(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年5 月7 日 (07.05.2009)

PCT

(10) 国際公開番号
WO 2009/057652 A1

(51) 国際特許分類:
G06F 21/24 (2006.01) *G06F 21/20* (2006.01)

(21) 国際出願番号: PCT/JP2008/069671

(22) 国際出願日: 2008 年10 月29 日 (29.10.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2007-280800
2007 年10 月29 日 (29.10.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目１番１号 Tokyo (JP). 東芝ソリューション株式会社 (TOSHIBA SOLUTIONS CORPORATION) [JP/JP]; 〒1056691 東京都港区芝浦一丁目１番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 岡田 光司 (OKADA, Koji) [JP/JP]. 池田 竜朗 (IKEDA, Tatsuro) [JP/JP]. 山田 正隆 (YAMADA, Masataka) [JP/JP]. 西澤 実 (NISHIZAWA, Minoru) [JP/JP]. 中溝 孝則 (NAKAMIZO, Takanori) [JP/JP]. 岡本 利夫 (OKAMOTO, Toshio) [JP/JP].

(74) 代理人: 鈴江 武彦, 外(SUZUYE, Takehiko et al.); 〒1050001 東京都港区虎ノ門１丁目１２番９号 鈴榮特許綜合事務所内 Tokyo (JP).

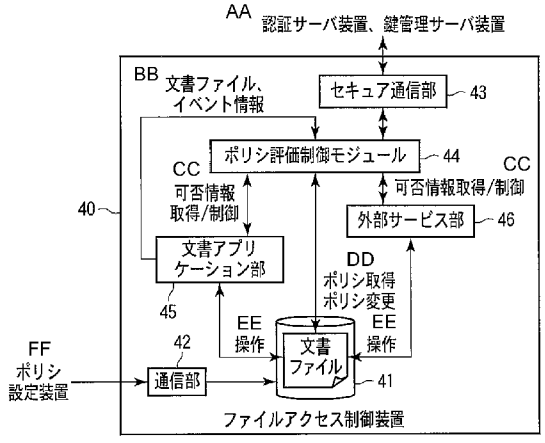
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

/続葉有/

(54) **Title:** FILE ACCESS CONTROL DEVICE AND PROGRAM

(54) 発明の名称: ファイルアクセス制御装置及びプログラム

[図9]



AA AUTHENTICATION SERVER DEVICE, KEY MANAGEMENT SERVER DEVICE
BB DOCUMENT FILE, EVENT INFORMATION
CC ENABLED/DISABLED INFORMATION ACQUISITION/CONTROL
DD POLICY ACQUISITION/POLICY MODIFICATION
EE OPERATION
FF POLICY SETTING DEVICE
40 FILE ACCESS CONTROL DEVICE
43 SECURE COMMUNICATION UNIT
44 POLICY EVALUATION CONTROL MODULE
45 DOCUMENT APPLICATION UNIT
46 EXTERNAL SERVICE UNIT
42 COMMUNICATION UNIT
41 DOCUMENT FILE

(57) **Abstract:** In a file access control system, control information corresponding to an operation is attached as a responsibility policy in advance to a document file. Next, a policy evaluation control module (44) evaluates and executes a responsibility policy in the document file according to the operation on the document file. The execution of the responsibility policy includes control of a document application unit based on the responsibility execution. Accordingly, it is possible to perform active control in accordance with the operation on the document and modify access control to the document.

(57) 要約: 本発明の一実施形態に係るファイルアクセス制御システムにおいては、予め操作に応じた制御情報を責務型ポリシとして文書ファイルに付与する。次に、文書ファイルに対する操作に応じて、ポリシ評価制御モジュール４４が文書ファイル内の責務型ポリシを評価及び実行する。この責務型ポリシの実行には、責務実行行為に基づく文書アプリケーション部の制御が含まれる。従って、文書に対する操作に応じて、能動的な制御を実施でき、また、文書へのアクセス制御を変更できる。

WO 2009/057652 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

ファイルアクセス制御装置及びプログラム

技術分野

[0001] 本発明は、文書ファイルを適切に保護するようにアクセス制御を実行するファイルアクセス制御装置及びプログラムに係り、例えば、文書ファイルに対する操作に基づいて、能動的な制御を実施でき、また、文書へのアクセス制御を変更し得るファイルアクセス制御装置及びプログラムに関する。

背景技術

[0002] 近年、特定の情報や処理に対するアクションを、権限情報に基づいて制御するアクセス制御技術の重要性が大きく高まってきている。このような技術としては、例えば、個人情報や承認処理に対するアクション要求を受けると、アクション要求者(アクセス主体、又はサブジェクト)が所有する権限情報と、権限情報とアクションの可否パターンを示したアクセス制御ルール又はアクセス制御ポリシに基づいて、当該アクションの実行可否を決定する方式がある。

[0003] アクセス制御ポリシとは、一般的に、アクセス制御ルールの集合として考えられる。アクセス制御ポリシは、標準的な記述仕様(例えば、Tim Moses, ″eXtensible Access Control Markup Language(XACML) Version 2.0″, [online], [2007年10月01日検索]、インターネット<URL:http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-NORMATIVE.zip>を参照。)が公開されたこともあり、広く利用されてきている。なお、この標準的な記述仕様では、付随的な要素として、責務(Obligation)を規定する要素が記述されている。この責務要素は、一般的に「～しなければならない」という責務行為内容を記述することを想定している。しかしながら、この標準的な記述仕様には、責務要素の詳細な内容記述が規定されていない。また、標準的な記述仕様には、責務を含めた場合のアクセス制御ポリシの取扱い、及び評価結果に対する処理方法が規定されていない。

[0004] 一方、文書ファイルに対するアクセス制御方法には、権限情報をセキュリティ属性として付与する方式がある。この方式では、例えば、ファイルに対する権限情報を「閲

覧許可」や「編集許可」といったアクション可否形式で記述し、権限情報をユーザに割り当てる。この種の権限情報は、アクセス制御マトリックス(Access Control Matrix)やアクセス制御リスト(Access Control List)として知られている。例えば特開2005－56418号公報では、「セキュリティコンテナ」として文書ファイルに権限(ルール)を付与する方法が示されている。

[0005] しかしながら、アクション可否形式では、許可されるアクセス時間やアクセス場所といった条件や、より詳細な制限などの如き、詳細で柔軟なアクセス制御内容を記述することが困難となっている。近年、アクセス制御ポリシ又はライセンスの如きを必要とする分野、特に一般的な文書アプリケーションなどでは、より詳細なアクセス制御内容を記述可能なアクセス制御ポリシ形式のアクセス制御方式が必要とされるようになってきている。

発明の開示

[0006] 上記説明の背景技術により、より詳細なアクセス制御内容を記述できるようになってきているが、それは主に特定のアクセスに対して許可か否かを判断するに留まっている。しかしながら、本発明者の検討によれば、文書等に対する制御という観点からみれば、特定のアクセスに対して許可か否かを判断するだけではなく、より能動的な制御を行う必要があると考える。例えば、文書ファイルに有効期限が設定され、有効期限が切れた場合、単純にアクセスを禁止するだけではなく、当該文書ファイルを能動的に削除したいという要求が存在すると考察される。これは、単純に有効期限が切れた文書ファイルへのアクセスを禁止するだけでは、文書ファイルそのものは存在し続けるため、潜在的なリスクが残り続けることになるからである。

[0007] また、文書ファイルを操作する状況において、操作した時点で当該文書のステータスが遷移するため、権限を変更したい場合がある。具体的には、適切な承認を介して発行された正規文書を編集操作したとき、「正規文書」を示すステータスが「非正規文書」を示すステータスに遷移するため、取り扱いの権限を「印刷許可」から「印刷禁止」に変更したい場合がある。

[0008] しかしながら、従来のアクセス制御方式では、ステータスの遷移前後にかかわらず、文書アプリケーションを起動した時の権限を継続的に適用している。このため、編集

後の非正規文書が「印刷許可」の取り扱い権限により印刷され、誤って配布される心配がある。

[0009] このように、従来のアクセス制御方式では、文書への操作に応じて、能動的な制御を実施したり、文書へのアクセス制御を変更できないという不都合がある。

[0010] 本発明の目的は、文書への操作に応じて、能動的な制御を実施でき、また、文書へのアクセス制御を変更し得るファイルアクセス制御装置及びプログラムを提供することにある。

[0011] 本発明の一つの局面(aspect)は、文書内容と禁止型ポリシ及び責務型ポリシとを含む文書ファイルを記憶可能な記憶装置、ポリシ評価制御モジュール、文書アプリケーション部及び外部サービス部を備え、前記文書ファイルへのアクセスを制御するためのファイルアクセス制御装置であって、前記ポリシ評価制御モジュールとしては、前記文書アプリケーション部及び外部サービス部からそれぞれ実行可否情報を取得して保持する可否情報取得手段と、ユーザの操作内容に対応したイベント情報及び前記記憶装置内の文書ファイルが前記文書アプリケーション部から入力されると、予め決められた評価情報リストに基づいて、前記ユーザの認証結果及びユーザ属性情報を取得する認証結果取得手段と、前記評価情報リストに基づいて、前記可否情報取得手段から実行可否情報を取得すると、この実行可否情報、前記認証結果及び前記ユーザ属性情報からなる評価情報、前記イベント情報、前記禁止型ポリシ及び前記責務型ポリシを送出する手段と、前記送出された評価情報内の認証結果及びユーザ属性情報並びにイベント情報と、前記禁止型ポリシに予め記述された認証結果、ユーザ属性情報及びイベント情報とをそれぞれ比較し、比較結果がそれぞれ一致していれば、前記禁止型ポリシに予め記述された許可又は禁止を示す評価結果を送出する禁止型ポリシ評価手段と、前記評価情報内の実行可否情報、前記イベント情報及び前記評価結果と、前記責務型ポリシに予め記述された実行可否情報、前記イベント情報及び前記評価結果とをそれぞれ比較し、比較結果がそれぞれ一致していれば、前記責務型ポリシに予め記述された責務実行主体及び責務実行行為を含む制御情報を送出する責務型ポリシ評価手段と、前記制御情報を受けると、前記制御情報内の責務実行主体に基づいて、当該制御情報を送出する制御管理手段と、前

記制御管理手段から送出された制御情報内の責務実行行為に基づいて、前記文書アプリケーション部を制御する文書アプリケーション制御手段とを備えたファイルアクセス制御装置である。

[0012] 本発明の一つの局面によれば、予め操作に応じた制御情報を責務型ポリシとして文書ファイルに付与する。次に、文書ファイルに対する操作に応じて、ポリシ評価制御モジュールが文書ファイル内の責務型ポリシを評価及び実行する。責務型ポリシの実行には、責務実行行為に基づく文書アプリケーション部の制御が含まれる。従って、文書に対する操作に応じて、能動的な制御を実施でき、また、文書へのアクセス制御を変更することができる。

図面の簡単な説明

[0013] [図1]図1は、本発明の第1の実施形態に係るファイルアクセス制御装置が適用されたファイルアクセス制御システムの構成例を示す模式図である。

[図2]図2は、同実施形態における認証サーバ装置の構成を示すブロック図である。

[図3]図3は、同実施形態における鍵管理サーバ装置の構成を示すブロック図である。

[図4]図4は、同実施形態におけるポリシ設定装置の構成を示すブロック図である。

[図5]図5は、同実施形態に係る文書ファイルの構成例を示す模式図である。

[図6]図6は、同実施形態における責務型ポリシを説明するための模式図である。

[図7]図7は、同実施形態における責務型ポリシを説明するための模式図である。

[図8]図8は、同実施形態における責務型ポリシを説明するための模式図である。

[図9]図9は、同実施形態におけるファイルアクセス制御装置の構成を示すブロック図である。

[図10]図10は、同実施形態におけるポリシ評価制御モジュールの構成を示すブロック図である。

[図11]図11は、同実施形態におけるファイルアクセス制御装置のハードウェア資源とソフトウェアとの組合せ構成を示す模式図である。

[図12]図12は、同実施形態における動作を説明するためのフローチャートである。

[図13]図13は、同実施形態における動作の変形例を説明するためのフローチャート

である。

発明を実施するための最良の形態

[0014] 以下、本発明の各実施形態について図面を用いて説明する。なお、以下の各装置は、装置毎に、ハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、予めネットワーク又は記憶媒体から対応する装置のコンピュータにインストールされ、対応する装置の機能を実現させるためのプログラムが用いられる。

