IMES DISCUSSION PAPER SERIES

分散台帳技術のセキュリティ要件：
銀行口座振替処理への適用

沖野（おきの） 健一（けんいち）

Discussion Paper No. 2017-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2017-J-6
2017 年 3 月

分散台帳技術のセキュリティ要件：銀行口座振替処理への適用

沖野（おきの） 健一（けんいち）*

要　　旨

本稿では、分散台帳技術を金融サービスに適用する際のセキュリティ要件を検討する。最初に、分散台帳技術を利用して金融サービス、特に、自行内口座振替をインターネット経由で処理するケースを想定し、モデル化を行う。次に、機密性、完全性、可用性にかかるセキュリティ要件を示し、こうした要件に沿って、セキュリティ評価を行う。その結果、分散台帳技術は、実装を適切に行うことによって、既存のインターネット・バンキングにおいて要求されるデータの機密性や完全性のレベルを概ね維持しつつ、データの可用性を高め得ることが示された。

キーワード：インターネット・バンキング、基幹系システム、口座振替処理、セキュリティ要件、ブロックチェーン、分散台帳技術

JEL classification: L86、L96、Z00

*　日本銀行金融研究所企画役補佐（E-mail:kenichi.okino@boj.or.jp）

本稿の作成に当たっては、セコム株式会社 IS 研究所主任研究員の佐藤雅史氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

分散台帳技術（distributed ledger technology）は、取引等の記録を、事後的に変更不可能なかたちで行い、複数のエンティティ間で共用するとともに、複数のエンティティの各々において保存する技術といえる（Mainelli and Milne [2016] p.3）。もともと、この技術は、ビットコイン等、仮想通貨の世界において、ユーザーが取引等を記録したデータベースを共用するために開発されたものであるが、最近では、さまざまな方面への応用が検討されている（European Central Bank [2016]）。

わが国でも、三菱UFJフィナンシャル・グループが「MUFG コイン」の開発を進めていると報じられたほか（岡部［2016］）、みずほ銀行、富士通、富士通研究所が共同でブロックチェーン技術[1]の証券決済分野への適用を想定した実証実験を行ったと発表した（みずほ銀行・富士通・富士通研究所［2016］）。また、日本取引所グループも、証券市場における分散台帳技術の活用の可能性について、実証実験を通じて得た知見をもとに、ワーキング・ペーパーを発表した（日本取引所グループ［2016］）。

これらに加え、いわゆる「基幹系」と呼ばれる預金口座への振込や入出金等の業務への適用を検討する事例（吉本［2016］）もみられる。一般に、こうした基幹系業務を担うシステム（以下、「基幹系システム」という）の構築・維持管理にかかるコスト負担は重く、金融機関では、そうしたコストの削減が長年の課題となっている。分散台帳技術は、基幹系システムの構築・維持管理にかかるコストを大幅に削減できる可能性を持つものとして注目を集めている（吉本［2016］）。

もちろん、セキュリティをはじめとして、そうした新技術を金融サービスに適用する際に考慮すべき論点が多数存在している。例えば、分散台帳技術を金融サービスに適用する場合、「取引のデータの機密性は従来のシステムと同様に維持されるのか（口座の残高や送金履歴が第三者に漏れることはないか）」、「送金は確実に実行されるのか」、「口座の資金が攻撃者に盗取されることはないか」といった安全性上の留意点が考えられる。筆者の知る限り、こうした論点を具体的な事例に即して検討・考察した研究成果は、これまでのところ報告されていない[2]。

本稿では、分散台帳技術を金融サービスに適用する場合に求められるセキュ

1 みずほ銀行・富士通・富士通研究所［2016］では「ブロックチェーン技術」を、「ネットワークに接続された複数のコンピュータが取引記録などを共有し、相互に検証する仕組み」と定義している。実質的には分散台帳技術のことを指していると考えられる。

2 分散台帳技術の他の応用例であるビットコインに関する分析では、例えば Bonneau *et al.* [2015] のような研究成果が、数多く報告されている。

リティ要件を検討するとともに、それに基づいた現時点での評価を報告する。最初に、分散台帳技術の概要を説明し、同技術を金融サービスに適用する場合、機密性、完全性、可用性、それぞれについて、どのような項目をセキュリティ要件として設定すべきかを示す。

次に、そうしたセキュリティ要件の具体的な活用例として、基幹系システムのうち、インターネット・バンキングのシステムに分散台帳技術を適用するケースを想定し、必要なセキュリティ要件を充足させる方法について検討する。インターネット・バンキングを例として取り上げるのは、これまでに開発された分散台帳技術のほとんどが、インターネットの利用を前提に開発されてきたからであり、もともとインターネットとの親和性が高いからに他ならない。

とりわけ本稿では、インターネット・バンキングのうち、自行内の決済性預金口座間の振替で完結することができるサービス（自行内送金、残高照会、振替明細の出力等。以下、「自行内口座振替処理」という）にフォーカスし、ここに分散台帳技術を適用するケースを考える。その際、自行内口座振替処理をすべて自行内で行うケースと、一部または全部を外部業者に委託するケースに分けて考察する。

本稿の主な考察結果を先取りすると以下のとおりである。分散台帳技術を用いて自行内口座振替を処理する場合、実装を適切に行うことによって、既存のインターネット・バンキングにおいて要求されるデータの機密性や完全性のレベルを概ね維持しつつ、データの可用性を一段と高めることが可能になる。ただし、一部のインターネット・バンキングで提供されている取引認証（金融取引の内容がサービス利用者の意図したとおりであることを金融機関が確認すること）については、具体的な実装方法に依存するため、一般的な評価を行うことは難しい。

