(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5543949号
(P5543949)
(45)発行日　平成26年7月9日(2014.7.9)　(24)登録日　平成26年5月16日(2014.5.16)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/00 156M

請求項の数 12 (全 22 頁)

(21)出願番号　特願2011-206151(P2011-206151)
(22)出願日　平成23年9月21日(2011.9.21)
(65)公開番号　特開2013-69053(P2013-69053A)
(43)公開日　平成25年4月18日(2013.4.18)
審査請求日　平成25年9月9日(2013.9.9)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目1番1号
(74)代理人　100117787
弁理士　勝沼　宏仁
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100103263
弁理士　川崎　康
(74)代理人　100107582
弁理士　関根　毅
(74)代理人　100118843
弁理士　赤岡　明
(74)代理人　100118876
弁理士　鈴木　順生

最終頁に続く

(54)【発明の名称】制御装置およびモニタプログラム

(57)【特許請求の範囲】
【請求項１】
管理サーバとメッセージ送受信を行う第1の機能と、前記管理サーバと同一または異なる外部装置に対し前記メッセージ送受信と異なるネットワークサービスを提供する第2の機能とを有するシステムソフトウェアを用いて、前記管理サーバと通信する制御装置であって、
前記システムソフトウェアからアクセス不能な、モニタプログラムを記憶するモニタプログラム記憶手段と、
前記モニタプログラムを読み出して実行する実行手段と、
前記モニタプログラムからアクセス可能で、前記システムソフトウェアからアクセス不能な第1の記憶手段と、
前記モニタプログラムおよび前記システムソフトウェアの両方からアクセス可能な第2の記憶手段と、
前記モニタプログラムおよび前記システムソフトウェアの両方からアクセス可能な第3の記憶手段と、
前記モニタプログラムから設定可能で、前記システムソフトウェアから設定不能なタイマと、
乱数を生成する乱数生成手段と、
前記モニタプログラムが実行されることにより、前記乱数生成手段により生成された乱数を第1の記憶手段に保存する第1の保存手段と、

前記モニタプログラムが実行されることにより前記第1の記憶手段内の乱数を前記管理サーバの公開鍵で暗号化して、前記管理サーバに送信するための要求メッセージを作成するメッセージ作成手段と、
前記モニタプログラムが実行されることにより前記要求メッセージを第2の記憶手段に保存する第2の保存手段と、
前記モニタプログラムが実行されることにより、所定の時間を指定して、前記タイマを起動するタイマ起動手段と、
前記モニタプログラムが実行されることにより前記システムソフトウェアを前記第1の機能と前記第2の機能を実行可能な第1の動作モードで起動するシステムソフトウェア起動手段と、
実行中のシステムソフトウェアから、前記モニタプログラムへの割り込みを受け付ける割り込み受け付け手段と、
前記割り込みにより前記モニタプログラムが実行されることにより、前記タイマを取り消すタイマ取り消し手段と、
前記割り込みにより前記モニタプログラムが実行されることにより、前記要求メッセージに対する前記管理サーバからの応答である通知メッセージを前記第3の記憶手段から読み出し、前記通知メッセージを前記公開鍵と、前記第1の記憶手段内の乱数により検証するメッセージ検証手段と、
前記タイマ取り消し手段による取り消し前に前記タイマが時間超過したとき、または前記メッセージ検証手段による検証が失敗したとき、前記モニタプログラムが実行されることにより、前記第1の機能を実行可能で前記第2の機能を実行不能な第2の動作モードで、前記システムソフトウェアを再起動する再起動手段と、
を備えた制御装置。
【請求項２】
前記モニタプログラムおよび前記システムソフトウェアの両方からアクセス可能な第4の記憶手段と、
前記モニタプログラムが実行されることにより、検証に成功した前記通知メッセージに、システムソフトウェアの更新版が前記管理サーバに存在するとの情報が含まれるとき、前記システムソフトウェアに対する前記更新版のダウンロード指示を第4の記憶手段に保存する手段と、
前記更新版のダウンロード指示が書き込まれた後、前記モニタプログラムが実行されることにより、前記システムソフトウェアに復帰する復帰手段と、
をさらに備え、
前記第1の機能は、前記更新版のソフトウェアをダウンロードする機能を含む
ことを特徴とする請求項1に記載の制御装置。
【請求項３】
前記割り込み受け付け手段は、前記復帰手段により復帰されたシステムソフトウェアから前記モニタプログラムへの割り込みを受け付け、
前記再起動手段は、前記割り込みにより前記モニタプログラムが実行されることにより、前記システムソフトウェアによりダウンロードされた更新版を、前記第1の動作モードで再起動する
ことを特徴とする請求項2に記載の制御装置。
【請求項４】
前記ダウンロードされたシステムソフトウェアには前記管理サーバの署名が付されており、
前記モニタプログラムが実行されることにより、前記公開鍵で前記署名の正当性を確認するシステムソフト検証手段をさらに備え、
前記再起動手段は、前記システムソフト検証手段で前記署名の正当性が確認された後、前記更新版のシステムソフトウェアを再起動する
ことを特徴とする請求項3に記載の制御装置。

【請求項５】
前記割り込み受け付け手段は、前記第2の動作モードで起動したシステムソフトウェアからの割り込みを受け付け、
前記メッセージ作成手段は、前記割り込みに応じて、前記要求メッセージを作成し、
前記第2の保存手段は、前記要求メッセージを前記第2の記憶手段に保存し、
前記タイマ起動手段は、前記要求メッセージの保存の後、前記タイマを起動し、
前記復帰手段は、前記タイマの起動後、前記システムソフトウェアに復帰し、
前記割り込み受け付け手段は、復帰されたシステムソフトウェアからの割り込みを受け付け、
前記タイマ取り消し手段は、前記復帰されたシステムソフトウェアからの割り込みに応じて、前記タイマを取り消し、
前記メッセージ検証手段は、前記タイマ取り消し手段による前記タイマの取り消し後、前記通知メッセージを検証し、
前記再起動手段は、前記通知メッセージの検証に成功したとき、前記システムソフトウェアを前記第1の動作モードで再起動する
ことを特徴とする請求項2ないし4のいずれか一項に記載の制御装置。
【請求項６】
前記通知メッセージは署名と乱数を含み、
前記メッセージ検証手段は、前記公開鍵で前記署名の正当性が確認され、かつ、前記通知メッセージに含まれる乱数が前記第1の記憶手段内の乱数に一致するとき、検証が成功したと判断する
ことを特徴とする請求項1ないし5のいずれか一項に記載の制御装置。
【請求項７】
管理サーバとメッセージ送受信を行う第1の機能と、前記管理サーバと同一または異なる外部装置に対し前記メッセージ送受信と異なるネットワークサービスを提供する第2の機能とを有するシステムソフトウェアを介して、前記管理サーバと通信するためのモニタプログラムであって、
乱数生成手段により生成された乱数を、システムソフトウェアからアクセス不能な第1の記憶手段に保存するステップと、
前記第1の記憶手段内の乱数を前記管理サーバの公開鍵で暗号化して、前記システムソフトウェアの実行により前記管理サーバに送信するための要求メッセージを作成するステップと、
前記要求メッセージを、前記システムソフトウェアからアクセス可能な第2の記憶手段に保存するステップと、
所定の時間を指定して、前記システムソフトウェアから設定不能なタイマを起動するステップと、
前記システムソフトウェアを前記第1の機能と前記第2の機能を実行可能な第1の動作モードで起動するステップと、
実行中のシステムソフトウェアから割り込みに応じて前記タイマを取り消すステップと、
前記要求メッセージに対する応答である通知メッセージを第3の記憶手段から読み出し、前記通知メッセージを、前記公開鍵と、前記第1の記憶手段内の乱数により検証するステップと、
前記タイマが取り消される前に前記タイマが時間超過したとき、または前記通知メッセージの検証が失敗したときに、前記第1の機能を実行可能で前記第2の機能を実行不能な第2の動作モードで、前記システムソフトウェアを再起動するステップと、
をコンピュータに実行させるためのモニタプログラム。
【請求項８】
検証に成功した前記通知メッセージに、前記システムソフトウェアの更新版が前記管理サーバに存在するとの情報が含まれるとき、前記更新版のダウンロード指示を、前記シス