[0015] （第1の実施形態）

図1は本発明の第1の実施形態に係るファイルアクセス制御装置が適用されたファイルアクセス制御システムの構成例を示す模式図である。このファイルアクセス制御システムは、認証サーバ装置10、鍵管理サーバ装置20、ポリシ設定装置30及びファイルアクセス制御装置40が互いにネットワークを介して接続されている。なお、認証サーバ装置10及び鍵管理サーバ装置20は、必須ではなく、例えばファイルアクセス制御装置40内でユーザ認証及び鍵管理を実行する場合などには省略可能となっている。この場合、ファイルアクセス制御装置40は、後述する認証用記憶装置11、ユーザ認証部13、鍵管理用記憶装置21及び鍵管理部23を付加した構成とすればよく、さらに各記憶装置11，21を、後述する記憶装置41に含めた構成としてもよい。

[0016] ここで、認証サーバ装置10は、図2に示すように、認証用記憶装置11、セキュア通信部12及びユーザ認証部13を備えている。

[0017] 認証用記憶装置11は、ユーザ認証部13から読出／書込可能であり、予めユーザ認証を行うための認証情報とユーザ属性情報とを互いに関連付けて保存している。認証情報は、例えばパスワードや認証鍵といったユーザ認証に用いる情報である。ユーザ属性情報とは、ユーザの個人名や、ユーザの属するグループ（ロール）の情報である。グループ（ロール）とは、例えば会社における役職、部門や、任意に設定されたユーザグループである。

[0018] セキュア通信部12は、ユーザ認証部13と、ポリシ設定装置30又はファイルアクセス制御装置40との間に安全な通信路を確保して両者を通信可能とする機能とをもっている。なお、セキュア通信部12はユーザ認証部13に含めてもよい。安全な通信路の

確保は、例えば、SSL(secure socket layer)やIPsec(IP security protocol)等の暗号通信プロトコル等により実現可能であり、これは他のセキュア通信部22, 32, 43でも同様である。

[0019] ユーザ認証部13は、ポリシ設定装置30からセキュア通信部12を介して認証情報及びユーザ属性情報を受けると、当該認証情報とユーザ属性情報とを互いに関連付けて認証用記憶装置11に書き込む機能と、ファイルアクセス制御装置40からセキュア通信部12を介してユーザ認証要求を受けると、セキュア通信部12を介してファイルアクセス制御装置40のユーザとの間でユーザ認証を行い、その認証結果やユーザ属性情報をセキュア通信部12からポリシ評価制御モジュール44に送信する機能を備えている。なお、認証情報およびユーザ属性情報は、ポリシ設定装置30から受け取る以外にも、例えば、認証サーバ装置が備える図示しない入力装置を介してサーバ管理者により入力されても良いし、その他手段により入力されても良い。

[0020] 鍵管理サーバ装置20は、図3に示すように、鍵管理用記憶装置21、セキュア通信部22及び鍵管理部23を備えている。

[0021] 鍵管理用記憶装置21は、鍵管理部23から読出／書込可能であり、文書特定情報と鍵情報とを互いに関連付けて保存している。文書特定情報は、例えばファイル名のように、文書ファイルを特定可能な情報である。鍵情報は、例えば共通鍵暗号方式の鍵情報であり、文書ファイルの暗号化に用いた鍵情報である。

[0022] セキュア通信部22は、鍵管理部23と、ポリシ設定装置30又はファイルアクセス制御装置40との間に安全な通信路を確保して両者を通信可能とする機能とをもっている。なお、セキュア通信部22は鍵管理部23に含めてもよい。

[0023] 鍵管理部23は、ポリシ設定装置30からセキュア通信部12を介して文書特定情報及び鍵情報を受けると、当該文書特定情報と鍵情報とを互いに関連付けて鍵管理用記憶装置21に書き込む機能と、ファイルアクセス制御装置40からセキュア通信部22を介して鍵送信要求を受けると、鍵送信要求内の文書特定情報に基づいて、鍵管理用記憶装置21から読み出した鍵情報をセキュア通信部22からファイルアクセス制御装置40に送信する機能をもっている。

[0024] ポリシ設定装置30は、図4に示すように、ポリシ設定用記憶装置31、セキュア通信

部32、通信部33及びポリシ設定部34を備えている。

[0025] ポリシ設定用記憶装置31は、ポリシ設定部34から読出／書込可能であり、文書ファイル、共通鍵及び署名鍵を保存している。この署名鍵は、ポリシ設定装置30の署名鍵（ポリシ設定装置30の秘密鍵）でもよく、ユーザ端末の署名鍵（ユーザ端末の秘密鍵）でもよい。

[0026] セキュア通信部32は、ポリシ設定部34と、認証サーバ装置10又は鍵管理サーバ装置20との間に安全な通信路を確保して両者を通信可能とする機能とをもっている。なお、セキュア通信部32はポリシ設定部34に含めてもよい。

[0027] 通信部33は、ポリシ設定部34と、ファイルアクセス制御装置40との間で通信を実行する機能をもっている。

[0028] ポリシ設定部34は、文書ポリシ設定者の操作により、セキュア通信部32を介して認証情報及びユーザ属性情報を認証サーバ装置10に送信する機能と、文書ポリシ設定者の操作により、セキュア通信部32を介して文書特定情報及び鍵管理情報を鍵管理サーバ装置20に送信する機能と、文書ポリシ設定者の操作により、ポリシ設定用記憶装置31内の文書ファイルのアクセス制御ポリシを文書ポリシ設定者により入力された値又は予め決められた値に設定する機能と、文書ポリシ設定者の操作により、ポリシ設定用記憶装置31内の文書ファイルを通信部33からファイルアクセス制御装置40に送信する機能とをもっている。

[0029] また、ポリシ設定部34は、文書内容を暗号化する機能、又は文書内容及びアクセス制御ポリシを分離できない形式で暗号化する機能を備えていても良い。分離できない形式で暗号化するとは、例えば文書内容とアクセス制御ポリシを併せて暗号化することである。ポリシ設定部34は、（暗号化された）文書内容及びアクセス制御ポリシの改竄を防ぐために、ポリシ設定用記憶装置31に記憶されているポリシ設定装置30の署名鍵（ポリシ設定装置30の秘密鍵）によりデジタル署名を生成する機能を備えていても良い。

[0030] ここで、文書（document）ファイルの具体例を図5に示す。文書ファイルd10は文書内容d11、アクセス制御ポリシd12、セキュリティ情報d15を含んでいる。

[0031] 文書内容d11は、文書特定情報としてのファイル名、所謂文書内容であるテキスト、

書式、マクロなどの情報が含まれる。また、文書の情報だけではなく、図面やプログラムなどの情報が含まれていても良く、文書アプリケーション特有の制御情報を含んでいても良い。また、文書内容d11は文書属性を含んでもよい。文書属性としては、例えば、作成者(個人名／作成部門)、所有者(文書管理責任部門)、作成日時(最終編集日時)、機密区分(極秘、秘、社外秘、公開)、ステータス情報(正規、ドラフト)、開示情報(開示、非開示)、有効期限、取り扱い関係者、などが適宜使用可能となっている。この文書属性は、後述する責務型ポリシd14の制御情報に基づき、更新される場合がある。

[0032] アクセス制御ポリシd12には、文書ポリシ設定者が設定する文書へのアクセス制御条件が記述される。具体的には、アクセス制御ポリシd12は、禁止型ポリシd13と、責務型ポリシd14との2種類のポリシが記述される。

[0033] 禁止型ポリシd13とは、『「アクセス主体(Subject)」は、「操作(action)」を許可(禁止)』という形式のルール集合である。ここで「アクセス主体」とは、操作を行う主体であり、例えばユーザやロールなどである。ここで「操作」とは、文書の新規作成、閲覧(文書を開く)、編集、印刷、複写、当該文書内容の全体または一部の複製などの操作である。よって禁止型ポリシd13は、例えば、『ユーザAは、閲覧を許可』や、『作成部門以外は、編集を禁止』などのルールが記述される。

[0034] 一方、責務型ポリシd14とは、『「条件」が成り立つ場合は、「制御」を実施』という形式のルール集合である。ここで「条件」とは、ユーザの認証可否や文書属性の有無、環境情報(例えば、時間情報)の状態などであり、さらに複数の条件がAND(論理積)やOR(論理和)で結合された条件集合でも良い。「制御」とは、文書アプリケーション、外部サービスの制御やアクセス制御ポリシの変更などの制御である。外部サービスの詳細については後述する。

[0035] ここで、責務型ポリシd14について図6～図8に示す例を参照しながら説明する。責務型ポリシd14においては、例えば、以下の要素を用いて責務内容(前記責務型ポリシにおける「制御」に当たる)を表現可能となっている。“subject”(主体)、“action”(行為)、“resource”(リソース)、“environment”(環境)、“complement”(補体)などである。

[0036] “subject”(主体)は責務の実行主体を示し、“action”(行為)は責務の実行内容を示す。“resource”(リソース)は責務の実行客体を示し、“environment”(環境)は責務を実行すべき環境を示す。“complement”(補体)は、責務の行為内容を補足する。

[0037] これら要素を、非特許文献1に記載のXACML V2．0を利用して記述したポリシ例を図6に示す。

[0038] 図6中、責務(Obligation)要素の属性割当て(AttributeAssignment)要素として、責務内容を表現している。責務を構成する要素を属性割当て要素の属性ID(Attribute ID)属性値として表現している。属性ID属性値“subject”を持つ属性割当て要素は、責務を実行すべき主体を示している。明示的に指定されている場合には、指定された責務主体が実行しなければならないことを示している。(暗黙的に)省略されている場合は、評価を要求した主体が責務主体にあたる。記述例では、サービス名称を文字列表現している。より特定した形式にする場合には、データ型(DataType)属性値を指定したい形式に対応した値にすればよい。これは、以降の責務要素の各属性割当て要素においても同様である。

[0039] 属性ID属性値“action”を持つ属性割当て要素は、責務の実行すべき行為を示している。原則的に、この属性は、明示的に指定されることが望ましい。また、属性ID属性値“subject”を持つ属性割当て要素と同様に、行為名称を文字列表現しており、より特定した形式にする場合には、データ型属性値を指定したい形式に対応した値にすればよい。この例では、データ型属性値を“DeleteFile”としており、ファイルを削除することを指定している。削除対象となるファイルは、属性ID属性値“resource”を持つ属性割当て要素を指定していないため、リクエスト要求に含まれるリソース要素と同一のリソースと解釈する。URI(Uniform Resource Identifier)形式などで明示的に指定した場合は、指定されたリソース(ファイル)が削除対象となる。その場合は、属性ID属性値“resource”を持つ属性割当て要素として定義すればよい。

[0040] 属性ID属性値“environment”を持つ属性割当て要素は、この記述例では省略しているが、責務の実行環境を指定する必要がある場合に記述してもよい。例えば、特定日(「2007年10月01日」)に責務を実行させたい場合は、図7に示すように記述する。

[0041] 属性ID属性値“complement”を持つ属性割当て要素は、この記述例では省略して

いる。属性ID属性値“action”を持つ属性割当て要素を補足する内容がある場合に記載される。例えば、属性ID属性値“action”を持つ属性割当て要素が、特定の機能を制限する行為を示す値を持つとき、制限する機能を示すために利用する。例えば、下記のような例では、属性ID属性値“action”を持つ属性割当て要素で、機能を制限することを示す“DisableFunctions”値を定義したとすると、制限する機能内容を属性ID属性値“complement”を持つ属性割当て要素で定義することができる。図8に示す例では、“Print”値により「印刷」機能を制限することを示している。

[0042] また、図6～図8に示す例では、責務の実行契機（前記責務型ポリシの「条件」に当たる）は、XACML V2．0で規定されている通りのものを利用している（責務要素のFulfillOn属性）。

[0043] 図6～図8に示す表記は、XACML V2．0の記法を拡張して、本実施形態で必要なポリシを表記できることを示した一例である。このため、他のポリシ表記法を用いたり、例と同様にXACML V2．0を利用したりする場合でも、本実施形態で必要な要素を表現できるのであれば、例に示したものと異なる表現を用いてもよい。

