Vol.2022-DPS-190 No.28
Vol.2022-CSEC-96 No.28
2022/3/11

ブロックチェーンインターオペラビリティのセキュリティ評価手法の検討

長谷川 悠貴[1,a)]　萱場 啓太[1]　米倉 裕貴[1]　東角 芳樹[1]　森永 正信[1]

概要：近年, ブロックチェーン (BC) 間での相互運用性を実現する技術が注目されており, 中でも, 連携処理の制御や記録を行う BC によって異なる BC 同士を連携する技術 (BCB, Blockchain for Connecting Blockchain) は, より多様な BC との接続や複数 BC 間での複雑な連携処理を実現する技術として特に注目されている. 一方, BCB を利用してセキュアなシステムを開発するためには, 各種 BCB で異なるセキュリティ上の特徴や想定される脅威を考慮した評価手法が必要となる. そこで本研究では, BCB に関する既存研究から抽出したセキュリティ観点や脅威を, BC のレイヤ分類および脅威分類手法を参考に定義した BCB の 5 つの評価カテゴリ (検証, 連携, 連携情報の保護, 接続 BC の管理, ガバナンス) に分類し, 各カテゴリごとに想定される脅威に紐づく 17 の評価項目から成る BCB のセキュリティ評価モデルを提案する. また, 本評価モデルを利用して想定されるユースケースのセキュリティを評価し, 既存手法による評価結果との比較を行うことで, 本評価モデルの有効性を確認する.

An Examination of Security Evaluation Method for Blockchain Interoperability

1. はじめに

ブロックチェーン (BC) は, 改ざんを防ぐ構造を持ったデータを参加者間で非中央集権的に共有する分散台帳技術であり, 取引の耐改ざん性や透明性を保証できる手段として, 従来より金融やサプライチェーンをはじめとする様々な業界で注目されている [1]. 一方, 多くの BC では処理の実行や確定の方式に互換性がなく, これまで BC 同士を安全に連携することが困難であったが, それに対して近年, BC 同士の相互運用性を実現するブロックチェーンインターオペラビリティ (BC インターオペラビリティ) 技術が注目されている. これにより, 異なる BC 間での暗号通貨の交換・転送や, 一方の BC での処理と連携して他方の BC でスマートコントラクトを実行するなどの処理が可能となり, これまで連携が難しかった組織間や業界横断での BC の活用が可能になると期待されている.

BC インターオペラビリティ技術は, BC の連携方式などによっていくつかの種類に分類されることが多く, 例えば Buterin によると, BC インターオペラビリティ技術は, HTLC (Hash Time Lock Contract), Relay schemes, Notary schemes, という 3 つに大別することができる [2]. このうち, Notary schemes は, BC 同士の連携を第三者が仲介する方式であり, その中でも, 連携処理の制御や記録を行う BC (BC ハブ) を仲介することで連携を実現する方式 (BCB, Blockchain for Connecting Blockchain) は, 異なる特性を持った多様な BC と接続できる点や, 複数の BC と連携した複雑な処理を実行できる点などにおいて特に注目されている.

一方, BCB では, BC ハブの特性や BC ハブと接続 BC との接続方式などによってセキュリティ上の特徴が異なるため, ユースケースのセキュリティ要件に適した BCB の選択やリスクに対する適切な対策が必要であり, 例えば, 機微なデータを扱う BC 同士が連携するユースケースでは, 国や企業の規則やプライバシーに関する問題が発生する可能性があるため, これらの問題に考慮した BCB の選択やデータ保護対策が重要となる. そのため, このような問題に対して漏れなく対応するためには, BCB のセキュリティ上の特徴や重要となるセキュリティ対策が十分になされて

[1] 富士通株式会社, 〒 211-8588 神奈川県川崎市中原区上小田中 4-1-1, Fujitsu Limited, 4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki-shi.
[a)] yuki.hasegawa@fujitsu.com

いるかを評価するセキュリティ評価手法が必要になると考えられる.

それに対しいくつかの既存研究では, BCB の脅威やセキュリティ評価観点について言及されているが, 各研究で評価・言及されている内容が異なるため, 利用する手法によって評価結果が異なるという課題がある [3], [4], [5]. また, 各手法によって評価の粒度が異なるため, 複数の手法の評価結果を直接組み合わせて利用することも難しいと考えられる.

そこで本研究の貢献として, 既存研究で言及されている BCB の脅威やセキュリティ評価観点を集約し, 一つのセキュリティ評価モデルとして提案することで, 既存研究での評価観点を集約したより網羅性の高い BCB のセキュリティ評価を可能とする. 本評価モデルは, 既存研究から BCB の脅威やセキュリティ評価観点をキーワードとして抽出し, BC のレイヤ分類および脅威分類手法を参考に定義した BCB の 5 つの評価カテゴリ (検証, 連携, 連携情報の保護, 接続 BC の管理, ガバナンス) に分類・整理することで, 各カテゴリごとに想定される脅威に紐づく 17 のセキュリティ評価項目として定義する.