テムソフトウェアによりアクセス可能な第4の記憶手段に書き込むステップと、
前記更新版のダウンロード指示が書き込まれた後、前記システムソフトウェアに復帰するステップと、
をさらに前記コンピュータに実行させるための請求項7に記載のモニタプログラム。
【請求項９】
前記復帰されたシステムソフトウェアからの割り込みを受け付けるステップと、
前記システムソフトウェアによりダウンロードされた更新版のシステムソフトウェアを、前記第1の動作モードで再起動するステップと、
をさらに前記コンピュータに実行させるための請求項8に記載のモニタプログラム。
【請求項１０】
前記ダウンロードされたシステムソフトウェアには前記管理サーバの署名が付されており、
前記公開鍵で前記署名の正当性を確認するステップと、をさらに前記コンピュータに実行させ、
前記署名の正当性が確認された後、前記更新版のシステムソフトウェアを再起動することを特徴とする請求項9に記載のモニタプログラム。
【請求項１１】
前記通知メッセージは署名と乱数を含み、
前記通知メッセージを検証するステップは、前記公開鍵で前記署名の正当性が確認され、かつ、前記通知メッセージに含まれる乱数が前記第1の記憶手段内の乱数に一致するとき、検証が成功したと判断する
ことを特徴とする請求項7ないし10のいずれか一項に記載のモニタプログラム。
【請求項１２】
前記第2の動作モードで起動したシステムソフトウェアからの割り込みを受け付けるステップと、
前記割り込みに応じて、前記要求メッセージを作成するステップと、
前記要求メッセージを前記第2の記憶手段に保存するステップと、
前記要求メッセージの保存の後、前記タイマを起動するステップと、
前記タイマの起動後、前記システムソフトウェアに復帰するステップと、
復帰されたシステムソフトウェアからの割り込みを受け付けるステップと、
前記復帰されたシステムソフトウェアからの割り込みに応じて、前記タイマを取り消すステップと、
前記タイマの取り消し後、前記通知メッセージを検証するステップと、
前記通知メッセージの検証に成功したとき、前記システムソフトウェアを前記第1の動作モードで再起動するステップと
をさらに前記コンピュータに実行させることを特徴とする請求項7ないし11のいずれか一項に記載のモニタプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、制御装置およびモニタプログラムに関する。
【背景技術】
【０００２】
ソフトウェア脆弱性は、今日のサイバー攻撃における主要なリスク要因となっている。
【０００３】
ソフトウェア脆弱性は一般のネットワークでも大きな問題だが、多数の均質な端末装置で構成されたネットワーク、たとえば同じ欠陥をもつ装置の割合が高い制御ネットワークでは、より一層顕著となるはずである。しかも、制御ネットワークの機能停止は、送配電や交通システム、生産設備などの社会インフラの機能が損なわれる点で、脅威はより深刻である。

【０００４】
制御ネットワークの安全性については、課金やプライバシ情報保護の観点で必要とされるデータ機密性、完全性に加えて、可用性、信頼性が強く求められる。前者（可用性）についてはSSL等のエンド・トゥー・エンドセキュリティ、後者（信頼性）については無線LANセキュリティや仮想専用線(VPN)などの、汎用ネットワークからの隔離技術の適用により実現される。
【０００５】
過去において、制御ネットワークは、物理的に隔離することで他の端末(特に不正端末)からのトラフィックの悪影響や攻撃を回避していた。配電網やセンサネットワークでは、公衆網の一部を仮想専用線(VPN)として制御ネットワークを構成することで、不正端末の接続を排除することも多くなっている。このような隔離に加えて、公衆網で行われているSSL等のエンド・トゥー・エンドのセキュリティを併用することが、制御ネットワークセキュリティの基本である。
【０００６】
これら隔離とエンド・トゥー・エンドセキュリティのいずれについても、それらを実現する暗号処理とアクセス制御の中核を担うのは、システムソフトウェア（部分的には暗号ハードウェア）である。
【０００７】
ソフトウェア脆弱性が大きな問題になるのは、システムソフトウェアが改ざん対象となることである。システムソフトウェアが改ざんされると、データ収集や制御手順などの応用上の機能に加えて、上記機密性に関わるセキュリティと隔離機能の両方の機能が損なわれてしまう。
【０００８】
制御ネットワーク内の端末がソフトウェア脆弱性によって侵入を受けた場合、上記隔離(例:無線LANセキュリティの認証処理)とエンド・トゥー・エンドセキュリティ(例:課金用アプリケーションの認証処理)のいずれについても、システムソフトウェアの暗号処理とアクセス制御の機能そのものが損なわれ、さらに秘密鍵の流出につながるおそれがある。
【先行技術文献】
【特許文献】
【０００９】
【特許文献１】特許第3233274号
【発明の概要】
【発明が解決しようとする課題】
【００１０】
ソフトウェア脆弱性の修正（予防と回復）には、システムソフトウェア更新の適用が必須である。ところが、通常想定されているシステムソフトウェアの更新は予防目的であり、システムソフトウェアが正常に機能していることが、前提とされている。ネットワークに大規模な侵入があった場合の対処として、ネットワーク管理者がネットワークの部分隔離などの操作を行い、最終的には各装置のソフトウェア更新をネットワーク経由でなく、装置の保守用インタフェースから人手によって行う。しかしながら、これらは多くの作業員を必要として、高コストである。
【課題を解決するための手段】
【００１１】
本実施形態の制御装置は、管理サーバとメッセージ送受信を行う第1の機能と、前記管理サーバと同一または異なる外部装置に対し前記メッセージ送受信と異なるネットワークサービスを提供する第2の機能とを有するシステムソフトウェアを用いて、前記管理サーバと通信する制御装置である。
【００１２】
前記制御装置は、モニタプログラム記憶手段と、実行手段と、第1の記憶手段と、第2の記憶手段と、タイマと、乱数生成手段と、第1の保存手段と、メッセージ作成手段と、第2

