(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5681028号
(P5681028)
(45)発行日　平成27年3月4日(2015.3.4)　(24)登録日　平成27年1月16日(2015.1.16)

(51)Int.Cl.　F I
G06F 21/12 (2013.01)　G06F 21/12

請求項の数 7　(全 73 頁)

(21)出願番号　特願2011-89302(P2011-89302)
(22)出願日　平成23年4月13日(2011.4.13)
(65)公開番号　特開2011-248865(P2011-248865A)
(43)公開日　平成23年12月8日(2011.12.8)
審査請求日　平成26年1月24日(2014.1.24)
(31)優先権主張番号　特願2010-100611(P2010-100611)
(32)優先日　平成22年4月26日(2010.4.26)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　110001900
特許業務法人　ナカジマ知的財産綜合事務所
(74)代理人　100090446
弁理士　中島　司朗
(74)代理人　100125597
弁理士　小林　国人
(74)代理人　100146798
弁理士　川畑　孝二
(74)代理人　100121027
弁理士　木村　公一

最終頁に続く

(54)【発明の名称】改ざん監視システム、管理装置及び管理方法

(57)【特許請求の範囲】
【請求項１】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備え、
前記検出手段は、一の監視モジュールに対する複数の監視結果を用いて、前記複数の監視結果の不一致を検出し、
前記特定手段は、前記複数の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡ることにより、改ざんされた前記監視モジュールを特定し、
前記情報セキュリティ装置の各監視モジュールは、一の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、
前記受信手段は、前記一の時点における前記監視結果を受信し、
前記検出手段は、受信した前記監視結果のうち、一の監視モジュールに対する第１の監

視結果と第２の監視結果とが一致するか否かを判断することにより、前記第１の監視結果と前記第２の監視結果の不一致を検出し、
前記特定手段は、前記第１の監視結果及び前記第２の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡り、前記第１の監視結果及び前記第２の監視結果毎に、正常であるとするその他の前記監視結果を用いて監視先の監視モジュールから監視元の監視モジュールへ遡ることを繰り返すことにより、同一の監視モジュールに到達するか否かを判断し、同一の監視モジュールに到達すると判断する場合に、当該同一の監視モジュールを改ざんされた監視モジュールとして特定する
ことを特徴とする管理装置。
【請求項２】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備え、
前記検出手段は、一の監視モジュールに対する複数の監視結果を用いて、前記複数の監視結果の不一致を検出し、
前記特定手段は、前記複数の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡ることにより、改ざんされた前記監視モジュールを特定し、
前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、
前記受信手段は、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、
前記検出手段は、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第１監視モジュールによる前記第２監視モジュールに対する第２の監視結果が前記第２監視モジュールが改ざんされていないことを示すという不一致を検出し、
前記特定手段は、前記不一致が検出された場合に、前記第１監視モジュールを改ざんされた監視モジュールとして特定する
ことを特徴とする管理装置。
【請求項３】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備え、
前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、

前記受信手段は、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、
前記検出手段は、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第２監視モジュールによる前記第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出し、
前記特定手段は、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が前記第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定する
ことを特徴とする管理装置。
【請求項４】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理方法であって、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信ステップと、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出ステップと、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定ステップとを含み、
前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、
前記受信ステップにおいて、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、
前記検出ステップにおいて、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第２監視モジュールによる前記第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出し、
前記特定ステップにおいて、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が前記第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定する
ことを特徴とする管理方法。
【請求項５】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
コンピュータである管理装置に、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信ステップと、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出ステップと、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定ステップとを実行させ、
前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、

前記受信ステップにおいて、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、
前記検出ステップにおいて、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第２監視モジュールによる前記第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出し、
前記特定ステップにおいて、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が前記第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定するための前記コンピュータプログラムを記録している記録媒体。

【請求項６】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する集積回路であって、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備え、
前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、
前記受信手段は、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、
前記検出手段は、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第２監視モジュールによる前記第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出し、
前記特定手段は、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が前記第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定する
ことを特徴とする集積回路。

【請求項７】
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置と、前記情報セキュリティ装置を管理する管理装置とから構成される監視システムであって、
前記管理装置は、
前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、
受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、
異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備え、
前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、
前記受信手段は、前記第１の時点における前記監視結果及び前記第２の時点における前

記監視結果を受信し、
前記検出手段は、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第２監視モジュールによる前記第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出し、
前記特定手段は、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が前記第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定する
ことを特徴とする監視システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報セキュリティ装置などの機器内部で動作するモジュール等の改ざんを監視し管理する技術に関する。
【背景技術】
【０００２】
従来、認証鍵等の秘匿データを有しているアプリケーションプログラムが、悪意のある第三者（以下、「攻撃者」という）に解析されないようにするため、当該アプリケーションプログラムを耐タンパモジュールにより保護することが知られている。耐タンパモジュールは、通常、ハードウェアとして機器上に実装され、アプリケーションプログラムを保護している。しかし、日々新たな攻撃手法が考案される昨今の現状を踏まえると、新たな攻撃手法に柔軟に対応するためにも、更新が容易なコンピュータプログラムであるソフトウェアにより、アプリケーションプログラムを保護することが望ましい。
【０００３】
ソフトウェアによってアプリケーションプログラムを保護する技術として、例えば、ハッシュ値を用いた改ざん検証や、アプリケーションプログラムを利用しない時にはプログラムを暗号化して保存しておき、利用する時にのみ暗号化されたプログラムを復号してメモリへロードする復号ロード機能等がある。
【０００４】
ところが、このような技術を利用しても、アプリケーションプログラムを保護するソフトウェア（以下、「保護制御モジュール」という）自体が攻撃者により攻撃され得る。保護制御モジュールが改ざんされると、アプリケーションプログラムが攻撃者の攻撃にさらされることになる。
【０００５】
特許文献１は、プログラムの改変の有無をチェックするチェックプログラム自体の改変が行われた場合でも、改変されたプログラムの実行を確実に阻止することが可能なプログラムの改変防止のための技術を開示している。この技術によると、コンピュータシステムにおいて、プログラムの改変の有無を監視するためのチェックプログラムを複数用意し、各チェックプログラムが他のチェックプログラムのうちのいずれかを監視する。以下にこの技術について簡単に説明する。
【０００６】
この技術によると、２つの監視モジュールＡ、Ｂが相互に監視を行う。監視モジュールＡ、Ｂはそれぞれ、攻撃者による改ざんから保護すべきプログラム（本体プログラムＡ、Ｂ）、他のモジュールが改ざんされているかを検出するためのプログラム（チェックプログラムＡ、Ｂ）、及びそれぞれのチェックプログラムが改ざん検出を行うために必要な情報（チェック情報Ａ、Ｂ）から構成される。チェックプログラムＡは、監視モジュールＢの本体プログラムＢとチェックプログラムＢの改ざん検出を、チェック情報Ａを用いて行う。また、チェックプログラムＢは、監視モジュールＡの本体プログラムＡとチェックプログラムＡの改ざん検出を、チェック情報Ｂを用いて行う。この様に、それぞれの監視モ

ジュールが、相手の監視モジュールの本体プログラム及びチェックプログラムの改ざん検出を行う。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】日本国特許第３０５６７３２号公報

【特許文献２】ＷＯ２００８／０９９６８２

【特許文献３】ＷＯ２００９／１１８８００

【非特許文献】

【０００８】

【非特許文献１】岡本龍明、山本博資、「現代暗号」、産業図書（１９９７年）

【非特許文献２】ＩＴＵ－Ｔ Ｒｅｃｏｍｍｅｎｄａｔｉｏｎ Ｘ．５０９ （１９９７Ｅ）： Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ － Ｏｐｅｎ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ － Ｔｈｅ Ｄｉｒｅｃｔｏｒｙ： Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ，１９９７

【非特許文献３】Ｆ．Ｐｒｅｐａｒａｔａ，Ｇ．Ｍｅｔｚｅ ａｎｄ Ｒ．Ｔ．Ｃｈｉｅｎ，"Ｏｎ Ｔｈｅ Ｃｏｎｎｅｃｔｉｏｎ Ａｓｓｉｇｎｍｅｎｔ Ｐｒｏｂｌｅｍ ｏｆ Ｄｉａｇｎｏｓａｂｌｅ Ｓｙｓｔｅｍｓ，" ＩＥＥＥ Ｔｒａｎｓ． Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｍｐｕｔｅｒｓ，ｖｏｌ．１６，ｐｐ．８４８－８５４，１９６８．

【発明の概要】

【発明が解決しようとする課題】

【０００９】

特許文献１に記載されているように、複数の監視モジュールが相互に監視を行うようにすると、何れかの監視モジュールが改ざんされた場合であっても、改ざんされずに残っている監視モジュールを用いて、他のモジュールの改ざん検出を行うことができ、コンピュータシステムの安全性を高めることができる。

【００１０】

しかし、監視モジュールの数が増えると、監視モジュールの数に依存して監視結果の数が増える。例えば、ｎ個の監視モジュールが完全に相互に監視を行う場合には、その監視結果の数は、ｎ（ｎ－１）／２で表現される。この場合には、監視モジュールの数の増加に比べて、監視結果の数の増加は急激である。このため、監視モジュールの数が増加した場合に、監視結果を用いて改ざんの状況を分析しようとすると、その分析のための演算量が多大となり、機器の処理の負荷が高くなるという問題がある。

【００１１】

上記のような問題を解決するために、本発明は、監視結果の分析のための演算量を大きく増やすことなく、改ざんされた監視モジュールを特定することができる改ざん監視システム、管理装置、管理方法、集積回路、プログラム及び記録媒体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】

【００１２】

上記目的を達成するために、本発明の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備え、前記検出手段は、一の監視モジュールに対する複数の監視結果を用いて、前記複数の監視結果の不一致を検出し、前記特定手段は、前記複数の監視結果のそれぞれを用い

て、監視先の監視モジュールから監視元の監視モジュールへ遡ることにより、改ざんされた前記監視モジュールを特定し、前記情報セキュリティ装置の各監視モジュールは、一の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記受信手段は、前記一の時点における前記監視結果を受信し、前記検出手段は、受信した前記監視結果のうち、一の監視モジュールに対する第１の監視結果と第２の監視結果とが一致するか否かを判断することにより、前記第１の監視結果と前記第２の監視結果の不一致を検出し、前記特定手段は、前記第１の監視結果及び前記第２の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡り、前記第１の監視結果及び前記第２の監視結果毎に、正常であるとするその他の前記監視結果を用いて監視先の監視モジュールから監視元の監視モジュールへ遡ることを繰り返すことにより、同一の監視モジュールに到達するか否かを判断し、同一の監視モジュールに到達すると判断する場合に、当該同一の監視モジュールを改ざんされた監視モジュールとして特定することを特徴とする。

【発明の効果】

【００１３】

この構成によると、一部の監視結果を用いて異常を検出し、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定するので、監視結果の分析のための演算量を大きく増やすことなく、改ざんされた監視モジュールを特定することができるという優れた効果を奏する。

【００１４】

本発明の目的、効果及び特徴は、以下の説明を添付図面と併せて読めば明らかとなろう。添付図面は、本発明の一態様を例示している。

【図面の簡単な説明】

【００１５】

【図１】本発明に係る実施の形態１における検知システム１０の全体構成図である。

【図２】機器１００における検知モジュール群１３０の構成図である。

【図３】機器１００における保護制御モジュール１２０の構成図である。

【図４】検知モジュール群１３０内の検知モジュール１３１の構成図である。

【図５】機器１００におけるアクセス制御モジュール１４０の構成図である。

【図６】機器１００のハードウェア構成図である。

【図７】機器１００のソフトウェア構成図である。

【図８】管理装置２００における判断部２１０の構成図である。

【図９】管理装置２００におけるモジュール無効化部２２０の構成図である。

【図１０】検知システム１０全体の動作を示すフローチャートである。

【図１１】機器１００における初期設定処理を示すシーケンス図である。

【図１２】機器１００における初期設定処理（検知モジュール初期化処理）を示すフローチャートである。

【図１３】機器１００における検知処理を示すフローチャートである。

【図１４】機器１００における検知処理（保護制御モジュール検知処理）を示すシーケンス図である。

【図１５】機器１００の検知モジュール群１３０における監視パターンについて説明するための図である。

【図１６】検知システム１０における検知処理（検知モジュール検知処理）を示すシーケンス図である。図１７へ続く。

【図１７】検知システム１０における検知処理（検知モジュール検知処理）を示すシーケンス図である。図１８へ続く。

【図１８】検知システム１０における検知処理（検知モジュール検知処理）のシーケンス図である。図１７から続く。

【図１９】判断部２１０が受信した検出結果について説明するための図である。

【図２０】管理装置２００における検証処理を示すフローチャートである。
【図２１】検知モジュール群１３０における検出結果について説明するための図である。
【図２２】検出結果リスト６０５１のデータ構造の一例を示す図である。
【図２３】検出結果について説明するための図である。
【図２４】検知システム１０における無効化処理を示すシーケンス図である。
【図２５】本発明に係る実施の形態２における検知システム１１の全体構成図である。
【図２６】監視パターン更新部２３０の構成図である。
【図２７】管理装置２００ａにおける検証処理を示すフローチャートである。図２８へ続く。
【図２８】管理装置２００ａにおける検証処理を示すフローチャートである。図２７から続く。
【図２９】正常モジュール特定処理の動作を示すシーケンス図である。図３０へ続く。
【図３０】正常モジュール特定処理の動作を示すシーケンス図である。図２９から続く。
【図３１】循環監視パターンについて説明するための図である。
【図３２】特定処理を示すフローチャートである。
【図３３】循環監視パターンによる検出結果について説明するための図である。
【図３４】本発明に係る実施の形態３におけるソフトウェア更新システム１２の全体構成図である。
【図３５】保護制御モジュール１２０ａの構成図である。
【図３６】検知モジュール１３１ａの構成図である。
【図３７】更新用ソフトウェア配布部２４０の構成図である。
【図３８】ソフトウェア更新システム１２の動作を示すフローチャートである。
【図３９】初期設定処理を示すシーケンス図である。
【図４０】初期設定処理（検知モジュール初期化処理）を示すフローチャートである。
【図４１】解析・判断処理を示すシーケンス図である。
【図４２】相互認証処理を示すシーケンス図であり、検知モジュール１３１ａが更新用ソフトウェア配布部２４０を認証するときのシーケンスを示す。
【図４３】相互認証処理を示すシーケンス図であり、更新用ソフトウェア配布部２４０が各検知モジュールを認証するときのシーケンスを示す。
【図４４】回復処理を示すフローチャートである。
【図４５】回復処理（相互監視処理）を示すシーケンス図である。
【図４６】回復処理（更新処理）を示すシーケンス図である。図４７へ続く。
【図４７】回復処理（更新処理）を示すシーケンス図である。図４８へ続く。
【図４８】回復処理（更新処理）を示すシーケンス図である。図４９へ続く。
【図４９】回復処理（更新処理）を示すシーケンス図である。図４８から続く。
【図５０】本発明の実施の形態３における相互監視処理と更新処理との連携動作について説明するための図である。
【図５１】回復処理（再暗号化処理）を示すシーケンス図である。
【図５２】次ラウンド準備処理を示すシーケンス図である。
【図５３】検知モジュール群１３０における検出結果について説明するための図である。
【図５４】本発明のその他の変形例としての改ざん監視システム１０ｃの構成を示すブロック図である。
【図５５】情報セキュリティ装置１００ｃから受信した監視結果の一例を示す。
【図５６】情報セキュリティ装置１００ｃから受信した監視結果の集合Ｃ１１２のデータ構造の一例を示す。
【図５７】特定部２１０ｃの動作を示すフローチャートである。
【図５８】情報セキュリティ装置１００ｃから受信した別の監視結果の一例を示す。
【００１６】
（ａ）時刻ｔ＝ｋのときの監視結果を示す。（ｂ）時刻ｔ＝ｋ＋ｉのときの監視結果を示す。

【図５９】情報セキュリティ装置１００ｃから受信した別の監視結果の集合Ｃ１２０のデータ構造の一例を示す。
【図６０】情報セキュリティ装置１００ｃから受信したさらに別の監視結果の一例を示す。
【００１７】
（ａ）時刻ｔ＝ｋのときの監視結果を示す。（ｂ）時刻ｔ＝ｋ＋ｉのときの監視結果を示す。
【図６１】情報セキュリティ装置１００ｃから受信したさらに別の監視結果の集合Ｃ１３０のデータ構造の一例を示す。
【図６２】本発明のその他の変形例としての改ざん監視システム１０ｄの構成を示すブロック図である。
【図６３】監視結果の集合Ｄ１００ａと監視パターンの集合Ｄ１００ｂの一例を示す。
【図６４】循環型の監視パターンＤ１０１、Ｄ１０２、・・・、Ｄ１０６のデータ構造の一例を示す。
【発明を実施するための形態】
【００１８】
本発明の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備える。
【００１９】
ここで、前記検出手段は、一の監視モジュールに対する複数の監視結果を用いて、前記複数の監視結果の不一致を検出し、前記特定手段は、前記複数の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡ることにより、改ざんされた前記監視モジュールを特定してもよい。
【００２０】
ここで、前記情報セキュリティ装置の各監視モジュールは、一の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記受信手段は、前記一の時点における前記監視結果を受信し、前記検出手段は、受信した前記監視結果のうち、一の監視モジュールに対する第１の監視結果と第２の監視結果とが一致するか否かを判断することにより、前記第１の監視結果と前記第２の監視結果の不一致を検出し、前記特定手段は、前記第１の監視結果及び前記第２の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡り、前記第１の監視結果及び前記第２の監視結果毎に、正常であるとするその他の前記監視結果を用いて監視先の監視モジュールから監視元の監視モジュールへ遡ることを繰り返すことにより、同一の監視モジュールに到達するか否かを判断し、同一の監視モジュールに到達すると判断する場合に、当該同一の監視モジュールを改ざんされた監視モジュールとして特定してもよい。
【００２１】
ここで、前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記受信手段は、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、前記検出手段は、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第１監視モジュールによる前記第２監視モジュールに対する第２の監視結果が前記第２監視モジュールが改ざんされていないことを示すという不一致を検出し、前記特定手段は、前記不一致が検出さ

れた場合に、前記第１監視モジュールを改ざんされた監視モジュールとして特定してもよい。

【００２２】

ここで、前記情報セキュリティ装置の各監視モジュールは、第１の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記第１の時点より後の第２の時点において、他の監視モジュールの改ざんを監視し、その監視結果を送信し、前記受信手段は、前記第１の時点における前記監視結果及び前記第２の時点における前記監視結果を受信し、前記検出手段は、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第２監視モジュールによる前記第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出し、前記特定手段は、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が前記第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定してもよい。

【００２３】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理方法であって、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信ステップと、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出ステップと、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定ステップとを含む。

【００２４】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、コンピュータである管理装置に、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信ステップと、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出ステップと、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定ステップとを実行させるための前記コンピュータプログラムを記録している。

【００２５】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する集積回路であって、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備える。

【００２６】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置と、前記情報セキュリティ装置を管理する管理装置とから構成される監視システムであって、前記管理装置は、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信手段と、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出手段と、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュール

を起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定手段とを備える。

【００２７】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定手段と、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成手段と、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信手段とを備え、前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【００２８】

ここで、前記生成手段により生成される前記複数の監視パターンは、循環型の監視パターンを構成するとしてもよい。

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理方法であって、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定ステップと、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成ステップと、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信ステップとを含み、前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【００２９】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、コンピュータである管理装置に、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定ステップと、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成ステップと、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信ステップとを実行させるためのコンピュータプログラムを記録しており、前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【００３０】

また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する集積回路であって、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定手段と、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成手段と、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信手段とを備え、前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【００３１】
また、本発明の別の一実施態様は、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置と、前記情報セキュリティ装置を管理する管理装置とから構成される監視システムであって、前記管理装置は、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定手段と、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成手段と、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信手段とを備え、前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。
（実施の形態）
１．実施の形態１
本発明に係る実施の形態１としての検知システム１０について、図面に基づき説明する。
【００３２】
１．１．検知システム１０の構成
（１）全体構成
図１は、検知システム１０の全体構成図である。検知システム１０は、図１に示すように、情報処理装置としての機器１００と、管理装置２００とから構成される。機器１００と管理装置２００とは、ネットワークを介して接続されている。
【００３３】
（２）機器１００の構成
機器１００は、ネットワークを介して、例えば、コンテンツ配信サーバから音楽や映像等のコンテンツを購入し再生したり、金融機関のシステムにアクセスし、ネットバンキング（預金の残高照会や口座振り込み等）を行ったりするなど、ユーザに対してネットワークを利用した様々な機能を提供するデータ処理装置である。
【００３４】
（ａ）機器１００のソフトウェア構成
機器１００は、アプリケーションソフト（以下、「アプリ」という）１１０、１１１と、保護制御モジュール１２０と、検知モジュール群１３０とを含んで構成される。
【００３５】
アプリ１１０及び１１１は、機器１００を使用するユーザに対して、ネットワークを利用した機能を提供するソフトウェアであり、例えば、ネットワーク上のコンテンツ配信サーバ（不図示）から音楽や映像等のコンテンツを購入し、購入したコンテンツを再生するソフトウェアや、ネットワークを介して金融機関のシステム（不図示）にアクセスし、預金の残高照会や口座振り込み等のネットバンキングを行うソフトウェア等である。
【００３６】
アプリ１１０及び１１１は、一例として、コンテンツ配信サーバや金融機関のシステムと認証を行うための認証鍵等の秘匿データを有している。この秘匿データは、悪意のある第三者（以下、「攻撃者」という）によりアプリから抜き取られ、不正に利用されないよう、保護される必要がある。
【００３７】
このように、機器１００は、秘匿データを扱うので、情報セキュリティ装置と呼ぶこともある。
保護制御モジュール１２０は、攻撃者によりアプリ１１０及び１１１が解析され、認証鍵等の秘匿データが抜き取られないようにアプリ１１０及び１１１を保護するための機能を有するモジュールである。アプリを保護するための機能としては、例えば、アプリを利用しない時には、アプリを暗号化して保存しておき、アプリを利用する時にのみ暗号化ア

プリを復号してメモリへロードする復号ロード機能や、アプリが改ざんされていないかをチェックする改ざん検出機能、デバッガなどの解析ツールが動作していないかをチェックする解析ツール検出機能などがある。保護制御モジュール１２０は、これらの機能の動作を制御し、アプリ１１０及び１１１を保護する。

【００３８】

保護制御モジュール１２０は、改ざん検出機能や解析ツール検出機能により、攻撃者による攻撃を検出した場合には、アプリ１１０及び１１１の動作を停止し、アプリ１１０及び１１１が利用していたメモリ領域、特に秘匿データが記憶されたメモリ領域のクリア処理等を行い、秘匿データの漏洩を防止する。

【００３９】

検知モジュール群１３０は、複数の検知モジュール１３１、１３２、１３３、１３４、１３５（ここでは、一例として、５つ）から構成される。図２は、検知モジュール群１３０の構成を示す図である。検知モジュール１３１、１３２、１３３、１３４、１３５は、それぞれ、機器１００内部のソフトウェア（ここでは保護制御モジュール１２０）が改ざんされていないかを検出する機能を持つ。

【００４０】

そして、検知モジュール群１３０の各検知モジュールは、攻撃者によって各検知モジュールが改ざんされ、各検知モジュールを不正に利用されることを防止するために、検知モジュール同士が相互に改ざん検出を実施する。そして、各検知モジュールは、改ざん検出結果を、管理装置２００へ送信する。管理装置２００により、ある検知モジュールが改ざんされていると判断された場合には、他の正常な検知モジュールは、管理装置２００からの無効化指示を受け、改ざんされた検知モジュールを無効化する。

【００４１】

これにより、検知モジュール群１３０に含まれる一部の検知モジュールが攻撃され、改ざんされた場合であっても、それを検出し、攻撃に対処することが可能となる。

アクセス制御モジュール１４０は、各検知モジュールが他のモジュールを消去するために必要なアクセス情報を保持する。アクセス情報は、例えば、消去対象であるモジュールが配置されているアドレスや、消去に必要な手順が書かれた手順書などである。なお、アクセス情報は、消去対象であるモジュール毎に、それぞれ個別のアクセス情報取得鍵で暗号化されている。

【００４２】

（ｂ）保護制御モジュール１２０の構成

ここでは、保護制御モジュール１２０の詳細について説明する。

図３は、保護制御モジュール１２０の機能的な構成を示す機能ブロック図である。保護制御モジュール１２０は、保護制御モジュール本体と、改ざん検出用証明書とを含む。改ざん検出用証明書は、保護制御モジュール本体を改ざん検出するための証明書であり、管理装置２００で保持する署名秘密鍵（署名私有鍵とも呼ぶ）を用いて生成したものである。

【００４３】

同図に示すように、保護制御モジュール１２０の本体は、受信部３０１、送信部３０２、制御部３０３、復号ロード部３０４、改ざん検出部３０５、解析ツール検出部３０６及び暗復号鍵保持部３０７から構成される。

【００４４】

受信部３０１は、検知モジュール１３１、１３２、１３３、１３４、１３５から、各種依頼などを受信する。

送信部３０２は、検知モジュール１３１、１３２、１３３、１３４、１３５へ、各種依頼などを送信する。

【００４５】

制御部３０３は、復号ロード部３０４、改ざん検出部３０５、及び解析ツール検出部３０６を制御することにより、アプリ１１０、１１１が攻撃者により攻撃されている場合に

、それを検出する。

【００４６】

復号ロード部３０４は、暗号化されているアプリ１１０、１１１を実行するときに、暗復号鍵を用いて復号し、メモリ上にロードする処理を行う。また、アプリ１１０、１１１の実行中に、他のアプリへのコンテキストスイッチ（context switch）が発生すると、復号ロード部３０４は、メモリ上のデータを、暗復号鍵を用いて暗号化する。そして、再びアプリ１１０、１１１へコンテキストスイッチしたときに、暗号化したデータを復号する処理を行う。なお、コンテキストスイッチとは、複数のモジュールが１つのＣＰＵを共有できるように、ＣＰＵの状態（コンテキスト）を保存したり復元したりする過程のことである。

