平成２９年６月１４日判決言渡

平成２８年（行ケ）第１００７１号　審決取消請求事件

口頭弁論終結の日　平成２９年４月１２日

判　　決

原　　告　　エンカレッジ・テクノロジ株式会社

同訴訟代理人弁理士　　谷　　川　　英　　和

同　　森　　本　　悟　　道

被　　告　　特　　許　　庁　　長　　官

同指定代理人　　辻　　本　　泰　　隆

同　　高　　木　　進

同　　野　　崎　　大　　進

同　　板　　谷　　玲　　子

主　　文

１　特許庁が不服２０１４－１１２７８号事件について平成２８年２月８日にした審決を取り消す。

２　訴訟費用は被告の負担とする。

事　実　及　び　理　由

第１　請求

主文同旨

第２　前提事実（いずれも当事者間に争いがない。）

１　特許庁における手続の経緯等

原告は，発明の名称を「機密管理装置，機密管理方法，及びプログラム」とする発明について，平成２２年１１月１７日に特許出願をしたが（特願２０１

０－２５６７３４号。以下「本願」という。），平成２６年３月１９日付け拒絶査定を受けたことから，特許庁に対し，同年６月１３日，拒絶査定不服審判を請求した。特許庁は，当該請求を不服２０１４－１１２７８号事件として審理をした上，平成２８年２月８日，「本件審判の請求は，成り立たない。」旨の審決をした（以下「本件審決」という。）。その謄本は，同月１８日，原告に送達された。

原告は，同年３月１７日，本件訴えを提起した。

２　特許請求の範囲

本願の請求項１～５に係る発明は，平成２５年１０月２２日付け手続補正書（甲５）により補正された特許請求の範囲の請求項１～５記載のとおりのものであるところ，その請求項１に係る発明（以下「本願発明」という。また，本願発明に係る明細書（特開２０１２－１０８７０４号公報（別紙）。甲４）を「本願明細書」という。）は，以下のとおりのものである。

【請求項１】

機密事項を扱うアプリケーションを識別する機密識別子が記憶される機密識別子記憶部と，

システムコールの監視において，実行部がアプリケーションを実行中に行う送信処理に応じたシステムコールをフックし，当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合に，当該フックしたシステムコールを破棄することによって当該送信を阻止し，そうでない場合に，当該フックしたシステムコールを開放する送信制御部と，を備えた機密管理装置。

３　本件審決の理由の要旨

本件審決の理由は，別紙審決書（写し）記載のとおりであるが，要するに，本願発明は，以下のとおり，本願の出願前に頒布された甲１（特開２００９－２１７４３３号公報。以下「引用例１」という。）に記載された発明（以下

「引用発明」という。）並びに当該技術分野の周知技術及び常とう手段に基づいて当業者が容易に発明することができたものであり，特許法（以下「法」という。）２９条２項により特許を受けることができないものであるから，その余の請求項に係る発明について検討するまでもなく，本願は拒絶すべきものである，というものである。

(1)　引用発明

アプリケーションの処理手段がアプリケーションを実行中に，処理対象となるファイルに対する送信を含む処理の指令を取得する第１の手段と，

前記第１の手段で取得された指令で特定される処理の内容に応じて，ＯＳに処理を渡す前にファイルに保護を施すか否かの判断を含む前記処理の内容に応じたファイルの保護方法を求め，その保護方法により前記処理対象となるファイルの保護処理を行う第２の手段と，

前記第２の手段は，前記第１の手段で取得された指令に関するファイルの入力元のアプリケーションの識別子とファイルの出力先となる記憶領域とに応じて，保護方法データベースによりファイルの保護方法を求め，その保護方法は，ファイルの出力先となる記憶領域の安全性が低い場合は処理を禁止することを含むものである，

を備えることを特徴とするファイル管理装置。

(2)　本願発明と引用発明との対比等

ア(ｱ)　引用発明では，「保護方法データベース」により，「第１の手段で取得された指令に関するファイルの入力元のアプリケーションの識別子とファイルの出力先となる記憶領域とに応じて，」「ファイルの保護」を行うところ，「保護方法データベース」に記憶された「入力元のアプリケーション」が保護対象データである「ファイル」を処理するのは自明であり，機密事項を保護対象データとして扱うことは当該技術分野の技術常識であることから，引用発明の「入力元のアプリケーション」，

「識別子」はそれぞれ，本願発明の「機密事項を扱うアプリケーション」，「機密識別子」に相当するということができる。

また，引用発明の「保護方法データベース」に「入力元のアプリケーション」の「識別子」が記憶されていることは明らかであるから，引用発明の「保護方法データベース」は本願発明の「機密事項を扱うアプリケーションを識別する機密識別子が記憶される機密識別子記憶部」に相当する。

(ｲ) 引用発明の「アプリケーション処理手段」，「処理の指令」，「ファイル管理装置」はそれぞれ，本願発明の「実行部」，「システムコール」，「機密管理装置」に相当する。

また，引用発明の「第２の手段」と本願発明の「送信制御部」とは，後記の点で相違するものの，“実行部がアプリケーションを実行中にファイルに対する送信処理に係るシステムコールを検知し，当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションである場合に，ファイルの送信先に応じて送信を阻止するか否かを決定する制御部”である点で共通する。

イ　一致点

機密事項を扱うアプリケーションを識別する機密識別子が記憶される機密識別子記憶部と，

実行部がアプリケーションを実行中にファイルに対する送信処理に係るシステムコールを検知し，当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションである場合に，ファイルの送信先に応じて送信を阻止するか否かを決定する制御部と

を備える機密管理装置。

ウ　相違点１

ファイル送信の阻止の条件に関し，本願発明では「アプリケーションが，前記機密識別子記憶部で記憶され」ているほかに，フックした「送信処理に応じたシステムコール」の「送信先がローカル以外である場合」が条件であるのに対して，引用発明では，ファイルの送信に係る「取得された指令に関するファイルの入力元のアプリケーションの識別子とファイルの出力先となる記憶領域」とが「保護方法データベース」に記憶されているほかに，「ファイルの出力先となる記憶領域の安全性が低い場合」が条件である点。

エ　相違点２

ファイル送信の阻止に伴う制御に関し，本願発明では「当該フックしたシステムコールを破棄することによって当該送信を阻止し，そうでない場合に，当該フックしたシステムコールを開放する」のに対して，引用発明では，「ファイルの出力」に係る「処理を禁止する」ための制御の詳細について言及されていない点。

オ　判断

(ｱ)　相違点１について

引用発明のごときファイル管理装置において，アプリケーションのファイルに対するいかなる処理の指令につきいかなるファイル保護処理を対応付けるかは，要求されるシステムの安全性と必要なシステム負荷等の相関関係等に基づき決定されるべき事項であり，当業者であれば適宜設計し得た事項である。

また，甲２（特開２００９－２５８８５２号公報。以下「引用例２」という。）に記載されるように，ファイルを含むパケットについて，内部ネットワークから外部ネットワークへの持出しを判断し，送信先に応じて許可／禁止を判定すること，すなわち，内部ネットワーク（ローカル）以外への送信の安全性が低いとしてセキュリティ対策を施すことは，

本願出願前には当該技術分野の周知の事項であった。さらに，甲３（特開２００２－２８８０３０号公報。以下「参考文献」という。）に記載されるように，機密ファイルをあるアプリケーションプログラムが開いた後は，電子メール等によって当該アプリケーションプログラムにより当該ファイルが機密情報保存用フォルダ（ローカル）以外に出力されることがないようにすることも，本願出願前には当該技術分野の周知技術であった。

そうすると，引用発明において，引用例２等に記載の周知技術を適用し，ファイル送信の阻止の条件として，アプリケーションが，機密識別子記憶部に記憶されることのほかに，適宜，オペレーションシステム（ＯＳ）への処理要求に基づくファイルに対する処理が，ローカル以外へのファイル送信であった場合を条件とすること，すなわち，相違点１に係る構成とすることは，当業者が容易に想到し得たことである。

(ｲ) 相違点２について

引用発明では，「ファイルに対する送信を含む処理の指令」が「ファイルの送信」の場合は，ＯＳに処理を渡す前にファイルに保護を施すことが読み取れる。

そして，ＯＳに処理を渡す前に，「ファイルの出力」に係る「処理を禁止する」ための制御として，ＯＳへの処理要求を破棄することは，当該技術分野における常とう手段である。

そうすると，引用発明において，ファイルの出力に係る処理の制御のために上記常とう手段を適用し，適宜，ファイルの出力に係る処理を禁止する場合はＯＳへの処理要求を破棄し，当該処理を禁止しない場合にはＯＳへの処理要求を開放すること，すなわち，相違点２に係る構成とすることは，当業者が容易に想到し得たことである。

第３　当事者の主張

１　原告の主張

(1)　原告の主張する取消事由は，概略以下のとおりである。

ア　取消事由１（引用発明の認定の誤り）

(ｱ)　取消事由１－１（送信の指令に関する引用発明の認定の誤り）

(ｲ)　取消事由１－２（保護方法に関する引用発明の認定の誤り）

（なお，取消事由１－１及び１－２は，原告の平成２８年４月２６日付け準備書面において「取消事由１」として主張されているものであるが，便宜上，上記のとおり別個の取消事由とする。）

イ　取消事由２（一致点の認定の誤り及び相違点の看過）

(ｱ)　取消事由２－１（本件審決は，引用発明の保護方法データベースに含まれる各アプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものと理解した場合。なお，原告の平成２８年４月２６日付け準備書面において「取消事由２」として主張されているものであるが，便宜上「取消事由２－１」とする。）

(ｲ)　取消事由２－２（本件審決は，引用発明の保護方法データベースに含まれる最高レベルの安全性に対応するアプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものと理解した場合。なお，原告の平成２８年１１月２８日付け準備書面（第５回）において「取消事由４」として主張されているものであるが，便宜上「取消事由２－２」とする。）

ウ　取消事由３（相違点の認定の誤り及び相違点に係る容易想到性判断の誤り）

(2)　取消事由１－１（送信の指令に関する引用発明の認定の誤り）

ア　本件審決の認定に係る引用発明には，第２の手段が，第１の手段で取得されたファイルの送信の指令に関する入力元のアプリケーションの識別

子と出力先となる記憶領域とに応じてファイルの保護方法を求める構成が含まれる。このことは，ファイルの送信の指令に入力元のアプリケーションの識別子と出力先となる記憶領域とが含まれており，それらを抽出できることを前提とする。

しかし，引用例１の記載等によれば，引用発明の送信の指令はアプリケーションの識別子の引数を取らないと解されることから，ファイルの送信の指令から入力元のアプリケーションの識別子を抽出することはできない。すなわち，引用発明においては，第１の手段がファイルの送信の指令を取得した場合，第２の手段が，第１の手段で取得されたファイルの送信の指令から入力元のアプリケーションの識別子を抽出することはできないことから，取得されたファイルの送信の指令に関する入力元のアプリケーションの識別子と出力先となる記憶領域とに応じてファイルの保護処理を求めることができない。このため，この場合，第２の手段は，取得されたファイルの送信の指令に関して，ファイルの出力先となる記憶領域の安全性が低い場合に送信の処理を禁止することもできないことになる。

このように，引用発明においては，取得されたファイルの送信の指令から入力元のアプリケーションの識別子を抽出することはできないところ，本件審決はその抽出ができるとした点で誤りがある。

イ　本願発明は，送信処理に応じたアプリケーションが機密識別子で識別されるアプリケーション（以下「機密アプリケーション」という。また，引用発明について論ずるに当たり，これに相当するものとの趣旨でこの語を用いることもある。）であり，送信先がローカル以外である場合に，その送信を阻止するのに対し，引用発明は，上記のとおり，ファイルの送信の指令に関し，その送信を禁止することができないという相違点がある。また，この相違点に係る本願発明の構成について，引用例２及び

参考文献に各記載の技術的事項から当業者が容易に想到することはできない。

したがって，上記送信の指令に関する引用発明の認定の誤りは，本件審決の結論に影響を及ぼす。

(3) 取消事由１－２（保護方法に関する引用発明の認定の誤り）

ア 仮に，上記送信の指令に関する引用発明の認定の誤りがなかったとしても，本件審決には，保護方法に関する引用発明の認定の誤りがある。

すなわち，本件審決は，引用発明における保護方法として「ファイルの出力先となる記憶領域の安全性が低い場合は処理を禁止することを含む」ことを認定しているが，引用発明については，それだけでなく，第１の手段で取得された指令に係るファイルの出力先となる記憶領域に応じた安全性が，入力元のアプリケーションの識別子に応じた安全性より高い場合に第２の手段が求める保護方法（ファイルの入力元となるアプリケーションの識別子の安全性に対応する保護処理）も含めて認定すべきであるのに，これを行っていない点で誤りがある。

イ 本願発明は，実行部がアプリケーションを実行中に行う送信処理に応じたシステムコールをフックし，当該アプリケーションが機密アプリケーションであり，送信先がローカル以外でない場合に，当該フックしたシステムコールを開放するのに対し，引用発明は，上記のとおり，ファイルの出力先となる記憶領域の安全性が高い場合であっても，入力元となるアプリケーションの識別子の安全性に対応する保護処理を行うという相違点がある。また，この相違点に係る本願発明の構成について，引用例２及び参考文献に各記載の技術的事項から当業者が容易に想到することはできない。

