【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和2年7月2日(2020.7.2)

【公表番号】特表2020-513183(P2020-513183A)
【公表日】令和2年4月30日(2020.4.30)
【年通号数】公開・登録公報2020-017
【出願番号】特願2019-554787(P2019-554787)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｇ０６Ｆ　21/62　３５４

【手続補正書】
【提出日】令和2年5月25日(2020.5.25)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ネットワークを介して通信するように構成された、データソース・コンピュータ、トークン化コンピュータ、およびデータ収集コンピュータを含むデータ・トークン化システムであって、
前記データソース・コンピュータは、前記データ収集コンピュータに送信するための、関連ＩＤデータを有するメッセージ・データを用意し、さらに、ノンスを使って前記ＩＤデータをブラインド化することによってブラインドＩＤを生成し、前記ブラインドＩＤを前記トークン化コンピュータに送信し、前記ノンスおよび前記メッセージ・データを、前記データ収集コンピュータによって受信されるように前記ネットワークを介して送信するように構成され、
前記トークン化コンピュータは、前記ブラインドＩＤの受信に応じ、前記ブラインドＩＤから、前記ノンスでブラインド化された前記ＩＤデータの関数および前記トークン化コンピュータの秘密鍵を含むブラインド・トークンを生成し、前記ブラインド・トークンを前記データ収集コンピュータに送信するように構成され、
前記データ収集コンピュータは、前記トークン化コンピュータからの前記ブラインド・トークンと、前記データソース・コンピュータによって送信された前記ノンスおよび前記メッセージ・データとの受信に応じ、前記ＩＤデータの確定関数および前記秘密鍵を含むＩＤトークンを得るべく前記ブラインド・トークンを可視化するため前記ノンスを使用し、前記ＩＤトークンおよび前記メッセージ・データを、前記データ収集コンピュータに動作可能に連結されたストレージ中に格納するように構成される、
システム。
【請求項２】
前記データソース・コンピュータは、前記ブラインドＩＤが値Ｒ＝Ｆ（Ｎ，ｈ）を含むように構成され、このＦは所定の関数であり、Ｎは前記ノンスであり、ｈは前記ＩＤデータの関数であり、
前記トークン化コンピュータは、前記ブラインド・トークンが値Ｒ’＝Ｆ（ｋ，Ｒ）を

含むように構成され、このｋは前記秘密鍵であり、
前記データ収集コンピュータは、前記ＩＤトークンが値Ｆ（ｎ，Ｒ’）を含むように構成され、このｎは前記ノンスＮの関数であり、
前記所定の関数Ｆは、Ｆ（ｎ，Ｒ’）＝Ｆ’（ｋ，ｈ）となるような関数であり、このＦ’は前記確定関数である、
請求項１に記載のシステム。
【請求項３】
前記所定の関数Ｆが、$F(x, y) = y^{x}$となるような関数であり、前記関数ｎが値N^{-1}を含む、請求項２に記載のシステム。
【請求項４】
前記トークン化コンピュータが、値ｋ’／ｋを含むトークン更新データΔを生成するため、新規の秘密鍵ｋ’を周期的に生成し、前記トークン更新データΔを前記データ収集コンピュータに送信するようにさらに構成され、
前記データ収集コンピュータが、前記トークン更新データΔの受信に応じて、前記ストレージ中の前記ＩＤトークンｔｏｋを、値ｔｏｋΔを含む更新されたトークンによって置き換えるようにさらに構成される、
請求項３に記載のシステム。
【請求項５】
前記関数ｈが前記ＩＤデータのハッシュを含む、請求項２に記載のシステム。
【請求項６】
前記データソース・コンピュータが、前記データ収集コンピュータに送信するための前記メッセージ・データに対するセッション識別子を選択し、前記ブラインドＩＤとともに前記セッション識別子を前記トークン化コンピュータに送信し、前記セッション識別子、前記メッセージ・データ、および前記ノンスを前記データ収集コンピュータに送信するようにさらに構成され、
前記トークン化コンピュータが、前記ブラインド・トークンとともに前記セッション識別子を前記データ収集コンピュータに送信するようにさらに構成される、
請求項１に記載のシステム。
【請求項７】
前記データソース・コンピュータが、暗号データを生成するため前記メッセージ・データおよび前記ノンスを暗号化し、前記ブラインドＩＤとともに前記暗号データを前記トークン化コンピュータに送信するようにさらに構成され、
前記トークン化コンピュータが、前記暗号データを前記ブラインド・トークンとともに前記データ収集コンピュータに送信するようにさらに構成され、
前記データ収集コンピュータが、前記メッセージ・データおよび前記ノンスを復元するために前記暗号データを解読するようにさらに構成される、
請求項１に記載のシステム。
【請求項８】
複数の前記データ収集コンピュータを含む、請求項１に記載のシステム。
【請求項９】
ネットワークを介して、データ収集コンピュータにデータを供給するためのコンピュータ実装の方法であって、前記方法は、前記ネットワーク中のトークン化コンピュータと通信するように構成されたデータソース・コンピュータにおいて、
前記データ収集コンピュータに送信するための、関連するＩＤデータを有するメッセージ・データを用意するステップと、
ノンスを使って前記ＩＤデータをブラインド化することによってブラインドＩＤを生成するステップと、
前記トークン化コンピュータによって前記データ収集コンピュータに送信するための、前記ノンスでブラインド化された前記ＩＤデータの関数および前記トークン化コンピュータの秘密鍵を含むブラインド・トークンのブラインドＩＤからの生成のため、前記ブライ

