【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】平成28年1月21日(2016.1.21)

【公表番号】特表2015-500585(P2015-500585A)
【公表日】平成27年1月5日(2015.1.5)
【年通号数】公開・登録公報2015-001
【出願番号】特願2014-544029(P2014-544029)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｇ０６Ｆ　21/24　１６６Ｅ

【手続補正書】
【提出日】平成27年11月26日(2015.11.26)
【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】
複数のデバイスを含むデバイスグループのメンバーシップを管理する方法であって、前記デバイスグループ内の各デバイスは、自身のデバイスキーを除き、前記デバイスグループ内の全ての他のデバイスのデバイスキーを保持し、前記方法は、
前記デバイスグループメンバーのうちの１つを、自身のデバイスキーを含め、前記デバイスグループ内の前記複数のデバイスの全てのデバイスキーを保持するグループマネージャーデバイスとして選出するステップを含み、
前記デバイスグループに新しいデバイスを加える場合、
前記新しいデバイスと前記グループマネージャーデバイスとの間に安全な接続を確立するステップと、
前記グループマネージャーデバイスによって、前記新しいデバイスに前記デバイスグループ内の全てのデバイスの前記デバイスキーを送信するステップと、
前記デバイスグループ内の前記複数のデバイスのうちの１つによって、前記新しいデバイスのデバイスキーを生成して、前記デバイスグループ内の他の全てのデバイスに配布するステップとを含み、
前記デバイスグループからデバイスを除外する場合、
前記デバイスグループ内に残るデバイスの任意の組み合わせによって、前記グループマネージャーデバイス以外のデバイスが自身の新しいデバイスキーを生成及び受信しないよう、前記デバイスグループ内に残る前記デバイスの新しいデバイスキーを生成して配布するステップを含む、方法。
【請求項２】
前記新しいデバイスの前記デバイスキーは、前記グループマネージャーデバイスによって生成及び配布される、請求項１に記載の方法。
【請求項３】
前記デバイスグループ内の各デバイスが、各デバイスが保持するデバイスキーを変更するステップをさらに含む、請求項１に記載の方法。
【請求項４】

各デバイスが保持する前記デバイスキーを変更する前記ステップは、当該デバイスキーに一方向性関数を適用することによって実行される、請求項３に記載の方法。
【請求項５】
前記新しいデバイスに前記デバイスグループ内の全てのデバイスの前記デバイスキーを送信する前に、前記グループマネージャーによって前記新しいデバイスを認証するステップをさらに含む、請求項１に記載の方法。
【請求項６】
前記デバイスグループ内に残る各デバイスの前記新しいデバイスキーはランダムに生成される、請求項１に記載の方法。
【請求項７】
前記デバイスグループ内に残る各デバイスの前記新しいデバイスキーは、前記デバイスグループから除外される前記或るデバイスのデバイスキー、及び前記デバイスグループ内に残る各デバイスの古い前記デバイスキーを用いて暗号化された後に配布される、請求項１に記載の方法。
【請求項８】
除外される前記或るデバイスは前記グループマネージャーデバイスであり、
前記デバイスグループ内に残る前記デバイスから新しいグループマネージャーデバイスを選出するステップをさらに含む、請求項１に記載の方法。
【請求項９】
ｎ（ｎ＞１）個のデバイスを含むデバイスグループのメンバーシップを管理する方法であって、前記デバイスグループ内の各デバイスは、ｋ－レジリエント方式（ｋ＞１）により、アドレス指定されたデバイスのみがメッセージを解読できるよう前記デバイスグループ全体又は前記デバイスグループの任意の部分集合へのメッセージを暗号化するために使用できるキー材料を保持し、前記方法は、
前記ｋレジリエント方式（ｋ＞１）により、グループマネージャーデバイスがメッセージを解読できるよう、前記デバイスグループメンバーのうちの１つを、自身のデバイスキーを含め、前記デバイスグループ内の前記複数のデバイスの全てのデバイスキーを保持する前記グループマネージャーデバイスとして選出するステップを含み、
前記デバイスグループに新しいデバイスを加える場合、
前記グループマネージャーデバイスによって、前記新しいデバイスにより拡張される最大でｋ－１のメンバーを有する前記デバイスグループの部分集合、すなわち最大でｋのメンバーデバイスを有する部分集合の全てに対して、前記デバイスグループの当該部分集合内のデバイス、及び前記新しいデバイスを除く全てのデバイスによって解読できるようメッセージを暗号化するための部分集合ごとの新しいキー材料を生成し、前記デバイスグループの当該部分集合に含まれていない前記デバイスグループ内の全てのデバイスに前記部分集合ごとのキー材料を配布するステップと、
前記新しいデバイスと前記グループマネージャーデバイスとの間に安全な接続を確立するステップと、
前記グループマネージャーデバイスによって、前記新しいデバイスに前記キー材料を送信するステップとを含み、
前記デバイスグループからデバイスを除外する場合、
前記グループマネージャーデバイスによって、最大でｋのメンバーを有し、前記デバイスグループから除外される前記デバイスを含まない前記デバイスグループの全ての部分集合に対して、前記デバイスグループの当該部分集合内のデバイスを除く全てのデバイスが解読できるようメッセージを暗号化するための部分集合ごとの新しいキー材料を生成し、前記部分集合ごとのキー材料を、前記デバイスグループの当該部分集合に含まれていない前記デバイスグループの全てのデバイスに配布するステップを含む、方法。
【請求項１０】
前記デバイスグループに新しいデバイスを加える場合、前記新しいデバイスに前記キー材料を送信する前に、前記グループマネージャーによって前記新しいデバイスを認証する

ステップをさらに含む、請求項９に記載の方法。
【請求項１１】
複数のデバイスを含むデバイスグループのデバイスであって、前記デバイスグループ内の各デバイスは、自身のデバイスキーを除き、前記デバイスグループ内の全ての他のデバイスのデバイスキーを保持し、前記デバイスは、
コードを含むメモリと通信するプロセッサを含み、前記プロセッサは、前記メモリにアクセスすることにより、
前記デバイスを、自身のデバイスキーを含め、前記デバイスグループ内の前記複数のデバイスの全てのデバイスキーを保持するグループマネージャーデバイスとして選出し、
新しいデバイスとの安全な通信を確立し、
前記デバイスグループ内の全てのデバイスの前記デバイスキーを前記新しいデバイスに送信し、
前記新しいデバイスのデバイスキーを生成し、前記新しいデバイスを除く前記デバイスグループ内の全ての他のデバイスに配布する、デバイス。
【請求項１２】
前記コードはさらに、前記プロセッサに、メッセージを他のデバイスグループメンバーが保持する全てのキーを用いて暗号化することにより、当該他のデバイスグループメンバーに対して前記デバイスが前記グループマネージャーデバイスであることを証明させる、請求項１１に記載のデバイス。
【請求項１３】
前記コードはさらに、前記プロセッサに前記グループマネージャー内のデバイスキーを変更させる、請求項１１に記載のデバイス。
【請求項１４】
前記デバイスキーの変更は、前記デバイスキーに一方向性関数を適用することを含む、請求項１３に記載のデバイス。
【請求項１５】
前記コードはさらに、前記新しいデバイスに前記デバイスグループ内の全てのデバイスの前記デバイスキーを送信する前に、前記プロセッサに前記新しいデバイスを認証させる、請求項１１に記載のデバイス。