

CARDANO ブロックチェーン エコシステム 憲法

フレーミングノート

これらのフレーミング ノートは、この憲法の一部とはみなされません

(英語版はこちら ***Draft Cardano Constitution 20.11.2024_PDF*** :

<https://2024constitutionalconsultation.docs.intersectmbo.org/cardanos-constitution/draft-cardano-constitution>)

Cardano ブロックチェーンは 2017 年に設立されました。2020 年 7 月には *Cardano* ブロックチェーンが拡張され、独立したブロック検証者が加わり、2024 年 9 月にはオンチェーン ガバナンス システムが導入されました。この憲法は、*Cardano* ブロックチェーンのガバナンストークンである *ada* の所有者を代表する、分散型システムのガバナンス アクターの権利と責任を概説しています。*Cardano* ブロックチェーンは現在、ブロックチェーン テクノロジー、スマートコントラクト、コミュニティ ガバナンスの分散型エコシステムです。

この憲法に取り組むにあたり、*Cardano* コミュニティは、これがブロックチェーンだけの憲法ではなく、ブロックチェーン エコシステムの憲法であり、はるかに野心的な取り組みであることを忘れてはならないことを認識しています。したがって、ガバナンス アクションの承認方法は非常に重要ですが、それがこの憲法の唯一の焦点ではありません。むしろ、この憲法は、*Cardano* コミュニティのすべての参加者が集まって自らを統治し、人間の相互作用とコラボレーションに対する根本的に新しいアプローチを形成するための基礎と基本的な枠組みを提供します。

必然的に、この憲法は憲法委員会の役割を認め、権限を与え、*Cardano* コミュニティが共同体に参加して協力する権利を確認し、オンチェーンガバナンスを実施し、*DReps*にオンチェーン投票における*ADA*所有者の代弁者として行動する権限を与えます。

また、この憲法では、*Cardano* ガードレールをこの憲法に盛り込むことにより、*Cardano* トレジャーへのアクセスと使用を保護する必要性も認めています。

前文

Cardano は、ブロックチェーン技術、スマートコントラクト、コミュニティ ガバナンスの分散型エコシステムであり、あらゆる場所のすべての人々のために経済、政治、社会システムを改善することに取り組んでいます。この基盤となるインフラストラクチャを提供することで、*Cardano* は、分散型アプリケーション、ビジネス、ネットワーク状態の出現を促進し、個人やコミュニティがアイデンティティ、価値、ガバナンスを管理できるようにします。

個人、組織、貢献者、その他で構成される私たち*Cardano* コミュニティの参加者は、不変のデータの公平な処理を通じて、デジタル技術を通じてコミュニティの絆を最初に築いた初期のイン

ターネットと暗号通貨の先駆者の足跡をたどることを選択します。私たちは、分散化された意思決定と説明責任のバランスをとり、Cardanoブロックチェーンのセキュリティを保護することで自己統治を実践し、共通の原理と原則に従っています。

従来の国家ガバナンスシステムに依存するのではなく、Cardanoコミュニティによる自治に依存し、ガバナンスプロセスにおいて可能かつ有益な限りブロックチェーン技術を活用する、より強固でダイナミックな統治フレームワークの必要性を認識し、Cardanoブロックチェーンエコシステムを統治し、Cardanoブロックチェーンの継続性を確保し、Cardanoブロックチェーンを利用する人々の権利を守るために、ここに本Cardano憲法を制定します。

これらの目的を念頭に置き、私たちCardano コミュニティは、Cardano ブロックチェーン エコシステムのガバナンスに参加するために、この憲法を遵守する意思を表明します。私たちは、私たちの価値観を共有するすべての人に加わっていただくよう呼びかけますが、別の道を歩むことを望む人の邪魔をすることはありません。

第1条 カルダノブロックチェーンの原則とガードレール

第1項

以下の原則は、憲法委員会を含むCardano コミュニティのすべての参加者を導くものであり、提案されたガバナンス活動はこれらの原則に従って評価されるものとします。以下の原則の順序は、原則間の優先順位を表すものではありません。

原則1 Cardano ブロックチェーン上のトランザクションは、遅延または検閲されてはならず、意図された目的に沿って適切に処理されるものとします。

原則2 Cardano ブロックチェーン上の取引コストは予測可能であり、不合理なものであってはなりません。

原則3 Cardano ブロックチェーン上でアプリケーションを開発および展開することを希望する者は、そのアプリケーションを意図したとおりに開発および展開することを不当に妨げられてはなりません。

原則4 Cardano ブロックチェーンにおける Cardano コミュニティの貢献は、SPO および DRep との報酬共有、適切なトークノミクス、およびマルチリソースのコンセンサスアプローチを通じて、公正に認識、記録、評価されるものとします。

原則5 Cardano ブロックチェーンは、ADA 所有者の同意なしにその所有者の価値をロックしてはなりません。

原則6 Cardano ブロックチェーンは相互運用性を不当に妨げてはなりません。

原則7 Cardano ブロックチェーンは、ADA 所有者がカルダノブロックチェーンに保存しようとするあらゆる価値と情報を安全な方法で保存するものとします。

原則8 Cardano ブロックチェーンはリソースを不当に消費しないものとします。

原則9 Cardano ブロックチェーンのすべてのユーザーは、Cardano ブロックチェーン コミュニ

ティの集合的な要望を考慮し、Cardano ブロックチェーンの長期的な持続可能性と実現可能性に沿って平等に扱われるものとします。

原則10 財政の安定性を維持し、ADA の総供給量は 45,000,000,000 (45,000,000,000,000,000 lovelace) を超えないものとします。

第2項

Cardanoブロックチェーンは、本憲法のガードレール付録に定めるCardanoブロックチェーンガードレールに従って運用されるものとします。Cardanoコミュニティは、随時、特定のCardanoブロックチェーンガードレールをデジタルコード化し、そのようなCardanoブロックチェーンガードレールがオンチェーンスクリプトまたは組み込みledgerルールを使用して、Cardanoブロックチェーン上で直接プログラムされ実装されるようにすることができます。

ガードレール付録に記載されているCardanoブロックチェーン ガードレールと、Cardano ブロックチェーン上でプログラムおよび実装されているCardano ブロックチェーン ガードレールとの間に矛盾がある場合、Cardano ブロックチェーン上に直接展開されているCardano ブロックチェーンガードレールのバージョンが優先され、憲法委員会は適切なオンチェーン ガバナンス アクションの促進を通じて、そのような矛盾を調整するよう努めるものとします。

第2条 Cardanoブロックチェーンコミュニティ

第1項

Cardanoブロックチェーンを使用し、これに参加し、その恩恵を受けるためには、正式な会員資格は必要ありません。その代わりに、ADA のすべての所有者、Cardano ブロックチェーンのすべての開発者、Cardano ブロックチェーンを構築するすべての人々、およびその他 Cardano ブロックチェーンをサポート、維持、または使用するすべての人々は、Cardano コミュニティの参加者とみなされ、Cardano ブロックチェーン エコシステムの受益者として認められます。したがって、Cardano コミュニティのすべての参加者は、この憲法の受益者であり、その権利、特権、および保護を受ける権利があり、したがって、この憲法を支持し、支持することが期待されます。

第2項

ADA を所有する Cardano コミュニティの参加者は、Cardano ブロックチェーンに関するオンチェーン ガバナンス アクションへの投票や参加など、Cardano ブロックチェーン エコシステムのオンチェーン意思決定プロセスにアクセスして参加する権利を有します。

第3項

Cardano コミュニティは、本憲法に従い、Cardano ブロックチェーンを運用し、Cardano ブロックチェーンのガバナンス活動に参加し、公正かつ透明な方法で紛争を解決することにより、Cardano ブロックチェーン エコシステムの完全性を維持する責任を負います。

第4項

Cardanoコミュニティは、本憲法の規定を通じて、Cardanoブロックチェーンのアプリケーションの開発、維持、構築に協力し、CardanoコミュニティがCardanoブロックチェーンエコシステムをサポートするために望ましい、または適切であると判断した一時的または永続的な組織、協会、その他の団体を結成する権利と奨励を受けます。

第3条 参加型および分散型ガバナンス

第1項

Cardano ブロックチェーンは、可能な限り有益な範囲でスマートコントラクトやその他のブロックチェーン ベースのツールを活用し、意思決定を容易にし、透明性を確保する、分散型のオンチェーン ガバナンス モデルによって管理されます。ガバナンス アクションに対するオンチェーン投票は、Cardano ブロックチェーン ガードレールに概説されているプロセスに従うものとします。

第2項

3 つの独立したガバナンス機関が、オンチェーン ガバナンス アクションの投票に参加し、委任代表者 (DReps)、ステークプール オペレーター (SPO)、憲法委員会 (CC) により Cardano ブロックチェーンのチェックとバランスを実現されます。

第3項

オンチェーン ガバナンスの決定は、Cardano ブロックチェーン ガードレールで要求される特定のコンセンサスしきい値要件を伴う集団意思決定プロセスを通じて行われます。すべてのオンチェーン ガバナンス アクションは、Cardano ブロックチェーン ガードレールに従って投票されます。

第4項

すべての ADA 所有者は、本憲法および Cardano ブロックチェーン ガードレールに規定されている制限または要件に従い、オンチェーン ガバナンス アクションの意思決定プロセスで投票する権利を持ちます。すべての ADA 所有者は、Cardano ブロックチェーン ガードレールに従って、Cardano ブロックチェーン エコシステムのガバナンス構造の変更を提案する権利を持ちます。ADA を保管するためにサードパーティ カストディアンまたはその他の指定者を使用する ADA 所有者は、そのようなサードパーティが自分に代わって投票することを承認するか、承認を保留することができます。