[0044] 一方、セキュリティ情報d15には、文書内容d11等が暗号化されているか否かを示す暗号状態情報と、暗号化に用いたアルゴリズムを特定可能な暗号化アルゴリズム特定情報、暗号化に用いた鍵を特定可能な鍵特定情報が記述される。さらに、セキュリティ情報d15には、ポリシ設定部34により生成されたデジタル署名と、このデジタル署名を検証する検証鍵を特定可能な検証鍵特定情報が記述されても良い。このとき、暗号状態情報、暗号化アルゴリズム特定情報、鍵特定情報、検証鍵特定情報そのものがセキュリティ情報として含まれていない場合であっても、これらの暗号状態情報、暗号化アルゴリズム特定情報、鍵特定情報、検証鍵特定情報が図示しない保管サーバ装置や鍵管理サーバ装置20の各記憶装置に記憶されている場合にそれらの記憶場所を指定する取得先アドレス情報（URLやURIなど）を暗号状態情報、暗号化アルゴリズム特定情報、鍵特定情報、検証鍵特定情報に代えてセキュリティ情報に含まれていても構わない。この場合、暗号状態情報、暗号化アルゴリズム特定情報、鍵特定情報、検証鍵特定情報がそれぞれ変更した場合であっても、図示しないサーバ装置や鍵管理サーバ20内部で変更しておけば構わない。

[0045] 続いて、ファイルアクセス制御装置40について説明する。

[0046] ファイルアクセス制御装置40は、図9に示すように、記憶装置41、通信部42、セキュア通信部43、ポリシ評価制御モジュール44、文書アプリケーション部45及び外部サービス部46を備えている。

[0047] 記憶装置41は、各部42～46から読出／書込可能であり、文書ファイルd10を記憶するものである。

[0048] 通信部42は、ポリシ設定装置30と通信するものであり、ポリシ設定装置30から受けた文書ファイルd10を記憶装置41に書き込む機能をもっている。なお、通信部42は外部サービス部46に含めてもよい。

[0049] セキュア通信部43は、認証サーバ装置10及び鍵管理サーバ装置20との間で安全な通信路を確保して両者を通信可能とする機能と、ポリシ評価制御モジュール44から受けた鍵特定情報、検証鍵特定情報または上述した取得先アドレス情報に基づいて、図示しないサーバ装置又は鍵管理サーバ装置20等から文書ファイルに対応した鍵情報やデジタル署名の検証鍵を取得してポリシ評価制御モジュール44に送出する機能とをもっている。なお、セキュア通信部43は、後述するポリシ評価制御モジュール44内の復号・署名検証部44b及び評価情報取得部44cに含めてもよい。

[0050] ポリシ評価制御モジュール44は、文書アプリケーション部45から入力されたイベント情報及び文書ファイルに基づいて、文書ファイルd10に記述されたアクセス制御ポリシd12を評価する機能と、その評価結果に基づいて、文書アプリケーション部45と外部サービス部46とを制御する機能と、当該評価結果に基づいて、記憶装置41内の文書ファイルd10の文書属性及びアクセス制御ポリシd12を変更する機能とを備えた耐タンパなモジュールである。イベント情報とは、文書の新規作成、閲覧（文書を開く）、編集、印刷、複写、当該文書内容の全体または一部の複製などを命令する操作に応じたコマンド情報である。耐タンパとは、機能の実行の不正な改竄・攻撃に対して耐性を持っているという意味である。

[0051] さらに、ポリシ評価制御モジュール44は、セキュア通信部43を介して認証サーバ装置10から認証結果やユーザ属性情報を取得する機能と、セキュア通信部43を介して鍵管理サーバ装置20から鍵情報を取得する機能と、文書アプリケーション部45や

外部サービス部46の状態（制御が可能か否か）を取得する機能とを備えている。ポリシ評価制御モジュール44は、一般的には文書アプリケーションのプラグインソフトウェアとして実装され、図示しない演算処理装置が当該プラグインソフトウェアのプログラムを実行することにより各機能を実現している。但し、ポリシ評価制御モジュール44は、プラグインソフトウェアに限らず、プラグインではないソフトウェアのプログラムを実行することにより各機能を実現するものとしてもよい。さらに、ポリシ評価制御モジュール44は、文書アプリケーションの提供ベンダや他のサービス提供ベンダ等が用意している特定Webサイトからダウンロードし、ファイルアクセス制御装置40にインストールされることによって当該ファイルアクセス制御装置40内に構成されることとしても良い。

[0052] 文書アプリケーション部45は、文書ファイルd10への外部からの操作に対応するイベント情報及び文書ファイルをポリシ評価制御モジュール44に入力する機能と、ポリシ評価制御モジュール44に制御され、文書内容d11に対する操作を制御する機能と、イベント情報に基づいて文書内容d11に対する操作を実行する機能とをもっている。操作を制御する機能とは、操作を許可又は禁止するように制御する機能と、操作を実行するように制御する機能とがある。操作を許可又は禁止するように制御する機能には、例えば、文書内容d11の閲覧だけを許可する機能や、文書内容d11の印刷を禁止する機能がある。操作を実行するように制御する機能には、例えば、文書内容d11を削除する機能がある。なお、文書アプリケーション部45は、耐タンパな文書アプリケーションプログラムを演算処理装置（図示せず）が実行することにより各機能を実現している。特に、文書アプリケーション部45が文書ファイルd10を操作する際、操作中の文書ファイルが外部から別途操作されないよう保護されていることが望ましい。これは、例えば文書ファイルを保護された形でメモリ上に複製し、その複製した文書ファイルに対して操作を行い、保存時にその操作結果を元の文書ファイルに反映させることで実現される。この場合、ポリシ評価制御モジュール44へは、文書ファイルそのものの入力に代えて、メモリ上に複製された文書ファイルへのポインタが入力され、ポリシ評価制御モジュール44ではこのメモリ上に複製された文書ファイルに対して操作を行う。

[0053] 外部サービス部46とは、文書アプリケーションが実行されるプラットフォーム上に備えられたサービス機能をもっている。ここで、サービス機能としては、例えば文書ファイルd10の削除サービス機能や、メールサービス機能などが適用可能となっている。また、外部サービス部46は、外部サービス用プログラムを演算処理装置(図示せず)が実行することにより各機能を実現している。

[0054] 次に、ポリシ評価制御モジュール44の内部構成を図10に示す。ポリシ評価制御モジュール44は、イベント制御部44a、復号・署名検証部44b、評価情報取得部44c、責務実行可否情報取得部44d、禁止型ポリシ評価部44e、責務型ポリシ評価部44f、制御管理機能44g、文書アプリケーション制御部44h、文書ファイル制御部44i及び外部サービス制御部44jを備えている。

[0055] イベント制御部44aは、文書アプリケーション部45からイベント情報及び文書ファイルd10が入力されると、イベント情報が「文書の閲覧(文書を開く)」であるか否かを判定する機能と、判定結果が「文書の閲覧」の場合には、文書ファイルd10のセキュリティ情報d15に基づいて文書内容d11及びアクセス制御ポリシd12が暗号化されているか否かを判定する機能と、当該セキュリティ情報d15がデジタル署名を含むか否かを判定する機能とをもっている。

[0056] イベント制御部44aは、判定の結果、文書内容d11等が暗号化されている場合、又はセキュリティ情報d15がデジタル署名を含む場合には、文書ファイルd10を復号・署名検証部44bに送出して復号処理及び署名検証処理を実行させる機能と、復号・署名検証部44bの各処理が成功した場合には、復号された文書内容d11及びアクセス制御ポリシd12を含む文書ファイルd10及びイベント情報を評価情報取得部44cに送出する機能とをもっている。ここで署名検証処理を簡単に説明すれば、セキュリティ情報d15にデジタル署名が含まれている場合に、ファイルアクセス制御装置40が署名鍵(例えばポリシ設定装置30の秘密鍵)に対する公開鍵を用いて署名検証(送信相手が正当な送信相手であるか否か、通信途中で当該文書内容d11が改竄等されていないかを判断)する処理がその一例である。

[0057] また、イベント制御部44aは、判定の結果、イベント情報が「文書の閲覧」ではなく「文書の保存」や「文書の印刷」である場合には、そのイベント情報が入力されている

際に開いている文書ファイル及びイベント情報を評価情報取得部44cに送出する機能をもっている。

[0058] なお、元々文書ファイルd10が暗号化されず、デジタル署名が付与されない運用の場合には、セキュリティ情報d15、イベント制御部44a及び復号・署名検証部44bが省略される一方、文書アプリケーション部45から入力されたイベント情報及び文書ファイルd10が評価情報取得部44cに入力される。

[0059] 復号・署名検証部44bは、イベント制御部44aから文書ファイルd10を受けると、文書ファイルd10のセキュリティ情報d15に基づいて文書内容d11及びアクセス制御ポリシd12が暗号化されているか否かを判定する機能と、当該セキュリティ情報d15がデジタル署名を含むか否かを判定する機能と、判定の結果、文書内容d11等が暗号化されている場合、又はセキュリティ情報d15がデジタル署名を含む場合には、文書内容d11等を鍵情報に基づいて復号する機能と、検証鍵に基づいてデジタル署名を検証する機能と、復号結果及び検証結果をイベント制御部44aに送出する機能とをもっている。

[0060] 復号・署名検証部44bは、復号のための鍵情報をセキュリティ情報d15に基づいて鍵管理サーバ装置20から取得する機能を有するが、これに限らず、別途異なる手段で鍵情報を取得しても良い。同様に、復号・署名検証部44bは、検証のための検証鍵をセキュリティ情報d15に基づいて鍵管理サーバ装置20等から取得する機能を有するが、これに限らず、別途異なる手段で検証鍵を取得しても良い。例えばデジタル署名の生成に用いた署名鍵がユーザの署名鍵の場合には、検証鍵はファイルアクセス制御装置40の記憶装置41から読み出すことにより、取得してもよい。復号・署名検証部44bは、復号又は署名検証に失敗した場合には、処理を停止する。また、復号・署名検証部44bは、文書内容d11のみが暗号化されている場合には、この時点では復号せずに、禁止型ポリシd13又は責務型ポリシd14が評価された後に復号しても良い。

[0061] 評価情報取得部44cは、予め決められた評価情報リストに記載の評価情報の種別、又は入力された文書ファイルd10のアクセス制御ポリシd12の評価に必要な評価情報を外部から取得する機能を備えている。評価情報リストとは、入力された文書ファイ

ルd10内のアクセス制御ポリシd12の評価に必要か否かにかかわらず、アクセス制御ポリシd12に記述される可能性をもつ全ての評価情報の種別が記載されたリストである。このような評価情報リストは、例えばプログラムコードの一部として記述される。

[0062] 評価情報とは、例えば、ユーザの認証結果、ユーザ属性情報、時間情報、外部機能の実行可否情報、などが使用可能となっている。上記した禁止型ポリシの用語定義における「アクセス主体」を特定できる情報や同様に上記した責務型ポリシの用語定義における「条件」を評価するための情報に相当するものも同様に評価情報に含まれる。

[0063] 評価情報取得部44cは、イベント制御部44aから文書ファイル及びイベント情報を受けると、ユーザの認証結果及びユーザ属性情報を取得する場合、ユーザ認証の要求をセキュア通信部43から認証サーバ装置10に送信し、認証結果(成功又は失敗)及びユーザの属性情報を認証サーバ装置10から取得する機能を備えている。

[0064] 評価情報取得部44cは、時間情報を取得する場合、外部から時間情報等を取得する機能を備えている。

[0065] 評価情報取得部44cは、実行可否情報を取得する場合、実行可否情報送出要求を責務実行可否情報取得部44dに送出し、実行可否情報を責務実行可否情報取得部44dから取得する機能と、所定時間経過後に更新後の実行可否情報を責務実行可否情報取得部44dから取得する機能とをもっている。

[0066] また、評価情報取得部44cは、文書ファイルd10のアクセス制御ポリシd12、イベント情報及び評価情報(例、ユーザの認証結果、ユーザ属性情報、時間情報、外部機能の実行可否情報、など)を禁止型ポリシ評価部44eに送出する機能を備えている。

[0067] 責務実行可否情報取得部44dは、責務型ポリシd14の制御実行に必要な外部機能の制御が可能か否かの実行可否情報を、文書アプリケーション制御部44h、文書ファイル制御部44i及び外部サービス制御部44jから個別に取得して保持する機能と、評価情報取得部44cから実行可否情報送出要求を受けると、これら実行可否情報を評価情報取得部44cに送出する機能と、実行可否情報を更新した場合には更新後の実行可否情報を評価情報取得部44cに送出する機能とをもっている。ここで、外部機能の制御としては、文書アプリケーション部45や様々な外部サービス部46、及

び文書ファイルd10の制御などが該当する。これら文書アプリケーション部45、様々な外部サービス部46のサービスが稼働している場合と稼働していない場合とによって、実行可否情報の結果も制御可能と制御不可能とに分かれることとなる。