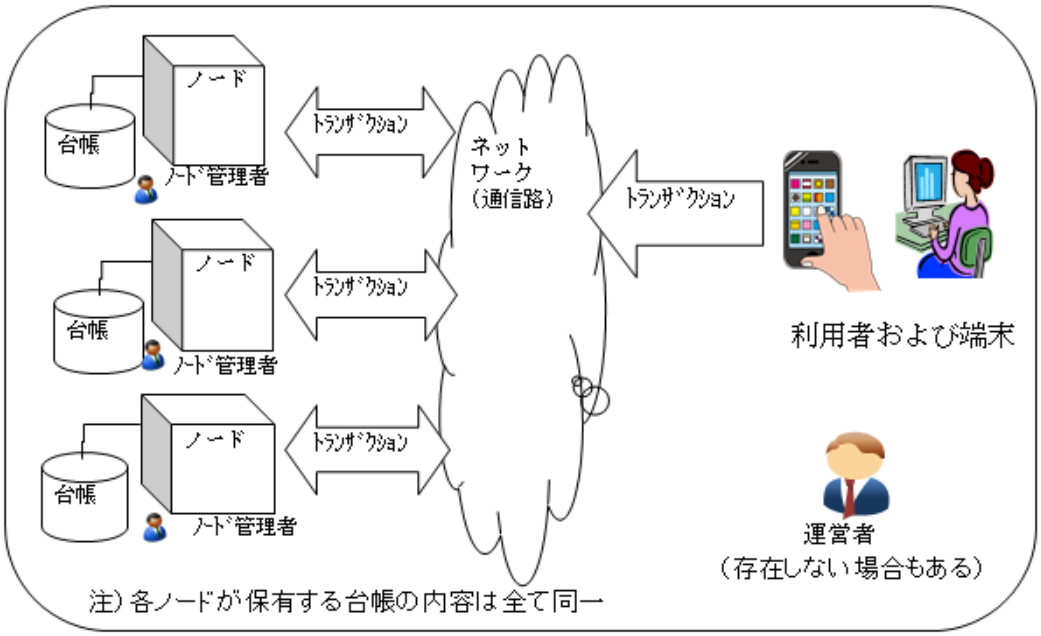
本稿の構成は以下のとおりである。2 節では、分散台帳技術の概要を紹介するとともに、分散台帳技術を用いて自行内口座振替処理を行うフローを概説する。3 節では、分散台帳技術を金融サービスに適用する際に必要となるセキュリティ要件について検討し、現時点での評価を行う。4 節は、むすびである。

２． 分散台帳技術と銀行口座振替への応用

（１）分散台帳技術の基本モデル

分散台帳技術は、いつくかの基本的な構成要素から成り立っている（図表 1）（Hancock and Vaizey [2016]）。「台帳」とは、サービスを提供する過程で発生する全てのトランザクション・データ（個々の取引等に関する情報を定形化した

図表1．分散台帳技術のモデル



データ）を集積したものを指す[3]。

「利用者」とは、分散台帳システムによって提供されるサービスを利用するために端末（パソコンやスマートフォン等）でトランザクションを生成する主体を指す。

「ノード」は、自ら台帳を保有し、利用者が生成・送信したトランザクションを受信し、正当性を確認する[4]（台帳への取込み可否の判定）。また、利用者から受信したトランザクションのうち正当性確認済のものや他のノードから受信したトランザクションを台帳に取り込んで、他のノードへ送信する[5]。他のノードの台帳との間で差異が生じた場合には、コンセンサスの形成（正しいノードの判定と、それに従った台帳の修正）を行う。併せて、台帳の内容に対する利用者からの問合せに応じる。

「運営者」とは、分散台帳システムが提供するサービスに対する責任を持つ

3 新たなトランザクションを台帳に追加・集積することを、本稿では、（トランザクションを台帳に）「取り込む」という。

4 正当性の確認の具体的な内容は実装に依存するが、少なくとも、①トランザクションに対する利用者による署名の検証（トランザクションの偽造、改ざんの検知）、②「不整合トランザクション」の検知（既に当該ノードの台帳に取込み済のトランザクションと矛盾しないかの検証。例えば、過去に送金済の資金を利用して別の先に送金するトランザクションでないか等）の検知が必要となる。

5 正当性確認において、他のノードでの実施結果を信頼する（すなわち、自ノードでの確認を省略する）か否かは、実装に依存する。一般的には、他のノードでの実施結果を信頼しない場合、全ノードで同一の正当性確認を行う必要がある。逆に、他のノードでの正当性確認の結果を信頼する場合には、それに先立つノード間認証の厳格化や、ノード間での台帳の不整合を回避するために、極力短い周期でコンセンサス形成を行うなどの対応が必要であると考えられる。

主体（組織、または、組織の集合体）を指す。運営者は、利用者へのシステム利用の許諾（ID やクライアント証明書の利用者への発行等）や、システムに不具合が発生した場合の対応（原因調査、問題解決等）を行う。個々のトランザクションの処理においては、必ずしもエンティティとして登場しないことも想定される。また、運営者が存在しないケースもある[6]。

（２）プライベート型分散台帳システム

一般に、分散台帳システムは、利用者の参加形態と運営者の性格によって、パブリック型、コンソーシアム型、プライベート型の 3 つに分類される。このうち、利用者が限定されており、単一の運営者が存在するものを「プライベート型分散台帳システム」という。本稿では、プライベート型にフォーカスして、分散台帳技術の応用を検討する。

サービスの提供に責任を持つという運営者の基本的な役割に照らせば、台帳を正しく維持し続けることが、運営者に期待されている役割の一つであることは言うまでもない。一方、ノードも、台帳を正しく維持する役割を担うエンティティである。したがって、ノード管理者が運営者と同一、または、運営者の支配下にあるとするのが自然である[7]。そこで、以下では、特に断らない限り、ノードと運営者が一体化したプライベート型分散台帳システムを前提に説明を行う。

プライベート型分散台帳システムにおける処理の流れは、例えば、以下の①～④のようになる（図表 2）[8]。

① 利用者は、端末でトランザクションを生成し、いずれかのノード 1 台に送信する。どのノードを選択するかは、実装に依存する[9]。

---

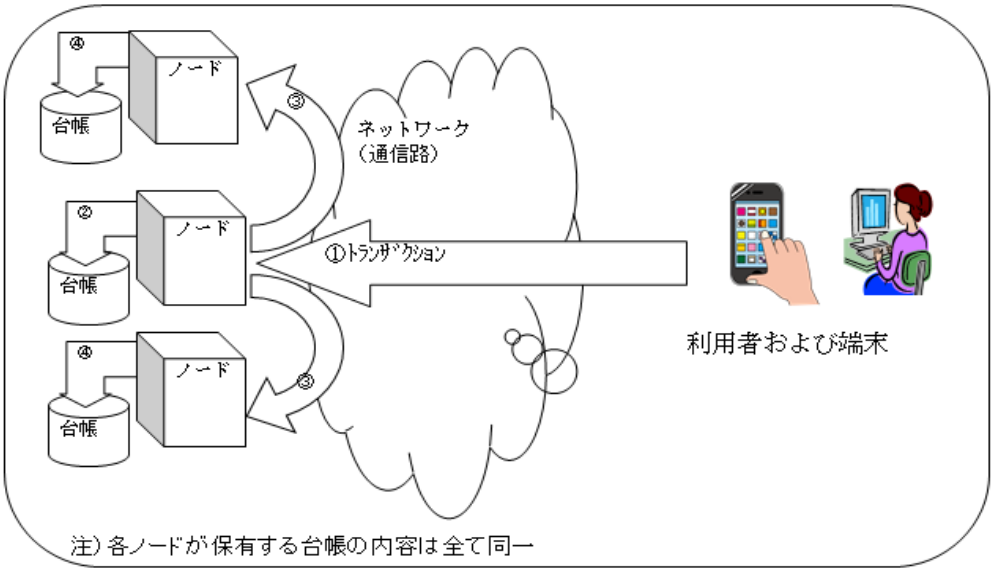
6 例えば、ビットコイン（Nakamoto [2008]）やイーサリアム（Buterin [2014]）は、運営者が存在しないシステムといえる。これらを、本稿では、「非集権型分散台帳システム」という。

