

第1回(平成25年度第1回)CRCフォーラム(平成25年7月4日(木)開催)
「ITシステムの利用者に安全安心をもたらすための研究開発」

超分散技術を応用した ディザスタリカバリシステムの研究実用化

宮保 憲治 教授
情報環境学部情報環境学科



東京電機大学第1回CRCフォーラム

超分散技術を応用した ディザスタリカバリシステムの研究実用化 —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@sie.dendai.ac.jp

<http://ine.sie.dendai.ac.jp>

於: 東京千住キャンパス1号館2階丹羽ホール

2013年7月4日 17時00分～17時30分

目次

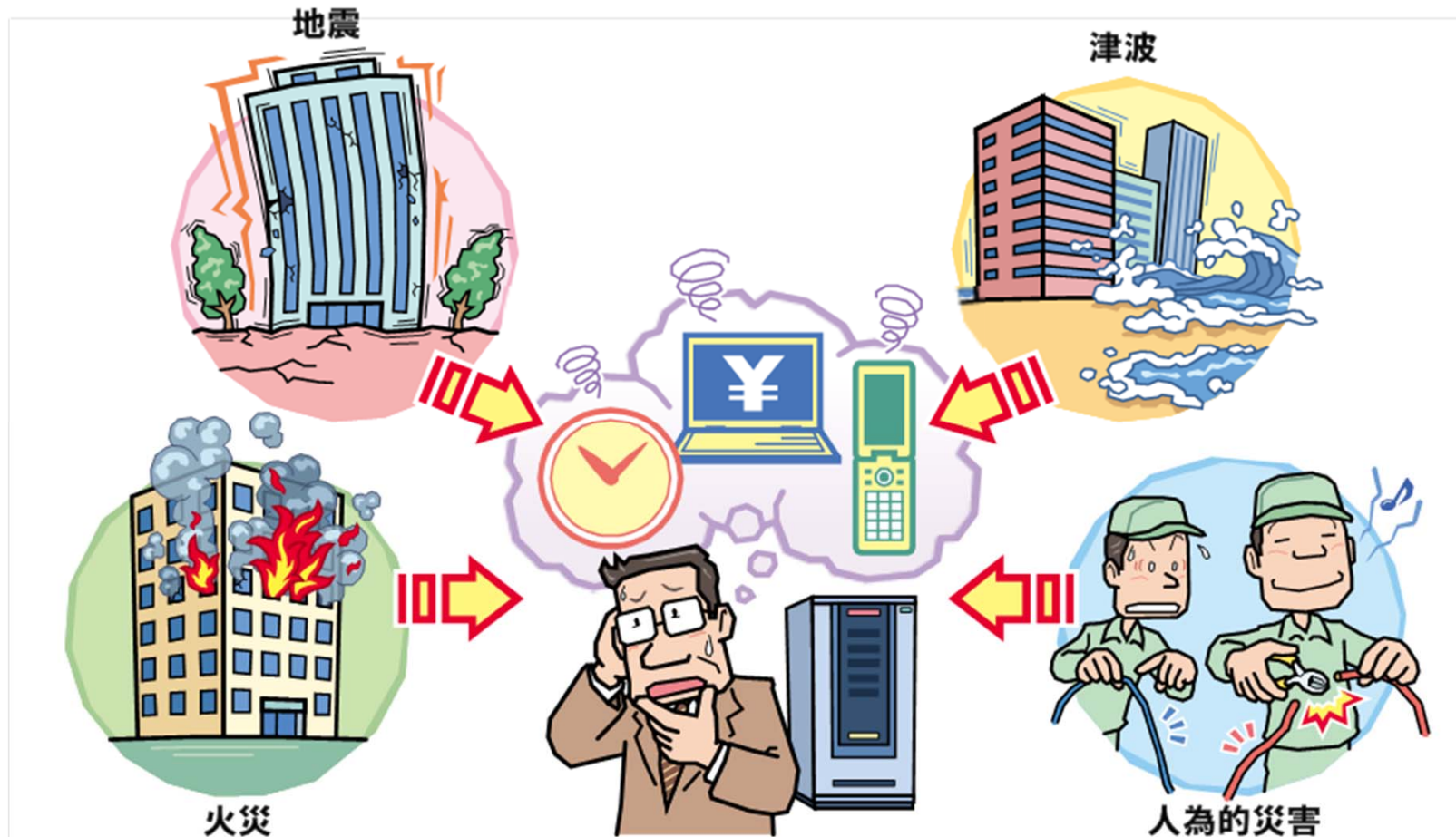
- ディザスタリカバリ(HS-DRT)技術の役割
- HS-DRTの技術の概念
- HS-DRTの技術の詳細
- 実用システムの紹介
- これからの展開

秘密動画像伝送への応用例

Android端末(スマホ)への適用例

安全なセンサーネットワークへの適用

予測不能の災害発生！
引き起こされた業務停止
⇒ **事業継続性**の保証が重要
(**BCP** : **B**usiness **C**ontinuity **P**lan)



事例検証

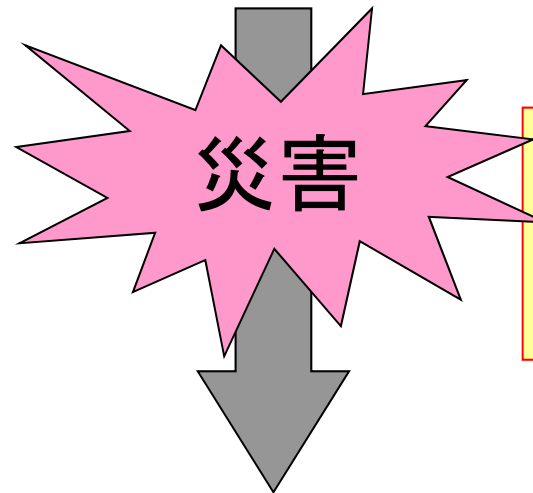
- 東北地方太平洋沖地震

- 直接被害: 地震によるサーバ障害や津波による戸籍データの消失
- 間接被害(1): 計画停電等により38%企業が事業に何らかの影響を受けた。
- 間接被害(2): 義援金の振り込みが殺到し, 10日間におよびシステム障害が発生。

ディザスタリカバリシステムの 研究実用化の背景

情報化社会において
電子データの重要性

個人情報の保護
災害時の業務継続の保証

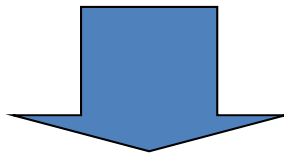


- ・自然災害
- ・サイバーテロ
- ・盗聴

いかに、重要データを、安全・確実に、完璧に復旧
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)



ネットワー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システム**」

2011年3.11東日本大震災

⇒ 電子情報基盤が破壊
IT基盤を頼る, 社会に大きな混乱

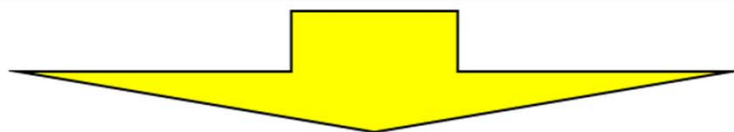
従来: ネットワーク回線の冗長化、
データセンタ二重化, 複数事業者へ2重帰属
(コストがかかる割には、信頼性は不十分)
(バックアップ場所が2~3箇所程度では不十分)

⇒ 超分散ネットワーク技術と高速暗号の融合
既存のインフラ設備: 殆ど無尽蔵の安価なクラウド,
PC, スマホ, 携帯, デジタルサイネージ

超分散ネットワーク技術を活用した ディザスタ・リカバリシステム

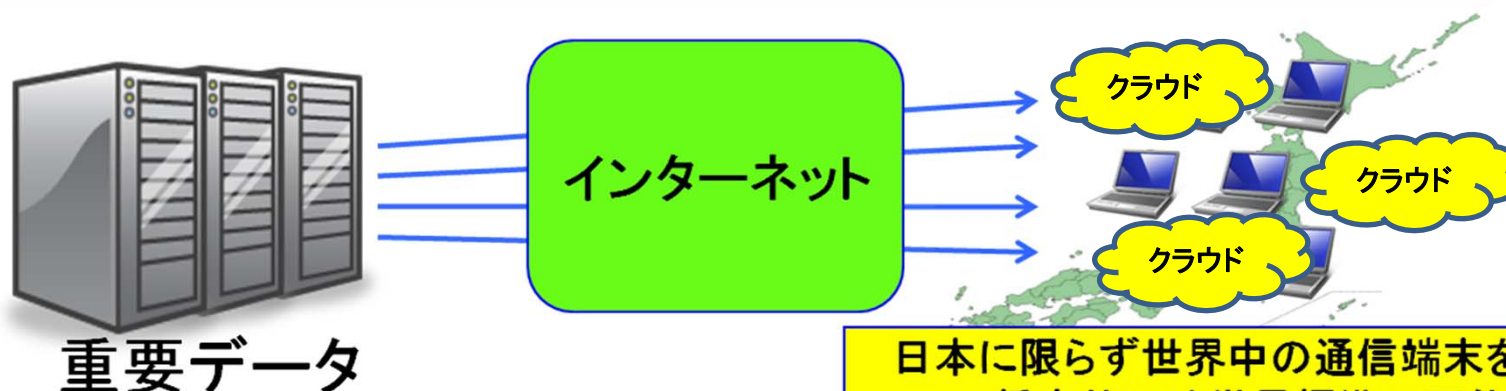
ディザスタ・リカバリシステム

- 通信端末の**ストレージの一部**を提供してもらう。(契約ベース)
- 高速な暗号化技術とファイルの超分散技術により, 高い**暗号強度を達成**



利点

- サーバーの運用管理費の削減, 専用線の経費問題の解消
- 世界中の, 通信端末をクライアントノードを対象とすることも可能
- 復元確率を極めて高くすることが可能

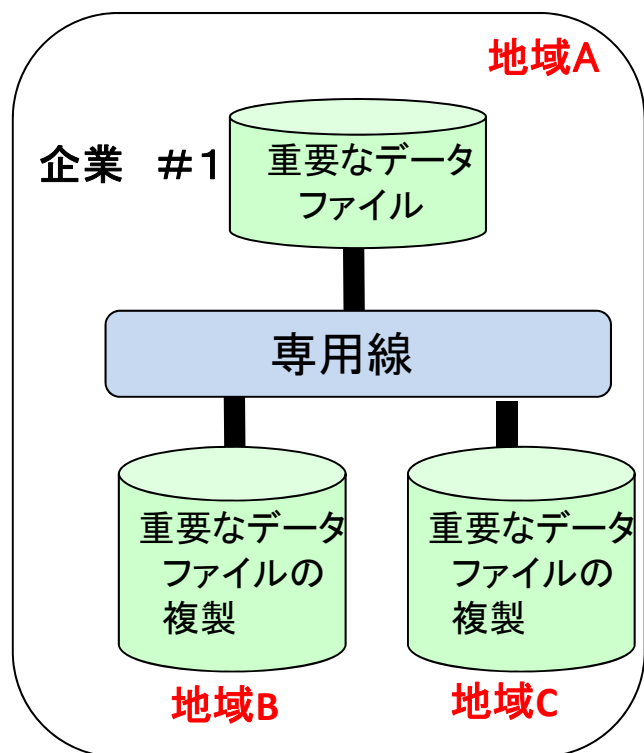


提案するディザスタリカバリシステムの概念

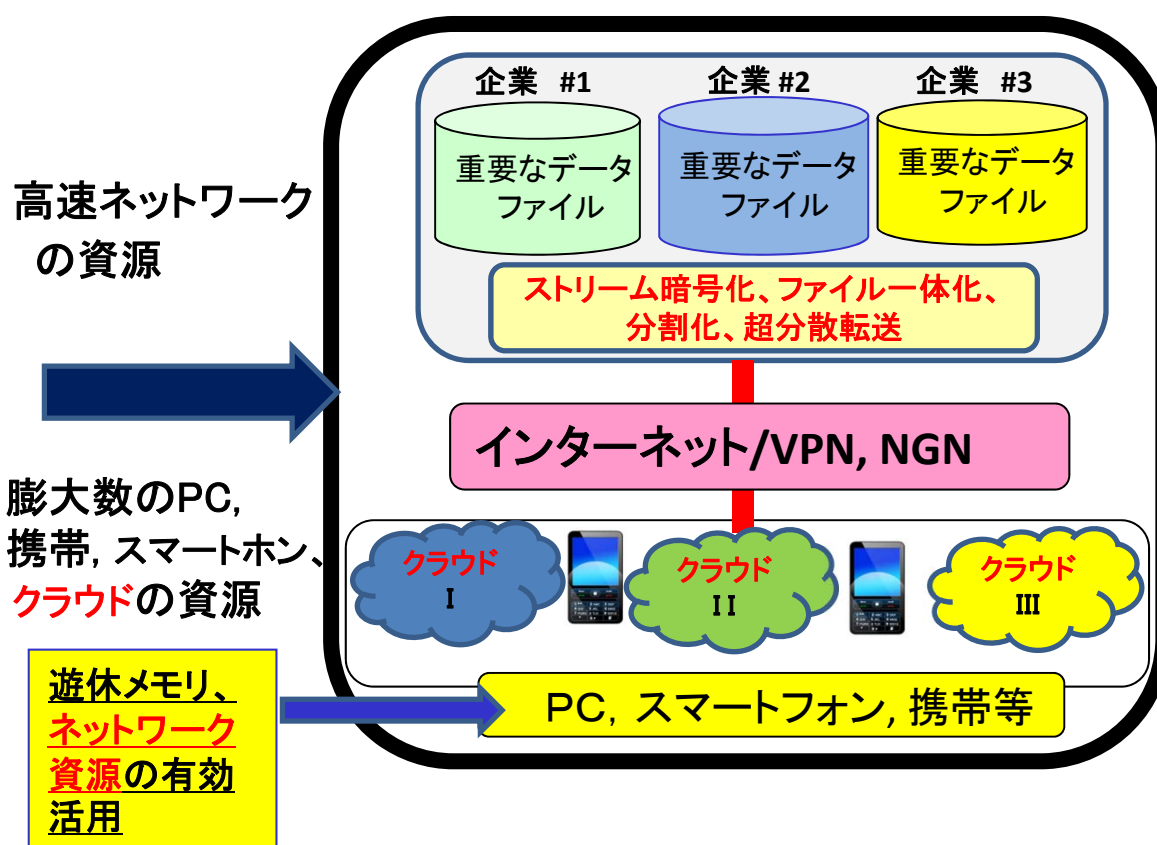
(**DRT**: **D**isaster **R**ecovery **T**echnology)

