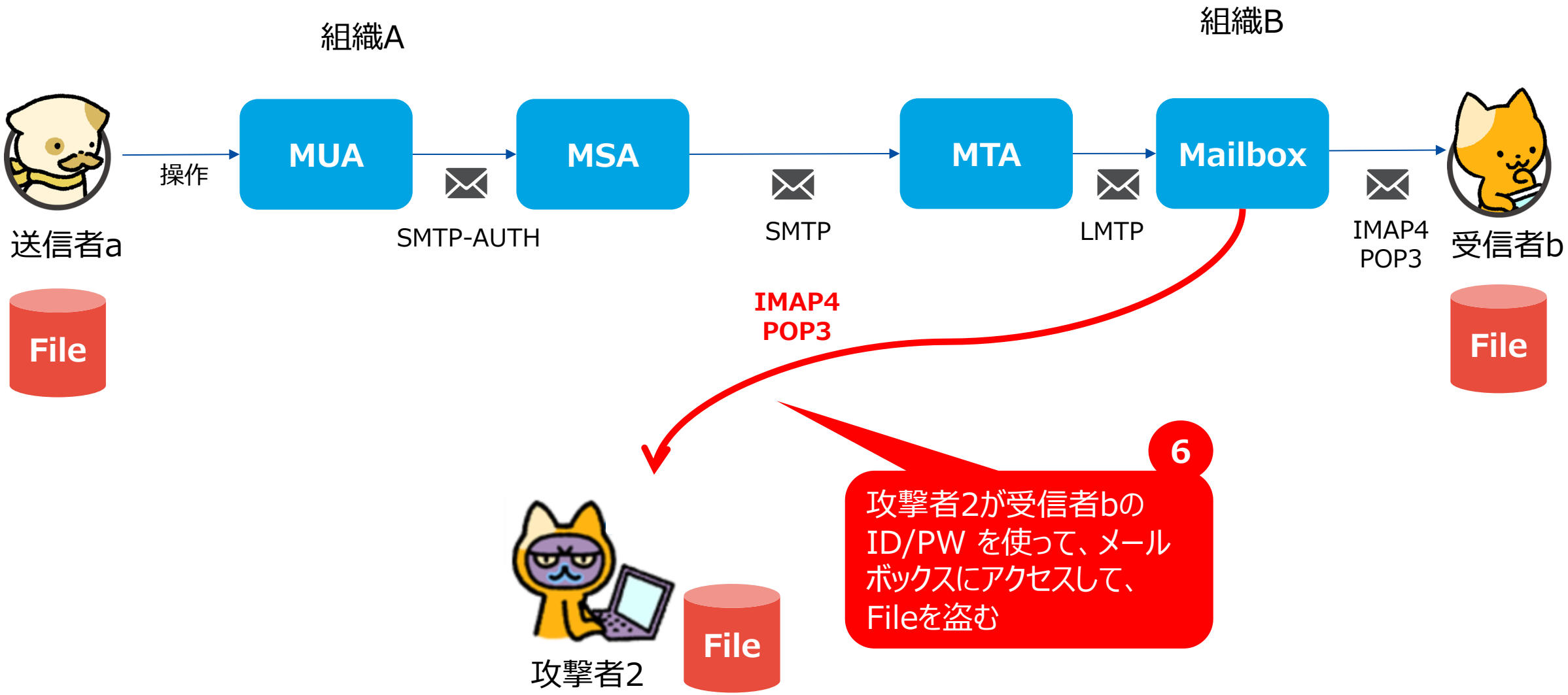
E 送信・受信で TLS / MTA-STS に対応

5. 盗聴によるデータ漏洩

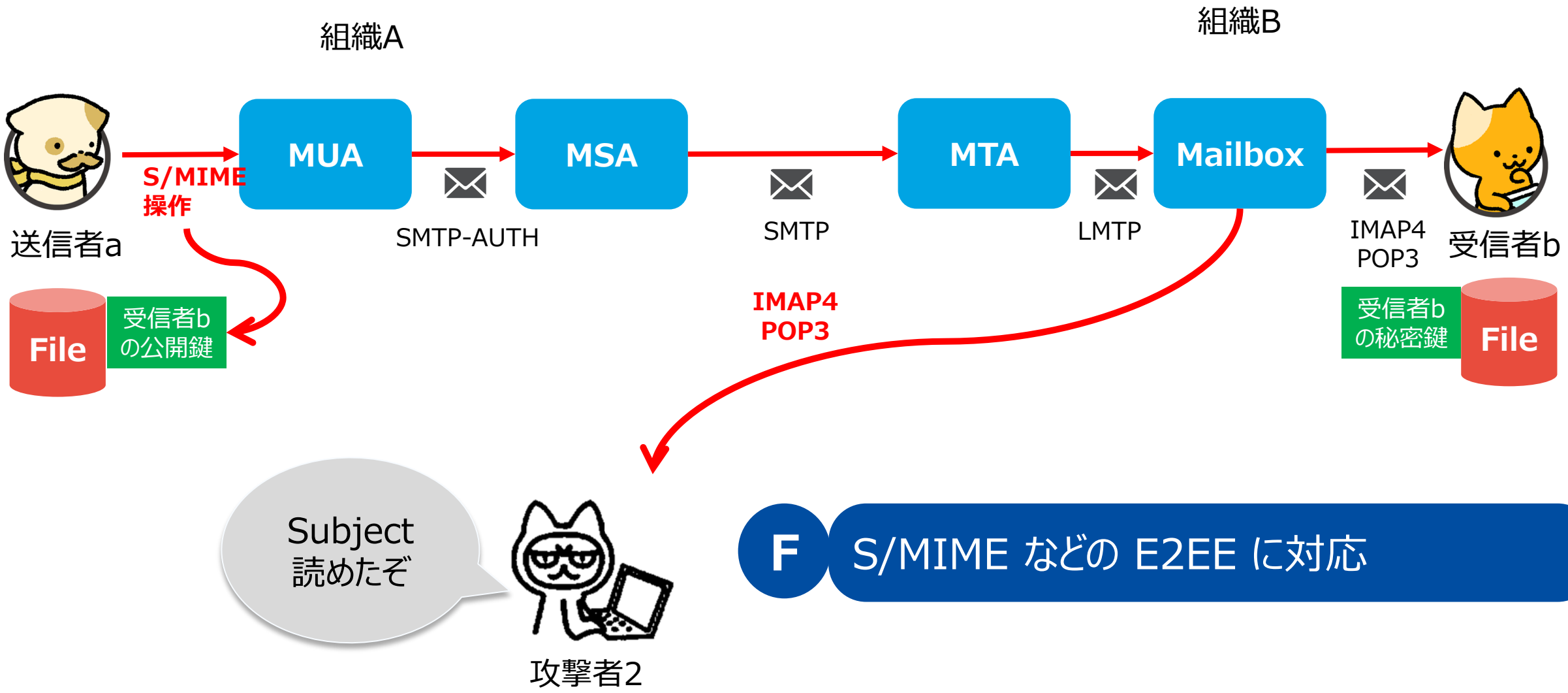


F S/MIME などの E2EE に対応

6. 受信者(IMAP4)を乗っ取りデータ漏洩

