日本銀行金融研究所
第18回情報セキュリティ・シンポジウム
2017年3月9日

-講演1-

公開鍵暗号型の高機能暗号の研究動向

日本銀行金融研究所
情報技術研究センター
清藤 武暢

- 本発表は、横浜国立大学大学院教授　四方順司様、情報通信研究機構研究員　青野良範様と共同で実施した研究に基づく。
- 本発表に示されている意見は、発表者たち個人に属し、横浜国立大学、情報通信研究機構および日本銀行の公式見解を示すものではない。

アジェンダ

■ 公開鍵暗号型の高機能暗号

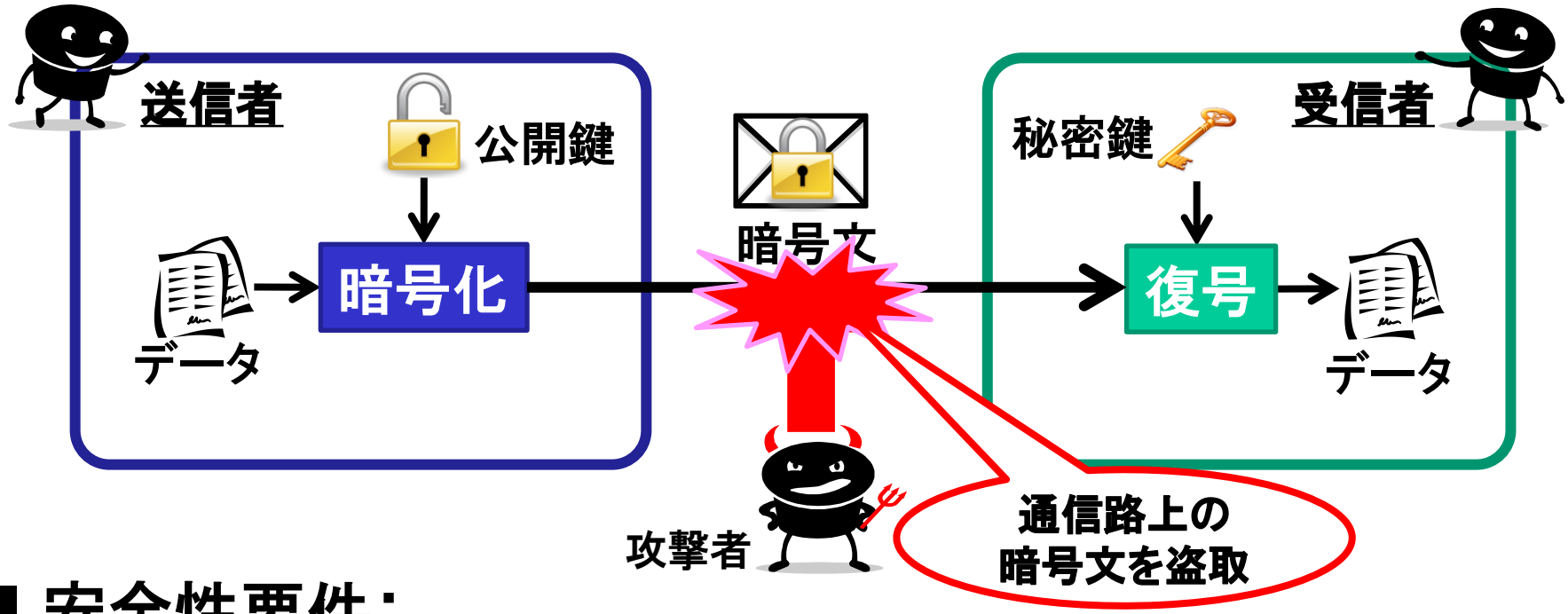
主な方式	主な機能
検索可能暗号（秘匿検索暗号）	データを暗号化したままキーワード検索を実行できる
準同型暗号	データを暗号化したまま統計解析等の演算処理を実行できる
属性ベース暗号	エンティティの属性に応じて暗号化したデータの復号権限を効率良く制御できる

金融分野で高機能暗号の適用しうるケースを想定し、その効果や課題について整理

■ 本発表の流れ

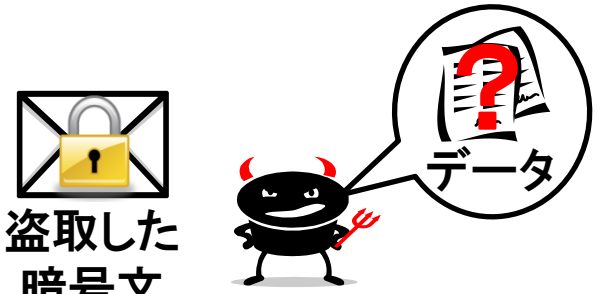
1. 属性ベース暗号、準同型暗号の機能と安全性要件
2. 高機能暗号の金融分野への活用
   - ✓ 営業支援システム
   - ✓ 口座情報サービス

