

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2013-80484  
(P2013-80484A)

(43) 公開日 平成25年5月2日(2013.5.2)

(51) Int.Cl.  
**G06F 21/62 (2013.01)**

F I  
G O 6 F 21/24 1 6 3 G

テーマコード (参考)

審査請求 有 請求項の数 58 O L 外国語出願 (全 64 頁)

<p>(21) 出願番号 特願2012-253480 (P2012-253480)</p> <p>(22) 出願日 平成24年11月19日 (2012.11.19)</p> <p>(62) 分割の表示 特願2010-540890 (P2010-540890) の分割</p> <p>原出願日 平成20年12月24日 (2008.12.24)</p> <p>(31) 優先権主張番号 11/963, 991</p> <p>(32) 優先日 平成19年12月24日 (2007.12.24)</p> <p>(33) 優先権主張国 米国 (US)</p>	<p>(71) 出願人 595020643 クアルコム・インコーポレイテッド QUALCOMM INCORPORATED アメリカ合衆国、カリフォルニア州 92121-1714、サン・ディエゴ、モアハウス・ドライブ 5775</p> <p>(74) 代理人 100108855 弁理士 蔵田 昌俊</p> <p>(74) 代理人 100109830 弁理士 福原 淑弘</p> <p>(74) 代理人 100088683 弁理士 中村 誠</p> <p>(74) 代理人 100103034 弁理士 野河 信久</p> <p style="text-align: right;">最終頁に続く</p>
--	--

(54) 【発明の名称】 モバイルデバイス上で時間ベースライセンスのポリシーを管理するための方法および装置

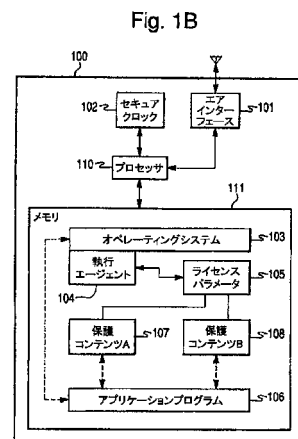
(57) 【要約】 (修正有)

【課題】 時間ベースライセンスを用いてゲーム、媒体、データ、または他のソフトウェアを保護するためにフレキシブルなデジタル著作権管理ライセンスポリシーを生成、管理、変更、および/または執行することを提供する。

【解決手段】 時間ソースが入手できないか、信用できないか、または信頼できない状況に対処する。ライセンスは、少数のパラメータによって定義され、パラメータ値は、保護コンテンツまたはアプリケーションによって定義され、それと共に含まれる。パラメータ値は、使いやすさとセキュリティ特性との間の所望の妥協レベルを定義し、執行するように選択されることができる。

【選択図】 図1B

図 1B



**【特許請求の範囲】****【請求項 1】**

モバイルデバイス上で保護コンテンツへのアクセスを制限するための方法であって、  
前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第 1 のポリシー条件を表す第 1 のパラメータ値を前記モバイルデバイス上に記憶することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを判断することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可することと、

前記モバイルデバイスが前記セキュア時間ソースへのアクセスを有した場合、前記第 1 のポリシー条件が満たされるかどうかを判断することと、

前記第 1 のポリシー条件が満たされる限り、前記保護コンテンツへのアクセスを与えることと、

を備える方法。

**【請求項 2】**

前記第 1 のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 1 に記載の方法。

**【請求項 3】**

前記第 1 のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 1 に記載の方法。

**【請求項 4】**

前記第 1 のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 1 に記載の方法。

**【請求項 5】**

前記第 1 のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 1 に記載の方法。

**【請求項 6】**

前記第 1 のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 1 に記載の方法。

**【請求項 7】**

前記第 1 のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、

前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードすることと、

前記第 1 のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶することと、

をさらに備える、請求項 1 に記載の方法。

**【請求項 8】**

前記第 1 のパラメータに対する前記更新は、暗号化され認証されたファイル中でダウンロードされる、請求項 7 に記載の方法。

**【請求項 9】**

前記第 1 のパラメータに対する前記更新は、SMS メッセージ中で受信される、請求項 7 に記載の方法。

**【請求項 10】**

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶することをさらに備える、請求項 1 に記載の方法。

10

20

30

40

50

**【請求項 1 1】**

前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数であり、前記複数のパラメータ値のうち別の一つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 1 0 に記載の方法。

**【請求項 1 2】**

前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 1 0 に記載の方法。

**【請求項 1 3】**

前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがローミング中であるときに前記モバイルデバイスがどのようにアクセス試行を扱うべきかを示す、請求項 1 0 に記載の方法。

**【請求項 1 4】**

前記複数のパラメータ値のうちの一つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 1 0 に記載の方法。

**【請求項 1 5】**

前記複数のパラメータ値のうちの一つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 1 0 に記載の方法。

**【請求項 1 6】**

前記複数のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、

前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードすることと、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す、前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶することと、

をさらに備える、請求項 1 0 に記載の方法。

**【請求項 1 7】**

前記複数のパラメータに対する前記更新は、暗号化され認証されたファイル中でダウンロードされる、請求項 1 6 に記載の方法。

**【請求項 1 8】**

前記複数のパラメータに対する前記更新は、SMS メッセージ中で受信される、請求項 1 6 に記載の方法。

**【請求項 1 9】**

新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードする、請求項 1 0 に記載の方法。

**【請求項 2 0】**

モバイルデバイス上で保護コンテンツの個々のファイルへのアクセスを制限するための方法であって、

少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第 1 のポリシー条件を表す第 1 のパラメータ値を前記モバイルデバイス上に記憶することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを判断することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、保護コンテンツの個々の各ファイルへのアクセスを許可することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、保護コンテン

10

20

30

40

50

ツの個々の各ファイルについて前記第 1 のポリシー条件が満たされるかどうかを判断することと、

前記第 1 のポリシー条件が満たされる限り、保護コンテンツの個々の各ファイルへのアクセスを与えることと、

を備える方法。

【請求項 2 1】

前記第 1 のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 2 0 に記載の方法。

【請求項 2 2】

前記第 1 のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 2 0 に記載の方法。

【請求項 2 3】

前記第 1 のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 2 0 に記載の方法。

【請求項 2 4】

前記第 1 のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 2 0 に記載の方法。

【請求項 2 5】

前記第 1 のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 2 0 に記載の方法。

【請求項 2 6】

前記第 1 のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、

前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードすることと、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第 1 のポリシー条件を表す前記第 1 のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶することと、

をさらに備える、請求項 2 0 に記載の方法。

【請求項 2 7】

前記第 1 のパラメータに対する前記更新は、暗号化され認証されたファイルにダウンロードされる、請求項 2 6 に記載の方法。

【請求項 2 8】

前記第 1 のパラメータに対する前記更新は、SMS メッセージ中で受信される、請求項 2 6 に記載の方法。

【請求項 2 9】

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶することをさらに備える、請求項 2 0 に記載の方法。

【請求項 3 0】

前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 2 9 に記載の方法。

【請求項 3 1】

前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された

10

20

30

40

50

猶予期間アクセス試行の回数である、請求項 29 に記載の方法。

【請求項 32】

前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 29 に記載の方法。

【請求項 33】

前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの 1 つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 29 に記載の方法。

10

【請求項 34】

前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 29 に記載の方法。

【請求項 35】

前記複数のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、

前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードすることと、

20

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶することと、

をさらに備える、請求項 29 に記載の方法。

【請求項 36】

前記複数のパラメータに対する前記更新は、暗号化されたファイル中でダウンロードされる、請求項 35 に記載の方法。

【請求項 37】

前記複数のパラメータに対する前記更新は、SMS メッセージ中で受信される、請求項 35 に記載の方法。

30

【請求項 38】

前記記憶された複数のパラメータ値のいずれかが、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示しているかどうかを判断するために、前記モバイルデバイスが電源投入されるたびに前記複数のポリシー条件を表す前記記憶された複数のパラメータ値の各々を問い合わせることをさらに備える、請求項 29 に記載の方法。

【請求項 39】

新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードする、請求項 29 に記載の方法。

【請求項 40】

40

モバイルデバイスであって、

プロセッサと、

前記プロセッサに結合され、ワイヤレスネットワークに接続するように構成されたワイヤレスランシーバと、

前記プロセッサに結合されたメモリであって、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第 1 のポリシー条件を表す第 1 のパラメータ値を前記モバイルデバイス上に記憶することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを判断することと、

50

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、前記第 1 のポリシー条件が満たされるかどうかを判断することと、

前記第 1 のポリシー条件が満たされる限り、前記保護コンテンツへのアクセスを与えることと、

を備えるステップを前記プロセッサに実行させるように構成されたソフトウェア命令を記憶したメモリと

を備えるモバイルデバイス。

【請求項 4 1】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である第 1 のパラメータ値を利用する、請求項 4 0 に記載のモバイルデバイス。

【請求項 4 2】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である第 1 のパラメータ値を利用する、請求項 4 0 に記載のモバイルデバイス。

【請求項 4 3】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である第 1 のパラメータ値を利用する、請求項 4 0 に記載のモバイルデバイス。

【請求項 4 4】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す第 1 のパラメータ値を利用する、請求項 4 0 に記載のモバイルデバイス。

【請求項 4 5】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す第 1 のパラメータ値を利用する、請求項 4 0 に記載のモバイルデバイス。

【請求項 4 6】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせるステップと、

前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードするステップと、

前記第 1 のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶するステップと、

を前記プロセッサに実行させるようにさらに構成される、請求項 4 0 に記載のモバイルデバイス。

【請求項 4 7】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータに対する前記ダウンロードされた更新を解析し、解読するステップを前記プロセッサに実行させるようにさらに構成される、請求項 4 6 に記載のモバイルデバイス。

【請求項 4 8】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータに対する前記更新を SMS メッセージ中で受信するステップを前記プロセッサに実行させるようにさらに構成される、請求項 4 7 に記載のモバイルデバイス。

【請求項 4 9】

10

20

30

40

50

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するステップを前記プロセッサに実行させるようにさらに構成される、請求項 40 に記載のモバイルデバイス。

【請求項 50】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 49 に記載のモバイルデバイス。

【請求項 51】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 49 に記載のモバイルデバイス。

【請求項 52】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 49 に記載のモバイルデバイス。

【請求項 53】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 49 に記載のモバイルデバイス。

【請求項 54】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 49 に記載のモバイルデバイス。

【請求項 55】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、  
前記複数のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせるステップと、  
前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするステップと、  
前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶するステップと、  
を前記プロセッサに実行させるようにさらに構成される、請求項 49 に記載のモバイルデバイス。

【請求項 56】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータに対する前記ダウンロードされた更新を解析し、解読するステップを前記プロセッサに実行させるようにさらに構成される、請求項 55 に記載のモバイルデバイス。

【請求項 57】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータに対する前記更新を SMS メッセージ中で受信するステップを前記プロセッサに実行させるようにさらに構成される、請求項 56 に記載のモバイルデバイス。

【請求項 58】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするステップを前

10

20

30

40

50

記プロセッサに実行させるようにさらに構成される、請求項 49 に記載のモバイルデバイス。

【請求項 59】

モバイルデバイスであって、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第 1 のポリシー条件を表す第 1 のパラメータ値を前記モバイルデバイス上に記憶するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを判断するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、前記第 1 のポリシー条件が満たされるかどうかを判断するための手段と、

前記第 1 のポリシー条件が満たされる限り、前記保護コンテンツへのアクセスを与えるための手段と、

を備えるモバイルデバイス。

【請求項 60】

前記モバイルデバイス上に記憶される前記第 1 のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 59 に記載のモバイルデバイス。

【請求項 61】

前記モバイルデバイス上に記憶される前記第 1 のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 59 に記載のモバイルデバイス。

【請求項 62】

前記モバイルデバイス上に記憶される前記第 1 のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 59 に記載のモバイルデバイス。

【請求項 63】

前記モバイルデバイス上に記憶される前記第 1 のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 59 に記載のモバイルデバイス。

【請求項 64】

前記モバイルデバイス上に記憶される前記第 1 のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 59 に記載のモバイルデバイス。

【請求項 65】

前記第 1 のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードするための手段と、

前記第 1 のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、

をさらに備える、請求項 59 に記載のモバイルデバイス。

【請求項 66】

前記第 1 のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項 65 に記載のモバイルデバイス。

【請求項 67】

前記第 1 のパラメータに対する前記更新を SMS メッセージ中で受信し、解析するための手段をさらに備える、請求項 65 に記載のモバイルデバイス。

10

20

30

40

50



## 【請求項 68】

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するための手段をさらに備える、請求項 59 に記載のモバイルデバイス。

## 【請求項 69】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 68 に記載のモバイルデバイス。

## 【請求項 70】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 68 に記載のモバイルデバイス。

10

## 【請求項 71】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 68 に記載のモバイルデバイス。

## 【請求項 72】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも 1 つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 68 に記載のモバイルデバイス。

20

## 【請求項 73】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 68 に記載のモバイルデバイス。

## 【請求項 74】

前記複数のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするための手段と、

30

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、

をさらに備える、請求項 59 に記載のモバイルデバイス。

## 【請求項 75】

前記複数のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項 74 に記載のモバイルデバイス。

## 【請求項 76】

前記複数のパラメータに対する前記更新を SMS メッセージ中で受信し、解析するための手段をさらに備える、請求項 74 に記載のモバイルデバイス。

40

## 【請求項 77】

新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするための手段をさらに備える、請求項 68 に記載のモバイルデバイス。

## 【請求項 78】

モバイルデバイスであって、

少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第 1 のポリシー条件を表す第 1 のパラメータ値を前記モバイルデバイス上に記憶するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを判断するた

50

め的手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、保護コンテンツの個々の各ファイルへのアクセスを許可するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、保護コンテンツの個々の各ファイルについて前記第1のポリシー条件が満たされるかどうかを判断するための手段と、

前記第1のポリシー条件が満たされる限り、保護コンテンツの個々の各ファイルへのアクセスを与えるための手段と、

を備えるモバイルデバイス。

【請求項79】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項78に記載のモバイルデバイス。

【請求項80】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項78に記載のモバイルデバイス。

【請求項81】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項78に記載のモバイルデバイス。

【請求項82】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項78に記載のモバイルデバイス。

【請求項83】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項78に記載のモバイルデバイス。

【請求項84】

前記第1のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記第1のパラメータ値に対する前記更新をダウンロードするための手段と、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第1のポリシー条件を表す前記第1のパラメータ値に対する前記更新を、前記モバイルデバイスの記憶するための前記手段に記憶するための手段と、

をさらに備える、請求項78に記載のモバイルデバイス。

【請求項85】

前記第1のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項84に記載のモバイルデバイス。

【請求項86】

前記第1のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、請求項84に記載のモバイルデバイス。

【請求項87】

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するための手段をさらに備える、請求項78に記載のモバイルデバイス。

【請求項88】

10

20

30

40

50

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 87 に記載のモバイルデバイス。

【請求項 89】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 87 に記載のモバイルデバイス。

【請求項 90】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 87 に記載のモバイルデバイス。

10

【請求項 91】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの一つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 87 に記載のモバイルデバイス。

【請求項 92】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの一つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 87 に記載のモバイルデバイス。

20

【請求項 93】

前記複数のパラメータ値に対する更新が存在するかどうかを判断するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするための手段と、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、

をさらに備える、請求項 87 に記載のモバイルデバイス。

30

【請求項 94】

前記第 1 のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項 93 に記載のモバイルデバイス。

【請求項 95】

前記第 1 のパラメータに対する前記更新を SMS メッセージ中で受信し、解析するための手段をさらに備える、請求項 93 に記載のモバイルデバイス。

【請求項 96】

前記記憶された複数のパラメータ値のいずれかが、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示しているかどうかを判断するために、前記モバイルデバイスが電源投入されるたびに前記複数のポリシー条件を表す前記記憶された複数のパラメータ値の各々を問い合わせるための手段をさらに備える、請求項 87 に記載のモバイルデバイス。

40

【請求項 97】

新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするための手段をさらに備える、請求項 87 に記載のモバイルデバイス。

【請求項 98】

保護コンテンツをモバイルデバイスに提供するためのサーバであって、

保護コンテンツの個々のファイルと、少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第 1 のポリシー条件を表す第 1 のパラメータ値を含むデータベースと、を記憶した大容量記憶メモリ

50

と、

前記大容量記憶メモリに結合され、ワイヤレスネットワークに接続するように構成されたプロセッサであって、

前記モバイルデバイスによる保護コンテンツをダウンロードする要求を受信するステップと、

前記要求に応答して前記保護コンテンツを前記モバイルデバイスに送信するステップと、

少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を前記モバイルデバイスに送信するステップと、

をプロセッサ実行可能ソフトウェア命令によって実行するように構成されたプロセッサと、

を備えるサーバ。

【請求項99】

前記少なくとも第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項98に記載のサーバ。

【請求項100】

前記少なくとも第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項98に記載のサーバ。

【請求項101】

前記少なくとも第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項98に記載のサーバ。

【請求項102】

前記少なくとも第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項98に記載のサーバ。

【請求項103】

前記少なくとも第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項98に記載のサーバ。

【請求項104】

前記プロセッサは、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す前記少なくとも第1のパラメータ値を更新するために前記大容量記憶メモリにアクセスするようにプロセッサ実行可能ソフトウェア命令によって構成される、請求項98に記載のサーバ。

【請求項105】

前記プロセッサは、

前記少なくとも第1のパラメータ値に対する更新が前記大容量記憶メモリ中に存在するかどうかを判断する問合せ要求を前記モバイルデバイスから受信するステップと、

前記更新が存在する場合、前記少なくとも第1のパラメータ値に対する前記更新を行う前記モバイルデバイスに送信するステップと、

をプロセッサ実行可能ソフトウェア命令によって実行するようにさらに構成される、請求項104に記載のサーバ。

【請求項106】

前記プロセッサは、暗号化され認証されたファイルとして前記少なくとも第1のパラメータに対する前記更新を送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、請求項105に記載のサーバ。

【請求項107】

10

20

30

40

50

前記プロセッサは、SMSメッセージを生成し、前記少なくとも第1のパラメータに対する前記更新をSMSメッセージとして送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、請求項105に記載のサーバ。

【請求項108】

前記プロセッサは、前記更新が存在する場合、前記更新が前記モバイルデバイスに対して行われるとすぐに、前記少なくとも第1のパラメータ値に対する前記更新を送信するステップを実行するようにプロセッサ実行可能ソフトウェア命令によってさらに構成される、請求項104に記載のサーバ。

【請求項109】

前記大容量記憶メモリは、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を含む、請求項98に記載のサーバ。

10

【請求項110】

前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項109に記載のサーバ。

【請求項111】

前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項109に記載のサーバ。

20

【請求項112】

前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項109に記載のサーバ。

【請求項113】

前記複数のパラメータ値のうちの1つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項109に記載のサーバ。

【請求項114】

前記複数のパラメータ値のうちの1つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項109に記載のサーバ。

30

【請求項115】

前記プロセッサは、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値の前記各々を更新するために前記大容量記憶メモリにアクセスするようにプロセッサ実行可能ソフトウェア命令によって構成される、請求項109に記載のサーバ。

【請求項116】

前記プロセッサは、  
前記複数のパラメータ値のいずれかに対する更新が前記大容量記憶メモリ中に存在するかどうかを判断する問合せ要求を前記モバイルデバイスから受信するステップと、  
前記更新が存在する場合、前記複数のパラメータ値に対する前記更新を行う前記モバイルデバイスに送信するステップと、  
をプロセッサ実行可能ソフトウェア命令によって実行するようにさらに構成される、請求項115に記載のサーバ。

40

【請求項117】

前記プロセッサは、暗号化されたファイル中で前記複数のパラメータ値に対する前記更新を送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、請求項116に記載のサーバ。

【請求項118】

前記プロセッサは、SMSメッセージを生成し、前記複数のパラメータ値に対する前記

50

更新をSMSメッセージとして送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、請求項116に記載のサーバ。

【請求項119】

前記プロセッサは、新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするステップを実行するようにプロセッサ実行可能ソフトウェア命令によってさらに構成される、請求項109に記載のサーバ。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ソフトウェアアプリケーション、データ、または他のデジタルコンテンツのための時間ベースデジタル著作権管理を生成、管理、変更、および/または実行するための方法およびシステムに関する。

10

【背景技術】

【0002】

デジタル著作権管理(DRM)は、デジタルコンテンツへのアクセスまたはその使用、ならびにデジタルワークまたはデバイスの特定のインスタンスに関連する制限を制御するためにソフトウェア開発者、出版者または著作権保持者によって使用される技術を指す包括的用語である。時間ベースDRMポリシーは、クライアントに、制限された時間期間だけ保護デジタルコンテンツへの無制限アクセスを許可する。効果的であるためには、時間ベースDRMポリシーを実装するプロセッサは信用できるセキュア(secure)時間ソースにアクセスできなければならない。時間ベースDRMポリシーの完全性を維持するためには、信用できるセキュア時間ソースが利用できない場合は、保護コンテンツへのアクセスは許可されるべきではない。しかしながら、そのような限定的なポリシーは、保護デジタルコンテンツへのアクセス権を適切に購入しており、したがって、信用できるセキュア時間ソースが利用できるかどうかにかかわらず、ライセンスが与えられた「制限された時間期間」が経過しない限り、アクセスが許可されるべきであると考えられるクライアントに、フラストレーションを起こさせることがある。

