

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2007-257085

(P2007-257085A)

(43) 公開日 平成19年10月4日(2007.10.4)

(51) Int. Cl.	F I	テーマコード (参考)
<b>G 0 6 F 11/30 (2006.01)</b>	G O 6 F 11/30 D	2 C O 6 1
<b>G 0 6 F 13/00 (2006.01)</b>	G O 6 F 13/00 3 5 1 N	5 B O 4 2
<b>B 4 1 J 29/46 (2006.01)</b>	G O 6 F 11/30 K	5 B O 8 9
	B 4 1 J 29/46	

審査請求 未請求 請求項の数 5 O L (全 13 頁)

(21) 出願番号 特願2006-77676 (P2006-77676)  
 (22) 出願日 平成18年3月20日 (2006.3.20)

(71) 出願人 000006747  
 株式会社リコー  
 東京都大田区中馬込 1 丁目 3 番 6 号  
 (74) 代理人 100110652  
 弁理士 塩野谷 英城  
 (72) 発明者 穂積 洋  
 東京都大田区中馬込 1 丁目 3 番 6 号 株  
 会社リコー内  
 F ターム (参考) 2C061 AP01 AP10 HV35 HX10  
 5B042 GA01 JJ02 KK12 KK14 KK17  
 MC15 MC40  
 5B089 JA35 MC00

(54) 【発明の名称】 機器遠隔監視システム

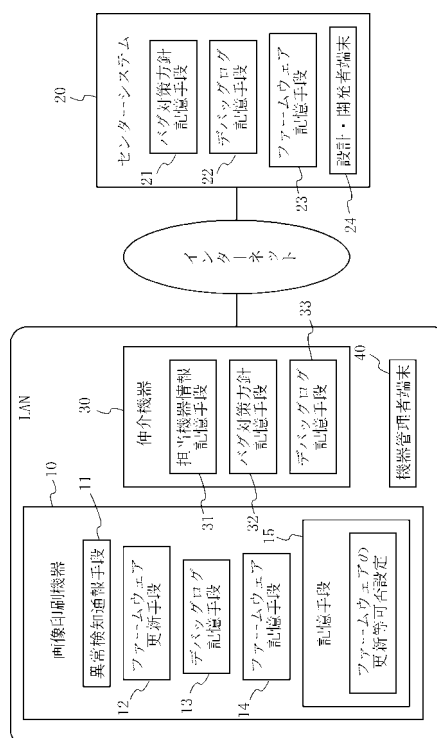
## (57) 【要約】

【課題】 お客様におけるソフトウェアバグの発生に対し、訪問によるタイムロスを省き、直ちに対策を開始することができるシステムの提供を課題とする。

【解決手段】 監視仲介装置 30 は、担当する機器の種別情報およびファームウェアバージョン情報をセンターシステム 20 に通知して当該機器に対応するソフトウェアバグ情報およびバグ対策方針の提供をセンターシステムに要求する。監視仲介装置は、センターシステムから送られたソフトウェアバグ情報およびバグ対策方針を受信する。

一方、機器 10 は、ファームウェアを読み出して動作し、異常を検知した場合、異常情報を監視仲介装置に送信する。監視仲介装置は、ソフトウェアバグ情報が一致するバグ対策方針を記憶手段から検索し実行する。

【選択図】 図 1



## 【特許請求の範囲】

## 【請求項 1】

機器を遠隔監視するセンターシステムと、このセンターシステムに遠隔監視される複数の機器と、この複数の機器の一部を担当し当該担当する機器と前記センターシステムとの間の通信を仲介する監視仲介装置とを備えた機器遠隔監視システムにおいて、

前記センターシステムは、前記機器のソフトウェアバグ情報と、各ソフトウェアバグへの対策方針（以下、「バグ対策方針」という）とを関連付けて登録したバグ対策方針記憶手段を備え、

前記ソフトウェアバグ情報は、前記機器の種別情報と、当該機器が動作に用いるファームウェアのバージョン情報と、当該機器とファームウェアとの組み合わせにおいて生じ得る機器の異常情報とを関連付けており、 10

また、前記バグ対策方針は、バグ対策済みファームウェアへの更新およびデバッグログ取得に関する方針を含み、

これらソフトウェアバグ情報およびバグ対策方針は、端末から随時更新可能な環境に置き、

前記監視仲介装置は、前記担当する機器の種別情報およびファームウェアバージョン情報を当該機器又は入力装置から取得した後、当該機器の種別情報およびファームウェアバージョン情報を前記センターシステムに通知して当該機器に対応するソフトウェアバグ情報およびバグ対策方針の提供を前記センターシステムに要求し、

当該センターシステムは、前記監視仲介装置から送られた機器の種別情報およびファームウェアバージョン情報に対応するソフトウェアバグ情報およびバグ対策方針を前記バグ対策方針記憶手段から抽出し、要求元の監視仲介装置に送信し、 20

監視仲介装置は、前記センターシステムから送られたソフトウェアバグ情報およびバグ対策方針を受信し、当該ソフトウェアバグ情報とバグ対策方針との関連付けを記憶手段に格納し、

