# セキュリティの観点からみた分散型台帳技術

日本銀行金融研究所
情報技術研究センター

宇根　正志

・本発表の内容は発表者個人に属し、日本銀行の公式見解を示すものではありません。

# 情報技術研究センター（CITECS）について

- 金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポートするために、2005年4月に設立。
  - 主に、①国際標準化の推進、②金融業界内の情報共有体制の整備、③新しい情報セキュリティ技術の研究開発といった役割を担う。

- 最近の主な研究テーマ
  - 高機能暗号の金融分野での活用
  - APIのオープン化のセキュリティ
  - 生体認証システムのセキュリティ

研究成果は、金融研究所ディスカッション・ペーパーとして公表するほか、情報セキュリティ・シンポジウムにおいても発表。
（URL: http://www.imes.boj.or.jp/citecs/）

第17回情報セキュリティ・シンポジウム
（2016年3月2日開催）

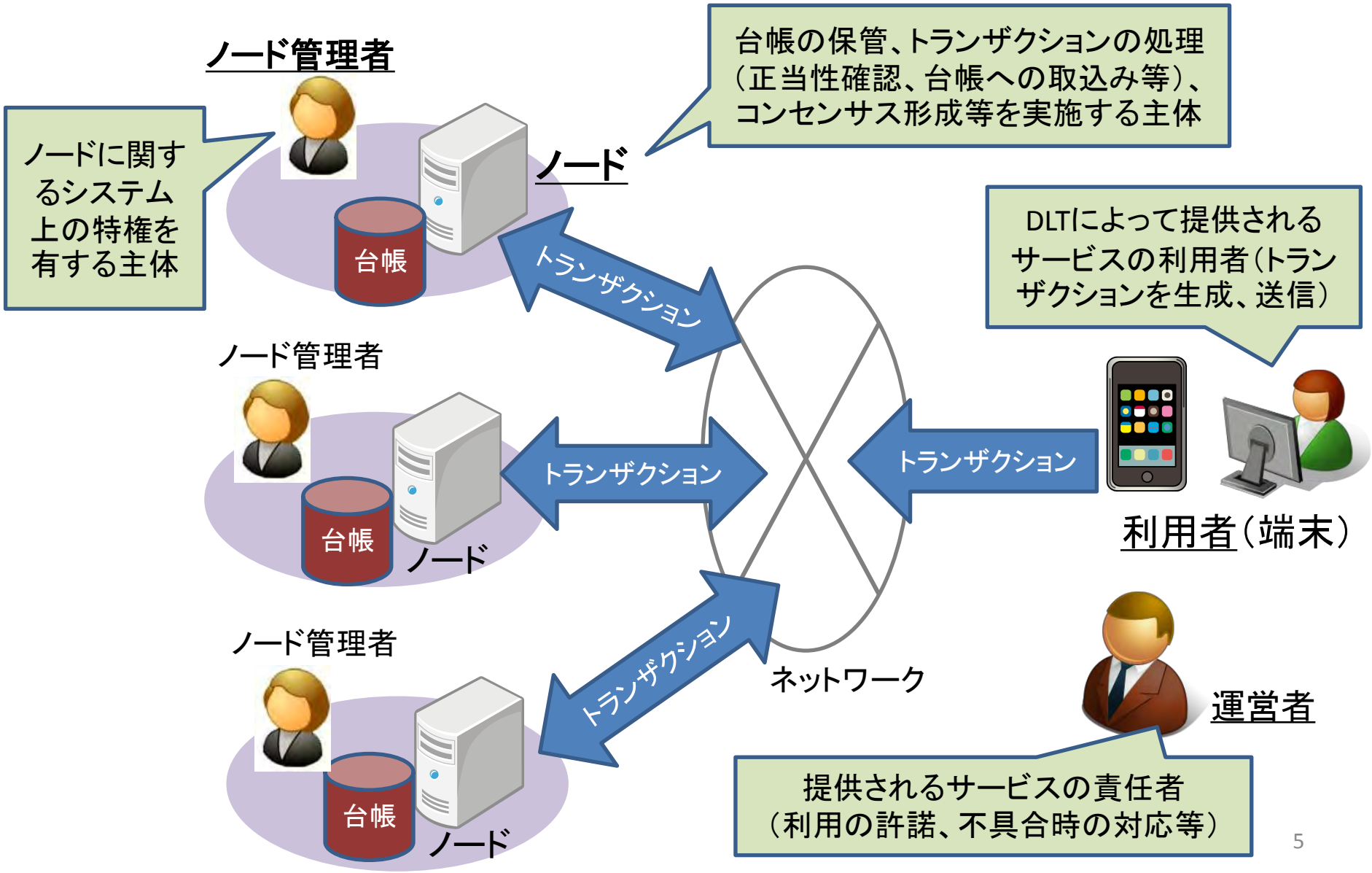
# アジェンダ

- 背景
- 分散型台帳技術と想定モデル
- セキュリティ要件の活用例
  - 自行向け口座振替処理への適用例
  - 金融機関管理型と外部業者管理型
- セキュリティ要件の詳細化と適用
- まとめ

