【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６部門第３区分
【発行日】令和3年7月26日(2021.7.26)

【公表番号】特表2020-524847(P2020-524847A)
【公表日】令和2年8月20日(2020.8.20)
【年通号数】公開・登録公報2020-033
【出願番号】特願2019-570081(P2019-570081)
【国際特許分類】
Ｇ０６Ｆ　21/31　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/31

【手続補正書】
【提出日】令和3年5月27日(2021.5.27)
【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】
コンピューティングデバイスによって、リソースにアクセスするための要求をクライアントデバイスから受信し、
前記コンピューティングデバイスによって、前記要求に対応するコンテキスト情報を決定し、
前記コンピューティングデバイスによって、前記コンテキスト情報に基づいてスコアを決定し、
前記コンピューティングデバイスによって、前記スコアに基づいて前記要求に認証レベルを割り当て、
前記コンピューティングデバイスによって、前記認証レベルに基づいて、前記コンピューティングデバイスから発行された初期トークンと、１つ以上の認証サービスのＩＤと、認証パラメータとを有する認証チャレンジを生成し、
前記コンピューティングデバイスによって、前記クライアントデバイスへの前記認証チャレンジの送信に応答して、前記クライアントデバイスから更新されたトークンを受信し、前記更新されたトークンは、前記１つ以上の認証サービスに対する前記クライアントデバイスのユーザの認証を示す情報を前記初期トークンに含めることによって生成され、前記ユーザの前記認証は、少なくとも１つの認証プロトコルと、前記認証チャレンジへの応答の前記認証パラメータとを用いて達成され、前記認証を示す情報は、前記認証チャレンジに応答してなされた前記クライアントデバイスからの認証要求に対する応答の一部として前記１つ以上の認証サービスによって前記初期トークンに含まれ、
前記コンピューティングデバイスによって、前記更新されたトークンで示された前記１つ以上の認証サービスに対する前記クライアントデバイスの前記ユーザの前記認証に基づいて、前記クライアントデバイスに前記リソースへのアクセスを提供する、
ことを含む方法。
【請求項２】
前記コンピューティングデバイスによって前記初期トークンを保存することをさらに含む、請求項１に記載の方法。
【請求項３】
前記コンピューティングデバイスによって、

少なくとも１つの認証スキームを実行するための認証サービスを識別し、
前記認証パラメータに前記認証サービスのＩＤを含める、
ことをさらに含む、請求項１に記載の方法。
【請求項４】
前記認証チャレンジの受信により、前記クライアントデバイスによって、前記初期トークンを有する認証要求を送信し、
前記クライアントデバイスによって、前記少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する前記更新されたトークンを受信する、
ことをさらに含む、請求項３に記載の方法。
【請求項５】
前記更新されたトークンの受信により、前記クライアントデバイスによって、前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたか否かを判断し、
前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたという判断により、前記更新されたトークンを前記コンピューティングデバイスに送信する、
ことをさらに含む、請求項４に記載の方法。
【請求項６】
前記更新されたトークンに含まれる１つ以上のアサーションが前記少なくとも１つの認証プロトコルを満たすという判断により、前記コンピューティングデバイスによって、前記リソースにアクセスするための前記要求を許可することをさらに含む、請求項５に記載の方法。
【請求項７】
前記リソースにアクセスするための前記要求を許可すると、前記コンピューティングデバイスによって、前記更新されたトークンを破棄することをさらに含む、請求項６に記載の方法。
【請求項８】
前記リソースにアクセスするための前記要求を許可すると、前記コンピューティングデバイスによって、前記初期トークンを破棄することをさらに含む、請求項６に記載の方法。
【請求項９】
前記コンピューティングデバイスによって、
前記更新されたトークンに関連付けられたタイムスタンプが規定の制限時間内にあるか否かを判断し、
前記タイムスタンプが前記規定の制限時間内にあるという判断により、前記リソースにアクセスするための前記要求を許可する、
ことをさらに含む、請求項６に記載の方法。
【請求項１０】
前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されていないという判断により、前記更新されたトークンを所定の認証サービスに送信することをさらに含む、請求項５に記載の方法。
【請求項１１】
前記初期トークンは、前記要求に含まれる１つ以上の認証資格情報のうち成功した認証を示す初期アサーションを有する、請求項１に記載の方法。
【請求項１２】
前記要求は、前記ユーザを識別するユーザ情報を有する、請求項１に記載の方法。
【請求項１３】
前記リソースは、セルフサービスパスワードリセットサービスである、請求項１に記載の方法。
【請求項１４】