の保存手段と、タイマ起動手段と、システムソフトウェア起動手段と、受け付け手段と、タイマ取り消し手段と、メッセージ検証手段と、再起動手段とを備える。

【００１３】

前記モニタプログラム記憶手段は、モニタプログラムを記憶し、前記システムソフトウェアからアクセス不能である。

【００１４】

前記実行手段は、前記モニタプログラムを読み出して実行する。

【００１５】

前記第1の記憶手段は、前記モニタプログラムからアクセス可能で、前記システムソフトウェアからアクセス不能である。

【００１６】

前記第2の記憶手段は、前記モニタプログラムおよび前記システムソフトウェアの両方からアクセス可能である。

【００１７】

前記第3の記憶手段は、前記モニタプログラムおよび前記システムソフトウェアの両方からアクセス可能である。

【００１８】

前記タイマは、前記モニタプログラムから設定可能で、前記システムソフトウェアから設定不能である。

【００１９】

前記乱数生成手段は、乱数を生成する。

【００２０】

前記第1の保存手段は、前記モニタプログラムが実行されることにより、前記乱数生成手段により生成された乱数を第1の記憶手段に保存する

前記メッセージ作成手段は、前記モニタプログラムが実行されることにより前記第1の記憶手段内の乱数を前記管理サーバの公開鍵で暗号化して、前記管理サーバに送信するための要求メッセージを作成する。

【００２１】

前記第2の保存手段は、前記モニタプログラムが実行されることにより前記要求メッセージを第2の記憶手段に保存する。

【００２２】

前記タイマ起動手段は、前記モニタプログラムが実行されることにより、所定の時間を指定して、前記タイマを起動する。

【００２３】

前記システムソフトウェア起動手段は、前記モニタプログラムが実行されることにより前記システムソフトウェアを前記第1の機能と前記第2の機能を実行可能な第1の動作モードで起動する。

【００２４】

前記割り込み受け付け手段は、実行中のシステムソフトウェアから、前記モニタプログラムへの割り込みを受け付ける。

【００２５】

前記タイマ取り消し手段は、前記割り込みにより前記モニタプログラムが実行されることにより、前記タイマを取り消す。

【００２６】

前記メッセージ検証手段は、前記割り込みにより前記モニタプログラムが実行されることにより、前記要求メッセージに対する前記管理サーバからの応答である通知メッセージを前記第3記憶手段から読み出し、前記通知メッセージを前記公開鍵と、前記第1の記憶手段内の乱数により検証する。

【００２７】

前記再起動手段は、前記タイマ取り消し手段による取り消し前に前記タイマが時間超過

したとき、または前記メッセージ検証手段による検証が失敗したとき、前記モニタプログラムが実行されることにより、前記第1の機能を実行可能で前記第2の機能を実行不能な第2の動作モードで、前記システムソフトウェアを再起動する。

【図面の簡単な説明】

【００２８】

【図１】本実施形態に係るネットワーク構成を示す図。

【図２】本実施形態に係る端末装置のハードウェア構成を示す図。

【図３】本実施形態に係る端末装置が備えるプロセッサの内部構成を示す図。

【図４】本実施形態に係る不揮発性メモリおよびRAMのメモリマップを示す図。

【図５】本実施形態に係る端末装置の構成を示すブロック図。

【図６】本実施形態に係るROMモニタプログラムの動作のフロー図。

【図７】本実施形態に係る更新システムソフトウェアのダウンロードのシーケンス図。

【図８】本実施形態に係る端末装置の動作モードの状態遷移図。

【図９】本実施形態に係るマルウェア兆候検出のシーケンス図。

【図１０】本実施形態に係る不揮発性メモリのROMモニタ専用RW領域のデータ配置図。

【図１１】本実施形態に係る不揮発性メモリの共用RW領域のデータ配置図。

【発明を実施するための形態】

【００２９】

まず、本発明の実施形態の技術的背景について、述べる。

【００３０】

端末装置のマルウェア検出ソフトで、マルウェアを検出して管理サーバに報告し、管理サーバから更新ソフトをプッシュして、端末装置が受信する方法がある。ところが、報告と受信は、一般にシステムソフトウェア(OS（Operating System）とアプリケーションのセット)を経由して行われるため、OSがマルウェアに感染した状態では報告と受信、そして受信した更新ソフトの適用が、各段階で妨害される脅威がある。また、マルウェア検出はパターンマッチング処理のために高負荷であることに加え、最新のパターン情報を受信しなければ正しく機能しない。最新のパターン情報取得については、マルウェアがシステム時刻の不正操作と受信妨害を組み合わせて妨害する脅威が、想定される。

【００３１】

一方、独立の監視プロセッサで稼働しメインシステムから独立した通信機能を持つ監視システムが、上記マルウェア対策を担う構成もありうる。この場合、監視システムによるマルウェア検出、報告、更新ソフト受信と最新のパターン情報からなる一連の動作が、メインシステム上のマルウェアから妨害を受ける脅威は小さい。しかしながら、この構成は、専用プロセッサを必要とするため、高コストである。さらに、監視システムはメインシステムと独立の通信機能を持つが、この通信機能自体が脆弱性を含む可能性が生じる。通信機能はもっとも脆弱性の入り込みやすいものであり、監視システムの追加によるメインシステムの安全性向上という課題に対して、一種の鶏卵問題が生じてしまう。

【００３２】

さらに、もし脆弱性の修正が行われた更新ソフトが配布されていない状況、または配布はされていてもマルウェアによる妨害もしくはネットワーク/サーバ輻輳により当該更新ソフトの入手が困難な状況では、自装置に対するさらなるマルウェア感染や、自装置に感染したマルウェアによる通信妨害を防止する対策をとることが必要である。

【００３３】

本発明の実施形態では、OSがマルウェアに感染している可能性を前提として、通信機能をもたないROM(Read Only Memory)モニタプログラムが、サーバとの間で制限された情報の交換を行い、その状況に基づいて自律的にシステムソフトウェアの更新動作を行う手順を採用する。これにより、通信を仲介するOSにマルウェアが感染した場合に想定される妨害行為を、独立の監視プロセッサを必要とすることなくかつ低負荷（メモリデータのパターンマッチングのような高負荷の検出処理を必要としない）で検出して、脆弱性への対処を可能とするものである。