従来の公開鍵暗号



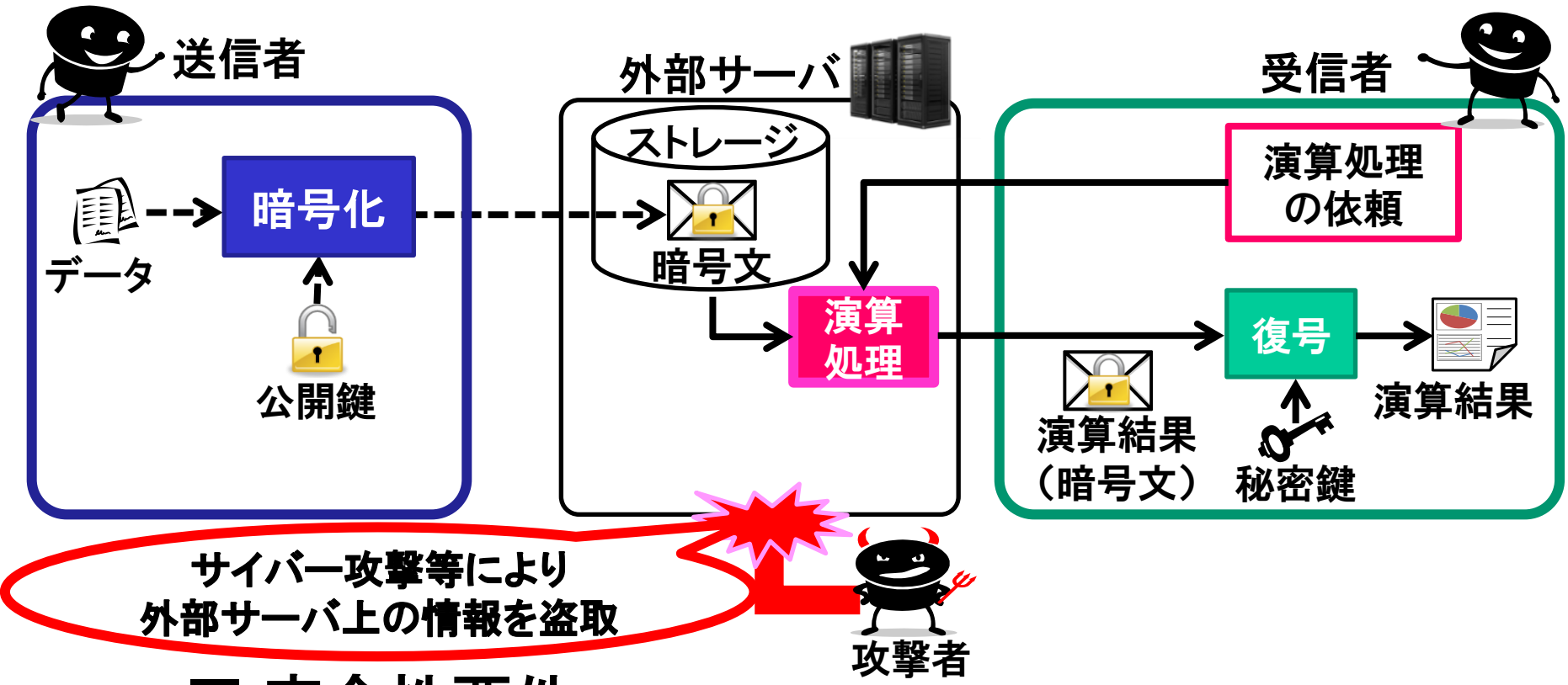
■ 安全性要件：

データの機密性確保



データの完全性確保

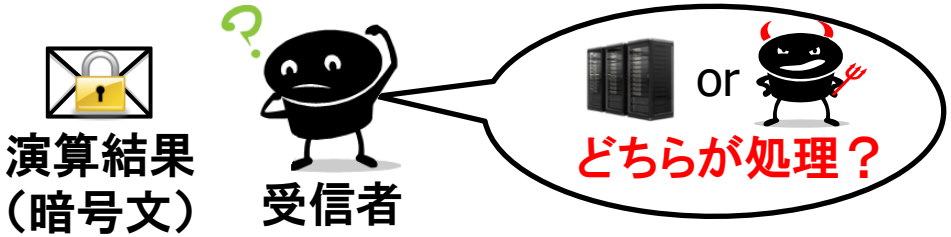
準同型暗号のモデル（イメージ）