2 章で, BC および BC インターオペラビリティの特徴について説明した後, 3 章で本研究における課題と目的を述べる. 4 章では, 提案するセキュリティ評価モデルの構成, および BCB の各評価カテゴリで重要となる 17 のセキュリティ評価項目について述べる. 5 章では, 提案した評価モデルを利用して, BCB の活用が想定される 2 つのユースケースを対象にセキュリティの評価を行い, 既存の評価手法による評価結果との比較を行うことで本評価モデルの有効性を確認し, 6 章でまとめと今後の研究方針について述べる.

2. 関連研究

2.1 ブロックチェーン

ブロックチェーン (BC) は, 暗号通貨やデータの取引処理 (トランザクション) をブロックと呼ばれる単位でまとめ, 正当性が検証されたブロックを参加者間で共有する非中央集権的な分散台帳技術である [1]. BC では, ブロックを共有することで取引の透明性を保証できるだけでなく, 各ブロックにそれ以前のブロックの内容を示すハッシュ値を格納し, ブロックを鎖状に連結することでデータの改ざんを困難にし, データの耐改ざん性を保証することが可能である.

BC は, 大きくパブリック型とコンソーシアム型に分類される. Bitcoin や Ethereum などのパブリック型 BC は, 特定の信頼主体を必要とせず誰でも参加可能な BC であり, 信頼関係のない参加者間での取引が可能であるのに対し, Hyperledger Fabric や Corda などのコンソーシアム型 BC では, 参加者の身元を証明する機関等の信頼主体を設置して BC への参加を制限することで, 特定の組織や個人間でのみ情報を共有し, より柔軟な運用や処理の高速化が可能である.

このように, 特徴の異なる BC を使い分けることで様々なユースケースを実現できる一方, 多くの BC では, 取引の形式やブロックを生成・確定する方式の互換性がないため, BC を活用したシステム同士の安全な連携が困難である.

2.2 ブロックチェーンインターオペラビリティ

このような課題を解決する手段として, 近年, BC 間での相互運用性を実現する BC インターオペラビリティ技術が注目されている. BC 間での相互運用性によって, 異なる種類の暗号通貨の交換や, サイドチェーンと呼ばれる補助的な BC と連携することによる BC の処理性能の向上, さらには, 異なる BC 間での処理の連携 (例えば, データの送信処理と暗号通貨の転送処理が連動して実行) などが可能となる.

2.2.1 特徴と分類

BC インターオペラビリティ技術は, 連携方式や第三者への依存度に応じて, HTLC (Hash Time Lock Contract), Relay schemes, Notary schemes の 3 つに分類して比較されることが多い [2], [6], [7]. HTLC は, BC の機能として提供される Time lock と, Hash lock と呼ばれる仕組みを組み合わせることで, 第三者に依存することなく処理が全て成功するかもしくは全て失敗となること (アトミック性) を保証する方式であり, トークンの交換でのみ利用される. また, Relay schemes は, 一方の BC から供給されるブロックヘッダーをもう一方の BC のスマートコントラクトが検証することによって, 第三者に依存することなく 2 つの BC 間での連携を実現する方式であり, 類似した特性を持つ BC 間でのトークンや任意のデータ交換, 連携処理が可能であるとされている.

一方, Notary schemes は, BC 間での連携処理を第三者が仲介する方式であり, その中でも, 連携処理の制御や記録を行う BC (BC ハブ) が BC 間の連携処理を仲介する方式 (BCB, Blockchain for Connecting Blockchain) は, 異なる特性を持った多様な BC との接続や, 複数 BC 間での複雑な連携処理を実現できる方式として特に注目されている [5], [7], [8], [9].

BCB では, BC ハブに対して BC を接続することで複数の接続 BC 間での連携を可能とするが, BC ハブと接続 BC との接続方式や BC 間での通信方式, 他にも BC ハブの種別 (パブリック型またはコンソーシアム型) や接続 BC 上で実行されたトランザクションの検証方式などの点において, 各 BCB でそれぞれ特徴が異なる.