したがって，上記保護方法に関する引用発明の認定の誤りは，本件審決の結論に影響を及ぼす。

(4)　取消事由２（一致点の認定の誤り及び相違点の看過）

ア　本件審決は，引用発明の保護方法データベースに含まれる各アプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定しているものと理解されるが，被告は，本件審決につき，引用発明の保護方法データベースに含まれる最高レベルの安全性に対応するアプリケーション（以下「最安全アプリケーション」という。）の識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものである旨主張する。

しかし，そのいずれと理解したとしても，本件審決には一致点の認定の誤り及び相違点の看過があり，この誤りは結論に影響を及ぼす。以下，本件審決の理解に応じて場合を分けて論ずるが，これらに共通する趣旨は，本件審決は，本願発明の機密識別子の作用ないし機能と引用発明の識別子の作用ないし機能が相違すること，すなわち，本願発明の「機密識別子」は「機密事項を扱うアプリケーションを識別する」ものであるのに対し，引用発明における「アプリケーションの識別子」は必ずしも機密事項を扱うアプリケーションを識別するものではなく，ファイルの保護方法を求める上で必要となる安全性の程度（例えば，数値）を得る前提として，入力元のアプリケーションを識別するものであることを看過したというものである。

イ　取消事由２－１（一致点の認定の誤り及び相違点の看過：本件審決につき，引用発明の保護方法データベースに含まれる各アプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものと理解した場合）

(ｱ) a　本件審決は，引用発明の保護方法データベースに含まれる各アプリケーションの識別子は，本願発明の機密識別子記憶部で記憶されている機密識別子に相当し，引用発明のアプリケーションの識別子を記

憶する「保護方法データベース」は，本願発明の機密識別子が記憶されている機密識別子記憶部に相当する旨認定しているところ，以下のとおり，この点に関する本件審決の認定には誤りがある。

b　引用例１の記載によれば，引用発明の保護方法データベースには，原則として全てのアプリケーションの識別子が含まれていると解されることから，実質的な保護処理を行わないアプリケーションの識別子も保護方法データベースに含まれることになる。また，保護処理が，引用発明の「ファイルの出力先となる記憶領域の安全性が低い場合は処理を禁止すること」であるとしても，安全性の最低の値に対応するアプリケーションについては，ファイルの出力先となる記憶領域の安全性がそのアプリケーションの識別子に対応する安全性よりも低くなることはないから，処理を禁止する保護処理は行われないことになる。

このように，引用発明の保護方法データベースには実質的な保護処理を行わないアプリケーションの識別子も含まれ，また，保護方法データベースに記憶された識別子により識別されるアプリケーションが処理を行う対象であるファイルが保護対象データであるとは限られない。

その結果，機密事項を保護対象データとして扱うことが技術常識であったとしても，保護方法データベースには機密事項を扱わないアプリケーションの識別子も含まれるため，引用発明の保護方法データベースは，本願発明の機密識別子記憶部とは異なることになる。すなわち，本願発明の機密識別子記憶部では，機密アプリケーションを識別する機密識別子が記憶されるのに対し，引用発明の保護方法データベースでは，機密事項を扱わないアプリケーションの識別子も記憶されるという相違点（以下「相違点Ａ」という。）が存在する。

したがって，引用発明の保護方法データベースが本願発明の機密

識別子記憶部に相当するとして一致点を認定し，相違点Ａを看過した本件審決には誤りがある。

(ｲ) 上記のとおり，本願発明と引用発明には相違点Ａが存在するところ，引用発明から，当該相違点に係る本願発明の構成に到達するためには，引用発明の保護方法データベースにおいて，実質的な保護処理を行わないアプリケーションを識別する識別子を除外する必要がある。

しかし，引用発明は「データの取得先や出力先に応じてデータの保護方法を変更したり，データを使用するアプリケーション毎にデータの保護方法を変更したりして，柔軟にデータを保護すること」（引用例１【０００８】）を課題としているため，保護方法データベースに種々のアプリケーションの識別子が存在することは引用発明の課題解決手段として必須の構成というべきである。そうすると，引用発明の保護方法データベースにおいて特定のアプリケーションの識別子のみが記憶されるように限定することには，引用発明の課題を解決する観点から阻害要因があるということができる。

このため，相違点Ａについて，引用発明から出発して本願発明に容易に想到可能であるということはできないから，上記一致点の認定の誤り及び相違点Ａの看過は，本件審決の結論に影響を及ぼす。

ウ 取消事由２－２（一致点の認定の誤り及び相違点の看過：本件審決につき，引用発明の保護方法データベースに含まれる最高レベルの安全性に対応するアプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものと理解した場合）

(ｱ) 本願発明において，送信が阻止される条件としては，送信処理を行うアプリケーションが，機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであるという部分条件（以下「第１部分条件」という。）と，送信先がローカル以外であるという部分条

件とが存在する。本件審決は，「実行部がアプリケーションを実行中にファイルに対する送信処理に係るシステムコールを検知し，当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションである場合に，ファイルの送信先に応じて送信を阻止するか否かを決定する制御部」を一致点と認定していることから，第１部分条件は一致点に含まれる。

他方，引用発明においては，送信の指令における入力元のアプリケーションが最安全アプリケーションであることは，送信阻止に関するアプリケーションの条件ではない。すなわち，引用発明では，送信の指令に含まれる入力元のアプリケーションの識別子に対応する安全性が出力先の記憶領域に対応する安全性よりも高い場合に送信が阻止される。このため，引用発明における送信阻止に関するアプリケーションの条件は，入力元のアプリケーションの識別子に対応する安全性が出力先の記憶領域に対応する安全性よりも高いことという相対的なものとなる。そうすると，送信の指令に含まれる入力元のアプリケーションが最安全アプリケーションであれば，出力先の記憶領域の安全性に応じて送信が阻止され得ることになるが，引用発明において安全性のレベルは３段階以上存在すると考えられるところ，送信の指令に含まれる入力元のアプリケーションに対応する安全性が２番目に高い場合にも，出力先の記憶領域の安全性に応じて送信が阻止され得ることになる。これは，引用発明において，入力元のアプリケーションが最安全アプリケーションであることは送信阻止に関するアプリケーションの条件ではないことを意味する。

したがって，本願発明の第１部分条件は一致点ではなく，「送信阻止に関するアプリケーションの条件が，本願発明では，送信処理を行うアプリケーションが機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであること（第１部分条件）であるのに対し，

引用発明では，送信の指令に含まれる入力元のアプリケーションの識別子に対応する安全性が出力先の記憶領域に対応する安全性よりも高いこと」という相違点（以下「相違点Ｂ」という。）が存在することとなる。

(ｲ)　この相違点Ｂの看過は，本件審決の結論に影響を及ぼす。

すなわち，前記のとおり，引用発明は，処理内容の入力元の安全性と出力先の安全性との相対的な高低関係に応じて保護方法を決定するという特徴を有しており，その結果，送信阻止に関するアプリケーションの部分条件も相対的なものとなっている。その相対的な部分条件を絶対的なものに変更することは，引用発明の上記特徴を喪失させることになる。このため，引用発明において本願発明の相違点Ｂに係る構成を採用することには阻害要因があり，引用発明から出発して本願発明の相違点Ｂに係る構成に到達するための論理付けを行うことはできないし，これを可能とする従来技術も周知技術も示されていない。

そうすると，本願発明の相違点Ｂに係る構成については，引用発明から出発して当業者が容易に想到可能であるということはできない。

したがって，本件審決には，一致点の認定の誤り及び相違点Ｂの看過があり，これは本件審決の結論に影響を及ぼす。

(5)　取消事由３（相違点の認定の誤り及び相違点に係る容易想到性判断の誤り）

ア(ｱ)　本件審決は，以下のとおり，ファイル送信が阻止されない条件に関する相違点を含めずに相違点１を認定した点で誤りがある。

(ｲ)　本願発明は，機密アプリケーションの実行中に行われた，送信先がローカル以外である送信を阻止し，送信先がローカルである送信を阻止しないものである。また，本願発明では，機密アプリケーションでないアプリケーション（以下「非機密アプリケーション」という。）の実行中に行われた送信は，送信先がローカルでもローカル以外でも

阻止されないことになる。したがって，本願発明においてアプリケーションによる送信が阻止されない条件は，送信を行ったアプリケーションの識別子が機密識別子記憶部に記憶されていないこと，又は，送信先がローカルであることである。

他方，前記のとおり，引用発明の保護方法データベースに含まれるアプリケーションの識別子には，処理の禁止等の実質的な保護処理を行わないアプリケーションのものも含まれると解されることから，引用発明においてファイル送信が阻止される条件は，入力元であるアプリケーションの識別子の安全性よりも出力先である記憶領域の安全性の方が低いことであり，送信が阻止されない条件は，入力元であるアプリケーションの識別子の安全性よりも出力先である記憶領域の安全性の方が低くないことである。

したがって，本願発明と引用発明とは，本願発明では，送信が阻止される条件が，アプリケーションの識別子が機密識別子記憶部で記憶されており，かつ，送信先がローカル以外であることであり，阻止されない条件が，アプリケーションの識別子が機密識別子記憶部で記憶されていないこと，又は，送信先がローカルであることであるのに対し，引用発明では，ファイル送信が阻止される条件が，入力元であるアプリケーションの識別子の安全性よりも出力先である記憶領域の安全性の方が低いことであり，阻止されない条件が，入力元であるアプリケーションの識別子の安全性よりも出力先である記憶領域の安全性の方が低くないことであるという相違点（以下「相違点Ｃ」という。）があり，相違点１は，正しくは相違点Ｃのように認定されるべきである。また，このことは，仮に取消事由２－１として主張した一致点の認定の誤り及び相違点の看過がなかったとしても異ならない。

イ(ｱ)　前記のとおり，引用発明の保護方法データベースには，原則として，

実行され得る全てのアプリケーションの識別子が含まれると解されるため，非機密アプリケーションの識別子も保護方法データベースに含まれている。

引用発明においては，ファイルの入力元の安全性が高いほど低い程度の保護処理を行えばよく，安全性が低いほどより厳重な保護処理を行う必要がある。このため，引用発明において，本願発明と同様に，機密アプリケーションによるローカル以外への送信が禁止され，非機密アプリケーションによるローカル以外への送信が少なくとも禁止されないようにするためには，非機密アプリケーションの安全性を機密アプリケーションの安全性よりも低く設定しなければならないことになる。このことは，機密事項を扱わないアプリケーションに対する保護方法が，機密事項を扱うアプリケーションに対する保護方法よりも厳重でなくてはならないことを意味しており，引用発明の属する技術分野における技術常識に反する。

したがって，引用発明において，本願発明と同様の保護処理が行われるように安全性を設定することには阻害要因があるから，相違点Ｃに係る本願発明の構成は，引用発明において当業者が適宜設計し得たものではない。

(ｲ) 仮に，引用発明の保護方法データベースに，実行され得る全てのアプリケーションの識別子が含まれているのではないとしても，相違点Ｃに係る本願発明の構成が，引用発明において当業者が適宜設計し得たものでないことは異ならない。

すなわち，引用発明では，保護方法データベースに含まれないアプリケーションの識別子や記憶領域については，最も高い安全性を用いて保護方法を求めることになると解される。他方，機密アプリケーションによるローカル以外への送信が禁止されるように機密アプリケーションの

安全性とローカル以外の記憶領域の安全性とが設定されている場合，ローカル以外の記憶領域の安全性は，少なくとも，最も高い安全性ではないことになる。そうすると，非機密アプリケーションによるローカル以外へのファイル送信も機密アプリケーションによるものと同様に阻止されることになり，非機密アプリケーションのローカル以外へのファイル送信が阻止されない本願発明の構成とは異なるものになる。

このように，仮に，引用発明の保護方法データベースに，実行され得る全てのアプリケーションの識別子が含まれているのではないとしても，当業者が，引用発明から相違点Ｃに係る本願発明の構成に想到することはできない。

ウ(ｱ) 引用例２に記載された技術は，送信先のＩＰアドレス等をチェックすることによって，クライアントからの送信情報の持出しの可否について判定し，不可と判定された場合に通信を遮断するものである。この技術は，ネットワーク上において上記処理を行うものであり，クライアントＰＣにおいて用いられるものではなく，情報漏えいを防止するための処理をネットワーク以外のローカルの装置等において実行するように変更することは，当該技術の目的に反することになる。

また，当該技術は，パケットのＩＰアドレス，パケットのポート番号，パケットに含まれるキーワード及びファイルのサイズの少なくとも１つを用いて判定を行うため，送信先のＩＰアドレス等がわからなければ，送信情報の持出しの可否判定を行うことができない。このため，指令からＩＰアドレスを取得しない引用発明に，ＩＰアドレスを用いて情報漏えいの防止を行う引用例２記載の技術的事項を適用することはできない。

(ｲ) 参考文献に記載された技術は，あらかじめ定められた機密情報保存用フォルダに保存されているファイルの内容が当該フォルダ以外に出力されないように制限するものであり，当該フォルダは，ローカルの

全てのフォルダではなく，一部のフォルダである。したがって，当該技術は，ローカルにおける複数のフォルダのうち特定のフォルダに保存されているファイルのみを保護するものである。

このため，引用発明に当該技術を適用した場合，ローカルの特定のフォルダに関する持出しの処理が制限されるだけであり，他のフォルダに保存されているファイルについては制限されないことになるから，引用発明に参考文献記載の技術的事項を適用することにより，機密アプリケーションによるローカル以外への送信を全て阻止することができる本願発明に想到することはできない。