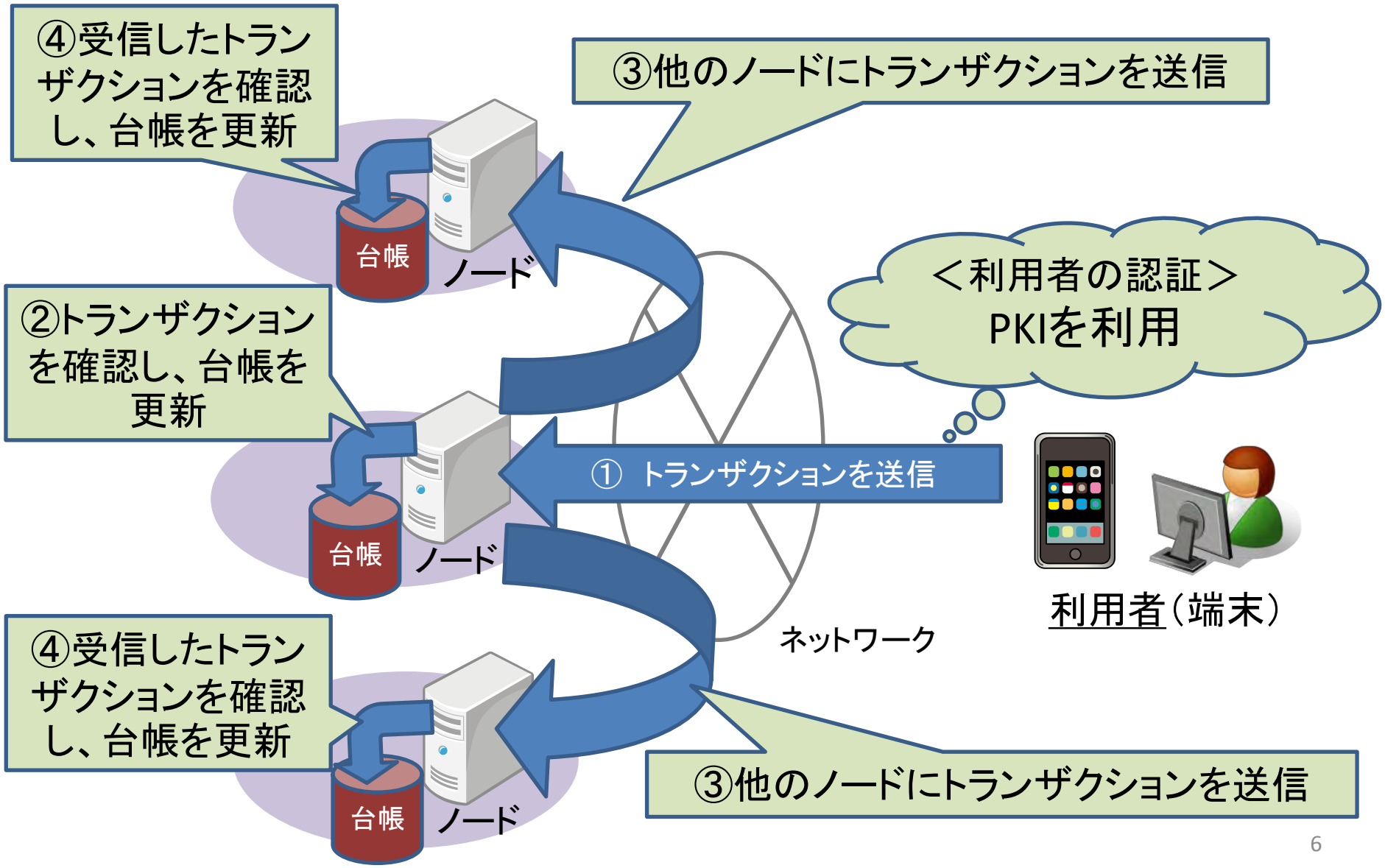
# 背景

- 分散型台帳技術（DLT: distributed ledger technology）の活用にかかる検討が進展している。
  - 分散型台帳： 適用されるサービスにおいて発生したすべてのトランザクション（個々の取引等に関する情報を定型化したもの）を集積したデータ
  - 銀行勘定系や証券決済系への適用を想定した実証実験の事例も。
- DLTにおけるセキュリティ上の留意点を明確にすることが重要。
- DLTを金融サービスに適用する場合に求められるセキュリティ要件を検討する。

# 想定するモデル


ノード管理者
台帳の保管、トランザクションの処理（正当性確認、台帳への取込み等）、コンセンサス形成等を実施する主体
ノードに関するシステム上の特権を有する主体
ノード
台帳
トランザクション
DLTによって提供されるサービスの利用者（トランザクションを生成、送信）
ノード管理者
台帳
ノード
トランザクション
トランザクション
利用者（端末）
ノード管理者
トランザクション
ネットワーク
運営者
台帳
ノード
提供されるサービスの責任者（利用の許諾、不具合時の対応等）