ンドＩＤを前記トークン化コンピュータに送信するステップと、
　前記ノンスおよび前記メッセージ・データを、前記データ収集コンピュータが受信するように前記ネットワークを介して送信するステップと、を含み、
　これらにより、前記データ収集コンピュータは、前記メッセージ・データに対する前記ＩＤデータの確定関数および前記秘密鍵を含むＩＤトークンを得るべく前記ブラインド・トークンを可視化するため前記ノンスを使ことが可能となる、
方法。
【請求項１０】
　データソース・コンピュータによってネットワークを介してデータ収集コンピュータに供給するためのメッセージ・データに関連付けられた、ＩＤデータをトークン化するためのコンピュータ実装の方法であって、前記方法は、前記ネットワーク中のトークン化コンピュータにおいて、
　前記データソース・コンピュータから、ノンスを使って前記ＩＤデータをブラインド化することによって生成されたブラインドＩＤを受信するステップと、
　前記ブラインドＩＤから、前記ノンスでブラインド化された前記ＩＤデータの関数および前記トークン化コンピュータの秘密鍵を含む、ブラインド・トークンを生成するステップと、
　前記ブラインド・トークンを前記データ収集コンピュータに送信するステップと、
を含み、
　これらにより、前記データ収集コンピュータは、前記ノンスおよび前記メッセージ・データを受信すると、前記メッセージ・データに対する、前記ＩＤデータの確定関数および前記秘密鍵を含むＩＤトークンを得るべく前記ブラインド・トークンを可視化するため、前記ノンスを用いることが可能となる、
方法。
【請求項１１】
　ネットワークを介してデータソース・コンピュータからデータを取得するためのコンピュータ実装の方法であって、前記方法は、前記ネットワーク中でトークン化コンピュータと通信するように構成されたデータ収集コンピュータにおいて、
　前記データソース・コンピュータによって送信された、前記データソース・コンピュータでＩＤデータに関連付けられたメッセージ・データ、およびノンスを前記ネットワークを介して受信するステップと、
　前記トークン化コンピュータから、前記データソース・コンピュータで、前記ノンスを使って前記ＩＤデータをブラインド化することによって生成されたブラインドＩＤから生成されたブラインド・トークンを受信するステップであって、前記ブラインド・トークンは、前記ノンスでブラインド化された前記ＩＤデータの関数、および前記トークン化コンピュータの秘密鍵を含む、前記受信するステップと、
　前記ＩＤデータの確定関数および前記秘密鍵を含むＩＤトークンを得るべく前記ブラインド・トークンを可視化するため、前記ノンスを使用するステップと、
　前記ＩＤトークンおよび前記メッセージ・データを、前記データ収集コンピュータに動作可能に連結されたストレージ中に格納するステップと、
を含む、方法。
【請求項１２】
　コンピュータ・プログラムがコンピュータ上で実行されたとき、請求項９～１１のいずれか一項に記載の方法を遂行するように構成されたプログラム・コード手段を含む、コンピュータ・プログラム。