HS-DRT(**H**igh **S**ecurity-**D**istribution and **R**ake **T**echnology)

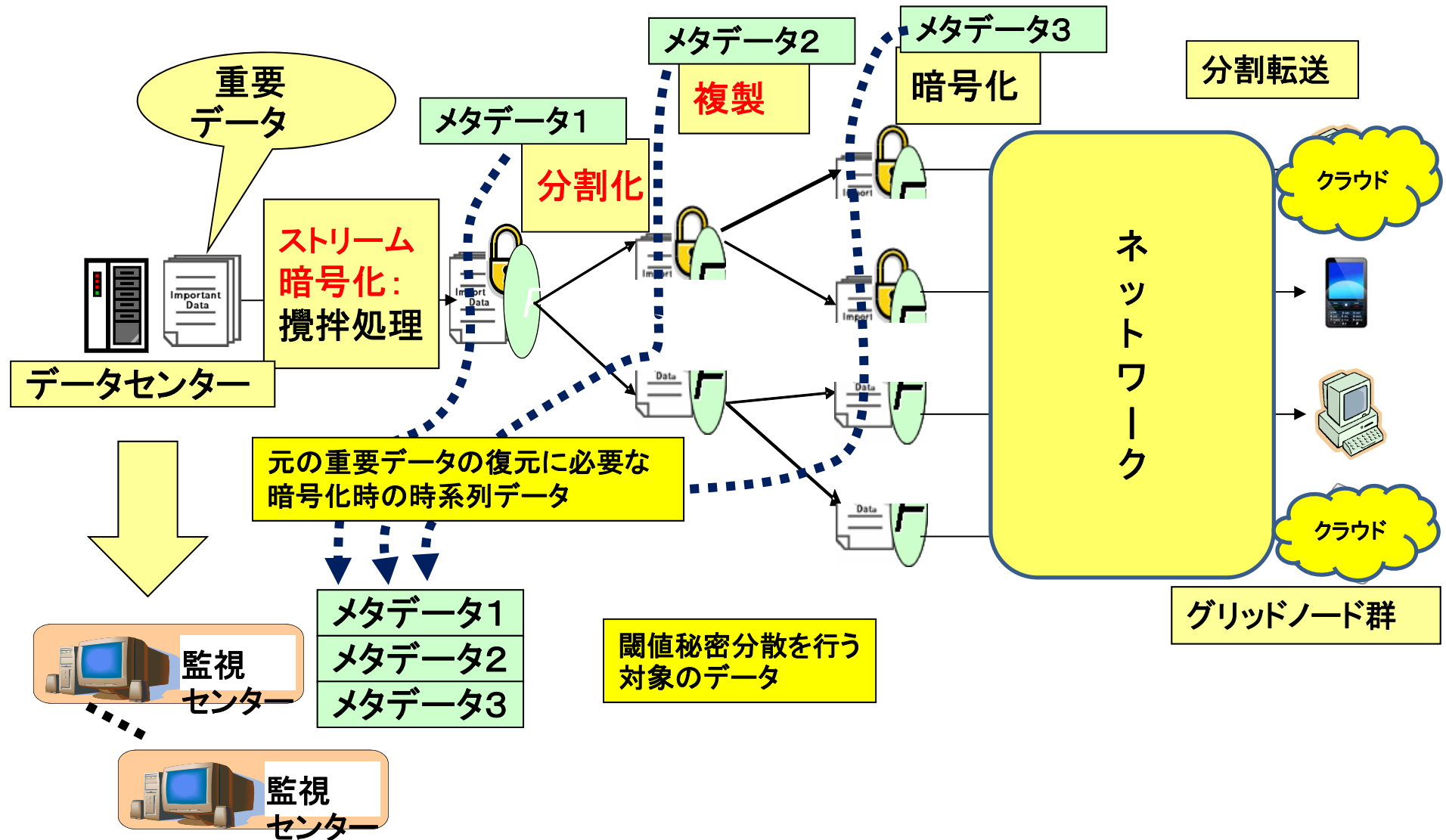
従来のバックアップシステム



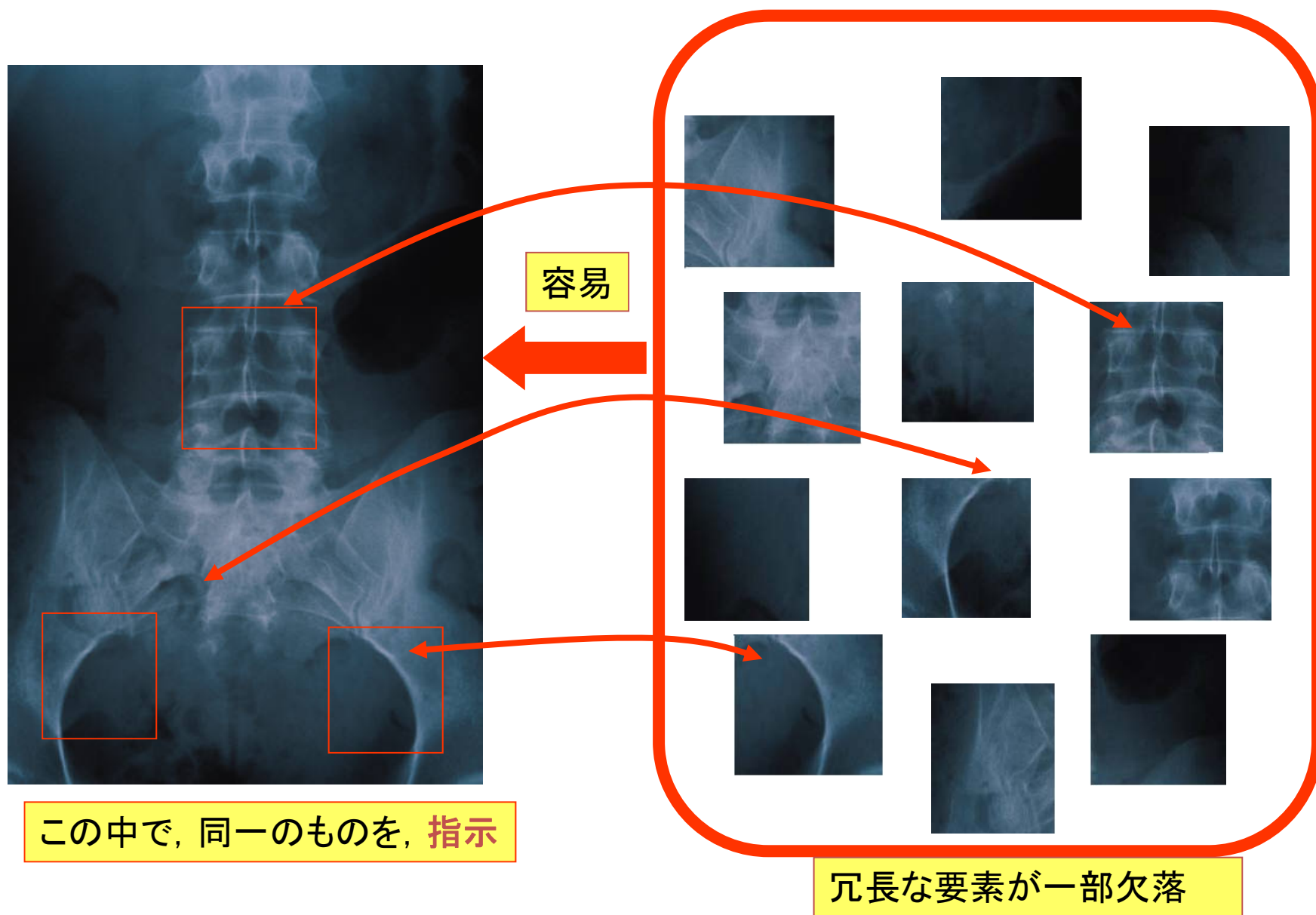
提案のバックアップシステム



技術の概要(その1)

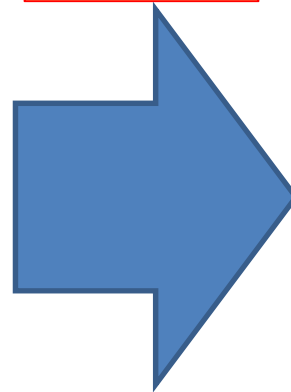


個人のレントゲン写真の単純分割の例





高速
暗号化



...//*:m 無///...	(權?*?><. ・KI+ * *
..?//M本 //?"!&?..	..?//* 便//??...?///(&
.....	%本a//..
/+*'&/*: ky///...	?//JU&/+*'&/*:
..//C :* /// ?.	J&佐(?..ky///...
////////// ..?//*	?//*.....
貼//??..//	//??.. xβ///.
////.●//////////	
..//GG///	//////////.....
中/// ?..	//////////.....///

分割写真が，正しい暗号鍵で復号に成功した場合



12!
≒5億
の組合せ

断片化数80⇒80!の組合わせ数
⇒400bitのAESと同等の暗号強度

1 ...///*:m 無///...	2 ..?///(& %本a//..	3 ..?//* 便//??..
4 (權?*?>< ・KI+ * *	5// xβ///...	6 ..?//* //??..
7 ..?//M本 //?"!&?..	8 ..//C:* 伝/// ?..	9 ..?//* 貼//??..
10 ..?//JU& J&'/(?..	11 ..//GG/// 中/// ?..	12 /+*'/&/*: ky///...

盗聴者は断片ファイルの暗号解読に成功した場合でも，成功した事が，気がつかない！

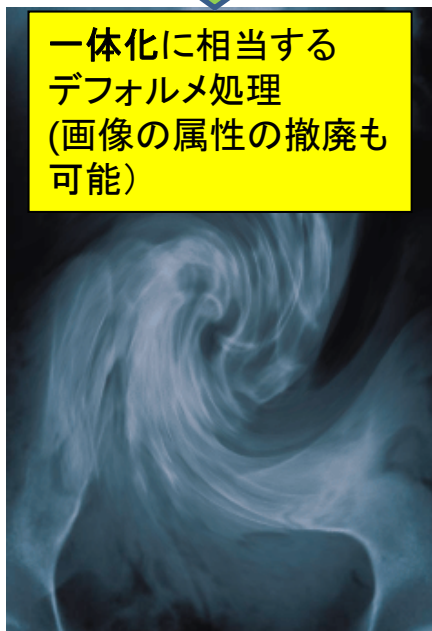
技術の概要（その2）

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

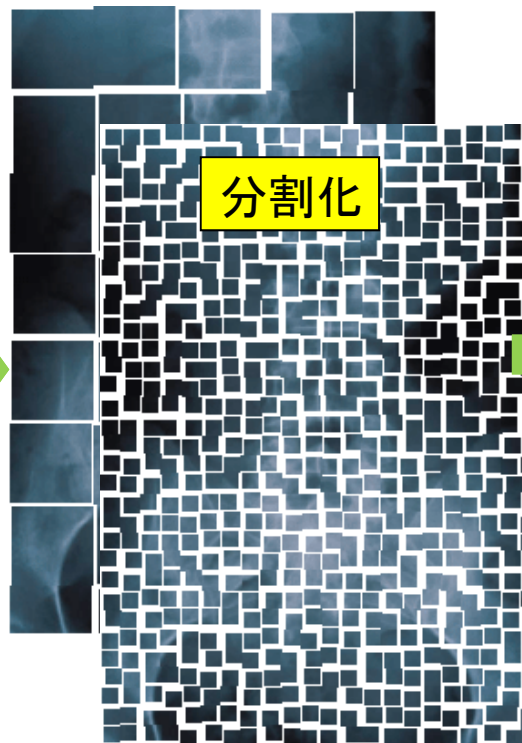


一体化に相当する
デフォルメ処理
(画像の属性の撤廃も
可能)



HS-DRTの採用

⇒ 分割化



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)