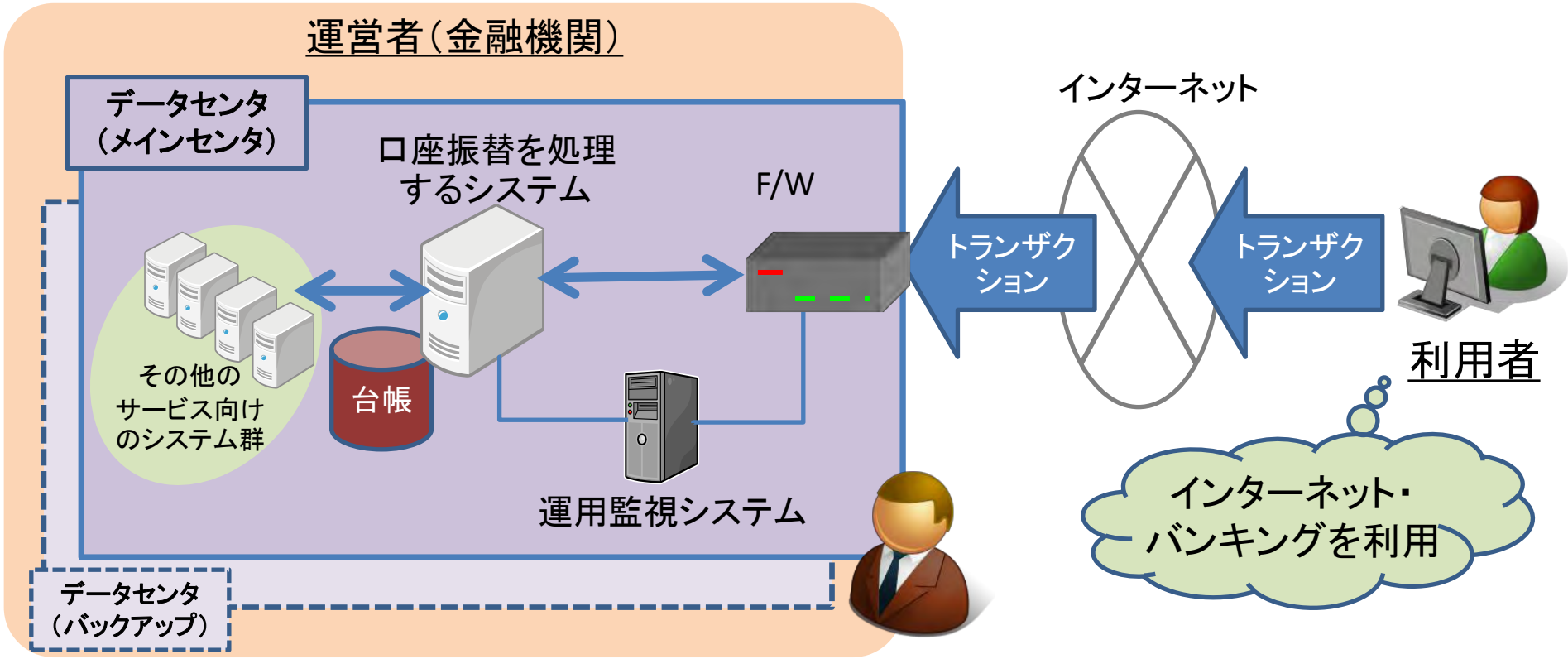
# トランザクションの処理の流れ



# 金融サービスへのDLTの適用例

