取扱暗号資産の概要説明書

	概要書更新年月日	2022年10月31日
【基礎情報】	日本語の名称	イーサリアム
	現地語の名称	Ethereum
	呼称（日本語の名称と同じ場合は一表記）	—
	ティッカーコード（シンボル）	ETH
	発行開始（年、月、日）	2015年7月30日
	時価総額（ドル基準、例：＄1.000.000）	$187,687,656,376
	時価総額（円基準、例：￥100.000.000）	¥27,965,460,800,000
	主な利用目的	送金、決済、スマートコントラクト
	利用制限の有無	なし
	海外流通の有無	あり
	国内流通の有無	あり
	店舗等の利用制限の有無	なし
	利用制限を行う者の属性	なし
	利用制限の内容	なし
	一般的な性格	分散型の価値保有・価値移転の台帳データ維持のための、暗号計算および価値記録を行う記録者への対価・代償として発行される暗号資産。 分散型アプリケーションが動作する実行環境の役割を果たす特徴を持つ。
	法的性格（資金決済法第2条第5項第１号、第2号の別　例：第1号）	第1号
	2号の場合：相互に交換可能な1号暗号資産の名称	—
	発行暗号資産に対する資産（支払準備資産）の有無および名称	なし
	発行者に対する保有者の支払請求権（買取請求権）	なし
	支払請求（買取請求）による受渡資産	—
	発行者が保有者に付与するその他の権利	なし
	発行者に対して保有者が負う義務	なし
	価値の決定	保有者間の自由売買による
	交換（売買）の制限	なし
	価値移転、保有情報を記録する電子情報処理組織の形態	パブリック型ブロックチェーン
	保有・移転記録台帳の公開、非公開の別	公開
	保有・移転記録の秘匿性	公開鍵暗号の暗号化処理を施しデータを記録
	利用者の真正性の確認	秘密鍵と公開鍵を用いた暗号化技術により、利用者本人が発信した移転データと特定し、記帳する。
	価値移転記録の信頼性確保の仕組み	Proof of Stake（PoS） PoSは、手元のPCからでも「ステーク」と呼ばれる一定額の暗号資産を引き出し不能なかたちでネットワークに投じることができる。ステークした人のなかから、通常はランダムなプロセスによって一部が選ばれ、選ばれた人は特定のブロックを検証して対価として報酬と手数料を暗号資産で受け取ることになる。
	誕生時に技術的なベースとなったコインの有無とその名称（アルトコインのみ）	なし
【取引単位・交換制限】	取引単位の呼称	finney=0.001ETH szabo=0.000001ETH wei=0.000000000000000001ETH
	保有・移転記録の最低単位	1wei (=0.000000000000000001 ETH)
	交換可能な通貨又は暗号資産	JPY、BTC
	交換制限	なし
	制限内容	—
	交換市場の有無	あり
【連動する資産の有無等】	価値が連動する資産等の有無	なし
	価値連動する資産等の名称	—
	価値連動する資産等の内容	—
	価値連動する資産との交換の可否	—
	価値連動する資産との交換比率	—
	価値連動する資産との交換条件	—
【付加価値】	その他の付加価値（サービス）の有無	あり
	付加価値（サービス）の内容	Ethereumネットワーク上でのスマートコントラクトの記録と実行
	過去3年間の付加価値（サービス）の提供状況	安定してサービスが続いている

【発行状況】	発行者	あり
	発行主体の名称	Ethereum Foundation
	発行主体の所在地	スイス連邦ツーク州
	発行主体の属性等	次世代の分散型アプリケーションの開発
	発行主体概要	不特定の保有・移転管理台帳記録者による発行プログラムの集団・共有管理
	発行暗号資産の信用力に関する説明	多数の記録者による多数決をもって移転記録が認証される仕組み。 ブロックチェーンによる保有・移転管理台帳による記録管理と重層化した暗号化技術による記録の保全能力 保有・移転管理台帳の公開 暗号化技術による保有者個人情報の秘匿性
	発行方法	初期発行と、分散型の価値保有・価値移転の台帳データ維持のための、暗号計算および価値記録を行う記録者への対価・代償としてプログラムにより自動発行
	発行可能数	未定
	発行可能数の変更可否	不可
	変更方法	―
	変更の制約条件	―
	発行済み数量	120,520,000ETH(2022年10月31日時点)
	今後の発行予定または発行条件	PoSにアップデートしたことで、ネットワークアップグレードEIP-1559で導入された焼却メカニズムのため、ブロックごとに発行される新しいETHの数は劇的に減少した。9月15日の「Merge」後、約4,000の新しいETHが発行された(2022年9月25日時点)。これはPoWであれば発行されていたと考えられるETH(約7万)より約95%も少ない数となっている。
	過去3年間の発行状況	2022年9月の「The Merge」実施に伴い 、これまで発生していたマイニング報酬(13,000ETH/日)が0(ゼロ)になり、1日のETH新規発行量はステーキング報酬(2022年9月時点、1,700ETH)のみとなった。
	過去3年間の発行理由	2014年7月-8月　クラウドセールによる発行 2015年7月30日以降 プログラムによる自動発行
	過去3年間の償却状況	なし
	過去3年間の償却理由	―
	発行者の行う発行業務に対する監査の有無	なし
	監査を実施する者の氏名又は名称	―
	直近時点で行われた監査年月日	―
	直近時点における監査結果	―
【価値移転記録台帳に係る技術】	ブロックチェーン技術の利用の有無	あり
	ブロックチェーンの形式	パブリック型
	ブロックチェーン技術を利用しない場合には、その名称	―
	利用するブロックチェーン技術以外の技術の内容	―
	価値移転認証の仕組み	台帳形式。価値移転認証を求める暗号データを記録者が解読し、利用者および移転内容の真正性を確認して価値移転記録台帳の記録を確定する。
	価値記録公開/非公開の別	公開
	保有者個人データの秘匿性の有無	あり
	秘匿化の方法	公開鍵と秘密鍵による暗号化
	価値移転ネットワークの信頼性に関する説明	オープンネットワークの脆弱性に対し、暗号により連鎖する台帳群(ブロックチェーン)および記録者による多数決をもって移転記録が認証される仕組みを用い、多数の記録者のネットワークへの参加を得ることによって、データ改竄の動機を排除し、信頼性を確保する。
【価値移転の記録者】	記録者の数	8,637ノード(2022年10月12日時点)
	記録者の分布状況	不特定
	記録者の主な属性	一定数のETHを所有する者であれば誰でも自由に記録者になることができる
	記録の修正方法	取引が一旦記録されると、取引は変更することができない。承認された送金はキャンセルすることができないので、その送金を無効とするためには反対の取引を別途行う必要がある。それらの履歴は全てブロックチェーン上に記録される。
	記録者の信用力に関する説明	PoSは、手元のPCからでも「ステーク」と呼ばれる一定額の暗号資産を引き出し不能なかたちでネットワークに投じることができる。ステークした人の中から、通常はランダムなプロセスによって一部が選ばれ、選ばれた人は特定のブロックを検証して対価として報酬と手数料を暗号資産で受け取ることになる。システムをだまそうとした場合、ネットワークは懲罰としてステークの一部または全部を「スラッシュ(破壊)」される。ETHの場合、ステークをする場合に少なくとも32ETHを投じなければ、検証に加わるチャンスは巡ってこない。また、検証にずさんな点があれば罰金が科される危険性があり、偽りがあれば投じた金額のすべてを失う可能性がある。
	価値移転の管理状況に対する監査の有無	なし
	監査を実施する者の氏名又は名称	―
	直近時点で行われた監査年月日	―
	その監査結果	―
	(統括者に関する情報)	
	記録者の統括者の有無	なし
	統括者の名称	―
	統括者の所在地	―
	統括者の属性	―
	統括者の概要	―