【００４７】

改ざん検出部３０５は、アプリ１１０、１１１の改ざん検出処理を実行する。改ざん検出処理は、アプリ１１０、１１１に付加されている検証用証明書を用いる方法と、ＭＡＣ値を比較する方法とがある。

【００４８】

解析ツール検出部３０６は、デバッガなどの解析ツールがインストールされたり、動作したときにそれを検出する。不正な攻撃者がアプリ１１０、１１１を攻撃するために、解析ツールをインストールしたり、動作させることが想定されるからである。検出方法としては、例えば、ファイル名を検索する方法や、デバッガが使用する特殊なレジスタが使用されているかを調べる方法や、デバッガが設定する割り込みを検出する方法などを用いる。

【００４９】

暗復号鍵保持部３０７は、アプリ１１０、１１１を暗復号するための暗復号鍵を保持する。

（ｃ）検知モジュールの構成

次に、検知モジュール１３１、１３２、１３３、１３４、１３５の詳細について説明する。

【００５０】

図４は、検知モジュール１３１の機能的な構成を示す機能ブロック図である。検知モジュール１３２、１３３、１３４及び１３５も同様の構成を有する。検知モジュール１３１は、検知モジュール本体と、改ざん検出用証明書と、ＭＡＣ値テーブルとを含む。改ざん検出用証明書は、検知モジュール本体の改ざんを検出するための証明書であり、管理装置２００で保持する署名秘密鍵を用いて生成したものである。

【００５１】

検知モジュール本体は、受信部４０１、送信部４０２、制御部４０３、検証部４０４、ＭＡＣ値生成部４０５、及びＭＡＣ値テーブル更新部４０６から構成される。

受信部４０１は、管理装置２００から、各種指示を受信する。また、受信部４０１は、他の検知モジュールから、改ざん検出を行うために必要な検知モジュール本体や検知モジュール改ざん検出用証明書などを受信する。さらに、受信部４０１は、他の検知モジュールから、依頼した処理の結果や、当該他の検知モジュールによる保護制御モジュール１２０の監視結果などを受信する。

【００５２】

送信部４０２は、管理装置２００、保護制御モジュール１２０、他の検知モジュール、及びアクセス制御モジュール１４０へ、各種処理結果や証明書などのデータを送信する。

制御部４０３は、受信部４０１が受信した各種指示や通知に基づいて、検証部４０４を制御することにより各種の処理を行う。

【００５３】

具体的には、制御部４０３は、保護制御モジュール１２０の改ざん検出処理、検知モジュール１３２、１３３、１３４、１３５の改ざん検出処理、保護制御モジュール１２０の無効化処理、検知モジュール１３２、１３３、１３４、１３５の無効化処理、監視パター

ンの更新処理などを行う。

【００５４】

検証部４０４は、制御部４０３の制御に基づき、保護制御モジュール１２０、検知モジュール１３２、１３３、１３４、１３５の改ざん検出処理を行う。

検証部４０４は、各モジュールに付加されている改ざん検出用証明書を用いて改ざん検出処理を行うとしてもよい。または、予め計算されたメッセージ認証コード（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）（以下、「ＭＡＣ値」という。）を用いてもよい。

【００５５】

検証部４０４が、どのタイミングでどのモジュールの改ざん検出処理を行うのかを示す情報は、予め、管理装置２００から与えられている。検証部４０４は、管理装置２００から改ざん検出対象のモジュールの変更や改ざん検出を行うタイミングの変更の指示があった場合には、指示に従い変更する。

【００５６】

ＭＡＣ値生成部４０５は、検証鍵を保持している。ＭＡＣ値生成部４０５は、検証部４０４が改ざん検出処理にＭＡＣ値を用いる場合、検証鍵を用いてＭＡＣ値を生成する。

ＭＡＣ値テーブル更新部４０６は、各モジュールのＭＡＣ値が格納されているＭＡＣ値テーブルを更新する。ＭＡＣ値テーブルには、モジュールを識別するためのモジュール識別子と、そのモジュールに対応するＭＡＣ値とが対になって格納されている。

【００５７】

ＭＡＣ値生成部４０５は、改ざん検出処理の対象であるモジュールを取得し、取得したモジュールのＭＡＣ値を計算する。検証部４０４は、計算されたＭＡＣ値とＭＡＣ値テーブルに格納されている対象モジュールのＭＡＣ値とを比較することにより改ざん検出を行う。検証部４０４は、計算されたＭＡＣ値とＭＡＣ値テーブルに格納されている対象モジュールのＭＡＣ値とが一致しない場合には、対象モジュールの改ざんを検出したとみなす。一致する場合には、改ざんを検出しなかったとみなす。

【００５８】

（ｄ）アクセス制御モジュール１４０の構成

図５は、アクセス制御モジュール１４０の構成を機能的に示す機能ブロック図である。同図に示すように、アクセス制御モジュール１４０は、受信部５０１、送信部５０２、及びアクセス情報保持部５０３から構成される。

【００５９】

受信部５０１は、検知モジュール１３１、１３２、１３３、１３４、１３５から、改ざんされた検知モジュールを消去するために必要な情報であるアクセス情報の取得依頼を受信する。

【００６０】

送信部５０２は、アクセス情報取得依頼に応じて、アクセス情報取得を依頼してきた検知モジュールへアクセス情報を送信する。

アクセス情報保持部５０３は、検知モジュール１３１、１３２、１３３、１３４、１３５毎に、そのモジュールを消去するためのアクセス情報を保持する。

【００６１】

各アクセス情報には、消去対象となる検知モジュールを識別するための検知モジュール識別子が付されている。また、各アクセス情報は、アクセス情報取得鍵で暗号化されている。

【００６２】

検知モジュール１３１、１３２、１３３、１３４、１３５からアクセス情報取得依頼を受け付けると、送信部５０２は、アクセス情報保持部５０３に記憶され、消去対象の検知モジュールの識別子が付されたアクセス情報を、依頼元の検知モジュールへ送信する。

【００６３】

（ｅ）機器１００のハードウェア構成

続いて、図６を用いて、機器１００のハードウェア構成について説明する。
図６に示すように、機器１００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１７１、不揮発性メモリであるＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１７２、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１７３、及びＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）１７４などを含んで構成される。また、これらはバスを介して、相互に通信可能に接続されている。

【００６４】
ＥＥＰＲＯＭ１７２には、保護制御モジュール１２０、検知モジュール群１３０及びアプリ１１０、１１１などが格納されている。
ＥＥＰＲＯＭ１７２に格納されている各種モジュールをＣＰＵ１７１が実行することにより、各種モジュールの各機能部が実現される。各機能部は、具体的には、コンピュータプログラムによって記述されている。

【００６５】
ＲＡＭ１７３は、ＣＰＵ１７１のワークエリアとして用いられる。ＲＡＭ１７３には検知モジュール群１３０及び、アプリ１１０、１１１がロードされる。改ざん検出処理及び無効化処理の対象となる検知モジュールは、ＲＡＭ１７３上で動作している検知モジュールである。

【００６６】
ＮＩＣ１７４は、ネットワークに接続するための拡張カードである。

（ｆ）ソフトウェア階層
続いて、図７を用いて、機器１００のソフトウェア階層について説明する。

【００６７】
図７に示すように、アクセス制御モジュール１４０及び検知モジュール群１３０は、ＯＳ１５０の中に組み込まれている。アプリ１１０及びアプリ１１１は、ＯＳ１５０上で動作し、保護制御モジュール１２０及びブートローダ１６０は、ＯＳ１５０の管理外にある。

【００６８】
機器１００の起動の際には、まず保護制御モジュール１２０及び検知モジュール群１３０が起動された上で各アプリが実行される。

（３）管理装置２００の構成
管理装置２００は、機器１００の検知モジュール群１３０から、改ざん検出結果を受信して、受信した改ざん検出結果を基に、無効化すべき異常な検知モジュールを特定する異常モジュール特定装置として機能する。

【００６９】
（ａ）全体構成
図１に示すように、管理装置２００は、判断部２１０、モジュール無効化部２２０、及び通信部２５０から構成される。管理装置２００は、具体的には、ＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどを備えるコンピュータシステムである。ＣＰＵが、ＲＯＭまたはハードディスクユニットに記憶されている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、管理装置２００は、上記の機能を発揮する。

【００７０】
判断部２１０は、機器１００の検知モジュール群１３０から、改ざん検出結果を受信して、受信した改ざん検出結果を基に、無効化すべき異常な検知モジュールを特定する。
モジュール無効化部２２０は、検知モジュール１３１、１３２、１３３、１３４、１３５からアクセス情報取得鍵の取得要求を受け付けると、要求元の検知モジュールへ、アクセス情報取得鍵を送信する。

【００７１】
通信部２５０は、機器１００と、管理装置２００内部の各部との間で情報の送受信を行う。例えば、通信部２５０は、機器１００から受信した改ざん検出結果を判断部２１０に

送信する。なお、機器１００と管理装置２００との間の通信には、データを暗号化するなど、セキュリティの確保された通信路を用いてもよい。

【００７２】

続いて、管理装置２００の各構成要素について説明する。

（ｂ）判断部２１０の構成

図８は、判断部２１０の構成を機能的に示す機能ブロック図である。

【００７３】

同図に示すように、判断部２１０は、受信部６０１、送信部６０２、指示生成部６０３、モジュール特定部６０４及び検出結果保持部６０５から構成される。

受信部６０１は、検知モジュール１３１、１３２、１３３、１３４、１３５から、改ざん検出結果、各種依頼などを受信し、それらを指示生成部６０３へ出力する。また、受信部６０１は、管理装置２００内の各部から、処理が完了した旨の通知を受け取り、それを指示生成部６０３へ出力する。

【００７４】

送信部６０２は、指示生成部６０３によって生成された指示を、管理装置２００内の各部へ出力する。

指示生成部６０３は、検知モジュール１３１、１３２、１３３、１３４、１３５から受信した改ざん検出結果（以下、「相互監視結果」又は単に「監視結果」ということがある。）を、モジュール特定部６０４へ出力する。また、指示生成部６０３は、モジュール特定部６０４から、改ざんされている異常な検知モジュールを識別する情報を取得し、取得した情報を基に、管理装置２００内の各部に対する指示を生成する。

【００７５】

モジュール特定部６０４は、検知モジュール１３１、１３２、１３３、１３４、１３５から受信した相互監視結果を用いて、各検知モジュールが改ざんされているか否かを判断し、改ざんされている異常な検知モジュールを特定する。モジュール特定部６０４は、異常な検知モジュールを識別する情報を指示生成部６０３へ出力する。

【００７６】

検出結果保持部６０５は、検知モジュール１３１、１３２、１３３、１３４、１３５から受信した相互監視結果のうち、改ざんされていると判定することにより得られた改ざん検出結果を記憶する。

【００７７】

（ｃ）モジュール無効化部２２０

図９は、モジュール無効化部２２０の機能的な構成を示す機能ブロック図である。

同図に示すように、モジュール無効化部２２０は、受信部７０１、送信部７０２、アクセス情報取得鍵保持部７０３、及び検知モジュール選択部７０４から構成される。

【００７８】

受信部７０１は、判断部２１０から改ざんされた異常な検知モジュールを無効化する指示を受信する。また、受信部７０１は、検知モジュール１３１、１３２、１３３、１３４、１３５からアクセス情報取得鍵の取得依頼を受信する。

【００７９】

送信部７０２は、アクセス情報取得鍵の取得依頼に応じて、アクセス情報取得鍵を依頼元の検知モジュールへ送信する。

アクセス情報取得鍵保持部７０３は、アクセス制御モジュール１４０が保持するアクセス情報を復号するための鍵であるアクセス情報取得鍵を保持する。

【００８０】

検知モジュール選択部７０４は、改ざんされた異常な検知モジュールの無効化処理を行う検知モジュールを選択し、選択した検知モジュールに、異常な検知モジュールの無効化を指示する。判断部２１０からどの検知モジュールを選択するかの指示を受けて、無効化処理を行う検知モジュールを選択するとしてもよい。

【００８１】

なお、検知モジュール選択部７０４が選択した検知モジュールからアクセス情報取得鍵の取得依頼があった場合には、送信部７０２は、アクセス情報取得鍵に、消去対象となる検知モジュールの識別子を付して、選択した検知モジュールへ送信する。

【００８２】

１．２　検知システム１０の動作

続いて、検知システム１０の動作を説明する。

（１）全体動作

図１０は、検知システム１０全体の処理の流れを示したフローチャートである。

【００８３】

検知システム１０は、先ず、初期設定処理を行う（Ｓ１００）。

初期設定処理とは、ソフトウェア（保護制御モジュール１２０や検知モジュール群）のインストールや、ソフトウェアを検知するために必要となるデータを検知モジュール１３１、１３２、１３３、１３４、１３５のそれぞれに埋め込む処理である。なお、初期設定処理は、機器１００が工場で製造される際に行われる。その後、機器１００は、工場から出荷され、ユーザの利用に供される。

【００８４】

ユーザにより機器１００が利用される際には、機器１００内部では、保護制御モジュール１２０がアプリ１１０、１１１を攻撃者による攻撃から保護する。これと同時に、検知モジュール１３１、１３２、１３３、１３４、１３５が保護制御モジュール１２０の改ざん検出を実施し、保護制御モジュール１２０が攻撃されていないかをチェックする検知処理を行う。また、各検知モジュールは、攻撃者によって各検知モジュールが改ざんされ、各検知モジュールを不正に利用されることを防止するために、検知モジュール同士が相互に改ざん検出を実施する（ステップＳ２００）。

【００８５】

検知処理を行った結果、保護制御モジュール１２０が改ざんされたと判明した場合には、改ざんされた旨を機器１００が備える表示部（図示していない）に表示したり、管理装置２００へ通知したりする。

【００８６】

続いて、上記２つの処理について、その詳細を順に説明する。

（２）初期設定処理の動作

ここでは、図１１から図１２を用いて、検知システム１０の初期設定処理（図１０のＳ１００）の詳細について説明する。

【００８７】

図１１は、検知システム１０における初期設定処理の流れを示すシーケンス図である。本シーケンスにおいて、検知モジュール１３１、１３２、１３３、１３４、１３５の各々が個別に行う処理を、検知モジュール群１３０としてまとめて記載している。

【００８８】

検知システム１０は、機器１００の工場製造時に、機器１００の不揮発メモリへアプリ（１１０、１１１）、保護制御モジュール１２０、検知モジュール（１３１、１３２、１３３、１３４、１３５）などをインストールする（Ｓ１００１）。

【００８９】

これらのソフトウェアには、ソフトウェアが改ざんされているか否かを検証するための改ざん検出用証明書が付加されている。この改ざん検出用証明書は、管理装置２００が保持する署名秘密鍵により署名が施されている。なお、Ｓ１００１では、上記のソフトウェア以外にも、機器１００の動作に必要なソフトウェアがインストールされる。

【００９０】

ここで、初期設定処理の際に機器１００に埋め込まれる鍵について説明する。

保護制御モジュール１２０には暗復号鍵が埋め込まれ、検知モジュール１３１、１３２、１３３、１３４、１３５には署名公開鍵及び検証鍵が埋め込まれる。更に、検知モジュール１３１、１３２、１３３、１３４、１３５には、それぞれの検知モジュールを識別す

るための検知モジュール識別子が埋め込まれ、保護制御モジュール１２０及び検知モジュール１３１、１３２、１３３、１３４、１３５は、それぞれ、その状態で機器１００にインストールされる。

【００９１】

暗復号鍵は、アプリ１１０、１１１を暗号化及び復号するための鍵である。アプリ１１０、１１１は、暗復号鍵を用いて暗号化された状態で不揮発メモリへ記憶され、実行時に保護制御モジュール１２０により、暗号化されたアプリ１１０、１１１が暗復号鍵を用いて復号された後、アプリ１１０、１１１が実行される。

【００９２】

機器１００が、コンテキストを切り替えながら複数のアプリを実行する場合には、コンテキスト切り替えのタイミングで、暗復号鍵を用いて、アプリ１１０、１１１が使用しているデータの暗号化及び復号を行うことにより、アプリ１１０、１１１の実行時に、デバッガなどの解析ツールによって、データが抜き取られることを防止する。

【００９３】

検知モジュール１３１、１３２、１３３、１３４、１３５に埋め込まれる鍵のうち、署名公開鍵は、すべての検知モジュールに共通の鍵である。検証鍵は、それぞれの検知モジュールで異なる鍵である。図１１に戻り説明を続ける。Ｓ１００１で各ソフトウェアをインストールした後、機器１００は、初期設定を行うソフトウェア、及び、正常に動作するかテストするためのソフトウェアなどを実行して、初期化する（Ｓ１００２）。また、機器１００は、検知モジュール１３１、１３２、１３３、１３４、１３５に対して、初期化指示を出力する（Ｓ１００３）。

【００９４】

指示を受信した検知モジュール群１３０は、検知モジュール初期化処理を実行する（Ｓ１００４）。

（ａ）検知モジュール初期化処理の動作

図１２は、検知モジュール初期化処理（図１１のＳ１００４）の動作を示すフローチャートである。

【００９５】

なお、ここでは、検知モジュール１３１についてのみ説明するが、検知モジュール１３２、１３３、１３４及び１３５の動作も基本的に検知モジュール１３１と同一であるので、これらの説明を省略する。

【００９６】

検知モジュール１３１は、改ざん検出対象である検知モジュール１３２、１３３、１３４、１３５及び保護制御モジュール１２０の改ざん検出用証明書の検証を行う（Ｓ１１０１）。この検証は、各検知モジュールから検証値を生成し、生成した検証値とそれぞれの改ざん検出用証明書に記述されている検証値とを比較することにより行われる。上記検証値は、ハッシュ値や署名である。署名の場合、署名が正しいか否かの検証を行う。

【００９７】

生成した各検証値がそれぞれの改ざん検出用証明書に記述されている検証値と一致するか否かを判定する（ステップＳ１１０２）。各検証値がそれぞれの改ざん検出用証明書に記述されている検証値と一致すれば（ステップＳ１１０２でＹＥＳ）、他の検知モジュール及び保護制御モジュール１２０それぞれに対してＭＡＣ値を生成し、ＭＡＣ値テーブルとして、他の検知モジュール及び保護制御モジュール１２０が有するＭＡＣ値保持部に保持する（ステップＳ１１０３）。少なくともいずれか一方の検証値が改ざん検出用証明書に記述されている検証値と一致しなければ（ステップＳ１１０２でＮＯ）、エラーを出力して機器を停止する（ステップＳ１１０４）。

【００９８】

（３）検知処理の動作

続いて、検知処理について説明する。

機器１００は、初期設定処理を終えると工場から出荷され、ユーザの元へ送られ、ユー

ザの元で機器１００が使用される。
【００９９】
機器１００でアプリ１１０、１１１が動作しているとき、機器１００内部では、保護制御モジュール１２０が復号ロード機能、改ざん検出機能、解析ツール検出機能などの機能を制御し、アプリ１１０、１１１を攻撃者による攻撃から保護する。
【０１００】
図１３は検知処理（図１０のＳ２００）のフローチャートである。検知処理は、保護制御モジュール１２０が改ざんされているかを検知する保護制御モジュール検知処理（Ｓ２０１）と、検知モジュールが改ざんされているかを検知する検知モジュール検知処理（Ｓ２０２）とからなる。
【０１０１】
（ａ）保護制御モジュール検知処理の動作
図１４のシーケンス図を用いて、保護制御モジュール検知処理の詳細について説明する。
【０１０２】
保護制御モジュール検知処理においては、先ず、検知モジュール１３１、１３２、１３３、１３４、１３５が、保護制御モジュール１２０の改ざん検出を実施する。改ざん検出は、検証鍵を使用して保護制御モジュール１２０のＭＡＣ値を計算し（Ｓ２０００）、計算したＭＡＣ値とＭＡＣ値テーブルに保持されているＭＡＣ値とを比較する（Ｓ２００１）ことにより行う。
【０１０３】
ＭＡＣ値が一致すれば（Ｓ２００１で「改ざんされていない」）、保護制御モジュール１２０は改ざんされていないと判定し、ＭＡＣ値が一致しなければ（Ｓ２００１で「改ざんされている」）、保護制御モジュール１２０は改ざんされていると判定する。
【０１０４】
なお、図１４では記載を簡略化し、検知モジュール１３１のみが保護制御モジュール１２０の改ざん検出を行っているように記載されているが、当然ながら、検知モジュール１３２、１３３、１３４、１３５でも同様の処理が行われる。
【０１０５】
保護制御モジュール１２０が改ざんされているか否か、即ち、ＭＡＣ値が一致するか否かを判定し（Ｓ２００１）、保護制御モジュール１２０が改ざんされていると判定した場合（Ｓ２００１で「改ざんされている」）、検知モジュール１３１は、その旨を、管理装置２００の判断部２１０へ通知する（Ｓ２００２）。
【０１０６】
保護制御モジュール１２０が改ざんされていないと判定した場合（Ｓ２００１で「改ざんされていない」）、検知モジュール１３１は、判断部２１０へ通知を行わず、改ざん検出処理へ戻る。
【０１０７】
判断部２１０は、検知モジュール１３１、１３２、１３３、１３４、１３５から改ざん検出結果を受信する（Ｓ２００２）。
（ｂ）検知モジュール検知処理の動作
続いて、図１５から図２４を用いて検知モジュール検知処理の詳細について説明する。
【０１０８】
検知モジュール検知処理では、攻撃者によって各検知モジュールが改ざんされ、各検知モジュールを不正に利用されることを防止するために、検知モジュール同士が相互に改ざん検出を実施する。各検知モジュールについては、監視パターンによって、どの検知モジュールの改ざん検出をするかが決まっている。
【０１０９】
実施の形態１における監視パターンについて、図１５に示す具体例を用いて説明する。図１５では、監視パターンの説明を容易にするため、監視パターンを有向グラフで表して

いる。矢印は、監視元（検証元）の検知モジュールから監視先（検証先）の検知モジュールへ向いている。

【０１１０】

たとえば、矢印Ａ２０００は、検知モジュール１３１から検知モジュール１３２へ向いていることから、検知モジュール１３１が、検知モジュール１３２の改ざん検出処理を行うことを示している。また、矢印Ａ２００６は、検知モジュール１３１から検知モジュール１３５へ向いていることから、検知モジュール１３１が、さらに、検知モジュール１３５の改ざん検出処理を行うことを示している。他の矢印も同様の改ざん検出処理を行うことを示している。

【０１１１】

まず、図１６から図１８のシーケンス図を用いて、検知モジュール検知処理の詳細について説明する。

検知モジュール１３１は、一例として図１５に示す監視パターンに従って、検知モジュール１３２の改ざん検出を行う（Ｓ２１０１）。検知モジュール１３１は検出結果を判断部２１０へ送信する（Ｓ２１０２）。

【０１１２】

図１９は、判断部２１０が受信した検出結果を示す図である。図１９では、「改ざんされていない」という検出結果を、矢印と対応して記載された○印で表している。「改ざんされている」という検出結果では、矢印と対応して記載された×印で表す。

【０１１３】

例えば、○印２０１０は、検知モジュール１３１が、検知モジュール１３２の改ざん検出処理を行った結果、「改ざんされていない」と判定されたことを表している。

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１０３）。検証処理の動作については後述する。

【０１１４】

次に、検知モジュール１３２は、一例として図１５に示す監視パターンに従って、検知モジュール１３３の改ざん検出を行う（Ｓ２１０４）。検知モジュール１３２は検出結果を判断部２１０へ送信する（Ｓ２１０５）。

【０１１５】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１０６）。

次に、検知モジュール１３３は、一例として図１５に示す監視パターンに従って、検知モジュール１３１の改ざん検出を行う（Ｓ２１０７）。検知モジュール１３３は検出結果を判断部２１０へ送信する（Ｓ２１０８）。

【０１１６】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１０９）。

次に、検知モジュール１３４は、一例として図１５に示す監視パターンに従って、検知モジュール１３５の改ざん検出を行う（Ｓ２１１０）。検知モジュール１３４は検出結果を判断部２１０へ送信する（Ｓ２１１１）。

【０１１７】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１１２）。

次に、検知モジュール１３５は、一例として図１５に示す監視パターンに従って、検知モジュール１３２の改ざん検出を行う（Ｓ２１１３）。検知モジュール１３５は検出結果を判断部２１０へ送信する（Ｓ２１１４）。

【０１１８】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１１５）。

次に、検知モジュール１３１は、一例として図１５に示す監視パターンに従って、検知モジュール１３５の改ざん検出を行う（Ｓ２１１６）。検知モジュール１３１は検出結果を判断部２１０へ送信する（Ｓ２１１７）。

【０１１９】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１１８）。

次に、検知モジュール１３３は、一例として図１５に示す監視パターンに従って、検知モジュール１３４の改ざん検出を行う（Ｓ２１１９）。検知モジュール１３２は検出結果を判断部２１０へ送信する（Ｓ２１２０）。

【０１２０】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１２１）。

次に、検知モジュール１３５は、一例として図１５に示す監視パターンに従って、検知モジュール１３４の改ざん検出を行う（Ｓ２１２２）。検知モジュール１３５は検出結果を判断部２１０へ送信する（Ｓ２１２３）。

