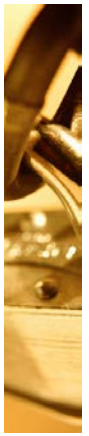
# 属性ベース暗号による建設業務のセキュアな情報共有の実現のための研究



アーク情報システム
半田　沙里

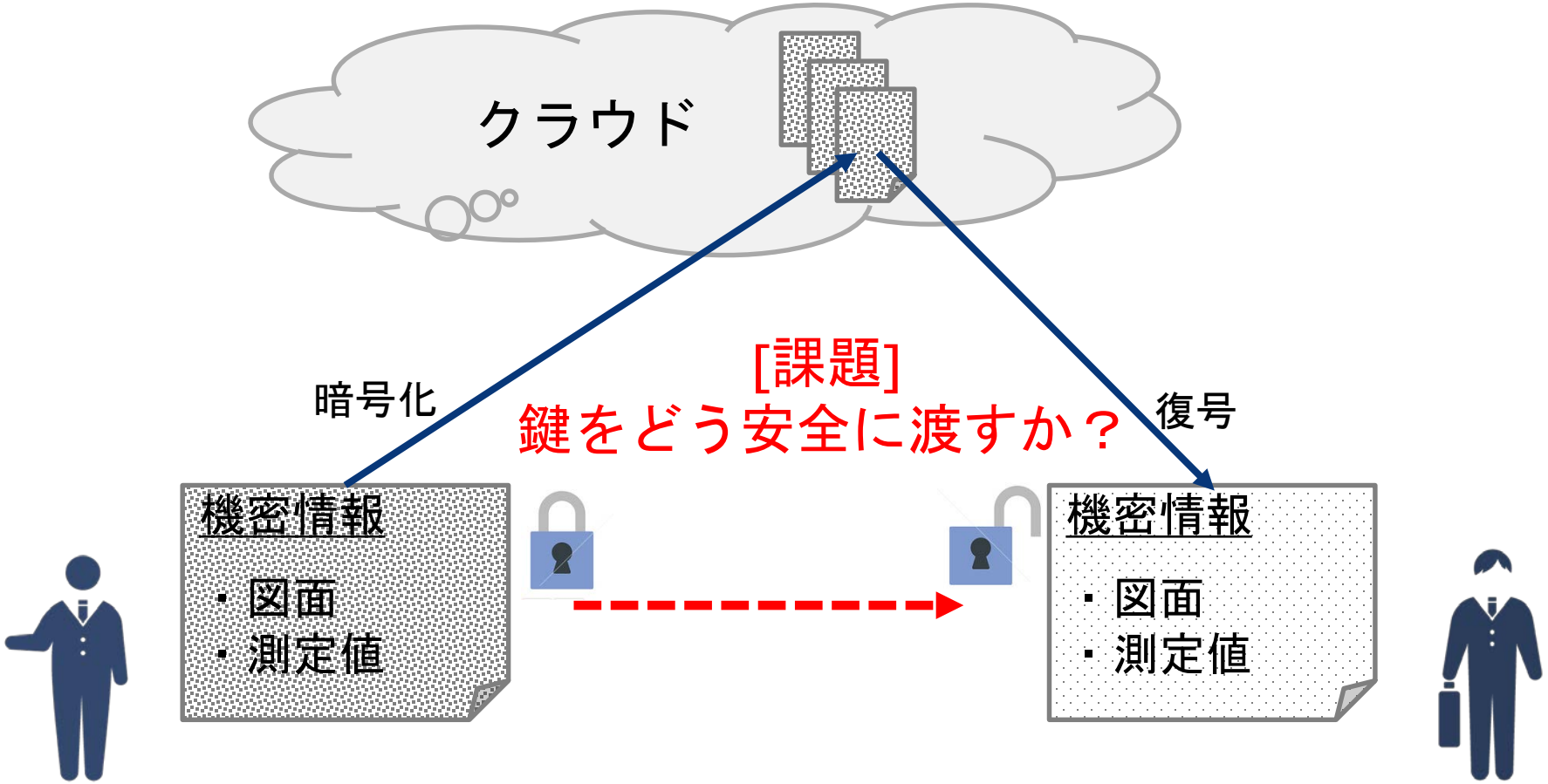
# 建設業務の情報セキュリティ

- 守るべき情報
  - 図面、工程表、写真、打ち合わせなどの資料
  - 発注者、近隣、工事関係者の個人情報
  - 工事の技術やノウハウ
- 建設特有のリスク
  - 工程ごとに作業者が入れ替わり、多くの関係者が出入りする。
  - 下請け構造が階層化していて、情報セキュリティの教育が行き届きにくい。
  - ITリテラシがさまざまで、自宅PCからの情報漏洩などのリスクがある。