前記初期トークンは、前記１つ以上の認証サービスによる前記少なくとも１つの認証プロトコルの実行の動作を指定する情報を含む、請求項１に記載の方法。
【請求項１５】
前記認証を示す情報は、少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する、請求項１に記載の方法。
【請求項１６】
プロセッサと、
コンピューティングシステムでユーザを認証するための方法を前記プロセッサに実施させるプログラミング命令を有する非一時的なコンピュータ読み取り可能な記憶媒体と、を備え、
前記プログラミング命令は、
ユーザに関連付けられたコンピューティングデバイスから、リソースサービスに関連付けられたリソースにアクセスするためのアクセス要求を受信し、
前記アクセス要求に対応するコンテキスト情報を決定し、
前記コンテキスト情報に基づいてスコアを決定し、
前記スコアに基づいて前記アクセス要求に認証レベルを割り当て、
前記認証レベルを用いて、前記ユーザを認証するための認証プロトコルであって、少なくとも１つの認証スキームを有する認証プロトコルを識別し、
前記識別された認証プロトコルに対応する初期トークンと認証パラメータとを有する認証チャレンジを生成し、
前記認証チャレンジを前記コンピューティングデバイスに送信するための命令を有する、コンピューティングシステム。
【請求項１７】
前記プログラミング命令は、前記初期トークンを保存するための命令をさらに有する、請求項１６に記載のコンピューティングシステム。
【請求項１８】
前記コンピューティングシステムは、１つ以上の認証サービスを備えており、
前記プログラミング命令は、さらに、
前記１つ以上の認証サービスのうち、前記少なくとも１つの認証スキームを実行する認証サービスを識別し、
前記認証パラメータに前記識別された認証サービスのＩＤを含めるための命令を有する、
請求項１６に記載のコンピューティングシステム。
【請求項１９】
前記プログラミング命令は、前記コンピューティングデバイスに、
前記初期トークンを有する認証要求を送信させ、
前記少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する更新されたトークンを受信させるための命令をさらに有する、
請求項１８に記載のコンピューティングシステム。
【請求項２０】
前記プログラミング命令は、前記コンピューティングデバイスに、
前記更新されたトークンの受信により、前記識別された認証プロトコルに含まれるすべての認証スキームが実行されたか否かを判断し、
前記識別された認証プロトコルに含まれるすべての認証スキームが実行されたという判断により、前記更新されたトークンを前記リソースサービスに送信すること、を実行させるための命令をさらに有する、
請求項１９に記載のコンピューティングシステム。
【請求項２１】
前記プログラミング命令は、前記更新されたトークンに含まれる１つ以上のアサーションが前記識別された認証プロトコルを満たすという判断により、前記リソースにアクセス