7 なお、前述の非集権型分散台帳システムは、ノード間が対等でかつお互いに全く信頼を置かないことを前提としており、コンセンサス形成について大きなコスト（例えば、膨大なハッシュ計算の実施など）をかけざるを得ない。これに対し、プライベート型分散台帳システムでは、各ノードの管理者にある程度信頼を置くことを前提としていることから、厳密な合意形成の仕組みの構築を省略し、その分安価なコストの（同じコストならばより性能の高い）システムを構築可能と考えられる。その反面、プライベート型分散台帳システムでは、非集権型分散台帳システムのような、不正ノードの排除機能が当然に備わっていることを期待して議論するのは危うい。このため、本稿においても、そうした機能を前提としない。

8 この処理の流れの検討にあたっては、代表的な分散台帳技術として知られており、広く仕様が公開されているビットコインとイーサリアムを参考にした。ここでは、利用者が 1 つのノードにのみトランザクションを送信する例を示したが、利用者が P2P ネットワークを通じて複数のノードに同じトランザクションを送信し、重複したトランザクションの整理（具体的には重複の排除）をノード間の調整に一任する実装も考えられる（ビットコインの実装はそれに近い）。

9 例えば、DNS から IP アドレスをラウンドロビンで引いてくる（アクセスして反応がなければ、次の IP を引く）方法や、逆に、通信中は定期的に全ノードの IP アドレスのリストを配信してお

図表2. 分散台帳技術における処理の流れ



② トランザクションを受信したノードは、必要に応じて正当性確認を行ったうえで、自分の台帳を更新する[10]。

③ 他のノードに当該トランザクションを転送する。

④ 転送されたトランザクションを受信したノードは、必要に応じ正当性確認を行ったうえで、自分の台帳を更新する。

これらの処理を各ノードが単独で、他のサーバやシステムに頼らずに行うことで、可用性が向上したり（いずれか一つのノードが稼働していればサービスを継続可能）、改ざんが困難になったりする（少なくとも過半数のノードの台帳が同時に改ざんされない限り、ノード間の台帳の照合で正しく修正可能であり、改ざんが失敗に終わる）。

当該システムの利用を希望する者を利用者として登録する手続きについては、一般的な PKI（公開鍵基盤）における認証機関（Certification Authority）が実施する（クライアント証明書を発行する）ことを想定する[11]。この場合、利用者の認証は同じ PKI を使って行うのが自然である。このため、利用者の ID／パスワードを管理するシステムを別途構築することは想定しない。

き、端末はその中からランダムに接続先ノードを選定するなどの方法が考えられる。

10 台帳の更新方法としては、正当性の確認が終了したトランザクションを台帳の末尾に付加していく方法等が考えられる。

11 分散台帳技術では、トランザクションの署名と検証に公開鍵暗号技術を利用するケースが一般的である。この場合、利用者が秘密鍵を紛失すると運営者が復旧対応を行う必要が出てくる。こうした問題に備えて、ここでは PKI の利用を想定する。

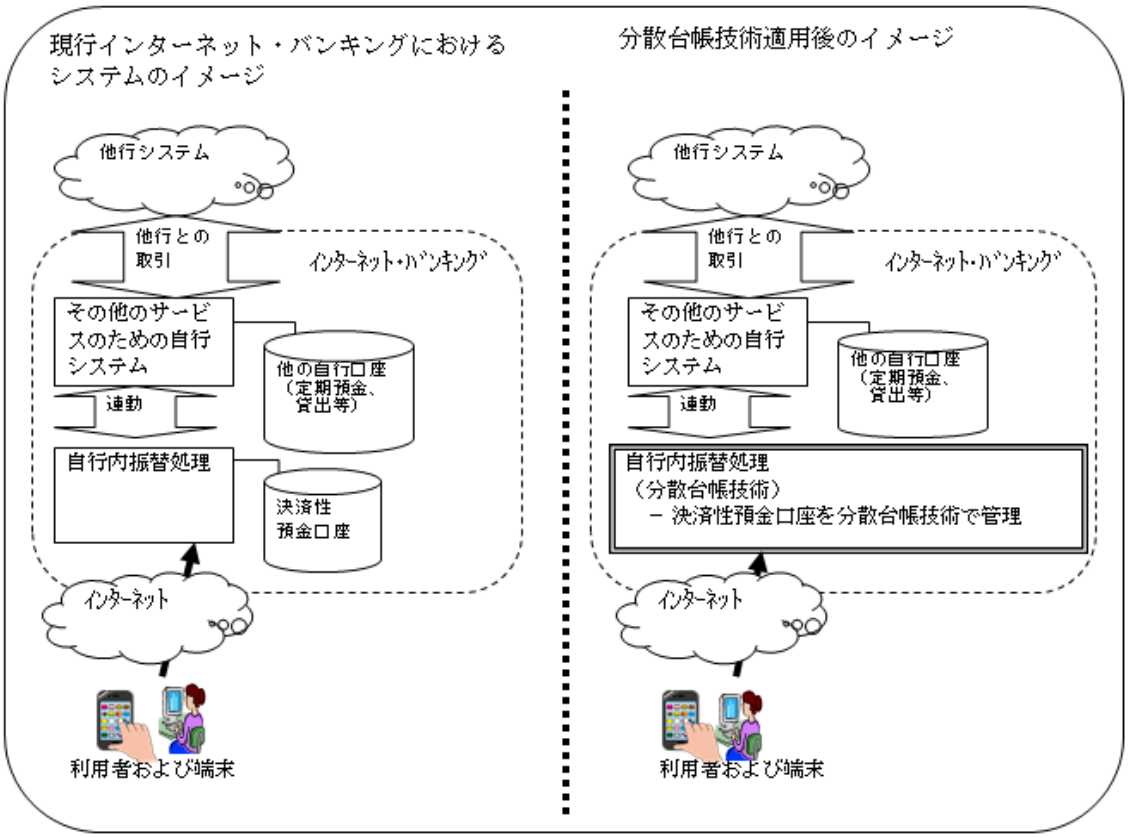
（３）口座振替処理のモデル化

分散台帳技術は汎用性の高い技術であり、すでに、さまざまな分野で応用を模索する動きがみられる。本稿では、金融分野への応用例として、インターネット・バンキングで行う自行内口座振替処理に、分散台帳技術を利用するケースを取り上げる（図表 3)。最初に、現行の口座振替処理を模式化し、次に、これをどのようにして分散台帳技術で実現することが可能かを示す。