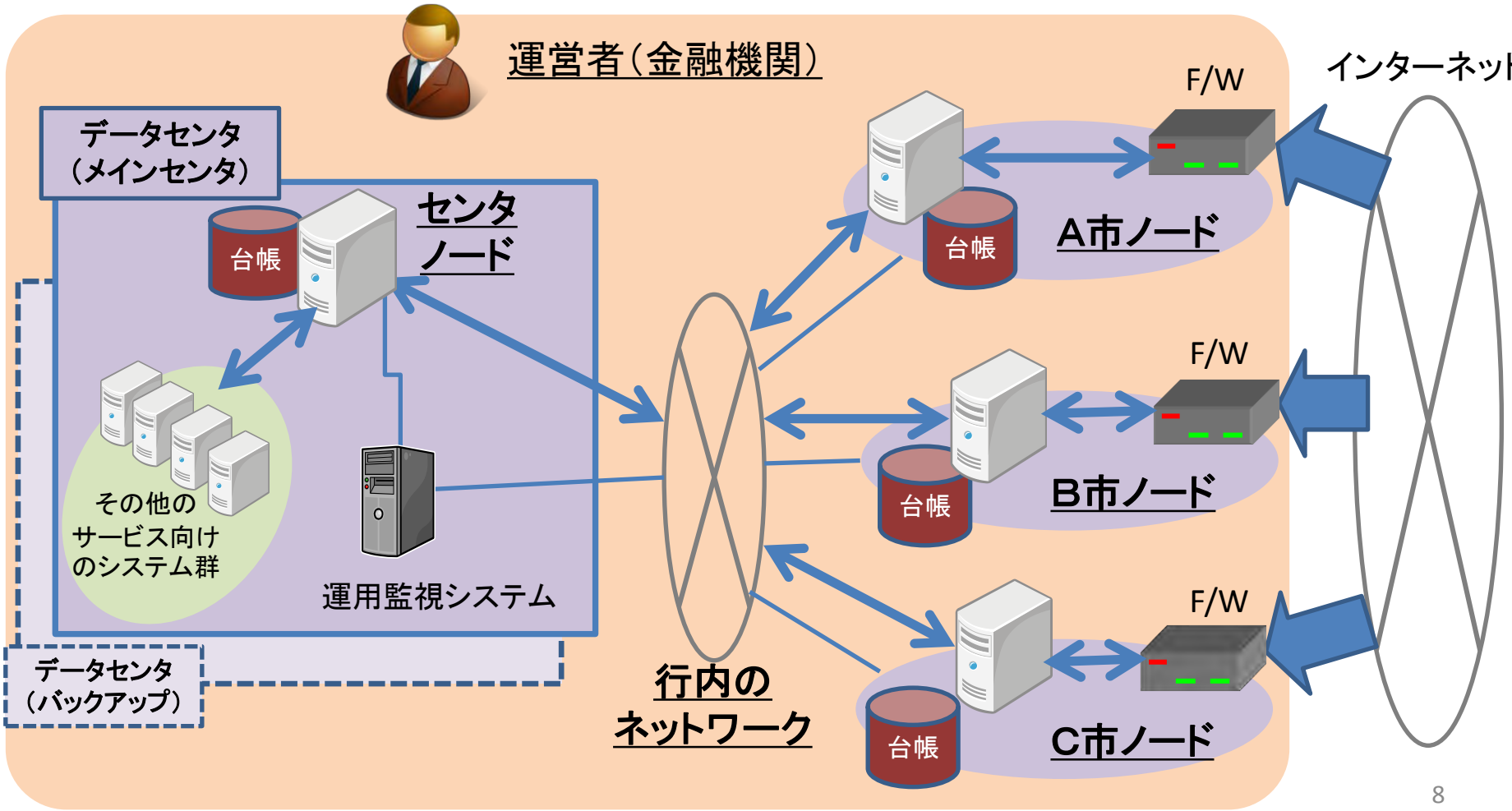
- インターネット・バンキングのうち、「自行内に閉じた口座振替処理」への適用を検討。