20

【0003】

そのようなクライアントの懸念を緩和するために、時間ベースDRMポリシーの下に保護されたデジタルコンテンツのいくつかのプロバイダは、信用できるセキュア時間ソースが利用できないときでも保護デジタルコンテンツへの継続的アクセスをクライアントに許可することを選ぶことがある。たいていのそのようなプロバイダは、ライセンス期間が満了する前に信用できるセキュア時間ソースが利用できるようになるという仮定の下にそのようにする。そのような代替の時間ベースDRMポリシーは、重大な不正行為を受けやすい。これは、不正なユーザが、「制限された時間期間」のライセンスが永久に通用するようにセキュアでない時間ソースを操作または変更することによって、「制限された時間期間」ライセンスを不適切に延長しようと試みることができるからである。さらに、いくつかの不正なユーザは、ライセンスが満了すべきだったにもかかわらず、保護デジタルコンテンツへの継続的アクセスが許可されるように、信用できるセキュア時間ソースを故意に利用不可能またはアクセス不可能にすることがある。

30

40

【0004】

モバイルデバイスの内部クロックは正確でないか、変更からセキュアでないか、または存在しないことさえあるので、モバイルデバイスは、特に、この脆弱性によって損害を被る。セルラー電話、個人情報端末(PDA)、ワイヤレスモデム、および同様のハンドヘルド通信デバイスは、内蔵式の正確でセキュアなクロックを有しないことがあるモバイルデバイスの例である。さらに、そのようなモバイルデバイスは、すべての状況下でセキュア時間を取り出す信頼できるおよび/またはセキュアな手段を有しないことがある。

【0005】

これらの理由により、時間以外の基準に基づいて、保護デジタルコンテンツの使用またはそれへのアクセスを制限するための代替DRMポリシーが考案されている。そのような

50

代替DRMポリシーの例は、実行の回数、消費のインスタンス、または保護コンテンツへのアクセスを追跡し、制限することを含む。そのような代替DRMポリシーは、時間ベースDRMポリシーの効果的な代替案を保護コンテンツプロバイダに与えるが、潜在的なクライアントは、そのようなDRMポリシーは限定的すぎると結論付けて保護デジタルコンテンツの購入を思いとどまることがある。その結果、デジタルコンテンツの売上げが少なくなる。したがって、保護デジタルコンテンツプロバイダは、信用できるセキュア時間ソースが利用できない場合にクライアントアクセスを許可するが、不正なクライアントによる過大な不正行為を防止する、時間ベースDRMライセンスポリシーのためのより信頼できる方法またはシステムを望むことがある。

【発明の概要】

【0006】

本明細書で提示する方法およびシステムの実施形態は、時間ベースライセンスを用いてデジタルコンテンツ（たとえば、媒体、データ、ゲーム、または他のソフトウェア）を保護するためのフレキシブルなライセンスポリシーを生成、管理、変更、および/または執行する問題の解決策を提供する。実施形態は、信用できるセキュア時間ソースが利用できず、コンテンツを含んでいるモバイルデバイス上に時間クロックが、あったとしても、信用できない、または信頼できない状況を扱う。

【0007】

少数のパラメータによって十分に特徴付けられる多種多様なポリシーを可能にする実施形態が説明される。パラメータの値、したがって選択されるポリシーは、最初に設定され、後で任意の時間において新しいパラメータ値のリモートダウンロードなどによって動的に変更されることができる。パラメータ値は、使いやすさとセキュリティ特性との間の所望の妥協レベルを定義し、執行するように選択されることができる。

【0008】

本明細書に組み込まれ、本明細書の一部をなす添付の図面は、好ましい本実施形態を示し、上記の概略的な説明および下記の詳細な説明とともに、実施形態の特徴を説明するのに役立つ。

【図面の簡単な説明】

【0009】

【図1A】図1Aは、セキュア時間ソースにアクセスできる多数のモバイルデバイスを含むシステムのシステム図である。

【図1B】図1Bは、あるタイプのモバイルデバイスの要素の回路ブロック図である。

【図1C】図1Cは、別のタイプのモバイルデバイスの要素の回路ブロック図である。

【図2】図2は、潜在的なライセンスポリシーパラメータ、それらの考えられる値、および意味の表である。

【図3】図3は、潜在的なパラメータ値のための様々な組合せによって定義される例示的なポリシーを示す表である。

【図4】図4は、パラメータ化時間ベースライセンスポリシーを執行するために執行エージェントによって実行されることができる手順の一実施形態のプロセス流れ図である。

【図4a】図4aは、図4に示されたプロセスを実装する手順のための代替の例示的な可能な擬似コードのリストである。

【図4b】図4bは、パラメータ化時間ベースライセンスポリシーを執行する代替手順のための例示的な可能な擬似コードのリストである。

【図5】図5は、執行エージェントによって実行されることができる手順の代替実施形態のプロセス流れ図である。

【図5a】図5aは、パラメータ化時間ベースライセンスポリシーを執行する手順のための例示的な可能な代替の擬似コードのリストである。

【図6】図6は、TimeCallAtStartupパラメータを採用する実施形態方法によって実行されるステップのプロセス流れ図である。

【図6a】図6aは、セキュアな時間をセキュア時間ソースから得る必要があるかどうか

10

20

30

40

50

を検査する手順のための例示的な可能な代替の擬似コードのリストである。

【図7】図7は、更新されたライセンスパラメータをチェックし、ダウンロードするための実施形態方法によって実行されるステップのプロセス流れ図である。

【図7a】図7aは、更新されたライセンスパラメータを検査し、ダウンロードする手順のための可能な代替の擬似コードリストの一例を提供する。

【発明を実施するための形態】

【0010】

本発明の様々な実施形態が添付の図を参照しながら詳細に説明されるだろう。可能な場合はいつでも、同じまたは同様の部分を指すために図面全体にわたって同じ参照番号が使用されるだろう。

【0011】

ライセンスを与えられた保護コンテンツ、または単に「保護コンテンツ」は、様々な種類の媒体、エンターテインメントレンタル、文書、ソフトウェア、データ、トライアルまたはデモコンテンツなどを含むことができるが、これに限定されない。コピープロテクションおよび保護コンテンツのためのDRMの様々な手法がある。

【0012】

最も一般的なDRMポリシーの1つは、時間ベースライセンスである。そのような時間ベースライセンスの下で、クライアントは、有効期限までなど、制限された時間期間の間、保護コンテンツへの無制限アクセスを許可される。本明細書では、「保護コンテンツにアクセスする」というフレーズおよび同様のフレーズは、コンテンツを閲覧、読み取り、再生、実行、編集、または変更することを包含する。制限された時間期間が経過すると、クライアントはもはや、既存のライセンスの下で保護されたコンテンツへのアクセスを許可されない。

【0013】

代替DRMポリシーは「無限の」ライセンスを備えることができる。保護コンテンツプロバイダは、ライセンス有効日/時を常に監視することを望まない場合、保護コンテンツに対して割増金を課金し、クライアントが保護コンテンツに無期限にアクセスできるようにすることがある。本質的に、クライアントは、制限された時間期間の間のライセンスではなく、所有するために保護コンテンツを購入する。しかしながら、多くの潜在的なクライアントは、意図された使用が制限されるとき、割増価格を支払うことを望まであろうから、そのような保護ポリシーは最適ではないことがある。したがって、保護コンテンツが時間ベースライセンスの下で利用可能である場合よりも、実際に保護コンテンツにアクセスする代金を支払うクライアントとなる潜在的なクライアントは少ないだろう。

【0014】

音楽セレクションへのアクセスをクライアントに与えるコンテンツプロバイダの例を考える。様々なDRMポリシーがコンテンツプロバイダにとって利用可能である。コンテンツプロバイダは、使用規則に基づくポリシーの下で音楽セレクションをクライアントにとって利用可能にすることができる。そのような使用規則は、クライアントがN回、音楽セレクションを再生するか、または音楽セレクションにアクセスできるようにするアクセスカウント制限を備えることができる。あるいは、コンテンツプロバイダは、特定の日付または時間まで音楽セレクションを再生することをクライアントに許すようにする時間ベースの使用制限の下で、音楽セレクションをクライアントにとって利用可能にすることができる。保護コンテンツ（すなわち、音楽セレクション）の性質と、大部分のクライアントがそのような保護コンテンツへのアクセスを選好する方法とのために、クライアントは、音楽セレクションを再生する回数によって制限されることを望まないが、むしろ、セレクションが再生される日数または時間によって制限されるだろう。したがって、そのような状況では、なぜ時間ベースライセンスが選好されるのかがわかる。ユーザが保護コンテンツへの無制限アクセスを望むが、時間とともにその保護コンテンツに飽きると予想することができる、ゲームやビデオなどの保護コンテンツの場合も、同様の状況が生じることがある。

10

20

30

40

50



## 【 0 0 1 5 】

保護コンテンツのための従来の時間ベースライセンスポリシーは、ライセンス有効日/時を、内部クロックによって与えられた時刻や日付の値と比較する。有効日/時とクロックとの比較により、ライセンス有効日/時がまだ経過していないことがわかる限り、プロセッサは保護コンテンツへの無制限アクセスを許可する。比較により、ライセンス有効日/時が経過したことがわかった場合、プロセッサは保護コンテンツへのさらなるアクセスを拒否する。形式は単純であるが、そのようなDRMポリシーおよび保護は、制限された時間期間が事実上無限になるように、不正なクライアントがデバイスクロックを操作することは比較的容易であるので、容易に回避される。PC（または他のデバイス）のクライアントは、制限された時間期間が決して経過しないように、PC（または他のデバイス）の内部クロックを繰り返し「ロールバックする」能力を有することができる。そのような「ロールバック」操作を検出するためのソフトウェアが存在するが、現在まで、そのようなソフトウェアが効果的であるとは判明していない。

10

## 【 0 0 1 6 】

よりロバスタな時間ベースライセンスポリシーでは、時間ベースライセンス有効日/時に対して比較するために使用されるクロックが、正確で確実な改ざん防止時間を何らかの形態で与える信用できるセキュア時間ソースであることを必要とすることがある。そのようなセキュア時間ソースは、モバイルデバイス自体内に配置されることができる。他の場合は、リモートでアクセス可能なセキュア時間ソースが利用されることができる。たとえば、インターネット上のウェブサイトwww.time.govは、クライアントが変更することができない、リモートアクセス可能な、正確で確実な時間ソースである。モバイルデバイスが、ローカルまたはネットワーク上で、信用できるセキュア時間ソースを参照させられる限り、よりロバスタな時間ベースライセンスが効果的に動作することができる。

20

## 【 0 0 1 7 】

モバイル、セルホン、PDA、ワイヤレスモデム、および他のモバイル通信デバイスであることは、一般に、セキュア時間ソースを参照するために必要ではない。CDMAデバイスは、時間保持を厳密に相関させるために使用される時間ソースを有するが、その時間は、クライアントによって変更または改ざんされることができるので、セキュアではないことがある。GSM（登録商標）デバイス中の時間は独立して提供または制御されるので、GSMデバイスは、時間の概念を有しないことがある。したがって、時間ベースDRMポリシーは、そのようなデバイス上で事実上執行することが困難であることがある。

30

## 【 0 0 1 8 】

一実施形態は、保護コンテンツへのアクセスが許可される前に、セキュア時間がライセンス有効日/時に対する比較のために利用可能であることを強要することができる、限定的なDRMポリシーを備えることができる。そのような強要は、クライアント/ユーザにフラストレーションを与えることがある。第1に、セキュア時間ソースがローカルで利用可能でない場合、外部のセキュア時間ソースを得るためにデータ呼が必要になることがある。このデータ呼は、保護コンテンツへのアクセスを遅延させ、データ呼が成功しない場合、クライアント/ユーザにフラストレーションを与えることがある。第2に、クライアントが、適切にライセンスを与えられた保護コンテンツにアクセスすることを望んでいるが、クライアント/ユーザの制御を超えるという理由のために、セキュア時間ソースが利用できない多くの状況があることがある。そのような状況の例は、モバイルデバイスが、内部のセキュアなクロックなしに、そのサービスプロバイダネットワークの外側に地理的に配置される場合である。クライアント/ユーザが移動しており、そのサービスプロバイダネットワーク外に出ることがあると、そのような状況が生じることがある。この状況は「ネットワーク外(out of network)」と呼ばれる。モバイルデバイスがネットワーク外であるので、モバイルデバイスは、少なくともローミングなしに、モバイルデバイスがセキュア時間ソースとのデータリンクを生成できるようにする信号を得ることができないだろう。

40

50

## 【 0 0 1 9 】

そのような状況の別の例は、モバイルデバイスが、内部のセキュアなクロックなしに、そのサービスプロバイダネットワーク内に地理的に配置されるが、クライアントがモバイルデバイスのトランシーバ機能を使用不能にしたときである。クライアント/ユーザが、モバイルデバイスのトランシーバ機能を使用不能にする必要がある位置に入ったとき、そのような状況が生じることがある。たとえば、クライアント/ユーザが飛行機上または病院内にいるときである。この状況は「ネットワーク内 (in network)」と呼ばれる。モバイルデバイスのトランシーバ機能が使用不能になったので、モバイルデバイスは、モバイルデバイスがセキュア時間ソースとのデータリンクを生成できるようにする信号を得ることができないだろう。

10

## 【 0 0 2 0 】

そのような状況の別の例は、モバイルデバイスが「ローミングモード」にあるときである。クライアント/ユーザがその特定のサービスプロバイダネットワークの外側を移動しているが、依然として別のサービスプロバイダネットワーク内にあるとき、そのような状況が生じることがある。モバイルデバイスは、ローミングモードにあるとき、電話通話を行い、受信することができるが、セキュア時間ソースとのデータリンクを確立することができない。

## 【 0 0 2 1 】

クライアント/ユーザは、保護コンテンツが適切にライセンスを与えられ、有効日/時が経過していないにもかかわらず、これらの状況で保護コンテンツへのアクセスが許可されないことにフラストレーションを感じることもある。そのようなフラストレーションは、クライアント/ユーザが、否定的な経験のために将来の時間ベースライセンスを実行するのを思いとどまらせることがある。

20

## 【 0 0 2 2 】

代替実施形態は、上述の状況が本質的に一時的なものであり、延長された時間期間の間、またはライセンス有効日/時を超える時間期間の間に生じる可能性がないという仮定の下で、セキュア時間が利用できないにもかかわらず、クライアント/ユーザに保護コンテンツにアクセスすることを許すことができる。しかしながら、そのような代替実施形態は、ライセンスを与えられる時間期間が事実上無限になるように、引き延ばされた時間期間の間、上記の状況のいずれかを意図的に生成する不正なクライアントによって利用されることがある。

30

## 【 0 0 2 3 】

したがって、特にマルチモードデバイス（たとえば、CDMAおよび/またはGSM環境のいずれかにおいて動作することができるデバイス）およびマルチモード市場において使用するための、クライアント/ユーザ経験を保持しながら保護コンテンツへの限定的なアクセスを与えるライセンスポリシーの柔軟な選択肢が望まれる。コンテンツプロバイダも、時間ベースライセンスを延長または変更することを含む、販売後に保護ポリシーを動的に変更する能力を望んでいる。さらに、ワイヤレスデバイス製造業者およびサービスプロバイダには、工業の現場で、または販売時に、デフォルトのポリシーまたは調整されたポリシーを構成することが可能であることが望ましい。したがって、時間ベースDRMポリシーを生成、管理、変更、および/または実行するための代替方法およびシステムが必要である。

40

## 【 0 0 2 4 】

代替実施形態は、信用できるセキュア時間ソースが利用できず、コンテンツを含んでいるモバイルデバイス上に時間クロックが、あったとしても、信用できない、または信頼できない状況を扱う。様々な実施形態は、比較的少ない数のパラメータの構成値に基づく改善された時間ベースライセンスおよびDRMポリシーを与える。そのような実施形態は、特に、正確で信用できる時間を与えるセキュア時間ソースが常に利用可能ではない時間ベースポリシーを対象とする。実施形態は、セキュア時間が利用可能であるか利用可能でないかに基づいて時間ベースポリシーを執行する適応型執行エージェントを含むことができ

50

る。

【 0 0 2 5 】

数個の精選されたパラメータが、広範囲の柔軟な D R M ポリシーを生成し、制御するために使用されることができる。広範囲の柔軟な D R M ポリシーは、変動するセキュリティレベルと、逆に関係することがあるクライアント / ユーザ経験の変動する程度とを与えることができる。たとえば、非常に強いセキュリティレベルを有するポリシーは、クライアント / ユーザ経験に対して極めて悪いレーティングを有することがある。反対に、「可 ( okay ) 」セキュリティレベルを有するポリシーは、クライアント / ユーザ経験に対して「極良 ( very good ) 」レーティングを有することがある。ライセンスパラメータの様々な置換は、ポリシーのスペクトルを生成することができる。ほんの数個のパラメータを使用することは、保護コンテンツの多数のアイテムに対するライセンスが、モバイルデバイスのメモリ中にコンパクトに含められることができるということを意味する。これは、モバイルデバイス上の単一の比較的単純でセキュアな実行エージェントが、D R M の多くまたはすべての要求を処理することを可能にする。

10

【 0 0 2 6 】

一般に、ロバスタな D R M 保護は、クライアントの経験に影響を及ぼすことができる遅延、使用制限、または他の不便を生じることがある。たとえば、セキュア時間を得るためにサービスプロバイダネットワークへのワイヤレスデータ呼が必要になることは、D R M 保護方式を改善するだろうが、クライアントの保護コンテンツへのアクセスを遅延させることになるだろう。また、セキュア時間を取り出すために必要とされるワイヤレスエアタイムは、クライアントが諒解しないであろう追加コストを必要とすることがあり、特に保護コンテンツへの各アクセスがそのような通話を必要とする場合、アクセスが頻繁になり、クライアントは各時間取り出し呼を承認しなければならない。クライアントの経験を改善するために、たとえば、モバイルデバイスが最初に電源投入されたときのみ、異なるパラメータによって生成されたポリシーがセキュア時間へのアクセスを必要とすることができる。

20

【 0 0 2 7 】

以下のパラグラフは、特定のパラメータを用いた実施形態、パラメータ値の組合せに基づくポリシーの例、およびパラメータ値の特定の組合せによって特徴付けられたポリシーを執行するための手順を説明する。論じられる特定のパラメータは、説明のためにのみ与えられるものであり、本発明の範囲または特許請求の範囲を限定するものではない。

30

【 0 0 2 8 】

図 1 A は、時間ベースライセンスが動作することができるシステムの一実施形態を示す。サービスプロバイダネットワーク 2 0 1 は、ワイヤレスボイスおよび / またはデータ通信をサポートする。サービスプロバイダネットワーク 2 0 1 は、C D M A ( 符号分割多元接続 ( Code Division Multiple Access ) )、G S M ( モバイル通信のためのグローバルシステム ( Global System for Mobile Communications ) )、ユニバーサルモバイル通信システム ( Universal Mobile Telecommunications System ) ( U M T S )、または他のワイヤレス技術を採用することができる。モバイルデバイス 1 0 0、2 0 0 とサービスプロバイダネットワーク 2 0 1 との間の双方向無線通信は、基地局 2 0 5 を介して行われる。サービスプロバイダネットワーク 2 0 1 は、当該サービスプロバイダネットワーク 2 0 1 を介してモバイルデバイス 1 0 0、2 0 0 に対してアクセス可能な、確実に正確なセキュア時間ソース 2 0 2 にアクセスすることができる。

40

【 0 0 2 9 】

例示的なモバイルデバイス 1 0 0 が図 1 B に、より詳細に示されている。モバイルデバイス 1 0 0 は、エインターフェース 1 0 1 と、セキュアクロック 1 0 2 と、命令プロセッサ 1 1 0 と、メモリ 1 1 1 と、を含むことができ、それらはハードウェア、ソフトウェア、またはそれらの組合せで実装できる要素である。エインターフェース 1 0 1 は、C D M A ( 符号分割多元接続 ( Code Division Multiple Access ) ) インターフェース、G S M ( モバイル通信のためのグローバルシステム ( Global System for Mobile Communica

50

tions) ) インターフェース、CDMAとGSMとをサポートするマルチモードインターフェース、またはこれらのワイヤレスインターフェースのうちの1つの後続派生物とすることができる。セキュアクロック102は、ローカルセキュア時間ソースを与えることができる。モバイルデバイス100は、サービスプロバイダネットワーク201を介してアクセス可能なシステムセキュア時間ソース202を使用して、時々ローカルセキュアクロック102をセキュアに更新することができる。命令プロセッサ110は、1つまたは複数のマイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、またはそれらの任意の組合せとすることができる。メモリ111は、プロセッサ命令および/またはデータのソースとして命令プロセッサ110によってアクセス可能である。メモリ111は、ランダムアクセスメモリ(RAM)、読み取り専用メモリ(ROM)、フラッシュメモリ、プログラマブル読み取り専用メモリ(PROM)、消去可能電氣的プログラマブルメモリ(EEPROM)、消去可能読み取り専用メモリ(EPROM)、ディスクドライブメモリ、などの任意の組合せを含むことができる。命令プロセッサ110は、エアインターフェース101への、セキュアクロック102への、メモリ111の1つまたは複数の部分への、および/または入力/出力ユニットなどのモバイルデバイス100の他のリソースへの、アクセスを制御することができるハードウェアを含むことができる。

