第12回（平成28年度　第3回）
サイバーセキュリティシンポジウム in TDU

ディザスタリカバリ技術の研究

–クラウド，超分散ネットワークの有効活用－

東京電機大学 情報環境学部教授
工博　宮保憲治
miyaho@mail.dendai.ac.jp

於: 東京千住キャンパス1号館2階丹羽ホール
2017年3 月14日　15時30分～15時55分

講演内容 （HS-DRTの概要）

ー高いセキュリティを備えたディザスタリカバリ技術

(High Security-Disaster Recovery Technology)

- HS-DRTの研究・開発のターゲット
- ディザスタリカバリ(HS-DRT)技術の原理
- クラウドを利用する実用化システム解説
- 今後の展開

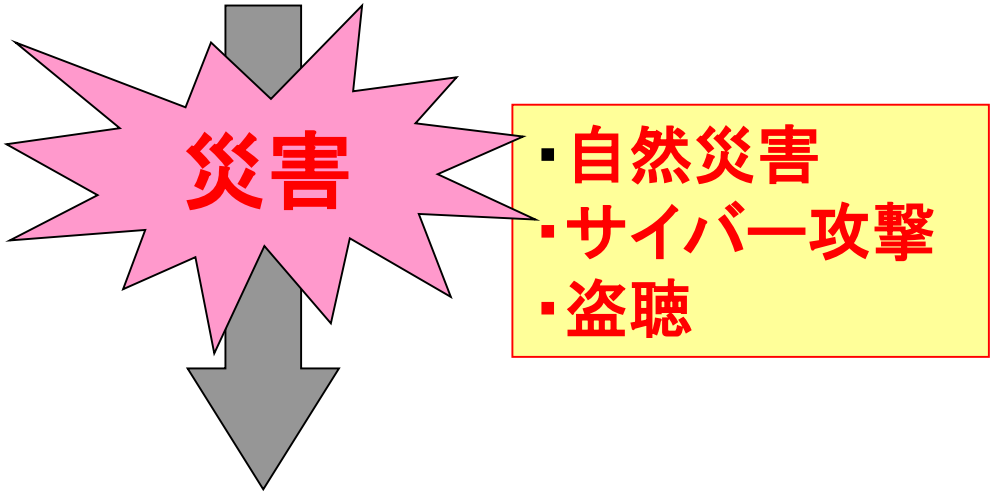
  秘密動画像伝送への適用

  安全な電子メールシステムへの適用

「ディザスタ・リカバリ技術」の研究実用化の背景

情報化社会における、
電子データ保管の重要性

個人情報の保護
災害時の、業務継続の保証



いかに、重要データを，安全・確実に，完璧に、保存・回復できる，バックアップシステムを、安価に提供できるか。

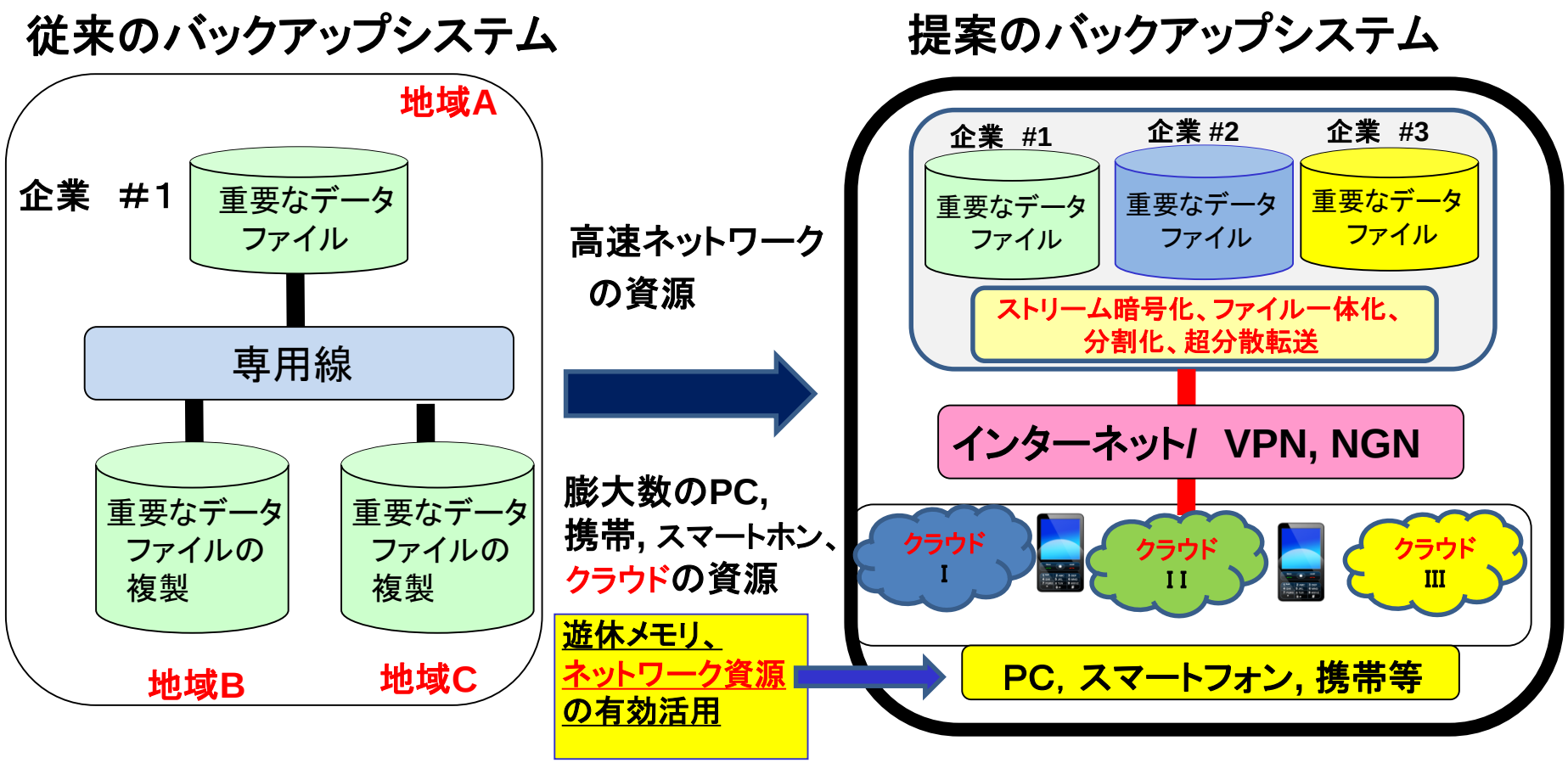
研究・開発のターゲット

- **安全，セキュアー**な機能に重点を置いた，
  効率的な**バックアップ**システムを，**低コスト**で実現
- **自然災害，データ盗聴**に，影響されない，
  バックアップシステムの開発（⇒完全復旧を目標）

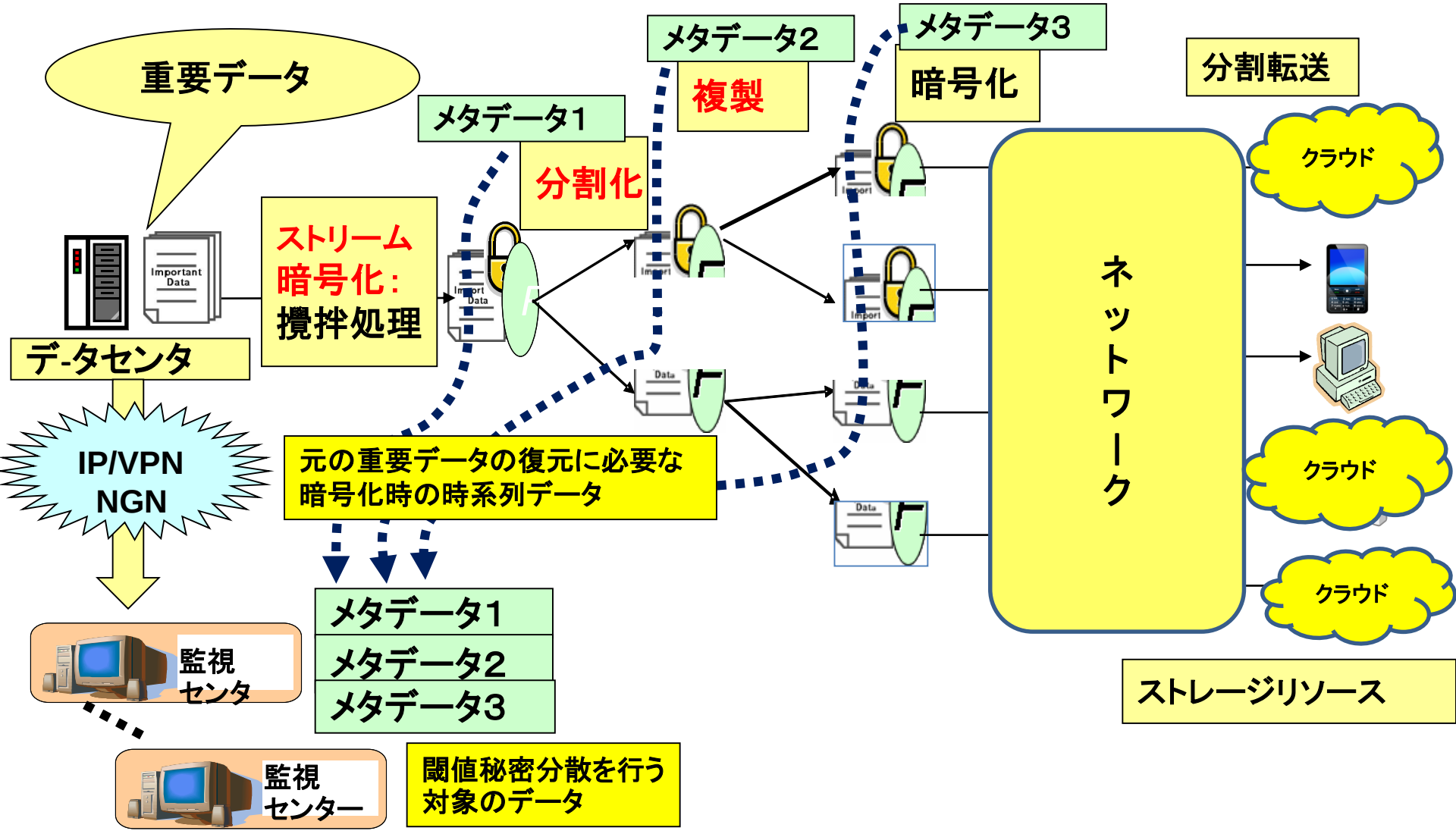
ネットワ-ク活用した超分散技術と，**高速暗号**技術
を活用した「ディザスタリカバリ技術」を，
①クラウド活用のバックアップシステム，②秘密動画伝送システム，③安全な電子メールシステムに応用