＜既存のシステムのイメージ＞



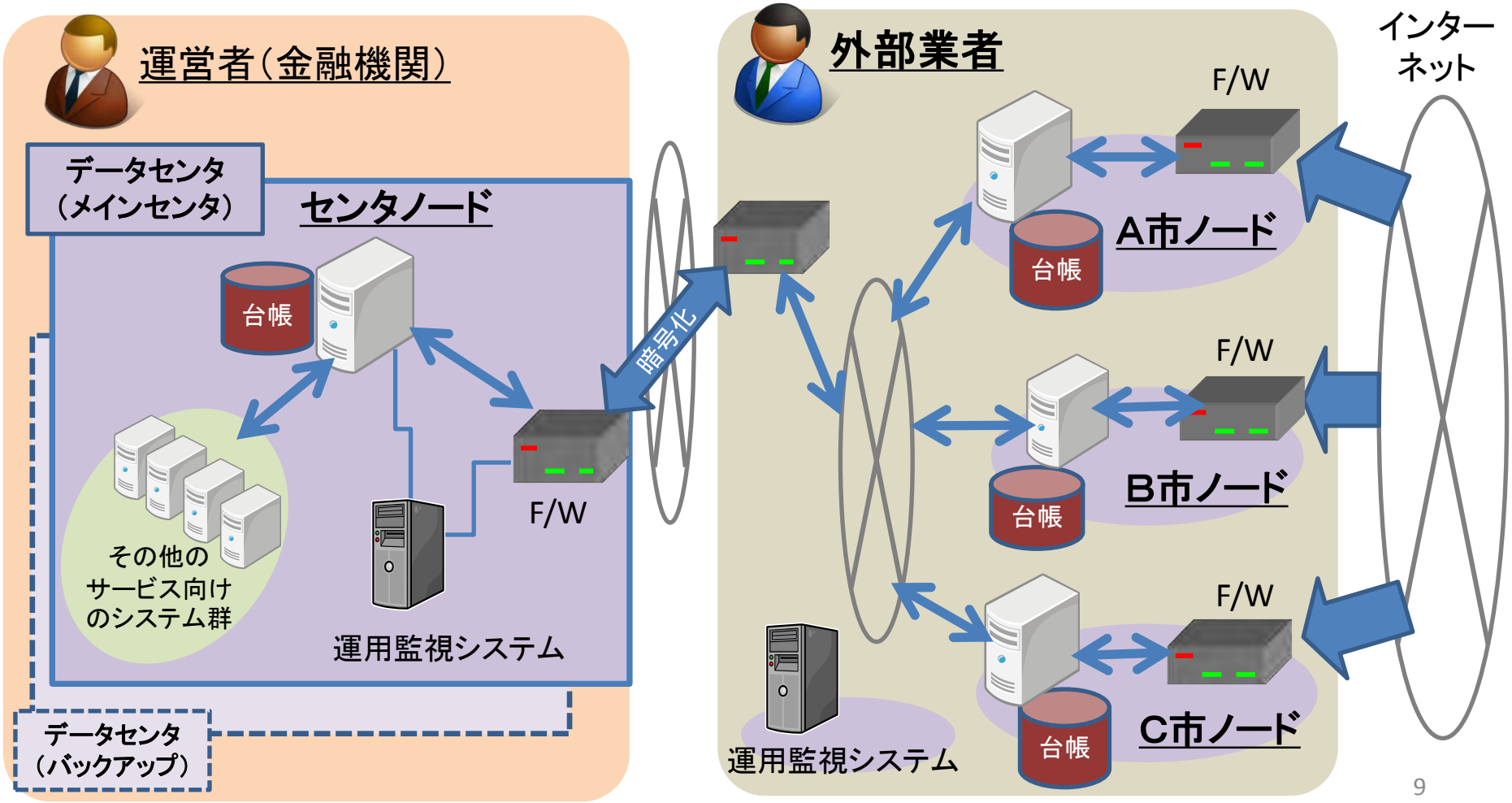
# 金融機関管理型のモデル

- すべてのノードを金融機関の施設内に設置。



# 外部業者管理型のモデル

- センタノードを金融機関の施設内に、他のノードを外部に設置。



# DLT向けのセキュリティ要件 (1)

- 自行内に閉じた口座振替処理にDLTを適用するケースを想定し、主なセキュリティ要件を導出。
  - 金融機関管理型と外部業者管理型にセキュリティ要件を適用する場合の留意点等を考察。