10

#### 【0030】

メモリ111に記憶されるのは、命令プロセッサ110によって実行されるべき命令、および/または命令プロセッサ110によって実行される命令によってアクセスされるべきデジタルデータであることができる。命令およびデータは、オペレーティングシステム(OS)103と、ライセンス実行エージェント104と、ライセンスパラメータ105と、1つまたは複数のアプリケーションプログラム106と、保護コンテンツ107、108のアイテムと、を含むことができる。オペレーティングシステム103は、モバイルデバイス100の基本動作を制御する命令のセットである。オペレーティングシステム103は、ライセンスパラメータ値105を含むメモリ111のいくつかのセキュアな部分、および/またはメモリ111に記憶された保護コンテンツ107、108の1つまたは複数のインスタンスへのクライアントアクセスを制御することができる。オペレーティングシステム103自体は、保護コンテンツ107、108のセキュリティを執行するためにクライアントからセキュアでなければならない(すなわち、改ざん防止されていなければならない)。保護コンテンツ107、108のアイテムごとにライセンスパラメータ値の別々のセットがあることができる。代替実施形態では、パラメータ値の1つのセットは、保護コンテンツ107、108の2つ以上のアイテムに適用することができる。オペレーティングシステム103は、ライセンスパラメータ105への特権的なアクセスなど、メモリ111のいくつかのセキュアな部分への特権的なアクセスをライセンス実行エージェント104に許可することができる。1つまたは複数のアプリケーションプログラム106の実行は、該アプリケーションプログラム106が実行することができるかどうかを含めて、オペレーティングシステム103の制御下で行われることができる。オペレーティングシステム103はまた、アプリケーション106がハードウェアリソースおよびメモリ111にアクセスすることができるかどうかを制御することができる。たとえば、オペレーティングシステム103は、メモリ111の連続するアドレスの様々なブロックを、実行可能、読み書き、読み取り専用、またはアクセス不可能であるとして動的に制限する、プロセッサ110中のハードウェアを制御することができる。

20

30

40

#### 【0031】

セキュアなローカルクロックを含まない別の例示的なモバイルデバイス200が、図1Cに示される。図1Cに示されるモバイルデバイス200は、図1Bに示されるモバイルデバイス100の要素の機能と同様の機能をもつ要素を含む。ローカルセキュアクロックまたは均等物のないモバイルデバイス200は、ローカルセキュア時間ソースを有しない。しかしながら、モバイルデバイス200は、命令プロセッサ110中で実行される、メモリ111に記憶されたソフトウェア命令によって制御されるように、エアインターフェ

50

ース101を介してサービスプロバイダネットワーク201にデータ呼を発することによってセキュア時間を得ることが可能であるだろう。

【0032】

このデータ呼は、様々な方法で達成されることができる。モバイルデバイス200は、ワイヤレスデータパケットとしてセキュア時間データを受信するためにソースセキュア時間とのデータ通信リンクを確立することができる特定の番号に、セルラー電話呼を発することができる。あるいは、モバイルデバイス200は、ブラウザを開き、セキュア時間ソースのIPアドレスにアクセスすることによってセキュア時間ソースに接続する、インターネットへのワイヤレス接続を介したセキュア時間ソースへの接続を確立することができる。第3の代替案として、セキュア時間を帰すことができるアドレスに特別SMSメッセージを送信し、それに応じたSMSメッセージを待つことによって、データ呼が達成されることができる。セキュア時間ソースを呼び出すためのこれらの代替方法の各々は、命令プロセッサ110中で実行される、メモリ111に記憶されたソフトウェア命令によって制御されるエアインターフェース101によって管理されることができる。本明細書における「データ呼」への言及は、これらの代替案の各々、およびモバイルデバイスが確立することができるセキュア時間ソースとの任意の他のワイヤレスデータ通信リンクを包含するものとする。

【0033】

サービスプロバイダネットワーク201がデータ呼の一部として帰すセキュア時間も、クライアントが受信された時間を改ざんすることができないようにするためにセキュアでなければならない。オペレーティングシステム103は、データ呼のセキュリティ、またはデータ呼中にデータとして帰されるセキュア時間のセキュリティを守らせることができる。たとえば、セキュア時間のセキュリティは、データ呼中のデータを認証することによって与えられることができる。時間データの認証は、時間データのデジタル署名またはハッシュ関数ベースのメッセージ認証コード(HMAC)を含むことによって、これらのよく知られている認証方法を使用して達成されることができる。さらに、時間データは、よく知られている暗号化方法を使用して暗号化されることができる。あるいは、オペレーティングシステム103は、クライアントが、データ呼中に帰されるセキュア時間を傍受または改ざんする方法がないようにすることができる。たとえば、オペレーティングシステム103は、直接的または間接的に、任意のアプリケーションプログラム106へのコマンドまたは入力を介した、あるいはクライアントにとって利用可能なモバイルデバイス200の通常の機能を介した、データ呼へのクライアントアクセスを防ぐことができる。

【0034】

任意の数のモバイルデバイスが、1つまたは複数の基地局205を介してサービスプロバイダネットワーク201と通信することができる。様々な実施形態の説明を簡単にするために、参照は、モバイルデバイスの2つのクラス、すなわちセキュアクロックを有する1つのクラス(モバイルデバイス100)と、セキュアクロックがない1つのクラス(モバイルデバイス200)とを表すモバイルデバイス100およびモバイルデバイス200になされるだろう。

【0035】

保護コンテンツ107、108のアイテムは、ライセンスパラメータ値105の記憶されたセットによって特徴付けられたライセンスポリシーによって保護される。パラメータ値105は、モバイルデバイスのメニューオプションまたは通常の機能を介してクライアントアクセス可能ではない、メモリ111のセキュアな部分に記憶されることができる。その方法では、クライアントは、パラメータ値105によって特徴付けられたライセンスポリシーの設定を無効にするようにパラメータ値105を変更することはできない。したがって、ライセンスパラメータ105は、クライアントの改ざんからセキュアであると考えられる。

【0036】

保護コンテンツ107、108へのアクセスは、ハードウェア、ファームウェア、ソフ

10

20

30

40

50

トウェア、および/またはそれらの組合せで実施されることができる、執行エージェント 104 によって管理されることができる。サービスプロバイダネットワーク 201 は、データが、オペレーティングシステム 103 に、または、モバイルデバイス 100、200 上で実行中のライセンス執行エージェント 104 に送信される、モバイルデバイス 100、200 とサービスプロバイダネットワーク 201 との間のセキュアなデータ呼などを介して、パラメータ値を変更することができる。執行エージェント 104 はまた、不正なユーザによる改ざんに対してセキュアでなければならない。たとえば、執行エージェント 104 は、メモリ 111 のセキュアな部分に記憶された、プロセッサ 110 のための命令とすることができる。

#### 【0037】

執行エージェント 104 の主要な義務は、保護コンテンツ 107、108 のアイテムへのアクセスが、ライセンスパラメータ値が表すライセンスポリシーの下で許可されることを検証することである。執行エージェント 104 は、一般に、特権的でセキュアなプロセッサ状態で動作し、特に保護コンテンツ 107、108 のためのライセンスパラメータ値 105 を含んでいる、メモリ 111 の少なくともいくつかのセキュアな部分にアクセスできる。ライセンスパラメータ値をメモリ 105 のセキュアな部分中に保持することは、不正なユーザが、保護コンテンツ 107、108 の 1 つまたは複数のアイテムの保護を回避するようにライセンスパラメータ値を変更することを防止するのに必要である。執行エージェント 104 は、保護コンテンツ 107、108 自体へのアクセスを必要としないことができる。

#### 【0038】

一方、アプリケーションプログラムは、通常、オペレーティングシステム 103 によって割り当てられる特権の制限されたセットの下で動作し、したがって、メモリ 111 のセキュアな部分中のライセンスパラメータ値 105 にアクセスすることができない。アプリケーションプログラムは、保護コンテンツ 107、108 にアクセスすることはできるだろうが、保護コンテンツ 107、108 へのアクセスが許可されることを確認するために、保護コンテンツ 107、108 に関連するライセンスパラメータ値 105 が執行エージェント 104 によって最初に使用された後のみである。ライセンスパラメータ値 105 がもはや有効ではないライセンスを表すと執行エージェント 104 が判断した場合、保護コンテンツ 107、108 へのアクセスは阻止される。執行エージェント 104 が保護コンテンツ 107、108 へのアクセスを許す場合、執行エージェント 104 は、アプリケーションプログラム 106 に一時的に保護コンテンツ 107、108 へアクセスを許すことを、オペレーティングシステムに通知することができる。

#### 【0039】

執行エージェント 104 の例は、Qualcomm の BREW システムである。BREW ベースのアプリケーションは、たとえば、必要とされるリソースにアクセスするために必要な特権を用いて、(Qualcomm またはコンテンツプロバイダによって) デジタル署名されることができる。したがって、アプリケーションは、それらの特権の下でアクセス可能なリソースにしかアクセスすることがない。したがって、BREW は、少なくとも最初に、ポリシーパラメータのメモリへの書込みアクセスからアプリケーションを除外し、保護コンテンツを含むメモリへのすべてのアプリケーションアクセスを除外することができる。

#### 【0040】

執行エージェント 104 は、セキュアクロック 102 が存在する場合、セキュアクロック 102 へのアクセスを必要とすることがある。セキュア時間は、好ましくはデバイス上で維持されるが、ネットワーク接続が確立されることができ、セキュア時間ソース 202 からのセキュア時間が利用可能であるときはいつでも、デバイスは、少なくとも、要求に応じて時間を取り出すまたは更新することが可能であるだろう。執行エージェント 104 によって執行されるライセンスポリシーは、セキュア時間が利用可能でない場合、およびデバイスのネットワーク接続がカバレッジ内 (in-coverage)、カバレッジ外 (outside-c

10

20

30

40

50

overage)、またはローミング中であるとき、どのように反応すべきかなど、様々な場合を記述することができる。

【0041】

図2の表は、ライセンスパラメータの例、それらの取り得る値、およびそれらの意味の簡単な説明を列記している。図2は、網羅的なものではないが、ライセンス方式を定義または説明するために使用されることができる潜在的なパラメータを示すための例示的なものにすぎない。図2で識別される第1のパラメータは、ライセンスが通常的时间ベースDRMポリシーの下で期限切れになる日の日付および/または時間とすることができるExpirationDateである。この値は、従来の時間ベースライセンスDRMデータファイル中の有効日付または有効時間と同様である。

10

【0042】

図2で識別される第2のパラメータは、TimeCallAccessである。このパラメータは、保護コンテンツ(たとえば、107、108)にアクセスする前に、ライセンス実行エージェント104が最初にデータ呼などを介して、セキュア時間ソース202からセキュア時間を正常に取り出さなければならないかどうかを規定することができる。当然、内部セキュアクロック102はセキュア時間ソースを構成するので、セキュアクロックが利用可能であり、正しく維持される(これらの更新がまれな場合でも、さらにセキュアクロックはどこかからの入力を必要とする)場合、そのようなデータ呼は不要になるだろう。モバイルデバイス200がセキュア時間を取り出すためにデータ呼を行う必要がある(たとえば、デバイスが内部セキュアクロック102を有さず、TimeCallAccess = 「1」である)場合、クライアントは、モバイルデバイス200がリモートセキュア時間ソース202と通信するためにデータ呼を発することによって生じた、保護コンテンツへのアクセスの遅延によって不便を感じることもある。そのような遅延がクライアントにとって不便であり、ユーザ/クライアント経験を劣化させることがあるが、そのような基準は、不正使用からの保護コンテンツのロバストな保護を保証するのに必要であるだろう。時間ベースライセンスに従って、意図された動作が進行する前にアクセスが許可されたかどうかを判断するために、有効日/時ExpirationDateが、セキュア時間ソースから取り出されたセキュア時間と比較される。

20

【0043】

サービスプロバイダは、セキュア時間がモバイルデバイス200にとって一時的に利用できなくても、制限的に使用保護コンテンツにアクセスし続ける能力をクライアントに与えることを望むことがある。クライアントのモバイルデバイス200が、サービスプロバイダネットワークカバレッジエリア201内であるが、セキュア時間ソース202からのセキュア時間にアクセスすることができない(すなわち、カバレッジ内の)場合、クライアントは、保護コンテンツへの制限された数の「猶予期間(grace period)」アクセスを許可されることができる。たとえば、訪問客は、病院内にいる間、セルラー電話の電源をオフにするようにしばしば要求される。別の例として、航空機が飛んでいる間、航空機の乗客はモバイルデバイス200の送信機部分を使用不能にすることを要求される。また、何らかの建築物または地下鉄システムの中にあるときに、モバイルデバイス200は、サービスプロバイダネットワーク201から信号を受信することができないことがある。さらなる一例として、「猶予期間」ライセンスを用いて、これらの状況の各々におけるクライアントは、ワイヤレス機能がオフにされてもモバイルデバイス200上で動作する、ライセンスを与えられたゲーム、音楽、ビデオ、アプリケーションなどを依然として使用することができる。これらの例では、モバイルデバイス200は、サービスプロバイダネットワーク201のカバレッジ内であることができるが、ワイヤレス機能が使用不能にされるか、または信号が構造によって阻止されるので、セキュア時間ソース202からのセキュア時間にアクセスすることができない。あるいは、ワイヤレスデバイスがサービスプロバイダネットワーク201のカバレッジの外側である場合、ワイヤレス機能が使用不能であるかどうかにかかわらず、セキュア時間ソースからのセキュア時間は利用できないことがある。どちらの場合にも、クライアントは、保護コンテンツへの制限されたアクセスを

30

40

50

許可されることができる。

【0044】

図2に示されるInCoverageUseLimitパラメータは、モバイルデバイス200がサービスカバレッジエリア内である状況に対して、「猶予期間」使用の数（または時間）における制限を規定するパラメータである。このカバレッジ内猶予期間パラメータは、モバイルデバイス200がサービスプロバイダネットワーク201カバレッジの内側であるが、モバイルデバイス200がセキュア時間ソースからの時間を正常に取り出すまたは検証することができない間、保護コンテンツがアクセスされることができる最大回数を表すための非負整数値Mを有する。

【0045】

図2に示されるOutCoverageUseLimitパラメータは、モバイルデバイス200がサービスカバレッジエリアの外側（すなわち、カバレッジ外）である状況に対して、「猶予期間」使用の数（または時間）における制限を規定する、同様のパラメータである。このカバレッジ外猶予期間パラメータは、モバイルデバイス200がサービスプロバイダネットワーク201カバレッジエリアの外側であり、モバイルデバイス200がセキュア時間ソースからの時間を正常に取り出すまたは検証することができないとき、保護コンテンツがアクセスされることができる最大回数を表すための非負値Nを有する。

【0046】

InCoverageUseLimitおよびOutCoverageUseLimitパラメータによって特徴付けられる時間ベースライセンスでは、執行エージェント104内の猶予期間アクセスカウンタは、セキュア時間が利用できない間、保護コンテンツがアクセスされる回数を追跡する。カバレッジエリア中、およびカバレッジエリアの外側である間、利用可能なセキュア時間なしに行われるアクセス数をカウントするための別々のカウンタがあることができる。セキュア時間が利用できない間、保護コンテンツがアクセスされるたびに、アクセスが許可されるかどうかを判断するために、適宜にMまたはNの値が、関連する猶予期間カウンタと比較されることができる。また、保護コンテンツの個々のアイテムごとに、別個の猶予期間カバレッジ内アクセスカウンタおよびカバレッジ外アクセスカウンタがあることができる。言い換えれば、別々の猶予期間カウンタは、セキュア時間が利用できないときにアクセスされる曲、ゲーム、ビデオ、またはアプリケーションプログラムごとに増分されることができる。あるいは、クライアントが任意のタイプの保護コンテンツにアクセスした回数をカウントするために単一のカウンタが実装されることができる。

【0047】

保護コンテンツ（たとえば、107、108）にアクセスしたいというクライアントの要求時に、執行エージェント104は、適切な猶予期間カウンタのカウントを、対応する限界値MまたはNと比較する。カウンタが限界値（すなわち、MまたはN）以上である場合、執行エージェント104は、保護コンテンツへのアクセスを禁止する。さもなければ、執行エージェントは、適切な猶予期間カウンタを増分し、保護コンテンツにアクセスし続けることができるようにする。このようにして、セキュア時間が利用できないとき、クライアントは保護コンテンツへの制限されたアクセス数を許可される。アクセス試行の数が所定の制限を超えると、セキュア時間がセキュア時間ソースから利用可能になるまで、さらなるアクセスは拒否される。

【0048】

カバレッジ内およびカバレッジ外アクセス状況に対して、別々の制限（MおよびN）およびカウンタを設けることによって、ライセンサーは、1つの制限および1つのカウンタしかない場合に考えられるDRMポリシーよりも柔軟なDRMポリシーを提供することができる。たとえば、ライセンサーは、セキュア時間がなぜアクセス可能でないかについて仮定し、アクセスできないことについての考えられる理由を区別するように時間ベースライセンスポリシーを巧みに作る（craft）ことができる。たとえば、ライセンスポリシーの作成者が、ライセンスの有効期限の後にモバイルデバイス200がサービスプロバイダ

10

20

30

40

50



ネットワーク 201 カバレッジの外側にあるように見えるように、クライアントがモバイルデバイス 200 を意図的に遮蔽することができる場合、DRM ポリシーは、ライセンスによって対象とされる保護コンテンツへのアクセス数を制限するように巧みに作られることができる。ポリシーの作成者が、カバレッジ内のモバイルデバイス 200 がリモートセキュア時間ソース 202 に確実にアクセスすることができないことを懸念する場合、ポリシーは、使用保護コンテンツへのアクセス数をより大きくできるように設定されることができる。

【0049】

代替実施形態は、クライアントのモバイルデバイス 200 がカバレッジ内かまたはカバレッジ外かにかかわらず、セキュア時間が利用できないときはいつでも採用される、単一の猶予期間制限および関連するアクセスカウントカウンタを設けることができる。

10

【0050】

一実施形態では、セキュア時間が利用可能ではなかった間の期間（保護コンテンツへのアクセス数）の後、セキュア時間が再び利用可能になるときはいつでも、様々な猶予期間カウンタがリセットされることができる。セキュア時間が利用可能になると、実行エージェント 104 は、対応するライセンスの期間が依然として有効か、まだ期限切れになっていないかどうかを判断することができる。ライセンスが期限切れになっていない場合、実行エージェント 104 は、それに応じて猶予期間カウンタをリセットすることができる。

【0051】

セキュア時間が利用可能になる場合、および実行エージェント 104 が現在の時間が有効期限を過ぎている、すなわち、ライセンスが期限切れになったと判断した場合、実行エージェント 104 は、使用保護コンテンツ（たとえば 107、108）および/またはライセンスパラメータ（たとえば、105）を明示的に非活動状態にするか、またはさらにメモリ 110 から削除することができる。あるいは、実行エージェント 104 は、関連するコンテンツ（107、108）が、カバレッジ内またはカバレッジ外にかかわらず、いかなる状態の下でもアクセスされることができないように、期限切れになったことを発見されたライセンスのポリシーパラメータ（105）を変更することができる。たとえば、すべてのさらなるアクセスを防止することは、M および N を 0 に設定することによって達成されることができる。クライアントが保護コンテンツ（107、108）にアクセスしようとするときはいつでも、モバイルデバイス 100、200 は、クライアントにその状況について通知し、また、ライセンスを更新するようにクライアントに奨励することができる。サービスプロバイダは、ライセンスを更新し、更新されたライセンスパラメータ値をダウンロードするクライアントフレンドリな方法をさらに与えることができる。

20

30

【0052】

図 2 に列記された別のパラメータは、モバイルデバイスがローミングモードであり、セキュア時間が利用可能ではない状況を別々に扱うように TRUE または FALSE の値を有することができる Use In Coverage For Roaming である。別々のローミングライセンスパラメータを設けることは、ライセンサーに、ライセンサーが移動しており、したがって、データ呼をセキュア時間ソースに発することからのより高いエアタイム料金に直面することになるだろう一般的な状況を扱うことを許す。ライセンサーに対してより高いコストを課するよりはむしろ、カバレッジ外またはカバレッジ内の状況としてその状況を扱うように、DRM ライセンスが巧みに作られることができる。このパラメータが採用されると、パラメータの値が TRUE である場合、モバイルデバイスがローミングモードであり、セキュア時間が利用可能ではないときに、ポリシーのカバレッジ内部分適用される。したがって、モバイルデバイスがローミングモードであるとき、実行エージェント 104 は、使用を制限するための In Coverage Use Limit パラメータ M を使用して、モバイルデバイスがカバレッジ内であるが、セキュア時間が利用可能ではない（たとえば、ワイヤレス機能が使用不能にされた）かのように、使用ポリシーを執行するだろう。あるいは、パラメータの値が FALSE に設定された場合、モバイルデバイスがローミングモードであり、セキュア時間が利用可能でないとき、カバレッジ外

40

50

ポリシーが適用され、したがって、OutCoverageUseLimitパラメータNの使用を実施する。または、第3の猶予期間制限（たとえば、RoamCoverageUseLimit）および関連するアクセスカウントカウンタ（たとえば、RoamUsesRemaining）は、モバイルデバイス200がローミング中である状況に固有のライセンス期間を与えるように実装されることができる。さらなる実施形態では、UseInCoverageForRoamingパラメータの代わりに、RoamCoverageUseLimitが使用されることができる。

#### 【0053】

TRUEまたはFALSEとすることができる、図2に列記された最後のパラメータTimeCallAtStartupは、モバイルデバイスの電源がオンにされたとき、モバイルデバイスがセキュア時間を取り出そうとすべきかどうか特定するために設けられることができる。このパラメータがTRUEである場合、執行エージェント104は、保護コンテンツへのアクセスが湯ねされることができる前、起動時にセキュア時間を取り出さなければならない。モバイルデバイス100の起動時のデータ呼は、電源がオフの間、モバイルデバイス100上のセキュアクロック102が時間を見失うことがあるので、または電源がオフの間、セキュア時間が信頼できなくなることがあるので、要求されることができる。