従来技術からの脱皮

HS-DRT (High Security – Distribution and Rake Technology)
または,High Security – Disaster Recovery Technology)



HS-DRT(ディザスタリカバリ技術)の原理



情報セキュリティの評価基準

セキュリティの評価のCIA

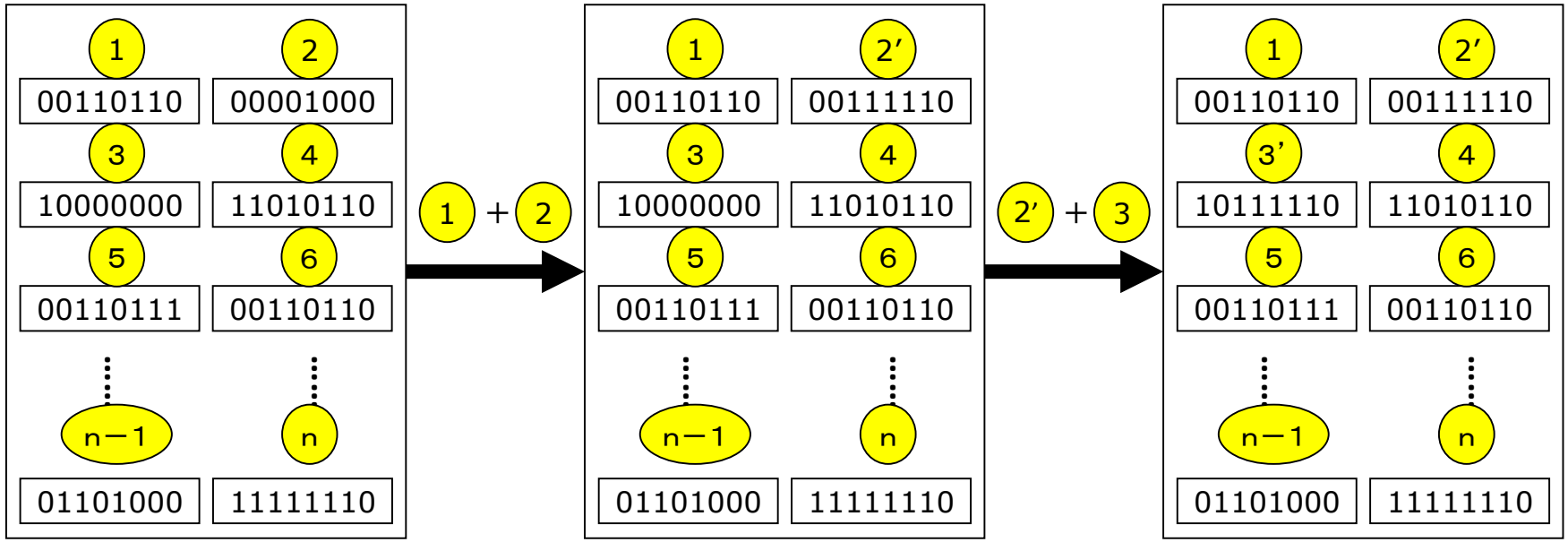
C:　Confidnentiality :**機密性**: 盗まれない
I :　Ingtegurity :**完全性**:　改竄されない
A:　Availability :稼働性（稼働率，回復確率）

CIAの全要素は、複数の(異業者の)クラウドを
適切に組合みわせて活用することで実現可能

ファイルの高速暗号化（一体化処理の例）

（複数ファイルの連結一体化処理も同様に可能）

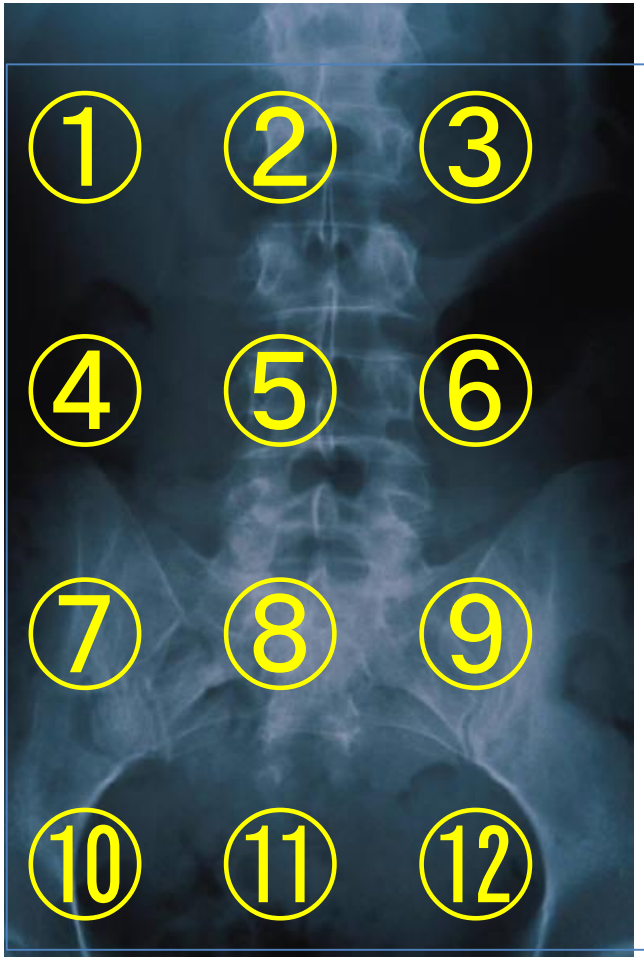
1つまたは複数ファイルを連結決した処理が可能



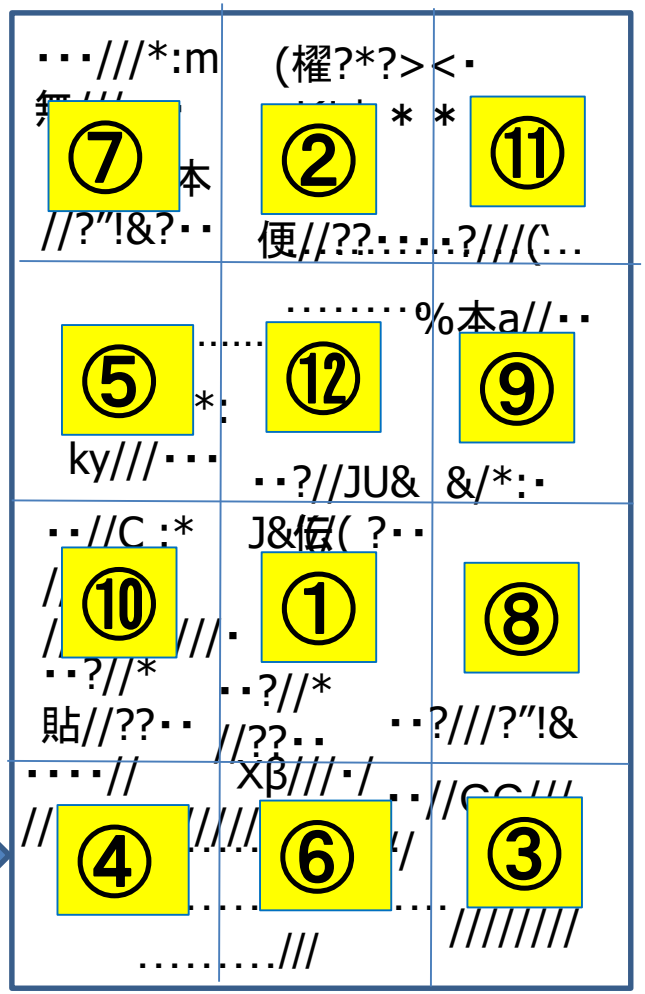
・暗号化対象となるファイルデータ内の隣接ワード毎に、
可逆演算を実施（例えば、2進加算,EXOR演算等を組み合わせ実行）。
・対象ファイルの全ワード数（n）の最後まで,これらの処理を実行し、全てのワードを空間的に攪拌する。
・実用的には、**処理ワード数**や**演算処理内容**を**適宜、変更（メタデータ）する。**