【００３４】
具体的に、本発明の実施形態は、単純なウォッチドッグタイマ回路と、不揮発性メモリと、アクセス制御機能とを持つシングルマイコンにおいて、大規模なマルウェア感染からの自律的回復を可能とする。特に、自律的回復における特徴として、特にマルウェア検出とソフトの更新有無の確認にサーバとの通信を利用することにより、更新通知の受信妨害のような迂回手段を含むマルウェアに対して、一定期間内にシステムソフトウェア更新版を適用することができる。本実施形態では、端末装置上でのマルウェア検出処理、たとえばメモリ上のパターンマッチング処理のような高負荷の処理を行う必要はない。
【００３５】
以下、図面を参照しながら、本発明の実施形態について、詳細に説明する。
【００３６】
図1に、本実施形態に係るネットワーク構成を示す。
【００３７】
本ネットワーク構成は、制御ネットワーク1と、管理サーバ2と、無線アクセスポイント10と、端末装置（制御装置）101-1～101-3 とを備える。制御ネットワーク1は、管理サーバ2および無線アクセスポイント10と有線接続されている。
【００３８】
端末装置101-1～101-3は、無線アクセスポイント10に無線リンクを介して、接続されている。制御ネットワーク1は、インターネットプロトコルを利用するネットワークである。上記の構成の他、図1には、本ネットワーク構成への攻撃を行う攻撃端末999が記載されている。
【００３９】
図2に、端末装置101-1～101-3のハードウェア構成を示す。
【００４０】
CPU（Central Processing Unit）200が、無線データリンク232を通じて、無線アンプ部 181に接続されている。無線アンプ部 181 は、外部入出力端子183を介して、アンテナ182に接続されている。CPU200は UART（Universal Asynchronous Receiver Transmitter）接続223を通じて、計測・制御部191 に接続されている。計測・制御部191は外部入出力端子 192 に接続されている。計測・制御部191は、たとえば外部入出力端子 192を介して電力メータと通信して、機器の消費電力を計測し、CPU200に渡す。CPU200は、そのデバッグインタフェース（図3参照）において、外部保守インタフェース 111に接続されている。
【００４１】
図3に、CPU 200 の内部構成を示す。
【００４２】
命令実行ユニット（実行手段）201 は、メモリ保護ユニット202を経由して、内部バス208に接続されている。
【００４３】
メモリ保護ユニット202は、命令実行ユニット201に投入される命令が、不揮発性メモリ203内のROMモニタプログラム301 (図4参照)に割り当てられたものかどうかを表す信号を出力する。この信号は、信号線 211を介して、命令実行ユニット201に入力される。
【００４４】
不揮発性メモリ（フラッシュメモリ）203 と RAM (Random Access Memory)204 が、内部バス 208 に接続されている。
【００４５】
ウォッチドッグタイマ (WDT: Watch Dog Timer) 210 と制御レジスタ 209 も内部バス208に接続されている。制御レジスタ 209の一の出力であるリセット信号、およびWDT 210の出力（リセット信号）は、ワイヤードORでリセット信号線 212 を介して、命令実行ユニット201に入力される。また、制御レジスタ 209の他の出力であるNMI(Non Maskerable Interrupt：マスク不能割り込み)信号は、NMI信号線213を介して、命令実行ユニット201に入力される。

【００４６】
暗号アクセラレータ 205、および乱数発生器(RNG) 206 も、同様に内部バス208に接続されている。無線データリンク 218および UART（Universal Asynchronous Receiver Transmitter）207 も、内部バス208に接続される。
【００４７】
デバッグ部 220 は、命令実行ユニット 201 に直接接続されるとともに、デバッグポート 231を介して、外部（図2の保守用インタフェース111）に接続されている。
【００４８】
図4に、不揮発性メモリ203およびRAM204のメモリマップを示す。
【００４９】
不揮発性メモリ203は、大きく、ROMモニタ専用領域11と、システムプログラム領域12とを備える。
【００５０】
ROMモニタ専用領域11は、ROMモニタプログラム領域（モニタプログラム記憶手段）301、管理サーバ公開鍵領域302およびROMモニタ専用RW領域303を有する。なお本実施形態では、メモリの領域と、当該領域に格納されたデータに、同じ参照符号を付することがある。たとえばROMモニタプログラムと、ROMモニタプログラム領域に、同じ301を付している。
【００５１】
ROMモニタプログラム（以降、略してROMモニタと称することもある） 301 および管理サーバ公開鍵 302 は、不揮発性メモリの書換え禁止領域に配置される。
【００５２】
ROMモニタ専用RW領域 303 は、不揮発性メモリの書換え可能領域に配置される。ただし、ROMモニタ専用RW領域303は、ROMモニタ301 のみからアクセス可能であり、ROMモニタ301以外のプログラムからは、後述のアクセス制御機能により、アクセスが禁止される。
【００５３】
システムプログラム領域12には、共有RW領域 304と、それ以外の領域とが含まれる。
【００５４】
共有RW領域304は、ROMモニタ301からも、システムプログラム（システムソフトウェアあるいはファームウェアとも称される）からもアクセス可能な領域である。
【００５５】
共有RW領域以外の領域として、領域305,306には、ファームウェア（FW）#1およびファームウェア#1に対する署名が格納されている。領域307,308には、ファームウェア#2およびファームウェア#2に対する署名が格納されている。システムソフトウェアは、管理サーバとメッセージ送受信およびシステムソフトウェアのダウンロードを含む第1の機能と、当該管理サーバまたは他の外部サーバに所定のネットワークサービスを提供する第2の機能とを有する。
【００５６】
RAM204は、各種処理の作業領域である作業用RAM領域13を備える。
【００５７】
[アクセス制御]
不揮発メモリ203のROMモニタ専用RW領域 303へのアクセス、およびウォッチドッグタイマ210の設定（タイマ起動、タイマ取り消し）は、ROMモニタ301の実行に限定される。
【００５８】
この実現手段としては、実行のためにメモリ（不揮発性メモリおよびRAM）から取得した命令毎に、アドレス範囲がROMモニタ301の格納領域に該当するのか、それ以外なのかを示すタグ情報をメモリ保護ユニット202に保持しておくことで可能である。このほか、キャッシュメモリを持つ構成においては同様の機能を得る手段が多数あるが、それらのいずれを用いてもよい。このようなアクセス制御の実装は、プロセッサを複数持つ監視プロセッサの構成と比較して、低コストで実現可能である。

【００５９】
また、ROMモニタ301は、リセットおよびマスク不能割り込み（NMI）の2つのエントリポイントのみをもつ。ROMモニタ301は、これら2つのエントリポイント以外のアドレスからの実行はできない。すなわちROMモニタ301は、リセット時またはマスク不能割り込み時にのみ、実行される。
【００６０】
前者のリセットのエントリポイントに関し、ROMモニタ301以外のアドレスで実行されるシステムソフトウェアが、通常モードの実行状態からROMモニタを実行しようとした場合、ROMモニタ301内のアドレスへのジャンプ命令を発行する。このジャンプ命令が発行されると、メモリ保護ユニット 202からリセット信号が発生する。発生したリセット信号は、信号線211を介して、命令実行ユニット201に入力される。
【００６１】
また後者のNMIのエントリポイントに関し、通常モードの実行状態にあるプログラム（システムソフトウェア）から、制御レジスタ209内のNMI発生レジスタに書き込みを行うと、NMI信号が発生する。発生したNMI信号は、信号線213を介して、命令実行ユニット201に入力される。これにより、NMI開始アドレスから、ROMモニタ301が実行される。
【００６２】
ROMモニタ301の実行に関するこれらの機能は、既存プロセッサにおけるスーババイザビットの管理と同様であるが、本実施形態においては、ROMモニタモードとスーパバイザモードを合わせ持つことができる。
【００６３】
ここで、制御レジスタ209は、NMI信号とリセット信号のいずれも発生させる能力を有する。ただし、メモリ保護ユニット202のアクセス制御により、システムソフトウェアのモードで利用できるのはNMI信号の発行に限定され、リセット信号を発生させることはできない。リセット信号の発生は、ROMモニタ301に限定される。
【００６４】
以下、図5、図6および図7を参照しながら、正常運用において管理サーバ2から端末装置に更新ソフトウェアをダウンロードし、再起動により端末装置のシステムソフトウェアを更新する手順を説明する。
【００６５】
図5は、端末装置の機能構成を示す機能ブロック図である。
【００６６】
図6は、端末装置のROMモニタ動作概略フローチャートである。
【００６７】
図7は、端末装置の動作の更新ソフトダウンロードにおける概略シーケンス図である。
【００６８】
電源投入またはリセット信号入力により、CPU200は、初期状態からROMモニタ301を実行する(リセット受付部 501、S2021)。
【００６９】
はじめに、ROMモニタ301は、WDT 210および制御レジスタ209の状態を取得して、前回の再起動原因が、(1)WDT210のタイムアウトによるものか、(2)ROMモニタ301による制御レジスタ209の操作によるものか、(3)電源断によるものかを特定し、特定した原因を、ROMモニタ専用RW領域303に書き込む(タイムアウト判定部502, S2022)。具体的に、ROMモニタ専用RW領域の構成を表す図10に示すように、現在再起動状態領域 303-11(図10参照) に、当該特定した原因を、書き込む。
【００７０】
次に、リセットによる初期状態実行では、ROMモニタ301は、ROMモニタ専用RW領域303に格納された次回ブート指定情報（図10参照）に含まれる次回ブート領域番号 303-14 を読み出す。そして、ROMモニタ301は、次回ブート領域番号 303-14で指定された領域に格納されたシステムソフトウェアを、検証用公開鍵（管理サーバ公開鍵）302 で検証する。