イ．現行の口座振替処理

インターネット・バンキングで提供される主なサービスには、残高照会、入出金明細の表示、および、自行に開設された口座間の振替や他行の口座への振込（以下、両方をまとめて「送金」という）がある。また、その他の付加サービスとして、金融商品（定期預金、外貨預金、投資信託等）の預入・解約・売買等、ローン借入等がある。これらは、①自行に開設された決済性預金口座の口座間の振替だけで実現できるサービス（自行内送金、残高照会、振替履歴明細の出力等）と、②それ以外の口座等へのアクセスや他行等との取引が必要となるサービス（定期預金の預入・解約、外貨の購入・売却、他行への送金等）

図表3．自行内口座振替処理に分散台帳技術を適用するイメージ



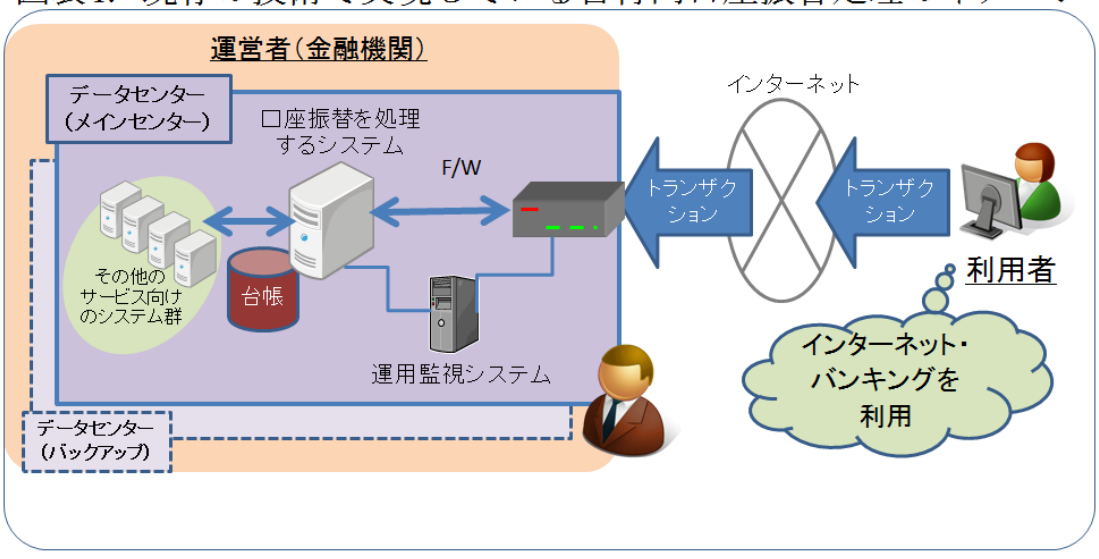
この図表の作成にあたっては、金融情報システムセンター［2015］129頁を参考にした。

に分類される。

本稿では、「自行内口座振替処理」にフォーカスして、分散台帳技術の応用可能性について検討する[12]。具体的には、①における決済性預金口座の管理、その利用者とのインタフェース、および、②のサービス提供に伴う決済性預金口座の残高の変動等の管理に、分散台帳技術を適用する。①に含まれるサービスは、決済性預金口座の残高等の管理により完結するのに対し、②のサービスは、それに伴う決済性預金口座残高の変動の管理に加え、他の口座（例えば、定期預金口座）の管理、他行への振替依頼等、追加的な処理を伴う。本稿では、①と②のサービスを提供する際に必要となるシステム間の連動を司るシステムや処理については、分散台帳技術を用いず、従来と同様のシステムで管理すると想定する。

図表 4 は、既存の技術で実現している自行内口座振替処理のイメージを示したものである。利用者からのトランザクションの全てをデータセンターで受信し（メインセンターの他にバックアップセンターを備える場合もある）、データセンター内の勘定系システムで集中的に処理する。その後、必要に応じて、その他のサービス（定期預金の管理や他行への送金等）を処理するための自行システムにつなぐ。このシステムでは、インターネットからの不正侵入に備えて、接続口にファイアウォール（Firewall: F/W）を設置しているほか、勘定系サーバや F/W の稼働状況を常時監視し、異常検知時に警報を発する運用監視システムを備えているのが一般的である。

図表4. 既存の技術で実現している自行内口座振替処理のイメージ



12　残高や入出金の明細は、ウォレットと呼ばれる専用のアプリケーションがノード上のプログラムに情報を要求し、当該プログラムから返された情報が端末のウォレットに表示される仕組みとする。

ロ．分散型台帳による口座振替

先の図表 4 は、自行内口座振替処理のイメージをおおまかに図示したものである。ここからさらに進んで、具体的な検討を始めるにあたり、運営者である金融機関が、すべてのノードの管理を行うか、あるいは、一部のノードの管理を他者（例えば、外部業者）に任せるか、を区別しておく[13]。「金融機関管理型」では、運営者である金融機関がノード管理者として、自らの施設内で全てのノードを運営する。一方、「外部業者管理型」では、運営者である金融機関が「センターノード」[14]（データセンターにある既存の自行システムと直接接続し連動を行うノード）のみを管理し、他のノードの管理を外部業者等に任せる。以下、これら 2 つのケースそれぞれについて、プライベート型分散台帳システムをどのように構築するかを提示する。

まず、金融機関管理型の概要は次のとおりである。

① 全てのノードを金融機関の施設内に設置する。
② ただし、ノードをデータセンターに集中せず、分散させる。例えば、金融機関のデータセンターと複数の支店にノードを設置する。
③ 各ノードと利用者の間の通信は、データセンターを経由せず、SSL 通信等によって暗号化した上で、インターネットを介して実施される。それに先立ち、ノードは認証機関が発行したクライアント証明書の提示を利用者に要求し、認証を行う。なお、ノードの設置場所において直接インターネットと接続することから、F/W をノードと共に各地に設置する。
④ 各ノードは、利用者から受信したトランザクションを自らの保有する台帳に取り込む。同時に、他のノードに、当該トランザクションを送信する。
⑤ 各ノードは、他のノードから受信したトランザクションを自らの保有する台帳に取り込む。
⑥ 各ノードは、他のノードと適宜のタイミングで台帳を照合し、不整合であれば、いずれの台帳を採用すべきかを自動的に判定し、その台帳に合わせる（照合のタイミングや方法、残すべき台帳の判定方法等は、分散台帳技

13ノードの管理を全く行わない（全てのノードを外部業者に任せる）という第 3 のケースも論理的にはありうる。実際、一部の金融機関では、システムの運用管理を直接自行で行わずに共同センターを利用している。この場合、扱う情報（特に個人情報）の管理について、契約等により、金融機関側のガバナンスが確保されているかという点が問題となる。この点、すべてのノードを 1 つの外部業者のみに任せる場合は、後述の「金融機関管理型」を、複数の外部業者に任せる場合は後述の「外部業者管理型」を、それぞれ参考にして検討することが可能と考えられる。