(ｳ) 引用発明は，指令に含まれるアプリケーションの識別子や記憶領域に対応する安全性を用いた保護処理を行うことによってその課題を解決していると解されることから，安全性を用いて保護処理を行うことを必須の構成とするものであって，引用発明に引用例２及び参考文献に各記載の技術的事項を適用し，安全性を用いないで保護処理を行うようにすることには阻害要因がある。

エ 以上のとおり，相違点Ｃに係る本願発明の構成は，引用発明において当業者が適宜設計し得た事項ではなく，また，引用発明に引用例２及び参考文献に各記載の技術的事項を適用することによって，相違点Ｃに係る本願発明の構成に容易に想到することもできない。

したがって，本件審決には容易想到性の判断に誤りがあり，その誤りは本件審決の結論に影響を及ぼす。

２ 被告の主張

(1) 取消事由１－１（送信の指令に関する引用発明の認定の誤り）について

ア 本件審決の認定した引用発明の内容

(ｱ) 本件審決の認定した引用発明

引用例１の【００７７】には，「＜変形例３＞ 上記の実施の形態で

は，出力先の安全性に応じて保護方法を決定したが，処理内容から入力元の記憶領域または識別子と出力先の記憶領域または識別子とを抽出し，入力元の安全性と出力先の安全性から，処理方法を決定するようにしてもよい。」（以下「変形例３」という。）と記載されている。この変形例３においてのみ，「出力先の安全性」に加え「入力元の安全性」にも応じて「保護方法」が決定されるものとなっており，かつ，①入力元と出力先が同じ安全性であることから再度保護処理を行わずそのままファイルの複写を行う態様，②入力元よりも出力先の安全性が低い場合に処理を禁止する態様，③入力元よりも出力先の安全性が高い場合には入力元の安全性に従った保護処理を施し，元の保護よりも弱い保護にはしないようにする態様，が例示されている（以下，各態様を「態様①」のようにいう。）。態様①～③は，設定された安全性に基づく情報の保護の方法ないし程度が異なっており，例えば態様②は，出力禁止となっていない出力先に対する出力であっても場合によっては禁止するものであり，「元の保護よりも弱い保護にはしないようにする」という態様③よりもより積極的に保護を行うものとなっている。

本件審決は，このような引用例１の記載のうち，態様②に係る箇所の記載を踏まえ，ファイルの入力元よりも出力先の安全性が低い場合に処理を禁止し，それ以外の場合には処理を禁止しないものを引用発明として認定したものである。

(ｲ) 引用発明における「安全性」

引用例１の記載によれば，「安全性」はデータに対する指令の処理内容に含まれる入力元又は出力先の記憶領域やアプリケーションに対して数値レベルで設定される。この数値レベルは，情報セキュリティ上の信頼の度合いを数値化し，どのような保護を適用するかを特定する際に用いられるものであり，一般に「セキュリティレベル」と呼ばれ，データ

やリソース等のセキュリティレベル（安全性）の高さが機密性の高さと相関することは周知の事項である。

もっとも，変形例３の態様①～③においては，引用例１記載の他の実施の形態と異なり，「保護方法」は「安全性」の具体的な数値の値ではなく「入力元の安全性」と「出力先の安全性」との関係に対応するのであって，「安全性」の具体的な数値の値が「保護方法」に対応するわけではない。引用発明は，前記のとおり，変形例３の３つの態様のうち態様②を踏まえて認定されたものであり，「入力元の安全性」と「出力先の安全性」との関係に応じて所定の保護方法が適用され，ファイルの入力元のアプリケーションの安全性よりその出力先となる記憶領域の安全性が低いという関係にある場合に処理を禁止し，そうでない場合には処理を禁止しないというものである。

(ｳ)　引用発明の「第２の手段」

引用例１の記載によれば，引用発明のファイル管理装置は，「取得された指令で特定される処理の内容に応じて，ＯＳに処理を渡す前にファイルに保護を施すか否かの判断を含む前記処理の内容に応じたファイルの保護方法を求め，その保護方法により前記処理対象となるファイルの保護処理を行う」ものであって，そのための「第２の手段」を備えるものである。また，この「手段」によって「取得された指令で特定される処理の内容に応じたファイルの保護方法」を求めるに当たり，当該処理内容に含まれる「記憶領域」又は「アプリケーションを特定する識別子」が抽出される。さらに，「処理内容」に含まれる「記憶領域」又は「アプリケーションを特定する識別子」に応じて「保護方法データベース」が参照され，ファイルの「保護方法」が求められる。

加えて，前記【００７７】の記載によれば，態様①～③のいずれも，「取得された指令で特定される処理の内容」によっては，「指令」に関

するファイルの「入力元」と「出力先」とに応じてファイルの「保護方法」を求める態様である旨が示されているところ，ここでの「入力元」と「出力先」としては，「記憶領域」又は「アプリケーションを特定する識別子」のうちの任意の組合せがあり得，「入力元」を「アプリケーションの識別子」とし「出力先」を「記憶領域」とする組合せが含まれていることは明らかである。そうすると，同記載からは「取得された指令で特定される処理の内容」により，ファイルの「入力元」の「アプリケーションの識別子」とファイルの「出力先」となる「記憶領域」とに応じて，入力元よりも出力先の安全性が低い場合に処理を禁止する態様を読み取ることができる。

以上を踏まえると，引用発明のファイル管理装置は，「取得された指令で特定される処理の内容に応じて，ＯＳに処理を渡す前にファイルに保護を施すか否かの判断を含む前記処理の内容に応じたファイルの保護方法を求め，その保護方法により前記処理対象となるファイルの保護処理を行う」に当たり，「取得された指令に関するファイルの入力元のアプリケーションの識別子とファイルの出力先となる記憶領域とに応じて，入力元よりも出力先の安全性が低い場合に処理を禁止する」ものであって，そのための「第２の手段」を備えるものである。本件審決も，同旨を述べて引用発明を認定しており，その認定に誤りはない。

イ(ｱ)　引用例１の【００３８】には，「ステップＳ１２では，処理内容から出力先の記憶領域または識別子を抽出する。…なお，記憶領域または識別子は処理内容に直接含まれている場合と処理内容に含まれる情報から間接的に取得される場合がある。例えば，”read c:¥word¥test.txt HANDLE”のような処理内容があり，HANDLE が読み先のメモリ領域を示す情報である場合，HANDLE から読み込み先のプロセスを特定する。あるいは処理命令の指示元のプロセスを読み込み先としてもよい。」と

の記載がある。この記載は，「指令」に関する「ファイルの入力元のアプリケーションの識別子」と「ファイルの出力先となる記憶領域」を抽出する態様として，「指令」の「処理内容」にこれらが直接含まれる態様のほか，「指令」の「処理内容」に含まれる情報からこれらを間接的に取得する態様，「指令」の「処理命令」の指示元プロセスをこれらの読み込み先とする態様があることを前提としたものとなっている。

したがって，引用発明の構成として認定した「第１の手段で取得された指令」に関する「ファイルの入力元のアプリケーションの識別子」と「ファイルの出力先となる記憶領域」は，「指令」に直接含まれるものに限定されていない。

(ｲ) 取消事由１－１に関する原告の主張は，「記憶領域または識別子」を「処理内容から」「抽出する」ことが「処理内容に直接含まれている」ものを抽出することであるという前提に立つものであるが，引用例１は上記(ｱ)のとおり，これと異なる前提に立つものである。

(ｳ) また，引用例１のファイル管理装置が処理する命令に「ファイルの送信（send）」が含まれている旨明示され，他方，変形例３の態様②を記載する前記【００７７】において「処理の内容」から「ファイルの入力元のアプリケーションの識別子」と「ファイルの出力先となる記憶領域」を抽出できる「指令」の種類が限定されることが示されているわけでもないことから，引用例１には，「ファイルに対する送信を含む処理」の「指令に関するファイルの入力元のアプリケーションの識別子とファイルの出力先となる記憶領域とに応じて，保護方法データベースによりファイルの保護方法を求め」ることが記載されている。

ウ したがって，本件審決の引用発明の認定に誤りはない。原告の主張は引用例１の記載内容を誤解したものであり，失当である。

(2) 取消事由１－２（保護方法に関する引用発明の認定の誤り）について

ア　原告は，ファイルの出力先となる記憶領域に応じた安全性が入力元のアプリケーションの識別子に応じた安全性より高い場合には入力元となるアプリケーションの識別子の安全性に対応する保護処理を行うものであることも含めて，引用発明を認定すべきである旨主張する。

イ　しかし，前記(1)アのとおり，本件審決は，引用例１の記載のうち変形例３の態様②に係る箇所の記載を踏まえて引用発明を認定したものであり，態様③を認定したものではない。態様①～③は，設定された安全性に基づく情報の保護の方法ないし程度が異なっており，態様②は，出力禁止とされていない出力先に対する出力であっても場合によっては禁止するものである。他方，態様③は，「元の保護よりも弱い保護にはしないようにする」ものとなっている。入力先の安全性よりも出力先の安全性が高い場合の処理として態様③以外の記載がないとしても，明示されなくとも，態様②において仮に入力元の安全性より出力先の安全性が同じか高い場合には処理が禁止されないようにすれば足りるのであり，この場合に何らかの保護方法を適用するか否かについて，引用例１は述べていない。態様②と情報の保護の方法ないし程度が異なる態様①や③を組み合わせなければならない理由も見当たらない。

ウ　よって，原告の主張は，本件審決を正解しないものであり，また，引用例１の記載内容を誤解した根拠のない主張であって，失当である。

(3)　取消事由２（一致点の認定の誤り及び相違点の看過）について

ア(ｱ)　本願特許の特許請求の範囲請求項１の記載によれば，本願発明の「機密識別子記憶部」については「機密事項を扱うアプリケーションを識別する機密識別子が記憶される」ものである旨が特定されているが，「機密事項を扱うアプリケーション」でない「アプリケーション」を識別する識別子を記憶しない旨を含め，どのような態様で「機密識別子」を「記憶」するかについては特定されていない。また，「機密識別子記

憶部」に係る条件判断の内容も，「機密識別子記憶部」が「機密事項を扱うアプリケーション」でない「アプリケーション」を識別する識別子を記憶しないものであることを前提としたものにはなっておらず，「機密識別子記憶部」における「機密識別子」を「記憶」する態様がどのようなものであるかを示さない文言が用いられている。「当該フックしたシステムコールを開放する」条件も，「そうでない場合」という包括的なものであり，「機密識別子」を「記憶」する態様がどのようなものであるかを示すものではない。

これらの点を踏まえれば，本願発明においては，「機密識別子記憶部」が「機密識別子」でないものを記憶しているか否かは発明の構成と無関係の事情であり，例えば，全てのアプリケーションの識別子を記憶した上で，それらのうち「機密事項を扱うアプリケーション」であるか否かを別欄で示し，「機密事項を扱うアプリケーション」として記憶された「識別子」で識別されたアプリケーションであることを条件とする態様をも含んでいるということができる。

(イ) 引用発明の「保護方法データベース」は，アプリケーションの識別子を前記「安全性」の情報とともに格納しているものであるところ，引用発明における「指令」に係るファイルの出力の「処理」を「禁止」するアプリケーション（「安全性」が最高レベルのアプリケーションすなわち最安全アプリケーション）とは，これより信頼度が相対的に低い出力先への送信処理を禁止すべきであるほどに信頼度の高いアプリケーションである。一般に，機密情報の保護を目的として，不適切な送信先への機密情報の送信処理が禁止されるところ，送信処理の禁止という技術的な観点からは，送信処理が禁止された情報と機密情報とを区別することはできない。引用発明においても，信頼度が相対的に低い出力先への送信処理を禁止すべき情報は，送信処理が禁止され

ることによって機密情報として取り扱われているのであり，このような情報を「機密情報」（機密事項）とし，これを取り扱うことが予定されている信頼度の高いアプリケーションを「機密アプリケーション」と称することに問題はない。また，このような機密情報を扱う蓋然性の高いアプリケーションは，「安全性」が最高レベルであるから，保護方法データベースにおいて最高レベルの「安全性」が対応付けられた「識別子」に基づき識別し得ることになる。

他方，上記(ア)のとおり，本願発明の「機密識別子記憶部」は，全てのアプリケーションの識別子を記憶した上で，それらのうち「機密事項を扱うアプリケーション」であるか否かを別欄で示す態様を含み，また，ここでいう「機密事項」も，「機密事項を扱うアプリケーション」により扱われることによって送信が阻止されてその漏えいが防止される事項を一般的に示すにすぎず，これと異なる技術的な定義が与えられているわけではない。

そうすると，引用発明においても，機密情報を扱う「安全性」の最高レベルが対応付けられたアプリケーション（最安全アプリケーション）の「識別子」が本願発明の「機密識別子」に相当するとともに，そのようなアプリケーションの「識別子」が記憶される「保護方法データベース」が，本願発明の「機密識別子記憶部」の上記態様に相当する。

本件審決は，引用発明の「保護方法データベース」が本願発明の「機密識別子記憶部」に相当することを認定するに当たり，引用発明の「入力元のアプリケーション」が本願発明の「機密アプリケーション」に相当するといえる旨を示しているが，これは，前記のとおり，本願発明の「機密識別子記憶部」が「機密識別子」でないものを記憶しているか否かが発明の構成と無関係の事情であることを踏まえたものであり，最安全アプリケーションでないアプリケーションを含めて本願発明の機密ア