（例）レントゲン写真の分割転送

暗号化＋分割＋シャフリング



高速暗号化
（一体化）
＋
分割
＋
シャフリング
(並べ替え)



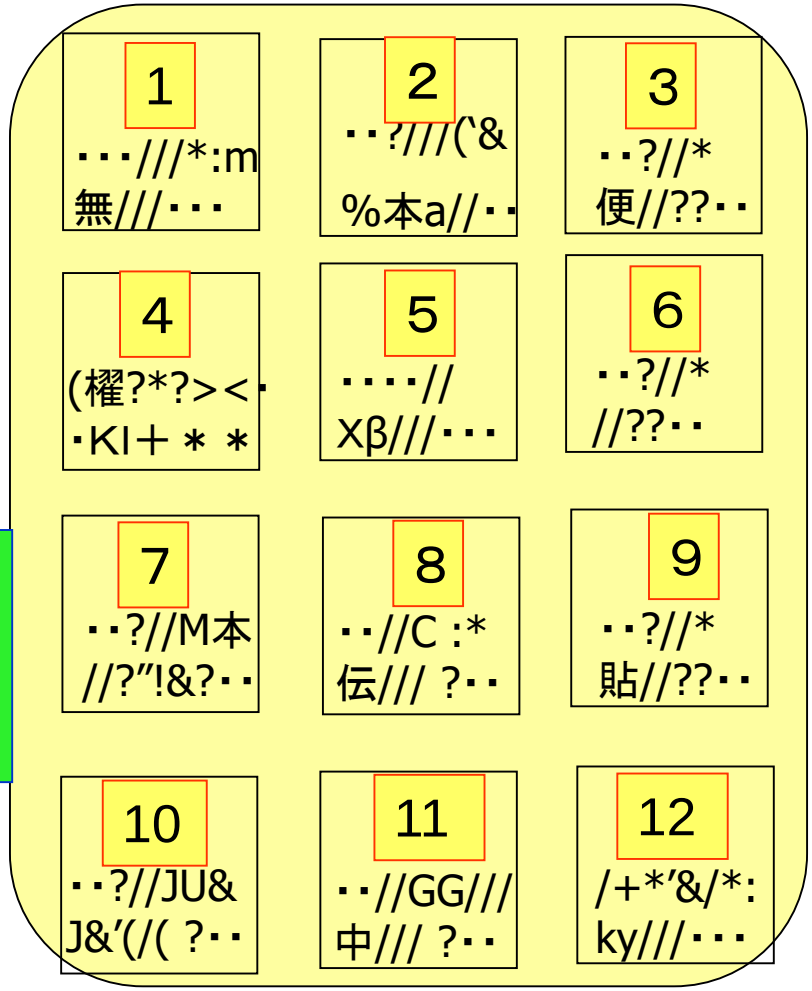
Fisher Yates shuffling アルゴリズム

分割写真が仮に正しい暗号鍵で復号に成功

断片化数　80⇒80！=2^{400}
の組合わせ数
⇒400bit のAESと同等
の暗号強度

12！
≒5億
の組合せ

80！
≒無数の
組合せ
≒(1兆)^{10}



盗聴者は断片ファイルの暗号解読に成功した場合でも成功した事に気がつかない！

提案技術の可視化イメージ

クラウドの最大の課題⇒セキュリティの向上

オリジナル画像

一体化に相当する
デフォルメ処理
(画像の属性識別子
の撤廃も可能)

分割化

**セキュリティ強度
が飛躍的に向上**

シャフリング
超分散転送
(秘密転送)

秘密分散

各断片
は別鍵
で暗号化

ハッシュ付き

各断片
は別鍵
で暗号化

ハッシュ付き

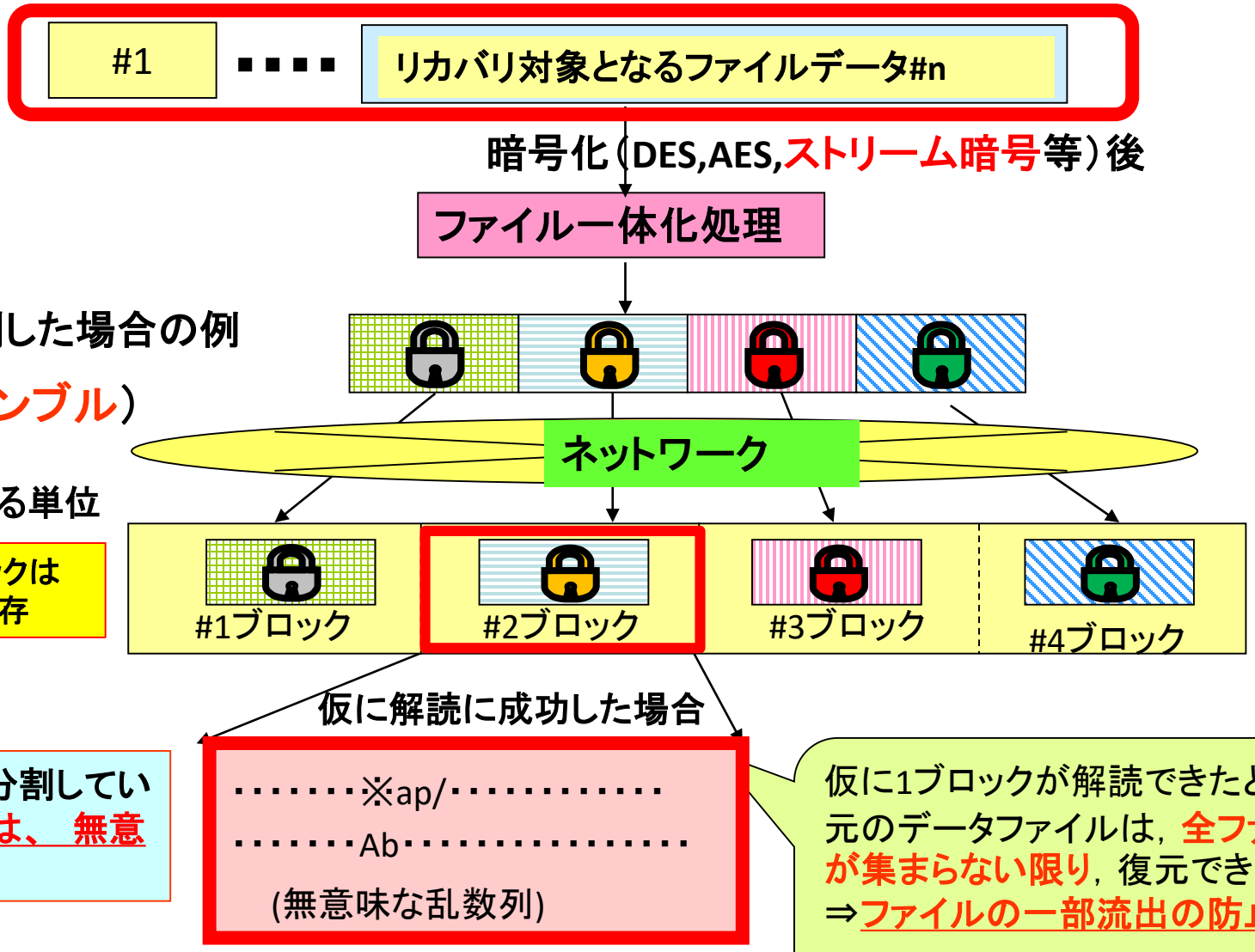
各断片
は別鍵
で暗号化

HS-DRTの採用 ⇒ 分割化 ⇒ 複製・暗号化・超分散・
(別鍵で再暗号化)

