(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
2012 年 6 月 14 日(14.06.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/077300 A1

(51) 国際特許分類:
G06F 21/00 (2006.01)

(21) 国際出願番号: PCT/JP2011/006668

(22) 国際出願日: 2011 年 11 月 29 日(29.11.2011)

(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 2010-274112 2010 年 12 月 8 日(08.12.2010) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 前田　学 (MAEDA, Manabu). 松島　秀樹 (MATSUSHIMA, Hideki). 芳賀　智之 (HAGA, Tomoyuki).

(74) 代理人: 新居　広守 (NII, Hiromori); 〒5320011 大阪府大阪市淀川区西中島５丁目３番１０号タナカ・イトーピア新大阪ビル６階新居国際特許事務所内 Osaka (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, CL, 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, JP, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

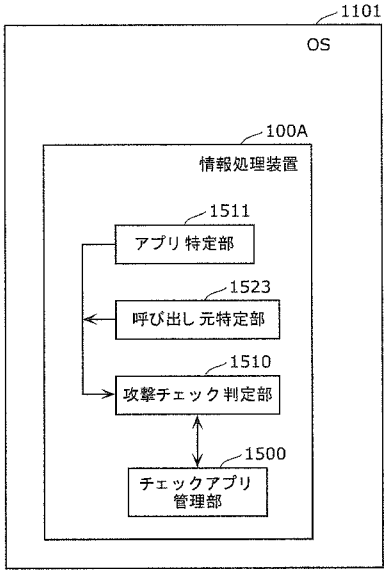
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[続葉有]

(54) **Title**: INFORMATION PROCESSING DEVICE AND INFORMATION PROCESSING METHOD

(54) 発明の名称 : 情報処理装置、及び、情報処理方法

[図9]



100A Information processing device
1101 OS
1500 Check application management unit
1510 Attack check judgment unit
1511 Application specification unit
1523 Call source specification unit

(57) **Abstract**: Provided is an information processing device (100A) that, in order to improve the responsiveness of system call processing without compromising safety, comprises: an application specification unit (1511) that specifies programs being executed by the information processing device, by obtaining application identifiers; a call source specification unit (1523) that specifies a call source that indicates which part of a program a program code was called from, when a program code is called by a specified program; a check application management unit (1500) that manages check results, which is data that includes the results of past checks of safety relating to the execution of a specified program; and an attack check judgment unit (1510) that judges whether or not to perform a check to see if the specified program is being attacked, based on the specified check source and the check results.

(57) 要約: 安全性を損なうことなく、システムコール処理の応答性を向上させるため、本発明に係る情報処理装置（１００Ａ）は、アプリ識別子を取得することにより情報処理装置において実行中のプログラムを特定するアプリ特定部（１５１１）と、特定されたプログラムが、プログラムコードの呼び出し時に、プログラムのどの部分からプログラムコードを呼び出したかを示す呼び出し元を特定する呼び出し元特定部（１５２３）と、特定されたプログラムを実行することに対する安全性について過去にチェックした結果を含む情報であるチェック結果を管理するチェックアプリ管理部（１５００）と、特定された呼び出し元とチェック結果とに基づいて、特定されたプログラムが攻撃されているかのチェックを行うか否かを判定する攻撃チェック判定部（１５１０）とを備える。

WO 2012/077300 A1

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（条約第 21 条(3)）

明　細　書

発明の名称 ： 情報処理装置、及び、情報処理方法

技術分野

[0001] 本発明は、不正なプログラムを付加したコンテンツによる情報の漏洩を防止する技術に関する。

背景技術

[0002] 近年、デジタルカメラなどで撮影した写真データを、デジタルカメラや記録媒体から取り込み、蓄積し、ユーザの要求に応じて蓄積した写真データを表示する機器が普及しつつある。また、このような機器では、機器の所有者が撮影した写真データだけでなく、所有者以外が撮影した写真データや、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）などの他の機器に蓄積されている写真データも取り込み、蓄積する。

[0003] このような機器に対して、不正なプログラムが付加された不正な写真データを取り込ませることにより、機器内部の他の写真データを漏洩させるという攻撃が考えられる。例えば、攻撃者が、ターゲットとする人のＰＣへ、メール等を利用して不正なプログラムが付加された不正な写真データを送付し、その写真データを上記のような機器に取り込ませる。又は、ＣＤ－Ｒ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ　Ｒｅｃｏｒｄａｂｌｅ）やＤＶＤ－Ｒ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ　Ｒｅｃｏｒｄａｂｌｅ）等の記録メディアに不正なプログラムが付加された不正な写真データを含む写真データを記録する。記録メディアに記録された写真データをターゲットとする人へ渡すことにより、不正なプログラムが付加された不正な写真データをターゲットが使用する機器へ取り込ませてもよい。不正なプログラムが付加された不正な写真データを用いた攻撃としては、バッファーオーバーフローの脆弱性を利用した攻撃方法がある。

[0004] ここで、バッファーオーバーフローの脆弱性を利用した攻撃方法について説明する。

[0005] まず、アプリ（以後、計算機により実行されるプログラムであって、一定の処理を行う処理部のことを、アプリと呼ぶ）は、実行中に利用するデータをＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）上に確保されたスタック領域に格納する。スタック領域には、アプリ内の関数（アプリの一部分であり、モジュール化された処理部を意味する）ごとにスタックフレームが作られ、スタックフレームは後入れ先出し（ＬＩＦＯ：Ｌａｓｔ　Ｉｎ　Ｆｉｒｓｔ　Ｏｕｔ、ＦＩＬＯ：Ｆｉｒｓｔ　Ｉｎ　Ｌａｓｔ　Ｏｕｔ）の構造で、スタック領域に格納される。

[0006] スタックフレームは、図１８に示す様に、ローカル変数領域２００、退避領域２０１、リターンアドレス２０２、引数領域２０３から構成される。ローカル変数領域２００には、関数内で使用するローカル変数が格納される。退避領域２０１には、関数が呼び出された時のＣＰＵの状態が退避（すなわち、記録）され、関数が終了した時には、記録されたＣＰＵ状態を退避領域から読み出すことで、ＣＰＵは退避前の状態へ復帰する。リターンアドレス２０２には、関数内で定義された処理の終了時に戻る戻り先のアドレス（すなわち、ＲＡＭ内のアドレス）が格納される。引数領域２０３には、関数を呼び出した時の引数が格納される。

[0007] バッファーオーバーフローの脆弱性とは、スタック上のローカル変数領域２００に確保されたバッファー（変数）へ外部から入力されたデータを保存する際に問題となる。具体的には、バッファーのサイズより大きいデータが入力された結果、退避領域２０１、リターンアドレス２０２及び引数領域２０３が書き換えられてしまうという脆弱性である。

[0008] このバッファーオーバーフローの発生時、例えば、攻撃者が写真データを工夫することで、ローカル変数領域２００を不正なプログラムで書き換え、リターンアドレス２０２を不正なプログラムの先頭アドレスに書き換えることができる。これにより、写真データに付加された不正なプログラムを、バッファーオーバーフローが発生した計算機上で実行できる。すなわち、バッファーオーバーフロー攻撃は、（１）特定のアプリ内の関数がバッファーオ

ーバーフローの脆弱性を有しており、かつ、（２）その関数が、不正なプログラムが仕込まれた不正な写真データを読み込むことで、実行される。

[0009] 従来のバッファーオーバーフロー攻撃対策としては、カーネルのシステムコール処理などのプログラムコードの呼び出し時に、リターンアドレスが示すアドレスの属性情報（領域情報）に基づいて不正なプログラムからの呼び出しであるかを判断する方法がある（例えば、特許文献１、２参照）。図１９は、前記特許文献１に記載された従来のバッファーオーバーフロー攻撃対策を示すものである。

[0010] 図１９において、タスク１０１は、データ領域１０２からのデータの読み込みを伴うシステムコール要求をＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）１０７に入力する。ＯＳ１０７は、システムコール要求をシステムコールテーブル１０３で受けとると、正当性検証部１０４へシステムコール要求の正当性の検査を依頼する。正当性検証部１０４は、システムコール要求の正当性を判定し、判定結果を出力する。正当性検証部１０４が、不正なシステムコール要求と判断した場合、そのシステムコール要求を棄却し、攻撃対策部１１２へ通知する。攻撃対策部１１２は、システムコールを要求したタスク１０１に対して、対策を講じる。一方、正当性検証部１０４が、正当なシステムコール要求と判断した場合、命令実行部１０６にシステムコール１０５を実行させる。

先行技術文献

特許文献

[0011] 特許文献1：特開２００４－１２６８５４号公報

特許文献2：特開２００９－１９９５２９号公報

発明の概要

発明が解決しようとする課題

[0012] しかしながら、前記従来の構成では、全てのシステムコール要求に対して正当性の検査を実施するため、システムコール要求に対して、処理の応答性

が悪化するという課題を有している。

[0013] そこで本発明は、前記従来の課題を解決するもので、安全性を損なうことなく、システムコール処理の応答性を向上させる情報処理装置を提供することを目的とする。

課題を解決するための手段

[0014] 本発明のある局面に係る情報処理装置は、一意な識別子であるアプリ識別子を有する１以上のプログラムを実行する情報処理装置であって、前記アプリ識別子を取得することにより前記情報処理装置において実行中のプログラムを特定するアプリ特定部と、前記特定されたプログラムが、プログラムコードの呼び出し時に、前記プログラムのどの部分から前記プログラムコードを呼び出したかを示す呼び出し元を特定する呼び出し元特定部と、前記特定されたプログラムを実行することに対する安全性について過去にチェックした結果を含む情報であるチェック結果を管理するチェックアプリ管理部と、前記特定された呼び出し元と前記チェック結果とに基づいて、前記特定されたプログラムが攻撃されているかのチェックを行うか否かを判定する攻撃チェック判定部とを備える。

[0015] 一般に、既に安全であることが確認されたプログラムコード（すなわち、システムコール）の呼び出しであれば、再度、安全性をチェックすることは、計算機資源の無駄となり、システムコール処理の応答性を害する。しかし、プログラムコードは、呼び出し経路で危険性が変化する。よって、過去、安全性をチェックし、安全であることが確認されたプログラムコードであっても、その呼び出し元が異なれば、安全とはいえない。よって、プログラムコードの安全性は、その呼び出し元とセットで、判断する必要がある。

[0016] 上記構成によると、呼び出し元特定部は、プログラムコードの呼び出し元を特定することができる。よって、攻撃チェック判定部は、特定された呼び出し元とセットで、プログラムコードが攻撃されているかのチェックする必要があるか否かを判定することができる。その結果、安全性を損なうことなく、システムコール処理の応答性を向上させる情報処理装置を提供すること

ができる。

[0017] 具体的には、前記情報処理装置は、さらに、前記特定されたプログラムが攻撃されているかをチェックする攻撃チェック部を備えており、前記攻撃チェック部は、前記攻撃チェック判定部が、前記特定されたプログラムに対して攻撃チェックを行うと判定した場合には、前記特定されたプログラムが攻撃されているか否かをチェックするとしてもよい。

[0018] より具体的には、前記呼び出し元特定部は、前記特定されたプログラムから前記プログラムコードを呼び出した後に前記特定されたプログラムへ実行処理を戻すための戻し先を示すメモリ内のアドレスであるリターンアドレスを用いて、前記呼び出し元を特定するとしてもよい。

[0019] これによると、情報処理装置は、リターンアドレスから、プログラムコードの呼び出し元を具体的に特定することができる。

[0020] さらに、前記呼び出し元特定部は、前記特定されたプログラムから前記プログラムコードを呼び出した場合に前記特定されたプログラムが使用するコールスタックのスタックポインタの値と、前記リターンアドレスとを用いて前記呼び出し元を特定するとしてもよい。

[0021] プログラムコードを呼び出す際のリターンアドレスと、コールスタックのスタックポインタとの２つの情報により、そのプログラムコードの呼び出し元を一意に決定できる。よって、呼び出し元特定部は、これらの情報を取得することで、呼び出し元を特定できる。

[0022] さらに、前記チェックアプリ管理部は、（Ａ）前記特定されたプログラムが攻撃されているか否かをチェックした結果を示す情報、及び、（Ｂ）前記特定されたプログラムが、攻撃されているか否かを判定するチェックが必要であるかを示す情報、の両方を含む情報を前記チェック結果として、前記特定されたプログラムが有する前記アプリ識別子と前記呼び出し元とに対応付けて記憶しているとしてもよい。

[0023] これにより、攻撃チェック判定部は、呼び出し元特定部で特定された呼び出し元からのプログラムコードの呼び出しの安全性を、チェックアプリ管理

部に記憶されている過去のチェック結果から、判定することができる。

[0024] 具体的には、前記攻撃チェック判定部は、前記特定されたプログラムが有するアプリ識別子に対応付けられて前記チェックアプリ管理部に記憶されている前記チェック結果を取得し、（Ａ）取得した前記チェック結果が、前記特定されたプログラムが攻撃されていないこと、又は、前記特定されたプログラムが攻撃されていることを表す場合には、攻撃されているかのチェックを行わないと判定し、（Ｂ）取得した前記チェック結果が、攻撃されているか否かを判定するチェックが必要であることを表す場合には、攻撃チェック部による攻撃がされているかのチェックを行うと判定するとしてもよい。

[0025] また、さらに、前記特定されたプログラムが前記プログラムコードを呼び出すことにより読み込もうとしているデータファイルを、前記データファイルを示す識別子であるコンテンツ識別子を用いて特定するコンテンツ特定部と、前記特定されたデータファイルを読み込むか否かを判定する読み込み可否判定部とを備え、前記読み込み可否判定部は、（Ａ）前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられた前記チェック結果が、前記チェックアプリ管理部に記憶されていないか、又は、（Ｂ）前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられた前記チェック結果が、前記チェックアプリ管理部に記憶されており、かつ、前記チェック結果が、前記特定されたプログラムが攻撃されていないことを示す場合には、前記特定されたデータファイルを読み込むと判定し、（Ｃ）前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられている前記チェック結果が、前記チェックアプリ管理部に記憶されており、かつ、前記チェック結果が、前記特定されたプログラムが以前に攻撃されたことを示す場合には、前記特定されたデータファイルを読み込まないと判定するとしてもよい。

[0026] 一般に、プログラムコードにバッファーオーバーフローの脆弱性があり、かつ、そのプログラムコードがバッファーオーバーフローを利用した攻撃を意図した、悪意あるデータファイルを読み込んだ際に、実質的に危険性が高

まる。よって、チェックアプリ管理部に、プログラムコードの呼び出し元と、呼び出されたプログラムコードが読み込むデータファイルの識別子をセットにして、その安全性に関するチェック結果を記録しておくことで、より正確に、安全性を判定することができる。

[0027] また、前記読み込み可否判定部は、前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられた前記チェック結果が、前記チェックアプリ管理部に記憶されていない場合には、前記アプリ識別子で特定されるプログラムが、攻撃されているか否かを判定するチェックが必要であることを示す情報を、前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けて前記チェックアプリ管理部に記憶させるとしてもよい。

[0028] また、前記チェックアプリ管理部は、前記プログラムが削除又は更新された場合には、削除又は更新された前記プログラムが有するアプリ識別子に対応づけられて記憶されているチェック結果を削除するとしてもよい。

[0029] これによると、アプリを最新のものに更新することによりバッファーオーバーフローの脆弱性が修正された場合には、情報処理装置は、読み込み処理を行えるようになる。また、アプリを削除した時、同じアプリ識別子を持つアプリが再度インストールされた場合には、情報処理装置は再度攻撃チェック処理を実施できるようになる。

[0030] また、前記チェックアプリ管理部は、前記チェック結果を、当該チェックアプリ管理部を備える前記情報処理装置、及び、当該チェックアプリ管理部を備える前記情報処理装置とは異なる情報処理装置の少なくとも一方に記憶しているとしてもよい。

[0031] これによると、他の情報処理装置が読み込んだことがあるファイルについては、自身が読み込んだことがなくても、チェックを行うことなく、安全性を判定することができる。

[0032] また、前記チェックアプリ管理部は、前記特定されたデータファイルが変更された場合には、当該変更されたデータファイルを示すコンテンツ識別子

に対応づけられて記憶されているチェック結果を削除するとしてもよい。

[0033] これによると、既存のコンテンツが、不正なプログラムが付加されたコンテンツに変更された場合においても、不正なプログラムを検出することができる。

[0034] なお、本発明は、このような情報処理装置として実現できるだけでなく、情報処理装置に含まれる特徴的な手段をステップとする情報処理方法として実現したり、そのような特徴的なステップをコンピュータに実行させるプログラムとして実現したりすることもできる。そして、そのようなプログラムは、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）等の記録媒体及びインターネット等の伝送媒体を介して流通させることができるのはいうまでもない。

[0035] さらに、本発明は、このような情報処理装置の機能の一部又は全てを実現する半導体集積回路（ＬＳＩ）として実現したりできる。

発明の効果

[0036] 本発明の情報処理装置によれば、安全性を損なうことなく、システムコール処理の応答性を向上させることができる。

図面の簡単な説明

[0037] [図1]図１は、本発明の実施の形態１におけるコンテンツ蓄積・表示システムの全体構成図である。

[図2]図２は、本発明の実施の形態１におけるコンテンツ蓄積・表示装置のソフトウェア構成図である。

[図3]図３は、本発明の実施の形態１におけるコンテンツ蓄積・表示装置のハードウェア構成図である。

[図4]図４は、本発明の実施の形態１における更新サーバの構成図である。

[図5]図５は、本発明の実施の形態１における関数の呼び出し関係図である。

[図6]図６は、本発明の実施の形態１における情報処理装置を有するＯＳの構成図である。

[図7]図７は、本発明の実施の形態１における攻撃チェック結果リストの構成

図である。

[図8]図８は、本発明の実施の形態１における要チェックアプリリストの構成図である。

[図9]図９は、本発明の実施の形態１における情報処理装置の他の構成を示すブロック図である。

[図10]図１０は、本発明の実施の形態１におけるチェック要否判定処理のフローチャートである。

[図11]図１１は、本発明の実施の形態１におけるファイル読み込み処理のフローチャートである。

[図12]図１２は、本発明の実施の形態２における情報処理装置の構成図である。

[図13]図１３は、本発明の実施の形態２における攻撃チェック結果リストの構成図である。

[図14]図１４は、本発明の実施の形態２におけるチェック要否判定処理のフローチャートである。

[図15]図１５は、本発明の実施の形態３におけるコンテンツ蓄積・表示システムの全体構成図である。

[図16]図１６は、本発明の実施の形態３における情報処理装置の構成図である。

[図17]図１７は、本発明の実施の形態３におけるチェック要否判定処理のフローチャートである。

[図18]図１８は、スタックの構成の一例を示す図である。

[図19]図１９は、従来のＯＳの構成の一例を示す図である。

発明を実施するための形態

[0038] 以下、本発明に係る情報処理装置の実施の形態について、図面を参照しながら詳細に説明する。

[0039] 以下、本発明の実施の形態について、図面を用いて詳細に説明する。なお、以下で説明する実施の形態は、いずれも本発明の好ましい一具体例を示す

ものである。以下の実施の形態で示される数値、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。本発明は、請求の範囲だけによって限定される。よって、以下の実施の形態における構成要素のうち、本発明の最上位概念を示す独立請求項に記載されていない構成要素については、本発明の課題を達成するのに必ずしも必要ではないが、より好ましい形態を構成するものとして説明される。

[0040] （実施の形態１）

本発明の実施の形態１に係る情報処理装置は、カメラやＰＣなどの機器から写真データを取り込み、蓄積し、ユーザの要求に応じて、写真データを表示するコンテンツ蓄積・表示装置である。