→情報へのアクセスの管理が重要

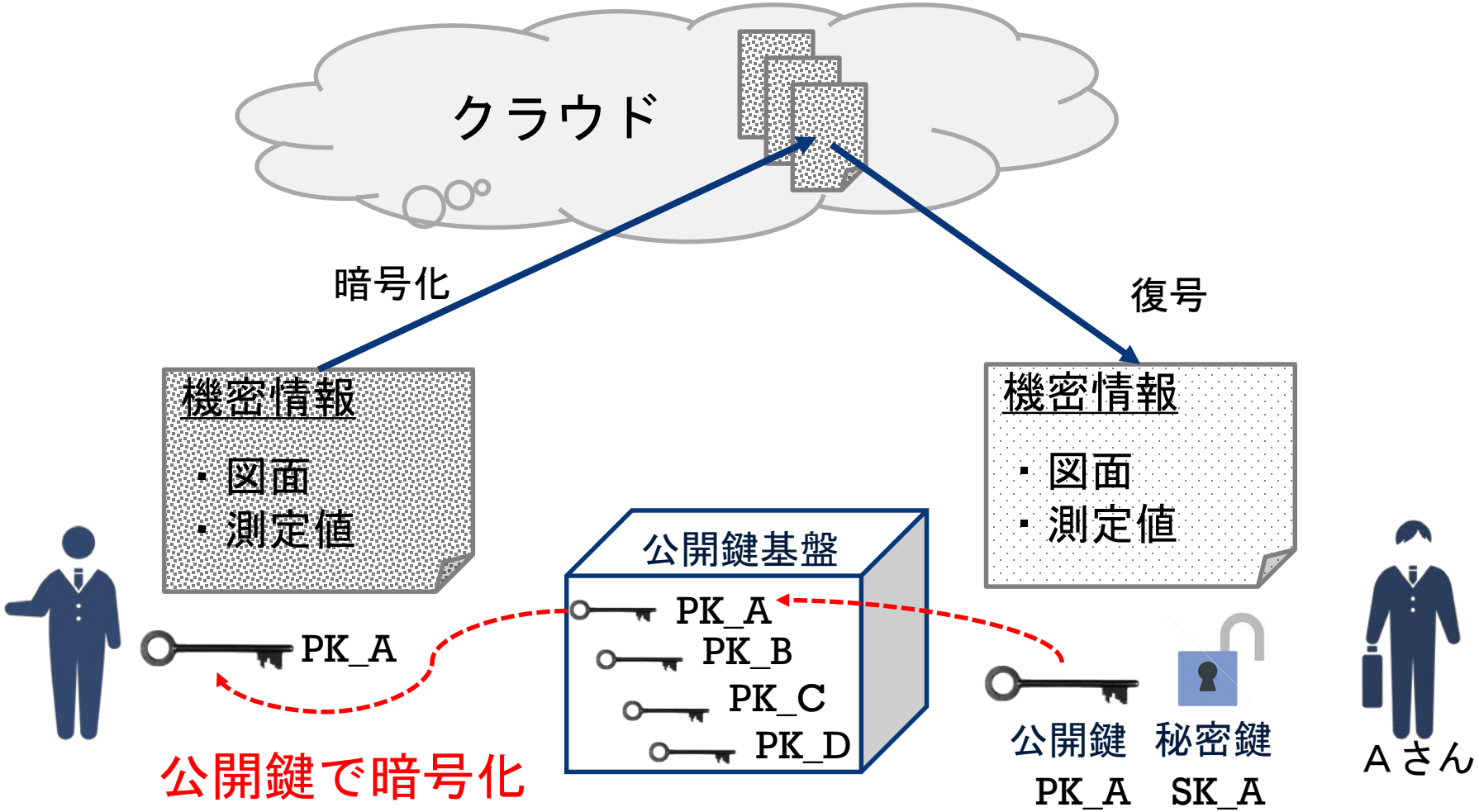
# ＋暗号化して情報共有

## 共通鍵暗号



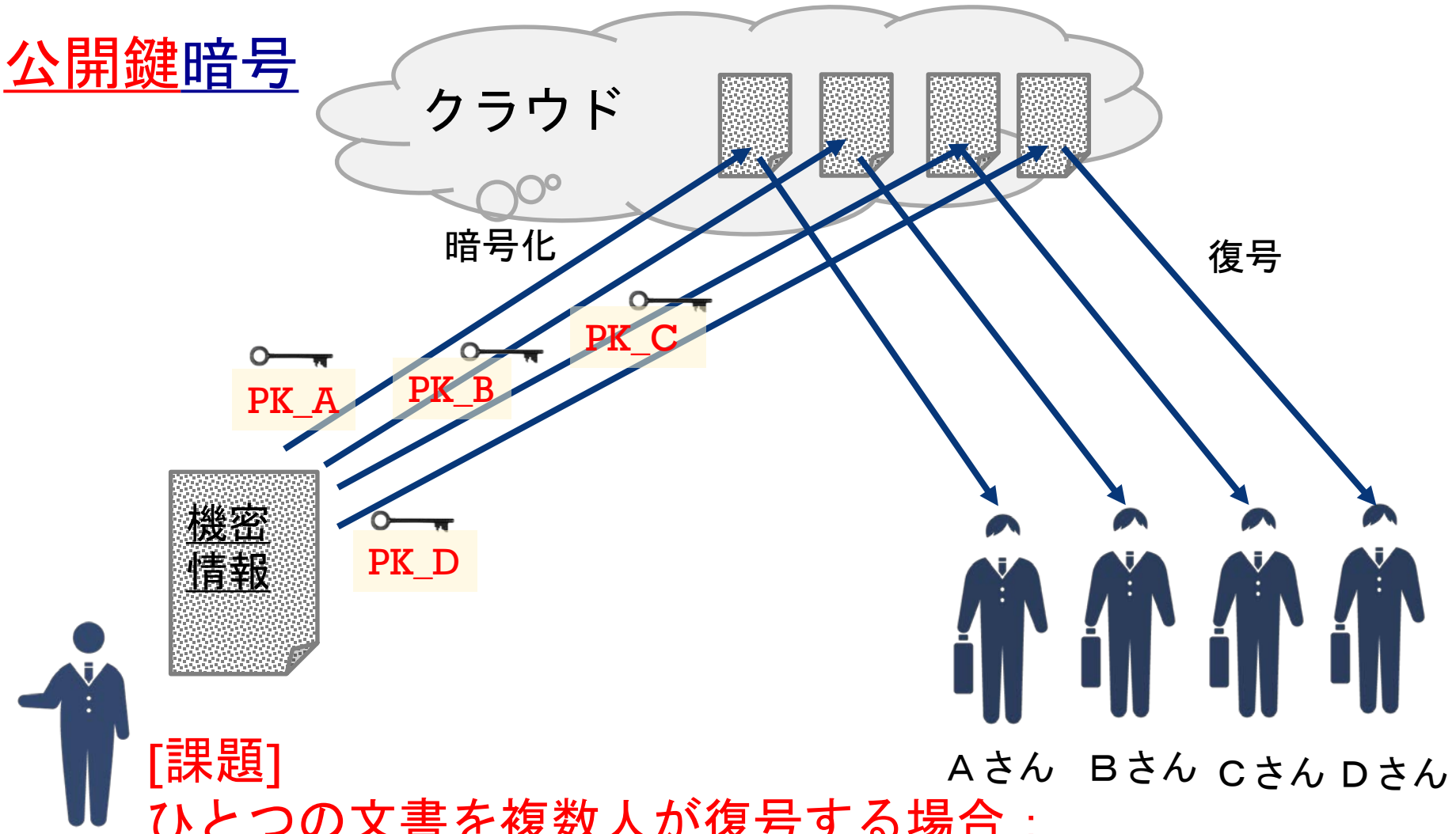
# ＋暗号化して情報共有

## 公開鍵暗号



# ＋暗号化して情報共有

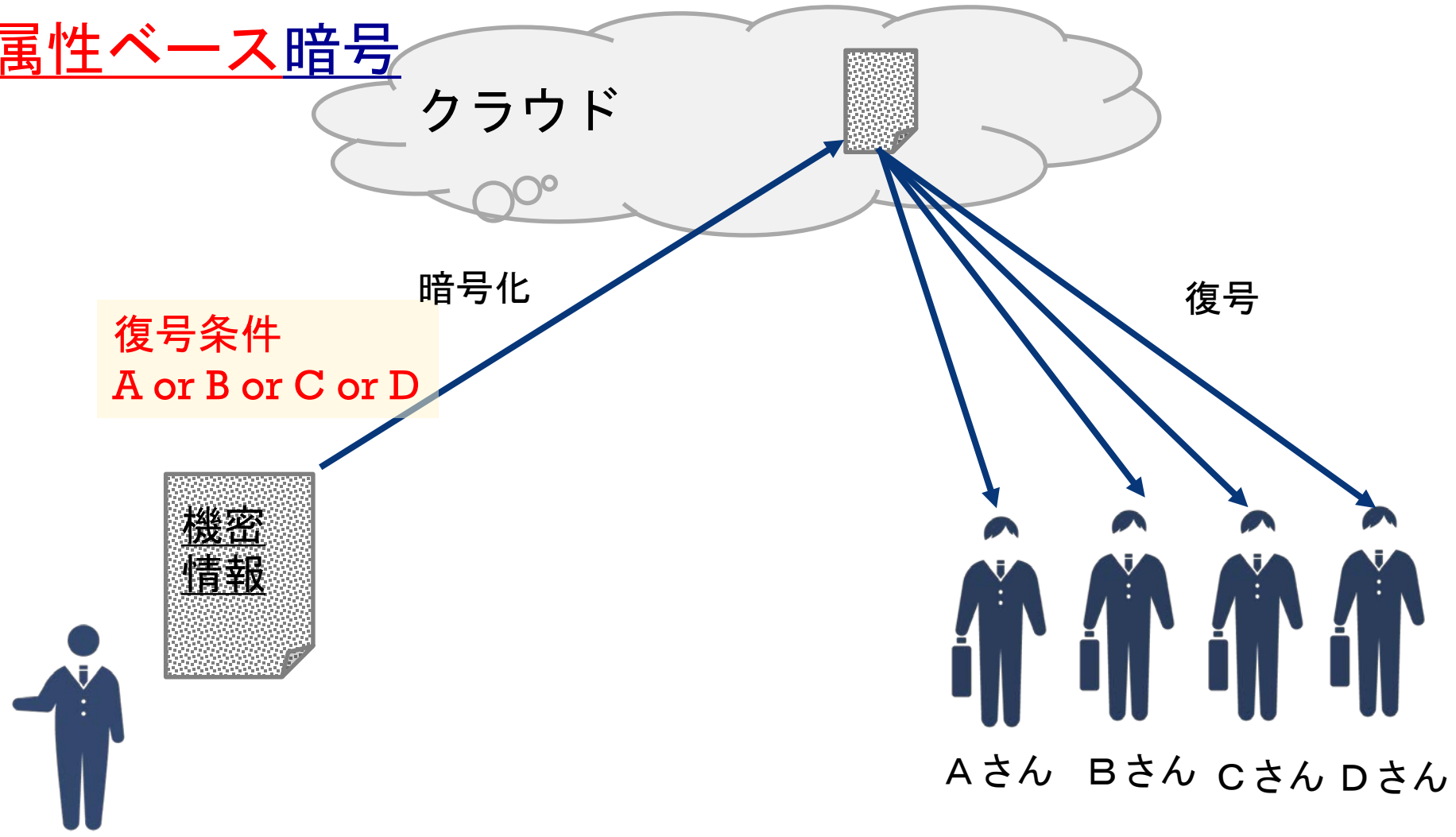
公開鍵暗号




[課題]
ひとつの文書を複数人が復号する場合：
→復号者の公開鍵で暗号化するのは手間

# ＋暗号化して情報共有

## 属性ベース暗号



# 建設の情報セキュリティに
# アクセスコントロール機能を持つ
# ”属性ベース暗号”が向いている

研究テーマ

## 属性ベース暗号の
## 建設業務の情報共有への
## 活用方法を探る

“属性”とは、
人の属性（所属や年齢）またはデータの属性のこと。

# ＋属性ベース暗号の二つの種類

## 暗号文ポリシー型

暗号文

機密情報
- 契約書
- 顧客情報

復号ポリシー
A会社 and
(営業部 or 部長)

ユーザの
秘密鍵

“営業部”
“担当営業”

“開発部”
“部長”

“経理部”
“係長”

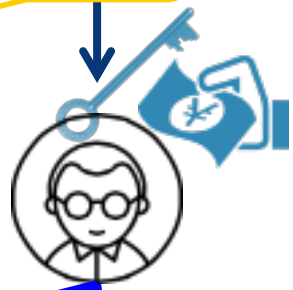
ユーザ
の属性

利用 アクセス制御

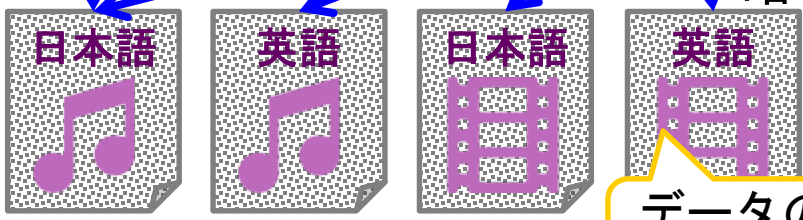