第5項

オンチェーン ガバナンス アクションの特別な形式である「情報」アクションは、Cardano ブロックチェーンのオンチェーン変更コミットすることなく、コミュニティの感情を測定できるようにするために存在します。「情報」アクションは、Cardano ブロックチェーンでの投票の結果を記録する以外には、オンチェーンには影響しません。

第6項

オンチェーン ガバナンスのプロセスの透明性を高めるために、オンチェーンで記録または施行される前に、提案されたすべてのガバナンスアクションは、文書化されたオフチェーンコンテンツにリンクされた URL とハッシュを含む、標準化された判読可能な形式に従うことが求められます。Cardano ブロックチェーンへの変更要求を正当化するために十分な根拠が提供されるものとします。根拠には、少なくとも、タイトル、概要、提案の理由、および関連する裏付け資料を含めるものとします。

すべてのオンチェーン ガバナンス アクションの内容は、提案されたアクションの最終的なオフチェーン バージョンと同一である必要があります。

「ハードフォークの開始」および「プロトコル パラメータの変更」ガバナンス アクションは、Cardano ブロックチェーン ガードレールで義務付けられている十分な技術的レビューと精査を受け、ガバナンス アクションが Cardano ブロックチェーンのセキュリティ、機能、パフォーマンス

ス、または長期的な持続可能性を危険にさらさないことを確認する必要があります。オンチェーンガバナンスアクションは、Cardano ブロックチェーン エコシステムへの予想される影響に対処する必要があります。

すべてのADA所有者は、オンチェーンガバナンスアクションへの参加、提出、投票のプロセスがオープンかつ透明であり、不当な影響や操作から保護されていることを保証する権利を有します。

第7項

Cardanoコミュニティは、この憲法を施行し、Cardanoブロックチェーンの将来のすべてのガバナンス活動についての認識と議論および形成の機会を確保するために必要となるオフチェーンガバナンスプロセスの作成、維持、および継続的な管理をサポートすることが期待されています。

第8項

Cardano コミュニティは、Cardano ブロックチェーンの継続的なメンテナンスと将来の開発のための予算を、少なくとも毎年提案することが求められています。ADA のすべての所有者は、オンチェーンの「情報アクション」を通じて、Cardano ブロックチェーンの予算を定期的に承認することが求められています。Cardanoブロックチェーンのトレジャリーからの引き出しは、Cardanoブロックチェーンのガードレールが要求しているように、その時点で有効であり、憲法委員会が違憲であると判断していないCardanoブロックチェーンの予算に基づいて、承認され、実行されていない限り、許可されないものとします。Cardano ブロックチェーン の予算には、Cardano ブロックチェーン のトレジャリーからの引き出しによる資金の使用を監視するプロセスが指定され、これにはそのような監視を担当する 1 人以上の管理者の指定が含まれます。

Cardano ブロックチェーン のトレジャリーから ADA を要求するガバナンスアクションには、定期的な独立監査の費用と、その ADA の使用に関する監視メトリックの実装をカバーするために、そのような資金要求の一部として ADA の割り当てが必要になります。Cardano 予算に従って Cardano ブロックチェーンのトレジャリーから受け取った ADA の使用を管理する契約上の義務には、紛争解決条項が含まれます。

第4条 委任代表者

第1項

ガバナンスアクションに参加するために、ADA の所有者は DRep として登録し、そのようなガバナンスアクションに直接投票するか、登録されている他の DRep に投票権を委任して、その DRep が代わりに投票することができます。

第2項

すべての ADA 所有者は、DRep として登録するオプションを持つものとします。ADA 所有者は、自分自身を含む 1 人以上の登録済み DRep に投票権を委任することができます。DRep は個人または調整されたグループです。ADA を保管するためにサードパーティのカストディアンまたはその他の指定者を使用する ADA 所有者は、そのようなサードパーティが所有者に代わって登録済み DRep に ADA 所有者の投票権を委任することを承認するか、または承認を保留することができます。DRep は、オンチェーン ガバナンス アクションに直接投票する権利を持ち、投票権を委任する ADA 所有者を代表します。

この投票システムは、ADA の所有者がシームレスに DRep を選択し、DRep として登録し、い

いつでも委任を取り消したり変更したりできる、液体民主主義モデルを制定するものとします。

第3項

他の ADA 所有者に代わって活動する DRep は、DRep としての活動を規定する行動規範を定期的に採用し、適切と思われる場合は更新し、そのような行動規範を一般に公開することが求められます。DRep は、行動規範に倫理ガイドラインを含めることが推奨されます。

第4項

Cardano コミュニティは、ADA 所有者が DRep 候補を調査および評価し、DRep 行動規範にアクセスして評価し、関連性があると思われる基準に基づいて DRep を選択できるようにするツールの作成、保守、継続的な管理をサポートすることが期待されています。

第5項

他の ADA 所有者に代わって活動する DRep には、その活動に対する報酬が支払われる場合があります。DRep は、DRep としての活動に関連して受け取った報酬をすべて開示する必要があります。DRep は、ADA 所有者またはその代理人によって DRep に任命されたこと、または ADA 所有者またはその代理人に代わって投票したものと引き換えに、ADA 所有者またはその代理人に報酬を支払うことはできません。

第5条 ステークプールオペレーター

第1項

SPO は、Cardano ブロックチェーン ガードレールに定められているように、DRep とは別個かつ独立して投票し、追加の監視と独立性を必要とする重要なオンチェーン ガバナンス アクションを承認する特定の役割を担います。SPO は、Cardano ブロックチェーンのコンセンサスメカニズムに参加するノードのオペレーターとして、ハードフォーク開始プロセスに参加します。

第2項

SPO は、例外的な状況下では、「不信任決議」と「委員会/しきい値の更新」ガバナンス アクション、およびセキュリティ上重要なパラメータに影響を与える「パラメータ更新」ガバナンス アクションに個別に投票することにより、憲法委員会の権限をチェックする役割を果たします。

第3項

SPO は、SPO としての活動を規定する行動規範を定期的に採用し、適切と思われる場合には更新し、その行動規範を一般に公開することが推奨されます。SPO は、行動規範に倫理ガイドラインを含めることが推奨されます。

第4項

SPO であり、かつ DRep としても機能している ADA の所有者は、オンチェーン ガバナンスの権利を行使する前に、両方の立場でオンチェーン ガバナンス アクションに参加していることを公に開示するものとします。

第6条 憲法委員会

第1項

オンチェーンで施行されるガバナンス活動が本憲法に準拠していることを保証する、Cardano のオンチェーン ガバナンス プロセスの部門として、憲法委員会が設立されます。憲法委員会は、チェーン上で施行される前のオンチェーン ガバナンス活動が合憲であることを保証する共同責任を負う ADA 所有者のグループで構成されます。本憲法に規定されている限定的な例外を除き、憲法委員会は、オンチェーンで施行されるガバナンス活動の合憲性に関する投票に限定されます。憲法委員会のメンバーは、Cardano ブロックチェーン エコシステムへの過去の貢献と関与を考慮して、必要な責任を遂行するために適切な専門知識を持っていることが求められます。

第2項

憲法委員会は、Cardano ブロックチェーンガードレール に準拠し、Cardano ブロックチェーン の継続的な整合性を保証するのに十分な数の ADA 所有者によって随時決定されるメンバーで構成されるものとします。

憲法委員会のメンバーの任期は、Cardano ブロックチェーンガードレール に規定されている最短および最長の任期と一致するように、ADA 所有者によって随時決定されるものとします。憲法委員会の運営の継続性を確保するため、憲法委員会のメンバーの任期は交互に設定されます。

第3項

Cardanoコミュニティは、Cardanoブロックチェーンガードレールの要件に従って、憲法委員会のメンバーを選出するためのプロセスを随時確立し、公開するものとします。

第4項

「不信任決議」または「憲法委員会しきい値の更新」以外のガバナンスアクションは、憲法委員会のメンバーのガードレールによって指定された必要な割合が、そのような提案が本憲法に違反していないことをオンチェーンアクションを通じて最初に決定し確認しない限り、オンチェーンで実装することはできません。

「情報」アクションはオンチェーン効果を持たず、したがって合憲でも違憲でもないため、憲法委員会のメンバーは「情報」アクションがオンチェーンに記録されるのを防ぐことはできません。ただし、憲法委員会のメンバーは、「情報」アクションに関する投票をオンチェーンに記録して、そのような「情報」アクションに関する意見を表明することはできます。これには、そのような「情報」アクションで提案された行動方針が、オンチェーンメカニズムによって強制された場合、そのメンバーの見解では違憲になるかどうかも含められます。

Cardanoブロックチェーンの予算を提案する「情報アクション」の場合、憲法委員会のメンバーは、提案された予算が「情報」アクションに含まれる形式で実施された場合にこの憲法に違反するかどうかについての意見を表明する投票をチェーン上で記録するものとします。

以前に承認された予算に従ってCardanoトレジャリーからの引き出しを提案する「情報」アクションの場合、憲法委員会のメンバーは、そのような「情報」アクションに従って行われた場合、提案された引き出しがこの憲法に違反するかどうかについての意見を示す投票をチェーン上で記録するものとします。