2.2.2 BCB のセキュリティ

2.2.1 節で述べたような各 BCB の特性は, セキュリティ要件にも大きく影響する可能性がある [7], [9]. そのため, BCB を利用したシステムの開発時には, ユースケースのセ

キュリティ要件に適した BCB の選択や, 各 BCB の特性に応じた適切なセキュリティ対応が必要となり, 例えば, 機微なデータを扱う BC 同士を連携するユースケースでは, 国や企業の規則やプライバシー問題に考慮した BCB の選択, およびデータ保護対策を行うことが望まれる [10], [11]. そのため, BCB を利用してセキュアなシステムを開発するためには, 各種 BCB で異なるセキュリティ上の特徴や想定される脅威を考慮した評価手法が必要となる.

2.3 BCB のセキュリティ評価手法

これまで, 複数の既存研究において, BCB に関連した脅威やセキュリティ評価項目について言及, 提案されている [3], [4], [5]. kannengiesser らの研究では, BC インターオペラビリティ技術の体系的な調査を行い, セキュリティを 17 の項目によって評価しており, Vo らの手法では, BC インターオペラビリティを実現するために必要不可欠となるセキュリティの要素について言及している. また, Belchior らの研究では, BC インターオペラビリティ技術に関する文献レビューと新しい分類方法の提案を行い, 分類カテゴリごとのセキュリティについて言及している.

3. 本研究における課題と目的

2.2.2 節で述べた通り, BCB を利用してセキュアなシステムを開発するためには, BCB のセキュリティ評価手法が必要となるが, 既存手法では, それぞれ言及されている内容や評価観点が異なるため, 利用する手法によって評価結果が異なるという課題がある. また, 各手法によって評価の粒度が異なる (例えば, 「可用性」や「機密性」のようなセキュリティ要素レベルで評価する手法と「検証者の数」のような具体的なレベルで評価を行う手法が存在する) ため, 複数の評価結果を直接組み合わせて利用することも難しいと考えられる.

そこで本研究では, 既存研究で言及されている BCB に関する脅威やセキュリティ評価観点を抽出し, それらの内容を集約した BCB のセキュリティ評価モデルを提案することで, より有効的なセキュリティ評価に貢献する.

4. 提案するセキュリティ評価モデル

本章では, 提案するセキュリティ評価モデルの構成および各評価項目について説明する. 提案する評価モデルは, BCB に関する 5 つの評価カテゴリ (検証, 連携, 連携情報の保護, 接続 BC の管理, ガバナンス) と 17 の評価項目から構成され, 各評価項目ごとに具体的な評価観点を例示している.

本評価モデルは, 既存手法で言及されている BCB の脅威やセキュリティ観点を集約しつつ, 粒度の差異がより小さい評価項目として定義するため以下の手順で検討を行った.

(1) 脅威・セキュリティ観点の抽出
kannengiesser らの手法を参考に, 先に述べた 3 つの既存研究から BCB で想定される脅威やセキュリティ観点をキーワードとして抽出する [3], [4], [5].

(2) 抽出内容の分類
Dasgupta や Zhao らの研究における BC のレイヤ分類および脅威分類手法を参考に BCB の 5 つの評価カテゴリ (検証, 連携, 連携情報の保護, 接続 BC の管理, ガバナンス) を定義し, (1) で抽出したキーワードをこれらのカテゴリに重複を許して分類する [10], [12]. これは, 抽出したキーワードからセキュリティ評価項目を検討する際, 同じキーワードから, 複数の評価カテゴリで評価観点を定義する必要があると考えるためであり, 例えば, 「検証方式」というキーワードからは, 主に BC ハブでの検証方式について評価する「検証」カテゴリと主に接続 BC でのトランザクションの検証方式について評価する「接続 BC の管理」カテゴリの両カテゴリで評価観点を定義している.

(3) 脅威に紐づくセキュリティ評価項目の検討
(2) で分類したキーワードをもとに, 各評価カテゴリごとに想定される脅威を調査・整理し, その脅威に紐づくセキュリティの観点を, 17 のセキュリティ評価項目および評価観点として整理する.

以下, 定義したセキュリティ評価項目について各評価カテゴリごとに説明する.

4.1 検証

4.1.1 検証方式

ハブとなる BC では, 連携処理を実現するためのトランザクションがコンセンサスアルゴリズム (CA) に基づき検証され, 新しいブロックとして生成されるが, 各 CA に対して, double spending attack や 51% attack, sybil attack などの攻撃の脅威がある [11], [13]. 加えて, 各 CA では, 正常に機能する条件 (例えば, 3 分の 2 以上の参加者が正しい振る舞いをしている場合に正しく動作する CA は, ビザンチン耐性があると言える) が定められており, 4.1.2 節でも言及する通り, 検証者の信頼性などに応じて適切な耐性を持った CA を選択することが重要である [2]. これらを踏まえ, 「コンセンサスアルゴリズムの堅牢性」では, BC ハブが採用する CA の特徴や安全性, それを実現するインセンティブメカニズムなどについて評価する.