## 鍵ポリシー型

| 復号ポリシー | 復号ポリシー | 復号ポリシー |
|---|---|---|
| 音楽 and 日本語 | (音楽 or 映画) and 日本語 | ALL |

秘密鍵に
ポリシー

暗号文




データの
属性

利用 情報配信

# ＋ 暗号文ポリシー型属性ベース暗号の活用 for 建設

1. アクセス可能期間を制限
2. 接続元IPアドレスを制限
3. エリアを制限

# 1. アクセス可能期間を制限

| | 会社 | 1月 | 2月 | 3月 | 4月 |
|---|---|---|---|---|---|
| 基礎工事 | A会社 | → | | | |
| 躯体工事 | B会社 | | → | → | |
| 外装工事 | C会社 | | | | → |
| 内装工事 | D会社 | | | | → |
| ・・・ | | | | | |

[建設業務に特有のリスク]
・多くの関係者が機密情報にアクセス
・工期ごとに関係者が入れ替わる

機密情報
・図面
・測定値

[対策]
担当の期間だけ、情報にアクセス可能にする

# ＋1. アクセス可能期間を制限

| | 会社 | 1月 | 2月 | 3月 | 4月 |
|---|---|---|---|---|---|
| 基礎工事 | A会社 | | | | |
| 躯体工事 | B会社 | | | | |
| 外装工事 | C会社 | | | | |
| 内装工事 | D会社 | | | | |
| ・・・ | | | | | |