第5項

憲法委員会は、常に次の 2 つの状態のいずれかにあるとみなされます: 信頼状態または不信

任状態。不信任状態では、その時点での憲法委員会のメンバーは、「情報」アクション以外の他のオンチェーン ガバナンス アクションを進める前に、「憲法委員会/きい値の更新」ガバナンス アクションを使用して復帰または交代する必要があります。不信任状態の間、予算案またはトレジャリー引き出し案に関連する「情報」アクション以外の「情報」アクションは、引き続きオンチェーンに記録される場合があります。

憲法委員会のメンバーが、SPO および DRep のガードレールで指定された必要な割合で決定された本憲法で要求される責任を果たしていない場合、または「不信任決議」ガバナンス アクションに従って個別に投票された場合、そのメンバーはガバナンス アクションの実行時に憲法委員会から除名されるものとします。その後、除名されたメンバーの代わりとなる選挙が、可能な限り速やかに実施されるものとします。

憲法委員会の全委員を同時に解任する「不信任決議」のガバナンス措置が、DRep および SPO のガードレールで指定された必要な割合で承認された場合、ガバナンス措置の実施時に、憲法委員会は、既存の憲法委員会委員の全員または一部を復職させるか、新しい憲法委員会委員を選出するための選挙が実施されるまで、不信任状態にあるものとみなされます。

第6項

憲法委員会のプロセスは透明でなければなりません。憲法委員会は、それぞれの決定を公表するものとします。オンチェーンで実行することが提案されているガバナンスアクションが違憲であると投票する場合、憲法委員会全体で、または憲法委員会の各メンバーが個別に投票する場合は、この憲法の特定の条項または特定の提案と矛盾するガードレール付録の条項を参照して、決定の根拠を示すものとします。投票前の憲法委員会メンバー間の内部審議は、公開する必要はありません。

憲法委員会は、憲法委員会が定期的に採択し公表する行動規範に従って運営されるものとします。憲法委員会は、その行動規範に倫理ガイドラインを含めることが推奨されます。憲法委員会は、その職務を遂行する上で必要であるとみなす方針および手順を定期的に採択し公表するものとします。

第7項

Cardano コミュニティは、憲法委員会が必要な機能を遂行するために必要かつ適切なツールの作成、保守、継続的な管理をサポートすることが期待されています。

第8項

憲法委員会のメンバーは、憲法委員会のメンバーとしての活動に対して報酬を受け取ることができます。憲法委員会のメンバーは、メンバーとしての活動に関連して受け取った報酬がすべて開示されるようにする必要があります。Cardano ブロックチェーン に承認された予算には、ADA 所有者によって随時承認される金額で憲法委員会のメンバーに報酬を支払うのに十分な Cardano ブロックチェーン のトレジャリーからの割り当てが含まれる場合があります。また、憲法委員会によって随時要求され、ADA 所有者によって承認される金額で憲法委員会の定期的な管理費用を賄う必要があります。

第7条 改正

第1項

この憲法は生きた文書として扱われるべきです。技術の進歩、カルダノコミュニティの希望、ニーズ、期待の変化、予期せぬ状況により、将来的にこの憲法を改正する必要性が生じる可能性があります。カルダノコ

コミュニティは、この憲法の条項を定期的に見直して議論し、必要に応じてカルダノコミュニティが適切と考えるフォーラムに集まり、この憲法の改正を提案します。改正は、本第7条に定めるところに従って行うことができます。

第2項

Cardano ブロックチェーンガードレール 付録に別途規定されている場合を除き、Cardano ブロックチェーンガードレール 付録を含む本憲法の改正は、その時点で有効な議決権の 67% 以上のしきい値を満たす ADA 所有者によるオンチェーン ガバナンス アクションを必要とする集団意思決定プロセスによって承認されるものとします。

第3項

Cardano ブロックチェーン ガードレールの付録に、本第7条第2項に含まれる改正しきい値とは異なる Cardano ブロックチェーン ガードレールの改正しきい値が定められている場合、その Cardano ブロックチェーン ガードレールについては Cardano ブロックチェーン ガードレールの付録に定められているしきい値が適用されるものとします。

付録1: カルダノブロックチェーン ガードレール

1. はじめに

Cardano ブロックチェーンのオンチェーン ガバナンスを実装するには、Cardano ブロックチェーンが安全かつ持続可能な方法で運用を継続できるようにする適切なガードレールを確立する必要があります。

この付録では、プロトコル パラメータの変更やトレジャリー引き出しの制限など、Cardano ブロックチェーンのオンチェーン ガバナンス アクションに適用する必要があるガードレールについて説明します。これらのガードレールは、設定に関する必須かつ固有の制限と、経験、測定、ガバナンスの目的に基づいた推奨事項の両方をカバーしています。

これらのガードレールは、Cardano ブロックチェーンの運用における予期しない問題を回避するために設計されています。これらは、適切なパラメータ設定の選択をガイドし、セキュリティ、パフォーマンス、機能、または長期的な持続可能性に関する潜在的な問題を回避することを目的としています。以下で説明するように、これらのガードレールの一部は自動化可能であり、オンチェーン スクリプトまたは組み込みのledgerルールを介して適用されます。

これらのガードレールは、Cardano ブロックチェーン レイヤー 1 メインネット環境にのみ適用されます。テスト環境や、Cardano ブロックチェーン ソフトウェアを使用する他のブロックチェーンには適用されません。

Cardano ブロックチェーンのすべてのパラメータを独立して考慮できるわけではありません。一部のパラメータは、他の設定と本質的に相互作用します。これらの相互作用については、既知の場合、この付録で説明します。

この付録のガードレールは現時点では技術的知見の現状を反映していますが、この付録は生きた文書として扱う必要があります。Cardano ブロックチェーンの実装の改善、新しいシミュ

レーション、またはパフォーマンス評価の結果により、これらのガードレールに含まれる制限の一部が、やがて緩和される可能性があります (または、状況によっては、制限を強化する必要があります)。

たとえば、新しいプロトコル パラメータが導入される場合には、追加のガードレールが必要になる場合もあります。

ガードレールの改正、追加、廃止

この付録に記載されているガードレールは、この付録に記載されている適用可能な投票しきい値を満たすオンチェーンガバナンスアクションに従って、随時修正される場合があります。ガードレールの修正には、新しいガードレールを含め、憲法自体の修正が必要であり、修正とみなされます。各ガードレールには固有のラベルがあります。ガードレールのテキストが修正された場合、既存のガードレールは廃止され、この付録では新しいラベルが使用されます。同様に、ガードレールが完全に廃止された場合、そのラベルは将来再利用されることはありません。すべての場合において、ガバナンスアクションに適用されるガードレールは、その後の修正に関係なく、ガバナンスアクションがオンチェーンに送信された時点で有効なものになります。

用語とガイダンス

****すべき/すべきでない(Should/Should not)**** この付録で、ある値を「下回って設定すべきではない」または「上回って設定すべきではない」と記載されている場合、これはガードレールが推奨事項またはガイドラインであり、特定の値は、Cardano ブロックチェーンのガバナンス システムまたは Cardano ブロックチェーンの運用に関する経験を考慮して、Cardano コミュニティによって認められた適切な専門家グループによって議論または変更される可能性があることを意味します。

****しなければならない/してはならない(Must/Must not)**** この付録で、ある値を「しなければならない」または「してはならない」と記載されている場合、これはガードレールが、Cardano ブロックチェーンのledgerルール、タイプ、またはその他の組み込みメカニズムによって可能な限り強制される要件であり、それに従わないと、プロトコル障害、セキュリティ侵害、またはその他の望ましくない結果が発生する可能性があることを意味します。

****ベンチマーク(Benchmarking)**** ベンチマークとは、たとえば、すべてのケースに必要な 5 秒の時間間隔内に、Cardano ブロックチェーン ノードのグローバル ネットワーク全体に 95% のブロックが拡散されることを事前に示すように設計された、慎重なシステム レベルのパフォーマンス評価を指します。これには、特定のテストワークフローの構築と、Cardano ブロックチェーン ノードの大規模なテスト ネットワークでの実行が必要になり、グローバルな Cardano ブロックチェーン ネットワークをシミュレートする必要がある場合があります。

****パフォーマンス分析(Performance analysis)**** パフォーマンス分析とは、理論的なパフォーマンス、経験的なベンチマーク、またはシミュレーションの結果を予測して、実際のシステムの動作を予測することを指します。たとえば、制御されたテスト環境 (既知のネットワーク プロパティを持つデータ センターのコレクションなど) でのテストから得られたパフォーマンス結果を推定して、実際の Cardano ブロックチェーン ネットワーク環境での可能性のあるパフォーマンス動作を予測することができます。

****シミュレーション(Simulation)**** シミュレーションとは、パフォーマンスや機能の決定を反復可能な方法で通知するように設計された合成実行を指します。たとえば、IOSim Cardano ブロックチェーン モジュールを使用すると、ネットワーク スタックの動作を制御された反復可能な方法でシミュレートできるため、コードを展開する前に問題を検出できます。

****パフォーマンス モニタリング (Performance Monitoring)**** パフォーマンス モニタリングには、タイミング プローブを使用してラウンドトリップ時間を評価したり、ブロックをテストしてネットワーク全体の健全性を評価したりするなど、Cardano ブロックチェーン ネットワークの実際の動作を測定することが含まれます。シミュレートされたワークロードや理論的な分析では取得できない実際のシステム動作に関する情報を提供することで、ベンチマークとパフォーマンス分析を補完します。