[0068] 責務実行可否情報取得部44dは、ポリシ評価制御モジュール44にイベント情報及び文書ファイルが入力された時点で実行可否情報を取得してもよく、評価情報取得部44cから要求された時点で実行可否情報を取得してもよい。また、責務実行可否情報取得部44dは、定期的に実行可否情報を更新してもよい。

[0069] 禁止型ポリシ評価部44eは、評価情報取得部44cから入力されたイベント情報、評価情報に基づいて、アクセス制御ポリシd12に記述された禁止型ポリシd13を評価する機能と、評価の後、イベント情報、評価情報、禁止型ポリシd13の評価結果(許可又は禁止)及びアクセス制御ポリシd12に記載された責務型ポリシd14を責務型ポリシ評価部へ送出する機能とをもっている。

[0070] 禁止型ポリシd13の評価とは、禁止型ポリシd13に記述されたルールのうち、「操作」がイベント情報に一致し、「アクセス主体」が評価情報に含まれるアクセス主体を特定できる情報に一致するものに対して、その結果(許可又は禁止)を出力することである。具体的には、例えば、入力されたイベント情報が閲覧であり、禁止型ポリシに『ユーザAは、閲覧を許可』というルールの記述がある場合は、評価情報としてユーザAの認証結果が入力されており、その認証結果が成功の場合に、評価結果として許可を出力する。

[0071] 補足すると、禁止型ポリシ評価部44eは、禁止型ポリシd13を評価するとき、取得した認証結果及びユーザ属性情報並びに入力されたイベント情報と、禁止型ポリシd13に予め記述された認証結果、ユーザ属性情報及びイベント情報とをそれぞれ比較し、比較結果がそれぞれ一致していれば、禁止型ポリシd13に予め記述された許可又は禁止を示す評価結果を送出する。なお、禁止型ポリシd13は、一致するルールがない、またはルールが全くないということがないように記述されていることが望ましい。これは、例えば一致するルールがない場合に出力するデフォルト評価結果を禁止型ポリシd13に記述することで実現される。

[0072] 責務型ポリシ評価部44fは、禁止型ポリシ評価部44eから入力されたイベント情報、

評価情報、禁止型ポリシ44eの評価結果に基づいて、責務型ポリシd14を評価する機能と、評価の後、実施する制御情報を制御管理部44gへ出力する機能とをもっている。

[0073] 責務型ポリシd14の評価とは、責務型ポリシd14に記述されたルールについて「条件」が満たされるか否を評価し、条件が満たされる場合にはその「制御情報」を出力することである。

[0074] 具体的には、責務型ポリシd14に『イベント情報が閲覧であり、かつ、禁止型ポリシの評価結果が許可であり、かつメールサービスが実行可ならば、メールでユーザ名を通知する』というルールの記述がある場合、イベント情報が「閲覧」で、かつ、禁止型ポリシd13の評価結果が「許可」で、かつ、メールサービスの実行可否情報が「制御可能」であれば、「メールでユーザ名を通知する」という制御情報を制御管理部44gへ出力する。

[0075] さらに、『日付が2008年1月1日以降ならば、文書内容を消去する』というルールの記述がある場合、評価情報に含まれる時間情報が条件を満たすならば、「文書内容を消去」という制御情報を制御管理部44gへ出力する。このとき、複数のルールで条件が満たされる場合は、全ての制御情報を制御管理部44gへ出力する。

[0076] 補足すると、責務型ポリシ評価部44fは、責務型ポリシd14を評価するとき、取得した実行可否情報、イベント情報及び評価結果と、責務型ポリシに予め記述された実行可否情報、イベント情報及び評価結果とをそれぞれ比較し、比較結果がそれぞれ一致していれば、責務型ポリシd14に予め記述された責務実行主体及び責務実行行為を含む制御情報を制御管理部44gに送出する。

[0077] 制御管理部44gは、責務型ポリシ評価部44fから制御情報を受けると、予め決められた順序に従い、この制御情報に記述された責務実行主体に基づいて、当該制御情報を文書アプリケーション制御部44h、文書ファイル制御部44i又は外部サービス制御部44jに送出する機能をもっている。

[0078] 文書アプリケーション制御部44hは、制御管理部44gから送出された制御情報内の責務実行行為に基づいて、文書アプリケーション部45を制御する機能をもっている。ここで、制御とは、文書内容d11に対する操作に関する制御であり、例えば、文書内

容d11の閲覧だけを許可する制御や、印刷を禁止する制御や、文書内容d11を消去する制御などである。さらに、文書アプリケーション制御部44hは、責務実行可否情報取得部44dから要求を受けると、文書アプリケーション部45に対する制御を実行可能か否かの実行可否情報を当該文書アプリケーション部45から取得して責務実行可否取得部44dに送出する機能をもっている。

[0079] 文書ファイル制御部44iは、制御管理部44gから送出された制御情報内の責務実行行為に基づいて、記憶装置41内の文書ファイルd10のアクセス制御ポリシd12やセキュリティ情報d15を変更する機能をもっている。例えば、アクセス制御ポリシd12のルール変更やセキュリティ情報d15の変更である。アクセス制御ポリシd12のルール変更は、禁止型ポリシd13又は責務型ポリシd14のいずれを変更してもよい。セキュリティ情報d15の変更とは、例えば暗号化しないなどの変更や、鍵情報を変えて暗号化し直すなどの変更である。また、文書ファイル制御部44iは、制御管理部44gから送出された制御情報内の責務実行行為に基づいて、記憶装置41内の文書ファイルd10の文書内容d11における文書属性を変更する機能を更に備えてもよい。文書属性の変更としては、例えば、ステータス情報を“正規”から“ドラフト”に変える等がある。

[0080] 外部サービス制御部44jは、制御管理部44gから送出された制御情報内の責務実行行為に基づいて、外部サービス部46を制御する機能をもっている。ここで制御とは、例えばメールサービスであれば、メーラを強制的に起動させたり、メールを送信させたりするといった制御である。すなわち、外部サービス制御部44jは、責務実行行為に基づいて、外部サービス部46としてのメーラを強制的に起動させる機能を有してもよい。また、外部サービス制御部44jは、この起動した又は以前から起動済みの当該メーラに対し、例えば、メールでユーザ名を通知するように制御を実行してもよい。通知先は、例えばポリシ設定装置30等であるが、これに限らず、任意の通知先が責務実行行為に設定可能である。さらに、外部サービス制御部44jは、各外部サービスに対する制御が実行可能であるか否かの実行可否情報を取得する機能を備えている。

[0081] なお、ポリシ評価制御モジュール44に入力されたイベント情報が「保存」であり、かつ入力された文書ファイルのセキュリティ情報d15において暗号化が指定されている

場合には、文書ファイルを再暗号化して保存することが望ましい。これは、ポリシ評価制御モジュール44が、ポリシ設定部34と同様な文書内容を暗号化する機能、又は文書内容及びアクセス制御ポリシを分離できない形式で暗号化する機能を備えることにより実現できる。

[0082] なお、以上のようなファイルアクセス制御装置40は、例えば図11に示すように、実現してもよい。ここで、前述した記憶装置41は、プログラム実行時にはメモリ41'に対応し、文書ファイルd10の更新時にはメモリ41'及び記憶装置41"に対応する。なお、メモリ41'はRAM等のメモリであり、記憶装置41"はハードディスク装置等の補助記憶装置である。

[0083] 前述した通信部42及び外部サービス部46は、通信部42に対応する外部メールプログラムを含む外部サービスプログラム46'、演算処理装置50、通信部51、入力部52及び出力部53により実現してもよい。なお、演算処理装置50は、プログラムを実行して各機能を実現するものである。通信部51はネットワークとファイルアクセス制御装置40内との間の通信インタフェースである。入力部52はキーボード等の入力装置である。但し、入力部は、入力装置が外部にある場合、外部の入力装置との間の入力インタフェースとしてもよい。出力部53は液晶ディスプレイ等の表示装置である。但し、出力部53は、表示装置が外部にある場合、外部の表示装置との間の出力インタフェースとしてもよい。また、出力部53は、外部のプリンタ装置に接続される場合、プリンタ装置との間の出力インタフェースを更に備えてもよい。

[0084] 前述したセキュア通信部43及びポリシ評価制御モジュール44は、ポリシ評価制御プログラム44'、通信部51及び演算処理装置50により実現してもよい。

[0085] 前述した文書アプリケーション部45は、文書アプリケーションプログラム45'、演算処理装置50、入力部52及び出力部53により実現してもよい。

[0086] 各プログラム44', 45', 46'は、コンピュータ読み取り可能な記憶媒体Mからファイルアクセス装置40にインストールされた後、演算処理装置50に実行されると、各機能が実現可能となる。

[0087] 次に、以上のように構成されたファイルアクセス制御システムの動作を図12及び図13のフローチャートを用いて説明する。

[0088] （準備）

予め認証サーバ装置10においては、ポリシ設定装置30から受けた認証情報とユーザ属性情報とが互いに関連付けられて認証用記憶装置11に書き込まれているとする。

[0089] 続いて、ポリシ設定装置30においては、文書内容d11にアクセス制御ポリシd12を設定するとする。

[0090] ポリシ設定装置30においては、ポリシ設定部34が、文書ポリシ設定者の操作により、ポリシ設定用記憶装置31内の文書ファイルd10のアクセス制御ポリシd12を文書ポリシ設定者により入力された値又は予め決められた値に設定する。

[0091] このとき、ポリシ設定部34は、ポリシ設定用記憶装置31内の共通鍵に基づいて、文書内容d11及びアクセス制御ポリシd12を暗号化するとする。また、ポリシ設定部34は、暗号化した文書内容d11及びアクセス制御ポリシd12に対し、ポリシ設定用記憶装置31内の署名鍵によりデジタル署名を生成する。

[0092] さらに、ポリシ設定部34は、暗号状態情報、暗号化アルゴリズム特定情報、鍵特定情報、デジタル署名及び検証鍵特定情報を含むセキュリティ情報d15を作成する。また、ポリシ設定部34は、暗号化した文書内容d11及びアクセス制御ポリシd12と、セキュリティ情報d15とからなる文書ファイルd10をポリシ設定用記憶装置31に書き込む。

[0093] 次に、ポリシ設定装置30においては、ポリシ設定部34が、文書ポリシ設定者の操作により、セキュア通信部32を介して文書特定情報及び鍵管理情報を鍵管理サーバ装置20に送信する。

[0094] 鍵管理サーバ装置20においては、鍵管理部23が、ポリシ設定装置30からセキュア通信部12を介して文書特定情報及び鍵情報を受けると、当該文書特定情報と鍵情報とを互いに関連付けて鍵管理用記憶装置21に書き込む。

[0095] しかる後、ポリシ設定装置30においては、文書ポリシ設定者の操作により、ポリシ設定用記憶装置31内の文書ファイルd10を通信部33からファイルアクセス制御装置40に送信する。

[0096] ファイルアクセス制御装置40においては、通信部42が、ポリシ設定装置30から受

けた文書ファイルd10を記憶装置41に書き込む。

[0097] 以上により、ファイルアクセス制御装置40において、文書ファイルd10に対するファイルアクセス制御を実行するための準備が完了する。

[0098] (ファイルアクセス制御)

ファイルアクセス制御装置40においては、図12に示すように、文書操作者としてのユーザが文書アプリケーション部45を介して文書ファイルd10に操作を行う。

[0099] このとき、文書アプリケーション部45は、操作内容に対応したイベント情報及び文書ファイルd10をポリシ評価モジュール44に入力する(ST1)。

[0100] ポリシ評価モジュール44においては、イベント制御部44aが、入力されたイベント情報及び文書ファイルd10を受けると、イベント情報が「文書の閲覧(文書を開く)」であるか否かを判定する(ST2)。

[0101] ステップST2の判定の結果、イベント情報が「文書の閲覧」ではない場合(ST2;NO)には、文書ファイル及びイベント情報を評価情報取得部44cに送出し、ステップST6に進む。

[0102] 一方、ステップST2の判定結果が「文書の閲覧」の場合(ST2;YES)には、イベント制御部44aは、文書ファイルd10のセキュリティ情報d15に基づいて文書内容d11及びアクセス制御ポリシd12が暗号化されているか否かを判定すると共に、当該セキュリティ情報d15がデジタル署名を含むか否かを判定する。