各断片
データは別鍵
で暗号
処理

⇒秘密・超分散・
別鍵で再暗号化

超分散技術を基礎としたHS-DRT

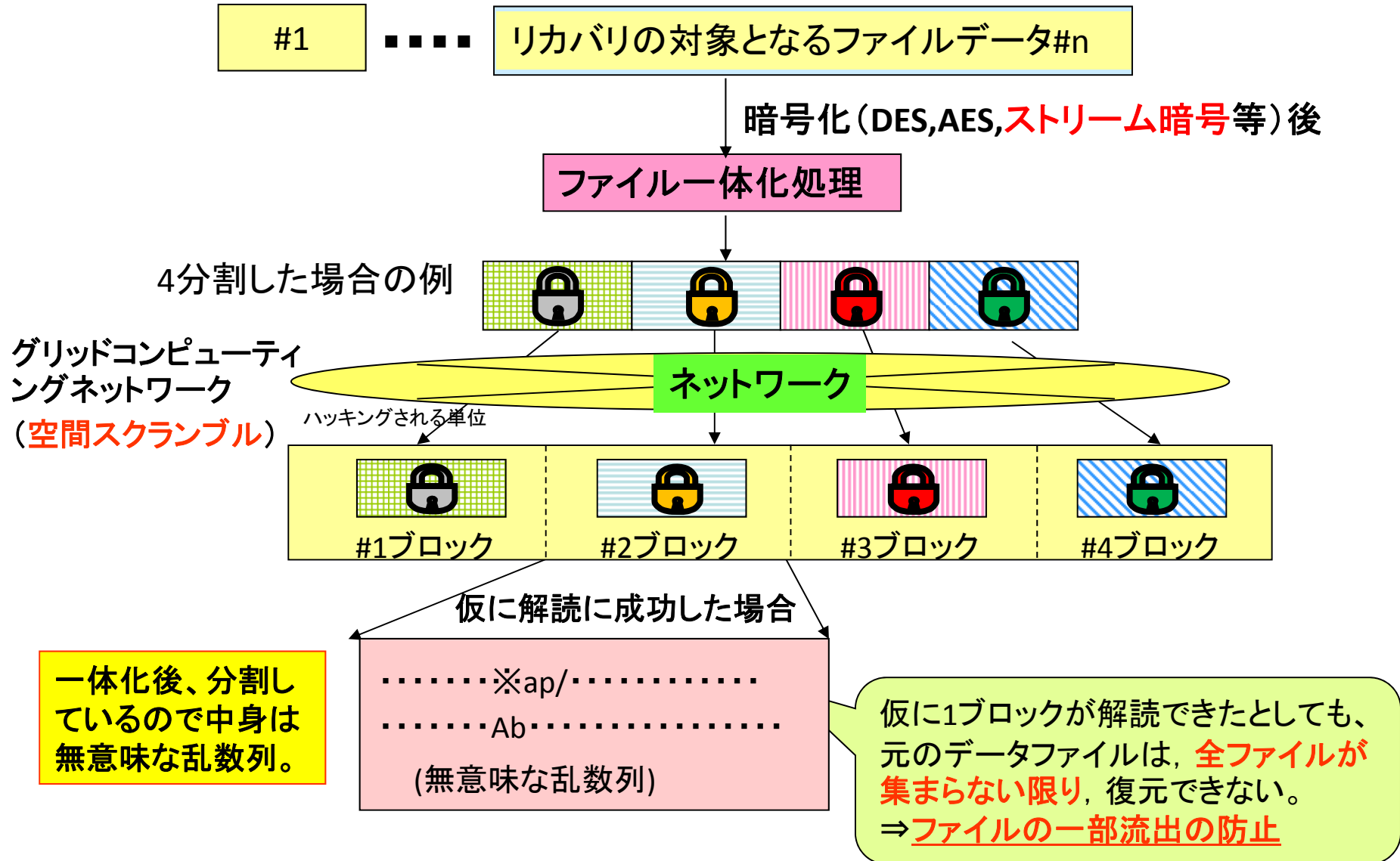
⇒新しい概念のセキュリティ 対策を提供

従来 : 一つのデータを一つの秘密鍵で暗号化
(データ変換後, 一カ所, 高々, 数か所で厳重に管理)

⇒HS-DRT: 一つまたは複数データを暗号化後,
超分割/シャッフル/再暗号化.
秘密の複数箇所に積極的に分散保管.
(⇒機密性は逆に増加したデータ管理)
⇒利用可能な通信リソースを, 任意に選択可能

技術の概要（その3）

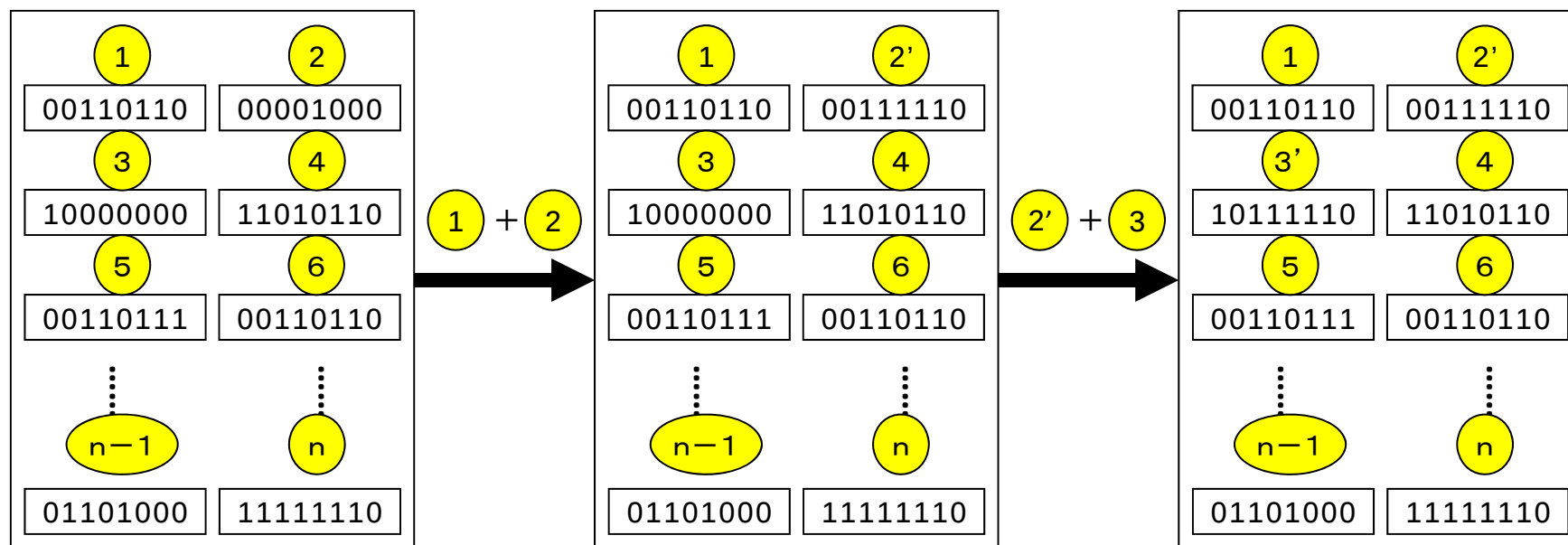
（一体化処理（ファイル攪拌）の事前導入）



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



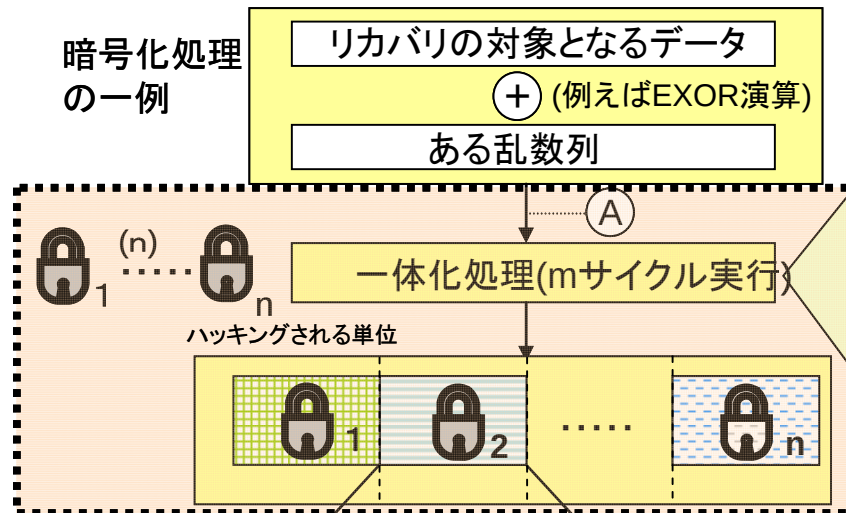
- ・暗号化対象となるファイルデータ内の隣接ワード毎に
可逆演算を実施(例えば2進加算を連続実行)
- ・ファイルの全ワード数(n)までこの処理を実行し、全ての
ワードを暗号化処理
- ・実用的には、処理ワード数や演算処理内容を適宜変更(メタデータ)

ストリーム暗号化とファイル一体化の融合

暗号化後に、一体化処理を含めて、
ファイル分割をする例

(データの空間分散化)

暗号化処理
の一例



一体化処理後、分割されたファイルの一部が、仮に、解読された場合

.....※ap/.....

.....Ab.....

(無意味な乱数列)

理由: 他のブロック情報と乱数が混入して、一体化されているので、仮に1ブロックが解読できたとしても、正解のデータファイルを回復できない。

【ポイント】

分割・配布した順番を特定できない限り、正しい情報をとりだすことは、殆ど不可能。

図面の簡略化のため、各ファイルは、例えば8ビット×nワードで表現する。(通常は32ビット×nワード構成)

(注) (#2)' は (#2) が1度一体化処理を行われ、データが暗号化された状態を示す。

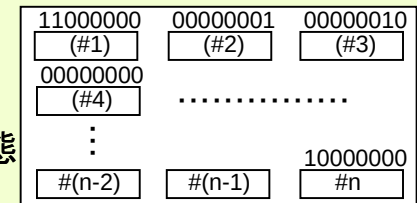
データ拡散
暗号化されたワード内容

一体化処理の1サイクル

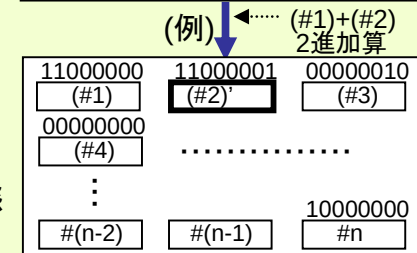
Mサイクル
実行する
(m>6が望ましい)

A ~ E により、1 ⇒ 全てのワードが暗号化処理が完成

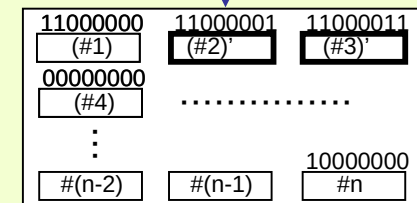
A
の状態



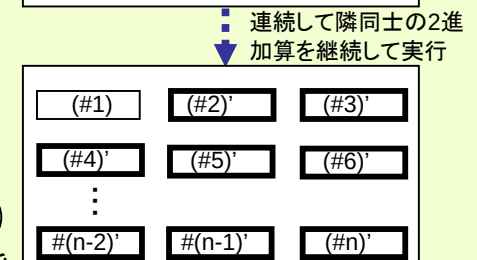
A から、
一体化処理
に関わる初
めの処理: B
の状態



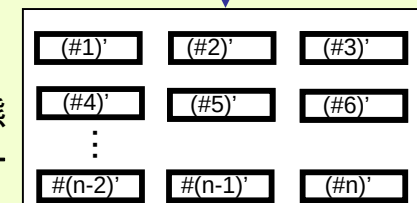
B から
一体化処理
に関わる2回
目の処理: C
の状態



C から以後
の、一体化処理
に関わる(最終
処理-1) までの
処理: D
の状態



E
の状態



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わせ= $20! \div 2^{61} \div 10^{18}$