****変更を元に戻す (Reverting Changes)**** パフォーマンス監視により、変更後の実際のネットワーク動作が Cardano ブロックチェーンのパフォーマンス要件と一致しないことが判明した場合、可能であれば変更を以前の状態に戻す必要があります。たとえば、ブロックサイズが 100 KB から 120 KB に増加し、ブロックの 95% が 5 秒以内に拡散されなくなった場合は、ブロックサイズを 100 KB に戻す変更を行う必要があります。これが不可能な場合は、パフォーマンス要件が満たされるように 1 つ以上の代替変更を行う必要があります。

****重大度レベル (Severity Levels)**** Cardano ブロックチェーン ネットワークに影響を与える問題は、重大度レベルによって分類されます。

- 重大度1は、Cardanoブロックチェーンネットワークのセキュリティ、パフォーマンス、機能、または長期的な持続可能性に非常に大きな影響を与える重大なインシデントまたは問題です。
- 重大度2は、Cardanoブロックチェーンネットワークのセキュリティ、パフォーマンス、機能、または長期的な持続可能性に重大な影響を与える重大なインシデントまたは問題です。
- 重大度3は、Cardanoブロックチェーンネットワークのセキュリティ、パフォーマンス、機能、または長期的な持続可能性への影響が低い軽微なインシデントまたは問題です。

****将来のパフォーマンス要件 (Future Performance Requirements)**** メモリ外ストレージ用の新しいメカニズムなどの計画された開発は、ブロックの拡散やその他の時間に影響を与える可能性があります。パラメータを変更するときは、Cardano ブロックチェーンの現在の動作だけでなく、これらの将来のパフォーマンス要件も考慮する必要があります。開発が完了するまでは、要件は控えめになりますが、実際のタイミング動作を考慮して緩和される可能性があります。

自動チェック(「ガードレール スクリプト」)

****新しい憲法またはガードレール スクリプト (New Constitution or Guardrails Script)**** ガバナンス アクションが施行されると、スクリプト ハッシュが憲法ハッシュに関連付けられます。これは、ledgerルールとタイプに対する追加の保護手段として機能し、準拠していないガバナンス アクションをフィルター処理します。

ガードレール スクリプトは、次の 2 種類のガバナンス アクションにのみ影響します。

- ****パラメータ更新 (Parameter Update)**** アクション
- ****トレジャリー引き出し (Treasury Withdrawal)**** アクション

スクリプトは、これらのいずれかのタイプのガバナンス アクションがオンチェーンで送信されたときに実行されます。これにより、たとえば、誤ったスクリプトによってチェーンがハード フォーク アクションを実行できなくなり、デッドロックが発生するといったシナリオを回避できます。スクリプトの使用には、3 つの異なる状況が当てはまります。

****シンボルと説明 (Symbol and Explanation)****

- (y) スクリプトを使用してガードレールを強制することができます。

- (x) スクリプトを使用してガードレールを強制することはできません。
- (~ - reason) 指定された理由により、スクリプトを使用してガードレールを強制することはできませんが、将来のledgerの変更によりこれが可能になる可能性があります。

ガードレールは重複する場合があります。この場合、最も制限の厳しいガードレール セットが適用されます。

このドキュメントにパラメータが明示的に記載されていない場合、スクリプトはパラメータの変更を許可してはなりません。

逆に、このドキュメントにパラメータが明示的にリストされているが、チェック可能なガードレールが指定されていない場合、スクリプトはパラメータの変更に制約を課してはなりません。

2. プロトコルパラメータ更新アクションに関するガードレールとガイドライン

以下は、プロトコル パラメータ更新ガバナンス アクションを介して更新可能なプロトコル パラメータ設定を変更するためのガードレールとガイドラインです。これにより、Cardano ブロックチェーンが変更の結果として回復不能な状態になることがなくなります。

曖昧さを避けるために、この付録では、他の規則ではなく、プロトコル パラメータ更新ガバナンス アクションで使用されるパラメータ名を使用していることに注意してください。

ガードレール

PARAM-01 (y) この文書で明示的に指定されていないプロトコルパラメータは、パラメータ更新ガバナンスアクションによって変更されてはなりません。

PARAM-02 (y) このドキュメントにプロトコルパラメータが明示的に記載されているが、チェック可能なガードレールが指定されていない場合、ガードレールスクリプトはパラメータの変更に制約を課してはなりません。チェック可能なガードレールは (y) で示されます。

2.1. 重要なプロトコルパラメータ

以下のプロトコル パラメータはセキュリティの観点から重要です。

ブロックチェーンの運用に重要なパラメータ

- *最大ブロック本体サイズ* (*maxBlockBodySize*)
- *最大トランザクション サイズ* (*maxTxSize*)
- *最大ブロック ヘッダー サイズ* (*maxBlockHeaderSize*)
- *シリアル化された資産値の最大サイズ* (*maxValueSize*)
- *単一ブロック内のスクリプト実行/メモリ単位の最大数* (*maxBlockExecutionUnits[steps/memory]*)
- *最小手数料係数* (*txFeePerByte*)
- *最低手数料定数* (*txFeeFixed*)
- *参照スクリプトの1バイトあたりの最低料金* (*minFeeRefScriptCoinsPerByte*) - *minimum Lovelace deposit per byte of serialized UTxO* (*utxoCostPerByte*)
- *ガバナンスアクションデポジット* (*govDeposit*)

ガードレール

PARAM-03 (y) 重要なプロトコル パラメータには、DRep 投票に加えて SPO 投票が必要です。SPOは、アクティブな全ブロック生産ステーク数の50%以上の総支持で「yes」と言わなければなりません。これは、ステーク プールの投票しきい値のガードレールによって強制されます。

PARAM-04 (x) 重要なプロトコルパラメータを変更するオフチェーン提案の公開から、対応するオンチェーンガバナンスアクションの提出まで、通常は少なくとも3 か月は経過するべきです。このガードレールは、慎重な技術的議論と評価の後に、重大度 1 または重大度 2 のネットワーク問題が発生した場合に緩和される可能性があります。

ガバナンスシステムにとって重要なパラメータ

- *委任キー Lovelace デポジット* (*stakeAddressDeposit*)
- *プール登録 Lovelace デポジット* (*stakePoolDeposit*)
- *プールの最小固定報酬カット* (*minPoolCost*)
- *DRepデポジット金額* (*dRepDeposit*)
- *憲法委員会の最小規模* (*committeeMinSize*)
- *憲法委員会メンバーの最大任期(エポック単位)* (*committeeMaxTermLength*)

ガードレール

PARAM-05 (y) DRepは、全アクティブ投票権者の50%以上の支持を得て「yes」に投票しなければなりません。これは、DRep 投票しきい値のガードレールによって強制されます。

PARAM-06 (x) ガバナンス システムにとって重要なパラメータを変更するオフチェーン提案の公開から、対応するオンチェーン ガバナンス アクションの提出までには、通常、少なくとも 3 か月は経過するべきです。このガードレールは、慎重な技術的議論と評価の後に、重大度 1 または重大度 2 のネットワーク問題が発生した場合に緩和されることがあります。

2.2. 経済パラメータ

経済パラメータを管理する際の全体的な目標は次のとおりです。

1. Cardano ブロックチェーン エコシステムの長期的な経済的持続可能性を実現します。
2. ステークプールがCardanoブロックチェーンの維持に対して適切な報酬を受けられるようにします。
3. ブロック生成のためにADAを委任する場合を含め、建設的な方法でステークを使用することで ADA保有者が適切に報酬を得られるよう保証する。
4. ステークプールオペレーター、ADA保有者、DeFiユーザー、インフラストラクチャユーザー、開発者(DAppsなど)、金融仲介者(取引所など)など、Cardanoブロックチェーンエコシステムのさまざまな利害関係者に対する経済的インセンティブのバランスをとります。

変化のきっかけ

1. ADAの法定価値の大幅な変化により、セキュリティ、パフォーマンス、機能性、長期的な持続可能性に問題が生じる可能性がある
2. 取引量や取引形態の変化
3. コミュニティからのリクエストや提案
4. 経済パラメータの変更を必要とする緊急事態

対策指標

経済指標の変更は単独で行うべきではありません。以下の点を考慮する必要があります。

- 外部経済要因
- ネットワークセキュリティに関する懸念

コア指標

- ADAのフィアット価値により、セキュリティ、パフォーマンス、機能性、長期的な持続可能性に潜在的な問題が生じる
- 取引量と種類
- ステークプールの数と健全性
- 外部経済要因

特定の経済パラメータの変更

バイトあたりのトランザクション手数料 (txFeePerByte) と固定トランザクション手数料 (txFeeFixed)

Lovelace での基本トランザクションのコストを定義します。

$$*fee(tx) = txFeeFixed + txFeePerByte \times nBytes(tx)*$$

ガードレール

TFPB-01 (y) *txFeePerByte* は 30 (0.000030 ada) 未満であつてはなりません
これにより、低コストのサービス拒否攻撃から保護されます

TFPB-02 (y) *txFeePerByte* は1,000 (0.001 ada) を超えてはなりません
これにより、取引の支払いが確実に行われるようになります

TFPB-03 (y) *txFeePerByte* は負であつてはなりません

TFF-01 (y) *txFeeFixed* は100,000 (0.1 ada) 未満であつてはなりません
これにより、低コストのサービス拒否攻撃から保護されます

TFF-02 (y) *txFeeFixed* は10,000,000 (10 ada) を超えてはなりません
これにより、取引の支払いが確実に行われるようになります