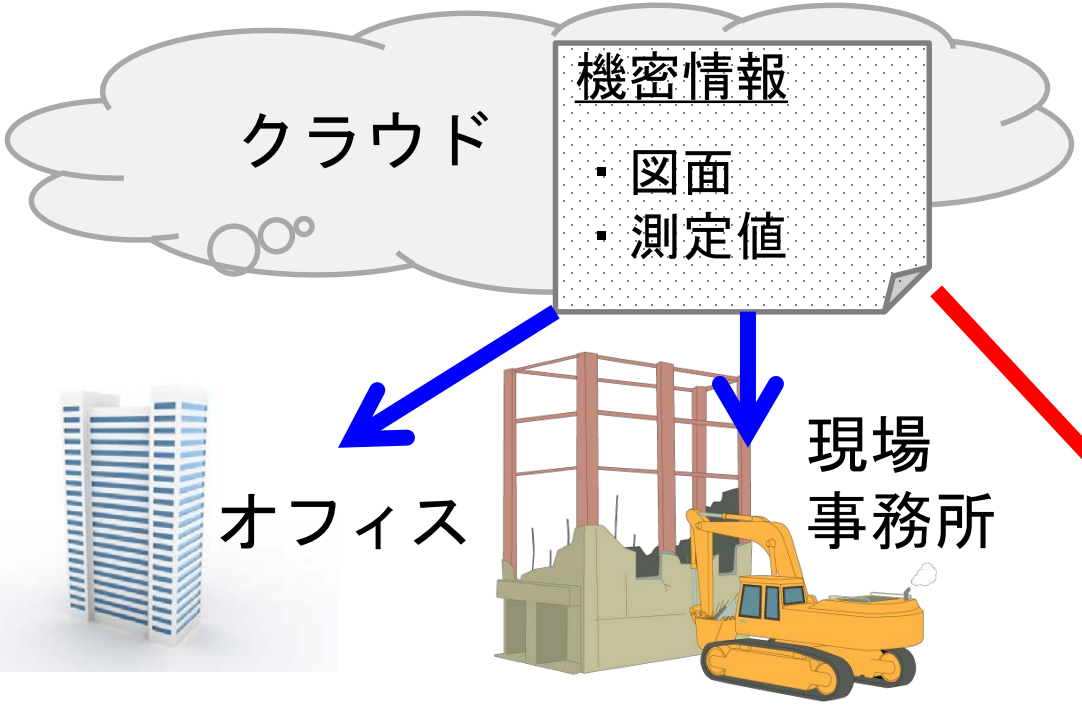
属性ベース暗号で自動的にアクセス制御

復号ポリシー

(A会社 and (2015/01/01 <= 期間 <= 2015/01/31) )
　or
(B会社 and (2015/02/01 <= 期間 <= 2015/03/31) )
　or
(C会社 and (2015/04/01 <= 期間 <= 2015/04/14) )
　or
(D会社 and (2015/04/15 <= 期間 <= 2015/04/30) )