この組み合わせ数は、DES (54ビット)暗号以上の安全性をもつ

② 分割数が40の場合

ファイルの並べ方の組み合わせ= $40! \div 2^{160} \div 10^{47}$

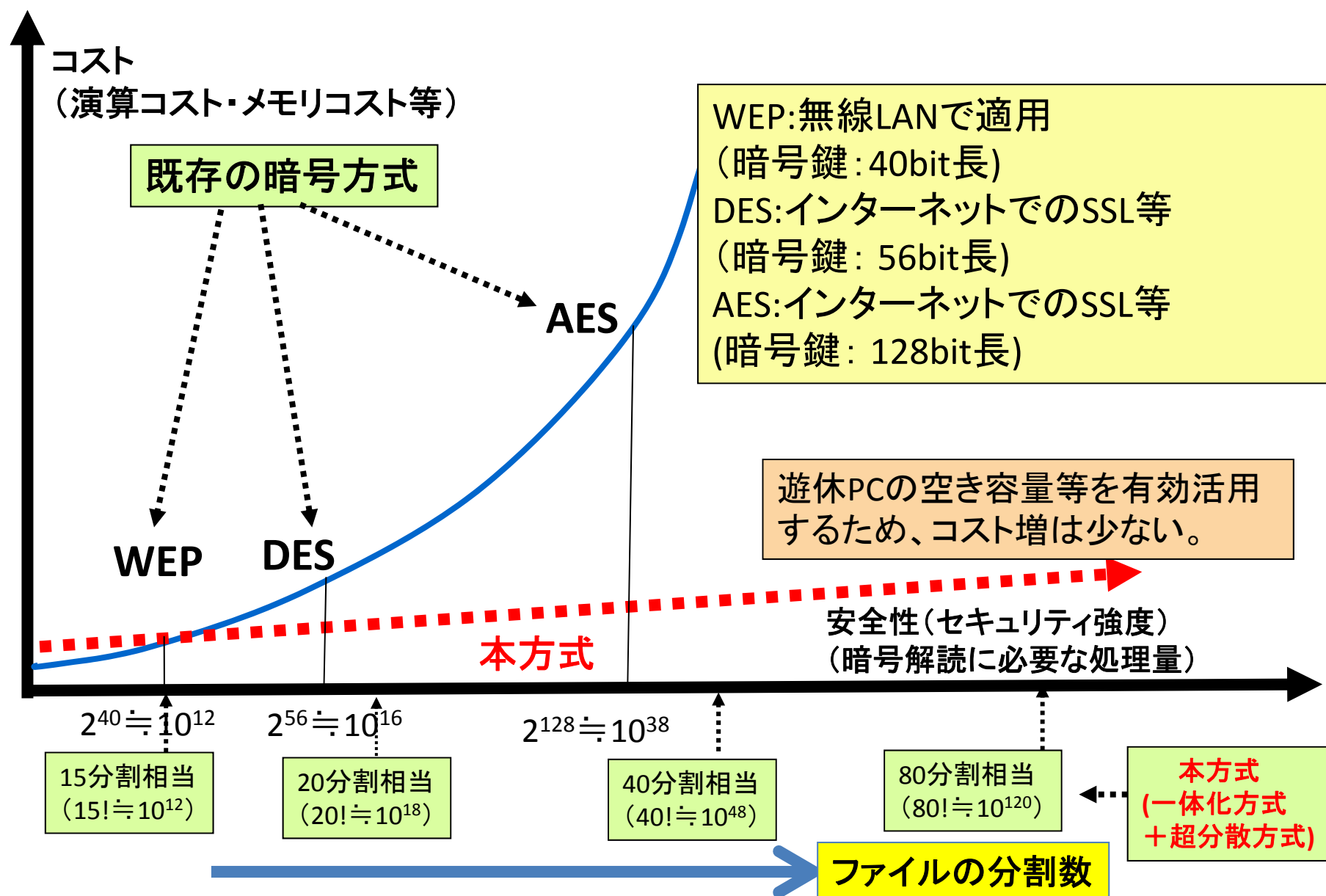
この組み合わせ数は、AES (128ビット) 暗号以上の安全性をもつ

③ 分割数が80 の場合

ファイルの並べ方の組み合わせ= $80! \div 2^{400} \div 10^{120}$

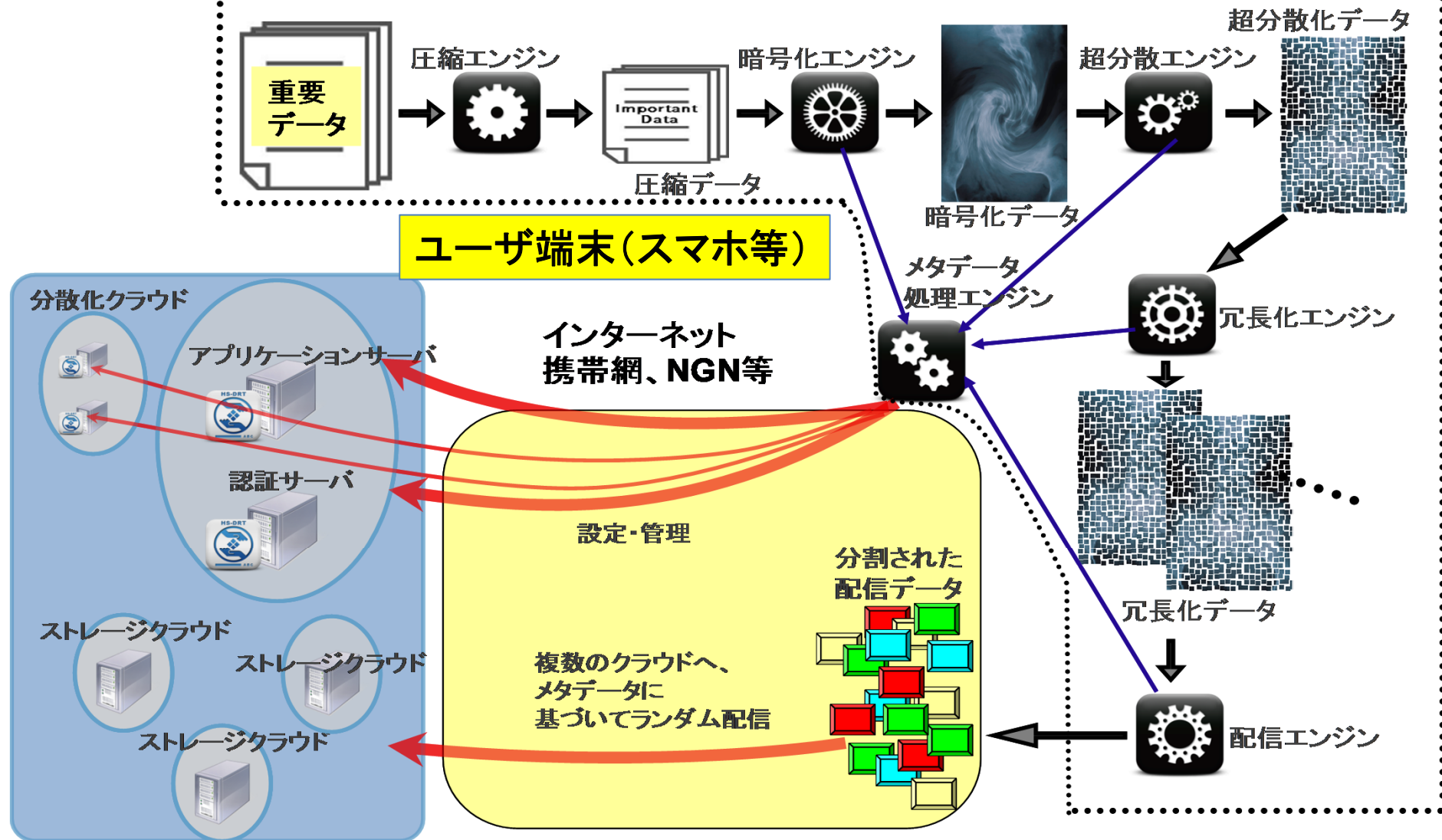
この組み合わせ数は、400ビット暗号の安全性をもつことと等価であり、このレベルに匹敵する安全性をもつ暗号は、まだ、実用化されていない。

従来のブロック暗号方式との定性的な比較



HS-DRTエンジンの実装例

事業者内、ユーザ宅に実装する場合のクラウドアクセス用エンジン群の構成例



対外的な主な成果

- (1) ソフトピアジャパン委託研究
- (2) JST(文科省)の競争的研究資金課題採用
- (3) 科研費(基盤研究C)課題採用
- (4) NICT(高機能光電子融合型パケットルータ基盤技術の研究)
- (5) HS-DRT 関連の特許出願7件(登録3件)
- (6) 国際会議 IARIA/ICSNC2009, 2010で二年連続

Best Paper Award受賞

- (7) 2010年6月～2013年6月まで展示会出展(審査・採択)
 - ① WTP2010～WTP2013(ベストプレゼン受賞)
 - ② イノベーションジャパン2011～2013(大学見本市)
⇒ オーム社のインタビュー: 雑誌「OHM」に掲載
- (8) 学術振興基金発明賞受賞(2013.2)
- (9) 電子情報通信学会より招待論文(2013.10予定)

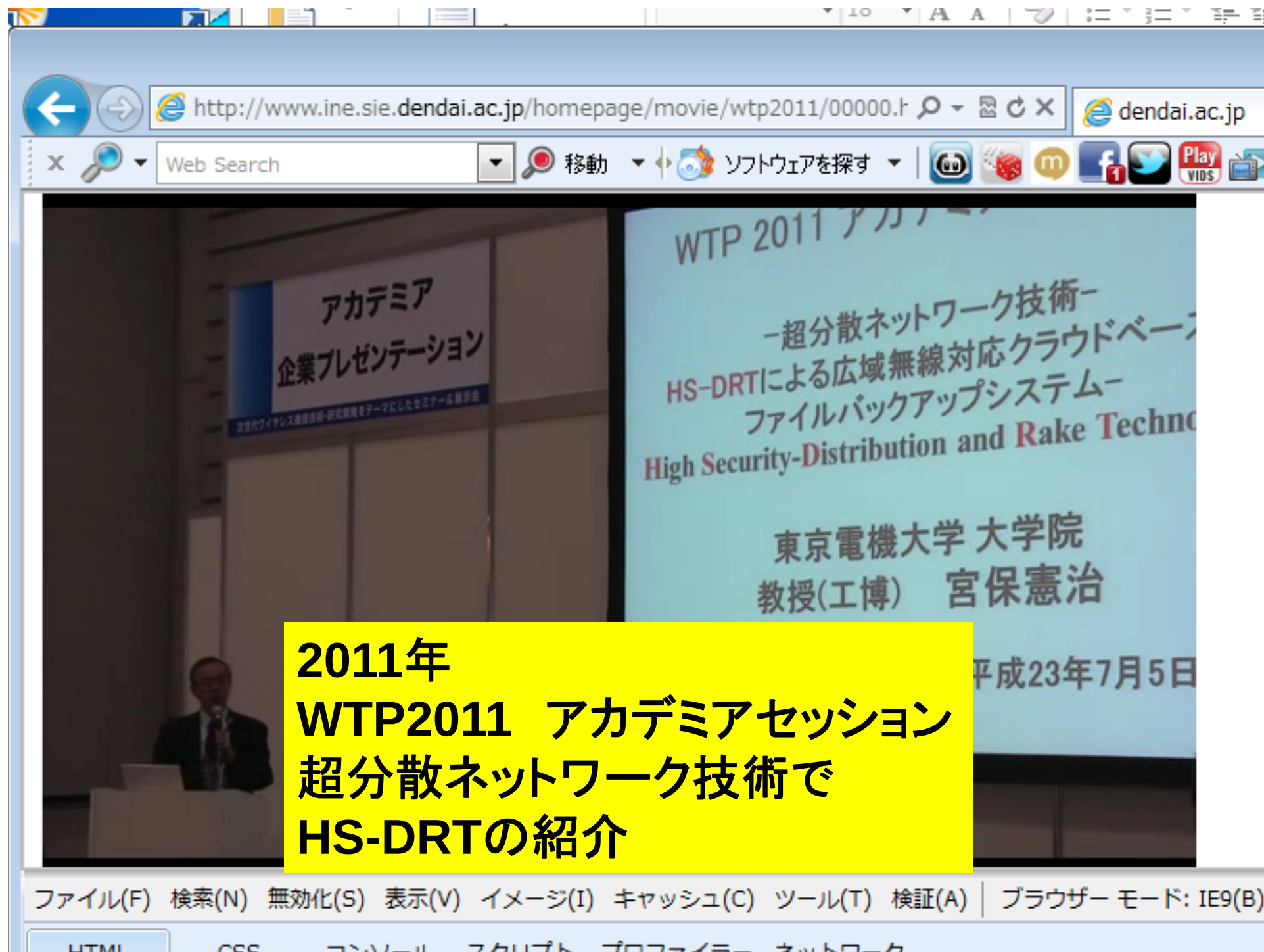


**2010年 12月NTTコミュニケーションズラボ
との共同実験開始
NTTCommunications のクラウドを
活用し、アマゾン、Googleとの性能評価を実施**

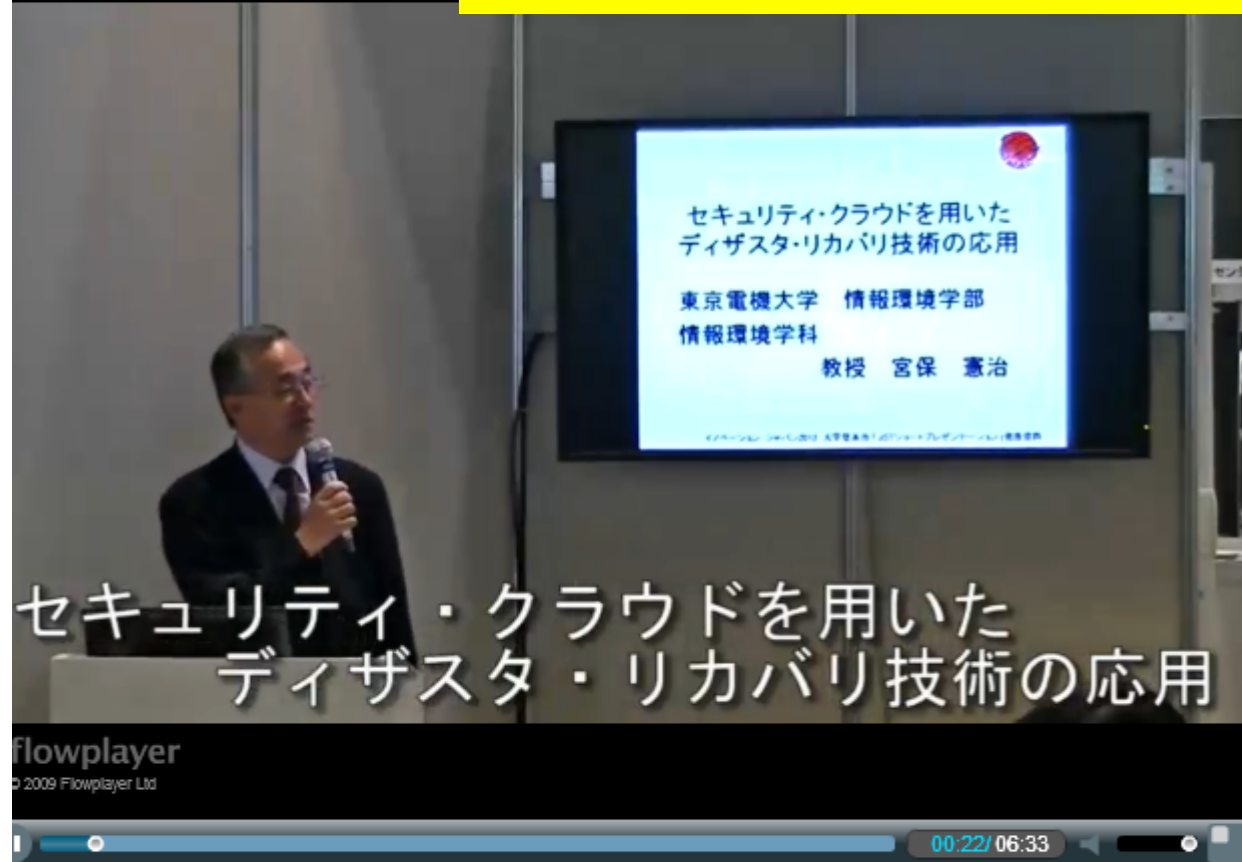
**2010年10月 イノベーションジャパン2010
上野洋一郎教授の発表**

**超分散ネットワークを用いた
安心・安全なディザスタリカバリ技術**

00:11 / 01:46



2012 年11月の
イノベーションジャパン大学見本市



Tokyo Denki University, School of Information Environment

HS-DRTによる広域無線対応クラウド ベース・ファイルバックアップシステム High Security - Distribution and Rake Technology

東京電機大学 情報環境学部/大学院 情報ネットワーク環境研究室
<http://www.ine.sie.dendai.ac.jp/homepage/>

○遠藤祐輔 永木佳人 鈴木勇人 高野広之 山下祐生 宮保憲治

於 パシフィコ横浜 平成24年7月6日

ワイヤレス・
テクノロジー・パーク
2012

Wireless Technology Park 2012

2012年ワイヤレステクノロジーパーク
アカデミックセッション

ベストプレゼンテーション賞受賞

宮保研 遠藤君(院1)

flowplayer

© 2009 Flowplayer Ltd

2013 年 WTP2013 展示説明ブース (東京ビッグサイト)



