IDOL3.0 PROJECT
NIDT IEO申込者限定 メンバー候補生決定最終投票

評価報告書

2023年10月5日

株式会社オーバース　評価委員会

目次

用語の定義

用 語	定 義
当社	株式会社オーバース
本投票	当社がIDOL3.0 PROJECTにおいて実施する「NIDT IEO申込者限定メンバー候補生決定最終投票」
当委員会	本投票のプロセスの合理性の検証のために当社が設置した評価委員会
本システム	本投票を実施するために当社が運営するシステム「NIDTポータル」
開発ベンダ	本システムの開発、運用を当社が委託するITベンダ
NIDT	ブロックチェーン上で当社が発行するユーティリティ・トークン（暗号資産の一種）
暗号資産交換業者	NIDTを取り扱う暗号資産交換業者であるDMM bitcoin及びcoinbook
IEO	2023/3/29～4/19に暗号資産交換業者が実施したNIDTの先行販売
クーポンコード	暗号資産交換業者からIEO申込者に配布され、本システムで投票権を付与されるために必要なユニークな11桁または13桁の文字列
クーポンコードリスト	ユーザごとのクーポンコード、IEO申込口数（IEOでのNIDT購入数）等が記載された暗号資産交換業者が作成するリスト
投票権	本システムでクーポンコードを登録したユーザに付与される本投票を行う権利（単位: 票）
投票日	投票期間中（2023/9/24 18:00～9/30 17:59）の18:00～翌日17:59の24時間ごとの期間
本検証	当委員会が実施した後記III・IVの検証
本障害	本システムの不具合により2023年9月26日18:00の投票権付与の一部が約8時間遅延した障害

1. 委員会の構成

- 当委員会は、当社から委嘱を受けた専門家3名の委員により構成されます。

永井 徳人	光和総合法律事務所 パートナー 弁護士・公認内部監査人・公認システム監査人 特定非営利活動法人日本システム監査人協会 理事
齋藤 孝道	明治大学 理工学部情報科学科 教授 レンジフォース株式会社 代表取締役 IPA情報処理技術者試験・情報処理安全確保支援士試験委員
上野 宣	株式会社トライコーダ 代表取締役 国立研究開発法人情報通信研究機構 実戦的サイバー防御演習 推進委員 情報経営イノベーション専門職大学 客員教員

- 各委員が選任した補助者は、当委員会に直属し、本検証等の業務を補助しました。

2. 委員会の独立性

- 当委員会の委員及び補助者は、過去に、役員、従業員、顧問、業務委託等の名目を問わず、当社の事業に関与したことはありません。
- 当委員会は、当社と締結した契約等により下記の体制を確保し、当社からの独立性をもって本検証を実施しました。
  - 当社は、当委員会の求めに応じて、迅速に、資料、情報等を提供する。
  - 開発ベンダ、暗号資産交換業者、その他の関係者に協力させる。
  - 上記の関係者の協力に際し、費用が発生する場合は、当社が負担する。
  - 当委員会は、上記の関係者と直接連絡をとることができる。
  - 本検証の手法は、当委員会の判断により選択する。
  - 本報告書の起案権は、当委員会に専属する。
- 委員及び補助者は、投票権を保有していません。

1. 投票結果の確認

- 当委員会は、当社が集計した投票結果を閲覧し、上位得票者11名が下記のとおりであり、当社が最終合格者として公表する11名と一致することを確認しました。

アオ	アリー	ココア	サマー
チョコ	ナコ	ナビ	ニコ
ハンナ	ピース	モモテレ	

（五十音順・敬称略）

2. プロセスの合理性

- 当委員会は、後記Ⅲ3の仮定を前提とする限り、後記Ⅲ2の本検証の対象範囲において、

> 投票結果に対する当社による恣意的な操作、第三者による不当な影響等の不適切な点は見当たらず、本投票のプロセスは一定の合理性をもって設計・運用された

と評価しました。

※ ただし、本委員会の活動には一定の制約があり、投票結果の完全性や本検証の対象範囲外での第三者を介した不当な影響等まで網羅的に検証できたものではありません。（後記Ⅲ2・3参照）