また, CA では, 生成したブロックが覆らないことを確定するファイナリティについても注意が必要である. BC のファイナリティは, 決定的ファイナリティと確率的ファイナリティの 2 種類に大別され, 決定的ファイナリティでは, ブロックが生成時に確定し後から覆る可能性がないのに対し, 確率的ファイナリティでは, 生成されたブロックが完全に確定することはなく, 時間経過に伴い覆る可能性が低下

表 1 提案するセキュリティ評価モデルの項目・観点
Table 1 Evaluation items of the proposed security evaluation model for BCB.

評価カテゴリ	評価対象	評価項目	具体的な評価観点
検証	検証方式	コンセンサスアルゴリズムの堅牢性	• 検証メカニズム • ビザンチン耐性 • インセンティブメカニズム
		コンセンサスアルゴリズムのファイナリティ	• ファイナリティの種別
	検証者	検証者の信頼性	• 検証者の信頼性 • 検証者の選出 • 検証者の分散性
		不正行為の監視・対処	• 不正な検証者の監視・対処
連携	通信方式	通信規格の安全性	• 通信規格 • アトミック性 • 規格外の BC やオラクルとの通信
		連携情報の伝搬	• 接続対象の探索 • 伝搬経路の管理
	接続方式	接続コンポーネントの安全性	• 接続コンポーネントの分散性 • 接続コンポーネントの信頼主体
	整合性の保証	BC 間の整合性	• 接続 BC のファイナリティに対する対策
	連携処理の制御	実行環境・言語の安全性	• スマートコントラクトの実行環境・言語
連携情報の保護	アカウント管理・アクセス制御	クレデンシャル情報の取り扱い	• 鍵管理方式 • クレデンシャル情報の管理
		アクセス制御	• リソース (連携情報やスマートコントラクト) へのアクセス制御
	連携情報の保存	連携情報の秘匿性	• 連携情報の暗号化
		連携情報の保存場所	• 連携情報の保存場所
接続 BC の管理	接続 BC の制御・検証	接続 BC との関係性	• 接続 BC との関係性 • 接続 BC の可用性
		接続 BC のセキュリティ管理	• 接続 BC の信頼性検証
ガバナンス	BC ガバナンス	ガバナンスメカニズム	• ガバナンス種別 • ガバナンスメカニズム • BC の分散性への影響
		ハードフォーク	• ハードフォークの有無・影響

する [14], [15]. ここで, BC ハブが確率的ファイナリティを採用している場合, 連携処理の実行後にブロックが覆ることで, 接続 BC 間で不整合が発生する可能性があるため,「コンセンサスアルゴリズムのファイナリティ」では, BC ハブが持つファイナリティの種別について評価する.

4.1.2 検証者

4.1.1 節でも述べた通り, CA が正しく動作するためには, BC を構成する参加者の信頼性に応じた検証者の選出方式を選択することが重要であり, 一般的にパブリック型 BC とコンソーシアム型 BC では, 想定される参加者の信頼性が大きく異なる [13], [14]. 加えて, 検証が特定の検証者に集中する場合, 検証者への攻撃などにより可用性や信頼性の問題が発生する可能性があるため,「検証者の信頼性」では, BC ハブの検証者の信頼性や, その選出方式, 分散性について評価する [3].

また, CA の正しい動作を維持するためには, 誤った検証などの不正行為を行っている, もしくは検証の維持が困難な検証者を特定し是正することが望まれるため,「不正行為の監視・対処」では, 不正な検証者の監視方式や罰則の仕組みについて評価する.

4.2 連携

4.2.1 通信方式

BCB では, BC 間での通信の形式などを定めた通信規格に基づき連携を実現している場合がある. しかし, こういった規格は開発中のものも多く, 各規格の特徴や安全性に注意が必要であり, その一例として, 連携処理でのアトミック性について評価する [5], [8]. 加えて, 4.2.2 節で言及する通り, BCB によっては, 通信規格で定義されていない独自の仕組みを持った BC やオラクル (BC 外のデータを提供する API 等) との接続を可能としている場合もあるため, そのような場合における通信方式についても注意が必要である. よって,「通信規格の安全性」では, 通信規格や連携処理のアトミック性, 規格外の BC やオラクルとの通信方式について評価する.

また, 今後, 多くの BC やオラクルとの接続が可能となった際, 接続対象の各リソース (BC や BC 上のデータ等) の探索方式が課題となる可能性がある [4]. 具体的に, 接続対象となる各リソースに関する情報を集中的に管理するシンプルな方式では, 分散性を特徴とする BC に対して必ずしも適切ではない可能性や, DoS 攻撃の対象となる可能性もあることに注意が必要である. これらのことを踏まえ,「連携情報の伝搬」では, 連携処理に関係する BC の場所や, トランザクションがその場所に到達するまでの伝搬経路を正しく管理する方式, およびその信頼主体について評価する.