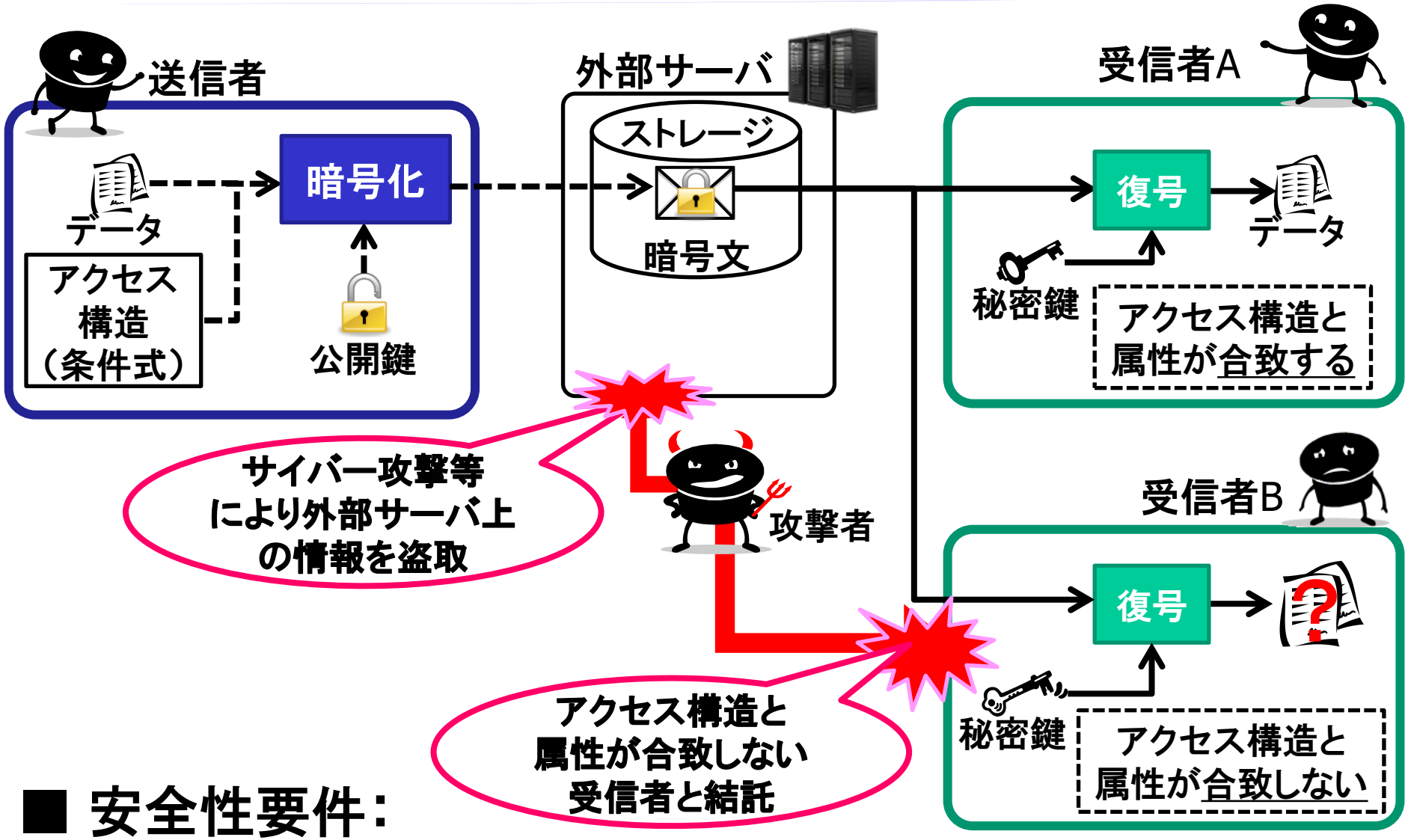
■ 安全性要件：

□ データの機密性確保のみ

※データの完全性確保は原理的に満たすことは難しい



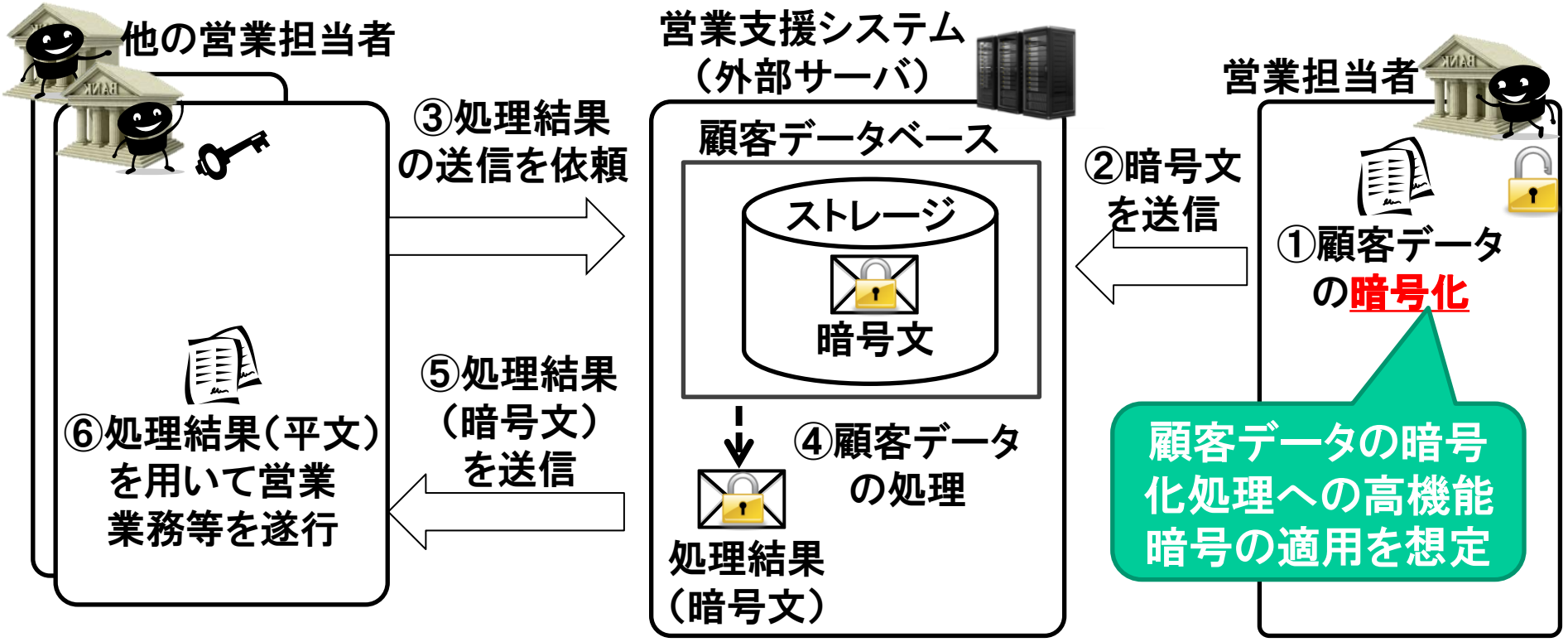
属性ベース暗号のモデル（イメージ）



■ 安全性要件：

ロ データの機密性・完全性確保

営業支援システムへの適用：概要



高機能暗号	期待される効果（メリット）
準同型暗号	顧客データを暗号化したまま外部サーバで統計解析等を実施可能
属性ベース暗号	顧客データの復号権限を営業担当者が効率的に制御可能