TFF-03 (y) *txFeeFixed* は負であつてはなりません

TFGEN-01 (x - "should") サービス拒否攻撃に対する一貫したレベルの保護を維持するために、Plutus 実行価格が調整されるたびに、*txFeeFixed* と *txFeeFixed* も調整されるべきです (executionUnitPrices[steps/memory])

TFGEN-02 (x - unquantifiable) *txFeeFixed* または *txFeeFixed* への変更は、サービス拒否攻撃のコスト削減の影響、またはトランザクションの構築が不可能になるような最大トランザクション手数料の増加を考慮しなければなりません

バイトあたりの UTxO コスト (*utxoCostPerByte*)

UTxO に保持されるストレージのバイトごとに課金されるデポジット (Lovelace 単位) を定義します。このデポジットは、UTxO がアクティブでなくなったときに返還されます。

- 単一のUTxO内に保持されるADAの最小しきい値を設定します
- UTxO ストレージに対する低コストのサービス拒否攻撃に対する保護を提供します。DoS 保護は、空きノード メモリに応じて低下します (UTxO の増加に比例)
- 不要になった UTxO を返却したり、UTxO をマージしたりするインセンティブを提供することで、ノード ユーザーの長期保存コストを削減します

ガードレール

UCPB-01 (y) **utxoCostPerByte** は 3,000 (0.003 ada) 未満であつてはなりません

UCPB-02 (y) **utxoCostPerByte** は 6,500 (0.0065 ada) を超えてはなりません

UCPB-03 (y) **utxoCostPerByte** はゼロであつてはなりません

UCPB-04 (y) **utxoCostPerByte** は負であつてはなりません

UCPB-05a (x - "should") 変更は以下を考慮すべきです

- i) 攻撃の許容コスト
- ii) 攻撃の許容時間
- iii) フルノードユーザーにとって許容可能なメモリ構成
- iv) UTxOのサイズ
- v) 現在のノードメモリ使用量の合計

ステークアドレスデポジット (*stakeAddressDeposit*)

不要になったステークアドレスを確実に廃棄します

- 長期保管コストの削減に役立ちます
- ledgerのCPUとメモリのコストを制限するのに役立ちます

デポジットの根拠は、希少なメモリリソースが不要になったときに返却されるように促すことです。アクティブなステーク アドレスの数を減らすと、ステーク スナップショットを計算する際のエポック境界での処理とメモリのコストも削減されます。

ガードレール

SAD-01 (y) **stakeAddressDeposit** は 1,000,000 (1 ada) 未満であつてはなりません

SAD-02 (y) **stakeAddressDeposit** は 5,000,000 (5 ada) を超えてはなりません

SAD-03 (y) **stakeAddressDeposit** は負であつてはなりません

ステークプールデポジット (*stakePoolDeposit*)

ステークプールが不要になったときにステークプールオペレーターによって廃止されることを保証します

- 長期保管コストの削減に役立ちます

デポジットの根拠は、希少なメモリ リソースが不要になったときに返却されるようにインセンティブを与えることです。報酬とステーク スナップショットの計算は、アクティブなステークプールの数によっても影響を受けます。

ガードレール

SPD-01 (y) *stakePoolDeposit* は250,000,000 (250 ada) 未満であつてはなりません

SPD-02 (y) *stakePoolDeposit* は500,000,000 (500 ada) を超えてはなりません

SPD-03 (y) *stakePoolDeposit* は負であつてはなりません

最小プールコスト (*minPoolCost*)

報酬メカニズムの一部

- 委任者報酬が支払われる前に、プールの最小コストがプール報酬アドレスに転送されます

ガードレール

MPC-01 (y) *minPoolCost* は負であつてはなりません

MPC-02 (y) *minPoolCost* は500,000,000 (500 ada) を超えてはなりません

MPC-03 (x - "should") *minPoolCost* は、プールを運営するための経済的コストに合わせて設定すべきです

トレジャリーカット (*treasuryCut*)

報酬メカニズムの一部

- 金融緩和によるトレジャリーカットは、プール報酬が支払われる前にトレジャリーに移される。
- 0.0～1.0 (0%～100%) の範囲で設定できます

ガードレール

TC-01 (y) *treasuryCut* は0.1 (10%) 未満であつてはなりません

TC-02 (y) *treasuryCut* は0.3 (30%) を超えてはなりません

TC-03 (y) *treasuryCut* は負であつてはなりません

TC-04 (y) *treasuryCut* は1.0 (100%) を超えてはなりません

TC-05 (~ - no access to change history) *treasuryCut* は、36 エポック期間 (約 6 か月) 内に 2 回以上変更してはなりません

通貨拡張率 (*monetaryExpansion*)

報酬メカニズムの一部

- 通貨拡張は、各エポックの報酬に使用されるリザーブの量を制御します

Cardanoの長期的な持続可能性を左右する

- リザーブは徐々に枯渇し、報酬は供給されなくなります

ガードレール

ME-01 (y) *monetaryExpansion* は 0.005 を超えてはなりません

ME-02 (y) *monetaryExpansion* は 0.001 未満であってはなりません

ME-03 (y) *monetaryExpansion* は 負であってはなりません

ME-04 (x - "should") *monetaryExpansion* は、73エポック期間 (約12か月) で +/- 10% 以上変化されるべきではありません

ME-05 (x - "should") *monetaryExpansion* は、36エポック期間 (約6か月) 内に複数回変更されるべきではありません

Plutus スクリプト実行価格 (*executionUnitPrices[priceSteps/priceMemory]*)

Plutusスクリプトの実行料金を定義する

Plutusスクリプトの実行に対して経済的な利益をもたらす

低コストのDoS攻撃に対するセキュリティを提供

ガードレール

EIUP-PS-01 (y) *executionUnitPrices[priceSteps]* は 2,000 / 10,000,000 を超えてはなりません

EIUP-PS-02 (y) *executionUnitPrices[priceSteps]* は 500 / 10,000,000未満であってはなりません

EIUP-PM-01 (y) *executionUnitPrices[priceMemory]* は 2,000 / 10,000 を超えてはなりません

EIUP-PM-02 (y) *executionUnitPrices[priceMemory]* は 400 / 10,000未満であってはなりません

EIUP-GEN-01 (x - "similar to") 実行価格は次のように設定しなければなりません

- i) 最大CPUステップでトランザクションを実行するコストは、最大サイズの非スクリプトトランザクションのコストと同程度であり、
- ii) 最大メモリユニットでトランザクションを実行するコストは、最大サイズの非スクリプトトランザクションのコストと同程度である。

EIUP-GEN-02 (x - "should") トランザクション手数料が調整されるたびに、実行価格も調整される必要があります (*txFeeFixed/txFeePerByte*)。目標は、トランザクションの種類に関係なく、処理の遅延が「完全な」トランザクションと同様になるようにすることです。

- これにより、ブロックの拡散/伝播時間に関する要件が満たされることが保証されます。

Lovelace で Plutus 参照スクリプトを使用するコストを定義します

ガードレール

MFRS-01 (y) **minFeeRefScriptCoinsPerByte** は 1,000 (0.001 ada) を超えてはなりません
- これにより、トランザクションの支払いが確実に行われます

MFRS-02 (y) **minFeeRefScriptCoinsPerByte** は負であってはなりません

MFRS-03 (x - "should") サービス拒否攻撃に対する一貫したレベルの保護を維持するために、Plutus 実行価格が調整されるたびに (**executionUnitPrices[steps/memory]**)、および **txFeeFixed** が調整されるたびに、**minFeeRefScriptCoinsPerByte** が調整されるべきです

MFRS-04 (x - unquantifiable) **minFeeRefScriptCoinsPerByte** への変更は、サービス拒否攻撃のコスト削減や最大取引手数料の増加の影響を考慮しなければなりません

2.3. ネットワークパラメータ

Cardano ブロックチェーン ネットワーク パラメータを管理する際の全体的な目標は次のとおりです。

1. 利用可能なCardanoブロックチェーンレイヤー1ネットワーク容量を、支払い取引、レイヤー1 DApp、サイドチェーン管理、ガバナンスのニーズなど、現在または将来のトラフィック需要に合わせる
2. 支払い取引、代替可能/非代替可能トークンの発行者、Plutusスクリプト、DeFi開発者、ステークプールオペレーター、投票取引など、さまざまなユーザーグループのトラフィック需要のバランスをとる

変化のきっかけ

ネットワーク パラメータの変更は、次の原因によって発生する可能性があります。

1. 2エポック期間(10日間)にわたる交通需要の測定された変化
2. 予想される交通需要の変化
3. コミュニティからのリクエスト

対策指標

以下の場合には、変更を元に戻す必要がある場合や、変更を実施しない必要がある場合があります。

- ブロック伝播の遅延が大きすぎる
- ステークプールがトラフィック量を処理できない
- スクリプトが実行を完了できない

コア指標

パラメータ変更に関するすべての決定は、以下の情報に基づいて行う必要があります。

- ブロック伝播遅延プロファイル
- トラフィック量(時間の経過に伴うブロックサイズ)

- スクリプトボリューム(スクリプトと実行ユニットのサイズ)
- スクリプト実行コストのベンチマーク
- ブロック伝播遅延/拡散ベンチマーク

変更がメインネットのパフォーマンスや動作に与える影響を施行前に確認するには、詳細なベンチマーク結果が必要です。通常のトランザクション、Plutus スクリプト、ガバナンスアクションなど、さまざまなトランザクションの組み合わせの影響を分析する必要があります。