4.2.2 接続方式

BCB では, 通常の BC との接続に加え, 規格外の仕組みを持った BC やオラクルと接続する際, 接続処理やトランザクションの監視・伝搬を行うサーバなどの接続コンポーネントを利用する場合がある. このような場合には, 接続コンポーネントのセキュリティについても注意が必要であり, 例えば, 単一の接続コンポーネントのみを利用する場合, 可用性や信頼性が問題となる可能性がある [3]. 他にも, 中間者攻撃を防止するための通信経路の暗号化や, データ入力に対するサニタイジングなどが重要になると考えられるため,「接続コンポーネントの安全性」では, 接続コンポーネントの分散性や管理に関して責任を持つ信頼主体について評価する [16].

4.2.3 整合性の保証

4.1.1 節では, BC ハブのファイナリティについて言及したが, 接続 BC でも同様の注意が必要であり, 確率的ファイナリティを持つ接続 BC との連携時に不整合を発生させないための対策 (例えば, ブロックが覆る可能性が十分に低くなるまで待機する) を検討することが重要である. よって,「BC 間の整合性」では, 接続 BC のファイナリティに対する対策ついて評価する.

4.2.4 連携処理の制御

BC 間での連携処理を制御する手段の一つとして, BC ハブに実装されているスマートコントラクトを利用することが想定される. その際に, スマートコントラクトを記述する各言語や実行環境の脆弱性などを利用したスマートコントラクトへの攻撃に注意が必要である [17], [18]. また, 記述したコードのロジックに意図せず含まれてしまう脆弱性についても検証可能であることが望ましい. ただし, これは BCB 自体のセキュリティとは直接関係しないため, 提案する評価モデルでは評価の対象外とする [19], [20]. 以上をまとめ,「実行環境・言語の安全性」では, BC ハブのスマートコントラクトの実行環境や言語に関する安全性について評価する.

4.3 連携情報の保護

4.3.1 アカウント管理・アクセス制御

秘密鍵などのクレデンシャル情報が漏洩した場合, 第三者による不正な送金や検証に利用される可能性があるため, BC ハブでのクレデンシャル情報の漏洩対策が行われていることが望ましい [21]. また, 接続 BC におけるクレデンシャル情報についても同様に注意が必要であり, 特に, 複数の BC にまたがった複雑な連携処理の実行時には, BC ハブやトランザクションに対して接続 BC のクレデンシャル情報を付与する可能性も想定されるため, その際に, クレデンシャル情報そのものを渡すのではなく, アクセストークンを利用するなど漏洩リスクを減らすための対策と連携できることが望ましい. よって,「クレデンシャル情報の取り扱い」では, 鍵管理方式やクレデンシャル情報の取り扱いについて評価する.

また, 一般的なアプリケーションと同様に, BCB におい

てもアクセス制御が重要であると考えられる. 特に, 機微なデータを扱う場合や, 複数のコンソーシアム型 BC を接続する場合にはプライバシーの問題が発生する可能性があり, 連携情報やスマートコントラクトに対するアクセス制御が重要となるため, 「アクセス制御」では, アクセス制御機能やその実現可能性について評価する [22].

4.3.2 連携情報の保存

アクセス制御だけでは, クレデンシャル情報や BC 上のデータの漏洩を完全に防止することは難しく, データそのものに対する対策も重要となる [4]. 特に, パブリック型 BC とコンソーシアム型 BC を接続する場合や, 複数のコンソーシアム型 BC を接続する場合には, データの適切な秘匿化が望まれるため, 「連携情報の秘匿性」では, 連携情報の暗号化について評価する.

また, 一般的には, BC 間での連携処理に伴い連携情報 (トランザクションやアカウントの情報) が BC ハブや接続 BC など複数の場所に保存されるが, パブリック型とコンソーシアム型の BC を接続した場合, プライバシーの問題だけでなく, データの扱いに関して複数国間での法律の問題が発生する可能性にも注意が必要である [7]. このことから, 「連携情報の保存場所」では, 各 BCB が連携情報を保存する場所について評価し, さらに, それらに対して適切なアクセス制御や秘匿化を検討することが望まれる.

4.4 接続 BC の管理

4.4.1 接続 BC の制御・検証

BC ハブと接続 BC の関係性は, 依存関係と同格関係に大別されることが多く, これらの違いは接続 BC の可用性や検証方式に影響を与える可能性がある.