セキュリティのCIAを実現

HS-DRT技術の効果

（一体化処理（ファイル攪拌）の導入）



（参考）暗号強度の定量的な比較

① 分割数が20の場合

ファイルの並べ方の組み合せ=**20!**≒2^{61} ≒10^{18}

この組み合せ数は、**DES (54ビット)暗号以上**の安全性

② 分割数が40の場合

ファイルの並べ方の組み合せ=**40!**≒2^{160} ≒10^{47}

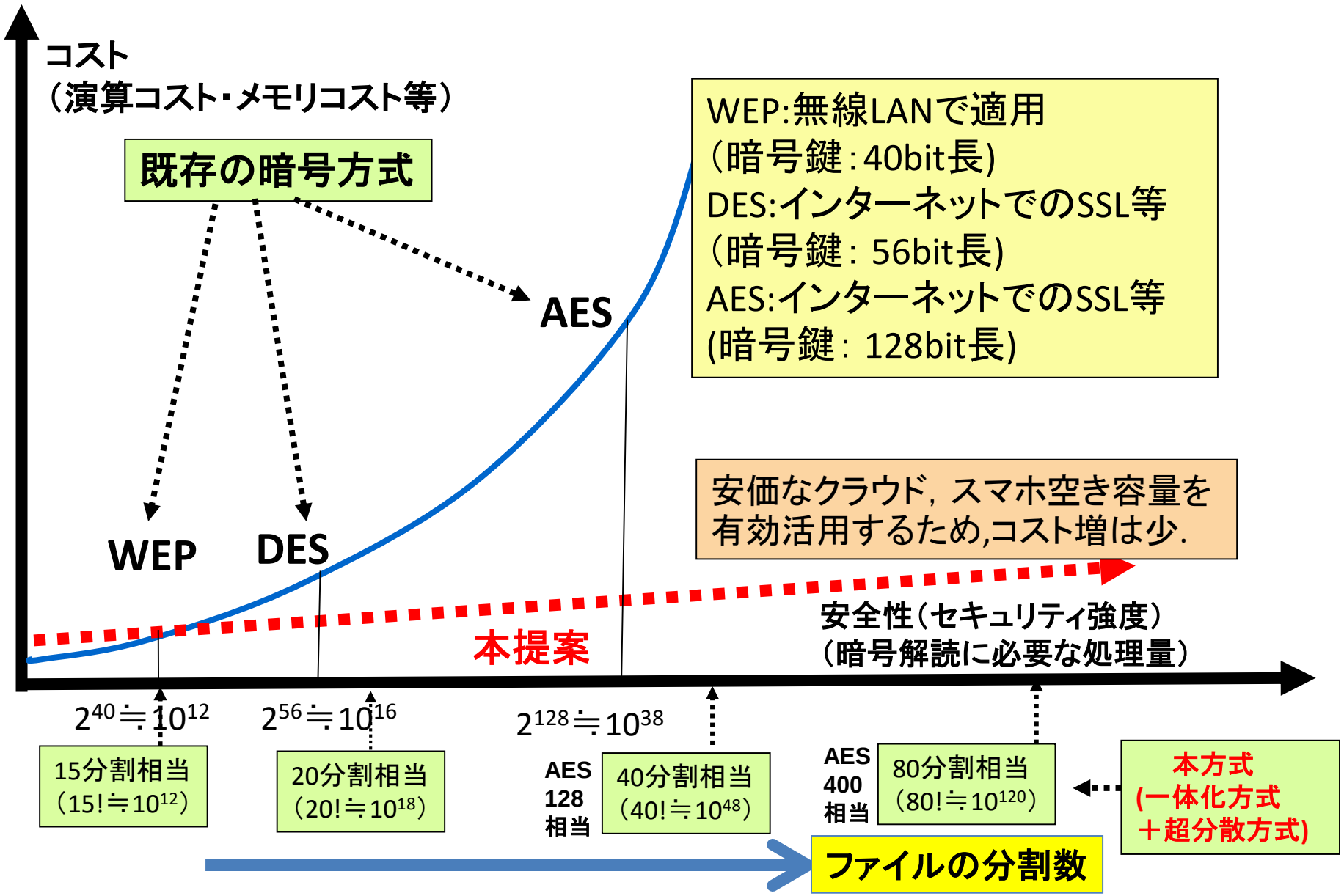
この組み合せ数は、**AES (128ビット) 暗号以上**の安全性

③ 分割数が80 の場合

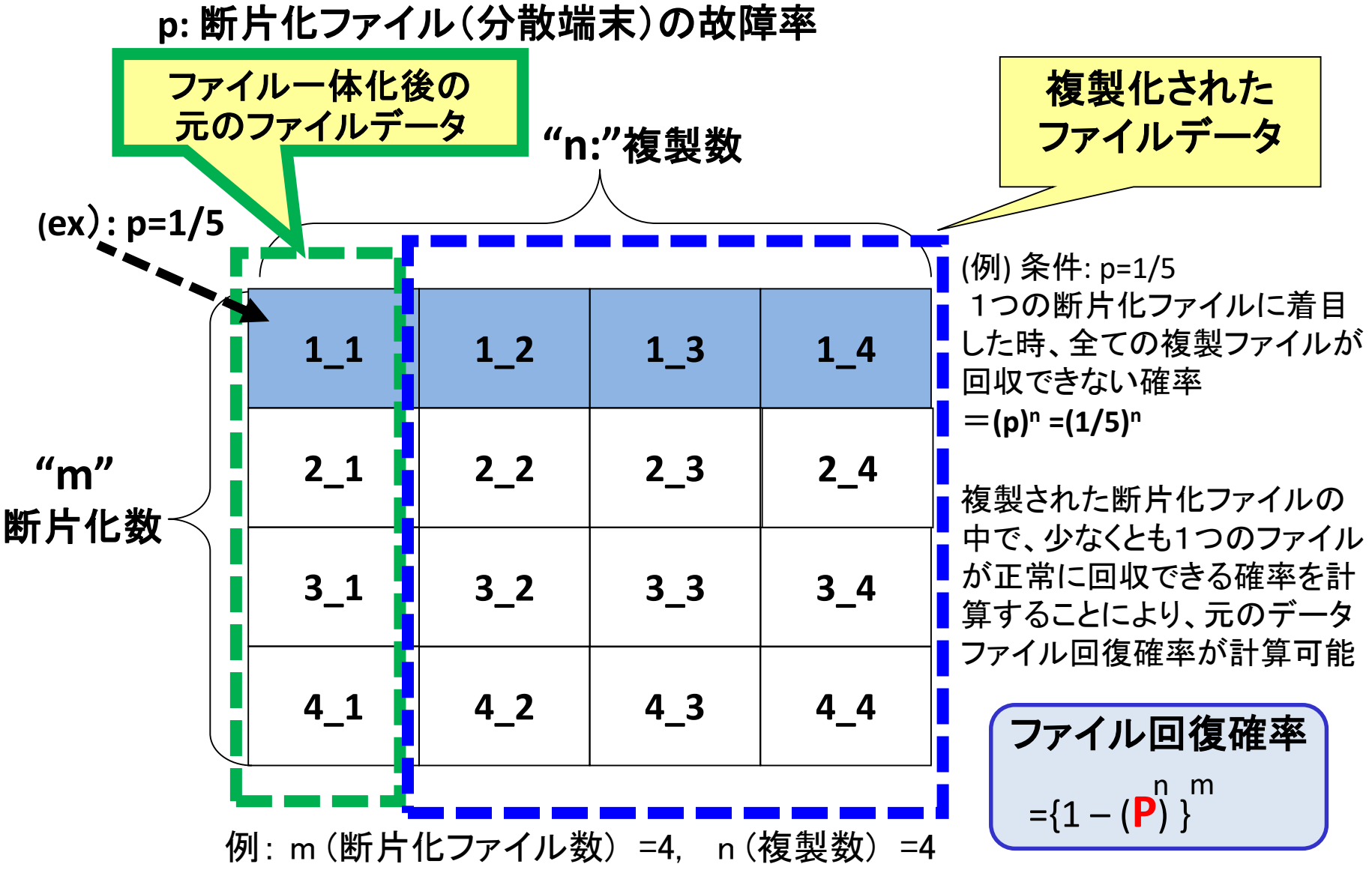
ファイルの並べ方の組み合せ=**80!**≒2^{400} ≒10^{120}