なお領域番号と、格納先アドレスとの対応を表すテーブルが、ROMモニタ専用FW領域内に別途設けられているとする。領域番号ではなく、格納先アドレスを直接、格納してもよく、この場合、テーブルは不要である。検証により、サーバ署名が正しく付与されていることと、システムソフトウェアヘッダ X に格納された当該システムソフトウェアのバージョン番号が、次回ブート指定情報（図10参照）に含まれる次回ブート時バージョン番号・モード303-12（図10参照）のバージョン番号に一致することとを、確認する(システムソフト検証部503, S2023)。

【００７１】

一致確認に失敗した場合、次候補として別の格納場所に格納されたシステムソフトウェアに対する検証を実行する。たとえば図4のファームウェア#1領域305に格納されたシステムソフトウェアのバージョン番号の不一致が検出された場合、次候補としてファームウェア#2領域307に格納されたシステムソフトウェア（ひとつ前にダウンロードしたシステムソフトウェア）の検証を実行する。そして、ROMモニタ301は、次回ブートバージョン番号・モード領域303-12に、次候補のバージョン番号と縮退動作モード（第2の動作モード）を指定する情報を書き込み、共用RW領域の起動・再開モード指定領域304-1に「縮退」を書き込む（起動モード修正部504、S2024）。

【００７２】

縮退動作モードは、システムソフトウェアの機能に対して稼働させる機能（サービス）を限定するモードのことであり、上述した第1および第2の機能のうち、第1の機能（メッセージの送受信およびシステムソフトウェアのダウンロード）のみを稼働させる（詳細は後述する）。第1の機能、および第2の機能（ネットワークサービス機能）のいずれも稼働するモードは、本実施形態では、通常動作モード（第1の動作モード）に相当する。

【００７３】

ROMモニタ301が、管理サーバ2から更新システムソフトの有無および脆弱性情報を入手するための問い合わせ用ROMメッセージ（要求メッセージ）を作成し、作成したROMメッセージを、共有RW領域304の要求メッセージ領域304-6（第2の記憶手段）に書き込むとともに、WDT210を設定する(送信メッセージ準備部505, S2025～S2027、図7のS1001)。送信メッセージ準備部505の詳細構成は、520のブロックによって表される。送信メッセージ準備部505は、乱数生成部521、送信メッセージ作成部523、送信メッセージ保存部（第1の保存手段、第2の保存手段）522、WDT設定部（タイマ起動手段、タイマ取り消し手段）524を含む。

【００７４】

ROMメッセージの作成手順は、次のとおりである。

【００７５】

はじめに、ランダムチャレンジとなる乱数値を、乱数発生器206を用いて生成し、生成した乱数値を、ROMモニタ専用RW領域303内の乱数値領域303-1（第1の記憶手段、図10参照）に保存する(乱数生成部521,送信メッセージ保存部522,S2025)。

【００７６】

次にブート予定のFW（システムソフトウェア）のバージョン番号とブートモードに、乱数値を連接（コンカチネイト）して連接データを生成する。そして、連接データのハッシュ値を計算し、ハッシュ値を含む全体をサーバ公開鍵302で暗号化する。これらの情報が大きく公開鍵暗号の1ブロックに格納できない場合は共通鍵を組み合わせたハイブリッド暗号を使用してもよい。暗号化した結果を、共用RW領域304の領域304-6（第2の記憶手段）に保存する(送信メッセージ作成部523,送信メッセージ保存部522、S2026)。

【００７７】

WDT 210に、管理サーバ2からのメッセージが返される所定の期待時間 T1 を設定する(WDT設定部524, S2027)。WDT 210は、ROMモニタ301以外のソフトウェア（プログラム）からは解除できない。もし所定の期待時間T1が経過してもWDT210が解除されない場合、WDT210はリセット信号を発生させる。これにより端末装置は再起動され、ROMモニタ301に制御が移る。これは、マルウェアによるシステム乗っ取りからの回復手段を提供する。なお、WD

T210がオーバフローしたこと（すなわち所定の期待時間T1が経過してもWDT210が解除されなかったこと）は、ROMモニタ301がWDT210内の所定のレジスタを読み出すことにより、判定できる。

【００７８】

ここまでの手順を行い、ROMモニタ301は、次回ブート領域番号303-14（図10参照）により指定された領域（もしくはアドレス）へのジャンプ命令を発行する(システムソフトウェア起動部506, S2028)。ジャンプ命令の発行により、システムソフトウェアが実行される。以後実行される命令は、ROMモニタ専用領域11とWDT210へのアクセスが禁止される。これによりROMモニタ301の内部情報と、WDT210による監視が、マルウェアによる不正操作から守られる。

【００７９】

[システムソフトウェアの処理]

システムソフトウェアは、共用RW領域 304 の起動・再開モード 304-1（図11参照）を参照する。ここでは起動・再開モードは「通常」の指定があり、そのため端末装置は通常のネットワークサービスを開始する。すなわち、端末装置のシステムソフトウェアは第1の動作モードで動作する。ネットワークサービスである所定のサービスの一例として、計測・制御部191で計測した消費電力データを管理サーバまたは他の装置に送信するサービスがある。

【００８０】

並行してシステムソフトウェアは、ROMモニタ301が共有RW領域304に書き込んだ要求メッセージ （ROMメッセージ）304-6 を、管理サーバ2に送信する（図7のS1002）。送信方法はUDPメッセージに格納してもよいし、要求メッセージをファイルとして、ファイル転送してもよい。ネットワーク輻輳のような状態を考慮した場合を想定して、送信が無用な輻輳を起こさないよう適切な送信レート制御を行い、かつネットワーク状態が不安定な場合でもメッセージ到達性を確保するために、接続手順は単純なものであることが望ましい。健全な状態のシステムソフトウェアは、要求メッセージ（ROMメッセージ）の送信、および管理サーバ2からの通知メッセージの受信に、最善の努力をするものとする。

【００８１】

[メッセージ形式]