プリケーションに相当する旨を示したものではない。すなわち，本件審決は，「識別子」が本願発明の「機密識別子」に相当する場合の引用発明の「入力元のアプリケーション」が本願発明の「機密事項を扱うアプリケーション」に相当し，引用発明の「保護方法データベース」が本願発明の「機密識別子記憶部」に相当すると認定したものであり，その認定に誤りはない。

イ　取消事由２－１（一致点の認定の誤り及び相違点Ａの看過）について

原告は，本願発明の「機密識別子記憶部」では機密アプリケーションを識別する機密識別子が記憶されるのに対し，引用発明の保護方法データベースでは非機密アプリケーションの識別子も記憶されるという相違点Ａが存在する旨主張するが，上記アのとおり，本願発明の「機密識別子記憶部」は，全てのアプリケーションの識別子を記憶した上で，それらのうち「機密事項を扱うアプリケーション」であるか否かを別欄で示す態様を含むことから，原告の主張する相違点Ａは存在しない。

したがって，原告の主張は失当である。

ウ　取消事由２－２（一致点の認定の誤り及び相違点Ｂの看過）について

(ｱ)　本件審決は，非機密アプリケーションを含めて本願発明の「機密アプリケーション」に相当するとするものではなく，本願発明が非機密アプリケーションについて何ら述べていないことに対応して，「識別子」が本願発明の「機密識別子」に相当する場合の引用発明の「入力元のアプリケーション」が本願発明の「機密事項を扱うアプリケーション」に相当する旨を述べたものであって，非機密アプリケーションについては何ら述べていない。そうである以上，引用発明の保護方法データベースが最安全アプリケーションでないアプリケーションの識別子を記憶するものであることは，本願発明との相違点となり得ない。

また，本件審決が認定した引用発明においては，「ファイルの入力元

のアプリケーションの識別子とファイルの出力先となる記憶領域とに応じて」「ファイルの出力先となる記憶領域」の「安全性」が低い場合とそうでない場合とを区別できる必要があるが，そのためには「安全性」は２段階であれば十分であり，３段階以上でなければならないものではない。すなわち，引用発明の，入力元のアプリケーションと出力先の記憶領域の安全性が，安全性“１”（高），安全性“０”（低）の２値に設定される態様においては，入力元の安全性として最高レベルが設定されたアプリケーションを「機密アプリケーション」と一意に識別できるように，アプリケーションに対して入力元の安全性を設定することが可能である。

そうすると，本願発明の機密識別子記憶部と，引用発明の保護方法データベースは，いずれも機密アプリケーションを一意に特定できるものであり，この観点から相違していることにはならない。また，引用発明において，保護方法データベースに入力元の安全性として最高レベルが設定されたアプリケーションであることは，本願発明の条件のうちの「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションである場合」に相当することになる。

本件審決は，これを踏まえて，「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションである場合に，ファイルの送信先に応じて送信を阻止するか否かを決定する制御部」を備えることを本願発明と引用発明の一致点としたものである。

(ｲ) 前記のとおり，引用発明は，安全性が３値以上の態様に限定されない。

もっとも，引用発明の安全性が３値以上の態様においては，ファイル

の送信処理が禁止される入力元のアプリケーションであるかどうかは，入力元のアプリケーションと出力先の記憶領域の安全性に基づいて相対的に決まることから，入力元の安全性として最高レベルが設定されないアプリケーションについてもファイルの送信を阻止できるように設定することは可能である。

しかし，本願発明においては，「機密識別子記憶部」が「機密識別子」でないものを記憶しているか否かは無関係の事情であり，非機密アプリケーションからの送信を一切阻止しない旨が積極的に特定されているわけではないから，非機密アプリケーションについて送信を阻止できるような設定はできないという趣旨までが含まれているわけではいない。

そうである以上，引用発明の３値以上の態様において非機密アプリケーション（最安全アプリケーションでないアプリケーション）につきファイルの送信を阻止できるように設定可能であることは，相違点看過の根拠とはならない。

(ｳ) 相違点Ｂが仮に相違点であるとしても，この点については，本件審決における相違点１の判断において事実上判断されている。

すなわち，本件審決は，引用発明の「入力元のアプリケーション」が本願発明の「機密事項を扱うアプリケーション」に相当する旨認定し，これを前提として相違点１についての判断を示したものであるが，本願発明の「アプリケーション」が「前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーション」である旨が引用発明において明示されていないことをもって相違点と考えたとしても，引用発明において，この相違点に係る送信処理を行うアプリケーションが「機密事項を扱うアプリケーション」すなわち「機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーション」であるとの構成が容易想到である旨の判断は，事実上示されている。

(4)　取消事由３（相違点の認定の誤り及び相違点に係る容易想到性判断の誤り）について

ア　相違点の認定の誤りについて

(ｱ)　本願発明におけるファイル送信が阻止されない条件は，「そうでない場合」という包括的なもの，つまりファイル送信が阻止される条件以外の全ての場合であって，ファイル送信が阻止される条件に応じて反射的必然的に決定されるものである。

　この点，原告は，「送信が阻止されない条件」は「アプリケーションの識別子が機密識別子記憶部で記憶されていないこと，又は，送信先がローカルであること」である旨主張するが，特許請求の範囲の記載によれば，「送信が阻止されない条件」は「そうでない場合」，つまり，送信が阻止される場合でない場合であって，原告主張のような限定的な特定はされていない。

(ｲ)　前記のとおり，引用発明は，引用例１の変形例３の態様②に係る記載を踏まえ，「ファイルの出力先となる記憶領域の安全性が低い場合」に「処理を禁止する」ものであるから，明示するまでもなく，それ以外の場合，すなわちファイルの出力先となる記憶領域の安全性が低い場合以外の場合には処理を禁止しないのであり，「処理」が「禁止」されないのは「ファイルの出力先となる記憶領域の安全性が低い場合」以外の場合となる。

(ｳ)　このように，ファイル送信が阻止される場合（ファイルの入力元のアプリケーションと出力先の記憶領域が所定の組合せである場合）でない場合という条件においては，本願発明と引用発明は相違せず，この条件は一致点となる。

(ｴ)　本件審決は，以上の対比の趣旨を踏まえて，本願発明における「ファイル送信が阻止される条件」を構成する２つの部分条件のうち「前

記アプリケーションが，（前記機密識別子記憶部で記憶されている）機密識別子で識別されるアプリケーションである場合」という部分条件については一致点とし，「送信先がローカル以外である場合」という部分条件との論理積条件となっている点については相違点（相違点１）と整理し，その際，「実行部がアプリケーションを実行中にファイルに対する送信処理に係るシステムコールを検知し，当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションである場合に，ファイルの送信先に応じて送信を阻止するか否かを決定する制御部」を本願発明と引用発明との一致点として認定したのであり，この認定に誤りはない。

(ｵ)　本願発明における送信が阻止されない条件のような反射的必然的に決定される条件が結果的にどのような条件と等価となっているかは，特許請求の範囲に記載されていない事項であり，発明特定事項ではない。相違点１を相違点Ｃと認定すべきとの原告の主張は，特許請求の範囲の記載を正解しないものであり，失当である。

イ　相違点に係る容易想到性判断の誤りについて

(ｱ)　原告の主張する相違点に係る容易想到性判断の誤りは，相違点Ｃの存在を前提としたものであるところ，前記のとおり，相違点Ｃを認定すべきとする原告の主張は失当である以上，ここでの原告の主張はその前提において失当である。

(ｲ)　相違点１についての容易想到性に関し

ａ　原告は，引用発明において本願発明と同様の保護処理が行われるように安全性を設定することには阻害要因があり，相違点１に係る本願発明の構成は，引用発明において当業者が適宜設計し得たものではない旨主張する。

しかし，引用例１における「入力元の安全性と出力先の安全性」

から保護方法を決定するもの（態様①～③）においては，「保護方法」は，「安全性」の具体的な数値の値ではなく「入力元の安全性」と「出力先の安全性」との関係に対応しているのであって，「出力先の安全性」に応じて「保護方法」を決定する引用例１の他の態様と異なり，「安全性」の具体的な数値の値は「保護方法」に対応しない。このため，非機密アプリケーションの安全性を機密アプリケーションの安全性よりも低く設定することは，前者に対する保護方法が後者に対するそれより厳重でなくてはならないことを意味するなどとする原告の主張は，態様①～③においては必ずしも妥当しない。原告の主張は，「出力先の安全性」に応じて「保護方法」を決定することを念頭に置いた「安全性」と「保護方法」の対応付けを根拠として「入力元」となるアプリケーションの保護方法を論ずるものであり，失当である。

b　引用発明では，取得された指令に係る入力元のアプリケーションよりも出力先の記憶領域の安全性が低い場合は処理を禁止することから，引用発明において相違点１に係る本願発明の条件を実現しようとすれば，引用発明の保護方法データベースに記憶された，機密アプリケーション（の識別子），ローカル記憶領域及びローカル以外の記憶領域の安全性について，機密アプリケーションの安全性のレベルをローカル以外の記憶領域の安全性のレベルより高く設定する必要がある。

ところで，引用発明の「保護方法データベース」は，そもそも「柔軟」なデータ保護のためのものである（引用例１の【０００８】）。これを用いてアプリケーションや記憶領域に合理的に安全性を設定することは，そもそも当業者が適宜行うことであり，引用発明において本願発明と同様の条件を実現することに何らの阻害事由もない。また，後記のとおり，情報保護の文脈における条件としての「ローカル」と「ローカル以外」との区別が周知であるということは，こ

のような区別に基づいて安全性を設定することが「合理的」であることにほかならない。

c　本件審決の認定に係る相違点１は，要するに，ファイル送信の阻止の条件について「送信先がローカル以外である場合」という部分条件を論理積条件として考慮しているか否かということであるから，この相違点１に係る本願発明の構成が引用発明に基づき容易想到であるとする根拠として考慮すべき技術内容は，「ローカル」と「ローカル以外」とが情報漏えい防止を含む情報保護の文脈における条件として区別されること，及び，引用発明において，このような区別に従った保護方法データベースの設定が可能であることである。本件審決は，このうち前者につき，「ローカル」と「ローカル以外」とが情報漏えい防止を含む情報保護の文脈における条件として区別されることが周知であることを示すに当たり，引用例２を示したものである。

d　参考文献は，拒絶理由通知に対する意見書（甲７）に答えて提示されたものであり，必ずしも本件審決の論旨に直接関係しない。

e　したがって，出力先となる記憶領域の安全性が低い場合は処理を禁止する引用発明において，上記区別を適用し，ファイル送信の阻止の条件として，アプリケーションが機密識別子記憶部に記憶されることの条件のほかに，ファイルの送信先が安全性の低い記憶領域であることに代えて，ファイルの送信先がローカル以外であることを条件とすること，すなわち相違点１に係る構成とすることは，当業者であれば適宜なし得たことである。この点に関する本件審決の判断に誤りはなく，原告の主張は失当である。

(ｳ)　相違点Ｃについての容易想到性に関し

a　上記(ｲ) a 及びｂの趣旨は，ここでも妥当する。

なお，引用発明の「保護方法データベース」を用いてアプリケー

ションや記憶領域に安全性を設定する場合の設定が「合理的」か否かについては，上記(イ) b と同様の考慮に加え，更に「入力元」が「非機密アプリケーション」である場合の設定についても考慮する必要があるが，この場合とは，いわば機密情報を考慮する必要がない場合であるから，「安全性」の設定の仕方は機密情報の保護と関係がなく，阻害事由とはなり得ない。

b　仮に相違点Cを前提とした場合，情報保護の文脈における条件としての「ローカル」と「ローカル以外」との区別が周知である旨だけでなく，機密事項に該当しないデータの送信処理については，送信先がローカル以外であっても送信を阻止しない点も周知である旨認定する必要があるところ，本件審決は，この認定を明示的には行っていない点で，不適切なところがあることになる。

もっとも，そもそも機密事項に該当しないデータの送信処理を許可すべきことは言わずもがなのことであるし，データの保護を課題とする情報セキュリティの技術分野において，情報漏えい防止のために，機密事項に係るデータの送信処理については，送信先がローカルであれば送信を許可し，ローカル以外であれば送信を阻止するとともに，機密事項に該当しないデータの送信処理については，送信先がローカル以外であっても送信を阻止しない旨の技術自体が周知である。また，引用発明において，本願発明と同様の条件を実現することは設計事項であって，何らの阻害事由もないことは前記 a （上記(イ) b ）のとおりであり，このような周知技術に倣って，引用発明において「ローカル」と「ローカル以外」とを区別しつつ，非機密アプリケーションの送信について送信先がローカル以外であっても送信を阻止しないように設定することは，容易想到である。

このように，仮に相違点Cを前提としても，結論において本件審

決に誤りはない。

第４　当裁判所の判断

１　本願発明

(1)　本願発明は，前記第２の２記載のとおりである。

(2)　本願明細書には，以下の記載がある。

ア　技術分野

「【０００１】

本発明は，アプリケーションにおける送信の制御を行う機密管理装置等に関する。」

イ　背景技術

「【０００２】

従来，情報処理装置や情報処理システムにおいて，不正行為から装置やシステム，データを保護する技術が知られている…。」

ウ　発明が解決しようとする課題

「【０００４】

しかしながら，そのような不正行為からの保護を行う装置等において，すべてのアプリケーションに関して同じ保護を行うと，安全性は高くなるが，利便性が低下するという問題が生じる。例えば，情報の漏洩を防止するために，すべてのアプリケーションに関して送信を制限すると，情報の漏洩を防止できたとしても，ユーザの利便性は著しく低下することになる。