[0041] ＜コンテンツ蓄積・表示システム１０００の構成＞

図１は、本発明の実施の形態１におけるコンテンツ蓄積・表示システム１０００の構成図である。

[0042] 図１において、コンテンツ蓄積・表示システム１０００は、コンテンツ蓄積・表示装置１００１と、カメラ１０１０と、ＰＣ１０１１と、更新サーバ１０２０とを含む。

[0043] コンテンツ蓄積・表示装置１００１は、カメラ１０１０やＰＣ１０１１などから写真データを取り込み、蓄積する。また、蓄積した写真データを、ユーザの要求に応じて表示する。さらに、記録ディスク１０３０などの記録媒体を読み取るための読み取り部を持ち、ユーザ以外が撮影した写真データを取り込むことも可能である。

[0044] コンテンツ蓄積・表示装置１００１は、これらコンテンツの蓄積及び表示機能を実現するため、一意な識別子であるアプリ識別子を有する１以上のプログラムをＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）で実行する。

[0045] カメラ１０１０は、コンテンツ蓄積・表示装置１００１とＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）や無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅ

ａ　Ｎｅｔｗｏｒｋ）などを用いて接続される。カメラ１０１０は、ユーザが旅行などのイベントで写真を撮影した写真データを、カメラ１０１０に内蔵された不揮発メモリや、取り出し可能な記録媒体へ記録する。また、カメラ１０１０が、コンテンツ蓄積・表示装置１００１と接続された時に、記録した写真データをコンテンツ蓄積・表示装置１００１へ転送する。また、ユーザが、カメラ１０１０から記録媒体を取り出し、コンテンツ蓄積・表示装置１００１へ装着することにより、記録媒体に記録した写真データをコンテンツ蓄積・表示装置１００１へ転送することも可能である。

[0046] ＰＣ１０１１は、ネットワークに接続され、ユーザがメールを受信したり、Ｗｅｂブラウジングを行う際に使用される計算機である。また、ＰＣ１０１１は、コンテンツ蓄積・表示装置１００１ともネットワークで接続される。メールに添付された写真データやＷｅｂブラウジング時にダウンロードした写真データなどは、ネットワークを介して、ＰＣ１０１１からコンテンツ蓄積・表示装置１００１へ取り込む。

[0047] 更新サーバ１０２０は、コンテンツ蓄積・表示装置１００１とネットワークで接続される。更新サーバ１０２０は、コンテンツ蓄積・表示装置１００１用の更新用ソフトウェアを格納し、コンテンツ蓄積・表示装置１００１からの要求に応じて、コンテンツ蓄積・表示装置１００１へ、更新用ソフトウェアを転送する。更新用ソフトウェアは、コンテンツ蓄積・表示装置１００１内で動作するソフトウェアに不具合が見つかった場合や、ソフトウェアに機能を追加する場合などに作成する。

[0048] 記録ディスク１０３０は、写真データを記録するための記録媒体である。

[0049] また、コンテンツ蓄積・表示装置１００１は、本発明に係る情報処理装置を有する。

[0050] ＜コンテンツ蓄積・表示装置１００１のソフトウェア構成＞

図２は、本発明の実施の形態１におけるコンテンツ蓄積・表示装置１００１のソフトウェア構成図である。

[0051] 図２において、コンテンツ蓄積・表示装置１００１は、ＯＳ１１０１と、

コンテンツ収集アプリ１１０２と、表示アプリ１１０３と、編集アプリ１１０４と、管理アプリ１１０５とを備える。

[0052] ＯＳ１１０１は、情報処理装置１００を有する。ＯＳ１１０１は、ＯＳ１１０１上で動作するアプリ（コンテンツ収集アプリ１１０２や表示アプリ１１０３、編集アプリ１１０４、管理アプリ１１０５等のプログラム）を、メモリ上にロードして実行する。また、ＯＳ１１０１が管理するリソースに対して、アプリから利用要求があった時に、ＯＳ１１０１は、要求してきたアプリがそのリソースを利用する権限があるかを確認する。確認の結果、権限があると判定した場合には、ＯＳ１１０１は、情報処理装置１００を介してアプリにリソースを提供する。アプリからＯＳ１１０１への要求としては、ファイルへの読み込み要求や書き込み要求、また、ネットワークで接続された他の機器への接続要求などがある。

[0053] コンテンツ収集アプリ１１０２は、カメラ１０１０やＰＣ１０１１、記録ディスク１０３０に記録された写真データを収集し、コンテンツ蓄積・表示装置１００１内に蓄積するアプリである。コンテンツ収集アプリ１１０２は、カメラ１０１０などの機器がＵＳＢや無線ＬＡＮなどで接続されるかを監視し、接続されたことを検出した場合には、その機器内や機器に装着された記録メディアに記録されている写真データを収集する。また、ネットワーク接続を監視し、ＰＣ１０１１などの機器が接続されたことを検出した場合には、その機器内に記録されている写真データを収集する。コンテンツ収集アプリ１１０２は、収集した写真データをコンテンツ蓄積・表示装置１００１内の不揮発性記憶装置へ保存し、蓄積する。

[0054] 表示アプリ１１０３は、コンテンツ収集アプリ１１０２が蓄積した写真データを液晶ディスプレイなどの表示装置に表示するアプリである。表示アプリ１１０３は、写真データに付属するサムネイル画像を一覧表示したり、ユーザが指定した１つの写真データを表示したりする。また、表示アプリ１１０３は、ユーザが選択した複数の写真データを、一定時間間隔で表示するスライドショー表示も行う。

[0055] 編集アプリ１１０４は、コンテンツ蓄積・表示装置１００１に保存している写真データを編集するアプリである。編集アプリ１１０４は、ユーザの選択に応じて、編集した写真データを新しい写真データとして保存したり、編集した写真データを上書き保存する。また、編集アプリ１１０４は、ユーザが不要と判断した写真データを、コンテンツ蓄積・表示装置１００１から削除する。

[0056] 管理アプリ１１０５は、コンテンツ蓄積・表示装置１００１内にインストールされているアプリやＯＳを管理する。管理アプリ１１０５は、更新サーバ１０２０と通信し、コンテンツ蓄積・表示装置１００１内にインストールされているアプリやＯＳ用の更新用ソフトウェアがあるか定期的に確認する。管理アプリ１１０５は、更新用ソフトウェアを検出した場合、ユーザに対して通知を行い、該当するアプリやＯＳの更新用ソフトウェアを更新サーバ１０２０から受信し、更新処理を行う。

[0057] ＜コンテンツ蓄積・表示装置１００１のハードウェア構成＞

図３は、本発明の実施の形態１におけるコンテンツ蓄積・表示装置１００１のハードウェア構成図である。

[0058] 図３において、コンテンツ蓄積・表示装置１００１は、システムＬＳＩ１２００と、メモリ１２１０と、不揮発性記憶装置１２２０とを含む。

[0059] システムＬＳＩ１２００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１２０１と、カードＩ／Ｆ（Ｉｎｔｅｒｆａｃｅ）１２０２と、ネットワークＩ／Ｆ１２０３と、入出力Ｉ／Ｆ１２０４とを含む。

[0060] ＣＰＵ１２０１は、メモリ１２１０に格納されたＯＳ１１０１や各アプリに含まれる命令コードを実行することにより、コンテンツ蓄積・表示装置１００１全体の動作を制御する。また、ＣＰＵ１２０１は、特権モードと非特権モードの２つのモードを持つ。ＯＳ１１０１は特権モードで動作し、メモリ１２１０やカードＩ／Ｆ１２０２、ネットワークＩ／Ｆ１２０３、入出力Ｉ／Ｆ１２０４などの各種リソースに、自由にアクセスできる。したがって、ＯＳ１１０１が有する本発明に係る情報処理装置１００は、特権モードで

動作する。

[0061] また、コンテンツ収集アプリ１１０２と、表示アプリ１１０３と、編集アプリ１１０４と、管理アプリ１１０５は非特権モードで動作し、ＯＳ１１０１が設定した範囲内のみアクセス可能である。 メモリ１２１０は、ＯＳ１１０１と、コンテンツ収集アプリ１１０２と、表示アプリ１１０３と、編集アプリ１１０４と、管理アプリ１１０５とを格納する。なお、図３は、図２に示されるソフトウェア構成の各要素をメモリ１２１０にロードした様子を示している。

[0062] 不揮発性記憶装置１２２０は、呼び出し元チェック結果表１２２１と、コンテンツＡ１２２２と、コンテンツＢ１２２３とを格納する。また、図示しないが、不揮発性記憶装置１２２０は、図２に示されるソフトウェア構成をメモリ１２１０にロードする前の各構成要素を格納する。具体的には、図２に示されるコンテンツ収集アプリ１１０２、表示アプリ１１０３、編集アプリ１１０４、及び管理アプリ１１０５は、それぞれ、図３に示されるメモリ１２１０に格納されたコンテンツ収集アプリ１１０２、表示アプリ１１０３、編集アプリ１１０４、及び管理アプリ１１０５に対応する。これらの各構成要素を実現するためのソフトウェアが、ＣＰＵ１２０１上で実行されることにより、各機能が実現される。

[0063] コンテンツ蓄積・表示装置１００１は、さらに、図３に図示されていない液晶ディスプレイなどの入出力装置を備えているが、これらは本発明の本質ではないので説明を省略する。また、システムＬＳＩ１２００は、さらに、図３に図示されていない周辺回路などを備えているが、これらは本発明の本質ではないので説明を省略する。また、メモリ１２１０は、さらに、図２や図３に図示されていないアプリや、写真データを処理するための作業領域を格納していてもよい。また、不揮発性記憶装置１２２０は、さらに、図２や図３に図示されていないアプリや、コンテンツを格納していてもよい。

[0064] ＜更新サーバ１０２０の構成＞

図４は、本発明の実施の形態１における更新サーバ１０２０の構成図であ

る。

[0065] 図４において、更新サーバ１０２０は、更新処理受付部１３００と、更新用ソフトウェア保持部１３０１とを含む。

[0066] 更新処理受付部１３００は、コンテンツ蓄積・表示装置１００１の管理アプリ１１０５から問い合わせを受ける。問い合わせの結果、更新が必要な場合には、更新処理受付部１３００は、管理アプリ１１０５と連携して、コンテンツ蓄積・表示装置１００１内のソフトウェアの更新処理を行う。更新処理において、更新処理受付部１３００は、更新用ソフトウェア保持部１３０１から更新用ソフトウェアを取得し、管理アプリ１１０５へ送信する。

[0067] 更新用ソフトウェア保持部１３０１は、コンテンツ蓄積・表示装置１００１内のソフトウェアの更新処理に必要な更新用ソフトウェアを保持する。

[0068] ＜攻撃チェック処理の実施タイミング＞

攻撃チェック処理（すなわち、アプリが攻撃されているか否かを判定する処理）は、攻撃される前には実施する必要がなく、攻撃された後に実施する必要がある。つまり、攻撃される可能性のあるタイミングが分かれば、その直後に攻撃チェック処理を実施すればよいことになる。なぜなら、攻撃された後、すなわち、実行中のアプリが使用するコールスタック上で不正なプログラムが動作している状態でなければ、攻撃されているか否かを判定することは困難なためである。よって、攻撃された直後に、攻撃チェック処理を実施できることが望ましい。

[0069] 本発明の実施の形態１におけるコンテンツ蓄積・表示装置１００１は、ＰＣの様に、ユーザが自由にアプリを追加したり、ネットワークを経由して写真データやアプリをダウンロードしたり出来ない装置である。そのため、攻撃者が、コンテンツ蓄積・表示装置１００１を攻撃するためには、コンテンツ蓄積・表示装置１００１が取り込む写真データなどの写真データを細工する方法しかない。例えば、攻撃者は、コンテンツ蓄積・表示装置１００１内で写真データを表示する表示アプリ１１０３の脆弱性（バッファーオーバーフロー等）を衝くような細工を行った写真データ（不正なプログラムを付加

したコンテンツ）を作成する。攻撃者は、この細工を行った写真データをコンテンツ蓄積・表示装置１００１に取り込ませることで、コンテンツ蓄積・表示装置１００１を攻撃する。

[0070] 上記の攻撃を行う時、コンテンツ蓄積・表示装置１００１は、表示アプリ１１０３で不正なプログラムを付加したコンテンツを読み込み、表示処理を行おうとしたタイミングで攻撃される。そのため、攻撃チェック処理は、写真データの読み込み処理を行った後のタイミングで実施する必要がある。

[0071] そこで、本発明の実施の形態１では、コンテンツ蓄積・表示装置１００１が写真データの読み込み処理を行った後、その次のシステムコール要求のタイミングで攻撃チェック処理を実施する。

[0072] また、バッファーオーバーフローの脆弱性を利用して攻撃する場合は、不正なプログラムを付加したコンテンツを表示アプリ１１０３が読み込めば、必ずバッファーオーバーフローが発生し、不正なプログラムが動作する。つまり、表示アプリ１１０３が攻撃されれば、その時に読み込んだ写真データは、不正なプログラムを付加したコンテンツであり、攻撃されなければ、通常の写真データを読み込んだと判断できる。

[0073] そこで、以前読み込んで攻撃されなかった写真データを再度読み込んだ時、コンテンツ蓄積・表示装置１００１は、その次のシステムコール要求のタイミングで攻撃チェック処理を実施しない。これにより、攻撃チェック処理の実施を省くことが出来る。

[0074] 但し、写真データが、表示アプリ１１０３のどの部分で処理されたかにより、攻撃チェック処理の実施を省ける場合とそうでない場合がある。

[0075] 図５は、表示アプリ１１０３内の関数呼び出し関係を表した模式図である。

[0076] 図５において、表示アプリ１１０３は、ｍａｉｎ関数１５６０と、サムネイル取得関数１５６１と、データ本体取得関数１５６２と、ｒｅａｄ関数１５６３とを含む。

[0077] ｍａｉｎ関数１５６０は、コンテンツ蓄積・表示装置１００１が蓄積して

いる写真データを、サムネイルを用いて一覧表示したり、ユーザがサムネイルから選択した写真データを表示する処理を行う。

[0078] サムネイル取得関数１５６１は、コンテンツ蓄積・表示装置１００１が蓄積している写真データからサムネイルデータを取得する。

[0079] データ本体取得関数１５６２は、コンテンツ蓄積・表示装置１００１が蓄積している写真データから写真本体のデータを取得する。

[0080] ｒｅａｄ関数１５６３は、サムネイル取得関数１５６１又はデータ本体取得関数１５６２から写真データの読み込み依頼を受けて、ＯＳ１１０１に対して、ファイル読み込みのシステムコール要求を行う。

[0081] 図５の表示アプリ１１０３において、例えば、データ本体取得関数１５６２にバッファーオーバーフローの脆弱性があった場合を考える。表示アプリ１１０３が、サムネイル表示を行う時には、ｍａｉｎ関数１５６０からサムネイル取得関数１５６１とｒｅａｄ関数１５６３とを経由し、ＯＳ１１０１に対して、ファイル読み込みのシステムコール要求を行う（経路１）。この場合、経路１の途中にバッファーオーバーフローの脆弱性を持つ関数はないため、攻撃されることはない。しかし、これだけの理由で、その後ユーザが同じ写真を選択し、この写真データの本体を表示する時に、攻撃チェック処理を実施しなくてもよいと判断することは危険である。バッファーオーバーフローの脆弱性を利用した攻撃は、前述の通り、不正なデータを、バッファーオーバーフローの脆弱性を有する関数から呼び出した時に、はじめて実行され、検出も可能になるためである。

[0082] 具体的に、写真データ本体の表示では、ｍａｉｎ関数１５６０からデータ本体取得関数１５６２とｒｅａｄ関数１５６３とを経由し、ＯＳ１１０１に対して、ファイル読み込みのシステムコール要求を行う（経路２）。ここで、経路２の途中にあるデータ本体取得関数１５６２にバッファーオーバーフローの脆弱性があるとする。この場合、読み込んだ写真データが、不正なプログラムが付加されたコンテンツであった場合、コンテンツ蓄積・表示装置１００１は不正なプログラムによって攻撃される。

[0083] 以上述べたように、攻撃チェック処理の実施を省くかどうかを、過去にその写真データを読み込んだか読み込んでいないかだけで単純に判断した場合、アプリに脆弱性があった場合には、攻撃される可能性が残る。よって、攻撃チェックが必要か否かを判定する際には、関数呼び出し関係における経路を特定し、特定された経路を考慮して、判定する仕組みが必要となる。

[0084] そこで、本発明の実施の形態１に係る情報処理装置１００は、経路が異なる場合は、その途中で実行される関数が異なることを利用して、経路の違いを判定する。具体的には、経路が異なる場合には、システムコールを要求した時のアプリ（例えば、図５では表示アプリ１１０３）のスタックポインタの値が異なる値になることを利用して、経路の違いを判定する。そのため、後述するように、攻撃チェック判定部１５１０が判定に利用する攻撃チェック結果リスト１５３０には、アプリ識別子とコンテンツ識別子以外に、システムコールを要求した時の呼び出し元アドレスとスタックポインタ値も、チェック結果に対応付けられて、一緒に格納される。

[0085] ＜情報処理装置１００の構成＞

図６は、本発明の実施の形態１におけるＯＳ１１０１が有する情報処理装置１００の構成図である。

[0086] 図６において、情報処理装置１００は、チェックアプリ管理部１５００と、システムコール管理部１５０１と、ファイル読み込み管理部１５０２とを含む。

[0087] チェックアプリ管理部１５００は、アプリが攻撃されているかをチェックしたチェック結果を管理する。また、攻撃されているかチェックする必要があるアプリを管理する。

[0088] 具体的には、チェックアプリ管理部１５００は、（Ａ）アプリ特定部１５１１により特定されたプログラム（アプリ）が攻撃されているか否かをチェックした結果、及び、（Ｂ）特定されたプログラムが、攻撃されているか否かを判定するチェックが必要であるかを示す情報、の両方を含む情報であるチェック結果を、特定されたプログラムが有するアプリ識別子と、呼び出し

元とに対応付けて記憶している。

[0089] より具体的には、チェックアプリ管理部１５００は、図７に示される攻撃チェック結果リスト１５３０を有している。チェックアプリ管理部１５００は、攻撃チェック結果リスト１５３０を更新することにより、チェック結果の管理を行う。

[0090] なお、本発明の実施の形態１～３において、「アプリが攻撃されている」とは、アプリに存在するバッファーオーバーフローの脆弱性を衝かれて、アプリのスタック上で不正なプログラムが動作している状態を意味する。

[0091] 図７は、攻撃チェック結果リスト１５３０の一例を示している。この攻撃チェック結果リスト１５３０は、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値と、チェック結果とを含む。

[0092] アプリ識別子は、ＯＳ１１０１上で動作するアプリを特定する識別子である。アプリ識別子は、例えば本発明の実施の形態１においては、アプリのファイル名である。

[0093] コンテンツ識別子は、不揮発性記憶装置１２２０に格納される写真データファイルを識別するための識別子である。コンテンツ識別子は、例えば本発明の実施の形態１においては、写真データファイルのファイル名である。

[0094] 呼び出し元アドレスは、アプリがシステムコールを要求した時におけるアプリの実行コードのアドレスである。例えば、表示アプリが写真データの読み込み要求をした時の表示アプリの実行コードのアドレスである。すなわち、呼び出し元アドレスは、本発明の実施の形態１においては、ＯＳ１１０１から表示アプリへ戻る時に使用するリターンアドレスとして使用されるアドレスである。

[0095] スタックポインタ値は、アプリがシステムコールを要求した時におけるアプリのスタックポインタの値である。例えば、表示アプリが写真データの読み込み要求をした時の、表示アプリのスタックポインタの値である。

[0096] チェックアプリ管理部１５００は、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値とを、ファイル読み込み管理