【０１２１】

判断部２１０は、検出結果を受信し、検証処理を行う（Ｓ２１２４）。

（ｃ）検証処理の動作

検証処理では、検知モジュール検知処理において、判断部２１０が各検知モジュールから検出結果を受信し、改ざんされた異常な検知モジュールを特定する。

【０１２２】

検証処理の動作について、図２０に示すフローチャートを用いて説明する。

判断部２１０は、各検知モジュールから受信した改ざん検出結果が正常であるかを判断する（Ｓ２２０１）。検出結果が異常であった場合（Ｓ２２０１でＮＯ）、検出結果を記憶する（Ｓ２２０２）。

【０１２３】

図２１は、一例として、判断部２１０が検知モジュール１３４から受信した検出結果を示す図である。図２１では、×印２０１４は、検知モジュール１３４が、検知モジュール１３５の改ざん検出処理を行った結果、「改ざんされている」と判定したことを表している。このとき、判断部２１０は、検知モジュール１３４が、検知モジュール１３５の改ざん検出処理を行った結果得られた「改ざんされている」という検出結果を、検出結果リスト６０５１として検出結果保持部６０５へ記憶する。図２２は、検出結果リスト６０５１のデータ構造の一例を示す図である。検知モジュール１３４が検知モジュール１３５の改ざん検出を行った結果、「改ざんされている」という検出結果を送信してきた場合、検出結果リスト６０５１の検証元が検知モジュール１３４であり、検証先が検知モジュール１３５の欄に、改ざんされていることを示す検出結果６０５２（この図において、×印により示している）を記憶する。

【０１２４】

図２０に戻り、判断部２１０は、受信した検出結果とすでに記憶している検出結果保持部６０５の検出結果に矛盾があるかを判断する（Ｓ２２０３）。矛盾がなかった場合（Ｓ２２０３でＮＯ）には、検証処理を終了する。矛盾があった場合（Ｓ２２０３でＹＥＳ）には、異常な検知モジュールを特定する（Ｓ２２０４）。

【０１２５】

次に、ステップＳ２２０３において判断する矛盾について、説明する。

判断部２１０は、すでに図２２に示すように、Ｓ２１１１において受信した検知モジュール１３４による検出結果６０５２（検知モジュール１３５が改ざんされている）を保持しているとする。その後、Ｓ２１２２において、検知モジュール１３５が検知モジュール１３４の改ざん検出を行った結果、図２３に示すように、検知モジュール１３４が「改ざんされていない」という検出結果２０１８を受信する。言い換えると、検知モジュール１３５は、検知モジュール１３５が「改ざんされている」と判定した検知モジュール１３４に対し、「改ざんされていない」と判定している。

【０１２６】

このとき、判断部２１０は検知モジュール１３５の改ざん検出結果は矛盾していると判定する。改ざん検出結果に矛盾があるため、判断部２１０は、検知モジュール１３５は異常な検知モジュールであると特定する。

【０１２７】

このようにして異常な検知モジュールを特定できる理由は、以下の通りである。

ここで、仮に、Ｓ２１１０の時点で、検知モジュール１３４が改ざんされていないと仮定した場合には、検知モジュール１３４による改ざん検出結果は正しいため、判断部２１０は、検知モジュール１３５は改ざんされていると断定できる。

【０１２８】

一方、Ｓ２１１０の時点で、検知モジュール１３４がすでに攻撃者によって改ざんされていたと仮定し、検知モジュール１３４が異常な検出結果を判断部２１０に送信していた場合に、Ｓ２１２２において検知モジュール１３５が検知モジュール１３４の改ざん検出したとき、検知モジュール１３５が改ざんされていない正常な検知モジュールであれば、検知モジュール１３４が「改ざんされている」という改ざん検出結果を送信するはずである。これは、一度改ざんされた検知モジュール（検知モジュール１３４）は、改ざんされていない正常な検知モジュールに戻ることはないからである。しかし、検知モジュール１３５は、検知モジュール１３４が「改ざんされていない」とする改ざん検出結果を送信している。よって、検知モジュール１３５は改ざんされていると断定できる。

【０１２９】

このように、検知モジュール１３５は、改ざんされた異常な検知モジュールであると断定できる。

図２０に戻り、判断部２１０は、異常な検知モジュールと特定した検知モジュールの無効化処理を実行するかを判断する（Ｓ２２０５）。無効化処理を実行しないと判断した場合（Ｓ２２０５でＮＯ）、検証処理を終了する。無効化処理を実行すると判断した場合（Ｓ２２０５でＹＥＳ）、異常な検知モジュールの無効化処理を実行する（Ｓ２２０６）。

【０１３０】

（ｄ）無効化処理の動作

図２４のシーケンス図を用いて、無効化処理の詳細について説明する。

ここでは、検知モジュール１３５が改ざんされ、それを検知モジュール１３４が検出した場合の処理を例に、無効化処理の動作の詳細を説明する。

【０１３１】

判断部２１０は、改ざんされた検知モジュールの識別情報と共に、モジュール無効化部２２０へ無効化の指示を出力する（Ｓ２９０１）。

モジュール無効化部２２０は、検知モジュール１３４へ、改ざんされた検知モジュール１３５の無効化を依頼する（Ｓ２９０２）。

【０１３２】

検知モジュール１３４は、モジュール無効化部２２０から、検知モジュール１３５の無効化依頼を受信すると（Ｓ２９０２）、モジュール無効化部２２０に対し、検知モジュール１３５を無効化するためのアクセス情報取得鍵の送付を依頼する（Ｓ２９０３）。更に、検知モジュール１３４は、アクセス制御モジュール１４０へ、検知モジュール１３５を無効化するためのアクセス情報の取得を依頼する（Ｓ２９０４）。

【０１３３】

モジュール無効化部２２０は、アクセス情報取得鍵の送付依頼を受信すると（Ｓ２９０３）、検知モジュール１３４が改ざんされたと判定されていない検知モジュールか否か、及び、依頼されたアクセス情報取得鍵が不正な（改ざんされた）検知モジュール１３５を無効化するためのアクセス情報取得鍵か否かを確認する（Ｓ２９０５）。この確認は、判断部２１０からモジュール無効化部２２０へ通知された検知モジュールの情報を利用して行う。

【０１３４】

確認した結果、改ざんされた検知モジュール１３５からの依頼であったり、或いは、改ざんされていない検知モジュール１３１、１３２、１３３に対するアクセス情報取得鍵の取得依頼であったりする場合には（Ｓ２９０５で「正しくない」）、モジュール無効化部２２０は、無効化処理を停止する。

【０１３５】

確認した結果、正しい依頼であれば（Ｓ２９０５で「正しい」）、モジュール無効化部

２２０は、依頼してきた検知モジュール１３４へ検知モジュール１３５を無効化するためのアクセス情報取得鍵を送付する（Ｓ２９０６）。

【０１３６】

検知モジュール１３４は、モジュール無効化部２２０からアクセス情報取得鍵を受信し（Ｓ２９０６）、さらに、アクセス制御モジュール１４０から暗号化されたアクセス情報を受信する（Ｓ２９０７）。検知モジュール１３４は、アクセス情報取得鍵と暗号化されたアクセス情報とから、アクセス情報を取得する（Ｓ２９０８）。取得したアクセス情報は、検知モジュール１３５を消去するための専用ドライバである。検知モジュール１３４は、専用ドライバを利用して、改ざんされた異常な検知モジュール１３５を消去する（Ｓ２９０９）。

【０１３７】

検知モジュール１３４は、無効化処理が終了すると、アクセス情報取得鍵、暗号化されたアクセス情報、及び、アクセス情報等を消去し、モジュール無効化部２２０へ完了通知を送信する（Ｓ２９１０）。モジュール無効化部２２０は、検知モジュール１３４から完了通知を受信したら（Ｓ２９１０）、判断部２１０へ無効化処理の完了通知を送信する（Ｓ２９１１）。

【０１３８】

上記実施の形態により、検知モジュール群１３０内の複数の検知モジュールが相互に改ざん検出を行うので、改ざんされた異常な検知モジュールを検出することが可能となり、検知システムの信頼性を高めることができる。また、改ざんされた異常な検知モジュールを無効化するので、改ざんされた異常な検知モジュールによる不正動作を防止することができる。これにより、検知モジュールが不正動作をしたとしても、保護制御モジュール１２０の情報を漏洩することがないため、システムの安全性を一層高めることができる。また、検出結果保持部６０５で改ざんされたという検出結果を保持することにより、検知モジュール群１３０内のすべての検知モジュールが一度に改ざん検出を行わなくても、矛盾があるか否かで異常な検知モジュールを特定することができるため、機器内の処理の負荷を軽減することができる。

【０１３９】

２．実施の形態２

本発明に係る別の実施の形態２における検知システム１１を説明する。

上記の実施の形態１では、異常な検知モジュールを無効化するために、改ざんされていると判定されていない検知モジュールを使用した。しかし、改ざんされていると判定されていない検知モジュールであっても、異常である可能性があるため、正しく異常な検知モジュールを無効化できるとは限らない。

【０１４０】

そこで、実施の形態２では、検証処理において、異常な検知モジュールを特定するだけでなく、正常な検知モジュールを特定する。

る。

【０１４１】

２．１　検知システム１１の構成

ここでは、検知システム１１について、より具体的に説明する。

（１）全体構成

実施の形態２に係る検知システム１１の構成について、図２５を用いて説明する。

【０１４２】

同図に示すように、検知システム１１は、情報処理装置としての機器１００と、管理装置２００ａとから構成される。そして、機器１００及び管理装置２００ａは、ネットワークを介して接続されている。

【０１４３】

管理装置２００ａは、判断部２１０、モジュール無効化部２２０、監視パターン更新部２３０及び通信部２５０から構成される。

図２５において、実施の形態１と同様の機能を有する構成要素には、図１と同一の符号を付し、詳細な説明を省略する。以下では、検知システム１１の特徴的な構成要素及び処理について詳細に説明する。

【０１４４】

（２）監視パターン更新部２３０の構成

監視パターン更新部２３０は、機器１００内部の検知モジュール群１３０の監視パターンを更新する場合に、判断部２１０による監視パターン更新の指示に応じて、検知モジュール群１３０内の各検知モジュールの監視パターンを更新するために、無効化処理のための監視パターンを生成し、生成した監視パターンを各検知モジュールへ送信する。

【０１４５】

監視パターン更新部２３０は、図２６に示すように、受信部８０１、送信部８０２、監視パターン生成部８０３及び制御部８０４から構成されている。

（ａ）受信部８０１

受信部８０１は、判断部２１０から、監視パターンの生成を示す生成指示及び指示した時点での検知モジュールリストを受信する。検知モジュールリストは、機器１００が有する検知モジュール群１３０に含まれる全ての検知モジュールをそれぞれ識別する識別番号を含んでいる。また、無効化すべき検知モジュールを識別する識別番号を受信する。

【０１４６】

受信部８０１は、受信した監視パターンの生成指示を制御部８０４へ出力する。また、受信した検知モジュールリストを、制御部８０４を介して、監視パターン生成部８０３へ出力する。また、無効化すべき検知モジュールを識別する識別番号を、制御部８０４を介して、監視パターン生成部８０３へ出力する。

【０１４７】

（ｂ）監視パターン生成部８０３

監視パターン生成部８０３は、受信部８０１から、制御部８０４を介して、検知モジュールリストを受信する。

【０１４８】

検知モジュールリストを受信すると、監視パターン生成部８０３は、受信した検知モジュールリストを用いて、どの検知モジュールがどの検知モジュールを監視するかを決定し、機器１００が有する検知モジュール群１３０における全体の監視パターンを生成する。

【０１４９】

特に、監視パターン生成部８０３は、受信した無効化すべきモジュールを識別する識別番号を用いて、無効化すべき検知モジュール以外の検知モジュールが一方向に循環して監視をするように、循環監視パターン（循環型の監視パターンとも呼ぶ）を生成する。

【０１５０】

なお、循環監視パターンの具体例については、後述する。

なお、監視パターン生成部８０３は、全体の監視パターンとして、例えば、すべての検知モジュールが他のすべての検知モジュールを監視するように、決定してもよい。

【０１５１】

（ｃ）送信部８０２

送信部８０２は、通信部２５０及びネットワークを介して、機器１００へ検知モジュール毎の監視パターンを送信する。また、判断部２１０へ監視パターンの生成及び送信の終了を通知する。

【０１５２】

（ｄ）制御部８０４

制御部８０４は、受信部８０１から、監視パターンの生成指示を受信する。

監視パターンの生成指示を受信すると、制御部８０４は、監視パターン生成部８０３に対して、機器１００が有する検知モジュール群１３０における全体の監視パターンを生成し、検知モジュール毎の監視パターンを生成し、機器１００へ検知モジュール毎の監視パターンを送信して、機器１００において監視パターンの更新処理をさせるように、制御す

る。
【０１５３】
（３）検証処理の動作
図２７及び図２８は、検証処理の動作を示すフローチャートである。
図２７のＳ２２１１からＳ２２１５までの動作は、実施の形態１における図２０のＳ２２０１からＳ２２０５までの動作にそれぞれ対応し同様の動作であり、無効化処理（Ｓ２２１７）は、実施の形態１の無効化処理（Ｓ２２０６）と同様の動作であるため、説明を省略する。以下で、ステップＳ２２１６の処理について説明する。
【０１５４】
判断部２１０は、異常な検知モジュールと特定した検知モジュールの無効化処理を実行するかを判断する（Ｓ２２１５）。無効化処理を実行しないと判断した場合（Ｓ２２１５でＮＯ）、検証処理を終了する。無効化処理を実行すると判断した場合（Ｓ２２１５でＹＥＳ）、正常な検知モジュールを特定する正常モジュール特定処理を行う（Ｓ２２１６）。
【０１５５】
（４）正常モジュール特定処理
図２９及び図３０は、正常モジュール特定処理の動作を示すフローチャートである。
判断部２１０は、無効化処理を実行すると判断し、監視パターン更新部２３０へ監視パターン生成指示を、検知モジュールリスト及び無効化すべき検知モジュールの識別番号と共に送信する（Ｓ２３０１）。ここでは、検知モジュール１３５を無効化すると判断した例を用いて説明する。
【０１５６】
監視パターン更新部２３０は、判断部２１０から、監視パターンの生成を示す生成指示、検知モジュールリスト及び無効化すべき検知モジュールを識別する識別番号（ここでは、検知モジュール１３５の識別番号）を受信する。検知モジュールリスト及び検知モジュール１３５の識別番号から、検知モジュール１３５以外の検知モジュール内での循環監視パターンを生成する（Ｓ２３０２）。
【０１５７】
循環監視パターンとは、一方向に循環して改ざん検出処理を行う複数の検知モジュールについて、監視対象（検証対象）のモジュールに関する情報を記述したものである。具体的には、循環監視パターンには、モジュール識別子、メモリ上の位置、サイズ、アドレス、ファイル名等が記述されている。
【０１５８】
図３１に示す具体例を用いて説明する。
一方向に循環して改ざん検出処理を行う一群の検知モジュールとは、図３１に示す具体例においては、検知モジュール１３１、検知モジュール１３２、検知モジュール１３３及び検知モジュール１３４である。図３１の矢印Ａ２１００、Ａ２１０１、Ａ２１０２及びＡ２１０３が示すように、検知モジュール１３１が検知モジュール１３２を検証し、検知モジュール１３２が検知モジュール１３３を検証し、検知モジュール１３３が検知モジュール１３４を検証し、検知モジュール１３４が検知モジュール１３１を検証する関係を有している。
【０１５９】
これらの検知モジュール１３１、１３２、１３３及び１３４における監視の形態の情報を記述したものが、循環監視パターンである。
図２９に戻り、監視パターン更新部２３０は、各検知モジュールへ監視パターンを送信する（Ｓ２３０３）。
【０１６０】
各検知モジュールは監視パターンを受信する（Ｓ２３０４）。さらに、各検知モジュールは受信した監視パターンを保持している監視パターンに上書きすることにより更新する（Ｓ２３０５）。更新が完了すると、完了通知を監視パターン更新部２３０へ送信する（

Ｓ２３０６）。
【０１６１】
監視パターン更新部２３０は、各検知モジュールから完了通知を受信すると（Ｓ２３０６）、判断部２１０へ監視パターン更新の完了通知を送信する（Ｓ２３０７）。
監視パターンを更新した、各検知モジュールは、更新された監視パターンにしたがって、改ざん検出を実行する。
【０１６２】
検知モジュール１３１は、検知モジュール１３２の改ざん検出を行い（Ｓ２３０８）、改ざん検出結果を判断部２１０へ送信する（Ｓ２３０９）。
検知モジュール１３２は、検知モジュール１３３の改ざん検出を行い（Ｓ２３１０）、改ざん検出結果を判断部２１０へ送信する（Ｓ２３１１）。
【０１６３】
検知モジュール１３３は、検知モジュール１３４の改ざん検出を行い（Ｓ２３１２）、改ざん検出結果を判断部２１０へ送信する（Ｓ２３１３）。
検知モジュール１３４は、検知モジュール１３１の改ざん検出を行い（Ｓ２３１４）、改ざん検出結果を判断部２１０へ送信する（Ｓ２３１５）。
【０１６４】
判断部２１０は各検知モジュールから、改ざん検出結果を受信し、特定処理を行う（Ｓ２３１６）。
（ａ）特定処理の動作
図３２は、特定処理の動作を示すフローチャートである。
【０１６５】
判断部２１０は、各検知モジュールから受信したすべての改ざん検出結果が「改ざんされていない（正常）」であるかを判断する（Ｓ２４０１）。すべての改ざん検出結果が「改ざんされていない（正常）」である場合（Ｓ２４０１でＹＥＳ）、すべての検知モジュールは改ざんされていない正常な検知モジュールであると特定し（Ｓ２４０２）、特定処理を終了する。
【０１６６】
すべての改ざん検出結果が「改ざんされていない（正常）」でない場合（Ｓ２４０１でＮＯ）、改ざん検出結果に矛盾があるかを判定する（Ｓ２４０３）。改ざん検出結果に矛盾がない場合（Ｓ２４０３でＮＯ）、機器を停止する。改ざん検出結果に矛盾がある場合（Ｓ２４０３でＹＥＳ）、改ざん検出結果に矛盾がある検知モジュールを異常な検知モジュールと特定する（Ｓ２４０４）。
【０１６７】
ここで、改ざん検出結果の矛盾について、図３３に示す例を用いて説明する。
図３３によれば、○印２１１０、○印２１１１及び○印２１１２に表されるように、検知モジュール１３１は検知モジュール１３２を、検知モジュール１３２は検知モジュール１３３を、検知モジュール１３３は検知モジュール１３４を「改ざんされていない（正常）」と判定している。しかし、×印２１１３に表されるように、検知モジュール１３４は検知モジュール１３１を「改ざんされている（異常）」と判定している。
【０１６８】
ここで、検知モジュール１３１が正常な検知モジュールであると仮定すると、正常な検知モジュール１３１が「改ざんされていない（正常）」と判定している検知モジュール１３２は正常であり、正常な検知モジュール１３２が「改ざんされていない（正常）」と判定している検知モジュール１３３は正常であり、正常な検知モジュール１３３が「改ざんされていない（正常）」と判定している検知モジュール１３４は正常であるはずである。しかし、正常な検知モジュール１３４が、正常な検知モジュール１３１に対して、「改ざんされている（異常）」と判定しているため、検知モジュール１３１は正常であるという仮定に矛盾が発生する。このため、検知モジュール１３１が正常な検知モジュールであるとする仮定は、誤りであり、検知モジュール１３１は改ざんされている異常な検知モジュ

ールであると特定することができる。

【０１６９】

異常な検知モジュールと特定した後、再び、正常モジュール特定処理を行う。

以上説明したように、循環監視パターンを用いて、すべての改ざん検出結果が「改ざんされていない（正常）」であると判定された場合に、すべての検知モジュールは改ざんされていない正常な検知モジュールであると特定することができる。また、循環監視パターンを用いることにより、最小限の監視数により、検知モジュールの監視を行うことができる。

【０１７０】

３．実施の形態３

本発明に係る実施の形態３としてのソフトウェア更新システム１２について説明する。

ソフトウェア更新システム１２においては、検知処理で保護制御モジュール１２０の改ざんを検出した場合、保護制御モジュール１２０を新しい保護制御モジュール１２１へ更新する。ソフトウェア更新システムにおける保護制御モジュール１２０の更新の方法は、特許文献３に詳しく記載されている方法に本発明を適用した方法である。ここでは、特許文献３における更新モジュールの更新機能を検知モジュールに含める。

【０１７１】

３．１　ソフトウェア更新システム１２の構成

（１）全体構成

ソフトウェア更新システム１２の構成について、図３４を用いて説明する。

【０１７２】

同図に示すように、ソフトウェア更新システム１２は、情報処理装置としての機器１００ａと、管理装置２００ｂとから構成される。そして、機器１００ａ及び管理装置２００ｂは、ネットワークを介して接続されている。

【０１７３】

管理装置２００ｂは、判断部２１０、モジュール無効化部２２０、監視パターン更新部２３０、更新用ソフトウェア配布部２４０及び通信部２５０から構成される。また、機器１００ａは、検知モジュール群１３０ａ、保護制御モジュール１２０ａ、アクセス制御モジュール１４０、アプリ１１０及びアプリ１１１を含んで構成されている。

【０１７４】

図３４において、実施の形態２と同様の機能を有する構成要素には、図２と同一の符号を付し、詳細な説明を省略する。以下では、ソフトウェア更新システム１２の特徴的な構成要素及び処理について詳細に説明する。

【０１７５】

（２）機器１００ａの構成

（ａ）保護制御モジュール１２０aの構成

ここでは、保護制御モジュール１２０aの詳細について説明する。

【０１７６】

図３５は、保護制御モジュール１２０aの機能的な構成を示す機能ブロック図である。

同図に示すように、保護制御モジュール１２０aは、図３の保護制御モジュール１２０の構成に加え、暗復号鍵分散部３０８、証明書生成部３０９、暗復号鍵復元部３１０、及び暗復号鍵生成部３１１から構成される。

【０１７７】

暗復号鍵分散部３０８は、初期設定時や次ラウンド準備時に、暗復号鍵から秘密分散法を用いて分散情報を生成する。

証明書生成部３０９は、暗復号鍵から生成された分散情報を復元したときに、正しく復元できたか否かを検証するために用いられる証明書を生成する。

【０１７８】

暗復号鍵復元部３１０は、配置情報に基づいて、各検知モジュールから、各検知モジュールに配布されていた分散情報を取得する。そして、暗復号鍵復元部３１０は、取得した

分散情報から暗復号鍵を復元し、復元した暗復号鍵を復号ロード部３０４に送信する。

【０１７９】

暗復号鍵生成部３１１は、アプリ１１０、１１１を暗復号するための暗復号鍵を生成する。

（ｂ）検知モジュール群１３０ａの構成

検知モジュール群１３０ａは、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａから構成されている。ここでは、検知モジュール１３１ａの詳細について説明し、その他の検知モジュール１３２ａ、１３３ａ、１３４ａ、１３５ａについての説明を省略する。

【０１８０】

図３６は、検知モジュール１３１ａの機能的な構成を示す機能ブロック図である。他の検知モジュールも同様の構成を有する。

同図に示すように、検知モジュール１３１ａは、図４の検知モジュール１３１の構成に加え、更新部４０７、認証部４０８、分散情報保持部４０９から構成される。

【０１８１】

更新部４０７は、制御部４０３の制御に基づき、管理装置２００ｂと連携して、機器１００a内部のソフトウェア、具体的には、アプリ１１０及び１１１、保護制御モジュール１２０ａ、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａを更新する。

【０１８２】

認証部４０８は、検知モジュールの認証鍵対（認証秘密鍵（認証私有鍵と呼ぶ事もある。）及び認証公開鍵）を保持し、他のモジュールとの認証を行う。

分散情報保持部４０９は、保護制御モジュール１２０ａがアプリ１１０、１１１の暗復号処理に利用する暗復号鍵から生成した分散情報（ｓｈａｒｅ）と、保護制御モジュール１２０ａが分散情報を配布したときの配置情報を保持する。配置情報は、どの分散情報をどの検知モジュールに配布したかを記述した情報である。

【０１８３】

署名方式に関しては非特許文献１の１７１ページから１８７ページに、証明書に関しては非特許文献２に詳しく説明されている。また、分散情報に関しては特許文献２に詳しく説明されている。

【０１８４】

（ｃ）更新用ソフトウェア配布部２４０

図３７は、更新用ソフトウェア配布部２４０の機能的な構成を示す機能ブロック図である。

【０１８５】

同図に示すように、更新用ソフトウェア配布部２４０は、受信部９０１、送信部９０２、制御部９０３、認証部９０４、暗号鍵生成部９０５、暗号処理部９０６、検知モジュール選択部９０７、証明書生成部９０８、署名秘密鍵保持部９０９、更新用ソフトウェア保持部９１０及び暗号鍵保持部９１１から構成される。

【０１８６】

受信部９０１は、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａから保護制御モジュール１２０ａに対する改ざん検出結果、及び検知モジュール間の相互監視結果を受信する。

【０１８７】

送信部９０２は、機器１００ａのアプリ１１０、１１１、保護制御モジュール１２０ａを更新する必要がある場合に、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ、更新処理の依頼、更新用ソフトウェア、復号に必要な鍵などのデータを送信する。

【０１８８】

制御部９０３は、更新用ソフトウェア配布部２４０の各構成要素を制御する。

認証部９０４は、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａ、及び保護制御モジュール１２０ａと相互認証を行う。

【０１８９】

暗号鍵生成部９０５は、更新用ソフトウェアを検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ送信するときに使用する暗号鍵を生成する。

暗号処理部９０６は、暗号鍵生成部９０５が生成した暗号鍵を用いて、更新用ソフトウェアを暗号化する。また、暗号処理部９０６は、各検知モジュール固有の鍵を用いて、暗号鍵を暗号化する。