【０００５】

本発明は，上記課題を解決するためになされたものであり，安全性を維持しながら，利便性も確保することができる機密管理装置等を提供することを目的とする。」

エ　課題を解決するための手段

「【０００６】

上記目的を達成するため，本発明による機密管理装置は，機密事項を扱うアプリケーションを識別する機密識別子が記憶される機密識別子記憶部と，機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションを実行部が実行中に，実行部が送信を行う場合であって，送信先がローカル以外である場合に，送信を阻止するように制御する送信制御部と，を備えたものである。

【０００７】

このような構成により，機密識別子によって識別されるアプリケーションにおいて，送信先がローカル以外である場合の送信が阻止されることになり，機密事項を含むファイル等が送信によって漏洩することを防止することができ，安全性が維持されることになる。一方，機密識別子で識別されるアプリケーション以外のアプリケーションについては，自由に送信をすることができ，ユーザの利便性も確保することができる。」

オ　発明の効果

「【００１０】

本発明による機密管理装置等によれば，アプリケーションに応じて送信を制御することができ，安全性の維持と，利便性の確保とを実現することができる。」

カ　発明を実施するための形態

「【００２０】

機密管理装置２は，機密識別子記憶部２１と，送信制御部２２とを備える。

機密識別子記憶部２１では，一または二以上の機密識別子が記憶される。機密識別子は，機密事項を扱うアプリケーションを識別する情報である。機密識別子は，アプリケーションを識別できる情報であれば，そ

の内容を問わない。例えば，機密識別子は，アプリケーションの名称や，アプリケーションのＩＤ等であってもよい。また，この機密識別子記憶部２１で記憶されている機密識別子で識別されるアプリケーションは，後述するように，そのアプリケーションにおける送信が制限されるアプリケーションとなる。したがって，機密事項を扱うと考えられるアプリケーションを識別する機密識別子を，機密識別子記憶部２１に蓄積しておくことになる。

【００２２】

送信制御部２２は，機密識別子記憶部２１で記憶されている機密識別子で識別されるアプリケーション（…「機密アプリケーション」…）を実行部１４が実行中に，実行部１４が送信を行う場合であって，送信先がローカル以外である場合に，送信を阻止するように制御する。機密アプリケーションの実行中に実行部１４が行う送信とは，その機密アプリケーションにおける送信である。例えば，機密アプリケーションにおけるデータやファイル等の送信であってもよい。ローカルの送信先とは，情報処理装置３と同じローカルのネットワークに属する送信先である。…ローカルでない送信先は，グローバルなネットワークに属する送信先であってもよく，情報処理装置３とは異なるローカルのネットワークに属する送信先であってもよい。なお，送信制御部２２は，結果として，機密アプリケーションにおいて，ローカル以外の送信先への送信を阻止するように制御できるのであれば，その阻止の方法は問わない。…

【００２３】

送信を阻止するように制御するとは，結果としてその送信が行われないようにすることであれば，その方法を問わない。例えば，送信制御部２２は，機密アプリケーションからＯＳに渡されるシステムコールをフックし，送信阻止の対象でないシステムコールであれば，そのフックし

たシステムコールを開放して送信が行われるようにし，一方，送信阻止の対象となるシステムコールであれば，そのフックしたシステムコールを破棄して送信を阻止してもよい。…

【００３４】

まず，ユーザが，アプリケーション「フォトビュアーＡＡＡ」を起動し，そのアプリケーションでファイル「ｐｈｏｔｏ２００９」をオープンする指示を出したとする。すると，…その指示に応じて，…その実行中のアプリケーション「フォトビュアーＡＡＡ」において，ファイル記憶部１１で記憶されているファイル「ｐｈｏｔｏ２００９」をオープンする処理を行う。その後，ユーザが，そのファイル「ｐｈｏｔｏ２００９」に含まれる写真を選択し，写真共有サイトのサーバに送信するためのボタンを選択する操作を行ったとする。すると，その操作に応じて実行部１４は，選択された写真のデータをあらかじめ設定されているドメイン名のサイトに送信する処理を行う。そして，送信制御部２２は，システムコールの監視において，その写真のデータの送信に対応するシステムコールをフックし，そのアプリケーションの名称「フォトビュアーＡＡＡ」と，送信先のドメイン名「ｐｈｏｔｏｓｈａｒｉｎｇ…ｃｏｍ」を取得する（ステップＳ１０１）。また，送信制御部２２は，その取得したアプリケーションの名称が，図３で示される機密識別子に含まれるかどうか判断する。この場合には，含まれなかったとする。すると，送信制御部２２は，送信を行ったアプリケーションが機密アプリケーションでないと判断し（ステップＳ１０２），そのフックしたシステムコールを開放する。その結果，その写真のデータが送信部１６によって写真共有サイトのサーバに送信されることになる。

【００３５】

次に，ユーザが，アプリケーション「会計ソフトＤＤＤ」を起動する

操作を行ったとする。すると，その操作に応じて実行部１４は，アプリケーションを起動する。そして，ユーザが，アプリケーション「会計ソフトＤＤＤ」において，新規ファイルを作成する操作を行い，その後にそのファイル「ｄａｔａ２０１０」を保存する操作を行ったとする。すると，その操作に応じて，実行部１４は，ファイル「ｄａｔａ２０１０」をファイル記憶部１１に蓄積する処理を行う。また，ユーザは，そのファイル「ｄａｔａ２０１０」をファイルサーバに送信するためのボタンを選択する操作を行ったとする。すると，その操作に応じて実行部１４は，そのファイルをあらかじめ設定されているドメイン名のサイトに送信する処理を行う。そして，送信制御部２２は，システムコールの監視において，そのファイルの送信に対応するシステムコールをフックし，そのアプリケーションの名称「会計ソフトＤＤＤ」と，送信先のドメイン名「ａｃｃｏｕｎｔｉｎｇ…ｃｏｍ」を取得する（ステップＳ１０１）。また，送信制御部２２は，その取得したアプリケーションの名称が，図３で示される機密識別子に含まれるかどうか判断する。この場合には含まれるため，送信制御部２２は，ファイルを送信するアプリケーションが機密アプリケーションであると判断する（ステップＳ１０２）。また，送信制御部２２は，その取得したドメイン名が，記憶されているドメイン名「ａｂｃ…ｃｏｍ」と異なるため，送信先がローカル以外であると判断する（ステップＳ１０３）。そのため，送信制御部２２は，そのフックしたシステムコールを破棄することによって，その送信を阻止する（ステップＳ１０４）。その結果，ファイル「ｄａｔａ２０１０」の送信は行われないことになる。

【００３６】

なお，そのアプリケーション「会計ソフトＤＤＤ」における送信において，送信先のドメイン名が「ａｂｃ…ｃｏｍ」である場合には，送信制

御部２２は，そのドメイン名が記憶されているものと同じであるため，送信先がローカルであると判断する（ステップＳ１０３）。その結果，ローカルの送信先への送信が行われることになる。

(3)　本願発明の特徴

ア　技術分野

本発明は，アプリケーションにおける送信の制御を行う機密管理装置等に関する。（【０００１】）

イ　本願発明が解決しようとする課題

従来，情報処理装置や情報処理システムにおいて，不正行為から装置やシステム，データを保護する技術が知られている。しかし，そのような不正行為からの保護を行う装置等において，全てのアプリケーションに関して同じ保護を行うと，安全性は高くなるが，利便性が低下するという問題が生じる。例えば，情報の漏洩を防止するために，全てのアプリケーションに関して送信を制限すると，情報の漏洩を防止できたとしても，ユーザの利便性は著しく低下することになる。（【０００２】，【０００４】）

本願発明は，上記課題を解決するためになされたものであり，安全性を維持しながら，利便性も確保することができる機密管理装置等を提供することを目的とする。（【０００５】）

ウ　課題解決手段

上記目的を達成するため，本願発明による機密管理装置は，機密事項を扱うアプリケーションを識別する機密識別子が記憶される機密識別子記憶部と，機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションを実行部が実行中に，実行部が送信を行う場合であって，送信先がローカル以外である場合に，送信を阻止するように制御する送信制御部と，を備えたものである。（【０００６】）

エ　効果

上記の構成により，機密識別子によって識別されるアプリケーション（機密アプリケーション）において，送信先がローカル以外である場合の送信が阻止されることになり，機密事項を含むファイル等が送信によって漏洩することを防止することができ，安全性が維持されることになる。一方，機密アプリケーション以外のアプリケーションについては，自由に送信をすることができ，ユーザの利便性も確保することができる。（【０００７】，【００１０】）

オ　実施の形態

(ｱ)　機密管理装置２は，機密識別子記憶部２１と，送信制御部２２とを備える。（【００２０】）

(ｲ)　機密識別子記憶部２１では，機密識別子が記憶される。

機密識別子は，機密事項を扱うアプリケーションを識別する情報である。機密識別子は，アプリケーションを識別できる情報であれば，その内容を問わない。例えば，機密識別子は，アプリケーションの名称や，アプリケーションのＩＤ等であってもよい。

また，この機密識別子記憶部２１で記憶されている機密アプリケーションは，後述するように，そのアプリケーションにおける送信が制限されるアプリケーションとなる。したがって，機密事項を扱うと考えられるアプリケーションを識別する機密識別子を，機密識別子記憶部２１に蓄積しておくことになる。（以上，【００２０】）

(ｳ)　送信制御部２２は，機密アプリケーションを実行部１４が実行中に，実行部１４が送信を行う場合であって，送信先がローカル以外である場合に，送信を阻止するように制御する。

機密アプリケーションの実行中に実行部１４が行う送信とは，その機密アプリケーションにおける送信である。例えば，機密アプリケーショ

ンにおけるデータやファイル等の送信であってもよい。

ローカルの送信先とは，情報処理装置３と同じローカルのネットワークに属する送信先である。（以上，【００２２】）

送信を阻止するように制御するとは，結果としてその送信が行われないようにすることであれば，その方法を問わない。例えば，送信制御部２２は，機密アプリケーションからＯＳに渡されるシステムコールをフックし，送信阻止の対象でないシステムコールであれば，そのフックしたシステムコールを開放して送信が行われるようにし，一方，送信阻止の対象となるシステムコールであれば，そのフックしたシステムコールを破棄して送信を阻止してもよい。（【００２３】）

(エ) 具体例

ａ　ユーザが，アプリケーション「フォトビュアーＡＡＡ」を起動し，写真を選択し，写真共有サイトのサーバに送信するためのボタンを選択する操作を行うと，その操作に応じて実行部１４は，選択された写真のデータをあらかじめ設定されているドメイン名のサイトに送信する処理を行う。

送信制御部２２は，システムコールの監視において，その写真のデータの送信に対応するシステムコールをフックし，そのアプリケーションの名称「フォトビュアーＡＡＡ」と，送信先のドメイン名「ｐｈｏｔｏｓｈａｒｉｎｇ…ｃｏｍ」を取得する。また，送信制御部２２は，その取得したアプリケーションの名称が，機密識別子に含まれるかどうか判断する。この場合には，含まれなかったとする。すると，送信制御部２２は，送信を行ったアプリケーションが機密アプリケーションでないと判断し，そのフックしたシステムコールを開放する。

その結果，その写真のデータが送信部１６によって写真共有サイトのサーバに送信されることになる。（以上，【００３４】）

ｂ　ユーザが，アプリケーション「会計ソフトＤＤＤ」を起動し，同アプリケーションにより作成，保存したファイル「ｄａｔａ２０１０」をファイルサーバに送信するためのボタンを選択する操作を行ったとする。すると，その操作に応じて実行部１４は，そのファイルをあらかじめ設定されているドメイン名のサイトに送信する処理を行う。

送信制御部２２は，システムコールの監視において，そのファイルの送信に対応するシステムコールをフックし，そのアプリケーションの名称「会計ソフトＤＤＤ」と，送信先のドメイン名「ａｃｃｏｕｎｔｉｎｇ…ｃｏｍ」を取得する。また，送信制御部２２は，その取得したアプリケーションの名称が機密識別子に含まれるかどうか判断する。この場合には含まれるため，送信制御部２２は，ファイルを送信するアプリケーションが機密アプリケーションであると判断する。さらに，送信制御部２２は，その取得したドメイン名が，記憶されているドメイン名「ａｂｃ…ｃｏｍ」と異なるため，送信先がローカル以外であると判断する。そのため，送信制御部２２は，そのフックしたシステムコールを破棄することによって，その送信を阻止する（ステップＳ１０４）。

その結果，ファイル「ｄａｔａ２０１０」の送信は行われないことになる。（以上，【００３５】）

他方，「会計ソフトＤＤＤ」における送信において，送信先のドメイン名が「ａｂｃ…ｃｏｍ」である場合には，送信制御部２２は，そのドメイン名が記憶されているものと同じであるため，送信先がローカルであると判断する。その結果，ローカルの送信先への送信が行われることになる。（【００３６】）