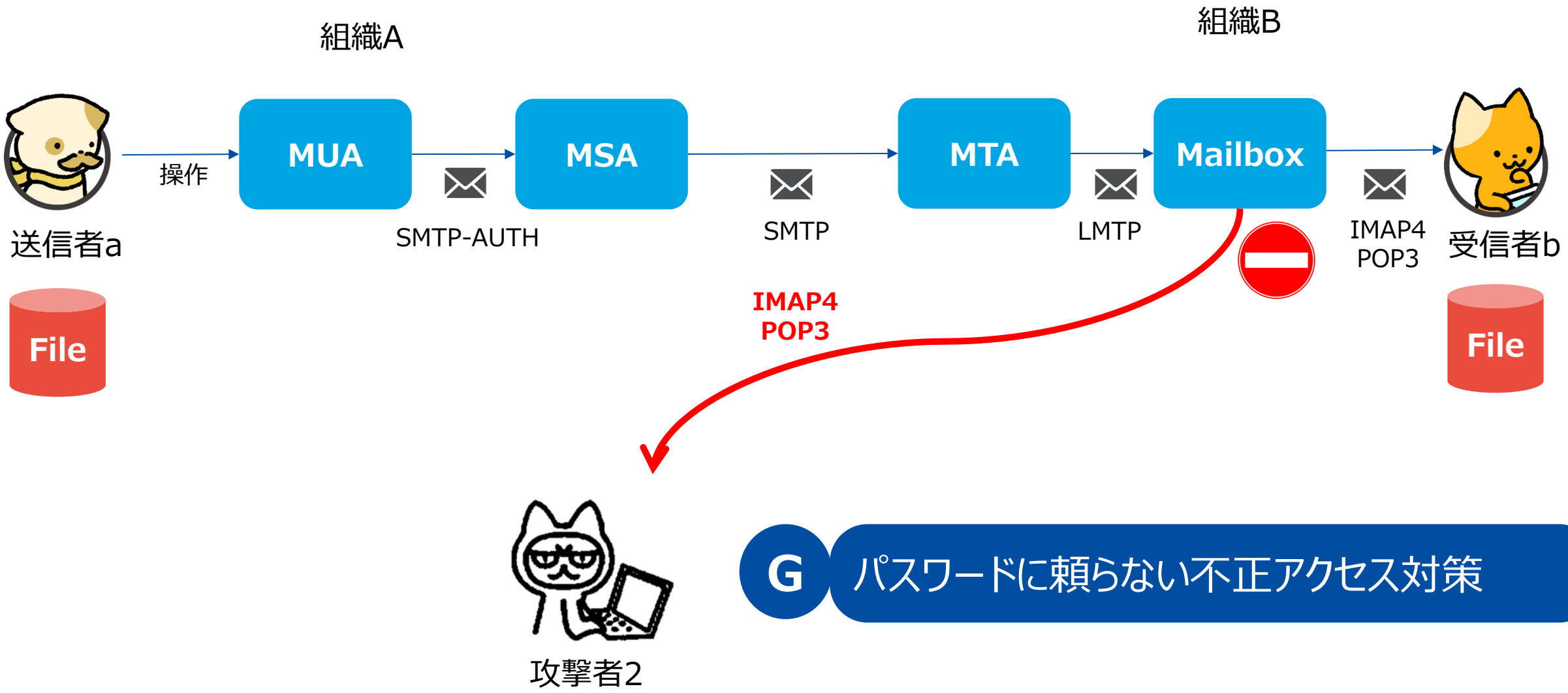


6. 受信者(IMAP4)を乗っ取りデータ漏洩



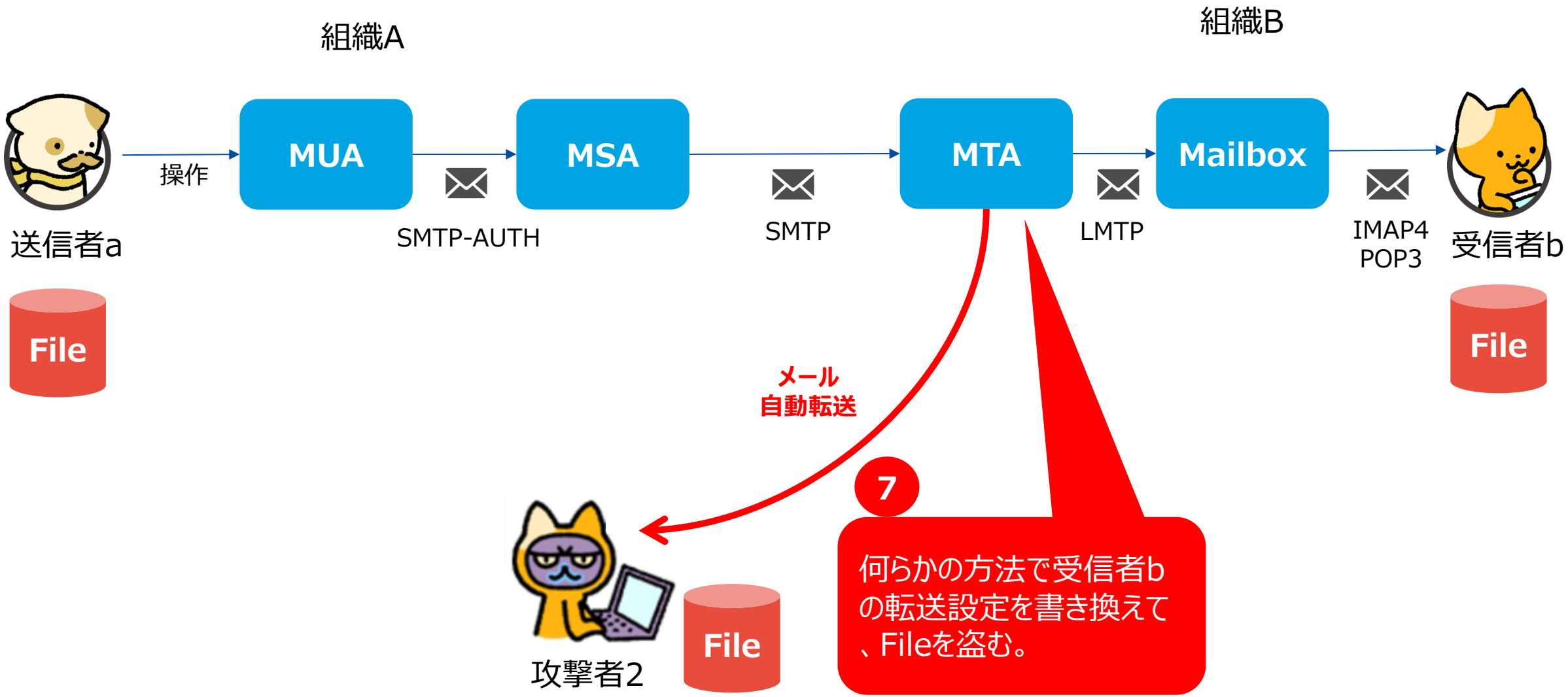
F S/MIME などの E2EE に対応

6. 受信者(IMAP4)を乗っ取りデータ漏洩

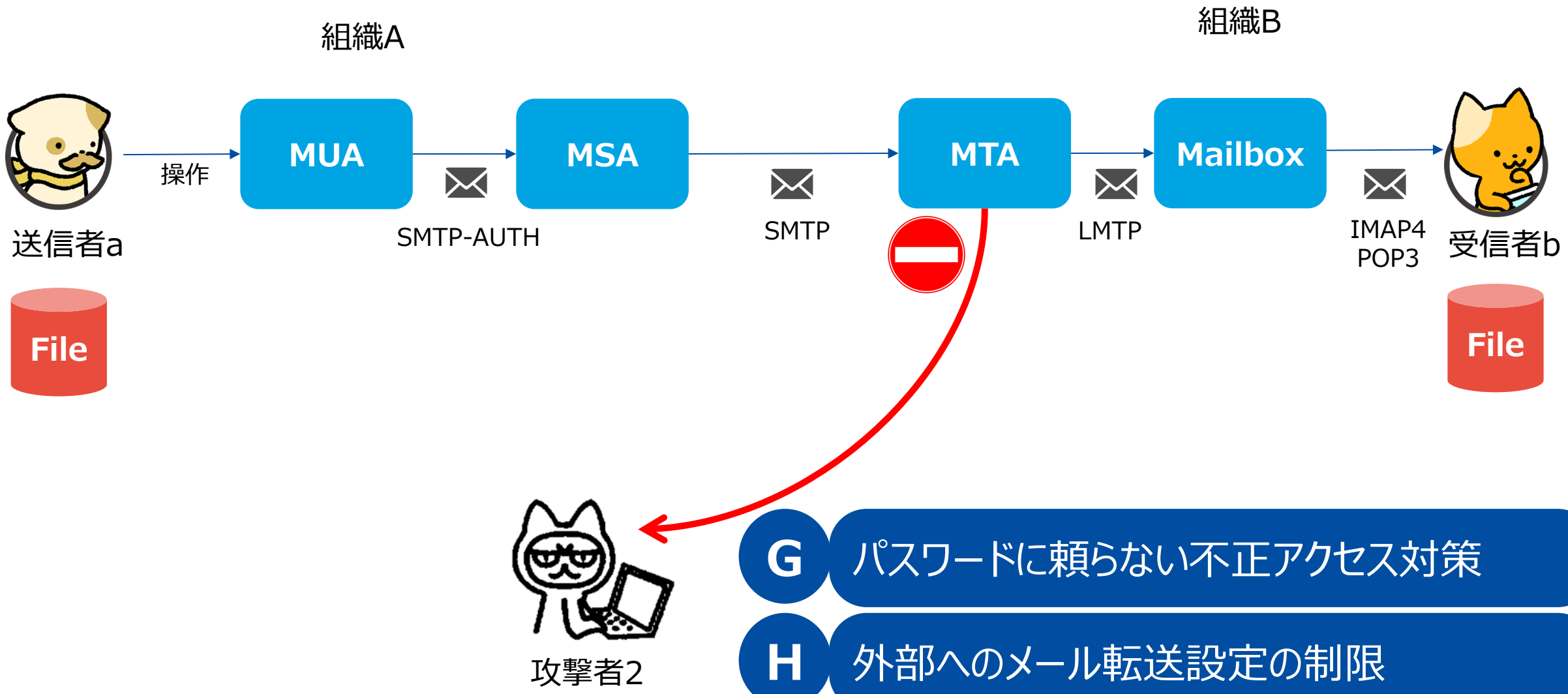