一方、前記機器は、予め組み込まれたファームウェアを記憶手段から読み出して動作し、異常を検知した場合、当該異常の内容を示す異常情報を当該機器を担当する監視仲介装置に送信し、

監視仲介装置は、前記担当する機器から異常情報を受信した場合、当該機器の種別情報、ファームウェアバージョン情報およびソフトウェアバグ情報に含まれる異常情報が一致するバグ対策方針を記憶手段から検索し、検索されたバグ対策方針を前記異常情報を出力した機器に対して実行する、 30

ことを特徴とした機器遠隔監視システム。

## 【請求項 2】

請求項 1 記載の機器遠隔監視システムにおいて、

前記監視仲介装置は、前記実行を決定したバグ対策方針が、「対策済みファームウェアの更新」である場合、前記異常情報を出力した機器に当該バグ対策済みファームウェアの更新を指示し、

または、前記監視仲介装置は、前記実行を決定したバグ対策方針が、「デバッグログ取得用ファームウェアへの更新」を含む場合、前記異常情報を出力した機器に当該デバッグログ取得用ファームウェアへの更新を指示し、 40

または、前記監視仲介装置は、前記実行を決定したバグ対策方針が、「一定期間に渡るデバッグログの取得」を含む場合、前記デバッグログ取得用ファームウェアを実行した機器から前記一定期間に渡りデバッグログを採取し、当該一定期間の経過後に、当該機器の通常動作用のファームウェアへの更新を指示し、

一方、前記ファームウェアを監視仲介装置から受信した機器は、前記ファームウェア更新の指示に従い、記憶手段にある現行のファームウェアを当該受信したファームウェアに更新し、その後、当該更新後のファームウェアを実行し、

当該更新後のファームウェアが、デバッグログの採取を要求する場合は、所定のデバッグログを記憶手段に採取し、採取したデバッグログを当該機器を担当する監視仲介装置に 50

送信する、  
ことを特徴とした機器遠隔監視システム。

【請求項 3】

請求項 2 記載の機器遠隔監視システムにおいて、  
前記監視仲介装置は、前記機器から送られるデバッグログを取得して記憶手段に蓄積し、当該記憶手段に蓄積するデバッグログが予め設定された転送単位を満たすごとに、当該転送単位を記憶手段から読み出して前記センターシステムに転送することを特徴とした機器遠隔監視システム。

【請求項 4】

請求項 2 又は 3 記載の機器遠隔監視システムにおいて、  
前記バグ対策方針が「一定期間に渡るデバッグログの取得」を含む場合、当該バグ対策方針には、当該デバッグログを機器から取得する際のプロトコルの指定を含め、  
前記監視仲介装置は、前記機器からデバッグログを取得する際に、前記バグ対策方針に含まれるプロトコルの指定に基づいてデバッグログ出力の際のプロトコルを機器に指示し、  
前記機器は、監視仲介装置に指示された所定のプロトコルで前記デバッグログを出力することを特徴とした機器遠隔監視システム。

【請求項 5】

請求項 2, 3 又は 4 記載の機器遠隔監視システムにおいて、  
前記機器は、前記ファームウェア更新又はデバッグログ取得について可否の設定を記憶手段に記憶すると共に、当該設定を変更するための管理者インタフェースを備え、機器管理者に当該管理者インタフェースを介して前記可否の設定を変更させる機能を有し、  
前記機器は、前記監視仲介装置からファームウェア更新又はデバッグログ取得を指示された場合、前記可否の設定を確認し、ファームウェア更新又はデバッグログ取得を禁止する設定になっている場合、その旨を前記監視仲介装置へ通知し、  
この通知を受信した監視仲介装置は、当該通知を出力した機器の管理者の連絡先を当該連絡先が予め登録されている記憶手段から読み出し、当該管理者の連絡先に前記設定の変更を促す通知を送信し、  
さらに、当該監視仲介装置は、前記機器において前記可否の設定が禁止から許可に変更されたことを知ると、前記ファームウェア更新又はデバッグログ取得を当該設定を変更した機器に対して指示する、  
ことを特徴とした機器遠隔監視システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、機器遠隔監視システムに係り、特に、ファームウェアに従って動作する機器の遠隔監視システムに関し、画像印刷機器にも好適な機器遠隔監視システムに関する。

【背景技術】

【0002】

従来の画像印刷機器の遠隔管理システムは、画像印刷機器と遠隔管理センターとの間に仲介機器を備えている。当該仲介機器は、管理する画像印刷機器の印刷枚数のカウンター（ログ）や状態情報を HTTPS/SOAP や MIB などのプロトコルで取得し、または画像印刷機器からの通報を受け、その内容をセンターに通知することで機器管理のシステムを運用している。（HTTPS = Hyper Text Transfer Protocol over SSL、SOAP = Simple Object Access Protocol、MIB = Management Information Base）

【0003】

しかし、機器の異常が発生した時に受け取る通知の内容は、部品の故障などのセンサーなどで検知しやすいものに関する通知が大半である。一方、機器の異常が、潜在的なソフトウェアバグなどに由来する場合、その原因はソフトウェアのエラーなどとして、大きく丸められて通知され、問題が大きくなるまで放置されることが多々存在する。