HS-DRT技術のもう一つの側面

⇒ファイルの回収確率の評価

超分散と複製を組み合わせた
メカニズムの評価

スマホ,PCを用いる場合と
クラウドを用いる場合の比較

ファイルの回復確率の算出法

p: 断片化ファイル(分散端末)の故障率

ファイル一体化後の
元のファイルデータ

“n:”複製数

複製化された
ファイルデータ

(ex): $p=1/5$

“m”
断片化数

1_1	1_2	1_3	1_4
2_1	2_2	2_3	2_4
3_1	3_2	3_3	3_4
4_1	4_2	4_3	4_4

(例) 条件: $p=1/5$

1つの断片化ファイルに着目した時、全ての複製ファイルが回収できない確率
 $= (p)^n = (1/5)^n$

複製された断片化ファイルの中で、少なくとも1つのファイルが正常に回収できる確率を計算することにより、元のデータファイル回復確率が計算可能

ファイル回復確率

$$= \{1 - (P)^n\}^m$$

例: m (断片化ファイル数) = 4, n (複製数) = 4

データの分割・複製の効果

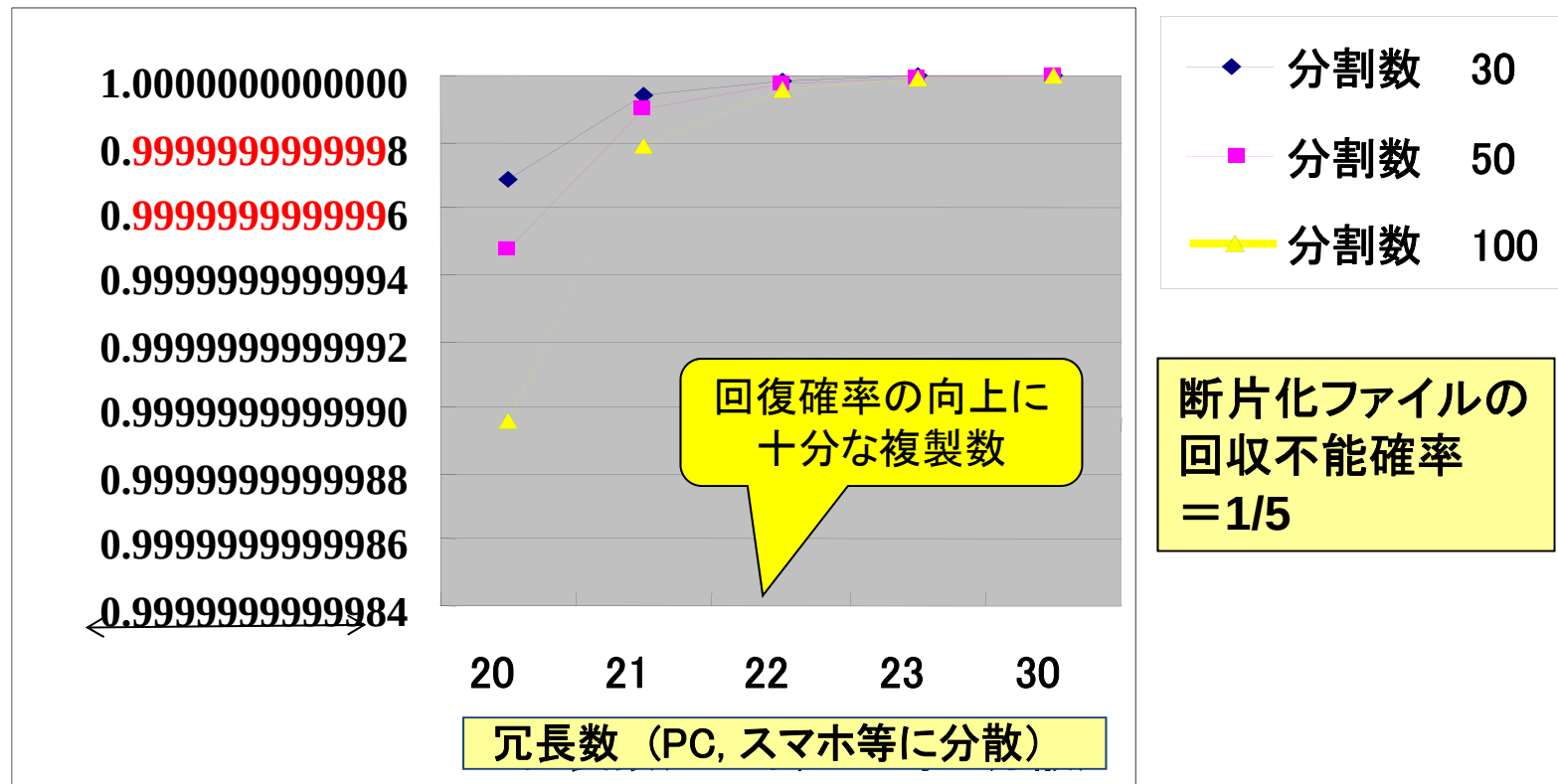
$$\text{回復率} = (1 - P^n)^m \doteq 1 - mP^n$$

(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

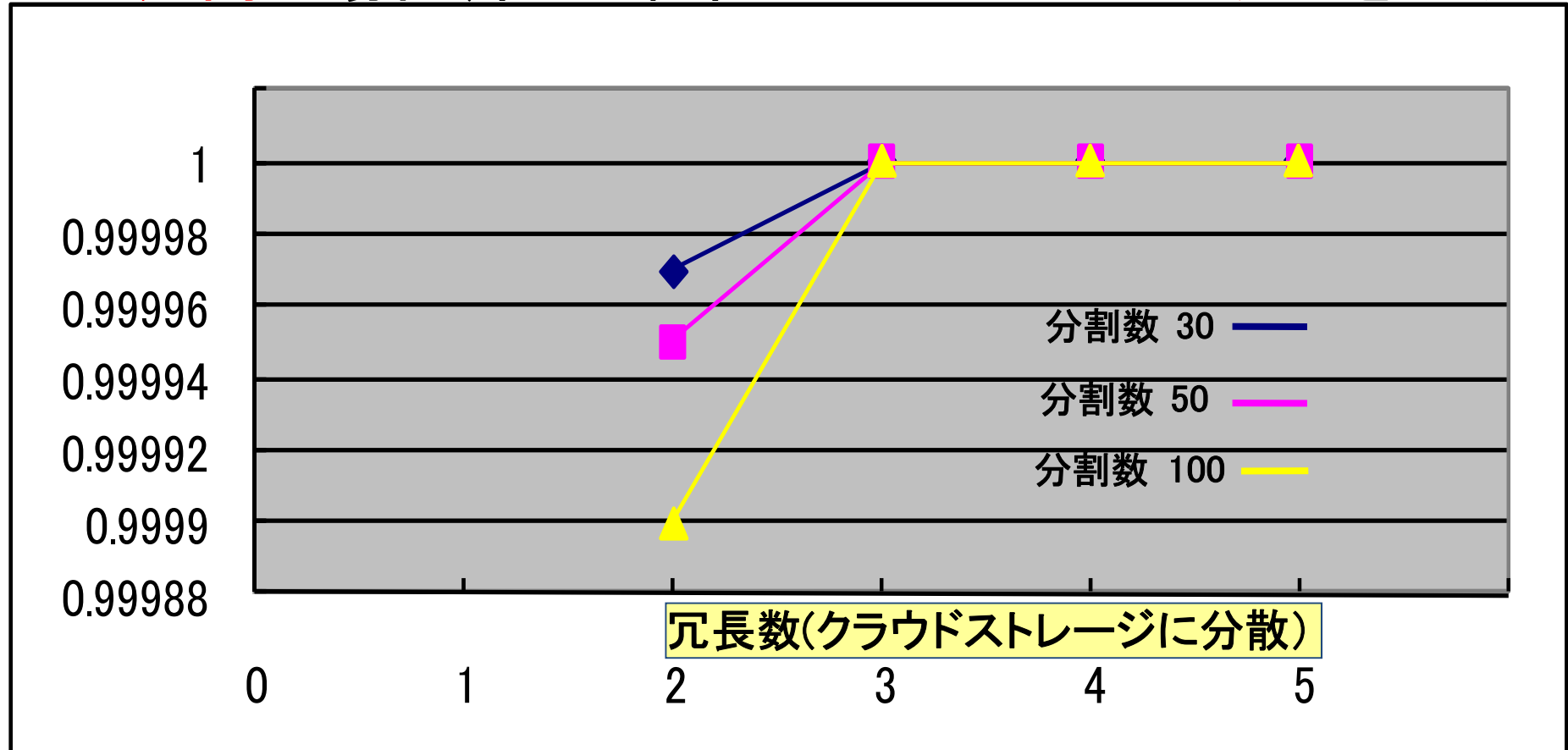
ファイル回復確率の算出例(1)



ファイル回復確率の算出例(2)

クラウドストレージ**4台以上**の時、

100分割の場合、回収確率は**0.999999999999**以上を達成



クラウドストレージの可用性については、**現在99.95%以上の稼働率**が達成されている状況に鑑み、安全側に見積もって、 **$P=1/1000$** を仮定。

HS-DRT技術

- (1) ファイル暗号化時の演算種別は、XOR演算に限らず、2進の加減算等、可逆演算が可能な演算種別であれば、何でも良く、自由に組み合わせ可能。**AES**も使用可能。
- (2) ストリーム暗号の処理遅延時間は短く、**リアルタイム**での高速暗号化・復号化を実現。
- (3) 安全・高速な暗号方式として甦らせる**キー技術**

[**高速**暗号化]+[**任意分割**]+[**シャフリング**化]+[分割片の**再暗号化**]+[異なる複製キー]+[**不特定地域**への**超分散**]
一連の処理の**組み合わせ**手法を**時系列的**に実現。

現状のクラウドにおける3つの課題と対策

①セキュリティ ②可用性 ③堅牢性(完全性)

①セキュリティ

⇒全ての断片ファイルを集めない限り、復号化は不可能
異種クラウドとの連携⇒クラウドの、セキュリティ上の課題を解決

②可用性: 99.999……% ?

ハードウェア・システム単独で、完璧な可用性を実現するのは困難。

⇒HS-DRTの特徴⇒自由に、複製数の設定が可能

(クラウドを4つ以上、組み合わせ使用⇒可用性の飛躍的向上)

クラウドの課題(つづき)