部１５０２から受け取る。

[0097] 攻撃チェック結果リスト１５３０には、攻撃チェック部１５１２によるチェック結果として、攻撃されたかどうかのチェック結果“○”、“×”、又は、攻撃されているかのチェックが必要なことを示す“要”の３つの値のうちいずれかが格納される。ここで、チェック結果が“○”であれば、対応するアプリ識別子を有するプログラム（アプリ）が攻撃されていないことを表す。また、チェック結果が“×”であれば、攻撃されていることを表す。また、チェック結果が“要”であれば、攻撃されているか否かを判定するチェックが必要であることを表す。なお、“○”、“×”、“要”という表記は、いずれも例示であり、任意のその他の文字や記号が攻撃チェック結果リスト１５３０に格納されてもよい。例えば、“○”の代わりに“ＯＫ”を、“×”の代わりに“ＮＧ”を、“要”の代わりに“不明”等を使用してもよい。

[0098] チェック結果は、システムコール管理部１５０１が備える攻撃チェック部１５１２からチェックアプリ管理部１５００が受け取る。

[0099] なお、攻撃チェック結果リスト１５３０は、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値と、チェック結果とを含めばよく、その順番はこれに限らない。例えば、コンテンツ識別子、アプリ識別子、呼び出し元アドレス、スタックポインタ値、チェック結果の順番でも、チェック結果、アプリ識別子、コンテンツ識別子、呼び出し元アドレス、スタックポインタ値の順番でもよい。

[0100] また、攻撃チェック結果リスト１５３０のデータ構造は、図７に示される表の形式である必要はない。アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値と、チェック結果との組み合わせを識別できる形式であればよい。例えば、横軸にアプリ識別子、縦軸にコンテンツ識別子を持つ表を用い、それぞれのアプリ識別子とコンテンツ識別子の組み合わせごとに、呼び出し元アドレスとスタックポインタ値との組み合わせのリストへのリンクを持っていてもよい。

[0101] 再度、図６を参照し、チェックアプリ管理部１５００は、アプリ識別子で示されるアプリのチェックが必要かどうかの問い合わせをシステムコール管理部１５０１から受ける。チェックアプリ管理部１５００は、システムコール管理部１５０１から問い合わせを受けると、攻撃チェック結果リスト１５３０から、アプリのチェック結果を取得し、その取得したチェック結果を返す。

[0102] また、チェックアプリ管理部１５００は、攻撃されていないかをチェックしたチェック結果とアプリ識別子とをシステムコール管理部１５０１が備える攻撃チェック部１５１２から受け取り、受け取ったチェック結果を攻撃チェック結果リスト１５３０へ記録する。

[0103] システムコール管理部１５０１は、攻撃チェック判定部１５１０と、アプリ特定部１５１１と、攻撃チェック部１５１２とを備える。

[0104] システムコール管理部１５０１は、システムコールを要求したアプリが攻撃されているかどうかを、攻撃チェック判定部１５１０を用いて判定する。攻撃されていないと判定した場合には、要求されたシステムコールの処理を実行する。攻撃されていると判定した場合には、システムコールを要求したアプリに対してエラーを返す。なお、システムコール要求時のチェック要否判定処理の詳細は、フローチャートを用いて後ほど説明する。

[0105] 攻撃チェック判定部１５１０は、システムコールを要求したアプリに対して、攻撃されているかどうかをチェックする必要があるかを判定する。具体的には、攻撃チェック判定部１５１０は、アプリ特定部１５１１で特定されたプログラムの呼び出し元に基づいて、特定されたプログラムが攻撃されているかのチェックを行うか否かを判定する。

[0106] より具体的には、攻撃チェック判定部１５１０は、特定されたプログラムが有するアプリ識別子に対応付けられてチェックアプリ管理部１５００が有する攻撃チェック結果リスト１５３０に記憶されているチェック結果を取得する。取得したチェック結果が、プログラム（アプリ）が攻撃されていないこと、又は、プログラム（アプリ）が攻撃されていることを表す場合には、

攻撃チェック判定部１５１０は、攻撃されているかのチェックを行わないと判定する。一方、取得したチェック結果が、攻撃されているか否かを判定するチェックが必要である（すなわち、安全か否かが不明である）ことを表す場合には、攻撃チェック判定部１５１０は、攻撃チェック部１５１２によるチェックを行うと判定する。

[0107] さらに具体的には、攻撃チェック判定部１５１０は、チェックアプリ管理部１５００からシステムコールを要求したアプリの攻撃チェック結果を取得する。取得したチェック結果が“要”であった場合には、攻撃チェック判定部１５１０は、攻撃チェック部１５１２へチェックを依頼する。また、チェック結果が“○”であった場合には、チェックを行わず、要求されたシステムコール処理を実行する。また、チェック結果が“×”であった場合には、システムコールを要求したアプリへエラーを返す。また、チェック結果がいずれの場合であっても、攻撃チェック判定部１５１０は、攻撃チェック部１５１２から取得したチェック結果の登録をチェックアプリ管理部１５００へ依頼する。

[0108] アプリ特定部１５１１は、システムコールを要求したアプリを特定する。具体的には、コンテンツ蓄積・表示装置１００１で実行されているプログラムが有するアプリ識別子を取得することで、システムコールを要求したアプリを特定する。

[0109] 本発明の実施の形態１においては、アプリ特定部１５１１は、ＯＳ１１０１が管理するプロセス管理用の構造体に格納されているファイル名をアプリ識別子として用いて、アプリを特定する。アプリ特定部１５１１は、アプリ識別子であるアプリのファイル名を攻撃チェック判定部１５１０へ通知する。

[0110] 攻撃チェック部１５１２は、攻撃チェック判定部１５１０が、アプリ特定部１５１１で特定されたアプリに対して攻撃チェックを行うと判定した場合には、そのアプリ（すなわち、システムコールを要求したアプリ）が攻撃されているか否かをチェックする。

[0111] チェック方法としては、例えば、前述した特許文献１又は特許文献２に詳しく説明されている。また、他のチェック方法を用いてもよい。

[0112] ファイル読み込み管理部１５０２は、読み込み可否判定部１５２０と、コンテンツ特定部１５２１と、アプリ特定部１５２２と、呼び出し元特定部１５２３とを備える。

[0113] ファイル読み込み管理部１５０２は、アプリからシステムコールによりファイル読み込みが要求された時に、システムコール管理部１５０１から呼び出され、ファイルの読み込み処理を行う。ファイル読み込み管理部１５０２は、ファイルの読み込み処理時に、攻撃チェック結果リスト１５３０を参照し、読み込み処理を実施するかどうかを判定する。なお、ファイル読み込み処理の詳細は、フローチャートを用いて後ほど説明する。

[0114] 読み込み可否判定部１５２０は、後述するコンテンツ特定部１５２１により特定されたデータファイルを読み込むか否かを判定する。すなわち、読み込み可否判定部１５２０は、（Ａ）コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられたチェック結果が、チェックアプリ管理部１５００に記憶されていないか、又は、（Ｂ）コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられたチェック結果が、チェックアプリ管理部１５００に記憶されており、かつ、チェック結果が、アプリ特定部１５１１により特定されたプログラム（アプリ）が攻撃されていないことを示す場合には、特定されたデータファイルを読み込むと判定する。

[0115] また、コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられているチェック結果がチェックアプリ管理部１５００に記憶されており、かつ、チェック結果が、アプリ特定部１５１１により特定されたプログラム（アプリ）が以前に攻撃されたことを示す場合には、読み込み可否判定部１５２０は、特定されたデータファイルを読み込まないと判定する。

[0116] より具体的には、読み込み可否判定部１５２０は、チェックアプリ管理部１５００から攻撃チェック結果を取得し、取得したチェック結果に応じて、読み込み可否を判定する。読み込み可否判定部１５２０は、チェック結果が

“○”の場合は、読み込み可と判定し、チェック結果が“×”の場合は、読み込み不可と判定する。

[0117] また、読み込み可否判定部１５２０は、攻撃チェック結果リスト１５３０にチェック結果が登録されていなかった場合には、読み込み可と判定し、チェックアプリ管理部１５００へチェック結果“要”を登録するように依頼する。すなわち、読み込み可否判定部１５２０は、判定を行った際に、コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられたチェック結果が、チェックアプリ管理部に記憶されていない場合には、アプリ特定部１５１１により特定されたプログラムが、攻撃されているか否かを判定するチェックが必要であることを示す情報を、コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けてチェックアプリ管理部１５００に記憶させる。

[0118] より詳細には、後述する。

[0119] コンテンツ特定部１５２１は、アプリ特定部１５１１で特定されたプログラム（アプリ）がプログラムコード（すなわち、システムコール）を呼び出すことにより読み込もうとしているデータファイルを、そのデータファイルを示す識別子であるコンテンツ識別子を用いて特定する。

[0120] コンテンツ特定部１５２１は、例えば、ユーザの操作により表示アプリ１１０３が読み込んだ写真データを特定する。本発明の実施の形態１においては、コンテンツ特定部１５２１がデータファイルを特定するための方法として、読み込み依頼時に通知されるファイル識別子に格納されている写真データのファイル名を用いて、写真データを特定する方法を用いる。コンテンツ特定部１５２１は、写真データのファイル名をコンテンツ識別子として読み込み可否判定部１５２０へ通知する。

[0121] アプリ特定部１５２２は、システムコール管理部１５０１が有するアプリ特定部１５１１と同じ機能を持つが、アプリ識別子を読み込み可否判定部１５２０へ通知する点が異なる。すなわち、アプリ特定部１５１１は、攻撃チェック結果リスト１５３０を参照するためにアプリ識別子を取得する。一方

、アプリ特定部１５２２は、攻撃チェック結果リスト１５３０を更新するためにアプリ識別子を取得する。

[0122] 呼び出し元特定部１５２３は、アプリ特定部１５１１により特定されたプログラム（アプリ）が、プログラムコードの呼び出し時に、プログラムのどの部分からプログラムコードを呼び出したかを特定する。具体的には、呼び出し元特定部１５２３は、ＯＳ１１０１のファイルの読み込み処理を呼び出した呼び出し元が、アプリのどの部分であるかを特定する。

[0123] 本発明の実施の形態１に係る呼び出し元特定部１５２３は、呼び出し元を特定するための方法として、アプリが写真データの読み込み要求をした時のアプリの実行コードのアドレスとスタックポインタの値とを用いて、呼び出し元を特定する。すなわち、呼び出し元特定部１５２３は、アプリ特定部１５１１により特定されたプログラム（アプリ）からプログラムコード（システムコール）を呼び出した場合の、（Ａ）プログラムコードの実行処理後、特定されたプログラムへ実行処理を戻すための戻し先を示すメモリ内のアドレスであるリターンアドレスと、（Ｂ）特定されたプログラムが使用するコールスタックのスタックポインタの値とを用いて、呼び出し元を特定する。より具体的には、呼び出し元特定部１５２３は、ファイルの読み込み処理終了時にアプリに戻るためのリターンアドレスと、ファイルの読み込み要求をした時点でのアプリのスタックポインタの値を利用して、呼び出し元を特定する。

[0124] なお、本発明の実施の形態１では、攻撃チェック判定部１５１０は攻撃チェック結果リスト１５３０を用いて攻撃チェック処理を行うかを判定したが、本発明はこれに限定されるものではない。例えば、チェックアプリ管理部１５００は、攻撃チェック処理が必要なアプリを要チェックアプリリスト１５３１として、攻撃チェック結果リスト１５３０とは別に管理してもよい。要チェックアプリリスト１５３１の構造の一例を図８に示す。この場合、チェックアプリ管理部１５００は、攻撃チェック結果リスト１５３０には、チェック結果として“○”又は“×”のみを格納する。

[0125] この場合、チェックアプリ管理部１５００は、読み込み可否判定部１５２０からチェック結果“要”を登録するように依頼された場合には、図８に示される要チェックアプリリスト１５３１へ依頼されたアプリを登録する。また、攻撃チェック判定部１５１０は、チェックアプリ管理部１５００が備える要チェックアプリリスト１５３１へ、システムコールを要求したアプリのアプリ識別子が登録されているかを問い合わせる。

[0126] また、攻撃チェック判定部１５１０は、攻撃チェック部１５１２によるチェック結果が“×”の場合、チェック結果が“×”となったコンテンツ識別子と同じコンテンツ識別子に関連するチェック結果を、全て“×”にするようにチェックアプリ管理部１５００へ依頼してもよい。具体的には、チェックアプリ管理部１５００は、過去のチェック結果に“×”が含まれているコンテンツ識別子と同じコンテンツ識別子を有する攻撃チェック結果リスト１５３０内の全ての行のチェック結果を“×”にしてもよい。

[0127] さらに、“×”となったアプリ識別子と同じアプリ識別子に関連するチェック結果を、全て“×”にしてもよい。具体的には、チェックアプリ管理部１５００は、過去のチェック結果に“×”が含まれているアプリ識別子と同じアプリ識別子を有する攻撃チェック結果リスト１５３０内の全ての行のチェック結果を“×”にしてもよい。

[0128] また、読み込み可否判定部１５２０は、過去のチェック結果に“×”が含まれているコンテンツ識別子と同じコンテンツ識別子を有する写真データ等の場合は、その写真データ等を読み込まないとしてもよい。さらに、過去のチェック結果に“×”が含まれている呼び出し元アドレスと同じ呼び出し元アドレスからの呼び出しは実行せず、その写真データ等を読み込まないとしてもよい。また、読み込み可否判定部１５２０は、アプリ識別子のほか、呼び出し元アドレスとスタックポインタの値とに関して同様の処理を行ってもよい。

[0129] なお、システムコール管理部１５０１とファイル読み込み管理部１５０２は、別々に存在せずともよい。例えば、ファイル読み込み管理部１５０２が

システムコール管理部１５０１の内部にあってもよい。

[0130] 図９は、情報処理装置の、他の構成を示したブロック図である。

[0131] 図９に示されるように、情報処理装置１００Ａは、アプリ特定部１５１１と、呼び出し元特定部１５２３と、攻撃チェック判定部１５１０と、チェックアプリ管理部１５００とを備えている。

[0132] この構成によっても、情報処理装置１００Ａは、図６に示される情報処理装置１００と同様の効果を奏する。

[0133] すなわち、情報処理装置１００Ａは、システムコールを要求したアプリを特定するアプリ識別子を、アプリ特定部１５１１から取得できる。

[0134] また、情報処理装置１００Ａは、アプリ識別子で特定されるアプリがシステムコールを要求した際の、アプリの実行スタックにおけるスタックポインタと、リターンアドレスとを、呼び出し元特定部１５２３から取得できる。

[0135] また、攻撃チェック判定部１５１０が、攻撃チェック結果リスト１５３０を有するチェックアプリ管理部１５００に問い合わせることで、情報処理装置１００Ａは、スタックポインタとリターンアドレスとで特定される呼び出し経路をたどるシステムコール要求が、既に安全性が確認されているか否かを判定することができる。

[0136] よって、図９の構成によっても、情報処理装置１００と同様の発明の効果を奏する。したがって、１度安全性が確認された呼び出し経路をたどるシステムコール要求については、攻撃チェックを省略することにより、情報処理装置１００Ａは、迅速にシステムコール要求を処理することができる。

[0137] なお、本発明の実施の形態１では、読み込み可否判定部１５２０は、攻撃チェック結果リスト１５３０にチェック結果が登録されていなかった場合には、チェックアプリ管理部１５００へチェック結果“要”を登録するとしたが、これに限定されるものではない。読み込み可否判定部１５２０は、アプリから読み込みを依頼された写真データの取り込み元に応じて、チェック不要と判定してもよい。この時、チェック結果として“要”ではなく、“○”を登録する。読み込み可否判定部１５２０が、チェック不要と判定すべき取

り込み元としては、写真データを攻撃者が書き換えられない、例えば、カメラ１０１０などがある。

[0138] また、上記とは逆に、特定の取り込み元から取り込んだ時のみチェックしてもよい。この時、読み込み可否判定部１５２０は、特定の取り込み元から取り込んだ写真データの読み込みを依頼された場合のみ、チェック結果“要”を登録する。また、それ以外の取り込み元であった場合には、チェック結果として“○”を登録する。チェックする取り込み元としては、写真データを攻撃者が書き換えられる機器、例えば、ＰＣ等がある。また、Ｉｎｔｅｒｎｅｔなどのネットワークを経由して取り込んだ写真データは全てチェックするとしてもよい。

[0139] ＜チェック要否判定処理＞

システムコール管理部１５０１は、システムコールを要求したアプリが攻撃されているかどうかを、攻撃チェック判定部１５１０を用いて判定する。攻撃されていないと判定した場合にのみ、要求されたシステムコールの処理を実行することで、不正なシステムコール要求の実行を防止する。この時、システムコールを要求したアプリに対して、そのアプリが攻撃されているかどうかのチェックが必要か判定し、チェックが必要な場合のみチェック処理を実行することで、システムコール要求時のＯＳ１１０１による処理を高速化する。

[0140] 以下、表示アプリ１１０３がＯＳ１１０１へシステムコールを依頼した時に、表示アプリ１１０３が攻撃されているかをチェックする必要があるか否かを判定する、チェック要否判定処理について、図１０のフローチャートを用いて説明する。

[0141] まず、表示アプリ１１０３は、ＯＳ１１０１が有する情報処理装置１００のシステムコール管理部１５０１へシステムコールを依頼する（Ｓ１０００）。

[0142] システムコール管理部１５０１は、アプリ特定部１５１１を利用して、システムコールを依頼したアプリである依頼アプリの識別子を取得する（Ｓ１

００１）。アプリ特定部１５１１は、ＯＳ１１０１が管理するプロセス管理用の構造体に格納されているアプリのファイル名を取得し、このファイル名をアプリ識別子とする。

[0143] 次に、システムコール管理部１５０１が備える攻撃チェック判定部１５１０は、システムコールを依頼してきたアプリが攻撃されているかチェックする必要があるか否かを判定するために、システムコールを依頼してきたアプリの、過去の攻撃チェック結果をチェックアプリ管理部１５００へ問い合わせる（Ｓ１００２）。この時、攻撃チェック判定部１５１０は、チェックアプリ管理部１５００へＳ１００１で取得したアプリ識別子を通知する。

[0144] チェックアプリ管理部１５００は、攻撃チェック判定部１５１０から通知されたアプリ識別子に関連づけられたデータの組を攻撃チェック結果として攻撃チェック結果リスト１５３０から取得する（Ｓ１００３）。アプリ識別子に関連づけられたデータの組とは、例えば、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値と、チェック結果とを含む。すなわち、アプリ識別子に関連づけられたデータの組とは、攻撃チェック結果リスト１５３０の各行のうち、通知されたアプリ識別子と同一のアプリ識別子を含む行に含まれる情報である。

[0145] チェックアプリ管理部１５００は、Ｓ１００３で取得した攻撃チェック結果を攻撃チェック判定部１５１０へ通知する（Ｓ１００４）。

[0146] システムコール管理部１５０１が有する攻撃チェック判定部１５１０は、受けとった攻撃チェック結果をもとに、チェック要否判定を行う（Ｓ１００５）。具体的には、受け取った攻撃チェック結果の「チェック結果」列に“要”が含まれている場合は攻撃チェックが必要（Ｓ１００５で「要」）であると判定し、含まれない場合は攻撃チェックが不要（Ｓ１００５で「否」）であると判定する。

[0147] 攻撃チェック判定部１５１０は、ステップＳ１００５で「要」と判定した場合には、攻撃チェック部１５１２を利用して、システムコールを要求したアプリが攻撃されているかどうかをチェックする（Ｓ１００６）。チェック

方法としては、例えば、特許文献１又は特許文献２に詳しく説明されている。また、他の方法を利用してもよい。

[0148] システムコール管理部１５０１は、チェックが終了すると、そのチェック結果の登録を、チェックアプリ管理部１５００へ依頼する（Ｓ１００７）。攻撃チェック判定部１５１０は、ステップＳ１００４で受け取った結果のうち、チェック結果が“要”となっていたデータの組（すなわち、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値と、チェック結果との組）に対して、チェック結果をステップＳ１００６でチェックした結果に書き換えたデータの組をチェックアプリ管理部１５００へ通知する。