前者の場合, BC ハブで選出された検証者が接続 BC のトランザクションの検証について責任を持つことで, 接続する全ての接続 BC で一定の信頼性を保証できる可能性などがある一方で, 接続 BC は BC ハブの影響を受けやすく, 何らかの原因で BC ハブが動作しなくなった場合には接続 BC も動作不能となる可能性があることから, 可用性などの観点で注意が必要である. 一方, 後者の場合, BC ハブで障害等が発生した場合にも接続 BC が動作を続けることができる可能性が高い半面, 接続 BC のトランザクションの検証は各接続 BC の検証者に依存するため, 各接続 BC の信頼性を確認・保証する仕組みの検討が重要となる.

以上をまとめると, 「接続 BC との関係性」では, BC ハブと接続 BC の関係性や接続 BC の可用性について評価し, また, 「接続 BC のセキュリティ管理」では, 接続 BC の信頼性の検証方式やその信頼主体について, 連携する接続 BC の信頼性と併せて評価することが望まれる.

4.5 ガバナンス

4.5.1 BC ガバナンス

BC ガバナンスは, 検証者の数など BC の基幹となるルールの追加・変更などを行うための運用形態であり, ルール変更に関する投票やアップデートなどを BC 上のコードとして自動的に実行する方式 (on-chain ガバナンス) と, BC の運営組織によってルール変更等が決定され, それに賛同する参加者が手動でアップデート等を行う方式 (off-chain ガバナンス) に分類できる [23], [24].

BC ガバナンスは, 種別 (on-chain または off-chain) やその仕組みによって, BC の脆弱性に対する攻撃など予期しない事態への対応や BC の分散性に影響を与える可能性があり, 例えば, 必要以上の権力の集中化によって分散性が損なわれることなどへの注意が必要である. 以上のことから, 「ガバナンスメカニズム」では, BC ガバナンスの種別・仕組みや, 分散性に与える影響について評価する.

また, BC ハブにて, ハードフォークが発生する可能性についても注意が必要である. ハードフォークとは, 変更前後で互換性のないルール変更が行われた場合に, 変更を支持して新しいルールを利用する参加者によって生成されるチェーンと, 変更を支持せず変更前のルールを利用し続ける利用者によって生成されるチェーンが分かれて存在することを指し, 複数のチェーンが存在することで, BCB の運用に影響を与える可能性がある [23], [25]. そのため, 「ハードフォーク」では, ハードフォークが発生する可能性や, ハードフォーク発生時の影響について評価する.

5. 提案評価モデルの有効性検証

本章では, 提案するセキュリティ評価モデルを利用して, BCB の活用が想定されるユースケースを対象としたセキュリティの評価を行い, 既存手法を利用した場合の評価結果と比較することで, 提案手法が既存手法での評価内容を集約していることを確認する.

5.1 BCB のユースケース

IETF (Internet Engineering Task Force) では, BC の相互運用性によって実現されるいくつかのユースケースを提案している. 本章では, その中でも, 連携処理などの特徴が異なると想定される 2 つのユースケースとして, CBDC (A Central Bank Digital Currency) 基盤の相互運用と, サプライチェーンの相互接続を対象にセキュリティの評価を行う [26]. CBDC とは一般に, 中央銀行の債務として発行された法定通貨建てであるデジタル通貨を指し, 近年, 各国で CBDC 基盤の実現に向けた検討が行われている.

ここで, 各ユースケースの特徴について簡単にまとめる. CBDC 基盤の相互運用では, これまで多くの CBDC 基盤でコンソーシアム型 BC の利用が検討されていることから, 各国が持つコンソーシアム型 BC 間でのトークン・デジタ

表 2 「連携情報の保護」に関するセキュリティの評価結果および既存手法との比較
Table 2 Security evaluation about "protection of interoperability information" and comparison with existing researches.

	ユースケースのセキュリティ評価		各手法での評価結果			
評価項目	CBDC 基盤の相互運用	サプライチェーンの相互接続	提案手法	既存手法 [3]	既存手法 [4]	既存手法 [5]
クレデンシャル情報の取り扱い	クレデンシャル情報漏洩への基本的な対策が望まれる	基本的な漏洩対策に加えて, 接続 BC のクレデンシャル情報をより安全に扱う仕組みと連携できることが望まれる	○	△	-	-
アクセス制御	連携情報やスマートコントラクトに対するアクセス制御が望まれる	連携情報やスマートコントラクトに対するアクセス制御が望まれる	○	△	○	○
連携情報の秘匿性	連携情報に応じてデータの秘匿化が望まれる (ただし, 秘匿化によるマネーロンダリング等の助長に注意)	連携情報に応じてデータの秘匿化が望まれる	○	△	○	△
連携情報の保存場所	各国や企業の規則およびプライバシー問題を考慮した場所にのみ連携データを保存することが望まれる	各国や企業の規則およびプライバシー問題を考慮した場所にのみ連携データを保存することが望まれる	○	-	-	△