10

#### 【0054】

執行エージェント104は、ネットワーク201を介して、オペレーティングシステム103、プロセッサ110およびエアインターフェース101によってSMSテキストメッセージなどの特別データメッセージを送信することによって、セキュア時間を取り出すためのデータ呼を開始することができる。特別データメッセージは、セキュア時間ソース202に宛てられることができ、セキュア時間ソース202がセキュア時間の要求として認識する特定のフォーマットを有することができる。執行エージェント104からのメッセージに回答して、セキュア時間ソース202は、SMSメッセージデータペイロード中にセキュア時間を含む回答SMSメッセージを執行エージェント104に送信することができる。回答メッセージ自体は、セキュア時間のセキュリティを維持するために、何らかの形式のセキュリティを採用しなければならない。回答メッセージは、回答メッセージ中に含まれるデータを暗号化し、認証することによって保全されることができる。執行エージェント104がセキュア時間を受信すると、そのセキュア時間がセキュアクロック102を更新するために使用されることができる。

20

30

#### 【0055】

TimeCallAtStartupパラメータは、「要求に応じて」（すなわち、保護コンテンツへのアクセスが要求された時点で）適用される他のライセンスパラメータとは異なる。ライセンスパラメータTimeCallAtStartupが、メモリ111中のすべてのライセンスパラメータ105によって表されるライセンスポリシーのいずれかに対して真の場合、執行エージェント104は、モバイルデバイス100、200が起動または電源投入された直後に、セキュア時間を収集しなければならない。ライセンスパラメータTimeCallAtStartupの使用は、他のライセンスパラメータと相互に排他的でなく、DRMライセンスのロバストネス（robustness）を向上させるために、他のパラメータとともに使用されることができる。TimeCallAtStartupは、いくつかの保護コンテンツライセンスポリシーに対して真であることができるが、すべてに対して真というわけではないので、モバイルデバイス100、200が起動した直後、執行エージェント104は、メモリ111中のすべてのライセンスパラメータ105を走査することが必要であることがある。ライセンスパラメータTimeCallAtStartupが少なくとも1つのライセンスポリシーに対して真の場合、執行エージェント104は、内部セキュア時間ソースについて確認しなければならない、それが存在しない場合、セキュア時間ソース202からセキュア時間を収集しようとしてデータ呼を発する。TimeCallAtStartupの真値をテストするためにライセンスパラメータ105を走査するための手順は、図6および図6aを参照しながら後述される。

40

50

## 【0056】

パラメータ `TimeCallAtStartup` の実装は、内部セキュア時間ソースなしのモバイルデバイス 200 がセキュア時間を取り出すためにデータ呼を行う要件により、クライアントに起動時に遅延を経験させることによって、ユーザ/クライアント経験を劣化させることがある。さらに、クライアント/ユーザは、保護コンテンツへのアクセス要求が行われなかったときにデータ呼がなぜ必要であるかについて混乱させられることがある。とはいえ、そのような手段は、不正な使用から保護コンテンツの保護のロバストネスを保証するために、いくつかのライセンスプロバイダによっては必要であると考えられることができる。起動時のデータ呼は、ユーザ/クライアントにとって邪魔で面倒であると考えられることができるが、保護コンテンツへのアクセスが要求されるたびにデータ呼が行われることを必要とするよりも、起動時の単一のデータ呼のほうが邪魔ではなく、または面倒ではないだろう。起動時のデータ呼と、各アクセス要求時のデータ呼の両方を必要とすることによって、保護機構は補強されるが、ユーザの経験が犠牲になる。

10

## 【0057】

図 2 に列記されたパラメータなどの少数のパラメータに値を割り当てることだけによって、ユーザの経験への邪魔に対してセキュリティをバランスさせるために使用されることができる、柔軟な時間ベースライセンスが特徴付けられることができる。図 3 は、図 2 の潜在的なパラメータのための値の様々な組合せが様々なポリシーをどのように特徴付けることができるかを示す。次に、選択された例示的なポリシーが、説明のために論じられるだろう。

20

## 【0058】

図 3 に示されるポリシー 1 は、`TimeCallAtAccess` の値が `TRUE` であり、したがって、保護コンテンツへのアクセスが要求されるときはいつでも、セキュア時間を取り出すことを実行エージェント 104 に要求するライセンスポリシーの例である。さらに、ポリシー 1 は、モバイルデバイス 200 がサービスプロバイダネットワーク 201 カバレッジ内、またはサービスプロバイダネットワーク 201 カバレッジ外であるとき、0 回の猶予期間アクセス試行を可能にする。したがって、いずれの場合も 0 回の猶予期間アクセスが可能にされるので、ローミングがカバレッジ内の場合をエミュレートするかどうかは重要ではない。すなわち、`UseInCoverageForRoaming` は、`TRUE` または `FALSE` のいずれかとすることができる。また、ポリシー 1 は、モバイルデバイス 100、200 の起動時にセキュア時間を取り出すことを実行エージェント 104 に要求する `TimeCallAtStartup` 値 `TRUE` を含む。これらの `DRM` ライセンスパラメータ設定を用いれば、セキュア時間が利用可能であるとき、クライアントはライセンスに関連する保護コンテンツにアクセスすることができるのみである。したがって、悪用からの保護または制約レベルは、ポリシーの最も強いものの 1 つであると考えられる。しかしながら、この保護は、ユーザの経験を犠牲にする。モバイルデバイス 200 がセキュア時間ソースを含まない場合、ポリシーは、セキュア時間を取り出すために頻繁なデータ呼を要求し、トランシーバが使用不能にされたか、またはモバイルデバイスがカバレッジエリア外であるときはいつでも、コンテンツへのアクセスが拒否されることになるだろう。

30

40

## 【0059】

図 3 に示されるポリシー 2 は、`TimeCallAtAccess` の値が `TRUE` であるライセンスポリシーの例であり、したがって、保護コンテンツへのアクセスが必要とされるときはいつでも、セキュア時間を取り出すことを実行エージェント 104 に要求する。セキュア時間が利用できず、モバイルデバイス 200 がカバレッジエリア内である場合、ポリシー 2 は、0 回の猶予期間アクセス試行を可能にする。しかしながら、セキュア時間が利用できず、モバイルデバイス 200 がカバレッジエリア外である場合、ポリシー 2 は、N 回の猶予期間アクセス試行を可能にする。このポリシーは、`TRUE` である `UseInCoverageForRoaming` パラメータをも含むので、モバイルデバイス 200 がローミングモードであるとき、該ポリシーはカバレッジ内状況に従う、すなわち

50

猶予期間アクセスを可能にしない。モバイルデバイス100、200が起動されたとき、ポリシー2は、セキュア時間を取り出すことを実行エージェント104に要求しない。これらのパラメータ設定が適切であれば、悪用に対する保護は、ポリシー1よりもわずかに耐悪用性が低い「強 (strong)」と考えられる。有効性レーティングが格下げされるのは、セキュア時間が利用できなくても、クライアントが数回の保護コンテンツへのアクセスを許可されるためである。さらに、ポリシー2は、起動時に追加されるデータ呼を必要としない。とはいえ、Nが小さいので、保護レベルは強いと考えられ、したがって、可能な猶予期間アクセス試行数は小さい。同じ理由から、ユーザ経験は、「極不良 (very poor)」から「不良 (poor)」に格上げされる。

#### 【0060】

図3に示されるポリシー3は、TimeCallAtAccessの値がTRUEであるライセンスポリシーの例であり、したがって、保護コンテンツへのアクセスが要求されるときはいつでも、セキュア時間を取り出すことを実行エージェント104に要求する。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア内である場合、ポリシー3は、0回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア外である場合、ポリシー3は、最大N回の猶予期間アクセス試行を可能にする。しかしながら、ポリシー2とは対照的に、Nは大きく、それによって多数のカバレッジ外猶予期間使用を与える。ポリシー3は、モバイルデバイス100、200の起動時にセキュア時間を取り出すことを実行エージェント104に要求する。ポリシー3では、多数の許可された猶予期間試行を利用するためにクライアントがカバレッジの外側に意図的に残る場合、ポリシー3が悪用される危険があるので、保護レベルは「可」と考えられる。これらのライセンスパラメータを用いると、モバイルデバイス200の起動時にデータ呼と、保護コンテンツへのアクセスが内部セキュア時間ソースを含まないモバイルデバイスに要求されたときのデータ呼とのために、ユーザ経験は「極不良」と考えられる。

#### 【0061】

ポリシー4は、ポリシー3とほぼ同じであるが、起動時にセキュア時間のためのデータ呼を必要としない。したがって、ポリシー4の保護レベルは「可」(であるが、ポリシー3よりも非常にわずかに小さい)と考えられる。しかしながら、ユーザ/クライアント経験は、主に起動時にデータ呼がないために、「極不良」から「不良」に格上げされる。

#### 【0062】

ポリシー5は、TimeCallAtAccessがTRUEであるライセンスポリシーの例であり、したがって、保護コンテンツへのアクセスが必要とされるときはいつでも、セキュア時間を取り出すことを実行エージェント104に要求する。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア内である場合、ポリシー5は、M回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス100、200がカバレッジエリア外である場合、ポリシー5は、N回の猶予期間アクセス試行を可能にする。ポリシー5では、Mは小さい値に設定され、Nは大きい値に設定される。UseInCoverageForRoamingパラメータがTRUEであるので、モバイルデバイス100、200がローミングモードであるとき、該ポリシーは、カバレッジ内の場合をエミュレートする、すなわちM回の猶予期間アクセスを可能にする。モバイルデバイス200がカバレッジの外側にある場合、Nが大きいので、コンテンツはほとんど無期限にアクセスされることができる。TimeCallAtStartupパラメータがTRUEであるので、ポリシー5は、モバイルデバイス100、200の起動時にセキュア時間を取り出すことを実行エージェント104に要求する。これらのパラメータ設定が適切であれば、ポリシー5の保護は「可」と考えられる。ポリシー5は、セキュア時間のためのデータ呼が、起動時に、および要求の各インスタンスにおいて行われるという要件から利益を得る一方、クライアントは、モバイルデバイス100、200がネットワーク内またはネットワーク外のいずれかにあるとき、数回の猶予期間アクセス試行を許可される。これらの許可された猶予期間試行のために、保護レベルは「可」に格下げ

10

20

30

40

50

される。モバイルデバイス200が内部セキュア時間ソースのない場合、ポリシー5は依然として複数のデータ呼を必要とするので、ポリシー5のユーザ経験は「極不良」と考えられる。その上、モバイルデバイス100、200がネットワーク中にあるときの、猶予期間試行の数は小さい。Mの小さい値は、カバレッジ内であるとき、ユーザをほんの数回の保護コンテンツへのアクセスに過度に拘束する。

#### 【0063】

ポリシー6は、ポリシー5と同様のライセンスポリシーの例であるが、起動時にセキュア時間のためのデータ呼を必要としない。したがって、ポリシー6の保護レベルは「可」（であるが、ポリシー5よりも非常にわずかに小さい）と考えられる。しかしながら、ユーザ/クライアント経験は、主に起動時にデータ呼がないために、「極不良」から「可」に格上げされる。

10

#### 【0064】

ポリシー7は、TimeCallAtAccessがTRUEであるライセンスポリシーの例であり、したがって、保護コンテンツへのアクセスが必要とされるときはいつでも、セキュア時間を取り出すことを実行エージェント104に要求する。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア内である場合、ポリシー7は、最大M回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス100、200がカバレッジエリア外である場合、ポリシー7は、最大N回の猶予期間アクセス試行を可能にする。ポリシー7では、MおよびNは大きい値に設定される。MとNの両方が大きいので、モバイルデバイス100、200がローミング中であるかどうかは特に関係しない。ポリシー7はまた、TimeCallAtStartupをFALSEに設定し、したがって起動時にデータ呼は必要ではなくなる。これらのパラメータ設定の場合、保護レベルは「可」と考えられるが、該ポリシーは、ユーザがデータ呼を機能させなかった場合、長期間悪用される危険がある。MおよびNが大きいので、ユーザ経験は「可」と考えられる。

20

#### 【0065】

ポリシー8は、TimeCallAtAccessがFALSEであるライセンスポリシーの例であるので、実行エージェント104は、保護コンテンツへのアクセスが必要とされるときはいつでも、セキュア時間を取り出すことを必要としない。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア内である場合、ポリシー8は、0回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア外である場合、ポリシー8は、最大N回の猶予期間アクセス試行を可能にし、Nは小さい。UseInCoverageForRoamingは真(true)に設定されるので、モバイルデバイス100、200がローミングモードであるとき、該ポリシーはカバレッジ内の状況をエミュレートする。ポリシー8は、モバイルデバイス100、200の起動時にのみセキュア時間を取り出すことを実行エージェント104に要求する。これらのパラメータ設定が適切であれば、Nが小さいので、ポリシー8における保護は「強」と考えられ、制限された期間中にのみ悪用される危険がある。ポリシー8は、モバイルデバイス100、200がネットワークの外にあるとき、依然として起動時にデータ呼を必要とし、制限された数の猶予期間アクセス試行のみを許可するので、ユーザ経験は「極不良」と考えられる。

30

40

#### 【0066】

ポリシー9は、ポリシー8と同様のライセンスポリシーの例であるが、もはや起動時にデータ呼を必要としない。したがって、保護レベルは「強」から「極良」に格下げされるが、予想されるユーザ経験は「極不良」から「不良」に格上げされる。これは、主にデータ呼がないためである。

#### 【0067】

ポリシー10は、TimeCallAtAccessがFALSEであるライセンスポリシーの例であるので、実行エージェント104は、保護コンテンツへのアクセスが必要とされるときはいつでも、セキュア時間を取り出すことを必要としない。セキュア時間が

50

利用できず、モバイルデバイス200がカバレッジエリア内である場合、ポリシー10は、最大M回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス200がカバレッジエリア外である場合、ポリシー10は、最大N回の猶予期間アクセス試行を可能にする。MとNの両方は小さいので、UseInCoverageForRoamingの設定は特に関係しない。ポリシー10は、モバイルデバイス100、200の起動時にのみセキュア時間を取り出すことを実行エージェント104に要求する。MおよびNが適度に小さいので、ポリシー10は、カバレッジ内か、カバレッジエリア外か、またはローミング中であるかどうかにかかわらず、セキュア時間が利用可能ではないとき、保護コンテンツへの制限されたアクセスのみを可能にする。これらのパラメータ設定が適切であれば、ポリシーは制限された時間の間のみ悪用される危険があるので、保護コンテンツの保護は「良 (good)」と考えられる。また、内部セキュア時間ソースがないモバイルデバイスに対して必要とされる起動時のデータ呼のために、ポリシー10の下での保護は「良」である。MおよびNが小さいので、また、モバイルデバイス200の起動時のデータ呼がユーザにとって邪魔で混乱を招くものなので、ポリシー10のユーザ経験は「不良」と考えられる。とはいえ、モバイルデバイス100、200がカバレッジ内であるか、カバレッジエリア外であるか、またはローミングモードであるかどうかにかかわらず、モバイルデバイス200がセキュア時間を頻繁に与えることができず、クライアントが制限された猶予期間を変更できない場合、ユーザ経験は「極不良」である。起動時の呼は、検証されているライセンスに関連する保護コンテンツにアクセスする試行に明らかに関係しないので、起動時の呼は、混乱を招くことがある。

10

20

**【0068】**

ポリシー11は、ポリシー10と同様のライセンスポリシーの例であるが、起動時にセキュア時間のためのデータ呼をもはや必要としない。セキュア時間のためのデータ呼がもはや必要とされないので、コンテンツを保護するポリシー11の有効性は「良」から「可」に格下げされる。しかしながら、予想されるユーザ経験は、「良」に改善することができるが、いくつかの状況下では「極不良」であることができる。データ呼が常に必要ではなく、そのため邪魔にならないので、ポリシー11のユーザ経験は「良」と考えられる。とはいえ、モバイルデバイス100、200がカバレッジ内であるか、カバレッジエリア外であるか、またはローミング中であるかどうかにかかわらず、モバイルデバイス100、200がセキュア時間を頻繁に与えることができず、クライアントが制限された猶予期間を変更できない場合、ユーザ経験は「極不良」であるだろう。

30

**【0069】**

ポリシー12は、TimeCallAtAccessの値を偽 (false) に設定するライセンスポリシーの例であるので、保護コンテンツへのアクセスが必要とされる時はいつでも、セキュア時間を取り出すことを実行エージェント104に要求しない。セキュア時間が利用できず、モバイルデバイス100、200がカバレッジエリア内である場合、ポリシー12は、最大M回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス100、200がカバレッジエリア外である場合、ポリシー12は、最大N回の猶予期間アクセス試行を可能にする。MとNの両方は大きいので、UseInCoverageForRoamingの設定は特に関係しない。ポリシー12は、モバイルデバイス100、200の起動時にのみセキュア時間を取り出すことを実行エージェント104に要求する。MおよびNの値は、ポリシー10とは対照的に大きく、したがって、モバイルデバイス100、200がカバレッジ外であるとき、ポリシー12の保護を弱める。これらのパラメータ設定が適切であれば、該ポリシーは、より多くの回数の猶予期間アクセス試行を利用することによって、より長い時間期間の間悪用されることがあるので、保護は「弱い (weak)」と考えられる。モバイルデバイス100、200の起動時のデータ呼が邪魔でユーザに混乱を招くので、ポリシー12のユーザ経験は「不良」と考えられる。起動時の呼は、検証されているライセンスに関連する保護コンテンツにアクセスする試行に明らかに関係しないので、混乱を招くことがある。

40

**【0070】**

50

ポリシー 13 は、ポリシー 12 と同様のライセンスポリシーの例であるが、起動時にデータ呼は必要ではなくなる。M および N の値は、ポリシー 11 とは対照的に大きく、モバイルデバイス 100、200 がカバレッジ外であるとき、ポリシー 13 の保護を弱める。したがって、このポリシーは、より長い猶予期間を利用することによってポリシー 11 の場合よりも長い期間の間悪用されることができる。さらに、データ呼がないことによって、ポリシー 13 はポリシー 12 よりも弱くなる。これらのパラメータ設定が適切であれば、保護は「極弱 (very weak)」と考えられる。データ呼が常に必要ではなく、そのため邪魔にならないので、ポリシー 13 のユーザ経験は「良」と考えられる。

#### 【0071】

ポリシー 14 は、TimeCallAtAccess の値を偽に設定するライセンスポリシーの例であるので、保護コンテンツへのアクセスが必要とされるときはいつでも、セキュア時間を取り出すことを実行エージェント 104 に要求としない。セキュア時間が利用できず、モバイルデバイス 100、200 がカバレッジエリア内である場合、ポリシー 14 は、最大 M 回の猶予期間アクセス試行を可能にする。セキュア時間が利用できず、モバイルデバイス 100、200 がカバレッジエリア外である場合、ポリシー 14 は、最大 N 回の猶予期間アクセス試行を可能にする。M と N の両方は大きいので、UseInCoverageForRoaming の設定は特に関係しない。これらのパラメータ設定が適切であれば、図 3 のポリシー 14 は、クライアントによる悪用からの最小のセキュア DRM 保護およびコンテンツプロバイダのための最小保護を与える。ポリシー 14 は、悪用するまでのユーザによる骨折りをほとんどなしに、長い期間の間、使用保護コンテンツへのアクセスを可能にするので、ポリシー 14 は「極弱」と考えられる。しかしながら、ポリシー 14 は、ユーザにとって完全に邪魔にならないので、「極良」と考えられる。

#### 【0072】

図 4 は、実行エージェント 104 によって実行される手順の一実施形態のプロセス流れ図である。図 4 a は、図 4 に示されるステップを実装するために当業者によって利用できる例示的な可能な擬似コードのリストである。保護コンテンツがクライアントによって最初にダウンロードされる時、ライセンスが実行され、ライセンスの期間を管理するパラメータが、メモリ 111 のセキュアな部分に記憶されることができる。メモリパラメータがメモリ 111 のセキュアな部分に記憶されると、ライセンスパラメータカウンタ (LP) が、記憶されたパラメータごとに増分されることができる。図 4 に示すステップ 301 において、実施形態方法は、保護コンテンツに関連するライセンスが適切であるかどうかを判断する。ライセンスパラメータがメモリ 111 のセキュアな部分に記憶されていない場合、LP の値は 0 であるだろう。LP の値が 0 である場合、ステップ 316 において、メモリ 111 に記憶されたすべてのデジタルコンテンツへのアクセスは許可される。しかしながら、LP の値が 0 でない場合、少なくとも 1 つの時間ベースライセンスが施行されることができる。

#### 【0073】

ステップ 302 において、プロセッサ 110 を介して実行エージェント 104 は、ローカルセキュア時間ソース 102 が存在するかどうかを判断することができる。セキュア時間ソースが利用可能な場合、ステップ 304 において、オペレーティングシステム 103 およびプロセッサ 110 を介して実行エージェント 104 は、クライアントが保護コンテンツへのアクセスを許可された制限された時間期間が経過したかどうかを確かめるために検査することができる。制限された時間期間が経過されていない場合、ステップ 307 において、オペレーティングシステム 103 およびプロセッサ 110 を介して実行エージェント 104 は、InCoverageUseLimit を M に、OutCoverageUseLimit を N に、および猶予期間カウンタを 0 に設定することができる。次いで、ステップ 319 において、クライアントは保護コンテンツへのアクセスを与えられる。

#### 【0074】

ステップ 304 において、制限された時間期間が経過したと判断された場合、ステップ 305 において、ライセンスが期限切れになったものとされることができ、ステップ 30