[0103] イベント制御部44aは、この判定の結果、文書内容d11等が暗号化されている場合、又はセキュリティ情報d15がデジタル署名を含む場合には、文書ファイルd10を復号・署名検証部44bに送出して復号処理及び署名検証処理を実行させる(ST3)。

[0104] 復号・署名検証部44bは、イベント制御部44aから文書ファイルd10を受けると、文書ファイルd10のセキュリティ情報d15に基づいて文書内容d11及びアクセス制御ポリシd12が暗号化されているか否かを判定すると共に、当該セキュリティ情報d15がデジタル署名を含むか否かを判定する。

[0105] この判定の結果、文書内容d11等が暗号化されている場合、又はセキュリティ情報d15がデジタル署名を含む場合には、復号・署名検証部44bは、セキュリティ情報d15内の鍵特定情報に基づいて鍵管理サーバ装置20から共通鍵及び検証鍵を取得

する。また、復号・署名検証部44bは、この共通鍵に基づいて文書内容d11等を復号すると共に、検証鍵に基づいてデジタル署名を検証する。しかる後、復号・署名検証部44bは、復号結果及び検証結果をイベント制御部44aに送出する。

[0106] イベント制御部44aは、復号・署名検証部44bの各処理が成功した場合には、復号された文書内容d11及びアクセス制御ポリシd12を含む文書ファイルd10及びイベント情報を評価情報取得部44cに送出する。

[0107] 評価情報取得部44cは、文書ファイルd10及びイベント情報を受けると、予め決められた評価情報リストに記載された種別の評価情報を外部から取得する。

[0108] 具体的には、評価情報取得部44cは、ユーザの認証結果及びユーザ属性情報を取得する場合、ユーザ認証の要求をセキュア通信部43から認証サーバ装置10に送信し、認証結果(成功又は失敗)及びユーザの属性情報を認証サーバ装置10から取得する。

[0109] 評価情報取得部44cは、時間情報を取得する場合、外部から時間情報等を取得する。

[0110] 評価情報取得部44cは、実行可否情報を取得する場合、実行可否情報送出要求を責務実行可否情報取得部44dに送出し、実行可否情報を責務実行可否情報取得部44dから取得する(ST4)。

[0111] これにより、評価情報取得部44cは、ユーザの認証結果、ユーザ属性情報、時間情報、外部機能の実行可否情報からなる評価情報を取得する(ST5)。なお、評価情報取得部44cは、評価情報リストに基づいて評価情報を取得する場合に限らず、アクセス制御ポリシd12に記述された評価情報を取得するようにしてもよい。

[0112] いずれにしても評価情報を取得した後、評価情報取得部44cは、文書ファイルd10のアクセス制御ポリシd12、イベント情報及び評価情報を禁止型ポリシ評価部44eに送出する。

[0113] 禁止型ポリシ評価部44eは、評価情報取得部44cから受けたイベント情報、評価情報に基づいて、アクセス制御ポリシd12に記述された禁止型ポリシd13を評価し(ST6)、評価の後、イベント情報、評価情報、禁止型ポリシd13の評価結果(許可又は禁止)及びアクセス制御ポリシd12に記載された責務型ポリシd14を責務型ポリシ評価

部へ送出する。

[0114] 責務型ポリシ評価部44fは、禁止型ポリシ評価部44eから受けたイベント情報、評価情報、禁止型ポリシ44eの評価結果に基づいて、責務型ポリシd14を評価し(ST7)、評価の後、責務実行主体及び責務実行行為を含む制御情報を制御管理部44gへ送出する。

[0115] 制御管理部44gは、この制御情報を受けると、予め決められた順序に従い、制御情報内の責務実行主体に基づいて、当該制御情報を文書アプリケーション制御部44h、文書ファイル制御部44i又は外部サービス制御部44jに送出する(ST8)。

[0116] 文書アプリケーション制御部44hは、送出された制御情報内の責務実行行為に基づいて、文書アプリケーション部45を制御する。

[0117] 文書ファイル制御部44iは、送出された制御情報内の責務実行行為に基づいて、記憶装置41内の文書ファイルd10のアクセス制御ポリシd12やセキュリティ情報d15を変更する。

[0118] 外部サービス制御部44jは、送出された制御情報内の責務実行行為に基づいて、外部サービス部46を制御する。

[0119] 以下、ポリシ評価モジュール44は、イベント制御部44aによりイベント情報が新たに入力されたか否かを判定し(ST9)、イベント情報が新たに入力されると(ST9;YES)、ステップST2以降の処理を繰り返す。

[0120] また、図13に示すように、責務実行可否情報取得部44dが定期的に実行可否情報を更新してもよい(ST10)。これにより、例えば、外部サービス部46の可否状態が変化しても対応することができる。

[0121] 上述したように本実施形態によれば、ポリシ評価制御モジュール44により、文書ファイルd10に対する操作に応じてアクセス制御を変更・実施することができると共に、文書アプリケーション部45や外部サービス部46の処理も設定・制御することができる。

[0122] 補足すると、予め操作に応じた制御情報を責務型ポリシd14として文書ファイルd10に付与し、文書ファイルd10に対する操作に応じて、文書ファイルd10内の責務型ポリシd14を評価・実施する。この責務型ポリシd14の実施には、文書アプリケーショ

ン部45等の制御が含まれる。従って、文書に対する操作に応じて、能動的な制御を実施でき、また、文書へのアクセス制御を変更することができる。

[0123] なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク(フロッピー(登録商標)ディスク、ハードディスクなど)、光ディスク(CD－ROM、DVDなど)、光磁気ディスク(MO)、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0124] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

[0125] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS(オペレーティングシステム)や、データベース管理ソフト、ネットワークソフト等のMW(ミドルウェア)等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0126] さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

[0127] また、記憶媒体は1つに限らず、複数の媒体から上記実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0128] 尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

[0129] また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0130] なお、本願発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除しても

よい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

産業上の利用可能性

[0131] 以上説明したように本発明によれば、文書への操作に応じて、能動的な制御を実施でき、また、文書へのアクセス制御を変更できる。

請求の範囲

[1] 文書ファイルへのアクセスを制御するためのファイルアクセス制御装置(40)であって、

文書内容と禁止型ポリシ及び責務型ポリシとを含む文書ファイルを記憶可能な記憶装置(41)、ポリシ評価制御モジュール(44)、文書アプリケーション部(45)及び外部サービス部(46)を備えており、

前記ポリシ評価制御モジュールは、

前記文書アプリケーション部及び外部サービス部からそれぞれ実行可否情報を取得して保持する可否情報取得手段(44d)と、

ユーザの操作内容に対応したイベント情報及び前記記憶装置内の文書ファイルが前記文書アプリケーション部から入力されると、予め決められた評価情報リストに基づいて、前記ユーザの認証結果及びユーザ属性情報を取得する認証結果取得手段(44c)と、

前記評価情報リストに基づいて、前記可否情報取得手段から実行可否情報を取得すると、この実行可否情報、前記認証結果及び前記ユーザ属性情報からなる評価情報、前記イベント情報、前記禁止型ポリシ及び前記責務型ポリシを送出する手段(44c)と、

前記送出された評価情報内の認証結果及びユーザ属性情報並びにイベント情報と、前記禁止型ポリシに予め記述された認証結果、ユーザ属性情報及びイベント情報とをそれぞれ比較し、比較結果がそれぞれ一致していれば、前記禁止型ポリシに予め記述された許可又は禁止を示す評価結果を送出する禁止型ポリシ評価手段(44e)と、

前記評価情報内の実行可否情報、前記イベント情報及び前記評価結果と、前記責務型ポリシに予め記述された実行可否情報、前記イベント情報及び前記評価結果とをそれぞれ比較し、比較結果がそれぞれ一致していれば、前記責務型ポリシに予め記述された責務実行主体及び責務実行行為を含む制御情報を送出する責務型ポリシ評価手段(44f)と、

前記制御情報を受けると、前記制御情報内の責務実行主体に基づいて、当該制

御情報を送出する制御管理手段(44g)と、

前記制御管理手段から送出された制御情報内の責務実行行為に基づいて、前記文書アプリケーション部を制御する文書アプリケーション制御手段(44h)と、

を備えたことを特徴とするファイルアクセス制御装置。

[2] 請求項1に記載のファイルアクセス制御装置において、

前記ポリシ評価制御モジュールは、

前記制御管理手段から送出された制御情報内の責務実行行為に基づいて、前記記憶装置内の文書ファイルの禁止型ポリシ又は責務型ポリシを変更するポリシ変更手段(44i)、

を更に備えたことを特徴とするファイルアクセス制御装置。

[3] 請求項1又は請求項2に記載のファイルアクセス制御装置において、

前記ポリシ評価制御モジュールは、

前記制御管理手段から送出された制御情報内の責務実行行為に基づいて、前記外部サービス部を制御する外部サービス制御手段(44j)、

を更に備えたことを特徴とするファイルアクセス制御装置。

[4] コンピュータ読み取り可能な記憶媒体(M)に記憶されたプログラムであって、

文書内容と禁止型ポリシ及び責務型ポリシとを含む文書ファイル(d10)を記憶可能な記憶装置(41', 41")、文書アプリケーション部(45')及び外部サービス部(46')を備え且つ前記文書ファイルへのアクセスを制御するためのコンピュータに関し、前記文書アプリケーション部及び外部サービス部からそれぞれ実行可否情報を取得して保持する処理を当該コンピュータに実行させるための第1プログラムコード(44d)、

ユーザの操作内容に対応したイベント情報及び前記記憶装置内の文書ファイルが前記文書アプリケーション部から入力されると、予め決められた評価情報リストに基づいて、前記ユーザの認証結果及びユーザ属性情報を取得する処理を前記コンピュータに実行させるための第2プログラムコード(44c)、

前記評価情報リストに基づいて、前記可否情報取得手段から実行可否情報を取得すると、この実行可否情報、前記認証結果及び前記ユーザ属性情報からなる評価情報、前記イベント情報、前記禁止型ポリシ及び前記責務型ポリシを送出する処理を前

記コンピュータに実行させるための第3プログラムコード(44c)、

前記送出された評価情報内の認証結果及びユーザ属性情報並びにイベント情報と、前記禁止型ポリシに予め記述された認証結果、ユーザ属性情報及びイベント情報とをそれぞれ比較し、比較結果がそれぞれ一致していれば、前記禁止型ポリシに予め記述された許可又は禁止を示す評価結果を送出する処理を前記コンピュータに実行させるための第4プログラムコード(44e)、

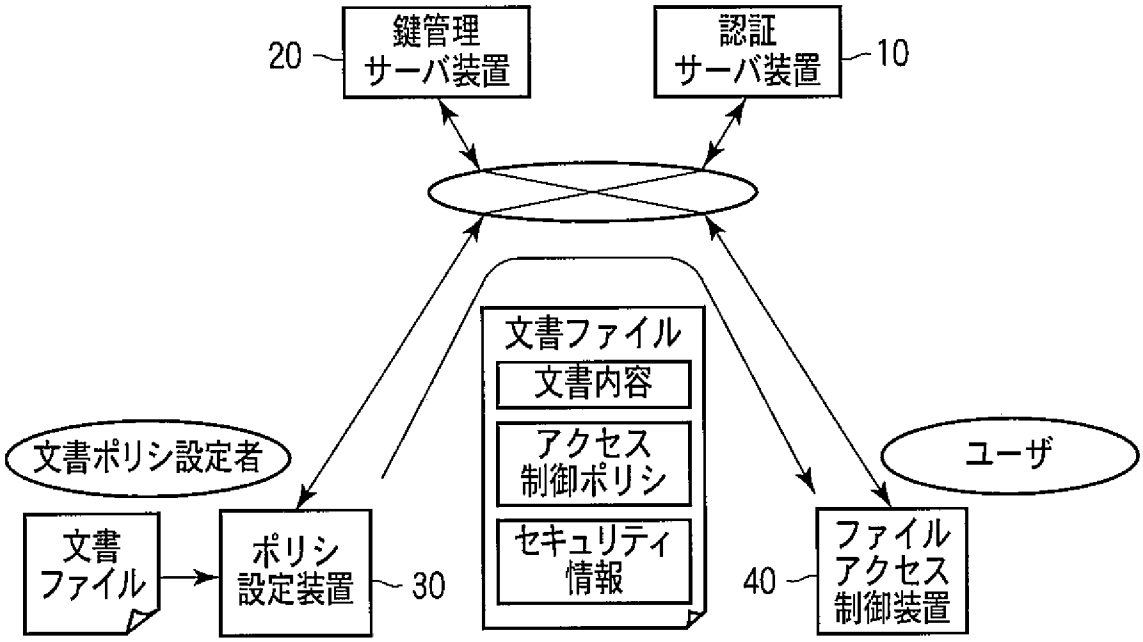
前記評価情報内の実行可否情報、前記イベント情報及び前記評価結果と、前記責務型ポリシに予め記述された実行可否情報、前記イベント情報及び前記評価結果とをそれぞれ比較し、比較結果がそれぞれ一致していれば、前記責務型ポリシに予め記述された責務実行主体及び責務実行行為を含む制御情報を送出する処理を前記コンピュータに実行させるための第5プログラムコード(44e)、