14 センターノードは、既存の自行システムとの連動の要であり、その障害は業務に重大な影響を及ぼすため、可用性確保の観点から、複数（可能であれば複数のサイトに）設置する設計が望ましい。もっとも、こうした設計は、シングルポイントになりやすい連動部分について一般的に考慮するものであり、分散台帳技術の採用と直接関係するわけではない。

術の実装に依存する)。

⑦ センターノードは、その他のサービスのために、自行システムと連動する。このステップの内容は、既存のシステムと同様である。

⑧ 各ノードや F/W の稼働状況は、行内ネットワークを介して、データセンターの運用監視システムが一括監視する。

分散台帳技術を採用した場合、あるノードに不具合が生じれば、残りのノードが、その管理を「肩代り」する必要がある。しかし、相応の能力を備えたノードや F/W、高速インターネット回線等を準備するための負担は小さくない。したがって、比較的規模の小さな金融機関は、支店の数も少なく、ノードに不具合が起こった場合にそれを「肩代り」する余裕がないことも考えられる。こうした点を踏まえると、金融機関管理型を採用できるのは、メガバンク等の一部の金融機関に限られ、それ以外の比較的小規模の金融機関では、金融機関管理型よりも、以下に説明する外部業者管理型を採用する方がリーズナブルである。この場合、金融機関は、他のシステムとの連携に必要なセンターノードのみを残し、他のノード、F/W、インターネット接続回線、運用監視システム等を外部業者に任せることができる。

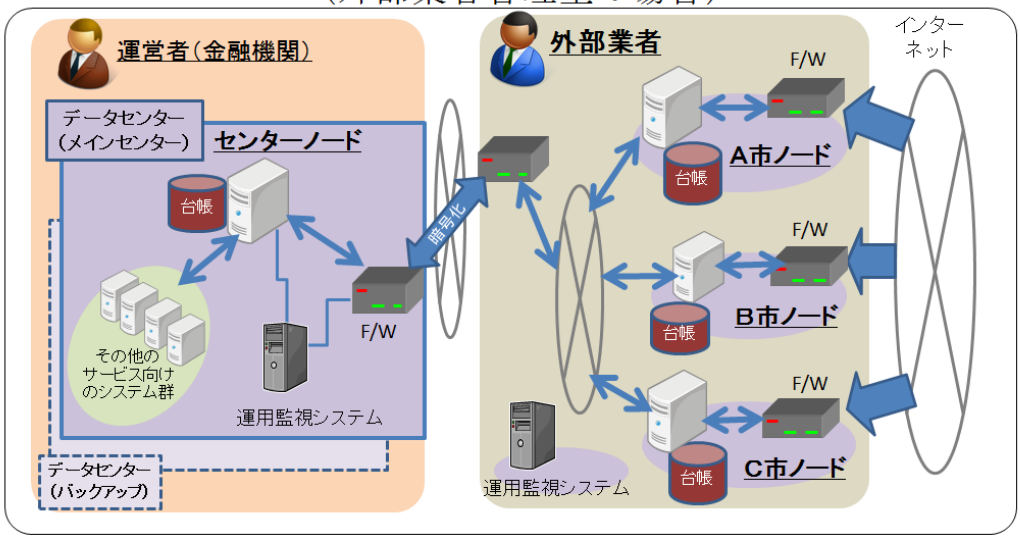
外部業者管理型の概要は次のとおりである（図表 5)。

① 金融機関は、センターノードのみを施設内に設置・管理する。その他のノードの管理は外部業者に一任し、設置場所も外部業者の施設内とする。

② 被災対応力を向上させるために、ノードを広く各地に分散させる。

③ ～⑦　金融機関管理型と同じ。

図表5. 分散台帳技術で自行内口座振替処理を実現するイメージ
（外部業者管理型の場合）



⑧ 金融機関は、センターノードのみの運用を監視する。センターノード以外のノードおよびF/Wの稼働状況は、運用監視システムのネットワーク構成を含めて外部業者に一任し、外部業者のデータセンターにて一括監視する。

３．分散台帳技術のセキュリティ要件と評価

（１）セキュリティ要件

本節では、分散台帳技術を金融サービスに応用する場合に最低限必要となるセキュリティ要件を整理する。これまでに説明したとおり、本稿では、分散台帳技術を自行内口座振替に応用するケースを念頭に置いている。セキュリティの観点からこれをみると、①顧客の財産の残高を管理するものであること、②当該財産の移転に関する顧客からの指示や処理結果の通知がインターネットを通じて行われることの 2 つが最も重要な論点となる。もちろん、性能や使い勝手、コスト等も重要な評価軸ではあるが、これらは具体的な実装の仕方に依存するため、一般的な評価はできない。このため、本稿では評価の対象としない。

図表 6 は、分散台帳技術を口座振替に応用する際に検討すべきセキュリティ要件を、既存のインターネット・バンキングによる処理を比較対象として整理したものである。ここでは、台帳およびトランザクションを、守るべき情報資産と考え、機密性、完全性、可用性を確保する際に求められるセキュリティ要件を導出した[15,16]。こうした情報資産にかかるシステム評価の方法は、ISO/IEC 27000 シリーズ等、特に、金融サービス関連の ISO/IEC TR 27015 (ISO/IEC [2012]) の考え方とも整合的である。

イ．機密性

本稿では、情報資産へのアクセスが発生する可能性のある場所を「ノード上」と「通信経路上」の 2 つに分類した。ノード上でのアクセスについては、利用者認証が必須の要件であり、加えて、偽のノードが正当なノードになりすましてアクセスを試みる場合に備えたノード間認証も必要である。場合によっては、ノード間通信をセキュアなネットワーク内に限定する等の対策も必要となる。また、利用者認証が完了した利用者に必要十分な権限のみを与えるために、適

15 フィンテックの分野でも、機密性、完全性、および可用性の確保を念頭においた、セキュリティガイドラインの策定に向けた自主的な取組みが進められている（落合［2016］）。

16 志茂［2016］では、情報セキュリティの 3 大要件（機密性、完全性、可用性）と、その他の 4 つの要件（真正性、責任追跡性、否認防止、信頼性）を分けて分析している。特に、後者の 4 つの要件については、システム構築段階での具体的な実装や設計において十分な配慮を行うべきと指摘している。なお、本稿はそうしたシステム構築に先立つ企画段階において十分に配慮すべき前者の 3 つの要件に注目するものであり、後者の 4 つの要件に十分な配慮を行うべきことを否定するものではない。