G パスワードに頼らない不正アクセス対策

7. 不正な転送設定でデータ漏洩



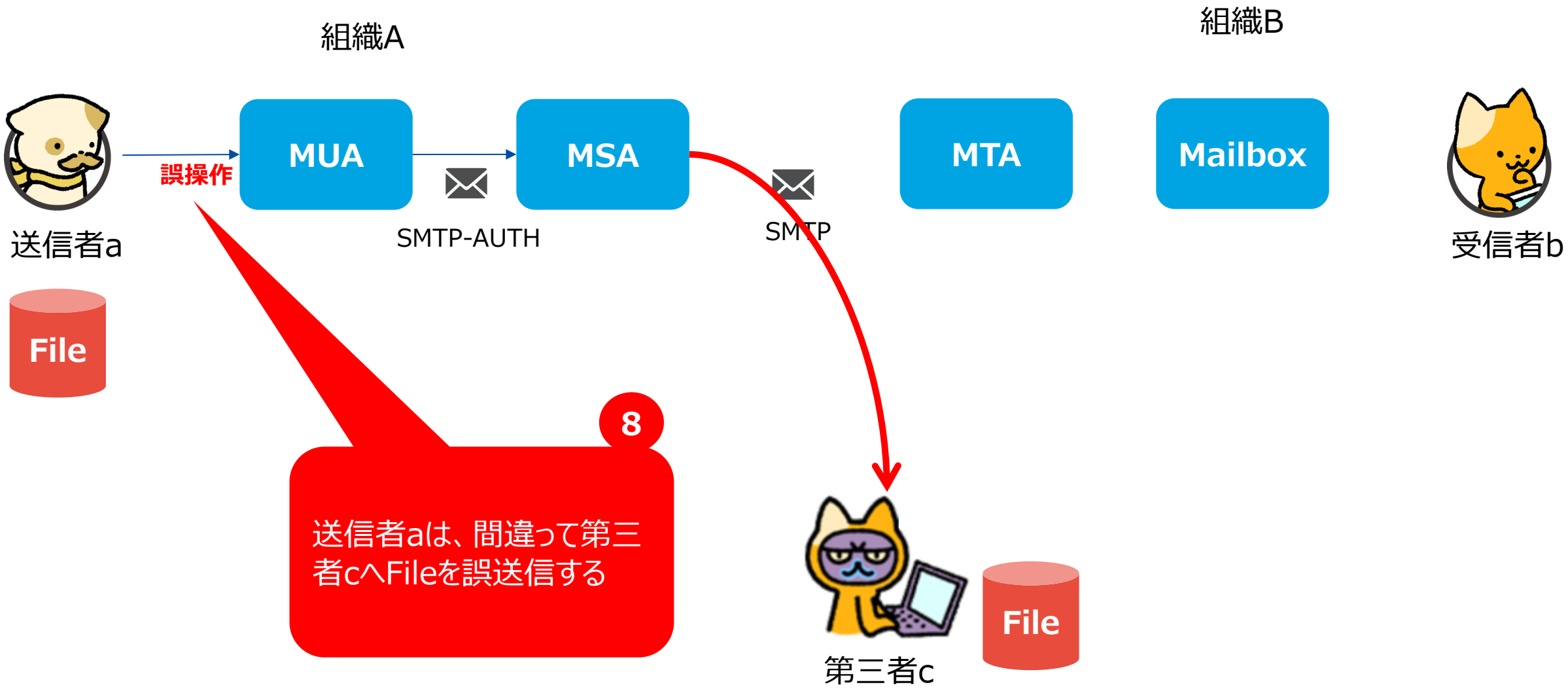
7. 不正な転送設定でデータ漏洩



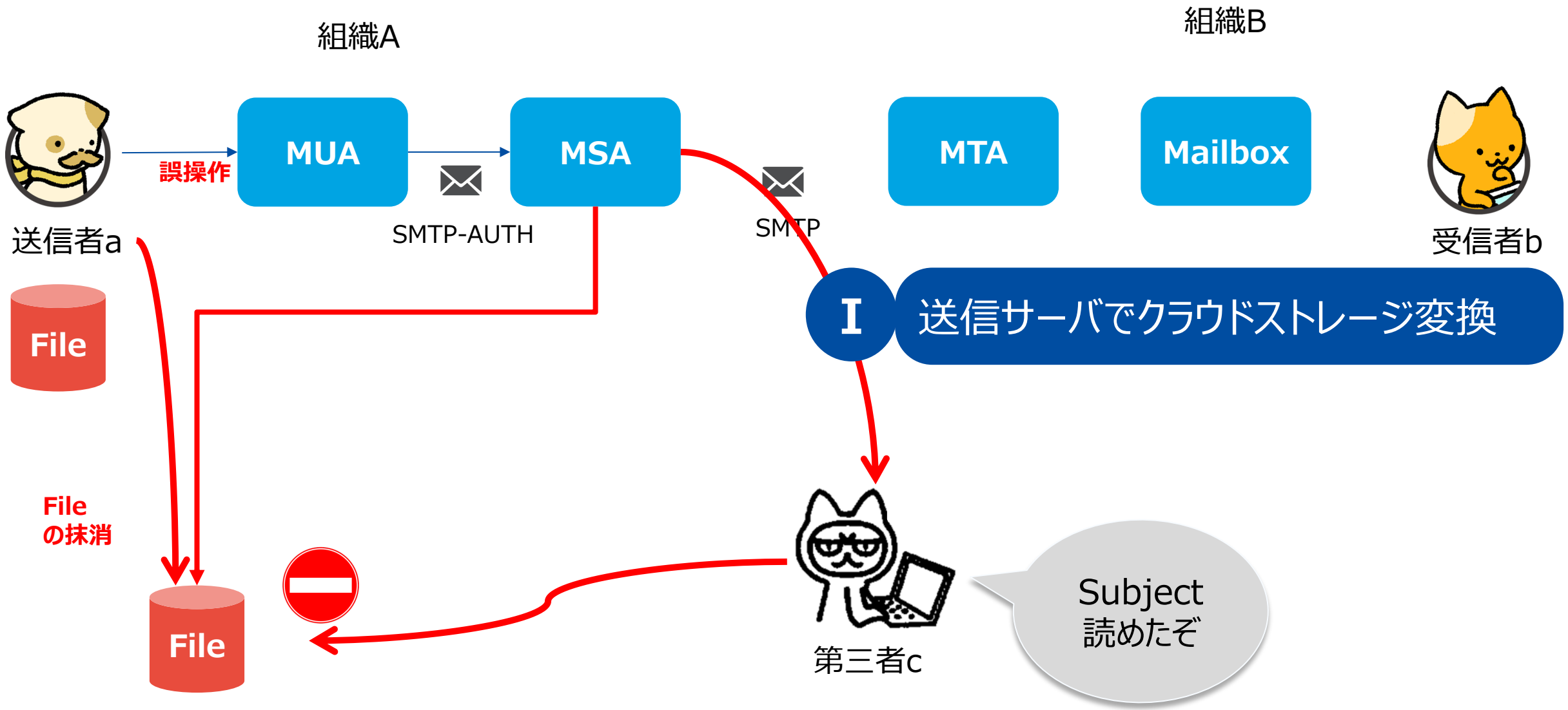
G パスワードに頼らない不正アクセス対策

H 外部へのメール転送設定の制限