２　取消事由１（引用発明の認定の誤り）について

(1)　引用発明

引用例１には，以下の記載がある。

ア　技術分野

「【０００１】

本発明は，ファイル管理プログラム及びファイル管理装置に関する。」

イ　背景技術

「【０００２】

コンピュータシステムにおいてデータを保護するための技術が知られている。

【０００３】

例えば，保護対象となるリソースに対してアクセス可能なプログラムの識別情報をアクセス許可管理テーブルに登録しておき，保護対象となるリソースに対するアクセス要求があると，アクセス要求したプログラムの識別情報を取得してアクセス許可管理テーブルにその識別情報が登録されているか否かにより，リソースへのアクセスの許否を判定する技術が開示されている…。

【０００４】

また，保護領域にアプリケーションがアクセスするとアプリケーションの識別情報を取得し，識別情報がテーブルに登録されているか否かを判定し，登録されていなければアクセスを許可し，テーブルに識別情報が登録されていればアクセス先を検出し，アクセス先が保護領域であればアクセスを許可し，保護領域でなければアクセスを禁止する技術が開示されている…。

【０００５】

また，ハードディスク等のデバイスドライバを制御するための制御関数を取得し，暗号領域内の暗号化ファイルが非暗号領域への移動又は複製されることを検知すると制御関数を用いて暗号化ファイルを開き，制

御関数を用いてオープンした暗号化ファイルを読み出して復号し，移動先又は複製先にて制御関数を用いて復号化されたファイルを書き込む技術が開示されている…。」

ウ　発明が解決しようとする課題

「【０００７】

ファイルやリソースへのアクセスの許可・不許可を行うことによりデータを保護する方法やデータの暗号化・復号化を行うことによりデータを保護する方法は知られている。

【０００８】

しかしながら，オペレーションシステム（ＯＳ）に対する処理要求の内容に応じてデータの保護方法を変更する技術は知られていない。したがって，データの取得先や出力先に応じてデータの保護方法を変更したり，データを使用するアプリケーション毎にデータの保護方法を変更したりして，柔軟にデータを保護することができなかった。」

エ　課題を解決するための手段

「【０００９】

本発明の１つは，コンピュータに，処理対象となるデータに対する処理の指令を取得する第１のステップと，前記第１のステップで取得された指令で特定される処理の内容に応じて前記処理の内容に応じたデータの保護方法を求め，その保護方法により前記処理対象となるデータの保護処理を行う第２のステップと，を含む処理を実行させることを特徴とするファイル管理プログラムである。

【００１０】

また，本発明の１つは，処理対象となるデータに対する処理の指令を取得する第１の手段と，前記第１の手段で取得された指令で特定される処理の内容に応じて前記処理の内容に応じたデータの保護方法を求め，

その保護方法により前記処理対象となるデータの保護処理を行う第２の手段と，…を備えることを特徴とするファイル管理装置である。

【００１２】

また，前記第２のステップ又は手段は，前記第１のステップ又は手段で取得された指令で特定される処理におけるデータの取得元又は出力先に応じてデータの保護方法を求め，その保護方法により前記処理対象となるデータの保護処理を行うものとしてもよい。

【００１４】

また，前記第１のステップ又は手段で取得された指令に関するアプリケーション又は前記第１のステップ又は手段で取得された命令の入力手段と，前記処理対象となるデータに対する処理を行うオペレーションシステムと，の間において前記第１のステップ又は手段及び前記第２のステップ又は手段を行うものとしてもよい。

【００１５】

また，前記第２のステップ又は手段は，前記第１のステップ又は手段で取得された指令で特定される処理に応じて，前記処理対象となるデータ処理の前又は前記処理対象となるデータ処理の後を切り替えて前記処理対象となるデータの保護処理を行うものとしてもよい。」

オ　発明の効果

「【００１６】

請求項１及び７の発明によれば，データの処理の内容に応じた保護方法でデータを保護することができる。

【００１８】

請求項３の発明によれば，処理対象となるデータの取得元，出力先等となる処理のアクセス先に応じた保護方法でデータを保護することができる。

【００２０】

請求項５の発明によれば，従来から使用してきたオペレーションシステム及びオペレーションシステム上で動作するアプリケーションを変更することなく柔軟にデータを保護することができる。

【００２１】

請求項６の発明によれば，処理の内容に応じて，データに対する処理の前又はデータに対する処理の後の適切なタイミングでデータに保護を施すことができる。」

カ　発明を実施するための最良の形態

「【００２２】

本発明の実施の形態におけるファイル管理装置１００は，…中央処理部１０，記憶部１２，入力部１４，表示部１６及びインターフェース部１８を含んで構成される。これらの構成部は，バスやネットワーク等の情報伝達手段によって相互に情報伝達可能に接続される。

【００２９】

ファイル管理装置１００は，…ファイル操作命令手段２０，アプリケーション処理手段２２，ファイル操作命令取得手段２４，ファイル保護手段２６，データ位置特定手段２８，保護方法データベース記憶手段３０及びオペレーティングシステム処理手段３２を含む装置として機能する。

【００３１】

ステップＳ１０では，データ（ファイル）に対する処理を特定する命令を取得する。中央処理部１０は，データに対する処理の命令を取得する。このステップの処理がファイル操作命令取得手段２４に相当する。取得された処理内容はファイル保護手段２６へ送られる。

【００３５】

例えば，ファイルの複写（ｃｏｐｙ）の指示には，"copy

c:¥work¥test.txt c:¥share"のように複写命令のコマンド"copy"，複写元の記憶領域"c:¥work"，複写先の記憶領域"c:¥share"及びファイル名"test.txt"が含まれる。

【００３６】

また，ファイルの書き込み（ｗｒｉｔｅ）の指示には，"write data c:¥share¥test.txt"のように，書き込み命令のコマンド"write"，書き込み対象となるデータ"data"，書き込み先の記憶領域"c:¥share"及び書き込みデータのファイル名"test.txt"が含まれる。

【００３７】

また，アプリケーションからのファイルの読み出し（ｒｅａｄ）の指示には，対象となるファイルを特定する情報とアプリケーションを特定する識別子（アプリケーション名，プロセス名等）とが含まれる。具体的には，"read c:¥work¥test.txt ‘Mail Tool’"のように，読み出し命令のコマンド"read"，処理対象となるファイルの記憶領域"c:¥work"，電子メールとして処理することを示す"Mail Tool"及びファイル名"test.txt"が含まれる。また，"read c:¥work¥test.txt ‘文書 Viewer’"のように，電子メールとして処理することを示す"Mail Tool"の代りに，ファイルの内容を表示してユーザに呈示する"文書 Viewer"を指定したり，プリンタによる画像形成をするためにプリンタ"printer A"を指定したりしてもよい。

【００３８】

ステップＳ１２では，処理内容から出力先の記憶領域または識別子を抽出する。ここでの処理はファイル保護手段２６及びデータ位置特定手段２８に相当する。なお，記憶領域または識別子は処理内容に直接含まれている場合と処理内容に含まれる情報から間接的に取得される場合がある。例えば，"read c:¥work¥test.txt HANDLE"のような処理内容があり，HANDLE が読み先のメモリ領域を示す情報である場合，HANDLE から読

み込み先のプロセスを特定する。あるいは処理命令の指示元のプロセスを読み込み先としてもよい。

【００４０】

ステップＳ１４では，処理内容に応じたデータ（ファイル）の保護方法を決定する。中央処理部１０は，記憶部１２に予め格納されている保護方法データベースを参照し，ステップＳ１０で取得した処理内容に応じてデータ（ファイル）の保護方法を決定する。ここでの処理はファイル保護手段２６及び保護方法データベース記憶手段３０に相当する。

【００４１】

保護方法データベースは，記憶領域又はアプリケーションを特定する識別子に保護方法を関連付けたデータベースである。保護方法データベースが格納及び保持された記憶部１０が保護方法データベース記憶手段３０に相当する。

【００４２】

例えば，図４に例示するように，記憶領域"c:¥share"に安全性"1"，記憶領域"c:¥Documents and Setting¥userA¥desktop"に安全性"2"，記憶領域"¥¥server1¥confidential"に安全性"3"，記憶領域"ごみ箱"に安全性"1"が関連付けられる。また，アプリケーションを特定する識別子"文書 viewer"に安全性"3"，識別子"Mail Tool"に安全性"1"，識別子"printer A"に安全性"2"，識別子"printer B"に安全性"1"が関連付けられる。

【００４３】

ここで，図５に例示するように，安全性"0"とはファイル操作禁止による保護を意味し，安全性"1"はＤＲＭ(Digital Rights Management)による保護を意味し，安全性"2"はファイル操作の履歴（ログ）の保存を意味し，安全性"3"は平文による処理（ＯＳによる通常のファイル操作）を許可することを意味する。

【００４４】

ここで，安全性は 0～3 としたが，これらは保護の安全性の順序やレベルを示す必要はなく，処理対象となるデータ（ファイル）にどのような保護を適用するか特定できるものであればよい。

【００４７】

ステップＳ１６では，処理内容毎に，処理前（オペレーションシステムに渡す前）にデータ（ファイル）に保護を施すか，処理後（オペレーションシステムから戻ってきた後）にデータ（ファイル）に保護を施すかを判断する。

【００４８】

データ（ファイル）に保護を施すタイミングは，処理の内容に応じて変更される。図６に例示するように，...ファイルの書き込み（ｗｒｉｔｅ），ファイルの送信（ｓｅｎｄ）については，データ（ファイル）に対する処理前に保護を施す。この場合，ステップＳ１８に処理を移行させる。一方，データ（ファイル）に対する処理が...ファイルの読み出し（ｒｅａｄ）...については，データ（ファイル）に対する処理後に保護を施す。この場合，ステップＳ２０に処理を移行させる。

【００４９】

ステップＳ１８では，決定された保護方法でデータ（ファイル）に保護を施す。中央処理部１０は，ステップＳ１０で指定されたデータ（ファイル）に対して取得して処理命令で特定される処理を施す前にステップＳ１４で決定した保護方法を施す。ここでの処理は，ファイル保護手段２６及びオペレーティングシステム処理手段３２で行われる。

【００５０】

例えば，ファイルの書き込み（ｗｒｉｔｅ）の指示として"write data c:¥share¥test.txt"という処理内容が取得された場合，ファイルに対する書

き込み処理前に保護処理を施す。中央処理部１０は，取得したファイルに対して保護を施した後，オペレーションシステムに書き込み対象となるデータ"data"を渡し，書き込み先の記憶領域"c:¥share"にファイル名"test.txt"としてデータ"data"を格納する。図４の保護方法データベースの例では書き込み先の記憶領域"c:¥share"は安全性"1"に指定されているので，オペレーションシステムにファイルを引き渡す前にデータ"data"にDRMによる保護を施す。

【００５３】

…送信（ｓｅｎｄ）についても同様にファイル操作前に保護を施す。

【００５６】

また，アプリケーションからのファイルの読み出し（ｒｅａｄ）の指示として"read c:¥work¥test.txt ‘Mail Tool’"という処理内容が取得された場合，ファイルに対する読み出し処理後に保護処理を施す。中央処理部１０は，対象となるファイルの記憶領域"c:¥work"からファイル名"test.txt"で特定されるファイルを読み出し，そのファイルに保護を施した後，電子メールのメールツールである"Mail Tool"へファイルの出力を行う。保護方法データベースでは，読み出し先のプロセス"Mail Tool"は安全性"1"に指定されているので，読み出し処理後にプロセス"Mail Tool"に出力される前にファイル名"test.txt"のファイルにDRMによる保護を施す。

【００５７】

同様に，"read c:¥work¥test.txt ‘文書 Viewer’"のようにファイルの内容を表示してユーザに呈示する"文書 Viewer"が指定された場合，ファイルに対する読み出し処理後に保護処理を施す。中央処理部１０はオペレーションシステムを呼び出し，処理対象となるファイルの記憶領域" c:¥work"からファイル名"test.txt"で特定されるファイルを読み出し，文書ビューアであるアプリケーションにファイルの出力を行う。保護方法データベースで

は，読み出し先のプロセス"文書Viewer"は安全性"3"に指定されているので，読み出し処理後にファイル名"test.txt"のファイルが平文であればそのまま文書ビューアであるアプリケーションにファイルを出力する。一方，ファイル名"test.txt"のファイルが平文でなければ，ファイルを平文に戻す処理を施して文書ビューアであるアプリケーションにファイルを出力する。【００７７】

＜変形例３＞

上記の実施の形態では，出力先の安全性に応じて保護方法を決定したが，処理内容から入力元の記憶領域または識別子と出力先の記憶領域または識別子とを抽出し，入力元の安全性と出力先の安全性から，処理方法を決定するようにしてもよい。例えば，図４の保護方法データベースを持つ時に"copy c:¥share¥doc1.txt c:¥share¥doc2.txt" という処理内容を実行する場合，入力元と出力先は同じ安全性なので，再度保護処理を行わずそのままファイルの複写を行うようにしてもよい。また，入力元よりも出力先の安全性が低い場合は処理を禁止するようにしてもよいし，逆に入力元よりも出力先の安全性が高い場合には入力元の安全性に従った保護処理を施し元の保護よりも弱い保護にはしないようにしてもよい。」

(2) 引用発明の特徴

ア 技術分野

引用発明は，ファイル管理プログラム及びファイル管理装置に関する。（【０００１】）

イ 引用発明が解決しようとする課題

従来より，コンピュータシステムにおいてデータを保護するための技術として，ファイルやリソースへのアクセスの許可・不許可を行うことによりデータを保護する方法やデータの暗号化・復号化を行うことによりデータを保護する方法は知られている。（【０００２】，【０００