ガードレール

NETWORK-01 (x - "should") 個々のネットワークパラメータは、2エポックごとに1回以上変更されるべきではありません

NETWORK-02 (x - "should") 直接関連しない限り、エポックごとに 1 つのネットワークパラメータのみを変更すべきです (例: トランザクションごと、ブロックごとのメモリ ユニット制限)。

特定のネットワークパラメータの変更

ブロック サイズ (*maxBlockBodySize*)

ブロックの最大サイズ(バイト単位)

ガードレール

MBBS-01 (y) *maxBlockBodySize* は122,880バイト (120KB) を超えてはなりません

MBBS-02 (y) *maxBlockBodySize* は24,576 バイト (24KB) 未満であってはなりません

MBBS-03a (x - "exceptional circumstances") *maxBlockBodySize* は、セキュリティ、パフォーマンス、機能性、または長期的な持続可能性に潜在的な問題がある例外的な状況を除き、減少してはなりません

MBBS-04 (~ - no access to existing parameter values) *maxBlockBodySize* は、少なくとも 1 つのトランザクションを含めるのに十分な大きさでなければなりません (つまり、*maxBlockBodySize* は少なくとも *maxTxSize* でなければなりません)

MBBS-05 (x - "should") *maxBlockBodySize* は、1エポック(5日)あたり最大10,240バイト (10KB)、好ましくは8,192バイト(8KB)以下で変更されるべきです

MBBS-06 (x - "should") ブロック サイズは、追加の伝送制御プロトコル (TCP) ラウンドトリップを引き起こすべきではありません。これを超える増加は、パフォーマンス分析、シミュレーション、ベンチマークによって裏付けられなければなりません。

MBBS-07 (x - "unquantifiable") *maxBlockBodySize* への変更の影響は、詳細なベンチマーク/シミュレーションによって確認され、以下で説明するブロック拡散/伝播時間予算の要件を超えてはなりません。*maxBlockBodySize* を増やす場合は、Plutus スクリプトの実行に関する将来の要件も考慮しなければなりません。

(*maxBlockExecutionUnits[steps]*) ブロック拡散目標は合計 3 秒で、ブロック伝播の 95% は 5 秒以内です。最大ブロックサイズの制限は、ベンチマークと監視結果によってサポートされる場合、将来的に増加する可能性があります。

トランザクション サイズ (*maxTxSize*)

トランザクションの最大サイズ(バイト単位)。

ガードレール

MTS-01 (y) *maxTxSize* は 32,768 バイト (32KB) を超えてはなりません

MTS-02 (y) *maxTxSize* は負であってはなりません

MTS-03 (~ - no access to existing parameter values) *maxTxSize* は減少してはなりません

MTS-04 (~ - no access to existing parameter values) *maxTxSize* は
**maxBlockBodySize* を超えてはなりません

MTS-05 (x - "should") *maxTxSize* は、どのエポックでも 2,560 バイト (2.5KB) 以上増やすべきではなく、エポックごとに 2,048 バイト (2KB) 以下で増加させるべきです。

MTS-06 (x - "should") *maxTxSize* はブロックサイズの 1/4 を超えてはなりません

メモリユニットの制限 (*maxBlockExecutionUnits[memory]*、*maxTxExecutionUnits[memory]*)

Plutus スクリプトでトランザクションごとまたはブロックごとに使用できるメモリ ユニットの最大数の制限。

ガードレール

MTEU-M-01 (y) *maxTxExecutionUnits[memory]* は 40,000,000 ユニットを超えてはなりません

MTEU-M-02 (y) *maxTxExecutionUnits[memory]* は負であってはなりません

MTEU-M-03 (~ - no access to existing parameter values) *maxTxExecutionUnits[memory]* は減少してはなりません

MTEU-M-04 (x - "should") *maxTxExecutionUnits[memory]* は、どのエポックでも 2,500,000 ユニットを超えて増加してはなりません

MBEU-M-01 (y) *maxBlockExecutionUnits[memory]* は 120,000,000 ユニットを超えてはなりません

MBEU-M-02 (y) *maxBlockExecutionUnits[memory]* は負であってはなりません

MBEU-M-03 (x - "should") *maxBlockExecutionUnits[memory]* は、どのエポックでも 10,000,000 単位を超えて変更 (増加または減少) すべきではありません

MBEU-M-04a (x - unquantifiable) *maxBlockExecutionUnits[memory]* へのいかなる変更の影響も、詳細なベンチマーク/シミュレーションによって確認され、*maxBlockExecutionUnits[steps]* および *maxBlockBodySize* にも影響されるように、ブロック拡散/伝播時間バジェットの要件を超えないようにしなければなりません。どのような増加も、5秒以内に95%のブロック伝搬を伴う3秒のブロック拡散目標に対して測定された、総ブロックサイズ(*maxBlockBodySize*)に対する、以前に合意された将来の要件も考慮しなければなりません。将来的にPlutusのパフォーマンスが向上すると、ブロックごとのメモリ制限が増加する可能性があります、前の文で指定した全体的な拡散制限と将来の要件とのバランスを取らなければなりません。

MEU-M-01 (~ - no access to existing parameter values) *maxBlockExecutionUnits[memory]* は、*maxTxExecutionUnits[memory]* より小さくてはなりません

CPU ユニット制限 (maxBlockExecutionUnits[steps]、maxTxExecutionUnits[steps])

トランザクションごとまたはブロックごとに、Plutus スクリプトで利用できる CPU ステップの最大数の制限。

ガードレール

MTEU-S-01 (y) *maxTxExecutionUnits[steps]* は 15,000,000,000 (15Bn) 単位を超えてはなりません

MTEU-S-02 (y) *maxTxExecutionUnits[steps]* は負であつてはなりません

MTEU-S-03 (~ - no access to existing parameter values) *maxTxExecutionUnits[steps]* は減少してはなりません

MTEU-S-04 (x - "should") *maxTxExecutionUnits[steps]* は、どのエポック (5 日間) でも 500,000,000 (500M) 単位を超えて増加してはなりません

MBEU-S-01 (y) *maxBlockExecutionUnits[steps]* は40,000,000,000 (40Bn) 単位を超えてはなりません

MBEU-S-02 (y) *maxBlockExecutionUnits[steps]* は負であつてはなりません

MBEU-S-03 (x - "should") *maxBlockExecutionUnits[steps]* は、どのエポック (5 日間) でも 2,000,000,000 (2Bn) 単位を超えて変更 (増加または減少) すべきではありません

MBEU-S-04a (x - unquantifiable) *maxBlockExecutionUnits[steps]* への変更の影響は、詳細なベンチマーク/シミュレーションによって確認する必要がある、*maxBlockExecutionUnits[memory]* および *maxBlockBodySize* によっても影響を受けるブロック拡散/伝播時間予算の要件を超えてはなりません。どのような増加も、5秒以内に95%のブロック伝搬で3秒の総ブロック拡散目標に対して測定された総ブロックサイズ(*maxBlockBodySize*)の以前に特定された将来の要件も考慮しなければなりません。将来のPlutusのパフォーマンス改善により、ブロックごとのステップ制限を増やすことができるようになるかもしれませんが、前の文で指定された全体的な拡散制限と将来の要件とのバランスをとらなければなりません。

MEU-S-01 (~ - no access to existing parameter values) *maxBlockExecutionUnits[steps]* は、*maxTxExecutionUnits[steps]* より小さくてはなりません

ブロック ヘッダー サイズ (maxBlockHeaderSize)

ブロック ヘッダーのサイズ。

ガードレール

MBHS-01 (y) *maxBlockHeaderSize* は5,000バイトを超えてはなりません

MBHS-02 (y) *maxBlockHeaderSize* は負であつてはなりません

MBHS-03 (x - "largest valid header" is subject to change) *maxBlockHeaderSize* は、最大の有効なヘッダーに対して十分な大きさになければなりません

MBHS-04 (x - "should") *maxBlockHeaderSize* は、通常、プロトコルが変更された場合にのみ増加されるべきです

MBHS-05 (x - "should") *maxBlockHeaderSize* は TCP の初期輻輳ウィンドウ (3 または 10 MTU) 内であるべきです

2.4. 技術/セキュリティパラメータ

技術/セキュリティパラメータを管理する際の全体的な目標は次のとおりです。

1. 分散化、シビル攻撃および51%攻撃からの保護、サービス拒否攻撃からの保護の観点からカルダノネットワークのセキュリティを確保する
2. Plutus言語の変更を有効にする

変化のきっかけ

1. アクティブSPO数の推移
2. Plutus言語の変更
3. セキュリティ上の脅威
4. コミュニティからのリクエスト

対策指標

- 経済的な懸念、例えばステークプールの数を変更する場合

コア指標

- ステークプールの数
- 分散化のレベル

特定の技術/セキュリティパラメータの変更

ステークプールのターゲット数 (*stakePoolTargetNum*)

ステークプールの目標数を設定する

- ネットワークが平衡状態にあるときのプールの期待数
- 主にセキュリティパラメータであり、プールの分割/複製による分散化を保証します
- 安全保障への影響だけでなく経済への影響もある - このパラメータを変更する際には経済的なアドバイスも必要です
- このパラメータに大きな変更があると、大量の再委任イベントが発生します

ガードレール

SPTN-01 (y) *stakePoolTargetNum* は250未満であってはなりません

SPTN-02 (y) *stakePoolTargetNum* は2,000を超えてはなりません

SPTN-03 (y) *stakePoolTargetNum* は負であってはなりません

SPTN-04 (y) *stakePoolTargetNum* はゼロであつてはなりません

誓約影響係数 (poolPledgeInfluence)