[0149] チェックアプリ管理部１５００は、攻撃チェック判定部１５１０から受け取ったデータの組を攻撃チェック結果リスト１５３０へ反映する（Ｓ１００８）。具体的には、攻撃チェック結果リスト１５３０に含まれる行のうち、攻撃チェック判定部１５１０から受け取ったデータの組に対応する行のチェック結果を、受けとったチェック結果で更新する。

[0150] 次にシステムコール管理部１５０１は、攻撃チェックの結果を判定する（Ｓ１００９）。具体的には、ステップＳ１００６における攻撃チェックの結果、アプリが攻撃されていなければ、ステップＳ１００９において「ＯＫ」と判定し、アプリが攻撃されていれば「ＮＧ」と判定する。

[0151] システムコール管理部１５０１は、ステップＳ１００９で「ＯＫ」と判定した場合には、アプリに要求されたシステムコールの処理を実行する（Ｓ１０１０）。また、システムコール管理部１５０１は、システムコール処理の終了後、システムコール処理の結果を表示アプリ１１０３へ返す。

[0152] 一方、システムコール管理部１５０１は、ステップＳ１００９で「ＮＧ」と判定した場合、表示アプリ１１０３へエラーを返す。

[0153] 本発明の実施の形態１においては、システムコール処理時に、上記に示したチェック要否判定処理を情報処理装置１００が実施することにより、アプリが攻撃されているか否かについて、不要な攻撃チェック処理を省くことが

可能となる。したがって、本実施の形態に係る情報処理装置１００は、システムコール要求時のＯＳ１１０１による処理を高速化することが可能となる。

[0154] ＜ファイル読み込み処理＞

次に、ファイル読み込みを伴うシステムコールが要求された場合における、ファイル読み込み管理部１５０２が行う処理について説明する。

[0155] ファイル読み込み管理部１５０２は、ファイルの読み込み処理前に、（１）そのファイルを読み込んでもよいかの判定と、（２）ファイル読み込み処理後のシステムコール処理で攻撃チェック処理を実施する必要があるかの判定（すなわち、チェック要否判定処理）とを行う。チェック要否判定処理では、ファイル読み込み処理でチェックする必要があると判定された時にのみ、チェック処理を実施する。これにより、不正なファイルの読み込みを防止でき、攻撃者による攻撃の拡大を防止できる。また、チェックが必要な場合のみチェック処理を実行するように指示できるため、チェック処理が省略でき、システムコール要求時のＯＳ１１０１による処理を高速化できる。

[0156] 以下、表示アプリ１１０３がＯＳ１１０１へファイルの読み込みを依頼した時の、ファイル読み込み処理を、図１１のフローチャートを用いて説明する。

[0157] 表示アプリ１１０３は、システムコール管理部１５０１へファイルの読み込みを依頼する（Ｓ１１００）。

[0158] システムコール管理部１５０１が備える攻撃チェック判定部１５１０は、図１０で示されるチェック要否判定処理により、表示アプリ１１０３が攻撃されているかチェックする必要があるか否かの判定を行う（Ｓ１１０１）。チェック要否判定処理において、システムコールの処理を行うと判定された場合（図１０のＳ１００９で「ＯＫ」）、システムコール管理部１５０１は、ファイルの読み込み処理をファイル読み込み管理部１５０２へ要求する（Ｓ１１０２）。

[0159] ファイル読み込み管理部１５０２は、コンテンツ特定部１５２１を利用し

て、読み込みが要求されているコンテンツの識別子であるコンテンツ識別子を取得する（Ｓ１１０３）。コンテンツ特定部１５２１は、読み込み要求時に通知されるファイル識別子に格納されている写真データのファイル名を取得し、このファイル名をコンテンツ識別子とする。

[0160] また、ファイル読み込み管理部１５０２は、アプリ特定部１５２２を利用して、読み込みを要求したアプリのアプリ識別子を取得する（Ｓ１１０４）。アプリ特定部１５２２は、ＯＳ１１０１が管理するプロセス管理用の構造体に格納されているアプリのファイル名を取得し、このファイル名をアプリ識別子とする。

[0161] さらに、ファイル読み込み管理部１５０２は、呼び出し元特定部１５２３を利用して、ファイル読み込み要求を呼び出した呼び出し元を識別するためのデータを取得する（Ｓ１１０５）。本発明の実施の形態１においては、アプリが写真データの読み込み要求をした時のアプリの実行コードのアドレス（リターンアドレス）と、スタックポインタの値を取得し、呼び出し元を識別するためのデータとする。

[0162] 次に、ファイル読み込み管理部１５０２は、チェックアプリ管理部１５００へ、攻撃チェック結果リスト１５３０から攻撃チェック結果を取得するよう、依頼を行う（Ｓ１１０６）。この時、ファイル読み込み管理部１５０２は、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値とをチェックアプリ管理部１５００へ通知する。

[0163] チェックアプリ管理部１５００は、ファイル読み込み管理部１５０２から受け取ったアプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値との全てに該当するチェック結果が攻撃チェック結果リスト１５３０に存在するか確認する。チェックアプリ管理部１５００は、存在する場合には、その結果を取得する（Ｓ１１０７）。その後、チェックアプリ管理部１５００は、取得したチェック結果をファイル読み込み管理部１５０２へ返す。なお、チェック結果が存在しない場合は、存在しない旨を示す情報を通知する（Ｓ１１０８）。

[0164] 次に、ファイル読み込み管理部１５０２は、チェックアプリ管理部１５００から受け取ったチェック結果を用いて、ファイルを読み込んでもよいか否かを判定する（Ｓ１１０９）。ファイル読み込み管理部１５０２は、受けとったチェック結果が“○”、又はチェック結果が存在しない旨を示す情報であった場合は、「可」と判定する。一方、受け取ったチェック結果が“×”であった場合は、「否」と判定する。

[0165] ファイル読み込み管理部１５０２は、ステップＳ１１０９で「可」と判定した場合には、ファイル読み込み要求を行ったアプリが攻撃されているかどうかをチェックする必要があるか否かを判定する（Ｓ１１１０）。具体的には、ファイル読み込み管理部１５０２は、ステップＳ１１０８で受けとったチェック結果が、チェック結果が存在しない旨を示す情報であった場合は、ステップＳ１１１０で「要」と判定する。また、受けとったチェック結果が“○”であった場合は、ステップＳ１１１０で「否」と判定する。

[0166] 次に、ファイル読み込み管理部１５０２は、ステップＳ１１１０で「要」と判定した場合には、チェックアプリ管理部１５００へアプリの攻撃チェックが必要である旨の登録を依頼する（Ｓ１１１１）。この時、ファイル読み込み管理部１５０２は、アプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値とをチェックアプリ管理部１５００へ通知する。

[0167] チェックアプリ管理部１５００は、ファイル読み込み管理部１５０２から受け取ったアプリ識別子と、コンテンツ識別子と、呼び出し元アドレスと、スタックポインタ値とを攻撃チェック結果リスト１５３０へ追加する。さらに、対応するチェック結果を“要”に設定する（Ｓ１１１２）。

[0168] また、ファイル読み込み管理部１５０２は、ステップＳ１１１０で「否」と判定した場合、及びステップＳ１１１２の処理後に、ファイルの読み込み処理を行う（Ｓ１１１３）。

[0169] なお、攻撃チェック結果リスト１５３０、コンテンツＡ１２２２、及び、コンテンツＢ１２２３（いずれも、図３を参照）は不揮発性記憶装置１２２

０に格納されるとしたが、これに限定されるものではない。例えば、システムＬＳＩ内部の保護されたメモリ（図示しない）や、耐タンパー化された不揮発性記憶装置（図示しない）に格納されてもよい。また、コンテンツＡ１２２２とコンテンツＢ１２２３は、コンテンツ収集アプリ１１０２により収集された直後は不揮発性記憶装置１２２０（図３を参照）へ格納され、攻撃チェック部１５１２によりチェックされた後、保護されたメモリや耐タンパー化された不揮発性記憶装置へ格納されるとしてもよい。

[0170] また、管理アプリ１１０５（図２を参照）により、アプリを更新／削除した場合、チェックアプリ管理部１５００は、更新／削除されたアプリのアプリ識別子に対応するチェック結果を攻撃チェック結果リスト１５３０から削除してもよい。これにより、アプリを最新のものに更新することによりバッファーオーバーフローの脆弱性が修正された場合には、読み込み処理を行えるようになる。また、アプリを削除した時、同じアプリ識別子を持つアプリが再度インストールされた場合に、再度攻撃チェック処理を実施できる。

[0171] さらに、編集アプリ１１０４により、写真データを更新／削除した場合、チェックアプリ管理部１５００は、更新／削除した写真データのコンテンツ識別子に関するチェック結果を攻撃チェック結果リスト１５３０から削除してもよい。これにより、写真データが不正なプログラムを付加したコンテンツに更新されてしまった場合に、それを検知可能となる。逆に、不正なプログラムを付加したコンテンツから通常の写真データへ更新された場合に、写真を表示できるようになる。

[0172] 以上述べたように、再度図９を参照して、本実施の形態に係る情報処理装置１００Ａは、一意な識別子であるアプリ識別子を有する１以上のプログラムを実行する。

[0173] また、情報処理装置１００Ａは、アプリ識別子を取得することによりアプリ（すなわち、情報処理装置１００Ａにおいて実行中のプログラム）を特定するアプリ特定部１５１１と、特定されたアプリが、システムコール等の関数（すなわち、プログラムコード）を呼び出す時に、アプリの中のどの部分

（すなわち、プログラム中のどの部分）から関数を呼び出したかを示す呼び出し元を特定する呼び出し元特定部１５２３と、特定されたプログラムを実行することに対する安全性について過去にチェックした結果を含む情報であるチェック結果を管理するチェックアプリ管理部１５００と、特定された呼び出し元とチェック結果とに基づいて、特定されたアプリ（プログラム）が攻撃されているかチェックを行うか否かを判定する攻撃チェック判定部１５１０とを備える。

[0174] また、コンテンツ蓄積・表示装置１００１は、さらに、特定されたアプリが攻撃されているかをチェックする攻撃チェック部１５１２を備えており、攻撃チェック部は、攻撃チェック判定部１５１０が、特定されたアプリに対して攻撃チェックを行うと判定した場合には、特定されたアプリが攻撃されているか否かをチェックする。

[0175] また、呼び出し元特定部１５２３は、特定されたアプリから関数を呼び出した後に特定されたアプリへ実行処理を戻すための戻し先を示すメモリ内のアドレスであるリターンアドレスを用いて呼び出し元を特定する。

[0176] また、呼び出し元特定部１５２３は、特定されたアプリから関数を呼び出した場合に特定されたアプリが使用するコールスタックのスタックポインタの値と、リターンアドレスとを用いて呼び出し元を特定してもよい。

[0177] また、チェックアプリ管理部１５００は、（Ａ）特定されたプログラムが攻撃されているか否かをチェックした結果を示す情報、及び、（Ｂ）特定されたプログラムが、攻撃されているか否かを判定するチェックが必要であるかを示す情報、の両方を含む情報をチェック結果として、特定されたプログラムが有するアプリ識別子と呼び出し元とに対応付けて記憶してもよい。

[0178] この場合、攻撃チェック判定部１５１０は、アプリ識別子と、呼び出し元とに対応付けられた情報であって、アプリ識別子で特定されるアプリが攻撃されているかチェックを行う必要があることを示す情報が、チェックアプリ管理部１５００に記憶されている場合には、チェックを行うと判定し、記憶されていない場合には、チェックを行わないと判定する。

[0179] すなわち、攻撃チェック判定部１５１０は、特定されたプログラムが有するアプリ識別子に対応付けられてチェックアプリ管理部１５００に記憶されているチェック結果を取得し、（Ａ）取得したチェック結果が、特定されたプログラムが攻撃されていないこと、又は、特定されたプログラムが攻撃されていることを表す場合には、攻撃されているかのチェックを行わないと判定し、（Ｂ）取得したチェック結果が、攻撃されているか否かを判定するチェックが必要であることを表す場合には、攻撃チェック部による攻撃されているかのチェックを行うと判定してもよい。

[0180] また、さらに、特定されたアプリが関数を呼び出すことにより読み込もうとしているデータファイルを、データファイルを示す識別子であるコンテンツ識別子を用いて特定するコンテンツ特定部１５２１と、特定されたデータファイルを読み込むか否かを判定する読み込み可否判定部１５２０とを備えてもよい。

[0181] ここで、読み込み可否判定部１５２０は、（Ａ）コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられたチェック結果が、チェックアプリ管理部１５００に記憶されていないか、又は（Ｂ）コンテンツ識別子と、アプリ識別子と、前記呼び出し元とに対応付けられたチェック結果が、チェックアプリ管理部１５００記憶されており、かつ、そのチェック結果が特定されたアプリが攻撃されていないことを示す場合には、特定されたデータファイルを読み込むと判定し、（Ｃ）コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられているチェック結果が、チェックアプリ管理部１５００に記憶されており、かつ、そのチェック結果が、特定されたアプリが以前に攻撃されたことを示す場合には、特定されたデータファイルを読み込まないと判定してもよい。

[0182] より詳細には、読み込み可否判定部１５２０は、コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けられたチェック結果が、チェックアプリ管理部１５００に記憶されていない場合には、アプリ識別子で特定されるアプリが、攻撃されているか否かを判定するチェックが必要であることを

示す情報を、コンテンツ識別子と、アプリ識別子と、呼び出し元とに対応付けてチェックアプリ管理部１５００に記憶させてもよい。

[0183] また、チェックアプリ管理部１５００は、アプリが削除又は更新された場合には、攻撃チェック結果リスト１５３５として記憶しているチェック結果のうち、削除又は更新されたアプリが有するアプリ識別子に対応づけられて記憶されているチェック結果の記録を削除してもよい。

[0184] また、チェックアプリ管理部１５００は、特定されたデータファイルが変更された場合には、変更されたデータファイルを示すコンテンツ識別子に対応づけられて記憶されているチェック結果を削除してもよい。

[0185] 以上説明したように、本発明の実施の形態１によれば、１度、安全性（攻撃されていないこと）が確認されたアプリからのシステムコールを処理する際は、攻撃チェック処理を省くことができる。さらに、システムコール内でファイルの読み込みが発生する際には、以前に攻撃されたファイルの読み込みを中止することができる。その結果、安全性を維持したまま、システムコール処理の応答性を向上させることが可能となる。

[0186] （実施の形態２）

本発明の実施の形態１では、ファイル読み込み管理部１５０２でアプリのチェックを実施するかを判定し、その判定結果に基づいてシステムコール管理部１５０１が攻撃チェック処理を行った。実施の形態２では、システムコール管理部１５０１がアプリのチェック実施の判定と、攻撃チェック処理を行う構成について説明する。

[0187] 以下、本発明の実施の形態２に係るシステムコール管理部１５０１の構成と、攻撃チェック結果リスト１５３５と、チェック要否判定処理とを説明する。なお、本発明の実施の形態１と同じ構成要素、同じ処理については、同じ符号を用い、説明を省略する。

[0188] ＜情報処理装置１００Ｂの構成＞

図１２は、本発明の実施の形態２に係る情報処理装置１００Ｂの構成図である。

[0189] 図１２において、システムコール管理部１５０１Ａは、攻撃チェック判定部１５１０と、アプリ特定部１５１１と、攻撃チェック部１５１２と、呼び出し元特定部１５２３とを含む。

[0190] 攻撃チェック判定部１５１０は、システムコールを要求したアプリに対して、攻撃されているかどうかをチェックする必要があるかを判定する。攻撃チェック判定部１５１０は、アプリ特定部１５１１からアプリ識別子を取得し、呼び出し元特定部１５２３から呼び出し元アドレスとスタックポインタ値とを取得する。攻撃チェック判定部１５１０は、チェックアプリ管理部１５００を介して、後述する攻撃チェック結果リストに、指定したアプリ識別子、呼び出し元アドレス及びスタックポインタの値と一致するデータがあるか確認する。攻撃チェック判定部１５１０は、一致するデータがない場合には、攻撃チェック部１５１２を利用して攻撃チェックを行う。一方、一致するデータがあった場合には、攻撃チェックを行わない。

[0191] 図１３は、攻撃チェック結果リスト１５３５の一例を示している。この攻撃チェック結果リスト１５３５は、アプリ識別子と、呼び出し元アドレスと、スタックポインタ値と、チェック結果とを含む。チェック結果は、本発明の実施の形態１の攻撃チェック結果リスト１５３０及び攻撃チェック結果リスト１５３５とは異なり、攻撃されたかどうかのチェック結果を示す“○”又は“×”のみを格納している。

[0192] なお、アプリ特定部１５１１と、攻撃チェック部１５１２と、呼び出し元特定部１５２３とに関しては、本発明の実施の形態１と同じである。

[0193] ＜チェック要否判定処理＞

本発明の実施の形態２に係るチェック要否判定処理は、本発明の実施の形態１に係るチェック要否判定処理（図１０、図１１）と一部は同じ処理となる。処理の異なる部分を中心に説明する。

[0194] 図１４を参照して、本発明の実施の形態２に係るシステムコール管理部１５０１Ａは、ステップＳ１２０４における攻撃チェック結果の取得処理において、アプリ識別子と、呼び出し元アドレスと、スタックポインタ値とを指

定して、チェックアプリ管理部１５００から攻撃チェック結果を取得する。この時、チェックアプリ管理部１５００は、指定されたアプリ識別子と、呼び出し元アドレスと、スタックポインタ値とを含む行が、攻撃チェック結果リスト１５３５に含まれている場合には、該当する行のチェック結果（“○”又は“×”）を返す。また、チェックアプリ管理部１５００は、指定されたアプリ識別子等の組み合わせに一致する行が攻撃チェック結果リスト１５３５に存在しなかった場合には、チェック結果として、“○”又は“×”に代わり、チェック結果が存在しないことを示す情報を返す。

[0195] その後、チェックアプリ管理部１５００は、ステップＳ１２０６におけるチェック要否判定において、受け取ったチェック結果が、チェック結果が存在しないことを示す情報であった場合には「要」と判定する。また、“○”であった場合には「否」と判定する。また、“×”であった場合には、「ＮＧ」と判定する。

[0196] 次に、システムコール管理部１５０１Ａは、ステップＳ１２０６で「要」と判定された場合には、攻撃チェック処理（Ｓ１００６）と、その結果の登録処理（Ｓ１１０８）を行う。さらに、チェック結果の判定処理（Ｓ１００９）を行う。

[0197] また、システムコール管理部１５０１Ａは、ステップＳ１２０６で「否」と判定された場合には、続けて、チェック結果の判定処理（Ｓ１００９）を行う。

[0198] また、システムコール管理部１５０１Ａは、ステップＳ１２０６で「ＮＧ」と判定された場合には、呼び出した表示アプリ１１０３に対してエラーを返す。

[0199] 以上説明したように、本発明の実施の形態２によれば、アプリからのシステムコール要求時に、チェック要否判定処理を行うことにより、システムコール処理の応答性を向上させることが可能となる。

[0200] （実施の形態３）

本発明の実施の形態３に係る情報処理装置は、本発明の実施の形態２に係

る情報処理装置１００Ｂのように攻撃チェック結果リスト１５３０を自機器内で生成及び管理せず、他の機器から攻撃チェック結果リスト１５３０を取得する。

[0201] 以下、本発明の実施の形態３に係る情報処理装置１００Ｃについて詳細に説明する。なお、本発明の実施の形態２に係る情報処理装置１００Ｂと同じ構成要素、同じ処理については、同じ符号を用い、説明を省略する。