ここで、ROMモニタ301と管理サーバ2との間で交換されるメッセージ形式について、詳細に説明する。

【００８２】

はじめに、以下の説明で用いる暗号処理及び定数を説明する。

・Kp: 管理サーバ公開鍵
・Ks: 管理サーバ秘密鍵
・Z = EP_Kp[A]: 公開鍵 Kpによるデータの非対称暗号化(RSAなど)。出力はZ。
・I= V_Kp[Msg, Sig] メッセージ Msg と署名 Sig に対する公開鍵 Kpによる署名検証。PSS等の所定のパディングを用いることが望ましい。Iは検証結果(1は検証成功、0は検証失敗)。
・Sig = S_Ks[Msg]: Msgに対する秘密鍵Ksによる署名生成。
・Y=E_S[X] : 秘密鍵Sによる Xの共通鍵ブロック暗号化。Yを計算する。S,X,Y全てのデータサイズはブロック長に一致。以下の例ではAES128を例にとりブロック長が128ビット(16バイト)として説明するが、そのほかの暗号アルゴリズムを用いても、差し支えない。
・Y=H[X] : Xに対するハッシュ計算。Yが出力。
・X=D_S[Y]: 秘密鍵Sによる Xの共通鍵ブロック復号。
・Rnd, Rnd(n): 端末装置内部で発生させた乱数。Rnd(n)の場合、 n は回数を表す。
・#CVer: 端末装置が現在使用しているシステムウェアのバージョン番号
・#NVer: 管理サーバが配布しているシステムソフトウェアの最新バージョン番号
・Act(#CVer): #CVer を使用している端末装置がとるべき動作
・Mode: 端末装置が現在使用しているシステムウェアのモード

【００８３】
ROMモニタ301による要求メッセージ(ROMメッセージ)RMsgは、以下の形式をとる。
RMsg = Ep_Kp[Rnd||#CVer||Mode||H[Rnd]] ・・・式1
【００８４】
RMsg は、端末装置の共有RW領域304の領域304-6に書き込まれ、システムソフトウェアによって管理サーバ2に送信される。
【００８５】
管理サーバ2は、ROMメッセージRMsg を秘密鍵Ksにより復号して、 Rnd||H[Rnd]を取り出す。そして 、Rndと、ハッシュ関数によりハッシュ値を計算し、当該ハッシュ値と、H[Rnd]との合致を確認する。合致を確認したら、管理サーバ2は、メッセージ本体
Ver = #NVer||Act(#CVer)
を作成する。メッセージ本体に、さらに、現在ソフトウェアバージョンに対する脆弱性情報や時間パラメータ等の情報を、連接してもよい。
【００８６】
このメッセージ本体に基づき、管理サーバ2は、以下の式2および式3により通知メッセージ（SMsg）を作成し、端末装置に送信する。
Msg = E_S[Rnd[Ver||Hash[Ver]]] ・・・式2
SMsg = Msg||S_Ks[Msg] ・・・式3
【００８７】
マスク不能割り込み（NMI）によって呼び出されたROMモニタ301（後述するようにシステムソフトウェアが制御レジスタ209に書き込みを行うことでNMIを発生させてROMモニタ301に制御を移す）は、システムソフトウェアが共用RW領域304の領域304-7に書き込んだ通知メッセージ（SMsg）を読み出し、サーバ公開鍵Kpによって完全性を検証する。
【００８８】
次に、保存していた乱数（Rnd）により、通知メッセージ（Msg）を復号し、メッセージ本体（Ver）に対するハッシュ値を計算する。そして、当該ハッシュ値と、通知メッセージ（Msg）に含まれるハッシュ値（Hash[Ver]）との一致を確認する。なお秘密鍵Sは、端末装置と管理サーバとの間で、事前に共有されている。
【００８９】
上述した手順では、以下の点で、ネットワーク上からの攻撃、およびマルウェアに感染したシステムソフトウェアによる攻撃から端末装置を守っている。
・最新バージョン番号 #NVer を含むサーバからのメッセージ（SMsg）が、乱数（Rnd）を含む先のROMメッセージ（RMsg）に対する応答であること。すなわち、当該メッセージ（SMsg）が、過去に管理サーバから送信された通知メッセージのリプレイでないこと
・端末装置がとるべき動作が、秘匿されていること
【００９０】
端末がとるべき動作は、不正端末や感染端末等の攻撃端末999（図1参照）による攻撃ターゲット絞り込みに使われるおそれがあり、秘匿が必要なケースがある。
【００９１】
ただし、端末装置群が属する制御ネットワークが、ほとんど均質な端末装置からなるネットワークの場合は、脆弱性情報がほぼすべての端末で一致するため、秘匿があまり意味をなさない場合もありうる。その場合は、上記管理サーバ2からの通知メッセージの構成を簡略化し、下記式4で定義されるように、乱数値と最新バージョン番号のみを含む形式を採用し、秘密鍵Sによる暗号化（上記式2参照）をしなくてもよい。
Msg' = Rnd||#NVer ・・・式4
SMsg = Msg'||S_Ks[Msg'] ・・・式5
【００９２】
管理サーバ2からの最新バージョン番号の通知は、リプレイ攻撃の排除が重要である。リプレイ攻撃は秘匿チャネルを使うことによっても防止できるが、一般に秘匿チャネルの確立に複数回の通信が必要である。脆弱性をさけるため、自身の通信を持たないROMモニ

タは、起動時およびサービス受付時にしか通信処理ができないため、秘匿チャネルの確立に時間を要してしまう。

【００９３】

この点、本実施形態では、システムソフトウェアの更新で最も重要な管理サーバ2からの最新バージョン（#NVer）の通知が、端末装置で生成したランダムチャレンジ（乱数値）をサーバ秘密鍵で暗号化して行われる。管理サーバメッセージの署名を付与されて返送される最新バージョン通知とランダムチャレンジが、端末装置が保持するものと一致することを確認する手段により、ランダムチャレンジを知らない攻撃者によるリプレイの脅威を排除できる。

【００９４】

システムソフトウェアにマルウェアが感染した状態でも、ランダムチャレンジ（乱数値）を格納する、ROMモニタ専用RW領域 303の領域303-1 へのアクセスが、システムソフトウェアに対し禁止されていれば、リプレイ攻撃を排除できる。

【００９５】

［管理サーバ側処理］

管理サーバ 2 は、要求メッセージ（ROMメッセージ）304-6 を受信すると、上述のとおり、サーバ公開鍵に対応する秘密鍵により要求メッセージを復号し、乱数を用いてハッシュ値の検証を行う。ハッシュ値が正しい場合、以下の付加情報を相互連接し、さらに署名を付与して、通知メッセージを生成する（詳細は前述したとおりである）。そして、通知メッセージを、送信元のシステムソフトウェア（端末装置）に返送する。

（付加情報）

- 最新システムソフトウェアバージョン番号
- 現在ソフトウェアバージョンに対する脆弱性情報
- 推奨動作モードおよび時間パラメータ

【００９６】

管理サーバ2からの通知メッセージを受信したシステムソフトウェアは（S1003）、共用RW領域304の領域304-7（第3の記憶手段）に、当該通知メッセージを書き込む。そして、システムソフトウェアは、制御レジスタ209に書込みを行うことで、マスク不能割り込み(NMI) を発生させて、ROMモニタ301に制御を移す（S1004)。