前記制御情報を受けると、前記制御情報内の責務実行主体に基づいて、当該制御情報を送出する処理を前記コンピュータに実行させるための第6プログラムコード(44g)、及び

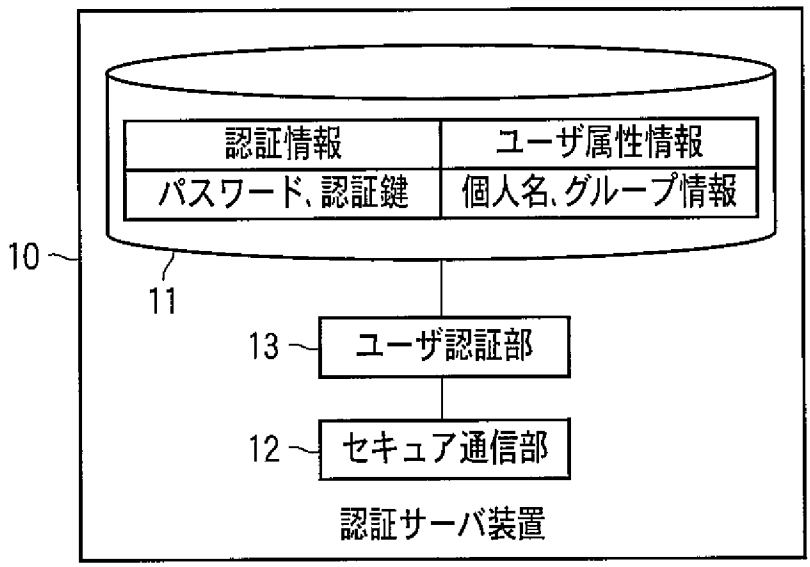
前記送出された制御情報内の責務実行行為に基づいて、前記文書アプリケーション部を制御する処理を前記コンピュータに実行させるための第7プログラムコード(44h)、

を備えている。

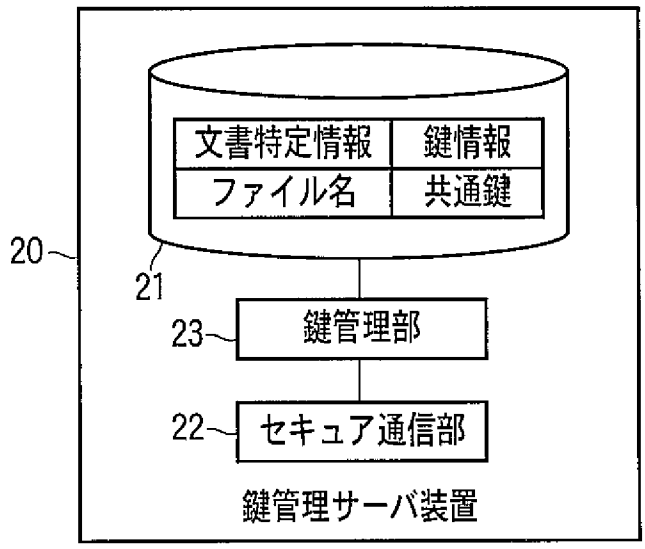
[図1]


鍵管理
サーバ装置
20
認証
サーバ装置
10
文書ファイル
文書内容
アクセス
制御ポリシ
セキュリティ
情報
文書ポリシ設定者
ユーザ
文書
ファイル
ポリシ
設定装置
30
ファイル
アクセス
制御装置
40

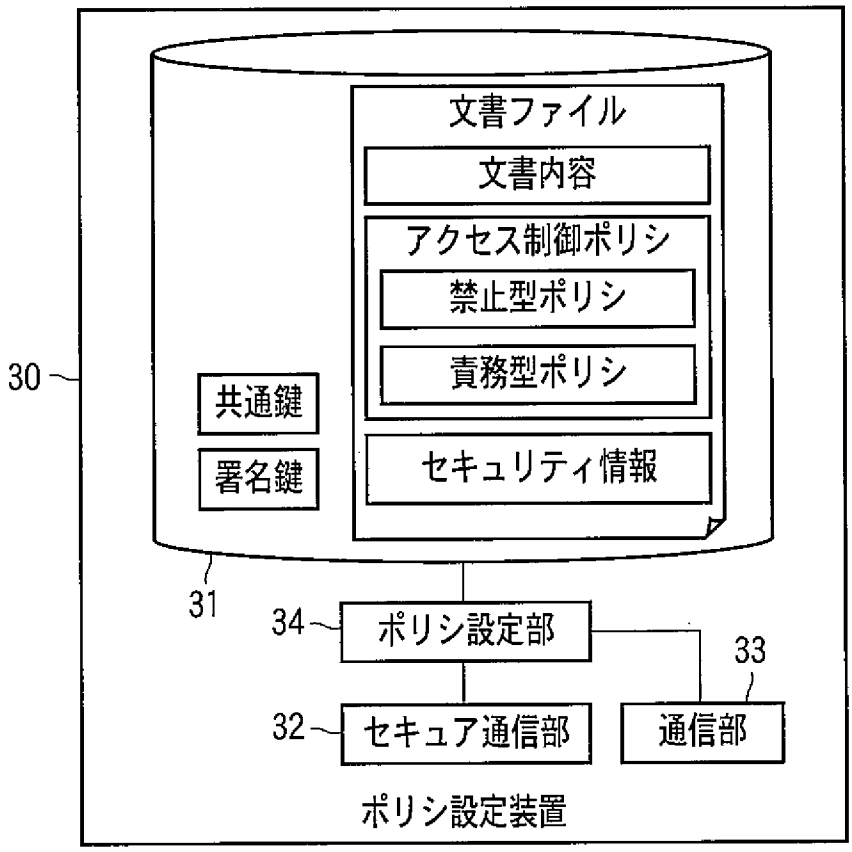
[図2]


認証情報
ユーザ属性情報
パスワード、認証鍵
個人名、グループ情報
10
11
13
ユーザ認証部
12
セキュア通信部
認証サーバ装置

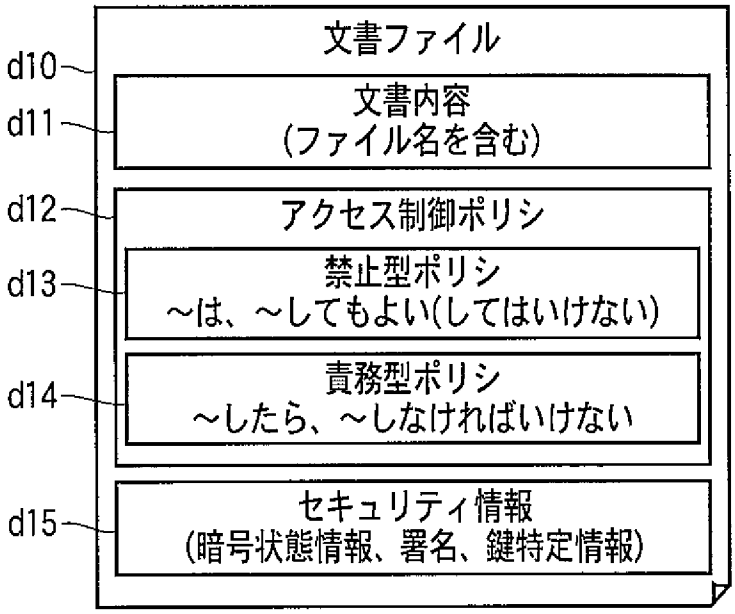
[図3]


文書特定情報
鍵情報
ファイル名
共通鍵
20
21
23
鍵管理部
22
セキュア通信部
鍵管理サーバ装置

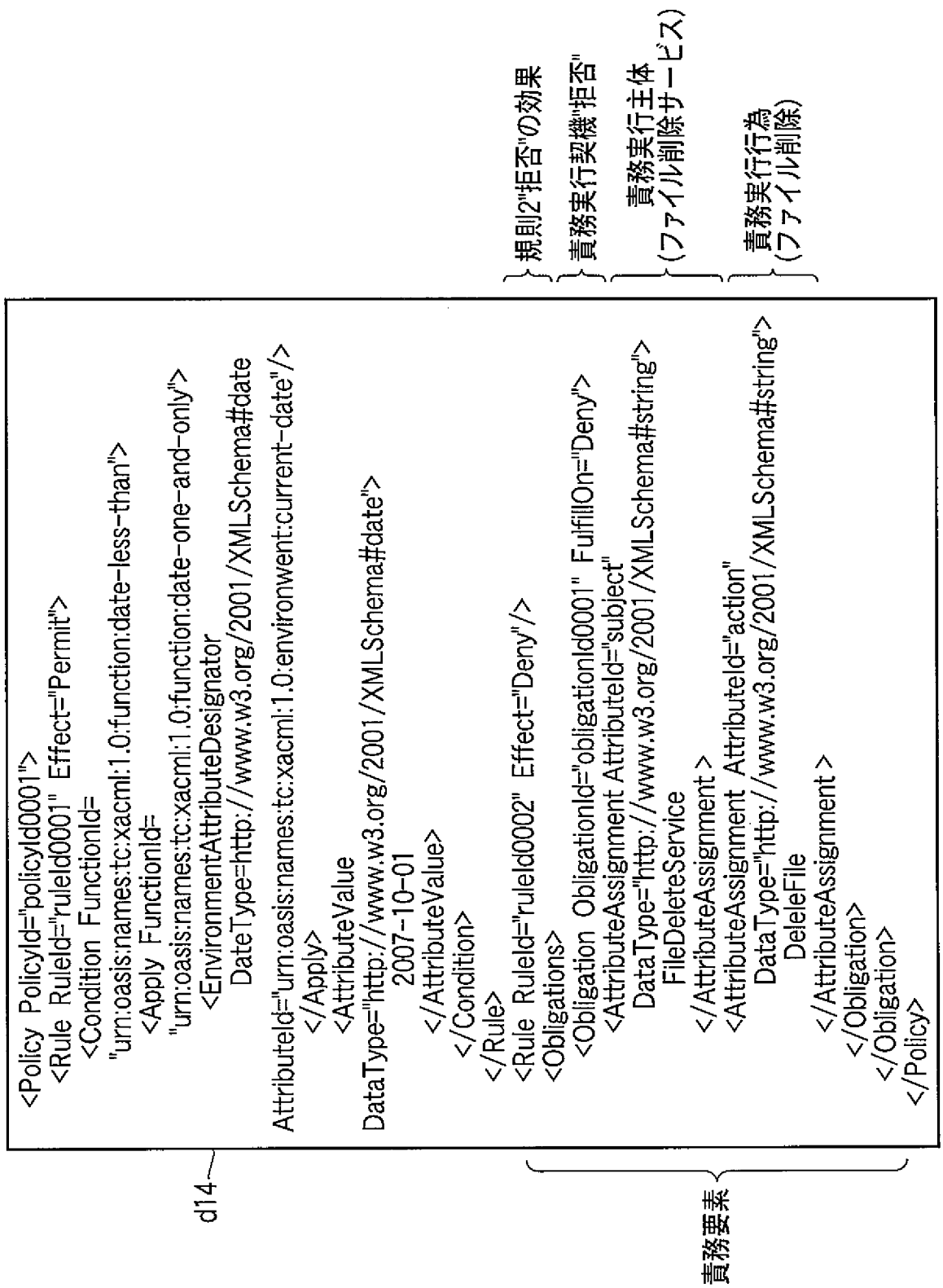
[図4]


文書ファイル
文書内容
アクセス制御ポリシ
禁止型ポリシ
責務型ポリシ
セキュリティ情報
共通鍵
署名鍵
30
31
34
ポリシ設定部
33
32
セキュア通信部
通信部
ポリシ設定装置

[図5]


文書ファイル
d10
d11
文書内容
(ファイル名を含む)
d12
アクセス制御ポリシ
d13
禁止型ポリシ
～は、～してもよい(してはいけない)
d14
責務型ポリシ
～したら、～しなければいけない
d15
セキュリティ情報
(暗号状態情報、署名、鍵特定情報)