この組み合せ数は**400ビット暗号の安全性**と等価であり，この レベルに匹敵する安全性をもつ暗号は、**実用化されていない。**

従来の暗号方式との定性的な比較



ファイルの回復確率の算出法



データの分割･複製の効果

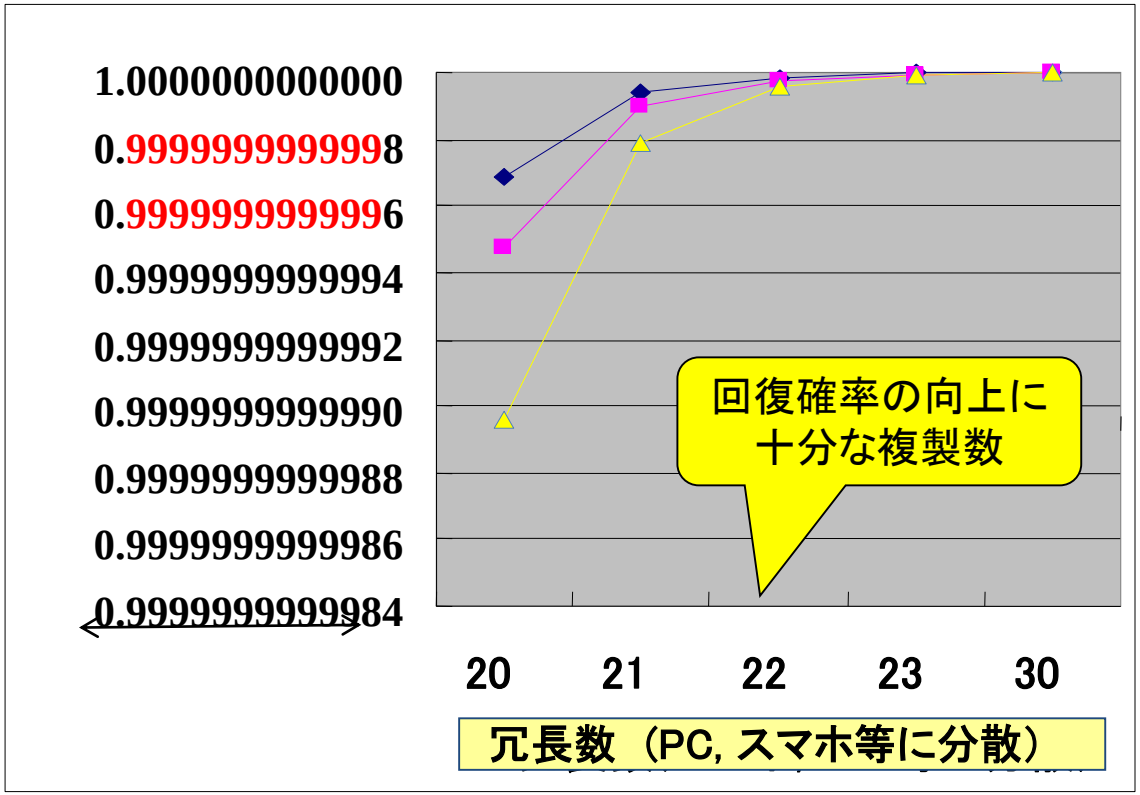
回復率＝(１－P^n)^m≒１－mP^n

(PはPC一台あたりの故障率で、通常0.1以下)

- **分割数(m)を増やす→暗号強度が増す。**
- **複製(n)を増やす→回復率が上がる。**

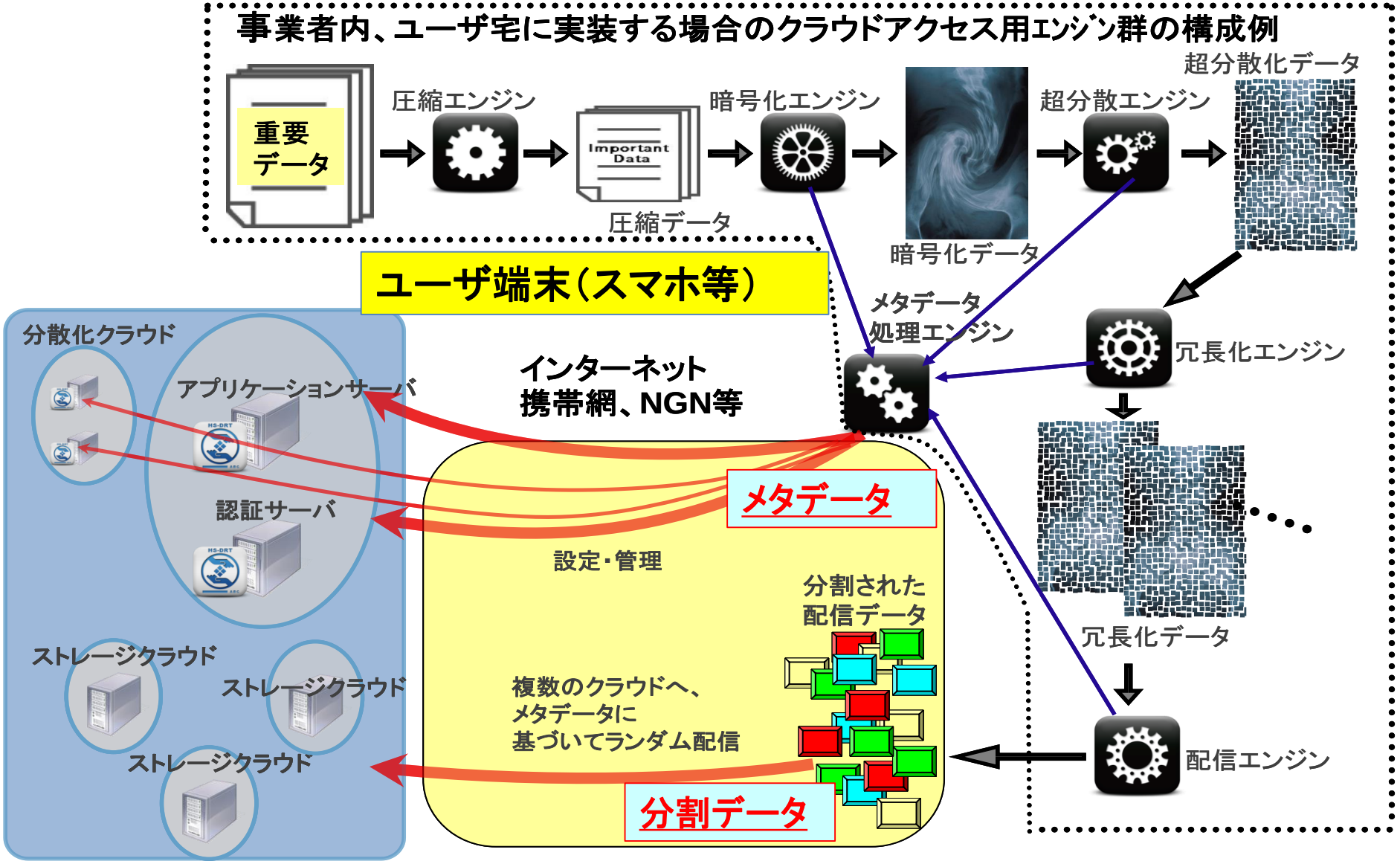
m,n,P(故障率）の値に着目し、ユーザの個別の要求に基づく**セキュリティ強度**の任意設定