【０１９０】

暗号鍵及び更新用ソフトウェアは、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ一度にすべてが送信されるのではなく、更新処理の中で、それぞれのデータが必要になったタイミングで、それぞれ各検知モジュールへ送信される。

【０１９１】

検知モジュール選択部９０７は、保護制御モジュール１２０ａを更新する場合に、更新処理に使用する検知モジュールを選択する。暗号処理部９０６は、更新用の保護制御モジュールの暗号化に使用した暗号鍵を、検知モジュール選択部９０７が選択した検知モジュール固有の鍵を用いて暗号化する。そして、送信部９０２は、検知モジュール選択部９０７が選択した検知モジュールへ、暗号鍵及び更新用の保護制御モジュールを送付する。

【０１９２】

証明書生成部９０８は、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａの認証公開鍵に対して署名秘密鍵（署名私有鍵とも呼ぶ）を用いて認証証明書を生成する。また、証明書生成部９０８は、更新用の保護制御モジュールに対して署名秘密鍵を用いて、機器１００にて、保護制御モジュールが正しく更新されたか否かを検証するための更新検証証明書を生成する。

【０１９３】

署名秘密鍵保持部９０９は、証明書生成部９０８が証明書を生成するときに用いる署名秘密鍵を保持する。

更新用ソフトウェア保持部９１０は、保護制御モジュール１２０ａが攻撃された場合に更新するための更新用の保護制御モジュールを保持する。

【０１９４】

暗号鍵保持部９１１は、暗号鍵生成部９０５が生成した暗号鍵及び暗号処理部９０６により暗号化された暗号鍵を保持する。

３．２　ソフトウェア更新システム１２の動作

続いて、ソフトウェア更新システム１２の動作を説明する。

【０１９５】

（１）全体動作

ソフトウェア更新システム１２は、上記実施の形態の初期設定処理（図１０のＳ１００）、検知処理（図１０のＳ２００）に加えて、次に示す４つの処理－解析・判断処理、相互認証処理、回復処理、次ラウンド準備処理を行う。図３８はソフトウェア更新システム１２の動作を示すフローチャートである。

【０１９６】

ソフトウェア更新システム１２は、初期設定処理（Ｓ１０１）を行い、検知処理（Ｓ２００）を行う。

次に、ソフトウェア更新システム１２は、図１３のＳ２０１で保護制御モジュール１２０ａの改ざんが検出された場合に、保護制御モジュール１２０ａを解析し、更新する必要があるか否か判断する解析・判断処理を行う（Ｓ３００）。

【０１９７】

次に、ソフトウェア更新システム１２は、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａと更新用ソフトウェア配布部２４０とが互いに正しいソフトウェアであるか否かを確認するための相互認証処理を行う（Ｓ４００）。

【０１９８】
次に、ソフトウェア更新システム１２は、回復処理を行う（Ｓ５００）。
回復処理とは、検知モジュール群１３０ａに含まれる検知モジュール間で相互に改ざん検出処理を行った後、更新用の保護制御モジュールを機器１００ａへインストールし、そして、機器１００ａにおいて、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ埋め込まれた分散情報を用いて、保護制御モジュールを更新する処理である。
【０１９９】
その後、ソフトウェア更新システム１２は、次に保護制御モジュールの更新が必要となる場合に備えて、更新に必要な鍵データや分散情報を生成し、各検知モジュールに埋め込む次ラウンド準備処理を行う（Ｓ６００）。その後、ソフトウェア更新システム１２は、Ｓ２００の検知処理へ戻り、処理を続ける。
【０２００】
（２）初期設定処理の動作
ここでは、図３９に示すシーケンス図及び図４０に示すフローチャートを用いて、ソフトウェア更新システム１２の初期設定処理（図３８のＳ１０１）の詳細について説明する。
【０２０１】
図３９におけるＳ１２０１からＳ１２０２の動作は、実施の形態１における図１１のＳ１００１からＳ１００２の動作にそれぞれ対応し同様の動作であるため、説明を省略する。
【０２０２】
機器１００ａは、機器の初期化後、保護制御モジュール１２０ａ、及び、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａに対して、初期化指示を出力する（Ｓ１２０３、Ｓ１２０４）。
【０２０３】
保護制御モジュール１２０ａは、暗復号鍵から秘密分散法を用いて分散情報を生成する（Ｓ１２０５）。なお、保護制御モジュール１２０ａは、分散情報保持部４０９を備える検知モジュールの数と同数の分散情報を生成する。検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａがすべて分散情報保持部４０９を備えている場合、保護制御モジュール１２０ａは、５つの分散情報を生成する。
【０２０４】
更に、保護制御モジュール１２０ａは、署名秘密鍵を用いて、暗復号鍵証明書を生成する（Ｓ１２０６）。暗復号鍵証明書は、暗復号鍵の復元時に、暗復号鍵が正しく復元できたか否かを確認するための証明書である。
【０２０５】
保護制御モジュール１２０ａは、生成した分散情報と暗復号鍵証明書とを、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ送信する（Ｓ１２０７、Ｓ１２０８）。
【０２０６】
なお、保護制御モジュール１２０ａは、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａが、それぞれ異なる分散情報の組を保持するように、各検知モジュールに分散情報の組を送信する。更に、保護制御モジュール１２０ａは、どの検知モジュールへどの分散情報を送信したかを示す配置情報を、各検知モジュールへ送信する。各検知モジュールに送信される配置情報は、同一の情報である。
【０２０７】
暗復号鍵から秘密分散法を用いて分散情報を生成する方法や、分散情報を検知モジュールへ送信する方法については、特許文献２の４７ページから４９ページに詳しく説明されている。特許文献２における秘密鍵ｄを本実施の形態の暗復号鍵に対応させ、認証局装置を保護制御モジュール１２０ａに対応させ、分散情報保持装置を検知モジュール１３１ａ

、１３２ａ、１３３ａ、１３４ａ、１３５ａに対応させることで、特許文献２と同じ方法を用いることができる。

【０２０８】

保護制御モジュール１２０ａから分散情報、配置情報及び暗復号鍵証明書を受信した各検知モジュールは、検知モジュール初期化処理を行う（Ｓ１２０９）。

（ａ）検知モジュール初期化処理の動作

図４０は、検知モジュール初期化処理（図３９のＳ１２０９）の動作を示すフローチャートである。

【０２０９】

図４０のＳ１３０２からＳ１３０５の動作は、実施の形態１における図１２のＳ１１０１からＳ１１０４の動作にそれぞれ対応し同様の動作であるため、説明を省略する。

検知モジュール１３１ａは、保護制御モジュール１２０ａから分散情報、配置情報及び暗復号鍵証明書を受信し、受信した各情報を分散情報保持部４０９に保持する（Ｓ１３０１）。

【０２１０】

（３）検知処理の動作

図３８のＳ２００の検知処理は、実施の形態１や実施の形態２の検知処理の動作と同様であるので、ここでは省略する。

【０２１１】

（４）解析・判断処理の動作

続いて、図４１のシーケンス図を用いて、解析・判断処理（図３８のＳ３００）の詳細について説明する。なお、図４１では、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａのそれぞれが個別に行う処理を、検知モジュール群１３０ａが行う処理としてまとめて記載している。

【０２１２】

検知処理において、判断部２１０が各検知モジュールから保護制御モジュール１２０ａの改ざん検出結果を受信すると、判断部２１０は、受信した改ざん検出結果に基づいて、保護制御モジュール１２０ａが正常であるか異常であるか（改ざんされているか否か）を判定する（Ｓ３００１）。

【０２１３】

判定方法の一例として、例えば、所定数の又は所定数以上の検知モジュールが改ざんを検出した場合には、保護制御モジュール１２０ａは異常である（改ざんされている）と判定し、また、所定数未満の検知モジュールが改ざんを検出した場合には、保護制御モジュール１２０ａは正常である（改ざんされていない）と判定する。前記所定数は、検知モジュール群１３０ａに含まれる検知モジュールの過半数としてもよい。また、検知処理のＳ２２１６と同様の正常モジュール特定処理を行い、正常と特定した検知モジュールが保護制御モジュール１２０ａの改ざんを検出した場合、保護制御モジュール１２０ａは異常である（改ざんされている）と判定し、正常と特定した検知モジュールが保護制御モジュール１２０ａの改ざんを検出しなかった場合には、保護制御モジュール１２０ａは正常である（改ざんされていない）と判定するとしてもよい。

【０２１４】

保護制御モジュール１２０ａが改ざんされていると判定した場合（Ｓ３００１で「改ざんされている」）、判断部２１０は、保護制御モジュール１２０ａを回復する必要があるか否かを判断するために、検知モジュール群１３０ａに対して、保護制御モジュール１２０ａのどの部分が改ざんされたかなどの改ざん情報の通知を依頼する（Ｓ３００２）。

【０２１５】

検知モジュール群１３０ａは、改ざん情報の通知を依頼されると、改ざん情報を収集して（Ｓ３００３）、判断部２１０へ通知する（Ｓ３００４）。

判断部２１０は、改ざん情報に基づいて、保護制御モジュール１２０ａを回復するか、機器１００ａをリボークするか、または、何もしないかを判断する（Ｓ３００５）。

【０２１６】
保護制御モジュール１２０ａを回復する場合（Ｓ３００５で「回復する」）、判断部２１０は、更新用の保護制御モジュールを準備し（Ｓ３００６）、検知モジュール群１３０ａに、更新処理の開始を指示する（Ｓ３００７）。また、機器１００ａをリボークする場合には（Ｓ３００５で「リボーク依頼」）、アプリ１１０、１１１にサービスを提供しているサーバに対して、機器１００ａをリボークするように依頼する（Ｓ３００８）。何もしない場合（Ｓ３００５で「何もしない」）、検知処理へ戻る。
【０２１７】
保護制御モジュール１２０ａが正常である（改ざんされていない）と判定した場合（Ｓ３００１で「改ざんされていない」）は、検知処理へ戻る。
（５）相互認証処理の動作
次に、図４２及び図４３のシーケンス図を用いて、ソフトウェア更新システム１２による相互認証処理（図３８のＳ４００）の詳細について説明する。
【０２１８】
管理装置２００ｂの判断部２１０が、解析・判断処理において、保護制御モジュール１２０ａを回復する必要があると判断した場合、判断部２１０は、更新用ソフトウェア配布部２４０へ、保護制御モジュール１２０ａの回復を指示する。
【０２１９】
更新用ソフトウェア配布部２４０は、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ更新処理の開始を指示した後、各検知モジュールとの間で、それぞれ１対１の相互認証処理を行う。これにより、機器１００ａが不正な管理装置と接続したり、管理装置２００ｂが不正な機器と接続することを防止する。なお、相互認証処理において、更新用ソフトウェア配布部２４０は、署名秘密鍵及び署名公開鍵を使用し、各検知モジュールは、認証鍵対（認証秘密鍵及び認証公開鍵）を使用する。
【０２２０】
図４２は、検知モジュール１３１ａが更新用ソフトウェア配布部２４０を認証するときのシーケンス図である。なお、検知モジュール１３２ａ、１３３ａ、１３４ａ、１３５ａも、図４２の検知モジュール１３１ａと同様に動作し、更新用ソフトウェア配布部２４０を認証する。
【０２２１】
検知モジュール１３１ａは、乱数生成器を用いて乱数（チャレンジデータ）を生成し（Ｓ４００１）、生成したチャレンジデータを更新用ソフトウェア配布部２４０へ送信する（Ｓ４００２）。この時、検知モジュール１３１ａを識別するための検知モジュールの識別子を、チャレンジデータと共に送信する。更新用ソフトウェア配布部２４０は、受信したチャレンジデータに署名秘密鍵を用いて署名データを生成し（Ｓ４００３）、生成した署名データをレスポンスデータとして、検知モジュール１３１ａへ返信する（Ｓ４００４）。
【０２２２】
検知モジュール１３１ａは、更新用ソフトウェア配布部２４０からレスポンスデータを受信すると（Ｓ４００５）、署名公開鍵を用いて、レスポンスデータが、チャレンジデータの署名データと一致するか否か検証する（Ｓ４００６）。
【０２２３】
検証の結果、レスポンスデータが正しく、更新用ソフトウェア配布部２４０が正当なモジュールである場合（Ｓ４００７で「正しい」）、検知モジュール１３１ａは、処理を継続する。レスポンスデータが正しくなく、更新用ソフトウェア配布部２４０が不正なモジュールである場合（Ｓ４００７で「正しくない」）、検知モジュール１３１ａは、エラーを出力し、処理を停止する（Ｓ４００８）。
【０２２４】
次に、更新用ソフトウェア配布部２４０が、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａを認証する。

図４３は、更新用ソフトウェア配布部２４０が各検知モジュール（一例として、検知モジュール１３１ａ）を認証するときのシーケンス図である。

【０２２５】

更新用ソフトウェア配布部２４０は、チャレンジデータを送信してきた各検知モジュールに対して、乱数生成器を用いてそれぞれ異なる乱数（チャレンジデータ）を生成し（Ｓ４１０１）、生成したチャレンジデータを、各検知モジュールへ個別に送信する（Ｓ４１０２）。

【０２２６】

各検知モジュールは、受信したチャレンジデータに認証秘密鍵を用いて署名データを生成し（Ｓ４１０３）、生成した署名データをレスポンスデータとして更新用ソフトウェア配布部２４０へ返信する（Ｓ４１０４）。

【０２２７】

このとき、各検知モジュールは、レスポンスデータと共に認証公開鍵と認証鍵証明書とを更新用ソフトウェア配布部２４０へ送信する。

更新用ソフトウェア配布部２４０は、それぞれの検知モジュールからレスポンスデータ、認証公開鍵及び認証鍵証明書を受信する（Ｓ４１０４）。更新用ソフトウェア配布部２４０は、認証鍵証明書が、自身が発行した証明書であるか否か検証し、更に、認証鍵証明書を用いて、認証公開鍵の正当性を検証する（Ｓ４１０５）。

【０２２８】

認証鍵証明書及び認証公開鍵が不正である場合（Ｓ４１０５で「鍵が正しくない」）、更新用ソフトウェア配布部２４０は、処理を停止する（Ｓ４１０６）。

認証鍵証明書及び認証公開鍵が正当であれば（Ｓ４１０５で「証明書及び鍵が正しい」）、更新用ソフトウェア配布部２４０は、認証公開鍵を用いて、受信したレスポンスデータがチャレンジデータの署名データと一致するか否か検証する（Ｓ４１０７）。

【０２２９】

次に、更新用ソフトウェア配布部２４０は、正しいレスポンスデータを返した検知モジュール（正当な検知モジュール）を用いて回復処理を行うかを判断する（Ｓ４１０８）。ここでは、正しいレスポンスデータを返した検知モジュール（正当な検知モジュール）の数が、予め設定されている回復処理に必要な数以上であるかを判断する。

【０２３０】

回復処理を行わない場合（Ｓ４１０８でＮＯ）、更新用ソフトウェア配布部２４０は、処理を停止する（Ｓ４１０６）。回復処理を行う場合（Ｓ４１０８でＹＥＳ）、相互認証処理を終了し、回復処理に移る。

【０２３１】

また、更新用ソフトウェア配布部２４０は、相互認証処理において、正当性が確認されたすべての検知モジュールの検知モジュール識別子を記載した認証リストを作成する。そして、これ以降の回復処理では、認証リストに識別子が記載されている検知モジュールのみを利用する。

【０２３２】

（６）回復処理の動作

続いて、図４４から５１を用いて、回復処理（図３８のＳ５００）の詳細について説明する。回復処理は、上述した相互認証処理において、相互認証が成功した場合に、改ざんされた保護制御モジュール１２０ａを、新しい更新用の保護制御モジュールへ更新する処理である。

【０２３３】

図４４は、回復処理時の動作を示すフローチャートである。

先ず、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａが、相互監視処理を行う（Ｓ５０００）。相互監視処理では、各検知モジュールが、他の検知モジュールの改ざん検出処理を実行する。

【０２３４】

さらに、更新用保護制御モジュールを用いて、保護制御モジュール１２０ａを更新する更新処理を行う（Ｓ５１００）。

そして、暗号化されたアプリ１１０、１１１を再暗号化する再暗号化処理を行う（Ｓ５２００）。

【０２３５】

（ａ）相互監視処理

ここでは、図４５のシーケンス図を用いて、相互監視処理（図４４のＳ５０００）の詳細について説明する。

【０２３６】

相互監視処理では、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａが、検知モジュール群１３０ａ内の他の検知モジュールに対して改ざん検出処理を実行する。相互監視処理において、どの検知モジュールに対して改ざん検出処理を実行するかは、検知モジュールが保持する監視パターンに記述されている。監視パターンには、改ざん検出対象であるモジュールに関する情報（モジュール識別子、メモリ上の位置、サイズ、アドレス、ファイル名等）が記述されている。

【０２３７】

相互監視処理の監視パターンは、循環監視パターンを用いる。ここでは、検知モジュール１３１ａが検知モジュール１３２ａを検証し、検知モジュール１３２ａが検知モジュール１３３ａを検証し、検知モジュール１３３ａが検知モジュール１３４ａを検証し、検知モジュール１３４ａが検知モジュール１３５ａし、検知モジュール１３５ａが検知モジュール１３１ａを検証する循環監視パターンを例に説明する。

【０２３８】

検知モジュール１３１ａは、検知モジュール１３２ａの改ざん検出を行う（Ｓ５００１）。改ざん検出結果を判断部２１０へ送信する（Ｓ５００２）。

検知モジュール１３２ａは、検知モジュール１３３ａの改ざん検出を行う（Ｓ５００３）。改ざん検出結果を判断部２１０へ送信する（Ｓ５００４）。

【０２３９】

検知モジュール１３３ａは、検知モジュール１３４ａの改ざん検出を行う（Ｓ５００５）。改ざん検出結果を判断部２１０へ送信する（Ｓ５００６）。

検知モジュール１３４ａは、検知モジュール１３５ａの改ざん検出を行う（Ｓ５００７）。改ざん検出結果を判断部２１０へ送信する（Ｓ５００８）。

【０２４０】

検知モジュール１３５ａは、検知モジュール１３１ａの改ざん検出を行う（Ｓ５００９）。改ざん検出結果を判断部２１０へ送信する（Ｓ５０１０）。

判断部２１０は各検知モジュールから、改ざん検出結果を受信する（Ｓ５０１１）。判断部２１０は、改ざんを検出した検知モジュールが存在するかを判定する（Ｓ５０１２）。改ざんを検出した検知モジュールが存在する場合（Ｓ５０１２でＹＥＳ）、回復処理を停止する（Ｓ５０１３）。改ざんを検出した検知モジュールが存在しない場合（Ｓ５０１２でＮＯ）、すべての検知モジュールは改ざんされていない正常な検知モジュールと特定し、処理を継続する。

【０２４１】

上記循環監視パターンで、検知モジュール間で相互監視をすることにより、すべての改ざん検出結果が「改ざんされていない（正常）」である場合、すべての検知モジュールが正常であると一度に特定することができる。これにより、効率的に相互監視処理を行うことができる。

【０２４２】

（ｂ）更新処理

続いて、図４６から図４９のシーケンス図を用いて、更新処理（図４４のＳ５１００）の詳細について説明する。

【０２４３】

先ず、更新用ソフトウェア配布部２４０の証明書生成部９０８は、署名秘密鍵を用いて、更新検証証明書を生成する（Ｓ５１０１）。更新検証証明書は、新しい保護制御モジュールが正しくインストールできたか否か、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａが確認するための証明書である。更新用ソフトウェア配布部２４０は、生成した証明書を、各検知モジュールへ送信する（Ｓ５１０２）。

【０２４４】

次に、更新用ソフトウェア配布部２４０の暗号鍵生成部９０５は、新しい保護制御モジュールを多重に暗号化するための暗号鍵を２つ（第１の鍵及び第２の鍵）生成する（Ｓ５１０３）。暗号処理部９０６は、第２の鍵を用いて新しい保護制御モジュールを暗号化し、暗号化新保護制御モジュールを生成する（Ｓ５１０４）。暗号処理部９０６は、暗号化新保護制御モジュールに対して、第１の鍵を用いてさらに暗号化し、多重暗号化新保護制御モジュールを生成する（Ｓ５１０５）。

【０２４５】

更新用ソフトウェア配布部２４０は、検知モジュール群１３０ａから検知モジュールを一つ選択し（Ｓ５１０６）、選択した検知モジュールの識別子を判断部２１０に通知する。ここでは、一例として、検知モジュール１３１ａを選択するものとする。

【０２４６】

更新用ソフトウェア配布部２４０は、選択した検知モジュール１３１ａへ多重暗号化新保護制御モジュールを送信し（Ｓ５１０７）、更に、第１の鍵を送信する（Ｓ５１０８）。

【０２４７】

検知モジュール１３１ａは、多重暗号化新保護制御モジュールと第１の鍵とを受信する（Ｓ５１０９）。検知モジュール１３１ａは、第１の鍵を用いて、多重暗号化新保護制御モジュールを復号し、暗号化新保護制御モジュールを取得する（Ｓ５１１０）。そして、復号が終了すると、その旨を更新用ソフトウェア配布部２４０へ通知する（Ｓ５１１１）。

【０２４８】

更新用ソフトウェア配布部２４０は、復号終了通知を受信すると、検知モジュール群１３０ａから、Ｓ５１０６で選択した検知モジュール１３１ａとは異なる検知モジュールを一つ選択する（Ｓ５１１２）。ここでは、一例として、検知モジュール１３２ａを選択するものとする。

【０２４９】

更新用ソフトウェア配布部２４０は、選択した検知モジュール１３２ａに、第２の鍵を送信する（Ｓ５１１３）。さらに、更新用ソフトウェア配布部２４０は、検知モジュール１３１ａに対して、Ｓ５１１０で取得した暗号化新保護制御モジュールを検知モジュール１３２ａへ送信するよう依頼する（Ｓ５１１４）。

【０２５０】

検知モジュール１３１ａは、更新用ソフトウェア配布部２４０からの依頼を受けて、暗号化新保護制御モジュールを検知モジュール１３２ａへ送信する（Ｓ５１１５）。

検知モジュール１３２ａは、更新用ソフトウェア配布部２４０から第２の鍵を受信し、検知モジュール１３１ａから暗号化新保護制御モジュールを受信する（Ｓ５１１６）。そして、第２の鍵を用いて、暗号化新保護制御モジュールを復号し、新しい保護制御モジュールを取得する（Ｓ５１１７）。

【０２５１】

検知モジュール１３２ａは、Ｓ５１１７で取得した新しい保護制御モジュールを保護制御モジュール１２０ａに上書きし、更新する（Ｓ５１１８）。そして、検知モジュール１３２ａは、更新の終了を他の検知モジュールへ通知する（Ｓ５１１９）。

【０２５２】

続いて、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａのそれぞれは、事前に受信した更新検証証明書を用いて、保護制御モジュールが正しく更新され

たか否か検証する（Ｓ５１２０）。さらに、検証結果を更新用ソフトウェア配布部２４０へ通知する（Ｓ５１２１）。

【０２５３】

更新用ソフトウェア配布部２４０は、各検知モジュールから送信された検証結果通知を受信する（Ｓ５１２１）。さらに、更新用ソフトウェア配布部２４０は、保護制御モジュールが正しく更新されたかを判定する（Ｓ５１２２）。正しく更新されていないと判定する場合（Ｓ５１２２でＮＯ）、更新用ソフトウェア配布部２４０は、機器１００を停止させる（Ｓ５１２３）。

【０２５４】

正しく更新されている場合（Ｓ５１２２でＹＥＳ）、更新用ソフトウェア配布部２４０は、更新処理終了を各検知モジュールへ通知する（Ｓ５１２４）。

各検知モジュールは、更新処理終了通知を受信すると（Ｓ５１２４）、新しい保護制御モジュールのＭＡＣ値を生成し、生成したＭＡＣ値と保護制御モジュールの識別子との組を、ＭＡＣ値テーブルに書き込む（Ｓ５１２５）。

【０２５５】

以上説明したように、更新処理では、更新用ソフトウェア配布部２４０が更新用の新保護制御モジュールを複数の鍵を用いて多重に暗号化し、検知モジュール群１３０ａへ送信する。検知モジュール群１３０ａは、受信した新保護制御モジュールで、保護制御モジュール１２０ａを更新する。

【０２５６】

このとき、更新用ソフトウェア配布部２４０は、多重に暗号化された新保護制御モジュールを復号するための複数の鍵を、検知モジュール群１３０ａに送信するタイミングを制御することにより、攻撃者が暗号化されていない新保護制御モジュールを入手することを困難にする。

【０２５７】

（ｃ）相互監視処理と更新処理との関係

上述した相互監視処理と更新処理とは、互いに連携しながら実行される。

相互監視処理は、更新用ソフトウェア配布部２４０から、検知モジュール群１３０ａに含まれる検知モジュールを送信先として、複数の鍵（第１の鍵及び第２の鍵）がそれぞれ送られる第１の時間帯、及び、検知モジュール群１３０ａに含まれる検知モジュールにより、多重暗号化新保護制御モジュール及び暗号化新保護制御モジュールがそれぞれ復号される第２の時間帯において、それぞれ、定期的に実施される。

【０２５８】

相互監視処理を定期的に実施する際の時間間隔は、例えば、更新用の新保護制御モジュールが通信路を通して、管理装置２００ｂから機器１００ａへ、完全に出力されるまでに要する時間より短い間隔である。完全に出力されるまでに１秒かかるのであれば、例えば、それより短い５００ミリ秒間隔のタイミングで監視処理を実行する。

【０２５９】

ここでは、図５０を用いて、相互監視処理と更新処理との連携動作について説明する。

先ず、機器１００ａは、管理装置２００ｂから多重暗号化新保護制御モジュールが送付される前に（Ｓ５１５０の前に）、相互監視処理（相互監視１（Ｓ５１６０））を実施する。改ざんされた異常な検知モジュールを選択して、更新処理を行わないようにするためである。

