受験番号:33IPE005

問１.

過去３０年間にわたり、世界中の核廃棄物の永久貯蔵のための主な計画は核廃棄物の地下貯蔵であった。しかしながら、閉じ込めの有効性、プルトニウム廃棄物の多くのエネルギー容量の損失、貯蔵された廃棄物における何千トンもの武器転用可能なプルトニウムの蓄積、及び永久貯蔵における廃棄物の再臨界の可能性についての懸念が、世界中で地下貯蔵の実施を遅らせてきた。現在のところ、高レベル核廃棄物の地下貯蔵ための恒久的な用地を特定した国はなく、地下廃棄物貯蔵がどこかで実施されるのは、少なくとも１０年は先になる。いくつかの国は、従来型の軽水炉（ＬＷＲ）又は廃棄物燃焼用に転用された高速増殖炉での混合酸化物（ＭＯＸ）廃棄物燃焼といった技術を使用して、廃棄物を破壊することによって、この問題に対処しようとしてきた。これらのアプローチを使用していくつかの利を得ることは可能であるが、廃棄物問題に対する影響が小さいか、著しい影響を与えるための時間的スケールが人間の一世代よりもはるかに長くなるかの、いずれかである。したがって、従来型の原子力技術を使用する廃棄物の破壊が、地下貯蔵を著しく改善するために実用的であるという合意はない。

問２.

先端の電界の強さに応じて、先端頂部１８７付近の原子棚における各原子は、対応するイオン化ディスク１４８を有しうる。イオン化ディスク１４８は、その中で、その中に進入する中性Ｈｅ原子がイオン化される確率が高い、空間領域である。典型的には、中性Ｈｅ原子のイオン化は、中性Ｈｅ原子から先端頂部原子への電子トンネリングにより発生する。したがって、イオン化ディスク１４８は、空間領域であって、その中でＨｅイオンが生成され、かつそこからＨｅイオンが出現する、空間領域を表す。

特定の先端頂部原子のイオン化ディスク１４８のサイズは、先端頂部１８７の形状、及び先端頂部１８７に印加される電位に依拠する。一般に、Ｈｅ原子のイオン化は、局所電界がＨｅ原子のイオン化電位を超過している先端頂部１８７と隣り合った空間領域で発生しうる。したがって、先端頂部１８７に大電位が印加された場合、多くの先端原子がイオン化ディスクを有することになる。加えて、先端頂部１８７の近傍の局所電界は、先端頂部１８７の形状に依拠する。先端頂部が比較的鋭い場合、先端頂部１８７の近傍の局所電界は比較的大きくなる。先端頂部が比較的鈍い場合には、先端頂部１８７の近傍であっても、局所電界は小さくなる。

問３．
【請求項１】
方法であって
ａ）ネットワーク又はシステムにおける複数の端末を、管理し、操作し、又は整備するステップと、
ｂ）選択又は更新を可能にする、第１のアカウントポータル、コンソール、又はシステムへのアクセスを可能にするステップとを含み、前記第１のアカウントポータル、コンソール、又はシステムが、
ｉ）一又は複数のグラフィカルユーザインターフェース（ＧＵＩ）を含み、前記ＧＵＩが、少なくとも、
１）端末の第１のセット中の一又は複数の端末に関連付けられた情報を含み、前記情報が、
（ａ）前記端末の第１のセット中の前記一又は複数の端末の各々に関連付けられた識別子ラベルと、
（ｂ）前記端末の第１のセット中の前記一又は複数の端末の各々の設定とを含み、前記設定が、
（ｉ）第１の設定を含み、前記第１の設定は、
（１）コンプライアンス設定、
（２）優先設定、
（３）料金設定、又は
（４）前記端末の第１のセットの各端末の制御、を含み、前記制御が、
ａ．リブートコマンドを含み、
前記方法は更に、
ｃ）前記第１のアカウントポータル、コンソール、又はシステムで行われた選択又は更新を受信するステップと、
ｄ）前記選択又は更新に基づいて、前記端末の第１のセット中の前記一又は複数の端末の各々の構成設定を更新するステップと、
ｅ）第１のユーザのための第１のユーザアカウントを作成するステップとを含み、前記第１のユーザアカウントを作成するステップは、
ｉ）第１のユーザデータを受信することであって、前記第１のユーザデータが、前記第１のユーザに関連付けられた本人識別文書情報又は本人識別情報を含む、第１のユーザデータを受信すること、
ｉｉ）前記第１のユーザに関連付けられた前記ユーザ識別子又はアカウント識別子を作成すること、及び／又は
ｉｉｉ）前記ユーザ識別子又はアカウント識別子を、前記第１のユーザア

カウントに関連して記憶すること、を含み、
前記方法は更に、
ｆ）第１のハードウェア端末におけるユーザによる操作を受信するステップであって、前記第１のハードウェア端末は、前記端末の第１のセット中の前記一又は複数の端末に属する、ユーザによる操作を受信するステップと、
ｇ）前記操作の第１の処理を実行するステップと、を含み、前記操作の前記第１の処理を実行するステップが、
ｉ）前記第１のハードウェア端末から暗号化された第１のペイロードを受信することと、
ｉｉ）前記暗号化された第１のペイロードが第１のペイロードを暗号化することによって生成され、前記第１のペイロードが前記ハードウェア端末によって生成され、前記第１のペイロードが電話番号を含み、前記電話番号が、前記第１のハードウェア端末において前記ユーザから受信されることと、
ｉｉｉ）前記暗号化された第１のペイロードが、セキュアセッション中に前記ハードウェア端末から通信されることと、
ｉｖ）前記電話番号にＳＭＳ認証コードを送信することと、を含む、
方法。