○ 評価可能, △ 一部評価可能, - 評価対象外

ル通貨の交換・転送処理が多く発生すると想定される. また, CBDC 基盤では, プライバシーや個人情報への配慮が重要になると多くの文献で言及されていることから, ユースケースの特徴として, 連携情報の保護が重要となる資産の交換・転送処理が多く発生すると考えられる [27]. 一方, サプライチェーンの相互接続では, サプライチェーンに関係する様々な業界・組織が持つ主にコンソーシアム型の BC やオラクルと接続する可能性があり, また, トークンに限らないデータの転送や複数の BC にまたがった複雑な連携処理 (例えば, 商品の購入 (決済), 輸送 (在庫情報の更新, 輸送の追跡) などの処理が複数の BC 上で連動して実行) が発生する可能性を持つことが特徴であると考えられる.

5.2 ユースケースのセキュリティ評価

提案した評価モデルを利用して, 先に挙げた 2 つのユースケースのセキュリティを評価する. ただし, 提案した評価モデルは 5 つの評価カテゴリおよび 17 のセキュリティ評価項目によって評価を行うが, 本章では, 5.1 節で説明した各ユースケースの特徴をもとに, 特に重要になると想定される評価カテゴリ「連携情報の保護」の 4 つのセキュリティ評価項目について評価を行う.

各ユースケースのセキュリティを評価した結果を表 2 に示す. 評価項目「クレデンシャル情報の取り扱い」に関して, CBDC 基盤の相互運用では, BC ハブや接続 BC でのクレデンシャル情報の漏洩に対する基本的な対策が望まれる一方, サプライチェーンの相互接続では, 複数 BC をまたがった複雑な連携処理を実行するために, BC ハブやトランザクションが接続 BC のクレデンシャル情報を保持する可能性が考えられる. その際に, クレデンシャル情報そのものを渡すことはセキュリティリスクが非常に高いため, クレデンシャル情報に代わってアクセストークンを発行する OAuth 等の仕組みと連携できることが望ましい.

また, 評価項目「連携情報の保存場所」に関して, 本来特定の国や企業の参加者のみで運用されていたコンソーシアム型 BC に保存していたデータが, BC ハブを運用する他の国や企業が持つサーバなどに保存される場合, 国や企業の規則違反やプライバシー問題が発生する可能性があるため, 両ユースケースにおいてこれらの問題が発生しない場所にのみデータを保存することが望まれる.

5.3 既存手法との比較

最後に, 5.2 節で説明した評価結果と, 既存手法による評価結果を比較する. 比較結果を表 2 に示す. 表 2 が示す通り, 提案した評価モデルは, いずれかの既存手法で言及されている評価内容を集約していることが確認できた. 特に, 評価項目「クレデンシャル情報の取り扱い」や「連携情報の保存場所」では, 既存手法では言及されていなかった, もしくは抽象的にのみ言及されていた内容を評価項目および評価観点として定義できていることを確認した.

以上より, 本研究で提案したセキュリティ評価モデルでは, 対象とした既存手法の評価内容を集約し評価できることを確認した.

6. まとめ

本研究では, 連携処理の制御や記録を行う BC によって BC 同士の相互運用性を実現する BC インターオペラビリティ技術を対象としたセキュリティ評価モデルを提案した. また, 提案したセキュリティ評価モデルを利用して, 想定されるユースケースのセキュリティを評価し, 既存手法を利用した場合の評価結果と比較することで, 対象とした既存手法での評価内容を集約し評価できることを確認した.

今後は, BCB を利用したシステム開発において, 実際に本評価モデルでの評価内容をもとに適切な BCB の選択やセキュリティ対策を実施することで, 本評価モデルの有効性を確認する.