【０２６０】

その後、機器１００ａは、管理装置２００ｂにより送信された第１の鍵を検知モジュール１３１が受信する前に（Ｓ５１５１の前に）、相互監視処理（相互監視２（Ｓ５１６１））を実施し、機器１００ａが第１の鍵を受信する時に、異常な検知モジュールを選択していないことを確認する。

【０２６１】

さらに、検知モジュール１３１ａが第１の鍵を受信し（Ｓ５１５１）、第１の鍵を用い

て多重暗号化新保護制御モジュールを復号する間（Ｓ５１５２）、定期的に、検知モジュール１３１ａによる復号処理を中断して、相互監視処理（相互監視３－１（Ｓ５１６２）、３－２（Ｓ５１６３））を実施する。これにより、復号処理中に、検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａが攻撃されたとしても、暗号化新保護制御モジュールがすべて漏洩する前に検知モジュールが攻撃されたことを検出し、漏洩を防止することが可能となる。

【０２６２】

これ以降の処理は、上記と同様である。即ち、機器１００ａは、管理装置２００ｂにより送信された第２の鍵を検知モジュール１３２ａが受信する前に（Ｓ５１５４の前に）、相互監視処理（相互監視４（Ｓ５１６４））を実施し、機器１００ａが第２の鍵を受信する時に、異常な検知モジュールを更新処理において、選択していないことを確認する。

【０２６３】

さらに、検知モジュール１３２ａが第２の鍵を受信し（Ｓ５１５４）、第２の鍵を用いて暗号化新保護制御モジュールを復号する間（Ｓ５１５５）、定期的に、検知モジュール１３２ａによる復号処理を中断し、相互監視処理（相互監視５－１（Ｓ５１６５）、５－２（Ｓ５１６６））を実施する。最後に、相互監視処理（相互監視６（Ｓ５１６７））を実施する。その後、各検知モジュールから更新用ソフトウェア配布部２４０へ、検証結果通知が送信される（Ｓ５１５６）。

【０２６４】

これにより、新保護制御モジュールがすべて漏洩する前に検知モジュールが攻撃されたことを検出し、漏洩を防止することが可能となる。

ここで、相互監視処理において、検知モジュールに改ざんが検出された場合には、回復処理を停止する。これにより、管理装置２００ｂは、第１の鍵や第２の鍵の送信を中止することが可能となり、攻撃者は、多重暗号化新保護制御モジュールを復号するための鍵を入手することが不可能となる。

【０２６５】

（ｄ）再暗号化処理

続いて、図５１のシーケンス図を用いて、再暗号化処理（図４４のＳ５２００）の詳細について説明する。

【０２６６】

ここでは、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａをまとめて、検知モジュール群１３０ａとしている。

先ず、更新された保護制御モジュール（図５１の説明においては、更新前の保護制御モジュール１２０ａと区別するために、「保護制御モジュール１２１」という。）が、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａに対して、それぞれが保持している分散情報及び暗復号鍵証明書の送信を依頼する（Ｓ５２０１）。

【０２６７】

各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａは、保護制御モジュール１２１からの依頼を受けて、分散情報及び暗復号鍵証明書を送信する（Ｓ５２０２）。

【０２６８】

保護制御モジュール１２１は、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａから分散情報及び暗復号鍵証明書を受信し（Ｓ５２０３）、受信した分散情報から更新前の保護制御モジュール１２０が使用していた暗復号鍵（ここでは、「旧暗復号鍵」という。）を復元する（Ｓ５２０４）。更に、保護制御モジュール１２１は、暗復号鍵証明書を用いて、旧暗復号鍵が正しく復元されたか否か検証する（Ｓ５２０５）。

【０２６９】

旧暗復号鍵が正しく復元されなかった場合（Ｓ５２０５でＮＯ）、保護制御モジュール１２１は、異常な検知モジュールを炙り出す（言い換えると、どの検知モジュールが不正な分散情報を送信したか特定する）（Ｓ５２０６）。特定された異常な検知モジュールは

、管理装置２００ｂへ通知される。
【０２７０】
旧暗復号鍵が正しく復元された場合（Ｓ５２０５でＹＥＳ）、保護制御モジュール１２１の暗復号鍵生成部３１１は、新しい暗復号鍵（ここでは、「新暗復号鍵」という。）を生成する（Ｓ５２０７）。そして、復号ロード部３０４は、旧暗復号鍵を用いて暗号化されたアプリ（１１０、１１１）を復号し、新暗復号鍵を用いてアプリ（１１０、１１１）を再暗号化する（Ｓ５２０８）。
【０２７１】
分散情報から旧暗復号鍵を復元する方法や異常な検知モジュールの特定方法については、特許文献２の５０ページから５２ページに詳しく説明されている。特許文献２における秘密鍵ｄを本実施形態の暗復号鍵に対応させ、認証局装置を本実施形態の保護制御モジュール１２１に対応させ、分散情報保持装置を検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａに対応させることで、特許文献２と同じ方法が利用可能である。
【０２７２】
また、Ｓ５２０６において、異常な検知モジュールを特定するための方法として、実施の形態１における検知モジュール検知処理を用いてもよい。
（７）次ラウンド準備処理の動作
続いて、図５２のシーケンス図を用いて、次ラウンド準備処理（図３８のＳ６００）の詳細について説明する。次ラウンド準備処理では、回復処理（図３８のＳ５００）の終了後、次の回復処理のための準備を行う。以下、具体的に説明する。
【０２７３】
まず、保護制御モジュール１２１は、新暗復号鍵から、秘密分散法を用いて分散情報を生成し（Ｓ６００１）、更に、署名秘密鍵を用いて、新暗復号鍵証明書を生成する（Ｓ６００２）。そして、保護制御モジュール１２１は、生成した分散情報と暗復号鍵証明書とを各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ送信する（Ｓ６００３）。
【０２７４】
ここで、初期設定処理時と同様に、分散情報は、検知モジュールの数と同数が生成され、それぞれの検知モジュールが、異なる分散情報のペアを保持するように送信される。新暗復号鍵証明書は、各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａへ同じ証明書が送信される。
【０２７５】
各検知モジュール１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａは、保護制御モジュール１２１から分散情報と新暗復号鍵証明書とを受信し、受信した分散情報と新暗復号鍵証明書とを分散情報保持部４０９に保持する（Ｓ６００４）。
【０２７６】
上記実施の形態により、検知処理において保護制御モジュール１２０ａの改ざんが検出された場合、改ざんされた保護制御モジュールを新しい保護制御モジュールに更新することで、システムの安全性を高めることができる。
【０２７７】
（その他の変形例）
なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記実施の形態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。
【０２７８】
（１）上記各実施の形態では、検知モジュールが５つの場合を説明しているが、これに限定するものではなく、複数の検知モジュールであればよい。
（２）上記各実施の形態では、検知処理の動作として、保護制御モジュール検知処理や検知モジュール検知処理を、複数回行うとしてもよい。
【０２７９】
（３）上記実施の形態では、検知モジュール検知処理の検証処理の動作として、図２２

に示す検出結果リスト６０５１を保持している場合、さらに、検知モジュール１３５により、検知モジュール１３４が「改ざんされていない」という改ざん検出結果が得られたとき、矛盾していると判定しているが、次のような場合も矛盾していると判定してもよい。

【０２８０】

図２２に示す検出結果リスト６０５１は、検知モジュール１３４が、検知モジュール１３５の改ざん検出処理を行った結果、検知モジュール１３５が「改ざんされている」と判定したことを示している。その後、検知モジュール１３４が検知モジュール１３５の改ざん検出処理を行った結果、判断部２１０は、検出結果を受信する。図５３は、再度、検知モジュール１３４が検知モジュール１３５の改ざん検出処理を行った検出結果を示している。この図に示す検出結果は、検知モジュール１３４が、検知モジュール１３５の改ざん検出処理を行った結果、検知モジュール１３５が「改ざんされていない」と判定していることを示している。このとき、判断部２１０は、検出結果リスト６０５１に検知モジュール１３４が、検知モジュール１３５の改ざん検出処理を行った結果、「改ざんされている」と判定したことを記憶しているため、検知モジュール１３４に対する改ざん検出結果は矛盾となる。つまり、監視元と監視先が同じである場合、以前の改ざん検出結果において、「改ざんされている」と判定し、新たに受信した改ざん検出結果が「改ざんされていない」と判定している場合、矛盾であると判定する。

【０２８１】

（４）上記実施の形態２では、正常モジュール特定処理の監視パターンとして、検知モジュール１３１が検知モジュール１３２を検証し、検知モジュール１３２が検知モジュール１３３を検証し、検知モジュール１３３が検知モジュール１３４を検証し、検知モジュール１３４が検知モジュール１３１を検証しているが、これに限定するものではなく、一方向に循環して改ざん検出処理を行えばよい。

【０２８２】

（５）上記実施の形態２では、特定処理の動作として、図３２のＳ２４０３で検出結果に矛盾がない場合、機器停止としているが、これに限定するものではなく、検知モジュール検知処理を行うとしてもよい。このとき、検知モジュール検知処理では、監視パターンを更新するとしてもよい。

【０２８３】

（６）上記実施の形態３では、検知モジュールが他のモジュールを更新する更新機能を備え、更新モジュールであるとしてもよい。このとき、管理装置から、更新用のモジュールを受信し、機器内のモジュールを更新する。更新対象のモジュールは、保護制御モジュールであってもよいし、他の検知モジュールであってもよいし、アプリであってもよい。これにより、機器内のモジュールが改ざんされたとしても、更新することが可能となり、機器の信頼性を向上することができる。

【０２８４】

（７）次のように構成してもよい。

（ａ）本発明の別の変形例としての改ざん監視システム１０ｃは、図５４に示すように、管理装置２００ｃ及び情報セキュリティ装置１００ｃから構成されている。

【０２８５】

情報セキュリティ装置１００ｃは、複数の監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃを有している。監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃのそれぞれは、他の監視モジュールの改ざんを監視する。

【０２８６】

管理装置２００ｃは、情報セキュリティ装置１００ｃを管理する。管理装置２００ｃは、図５４に示すように、受信部２３０ｃ、検出部２２０ｃ及び特定部２１０ｃを備える。

受信部２３０ｃは、情報セキュリティ装置１００ｃから、各監視モジュールによる他の監視モジュールに対する監視結果を受信する。

【０２８７】

検出部２２０ｃは、受信した監視結果のうち、一部の監視結果を用いて異常を検出する

。
特定部２１０ｃは、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する。
【０２８８】
ここで、改ざん監視システム１０ｃは、上記の実施の形態又は変形例の検知システムに相当し、管理装置２００ｃは、管理装置に相当し、情報セキュリティ装置１００ｃは、機器に相当し、各監視モジュールは、機器が保持する各検知モジュールに相当する。
【０２８９】
（ｂ）管理装置２００ｃの受信部２３０ｃが、情報セキュリティ装置１００ｃから受信した監視結果の一例を図５５に示す。
上述したように、監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃのそれぞれは、一の時点において、他の監視モジュールの改ざんを監視する。ここで、一の時点は、一瞬の時点のみならず、幅のある時間帯を含む概念であり、その時間帯内において、監視モジュールの改ざんがされることがないであろうと考えられる程度のものであればよい。例えば、１秒間、１０秒間、１分間、１時間などである。また、さらに長い時間であるとしてもよい。各監視モジュールは、監視対象の監視モジュールが改ざんされているか否かを示す監視結果を、情報セキュリティ装置１００ｃを介して、管理装置２００ｃへ送信する。
【０２９０】
本明細書に記載の改ざんされたモジュールの特定において、以下に述べるように、前提条件がある。
検知モジュール（又は監視モジュール）による監視の開始から、全ての監視結果が取得されるまでの時間帯において、各モジュールは変化しないものとする。つまり、各モジュールがこの時間帯内において、改ざんされることはないものとする。この時間帯内に各モジュールが改ざんされるとすれば、改ざんされたモジュールの特定が困難になるからである。
【０２９１】
また、全ての検知モジュール（又は監視モジュール）が改ざんされることはないものとしている。全ての検知モジュール（又は監視モジュール）が改ざんされたのであれば、改ざんされたモジュールの特定が困難になるからである。
【０２９２】
図５５に示すように、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１００は、監視モジュール１３２ｃが改ざんされていないことを示し、監視モジュール１３２ｃによる監視モジュール１３４ｃに対する監視結果Ｃ１０３は、監視モジュール１３４ｃが改ざんされていないことを示し、監視モジュール１３１ｃによる監視モジュール１３３ｃに対する監視結果Ｃ１０１は、監視モジュール１３３ｃが改ざんされていないことを示し、監視モジュール１３４ｃによる監視モジュール１３６ｃに対する監視結果Ｃ１０７は、監視モジュール１３６ｃが改ざんされていないことを示す。また、監視モジュール１３３ｃによる監視モジュール１３６ｃに対する監視結果Ｃ１０６は、監視モジュール１３６ｃが改ざんされていることを示す。
【０２９３】
さらに、監視モジュール１３２ｃによる監視モジュール１３５ｃに対する監視結果Ｃ１０４、監視モジュール１３４ｃによる監視モジュール１３５ｃに対する監視結果Ｃ１０５、監視モジュール１３５ｃによる監視モジュール１３７ｃに対する監視結果Ｃ１０９、監視モジュール１３７ｃによる監視モジュール１３４ｃに対する監視結果Ｃ１０８、監視モジュール１３７ｃによる監視モジュール１３６ｃに対する監視結果Ｃ１１１、監視モジュール１３６ｃによる監視モジュール１３７ｃに対する監視結果Ｃ１１０についても、図５５に示している。

【０２９４】
情報セキュリティ装置１００ｃから受信する監視結果のデータ構造の一例を図５６に示す。
図５６に示すように、情報セキュリティ装置１００ｃから受信する監視結果の集合Ｃ１１２は、監視結果Ｃ１００、Ｃ１０１、Ｃ１０３、Ｃ１０６、Ｃ１０７、・・・から構成されている。各監視結果は、ＩＤ、監視元、監視先、結果、監視時刻を含む。
【０２９５】
ＩＤは、当該監視結果を一意に識別するための識別番号である。
監視元は、当該監視結果を出力する監視元の監視モジュールを識別するモジュール識別子である。
【０２９６】
監視先は、当該監視結果における監視先の監視モジュールを識別するモジュール識別子である。
結果は、当該監視結果を示す。結果「○」は、監視先の監視モジュールが改ざんされていないという判断結果を示し、結果「×」は、監視先の監視モジュールが改ざんされているという判断結果を示す。しかし、監視元の監視モジュールが改ざんされている場合には、改ざんされていない監視モジュールについて、結果「×」を出力したり、改ざんされている監視モジュールについて、結果「○」を出力したりする場合もありうる。
【０２９７】
監視時刻は、監視元の監視モジュールにより、監視先の監視モジュールの改ざんチェックが行われた時刻を、年月日時分で示している。図５６に示すように、監視結果の集合Ｃ１１２に含まれる全ての監視結果は、同一の時刻「２０１１．１．３１　１３：００」を含むので、同一の時刻、２０１１年１月３１日１３時００分において、改ざんチェックが行われたことを示している。
【０２９８】
受信部２３０ｃは、一例として、図５５に示す全ての監視結果を受信し、受信した全ての監視結果を検出部２２０ｃへ出力する。
検出部２２０ｃは、受信部２３０ｃから監視結果を受け取り、受け取った監視結果のうちの一部の監視結果を用いて、つまり、一の監視モジュールに対する複数の監視結果を用いて、前記複数の監視結果の不一致を検出することにより、異常を検出する。一の監視モジュールに対する監視結果が２個存在する場合には、検出部２２０ｃは、受信した前記監視結果のうち、一の監視モジュールに対する第１の監視結果及び前記一の監視モジュールに対する第２の監視結果を用い、前記第１の監視結果と前記第２の監視結果が一致するか否かを判断することにより、前記第１の監視結果と前記第２の監視結果の不一致を検出する。
【０２９９】
図５５に示す例の場合には、検出部２２０ｃは、監視モジュール１３６ｃに対する監視結果Ｃ１０６と監視モジュール１３６ｃに対する監視結果Ｃ１０７を用いる。監視結果Ｃ１０６及び監視結果Ｃ１０７は、いずれも、同一の監視モジュール１３６ｃに対する監視結果であるが、監視結果Ｃ１０６は、監視モジュール１３６ｃが改ざんされていることを示し、監視結果Ｃ１０７は、監視モジュール１３６ｃが改ざんされていないことを示しており、監視結果Ｃ１０６と、監視結果Ｃ１０７とは一致していない。検出部２２０ｃは、監視結果Ｃ１０６と監視結果Ｃ１０７とが一致するか否かを判断し、監視結果Ｃ１０６と監視結果Ｃ１０７とは一致していないので、異常を検出する。
【０３００】
検出部２２０ｃは、このように、一の監視モジュールに対する一の監視結果と前記監視モジュールに対する他の監視結果との不一致を異常として検出する。
以上説明したように、検出部２２０ｃは、受信した全ての監視結果を用いることなく、受信した監視結果の一部を用いて、つまり、同一の監視モジュールに対する複数の監視結果のみを用いて、異常を検出する。

【０３０１】
異常が検出された場合に、検出部２２０ｃは、同一の監視モジュールに対する複数の監視結果が一致していない旨を特定部２１０ｃへ通知する。図５５に示す例の場合には、検出部２２０ｃは、監視結果Ｃ１０６と監視結果Ｃ１０７とが一致していない旨を、特定部２１０ｃへ通知する。
【０３０２】
特定部２１０ｃは、検出部２２０ｃから、同一の監視モジュールに対する第１の監視結果と第２の監視結果とが一致していない旨の通知を受け取り、前記通知を受け取った場合には、受信部２３０ｃから全ての監視結果を受け取る。次に、特定部２１０ｃは、以下に示すようにして、前記複数の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡ることにより、改ざんされた前記監視モジュールを特定する。つまり、特定部２１０ｃは、前記通知に係る前記第１の監視結果及び前記第２の監視結果のそれぞれを用いて、監視先の監視モジュールから監視元の監視モジュールへ遡り、前記第１の監視結果及び前記第２の監視結果毎に、その他の正常であるとする前記監視結果を用いて監視先の監視モジュールから監視元の監視モジュールへ遡ることを繰り返すことにより、同一の監視モジュールに到達するか否かを判断し、同一の監視モジュールに到達すると判断する場合に、当該同一の監視モジュールを改ざんされた監視モジュールとして特定する。
【０３０３】
図５５に示す例を用いて、さらに詳細に説明する。
同一の監視モジュール１３６ｃに対する第１の監視結果Ｃ１０６と第２の監視結果Ｃ１０７とが一致していない旨の通知を受け取ると、特定部２１０ｃは、第１の監視結果Ｃ１０６を用いて、監視元の監視モジュール１３３ｃを特定する。次に、特定した監視モジュール１３３ｃに対して正常であるとする監視結果を検索する。図５５に示す例においては、監視結果Ｃ１０１は、監視モジュール１３１ｃによる監視モジュール１３３ｃに対する監視結果であり、監視モジュール１３３ｃが正常であることを示しているので、監視モジュール１３３ｃの監視元の監視モジュールとして、監視モジュール１３１ｃを特定する。同様にして、監視モジュール１３１ｃに対して正常であるとする監視結果の検索を試みる。図５５に示す例においては、監視モジュール１３１ｃを監視する監視モジュールによる監視結果は存在しないので、監視結果の検索は、ここで終了する。こうして、特定部２１０ｃは、監視モジュール１３１ｃを特定する。
【０３０４】
また、特定部２１０ｃは、第２の監視結果Ｃ１０７を用いて、監視元の監視モジュール１３４ｃを特定する。次に、特定した監視モジュール１３４ｃに対して正常であるとする監視結果を検索する。図５５に示す例においては、監視結果Ｃ１０３は、監視モジュール１３２ｃによる監視モジュール１３４ｃに対する監視結果であり、監視モジュール１３４ｃが正常であることを示しているので、監視モジュール１３４ｃの監視元の監視モジュールとして、監視モジュール１３２ｃを特定する。同様にして、監視モジュール１３２ｃに対して正常であるとする監視結果の検索を試みる。図５５に示す例においては、監視結果Ｃ１００は、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果であり、監視モジュール１３２ｃが正常であることを示しているので、監視モジュール１３２ｃの監視元の監視モジュールとして、監視モジュール１３１ｃを特定する。さらに、同様にして、監視モジュール１３１ｃに対して正常であるとする監視結果の検索を試みる。図５５に示す例においては、監視モジュール１３１ｃを監視する監視モジュールによる監視結果は存在しないので、監視結果の検索は、ここで終了する。こうして、特定部２１０ｃは、監視モジュール１３１ｃを特定する。
【０３０５】
次に、特定部２１０ｃは、別々の検索経路において、特定した複数の監視モジュールが同一であるか否かを判断する。ここでは、特定部２１０ｃは、同一の監視モジュール１３１ｃを特定している。

【０３０６】
従って、特定部２１０ｃは、監視モジュール１３１ｃが改ざんされた監視モジュールであると特定する。
仮に、監視モジュール１３１ｃが改ざんされていないと仮定すると、監視モジュール１３１ｃによる監視結果Ｃ１０１は、正しく、監視結果Ｃ１０１により、監視モジュール１３３ｃは、改ざんされていないこととなる。また、監視モジュール１３３ｃによる監視結果Ｃ１０６によると、監視モジュール１３６ｃは、改ざんされている。一方、上記の仮定に基づいて、監視結果Ｃ１００により、監視モジュール１３２ｃは、改ざんされておらず、監視結果Ｃ１０３により、監視モジュール１３４ｃは、改ざんされておらず、監視結果Ｃ１０７により、監視モジュール１３６ｃは、改ざんされていない。
【０３０７】
そうすると、監視モジュール１３６ｃに対する２個の監視結果Ｃ１０６とＣ１０７とが一致しない。従って、上記の仮定が誤りであったと考えられる。即ち、監視モジュール１３１ｃが改ざんされていないとする仮定は、誤りであり、監視モジュール１３１ｃは改ざんされていると結論付けることができる。
【０３０８】
特定部２１０ｃの動作について、図５７に示すフローチャートを用いて説明する。
特定部２１０ｃは、検出部２２０ｃから同一の監視モジュールに対する第１の監視結果と第２の監視結果とが一致していない旨の通知を受け取る（ステップＳ５０１）。
【０３０９】
前記通知を受け取ると、特定部２１０ｃは、受信部２３０ｃから全ての監視結果を受け取る（ステップＳ５０２）。
特定部２１０ｃは、第１の監視結果を用いて、第１の監視結果を出力した監視元の監視モジュールを特定する（ステップＳ５０３）。次に、特定部２１０ｃは、特定した監視モジュールに対して正常であるとする監視結果を検索し、監視結果が存在しない場合（ステップＳ５０４で「無し」）、ステップＳ５０９へ制御を移す。監視結果が存在する場合（ステップＳ５０４で「有り」）、この監視結果を用いて、当該監視結果を出力した監視元の監視モジュールを特定し（ステップＳ５０５）、ステップＳ５０４へ戻って、処理を繰り返す。
【０３１０】
また、特定部２１０ｃは、第２の監視結果を用いて、第２の監視結果を出力した監視元の監視モジュールを特定する（ステップＳ５０６）。次に、特定部２１０ｃは、特定した監視モジュールに対して正常であるとする監視結果を検索し、監視結果が存在しない場合（ステップＳ５０７で「無し」）、ステップＳ５０９へ制御を移す。監視結果が存在する場合（ステップＳ５０７で「有り」）、この監視結果を用いて、当該監視結果を出力した監視元の監視モジュールを特定し（ステップＳ５０８）、ステップＳ５０７へ戻って、処理を繰り返す。
【０３１１】
次に、第１の監視結果による検索の経路（ステップＳ５０３～Ｓ５０５）により、最終的に特定された監視モジュールと、第２の監視結果による検索の経路（ステップＳ５０６～Ｓ５０８）により、最終的に特定された監視モジュールとが一致するか否かを判断し（ステップＳ５０９）、一致する場合に（ステップＳ５０９で「ＹＥＳ」）、当該特定された監視モジュールが、改ざんされた監視モジュールであると特定する（ステップＳ５１０）。
【０３１２】
（ｃ）管理装置２００ｃの受信部２３０ｃが、情報セキュリティ装置１００ｃから受信した監視結果の別の一例を図５８に示す。
上述したように、監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃのそれぞれは、第１の時点において、他の監視モジュールの改ざんを監視する。ここで、第１の時点は、一瞬の時点のみならず、幅のある時間帯を含む概念である。各監視モジュールは、監視

対象の監視モジュールが改ざんされているか否かを示す第１の時点における監視結果を、情報セキュリティ装置１００ｃを介して、管理装置２００ｃへ送信する。

【０３１３】

また、監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃのそれぞれは、第２の時点において、他の監視モジュールの改ざんを監視する。ここで、第２の時点は、第１の時点と同様に、一瞬の時点のみならず、幅のある時間帯を含む概念である。第２の時点は、第１の時点より遅い時点である。例えば、第１の時点が「２０１１年１月３１日１３時００分」であるとすると、第２の時点は、第２の時点より遅い「２０１１年２月５日９時００分」である。各監視モジュールは、監視対象の監視モジュールが改ざんされているか否かを示す第２の時点における監視結果を、情報セキュリティ装置１００ｃを介して、管理装置２００ｃへ送信する。

【０３１４】

なお、情報セキュリティ装置１００ｃは、第１の時点における監視結果を送信し、その後に、第２の時点における監視結果を送信しているが、これには限定されない。情報セキュリティ装置１００ｃは、第１の時点における監視結果と第２の時点における監視結果を、第２の時点の後に送信してもよい。