③ 堅牢性

ストレージクラウド自体が堅牢に、運用されていても、局地的な災害時に備えた、地理的な分散による二重化は、一般には、保証されていない。

⇒ **HS-DRT**では、広域(地理的)に分散された、

(a) 複数のストレージクラウドへ分散保管を行うことができ、

(b) 地理的な冗長度を自由に設定できる。

⇒ 万が一のデータ損失にも、備えることが可能。

クラウドの課題⇒事業継続性

ストレージクラウドを提供するサービスプロバイダの事業が停止してしまう事態が生じた場合の対処方法は？

→ より多くの(世界に跨る)複数のストレージクラウドを利用することにより、特定のサービスプロバイダが停止しても影響なくサービスを継続できる。

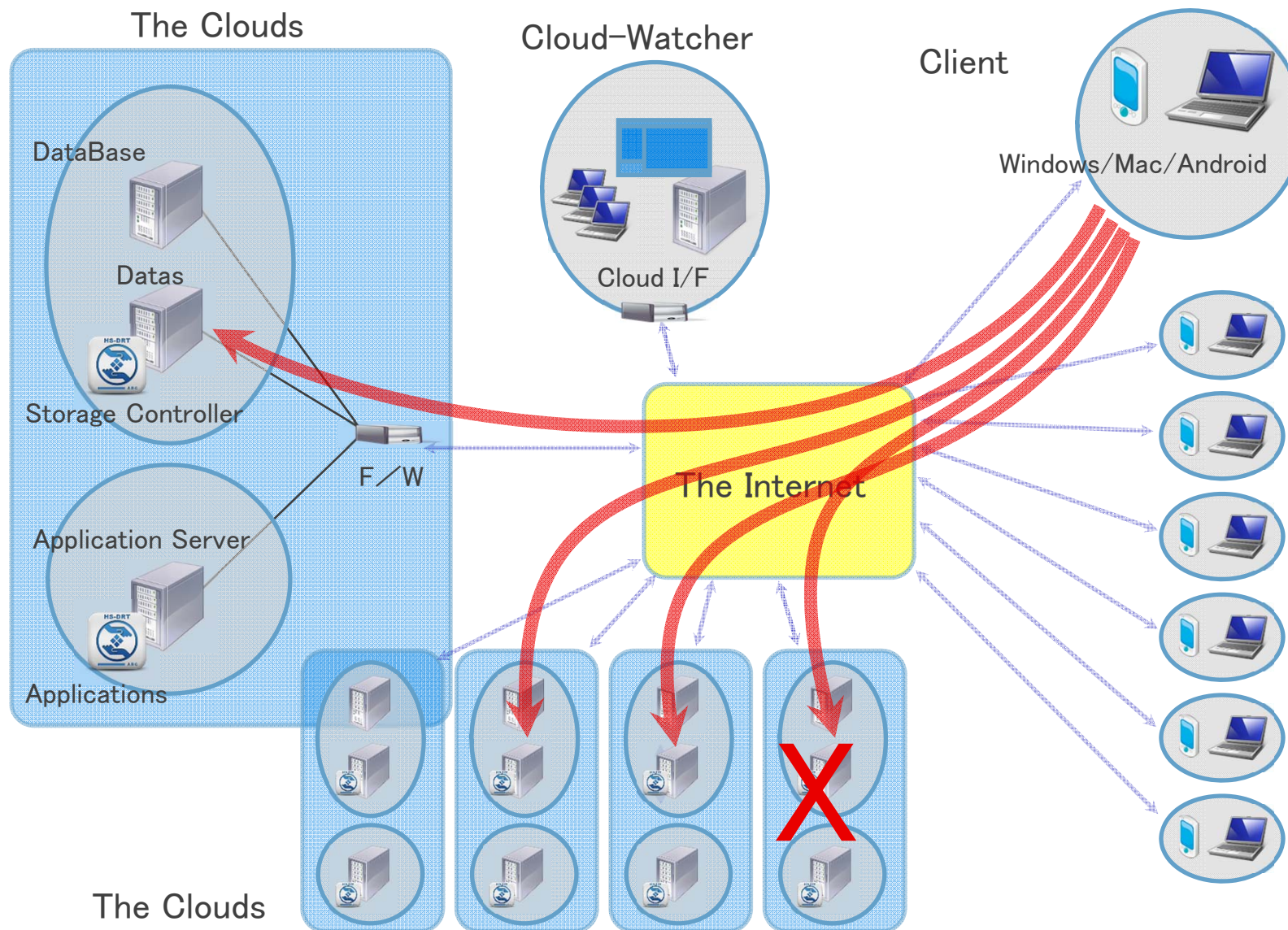
→ 特定のサービスプロバイダの事業継続性に影響されない



異質なクラウドを組み合わせるほど、信頼性が高まる性質を積極的に活用

HS-DRT基本動作

超分散ストレージ技術
HS-DRT
High Security Distribution and Rake Technology



クラウドは大丈夫なのか？

超分散ストレージ技術
HS-DRT
High Security Distribution and Rake Technology

可用性

完全性

いつでもOK？

壊れない？

コロンブスの卵で一気に解決
@Cloud

Cloud-base EZ Service Systems

超分散ストレージ技術
HS-DRT

高くない？

セキュリティ？

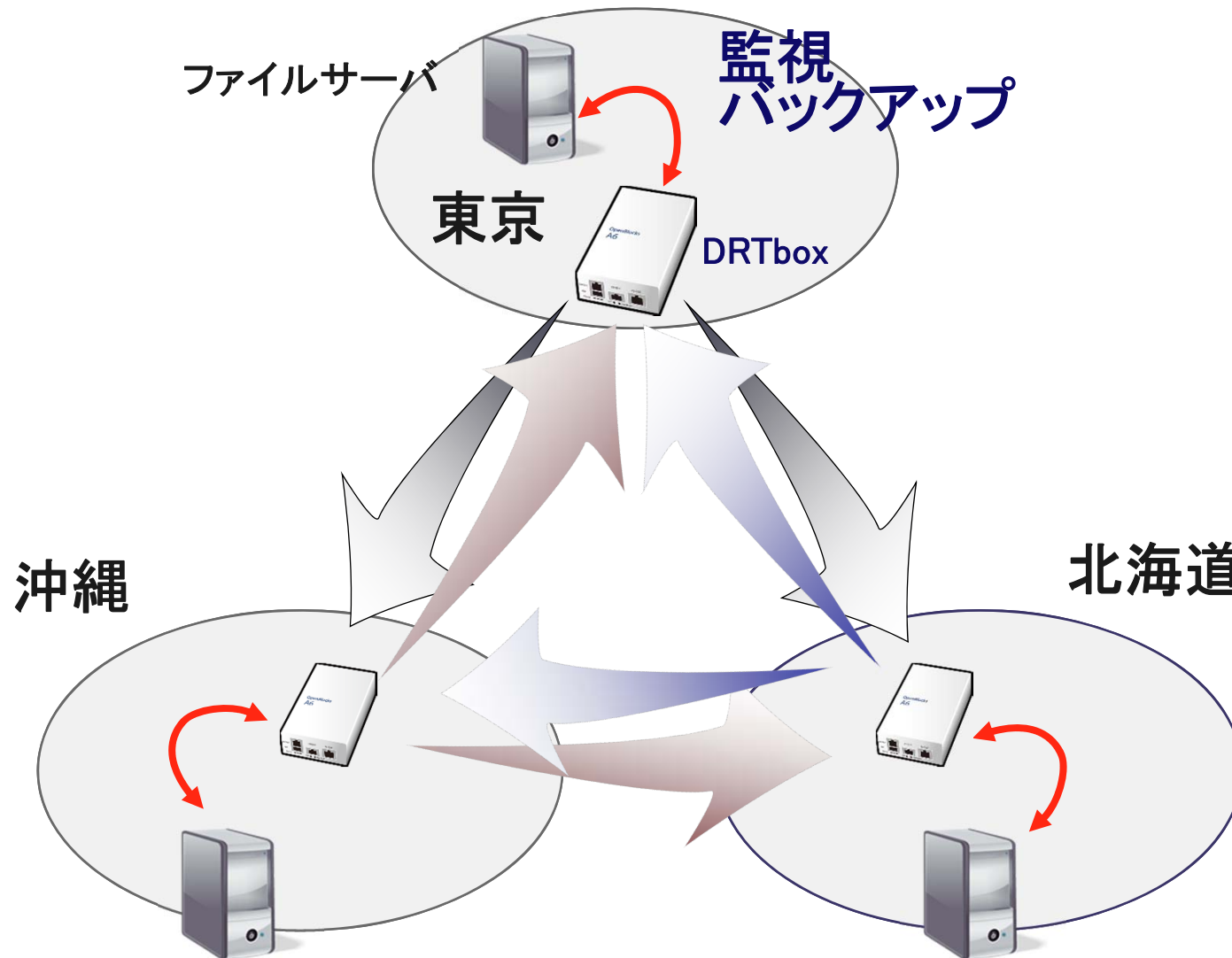
コスト High Security Distribution and Rake Technology 機密性

HS-DRTとクラウドを用いたバックアップの特長

	@Cloud-DRTbackup	無償オンライン ストレージ	市販バック アップソフト	プライベート クラウド
信頼性	☆	△	△	◎
耐障害性	☆	○～X	△	○
設置性	◎	☆	◎	X
コスト	○	☆	◎	X
拡張性	◎	△～X	△	◎

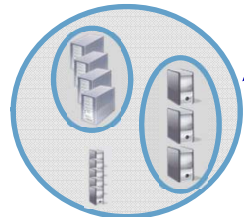
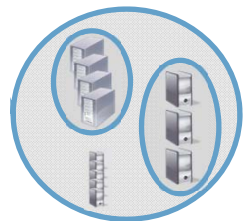
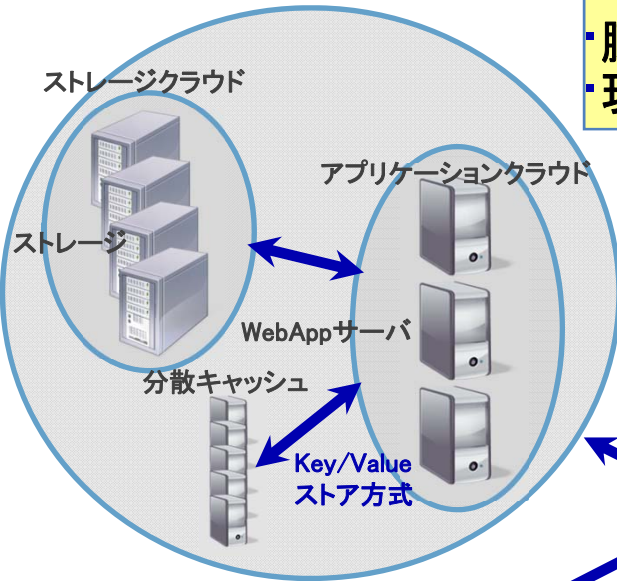
超分散HS-DRTの適用例

超分散ストレージ技術
HS-DRT
High Security Distribution and Rake Technology



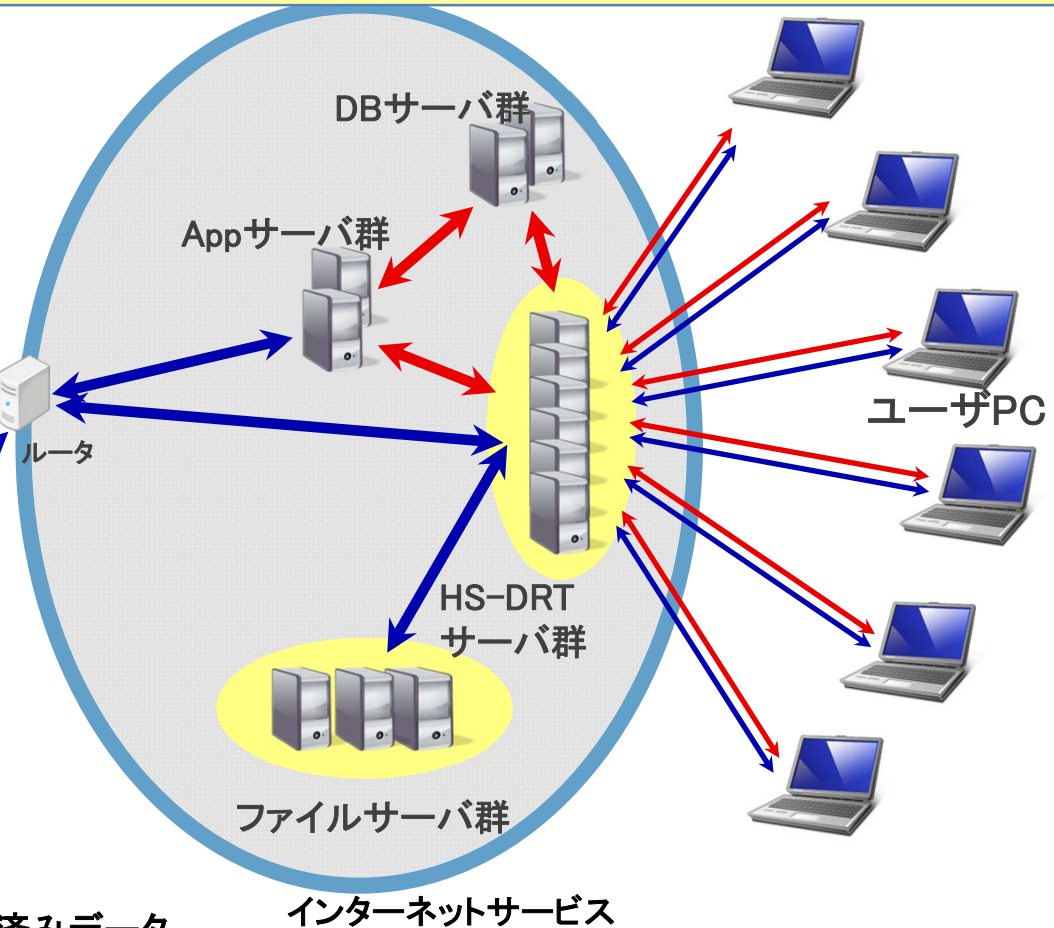
クラウド対応のHS-DRT技術の実用化

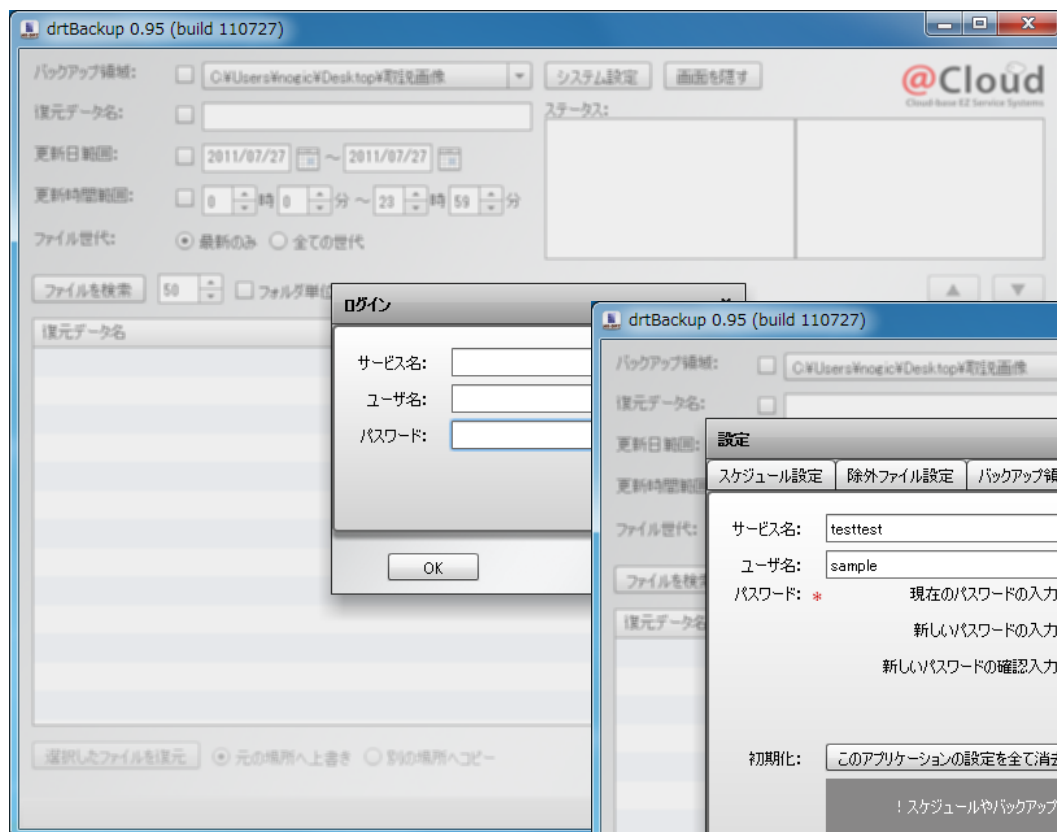
各種ストレージサービス



↔ HS-DRT処理済みデータ
↔ 生データ

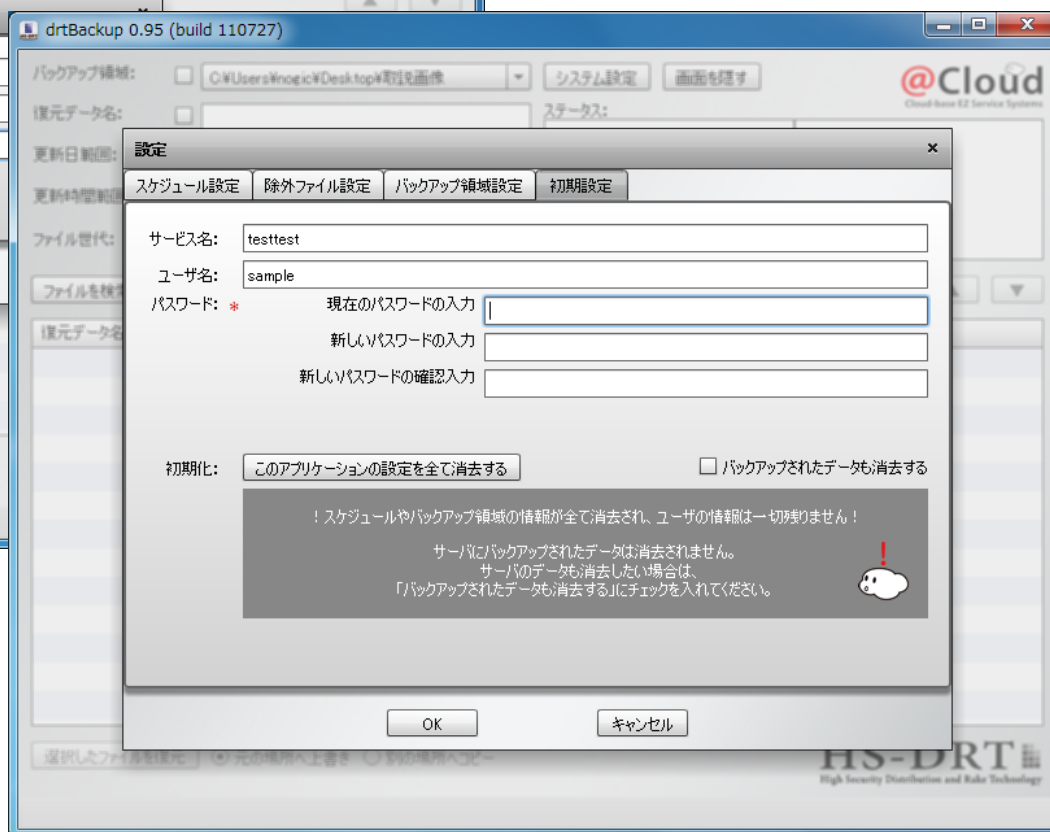
- Webアプリケーション群と連携し、バックエンドに、外部のストレージを[ファイル金庫]として利用。
- 膨大なデータの保管は、廉価な クラウドシステムを利用
- 現在, 「DRT Backup」として、商用化