[図6]


d14
<Policy PolicyId="policyId0001">
<Rule RuleId="ruleId0001" Effect="Permit">
<Condition FunctionId=
"urn:oasis:names:tc:xacml:1.0:function:date-less-than">
<Apply FunctionId=
"urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
<EnvironmentAttributeDesignator
DateType=http://www.w3.org/2001/XMLSchema#date
AttributeId="urn:oasis:names:tc:xacml:1.0:environent:current-date"/>
</Apply>
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">
2007-10-01
</AttributeValue>
</Condition>
</Rule>
<Rule RuleId="ruleId0002" Effect="Deny"/>
<Obligations>
<Obligation ObligationId="obligationId0001" FulfillOn="Deny">
<AttributeAssignment AttributeId="subject"
DataType="http://www.w3.org/2001/XMLSchema#string">
FileDeleteService
</AttributeAssignment >
<AttributeAssignment AttributeId="action"
DataType="http://www.w3.org/2001/XMLSchema#string">
DeleleFile
</AttributeAssignment >
</Obligation>
</Obligation>
</Policy>
責務要素
規則2"拒否"の効果
責務実行契機"拒否"
責務実行主体
(ファイル削除サービス)
責務実行行為
(ファイル削除)

[図7]

d14

```
<AttributeAssignment AttributeId="environment"
 DataType="http://www.w3.org/2001/XMLSchema#date">
  2007-10-01
</AttributeAssignment>
```

責務実行環境
(2007年10月1日)

[図8]

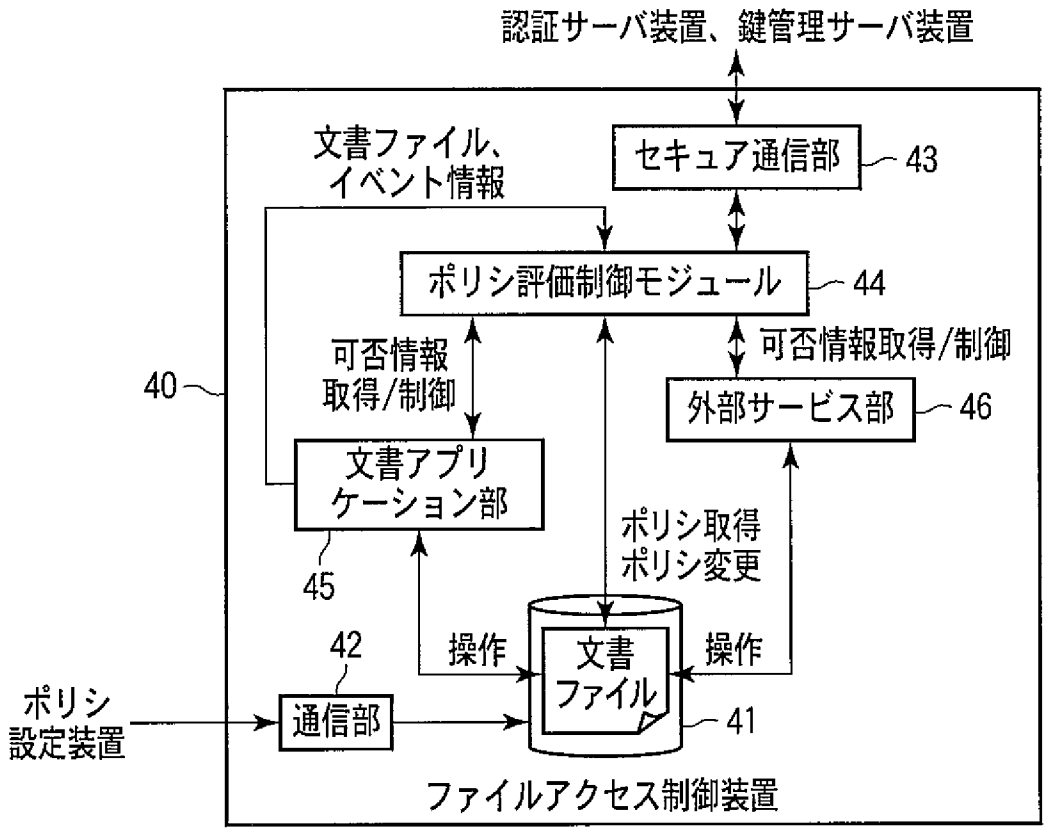
d14

```
<AttributeAssignment AttributeId="action"
 DataType="http://www.w3.org/2001/XMLSchema#string">
  DisableFunctions
</AttributeAssignment>
...
<AttributeAssignment AttributeId="complement"
 DataType="http://www.w3.org/2001/XMLSchema#string">
  Print
<AttributeAssignment>
```

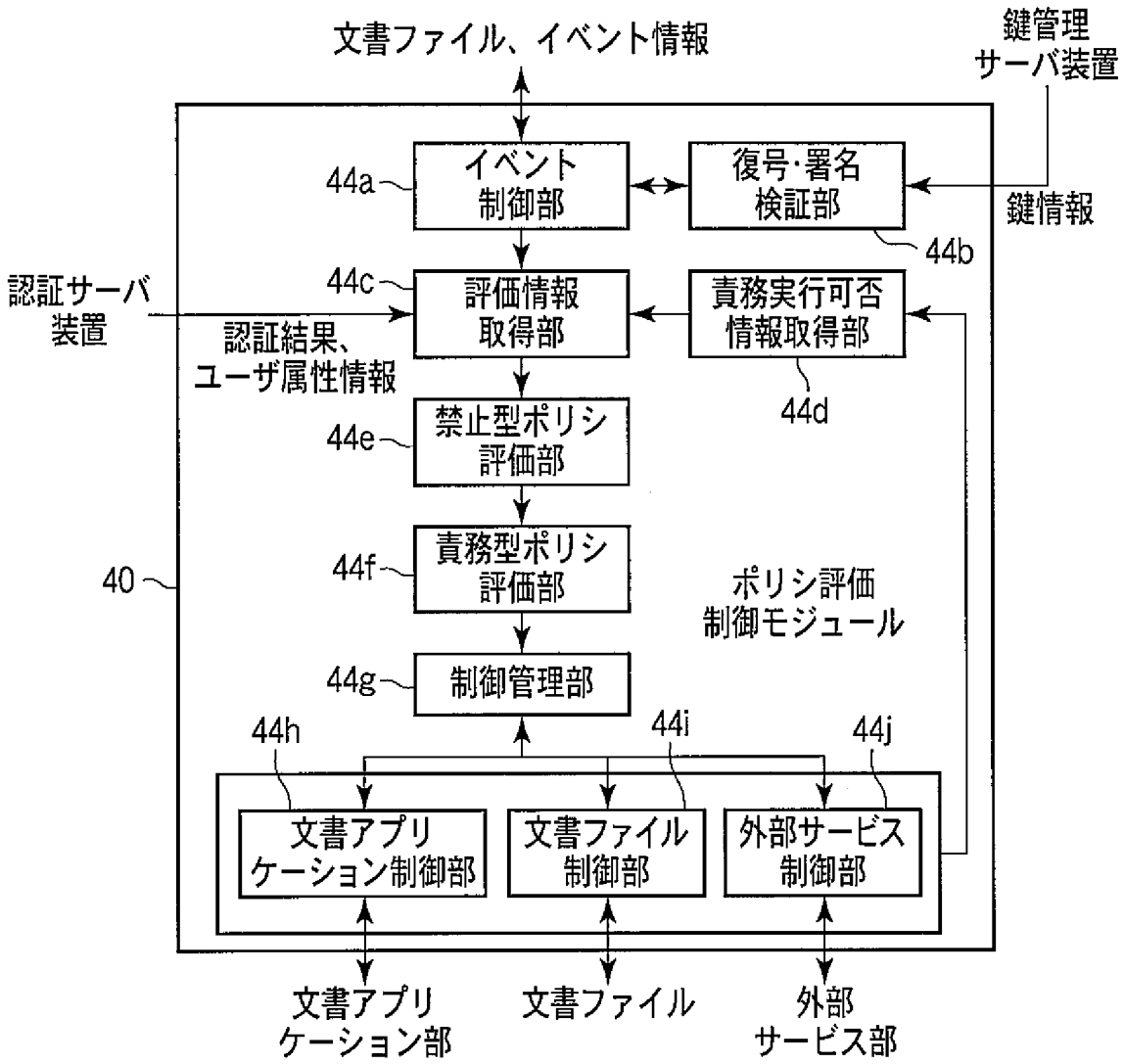
責務実行行為
(機能の制限)

責務実行補体
(印刷)

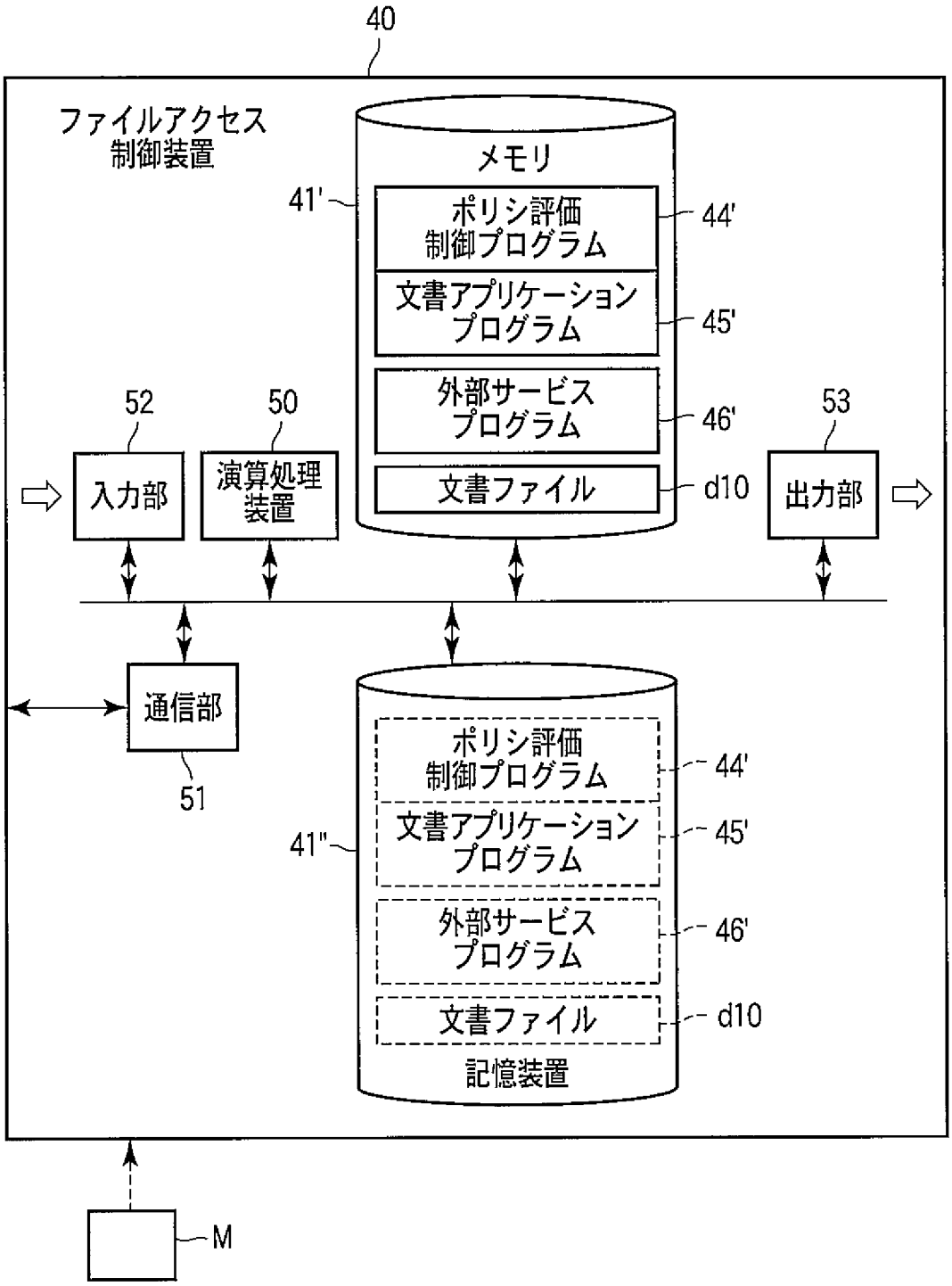
[図9]