1. 本検証の概要

(1) 実施期間

2023年9月25日～10月2日

(2) 検証方法

- 当社、開発ベンダからのヒアリング・質疑応答
- 本システムの仕様書等の開発時のドキュメント、IEO時の開示情報、本システムの利用規約、当社のユーザ向けリリース等の関係資料の閲覧
- 本システム（ユーザ画面、管理画面）のデモの閲覧、ステージング環境での操作
- 暗号資産交換業者から直接入手したオリジナルデータと本システム上のデータの照合
- クーポンコード、本システムから抽出したデータの分析
- 本システムでイレギュラーな操作が発生した場合の挙動の確認
- 本投票においてとられた不正防止措置の合理性の検討

2. 本検証の対象範囲

- 当委員会は、評価の主目的を「**本投票の投票結果を当社が恣意的に操作した疑いがないか検証すること**」とし、次ページの検討対象の範囲内で本検証を実施しました。
- 当委員会は、臨時の機関であり、その活動には、時間やリソースの制限、関係者の任意の協力に基づくこと、システムの設計・設定によるログ等の情報を取得可能な範囲の制限といった限界があります。そのため、網羅的な検証等は困難であり、下記の業務は、対象外としています。
  - 各候補者の得票数の集計
  - 本システムや暗号資産交換業者のシステムのバグ、脆弱性等の不具合（本障害を除く）の有無の検証
  - 第三者によるIDの盗用、不正アクセス等の有無の検証
  - その他、本委員会が短期間に合理的に検証することが困難な事項の確認

2. 本検証の対象範囲

検討対象

① ユーザが暗号資産交換業者のシステム上でIEOに申込（NIDT購入） 2023/3/29～4/19
（アカウント登録時に犯罪収益移転防止法に基づく本人確認）

② 暗号資産交換業者がユーザごとのクーポンコードを発行（クーポンコードリストを作成）

③ 暗号資産交換業者が当社にクーポンコードリストを送信

④ 当社がクーポンコードリストの情報を本システムにインポート

⑤ 暗号資産交換業者が各ユーザにクーポンコードを電子メールで送信

⑥ ユーザが本システム上でクーポンコードを登録（アカウント登録時にSMS認証）

暗号資産交換業者のシステム上のユーザアカウントと本システム上のユーザアカウントは、クーポンコードリスト上では紐づいておらず、クーポンコードの突合により、各ユーザのIEO申込口数を本システム上に反映

⑦ 本システム上でIEO申込口数（IEOでのNIDT購入数）に応じてユーザに投票権を付与

⑧ ユーザが本システム上で投票、本システムで得票数の集計 2023/9/24 18:00～9/30 17:59

3. 所与の前提

- 前記のとおり本検証には様々な制約があることから、下記の事項については、所与の前提として仮定した上で、本検証を実施しました。
（下記の事項についての検証は、実施していません。）

  - 暗号資産交換業者から当社に提供されたクーポンコードリストに誤りがないこと
  - 本システムについて、当委員会に開示された仕様書どおりに実装されていること
  - 開発ベンダが本委員会に提供するデータ、その他の情報に誤りがないこと
  - 当社及び開発ベンダ、その他の取引先等の役員、従業員、その親族等、当社の意向を受けて投票する関係者がユーザとなっていないこと
  - 本システム、暗号資産交換業者のシステム、ユーザが使用する電子メールシステム、その他本投票に関連するシステム、通信回線等が正常に稼働すること（本障害を除く）