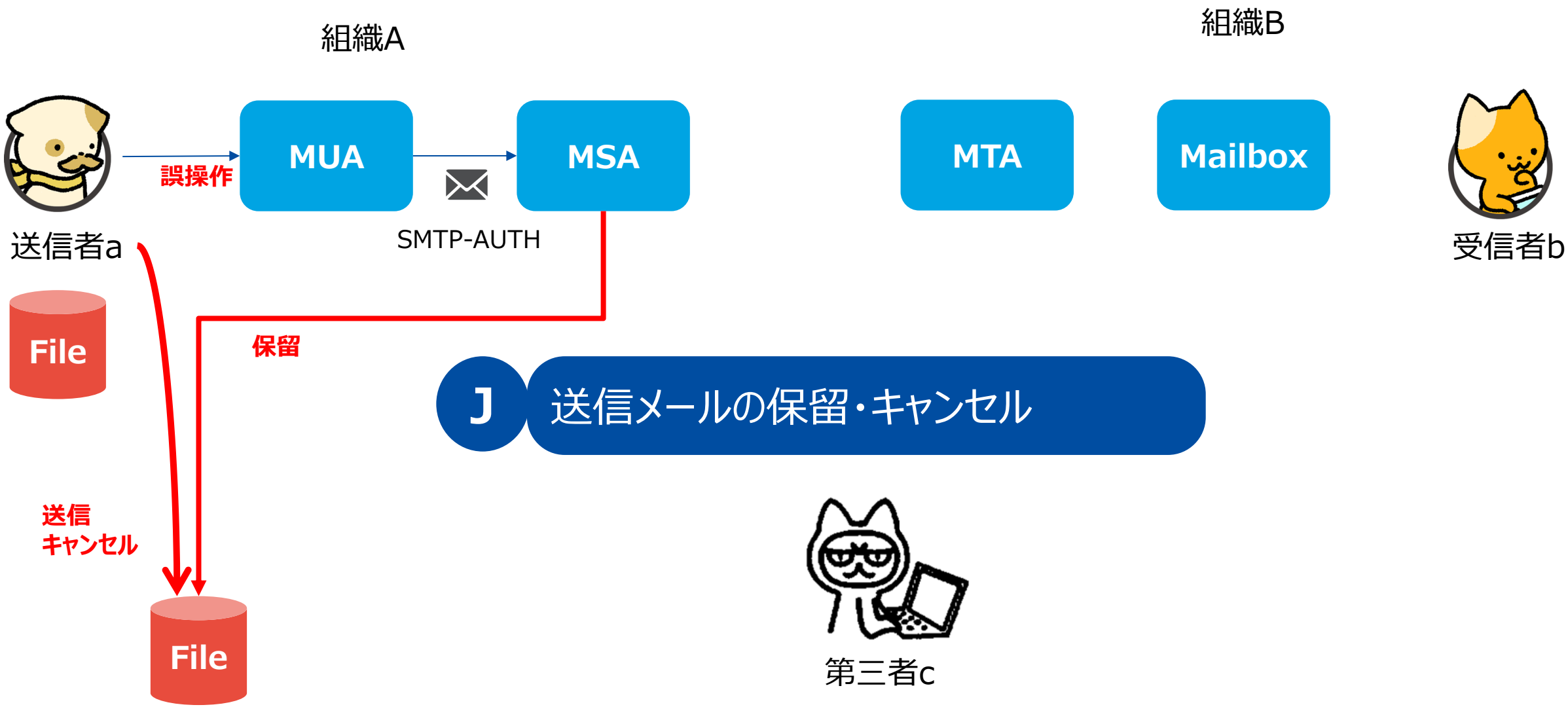
8. 誤送信によるデータ漏洩



8. 誤送信によるデータ漏洩



8. 誤送信によるデータ漏洩



10つの手段の整理

A	送信サーバで “暗号化ZIP” を禁止	ルール化とサーバ対応は比較的容易。 業種によっては、業務効率が下がるリスクあり。