【０３１５】

受信部２３０ｃは、第１の時点の直後に、第１の時点における監視結果を受信し、第２の時点の直後に、第２の時点における監視結果を受信する。なお、受信部２３０ｃは、第２の時点の直後に、第１の時点における監視結果と、第２の時点における監視結果とを受信してもよい。

【０３１６】

図５８（ａ）に示すように、時刻ｔがｋのときに、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１２１は、監視モジュール１３２ｃが改ざんされていることを示している。また、図５８（ｂ）に示すように、時刻ｔがｋ＋ｉのときに、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１２１は、監視モジュール１３２ｃが改ざんされていないことを示している。

【０３１７】

図５９に監視結果のデータ構造の一例を示す。この図に示すように、監視結果の集合Ｃ１２０は、監視結果Ｃ１２１及びＣ１２２を含み、各監視結果は、ＩＤ、監視元、監視先、結果及び監視時刻を含む。ＩＤ、監視元、監視先、結果及び監視時刻については、上述したとおりである。

【０３１８】

検出部２２０ｃは、受信した前記監視結果のうち、前記第１の時点における第１監視モジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における前記第１監視モジュールによる前記第２監視モジュールに対する第２の監視結果が前記第２監視モジュールが改ざんされていないことを示すという不一致を検出する。不一致を検出すると、検出部２２０ｃは、特定部２１０ｃに対して、その旨を通知する。

【０３１９】

図５８（ａ）及び（ｂ）に示す例によると、検出部２２０ｃは、受信した前記監視結果のうち、時刻ｔがｋのときに、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１２１が監視モジュール１３２ｃが改ざんされていることを示し、時刻ｔがｋ＋ｉのときに、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１２２が監視モジュール１３２ｃが改ざんされていないことを示すという不一致を検出する。

【０３２０】

特定部２１０ｃは、検出部２２０ｃから不一致の旨の通知を受け取ると、第１監視モジュールが改ざんされている監視モジュールであると特定する。図５８（ａ）及び（ｂ）に示す例の場合には、特定部２１０ｃは、監視モジュール１３１ｃが改ざんされた監視モジ

ュールであると特定する。
【０３２１】
特定部２１０ｃにより改ざんされた監視モジュールを特定できるのは、次のような理由による。
図５８（ａ）及び（ｂ）に示す例の場合に、監視モジュール１３１ｃが改ざんされておらず、正常であると仮定する。時刻ｔがｋのときに、監視モジュール１３１ｃは、監視モジュール１３２ｃが改ざんされていると判定しているが、時刻ｔがｋ＋ｉのときに、監視モジュール１３１ｃは、監視モジュール１３２ｃが正常であると判定している。監視モジュール１３２ｃが時刻ｔがｋからｋ＋ｉの間において、正常に戻ることはあり得ないので、監視結果Ｃ１２１とＣ１２２との間に矛盾が生じている。従って、監視モジュール１３１ｃが正常であるとした仮定が誤りであり、監視モジュール１３１ｃは、改ざんされた監視モジュールであると結論付けることができる。
【０３２２】
（ｄ）管理装置２００ｃの受信部２３０ｃが、情報セキュリティ装置１００ｃから受信した監視結果の別の一例を図６０に示す。
上述したように、監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃのそれぞれは、第１の時点において、他の監視モジュールの改ざんを監視する。ここで、第１の時点は、上述したように、幅のある時間帯を含む概念である。各監視モジュールは、監視対象の監視モジュールが改ざんされているか否かを示す第１の時点における監視結果を、情報セキュリティ装置１００ｃを介して、管理装置２００ｃへ送信する。
【０３２３】
また、監視モジュール１３１ｃ、１３２ｃ、・・・、１３７ｃのそれぞれは、第２の時点において、他の監視モジュールの改ざんを監視する。ここで、第２の時点は、第１の時点と同様に、一瞬の時点のみならず、幅のある時間帯を含む概念である。第２の時点は、上述したように、第１の時点より遅い時点である。各監視モジュールは、監視対象の監視モジュールが改ざんされているか否かを示す第２の時点における監視結果を、情報セキュリティ装置１００ｃを介して、管理装置２００ｃへ送信する。
【０３２４】
なお、情報セキュリティ装置１００ｃは、第１の時点における監視結果を送信し、その後に、第２の時点における監視結果を送信しているが、これには限定されない。情報セキュリティ装置１００ｃは、第１の時点における監視結果と第２の時点における監視結果を、第２の時点の後に送信してもよい。
【０３２５】
受信部２３０ｃは、第１の時点の直後に、第１の時点における監視結果を受信し、第２の時点の直後に、第２の時点における監視結果を受信する。なお、受信部２３０ｃは、第２の時点の直後に、第１の時点における監視結果と、第２の時点における監視結果とを受信してもよい。
【０３２６】
図６０（ａ）に示すように、時刻ｔがｋのときに、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１３１は、監視モジュール１３２ｃが改ざんされていることを示している。また、図６０（ｂ）に示すように、時刻ｔがｋ＋ｉのときに、監視モジュール１３２ｃによる監視モジュール１３１ｃに対する監視結果Ｃ１３３は、監視モジュール１３１ｃが改ざんされていないことを示している。
【０３２７】
図６１に監視結果のデータ構造の一例を示す。この図に示すように、監視結果の集合Ｃ１３０は、監視結果Ｃ１３１及びＣ１３３を含み、各監視結果は、ＩＤ、監視元、監視先、結果及び監視時刻を含む。ＩＤ、監視元、監視先、結果及び監視時刻については、上述したとおりである。
【０３２８】
検出部２２０ｃは、受信した前記監視結果のうち、前記第１の時点における第１監視モ

ジュールによる第２監視モジュールに対する第１の監視結果が前記第２監視モジュールが改ざんされていることを示し、前記第２の時点における第２監視モジュールによる第１監視モジュールに対する第２の監視結果が前記第１監視モジュールが改ざんされていないことを示すという異常を検出する。

【０３２９】

図６０（ａ）及び（ｂ）に示す例によると、検出部２２０ｃは、受信した前記監視結果のうち、時刻ｔがｋのときに、監視モジュール１３１ｃによる監視モジュール１３２ｃに対する監視結果Ｃ１３１が監視モジュール１３２ｃが改ざんされていることを示し、時刻ｔがｋ＋ｉのときに、監視モジュール１３２ｃによる監視モジュール１３１ｃに対する監視結果Ｃ１３３が監視モジュール１３１ｃが改ざんされていないことを示すという異常を検出する。

【０３３０】

特定部２１０ｃは、前記第１の監視結果が前記第２監視モジュールが改ざんされたことを示し、前記第２の監視結果が第１監視モジュールが改ざんされていないことを示す場合に、前記第２監視モジュールを改ざんされた監視モジュールとして特定する。

【０３３１】

図６０（ａ）及び（ｂ）に示す例によると、特定部２１０ｃは、監視結果Ｃ１３１が監視モジュール１３２ｃが改ざんされていることを示し、監視結果Ｃ１３３が監視モジュール１３１ｃが改ざんされていないことを示すという異常が検出された場合に、監視モジュール１３２ｃが改ざんされた監視モジュールであると特定する。

【０３３２】

特定部２１０ｃにより改ざんされた監視モジュールを特定できるのは、次のような理由による。

図６０（ａ）及び（ｂ）に示す例の場合に、時刻ｔがｋのときに、監視モジュール１３１ｃは、監視モジュール１３２ｃが改ざんされていると判定し、時刻ｔがｋ＋ｉのときに、監視モジュール１３２ｃは、監視モジュール１３１ｃが正常であると判定している。

【０３３３】

ここで、監視モジュール１３１ｃが正常な監視モジュールであるとする場合、監視結果Ｃ１３１により、監視モジュール１３２ｃは、改ざんされた監視モジュールである。

また、監視モジュール１３１ｃが改ざんされた監視モジュールであるとする場合、監視結果Ｃ１３３により、改ざんされた監視モジュールを正常と判断しているので、監視モジュール１３２ｃは、改ざんされた監視モジュールである。

【０３３４】

従って、監視モジュール１３２ｃは、改ざんされた監視モジュールであると結論付けることができる。

（８）次のように構成してもよい。

【０３３５】

管理装置及び情報セキュリティ装置（機器）は、通常モードと異常モードとの切り替えを行って動作する。

通常モードにおいて、管理装置及び情報セキュリティ装置（機器）は、異常なつまり改ざんされた検知モジュール（又は監視モジュール）を特定することを目的として動作する。通常モードは、言わば、異常モジュール特定モードである。通常モードにおいては、第１に、検知モジュール（監視モジュール）は、保護制御モジュールへの攻撃、つまり、保護制御モジュールの改ざんを検知する。第２に、複数の検知モジュール（複数の監視モジュール）は、相互に、異常つまり改ざんの検知（又は監視）を行う。

【０３３６】

通常モードにおいて、異常なモジュールが検出されると、管理装置及び情報セキュリティ装置（機器）は、通常モードから異常モードへ切り替えられる。

異常モードにおいて、第１に、管理装置及び情報セキュリティ装置（機器）は、保護制御モジュールの危殆化、つまり、改ざんを検知した場合、情報セキュリティ装置（機器）

の保護制御モジュールを正常な保護制御モジュールに更新する。第２に、異常なモジュールを検出した場合に、異常なモジュールを無効化する。第３に、検知モジュール（又は監視モジュール）が有する監視パターンを新たな監視パターンに更新する。監視パターンの更新については、次にその一例を説明する。

【０３３７】

（９）次のように構成してもよい。

（ａ）本発明の別の変形例としての改ざん監視システム１０ｄは、図６２に示すように、管理装置２００ｄ及び情報セキュリティ装置１００ｄから構成されている。

【０３３８】

情報セキュリティ装置１００ｄは、複数の監視モジュール１３１ｄ、１３２ｄ、・・・、１３７ｄを有している。監視モジュール１３１ｄ、１３２ｄ、・・・、１３７ｄのそれぞれは、他の監視モジュールの改ざんを監視する。

【０３３９】

管理装置２００ｄは、情報セキュリティ装置１００ｄを管理する。管理装置２００ｄは、図６２に示すように、送信部２５０ｄ、生成部２４０ｃ及び特定部２１０ｄを備える。

特定部２１０ｄは、複数の監視モジュール１３１ｄ、１３２ｄ、・・・、１３７ｄのうち、改ざんされた監視モジュールを特定する。

【０３４０】

生成部２４０ｄは、複数の監視モジュール１３１ｄ、１３２ｄ、・・・、１３７ｄのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する。

【０３４１】

送信部２５０ｄは、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する。

情報セキュリティ装置１００ｄは、正常監視モジュール毎の監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【０３４２】

送信部２５０ｄにより生成される前記複数の監視パターンは、循環監視パターンを構成する。

（ｂ）管理装置２００ｄについて、さらに詳細に説明する。

【０３４３】

管理装置２００ｄは、一例として図６３に示す監視結果の集合Ｄ１００ａを受信し、特定部２１０ｄは、上記の実施の形態や変形例において説明したように、監視モジュール１３１ｄが改ざんされた監視モジュールであると特定するものとする。監視結果の集合Ｄ１００ａは、図５５に示すものと同一であるので、詳細の説明を省略する。

【０３４４】

生成部２４０ｄは、複数の監視モジュール１３１ｄ、１３２ｄ、・・・、１３７ｄのうち、改ざんされた監視モジュール１３１ｄを除き、他の残りの監視モジュール１３２ｄ、・・・、１３７ｄを選択する。これらの監視モジュールを正常監視モジュールと呼ぶこととする。

【０３４５】

生成部２４０ｄは、図６３の監視パターンの集合Ｄ１００ｂに示すように、監視モジュール１３２ｄが監視モジュール１３４ｄを監視するように監視パターンＤ１０６を生成し、監視モジュール１３４ｄが監視モジュール１３３ｄを監視するように監視パターンＤ１０１を生成し、監視モジュール１３３ｄが監視モジュール１３６ｄを監視するように監視パターンＤ１０２を生成し、監視モジュール１３６ｄが監視モジュール１３７ｄを監視するように監視パターンＤ１０３を生成し、監視モジュール１３７ｄが監視モジュール１３５ｄを監視するように監視パターンＤ１０４を生成し、監視モジュール１３５ｄが監視モ

ジュール１３２ｄを監視するように監視パターンＤ１０５を生成する。
【０３４６】
監視パターンのデータ構造の一例を図６４に示す。監視パターンＤ１０１、Ｄ１０２、・・・、Ｄ１０６は、それぞれ、ＩＤ、監視元、監視先から構成されている。ＩＤは、当該監視パターンを一意に識別する識別子である。監視元は、当該監視パターンが配布される監視モジュールを識別するモジュール識別子である。当該監視パターンは、監視元により示される監視モジュール内に記憶され、当該監視モジュールは、当該監視パターンに従って、外の監視モジュールの改ざんを監視する。監視先は、当該監視パターンが配布される監視モジュールにより監視の対象となる監視モジュールを識別するモジュール識別子である。
【０３４７】
このようにして生成された監視パターンＤ１０１、Ｄ１０２、・・・、Ｄ１０６を用いることにより、監視モジュール１３２ｄが監視モジュール１３４ｄを監視し、監視モジュール１３４ｄが監視モジュール１３３ｄを監視し、監視モジュール１３３ｄが監視モジュール１３６ｄを監視し、監視モジュール１３６ｄが監視モジュール１３７ｄを監視し、監視モジュール１３７ｄが監視モジュール１３５ｄを監視し、監視モジュール１３５ｄが監視モジュール１３２ｄを監視することとなる。
【０３４８】
図６３の監視パターンの集合Ｄ１００ｂに示すように、監視の経路は、監視モジュール１３２ｄから始まり、全ての監視モジュール（改ざんされた監視モジュールを除く）を一巡して、監視モジュール１３２ｄに戻っている。このように、複数の監視の経路が閉路を形成しているので、図６３の監視パターンの集合Ｄ１００ｂを循環監視パターンと呼ぶ。
【０３４９】
上記のように、生成部２４０ｄにより生成される複数の監視パターンは、循環型の監視パターンを構成している。循環型の監視パターンでは、各監視モジュールが他のただ一つの監視モジュールのみを監視し、各監視モジュールが他のただ一つの監視モジュールのみから監視されるようになる。監視元の監視モジュールから監視先の監視モジュールへの監視の経路は、複数存在し、これらの複数の経路を接続すると閉路が完成する。
【０３５０】
このような循環監視パターンを生成することにより、各監視モジュールが他のただ一つの監視モジュールのみを監視し、各監視モジュールが他のただ一つの監視モジュールのみから監視されるようになる。このため、循環監視パターンを用いると、監視モジュールによる監視の回数を最小にすることができる。
【０３５１】
監視モジュールの数をｎとすると、ｎ個の監視モジュールにより、完全グラフを構成するように監視パターンを生成した場合と比較して、循環監視パターンを用いた場合の監視数は、１／（ｎ－１）となる。
【０３５２】
（１０）次のように構成してもよい。
改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信回路と、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出回路と、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定回路とを備える。
【０３５３】
また、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する集積回路であって、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信回路と、受信した監視結果のうち、一部の監

視結果を用いて異常を検出する検出回路と、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定回路とを備える。

【０３５４】

また、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、複数のコンピュータ命令が組み合わされて構成されるコンピュータプログラムを記憶しているメモリ部と、前記メモリ部に記憶されている前記コンピュータプログラムから１個ずつコンピュータ命令を読み出し、解読し、その解読結果に応じて動作するプロセッサとを備える。前記コンピュータプログラムは、コンピュータである管理装置に、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信ステップと、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出ステップと、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定ステップとを実行させる。

【０３５５】

また、次のように構成してもよい。

改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定回路と、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成回路と、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信回路とを備える。前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【０３５６】

改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する集積回路であって、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定回路と、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成回路と、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信回路とを備える。前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【０３５７】

また、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置であって、複数のコンピュータ命令が組み合わされて構成されるコンピュータプログラムを記憶しているメモリ部と、前記メモリ部に記憶されている前記コンピュータプログラムから１個ずつコンピュータ命令を読み出し、解読し、その解読結果に応じて動作するプロセッサとを備える。前記コンピュータプログラムは、コンピュータである管理装置に、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定ステップと、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成ステップと、

生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信ステップとを実行させる。前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【０３５８】

（１１）次のように構成してもよい。

改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な非一時的なプログラム記録媒体であるとしてもよい。前記コンピュータプログラムは、コンピュータである管理装置に、前記情報セキュリティ装置から、各監視モジュールによる他の監視モジュールに対する監視結果を受信する受信ステップと、受信した監視結果のうち、一部の監視結果を用いて異常を検出する検出ステップと、異常が検出された場合に、検出された異常に係る監視結果の生成元の監視モジュール、及び、当該監視モジュールを起点として、連鎖的に監視結果を生成元へ辿ることにより、特定される監視モジュールの中から、改ざんされた監視モジュールを特定する特定ステップとを実行させることを特徴とする。

【０３５９】

また、改ざんを監視する複数の監視モジュールを有する情報セキュリティ装置を管理する管理装置で用いられる管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な非一時的なプログラム記録媒体であるとしてもよい。前記コンピュータプログラムは、コンピュータである管理装置に、前記複数の監視モジュールのうち、改ざんされた監視モジュールを特定する特定ステップと、複数の監視モジュールのうち、改ざんされた監視モジュールを除く残りの正常監視モジュール毎に、各正常監視モジュールが他のただ一つの正常監視モジュールのみを監視し、各正常監視モジュールが他のただ一つの正常監視モジュールのみから監視されるように、監視先の正常監視モジュールを示す監視パターンを生成する生成ステップと、生成した正常監視モジュール毎の監視パターンを前記情報セキュリティ装置へ送信する送信ステップとを実行させることを特徴とする。前記情報セキュリティ装置は、正常監視モジュール毎の前記監視パターンを受信し、各正常監視モジュールに対して、受信した監視パターンに書き換えるように制御する。

【０３６０】

（１２）上記の各モジュールは、具体的には、それぞれ個別のコンピュータプログラムであってもよいし、オペレーティングシステムに組み込まれるモジュールであってもよいし、オペレーティングシステムから呼ばれるドライバであってもよいし、アプリケーションプログラムであってもよい。

【０３６１】

（１３）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、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。前記ＲＡＭまた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。前記マイクロプロセッサが、前記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されて構成されたものである。

【０３６２】

（１４）上記の各装置を構成する構成要素の一部または全部は、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。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記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。

【０３６３】
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良いし、一部又は全てを含むように１チップ化されてもよい。
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ＦＰＧＡ（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・プロセッサーを利用しても良い。
【０３６４】
さらには、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。
【０３６５】
（１５）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまた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カードまた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カードまた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カードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。
【０３６６】
（１６）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。
【０３６７】
また、本発明は、前記コンピュータプログラムまた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　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。
【０３６８】
また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、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。
【０３６９】
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。
【０３７０】
また、前記プログラムまた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、または前記プログラムまた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。
【０３７１】
（１７）次のように構成してもよい。
本発明の一実施態様は、ネットワークを介して接続されている情報処理装置上で動作する検知モジュールのうち改ざんされた異常な検知モジュールを特定する管理装置であって、前記管理装置は、前記情報処理装置内の複数の検知モジュールから改ざん検出結果を受信する受信手段と、前記改ざん検出結果のうち、異常と判定した結果を保持する改ざん検出結果保持手段と、前記複数の検知モジュールのうちの一つを正常な検知モジュールと仮

定し、前記仮定に基づいて、前記改ざん検出結果保持手段で保持する改ざん検出結果と、新たに受信した改ざん検出結果に矛盾の有無を判断し、矛盾がある場合に、正常と仮定した前記検知モジュールを異常な検知モジュールと特定する異常モジュール特定手段を備えることを特徴とする。

【０３７２】

この構成によると、改ざんされたという検出結果を保持することにより、複数の検知モジュールのすべての検知モジュールが一度に改ざん検出を行わなくても、矛盾があるか否かで異常な検知モジュールを特定することができるため、機器内の処理の負荷を軽減することができる。

【０３７３】

また、前記管理装置は、さらに、特定された異常な検知モジュールの無効化指示を出力する無効化指示手段を備えるとしてもよい。

これにより、検出した異常な検知モジュールを無効化することにより、異常な検知モジュールに妨害されることなく情報処理装置が動作することができ、情報処理装置の信頼性をより高めることができる。

【０３７４】

また、前記管理装置は、さらに、複数の検知モジュールのうち、異常な検知モジュールと特定した検知モジュール以外のすべての検知モジュールの改ざん検出を一方向に循環して改ざん検出を行う循環パターンへ更新させる監視パターン更新指示手段と、前記循環パターンの複数の検知モジュールが一方向に循環して改ざん検出を行った結果がすべて正常である場合に、前記複数の検知モジュールを正常な検知モジュールと特定する正常モジュール特定手段を備えるとしてもよい。

【０３７５】

これにより、情報処理装置において正常なモジュールを用いた処理を実行することができ、情報処理装置の信頼性を高めることができる。

また、前記情報処理装置が有する少なくとも１個の検知モジュールは、他のモジュールを更新する機能を備える更新モジュールであり、前記管理装置は、さらに、複数の検知モジュールのうち、異常な検知モジュールと特定した検知モジュール以外のすべての検知モジュールの改ざん検出を一方向に循環して改ざん検出を行う循環パターンへ更新させる監視パターン更新指示手段と、前記循環パターンの複数の検知モジュールが一方向に循環して改ざん検出を行った結果がすべて正常である場合に、前記複数の検知モジュールを正常な検知モジュールと特定するする正常モジュール特定手段を備え、正常な検知モジュールと特定された前記検知モジュールが、他のモジュールを更新する機能を有する前記更新モジュールである場合に、更新モジュールである当該検知モジュールに対して、他のモジュールを更新するように、制御する制御手段を備えるとしてもよい。

【０３７６】

これにより、前記正常な検知モジュールを用いて、確実に他のモジュールを更新することができ、情報処理装置の信頼性を高めることができる。

また、前記情報処理装置は、さらに、アプリケーションプログラム及び当該アプリケーションプログラムを保護する保護制御モジュールを有し、前記他のモジュールは、前記検知モジュール、前記アプリケーションプログラム、又は前記保護制御モジュールであるとしてもよい。

【０３７７】

また、本発明の実施態様である検知システムは、改ざんを監視する複数の検知モジュールを有する情報処理装置と、当該情報処理装置を管理する管理装置とから構成される検知システムであって、前記管理装置は、前記情報処理装置内の複数の検知モジュールから改ざん検出結果を受信する受信手段と、前記改ざん検出結果のうち、異常と判定した結果を保持する改ざん検出結果保持手段と、前記複数の検知モジュールのうちの一つを正常な検知モジュールと仮定し、前記仮定に基づいて、前記改ざん検出結果保持手段で保持する改ざん検出結果と、新たに受信した改ざん検出結果に矛盾の有無を判断し、矛盾がある場合

に、正常と仮定した前記検知モジュールを異常な検知モジュールと特定する異常モジュール特定手段を備える。

【０３７８】

ここで、前記検知システムにおいて、前記管理装置は、さらに、特定された異常な検知モジュールの無効化指示を出力する無効化指示手段を備えるとしてもよい。

ここで、前記検知システムにおいて、前記管理装置は、さらに、複数の検知モジュールのうち、異常な検知モジュールと特定した検知モジュール以外のすべての検知モジュールの改ざん検出を一方向に循環して改ざん検出を行う循環パターンへ更新させる監視パターン更新指示手段と、前記循環パターンの複数の検知モジュールが一方向に循環して改ざん検出を行った結果がすべて正常である場合に、前記複数の検知モジュールを正常な検知モジュールと特定する正常モジュール特定手段を備えるとしてもよい。

【０３７９】

ここで、前記検知システムにおいて、前記情報処理装置が有する少なくとも１個の検知モジュールは、他のモジュールを更新する機能を備える更新モジュールであり、前記管理装置は、さらに、複数の検知モジュールのうち、異常な検知モジュールと特定した検知モジュール以外のすべての検知モジュールの改ざん検出を一方向に循環して改ざん検出を行う循環パターンへ更新させる監視パターン更新指示手段と、前記循環パターンの複数の検知モジュールが一方向に循環して改ざん検出を行った結果がすべて正常である場合に、前記複数の検知モジュールを正常な検知モジュールと特定するする正常モジュール特定手段を備え、正常な検知モジュールと特定された前記検知モジュールが、他のモジュールを更新する機能を有する前記更新モジュールである場合に、更新モジュールである当該検知モジュールに対して、他のモジュールを更新するように、制御する制御手段を備えるとしてもよい。

【０３８０】

本発明の実施態様である集積回路は、改ざんを監視する複数の検知モジュールを有する情報処理装置を管理する機能を有する集積回路であって、前記情報処理装置内の複数の検知モジュールから改ざん検出結果を受信する受信手段と、前記改ざん検出結果のうち、異常と判定した結果を保持する改ざん検出結果保持手段と、前記複数の検知モジュールのうちの一つを正常な検知モジュールと仮定し、前記仮定に基づいて、前記改ざん検出結果保持手段で保持する改ざん検出結果と、新たに受信した改ざん検出結果に矛盾の有無を判断し、矛盾がある場合に、正常と仮定した前記検知モジュールを異常な検知モジュールと特定する異常モジュール特定手段を備える。

【０３８１】

本発明の実施態様である管理方法は、改ざんを監視する複数の検知モジュールを有する情報処理装置を管理する管理方法であって、前記情報処理装置内の複数の検知モジュールから改ざん検出結果を受信する受信ステップと、前記改ざん検出結果のうち、異常と判定した結果を保持する改ざん検出結果保持ステップと、前記複数の検知モジュールのうちの一つを正常な検知モジュールと仮定し、前記仮定に基づいて、前記改ざん検出結果保持手段で保持する改ざん検出結果と、新たに受信した改ざん検出結果に矛盾の有無を判断し、矛盾がある場合に、正常と仮定した前記検知モジュールを異常な検知モジュールと特定する異常モジュール特定ステップを含む。