10

20

30

40

50

## 【 0 0 0 4 】

また、機器の異常状態を解析するためには、機器のデバッグログを取得する必要があるが、それらは一時的な情報ですぐに流れてしまうログであり、また、その情報量は多く、その全てを取得しつづけると、膨大な情報量となってしまう。しかも問題によっては現在出力しているデバッグログのみでは解析の為に情報が足りないことさえある。

## 【 0 0 0 5 】

その為、現状では問題の発生しているお客様と交渉して、ログ取り用のツールを入れたノートPC等をお客様環境に置かせて頂き、ログをHDDに取り続けて、しばらく後にそのノートPCを回収する。また場合によってはログ出力用の画像処理装置のファームウェアを一時的に導入させていただいてログを取るなどと言った方法しかない。(HDD=Hard Disk Drive) 10

## 【 0 0 0 6 】

またその障害に対応したファームウェアがリリースされたときも、その障害が発生しているお客様は把握できず、全てのお客様へのファームウェア更新が必要になったり、ファームウェア更新が必要なお客様がいつまでも放置されるおそれもある。

## 【 0 0 0 7 】

出願人は、上記に関する公知技術文献の存在を知らない。

## 【 発明の開示 】

## 【 発明が解決しようとする課題 】

## 【 0 0 0 8 】

本発明は、かかる従来例の有する不都合を改善し、特に、お客様におけるソフトウェアバグの発生に対し、訪問によるタイムロスを省き、直ちに対策を開始することができるシステムの提供を課題とする。 20

## 【 課題を解決するための手段 】

## 【 0 0 0 9 】

本願発明にかかる機器遠隔監視システムは、機器を遠隔監視するセンターシステムと、このセンターシステムに遠隔監視される複数の機器と、この複数の機器の一部を担当し当該担当する機器とセンターシステムとの間の通信を仲介する監視仲介装置とを備える。

## 【 0 0 1 0 】

センターシステムは、機器のソフトウェアバグ情報と、各ソフトウェアバグへの対策方針(以下、「バグ対策方針」という)とを関連付けて登録したバグ対策方針記憶手段を備える。このうち、ソフトウェアバグ情報は、機器の種別情報と、当該機器が動作に用いているファームウェアのバージョン情報と、当該機器とファームウェアとの組み合わせにおいて生じ得る機器の異常情報とを関連付けている。また、バグ対策方針は、バグ対策済みファームウェアへの更新およびデバッグログ取得に関する方針を含む。これらソフトウェアバグ情報およびバグ対策方針は、設計・開発者の端末から随時更新可能な環境に置く。 30

## 【 0 0 1 1 】

監視仲介装置は、担当する機器の種別情報およびファームウェアバージョン情報を当該機器又は入力装置から取得した後、当該機器の種別情報およびファームウェアバージョン情報をセンターシステムに通知して当該機器に対応するソフトウェアバグ情報およびバグ対策方針の提供をセンターシステムに要求する。当該センターシステムは、監視仲介装置から送られた機器の種別情報およびファームウェアバージョン情報に対応するソフトウェアバグ情報およびバグ対策方針をバグ対策方針記憶手段から抽出し、要求元の監視仲介装置に送信する。監視仲介装置は、センターシステムから送られたソフトウェアバグ情報およびバグ対策方針を受信し、当該ソフトウェアバグ情報とバグ対策方針との関連付けを記憶手段に格納する。 40

## 【 0 0 1 2 】

一方、機器は、予め組み込まれたファームウェアを記憶手段から読み出して動作し、異常を検知した場合、当該異常の内容を示す異常情報を当該機器を担当する監視仲介装置に送信する。監視仲介装置は、担当する機器から異常情報を受信した場合、当該機器の種別 50

情報、ファームウェアバージョン情報およびソフトウェアバグ情報に含まれる異常情報が一致するバグ対策方針を記憶手段から検索し、検索されたバグ対策方針を異常情報を出力した機器に対して実行する。

【発明の効果】

【0013】

これによると、お客様におけるソフトウェアバグの発生に対し、訪問によるタイムロスを省き、直ちに対策を開始することができる。

【発明を実施するための最良の形態】

【0014】

以下、本発明の一実施形態である機器遠隔監視システムを、図面を参照しつつ説明する 10

【0015】

図1は機器遠隔監視システムの構成図である。機器遠隔監視システムは、画像印刷機器10を遠隔監視するセンターシステム20と、このセンターシステム20に遠隔監視される画像印刷機器10と、この画像印刷機器10を担当し当該担当する画像印刷機器10とセンターシステム20との間の通信を仲介する仲介機器30（監視仲介装置）とを備えている。符号40は、画像印刷機器10を管理する機器管理者の端末である。画像印刷機器10と仲介機器30はLAN（Local Area Network）に接続され、相互に通信が可能となっている。画像印刷機器10および仲介機器30は、便宜上1つだけ図示しているが実際には複数存在し、各仲介機器30は、担当する複数の画像印刷機器10と通信し、かつ、各 20  
仲介機器30はセンターシステム20と通信する。本実施形態において、画像印刷機器10および仲介機器30を含むLANと、センターシステム20とは、インターネットを介して通信を行うようになっている。