10

20

30

40

50

8において、クライアントは、ライセンスが期限切れになったことを通知される。クライアントがライセンスの期限切れについて通知された後、ステップ318において、保護コンテンツへのアクセスが拒否される。

【0075】

ステップ302において、ローカルセキュア時間ソース102が利用可能でない場合、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ステップ303において、TimeCallAtAccessパラメータがTRUEまたはFALSEに設定されたかを判断するために、保護コンテンツに関連するライセンスパラメータ105を調べるだろう。TimeCallAtAccessパラメータがFALSEに設定されていた場合、該実施形態方法は、モバイルデバイス200がカバレッジ内であるか、カバレッジ外であるか、またはローミング中であるとき、モバイルデバイス200が猶予期間アクセス試行を許可されるかどうかを判断する（以下のステップ310～319参照）。

10

【0076】

TimeCallAtAccessパラメータがTRUEに設定されていた場合、ステップ306において、セキュア時間を取り出すためにセキュア時間ソース202に対して呼が行われる。ステップ309において、セキュア時間ソースを取り出すためのデータ呼が成功した場合、該実施形態方法は、ステップ302において、ローカルセキュア時間ソースが利用可能であるかのように動作することができ、ステップ304、305、307、および308に続く。しかしながら、セキュア時間ソースを取り出すための呼が失敗した場合、該実施形態方法は、モバイルデバイス200がカバレッジ内であるか、カバレッジ外であるか、またはローミング中であるとき、クライアント/ユーザが猶予期間アクセス試行を許可されているかどうかを判断するだろう（以下のステップ310～319参照）。

20

【0077】

モバイルデバイス100、200がカバレッジ内であるか、カバレッジ外であるか、またはローミング中のいずれかであるとき、クライアント/ユーザが猶予期間アクセス試行を行うのを許可されているかどうかを判断するために、該実施形態方法は、モバイルデバイス200がどの状態（すなわち、カバレッジ内、カバレッジ外、またはローミング中）であるかを最初に判断しなければならない。この判断を行うために、ステップ310において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、モバイルデバイスの200のトランシーバ機能が使用可能かどうかを判断する。

30

【0078】

トランシーバ機能が使用不能であるか、またはデータ呼が失敗した場合、モバイルデバイス200がカバレッジ内であると仮定することができる。トランシーバ機能が使用不能であった場合、使用不能なトランシーバ機能がなければ、モバイルデバイス200がセキュア時間を取り出すためのデータ呼を正常に完了することが可能であると仮定する。モバイルデバイス200がカバレッジ内であるので、ステップ312において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ライセンスポリシーが、クライアント/ユーザがカバレッジ内猶予期間アクセス試行をM回行うことを可能にするかどうかを判断する。ステップ312において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、猶予期間カウンタを検査し、クライアントにとって依然として利用可能である猶予期間アクセス試行があるかどうかを判断するために、それをIntCoverageUseLimit値Mと比較するだろう。ステップ312において、猶予期間カウンタとIntCoverageUseLimit値Mとの比較が、さらなる猶予期間アクセス試行が利用可能であると判断した場合、ステップ315において、猶予期間試行カウンタが増分され、ステップ319において、保護コンテンツへのアクセスが許可される。ステップ312において、猶予期間カウンタとIntCoverageUseLimit値Mとの比較が、さらなる猶予期間ア

40

50



クセス試行が利用可能ではないと判断した場合、ステップ318において、保護コンテンツへのアクセスが阻止される。

【0079】

ステップ310において、トランシーバ機能が使用可能であるが、モバイルデバイス200が、セキュア時間ソース202からセキュア時間を取り出すためのデータ呼を完了することに失敗したと判断した場合、モバイルデバイス200がカバレッジ外であるか、またはローミングモードであるかのいずれかであると仮定することができる。したがって、該実施形態方法は、どの条件を適用するかを判断しなければならない。ステップ311において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、モバイルデバイスがローミングモードである（すなわち、音声呼出しが利用可能であるが、データ呼が利用可能ではない）かどうかを判断する。大部分のモバイルデバイス200では、音声呼出しのための追加料金が適用すべきかどうかを判断するために、この判断は事前に行われる。モバイルデバイス200がローミングモードである場合、ステップ313において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ライセンスポリシーが、クライアント/ユーザにローミング猶予期間アクセス試行をR回行うことを可能にするかどうかを判断する。ステップ313において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、猶予期間カウンタを検査し、クライアントにとって依然として利用可能である猶予期間アクセス試行があるかどうかを判断するために、それをRoamUseLimit値Rと比較するだろう。ステップ313において、猶予期間カウンタとRoamUseLimit値Rとの比較が、さらなる猶予期間アクセス試行が利用可能であると判断した場合、ステップ316において、猶予期間試行カウンタが増分され、ステップ319において、保護コンテンツへのアクセスが許可される。ステップ313において、猶予期間カウンタとRoamUseLimit値Rとの比較が、さらなる猶予期間アクセス試行が利用可能ではないと判断した場合、ステップ318において、保護コンテンツへのアクセスが阻止される。

10

20

【0080】

ステップ311において、モバイルデバイス200がローミングモードではないと判断された場合、モバイルデバイス200がカバレッジ外であると仮定されることができる。ステップ311において、モバイルデバイス200がカバレッジ外である場合、ステップ314において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ライセンスポリシーが、クライアント/ユーザにカバレッジ外猶予期間アクセス試行をN回行うことを可能にするかどうかを判断する。ステップ314において、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、猶予期間カウンタを検査し、クライアントにとって依然として利用可能である猶予期間アクセス試行があるかどうかを判断するために、それをOutCoverageUseLimit値Nと比較するだろう。ステップ314において、猶予期間カウンタとOutCoverageUseLimit値Nとの比較が、さらなる猶予期間アクセス試行が利用可能であると判断した場合、ステップ317において、猶予期間試行カウンタが増分され、ステップ319において、保護コンテンツへのアクセスが許可される。ステップ314において、猶予期間カウンタとOutCoverageUseLimit値Nとの比較が、さらなる猶予期間アクセス試行が利用可能ではないと判断した場合、ステップ318において、保護コンテンツへのアクセスが阻止される。

30

40

【0081】

代替実施形態（図示せず）は、RoamUseLimitパラメータ値Rをなくすことによって、本方法を簡単に行うことができる。代わりに、TRUEまたはFALSEのいずれかに設定されることができる、UseInCoverageForRoamingパラメータ値などのパラメータが利用されることができる。それがTRUEに設定され、モバイルデバイス200がローミングモードであると判断された場合には、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ローミン

50

グモードのモバイルデバイス200を、モバイルデバイス200がカバレッジ内（すなわち、トランシーバ機能が使用不能にされたカバレッジ内）であるかのように扱う。したがって、ローミングモードである間の猶予期間アクセス試行は、InCoverageUseLimit Mに対して課金される。UseInCoverageForRoamingパラメータがFALSEに設定され、モバイルデバイス200がローミングモードであると判断された場合には、オペレーティングシステム102およびプロセッサ110を介して実行エージェント104は、ローミングモードであるモバイルデバイス200を、モバイルデバイス200がカバレッジ外であるかのように扱う。したがって、ローミングモードである間の猶予期間アクセス試行は、OutCoverageUseLimit Nに対して課金される。

10

#### 【0082】

図4aは、図4に示され上述されたステップを実行するように実装されることができるとするサンプル擬似コードを列記する。図4aに示すように、ライン401において、プロシージャTestContentLicensingが命名される。LicenseParametersは、ライセンスポリシーのライセンスパラメータ105を保持するデータ構造を参照する。ライン402は、プロシージャTestContentLicensingの本体を開始する。ライン403は、プロシージャTestContentLicensingに渡される引数がヌルであるかどうかを検査する（図4のステップ301参照）。ヌル引数は、プロシージャTestContentLicensingがライセンスがないコンテンツに対して呼び出されたとき、偶然に、または意図的に生じることがある。ライセンスがない場合、プロシージャは、コンテンツがアクセスされることができると仮定するので、ライン404は、AllowAccess（図4のステップ319）と標示されたステートメントにおいて実行が継続することを指示する。

20

#### 【0083】

ライン410のアサーション（assertion）は、単にコメントとして扱われるか、あるいはライン410は、手動または自動デバッグまたはプロシージャの正当性の検証を指示するために使用される。ライン411は、モバイルデバイス100上のセキュアクロック102などのローカルセキュア時間ソースがあるかどうかを判断する（ステップ302）。一実施形態では、セキュアクロック102は、モバイルデバイス100の残部が電源切断された後も動作し続けることができる。ローカル時間ソース102がセキュアな場合、ライン413は実行をTestForExpirationと標示されたステートメントで続行することに向ける（図4のステップ304）。さもなければ、実行は、ライン413の後に続く。ライン420は、コメントとして考えられるか、またはプロシージャの正当性の検証のために使用される。ライン421は、LicenseParametersによって参照されるデータ構造中の、TimeCallAtAccessパラメータの値を判断する（図4のステップ303）。値がTrueに設定された場合、ライン422は、サービスプロバイダネットワーク201上のセキュア時間ソース202からセキュア時間を取り出すために、呼を開始する（図4のステップ306）。ライン422において呼がセキュア時間を正常に取り出した場合、セキュア時間は局所変数STimeに記憶され、ライン424は、実行をTestForExpirationと標示されたステートメントで続行することに向ける（図4のステップ304）。

30

40

#### 【0084】

図4aにおいては、ライン430は、セキュア時間が利用できないことをアサートする。ライン431は、モバイルデバイス200の動作モードを判断する一連の場合を開始する。ライン431は、モバイルデバイス200がカバレッジ内であるか、カバレッジ外であるか、またはローミングモードで動作しているかどうかを判断する（図4のステップ310および311）。すなわち、モバイルデバイス100、200の動作モードがカバレッジ内である場合、ライン432は、実行をCoverageInと標示されたステートメントで続行することに向ける（図4のステップ312、315）。モバイルデバイス200の動作モードがローミング中である場合、ライン434は、実行をRoamingと

50

標示されたステートメントで続行することに向ける。モバイルデバイス200の動作モードがカバレッジ外である場合、ライン436は、実行をCoverageOutと標示されたステートメントで続行することに向ける。

【0085】

図4aにおいては、ライン440は、ラベルCoverageInを用いて一連のステートメントを標示する。ライン440で開始するラインは、カバレッジ内モードであるモバイルデバイスの場合に応じる(図4のステップ312)。ライン441は、モバイルデバイス200がカバレッジ内モードで動作している間、保護コンテンツへのより多くの猶予期間アクセスが残っているかどうかを確かめるために、InUsesAttemptsアクセスカウンタの変数値を調査する(図4のステップ312)。もはやカバレッジ内猶予期間アクセスが残っていない場合、ライン442は、実行をBlockAccessと標示されたステートメントで続行することに向ける(図4のステップ318)。さもなければ、実行は、InUsesAttemptedと呼ばれるカウンタを増分するライン443に続く(図4のステップ315)。プログラミングを簡単にするために、カウンタInUsesAttemptedは、ライセンスパラメータをも含む、LicenseParametersによって参照される同じデータ構造で位置付けられる整数変数フィールドとすることができる。ライン444は、実行をAllowAccessと標示されたステートメントで続行することに向ける(図4のステップ319)。

10

【0086】

図4aにおいては、ライン450は、ラベルRoamingを用いて一連のステートメントを標示する。ライン450で開始するラインは、ローミングモードであるモバイルデバイスの場合に応じる(図4のステップ313)。ライン451は、モバイルデバイス200がローミングモードで動作している間、保護コンテンツへのより多くの猶予期間アクセスが残っているかどうかを確かめるために、RoamUsesAttemptsアクセスカウンタの変数値を調査する(図4のステップ313)。もはやローミング猶予期間アクセスが残っていない場合、ライン452は、実行をBlockAccessと標示されたステートメントで続行することに向ける(図4のステップ318)。さもなければ、実行は、RoamUsesAttemptedと呼ばれるカウンタを増分するライン453に続く(図4のステップ316)。プログラミングを簡単にするために、カウンタRoamUsesAttemptedは、ライセンスパラメータをも含む、LicenseParametersによって参照される同じデータ構造で位置付けられる整数変数フィールドとすることができる。ライン454は、実行をAllowAccessと標示されたステートメントで続行することに向ける(図4のステップ319)。

20

30

【0087】

図4aにおいては、ライン460は、ラベルCoverageOutを用いて一連のステートメントを標示する。ライン460で開始するラインは、カバレッジ外モードであるモバイルデバイスの場合に応じる。ライン461は、モバイルデバイス200がカバレッジ外モードで動作している間、保護コンテンツへのより多くの猶予期間アクセスが残っているかどうかを確かめるために、OutUsesAttemptsの値を調査する(図4のステップ314)。もはやカバレッジ外猶予期間アクセスが残っていない場合、ライン462は、実行をBlockAccessと標示されたステートメントで続行することに向ける(図4のステップ318)。さもなければ、実行は、OutUsesAttemptedと呼ばれるカウンタを増分するライン463に続く(図4のステップ317)。プログラミングを簡単にするために、OutUsesAttemptedは、ライセンスパラメータをも含む、LicenseParametersによって参照される同じデータ構造で位置付けられる整数変数フィールドとすることができる。ライン464は、実行をAllowAccessと標示されたステートメントで続行することに向ける(図4のステップ319)。

40

【0088】

図4aにおいては、ライン470は、ラベルTestForExpirationを用

50

いて一連のステートメントを標示し、ライン471でアサートされるように、時間S T i m eがセキュアであると知られているときはいつでも、ライセンスを検証する(図4のステップ302)。ライン472は、現在のセキュア時間S T i m eをL i c e n s e P a r a m e t e r sによって参照されるデータ構造のE x p i r a t i o n D a t eパラメータと比較する(図4のステップ307)。S T i m eがL i c e n s e P a r a m e t e r sのパラメータE x p i r a t i o n D a t eの有効日/時値より大きい、すなわち、有効日/時より後の場合、ライセンスは期限切れになる。ライン473は、ライセンスが期限切れになったことを明解に示すためにいくつかの動作を実行する(図4のステップ305)。動作は、ライセンスパラメータデータ構造および保護コンテンツを削除することがあるが、これは、アクセス権利の次の更新を複雑にする。ライン473の代替動作は、L i c e n s e P a r a m e t e r sによって参照されるデータ構造内で期限切れになったものとしてライセンスを示すことである(図4のステップ305)。たとえば、データ構造は、T r u eに設定されているE x p i r e dと呼ばれる、ブーリアンフィールドを有することができる。いずれの場合も、ライン474は、I n U s e A t t e m p t sの値をI n C o v e r a g e U s e L i m i t Mよりも大きい値に設定する。ライン475は、R o a m U s e A t t e m p t sの値をR o a m C o v e r a g e U s e L i m i t Rよりも大きい値に設定する。ライン476は、O u t U s e A t t e m p t sの値をO u t C o v e r a g e U s e L i m i t Nよりも大きい値に設定する。ライン477~479で、I n C o v e r a g e U s e L i m i t、R o a m U s e L i m i tおよびO u t C o v e r a g e U s e L i m i tの値はそれぞれ、L i c e n s e P a r a m e t e r sによって参照されるデータ構造で0に設定される。0値は、カバレッジからモバイルデバイス200を意図的に遮蔽することによって、クライアントが不正をして、任意の残りの未使用のカバレッジ外猶予期間アクセスを使用することを防止する。ライン480は、クライアントにライセンスが期限切れになったことを通知し、クライアントにライセンスを更新するように勧誘することができる(図4のステップ308)。ライン481は、保護コンテンツをアクセスされることから防止するだろうB l o c k A c c e s sと標示されたステートメントに、実行を向ける(図4のステップ318)。

#### 【0089】

ライン472での比較により、ライセンスがS T i m eに基づいて依然として有効であることがわかった場合(図4のステップ304)、ライン483~485は、ライセンスポリシーのライセンスパラメータを含む、同じデータ構造L i c e n s e P a r a m e t e r s中に位置付けられる、整数猶予期間アクセスカウンタI n U s e s A t t e m p t s、R o a m U s e A t t e m p t sおよびO u t U s e A t t e m p t sを0にリセットする(図4のステップ307)。ライセンスが期限切れになったと判断され、時間がセキュアであったので、猶予期間アクセスカウンタ、I n U s e s A t t e m p t s、R o a m U s e A t t e m p t sおよびO u t U s e s A t t e m p t sは0にリセットされる。

#### 【0090】

図4aにおいては、ライン490は、ラベルA l l o w A c c e s sをライン491のステートメントに添付し、プロシージャを抜けて、セキュア時間が利用可能ではなかったとしても、ライセンスが期限切れになっていないものとして扱われるべきであることを示すために、プロシージャT e s t C o n t e n t L i c e n s i n gの呼出し側に値T r u eを帰す(図4のステップ319)。ライン495は、ラベルB l o c k A c c e s sをライン496のステートメントに添付し、プロシージャを抜けて、ライセンスが期限切れになったものとして扱われるべきであることを示すために、プロシージャT e s t C o n t e n t L i c e n s i n gの呼出し側に値F a l s eを帰す(図4のステップ318)。ライン499は、プロシージャT e s t C o n t e n t L i c e n s i n gの終了を示す。

#### 【0091】

図4bは、R o a m U s e L i m i tの値が利用されないとき、代替プロシージャを実

10

20

30

40

50

施するために実装されるサンプル擬似コードを列記するが、むしろ、本方法は、ローミングモードであるときに、いずれかの `InUseLimit` にデフォルト設定される。サンプル擬似コードは、図 4 a のサンプル擬似コードと実質的に同様であるが、`RoamUseAttempts` および `RoamUseLimits` を参照するコードのラインはない。代わりに、新しいコードライン 435 ~ 439 が追加されている。当業者は、必要な場合、`OutUseLimit` にデフォルト設定されるサンプル擬似コードを容易に生成することができる。ライン 435 で、モバイルデバイス 200 がカバレッジ内でもカバレッジ外でもないと考えられる場合、モバイルデバイス 200 は、ローミングモードであると考えられることができる。ライン 436 で、オペレーティングシステム 103 およびプロセッサ 110 を介して実行エージェント 104 は、`LicenseParameters` によって参照されるデータ構造の `UseInCoverageForRoaming` パラメータから、カバレッジ内の場合またはカバレッジ外の場合と同様にローミングモードを扱うべきかどうかを判断する。`UseInCoverageForRoaming` パラメータの値が `True` である場合、ローミングモードは、カバレッジ内モードの場合と同じポリシーパラメータを使用し、ライン 437 は、実行を `CoverageIn` と標示されたステートメントで続行することに向ける。`UseInCoverageForRoaming` パラメータの値が `False` である場合、ローミングモードは、カバレッジ外モードの場合と同じポリシーパラメータを使用し、ライン 439 は、実行を `CoverageOut` と標示されたステートメントで続行することに向ける。図 4 a および図 4 b に示すサンプル擬似コードリストは、様々な実施形態のステップを実装するために使用されることができ、可能な擬似コードの例を意味するにすぎない。それらは、いかなる形でも実施形態を制限することを意味するものではない。

#### 【0092】

いくつかの実施形態の場合、サービスプロバイダは、フィールドにおいてリモートでおよび/またはオンザフライでライセンスパラメータを構成するかまたは変更することが可能であることができる。たとえば、サービスプロバイダは、誤用で特定されることがあるライセンスを終了することができ、または、サービスプロバイダは、既存のライセンスを与えられたユーザからの支払い時に、ライセンスをリモートでアップグレードするかまたは更新することができる。リモートアップグレードまたは更新は、新しいライセンスパラメータ値をセキュアに無線で送信するための標準の方法を使用することによって達成されることができ、パラメータに対する更新は、デジタル署名を用いて SMS などのいくつかの手段を使用してデバイスにプッシュされることができ。

#### 【0093】

図 5 は、実行エージェント 104 によって実行できる手順の代替実施形態の流れ図である。代替実施形態は、図 1 に示すステップのすべてを含むが、リモートで、または、フィールドにおいてライセンスパラメータを構成するかまたは変更する能力をもつサービスプロバイダを許可するためのステップをも含む。図 5 a は、図 5 で示されるステップを実装するために当業者によって利用される擬似コードを列記しているサンプルを与える。

#### 【0094】

図 5 に示される代替実施形態は、図 4 に示され上述されたステップ 301 ~ 319 を実装し続ける。しかしながら、図 5 の代替実施形態において、オペレーティングシステム 103 およびプロセッサ 110 を介して実行エージェント 104 が、ステップ 302 においてローカルセキュア時間が利用可能であると判断した場合、または、ステップ 309 においてセキュア時間を取り出すための呼が成功した場合、オペレーティングシステム 103 およびプロセッサ 110 を介して実行エージェント 104 は、ステップ 320 において、メモリ 111 のセキュアな部分に記憶されたライセンスポリシーおよび/またはパラメータを更新すべき時間かどうかを判断する。更新間の時間は、任意の時間期間 T とすることができる。時間 T は、サービスプロバイダによって予め設定されることができ、または、時間ごとに、日ごとに、月ごとになどに基づいて行われることができる。予め設定された時間期間 T が経過した場合、オペレーティングシステム 103 およびプロセッサ 110 を

介して執行エージェント104は、ステップ321において、ライセンスパラメータ(LP)の更新が利用可能であるかどうかを判断するために、サービスプロバイダサーバ(図示せず)と通信するだろう。ライセンスパラメータの更新が利用可能である場合、ライセンスパラメータは、ステップ322において、メモリ111のセキュアな部分にダウンロードされるだろう。更新されたライセンスパラメータがダウンロードされた後は、オペレーティングシステム103およびプロセッサ110を介して執行エージェント104は、ステップ304において、クライアント/ユーザの時間ベースライセンスが期限切れになったかどうかを判断し続けるだろう。ライセンスが期限切れになっていない場合、ステップ307において、新しいライセンスパラメータが設定されるだろう。新しいライセンスパラメータは、モバイルデバイスがカバレッジ内であるか、カバレッジ外であるか、またはローミング中である場合に、クライアント/ユーザにとって利用可能な猶予期間アクセス試行を改変することができる。