- セキュリティ要件として、機密性（confidentiality）、完全性（integrity）、可用性（availability）に焦点を当てる。
  - 保護対象資産は「台帳」と「トランザクション」。
  - 前述の「想定するモデル」に各要件を当てはめて、セキュリティ要件を細分化。

# DLT向けのセキュリティ要件 (2)

| 大分類 | 中分類 | | 小分類 |
|---|---|---|---|
| 機密性 | ノード上の機密性 | 認証 | 利用者認証 |
| | | | ノード間での認証 |
| | | 認可 | 台帳へのアクセス制御 |
| | 通信経路上の機密性 | | 通信経路上のデータの暗号化 |
| 完全性 | 台帳の完全性 | | 台帳の改ざんの防止・検知 |
| | | | ノード間での台帳の不整合の解消 |
| | トランザクションの完全性 | | トランザクションの正当性確認 |
| | | | 取引認証 |
| 可用性 | 台帳の消失防止 | | (ノードでの)台帳の消失防止 |
| | | | システム全体での台帳の消失防止 |
| | 大規模被災への対策 | | 広域被災時等におけるサービスの継続 |

# 金融機関管理型へのセキュリティ要件の適用

| セキュリティ要件 | | 要件の充足例（留意点） |
|---|---|---|
| 機密性 | 利用者認証 | クライアント証明書による認証等 |
| | ノード間での認証 | VPN等によるノード間の安全な接続 |
| | 台帳へのアクセス制御 | ノードのプログラムによる一元管理 |
| | 通信経路上のデータの暗号化 | SSL/TLSによる暗号化等 |
| 完全性 | 台帳の改ざんの防止・検知 | ノードへの適切なパッチ適用等 |
| | ノード間での台帳の不整合の解消 | ノード間での台帳の内容の調整 |
| | トランザクションの正当性確認 | トランザクションの署名の検証 |
| | 取引認証 | （実装に向けた検討が望まれる） |
| 可用性 | （ノードでの）台帳の消失防止 | 台帳の定期的なバックアップ取得等 |
| | システム全体における台帳の消失防止 | ノードの地理的分散配置等 |
| | 広域被災時等におけるサービスの継続 | |

# 外部業者管理型へのセキュリティ要件の適用

| | セキュリティ要件 | 「金融機関管理型」での要件の充足例（留意点） | 「金融機関管理型」との差異 |
|---|---|---|---|
| 機密性 | 利用者認証 | クライアント証明書による認証等 | ―― |
| | ノード間での認証 | VPN等によるノード間の接続 | 外部業者との安全な通信 |
| | 台帳へのアクセス制御 | ノードによる一元管理 | **外部業者からの台帳へのアクセスを制御するか** |
| | 通信経路上のデータの暗号化 | SSL/TLSによる暗号化等 | ―― |
| 完全性 | 台帳の改ざんの防止・検知 | ノードへの適切なパッチ適用等 | ―― |
| | ノード間での台帳の不整合の解消 | ノード間での台帳の内容の調整 | ―― |
| | トランザクションの正当性確認 | トランザクションの署名の検証 | ―― |
| | 取引認証 | （実装に向けた検討が望まれる） | ―― |
| 可用性 | （ノードでの）台帳の消失防止 | 台帳の定期的なバックアップ取得等 | ―― |
| | システム全体における台帳の消失防止 | ノードの地理的分散配置等 | **外部業者の施設を利用することで、地理的分散の選択肢が拡大する可能性** |
| | 広域被災時等におけるサービスの継続 | | |

# まとめ

- DLTにおけるセキュリティ要件を抽出
  - 機密性、完全性、可用性の観点からセキュリティ要件を詳細化。
- 活用例として、インターネット・バンキングでの自行内の口座振替処理への適用について考察
  - 機密性の観点では、外部業者にノードの管理を依頼する場合、外部業者からの台帳へのアクセスの制御が主な留意点。
  - 完全性の観点では、ノード間での台帳の内容の調整、取引認証の実現が主な留意点。
  - 可用性の観点では、外部業者の施設活用によって可用性が向上する可能性がある。
- 個別のアプリケーションと実装方法を前提に、セキュリティ要件をさらに詳細化し、それらの項目の充足方法を検討することができる。
  - セキュリティ要件を充足するように実装方法を事前に決定しておくことで、セキュリティに配慮した実験等が実施可能になる。