図表6．分散台帳技術を自行内口座振替処理に利用するにあたり配慮すべきセキュリティ要件

セキュリティ要件				内容等
機密性の確保	ノード上の機密性確保	認証	利用者認証	台帳に保管された利用者に関する情報（口座残高等）を利用者本人以外に開示しないためには、利用者の本人確認を実施することが必須。
			ノード間認証	通信相手のノードへの信頼を前提としたシステムを構築する場合には、偽ノードのなりすまし対策としてノードの認証が必要。
		認可	ノードによる台帳へのアクセス制御	攻撃者に情報（またはその手がかり）を与えるのを避けるために、不必要な者からのアクセスを禁止し、台帳にアクセスできる者を適切に制御することが必須。
	通信経路上の機密性確保		通信経路上のデータの暗号化	通信の傍受によるデータ漏えいを防ぐためには通信経路上でのデータの暗号化が必須。
完全性の確保	台帳の情報の完全性の確保		台帳の改ざん防止	台帳の改ざん防止は「分散台帳技術」をノードの台帳管理プログラムに忠実に実装することで担保されると思われているが、当該プログラムの不備や土台となるＯＳの脆弱性が放置されれば、攻撃者に当該プログラムが支配されかねず、台帳の情報の完全性は揺らぎかねない。このため、台帳管理プログラムやＯＳへの適切なパッチ適用が必要。
			ノード間の不整合発生時における収束処理	分散台帳の性質上、ノード間での不整合の発生は原理的に不可避であり、それを円滑かつ早期に収束させる設計が望まれる。
	トランザクションの完全性の確保		トランザクションの正当性確認	トランザクションの内容の改ざんの有無について、送信者の署名により確認。また、送信者が過去の取引と整合性のとれないトランザクション（例えば、口座残高以上の金額の送金）を送信していないかを、可能な範囲で検知することが必要。
			取引認証	利用者の端末等が攻撃者の支配下にある場合、利用者の意図しないトランザクション（別の送金先への多額の送金など）が、利用者の正当な署名が付与されて送信されそのまま処理されてしまうことを防ぐために、別のパスで利用者の意思を確認することが望まれる。
可用性の確保	台帳の消失防止		ノードにおける台帳の消失防止	ノードにおいて台帳が消失(または破損)すると、ノードはその機能を失う。分散台帳技術の一般的な理解では、台帳は他のノードから自動的にコピーされることで自然復旧するとされているが、消失・破損の状況によっては迅速な復旧は困難となる可能性がある。ノードを「業務」として運営する以上速やかな復旧が求められるためそれに備えた対応の整備が望まれる。
			システム全体としての台帳消失の防止	分散したノードがすべて(またはその大半)が破損する場合も皆無とは言えないので、それに備えた対応の整備が望まれる。
	大規模被災への対策		広域被災等の場合におけるサービスの継続	

切な認可の実施も必要となる。一方、通信経路上では、ノード上での認証の有無にかかわりなく、そこを流れるデータに誰もがアクセスできてしまうことから、これを防ぐためには、通信経路上のデータの暗号化が必須である。

ロ．完全性

分散台帳技術を利用する場合、台帳の完全性、および、台帳の更新の契機となるトランザクションの完全性の両方が必要となる。本来、外部の攻撃者にはノードへのアクセス権限が与えられていない。しかしながら、外部の攻撃者がノードのプログラムや OS 等に潜在する脆弱性を悪用してノード上の権限を不正に取得し、台帳の改ざんを行うケースも考えられるため、これに備えた対策を行うことが要件となる。また、トランザクションの完全性を確保するためには、その送信者が生成した署名の検証、および送信者の口座残高の確認が不可欠となる。なお、インターネット・バンキングを提供している金融機関の中には、マルウェア等による不正なトランザクションによる取引への対策の観点から、取引認証（取引実行に先立ち、取引を入力した手段とは別の方法で本人が取引内容を確認する仕組み）を行っているものも存在するため、これもセキュリティ要件に加えた。

ハ．可用性

本稿では、台帳の消失やシステム全体の大規模被災を検討の対象とした。現行の単一台帳システムには、権限を持たない第三者による特定のデータセンターに対する DoS（Denial-of-Service）攻撃等により、可用性が侵害されるおそれがある。これに対し、分散台帳技術を利用する場合は、複数のノードが存在するため、いずれか 1 つのノードが稼働していれば、サービスの継続が可能となり、DoS 攻撃等への耐性が一般的には向上する。このため、外部の第三者からの攻撃への対応については要件としない[17]。

（２）セキュリティ評価

ここでは、図表 6 に示したセキュリティ要件を、分散台帳技術を利用した口座振替に適用し、その充足の方法や度合いの評価を試みる。最初に、金融機関管理型のシステムについて評価を行い、次に、外部業者管理型について、金融機関管理型との差異が存在すると考えられる要件を中心に評価の結果を述べる。

[17] ただし、台帳の更新の管理を実質的に一部のノードに依存するような実装を行うと、当該ノードが攻撃等の対象となった場合には耐性が損なわれる可能性がある点には留意する必要がある。

イ．金融機関管理型（図表 7）

機密性の要件のうち、利用者認証については、金融機関が PKI の発行するクライアント証明書を利用することによって充足することができる。この場合、利用者は、トランザクションを発信する際、秘密鍵による署名を行うことによって、クライアント証明書を用いて身元を証明する必要が生ずる[18]。このため、インターネット・バンキングのように、ID とパスワードさえ記憶していれば、どの端末からでもログインが可能という形の利便性は失われる。ノード間認証に

図表7．分散台帳技術による金融機関管理型における評価・留意点等

	セキュリティ要件			金融機関管理型における評価･留意点等
機密性の確保	ノード上の機密性確保	認証	利用者認証	クライアント証明書における認証にて実現可能。なお、ID/パスワードによる認証とは違い、異なる複数の端末からアクセスしたいという利用者のニーズには対応しにくい点には留意する必要。
			ノード間認証	ノード間通信をセキュアなネットワーク内に限定することで実現可能。
		認可	ノードによる台帳へのアクセス制御	ノード上のプログラムによる一元管理にて実現可能（利用者による台帳への直接のアクセスは禁止する）。
	通信経路上の機密性確保		通信経路上のデータの暗号化	SSLによる暗号化で実現可能。
完全性の確保	台帳の情報の完全性の確保		台帳の改ざん防止	ノード上のプログラムおよびOS等への適切なパッチ適用を確実に実施することが肝要。 なお、ノード間の台帳内容の調整機能を有効に機能させるためには、一部のノードに多大な（例えば過半数の）投票権を与えないような配慮が望まれる。
			ノード間の不整合発生時における収束処理	分散台帳技術におけるノード間の台帳内容の調整機能にて実現可能。
	トランザクションの完全性の確保		トランザクションの正当性確認	トランザクションに付与された署名の検証（過去の取引と整合性のとれないトランザクションの排除については、台帳との突合などの適宜の方法）で実現可能。
			取引認証	実装に向けて今後の検討が望まれる。
可用性の確保	台帳の消失防止		ノードにおける台帳の消失防止	台帳の定期的および随時のバックアップ取得により実現可能。
			システム全体としての台帳消失の防止	ノードを地理的に分散することで実現可能。 ただし、ノード設置場所を新設するには、相応のコスト負担増につながる点には留意する必要。
	大規模被災への対策		広域被災等の場合におけるサービスの継続	