10

20

30

40

50

**【0095】**

図5aは、図5に示す追加のステップを実行するように実装されることができるサンプル擬似コードを示す。さらなる擬似コードライン500~511が追加されている。図5aによって、ライン411はローカルセキュア時間ソースが利用可能であるかどうかを検査する。ローカルセキュア時間ソースが利用可能である場合、Check Updatesと標示されたステップのシーケンスを実行する(図5のステップ320)。さらに、ライン420において、ローカルセキュア時間が利用可能でない場合、ライン421~424において、セキュア時間を取り出す一連のステップが行なわれる(図5のステップ303、306、309参照)。セキュア時間を取り出すための呼が成功した場合(図5のステップ309)、Check Updatesと標示されたステップのシーケンスが実行される(図5のステップ320)。Check Updatesシーケンス、ライン500~510においては、ライン501で、予め設定された時間Tが経過したかどうかを確認するために検査が行われる(図5のステップ320)。予め設定された時間期間Tが経過した場合、ライン502で、更新がサービスプロバイダから利用可能であるかどうかを判断するために検査が行われる(図5のステップ321)。更新が利用可能である場合、ライン504で、セキュアなデータチャネルを開く命令が実行され、ライン505で、アクセス統計がサービスプロバイダに送信される。ライン506および507で、新しいライセンスパラメータがサービスプロバイダから受信されて、記憶される(図5のステップ322)。新しいライセンスパラメータが記憶されると、ライン508で、セキュアなデータチャネルが閉じられる。ライン508でセキュアなデータチャネルが閉じられると、サンプル擬似コードは、図4aに対して上記で概説したTestForExpirationプロシージャに移動する。ライン501で、予め設定された時間期間Tが経過していない場合、図4aに対して上記で概説したようにTestForExpirationプロシージャが実行される。

**【0096】**

ライセンスパラメータに対する更新は、クライアント/ユーザが新しいライセンスおよびコンテンツを購入するか、あるいは現在のライセンスを更新するかまたはアップグレードすることの結果であることがある。新しいライセンスまたはコンテンツが購入されたとき、新しいライセンスまたはコンテンツをアップロードするプロセスは、猶予期間カウンタをリセットすることを含む、新しいライセンスパラメータ値を記憶することを含む。本方法では、更新されたライセンスパラメータは、基本的に新しいコンテンツおよびライセンスのダウンロードの一部として搬送される。ユーザが、新しい1つのコンテンツを購入/アップグレードするためにサーバと通信するとき、コンテンツ自体を制御するコンテンツおよびライセンス規則(2008年8月15日まで再生)に伴うのは、ライセンスパラメータ(起動時の呼、カバレッジ外猶予期間など)に対する更新である。これらの更新されたライセンスパラメータは、グローバルである、すなわち、すべてのコンテンツ/データに適用されることができ、または、新たにダウンロードされたコンテンツ自体にのみ適用されることができ、新しいコンテンツの購入がセキュアなデータ接続の確立を必要

とするので、ライセンスパラメータは、コンテンツデータと同様の方法で認証され、暗号化され、保全されることができる。本方法は、ユーザが新しいコンテンツダウンロードを購入するときライセンスパラメータ更新を実装し、またある時にはサーバとの明示的データ接続の必要をなくし、それによってユーザの経験を改善することを許す。より多くのコンテンツを買うことの報酬がより良いユーザ経験になるように、本方法を使用してコンテンツプロバイダは、より良い/より親しみやすいライセンスパラメータ(たとえば、より長いライセンス、より多くの猶予期間使用など)で、コンテンツの頻繁な購入者に報いることができる。したがって、新しい購入ごとに、コンテンツプロバイダは、同じダウンロードトランザクション中でそのコンテンツのすべてのライセンスパラメータを変更することができる。

10

**【0097】**

保護コンテンツへの更新の場合、ライセンスパラメータの更新は、図5に図示されないステップでの更新が伴われることができる。ライン503が、更新が利用可能であると判断した場合、ライン504はセキュアなデータ接続を開く。データ接続は、モバイルデバイス100、200が、その接続へのクライアント/ユーザアクセスおよびその接続を介した伝送を防止するという意味では、セキュアであることができる。パラメータ値を保全して、値の考えられる改ざんを妨害するために、パラメータを暗号化するか、または小さい1つの実行コード中にパラメータ値を埋め込み、デジタル署名またはHMAC認証を含むことは有利であることができる。ライン505は、現在のライセンスパラメータおよび/または保護コンテンツのためのアクセスアクティビティに関する統計をサービスプロバイダネットワークに送信させる。たとえば、保護コンテンツへのアクセス総数は、AccessStatisticsと呼ばれるデータ構造中に保持された統計値とすることができる。他の統計値は、猶予期間カウンタLicenseParameters.InUseAttemptsおよび、LicenseParameters.OutUseAttemptsがそれぞれ、制限MおよびNを上回って増分した回数とすることができる。サービスプロバイダは、サービスプロバイダネットワーク201がモバイルデバイス100、200に送信するライセンスパラメータの更新のための値を判断するために、これらの統計値を使用することができる。ライン506は、更新の新しいライセンスパラメータを一時的データ構造NewLicenseParametersに保存する。次いで、ライン507は、ライセンスパラメータの新しい値をLicenseParametersによって参照されるデータ構造に複製する。ライン508は、セキュアなデータ接続を閉じる。

20

30

**【0098】**

上述のように、実施形態によって採用される可能な使用ライセンスパラメータの1つは、TimeCallAtStartupである。任意の保護ポリシーがこのライセンスパラメータをTRUEに設定した場合、セキュア時間は、モバイルデバイス100中の内部セキュア時間ソースから、またはモバイルデバイス200が電源投入されたときのデータ呼によって、アクセスされなければならない。図6は、TimeCallAtStartupパラメータを採用する実施形態方法によって実行されるステップを示す。

**【0099】**

図6に示されるように、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ステップ901において、モバイルデバイス100、200がローカルセキュア時間ソースを含むかどうかを判断する。モバイルデバイス100がローカルセキュア時間ソースを含む場合、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ステップ903において、セキュア時間がモバイルデバイス100上にローカルにすでに存在するので、データ呼が必要ではないことを示すFALSEの値を帰すだろう。しかしながら、ステップ900において、モバイルデバイス200がローカルセキュア時間ソースを含まない場合、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ステップ902において、メモリ111のセキュアな部分に記憶されたライセンスポリシーのライセ

40

50

ンスパラメータが、TRUEに設定されたTimeCallAtStartupを有するかどうかを判断する。そうであれば、ステップ904において、保護コンテンツへのアクセスの許可の前にデータ呼が必要であるだろう。

#### 【0100】

第1のライセンスポリシーがTimeCallAtStartupに対してTRUEを示すライセンスパラメータを含まない場合、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ステップ902において、メモリ111のセキュアな部分に記憶された各ライセンスポリシーを検査し続けるだろう。メモリ111のセキュアな部分内に記憶された任意の他のライセンスポリシーが、パラメータTimeCallAtStartupに対してTRUEの値を帰す場合、オペレーティングシステム103およびプロセッサ110を介して実行エージェント104は、ステップ904において、保護コンテンツへのアクセスの許可より前にセキュア時間ソースへのデータ呼を必要とするだろう。TimeCallAtStartupに対してTrueの値を帰すメモリ111のセキュアな部分に記憶されたライセンスポリシーがない場合、ステップ905において、データ呼は行われまいだろう。

10

#### 【0101】

図6aは、図6に示されたステップを実行するように実装されることができるとするサンプル擬似コードを示す。図6aに示されるように、擬似コードループは、モバイルデバイスが電源投入されたときに開始されるソフトウェアの一部として呼び出されることができるとするIsStartupTimeFetchNeededと呼ばれることができる。ライン601、602は、プロシージャ本体を開始する。ライン603は、モバイルデバイス100、200が電源切断されている間に時間を維持する、モバイルデバイス100、200上にセキュアロックがあるかどうかなど、セキュア時間102がローカルで利用可能かどうかを判断する。ローカルセキュア時間ソース102がある場合、プロシージャは、ライン604において抜けて、データ呼が必要ではないことを示す結果(FALSE)を帰す。ローカルセキュア時間ソース102がないか、あるいはセキュアロックが初期化、検証、または同期を必要とする場合、プロシージャの実行はライン610に続く。ライン610のアサーションは、コメントとして扱われることができ、またはプロシージャの正当性を手動または自動的に検証することに役立つことができる。ライン611は、モバイルデバイス200上で発見されたライセンスLごとに循環するループの始端である。ライン613は、ループのラインのインデントによって示されるようにループの最後のラインである。ライン612は、パラメータTimeCallAtStartupが任意のライセンスLに対してTRUEに設定されているかどうかを検査する。ライセンスLが、TimeCallAtStartupがTRUEであるとわかった場合、プロシージャは、ライン613で抜け、モバイルデバイス200が起動したときにサービスプロバイダのネットワークからセキュア時間にアクセスしなければならないことのインジケータとしてTRUEを帰す。ライセンスLがTimeCallAtStartupをTrueに設定したことがわからなかった場合、ループは最終的に停止し、ライン620において実行を続ける。ライン620のアサーションは、コメントとして扱われることができ、またはプロシージャの正当性を手動または自動的に検証することに役立つことができる。ライン621は、プロシージャを抜け、ライセンスには、サービス加入者ネットワーク201上のセキュア時間ソース202からセキュア時間をアクセスする必要がないという指示、すなわちFALSEを帰すことを実行させる。ライン622は、プロシージャIsStartupTimeFetchNeeded本体の終了を示す。プロシージャがTRUEを帰した場合、モバイルデバイス200は、サービスプロバイダネットワーク201上のセキュア時間ソース202からセキュア時間を取り出すためにデータ呼を発する。

20

30

40

#### 【0102】

別の実施形態では、単一のライセンスポリシーよりも多く、すなわち、ポリシーパラメータの2つ以上のセットが採用されることができるとする。デフォルトポリシー(ライセンスパラメータのデフォルトセット)は、相手先ブランドによる製造(OEM)によって、モバ

50



イルデバイス100、200中で構成されることができる。モバイルデバイスを購入し、次いでその後再販するサービスプロバイダは、他のポリシーパラメータを規定することができる。包括的アップグレードまたは拡大ポリシーは、サービスプロバイダからユーザへの追加料金のために利用可能であることができる。あるいは、サービスプロバイダは、いくつかのデフォルトポリシーパラメータをさらに制限することができる。さらに、特定の使用保護コンテンツを対象としている個々のライセンスの取引条件は、モバイルデバイスおよび/またはサービスプロバイダライセンスパラメータを無効にする、すなわち、モバイルデバイスおよび/またはサービスプロバイダポリシーを延長するか、またはさらに制限するかのいずれかを行うことができる。

#### 【0103】

代替実施形態では、ポリシーパラメータまたはコンテンツ使用統計は、場合によってはセキュアなチャネルを介して、ユーザのワイヤレスデバイスがコンテンツサーバと通信するときなどに、コンテンツサーバに報告して返されることがある。特に重要なのは、セキュア時間が利用可能ではなかったとき、アプリケーション/コンテンツが起動された、または起動しようとして試みられた回数を示すデータであることがある。あるいは、一実施形態は、(図2および図3の)カバレッジ内猶予期間制限Mおよびカバレッジ外猶予期間制限Nが超えられたかどうか、または猶予期間が制限する回数を超えられ、その後、最後の報告以降にリセットしたかどうかを報告することができる。そのような統計値は、悪用しようとする潜在的な試行を知らせることができ、その特定のユーザがさらに使用したり、またはさらにコンテンツを購入したりすることができないように使用されることができる。一実施形態では、アップグレードの購入または悪用の疑いに応じて、プロバイダネットワークがパラメータを動的に変更できるようにすることができる。使用統計値は、また、コンテンツの人気についてのフィードバックを与えることもできる。一実施形態は、猶予期間またはローミング期間中に残っているアクセス試行のカウントなど、現在の使用保護コンテンツの使いやすさのステータスについての指示をもユーザに与えることができる。

#### 【0104】

別の実施形態では、特定のライセンスを与えられたコンテンツに関連するライセンスパラメータおよび/または使用統計は、モバイルデバイス100、200上の実行エージェントがアプリケーションサーバからSMSメッセージを受信したとき、サービスプロバイダのネットワーク201上のアプリケーションサーバに送信されることができる。次いで、サーバは、ライセンスを与えられたコンテンツまたは補足コンテンツを拒否するかまたはそれらにアクセスできるようにするために、パラメータ値および/または統計値を使用する。

#### 【0105】

図7は、モバイルデバイス100、200がSMSメッセージを受信し、SMSメッセージ中で送信された統計に基づいてライセンスポリシーを変更することを可能にする一実施形態方法によって実行されるステップを示す。図7に示されるように、モバイルデバイス100、200によってSMSメッセージが受信されるとき、ステップ801において、そのSMSメッセージが、サービスプロバイダからの正規のSMSメッセージであり、偽メッセージではないことを検証されなければならない。ステップ801においてSMSメッセージが有効ではない場合、そのSMSメッセージは無視され、モバイルデバイス100、200は、ステップ805において、次のメッセージを待つことに戻る。SMSメッセージが正規のSMSメッセージであると検証された場合、テキストフィールドを新規のライセンスポリシーパラメータ値に変換するために、SMSメッセージはステップ802において解析される。ステップ803において、これらのデータフィールドに含められるのは、どのライセンスポリシーが新規のライセンスパラメータ値を適用すべきかを識別するための識別子であることができる。変更用に適切なライセンスポリシーが、ステップ803において識別されると、ステップ804において、新規のライセンスパラメータ値がメモリ111のセキュアな部分の中に設定される。ステップ804において新規のライセンスパラメータ値が識別されたライセンスポリシー用に設定された後)、モバイルデ

10

20

30

40

50

バイス100、200は、ステップ805において次のSMSメッセージを待つ状態に戻る。

#### 【0106】

図7aは、図7に示すステップを実行するように実装されることが出来るサンプル擬似コードを示す。列記されたサンプル擬似コードは、SMSメッセージがモバイルデバイス100、200によって受信され、ライセンスを更新するためのSMSメッセージとして識別されたときに呼び出すことができる、プロシージャDoLicenseUpdateFromSMSを実装することができる。ライン701では、SMSメッセージは、プロシージャDoLicenseUpdateFromSMSに渡されるSMSメッセージへの参照である。ライン702は、プロシージャの本体を開始する。ライン703は、SMSメッセージが合法的にサービスプロバイダから来ており偽メッセージでないかどうかを判断する(図7のステップ801)。ライン704は、メッセージコンテンツを解析し、必要に応じてテキストフィールドをライセンスパラメータ値に変換する(図7のステップ802)。SMSメッセージは、少なくとも1つのライセンスまたはライセンスポリシーのためのライセンスパラメータのうちの一つ、一部、または全部の値を含むことができる。SMSメッセージは、SMSメッセージによってターゲットにされた個々の保護コンテンツライセンスLを識別することができる(図7のステップ803)。DoLicenseUpdateFromSMSは、典型的なケースであることができる、SMSメッセージによって1つのライセンスが更新されるのを仮定している。しかしながら、SMSメッセージを用いて2つ以上のライセンスが更新されることができる。ライン705は、SMSメッセージコンテンツが、ライセンスLのライセンスパラメータを識別し、配置することを決定する。ライン706は、ライセンスLのライセンスパラメータ(LicenseParameters)を、SMSメッセージSMSMessageのユーザデータ部分を解析することによって決定された新規の値に設定する(図7のステップ804)。ライン707は、プロシージャDoLicenseUpdateFromSMSの呼出し元に戻す(図7のステップ805)。ライン710は、SMSMessageがフェイクであるとのコメントとして扱われることができる。ライン711は、プロシージャDoLicenseUpdateFromSMSの呼出し元に戻す。ライン712は、プロシージャ本体の終了を示す。

10

20

30

#### 【0107】

図4、図4a、図4b、図5、図5a、図6、図6a、図7、図7aの方法ステップと図3に示すポリシーとを実装するために使用されるハードウェアは、上記のポリシーに対応する方法ステップを実行するための命令のセットを実行するように構成された処理要素およびメモリ要素とすることができる。あるいは、いくつかのポリシーは、所与の機能に固有である回路によって実施されることができる。

#### 【0108】

電力管理集積回路(WMIC)を有する一実施形態では、主電池が取り外されてもクロックへの電力が維持される。これは、ローカルのセキュアクロック102が、少なくともいくつかの特定の時間期間、たとえば数日間、の電力サイクル間でその状態を維持することができることを意味する。これは、クライアントは、保護コンテンツにアクセスできるようになる前に、リモートソースからの時間を取り出すかまたは更新するために生じる遅延をクライアントは経験しないので、よりユーザフレンドリな経験を与える。それはまた、ローミング中であるかまたは任意のサービスプロバイダネットワーク201エリアの外側におり、ネットワークから外部のセキュア時間入手することができない間、クライアントは、時間ベースライセンスポリシーの下にライセンスを与えられた保護コンテンツに依然としてアクセスできるということの意味する。

40

#### 【0109】

当業者は、本明細書で開示された実施形態に関連して説明された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両者の組合せとして実装されることが出来ることを諒解する

50

だろう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的なコンポーネント、ブロック、モジュール、回路、およびステップが、上記では概してそれらの機能に関して説明された。そのような機能がハードウェアで実装されるかソフトウェアで実装されるかは、システム全体に課せられた特定の適用および設計上の制約に依存する。当業者は、説明された機能を特定の適用例ごとに様々な方法で実装することができるが、そのような実装の決定は、本発明の範囲からの逸脱を生じるものと解釈されるべきではない。

#### 【0110】

本明細書で開示された実施形態に関して説明された様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)または他のプログラマブル論理デバイス、個別ゲートまたはトランジスタロジック、個別ハードウェアコンポーネント、あるいは本明細書で説明された機能を実行するように設計されたそれらの任意の組合せを用いて実装または実行されることができる。汎用プロセッサは、マイクロプロセッサとされることができるが、代替として、プロセッサは、従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。プロセッサは、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、あるいは任意の他のそのような構成としても実装されることができる。

10

#### 【0111】

本明細書で開示された実施形態に関連して説明された方法またはアルゴリズムのステップは、直接ハードウェアで実施されるか、プロセッサによって実行されるソフトウェアモジュールで実施されるか、またはその2つの組合せで実施されることができる。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、DVDディスク、または当技術分野で知られている任意の他の形態の記憶媒体中に常駐することができる。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体は、プロセッサに一体化されることができる。プロセッサおよび記憶媒体は、ASIC内に常駐することができる。ASICは、ユーザ端末内に常駐することができる。代替として、プロセッサおよび記憶媒体は、ユーザ端末内に個別コンポーネントとして常駐することもできる。

20

30

#### 【0112】

本発明が特定の例実施形態を参照しながら開示されたが、添付の特許請求の範囲において定義された本発明の領域および範囲から逸脱しなければ、説明された実施形態に対して多数の修正、改変および変更が可能である。したがって、本発明は、説明された実施形態に限定されるものではなく、以下の特許請求の範囲およびその均等物の言い回しによって定義された最大限の範囲を有するものである。

【 図 1 A 】

図 1A

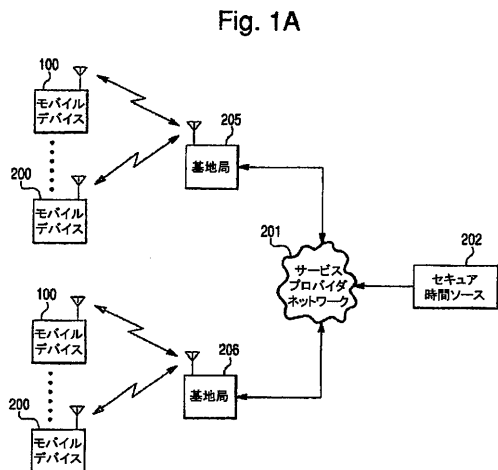


Fig. 1A

【 図 1 B 】

図 1B

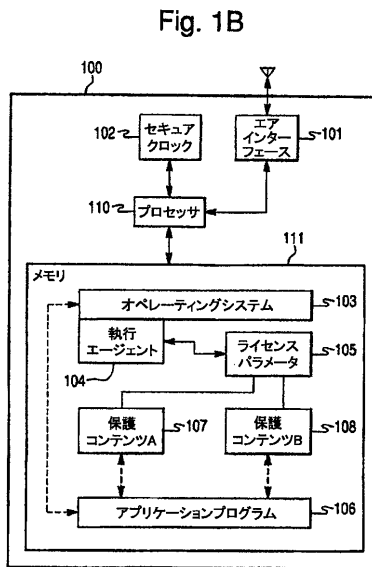


Fig. 1B

【 図 1 C 】

図 1C

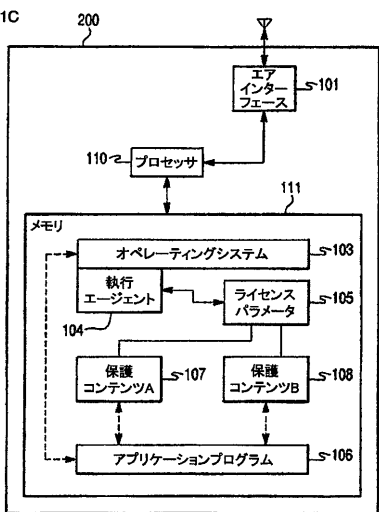


Fig. 1C

【 図 3 】

図 3

Figure 3

ポリシーの事例	TimeCallAtAccess	InCoverageUseLimit	OutCoverageUseLimit	UseInCoverageForRoaming	TimeCallAtStartup	注	悪用からの保護、または制約のレベル	予想されるユーザ経験: 「ユーザの使い勝手の良さ」
1	T	0	0	-	T	デバイス起動時および保護コンテンツにアクセスするときにデータ呼を試みる	最強	極不良
2	T	0	N	T	F	デバイス起動時にデータ呼を試みられない。Nが小さい	強	不良
3	T	0	N	T	T	デバイス起動時にデータ呼を試みる。Nが大きい	可	極不良
4	T	0	N	T	F	デバイス起動時にデータ呼を試みられない。Nが大きい	可	不良
5	T	M	N	T	T	デバイス起動時にデータ呼を試みる。Mが小さい。Nが大きい	可	極不良
6	T	M	N	T	F	デバイス起動時にデータ呼を試みられない。Mが小さい。Nが大きい	可	可
7	T	M	N	-	F	デバイス起動時にデータ呼を試みられない。MおよびNが大きい	可	可
8	F	0	N	T	T	コンテンツにアクセスするとき、データ呼を試みられない。Nが小さい	強	極不良
9	F	0	N	T	F	コンテンツにアクセスするとき、データ呼を試みられない。Nが小さい	優良	不良
10	F	M	N	-	T	デバイス起動時にデータ呼を試みる。MおよびNが適度に小さい	良	不良
11	F	M	N	-	F	データ呼が常に試みられない。MおよびNが小さい	可	良から極不良
12	F	M	N	-	T	MおよびNが大きい。ローミングがカバレッジ内をエミュレートする	弱	不良
13	F	M	N	-	F	MおよびNが大きい。ローミングがカバレッジ内をエミュレートする	極弱	良から極不良
14	F	M	N	-	F	MおよびNが大きい。非常にオープンなポリシー	最弱	優良