【0016】

センターシステム20は、画像印刷機器10のソフトウェアバグ情報と、各ソフトウェアバグへの対策方針（以下、「バグ対策方針」という）とを関連付けて登録したバグ対策方針記憶手段21を備えている。また、センターシステム20は、画像印刷機器10において採取されるデバッグログを取得して格納するデバッグログ記憶手段22と、画像印刷機器10が利用する数種のファームウェアを記憶したファームウェア記憶手段23と、設計・開発者がバグ対策方針記憶手段21の内容の更新や、デバッグログ記憶手段22に格 30  
納されたデバッグログの内容を参照するための設計・開発者端末24とを備えている。ここで、設計・開発者端末24の設置場所は問わない。各記憶手段に記憶された情報を操作又は閲覧できる環境にあればよい。

【0017】

図2および図3は、バグ対策方針記憶手段21に登録されるソフトウェアバグ情報と、バグ対策方針との関連付けを示している。図2の図表の下に図3の図表が接続する。

【0018】

ソフトウェアバグ情報は、画像印刷機器10の種別情報と、当該機器が動作に用いるファームウェアのバージョン情報と、当該機器とファームウェアとの組み合わせにおいて生じ得る機器の異常情報とを関連付けている。本実施形態において、画像印刷機器10の種 40  
別情報は、画像印刷機器10のAAAA等の機種と、00000～200000等の機番とにより分類されている。また、ファームウェアバージョン情報は、～1.01等の番号により分類されている。また、異常情報としては、異常状態を示すSC001等のコードと、その発生頻度との組み合わせによって分類されている。

【0019】

ここで、上記異常状態には、特定サービスコールの発生、パースエラーや取得情報の異常などが含まれる。また、上記発生頻度には、発生したら即、所定回数以上発生したら、所定期間内に連続して発生したら、などが含まれる。

【0020】

また、バグ対策方針は、バグ対策済みファームウェアへの更新およびデバッグログ取得 50

に関する方針を含む。本実施形態において、バグ対策方針には、ファームウェアを所定のバージョンのバグ対策済みファームウェアに更新する、デバッグログをrsh(remote shell)コマンド等の所定のコマンドで取得する、デバッグログをHTTPS/SOAP等の所定のプロトコルで取得する、ログ採取用特別ファームウェア(通常動作用のファームウェアにおいてデバッグログの採取機能を特化したもの)に更新しその後デバッグログを取得する、等の種類が含まれる。また、バグ対策方針がデバッグログの取得を含む場合、その取得期間も1ヶ月、スナップショット、一週間、等のように登録される。また、取得したデバッグログの識別子としてデバッグログ番号を登録すると共に、当該デバッグログの通知連絡先の識別子を設計者XXXのように登録できるようになっている。

#### 【0021】

10

ここで、上記デバッグログの取得期間としては、スナップショット、数時間、指定日まで、等を設定できるようになっている。また、その取得ログ中で必要な情報のみを抜き出す為の、複数の正規表現を指定できるようにしてもよい。

#### 【0022】

これらソフトウェアバグ情報およびバグ対策方針は、設計・開発者端末24から随時更新できるようになっている。設計・開発者は設計・開発者端末24を操作し、ファームウェアの開発時、評価時または運用時に発見されたバグについて、ソフトウェアバグ情報およびバグ対策方針をバグ対策方針記憶手段21に登録する。

#### 【0023】

設計・開発者がソフトウェアバグ情報に対応するバグ対策方針を登録する際は、例えば次の判断に基づくといよい。(1)既知のバグでバグ対策ファームウェアがリリース済みの場合、バグ対策方針はバグ対策ファームウェアへの更新を選択する。(2)既知のバグであるが対策が不要で無視できる場合、バグ対策方針を登録する必要は必ずしもない。(3)既知のバグであるが未対策でありデバッグログ取得用ファームウェアがリリース済みである場合、バグ対策方針としてはデバッグログ取得用ファームウェアに更新し所定期間のデバッグログの取得を行い、その後通常動作用のファームウェアに書き戻す。(4)未知のバグでありデバッグログ取得用ファームウェアがリリース済みである場合、バグ対策方針としてはデバッグログ取得用ファームウェアに更新し所定期間のデバッグログの取得を行い、その後通常動作用のファームウェアに書き戻す。以上の判断により決定したバグ対策方針を、対応する機種、機番、ファームウェアバージョン、異常状態および発生頻度に関連付けて、バグ対策方針記憶手段21に登録する。