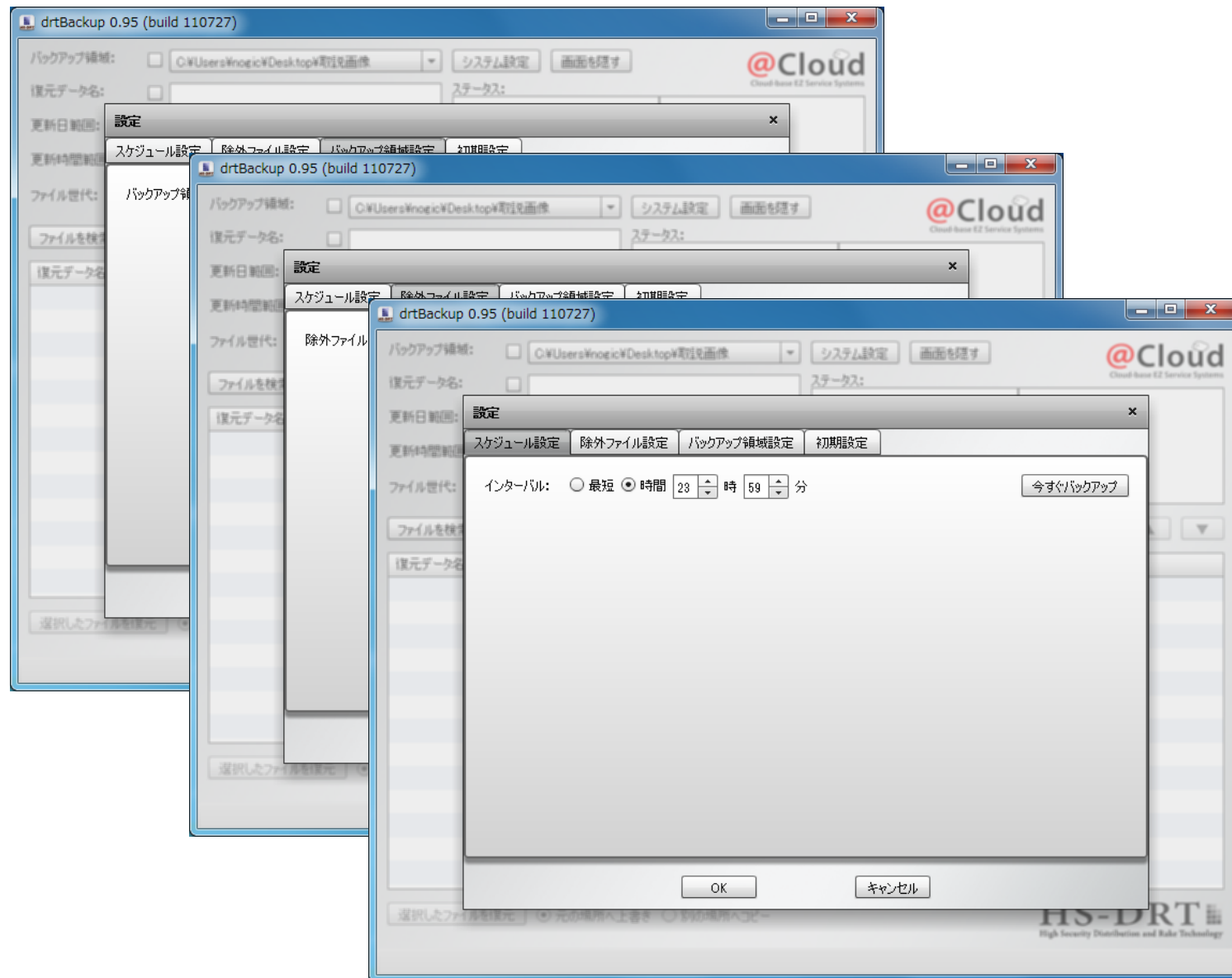




ログイン

僅かな初期設定

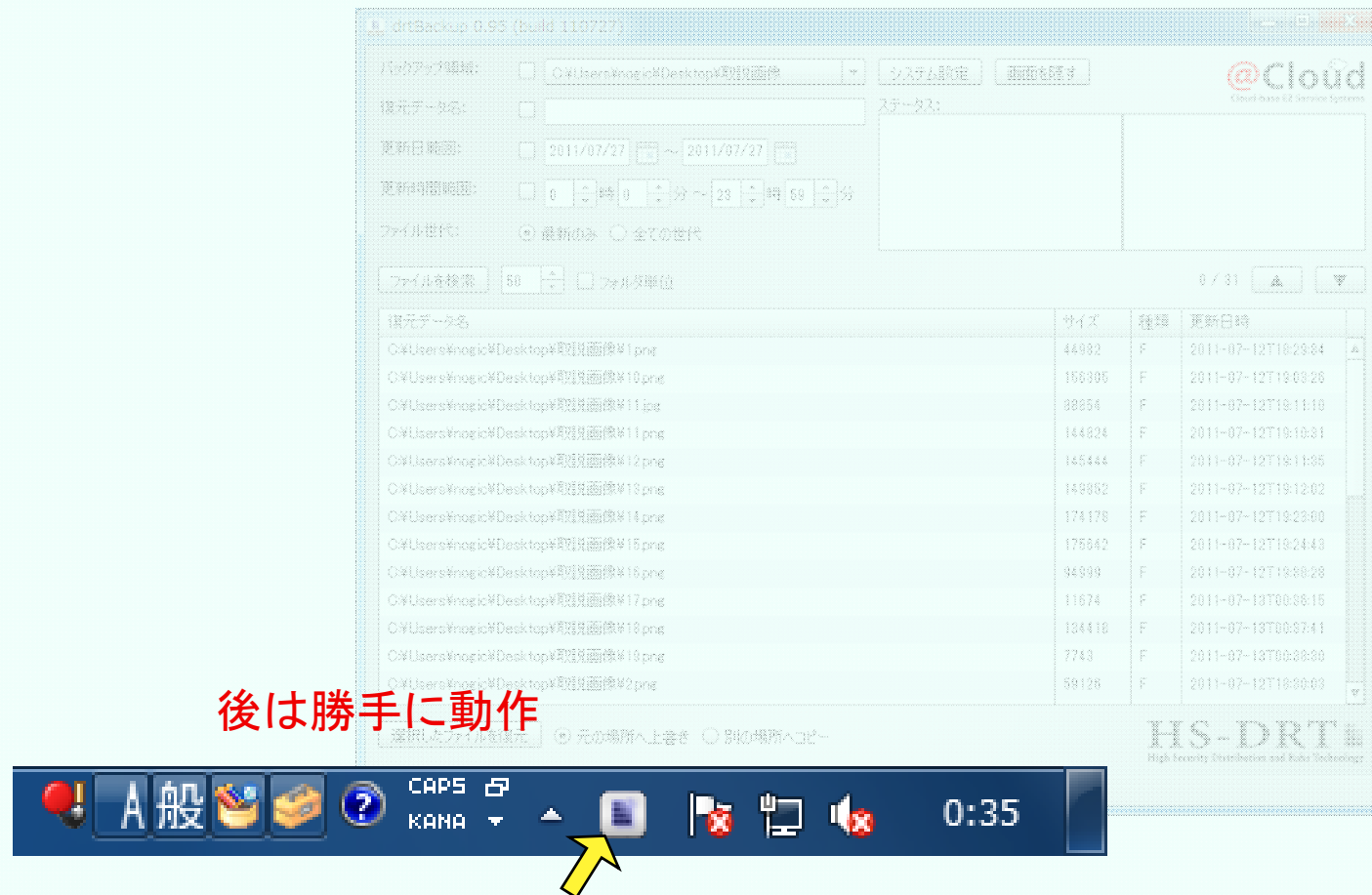




復元もファイル単位、フォルダ単位で可能
ダブルクリックで元の場所、違う場所へ



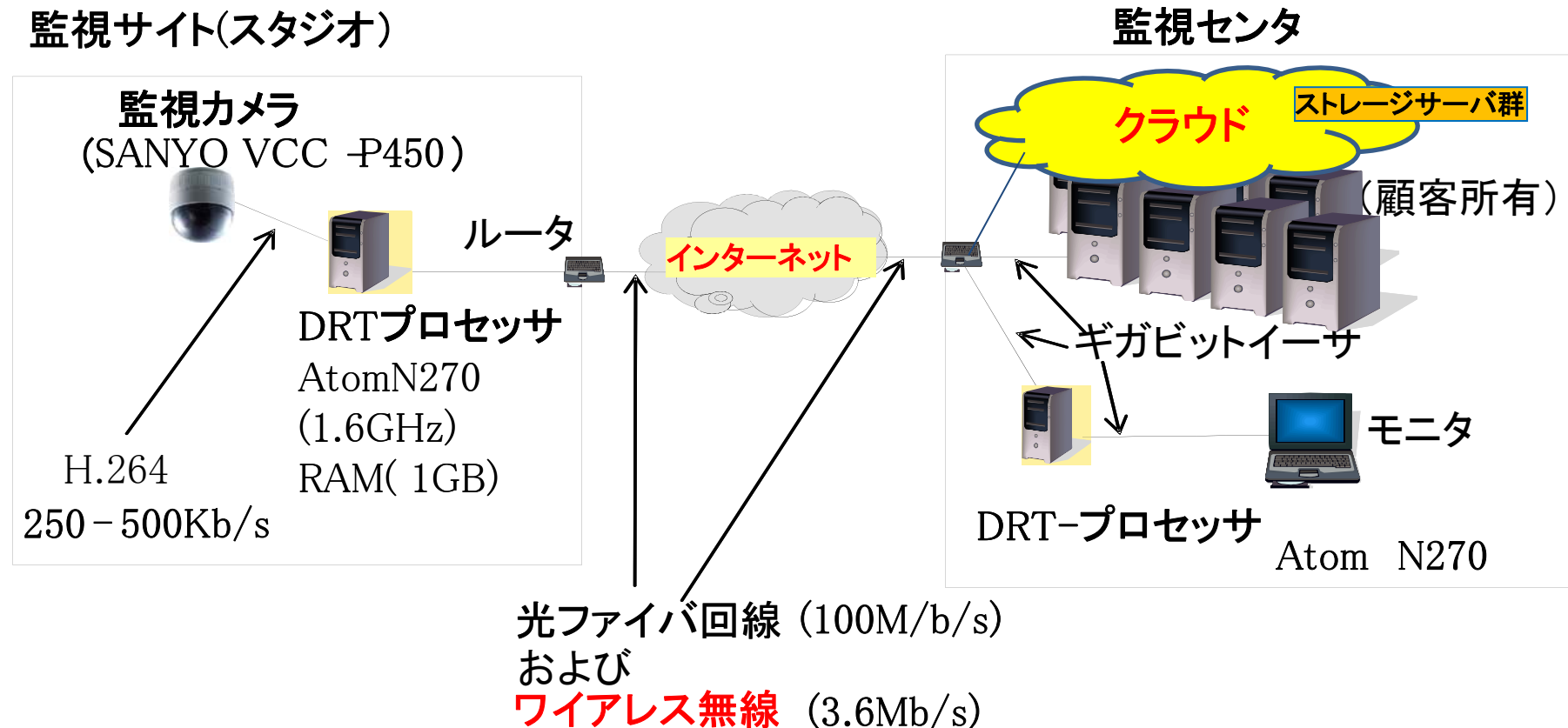
復元もファイル単位、フォルダ単位で可能
ダブルクリックで元の場所、違う場所へ



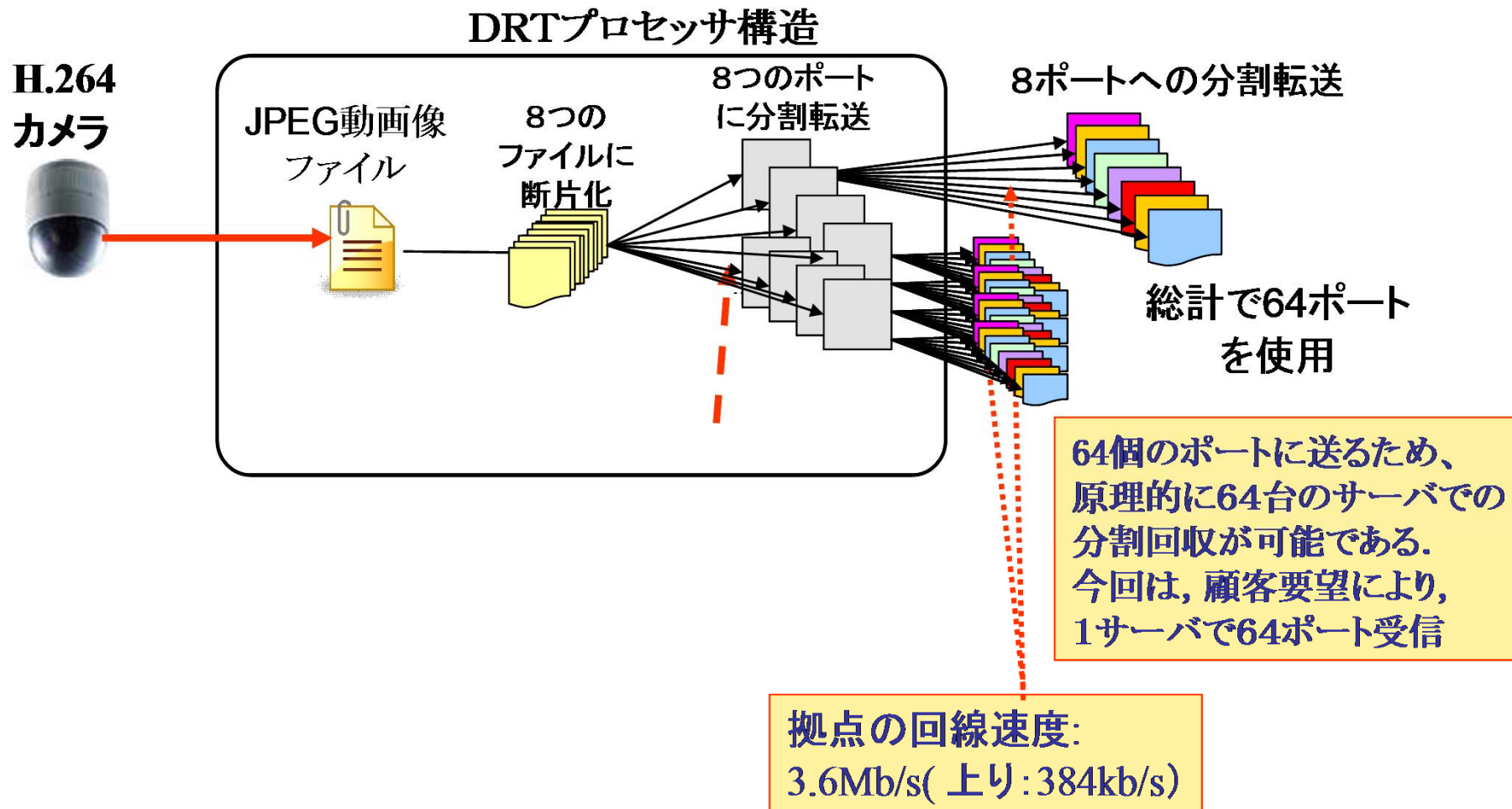
後は勝手に動作

HS-DRTを応用した映像伝送システムの例

動画映像の秘密分散伝送

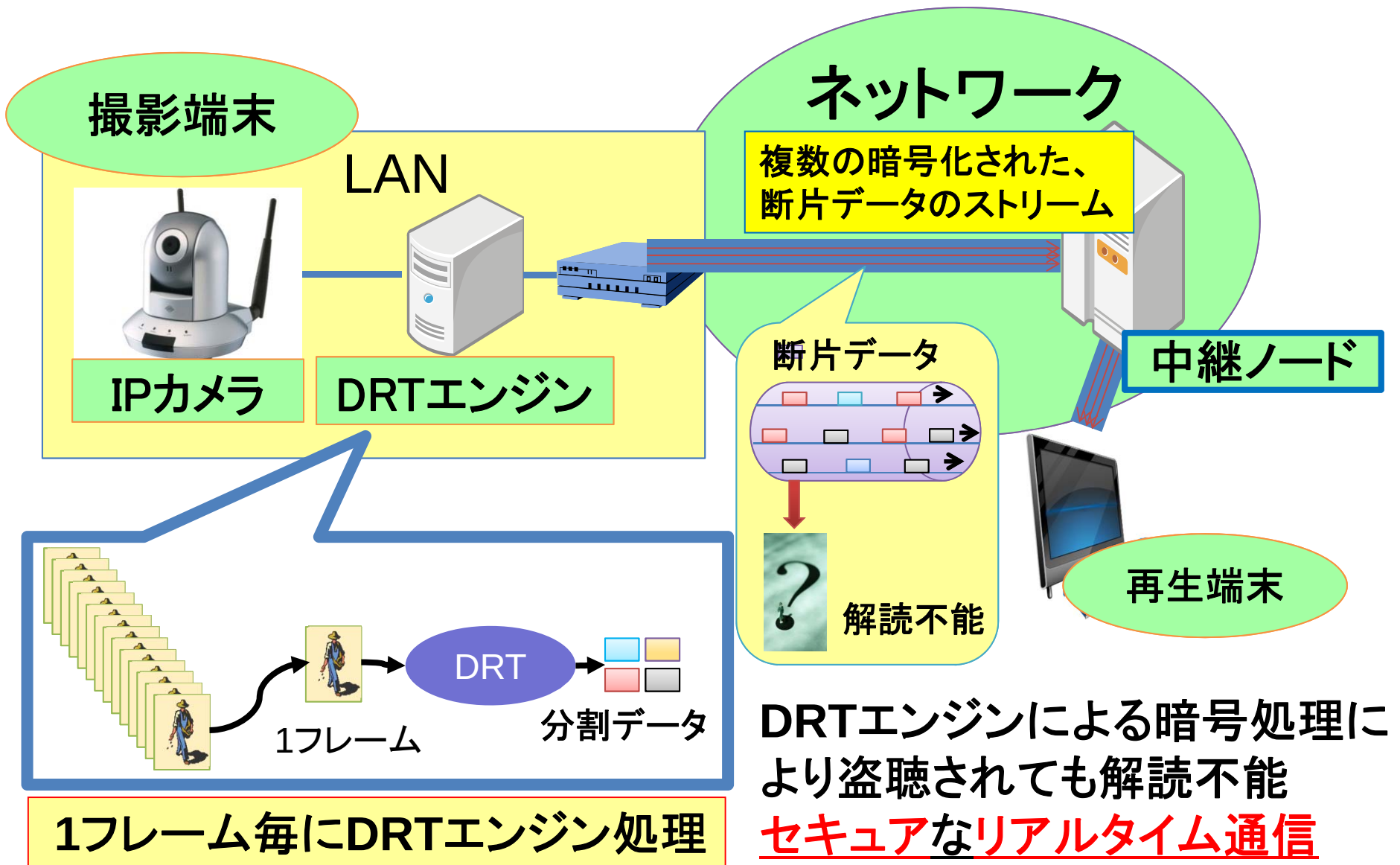


DRTプロセッサの内部メカニズム



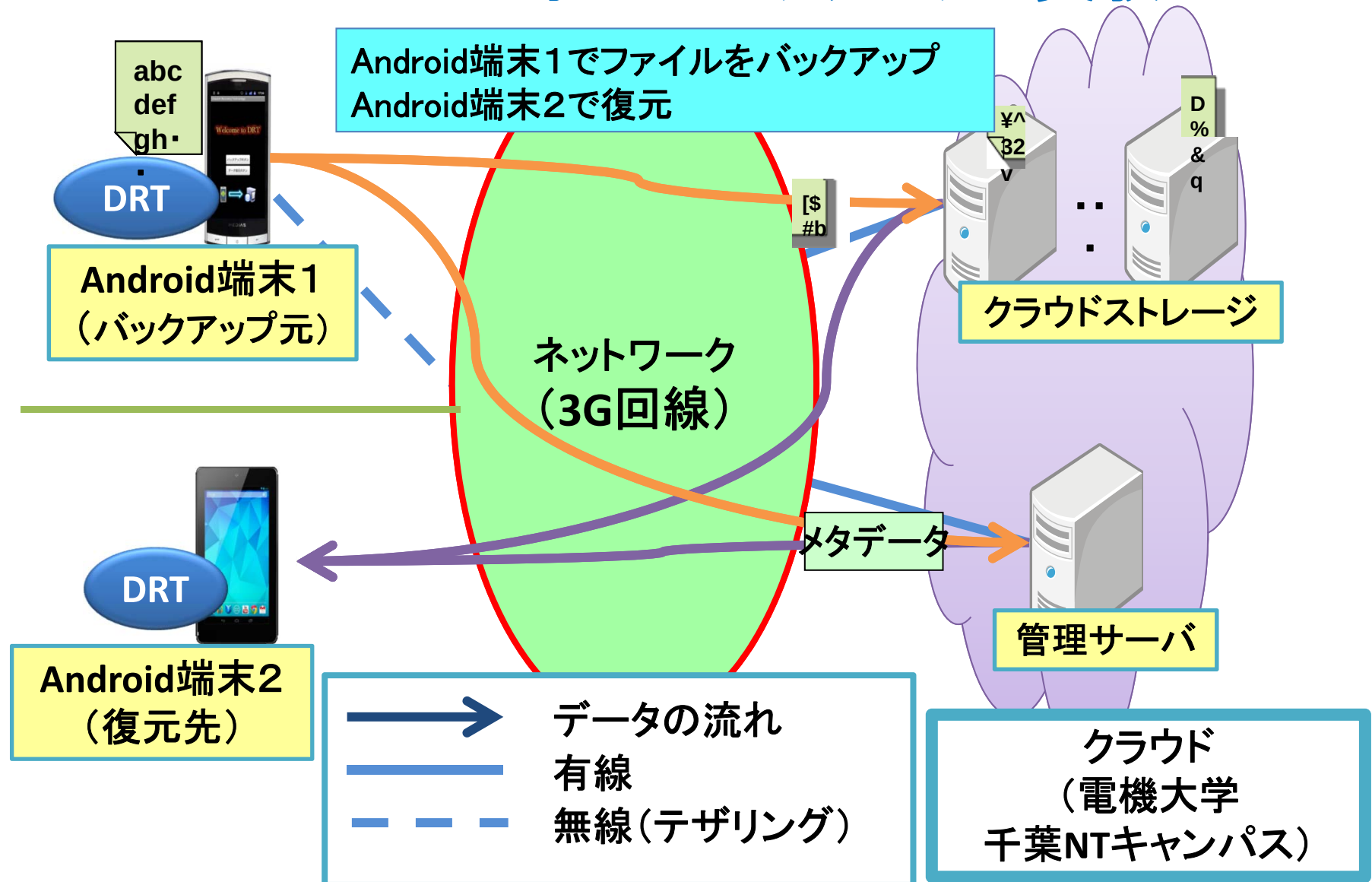
WTP2013 デモ(その2)

秘密動画像伝送システム



WTP2013 デモ(その1)

スマートフォンのバックアップ実験



産業界での用途

応用製品1:

DRT box, ファイル金庫, →ドラッグ & ドロップ的に, 手軽に, 重要情報をクラウド上にセキュア-にバックアップ

応用製品2: 動画像のセキュアなストリーミング

→暗号化＋断片化＋分散転送・保存で機密性を実現

ターゲットユーザ

- ①クラウドを積極的に利用し、コストの低廉化、付加価値のあるデータ保管サービスを実施予定のバックアップ事業者。
- ②インターネットの低廉化と信頼性向上により、セキュリティの高い(秘密)配信メディアを実施したい中規模のメディア配信事業者
- ③監視映像記録サービスを実現予定のバックアップ事業者

すでに、導入が進んでいる例

- (1) 医療機器メーカーの映像保存
- (2) 学習塾の映像配信
- (3) 大学等教育機関の重要データ保管
- (4) 広域車両管理システム
- (5) 行政機関の重要データ保管

多くの企業での実態

現状のバックアップ体制を根本的な見直し、
煩雑かつ不経済なデータ管理体制の払拭

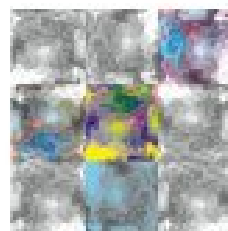