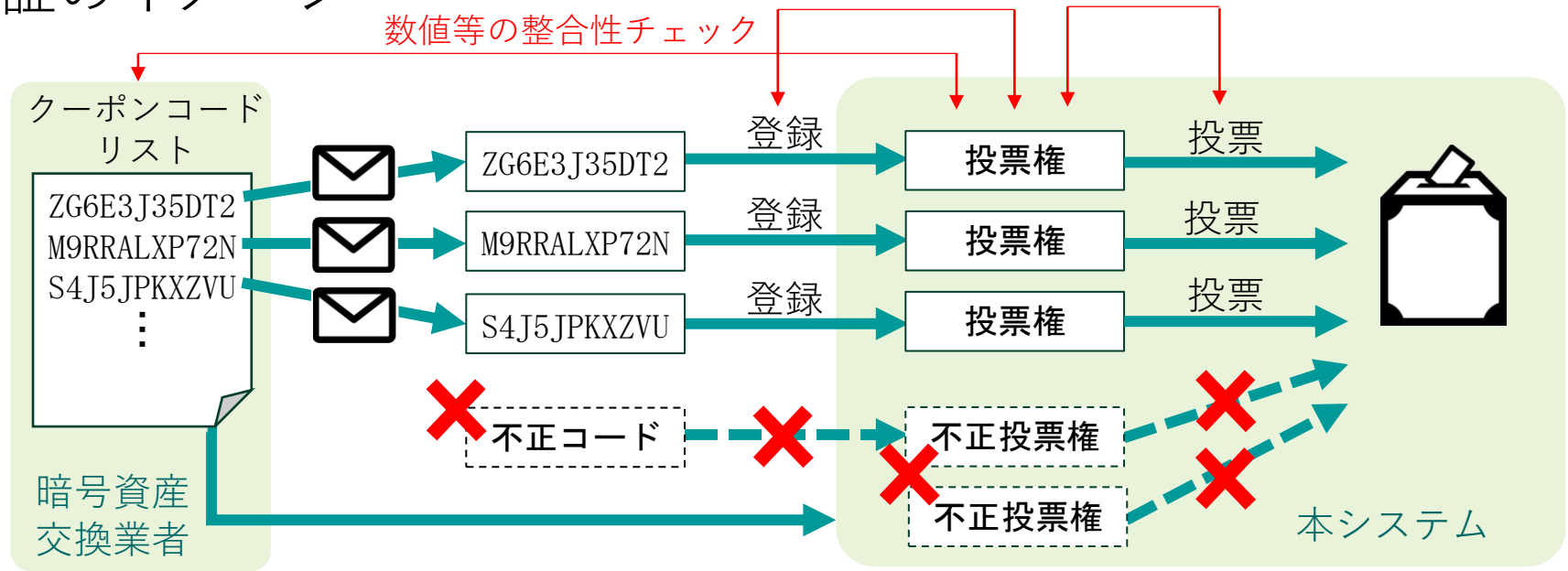
3. 所与の前提

- 仮に前ページの仮定が事実と異なる場合、下記の可能性は排除できません。ただし、下記のとおり一定の防止策はとられています。

排除できない可能性	左記の点に対してとられた防止策等
システムエラー、不正アクセス等により、本投票の集計結果に誤りが生じる。	• システム開発時のテスト • 一般的なセキュリティ対策
当社が、開発ベンダや暗号資産交換業者の協力を得て、投票結果を恣意的に改ざんする。	• 当委員会の設置 • 当社が、当委員会との契約において、投票結果に不当に影響を及ぼす行為を、直接・間接に行っていないことを表明・保証
当社役員・従業員が、親族・知人等の名義を借りて、正当なプロセスに則って、実際にNIDTを購入し、意図する結果が生じるように投票を行う。	• 当社の役員・従業員、開発ベンダ、その他の協力者等の関係者に対し、IEO申込をしないよう注意喚起 • 関係者リストを暗号資産交換業者と共有し、関係者からのIEO申込がないか、暗号資産交換業者が確認（実際にリスト掲載者からのIEO申込はなかった）

1. 本検証の結果

- 本検証の結果、正規のクーポンコードにより、IEO申込口数に応じた投票権がP16のルールにしたがって付与され、クーポンコードを登録したユーザのみが投票を行い、各候補者の得票数に反映されたことを確認しました。
- 本検証のイメージ



2. クーポンコードに関する検証

- 下記の検証等により、不正な投票権は存在せず、クーポンコードを登録したユーザのみが投票を行ったと考えられます。
  - オリジナルデータと実データの照合

A 暗号資産交換業者から当委員会が直接（当社や開発ベンダを介さずに）入手したオリジナルのクーポンコードリスト

ZG6E3J35DT2	40口
M9RRALXP72N	150口
S4J5JPKXZVU	3口
⋮	
（4,572件）	

当委員会独自のプログラムで照合

B 投票期間終了後に本システムのデータベースから抽出した登録済クーポンコードとIEO申込口数のリスト

ZG6E3J35DT2	40口
M9RRALXP72N	150口
S4J5JPKXZVU	3口
⋮	
（1,394件）	

B に含まれるクーポンコードとIEO申込口数の組み合わせ（投票権付与の対象）は、全て **A** に含まれることを確認。

2. クーポンコードに関する検証

- クーポンコードリストに記載されていないクーポンコードは本システムに登録できない仕様であることを確認。
- 本システムにおいて、短時間に繰り返し誤ったクーポンコードを登録しようとするとユーザアカウントがロックされる仕様であることを確認。クーポンコードは、ランダムに生成された11桁または13桁の英数字だが、上記仕様により、いわゆる「総当たり」により正規のクーポンコードを登録することは事実上不可能。
- IEO申込は、暗号資産交換業者2社に対し各1回のみで、申込1回につき1個のクーポンコードが発行されるため、1ユーザが登録したクーポンコード数は、2を超えない。この点を全ユーザについて、投票期間終了後に本システムから抽出したデータで確認。
- 暗号資産交換業者のシステムのアカウント登録時には犯罪収益移転防止法に基づく運転免許証等による本人確認、本システムのアカウント登録時にはSMSによる認証が行われ、容易に架空アカウントの作成ができない仕組みになっていることを確認。