【 図 2 】

図 2

Figure 2

パラメータ名	パラメータ値	説明
ExpirationDate	日のカレンダー日付および/または時間	有効日/時
TimeCallAtAccess	TRUEまたはFALSE	コンテンツアクセスの開始時に時間をフェッチする
InCoverageUseLimit	非負整数M	カバレッジ内播予期間アクセス使用制限 (デバイスがカバレッジ内である間のアクセス数)
OutCoverageUseLimit	非負整数N	カバレッジ外播予期間アクセス使用制限 (デバイスがカバレッジ外である間のアクセス数)
UseInCoverageForRoaming	TRUEまたはFALSE	ローミングポリシーがカバレッジ内
TimeCallAtStartup	TRUEまたはFALSE	デバイス起動時にユーザにデータ呼を促す

【 図 4 】

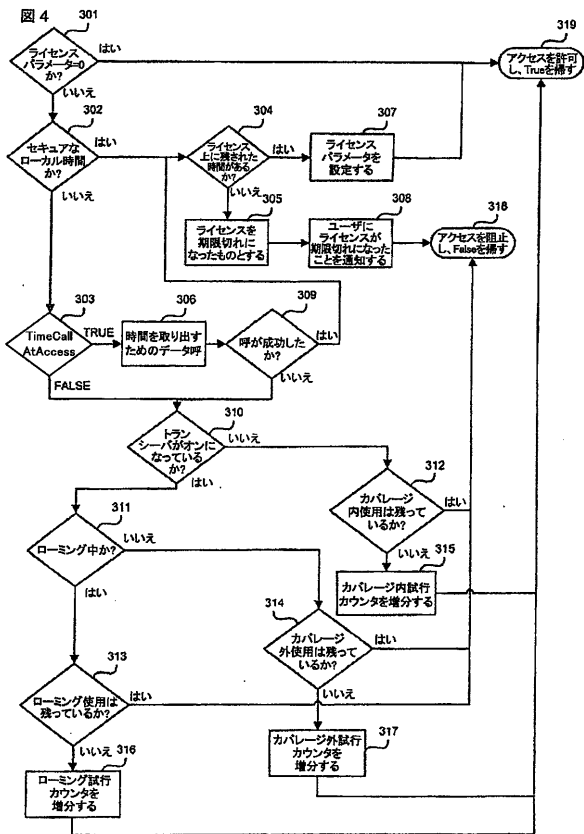


FIG. 4

【 図 4 a 】

図 4a

Figure 4a

```

401 procedure TestContentLicensing( LicenseParameters )
402 {
403   if LicenseParameters == 0;
404     goto AllowAccess.
405   assertion: ReferencedContent has LicenseParameters.
406   if LocalTimeIsSecure();
407     Set STime = SecureDate(Time).
408     goto TestForExpiration.
409   assertion: Local time is not secure.
410   if LicenseParameters.TimeCallAtAccess;
411     Place call to retrieve secure time into STime.
412     if STime was retrieved;
413       goto TestForExpiration.
414   assertion: Secure time cannot be accessed.
415   if Device.Mode == ModeInCoverage;
416     goto CoverageIn.
417   if Device.Mode == ModeRoaming;
418     goto Roaming.
419   else if Device.Mode == ModeOutCoverage;
420     goto CoverageOut.
421 CoverageIn:
422   if LicenseParameters.InUsesAttempts > M;
423     goto BlockAccess.
424   Increment LicenseParameters.InUsesAttempts.
425   goto AllowAccess.
426 Roaming:
427   if LicenseParameters.RoamUsesAttempts > R;
428     goto BlockAccess.
429   Increment LicenseParameters.RoamUsesAttempts.
430   Goto AllowAccess.
431 CoverageOut:
432   if LicenseParameters.OutUsesAttempt > N;
433     goto BlockAccess.
434   Increment LicenseParameters.OutUsesAttempts.
435   goto AllowAccess.
436 TestForExpiration:
437   assertion: STime is secure
438   if STime > LicenseParameters.ExpirationDate;
439     Mark license as expired.
440     Set LicenseParameters.InUsesAttempts > M.
441     Set LicenseParameters.RoamUsesAttempts > R.
442     Set LicenseParameters.OutUsesAttempts > N.
443     Set LicenseParameters.InCoverageUseLimit = 0.
444     Set LicenseParameters.RoamUseLimit = 0.
445     Set LicenseParameters.OutCoverageUseLimit = 0.
446     Inform the user that the license is expired.
447     goto BlockAccess.
448   else:
449     Set LicenseParameters.InUsesAttempts = 0
450     Set LicenseParameters.RoamUsesAttempts = 0
451     Set LicenseParameters.OutUsesAttempts = 0
452     goto AllowAccess.
453 AllowAccess:
454   return True.
455 BlockAccess:
456   return False.
457 }
  
```

【 図 4 b 】

図 4b

Figure 4b

```

401 procedure TestContentLicensing( LicenseParameters )
402 {
403   if LicenseParameters == 0;
404     goto AllowAccess.
405   assertion: ReferencedContent has LicenseParameters.
406   if LocalTimeIsSecure();
407     Set STime = SecureDate(Time).
408     goto TestForExpiration.
409   assertion: Local time is not secure.
410   if LicenseParameters.TimeCallAtAccess;
411     Place call to retrieve secure time into STime.
412     if STime was retrieved;
413       goto TestForExpiration.
414   assertion: Secure time cannot be accessed.
415   if Device.Mode == ModeInCoverage;
416     goto CoverageIn.
417   if Device.Mode == ModeRoaming;
418     goto CoverageForRoaming;
419   else:
420     goto CoverageOut.
421 CoverageIn:
422   if LicenseParameters.InUsesAttempts > M;
423     goto BlockAccess.
424   Increment LicenseParameters.InUsesAttempts.
425   goto AllowAccess.
426 CoverageOut:
427   if LicenseParameters.OutUsesAttempt > N;
428     goto BlockAccess.
429   Increment LicenseParameters.OutUsesAttempts.
430   goto AllowAccess.
431 TestForExpiration:
432   assertion: STime is secure
433   if STime > LicenseParameters.ExpirationDate;
434     Mark license as expired.
435     Set LicenseParameters.InUsesAttempts > M.
436     Set LicenseParameters.OutUsesAttempt > N.
437     Set LicenseParameters.InCoverageUseLimit = 0.
438     Set LicenseParameters.OutCoverageUseLimit = 0.
439     Inform the user that the license is expired.
440     goto BlockAccess.
441   else:
442     Set LicenseParameters.InUsesAttempt = 0
443     Set LicenseParameters.OutUsesAttempt = 0
444     goto AllowAccess.
445 AllowAccess:
446   return True.
447 BlockAccess:
448   return False.
449 }
  
```

【 図 5 】

図 5

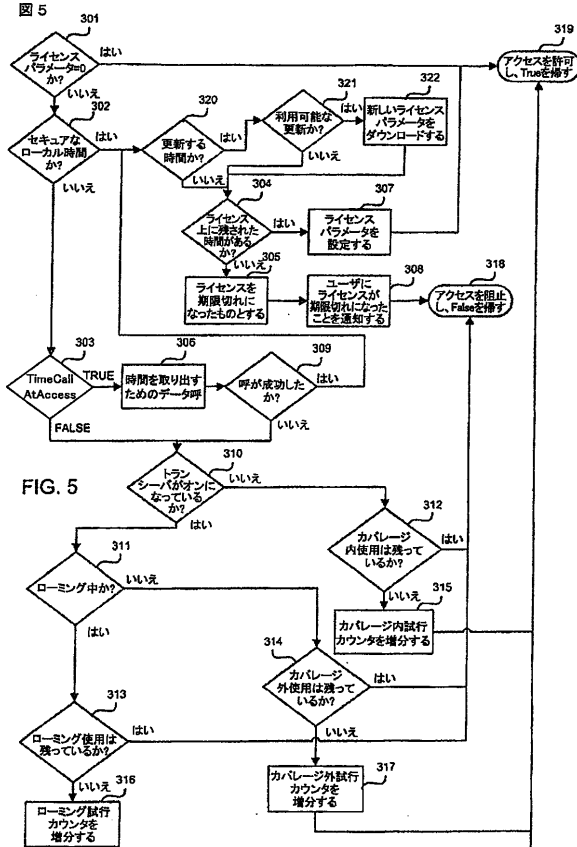


FIG. 5

【 図 5 a 】

図 5a Figure 5a

```

401 procedure TestContentLicense(LicenseParameters)
402 {
403   if LicenseParameters == 0:
404     goto AllowAccess.
405   assertion: ReferencedContent has LicenseParameters.
406   if LocalTimeIsSecure():
407     Set STime = SecureDataTime().
408     goto CheckUpdates.
409   assertion: Local time is not secure.
410   if LicenseParameters.TimeCallAccess:
411     Place call to retrieve secure time into STime.
412     if STime was retrieved:
413       goto CheckUpdates.
414   assertion: Secure time cannot be accessed.
415   if Device.Mode == ModeInCoverage:
416     goto CoverageIn.
417   if Device.Mode == Roaming:
418     goto Roaming.
419   else if Device.Mode == ModeOutCoverage:
420     goto CoverageOut.
421   CoverageIn:
422     if LicenseParameters.InUsesAttempts > M:
423       goto BlockAccess.
424     Increment LicenseParameters.InUsesAttempts.
425     goto AllowAccess.
426   Roaming:
427     if LicenseParameters.RoamUsesAttempts > R:
428       goto BlockAccess.
429     Increment LicenseParameters.RoamUseAttempts.
430     Goto AllowAccess.
431   CoverageOut:
432     if LicenseParameters.OutUsesAttempt > N:
433       goto BlockAccess.
434     Increment LicenseParameters.OutUsesAttempts.
435     goto AllowAccess.
436   TestForExpiration:
437     assertion: STime is secure
438     if STime > LicenseParameters.ExpirationDate:
439       Mark license as expired.
440       Set LicenseParameters.InUsesAttempts > M.
441       Set LicenseParameters.RoamUse Attempt > R
442       Set LicenseParameters.OutUsesAttempt > N.
443       Set LicenseParameters.InCoverageUseLimit = 0.
444       Set LicenseParameters.RoamUseLimit = 0
445       Set LicenseParameters.OutCoverageUseLimit = 0.
446       Inform the user that the license is expired.
447       goto BlockAccess.
448     else:
449       Set LicenseParameters.InUsesAttempt = 0
450       Set LicenseParameters.OutUsesAttempt = 0
451       goto AllowAccess.
452   AllowAccess:
453     return True.
454   BlockAccess:
455     return False.
456   CheckUpdates:
457     if STime == T:
458       Check for update from service provider.
459       if update is available:
460         Open a secure data channel.
461         Send AccessStatistics to provider.
462         Receive NewLicenseParameters from provider.
463         LicenseParameters = NewLicenseParameters.
464         Close secure data channel.
465       else goto Test for Expiration
466     else goto Test for Expiration
467 }
511

```

【 図 6 】

図 6

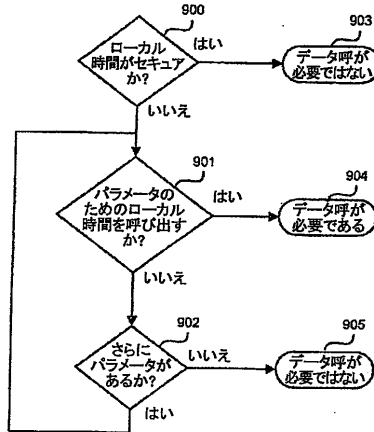


FIG. 6

【 図 6 a 】

図 6a

Figure 6a

```

601 procedure IsStartupTimeFetchNeeded()
602 {
603   if LocalTimeIsSecure():
604     return False.
605   assertion: Local time is not secure.
606   for all license parameters L:
607     if L--TimeCallAccessStartup:
608       return True.
609   assertion: Secure time cannot be accessed.
610   return False.
611 }
612

```

【 図 7 】

図 7

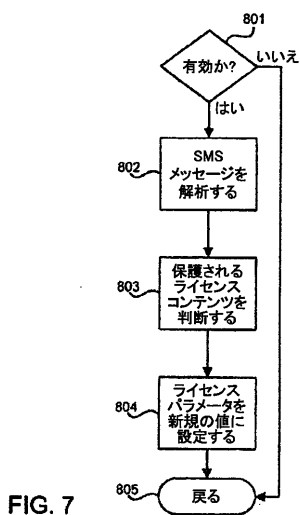


FIG. 7

【 図 7 a 】

図 7a

Figure 7a

```

701 procedure DoLicenseUpdateFromSMS(SMSMessage)
702 {
703   if Validate(SMSMessage):
704     Parse SMSMessage.
705     Determine the protected content license L which SMSMessage identifies.
706     Set L--LicenseParameters to new values.
707     return.
708   assertion: SMSMessage is fake.
709   return.
710 }
711

```

## 【手続補正書】

【提出日】平成24年12月18日(2012.12.18)

## 【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】

モバイルデバイスであって、

プロセッサと、

前記プロセッサに結合され、ワイヤレスネットワークに接続するように構成されたワイヤレスランシーバと、

前記プロセッサに結合されたメモリと、を具備し、前記メモリは、

制限された期間に対して許可された保護コンテンツを前記メモリに記憶すること、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す、前記モバイルデバイス上の第1のパラメータ値をクライアントアクセス可能ではない前記メモリのセキュア部分に記憶することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可することと、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、前記第1のポリシー条件が満たされるかどうかを決定することと、

前記第1のポリシー条件が満たされる限り、前記保護コンテンツへアクセスすることと、

を前記プロセッサに実行させるように構成されたソフトウェア命令を記憶する、モバイルデバイス。

【請求項2】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である第1のパラメータ値を利用する、請求項1に記載のモバイルデバイス。

【請求項3】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である第1のパラメータ値を利用する、請求項1に記載のモバイルデバイス。

【請求項4】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である第1のパラメータ値を利用する、請求項1に記載のモバイルデバイス。

【請求項5】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す第1のパラメータ値を利用する、請求項1に記載のモバイルデバイス。

【請求項6】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す第1のパラメータ値を利用する、請求項1に記載の

モバイルデバイス。

【請求項 7】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、

前記第 1 のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるステップと、

前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードするステップと、

前記第 1 のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶するステップと、

を前記プロセッサに実行させるようにさらに構成される、請求項 1 に記載のモバイルデバイス。

【請求項 8】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータに対する前記ダウンロードされた更新を解析し、解読するステップを前記プロセッサに実行させるようにさらに構成される、請求項 7 に記載のモバイルデバイス。

【請求項 9】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第 1 のパラメータに対する前記更新を SMS メッセージ中で受信するステップを前記プロセッサに実行させるようにさらに構成される、請求項 8 に記載のモバイルデバイス。

【請求項 10】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するステップを前記プロセッサに実行させるようにさらに構成される、請求項 1 に記載のモバイルデバイス。

【請求項 11】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 10 に記載のモバイルデバイス。

【請求項 12】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 10 に記載のモバイルデバイス。

【請求項 13】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 10 に記載のモバイルデバイス。

【請求項 14】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 10 に記載のモバイルデバイス。

【請求項 15】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも 1 つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 10 に記載のモバイルデバイス。

【請求項 16】



前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、  
前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるステップと、  
前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするステップと、  
前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶するステップと、  
を前記プロセッサに実行させるようにさらに構成される、請求項10に記載のモバイルデバイス。

【請求項17】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータに対する前記ダウンロードされた更新を解析し、解読するステップを前記プロセッサに実行させるようにさらに構成される、請求項16に記載のモバイルデバイス。

【請求項18】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータに対する前記更新をSMSメッセージ中で受信するステップを前記プロセッサに実行させるようにさらに構成される、請求項17に記載のモバイルデバイス。

【請求項19】

前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするステップを前記プロセッサに実行させるようにさらに構成される、請求項10に記載のモバイルデバイス。

【請求項20】

モバイルデバイスであって、  
制限された期間に対して許可された保護コンテンツを前記モバイルデバイス上に記憶する手段と、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値をクライアントアクセスできないセキュア方法で前記モバイルデバイス上に記憶するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、前記第1のポリシー条件が満たされるかどうかを決定するための手段と、

前記第1のポリシー条件が満たされる限り、前記保護コンテンツへアクセスするための手段と、

を備えるモバイルデバイス。

【請求項21】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項20に記載のモバイルデバイス。

【請求項22】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項20に記載のモバイルデバイス。

【請求項23】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項20に記載のモバイルデバイス。

## 【請求項 24】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項20に記載のモバイルデバイス。

## 【請求項 25】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項20に記載のモバイルデバイス。

## 【請求項 26】

前記第1のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記第1のパラメータ値に対する前記更新をダウンロードするための手段と、

前記第1のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、

をさらに備える、請求項20に記載のモバイルデバイス。

## 【請求項 27】

前記第1のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項26に記載のモバイルデバイス。

## 【請求項 28】

前記第1のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、請求項26に記載のモバイルデバイス。

## 【請求項 29】

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するための手段をさらに備える、請求項20に記載のモバイルデバイス。

## 【請求項 30】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの少なくとも1つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項29に記載のモバイルデバイス。

## 【請求項 31】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの少なくとも1つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項29に記載のモバイルデバイス。

## 【請求項 32】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの少なくとも1つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項29に記載のモバイルデバイス。

## 【請求項 33】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの少なくとも1つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項29に記載のモバイルデバイス。

## 【請求項 34】

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの少なくとも1つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項29に記載のモバイルデバイス。

## 【請求項 35】

前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保

護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするための手段と、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、

をさらに備える、請求項20に記載のモバイルデバイス。

【請求項36】

前記複数のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項35に記載のモバイルデバイス。

【請求項37】

前記複数のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、請求項35に記載のモバイルデバイス。

【請求項38】

新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするための手段をさらに備える、請求項29に記載のモバイルデバイス。

【請求項39】

モバイルデバイスであって、

保護コンテンツの個別のファイルが制限された期間に対して許可されている前記保護コンテンツのファイルを前記モバイルデバイス上に記憶する手段と、

少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個別のファイルの各々へのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値をクライアントアクセスできないセキュア方法で前記モバイルデバイス上に記憶するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、保護コンテンツの個別のファイルの各々へのアクセスを許可するための手段と、

前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、保護コンテンツの個別のファイルの各々について前記第1のポリシー条件が満たされるかどうかを決定するための手段と、

前記第1のポリシー条件が満たされる限り、保護コンテンツの個別のファイルの各々へアクセスするための手段と、

を備えるモバイルデバイス。

【請求項40】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項39に記載のモバイルデバイス。

【請求項41】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項39に記載のモバイルデバイス。

【請求項42】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項39に記載のモバイルデバイス。

【請求項43】

前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項39に記載のモバイルデバイス。

**【請求項 4 4】**

前記モバイルデバイス上に記憶される前記第 1 のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 3 9 に記載のモバイルデバイス。

**【請求項 4 5】**

前記第 1 のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードするための手段と、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第 1 のポリシー条件を表す前記第 1 のパラメータ値に対する前記更新を、前記モバイルデバイスの記憶するための前記手段に記憶するための手段と、

をさらに備える、請求項 3 9 に記載のモバイルデバイス。

**【請求項 4 6】**

前記第 1 のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項 4 5 に記載のモバイルデバイス。

**【請求項 4 7】**

前記第 1 のパラメータに対する前記更新を SMS メッセージ中で受信し、解析するための手段をさらに備える、請求項 4 5 に記載のモバイルデバイス。

**【請求項 4 8】**

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するための手段をさらに備える、請求項 3 9 に記載のモバイルデバイス。