# ＋2. 接続元IPアドレスを制限

クラウドはどこでも使えて便利



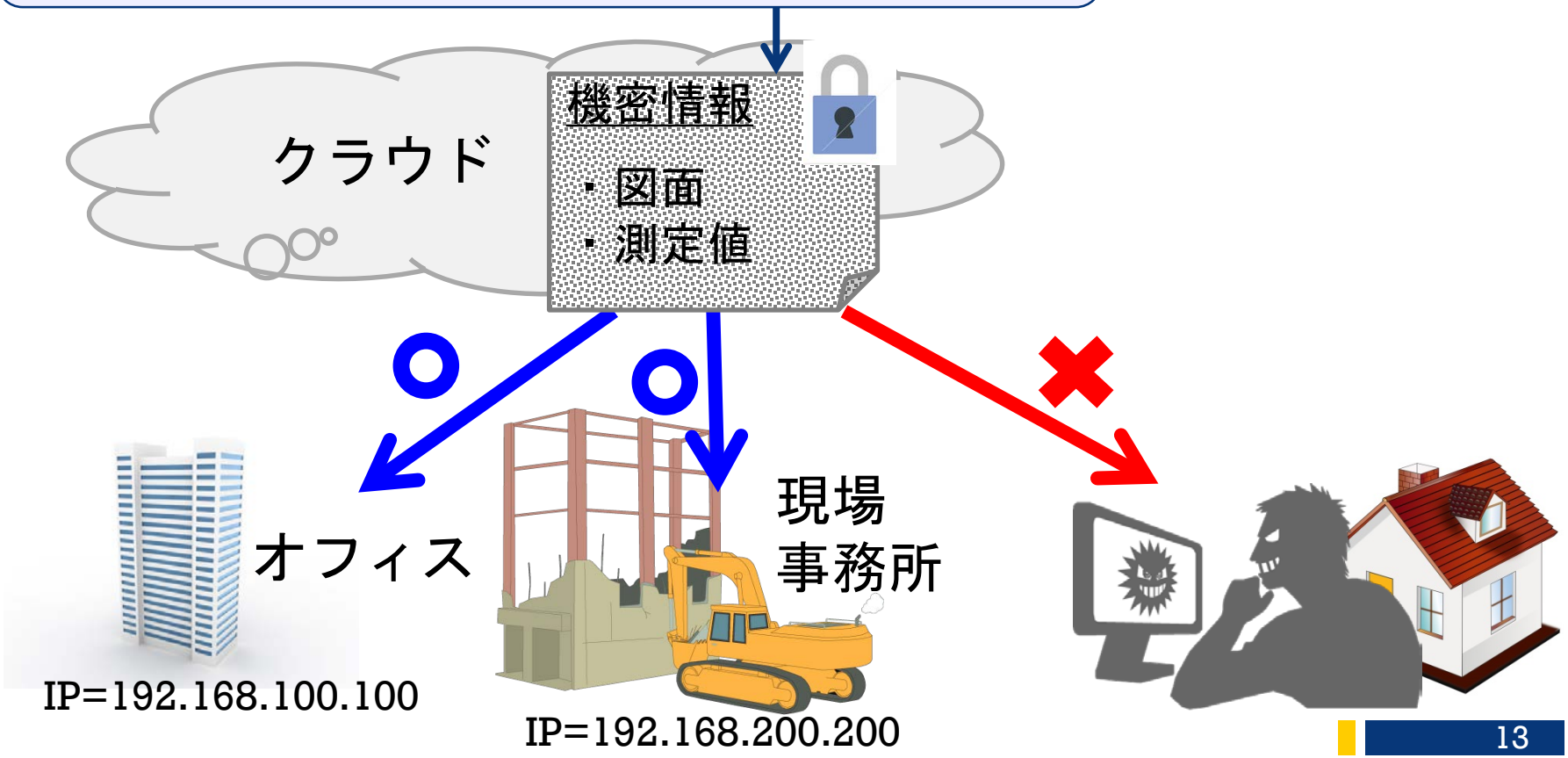

でも、『どこでも使われてしまう』リスクがある

[対策]　接続元のIPアドレスで制限

# 2. 接続元IPアドレスを制限

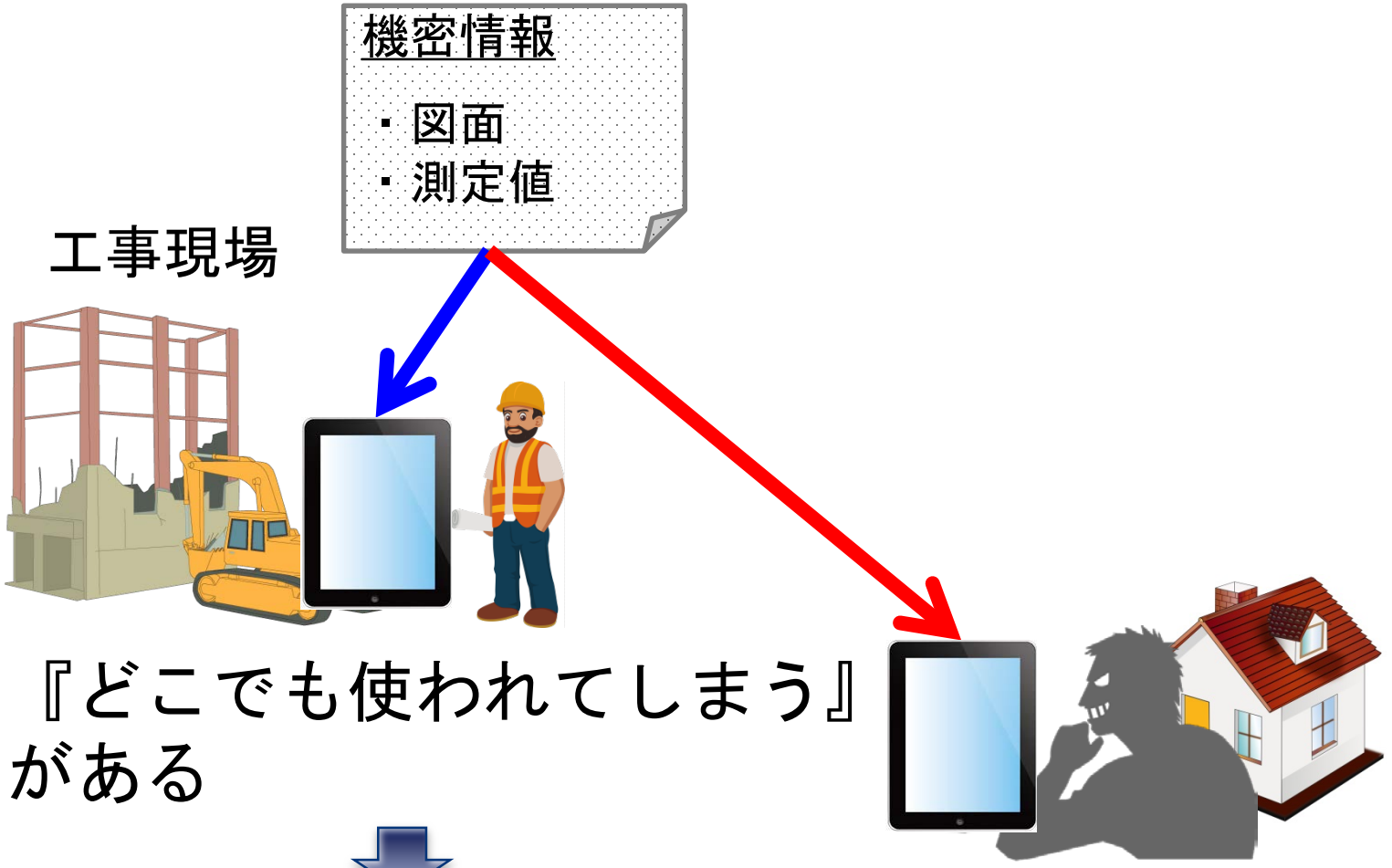
復号ポリシー

(IPアドレス=192.168.100.100) // オフィス
or
(IPアドレス=192.168.200.200) // 現場事務所



# ＋3. エリアを制限

モバイル端末はどこでも使えて便利




でも、『どこでも使われてしまう』リスクがある

[対策]　エリアで制限

# +3. エリアを制限

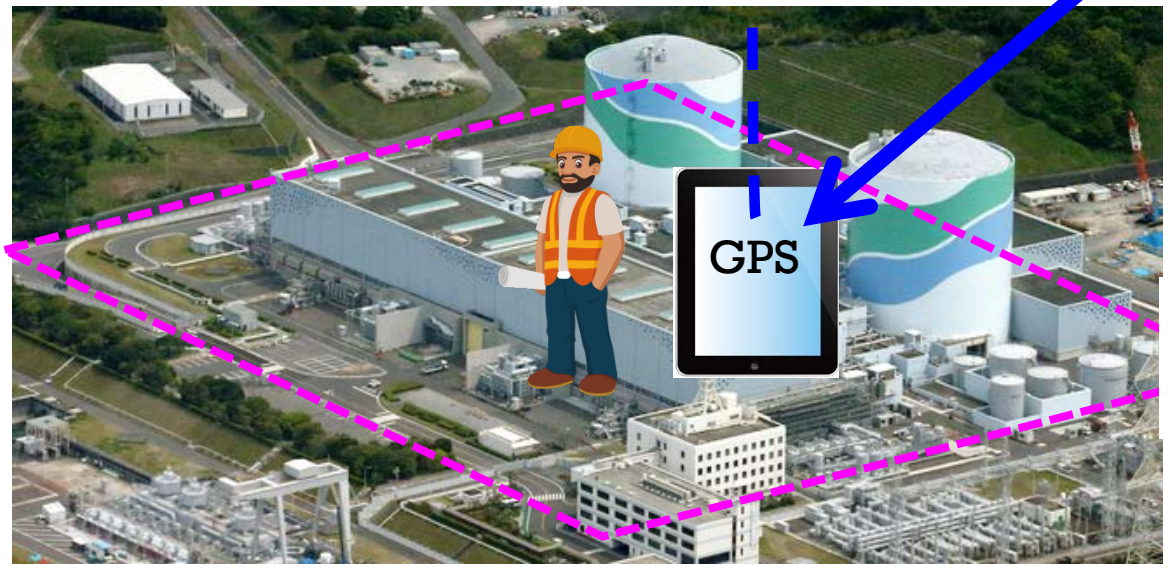
復号ポリシー

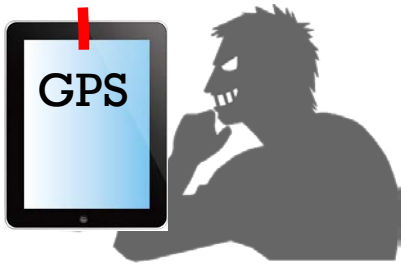
31.831706 <= 緯度 <= 31.835099
130.188539 <= 経度 <= 130.919208