3. 投票権付与プロセスの検証

◘ 投票権の付与ルール

- 毎投票日の18:00に投票権が付与され、24時間で失効（毎投票日に投票可能）

  各投票日18:00に付与される投票権数
  ＝IEO申込口数＋増量分(IEO申込口数10口ごとに10票)

  ※ 暗号資産交換業者2社の両方でIEOに申し込んだ場合、各申込口数を合算して計算

  ※ 例えば、IEO申込口数がDMM bitcoinで38口・coinbookで26口の場合、1投票日に付与される投票権数は、64票＋増量分60票＝124票

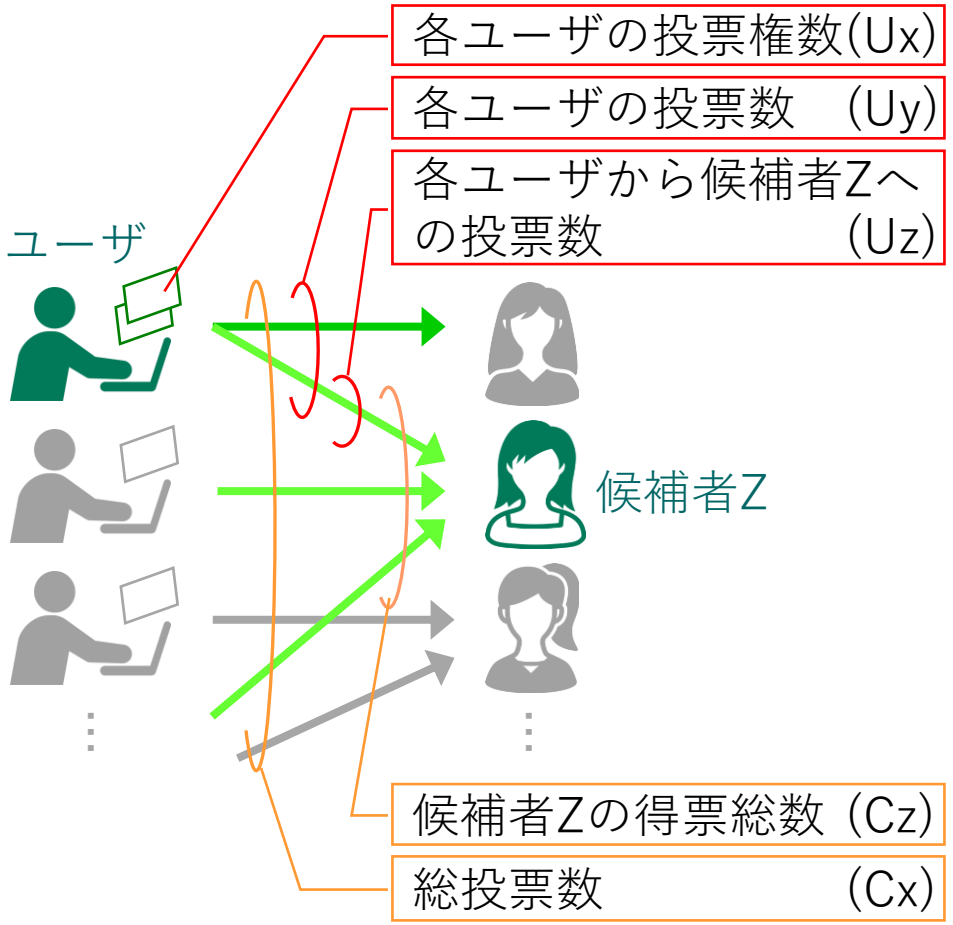
  ※ 投票期間の途中でクーポンコードを登録した場合、次の投票日から投票権を付与

◘ 投票日ごとに、各ユーザに対して、IEO申込口数に応じて上記ルールに基づき、投票権が正確に付与されていることを確認しました。

- 仕様書を閲覧し、本システムの仕様が上記ルールに沿っていることを確認。
- 「クーポンコードを登録したタイミング」も踏まえ「上記の付与ルールに基づく投票権の総数」が正確であることを、投票期間終了後に本システムから抽出したデータで確認。