20

30

#### 【0024】

続いて、画像印刷機器10の構成を説明する。画像印刷機器10は、ファームウェア実行中の異常を検知し当該異常を示すコードを仲介機器30に通知する異常検知通報手段11と、仲介機器30の指示を受けて当該指示された所定のファームウェアをファームウェア記憶手段14に更新するファームウェア更新手段12とを備えている。また、画像印刷機器10は、ファームウェアの実行に伴って採取したデバッグログを蓄積するデバッグログ記憶手段13と、画像印刷機器10が起動時に読み込んで動作するファームウェアを記憶したファームウェア記憶手段14とを備えている。また、記憶手段15には、ファームウェアの更新やデバッグログの取得を許可するか否かの設定が記憶されている。

40

#### 【0025】

続いて、仲介機器30の構成を説明する。仲介機器30は、仲介機器30が担当する複数の画像印刷機器10の機器情報を記憶する担当機器情報記憶手段31を備えている。担当機器情報記憶手段31には、仲介機器30が担当する画像印刷機器10の機種、機番、ファームウェアのバージョン情報および機器管理者の連絡先が登録される。また、仲介機器30は、センターシステム20がバグ対策方針記憶手段21に格納しているソフトウェアバグ情報およびバグ対策方針のうち、担当機器情報記憶手段31に登録した担当機器に対応するソフトウェアバグ情報およびバグ対策方針だけを抜粋して保持するバグ対策方針記憶手段32を備えている。また、仲介機器30は、画像印刷機器10から取得したデバッグログを保存するデバッグログ記憶手段33を備えている。

50

## 【 0 0 2 6 】

ここで、以上の画像印刷機器 1 0、センターシステム 2 0 および仲介機器 3 0 は、プロセッサ等の処理手段がファームウェア等のプログラムを実行することにより、種々の機能、動作ないし動作手段を実現する。また、各記憶手段は、記憶装置の記憶領域として設けられる。また、機器およびシステム間の通信は、通信プロトコルに対応した所定の通信装置を介して行われる。

## 【 0 0 2 7 】

次に、上記構成の動作について具体的に説明する。

## 【 0 0 2 8 】

図 4 乃至図 7 は、上記構成による機器遠隔監視システムの動作を示すフローチャートである。図中、上記構成と同一部分については同一の符号を付する。また、図 4 の端子 1 ~ 4 は図 5 に接続し、図 6 の端子 1 1 ~ 1 4 は、図 7 に接続する。 10

## 【 0 0 2 9 】

まず、図 4 および図 5 のフローチャートに沿って、仲介機器 3 0 がセンターシステム 2 0 からバグ対策方針の抜粋を取得する動作について説明する。

## 【 0 0 3 0 】

仲介機器 3 0 は、画像印刷機器 1 0（機種 AAAA、機番 000001 とする）の担当を指示されると、画像印刷機器 1 0 の機種、機番、ファームウェアバージョン情報および当該機器の管理者の連絡先情報を取得し、それらの情報を関連付けて担当機器情報記憶手段 3 1 に登録する。また、仲介機器 3 0 は、画像印刷機器 1 0 の登録をセンターシステム 2 0 に通知する。センターシステム 2 0 は、この通知を受けて画像印刷機器 1 0 の登録に関する情報処理を実施し、当該情報処理が完了すると、仲介機器 3 0 に対し、画像印刷機器 1 0 の登録に関する情報処理が完了した旨を通知する（登録 OK）。この通知を受けた仲介機器 3 0 は、本件登録に関する所定の登録パラメータの変更を画像印刷機器 1 0 に指示する。この指示を受けた画像印刷機器 1 0 は、指示された登録パラメータの変更が完了すると、当該登録パラメータの変更完了を仲介機器 3 0 に通知する。この通知を受けた仲介機器 3 0 は、画像印刷機器 1 0 において登録パラメータの変更が完了した旨を、登録完了の通知としてセンターシステム 2 0 に通知する。この通知を受理したセンターシステム 2 0 は、登録完了通知の受理に対する応答を仲介機器 3 0 に返信する。 20

## 【 0 0 3 1 】

この返信を受けた仲介機器 3 0 は、いま登録した画像印刷機器 1 0 の機種、機番およびファームウェアのバージョン情報を担当機器情報記憶手段 3 1 から読み出し、センターシステム 2 0 に送信すると共に、当該画像印刷機器 1 0 に対応するバグ対策方針の提供を求める（関連バグ情報情報確認）。 30

## 【 0 0 3 2 】

この要求を受けたセンターシステム 2 0 は、仲介機器 3 0 から受信した画像印刷機器 1 0 の機種、機番およびファームウェアのバージョン情報の組み合わせに関連付けられたソフトウェアバグ情報およびバグ対策方針をバグ対策方針記憶手段 2 1 から抽出する。そして、抽出したソフトウェアバグ情報およびバグ対策方針を仲介機器 3 0 に送信する（関連バグ情報確認応答）。 40

## 【 0 0 3 3 】

センターシステム 2 0 からソフトウェアバグ情報およびバグ対策方針を受信した仲介機器 3 0 は、当該ソフトウェアバグ情報およびバグ対策方針の関連付けをバグ対策方針記憶手段 3 2 に登録する（関連バグ情報 DB 書き込み）。これによると、仲介機器 3 0 は、担当する画像印刷機器 1 0 のために必要なバグ対策方針だけを抜粋して保存するので、情報量を抑えることができる。