するための前記アクセス要求を前記プロセッサに許可させるための命令をさらに有する、請求項２０に記載のコンピューティングシステム。
【請求項２２】
前記プログラミング命令は、前記リソースにアクセスするための前記アクセス要求を許可すると、前記プロセッサに前記更新されたトークンを破棄させるための命令をさらに有する、請求項２１に記載のコンピューティングシステム。
【請求項２３】
前記プログラミング命令は、前記リソースにアクセスするための前記アクセス要求を許可すると、前記プロセッサに前記初期トークンを破棄させるための命令をさらに有する、請求項２１に記載のコンピューティングシステム。
【請求項２４】
前記プログラミング命令は、前記プロセッサに、
前記更新されたトークンに関連付けられたタイムスタンプが規定の制限時間内にあるか否かを判断させ、
前記タイムスタンプが前記規定の制限時間内にあるという判断により、前記リソースにアクセスするための前記アクセス要求を許可させるための命令をさらに有する、請求項２１に記載のコンピューティングシステム。
【請求項２５】
前記初期トークンは、前記アクセス要求に含まれる１つ以上の認証資格情報のうち成功した認証を示す初期アサーションを有する、請求項１６に記載のコンピューティングシステム。
【請求項２６】
前記アクセス要求は、前記ユーザを識別するユーザ情報を有する、請求項１６に記載のコンピューティングシステム。
【請求項２７】
前記アクセス要求に対応する前記コンテキスト情報を決定することは、前記ユーザ情報に基づいて前記コンテキスト情報を決定することを含む、請求項２６に記載のコンピューティングシステム。
【請求項２８】
前記コンテキスト情報は、前記ユーザの１つ以上の特性、前記リソースの１つ以上の特性、または前記コンピューティングデバイスの１つ以上の特性のうちの１つ以上を有する、請求項１６に記載のコンピューティングシステム。
【請求項２９】
プロセッサと、
コンピューティングシステムでユーザを認証するための方法を前記プロセッサに実施させるプログラミング命令を有する非一時的なコンピュータ読み取り可能な記憶媒体と、を備え、
前記プログラミング命令は、
リソースにアクセスするための要求をクライアントデバイスから受信し、
前記要求に対応するコンテキスト情報を決定し、
前記コンテキスト情報に基づいてスコアを決定し、
前記スコアに基づいて前記要求に認証レベルを割り当て、
前記認証レベルに基づいて、前記コンピューティングデバイスから発行された初期トークンと、１つ以上の認証サービスのＩＤと、認証パラメータとを有する認証チャレンジを生成し、
前記クライアントデバイスへの前記認証チャレンジの送信に応答して、前記クライアントデバイスから更新されたトークンを受信し、前記更新されたトークンは、前記１つ以上の認証サービスに対する前記クライアントデバイスのユーザの認証を示す情報を前記初期トークンに含めることによって生成され、前記ユーザの前記認証は、少なくとも１つの認証プロトコルと、前記認証チャレンジへの応答の前記認証パラメータとを用いて達成され

、前記認証を示す情報は、前記認証チャレンジに応答してなされた前記クライアントデバイスからの認証要求に対する応答の一部として前記１つ以上の認証サービスによって前記初期トークンに含まれ、

前記更新されたトークンで示された前記１つ以上の認証サービスに対する前記クライアントデバイスの前記ユーザの前記認証に基づいて、前記クライアントデバイスに前記リソースへのアクセスを提供するための命令を有する、コンピューティングシステム。

【請求項３０】

前記プログラミング命令は、前記クライアントデバイスに、

前記初期トークンを有する認証要求を送信させ、

前記少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する前記更新されたトークンを受信させるための命令をさらに有する、請求項２９に記載のコンピューティングシステム。

【請求項３１】

前記プログラミング命令は、前記クライアントデバイスに、

前記更新されたトークンの受信により、前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたか否かを判断し、

前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたという判断により、前記更新されたトークンを前記プロセッサに送信すること、を実行させるための命令をさらに有する、請求項２９に記載のコンピューティングシステム。

【請求項３２】

前記プログラミング命令は、前記更新されたトークンに含まれる１つ以上のアサーションが前記少なくとも１つの認証プロトコルを満たすという判断により、前記リソースにアクセスするための前記要求を前記プロセッサに許可させるための命令をさらに有する、請求項３０に記載のコンピューティングシステム。