【暗号資産に内在するリスク】	価値移転ネットワークの脆弱性に関する特記事項	Ethereum PoSでは、1バリデータが32ETHのDepositを必要とし、ブロックの接続権の割り当てが行われる。バリデータたちの「Stake」されたETHは悪意あるアタックを行った場合やオフラインになった場合は没収されうる等、暗号資産の価値を損ねる行動をとることの経済的メリットはない。Etereum PoSの仕組み上、Reorg（巻き戻し）がないことも考慮すると、二重移転は発生しにくいと思料する。
	保有情報暗号化技術の脆弱性に関する特記事項	第三者に秘密鍵を知られた場合には、利用者になりすまして送付指示を行うことができる。
	発行者の破たんによる価値喪失の可能性に関する特記事項	なし
	価値移転記録者の破たんによる価値喪失の可能性に関する特記事項	―
	移転の記録が遅延する可能性に関する特記事項	―
	プログラムの不具合によるリスク等 に関する特記事項	ブロックチェーン上にデプロイされたコントラクトコードに脆弱性があった場合に不正に資産が盗み取られるリスクがある。
	過去に発生したプログラムの不具合の発生状況に関する特記事項	Ethereum上のアプリケーション「The DAO」のプログラム（スマートコントラクト）のバグ（脆弱性）を攻撃されて、集まったファンド資金3分の1以上を盗み取られた事例がある。
	非互換性のアップデート（ハードフォーク）の状況	2016年7月 The DAOの攻撃によって盗まれたDAOを取り戻すEthereum Classicハードフォーク（注1）
	今後の非互換性アップデート予定	―
	正常な稼働に影響を与えたサイバー攻撃の履歴	―
【流通状況】	価格データの出所	出所：当社Orderbook trading
	1取引単位当たり計算単価（ドル基準、例：＄1.000.000）	$1,557.32
	1取引単位当たり計算単価（円基準、例：￥100.000.000）	¥232,040
	ドル/円計算レート　2022年10月31日基準	1ドル/約149円
	四半期取引数量（協会加盟会員合計、現物、単位は百万円）	1,865,750（4-6月期）
備考		注1　旧来のイーサリアムをハードフォークすることにより、2016年6月の自律分散型投資ファンド「The DAO」への攻撃によって盗難されたDAOを救出した。このHFを支持しなかったマイナーによって存続することとなった旧仕様のイーサリアムはEthereum Classicに改称され、HF側がイーサリアムの名称を引き継いだ。スマートコントラクトの実行プラットフォームとして開発された現在のETCの性格を引き継いでいる。 イーサリアムのアップデートには遅れが出ていたが、2022年9月の「The Merge」を無事にクリアし、コンセンサス・アルゴリズムはPoWからPoSに移行した。ただ、「The Merge」はキャパシティの増加や拡張を図るといったものではなく、合意形成メカニズム（ETHがトランザクションを検証するための手段）の変更に関するアップグレードであるため、短期的にはガス代の削減は見込めない。そのため、「The Merge」に次ぐ他のアップデートもまだ続々と控えている。 「The Surge」「The Verge」「The Purge」「The Splurge」が予定されている。 「The Surge」・・・ステーキングしたETHの出庫が可能になる「上海」アップグレードや、大量のデータ処理や対応の負担をネットワーク全体に分散させ、スケーラビリティの向上を図る「シャーディング」などが含まれる。 「The Verge」・・・ユーザーが大量のデータを保存する必要なくネットワークバリデーターになることができ、さらなる分散化が可能となる。 「The Purge」・・・古いネットワーク履歴の削除が目的。 「The Splurge」・・・これまでのステップの微調整を実施。