質権保護メカニズムを有効にする

シビル攻撃に対する保護を提供します

- より高い値は、より多くの誓約をしたプールに報酬を与え、より少ない誓約をしたプールにペナルティを与えます

技術的効果だけでなく経済的効果もあるため、経済的アドバイスも必要

ガードレール

PPI-01 (y) *poolPledgeInfluence* は 0.1 未満であつてはなりません

PPI-02 (y) *poolPledgeInfluence* は 1.0 を超えてはなりません

PPI-03 (y) *poolPledgeInfluence* は負であつてはなりません

PPI-04 (x - "should") *poolPledgeInfluence* は、18エポック期間 (約3か月) で +/- 10% 以上変動すべきではありません

プールのリタイア期間 (poolRetireMaxEpoch)

プールがリタイアを計画する際に通知できるエポックの最大数を定義します。

ガードレール

PRME-01 (y) *poolRetireMaxEpoch* は負であつてはなりません

PRME-02 (x - "should") *poolRetireMaxEpoch* は 1 未満であつてはなりません

担保率 (collateralPercentage)

Plutus スクリプトを実行するときに、通常の実行コストのパーセンテージとして提供する必要がある担保の量を定義します。

- 手数料の支払いに加えて担保も必要となる
- スクリプトの実行に失敗した場合、担保は失われます
- スクリプトが正常に実行された場合、担保が失われることはありません

失敗したスクリプトの実行コストを下げるのではなく、高くすることで、低コストの攻撃に対するセキュリティを提供します。

ガードレール

CP-01 (y) *collateralPercentage* は100未満であつてはなりません

CP-02 (y) *担保率* は200を超えてはなりません

CP-03 (y) *collateralPercentage* は負であってはなりません

CP-04 (y) *collateralPercentage* はゼロであってはなりません

担保入力 of 最大数 (*maxCollateralInputs*)

Plutus スクリプトを実行するときに担保に使用できる入力の最大数を定義します。

ガードレール

MCI-01 (y) *maxCollateralInputs* は 1 未満であってはなりません

最大値サイズ (*maxValueSize*)

各出力における値のシリアル化されたサイズの制限。

ガードレール

MVS-01 (y) *maxValueSize* は12,288 バイト (12KB) を超えてはなりません

MVS-02 (y) *maxValueSize* は負であってはなりません

MVS-03 (~ - no access to existing parameter values) *maxValueSize* は *maxTxSize* より小さくなくてはなりません

MVS-04 (~ - no access to existing parameter values) *maxValueSize* は減少してはなりません

MVS-05 (x - "sensible output" is subject to interpretation) *maxValueSize* は、適切な出力 (既存のオンチェーン出力や新しい ledger ルールによって生成される可能性のある予測出力など) を許可するのに十分な大きさになくてはなりません

Plutus コスト モデル (*costModels*)

CPUとメモリユニットの観点から各Plutusプリミティブの基本コストを定義します

Plutus のバージョンごとに異なるコスト モデルが必要です。各コスト モデルは、多くの異なるコスト モデル値で構成されます。コスト モデルは、Plutus 言語バージョンごとに定義されます。新しい言語バージョンでは、追加のコスト モデル値が導入されたり、既存のコスト モデル値が削除されたりすることがあります。

ガードレール

PCM-01 (x - unquantifiable) *Cost model* の値は、リファレンスアーキテクチャのベンチマークによって設定されなくてはなりません

PCM-02 (x - primitives and language versions aren't introduced in transactions) 新しいプリミティブが導入された場合、または新しい Plutus 言語バージョンが追加された場合は、*Cost model* を更新しなくてはなりません

PCM-03a (~ - no access to *Plutus cost model* parameters) *Cost model* の値は、通常、負の値になるべ

きではありません。負の値は、関連するプリミティブの基礎となるコスト モデルに対して正当化される必要があります。

PCM-04 (~ - no access to *Plutus cost model* parameters) プロトコルがサポートする各Plutus言語バージョンには、*Cost model*が提供されなければなりません

2.5. ガバナンスパラメータ

ガバナンス パラメータを管理する際の全体的な目標は次のとおりです。

1. ガバナンスの安定性を確保する
2. 代表制によるガバナンス形態を維持する

変化のきっかけ

ガバナンス パラメータの変更は、次の原因によって発生する可能性があります。

1. コミュニティのリクエスト
2. 規制要件
3. 予期しない、または望ましくないガバナンスの結果
4. 自信が持てない状態になる

対策指標

以下の場合には、変更を元に戻す必要がある場合や、変更を実施しない必要がある場合があります。

- ガバナンスへの予期せぬ影響
- オンチェーン投票やガバナンスアクションの過剰によるレイヤー1の過負荷

コア指標

パラメータ変更に関するすべての決定は、以下の情報に基づいて行う必要があります。

- ガバナンス参加レベル
- ガバナンスの行動とパターン
- 規制上の考慮事項
- ガバナンスシステムへの信頼
- 必要な変更を管理するガバナンスシステムの有効性

特定のガバナンスパラメータの変更

ガバナンスアクションのためのデポジット (govDeposit)

ガバナンスアクションを送信するときに請求されるデポジット。

- 送信されるアクションの数を制限するのに役立ちます

ガードレール

GD-01 (y) *govDeposit* は負であってはなりません

GD-02 (y) *govDeposit* は1,000,000 (1 ada) 未満であってはなりません

GD-03 (y) *govDeposit* は10,000,000,000,000 (1000万ADA) を超えてはなりません

GD-04 (x - "should") *govDeposit* はフィアット通貨の変更に合わせて調整されるべきです

DReps のデポジット (dRepDeposit)

DRep を登録する際に請求されるデポジット。

- アクティブなDRepの数を制限するのに役立ちます

ガードレール

DRD-01 (y) *dRepDeposit* は負であってはなりません

DRD-02 (y) *dRepDeposit* は1,000,000 (1 ada) 未満であってはなりません

DRD-03 (y) *dRepDeposit* は100,000,000,000 (100,000 ada) を超えてはなりません

DRD-04 (x - "should") *dRepDeposit* はフィアット通貨の変更に合わせて調整されるべきです

DRep アクティビティ期間 (dRepActivity)

DRep がどの提案にも投票しない場合、投票計算の目的で非アクティブであると見なされる期間 (エポックの整数として)。

ガードレール

DRA-01 (y) *dRepActivity* は 13 エポック (2 か月) 未満であってはなりません

DRA-02 (y) *dRepActivity* は 37エポック (6か月) を超えてはなりません

DRA-03 (y) *dRepActivity* は負であってはなりません

DRA-04 (~ - no access to existing parameter values) *dRepActivity* は *govActionLifetime* より大きくなければなりません

DRA-05 (x - "should") *dRepActivity* は、人間の期間 (2 か月など) で計算されるべきです

DRep および SPO ガバナンス アクションしきい値 (dRepVotingThresholds[...], poolVotingThresholds[...])

DRep または SPO のいずれかによる特定の種類のガバナンス アクションを承認するために必要なアクティブな投票ステークのしきい値。

- 行動の正当性を保証する

しきい値パラメータは以下のとおりです。

dRepVotingThresholds:

- *dvtCommitteeNoConfidence*
- *dvtCommitteeNormal*
- *dvtHardForkInitiation*
- *dvtMotionNoConfidence*
- *dvtPPEconomicGroup*
- *dvtPPGovGroup*

- *dvtPPNetworkGroup*
- *dvtPPTechnicalGroup*
- *dvtTreasuryWithdrawal*
- *dvtUpdateToConstitution*

poolVotingThresholds:

- *pvtCommitteeNoConfidence*
- *pvtCommitteeNormal*
- *pvtHardForkInitiation*
- *pvtMotionNoConfidence*
- *pvtPPSecurityGroup*

ガードレール

VT-GEN-01 (y) すべてのしきい値は50%より大きく、100%以下でなければなりません

VT-GEN-02 (y) 経済、ネットワーク、技術パラメータのしきい値は51%～75%の範囲でなければなりません

VT-GEN-03 (y) ガバナンスパラメータのしきい値は 75% ～ 90% の範囲でなければなりません

VT-HF-01 (y) **Hard fork**アクションのしきい値は 51% ～ 80% の範囲でなければなりません

VT-CON-01 (y) **New Constitution or guardrails script action**のしきい値は65%-90%の範囲でなければなりません

VT-CC-01 (y) **Update Constitutional Committee action**のしきい値は51%-90%の範囲でなければなりません

VT-NC-01 (y) **No confidence**アクションのしきい値は 51% ～ 75% の範囲でなければなりません

ガバナンスアクションライフタイム (govActionLifetime)

ガバナンスアクションが実行されなかった場合に期限が切れる期間 - エポックの全体数として

ガードレール

GAL-01 (y) *govActionLifetime* は 1 エポック (5 日) 未満であってはなりません

GAL-03 (x - "should") *govActionLifetime* は 2 エポック (10 日) 未満であってはなりません

GAL-02 (y) *govActionLifetime* は 15 エポック (75 日) を超えてはなりません

GAL-04 (x - "should") *govActionLifetime* は、投票などを行うのに十分な時間を確保するために、人間の時間 (例:30日、2週間) に合わせて調整すべきです

GAL-05 (~ - no access to existing parameter values) *govActionLifetime* は *dRepActivity* より小さくなければなりません

憲法委員会の最大任期 (committeeMaxTermLength)