[0202] ＜コンテンツ蓄積・表示システム１０００Ａの構成＞

図１５は、本発明の実施の形態３におけるコンテンツ蓄積・表示システム１０００Ａの構成図である。

[0203] 図１５において、コンテンツ蓄積・表示システム１０００Ａは、コンテンツ蓄積・表示装置１００１Ａ、１００２Ａと、カメラ１０１０と、ＰＣ１０１１と、更新サーバ１０２０とを含む。

[0204] コンテンツ蓄積・表示装置１００１Ａは、コンテンツ蓄積・表示装置１００２Ａとネットワークを介して接続される。

[0205] コンテンツ蓄積・表示装置１００１Ａとコンテンツ蓄積・表示装置１００２Ａとで写真データを共有するために、コンテンツ蓄積・表示装置１００１Ａは、自機器内に蓄積する写真データをコンテンツ蓄積・表示装置１００２Ａへ送信する。この時、コンテンツ蓄積・表示装置１００１Ａは、写真データと一緒に、攻撃チェック結果リスト１５３５を送信する。

[0206] コンテンツ蓄積・表示装置１００２Ａは、コンテンツ蓄積・表示装置１００１Ａとネットワークを介して接続される。コンテンツ蓄積・表示装置１００２Ａは、コンテンツ蓄積・表示装置１００１Ａから受信した写真データを表示する時には、コンテンツ蓄積・表示装置１００１Ａから受信した攻撃チェック結果リスト１５３５を参照し、チェック結果が“○”の写真データのみを表示する。

[0207] コンテンツ蓄積・表示装置１００１Ａとコンテンツ蓄積・表示装置１００２Ａとは、上記以外の機能は本発明の実施の形態１に係るコンテンツ蓄積・表示装置１００１と同じである。

[0208] なお、コンテンツ蓄積・表示装置１００１Ａ、１００２Ａと、カメラ１０１０と、ＰＣ１０１１と、更新サーバ１０２０とに関しては、本発明の実施の形態１及び２と同じである。

[0209] ＜情報処理装置１００Ｃの構成＞

図１６は、本発明の実施の形態３に係るコンテンツ蓄積・表示装置１００１Ａ、及びコンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃの構成図である。

[0210] 図１６において、コンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃは、攻撃チェック判定部１５１０と、アプリ特定部１５１１と、呼び出し元特定部１５２３とを有する。また、コンテンツ蓄積・表示装置１００１Ａが備える情報処理装置１００Ｄは、チェックアプリ管理部１５００Ａと、攻撃チェック結果リスト１５３５とを有する。

[0211] なお、コンテンツ蓄積・表示装置１００１Ａ、及びコンテンツ蓄積・表示装置１００２Ａの各構成要素のうち、実施の形態２と同様の構成要素については詳細な説明は省略する。

[0212] 攻撃チェック判定部１５１０は、システムコールを要求したアプリに対して、攻撃されているかどうかをチェックする必要があるかを判定する。攻撃チェック判定部１５１０は、アプリ特定部１５１１からアプリ識別子を取得し、呼び出し元特定部１５２３から呼び出し元アドレスとスタックポインタ値とを取得する。攻撃チェック判定部１５１０は、チェックアプリ管理部１５００を介して、チェックアプリ管理部１５００Ａが有している攻撃チェック結果リスト１５３５を取得する。その後、取得した攻撃チェック結果リスト１５３５の中に、アプリ識別子と、呼び出し元アドレスと、スタックポインタ値との全てが一致するデータ（行）があるか確認する。

[0213] 一致するデータがあった場合、一致するデータのチェック結果が“○”の場合は、システムコール処理を実施し、“×”の場合は、システムコール処理を実施しない。

[0214] すなわち、本発明の実施の形態３に係る情報処理装置１００Ｃが有するチ

ェックアプリ管理部１５００は、チェック結果を、当該チェックアプリ管理部１５００を有する情報処理装置Ｃとは異なる情報処理装置１００Ｄに記憶していてもよい。また、チェックアプリ管理部１５００が、チェック結果を、当該チェックアプリ管理部１５００を備える情報処理装置１００Ｃ、及び、当該チェックアプリ管理部を備える情報処理装置１００Ｃとは異なる情報処理装置１００Ｄの少なくとも一方に記憶していてもよい。

[0215] なお、アプリ特定部１５１１と、呼び出し元特定部１５２３とが行う処理内容は、本発明の実施の形態２と同じである。

[0216] ＜チェック要否判定処理＞

本発明の実施の形態３に係るコンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃが行うチェック要否判定処理は、本発明の実施の形態２に係るチェック要否判定処理（図１４）と大部分は同じ処理となる。よって、図１７を参照して、処理の異なる部分を中心に説明する。なお、本実施の形態に係るコンテンツ蓄積・表示装置１００１Ａが備える情報処理装置１００Ｄの処理は、実施の形態２と同様であるため、説明を省略する。

[0217] 図１７を参照して、本実施の形態に係るコンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃは、攻撃チェック結果の取得処理において、アプリ識別子と、呼び出し元アドレスと、スタックポインタ値とを指定する。また、情報処理装置１００Ｃを介して、ネットワークで接続されている情報処理装置１００Ｄが有するチェックアプリ管理部１５００Ａから、指定したアプリ識別子等に一致するチェック結果を取得する（Ｓ１２０４）。

[0218] この時、コンテンツ蓄積・表示装置１００１Ａが備えるチェックアプリ管理部１５００Ａは、攻撃チェック結果リスト１５３５を参照する。その結果、チェック結果として、例えば“○”又は“×”を返す。また、チェックアプリ管理部１５００Ａは、指定されたアプリ識別子等の組み合わせに一致する行が攻撃チェック結果リスト１５３５に存在しなかった場合には、チェック結果として、“○”又は“×”に代わり、例えば、「チェック結果が存在しない」という結果を返す。

[0219] 攻撃チェック判定部１５１０は、その後のチェック結果判定処理において、受け取ったチェック結果が“○”であった場合には、ステップＳ１００９で「ＯＫ」と判定する。また、チェック結果が“×”又は「チェック結果が存在しない」であった場合には、ステップＳ１００９で「ＮＧ」と判定する（Ｓ１００９）。

[0220] 情報処理装置１００Ｃは、ステップＳ１００９で「ＯＫ」と判定された場合には、システムコール処理（Ｓ１０１０）を行う。一方、ステップＳ１００９で「ＮＧ」と判定された場合には、システムコールを呼び出したアプリに対してエラーを返す。

[0221] なお、本実施の形態に係るコンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃは攻撃チェック処理を行わなくてもよいが、これに限定されるものではない。例えば、コンテンツ蓄積・表示装置１００２Ａが独自に収集した写真データを読み込んだ場合には、本発明の実施の形態１や実施の形態２と同様に、コンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃが攻撃チェック処理を実施し、一方、コンテンツ蓄積・表示装置１００１Ａから受信した写真データに関しては、攻撃チェック処理を実施しないというように、組み合わせてもよい。

[0222] なお、本発明の実施の形態３では、コンテンツ蓄積・表示装置１００１Ａとコンテンツ蓄積・表示装置１００２Ａとの２台で写真データを共有する場合を説明したが、これに限定されるものではない。例えば、２台以上の任意の台数のコンテンツ蓄積・表示装置の間で、コンテンツ及び攻撃チェック結果リストを共有してもよい。より具体的には、コンテンツ蓄積・表示装置１００２Ａは、さらに、コンテンツ蓄積・表示装置１００１Ａ以外の第３のコンテンツ蓄積・表示装置とも写真データを共有してもよい。このとき、コンテンツ蓄積・表示装置１００２Ａは、コンテンツ蓄積・表示装置１００１Ａから取得した攻撃チェック結果リスト１５３５と、第３のコンテンツ蓄積・表示装置から取得した攻撃チェック結果リストとを結合し、１つの攻撃チェック結果リストとして利用・管理してもよい。

[0223] なお、コンテンツ蓄積・表示装置１００２Ａが備える情報処理装置１００Ｃは、必ずしも、ステップＳ１２０４において、システムコールの発行ごとに攻撃チェック結果リスト１５３５を取得しなくてもよい。例えば、コンテンツ蓄積・表示装置１００２Ａがコンテンツ蓄積・表示装置１００１Ａから写真等のコンテンツを受信するタイミングで、同時に、攻撃チェック結果リスト１５３５を取得しておいてもよい。

[0224] また、実施の形態１～３において、情報処理装置を有する装置の具体例として、コンテンツ蓄積・表示装置を用いて説明したが、本発明に係る情報処理装置が適用される対象は、コンテンツ蓄積・表示装置に限定されない。例えば、表示対象となるコンテンツを蓄積せず、外部のストレージから一時的に取得して表示を行う、コンテンツ表示装置に適用されてもよい。

[0225] 以上説明したように、本発明の実施の形態３によれば、コンテンツ蓄積・表示装置１００２Ａは、（Ａ）他の機器（例えば、コンテンツ蓄積・表示装置１００１Ａ）から写真データを受信する時に、攻撃チェック結果リスト１５３５を一緒に受信することにより、又は、（Ｂ）システムコールの発行ごとに、攻撃チェック結果リスト１５３５を他の機器（例えば、コンテンツ蓄積・表示装置１００１Ａ）から受信することにより、コンテンツ蓄積・表示装置１００２Ａ自身が攻撃チェック処理を行わなくてもよくなる。その結果、システムコール処理の応答性を大幅に向上させることが可能となる。

[0226] なお、本発明は、上記の実施の形態１～３に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

[0227] （１）上記実施の形態におけるコンテンツ識別子は、写真データファイルのファイル名としたが、これに限定されるものではない。例えば、ファイル名とファイルサイズの組み合わせとしてもよいし、写真データのハッシュ値としてもよいし、写真データに埋め込まれた識別子としてもよい。

[0228] また、写真データは、ファイルではなくデータベースのように複数の写真が１つのファイルに含まれてもよい。

[0229] （２）上記実施の形態１～３における「アプリが攻撃されている」とは、

アプリに存在するバッファーオーバーフローの脆弱性を衝かれて、アプリのスタック上で不正なプログラムが動作している状態であるとしたが、これに限定されるものではない。例えば、アプリのコード領域が改ざんされるとしてもよい。この場合、攻撃チェック処理としては、メモリ１２１０上のアプリのコード領域の改ざん検出処理を行う。

[0230] （３）上記実施の形態１～３における攻撃チェック処理は、リターンアドレスがスタック領域のアドレスではないかをチェックする処理としたが、これに限定されるものではない。例えば、「カナリア」と呼ばれる特殊な値をスタックのローカル変数領域とリターンアドレスの間に配置し、関数終了時に、「カナリア」の値をチェックしてもよい。

[0231] また、上記実施の形態３において、コンテンツ蓄積・表示装置１００２Ａが独自に収集した写真データを読み込んだ場合には、情報処理装置１００Ｃは、本発明の実施の形態１や実施の形態２と同様に、攻撃チェック処理を実施してもよいと説明した。また、その場合においても、コンテンツ蓄積・表示装置１００１Ａから受信した写真データに関しては、情報処理装置１００Ｃは、攻撃チェック処理を実施しないというように、組み合わせてもよいと説明した。この時、情報処理装置１００Ｃは、コンテンツ蓄積・表示装置１００２Ａが独自に収集した写真データを読み込む場合は「カナリア」値をチェックするアプリを用い、コンテンツ蓄積・表示装置１００１Ａから受信した写真データを読み込む場合は、「カナリア」値をチェックしないアプリを用いるとしてもよい。

[0232] （４）上記実施の形態１～３において、攻撃チェック処理は、システムコール要求時に、システムコール処理の前に実行するとしたが、これに限定されるものではない。例えば、システムコール処理と並行して処理してもよい。また、情報処理装置では、攻撃チェック処理の依頼のみを行い、実際の処理は、アプリが動作するバックグラウンドで行ってもよい。

[0233] （５）上記実施の形態１～３におけるチェック要否判定処理や、ファイル読み込み処理は、ユーザが写真データを選択した時等を契機に処理を開始す

るとしたが、これに限定されるものではない。例えば、スリープモードなどユーザが装置を使用していない時や、写真データを取り込んだ直後等に、写真データの読み込み処理をバックグラウンドで行うことにより、ユーザが写真を表示する前に攻撃チェック結果リスト１５３０、１５３５を作成してもよい。

[0234] （６）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせされて構成されたものである。

[0235] （７）上記の各装置を構成する構成要素の一部又は全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。ＲＡＭには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。

[0236] また、上記の各装置を構成する構成要素の各部は、個別に１チップ化されていてもよいし、一部又は全てを含むように１チップ化されてもよい。

[0237] また、ここでは、システムＬＳＩとしたが、集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧ

Ａ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

[0238] さらに、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

[0239] （８）上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしてもよい。前記ＩＣカード又は前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカード又は前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカード又は前記モジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパー性を有するとしてもよい。

[0240] （９）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0241] また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ（登録商標）　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

[0242] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

[0243] また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシス

テムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

[0244] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0245] （１０）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0246] 本発明は、情報の漏洩を防止できる情報処理装置等に適用できる。

符号の説明

[0247] １００、１００Ａ、１００Ｂ、１００Ｃ、１００Ｄ　情報処理装置
１０１　タスク
１０２　データ領域
１０３　システムコールテーブル
１０４　正当性検証部
１０５　システムコール
１０６　命令実行部
１０７、１１０１　ＯＳ
１１２　攻撃対策部
１０００、１０００Ａ　コンテンツ蓄積・表示システム
１００１、１００１Ａ、１００２Ａ　コンテンツ蓄積・表示装置
１０１０　カメラ
１０１１　ＰＣ
１０２０　更新サーバ
１０３０　記録ディスク
１１０２　コンテンツ収集アプリ

１１０３　表示アプリ

１１０４　編集アプリ

１１０５　管理アプリ

１２００　システムＬＳＩ

１２０１　ＣＰＵ

１２０２　カードＩ／Ｆ

１２０３　ネットワークＩ／Ｆ

１２０４　入出力Ｉ／Ｆ

１２１０　メモリ

１２２０　不揮発性記憶装置

１２２１　呼び出し元チェック結果表

１２２２　コンテンツＡ

１２２３　コンテンツＢ

１３００　更新処理受付部

１３０１　更新用ソフトウェア保持部

１５００、１５００Ａ　チェックアプリ管理部

１５０１、１５０１Ａ　システムコール管理部

１５０２　ファイル読み込み管理部

１５１０　攻撃チェック判定部

１５１１、１５２２　アプリ特定部

１５１２　攻撃チェック部

１５２０　読み込み可否判定部

１５２１　コンテンツ特定部

１５２３　呼び出し元特定部

１５３０、１５３５　攻撃チェック結果リスト

１５３１　要チェックアプリリスト

１５６０　ｍａｉｎ関数

１５６１　サムネイル取得関数

１５６２　データ本体取得関数

１５６３　ｒｅａｄ関数

請求の範囲

[請求項1] 一意な識別子であるアプリ識別子を有する１以上のプログラムを実行する情報処理装置であって、

前記アプリ識別子を取得することにより前記情報処理装置において実行中のプログラムを特定するアプリ特定部と、

前記特定されたプログラムが、プログラムコードの呼び出し時に、前記プログラムのどの部分から前記プログラムコードを呼び出したかを示す呼び出し元を特定する呼び出し元特定部と、

前記特定されたプログラムを実行することに対する安全性について過去にチェックした結果を含む情報であるチェック結果を管理するチェックアプリ管理部と、

前記特定された呼び出し元と前記チェック結果とに基づいて、前記特定されたプログラムが攻撃されているかのチェックを行うか否かを判定する攻撃チェック判定部とを備える

情報処理装置。

[請求項2] 前記情報処理装置は、さらに、

前記特定されたプログラムが攻撃されているかをチェックする攻撃チェック部を備えており、

前記攻撃チェック部は、前記攻撃チェック判定部が、前記特定されたプログラムに対して攻撃チェックを行うと判定した場合には、前記特定されたプログラムが攻撃されているか否かをチェックする

請求項１に記載の情報処理装置。

[請求項3] 前記呼び出し元特定部は、前記特定されたプログラムから前記プログラムコードを呼び出した後に前記特定されたプログラムへ実行処理を戻すための戻し先を示すメモリ内のアドレスであるリターンアドレスを用いて、前記呼び出し元を特定する

請求項２に記載の情報処理装置。

[請求項4] 前記呼び出し元特定部は、前記特定されたプログラムから前記プロ

グラムコードを呼び出した場合に前記特定されたプログラムが使用するコールスタックのスタックポインタの値と、前記リターンアドレスとを用いて前記呼び出し元を特定する

請求項３に記載の情報処理装置。

［請求項5］ 前記チェックアプリ管理部は、（Ａ）前記特定されたプログラムが攻撃されているか否かをチェックした結果を示す情報、及び、（Ｂ）前記特定されたプログラムが、攻撃されているか否かを判定するチェックが必要であるかを示す情報、の両方を含む情報を前記チェック結果として、前記特定されたプログラムが有する前記アプリ識別子と前記呼び出し元とに対応付けて記憶している

請求項３又は４に記載の情報処理装置。

［請求項6］ 前記攻撃チェック判定部は、前記特定されたプログラムが有するアプリ識別子に対応付けられて前記チェックアプリ管理部に記憶されている前記チェック結果を取得し、

（Ａ）取得した前記チェック結果が、前記特定されたプログラムが攻撃されていないこと、又は、前記特定されたプログラムが攻撃されていることを表す場合には、攻撃されているかのチェックを行わないと判定し、

（Ｂ）取得した前記チェック結果が、攻撃されているか否かを判定するチェックが必要であることを表す場合には、攻撃チェック部による攻撃がされているかのチェックを行うと判定する

請求項５に記載の情報処理装置。

［請求項7］ さらに、前記特定されたプログラムが前記プログラムコードを呼び出すことにより読み込もうとしているデータファイルを、前記データファイルを示す識別子であるコンテンツ識別子を用いて特定するコンテンツ特定部と、

前記特定されたデータファイルを読み込むか否かを判定する読み込み可否判定部とを備え、

前記読み込み可否判定部は、

（Ａ）前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられた前記チェック結果が、前記チェックアプリ管理部に記憶されていないか、又は、（Ｂ）前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられた前記チェック結果が、前記チェックアプリ管理部に記憶されており、かつ、前記チェック結果が、前記特定されたプログラムが攻撃されていないことを示す場合には、前記特定されたデータファイルを読み込むと判定し、

（Ｃ）前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられている前記チェック結果が、前記チェックアプリ管理部に記憶されており、かつ、前記チェック結果が、前記特定されたプログラムが以前に攻撃されたことを示す場合には、前記特定されたデータファイルを読み込まないと判定する

請求項５に記載の情報処理装置。

[請求項8] 前記読み込み可否判定部は、

前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けられた前記チェック結果が、前記チェックアプリ管理部に記憶されていない場合には、前記アプリ識別子で特定されるプログラムが、攻撃されているか否かを判定するチェックが必要であることを示す情報を、前記コンテンツ識別子と、前記アプリ識別子と、前記呼び出し元とに対応付けて前記チェックアプリ管理部に記憶させる

請求項７に記載の情報処理装置。

[請求項9] 前記チェックアプリ管理部は、前記プログラムが削除又は更新された場合には、削除又は更新された前記プログラムが有するアプリ識別子に対応づけられて記憶されているチェック結果を削除する

請求項５に記載の情報処理装置。

[請求項10] 前記チェックアプリ管理部は、前記チェック結果を、当該チェック

アプリ管理部を備える前記情報処理装置、及び、当該チェックアプリ管理部を備える前記情報処理装置とは異なる情報処理装置の少なくとも一方に記憶している

請求項１に記載の情報処理装置。

[請求項11] 前記チェックアプリ管理部は、前記特定されたデータファイルが変更された場合には、当該変更されたデータファイルを示すコンテンツ識別子に対応づけられて記憶されているチェック結果を削除する