## 【 0 0 3 4 】

次に、画像印刷機器 1 0 が異常情報を検出した場合の動作を図 6 および図 7 のフローチャートに沿って説明する。

## 【 0 0 3 5 】

画像印刷機器 10 (機種 AAAA、機番 000001) においてファームウェアの実行に伴う異常を生じると、異常検知通報手段 11 は、異常状態を把握し、当該異常状態を表すコード (SC001 とする) を仲介機器 30 に通報する。この通報を受けた仲介機器 30 は、通報してきた画像印刷機器 10 に対し応答を返すと共に、センターシステム 20 に対し機種 AAAA、機番 000001 の画像印刷機器 10 が異常状態 SC001 を出力した旨を通知する。この通知を受けたセンターシステム 20 は、通知元の仲介機器 30 に応答を返す。この応答を受けた仲介機器 30 は、センターシステム 20 への通報が完了した旨を前記通報を出力した画像印刷機器 10 に通知する。この通知を受けた画像印刷機器 10 は、仲介機器 30 に対し応答を返す。

【 0 0 3 6 】

10

この応答を受けた仲介機器 30 は、通報をしてきた画像印刷機器 10 の機種、機番およびファームウェアのバージョン情報を担当機器情報記憶手段 21 から知得し、当該知得した機種、機番およびバージョン情報と、異常状態を表すコード SC001 との組み合わせ、即ちソフトウェアバグ情報がバグ対策方針記憶手段 32 に登録されているか調査する (バグ情報パターンマッチ)。

【 0 0 3 7 】

この結果、ソフトウェアバグ情報が登録されており、かつ、発生頻度の条件を満たすことを確認した仲介機器 30 は、当該ソフトウェアバグ情報に関連付けられているバグ対策方針をバグ対策方針記憶手段 32 から読み出し、そこに指示されたバグ対策方針を以下のように実行する。

20

【 0 0 3 8 】

(動作 1) バグ対策方針として、「解析用デバッグログの採取機能を強化した強化版ファームウェア (以下、ログ強化版ファームウェアという) に更新する」ことが指定されていれば、仲介機器 30 は、当該ログ強化版ファームウェアの提供をセンターシステム 20 に要求する。

【 0 0 3 9 】

この要求を受けたセンターシステム 20 は、要求されたログ強化版ファームウェアをファームウェア記憶手段 23 から読み出し、要求元の仲介機器 30 に提供する (ファームウェアのダウンロード)。仲介機器 30 は、センターシステム 20 から提供されたログ強化版ファームウェアを記憶手段に保管し、次に当該保管したログ強化版ファームウェアを前記通報を出力した画像印刷機器 10 に送信すると共に、ファームウェアの更新を指示する。

30

【 0 0 4 0 】

この指示を受けた画像印刷機器 10 では、ファームウェア更新手段 12 が、仲介機器 30 から受信したログ強化版ファームウェアをファームウェア記憶手段 14 に更新し、画像印刷機器 10 を再起動 (リブート) する。再起動した画像印刷機器 10 は、ファームウェア記憶手段 14 からログ強化版ファームウェアを読み込んで動作を開始し、ファームウェアの更新が完了した旨を仲介機器 30 に通知する (ファームウェア更新結果通知)。この通知を受けた仲介機器 30 は、画像印刷機器 10 においてファームウェアの更新が完了した旨をセンターシステム 20 に通知する (ログ強化版ファームウェア更新結果通知)。この通知を受けたセンターシステム 20 は、仲介機器 30 に応答を返す。

40

【 0 0 4 1 】

(動作 2) 次に、仲介機器 30 は、今回の画像印刷機器 10 の通報に対応するバグ対策方針としてデバッグログの取得が指定されている場合、デバッグログの取得を画像印刷機器 10 に要求する。この際、バグ対策方針に規定された所定のプロトコルによりデバッグログが提供されるよう画像印刷機器 10 に求める。

【 0 0 4 2 】

ログ強化版ファームウェアを実行中の画像印刷機器 10 は、当該ファームウェアの実行に伴って揮発性のデバッグログをモジュール毎に標準出力やデバッグログ記憶手段 13 としての小メモリ領域に書き出すようになっている。

50



## 【 0 0 4 3 】

画像印刷機器 1 0 は、仲介機器 3 0 からデバッグログの取得を要求されると、標準出力やデバッグログ記憶手段 1 3 に格納したデバッグログを読み出し、要求されたプロトコルに従って仲介機器 3 0 に随時送信する。

## 【 0 0 4 4 】

仲介機器 3 0 は、画像印刷機器 1 0 から受けたデバッグログをデバッグログ記憶手段 3 3 に蓄積し、蓄積中のデバッグログが予め設定された転送単位に達すると、当該転送単位のデバッグログをデバッグログ記憶手段 3 3 から読み出して、センターシステム 2 0 に通知する。センターシステム 2 0 は、デバッグログを出力した画像印刷機器 1 0 のソフトウェアバグ情報についてバグ対策方針記憶手段 2 1 に登録されたデバッグログ通知先を確認し、当該デバッグログ通知先である設計・開発者端末 2 4 に、デバッグログを送信する。以上のデバッグログの取得動作は、バグ対策方針に規定されたデバッグログ取得期間に渡って実施される。