【００９７】

システムソフトウェアからマスク不能割り込み (NMI)によって、ROMモニタ301の実行が再開される(図5のNMI受付部（割り込み受け付け手段）510、図6のS2001)。ROMモニタ301は、WDT210をクリアして、共用RW領域304の領域304-7に保存された通知メッセージの署名を、管理サーバ公開鍵 302 により検証する(受信メッセージ検証部511, S2002)。検証に成功した場合、ROMモニタ301は、通知メッセージの内容に基づいて、以下の処理を行う。

【００９８】

すなわち、通知された最新システムソフトウェアのバージョンと、現在実行中のシステムソフトバージョンを比較する。

【００９９】

両者に相違があれば、共有RW領域304の領域304-3に、最新システムソフトバージョン番号をパラメータとして書き込み(動作モード決定部512, S2003)、さらに起動・再開モードとして「ソフトウェアダウンロード」、すなわち更新版のダウンロード指示を、領域304-1（第4の記憶手段）に、書き込む（図7のS1005）。

【０１００】

一方、両者が一致する場合は、起動・再開モード 304-1を、「通常」のままとする。

【０１０１】

続いてROMモニタ301は、送信メッセージの準備とWDT設定を行う（送信メッセージ準備部513, S2005～S2007)。送信メッセージ準備部513の構成は、送信メッセージ準備部505と同じであり、520のブロックにその詳細が示される。そして、ROMモニタ301は、マスク不能割り込み (NMI)からシステムソフトウェアへ復帰する(復帰処理部514, S2008)。

【０１０２】
システムソフトウェアは、再開モード304-1が「ソフトウェアダウンロード」となっていることを確認し、割り込み終了処理を行い、自身の実行を再開する。
【０１０３】
システムソフトウェアは、共用RW領域304における起動・再開モード領域304-1を確認し、起動・再開モードが「ソフトウェアダウンロード」であるため、通常サービスを継続しながら、管理サーバもしくは他の装置（更新ソフトウェアをダウンロード済みの他の端末装置）から、更新ソフトウェアをダウンロードする（図7のS1006）。システムソフトウェアは、ダウンロードした更新ソフトウェアを、システムプログラム領域12（図4参照）の空き領域に書き込む。またバージョン番号および格納領域番号（あるいはアドレス）等を共用RW領域304-2に書き込む。ダウンロードが完了すると、共用RW領域304の領域304-5に、ROMモニタ再開パラメータとして、「ダウンロード完了」を書き込む。その後、再びマスク不能割り込み（NMI)を発行し（S1007）、ROMモニタ301に制御を移す（S2001）。
【０１０４】
ROMモニタ301は、ROMモニタ再開パラメータ304-5 の「ダウンロード完了」を確認すると、更新ソフトウェアの完全性を、管理サーバ公開鍵302の署名検証により確認する（S2002）。さらに、更新ソフトウェアのバージョン番号が、管理サーバ2からの通知メッセージに含まれていた最新バージョンに一致することを確認する。確認ができた場合、ROMモニタ301は、共用RW領域304における次回起動・再開モード 304-1 を「通常」に設定する(動作モード決定部512,S2003)。また、上記更新ソフトウェアに対応して、図10における次回ブート指定情報（303-12、303-13、303-14）を、共用RW領域の予備領域304-2に格納された情報（バージョン番号、格納領域等）に基づき、更新する。
【０１０５】
この後、ROMモニタ301は、制御レジスタ209を用いてリセット信号を発生させることにより、再起動処理を行う(再起動部517、S2010、S2021、S1008)。すなわち、CPUリセットにより、ROMモニタ301もシステムソフトウェアも終了して、ROMモニタ301が新たに起動される（必要に応じてRAMも全部消去される）。
【０１０６】
続くROMモニタ301による再起動後の処理は、上述と同じである。ダウンロードが正常に完了している場合、リブート処理でもシステムソフトウェアの検証が成功する。ROMモニタ301は上述の一連の処理を行い、更新されたシステムソフトウェアへと制御を移し、システムソフトウェアが起動する。
【０１０７】
さて、上記通常時のソフトウェア更新シーケンスは、端末装置内で動作中のシステムソフトウェア、および制御ネットワーク1がともに健全な状態の動作である。
【０１０８】
以下では、制御ネットワーク1にマルウェアが侵入し、端末装置の一部もしくは大多数の端末装置がマルウェアに感染した状態から、端末装置のROMモニタが自律的に更新ソフトウェアの取得および機能縮退の動作を組み合わせて行うことにより、マルウェアがネットワーク状態に与える悪影響を限定し、更新ソフトウェアの早期取得を可能にする例を説明する。
【０１０９】
［マルウェアによる制御権不正取得、ソフトウェア更新通知の配布妨害］
マルウェアに対する根本的な対策は、マルウェアの侵入源となる脆弱性を更新したシステムソフトウェアを、全ての端末装置に配布し、実行することである。ところが、マルウェアに端末装置の制御権を取得されてしまった状態では、管理サーバ2が更新版のシステムソフトウェアを配布しても、マルウェアに乗っ取られた端末装置はそれを受信できなくなる脅威が想定される。
【０１１０】
本実施形態の端末装置では、管理サーバ2からの通知メッセージの受信と、WDT210のタ

イムアウトとを組み合わせることで、システムソフトウェアがマルウェアに乗っ取られた状態から強制的にROMモニタ301に制御を戻し、更新ソフトウェアのダウンロードを強制する。

【０１１１】

以下、図9および図8を用いて、本例の詳細について説明する。

【０１１２】

図9は、マルウェア検出のシーケンス図である。図8は、ROMモニタ301が決定するシステムソフト起動モードの状態遷移図である。

【０１１３】

図9において、ROMモニタ301は、起動時に上述のとおりWDT210をセットし(S1100)、 要求メッセージを共有RW領域（共有メモリ）304の領域304-6（第2の記憶領域）に書込み、システムソフトウェアに制御を移す(S1101)。

【０１１４】

システムソフトウェアは、管理サーバ2に要求メッセージを送信し(S1102)、管理サーバ2は、通知メッセージを送信する(S1104)。ところが、通知メッセージを端末装置が受ける前に、不正端末 999 (図1参照)により、システムソフトウェアの脆弱性を攻撃するマルウェアが送信され(S1103)、システムソフトウェアがこのマルウェアに感染したとする。

【０１１５】

マルウェアは管理サーバ2に感染が発覚しないよう、更新ソフトウェアの適用を指示する通知メッセージを正しく受信し、更新ソフトウェアのダウンロードも行う(図示せず)。しかしながら、マルウェアは、脆弱性が修正された更新ソフトウェアのデータは消去してしまい、再起動による更新ソフトウェアの適用も行わない(図示せず)。このような状況になってしまった場合、管理サーバ2は直接には何の操作もできず、兆候を検出することすらできない。