請求項７に記載の情報処理装置。

[請求項12] 一意な識別子であるアプリ識別子を有する１以上のプログラムを実行する情報処理方法であって、

前記アプリ識別子を取得することにより前記情報処理方法によって実行中のプログラムを特定するアプリ特定ステップと、

前記特定されたプログラムが、プログラムコードの呼び出し時に、前記プログラムのどの部分から前記プログラムコードを呼び出したかを示す呼び出し元を特定する呼び出し元特定ステップと、

前記特定されたプログラムを実行することに対する安全性について過去にチェックした結果を含む情報であるチェック結果を管理するチェックアプリ管理ステップと、

前記特定された呼び出し元と前記チェック結果とに基づいて、前記特定されたプログラムが攻撃されているかのチェックを行うか否かを判定する攻撃チェック判定ステップとを含む

情報処理方法。

[請求項13] 請求項１２に記載の情報処理方法をコンピュータに実行させる

プログラム。

[請求項14] 請求項１３に記載のプログラムを記録した

コンピュータ読み取り可能な記録媒体。

[請求項15] 一意な識別子であるアプリ識別子を有する１以上のプログラムを実行する集積回路であって、

前記アプリ識別子を取得することにより前記集積回路において実行中のプログラムを特定するアプリ特定部と、

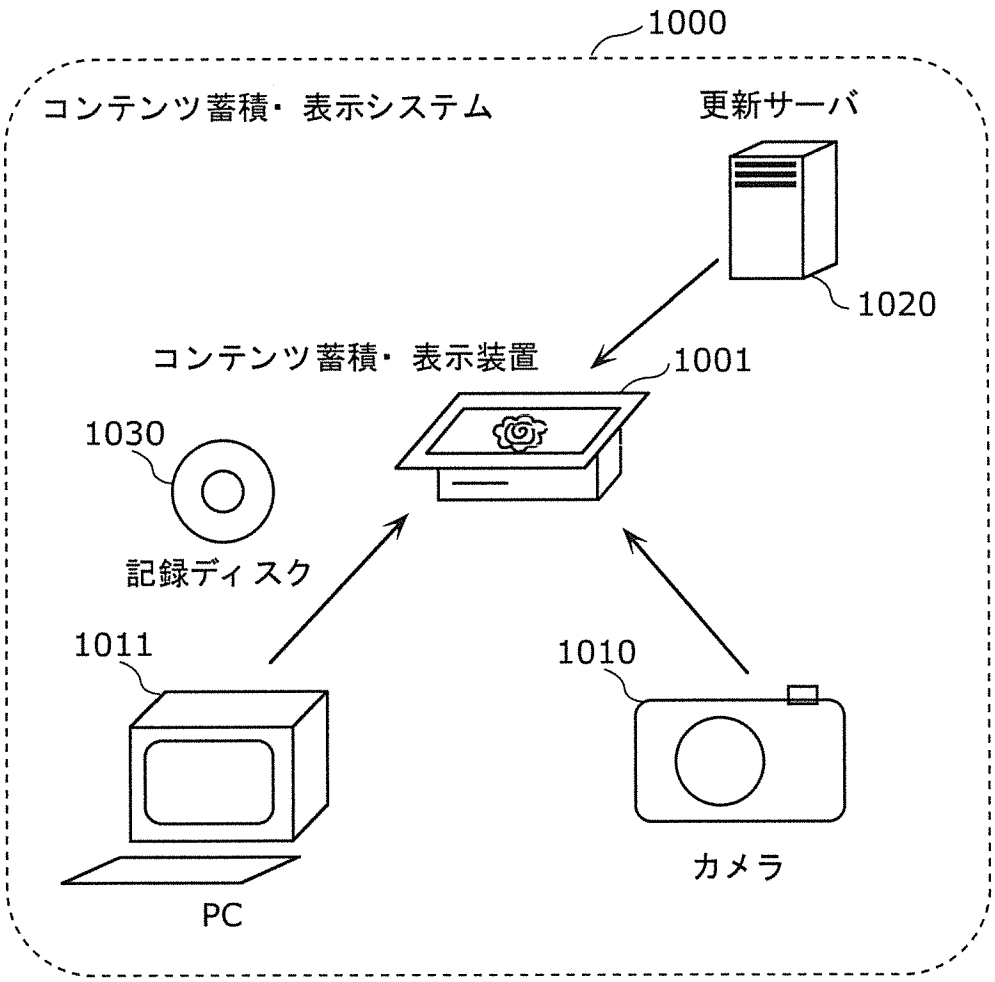
前記特定されたプログラムが、プログラムコードの呼び出し時に、前記プログラムのどの部分から前記プログラムコードを呼び出したかを示す呼び出し元を特定する呼び出し元特定部と、

前記特定されたプログラムを実行することに対する安全性について過去にチェックした結果を含む情報であるチェック結果を管理するチェックアプリ管理部と、

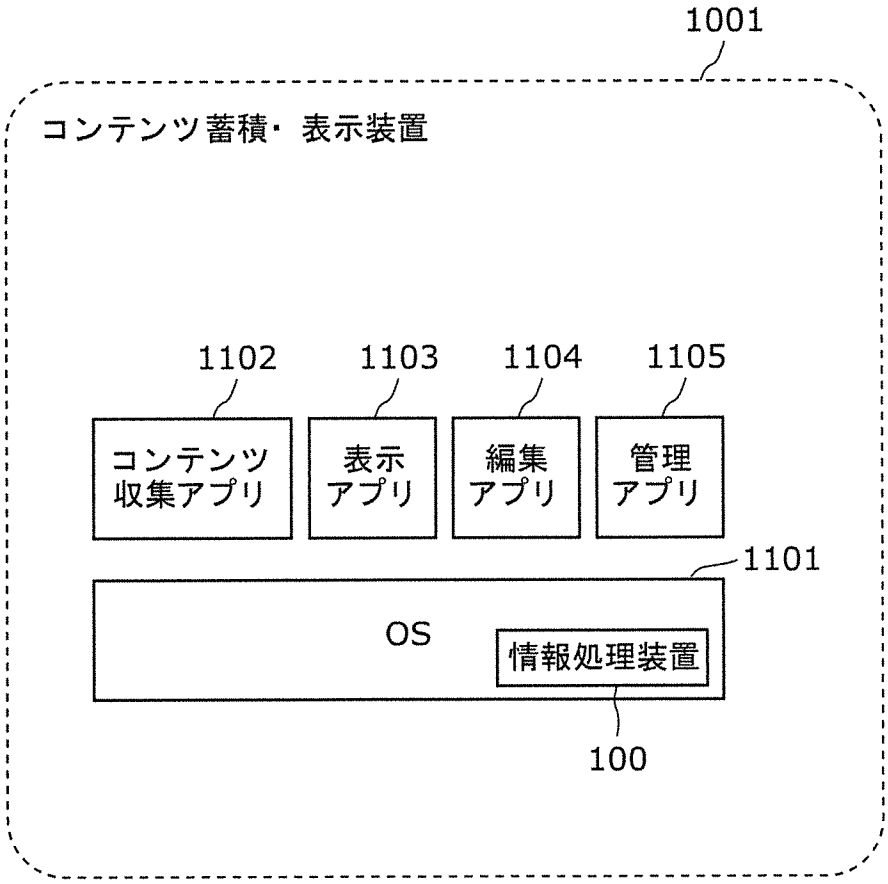
前記特定された呼び出し元と前記チェック結果とに基づいて、前記特定されたプログラムが攻撃されているかのチェックを行うか否かを判定する攻撃チェック判定部とを備える

集積回路。

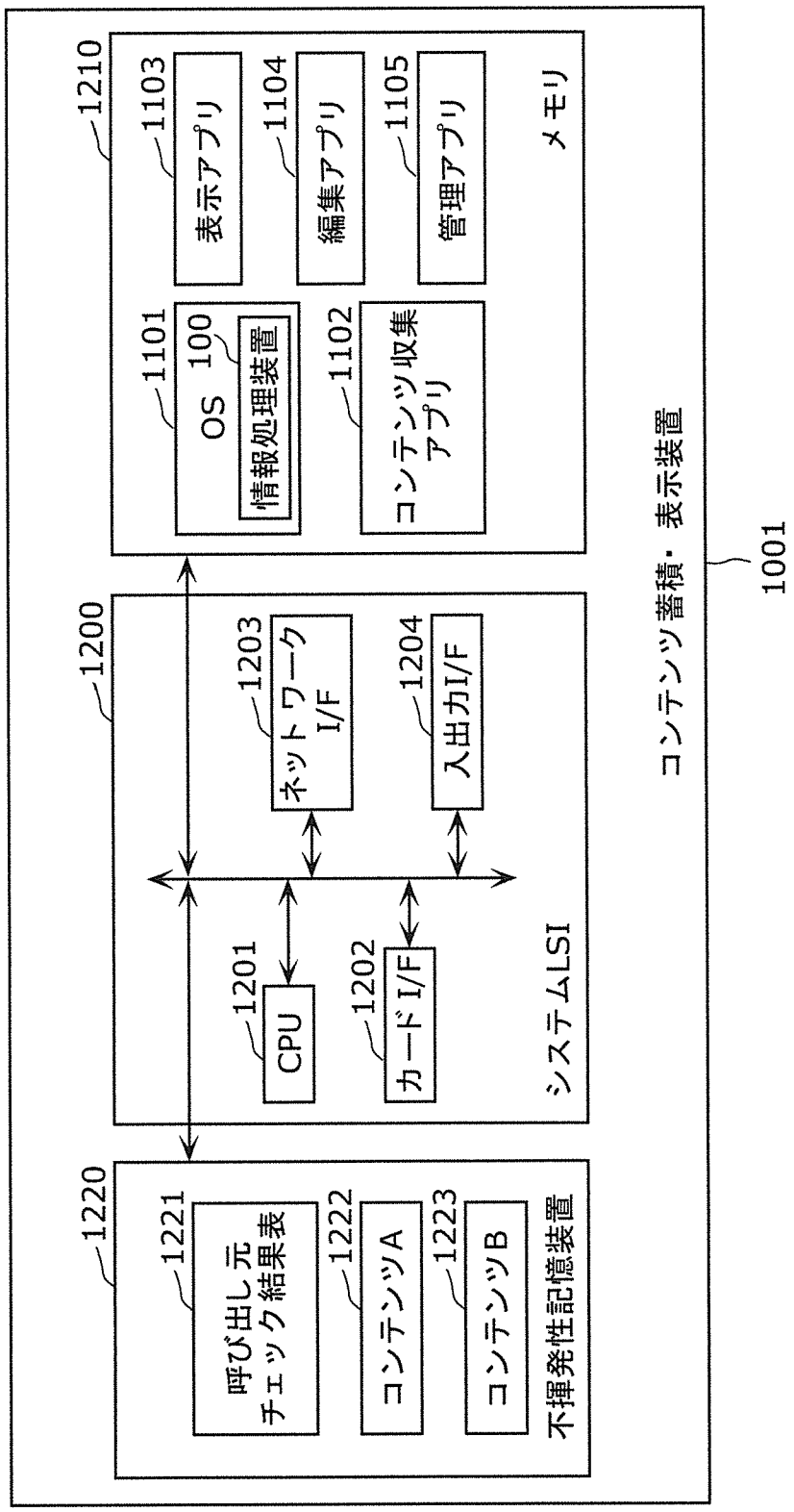
[図1]


1000
コンテンツ蓄積・表示システム
更新サーバ
1020
コンテンツ蓄積・表示装置
1001
1030
記録ディスク
1011
1010
PC
カメラ

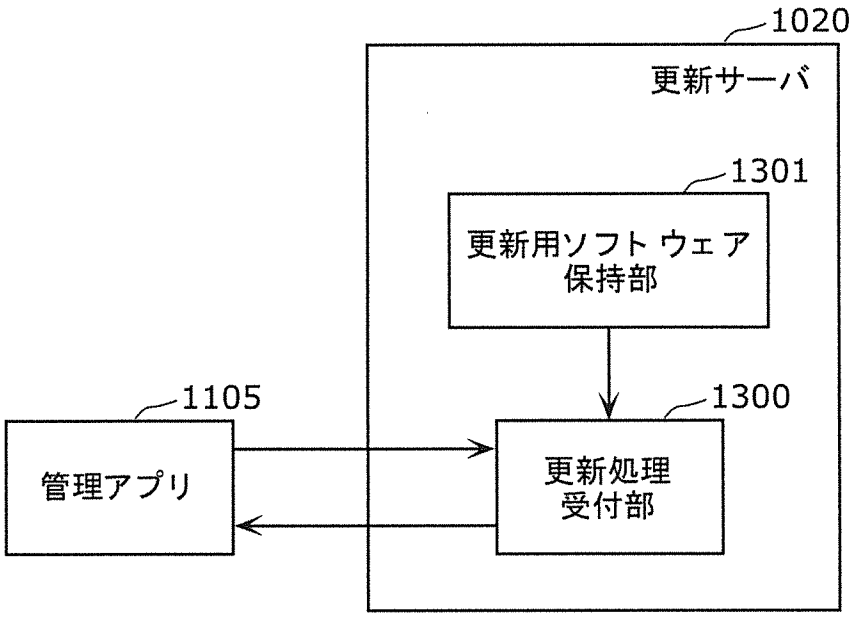
[図2]


1001
コンテンツ蓄積・表示装置
1102
1103
1104
1105
コンテンツ収集アプリ
表示アプリ
編集アプリ
管理アプリ
1101
OS
情報処理装置
100

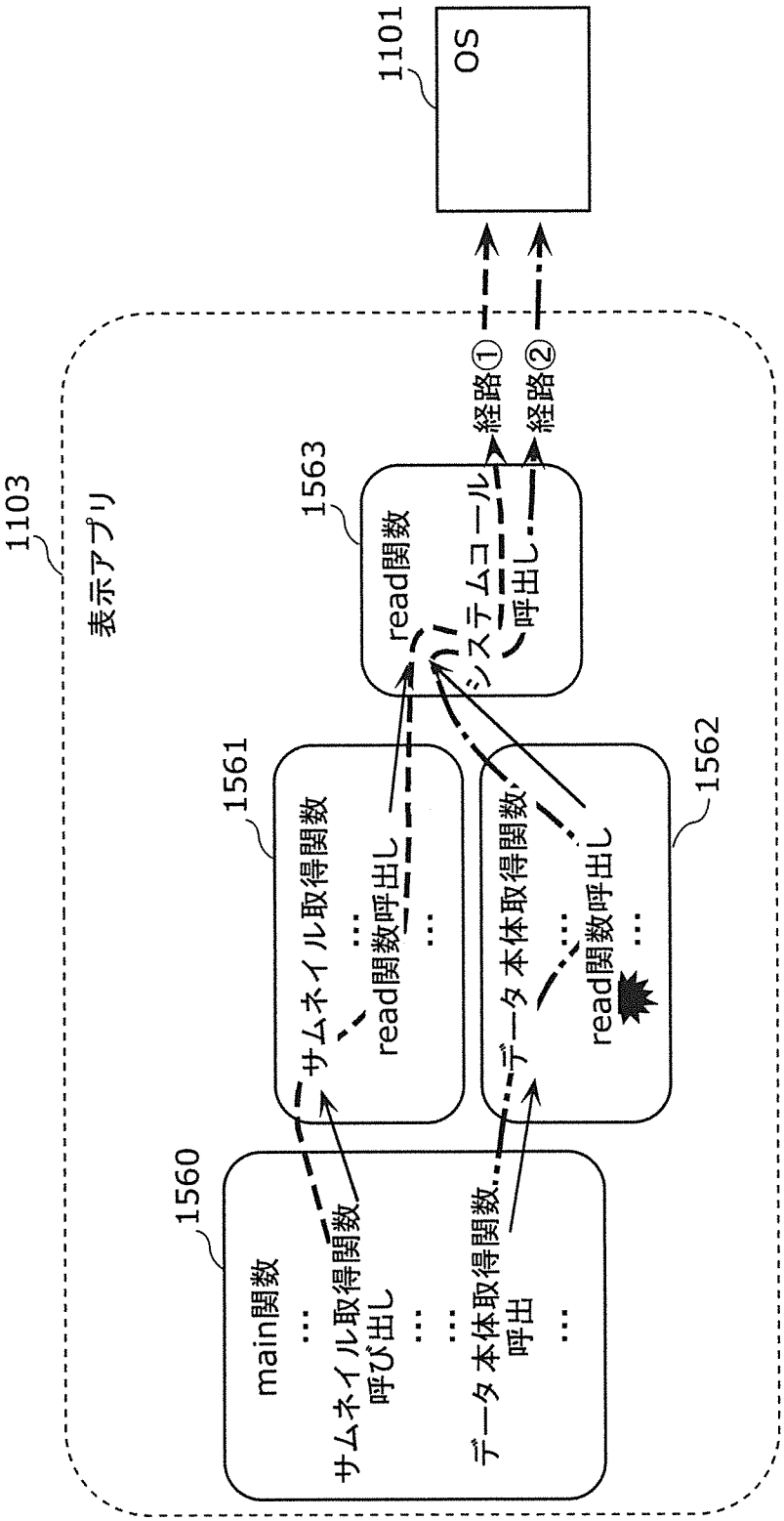
[図3]


コンテンツ蓄積・表示装置
1001
1210
メモリ
1103
表示アプリ
1104
編集アプリ
1105
管理アプリ
1101
OS
100
情報処理装置
1102
コンテンツ収集アプリ
1200
システムLSI
1201
CPU
1202
カードI/F
1203
ネットワークI/F
1204
入出力I/F
1220
不揮発性記憶装置
1221
呼び出し元チェック結果表
1222
コンテンツA
1223
コンテンツB

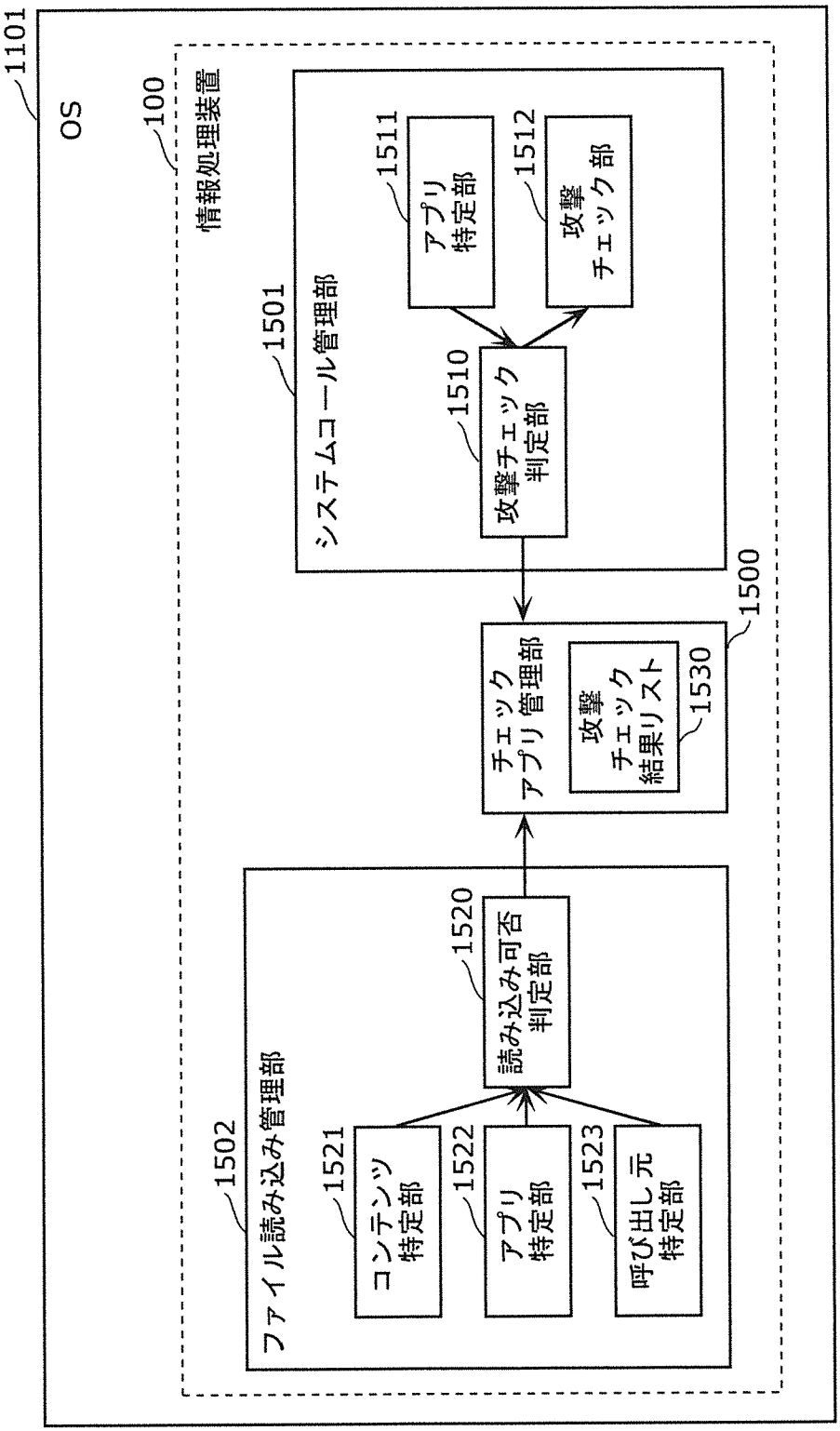
[図4]