10

## 【 0 0 4 5 】

( 動作 3 ) 仲介機器 3 0 は、デバッグログの取得を開始してからバグ対策方針に規定されたデバッグログ取得期間の経過を検出すると、画像印刷機器 1 0 の機種機番に対応する最新のファームウェアの提供をセンターシステム 2 0 に求める。この要求を受けたセンターシステム 2 0 は、当該画像印刷機器 1 0 の機種機番に対応する最新のファームウェアをファームウェア記憶手段 2 3 から読み出し、要求元の仲介機器 3 0 に送信する(最新ファームウェアのダウンロード)。仲介機器 3 0 は、センターシステム 2 0 から提供された最新ファームウェアを記憶手段に保管し、次に当該保管した最新ファームウェアを画像印刷機器 1 0 に送信すると共に、ファームウェアの更新を指示する。

20

## 【 0 0 4 6 】

この指示を受けた画像印刷機器 1 0 では、ファームウェア更新手段 1 2 が、仲介機器 3 0 から受信した最新ファームウェアをファームウェア記憶手段 1 4 に更新し、画像印刷機器 1 0 を再起動(リブート)する。再起動した画像印刷機器 1 0 は、ファームウェア記憶手段 1 4 から最新のファームウェアを読み込んで動作を開始し、ファームウェアの更新が完了した旨を仲介機器 3 0 に通知する(ファームウェア更新結果通知)。この通知を受けた仲介機器 3 0 は、画像印刷機器 1 0 においてファームウェアの更新が完了した旨をセンターシステム 2 0 に通知する(最新ファームウェア更新結果通知)。この通知を受けたセンターシステム 2 0 は、仲介機器 3 0 に応答を返す。(ここにいう最新ファームウェアは、ログ強化版ファームウェアへ更新する前のファームウェアのバージョンと同一の場合も有り得る。それはつまり、ログ強化版ファームウェアへの更新を行う以前のファームウェアに書き戻すことを意味する。)

30

## 【 0 0 4 7 】

( 動作 4 ) 一方、上述したバグ情報パターンマッチの結果、ソフトウェアバグ情報に対応するバグ対策方針が、「最新のファームウェアに更新」することのみであれば、デバッグログ取得期間とは無関係に、上記(動作 3)を実行する。(ソフトウェアバグが既知かつ対応済みのものであれば、通常このバグ対策方針が採用される。)

## 【 0 0 4 8 】

( 動作 5 ) また、上述したバグ情報パターンマッチの結果、ソフトウェアバグ情報に対応するバグ対策方針が、「デバッグログの取得」のみであれば、上記(動作 2)のみを行う。(機器の通常動作用ファームウェアが簡易なデバッグログ採取機能を備えている場合がある。この場合で、対応するログ強化版ファームウェアが未だリリースされていない機種等の場合は、デバッグログの取得のみをバグ対策方針とすることが考えられる。)

40

## 【 0 0 4 9 】

( 動作 6 ) また、上述したバグ情報パターンマッチの結果、マッチするソフトウェアバグ情報が未だ登録されていない場合、仲介機器 3 0 は、マッチするソフトウェアバグ情報およびバグ対策方針が現時点でセンターシステム 2 0 に登録されているか否かを当該センターシステムに問い合わせる。この問い合わせを受けたセンターシステム 2 0 は、問い合

50

わせを受けたソフトウェアバグ情報およびバグ対策方針が現時点でバグ対策方針記憶手段 21 に登録されているか否かを確認し、登録されていた場合は、そのソフトウェアバグ情報およびバグ対策方針を読み出して仲介機器 30 に送信する。この送信を受けた仲介機器 30 は、センターシステム 20 から受信したソフトウェアバグ情報およびバグ対策方針をバグ対策方針記憶手段 32 に格納する。そして、当該バグ対策方針に従って、上記動作 1～5 等の該当する動作を実行する。

【0050】

(動作7：ファームウェア更新等の拒否設定)

【0051】

以上の動作のうち、ファームウェア更新を伴う動作またはデバッグログの取得を伴う動作について、画像印刷機器 10 において動作拒否の設定を行うことができる。画像印刷機器 10 の管理者は、画像印刷機器 10 が提供する管理者インタフェースを介し、動作拒否の設定を行うことができる。画像印刷機器 10 は、記憶手段に、ファームウェアの更新等の可否設定を記憶している。画像印刷機器 10 は、画像印刷機器 10 の操作パネルや外部の機器管理端末 40 に提供する管理者インタフェースを介し、ファームウェアの更新等の可否設定を受け付け、その設定変更に応じて記憶手段に記憶している設定を更新する。本実施形態において、管理者は、(1) 最新ファームウェアへの更新の禁止、(2) ログ強化版ファームウェアへの更新の禁止、(3) デバッグログ取得の禁止、のそれぞれをお客様のセキュリティポリシーに応じて設定できるようになっている。