ファイル回復確率の算出の一例



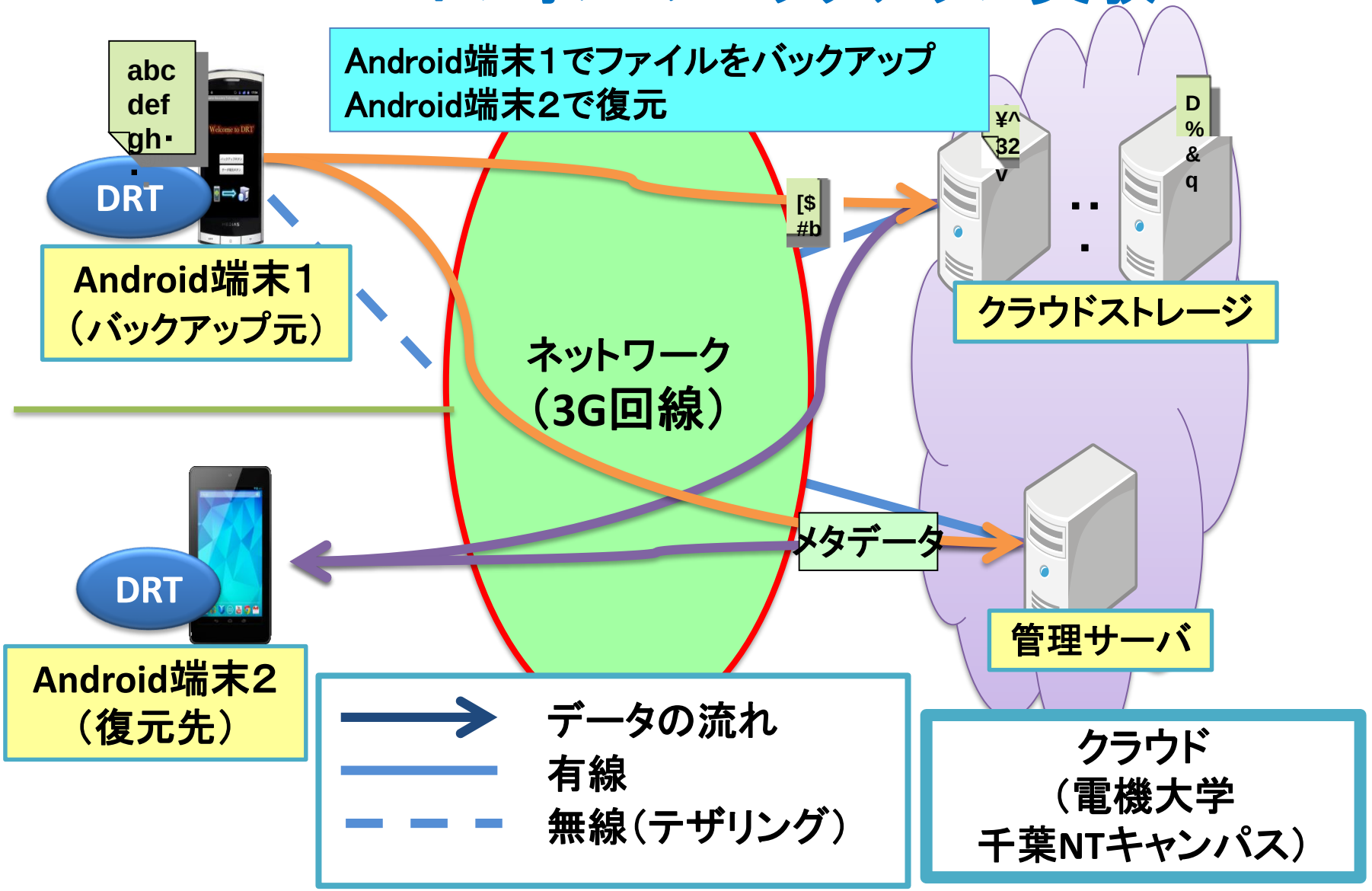
断片化ファイルの回収不能確率＝1/5

HS-DRTエンジンの実装例



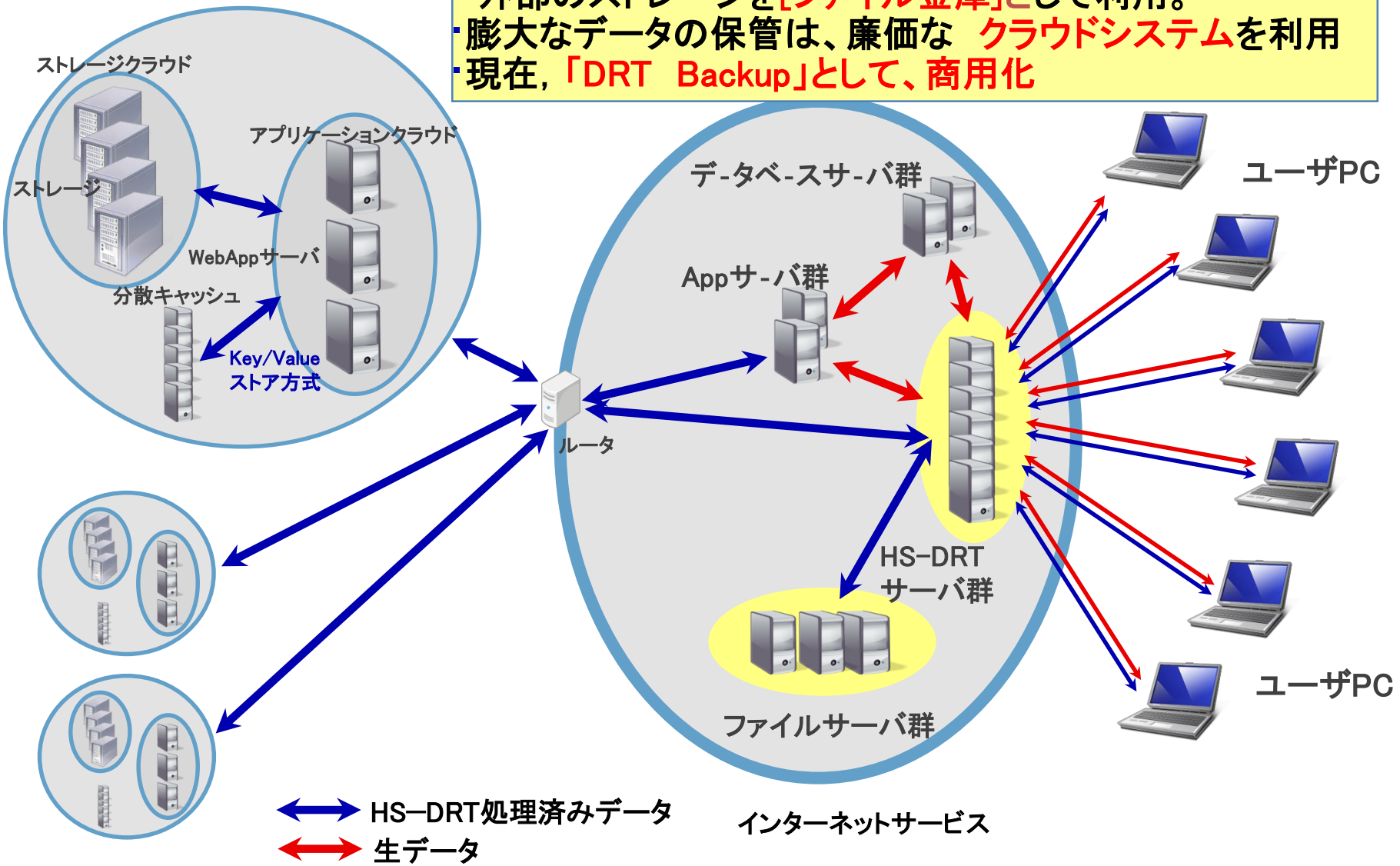
WTP2013 デモ

スマートフォンのバックアップ実験

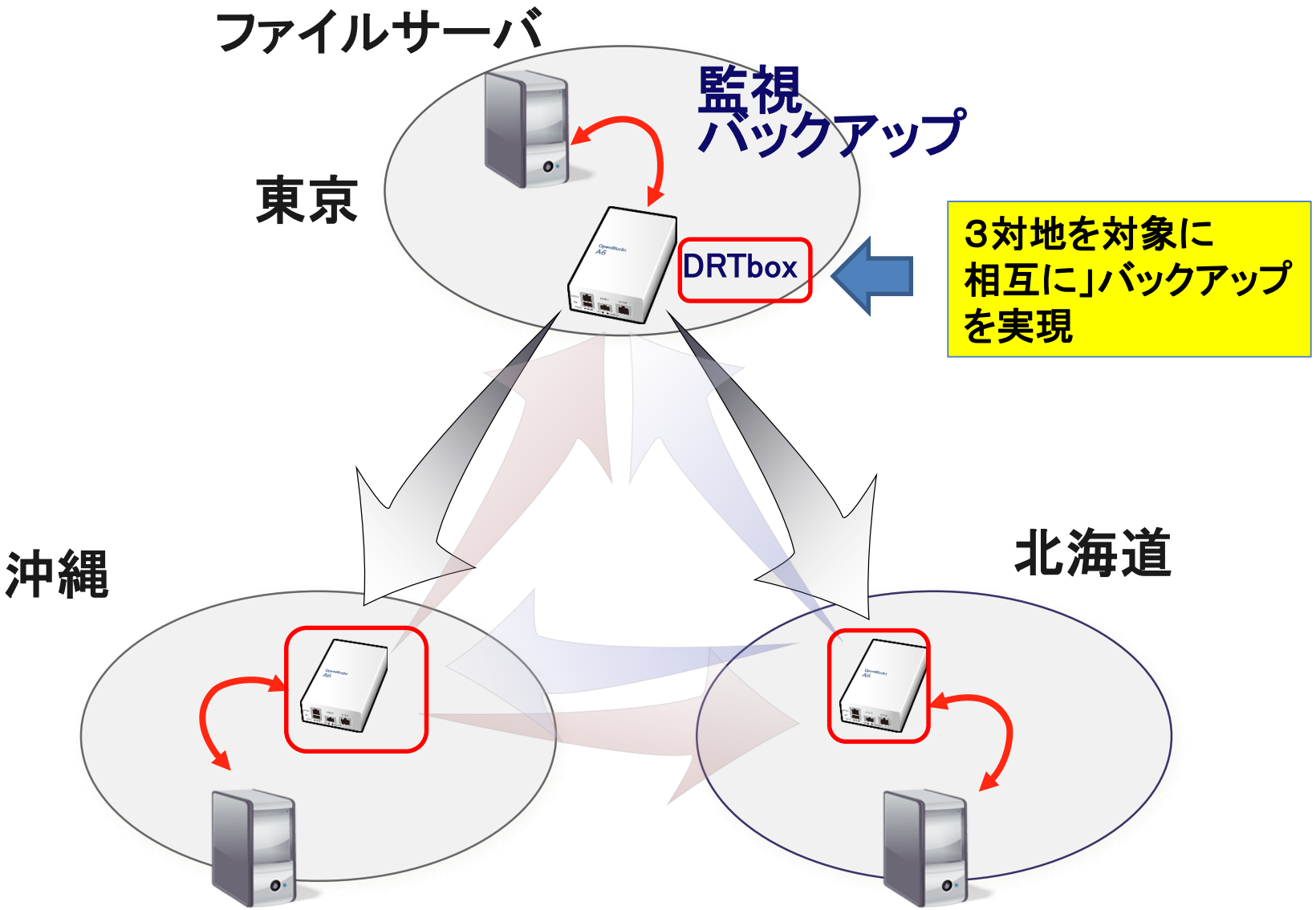


クラウド対応のHS-DRT技術の実用化

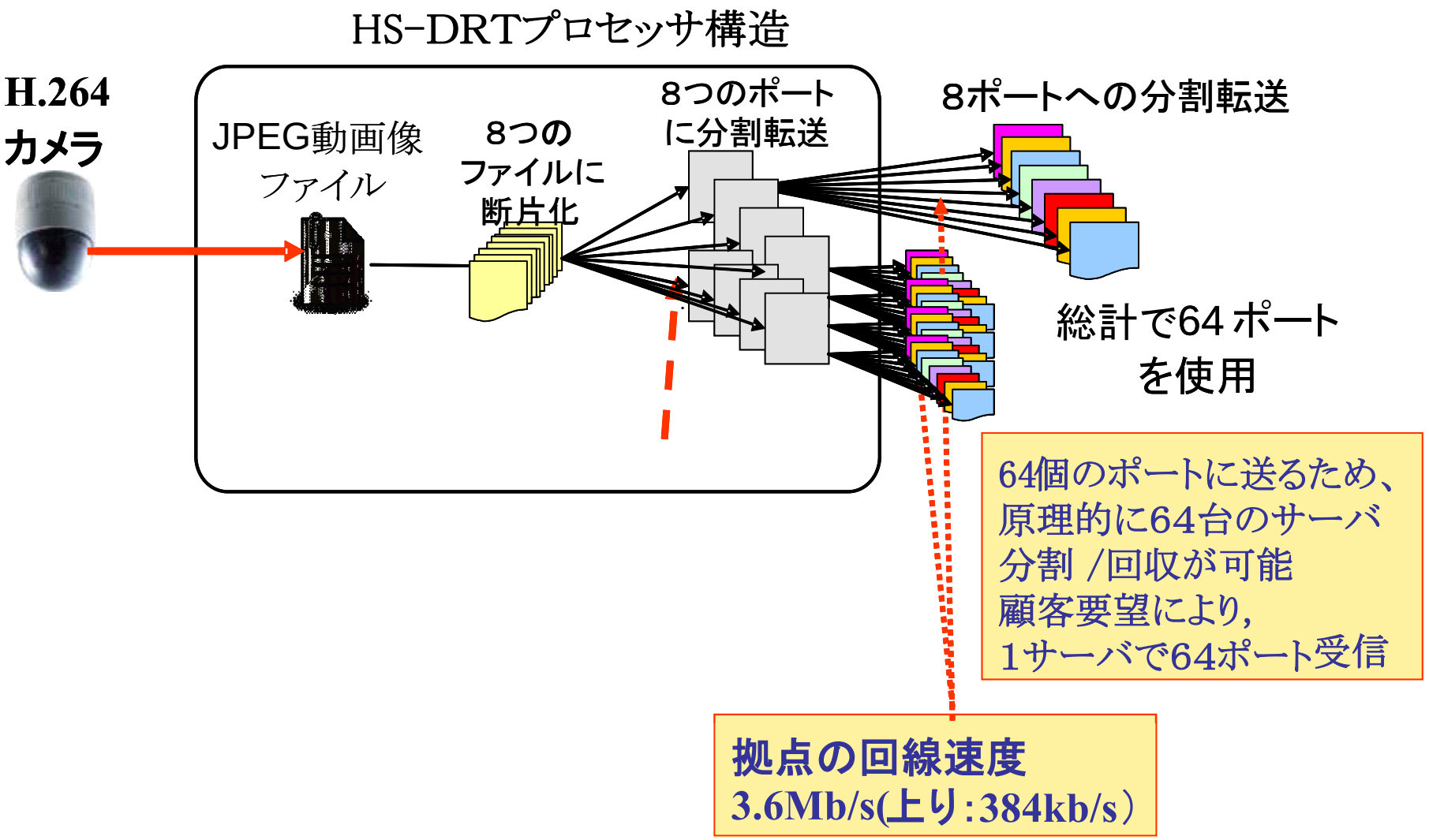
- Webアプリケーション群と連携し、バックエンドに、外部のストレージを[ファイル金庫]として利用。
- 膨大なデータの保管は、廉価な　クラウドシステムを利用