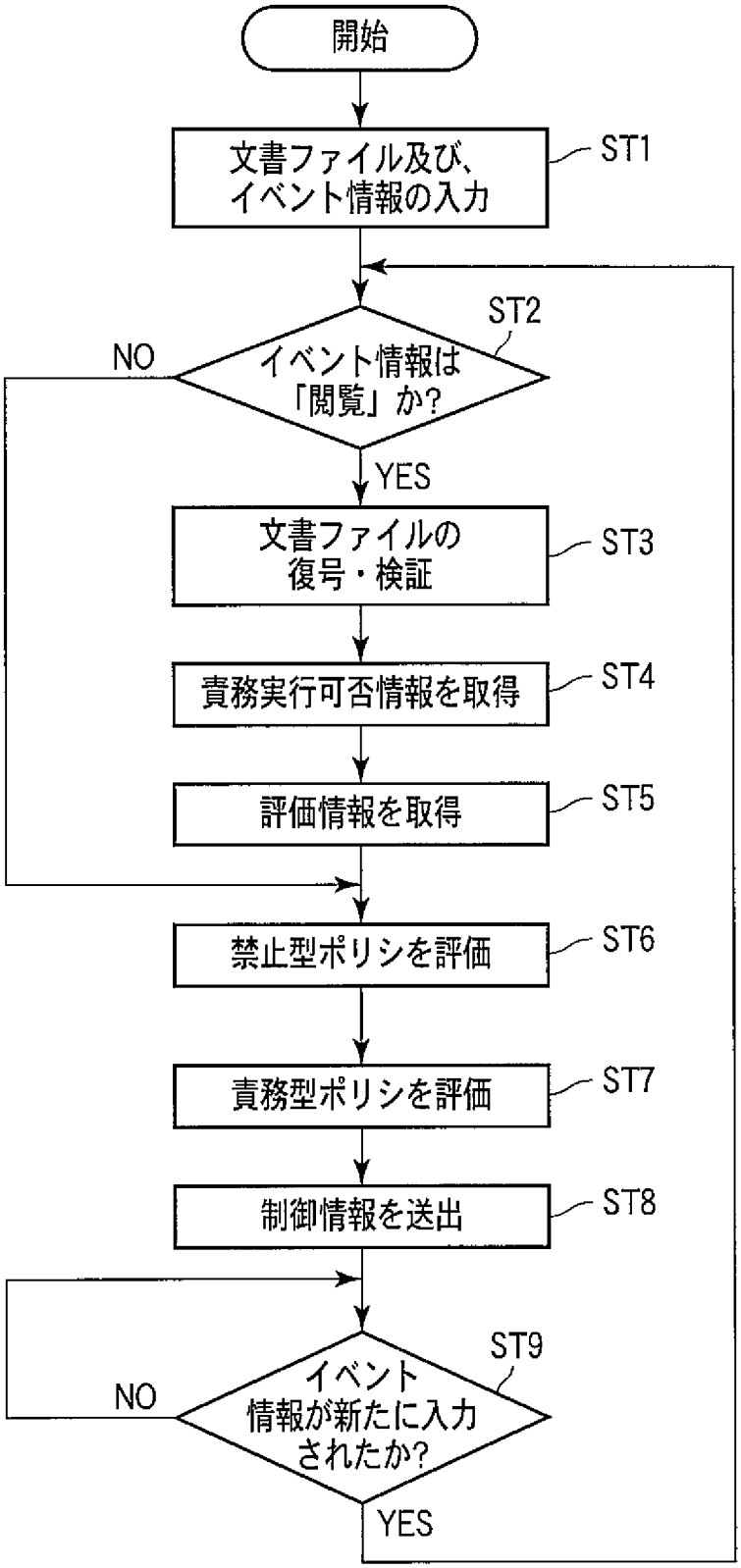
[図10]


文書ファイル、イベント情報
鍵管理
サーバ装置
44a
イベント
制御部
復号･署名
検証部
鍵情報
44b
認証サーバ
装置
44c
評価情報
取得部
責務実行可否
情報取得部
認証結果、
ユーザ属性情報
44d
44e
禁止型ポリシ
評価部
44f
責務型ポリシ
評価部
40
ポリシ評価
制御モジュール
44g
制御管理部
44h
44i
44j
文書アプリ
ケーション制御部
文書ファイル
制御部
外部サービス
制御部
文書アプリ
ケーション部
文書ファイル
外部
サービス部

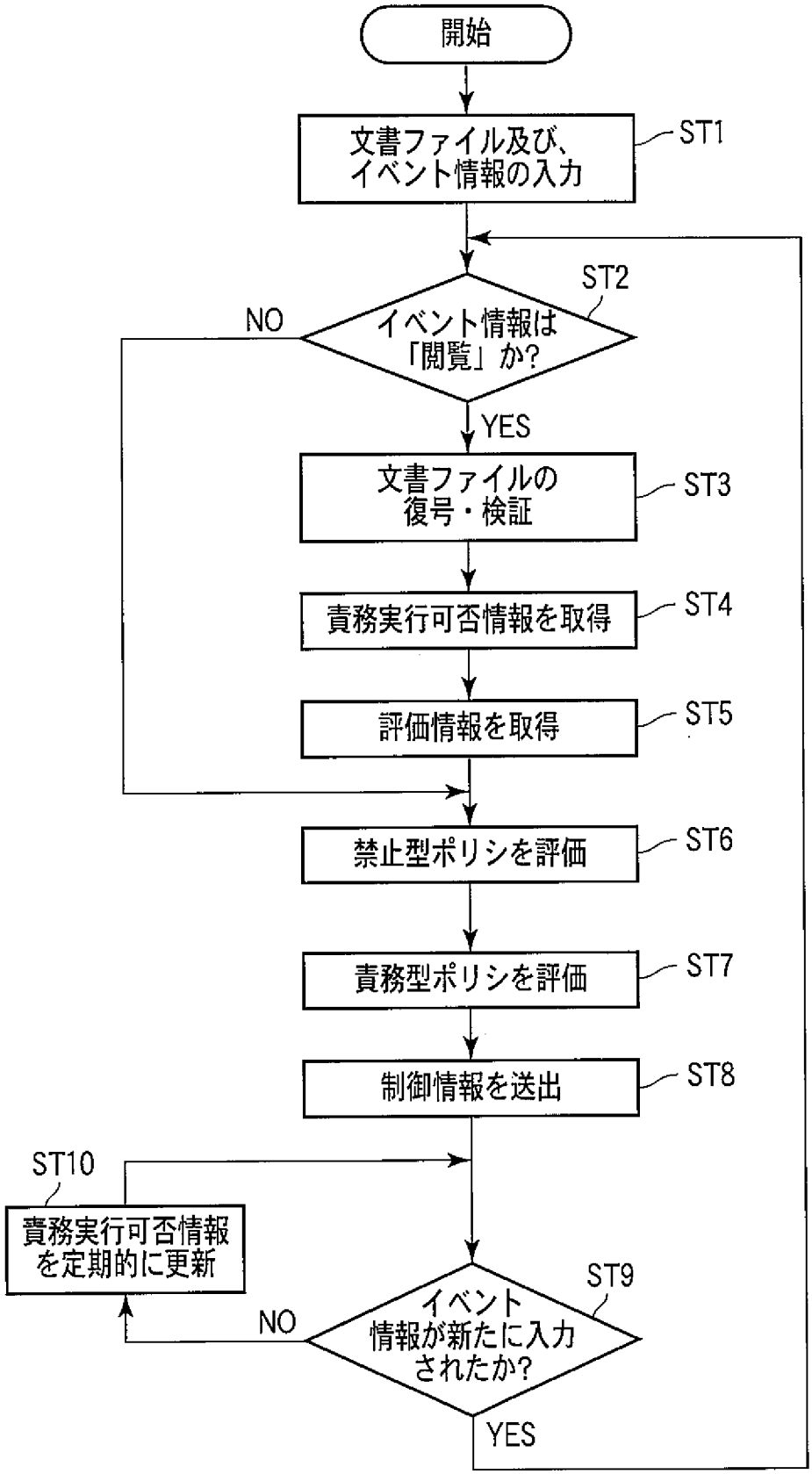
[図11]


40
ファイルアクセス
制御装置
メモリ
41'
ポリシ評価
制御プログラム
44'
文書アプリケーション
プログラム
45'
外部サービス
プログラム
46'
文書ファイル
d10
52
50
53
入力部
演算処理
装置
出力部
通信部
51
41"
ポリシ評価
制御プログラム
44'
文書アプリケーション
プログラム
45'
外部サービス
プログラム
46'
文書ファイル
d10
記憶装置
M

[図12]


開始
文書ファイル及び、
イベント情報の入力
ST1
ST2
NO
イベント情報は
「閲覧」か?
YES
文書ファイルの
復号・検証
ST3
責務実行可否情報を取得
ST4
評価情報を取得
ST5
禁止型ポリシを評価
ST6
責務型ポリシを評価
ST7
制御情報を送出
ST8
ST9
NO
イベント
情報が新たに入力
されたか?
YES

[図13]


開始
文書ファイル及び、
イベント情報の入力
ST1
ST2
NO
イベント情報は
「閲覧」か?
YES
文書ファイルの
復号・検証
ST3
責務実行可否情報を取得
ST4
評価情報を取得
ST5
禁止型ポリシを評価
ST6
責務型ポリシを評価
ST7
制御情報を送出
ST8
ST10
責務実行可否情報
を定期的に更新
ST9
NO
イベント
情報が新たに入力
されたか?
YES

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/069671

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01)i, *G06F21/20*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/24, G06F21/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ken'ichi OTO Kenichi OOTO, "Koshu Musen LAN no On-demand Riyo no Tameno Riyoken Kijutsuho A description method of use-right for on-demand wireless LAN usage", IEICE Technical Report, Vol.105, No.357, IEICE Technical Report, 13 October, 2005 (13.10.05), Vol.105, pages 9 to 12	1-4
A	Sumitaka OKAJO Sumitaka OKAJO, "Security Un'yo Kanri no Tameno Policy Gengo SCCML A Policy Description Language for Policy-based Security Management", IPSJ SIG Notes, Vol.2004, No.129, IPSJ SIG Technical Reports, 20 December, 2004 (20.12.04), Vol.2004, pages 89 to 94	1-4

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 January, 2009 (26.01.09)	03 February, 2009 (03.02.09)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/069671

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-257352 A (Ricoh Co., Ltd.), 04 October, 2007 (04.10.07), Full text; all drawings (Family: none)	1-4
A	JP 2007-048241 A (Nomura Research Institute, Ltd.), 22 February, 2007 (22.02.07), Full text; all drawings (Family: none)	1-4
A	JP 2007-213208 A (Nippon Telegraph And Telephone Corp.), 23 August, 2007 (23.08.07), Full text; all drawings (Family: none)	1-4
A	JP 2005-301510 A (Ricoh Co., Ltd.), 27 October, 2005 (27.10.05), Full text; all drawings & US 2005/0262572 A1	1-4

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０６９６７１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24(2006.01)i, G06F21/20(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24, G06F21/20

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	大戸　健一　Kenichi　OOTO, 公衆無線ＬＡＮのオンデマンド利用のための利用権記述法　A description method of use-right for on-demand wireless LAN usage, 電子情報通信学会技術研究報告　Ｖｏｌ．１０５　Ｎｏ．３５７　IEICE Technical Report, 2005.10.13, 第105巻, pp.9-12	１－４
Ａ	岡城　純孝　Sumitaka　OKAJO, セキュリティ運用管理のためのポリシー言語ＳＣＣＭＬ　A Policy Description Language for Policy-based Security Management, 情報処理学会研究報告　Ｖｏ	１－４

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２６．０１．２００９	国際調査報告の発送日 ０３．０２．２００９
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３９８３ 岸野　徹 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	１．２００４　Ｎｏ．１２９　IPSJ SIG Technical Reports, 2004.12.20, 第2004巻, pp.89-94	
A	JP 2007-257352 A (株式会社リコー) 2007.10.04, 全文、全図　(ファミリーなし)	１－４
A	JP 2007-048241 A (株式会社野村総合研究所) 2007.02.22, 全文、全図　(ファミリーなし)	１－４
A	JP 2007-213208 A (日本電信電話株式会社) 2007.08.23, 全文、全図　(ファミリーなし)	１－４
A	JP 2005-301510 A (株式会社リコー) 2005.10.27, 全文、全図　& US 2005/0262572 A1	１－４