７】）

しかし，オペレーションシステム（ＯＳ）に対する処理要求の内容に応じてデータの保護方法を変更する技術は知られておらず，データの取得先や出力先に応じてデータの保護方法を変更したり，データを使用するアプリケーション毎にデータの保護方法を変更したりして，柔軟にデータを保護することができなかった。（【０００８】）

ウ　課題解決手段

引用発明は，処理対象となるデータに対する処理の指令を取得する第１の手段と，前記第１の手段で取得された指令で特定される処理の内容に応じて前記処理の内容に応じたデータの保護方法を求め，その保護方法により前記処理対象となるデータの保護処理を行う第２の手段とを備えるファイル管理装置であって，（【００１０】）

前記第２の手段は，前記第１の手段で取得された指令で特定される処理におけるデータの取得元及び出力先の安全性に応じて，入力元よりも出力先の安全性が低い場合は処理を禁止するようにデータの保護方法を求め，（【００１２】，【００７７】）

前記第２の手段は，前記第１の手段で取得された指令で特定される処理に応じて，前記処理対象となるデータ処理の前又は前記処理対象となるデータ処理の後を切り替えて前記処理対象となるデータの保護処理を行うものである。（【００１５】）

エ　効果

引用発明によれば，データの処理の内容に応じた保護方法，特に，処理対象となるデータの取得元，出力先等となる処理のアクセス先に応じた保護方法でデータを保護することができ（【００１６】，【００１８】），処理の内容に応じて，データに対する処理の前又はデータに対する処理の後の適切なタイミングでデータに保護を施すことができる。

（【００２１】）

オ　実施の形態（変形例３）

ファイル管理装置１００は，ファイル操作命令手段２０，アプリケーション処理手段２２，ファイル操作命令取得手段２４，ファイル保護手段２６，データ位置特定手段２８，保護方法データベース記憶手段３０及びオペレーティングシステム処理手段３２を含む装置として機能する。（【００２９】）

ステップＳ１０（ファイル操作命令取得手段２４に相当）では，中央処理部１０は，データ（ファイル）に対する処理を特定する命令を取得する。取得された処理内容はファイル保護手段２６へ送られる。（【００３１】）

ステップＳ１２（ファイル保護手段２６及びデータ位置特定手段２８に相当）では，処理命令の指示元のプロセスを読み込み先とし，又は，処理内容から入力元の記憶領域若しくは識別子を抽出し，かつ，処理内容から出力先の記憶領域または識別子を抽出する。なお，記憶領域または識別子は処理内容に直接含まれている場合と処理内容に含まれる情報から間接的に取得される場合がある。（【００３８】，【００７７】）

ステップＳ１４（ファイル保護手段２６及び保護方法データベース記憶手段３０に相当）では，中央処理部１０は，記憶部１２に予め格納されている保護方法データベースを参照し，入力元よりも出力先の安全性が低い場合は処理を禁止するように，処理内容に応じたデータ（ファイル）の保護方法を決定する。（【００４０】，【００７７】）

保護方法データベースは，記憶領域又はアプリケーションを特定する識別子に安全性を関連付けたデータベースである。保護方法データベースが格納及び保持された記憶部１０が保護方法データベース記憶手段３０に相当する。（【００４１】～【００４４】，【００７７】）

ステップＳ１６では，処理内容毎に，処理前（オペレーションシステムに渡す前）にデータ（ファイル）に保護を施すか，処理後（オペレーションシステムから戻ってきた後）にデータ（ファイル）に保護を施すかを判断する。ファイルの送信（ｓｅｎｄ）については，データ（ファイル）に対する処理前に保護を施す。この場合，ステップＳ１８に処理を移行させる。（【００４７】，【００４８】）

ステップＳ１８では，決定された保護方法でデータ（ファイル）に保護を施す。中央処理部１０は，ステップＳ１０で指定されたデータ（ファイル）に対して取得して処理命令で特定される処理を施す前にステップＳ１４で決定した保護方法を施す。ここでの処理は，ファイル保護手段２６及びオペレーティングシステム処理手段３２で行われる。（【００４９】）

(3) 取消事由１－１（送信の指令に関する引用発明の認定の誤り）について

ア 原告は，引用発明においては，取得されたファイルの送信の指令から入力元のアプリケーションの識別子を抽出することはできないところ，本件審決はその抽出ができるとした点で誤りがある旨主張する。

イ この点につき，引用発明の実施の形態である変形例３を記載した引用例１の【００７７】には，入力元のアプリケーションの識別子の取得に関して，単に「処理内容から入力元の記憶領域または識別子と出力先の記憶領域または識別子とを抽出し」との記載があるのみであり，また，処理内容の例を見ると，処理の命令が read の場合に"Mail Tool"及び"文書Viewer"というアプリケーションの識別子を出力先に指定した例が記載されているが（【００３７】，【００５６】及び【００５７】），入力元にアプリケーションの識別子を直接指定した例は見当たらない。間接的に識別子を取得する例も，前記【００３８】の HANDLE の例のみである。

これらの事情等を踏まえると，引用例１には，入力元のアプリケーシ

ョンの識別子を取得する具体的手法についての記載はなく，【００７７】に抽象的に「処理内容から入力元の…識別子…を抽出し」と記載されているにとどまることになる。

しかし，他方で，引用例１には，入力元にアプリケーションの識別子を直接指定することができない旨，入力元に HANDLE を指定して HANDLE から入力元のアプリケーションを特定する手法を取り得ない旨，及び，処理命令の指示元のプロセスを入力元とすることができない旨についての記載もない。

加えて，引用発明が既存の特定のＯＳを前提とするものであり，当該ＯＳの仕様によって入力元のアプリケーションの識別子を取得することができないとする理由もない。そもそも，引用例１には，処理内容が特定のＯＳのシステムコール又はＡＰＩに準拠していることをうかがわせる記載はない。

さらに，処理命令の入力元をアプリケーションとすることも考えられないではなく，それが必ずしも非現実的とまではいえない。

以上より，引用例１は，入力元のアプリケーションの識別子を取得する具体的手法を明らかにはしていないものの，その取得が不可能とまでいうことはできない。

ウ　したがって，取消事由１－１は理由がない。この点に関する原告の主張は採用し得ない。

(4)　取消事由１－２（保護方法に関する引用発明の認定の誤り）について

ア　前記のとおり，変形例３には，入力元よりも出力先の安全性が低い場合には処理を禁止するように，処理内容に応じたデータ（ファイル）の保護方法を決定することが記載されている。そうである以上，本件審決が引用発明の保護方法につき「その保護方法は，ファイルの出力先となる記憶領域の安全性が低い場合は処理を禁止することを含む」と認定した

ことに誤りはない。

したがって，取消事由１－２は理由がないというべきである。

イ　これに対し，原告は，引用発明の認定は変形例３の態様②のみでなく態様③も含めて行われるべきである旨主張する。

しかし，変形例３の態様①～③は，それぞれ「してもよい」という選択肢を示す記載により結ばれており，いずれも選択的に採用され得るものにすぎないことは明らかである。また，これらの全部又は一部を組み合わせた処理方法を採用すべき旨の記載も見当たらない。

その他原告がるる指摘する点を考慮しても，この点に関する原告の主張は採用し得ないというべきである。

３　取消事由２（一致点の認定の誤り及び相違点の看過）について

(1)　取消事由２につき，原告は，本件審決の理解に応じて取消事由２－１及び２－２の２つの場合を分けて論じつつ，これらに共通する趣旨は，本件審決は，本願発明の機密識別子の作用ないし機能と引用発明の識別子の作用ないし機能が相違すること，すなわち，本願発明の「機密識別子」は「機密事項を扱うアプリケーションを識別する」ものであるのに対し，引用発明における「アプリケーションの識別子」は必ずしも機密事項を扱うアプリケーションを識別するものではなく，ファイルの保護方法を求める上で必要となる安全性の程度（例えば，数値）を得る前提として，入力元のアプリケーションを識別するものであることを看過したというものである旨主張する。

そこで，以下では，上記相違点に係る取消事由を取消事由２－１及び２－２を包摂するものとして「取消事由２」とし，その理由の有無について検討する。

(2)ア　本件審決は，「保護方法データベース」に記憶された「入力元のアプリケーション」が保護対象データである「ファイル」を処理するのは自明であり，機密事項を保護対象データとして扱うことは当該技術分野の技術

常識であることから，引用発明の「入力元のアプリケーション」，「識別子」はそれぞれ，本願発明の「機密事項を扱うアプリケーション」，「機密識別子」に相当し，また，引用発明の「保護方法データベース」に「入力元のアプリケーション」の「識別子」が記憶されていることは明らかであるから，引用発明の「保護方法データベース」は本願発明の「機密事項を扱うアプリケーションを識別する機密識別子が記憶される機密識別子記憶部」に相当する旨認定・判断した。

イ(ｱ)　しかし，前記認定に係る本願明細書及び引用例１の記載によれば，本願発明における「機密識別子」は「機密事項を扱うアプリケーションを識別する」ものとして定義されている（本願明細書【０００６】等）のに対し，引用発明におけるアプリケーションの「識別子」は，アプリケーションを特定する要素（アプリケーション名，プロセス名等）として位置付けられるものであって（引用例１【００３７】等），必ずしも直接的ないし一次的に機密事項を扱うアプリケーションを識別するものとはされていない。

(ｲ)　また，本願発明は，「すべてのアプリケーションに関して同じ保護を行うと，安全性は高くなるが，利便性が低下するという問題が生じる」（本願明細書【０００４】）という課題を解決するために，「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合に」「送信を阻止」するという構成を採用したものである。このような構成を採用することによって，「機密事項を含むファイル等が送信によって漏洩することを防止することができ」，かつ，「機密識別子で識別されるアプリケーション以外のアプリケーションについては，自由に送信をすることができ，ユーザの利便性も確保することができる」という効果が奏せられ（本願明細書【０００７】），前

記課題が解決され得る。このことに鑑みると，本願発明の根幹をなす技術的思想は，アプリケーションが機密事項を扱うか否かによって送信の可否を異にすることにあるといってよい。

他方，引用発明において，アプリケーションは，機密事項を扱うか否かによって区別されていない。すなわち，そもそも，引用例１には機密事項の保護という観点からの記載が存在しない。また，引用発明は，柔軟なデータ保護をその解決すべき課題とするところ（【０００８】），保護対象とされるデータの保護されるべき理由は機密性のほかにも考え得る。このため，機密事項を保護対象データとして取り扱うことは技術常識であったとしても，引用発明における保護対象データが必ず機密事項であるとは限らない。しかも，引用発明は，入力元のアプリケーションと出力先の記憶領域とにそれぞれ安全性を設定し，それらの安全性を比較してファイルに保護を施すか否かの判断を行うものである。このため，同じファイルであっても，入力元と出力先との安全性に応じて，保護される場合と保護されない場合とがあり得る。

これらの点に鑑みると，引用発明の技術的思想は，入力元のアプリケーションと出力先の記憶領域とにそれぞれ設定された安全性を比較することにより，ファイルを保護対象とすべきか否かの判断を相対的かつ柔軟に行うことにあると思われる。かつ，ここで，「入力元のアプリケーションの識別子」は，それ自体として直接的ないし一次的に「機密事項を扱うアプリケーション」を識別する作用ないし機能は有しておらず，上記のようにファイルの保護方法を求める上で比較のため必要となる「入力元のアプリケーション」の安全性の程度（例えば，その程度を示す数値）を得る前提として，入力元のアプリケーションを識別するものとして作用ないし機能するものと理解される。

そうすると，本願発明と引用発明とは，その技術的思想を異にするも

のというべきであり，また，本願発明の「機密識別子」は「機密事項を扱うアプリケーションを識別する」ものであるのに対し，引用発明の「アプリケーションの識別子」は必ずしも機密事項を扱うアプリケーションを識別するものではなく，ファイルの保護方法を求める上で必要となる安全性の程度（例えば，数値）を得る前提として，入力元のアプリケーションを識別するものであり，両者はその作用ないし機能を異にするものと理解するのが適当である。

(ｳ) このように，本願発明の「機密識別子」と引用発明の「識別子」が相違するものであるならば，それぞれを記憶した本願発明の「機密識別子記憶部」と引用発明の「保護方法データベース」も相違することになる。

ウ 以上より，この点に関する本件審決の前記認定・判断は，上記各相違点を看過したものというべきであり，誤りがある。

エ これに対し，被告は，引用発明における最高レベルの安全性が対応付けられたアプリケーション（最安全アプリケーション）の「識別子」が本願発明の「機密識別子」に相当する（したがって，そのようなアプリケーションの「識別子」が記憶される「保護方法データベース」が，本願発明の「機密識別子記憶部」に相当する）などと主張する。

確かに，引用発明における最安全アプリケーションは，それ未満の安全性を対応付けられた記憶領域へのファイルの送信が阻止されることから，本願発明の「機密アプリケーション」とその作用ないし機能において類似する。

しかし，これは入力元と出力先との安全性の比較という引用発明独自の保護方法を適用したことにより，結果的に類似する作用ないし機能が生じたというにすぎず，最安全アプリケーションの場合といえども，引用発明において，アプリケーションが，「機密事項を扱う」か否かの観

点からではなく，関連付けられている安全性の程度を得る観点から区別されていることに変わりはない。このことは，上記安全性の程度が２値を採るか３値以上の値を採るかにより異ならない。