営業支援システムへの適用：安全性とコスト

■ 安全性：顧客データの情報漏えいリスクは軽減

ロ　想定する攻撃者：通信路上および外部サーバの情報を盗取

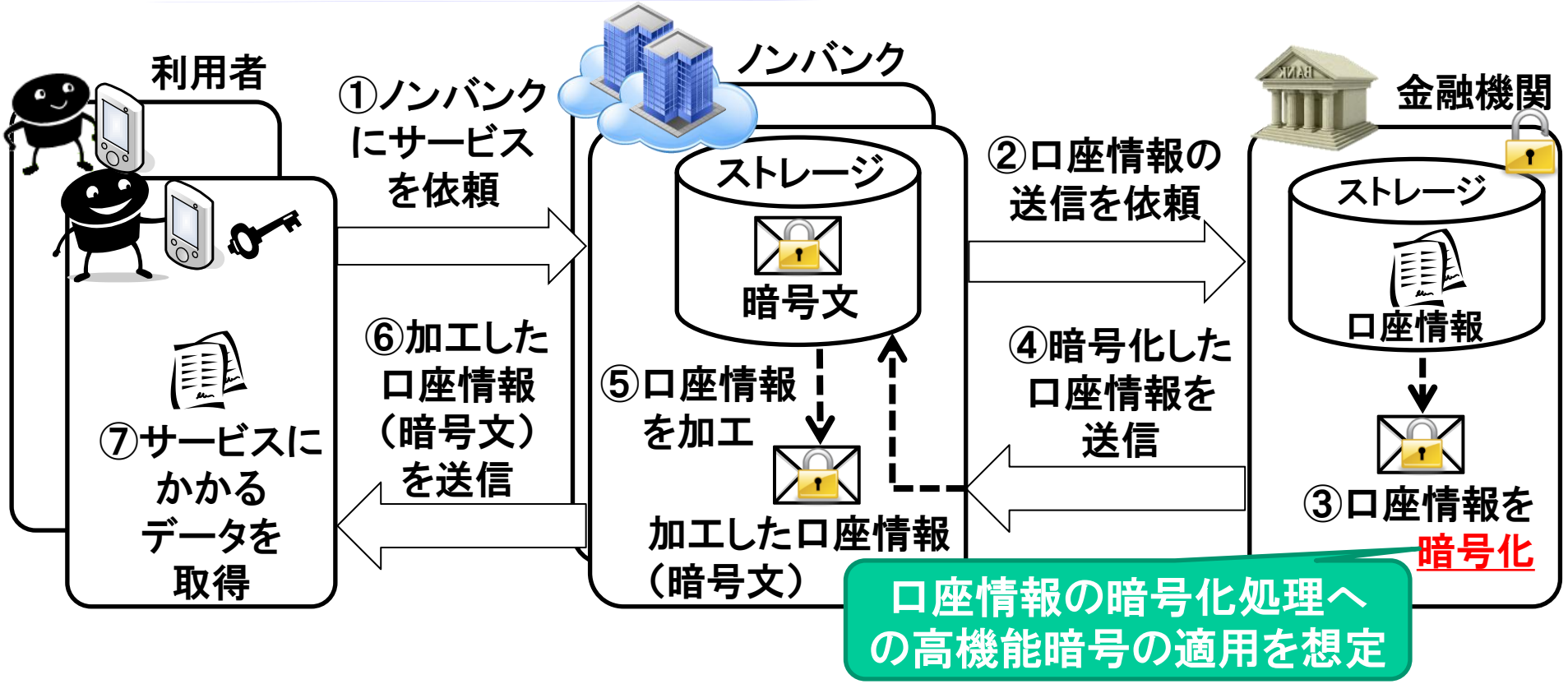
要件	準同型暗号	属性ベース暗号
顧客データの機密性	満たす	満たす
顧客データの完全性	満たさない	満たす

■ コスト：鍵管理コストは概ね軽減、暗号処理コストは少し増加

項目	エンティティ	準同型暗号	属性ベース暗号
鍵管理（公開鍵の個数やサイズ）	営業担当者	○	◎
	他の営業担当者	○	○
暗号処理（暗号化処理の回数）	営業担当者	△	◎
	他の営業担当者	△	△

◎：従来の暗号よりも軽減、○：従来の暗号と同程度、△：従来の暗号よりも増加

口座情報サービスへの適用：概要



高機能暗号	期待される効果（メリット）
準同型暗号	口座情報を暗号化したままノンバンクが統計解析等の加工を実施可能
属性ベース暗号	口座情報の復号権限を金融機関が効率的に制御可能

口座情報サービスへの適用：安全性とコスト

■ 安全性：口座情報の情報漏えいリスクは軽減

口　想定する攻撃者：通信路上、ノンバンクおよび一部の利用者の情報を盗取

要件	準同型暗号	属性ベース暗号
口座情報の機密性	満たす	満たす
口座情報の完全性	満たさない	満たす

■ コスト：鍵管理コストは概ね軽減、暗号処理コストは少し増加

項目	エンティティ	準同型暗号	属性ベース暗号
鍵管理（公開鍵の個数やサイズ）	金融機関	○	◎
	ノンバンク	◎	○
	利用者	○	○
暗号処理（暗号化処理の回数）	金融機関	△	◎
	ノンバンク	△	△
	利用者	△	△

◎：従来の暗号よりも軽減、○：従来の暗号と同程度、△：従来の暗号よりも増加

まとめ

■ 営業支援システム、口座情報サービスに高機能暗号を適用した際の効果と課題について整理

□ 効果（メリット）
- ✓ 外部サーバやノンバンクからの情報漏えいリスクの軽減
- ✓ 各エンティティにおける鍵管理コストの軽減

□ 課題
- ✓ 各エンティティにおける暗号処理コストの増加
- ✓ 準同型暗号を利用した際のデータの完全性確保