- (1) 大容量テープやDVDに記録し、頻繁に離れた場所に保管したり、人手で運んでいる状況。
- (2) 同じ建物内にHDD/DVDを配備し、冗長保管する状況。
- (3) インターネットを用いて、無防備に転送している状況。
(安全でない暗号化方式の多用)(無料クラウドの多用)
- (4) 高価な専用線でデータバックアップをしている状況。

産業界への広報活動

◎現在、実際に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**付加価値**として提供できる。⇒利用ユーザ層の拡大

◎特に、1社のクラウドのみでは、今後、想定されるサイバー攻撃等に対して、十分な安全性を保障することが困難 ⇒ 危険分散が容易。

平成23年 特許法の一部改正
産業財産権法の解説



特許庁編

平成23年特許法等の一部改正 産業財産権法の解説

特許庁工業所有権制度改正審議室

価格: ￥ 700

6点の新品／中古品を見る: ￥ 700より

なか見! 検索

技術者・研究者のための
**特許
の
取り方**

宮保憲治
岡田賢治

明日からできる特許出願!

大学卒業
企業研究員出身の
特許士

技術者・研究者のための特許の取り方

宮保憲治, 岡田賢治

★★★★★ (5)

価格: ￥ 1,995

2点の新品／中古品を見る: ￥ 1,995より

田村善之・時井真 著
**ロジスティクス
知的財産法**
① 特許法

ロジスティクス
知的財産法
特許法

ロジスティクス知的財産法I(特許法)

田村 善之, 時井 真

価格: ￥ 2,940

5点の新品／中古品を見る: ￥ 2,940より

アマゾン

(Amazon)

発明・特許部門

ベストセラー

(平成24年3月出版)

第1位

(平成25年6月19日)

第9位

(平成25年7月1日)

ご清聴ありがとうございました

miyaho@sie.dendai.ac.jp

超分散ストレージ技術

HS-DRT 

High Security Distribution and Rake Technology

情報ネットワーク環境研究室(宮保研) ホームページ
<http://www.ine.sie.dendai.ac.jp/>