18 秘密鍵等の管理において、危殆化による鍵ペアの変更が行いにくいことなどが、分散台帳技術を普及させるにあたっての課題の 1 つとなっている。例えば、斉藤［2016］では、識別子（ユーザーID 等）と鍵ペアを分離して管理する方式が提案されている。

ついては、インターネット等の外部環境から隔離され、金融機関の管理下にあるセキュアなネットワークにノード間の通信を限定することで、要件を充足可能となる。認可については、利用者による台帳への直接のアクセスを許さず、ノード上の「台帳管理プログラム」のみが台帳にアクセス可能とする仕組みを採用することが考えられる。この場合、利用者は、トランザクションを発行して、台帳管理プログラムに台帳の更新を依頼できるのみである。また、通信経路上の機密性確保のためには、SSL 等で暗号化すべきである。

台帳の完全性については、改ざん防止という観点からは、ノード上の台帳管理プログラムが改ざんの「踏み台」となり得ることに注意が必要である。これを防止するためには、台帳管理プログラムやそれを制御するノードの OS 等に適切なパッチを適用し続けることが重要となる。

なお、ノード間に不整合が発生した場合に備え、収束処理を極力短時間で行うような仕組みを実装しておくことが望ましい。しかし、一部のノードに「投票権」を過大に（例えば、過半数を超えて）与えてしまうと、別の脅威が発生することには留意が必要である。すなわち、投票権の多いノードが攻撃者の支配下に入ってしまうと、台帳の更新権限が事実上攻撃者に委ねられてしまうことになる。このため、「一部のノードに不具合があっても、収束により速やかにカバーされる」という分散台帳技術のメリットを活かすには、たとえセンターノードであっても、過大な投票権を与えないといった工夫が必要になる。

トランザクションの完全性については、まずトランザクション自体の正当性を確認するために、それに付された利用者の署名の検証や、送金の元手となる口座残高の確認が必須となる。取引認証の完全性については、分散台帳技術においては、ノードは端末との間のセッション状態の保持等を管理しないことから、「依頼を受けた取引を意思確認ができるまで保留する」仕組みを具体的にどう実装するかが、今後の課題となろう。

可用性の確保のうち、台帳の消失防止については、バックアップを保持しておく、ノードを地理的に分散するといった対策が考えられる。台帳のバックアップ取得は、何らかの理由で他のノードからのコピーによる復旧が困難な場合に備えた対策となる[19]。ノードの地理的分散は、大規模被災への対策にもなる。ただし、ノードの台帳には全利用者の口座の情報（過去からの履歴を含む）が収容されているため、そうしたノードを設置する場所には、従来の勘定系サーバ

19 既存の技術においても、同様の対策がとられている。すなわち、台帳に相当するデータは、メインセンターとバックアップセンターとの間でほぼリアルタイムで同期がとられており、メインセンターのデータ破損の際には、原理的にはバックアップセンターのデータからの復旧が可能と考えられるが、実運用においては、そうした復旧方法が困難な場合もある。それに備えてメインセンターにおいて（場合によりバックアップセンターにおいても）定期的に別媒体にバックアップを取得している。

に準じたセキュリティ・レベルの確保が必要となることに留意が必要である。この場合、ノードの地理的分散を図るために、設置場所を既存のデータセンター以外に新たに準備するには、莫大なコストがかかる可能性がある。

以上の検討結果を総括すると、既存のインターネット・バンキングの場合と比べた場合、分散台帳技術は、機密性や完全性の面で見劣りしないことに加え[20]、可用性の面で一定の改善が期待できるといえる。したがって、分散台帳技術の採用には、相応の有用性があると考えられる。

ロ．外部業者管理型（図表 8）

外部業者管理型についての評価は、金融機関管理型と多くの点で共通している。このため、以下では、重複を避けるために、両者で評価結果が異なる要件を中心に説明を行う。

ノード間認証の機密性は、外部業者との間に専用回線やインターネット VPN 等でセキュアなネットワークを構築すれば充足される。認可については、外部業者はノードへのアクセス権限を有するため、ノード上の台帳を全て閲覧できてしまう点に留意する必要がある。もちろん、準同型暗号をはじめとする高機能暗号等を利用し、暗号化したままノードで処理するという実装が可能になれば、それは一つの解決策となりうる。例えば、高機能暗号で送金額等を暗号化し、ノードは暗号化したまま口座残高と送金額の大小比較を行い、残高ありと判断した場合には送金額を暗号化したまま台帳に取り込むという仕組みが実現すれば、セキュリティがより高まる。しかし、筆者が知る限り、現在のところ、高機能暗号と分散台帳技術を組み合わせたシステムは未開発のようである。

完全性確保の観点では、金融機関管理型と比較して、外部業者管理型に特有のメリットや留意点は特段ない。

可用性確保の観点では、以下のようなメリットがある。外部業者管理型を採用すれば、ノードの設置場所を金融機関の施設内にする必要がないため、ノードを地理的に分散させることが比較的容易になり、自然災害等に対する可用性が高まる。また、外部業者は耐災害性を「売り」にした施設を運営している場合も多いので、各ノードにおける耐災害性を相対的に低いコストで整備するメリットが享受できる可能性もある。