- 現在，「DRT　Backup」として、商用化



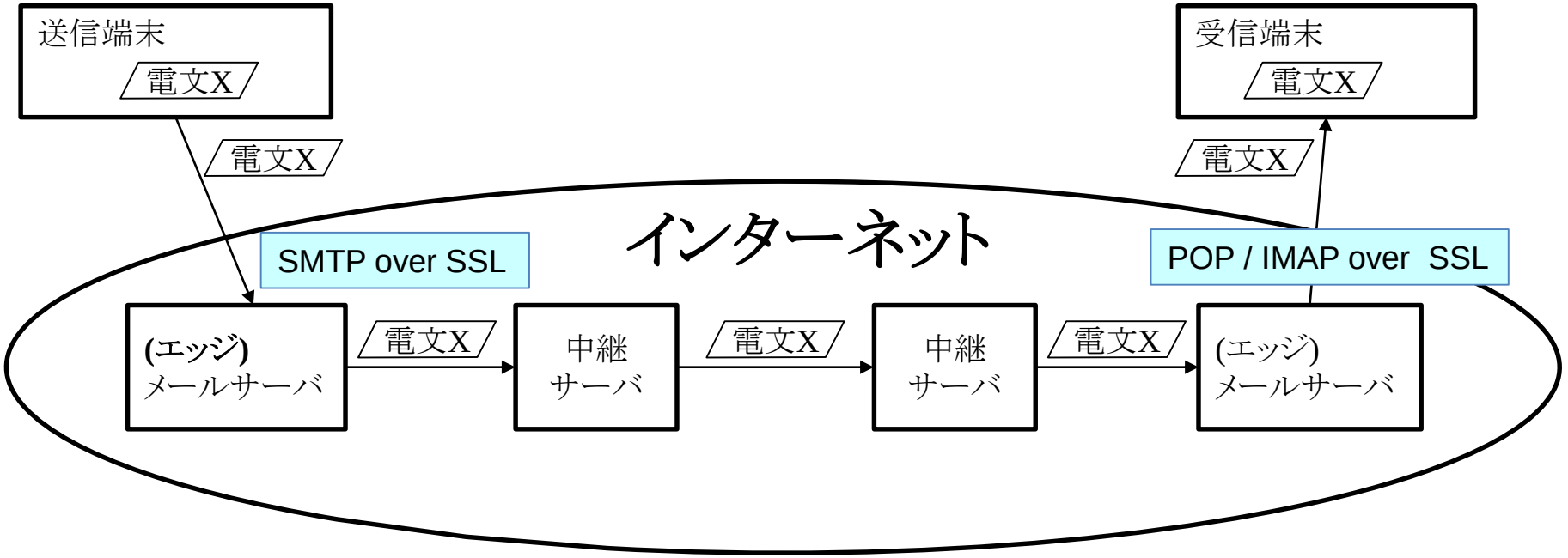
超分散　HS-DRTの適用



秘密映像伝送システムの実現例



インターネットにおける基本的な電子メールシステム



基本的に1つの経路内での情報伝達

- 一つのアカウント,またはマルチアカウントを用いて相手先のアドレスに対してSMTP over SSL/TLS暗号化等を活用。
- 送信クライアント - 送信メールサーバ間およびクライアント間同士で暗号化されたデータ転送を行う方式

従来の電子メールの課題

(1)従来の方式は、基本的には**1対1の通信形態でのメール中継**をバケツリレー的に、中継サーバを介して実現する

→①メール内容が利用するプロバイダの中継サーバ間で解読される**可能性**.