[図5]


1101
OS
1103
表示アプリ
1563
read関数
システムコール
呼出し
経路①
経路②
1561
サムネイル取得関数
read関数呼出し
1562
データ本体取得関数
read関数呼出し
1560
main関数
サムネイル取得関数
呼び出し
データ本体取得関数
呼出

[図6]


1101
OS
100
情報処理装置
1501
システムコール管理部
1511
アプリ特定部
1512
攻撃チェック部
1510
攻撃チェック判定部
1500
チェックアプリ管理部
攻撃チェック結果リスト
1530
1502
ファイル読み込み管理部
1520
読み込み可否判定部
1521
コンテンツ特定部
1522
アプリ特定部
1523
呼び出し元特定部

[図7]

1530

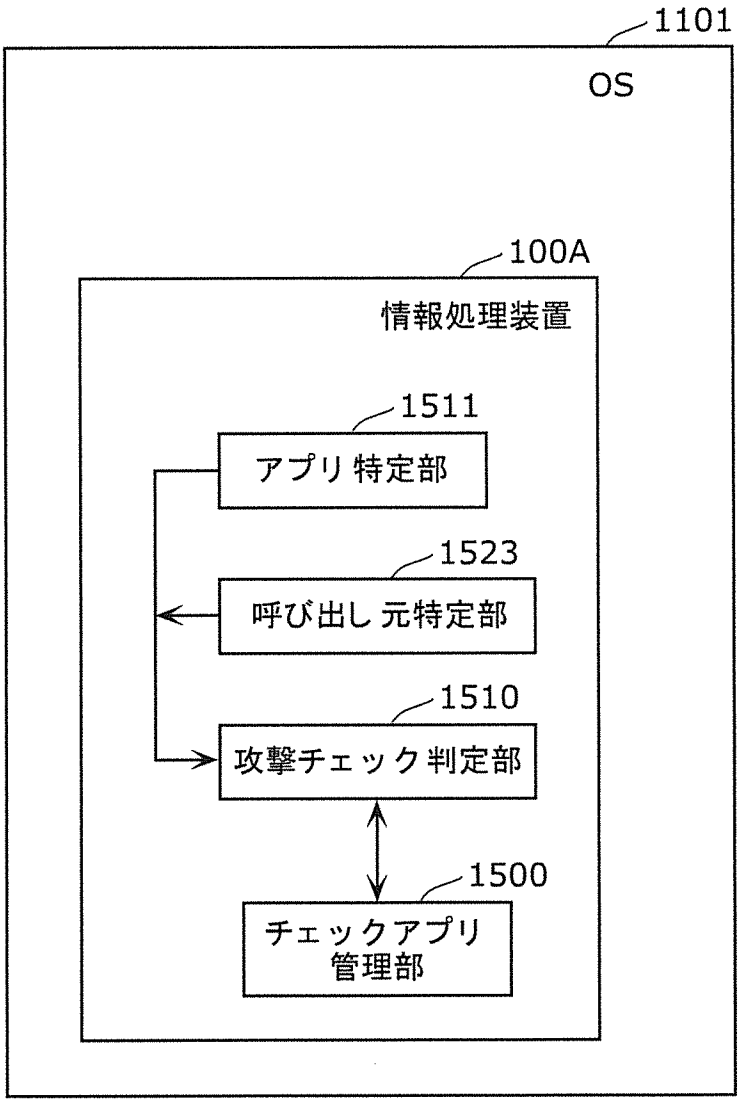
アプリ識別子	コンテンツ識別子	呼び出し元アドレス	スタックポインタ値	チェック結果
アプリA	コンテンツA	afe_0000	bff5_8000	○
アプリA	コンテンツA	afe_0000	bef5_0000	×
アプリA	コンテンツB	8cf0_0000	bff4_0000	要
アプリB	コンテンツA	0000_c000	bff4_c000	○
・・・	・・・	・・・	・・・	

[図8]

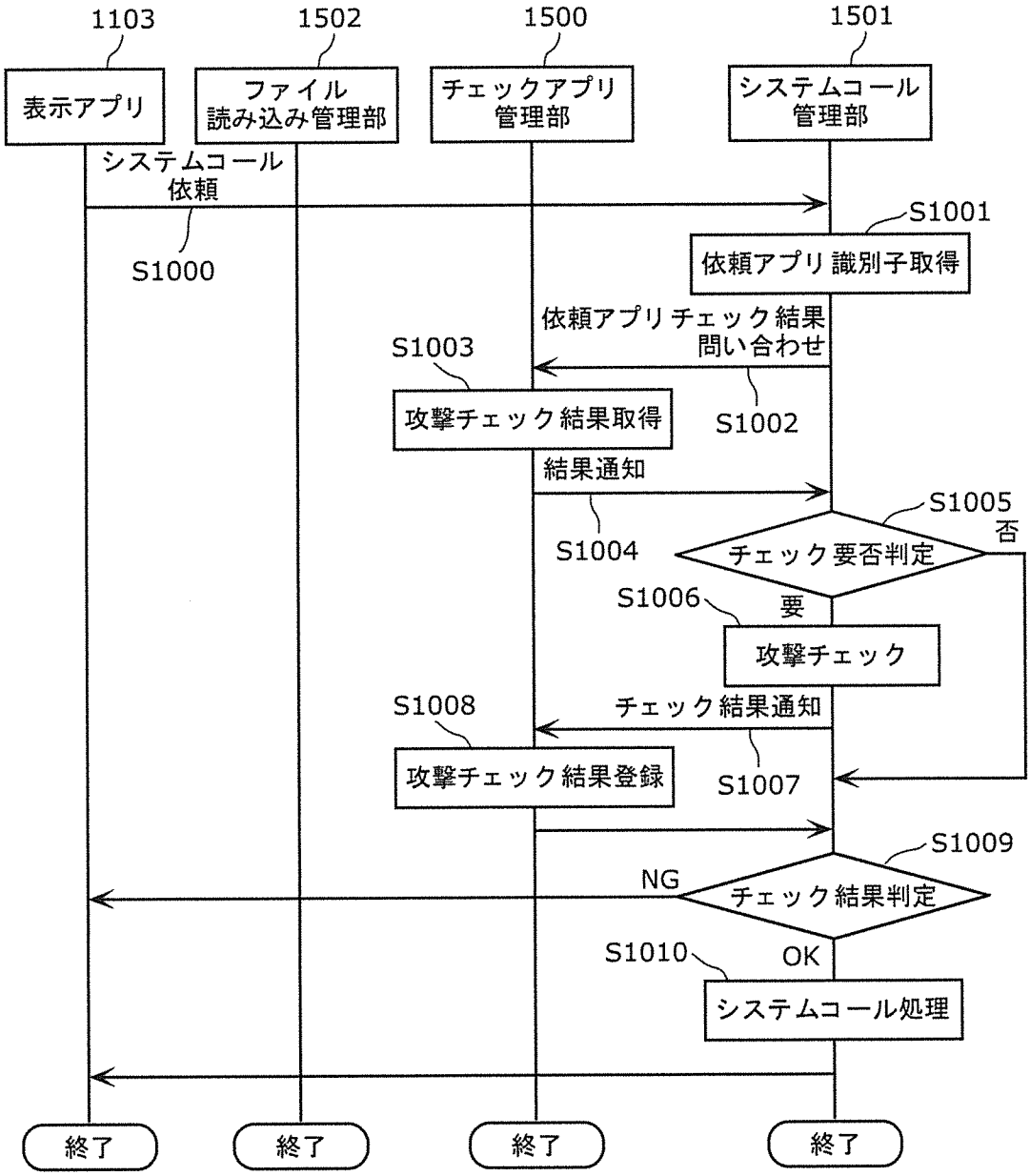
1531

アプリ識別子	コンテンツ識別子	呼び出し元アドレス	スタックポインタ値
アプリA	コンテンツA	afe_0000	bff5_8000
アプリB	コンテンツA	0000_0000	bff4_0000
・・・	・・・	・・・	・・・

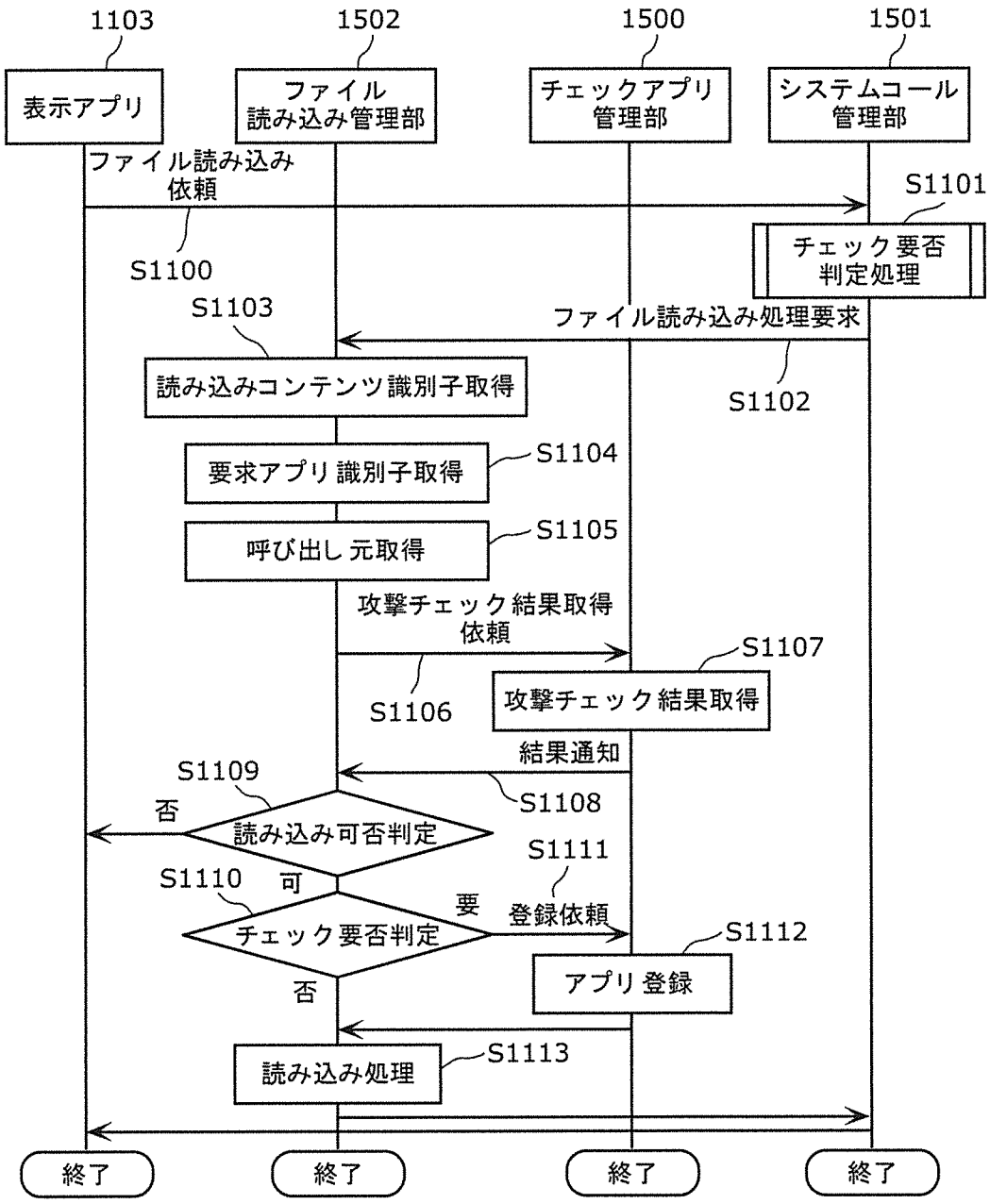
[図9]


1101
OS
100A
情報処理装置
1511
アプリ特定部
1523
呼び出し元特定部
1510
攻撃チェック判定部
1500
チェックアプリ管理部

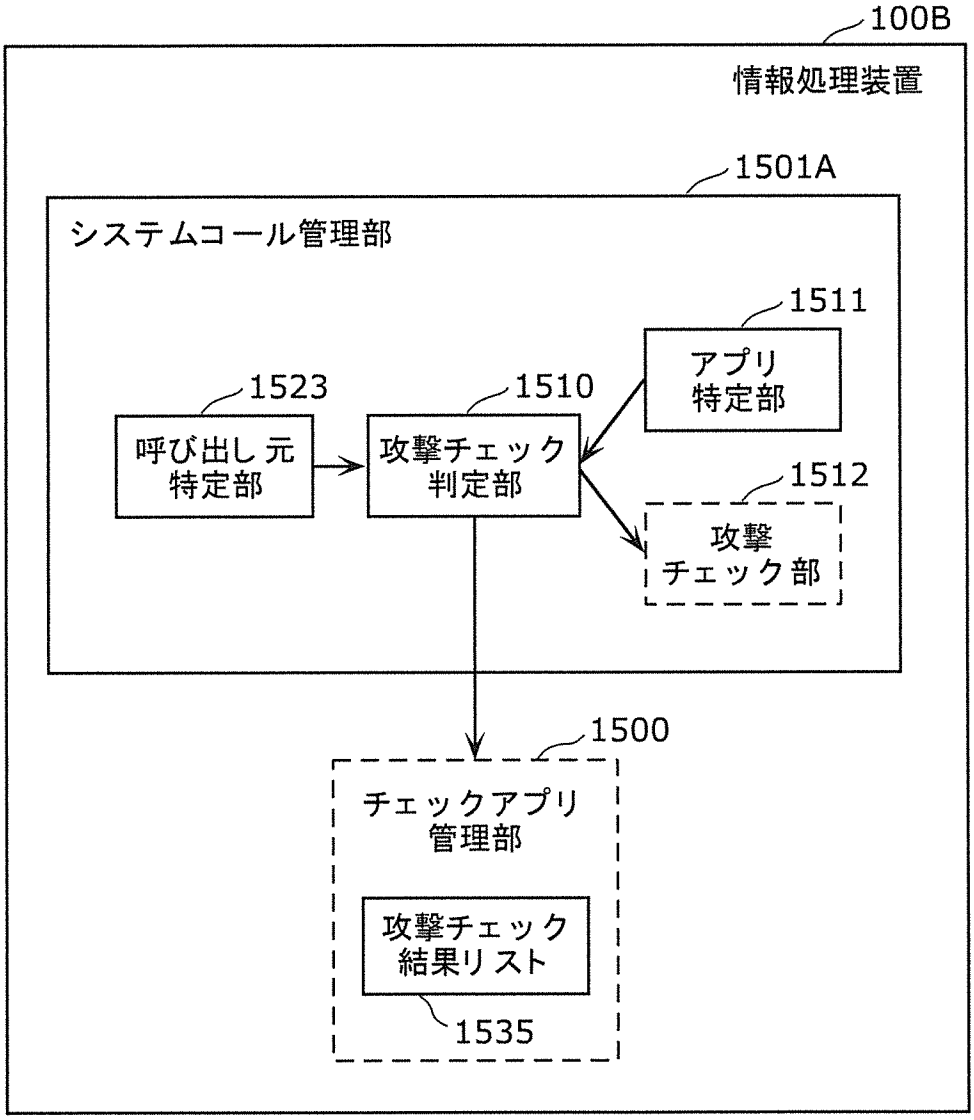
[図10]


1103
1502
1500
1501
表示アプリ
ファイル
読み込み管理部
チェックアプリ
管理部
システムコール
管理部
システムコール
依頼
S1000
S1001
依頼アプリ 識別子取得
依頼アプリチェック結果
問い合わせ
S1003
S1002
攻撃チェック結果取得
結果通知
S1004
S1005
否
チェック要否判定
S1006
要
攻撃チェック
S1008
チェック結果通知
攻撃チェック結果登録
S1007
S1009
NG
チェック結果判定
S1010
OK
システムコール処理
終了
終了
終了
終了

[図11]


1103
1502
1500
1501
表示アプリ
ファイル
読み込み管理部
チェックアプリ
管理部
システムコール
管理部
ファイル読み込み
依頼
S1101
S1100
チェック要否
判定処理
S1103
ファイル読み込み処理要求
読み込みコンテンツ識別子取得
S1102
要求アプリ識別子取得
S1104
呼び出し元取得
S1105
攻撃チェック結果取得
依頼
S1107
S1106
攻撃チェック結果取得
結果通知
S1109
S1108
否
読み込み可否判定
S1111
S1110
可
要
登録依頼
チェック要否判定
S1112
アプリ登録
否
読み込み処理
S1113
終了
終了
終了
終了

[図12]