また，引用発明の「入力元のアプリケーション」は機密事項を扱うか否かで区別されていない以上，その識別子が本願発明の「機密識別子」に相当することはない。そうである以上，引用発明の「入力元のアプリケーション」を最安全アプリケーションとそうでないアプリケーションとに分けて論じたところで，これによって本願発明における「機密識別子」が引用発明においても存在することが論証されるわけではないというべきである。

以上より，この点に関する被告の主張は採用し得ない。

(3)ア　そうすると，本件審決につき，引用発明の保護方法データベースに含まれる各アプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものと理解した場合（取消事由２－１の場合）は，相違点Ａ（ただし，上記(2)に鑑みると，「本願発明の機密識別子記憶部では，機密事項を扱うアプリケーションを識別する機密識別子が記憶されるのに対し，引用発明の保護方法データベースでは，アプリケーションの識別子が記憶されるものの，当該識別子によっては，当該アプリケーションが機密事項を扱うものであるか否かは特定し得ない」とするのがより正確である。）が存在するものと認められる。すなわち，本件審決は，一致点の認定を誤り，相違点Ａを看過したものというべきである。

そして，相違点Ａにつき，引用発明から本願発明の構成に至るためには，引用発明の保護方法データベースにおいて，同データベースで管理するアプリケーションの識別子を機密事項を扱うアプリケーションの識別子に限定する代わりに，同アプリケーションが扱うファイルについて

は，外部への送信等を絶対的に禁止するなど，入力元と出力先との安全性の比較の余地を排するものとする必要があることとなる。しかし，前記のとおり，引用発明の技術的思想は，入力元と出力先とにそれぞれ設定された安全性を比較することにより，ファイルを保護対象とすべきか否かの判断を相対的かつ柔軟に行うことにあるところ，上記のように引用発明の構成を変更することがその技術的思想に相反することは明らかである。その意味で，そのような構成を採ることには阻害事由がある。

そうである以上，相違点Ａにつき，引用発明から出発して本願発明の構成に至ることは容易に想到可能であるということはできない。すなわち，本件審決における一致点の認定の誤り及び相違点Ａの看過は，審決の結論に影響を及ぼすものであるから，取消事由２－１には理由がある。

イ　他方，本件審決につき，引用発明の保護方法データベースに含まれる最安全アプリケーションの識別子が，本願発明の機密識別子記憶部で記憶されている機密識別子に相当する旨認定したものと理解した場合（取消事由２－２の場合）は，相違点Ｂが存在するものと認められる。すなわち，本件審決は，一致点の認定を誤り，相違点Ｂを看過したものというべきである。

そして，相違点Ｂにつき，引用発明から本願発明の構成に至ることが引用発明の技術的思想に相反し，そのような構成を採ることに阻害事由があるため，容易に想到可能とはいえないことは，上記アと同様である。

したがって，本件審決における一致点の認定の誤り及び相違点Ｂの看過は，審決の結論に影響を及ぼすものであるから，取消事由２－２には理由がある。

なお，原告は，相違点Ｂの存在を主張するに当たり，引用発明において安全性は３段階以上存在することに言及するところ，引用発明についてのこのような理解は失当というべきである。もっとも，安全性を２段

階とすることにより引用発明のアプリケーションが機密事項を扱うか否かによる区別されるものとなるわけでないことは前記（(2)エ）のとおりであるから，この点は結論に影響しない。

ウ　以上より，本件審決につきいかに理解するのであれ，取消事由２－１及び２－２を包摂する取消事由２は理由があるということができる。

エ　これに対し，被告は，相違点ＡないしＢの看過を争うとともに，仮に相違点Ｂが存在するとしても，その点については，本件審決の相違点１に関する判断において事実上判断されている旨主張する。

このうち，相違点ＡないしＢの看過については，上記ア及びイのとおりである。

また，本件審決の判断は，①引用例２に記載されるように，ファイルを含むパケットについて，内部ネットワークから外部ネットワークへの持ち出しを判断し，送信先に応じて許可／不許可を判定すること，すなわち，内部ネットワーク（ローカル）以外への送信の安全性が低いとしてセキュリティ対策を施すことは，本願出願前には当該技術分野の周知の事項であったこと，②参考文献に記載されるように，機密ファイルをあるアプリケーションプログラムが開いた後は，電子メール等によって当該アプリケーションプログラムにより当該ファイルが機密情報保存用フォルダ（ローカル）以外に出力されることがないようにすることも，本願出願前には当該技術分野の周知技術であったことをそれぞれ踏まえて行われたものである。

しかし，①に関しては，本件審決の引用する引用例２には，送信の許可／禁止の判定は送信元及び送信先の各ＩＰアドレスに基づいて行われることが記載されており（【００３０】），アプリケーションの識別子に関する記載は見当たらない。また，前記のとおり，引用発明における識別子は，アプリケーションが機密事項を扱うものか否かを識別する作

用ないし機能を有するものではない。

②に関しては，参考文献記載の技術は，機密情報保存用フォルダ内のファイルが当該フォルダの外部に移動されることを禁止するものであるところ（【００１１】），その実施の形態として，機密情報保存用フォルダ（機密フォルダ１５Ａ）の設定につき，「システム管理者は，各ユーザが使用するコンピュータ１０内の補助記憶装置１５内に特定の機密ファイルを保存するための機密フォルダ１５Ａを設定し，ユーザが業務で使用する複数の機密ファイルを機密フォルダ１５Ａ内に保存する。」（同【００１８】）との記載はあるものの，起動されたアプリケーションプログラムが機密事項を扱うものであるか否かという点に直接的に着目し，これを識別する標識として本願発明の機密識別子に相当するものを用いることをうかがわせる記載は見当たらない（本件審決は，参考文献の記載（【０００８】，【０００９】，【００６４】）に言及するものの，そこでの着目点は機密ファイルをあるアプリケーションプログラムが開いた後の取扱いであって，その前段階として機密ファイルを定める要素ないし方法に言及するものではない。）。このように，当該周知技術においては，アプリケーションが機密事項を扱うものであるか否かを識別する機密識別子に相当するものが用いられているとはいえない。

なお，参考文献の記載（【００３２】等）によれば，アプリケーションプログラムのハンドル名がアプリケーションの識別子として作用することがうかがわれるが，参考文献記載の技術は，アプリケーションが実際に機密ファイルをオープンしたか否かによって当該アプリケーションによるファイルの外部への格納の可否が判断されるものであり，入力元と出力先との安全性の比較により処理の可否を判断する引用発明とは処理の可否の判断の原理を異にする。また，扱うファイルそのものの機密性に着目して機密ファイルを外部に出すことを阻止することを目的とす

る点で，扱うファイルそのものの機密性には着目していない引用発明とは目的をも異にする。このため，引用発明に対し参考文献記載の技術を適用することには，動機付けが存在しないというべきである。

そうすると，相違点Ｂにつき，引用発明に，引用例２に記載の上記周知の事項を適用しても，本願発明の「機密識別子」には容易に想到し得ないというべきであるし，参考文献記載の周知技術はそもそも引用発明に適用し得ないものであり，また，仮に適用し得たとしても，本願発明の「機密識別子」に想到し得るものではない。そうである以上，相違点Ｂにつき，本件審決における相違点１の判断において事実上判断されているとはいえない。

したがって，この点に関する被告の主張は採用し得ない。

４　取消事由３（相違点の認定の誤り及び相違点に係る容易想到性判断の誤り）について

(1)　上記３のとおり，本件審決は，本願発明の「機密識別子」及び「機密識別子記憶部」と引用発明の「識別子」及び「保護方法データベース」とに係る相違点を看過したものであり，この点は審決の結論に影響を及ぼす。

しかし，更に進んで，仮にこの相違点の看過がなかったとしても，本件審決は相違点Ｃを看過したものであり，この点は審決の結論に影響を及ぼすというべきである。その理由は，以下のとおりである。

(2)ア　本願発明における送信の可否の動作は，「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合に，当該フックしたシステムコールを破棄することによって当該送信を阻止し，そうでない場合に，当該フックしたシステムコールを開放する」（請求項１）との記載により規定されている。

ここでいう「そうでない場合」とは，その記載に先立つ「当該アプリ

ケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合」との記載と対をなすものと理解するのが合理的である。そうすると，「そうでない場合」とは，『「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合」でない場合』を意味することとなる。これは，すなわち，「当該アプリケーションが，機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションでないか，又は，送信先がローカルである場合」にほかならない。

他方，「システムコールを開放する」との動作は，本願明細書の「システムコールを開放して送信が行われるようにし」（【００２３】）及び「システムコールを開放する。その結果，その写真のデータが送信部１６によって写真共有サイトのサーバに送信されることになる。」（【００３４】）との記載から，送信を実行するための動作であると認められる。

以上より，本願発明は，「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合に，当該フックしたシステムコールを破棄することによって当該送信を阻止する一方，当該アプリケーションが，機密識別子で識別されるアプリケーションでないか，又は，送信先がローカルである場合に，当該フックしたシステムコールを開放することによって当該送信を実行する」ものであると解される。このように解することは，本願発明の課題及び効果（前記１(3)イ，エ）とも整合する。

そうすると，本願発明と引用発明との一致点及び相違点の認定に当たっては，ファイル送信の阻止の条件とともにファイル送信を阻止しない

条件についても対象とすべきところ，本件審決は，ファイル送信の阻止の条件を相違点１として認定するにとどまり，ファイル送信を阻止しない条件に関する対比及び認定が欠落しているというべきである。

そして，引用発明においてファイル送信を阻止しない条件は，入力元のアプリケーションの識別子の安全性よりも出力先の記憶領域の安全性の方が低くないことであり，この点は，本願発明のファイル送信を阻止しない条件とは相違する。

以上より，本願発明と引用発明とは，本願発明においては，「当該アプリケーションが，機密識別子で識別されるアプリケーションでないか，又は，送信先がローカルである場合に，当該フックしたシステムコールを開放することによって当該送信を実行する」のに対し，引用発明においては，「入力元のアプリケーションの識別子の安全性よりも出力先の記憶領域の安全性の方が低くない場合に，ファイル送信を実行する」点でも相違すると見るのが適当である（これと相違点１とを合わせると，相違点Ｃとなる。以下では，正しくは相違点１ではなく相違点Ｃが認定されるべきであったものとして論ずる。）。このような相違点Ｃを看過した点で，本件審決における本願発明と引用発明との一致点及び相違点の認定は誤りがある。

イ　これに対し，被告は，本願発明におけるファイル送信が阻止されない条件は，「そうでない場合」という包括的なもの，つまりファイル送信が阻止される条件以外の全ての場合であって，ファイル送信が阻止される条件に応じて反射的必然的に決定されるものであり，これが結果的にどのような条件と等価となっているかは発明特定事項ではないとし，ファイル送信が阻止される場合でない場合という条件においては，本願発明と引用発明は相違せず，この条件は一致点となる旨主張する。

この被告の主張の趣旨はやや判然としない部分があるが，「そうでな

い場合」の「そう」が「当該アプリケーションが，前記機密識別子記憶部で記憶されている機密識別子で識別されるアプリケーションであり，送信先がローカル以外である場合」を指すとすれば，ファイル送信が阻止される条件が具体的に特定されていることの反面として，阻止されない条件も「当該アプリケーションが，機密識別子で識別されるアプリケーションでないか，又は，送信先がローカルである場合」として具体的に特定されると見るのが合理的であるし，本願発明の課題及び効果に鑑みると，ファイル送信が阻止されない条件を本願発明の発明特定事項でないとする理由もないというべきである。そして，このような本願発明におけるファイル送信が阻止されない条件が引用発明におけるそれと相違することは，上記アのとおりである。また，なお，「そうでない場合」の「そう」が「当該フックしたシステムコールを破棄することによって当該送信を阻止」を指すものと理解する余地もあるが，このような理解は被告の前記主張とは整合しないと思われる。

したがって，この点に関する被告の主張は採用し得ない。

(3)ア　上記３のとおり，本件審決は，本願発明の「機密識別子」及び「機密識別子記憶部」と引用発明の「識別子」及び「保護方法データベース」とに係る相違点を看過したものであり，この点は審決の結論に影響を及ぼす。そうである以上，「機密識別子」及び「機密識別子記憶部」を含む相違点Ｃの看過も，審決の結論に当然影響を及ぼすということができる。

したがって，取消事由３は理由がある。

イ　この点につき，被告は，引用発明のアプリケーションや記憶領域に合理的に安全性を設定することは当業者が適宜行うことであり，引用発明において本願発明と同様の条件を実現することに阻害事由はない旨などを主張するけれども，相違点Ｃにつき，引用発明から本願発明の構成に至ることが引用発明の技術的思想に相反し，そのような構成を採ることに

阻害事由があるため，容易に想到可能とはいえないことは，相違点Ａないし Ｂにつき論じたところと同様である。

以上より，この点に関する被告の主張は採用し得ない。

５　結論

以上のとおり，原告の主張に係る取消事由のうち，取消事由１は理由がないものの，取消事由２及び３はいずれも理由があるから，本件審決は取り消されるべきである。

よって，原告の請求は理由があるからこれを認容することとし，主文のとおり判決する。

知的財産高等裁判所第３部

裁判長裁判官　　鶴　岡　稔　彦

裁判官　　杉　浦　正　樹

裁判官　　寺　田　利　彦