【０３８２】

本発明の実施態様である記録媒体は、改ざんを監視する複数の検知モジュールを有する情報処理装置を管理する管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、コンピュータに、前記情報処理装置内の複数の検知モジュールから改ざん検出結果を受信する受信ステップと、前記改ざん検出結果のうち、異常と判定した結果を保持する改ざん検出結果保持ステップと、前記複数の検知モジュールのうちの一つを正常な検知モジュールと仮定し、前記仮定に基づいて、前記改ざん検出結果保持手段で保持する改ざん検出結果と、新たに受信した改ざん検出結果に矛盾の有無を判断し、矛盾がある場合に、正常と仮定した前記検知モジュールを異常な検知モジュールと

特定する異常モジュール特定ステップとを実行させるためのコンピュータプログラムを記録している。

【０３８３】

本発明の実施態様であるコンピュータプログラムは、改ざんを監視する複数の検知モジュールを有する情報処理装置を管理する管理用のコンピュータプログラムであって、コンピュータに、前記情報処理装置内の複数の検知モジュールから改ざん検出結果を受信する受信ステップと、前記改ざん検出結果のうち、異常と判定した結果を保持する改ざん検出結果保持ステップと、前記複数の検知モジュールのうちの一つを正常な検知モジュールと仮定し、前記仮定に基づいて、前記改ざん検出結果保持手段で保持する改ざん検出結果と、新たに受信した改ざん検出結果に矛盾の有無を判断し、矛盾がある場合に、正常と仮定した前記検知モジュールを異常な検知モジュールと特定する異常モジュール特定ステップとを実行させる。

【０３８４】

（１８）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。

以上、本発明を添付図面を用いて詳細に説明したが、種々の改良や変形が当業者に明らかとなり得ることは言うまでもない。したがって、かかる改良や変形が本発明の範囲を逸脱しない限り、これらも本発明に含まれると理解されるべきである。

【産業上の利用可能性】

【０３８５】

本発明は、情報処理装置に対してソフトウェアを提供する管理装置を製造及び販売する産業において、前記管理装置が、情報処理装置上で動作する不正なソフトウェアを特定し、安全にソフトウェアを更新する技術として利用することができる。

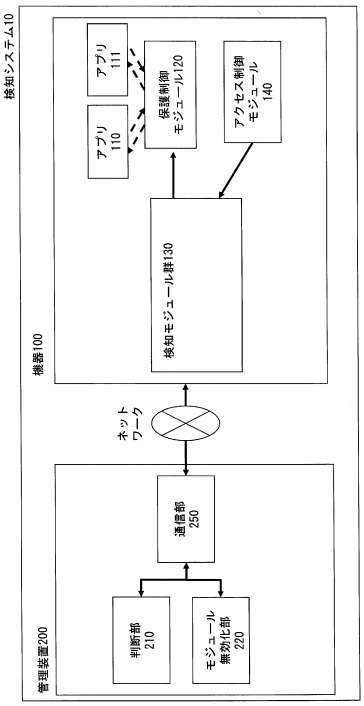
【符号の説明】

【０３８６】

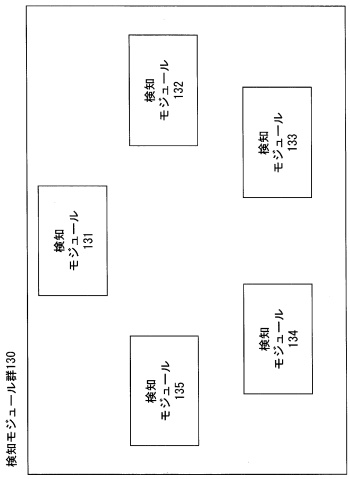
１０、１１　検知システム
１２　ソフトウェア更新システム
１００、１００ａ　機器
１１０、１１１　アプリ
１２０、１２０ａ　保護制御モジュール
１２１　新しい保護制御モジュール
１３０、１３０ａ　検知モジュール群
１３１、１３２、１３３、１３４、１３５　検知モジュール
１３１ａ、１３２ａ、１３３ａ、１３４ａ、１３５ａ　検知モジュール
１４０　アクセス制御モジュール
１５０　ＯＳ
１６０　ブートローダ
１７１　ＣＰＵ
１７２　ＥＥＰＲＯＭ
１７３　ＲＡＭ
１７４　ＮＩＣ
２００、２００ａ、２００ｂ　管理装置
２１０　判断部
２２０　モジュール無効化部
２３０　監視パターン更新部
２４０　更新用ソフトウェア配布部
２５０　通信部
３０１　受信部
３０２　送信部
３０３　制御部
３０４　復号ロード部

３０５　改ざん検出部
３０６　解析ツール検出部
３０７　暗復号鍵保持部
３０８　暗復号鍵分散部
３０９　証明書生成部
３１０　暗復号鍵復元部
３１１　暗復号鍵生成部
４０１　受信部
４０２　送信部
４０３　制御部
４０４　検証部
４０５　ＭＡＣ値生成部
４０６　ＭＡＣ値テーブル更新部
４０７　更新部
４０８　認証部
４０９　分散情報保持部
５０１　受信部
５０２　送信部
５０３　アクセス情報保持部
６０１　受信部
６０２　送信部
６０３　指示生成部
６０４　モジュール特定部
６０５　検出結果保持部
７０１　受信部
７０２　送信部
７０３　アクセス情報取得鍵保持部
７０４　検知モジュール選択部
８０１　受信部
８０２　送信部
８０３　監視パターン生成部
８０４　制御部
９０１　受信部
９０２　送信部
９０３　制御部
９０４　認証部
９０５　暗号鍵生成部
９０６　暗号処理部
９０７　検知モジュール選択部
９０８　証明書生成部
９０９　署名秘密鍵保持部
９１０　更新用ソフトウェア保持部
９１１　暗号鍵保持部

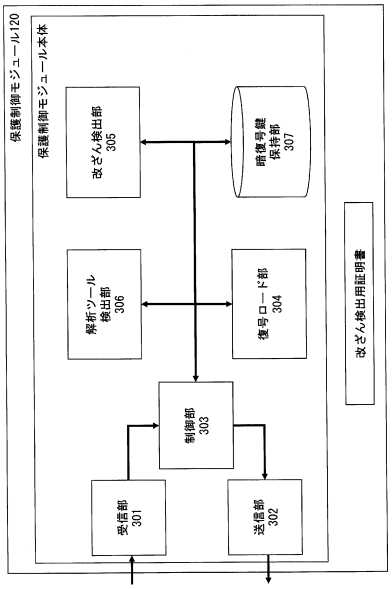
【図１】


検知システム10
機器100
アプリ
110
アプリ
111
保護制御
モジュール120
アクセス制御
モジュール
140
検知モジュール群130
ネット
ワーク
管理装置200
通信部
250
判断部
210
モジュール
無効化部
220

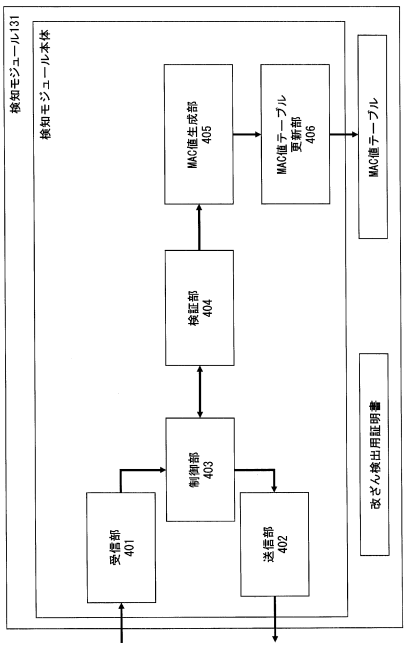
【図２】


検知モジュール群130
検知
モジュール
131
検知
モジュール
132
検知
モジュール
133
検知
モジュール
134
検知
モジュール
135

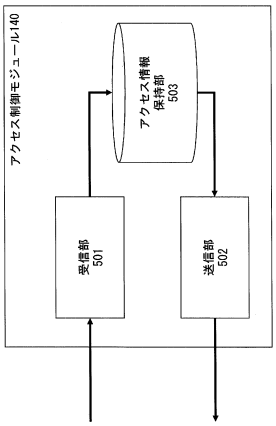
【図３】


保護制御モジュール120
保護制御モジュール本体
改ざん検出部
305
暗復号鍵
保持部
307
解析ツール
検出部
306
復号ロード部
304
制御部
303
受信部
301
送信部
302
改ざん検出用証明書

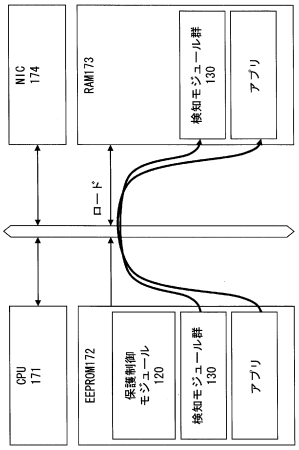
【図４】


検知モジュール131
検知モジュール本体
MAC値生成部
405
MAC値テーブル
更新部
406
MAC値テーブル
検証部
404
制御部
403
受信部
401
送信部
402
改ざん検出用証明書

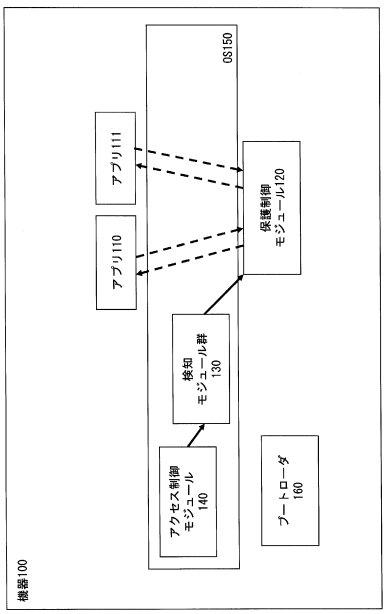
【図５】


アクセス制御モジュール140
アクセス情報
保持部
503
受信部
501
送信部
502

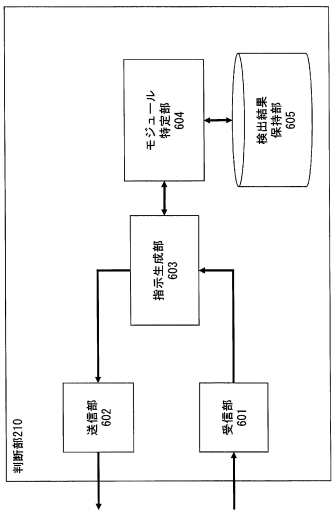
【図６】


NIC
174
RAM173
検知モジュール群
130
アプリ
ロード
CPU
171
EEPROM172
保護制御
モジュール
120
検知モジュール群
130
アプリ

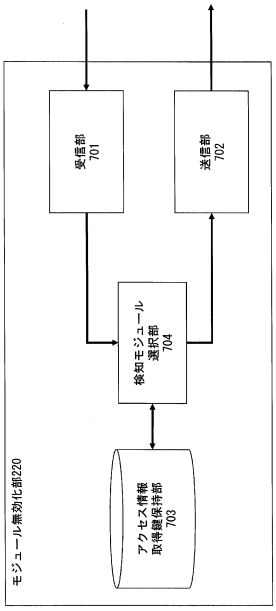
【図７】


機器100
OS150
アプリ111
アプリ110
保護制御
モジュール120
検知
モジュール群
130
アクセス制御
モジュール
140
ブートローダ
160