機密情報
・図面
・測定値

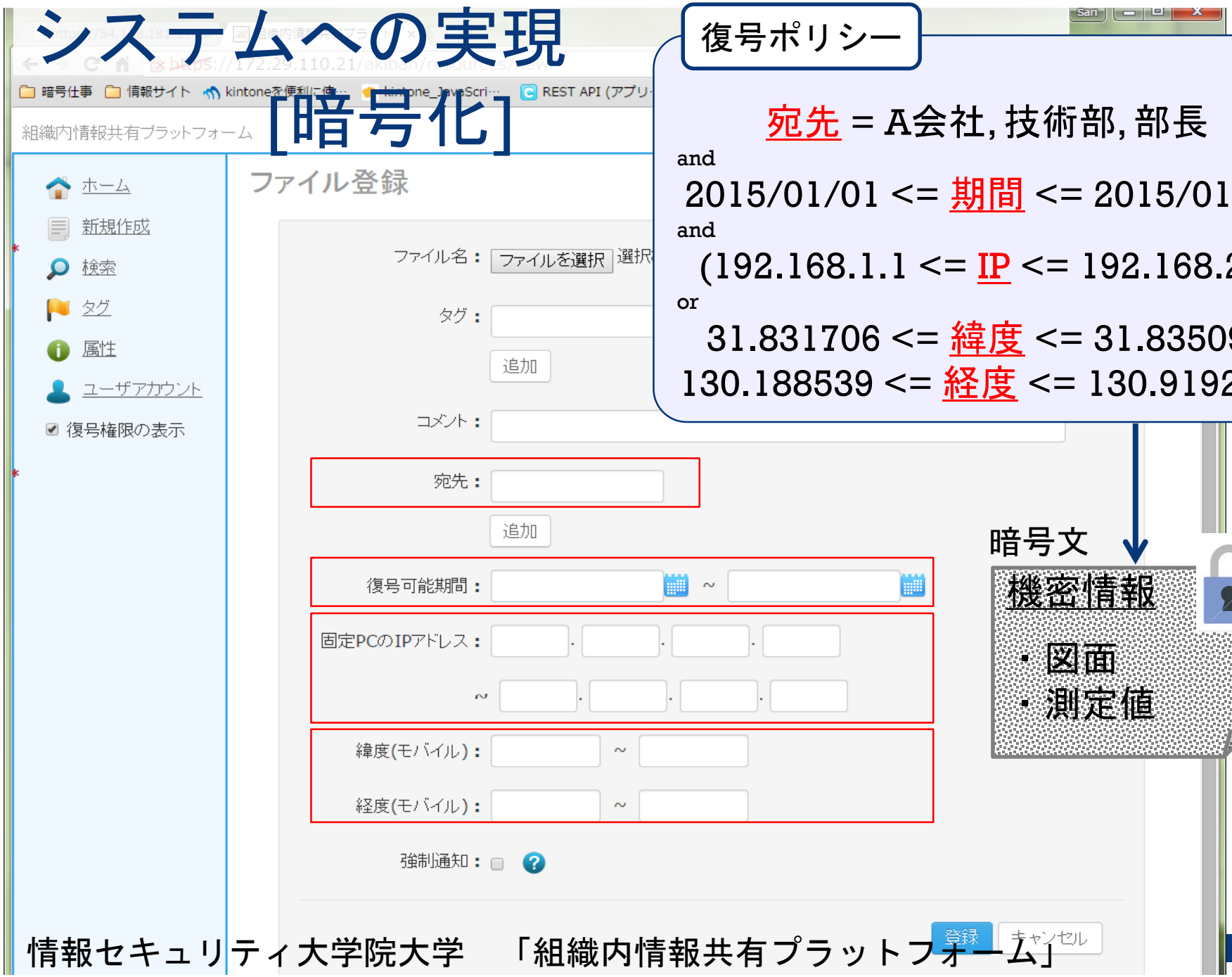
復号できる

復号できない



# システムへの実現 [暗号化]



# ＋システムへの実現　[復号]

利用者の属性

- 所属会社
- 部署
- 役職
- 年齢

＋ システム設定値

- 現在日

- オフィスの固定PCのIPアドレス

- モバイルの緯度/経度


復号ポリシー

宛先 = A会社, 技術部, 部長
and
2015/01/01 <= 期間 <= 2015/01/31
and
(192.168.1.1 <= IP <= 192.168.2.2
or
31.831706 <= 緯度 <= 31.835099
130.188539 <= 経度 <= 130.919208)