参考文献

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review*, p. 21260 (2008).
[2] Buterin, V.: Chain interoperability, *R3 Research Paper*, Vol. 9 (2016).
[3] Kannengießer, N., Pfister, M., Greulich, M., Lins, S. and Sunyaev, A.: Bridges between islands: Cross-chain technology for distributed ledger technology (2020).
[4] Vo, H. T., Wang, Z., Karunamoorthy, D., Wagner, J., Abebe, E. and Mohania, M.: Internet of blockchains: Techniques and challenges ahead, *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, IEEE, pp. 1574–1581 (2018).
[5] Belchior, R., Vasconcelos, A., Guerreiro, S. and Correia, M.: A survey on blockchain interoperability: Past, present, and future trends, *ACM Computing Surveys (CSUR)*, Vol. 54, No. 8, pp. 1–41 (2021).
[6] Hewett, N., van Gogh, M. and Pawczuk, L.: Inclusive Deployment of Blockchain for Supply Chains: Part 6–A Framework for Blockchain Interoperability, *World Economic Forum* (2020).
[7] Koens, T. and Poll, E.: Assessing interoperability solutions for distributed ledgers, *Pervasive and Mobile Computing*, Vol. 59, p. 101079 (2019).
[8] Bhatia, R. et al.: Interoperability solutions for blockchain, *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, IEEE, pp. 381–385 (2020).
[9] Siris, V. A., Nikander, P., Voulgaris, S., Fotiou, N., Lagutin, D. and Polyzos, G. C.: Interledger approaches, *IEEE Access*, Vol. 7, pp. 89948–89966 (2019).
[10] Dasgupta, D., Shrein, J. M. and Gupta, K. D.: A survey of blockchain from security perspective, *Journal of Banking and Financial Technology*, Vol. 3, No. 1, pp. 1–17 (2019).
[11] Zhang, R., Xue, R. and Liu, L.: Security and privacy on blockchain, *ACM Computing Surveys (CSUR)*, Vol. 52, No. 3, pp. 1–34 (2019).
[12] Zhao, H., Zhang, M., Wang, S., Li, E., Guo, Z. and Sun, D.: Security risk and response analysis of typical application architecture of information and communication blockchain, *Neural Computing and Applications*, Vol. 33, No. 13, pp. 7661–7671 (2021).
[13] Bamakan, S. M. H., Motavali, A. and Bondarti, A. B.: A survey of blockchain consensus algorithms performance evaluation criteria, *Expert Systems with Applications*, Vol. 154, p. 113385 (2020).
[14] Chaudhry, N. and Yousaf, M. M.: Consensus algorithms in blockchain: comparative analysis, challenges and opportunities, *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, IEEE, pp. 54–63 (2018).
[15] Zhang, S. and Lee, J.-H.: Analysis of the main consensus protocols of blockchain, *ICT express*, Vol. 6, No. 2, pp. 93–97 (2020).
[16] Chondamrongkul, N., Sun, J. and Warren, I.: Formal Security Analysis for Blockchain-based Software Architecture., *SEKE*, pp. 532–537 (2020).
[17] Wang, D., Jiang, B. and Chan, W.: WANA: Symbolic execution of wasm bytecode for cross-platform smart contract vulnerability detection, *arXiv preprint arXiv:2007.15510* (2020).
[18] Yamashita, K., Nomura, Y., Zhou, E., Pi, B. and Jun, S.: Potential risks of hyperledger fabric smart contracts, *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, IEEE, pp. 1–10 (2019).
[19] Mou, B. and Liu, F.: New Technology Architecture and Research Hotspot of Blockchain in 2020, *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, IEEE, pp. 277–281 (2020).
[20] Sayeed, S., Marco-Gisbert, H. and Caira, T.: Smart contract: Attacks and protections, *IEEE Access*, Vol. 8, pp. 24416–24427 (2020).
[21] Morganti, G., Schiavone, E. and Bondavalli, A.: Risk assessment of blockchain technology, *2018 Eighth Latin-American Symposium on Dependable Computing (LADC)*, IEEE, pp. 87–96 (2018).
[22] Lan, Y., Gao, J., Wang, K., Zhang, J., Wu, Z., Zhu, Y. and Chen, Z.: TrustCross: Enabling Confidential Interoperability across Blockchains Using Trusted Hardware, *arXiv preprint arXiv:2103.13809* (2021).
[23] Tan, E., Mahula, S. and Crompvoets, J.: Blockchain governance in the public sector: A conceptual framework for public management, *Government Information Quarterly*, Vol. 39, No. 1, p. 101625 (2022).
[24] De Filippi, P. and McMullen, G.: Governance of blockchain systems: Governance of and by Distributed Infrastructure, PhD Thesis, Blockchain Research Institute and COALA (2018).
[25] Lin, I.-C. and Liao, T.-C.: A survey of blockchain security issues and challenges., *Int. J. Netw. Secur.*, Vol. 19, No. 5, pp. 653–659 (2017).
[26] Aetienne, S., Thomas, H. and Mike, M.: Blockchain Gateways: Use-Cases (draft-sardon-blockchain-gateways-usecases-02) (2021). `https://datatracker.ietf.org/doc/draft-sardon-blockchain-gateways-usecases/02/`.
[27] Darbha, S. and Arora, R.: Privacy in CBDC technology, Technical report, Bank of Canada (2020).