4. 投票プロセスの検証

- 投票日ごとに下記の関係の整合性を確認し、「ユーザの投票数」と「候補者の得票数」が矛盾しないことを、投票期間終了後に本システムから抽出したデータから確認しました。
  - UxとCxの関係を検証し、「候補者の得票総数」が「各ユーザが保有する投票権の総数」を超えていないこと
  - UxとUyの関係を検証し、各ユーザが保有する投票権数を超えて投票していないこと
  - UzとCzの関係を検証し、「候補者Zの得票総数」と「各ユーザから候補者Zへの投票数の総数」が一致すること

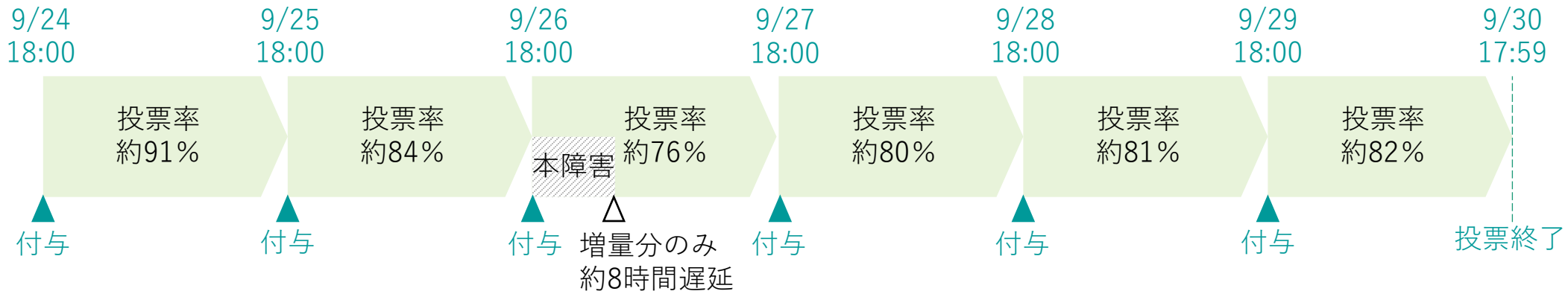


4. 投票プロセスの検証

- 下記のような操作をしても、本システムの仕様上、重複して投票ができないことを確認しました。
  - 投票直後にブラウザバック（「戻る」ボタンを押下）
  - 複数の端末（例えばPCとスマートフォン）で、または、同一端末の複数のブラウザで、同時に本システムにログイン
- 本システムの仕様や運用設計上、当社が本システム上の投票結果を直接改ざんできないことを確認しました。
  - 当社は、本システムの管理画面のアカウントを保有しているが、管理画面の仕様上、投票数を直接変更することはできない。
  - 投票数が記録される本システムのデータベースへのアクセス権は、本システムの運用業務の委託先のみが保有しており、当社は保有していない。

5. 本障害の影響

- 本障害による影響は否定できないものの、次の点で限定的と考えられます。
  - 投票権（増量分のみ）付与の遅延発生は、投票期間6日のうち1日のみ。
  - 遅延発生中も、メンテナンスのためにシステム停止した約1時間を除き、正常に付与された投票権（当日付与されるべき投票権の50％強）については、投票可能であった。
  - 付与が遅延した投票権での投票ができなかったのは、有効期間24時間中約8時間で、残りの約16時間は正常に投票可能であった。
  - 本障害発生日の投票率（24時間ごとに有効な投票権総数のうち実際の投票数の割合）には本障害の影響がうかがわれるが、前後の投票日との差異は重大とまではいえない。



5. 本障害の影響

- 本障害は、下記のとおり、一部の特定の候補者に有利・不利に働くものではなく、当社による恣意的な操作によるものではないと考えられます。
  - 投票権（増量分）の付与の遅延は、全ユーザ（10口未満で増量分がないユーザを除く）に対して、同条件で発生。
  - 本障害の原因は、投票権（増量分）付与の処理時間が予測を超えて長くなり、設定されていたタイムアウト※閾値を超えたため、処理が停止したこと。

    ※処理時間が一定の時間を超えるとエラーと判定して処理を中止する機能
  - 恣意的に投票結果に影響を与えようとすれば、相当数の投票権を操作する必要があるが、本障害では逆に投票権数が多い程、投票できない数が増えるため、恣意的な操作の手段としては非効率。

以上