**【請求項 4 9】**

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、請求項 4 8 に記載のモバイルデバイス。

**【請求項 5 0】**

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、請求項 4 8 に記載のモバイルデバイス。

**【請求項 5 1】**

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、請求項 4 8 に記載のモバイルデバイス。

**【請求項 5 2】**

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの 1 つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 4 8 に記載のモバイルデバイス。

**【請求項 5 3】**

前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、請求項 4 8 に記載のモバイルデバイス。

**【請求項 5 4】**

前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、

前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードす

るための手段と、

前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、

をさらに備える、請求項48に記載のモバイルデバイス。

【請求項55】

前記第1のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、請求項54に記載のモバイルデバイス。

【請求項56】

前記第1のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、請求項54に記載のモバイルデバイス。

【請求項57】

前記記憶された複数のパラメータ値のいずれかが、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示しているかどうかを決定するために、前記モバイルデバイスが電源投入されるたびに前記複数のポリシー条件を表す前記記憶された複数のパラメータ値の各々を問い合わせるための手段をさらに備える、請求項48に記載のモバイルデバイス。

【請求項58】

新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするための手段をさらに備える、請求項48に記載のモバイルデバイス。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0112

【補正方法】変更

【補正の内容】

【0112】

本発明が特定の例実施形態を参照しながら開示されたが、添付の特許請求の範囲において定義された本発明の領域および範囲から逸脱しなければ、説明された実施形態に対して多数の修正、改変および変更が可能である。したがって、本発明は、説明された実施形態に限定されるものではなく、以下の特許請求の範囲およびその均等物の言い回しによって定義された最大限の範囲を有するものである。

以下に本件出願当初の特許請求の範囲に記載された発明を付記する。

[1] モバイルデバイス上で保護コンテンツへのアクセスを制限するための方法であって、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を前記モバイルデバイス上に記憶することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可することと、前記モバイルデバイスが前記セキュア時間ソースへのアクセスを有し場合、前記第1のポリシー条件が満たされるかどうかを決定することと、前記第1のポリシー条件が満たされる限り、前記保護コンテンツへのアクセスを与えることと、を備える方法。

[2] 前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[1]に記載の方法。

[3] 前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[1]に記載の方法。

[4] 前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[1]に記載の方法。

[5] 前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるた

びに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 1 ]に記載の方法。

[ 6 ] 前記第 1 のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 1 ]に記載の方法。

[ 7 ] 前記第 1 のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、前記更新が存在する場合、前記第 1 のパラメータ値に対する前記更新をダウンロードすることと、前記第 1 のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶することと、をさらに備える、[ 1 ]に記載の方法。

[ 8 ] 前記第 1 のパラメータに対する前記更新は、暗号化され認証されたファイル中でダウンロードされる、[ 7 ]に記載の方法。

[ 9 ] 前記第 1 のパラメータに対する前記更新は、SMSメッセージ中で受信される、[ 7 ]に記載の方法。

[ 10 ] 前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶することをさらに備える、[ 1 ]に記載の方法。

[ 11 ] 前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数であり、前記複数のパラメータ値のうちの別の 1 つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[ 10 ]に記載の方法。

[ 12 ] 前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[ 10 ]に記載の方法。

[ 13 ] 前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスがローミング中であるときに前記モバイルデバイスがどのようにアクセス試行を扱うべきかを示す、[ 10 ]に記載の方法。

[ 14 ] 前記複数のパラメータ値のうちの 1 つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 10 ]に記載の方法。

[ 15 ] 前記複数のパラメータ値のうちの 1 つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 10 ]に記載の方法。

[ 16 ] 前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードすることと、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す、前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶することと、をさらに備える、[ 10 ]に記載の方法。

[ 17 ] 前記複数のパラメータに対する前記更新は、暗号化され認証されたファイル中でダウンロードされる、[ 16 ]に記載の方法。

[ 18 ] 前記複数のパラメータに対する前記更新は、SMSメッセージ中で受信される、[ 16 ]に記載の方法。

[ 19 ] 新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードする、[ 10 ]に記載の方法。

[ 20 ] モバイルデバイス上で保護コンテンツの個々のファイルへのアクセスを制限するための方法であって、少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第 1 のポ

リシー条件を表す第1のパラメータ値を前記モバイルデバイス上に記憶することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、保護コンテンツの個々の各ファイルへのアクセスを許可することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、保護コンテンツの個々の各ファイルについて前記第1のポリシー条件が満たされるかどうかを決定することと、前記第1のポリシー条件が満たされる限り、保護コンテンツの個々の各ファイルへのアクセスを与えることと、を備える方法。

[21] 前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[20]に記載の方法。

[22] 前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[20]に記載の方法。

[23] 前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[20]に記載の方法。

[24] 前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[20]に記載の方法。

[25] 前記第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[20]に記載の方法。

[26] 前記第1のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、前記更新が存在する場合、前記第1のパラメータ値に対する前記更新をダウンロードすることと、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第1のポリシー条件を表す前記第1のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶することと、をさらに備える、[20]に記載の方法。

[27] 前記第1のパラメータに対する前記更新は、暗号化され認証されたファイルにダウンロードされる、[26]に記載の方法。

[28] 前記第1のパラメータに対する前記更新は、SMSメッセージ中で受信される、[26]に記載の方法。

[29] 前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶することをさらに備える、[20]に記載の方法。

[30] 前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[29]に記載の方法。

[31] 前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[29]に記載の方法。

[32] 前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[29]に記載の方法。

[33] 前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値のうちの一つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[29]に記載の方法。

[34] 前記モバイルデバイスの前記メモリに記憶された前記複数のパラメータ値の

うちの1つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[29]に記載の方法。

[35] 前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせることと、前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードすることと、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶することと、をさらに備える、[29]に記載の方法。

[36] 前記複数のパラメータに対する前記更新は、暗号化されたファイル中でダウンロードされる、[35]に記載の方法。

[37] 前記複数のパラメータに対する前記更新は、SMSメッセージ中で受信される、[35]に記載の方法。

[38] 前記記憶された複数のパラメータ値のいずれかが、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示しているかどうかを決定するために、前記モバイルデバイスが電源投入されるたびに前記複数のポリシー条件を表す前記記憶された複数のパラメータ値の各々を問い合わせることをさらに備える、[29]に記載の方法。

[39] 新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードする、[29]に記載の方法。

[40] モバイルデバイスであって、プロセッサと、前記プロセッサに結合され、ワイヤレスネットワークに接続するように構成されたワイヤレスランシーバと、前記プロセッサに結合されたメモリであって、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を前記モバイルデバイス上に記憶することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可することと、前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、前記第1のポリシー条件が満たされるかどうかを決定することと、前記第1のポリシー条件が満たされる限り、前記保護コンテンツへのアクセスを与えることと、を備えるステップを前記プロセッサに実行させるように構成されたソフトウェア命令を記憶したメモリとを備えるモバイルデバイス。

[41] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である第1のパラメータ値を利用する、[40]に記載のモバイルデバイス。

[42] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である第1のパラメータ値を利用する、[40]に記載のモバイルデバイス。

[43] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である第1のパラメータ値を利用する、[40]に記載のモバイルデバイス。

[44] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す第1のパラメータ値を利用する、[40]に記載のモバイルデバイス。

[45] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバ



イルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す第1のパラメータ値を利用する、[40]に記載のモバイルデバイス。

[46] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるステップと、前記更新が存在する場合、前記第1のパラメータ値に対する前記更新をダウンロードするステップと、前記第1のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶するステップと、を前記プロセッサに実行させるようにさらに構成される、[40]に記載のモバイルデバイス。

[47] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータに対する前記ダウンロードされた更新を解析し、解読するステップを前記プロセッサに実行させるようにさらに構成される、[46]に記載のモバイルデバイス。

[48] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータに対する前記更新をSMSメッセージ中で受信するステップを前記プロセッサに実行させるようにさらに構成される、[47]に記載のモバイルデバイス。

[49] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するステップを前記プロセッサに実行させるようにさらに構成される、[40]に記載のモバイルデバイス。

[50] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[49]に記載のモバイルデバイス。

[51] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[49]に記載のモバイルデバイス。

[52] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[49]に記載のモバイルデバイス。

[53] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも1つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[49]に記載のモバイルデバイス。

[54] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令によって利用される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[49]に記載のモバイルデバイス。

[55] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるステップと、前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするステップと、前記複数のパラメータ値に対する前記更新を前記モバイルデバイスの前記メモリに記憶するステップと、を前記プロセッサに実行させるようにさらに構成される、[49]に記載のモバイルデバイス。

[56] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータに対する前記ダウンロードされた更新を解析し、解読するステップを前記プロセッサに実行させるようにさらに構成される、[55]に記載のモバイルデバイス。

[57] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、前記第1のパラメータに対する前記更新をSMSメッセージ中で受信するステップを前記プロセッサ

サに実行させるようにさらに構成される、[ 5 6 ]に記載のモバイルデバイス。

[ 5 8 ] 前記モバイルデバイスの前記メモリ中の前記ソフトウェア命令は、新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするステップを前記プロセッサに実行させるようにさらに構成される、[ 4 9 ]に記載のモバイルデバイス。

[ 5 9 ] モバイルデバイスであって、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を前記モバイルデバイス上に記憶するための手段と、前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定するための手段と、前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、前記保護コンテンツへのアクセスを許可するための手段と、前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、前記第1のポリシー条件が満たされるかどうかを決定するための手段と、前記第1のポリシー条件が満たされる限り、前記保護コンテンツへのアクセスを与えるための手段と、を備えるモバイルデバイス。

[ 6 0 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[ 5 9 ]に記載のモバイルデバイス。

[ 6 1 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[ 5 9 ]に記載のモバイルデバイス。

[ 6 2 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[ 5 9 ]に記載のモバイルデバイス。

[ 6 3 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 5 9 ]に記載のモバイルデバイス。

[ 6 4 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 5 9 ]に記載のモバイルデバイス。

[ 6 5 ] 前記第1のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、前記更新が存在する場合、前記第1のパラメータ値に対する前記更新をダウンロードするための手段と、前記第1のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、をさらに備える、[ 5 9 ]に記載のモバイルデバイス。

[ 6 6 ] 前記第1のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、[ 6 5 ]に記載のモバイルデバイス。

[ 6 7 ] 前記第1のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、[ 6 5 ]に記載のモバイルデバイス。

[ 6 8 ] 前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するための手段をさらに備える、[ 5 9 ]に記載のモバイルデバイス。

[ 6 9 ] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[ 6 8 ]に記載のモバイルデバイス。

[ 7 0 ] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[ 6 8 ]に記載のモバイルデバイス。

[ 7 1 ] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間ア

クセス試行の回数である、[ 6 8 ]に記載のモバイルデバイス。

[ 7 2 ] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも1つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 6 8 ]に記載のモバイルデバイス。

[ 7 3 ] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうち少なくとも1つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 6 8 ]に記載のモバイルデバイス。

[ 7 4 ] 前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするための手段と、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、をさらに備える、[ 5 9 ]に記載のモバイルデバイス。

[ 7 5 ] 前記複数のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、[ 7 4 ]に記載のモバイルデバイス。

[ 7 6 ] 前記複数のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、[ 7 4 ]に記載のモバイルデバイス。

[ 7 7 ] 新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするための手段をさらに備える、[ 6 8 ]に記載のモバイルデバイス。

[ 7 8 ] モバイルデバイスであって、少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を前記モバイルデバイス上に記憶するための手段と、前記モバイルデバイスが前記セキュア時間ソースへアクセスするかどうかを決定するための手段と、前記モバイルデバイスが前記セキュア時間ソースへアクセスする場合、保護コンテンツの個々の各ファイルへのアクセスを許可するための手段と、前記モバイルデバイスが前記セキュア時間ソースへアクセスしない場合、保護コンテンツの個々の各ファイルについて前記第1のポリシー条件が満たされるかどうかを決定するための手段と、前記第1のポリシー条件が満たされる限り、保護コンテンツの個々の各ファイルへのアクセスを与えるための手段と、を備えるモバイルデバイス。

[ 7 9 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[ 7 8 ]に記載のモバイルデバイス。

[ 8 0 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[ 7 8 ]に記載のモバイルデバイス。

[ 8 1 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[ 7 8 ]に記載のモバイルデバイス。

[ 8 2 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 7 8 ]に記載のモバイルデバイス。

[ 8 3 ] 前記モバイルデバイス上に記憶される前記第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 7 8 ]に記載のモバイルデバイス。

[ 8 4 ] 前記第1のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、前記更新が存在

する場合、前記第1のパラメータ値に対する前記更新をダウンロードするための手段と、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに保護コンテンツの個々の各ファイルへのアクセスを制御する第1のポリシー条件を表す前記第1のパラメータ値に対する前記更新を、前記モバイルデバイスの記憶するための前記手段に記憶するための手段と、をさらに備える、[78]に記載のモバイルデバイス。

[85] 前記第1のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、[84]に記載のモバイルデバイス。

[86] 前記第1のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、[84]に記載のモバイルデバイス。

[87] 前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を記憶するための手段をさらに備える、[78]に記載のモバイルデバイス。

[88] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[87]に記載のモバイルデバイス。

[89] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[87]に記載のモバイルデバイス。

[90] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[87]に記載のモバイルデバイス。

[91] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの1つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[87]に記載のモバイルデバイス。

[92] 前記モバイルデバイス上に記憶される前記複数のパラメータ値のうちの1つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[87]に記載のモバイルデバイス。

[93] 前記複数のパラメータ値に対する更新が存在するかどうかを決定するために周期的に保護コンテンツプロバイダサーバに問い合わせるための手段と、前記更新が存在する場合、前記複数のパラメータ値に対する前記更新をダウンロードするための手段と、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値に対する前記更新を前記モバイルデバイス上に記憶するための手段と、をさらに備える、[87]に記載のモバイルデバイス。

[94] 前記第1のパラメータに対する前記ダウンロードされた更新を解読するための手段をさらに備える、[93]に記載のモバイルデバイス。

[95] 前記第1のパラメータに対する前記更新をSMSメッセージ中で受信し、解析するための手段をさらに備える、[93]に記載のモバイルデバイス。

[96] 前記記憶された複数のパラメータ値のいずれかが、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示しているかどうかを決定するために、前記モバイルデバイスが電源投入されるたびに前記複数のポリシー条件を表す前記記憶された複数のパラメータ値の各々を問い合わせるための手段をさらに備える、[87]に記載のモバイルデバイス。

[97] 新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするための手段をさらに備える、[87]に記載のモバイルデバイス。

[98] 保護コンテンツをモバイルデバイスに提供するためのサーバであって、保護コンテンツの個々のファイルと、少なくとも、前記モバイルデバイスがセキュア時間ソ-

スへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を含むデータベースと、を記憶した大容量記憶メモリと、前記大容量記憶メモリに結合され、ワイヤレスネットワークに接続するように構成されたプロセッサであって、前記モバイルデバイスによる保護コンテンツをダウンロードする要求を受信するステップと、前記要求に回答して前記保護コンテンツを前記モバイルデバイスに送信するステップと、少なくとも、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す第1のパラメータ値を前記モバイルデバイスに送信するステップと、をプロセッサ実行可能ソフトウェア命令によって実行するように構成されたプロセッサと、を備えるサーバ。

[ 9 9 ] 前記少なくとも第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[ 9 8 ]に記載のサーバ。

[ 1 0 0 ] 前記少なくとも第1のパラメータ値は、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[ 9 8 ]に記載のサーバ。

[ 1 0 1 ] 前記少なくとも第1のパラメータ値は、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[ 9 8 ]に記載のサーバ。

[ 1 0 2 ] 前記少なくとも第1のパラメータ値は、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 9 8 ]に記載のサーバ。

[ 1 0 3 ] 前記少なくとも第1のパラメータ値は、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 9 8 ]に記載のサーバ。

[ 1 0 4 ] 前記プロセッサは、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する第1のポリシー条件を表す前記少なくとも第1のパラメータ値を更新するために前記大容量記憶メモリにアクセスするようにプロセッサ実行可能ソフトウェア命令によって構成される、[ 9 8 ]に記載のサーバ。

[ 1 0 5 ] 前記プロセッサは、前記少なくとも第1のパラメータ値に対する更新が前記大容量記憶メモリ中に存在するかどうかを決定する問合せ要求を前記モバイルデバイスから受信するステップと、前記更新が存在する場合、前記少なくとも第1のパラメータ値に対する前記更新を行う前記モバイルデバイスに送信するステップと、をプロセッサ実行可能ソフトウェア命令によって実行するようにさらに構成される、[ 1 0 4 ]に記載のサーバ。

[ 1 0 6 ] 前記プロセッサは、暗号化され認証されたファイルとして前記少なくとも第1のパラメータに対する前記更新を送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、[ 1 0 5 ]に記載のサーバ。

[ 1 0 7 ] 前記プロセッサは、SMSメッセージを生成し、前記少なくとも第1のパラメータに対する前記更新をSMSメッセージとして送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、[ 1 0 5 ]に記載のサーバ。

[ 1 0 8 ] 前記プロセッサは、前記更新が存在する場合、前記更新が前記モバイルデバイスに対して行われるとすぐに、前記少なくとも第1のパラメータ値に対する前記更新を送信するステップを実行するようにプロセッサ実行可能ソフトウェア命令によってさらに構成される、[ 1 0 4 ]に記載のサーバ。

[ 1 0 9 ] 前記大容量記憶メモリは、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す複数のパラメータ値を含む、[ 9 8 ]に記載のサーバ。

[ 1 1 0 ] 前記複数のパラメータ値のうちの1つは、前記モバイルデバイスがサービ

スネットワークカバレッジ外であるときの許可された猶予期間アクセス試行の回数である、[ 1 0 9 ]に記載のサーバ。

[ 1 1 1 ] 前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがサービスネットワークカバレッジ内であるときの許可された猶予期間アクセス試行の回数である、[ 1 0 9 ]に記載のサーバ。

[ 1 1 2 ] 前記複数のパラメータ値のうちの一つは、前記モバイルデバイスがローミング中であるときの許可された猶予期間アクセス試行の回数である、[ 1 0 9 ]に記載のサーバ。

[ 1 1 3 ] 前記複数のパラメータ値のうちの一つは、前記保護コンテンツへのアクセスが許可されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 1 0 9 ]に記載のサーバ。

[ 1 1 4 ] 前記複数のパラメータ値のうちの一つは、前記モバイルデバイスが電源投入されるたびに前記モバイルデバイスがリモートセキュア時間ソースにアクセスしなければならないかどうかを示す、[ 1 0 9 ]に記載のサーバ。

[ 1 1 5 ] 前記プロセッサは、前記モバイルデバイスがセキュア時間ソースへアクセスしないときに前記保護コンテンツへのアクセスを制御する複数のポリシー条件を表す前記複数のパラメータ値の前記各々を更新するために前記大容量記憶メモリにアクセスするようにプロセッサ実行可能ソフトウェア命令によって構成される、[ 1 0 9 ]に記載のサーバ。

[ 1 1 6 ] 前記プロセッサは、前記複数のパラメータ値のいずれかに対する更新が前記大容量記憶メモリ中に存在するかどうかを決定する問合せ要求を前記モバイルデバイスから受信するステップと、前記更新が存在する場合、前記複数のパラメータ値に対する前記更新を行う前記モバイルデバイスに送信するステップと、をプロセッサ実行可能ソフトウェア命令によって実行するようにさらに構成される、[ 1 1 5 ]に記載のサーバ。

[ 1 1 7 ] 前記プロセッサは、暗号化されたファイル中で前記複数のパラメータ値に対する前記更新を送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、[ 1 1 6 ]に記載のサーバ。

[ 1 1 8 ] 前記プロセッサは、SMSメッセージを生成し、前記複数のパラメータ値に対する前記更新をSMSメッセージとして送信するようにプロセッサ実行可能ソフトウェア命令によって構成される、[ 1 1 6 ]に記載のサーバ。

[ 1 1 9 ] 前記プロセッサは、新しい保護コンテンツの購入とともに前記複数のパラメータ値に対する更新をダウンロードするステップを実行するようにプロセッサ実行可能ソフトウェア命令によってさらに構成される、[ 1 0 9 ]に記載のサーバ。

## フロントページの続き

- (74)代理人 100095441  
弁理士 白根 俊郎
- (74)代理人 100075672  
弁理士 峰 隆司
- (74)代理人 100119976  
弁理士 幸長 保次郎
- (74)代理人 100153051  
弁理士 河野 直樹
- (74)代理人 100140176  
弁理士 砂川 克
- (74)代理人 100158805  
弁理士 井関 守三
- (74)代理人 100172580  
弁理士 赤穂 隆雄
- (74)代理人 100179062  
弁理士 井上 正
- (74)代理人 100124394  
弁理士 佐藤 立志
- (74)代理人 100112807  
弁理士 岡田 貴志
- (74)代理人 100111073  
弁理士 堀内 美保子
- (74)代理人 100134290  
弁理士 竹内 将訓
- (72)発明者 イバン・マククリーン  
アメリカ合衆国、カリフォルニア州 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5
- (72)発明者 ケネス・エム．・ゲイブ  
アメリカ合衆国、カリフォルニア州 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5
- (72)発明者 ローレンス・ジー．・ランドブレード  
アメリカ合衆国、カリフォルニア州 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5
- (72)発明者 チャンユ・エル．・ダモレ  
アメリカ合衆国、カリフォルニア州 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5
- (72)発明者 ブライアン・エイチ．・ケリー  
アメリカ合衆国、カリフォルニア州 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5

【外国語明細書】

2013080484000001.pdf