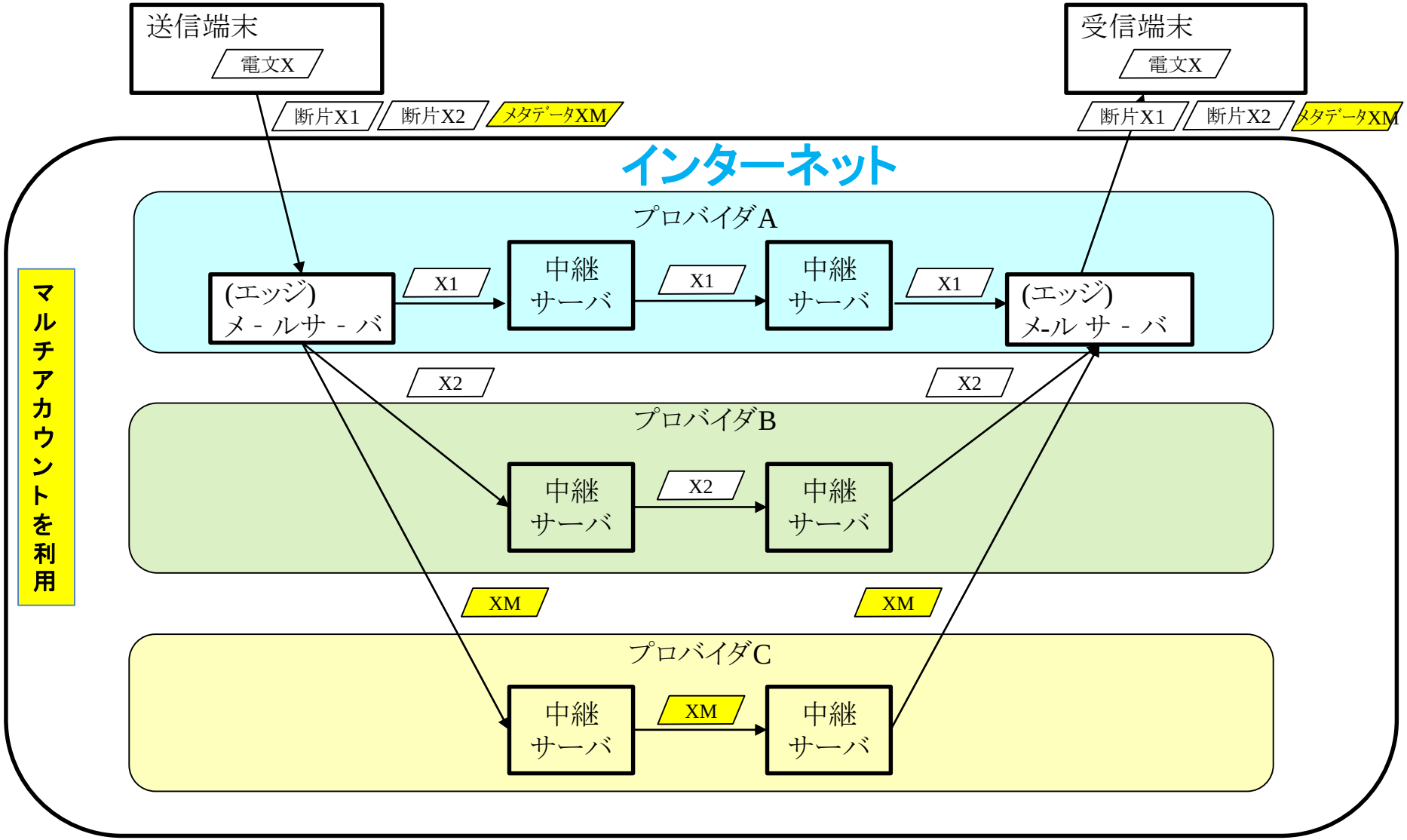
→②第3者がアクセス可能なメールサーバに蓄えられた段階で、盗聴される**可能性**.

(公開鍵暗号の危殆化が想定され，**将来的には無視できない**。)

(2)送信者のなりすましメール問題の解決策として、S/MIMEが　ディジタル認証に利用されているが、相変わらず**1対1通信形態**を前提。

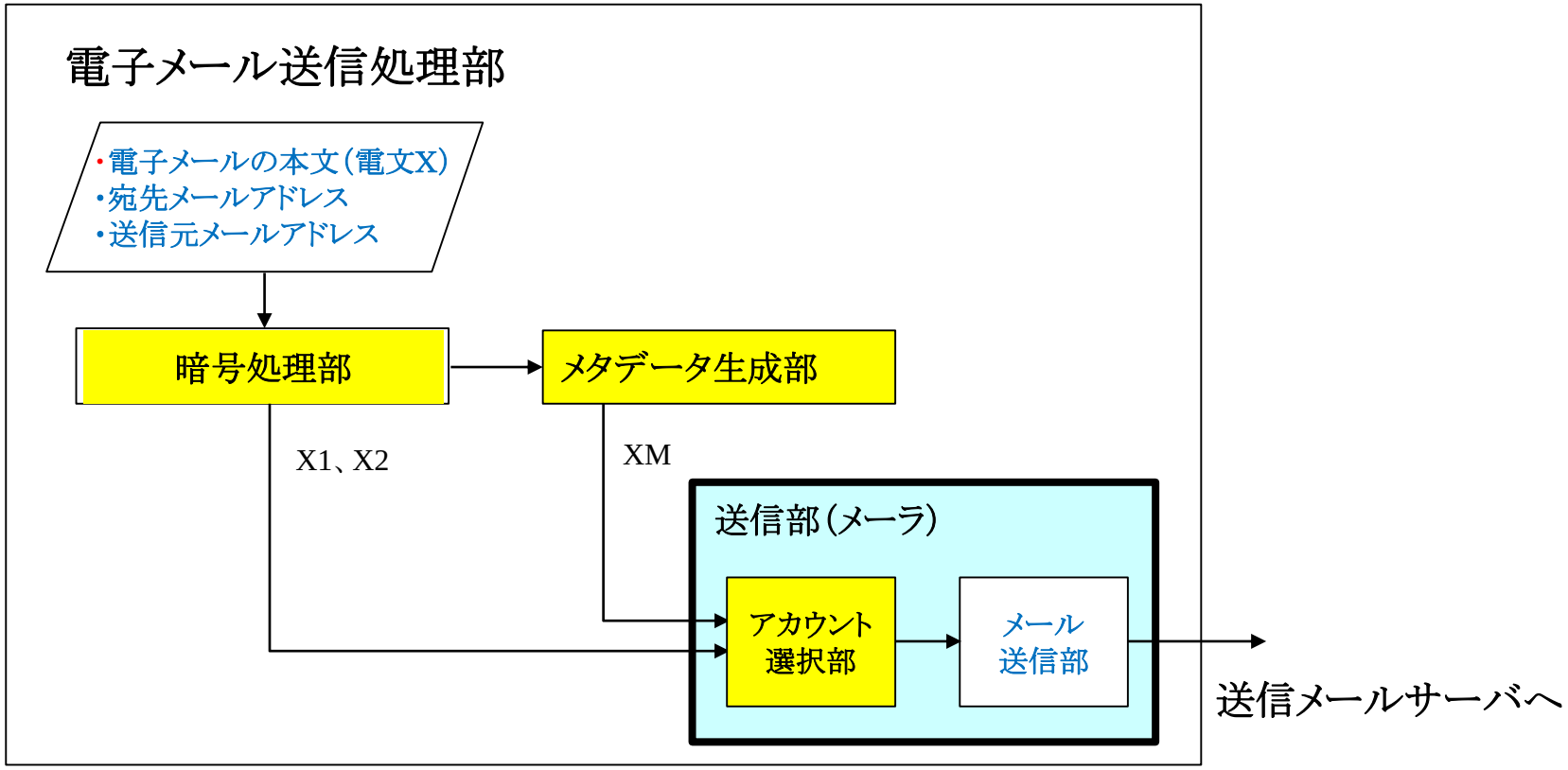
→中継サーバにおけるデータの盗聴や安全性の確保は**完全には保障できない。**

セキュアー電子メールシステムの実現方法



セキュア−電子メールシステムを実現する要素技術

発側（端末）から転送する暗号断片（パケット）の 分散転送例



セキュア-電子メールへの実現

(1)**ディザスタリカバリ技術**を活用し、電子メ-ルの転送経路において電子メールが盗聴される 可能性を排除し、**電子メールの高速転送**が可能にし、かつメ-ル**解読**が受信者以外の第３者には**不可能**にできる。

(2) ユーザが個別に使用可能な **マルチアカウント**を効果的に**同時に活用**することにより、 **セキュリティを一層高める。**

➡既存のネットワ-クにおける電子メールシステムを活用し，ユーザ側の**メーラーに機能追加**を行うことにより、**容易に「セキュリティ」 に優れる**電子メールを実現。

まとめ
本技術の適用が可能な対象

- クラウドを運用している事業者に対して，強力なセキュリティ機能を付加する技術を提供。
- バックアップ利用のユーザ層を拡大し，通信事業者にとってコスト・メリットの高いソリューションを提供.
- 暗号の高速化により,医療機関の膨大画像デ-タ，手術時のリアルタイム映像を安全に データ保管
- 行政機関の重要データ保管.
- 極めて安全な電子メールシステムの構築
（既存のネットワークインフラの有効活用）

ご清聴をどうも有難うございました。

miyaho@mail.dendai.ac.jp

研究室ホームページ

http://www.ine.sie.dendai.ac..jp/wordpress