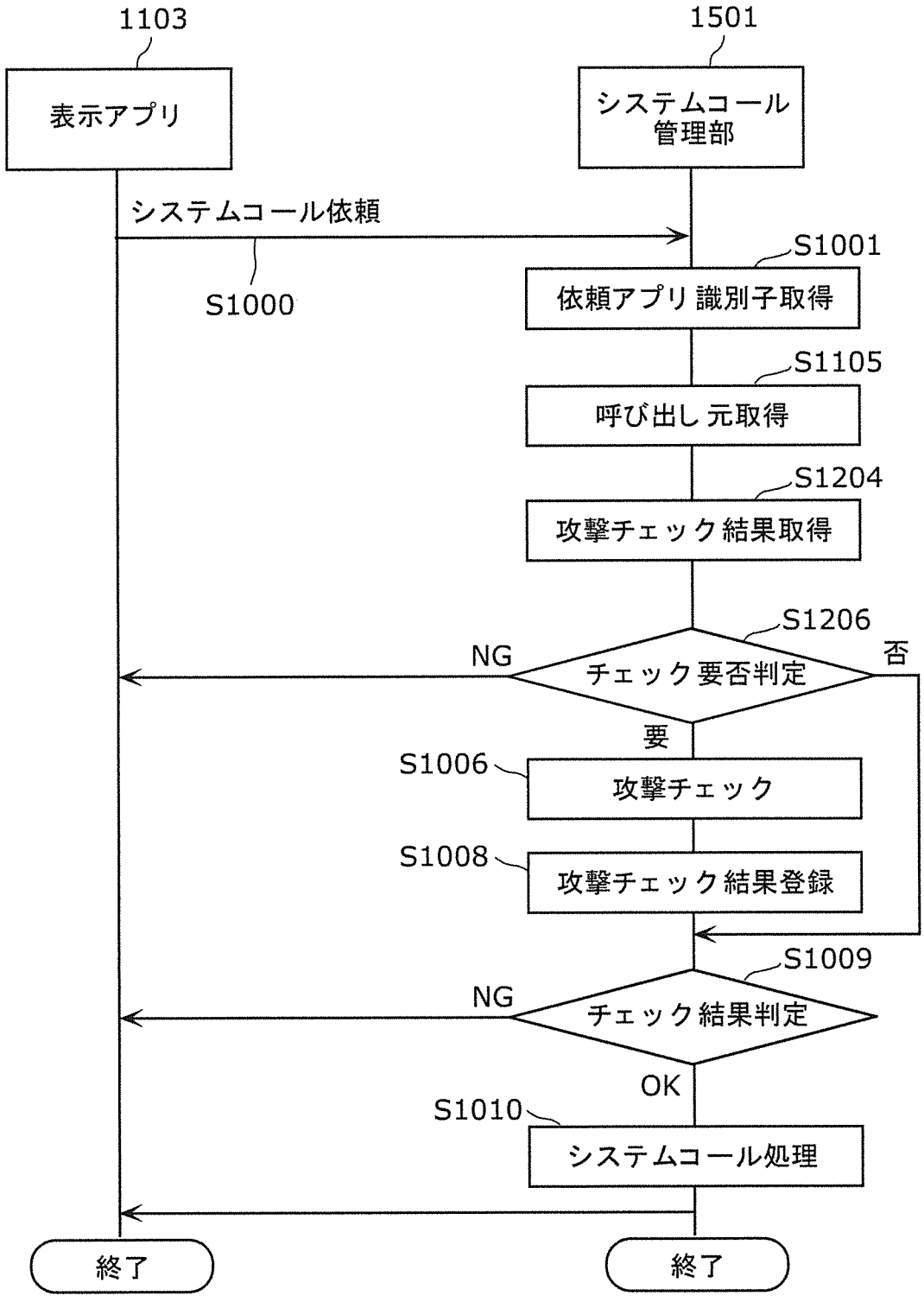


[図13]

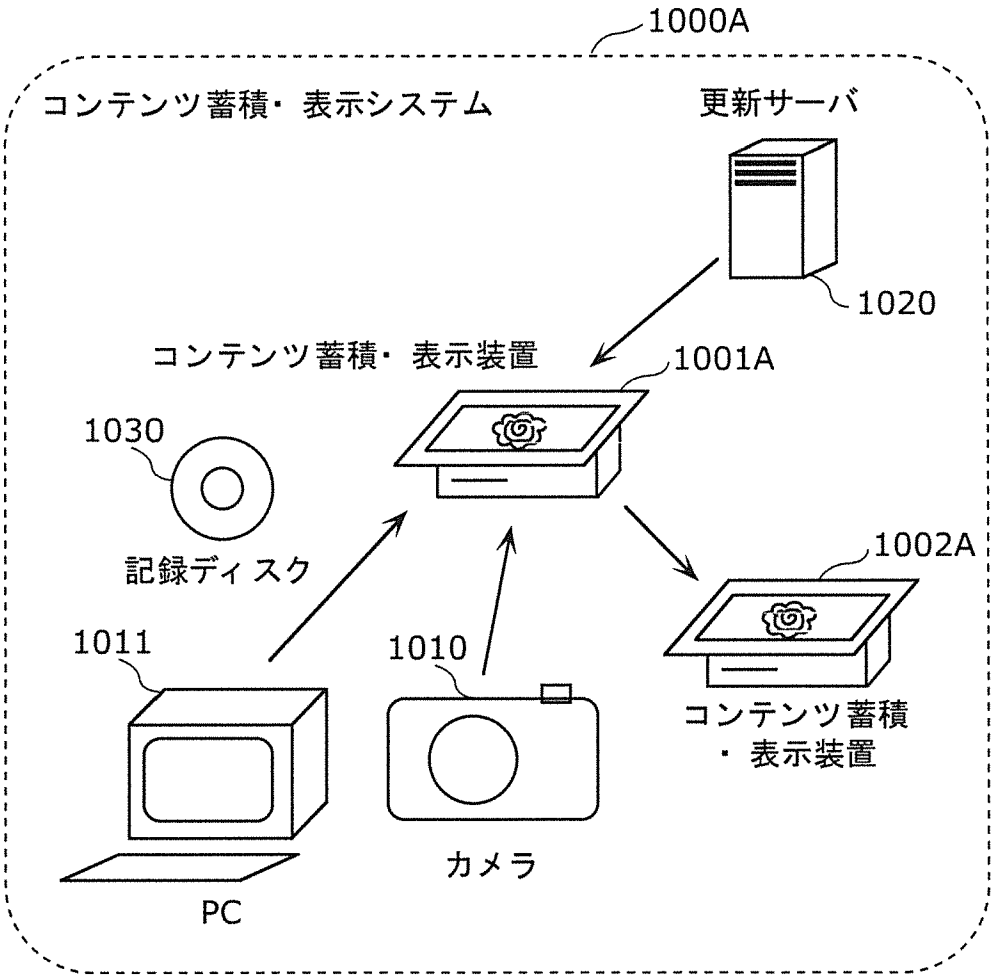
1535

アプリ識別子	呼び出し元アドレス	スタックポインタ値	チェック結果
アプリA	afe_0000	bff5_8000	○
アプリA	afe_0000	bef5_0000	×
アプリA	8cf0_0000	bff4_0000	○
アプリB	0000_c000	bff4_c000	○
・・・	・・・	・・・	

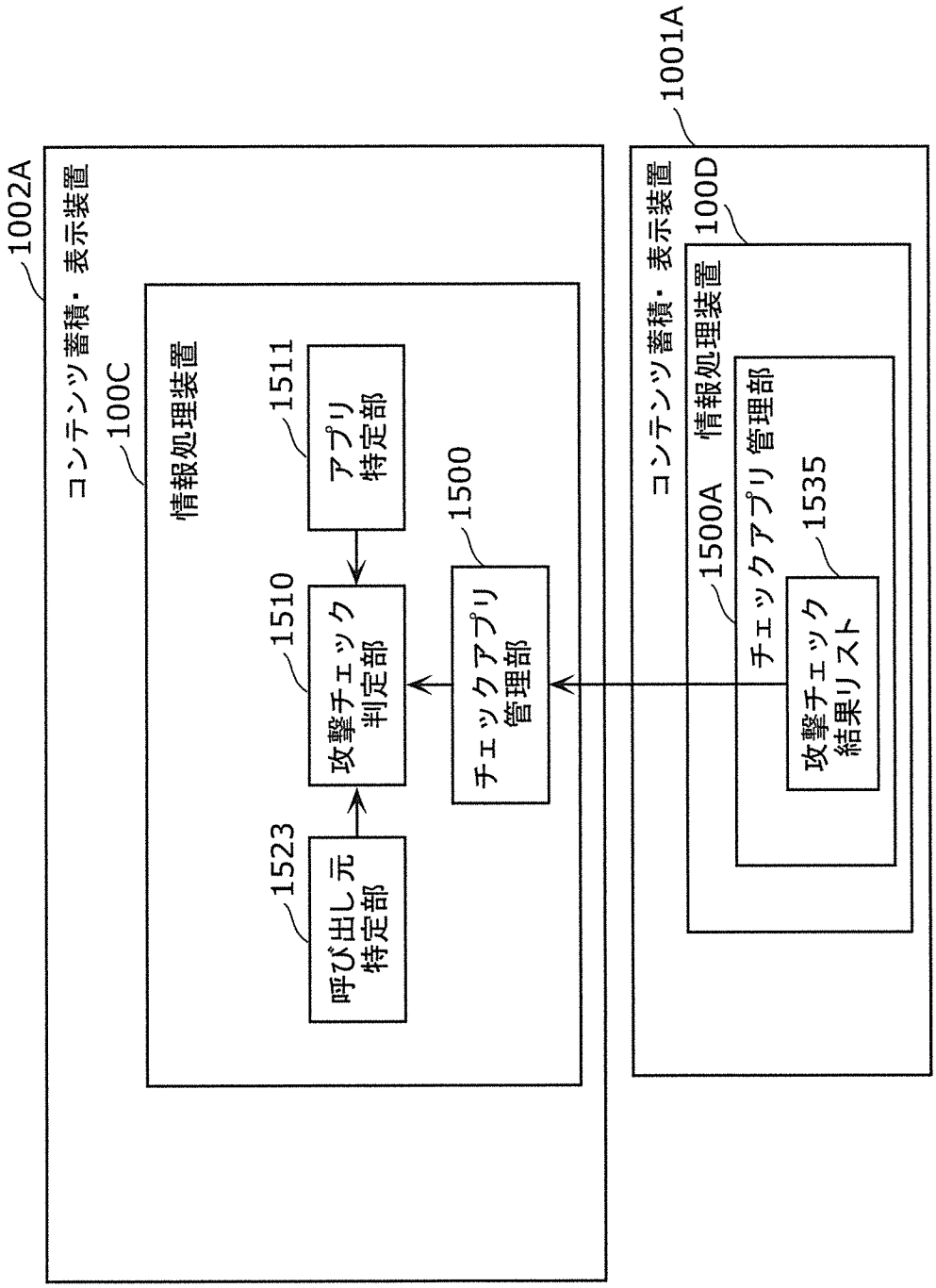
[図14]


1103
表示アプリ
1501
システムコール
管理部
システムコール依頼
S1000
S1001
依頼アプリ 識別子取得
S1105
呼び出し 元取得
S1204
攻撃チェック結果取得
S1206
NG
チェック要否判定
否
要
S1006
攻撃チェック
S1008
攻撃チェック結果登録
S1009
NG
チェック結果判定
OK
S1010
システムコール処理
終了
終了

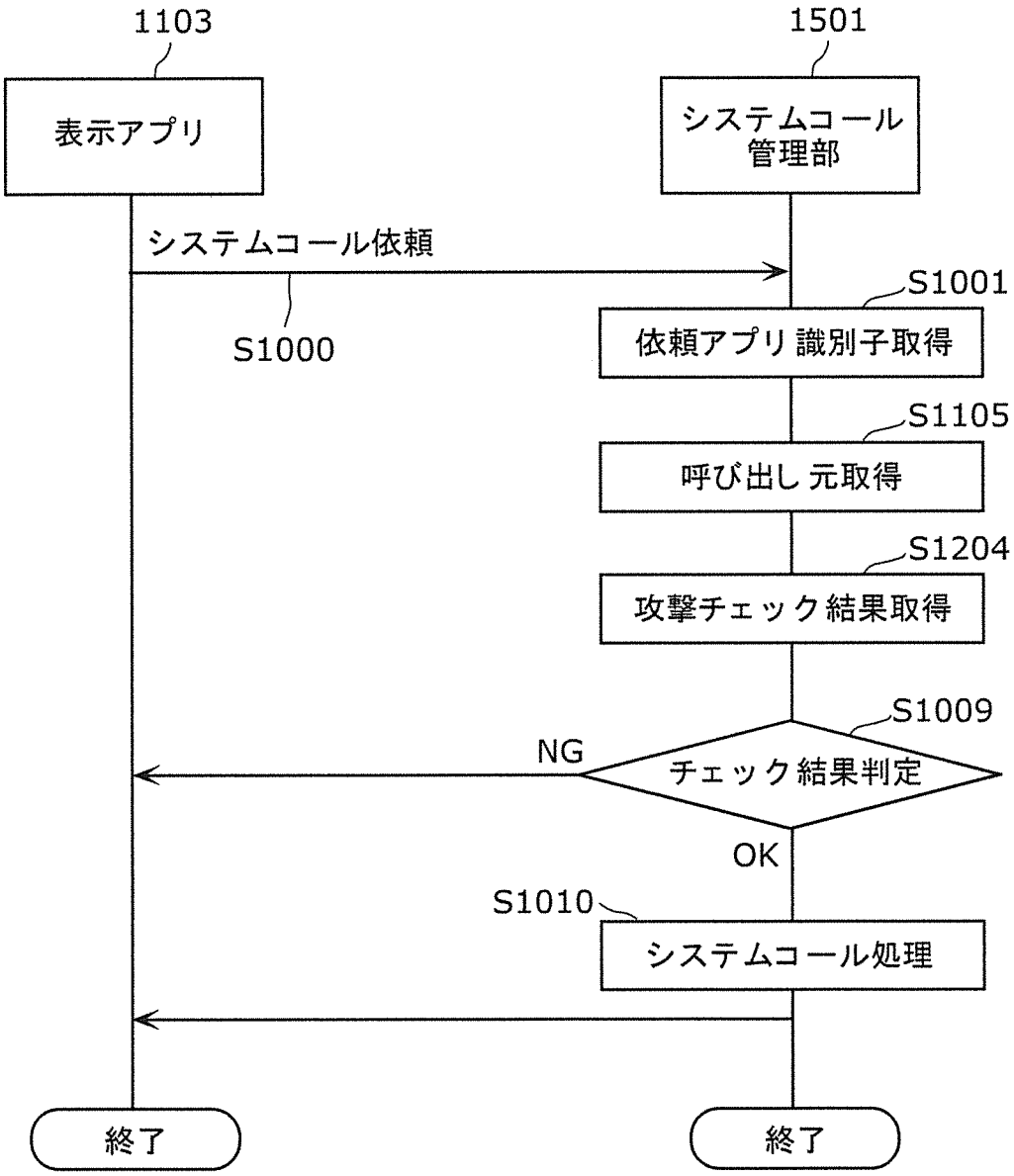
[図15]


1000A
コンテンツ蓄積・表示システム
更新サーバ
1020
コンテンツ蓄積・表示装置
1001A
1030
記録ディスク
1002A
1011
1010
コンテンツ蓄積
・表示装置
カメラ
PC

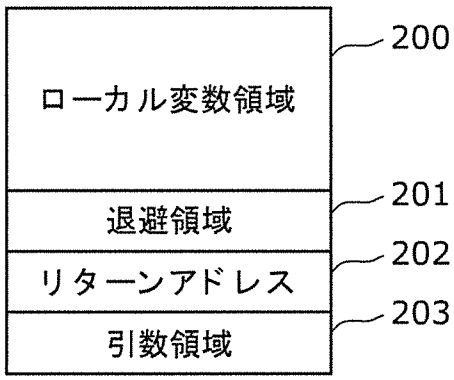
[図16]


1002A
コンテンツ蓄積・表示装置
100C
情報処理装置
1511
アプリ特定部
1500
1510
攻撃チェック判定部
チェックアプリ管理部
1523
呼び出し元特定部
1001A
コンテンツ蓄積・表示装置
100D
1500A 情報処理装置
チェックアプリ管理部
1535
攻撃チェック結果リスト

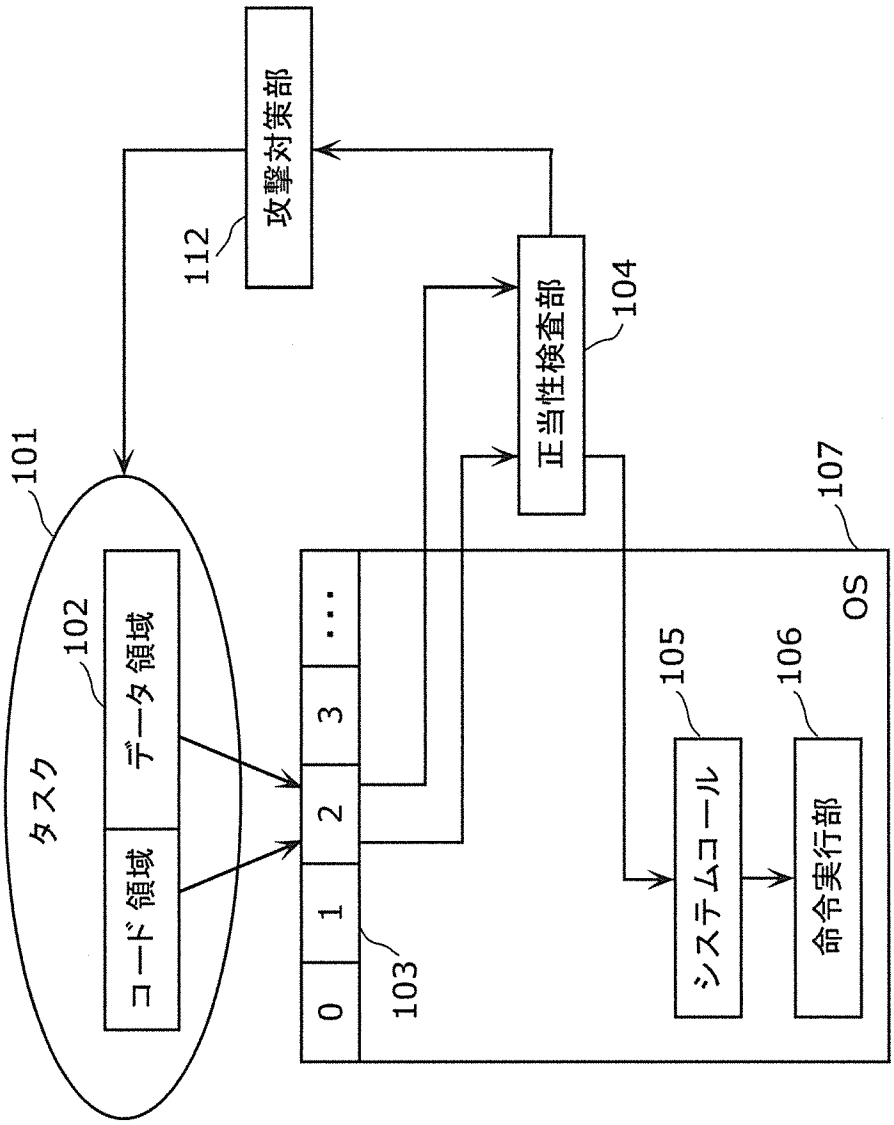
[図17]


1103
表示アプリ
1501
システムコール
管理部
システムコール依頼
S1000
S1001
依頼アプリ識別子取得
S1105
呼び出し元取得
S1204
攻撃チェック結果取得
S1009
NG
チェック結果判定
OK
S1010
システムコール処理
終了
終了

[図18]


ローカル変数領域
200
退避領域
201
リターンアドレス
202
引数領域
203

[図19]


攻撃対策部
112
正当性検査部
104
101
107
OS
タスク
102
データ領域
コード領域
0
1
2
3
...
103
105
システムコール
106
命令実行部

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/006668

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/00(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)
G06F21/00

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

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	JP 2010-97594 A (NTT Docomo Inc.), 30 April 2010 (30.04.2010), entire text; all drawings & US 2010/0077473 A1 & EP 2166478 A2 & CN 101685487 A	1-15
A	JP 2009-199529 A (Fourteenforty Research Institute, Inc.), 03 September 2009 (03.09.2009), entire text; all drawings (Family: none)	1-15
A	JP 2004-126854 A (Mitsubishi Electric Corp.), 22 April 2004 (22.04.2004), entire text; all drawings (Family: none)	1-15

☐ 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 December, 2011 (26.12.11)	10 January, 2012 (10.01.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／００６６６８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/00(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.　G06F21/00

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	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１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	関連する請求項の番号
A	JP 2010-97594 A (株式会社エヌ・ティ・ティ・ドコモ) 2010.04.30, 全文、全図 & US 2010/0077473 A1 & EP 2166478 A2 & CN 101685487 A	１－１５
A	JP 2009-199529 A (株式会社フォティーンフォティ技術研究所) 2009.09.03, 全文、全図（ファミリーなし）	１－１５
A	JP 2004-126854 A (三菱電機株式会社) 2004.04.22, 全文、全図（ファミリーなし）	１－１５

☐　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 ２６．１２．２０１１	国際調査報告の発送日 １０．０１．２０１２
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　３６５１ 児玉　崇晶 電話番号　０３－３５８１－１１０１　内線　３５４６