B	受信サーバで “暗号化ZIP” を禁止	メール不達のリスクはあるが、セキュリティ対策として効果は高い。救済措置が必要。
C	送信・受信で DMARC に対応	DNS で宣言するのは容易。強いポリシーで運用するのは難しい割に、効果は限定的。
D	ドメインレピュテーション	データがあり、DMARC と組み合わせれば効果は大きい。データの精度によって FN リスクあり。
E	送信・受信で TLS / MTA-STS に対応	最近では TLS 対応サーバは一般的。TLS バージョンや証明書検証などの手間の割に、盗聴リスクは小さい？

10つの手段の整理

F	S/MIME などの E2EE に対応	技術規格としては有名で、有効な手段。 ゲートウェイでの無害化や、難易度がネック。
G	パスワードに頼らない不正アクセス対策	パスワードレス認証や MFA は効果が大きい。 メールプロトコルでは普及した規格が乏しい。
H	外部へのメール転送設定の制限	ルール化とサーバ対応は比較的容易。 業務の一部になっている場合は、救済が必要。
I	送信サーバでクラウドストレージ変換	対応した SaaS は選択肢が多く、履歴管理もできる。気づくのが遅ければ、救済できない。
J	送信メールの保留・キャンセル	誤送信の直後に気付くケースを救済できる。 保留にする時間だけメール到達が遅延する。