【0052】

上記動作 1～6 において、画像印刷機器 10 は、禁止設定になっている動作を仲介機器 30 に要求された場合、当該要求に対応する動作は禁止されている旨を仲介機器 30 に通知する。

【0053】

この通知を受けた仲介機器 30 は、当該通知を出した画像印刷機器 10 の管理者の連絡先を担当機器情報記憶手段 31 から読み出し、当該管理者の連絡先に宛てて、設定変更を打診するメールを作成し送信する。この設定変更を打診するメールには、現在の禁止設定の状況と、ファームウェア更新またはデバッグログの取得が必要な理由と、当該禁止設定を変更するためのインタフェースにアクセスする URL や WebUI のリンクとを自動挿入する。

【0054】

その後、仲介機器 30 は、画像印刷機器 10 の禁止設定が解かれるのを監視する。画像印刷機器 10 は、ファームウェア更新又はデバッグログ取得の禁止設定が管理者によって解かれると、その旨を仲介機器 30 に通知する。この通知を受けた仲介機器 30 は、実行予定であったバグ対策方針の実行を再開し、前述の動作 1～6 のうちの所定の動作を実行する。

【0055】

(動作8：デバッグログを取得する他の方法)

【0056】

センターシステム 20 又は設計・開発者端末 24 から、画像印刷機器 10 を指定してデバッグログの取得を仲介機器 30 に要求し、この要求を受けた仲介機器 30 が、指定された画像印刷機器 10 のデバッグログをデバッグログ記憶手段 33 から読み出してセンターシステム 20 又は設計・開発者端末 24 に提供する構成としてもよい。

【0057】

さて、以上説明した本実施形態によれば以下の種々の効果を得ることができる。

(1) ソフトウェアバグの中には、画像印刷機器の使い方や使用環境の影響を受けて生じる現象もある。本実施形態によれば、画像印刷機器の固体ごとにバグ対策方針を自動的に判断し実行するので、ファームウェアの更新やデバッグログの取得が必要なお客様だけを特定して実行することができる。

(2) 本実施形態によれば、ファームウェアのリモート更新を自動的に行うことができ、また、デバッグログの取得もリモートにて自動的に行うことができ、かつ、お客様のサイ

10

20

30

40

50

トにおける実作業も伴わない。このため、従来の作業にくらべ、お客様機器のダウンタイムを最小にすることができ、また、デバッグログ収集のためにお客様サイトにノートPCを設置するなどの準備にかかる時間も不要となる。

(3) 本実施形態によれば、デバッグログをリモートにて自動的に取得することができ、かつ、デバッグログの取得が必要な異常状態が生じた適切なタイミングで速やかにデバッグログを取得し、転送単位ごとに随時適切な設計・開発者の元に届けることができる。このため、従来のようにお客様サイトに出向く必要がなく迅速にデバッグログを取得することができ、バグ対策に向けたログ解析を速やかに進めることができる。

(4) 本実施形態によれば、画像印刷機器の管理者がファームウェアの更新やデバッグログの取得を禁止に設定することが可能なので、上記バグの対応や解析の自動作業をお客様のセキュリティポリシーに従った形で行うことができる。 10

#### 【0058】

ここで、本発明は上記実施形態に限定されない。特に、本発明は、画像印刷機器に限らずファームウェアの実行により動作する種々の機器に採用することができる。

#### 【図面の簡単な説明】

#### 【0059】

【図1】本発明の一実施形態である機器遠隔監視システムのブロック構成図である。

【図2】図1のバグ対策方針記憶手段に格納されるソフトウェアバグ情報およびバグ対策方針の組み合わせの一例を示した図表である。

【図3】図1のバグ対策方針記憶手段に格納されるソフトウェアバグ情報およびバグ対策方針の組み合わせの一例を示した図表である。 20

【図4】図1に示す機器遠隔監視システムの動作を示すフローチャートである。

【図5】図1に示す機器遠隔監視システムの動作を示すフローチャートである。

【図6】図1に示す機器遠隔監視システムの動作を示すフローチャートである。

【図7】図1に示す機器遠隔監視システムの動作を示すフローチャートである。

#### 【符号の説明】

#### 【0060】

- |    |              |    |
|----|--------------|----|
| 10 | 画像印刷機器（機器）   |    |
| 11 | 以上検知通報手段     |    |
| 12 | ファームウェア更新手段  | 30 |
| 13 | デバッグログ記憶手段   |    |
| 14 | ファームウェア記憶手段  |    |
| 15 | 記憶手段         |    |
| 20 | センターシステム     |    |
| 21 | バグ対策方針記憶手段   |    |
| 22 | デバッグログ記憶手段   |    |
| 23 | ファームウェア記憶手段  |    |
| 24 | 設計・開発者端末     |    |
| 30 | 仲介機器（監視仲介装置） |    |
| 31 | 担当機器情報記憶手段   | 40 |
| 32 | バグ対策方針記憶手段   |    |
| 33 | デバッグログ記憶手段   |    |
| 40 | 機器管理者端末      |    |