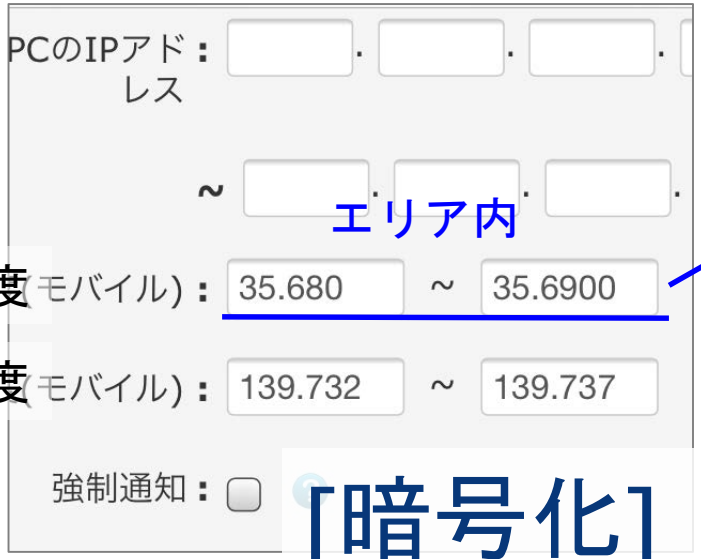
利用者の秘密鍵

機密情報
- 図面
- 測定値

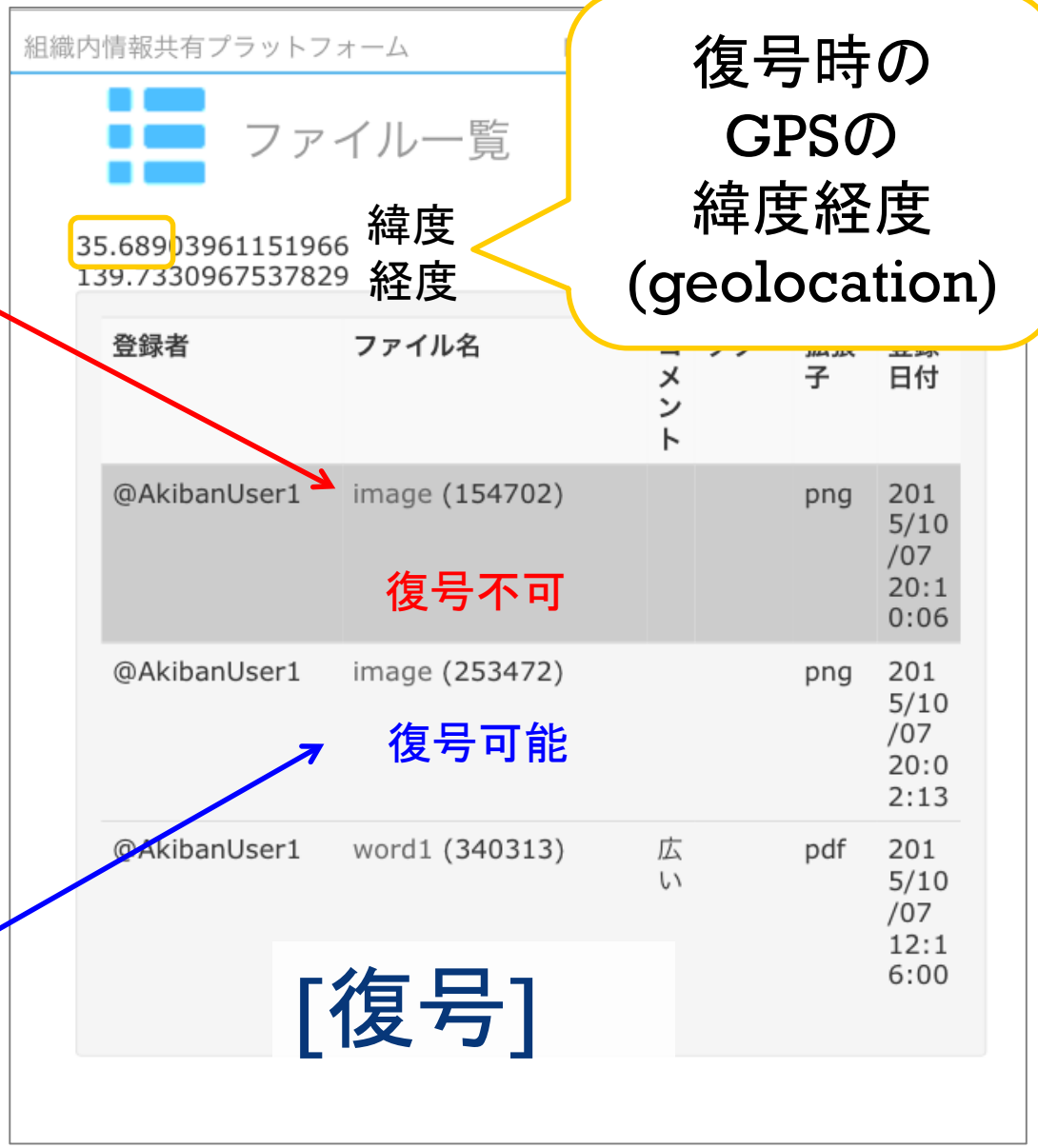
暗号文

秘密鍵が復号ポリシーを満たせば復号できる

# ＋モバイルのエリア制限

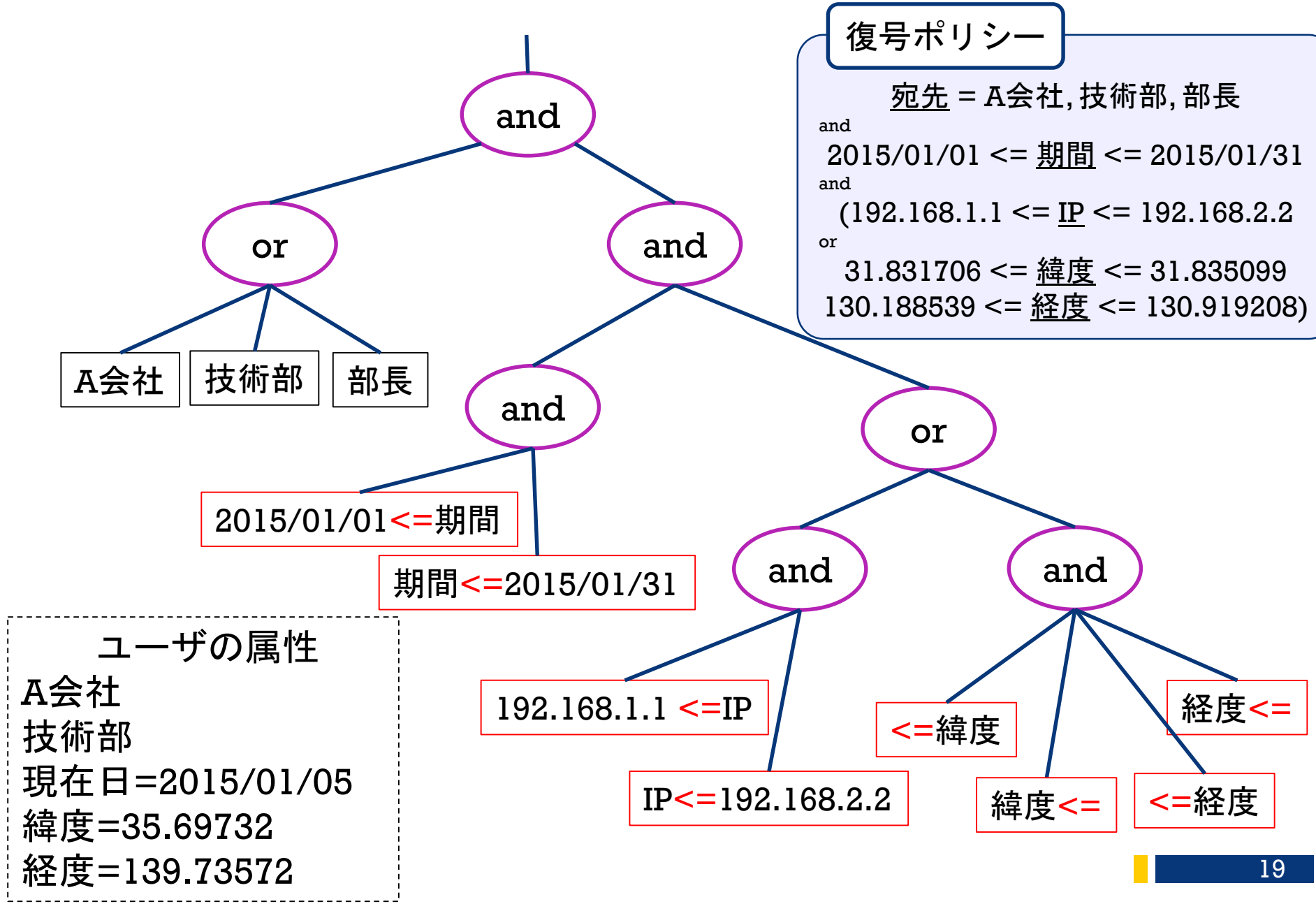

[暗号化]




[復号]

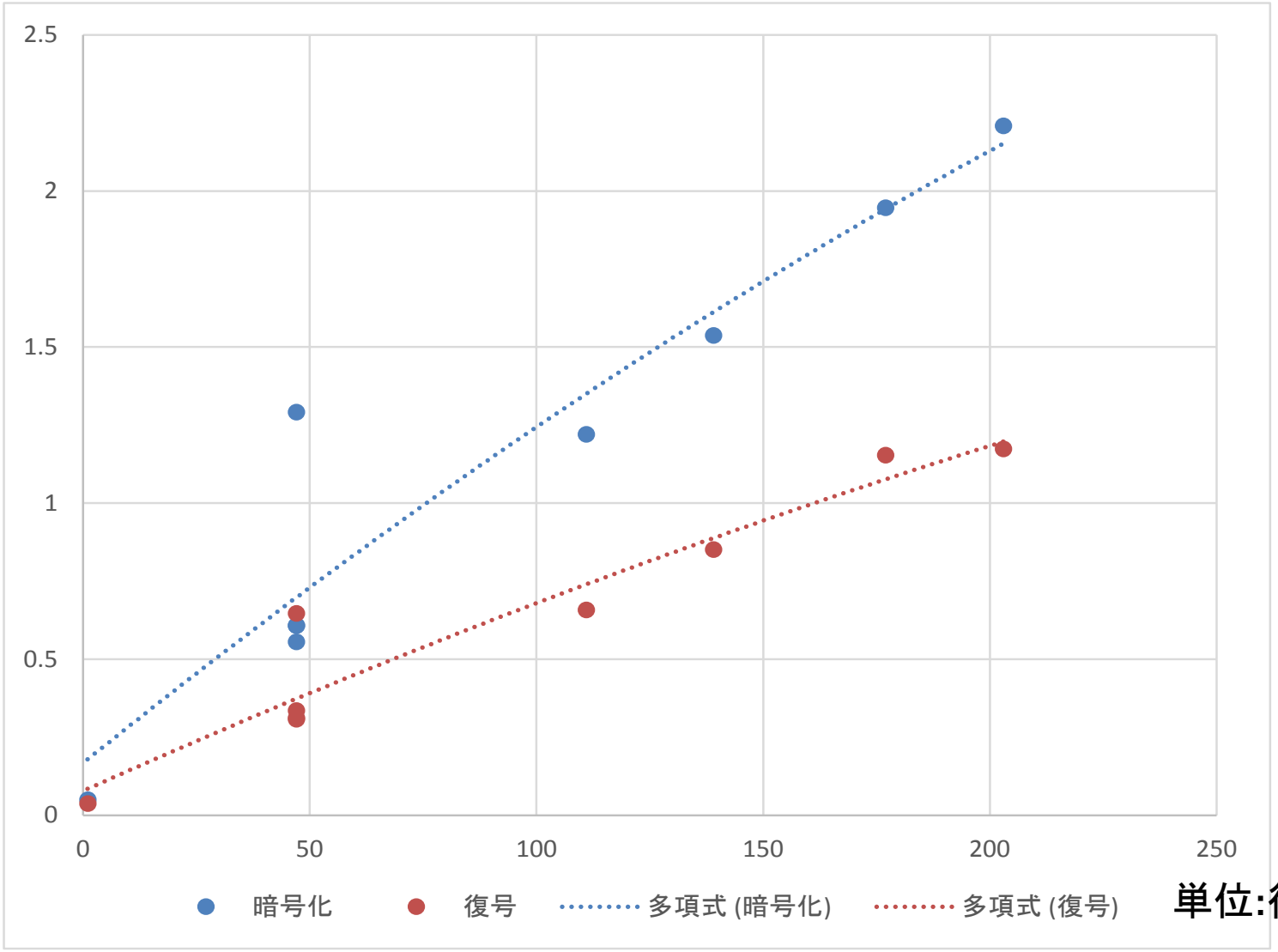
復号時の
GPSの
緯度経度
(geolocation)

# ＋属性ベース暗号の数値範囲指定



# システムの速度評価

単位:秒




単位:復号条件数

# ＋ 鍵ポリシー型属性ベース暗号の活用 for 建設

利用 → 情報配信

1. センサー測定値の配信制御

# ＋センサー測定値の配信制御

[対象]

[モニタリング項目]
変位、剛性、応力、荷重
腐食、ひび割れ

無線センサネットワーク

暗号文

02/01
01/01
東京
A橋
ひび割れ
15mm

02/01
01/01
神奈川
Bビル
変形
10mm

02/01
01/01
栃木
鬼怒川
水位
5m

復号ポリシー
計測場所=東京都

復号ポリシー
01/01<=計測日<=01/31

復号ポリシー
計測項目=変位orひび割れ
and
計測値>=10mm

# ＋まとめ

## 属性ベース暗号の建設業務への活用

- 暗号文ポリシー型　[アクセス制御]
  - 復号可能期間の制限
  - 接続元IPアドレスの制限
  - エリアの制限

  →セキュアな情報共有システムを実現

- 鍵ポリシー型　[配信制御]
  - センサー測定値の配信制御

# 今後の研究

- IoT向け軽量暗号
  - センサーなどの機器のマイクロコントローラ上で動作する軽量暗号
  - 格子暗号で実現する