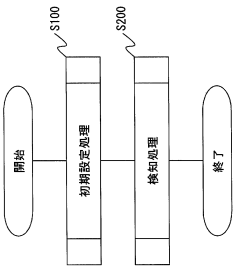
【図８】


判断部210
モジュール
特定部
604
検出結果
保持部
605
指示生成部
603
送信部
602
受信部
601

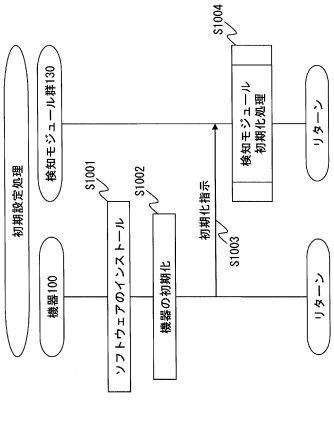
【図９】



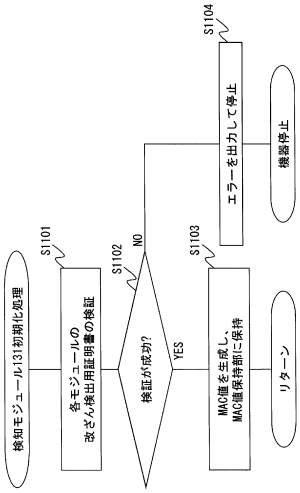
【図１０】



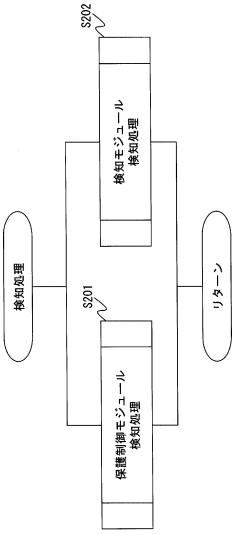
【図１１】



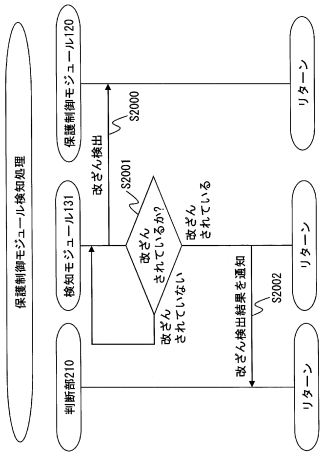
【図１２】



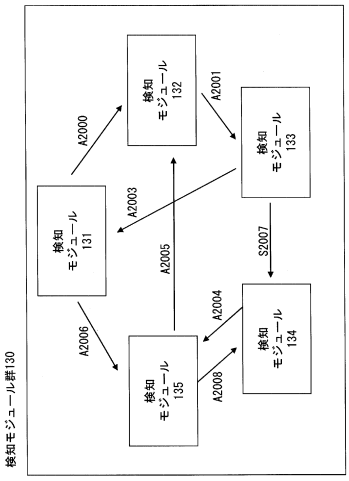
【図１３】



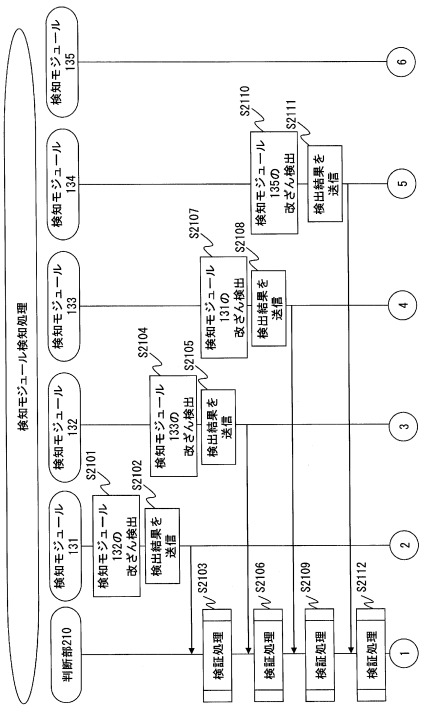
【図１４】



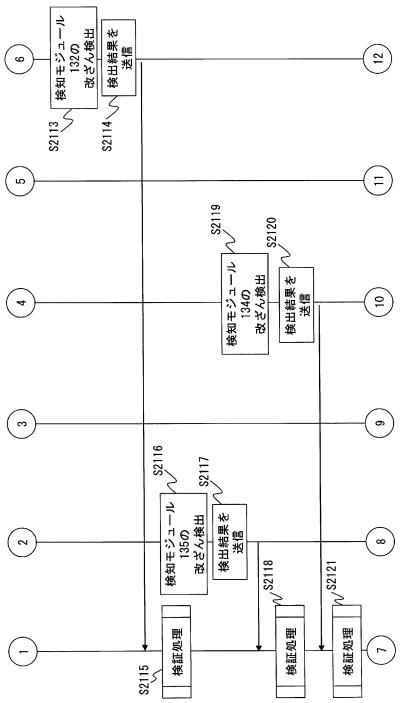
【図１５】



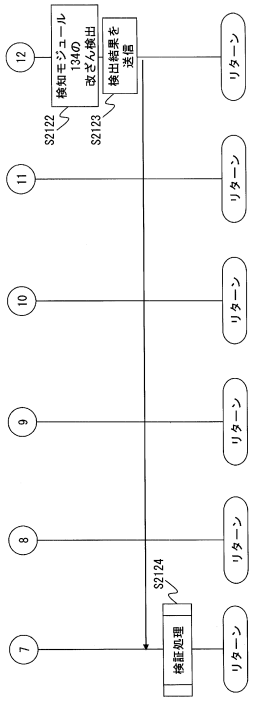
【図１６】



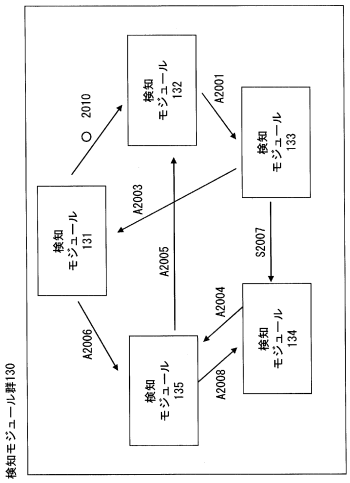
【図１７】



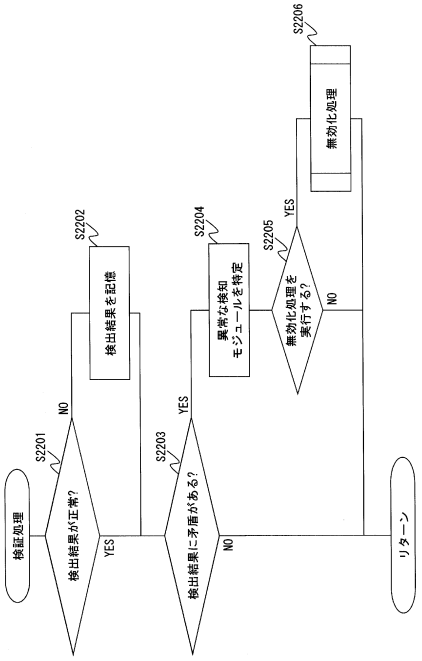
【図１８】



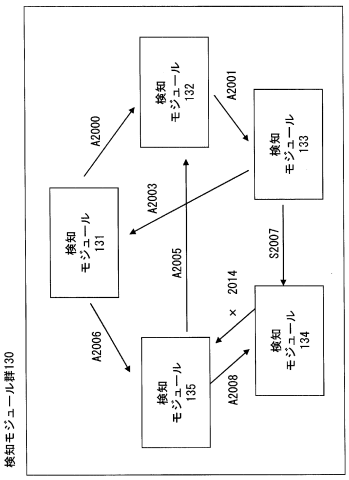
【図１９】



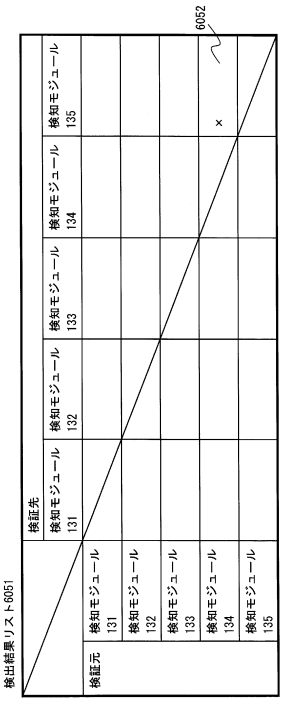
【図２０】



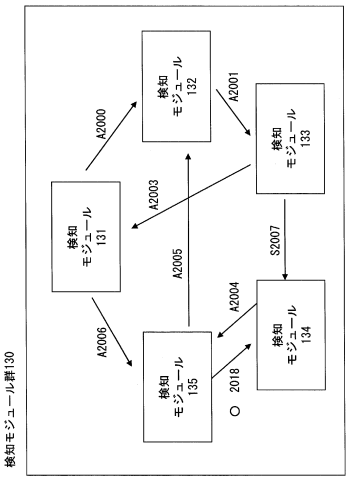
【図２１】



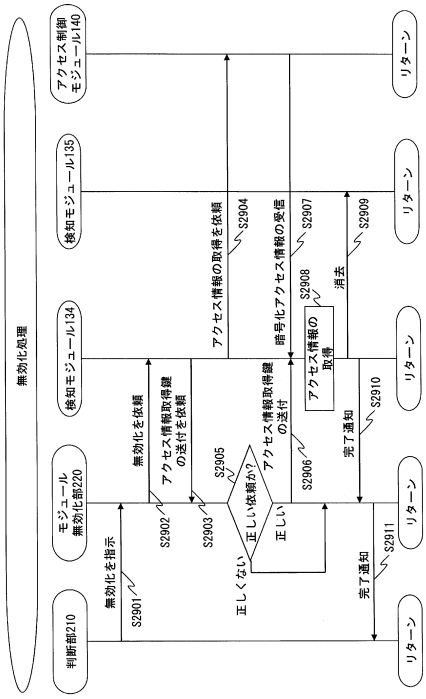
【図２２】



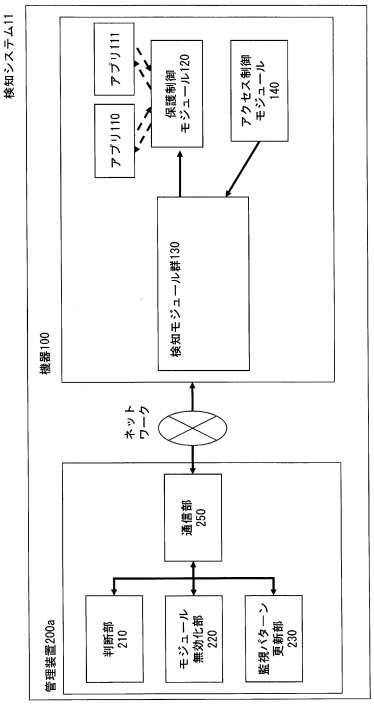
【図２３】



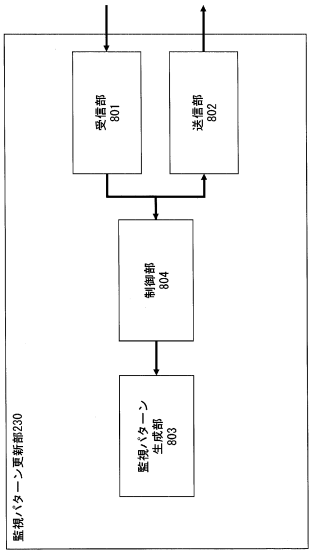
【図２４】



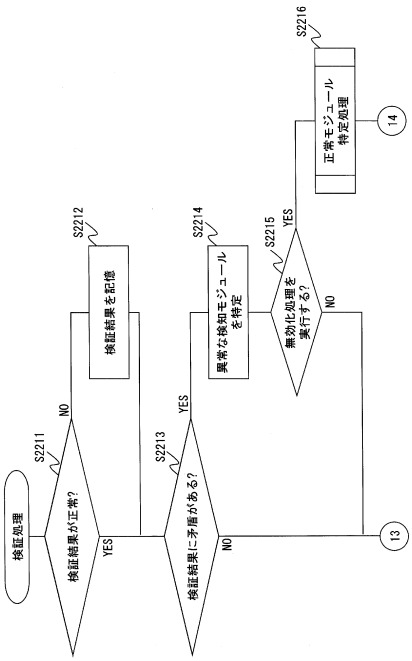
【図２５】



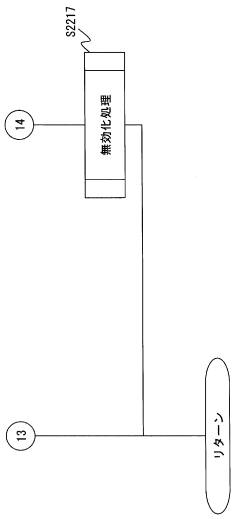
【図２６】



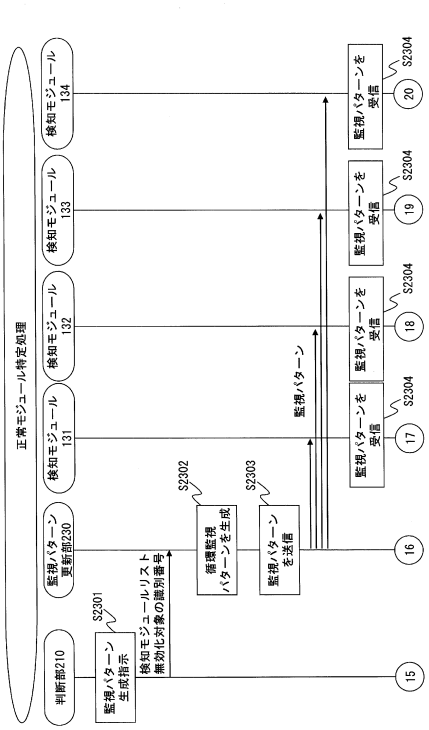
【図２７】



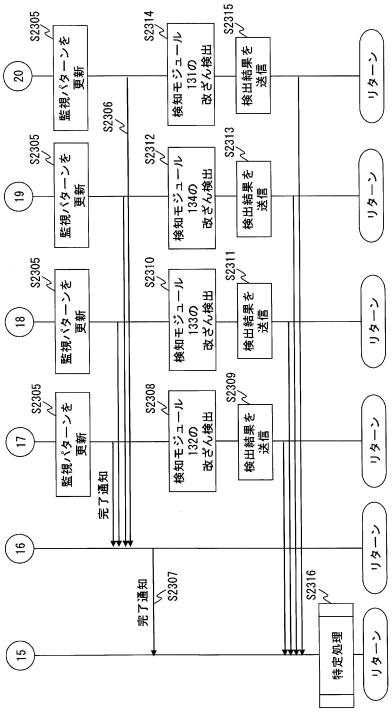
【図２８】



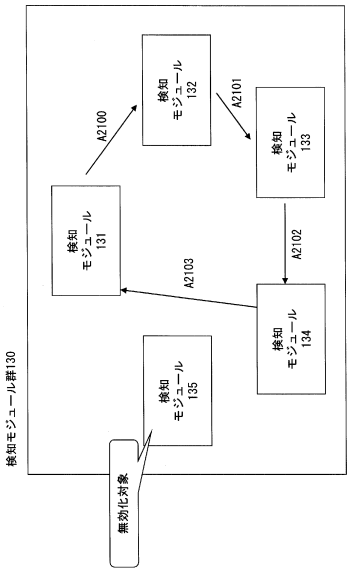
【図２９】



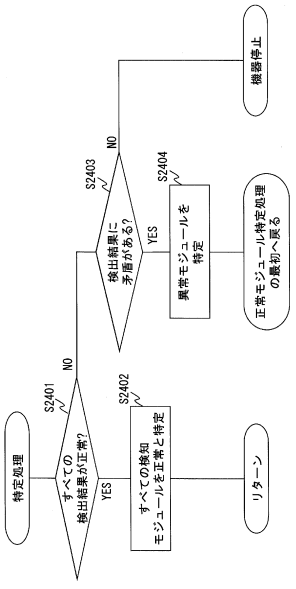
【図３０】



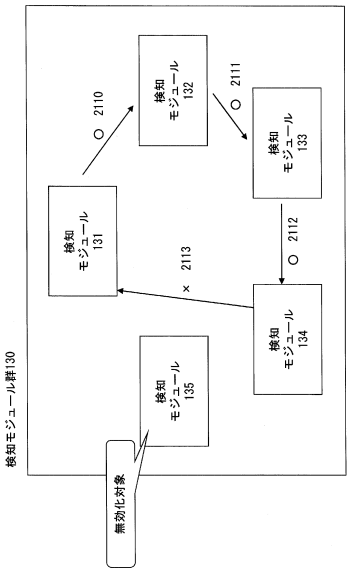
【図３１】



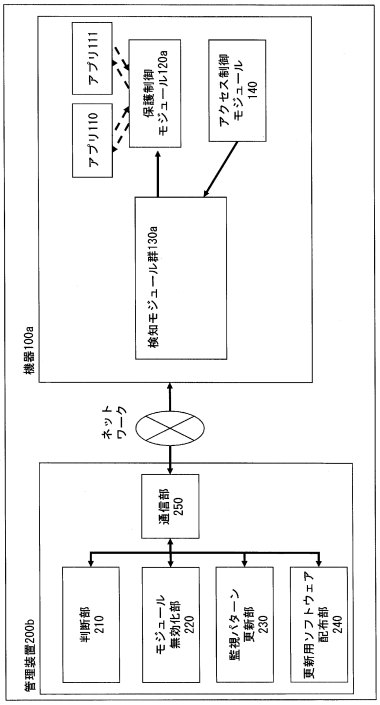
【図３２】



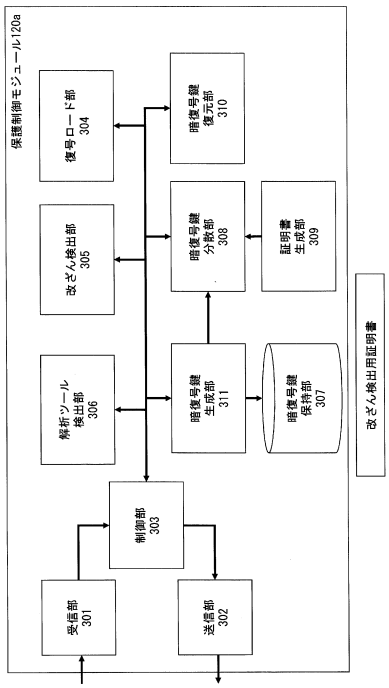
【図３３】



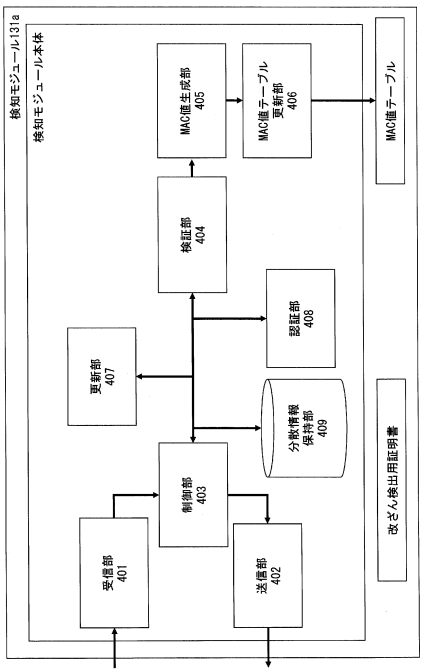
【図３４】



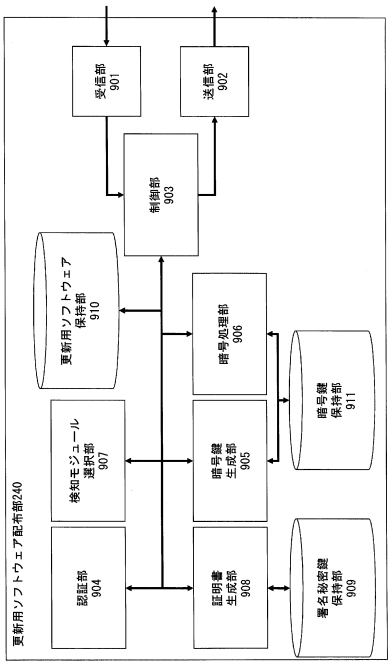
【図３５】



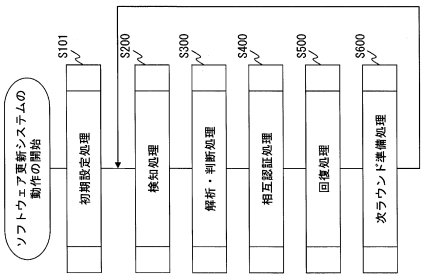
【図３６】



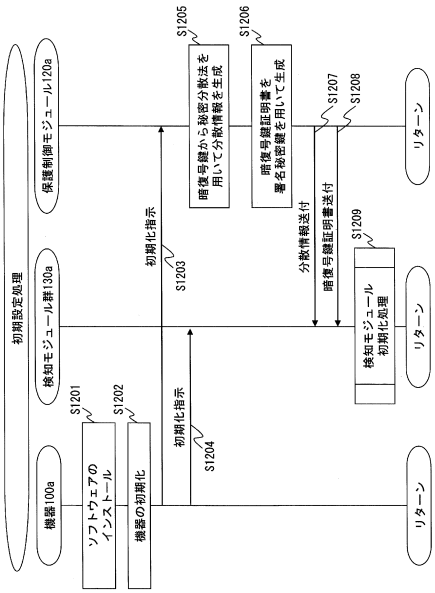
【図３７】



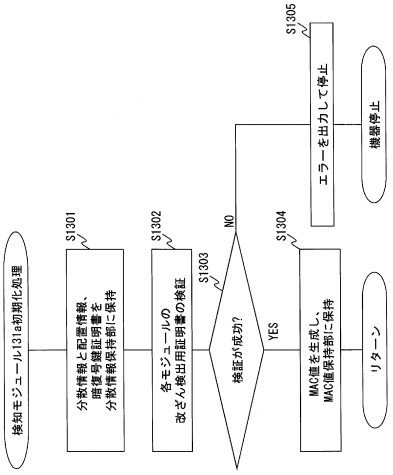
【図３８】



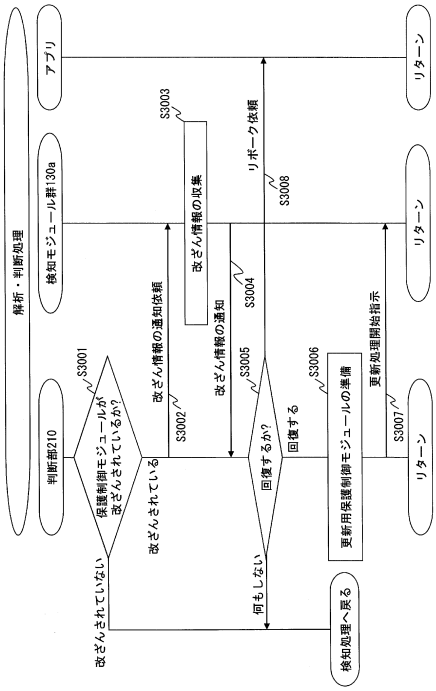
【図３９】



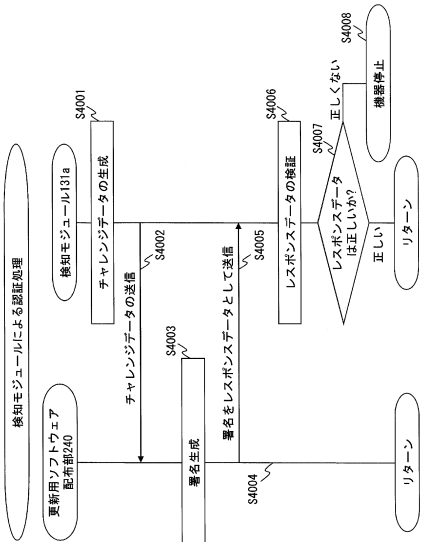
【図４０】



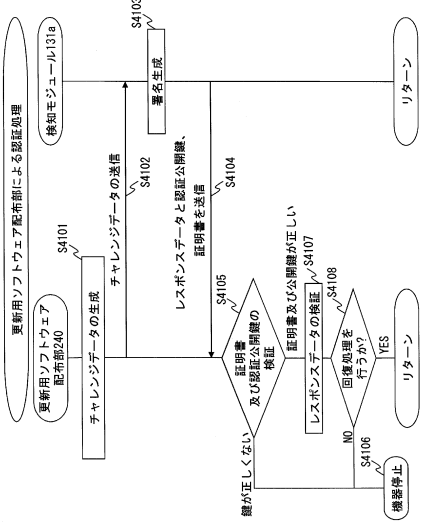
【図４１】



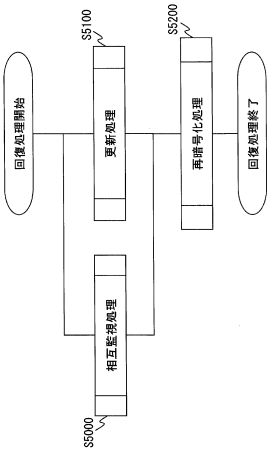
【図４２】



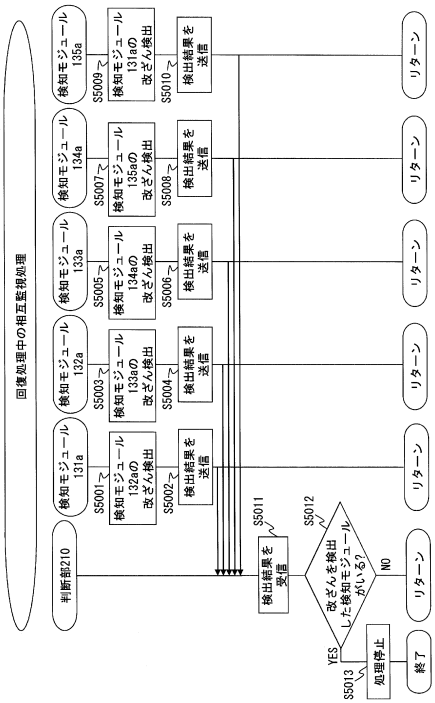
【図４３】



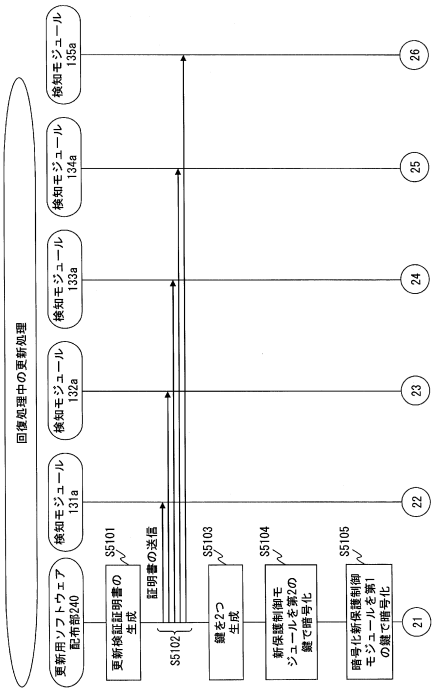
【図４４】



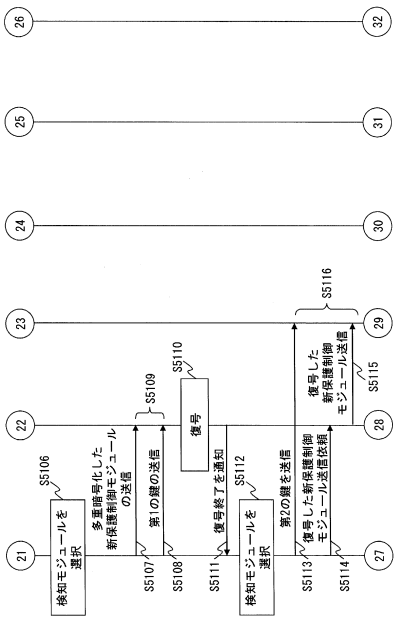
【図４５】



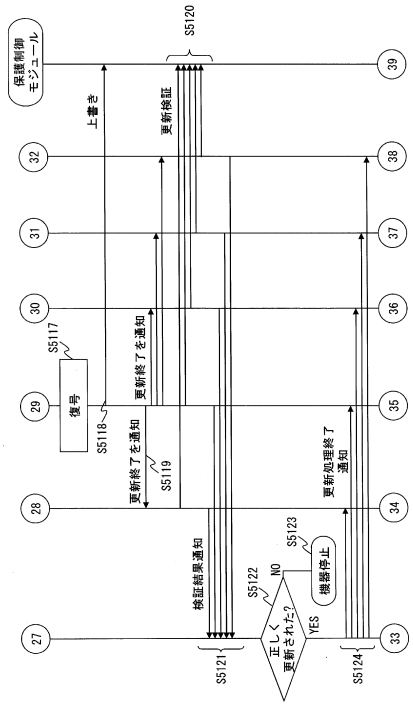
【図４６】



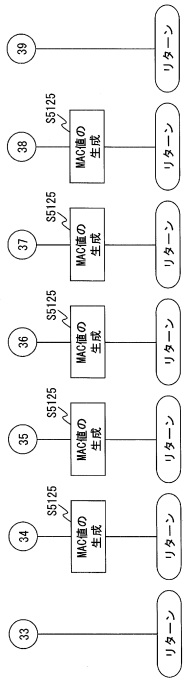
【図４７】



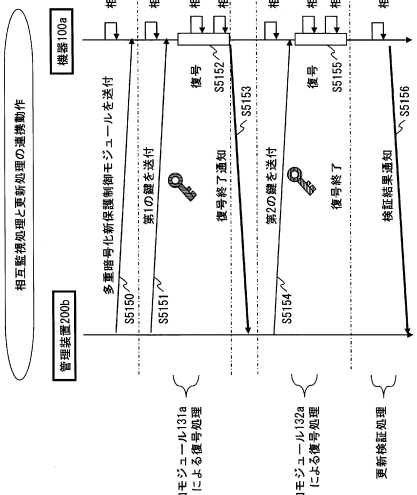
【図４８】



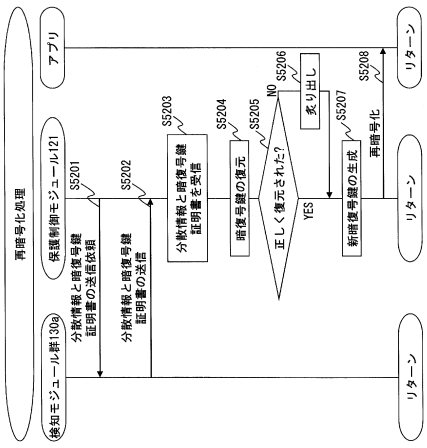
【図４９】



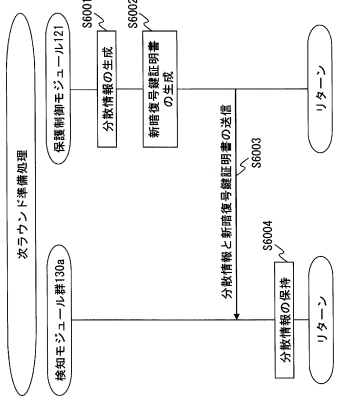
【図５０】



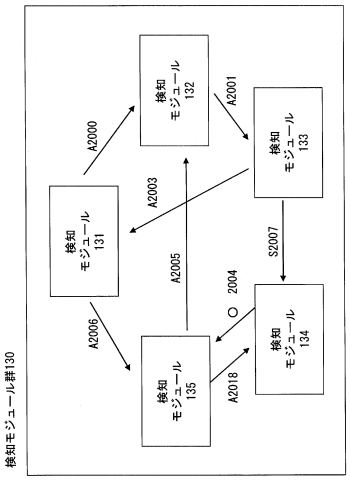
【図５１】



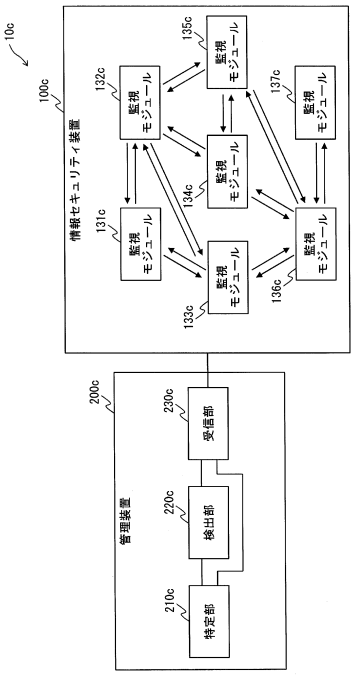
【図５２】



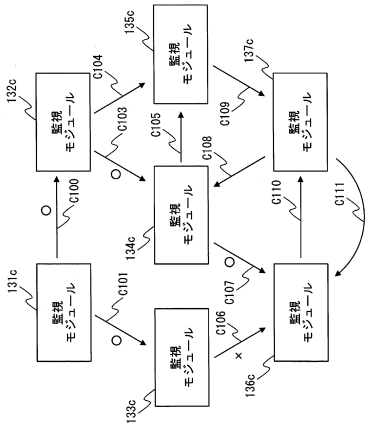
【図５３】



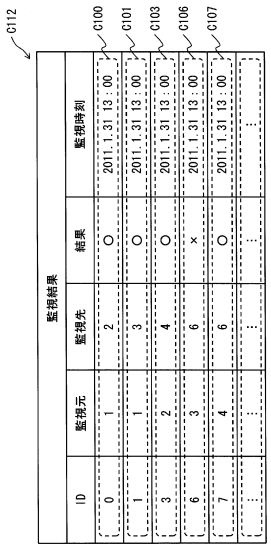
【図５４】



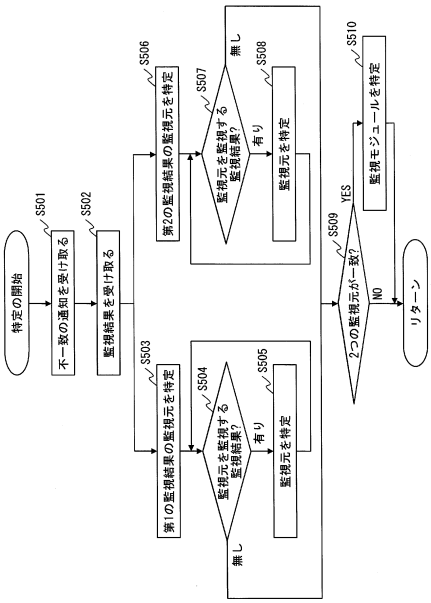
【図５５】



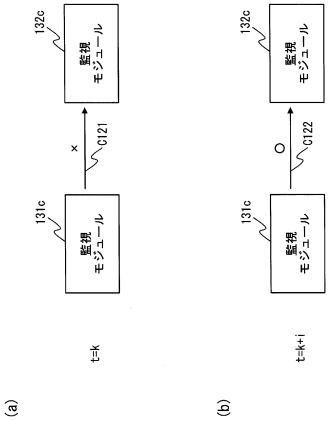
【図５６】



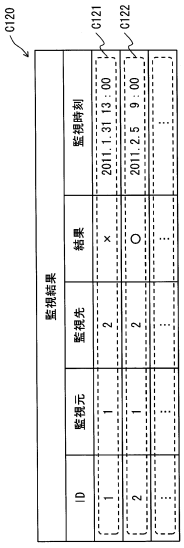
【図５７】



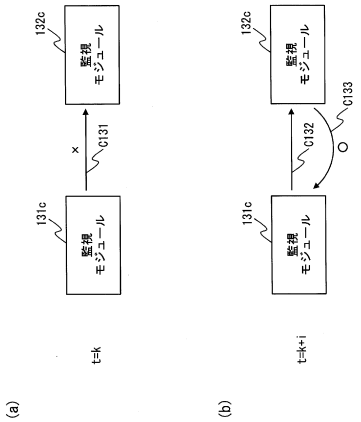
【図５８】



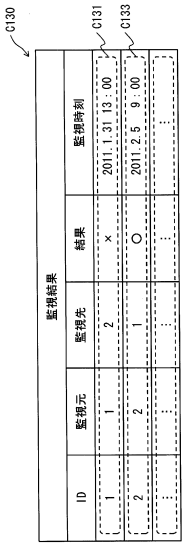
【図５９】



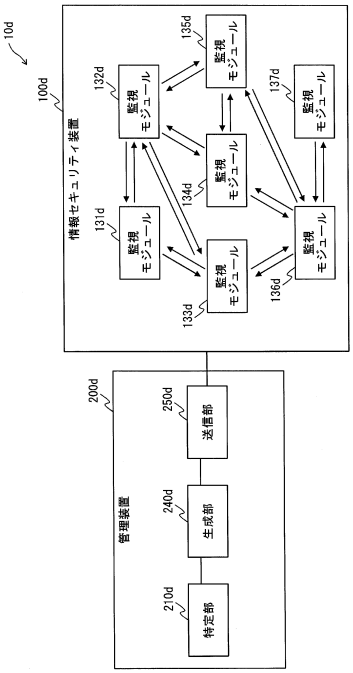
【図６０】



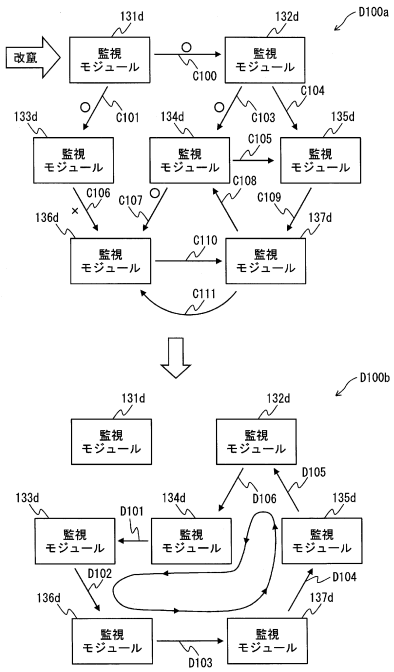
【図６１】



【図６２】



【図６３】



【図６４】

監視パターン D106

ID	監視元	監視先
6	2	4

監視パターン D101

ID	監視元	監視先
1	4	3

監視パターン D102

ID	監視元	監視先
2	3	6

監視パターン D103

ID	監視元	監視先
3	6	7

監視パターン D104

ID	監視元	監視先
4	7	5

監視パターン D105

ID	監視元	監視先
5	5	2

フロントページの続き

(72)発明者　海上　勇二
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　布田　裕一
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　松崎　なつめ
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　静谷　啓樹
宮城県仙台市青葉区片平二丁目１番１号　国立大学法人東北大学内
(72)発明者　酒井　正夫
宮城県仙台市青葉区片平二丁目１番１号　国立大学法人東北大学内
(72)発明者　磯辺　秀司
宮城県仙台市青葉区片平二丁目１番１号　国立大学法人東北大学内
(72)発明者　小泉　英介
宮城県仙台市青葉区片平二丁目１番１号　国立大学法人東北大学内
(72)発明者　長谷川　真吾
宮城県仙台市青葉区片平二丁目１番１号　国立大学法人東北大学内

審査官　戸島　弘詩

(56)参考文献　国際公開第２０１０／０９２８３０（WO，Ａ１）
特開２０００－２９３３７０（ＪＰ，Ａ）
特開２００７－１１４９４１（ＪＰ，Ａ）
特開２０００－０４７９０６（ＪＰ，Ａ）
国際公開第２００９／１１８８０１（WO，Ａ１）
国際公開第２００９／１１９０４９（WO，Ａ１）
特開２００９－００９５５７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／１２－２１／１６，２１／５０－２１／５７
Ｇ０６Ｆ１１／３０