４．おわりに

本稿では、分散台帳技術を金融サービスに適用する際に求められるセキュリティ要件について検討した。具体的には、金融機関が分散台帳技術を利用して

20 ただし、ノード間の台帳の収束に時間がかかる設計の場合には、完全性が確保できているとは言い難い点に留意する必要がある。

図表8. 分散台帳技術による外部業者管理型における評価・留意点等

<table>
<tr><th colspan="3">セキュリティ要件</th><th>外部業者管理型における評価･留意点等</th><th>金融機関管理型との差異</th></tr>
<tr><td rowspan="5">機密性の確保</td><td rowspan="3">ノード上の機密性確保</td><td rowspan="2">認証</td><td>利用者認証</td><td>クライアント証明書における認証にて実現可能。
なお、ID/パスワードによる認証とは違い、異なる複数の端末からアクセスしたいという利用者のニーズには対応しにくい点には留意する必要。</td><td>特段なし</td></tr>
<tr><td>ノード間認証</td><td>外部業者との間にセキュアなネットワークを構築することで実現可能。</td><td rowspan="2">追加的な留意点あり</td></tr>
<tr><td>認可</td><td>ノードによる台帳への
アクセス制御</td><td>ノード上の台帳管理プログラムによる一元管理にて実現可能（利用者による台帳への直接のアクセスは禁止する）。
ただし、ノード管理者である外部業者に対してもノード上の機密性を確保することは現時点では困難（外部業者はノード上の全情報を閲覧可能）であり、その解決策の1つとして高機能暗号等の活用による今後の開発を期待。</td></tr>
<tr><td colspan="2">通信経路上の機密性確保</td><td>通信経路上のデータの暗号化</td><td>SSLによる暗号化で実現可能。</td><td rowspan="5">特段なし</td></tr>
<tr><td rowspan="4">完全性の確保</td><td rowspan="2">台帳の情報の完全性の確保</td><td>台帳の改ざん防止</td><td>ノード上のプログラムおよびOS等への適切なパッチ適用を確実に実施することが肝要。
なお、ノード間の台帳内容の調整機能を有効に機能させるためには、一部のノードに多大な（例えば過半数の）投票権を与えないような配慮が望まれる。</td></tr>
<tr><td>ノード間の不整合発生時における収束処理</td><td>分散台帳技術におけるノード間の台帳内容の調整機能にて実現可能。</td></tr>
<tr><td rowspan="2">トランザクションの完全性の確保</td><td>トランザクションの正当性確認</td><td>トランザクションに付与された署名の検証（過去の取引と整合性のとれないトランザクションの排除については、台帳との突合などの適宜の方法）で実現可能。</td></tr>
<tr><td>取引認証</td><td>実装に向けて今後の検討が望まれる。</td></tr>
<tr><td rowspan="3">可用性の確保</td><td rowspan="2">台帳の消失防止</td><td>ノードにおける台帳の消失防止</td><td>台帳の定期的および随時のバックアップ取得により実現可能。</td></tr>
<tr><td>システム全体としての台帳消失の防止</td><td rowspan="2">ノードを地理的に分散することで実現可能。
なお、外部業者の施設を活用することで、地理的分散の選択肢が拡大し、より実効的な地理的分散の実現が期待できるというメリットあり。</td><td rowspan="2">追加的なメリットあり</td></tr>
<tr><td>大規模被災への対策</td><td>広域被災等の場合における
サービスの継続</td></tr>
</table>

自行内口座振替を行うことを想定し、必要とされるセキュリティ要件を機密性・完全性・可用性という 3 つの観点から整理した。検討の結果、既存のインターネット・バンキングと比較した場合、分散台帳技術による自行内口座振替は、機密性と完全性の面でのセキュリティ・レベルはほぼ同じであることに加

え、可用性の面では次のようなメリットがあることが分かった。すなわち、金融機関は、自社の多数の拠点にノードを設置・台帳を管理することによって、相応のコスト負担が発生するものの、台帳が喪失するリスクや大規模被災によるリスクを軽減することが可能になる。

ノードの広域分散化を実現するには、外部業者の活用が選択肢の 1 つとなりうる。もちろん、外部業者の活用にあたっては契約等による適切なガバナンスの確保が前提となる。この点、今後、高機能暗号の開発が進めば、外部業者の活用がより現実味を帯びるようになると考えられる。外部業者が所有する複数のデータセンターを活用すれば、ノードの地理的分散を柔軟に図ることが可能となり、金融機関管理型よりも低いコストで可用性を向上させることができるようになると期待される。

また、分散台帳技術については、1 節で述べたように、基幹系システムの構築・維持管理にかかるコストを大幅に削減することができるのではないかと期待する見方がある。今後、具体的な実装内容や管理・運用負担が明らかになってくれば、本稿でのセキュリティ要件の検討を参照しつつ、分散台帳技術の採用がコストの削減にどの程度役立つのかについて、より現実的な議論が可能になると期待される。

以　上

参考文献

岡部一詩、「三菱東京 UFJ 銀が独自コイン」、『日経 FinTech』2016 年 6 月号、日経 BP 社、2016 年、1～2 頁

落合孝文、「セキュリティガイドライン策定に向けた自主的取り組み ～ガイドライン策定の基本方針～」、日本銀行第 2 回 FinTech フォーラム発表資料、日本銀行決済機構局、2016 年（https://www.boj.or.jp/announcements/release_2016/data/rel161107c5.pdf）

金融情報システムセンター、『平成 28 年版金融情報システム白書』、財経詳報社、2015 年

斉藤賢爾、「ブロックチェーンにおける識別子と鍵管理」、日本銀行第 1 回 FinTech フォーラム発表資料、日本銀行決済機構局、2016 年（https://www.boj.or.jp/announcements/release_2016/data/rel160831b5.pdf）

志茂博、「ブロックチェーンの安全性とセキュリティ」、日本銀行第 1 回 FinTech フォーラム発表資料、日本銀行決済機構局、2016 年（https://www. boj.or.jp/announcements/release_2016/data/rel160831b4.pdf）

日本銀行金融機構局、「IT の進歩がもたらす金融サービスの新たな可能性とサイバーセキュリティ」、日本銀行金融機構局、2016 年（https://www.boj.or.jp/research/brp/fsr/data/fsrb160302.pdf）

日本取引所グループ、「金融市場インフラに対する分散型台帳技術の適用可能性について」、『JPX ワーキング・ペーパー』Vol.15、日本取引所グループ、2016 年（http://www.jpx.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX_working_paper_No15.pdf）

みずほ銀行・富士通・富士通研究所、「みずほ銀行と富士通、国境を越えた証券取引の決済プロセス効率化に向けた実証実験を実施」、2016 年 3 月 8 日付プレスリリース、みずほ銀行、2016 年（https://www.mizuhobank.co.jp/release/pdf/20160308release_jp.pdf）

吉本憲文、「住信 SBI ネット銀行のブロックチェーン実証実験の成果」、『金融財政事情』 67 巻 18 号、金融財政事情研究会、2016 年、18～21 頁

Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten, “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121 (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163021).

Buterin, Vitalik, “A Next Generation Smart Contract & Decentralized Application Platform,” 2014 (https://github.com/ethereum/wiki/wiki/White-Paper).

European Central Bank, “Distributed ledger technologies in securities post-trading,”

Occasional Paper Series, No 172, European Central Bank, 2016 (https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf).

Hancock, Matthew, and Ed Vaizey, "Distributed Ledger Technology: beyond block chain," Government Office for Science, 2016 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf).

International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC), *ISO/IEC TR 27015:2012, Information Technology – Security Techniques – Information Security Management Guidelines for Financial Services*, ISO, 2012.

Mainelli, Michael, and Alistair Milne, "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle," *Swift Institute Working Paper*, No. 2015-007, Swift Institute, 2016 (https://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf).

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008 (http://bitcoin.org/bitcoin.pdf).