委員の任期の上限

ガードレール

CMTL-01a (y) *committeeMaxTermLength* はゼロであってはなりません

CMTL-02a (y) *committeeMaxTermLength* は負であってはなりません

CMTL-03a (y) *committeeMaxTermLength* は 18 エポック (90 日、または約 3 か月) 未満であってはなりません

CMTL-04a (y) *committeeMaxTermLength* は 293エポック(約4年)を超えてはなりません

CMTL-05a (x - "should") *committeeMaxTermLength* は 220 エポック (約 3 年) を超えてはなりません

憲法委員会の最小規模 (committeeMinSize)

憲法委員会を変更するガバナンス アクションの後に憲法委員会に含めることができるメンバーの最小数。

ガードレール

CMS-01 (y) *committeeMinSize* は負であってはなりません

CMS-02 (y) *committeeMinSize* は 3 未満であってはなりません

CMS-03 (y) *committeeMinSize* は 10を超えてはなりません

2.6. パラメータ変更の監視と元に戻す

すべてのネットワークパラメータの変更は、少なくとも2エポック(10日間)は注意深く監視する必要があります

- ブロックの伝搬遅延が6時間のローリングウィンドウでブロックの5%以上で4.5秒を超えた場合、変更はできるだけ早く元に戻さなければなりません

その他のパラメータの変更はすべて監視する必要があります

- パフォーマンス、セキュリティ、機能性、または長期的な持続可能性への全体的な影響が許容できない場合は、復元計画を実装するべきです

各パラメーターの変更について、具体的な復帰/回復計画を作成しなければなりません。この計画には以下が含まれなければなりません。

- 以前の状態(または類似の状態)に戻るには、どのパラメータをどのように変更する必要があるか
- 壊滅的な障害が発生した場合にネットワークを回復する方法

パラメータ変更後に問題が発生した場合、この計画に従うべきです。

すべての変更を元に戻せるわけではないことに注意してください。これらのパラメータを変更する場合は、さらに注意する必要があります。

2.7. 更新不可能なプロトコルパラメータ

一部の基本的なプロトコル パラメータは、プロトコル パラメータ更新ガバナンス アクションでは変更できません。これらのパラメータは、ハードフォークの一部として新しい Genesis ファイルでのみ変更できます。これらのパラメータの更新に関して、特定のガードレールを提供する必要はありません。

3. トレジャリー引出措置に関するガードレールとガイドライン

****Treasury withdrawal**** アクションは、Cardano トレジャリーからの引き出し先と金額を指定します。

ガードレール

TREASURY-01a (x) 一定期間ごとのCardano トレジャリー残高の純変更限度額は、アクティブな投票ステークの50%を超えるしきい値でオンチェーンガバナンスアクションを介してDRepsによって合意されなければなりません

TREASURY-02 (x) Cardano トレジャリーの予算は、一定期間のCardano トレジャリー残高の純変動限度を超えてはなりません

TREASURY-03 (x) Cardano トレジャリーの予算はADA建てでなければなりません

TREASURY-04 (x) トレジャリーの引き出しは、DRepsが合意した以前のオンチェーンガバナンスアクションに従って、アクティブな投票ステークの50%を超えるしきい値でコミュニティが承認したCardano 予算が存在するまで、承認されてはなりません

4. ハードフォーク開始アクションに関するガードレールとガイドライン

****hard fork initiation**** アクションでは、新しいメジャー プロトコル バージョンと新しいマイナー プロトコル バージョンの両方を指定する必要があります。

- 正の整数として

ハードフォークの結果、新しい更新可能なプロトコル パラメータが導入される可能性があります。これらのパラメータに対してガードレールが定義され、ハードフォーク後に有効になります。既存の更新可能なプロトコル パラメータもハードフォークによって廃止される可能性があり、その場合、ガードレールは将来のすべての変更に対して無効になります。

ガードレール

HARDFORK-01 (~ - no access to existing parameter values) メジャープロトコルのバージョンは、この変更の直前に施行されるメジャーバージョンと同じか、1つ大きくなければなりません。メジャープロトコルのバージョンが1つ大きい場合、マイナープロトコルのバージョンは 0 でなければなりません。

HARDFORK-02a (~ - no access to existing parameter values) メジャー プロトコル バージョンも変更されない限り、マイナー プロトコル バージョンは、この変更の直前に施行されるマイナー バージョンよりも大きくなければなりません

HARDFORK-03 (~ - no access to existing parameter values) 少なくとも1つのプロトコルバージョン (メジャーまたはマイナー、あるいは両方) を変更しなければなりません

HARDFORK-04 (x) アクティブステークによるステークプールの少なくとも85%は、新しいプロトコルバージョンに関連付けられたルールを処理できるCardano ノードバージョンにアップグレードされているべきです

HARDFORK-05 (x) ハードフォークで導入される新しい更新可能なプロトコルパラメータは、この付録に必ず含まれ、それらのパラメータに対して適切なガードレールが定義されなければなりません

HARDFORK-06 (x) ハードフォークで導入される新しいプロトコルパラメータの設定は、適切なGenesis ファイルに含めなければなりません

HARDFORK-07 (x) 廃止されたプロトコルパラメータは、この付録に必ず記載しなければなりません

HARDFORK-08 (~ - no access to *Plutus cost model* parameters) 新しい Plutus バージョンは、新しい Plutus バージョンで利用可能な各プリミティブをカバーするバージョン固有の *Plutus cost model* によってサポートされていなければなりません

5. 憲法委員会またはしきい値アクションの更新に関するガードレールとガイドライン

****Update Constitutional Committee or Threshold**** ガバナンス アクションにより、憲法委員会の規模、構成、または必要な投票しきい値が変更される場合があります。

ガードレール

UPDATE-CC-01a (x) ****Update Constitutional Committee and/or threshold**** ****and/or term**** ガバナンスアクションは、ADA保有者がオンチェーンガバナンスアクションを通じてこの憲法を承認するまで承認してはならない

6. 新しい憲法またはガードレールスクリプトアクションに関するガードレールとガイドライン

新しい構成またはガードレール スクリプト アクションは、オンチェーン構成のハッシュと関連するガードレール スクリプトを変更します。

ガードレール

NEW-CONSTITUTION-01a (x) ハードフォークガバナンスアクションによって導入される新しいパラメータに必要なガードレールを定義するために、****New Constitution**** ****or Guardrails Script**** ガバナンスアクションが提出されなければなりません

NEW-CONSTITUTION-02 (x) 指定されている場合、新しいガードレールのスクリプトはこの憲法と一致していなければなりません

7. 不信任決議に関するガードレールとガイドライン

****No confidence**** アクションは、ガバナンス システムに対する不信任の状態を示します。****No Confidence**** アクションにはガードレールは課されません。

ガードレール

- なし

8. 情報行動に関するガードレールとガイドライン

****Info**** アクションはチェーン上で実行されません。****Info**** アクションにはガードレールはありません。

ガードレール

- なし

9. プロトコルパラメータグループのリスト

プロトコル パラメータはタイプ別にグループ化されており、グループごとに異なるしきい値を設定できます。

ネットワークグループは以下の要素で構成されています

- *最大ブロック本体サイズ* (*maxBlockBodySize*)
- *最大トランザクション サイズ* (*maxTxSize*)
- *最大ブロック ヘッダー サイズ* (*maxBlockHeaderSize*)
- *シリアル化された資産値の最大サイズ* (*maxValueSize*)
- *単一トランザクションにおけるスクリプト実行単位の最大数* (*maxTxExecutionUnits[steps]*)
- *単一ブロック内のスクリプト実行単位の最大数* (*maxBlockExecutionUnits[steps]*)
- *担保入力の最大数* (*maxCollateralInputs*)

経済グループは以下の要素で構成されています

- *最小手数料係数* (*txFeePerByte*)
- *最低手数料定数* (*txFeeFixed*)
- *参照スクリプトの1バイトあたりの最低料金* (*minFeeRefScriptCoinsPerByte*)
- *委任キー Lovelace デポジット* (*stakeAddressDeposit*)
- *プール登録 Lovelace デポジット* (*stakePoolDeposit*)
- *通貨拡張* (*monetaryExpansion*)
- *トレジャリー拡大* (*treasuryCut*)
- *プールの最小固定報酬カット* (*minPoolCost*)
- *シリアル化された UTxO のバイトあたりの最小 Lovelace デポジット* (*coinsPerUTxOByte*)
- *Plutus 実行ユニットの価格* (*executionUnitPrices[priceSteps/priceMemory]*)

技術グループは以下の要素で構成されています

- *プール誓約の影響力* (*poolPledgeInfluence*)
- *プールの引退最大エポック* (*poolRetireMaxEpoch*)
- *希望するプールの数* (*stakePoolTargetNum*)
- *Plutus 実行コスト モデル* (*costModels*)
- *スクリプトに必要な担保の割合* (*collateralPercentage*)

ガバナンスグループは以下の要素で構成されています

- *ガバナンス投票しきい値* (*dRepVotingThresholds[...], poolVotingThresholds[...]*)
- *ガバナンスアクションの最大存続期間(エポック単位)* (*govActionLifetime*)
- *ガバナンスアクションデポジット* (*govActionDeposit*)
- *DRepデポジット金額* (*dRepDeposit*)
- *DRep アクティビティ期間(エポック単位)* (*dRepActivity*)
- *憲法委員会の最小規模* (*committeeMinSize*)
- *憲法委員会メンバーの最長任期(エポック)* (*committeeMaxTermLength*)