【０１１６】

本実施形態では、通知メッセージを受信したシステムソフトウェアがWDT210で設定した期間T1内にROMモニタ301に制御を戻さない場合、強制的にROMモニタ301に制御が移行する(S1105)。タイムアウト発生が検出された場合(S1106)、または、ROMモニタ301のチャレンジ乱数に対する管理サーバ2の正しい通知メッセージが共有RW領域（共有メモリ）304の領域304-7に書かれていない場合といったような、マルウェアの侵入の兆候が検出された場合は（図8の604）、システムソフトウェアの再起動を行う(図5の再起動部517, 図6のS2010参照)。すなわちCPUリセットにより、いったんROMモニタおよびシステムソフトウェアを終了し、ROMモニタを起動し、ROMモニタからシステムソフトウェアを、前述した手順にしたがって、新たに起動する。

【０１１７】

さらに、侵入の兆候が連続的に検出された場合は、システムソフトウェアの起動モードを縮退動作モード(図8の605、図9のS1107)として、システムソフトウェアの機能と接続先を、管理サーバ2からのメッセージ送受信に限る最低限の機能に限定して、マルウェア感染を回避した状態で、管理サーバ2との通信回復を試みる。具体的に、最新バージョンのシステムソフトウェアがマルウェアに感染して異常動作をしたが、不揮発性メモリ上の当該最新バージョンのシステムソフトウェアのイメージが書き換えられていない（検証成功）の場合は、最新バージョンのシステムソフトウェアを縮退動作モード（第2の動作モード）で実行する。最新バージョンのシステムソフトウェアがマルウェアに感染して、不揮発性メモリ上の当該システムソフトウェアのイメージも改ざんされた場合（検証失敗）の場合は、ひとつ前のバージョンのシステムソフトウェアの縮退動作モード（第2の動作モード）で実行する。

【０１１８】

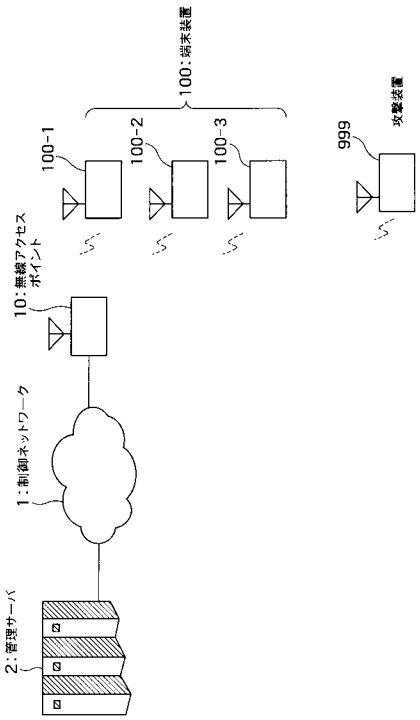
管理サーバ2から一定時間以内に通知メッセージが取得できない場合や、通知メッセージに誤りがある場合には、以下の原因が考えられる。

(1) システムソフトウェアのマルウェア感染による、要求メッセージおよび通知メッセー

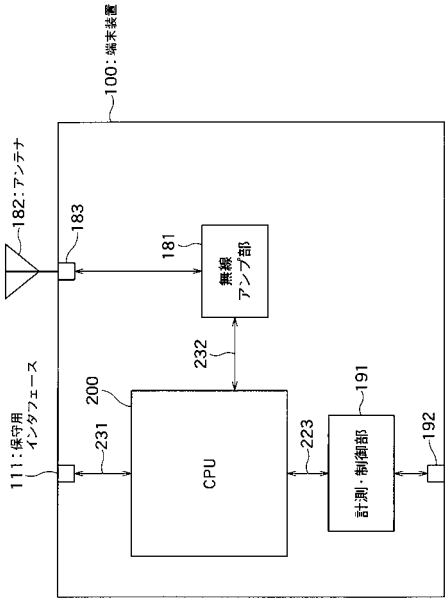
ジの送受信処理放棄
(2) ネットワーク上またはシステムソフトウェアのマルウェア感染による通知メッセージの偽造
(3) システムソフトウェアの不具合または過負荷による応答遅れ
(4) ネットワークまたは管理サーバの輻輳
【０１１９】
(1) および(2) の場合は、マルウェアの感染から回復し、再感染を防止するためにシステムソフトウェアの更新と再起動が必要である。システムソフトウェアの更新版がダウンロードできていない場合は、現在のシステムソフトウェアを縮退運転で動作させて（図8の603、605）、更新版を取得し、再起動する必要がある。更新版が準備できていない場合であっても、マルウェアの自装置への感染と他装置への感染拡大を防止する観点から、更新版のシステムソフトウェアが準備できるまでは縮退運転を続け、その間は定期的に更新版の提供状況に関する問い合わせを続け、これまでに説明したROMモニタ301はそれにかなった動作を行う。ネットワーク上のマルウェアが通知メッセージを偽造した場合は、自装置はマルウェアに感染していないはずだが、ROMモニタ301単独ではこの区別はできない。しかしながら、メッセージ偽造があったということは、なんらかの不正システムがネットワーク上に存在するということであり、それはマルウェアに感染した他の端末装置である可能性が高い。自装置が縮退動作モード（図8の603、605）に入ることで感染を防止することは、安全側の動作といえる。
【０１２０】
ROMモニタ301はシステムソフトウェアと比較して規模が小さく、通信機能を持たない。ROMモニタ301の動作は、定形データの操作に限られている。このため、ソースコードに対する静的検証技術等の脆弱性検出手法の適用により、全ての脆弱性が排除できることが期待できる。
【０１２１】
(3) の場合は、原因はマルウェア感染ではないが、システムソフトウェアの不具合は速やかに修正されるべきであり、システムソフトウェア更新のための縮退運転（図8の603、605）に入ることは合理的な動作である。不具合が一時的なものである場合、管理サーバ2からの通知メッセージ受信に成功すれば、運転状態は通常モード（図8の601）に戻る。
【０１２２】
(4) の場合は、ネットワーク1や管理サーバ2の一時的な不具合の場合、回復が期待できる。やはり不具合が一時的なものである場合、管理サーバ2からの通知メッセージの受信に成功すれば、運転状態は縮退運転（図8の603、605）から、通常（図8の601）に戻る。
【０１２３】
本実施形態では、ソフトウェア脆弱性の早期修正を目的として、管理サーバ2からの通知メッセージを取得する処理と、ROMモニタ301と管理サーバ2との間の通信の健全性確認と、マルウェア感染からの回復処理である再起動処理との3者を、ROMモニタ301が連携させる。これにより、パターンマッチングのような負荷の高い処理なしにマルウェア感染の兆候を検出し、マルウェアの妨害にあっても感染防止と正常状態への復帰のための更新ソフトウェア取得を確実に実行できる。つまり、自律的回復における特徴として、特に、マルウェア感染の兆候検出と更新有無の確認に、管理サーバ2との通信を利用することにより、端末装置上での高負荷なマルウェア検出（たとえばメモリ上のパターンマッチング処理）を必要とすることなく、更新通知の受信妨害のような迂回手段を含むマルウェアに対して、一定期間内にシステムソフトウェア更新版を適用することができる。
【０１２４】
本実施形態のマルウェア感染兆候検出は、マルウェアの種別までも検出できるものではなく、未知脆弱性を攻撃するマルウェアの対処を考慮した場合、ネットワーク全体の運用においてはマルウェアの種別特定可能な検出手段を併用することが望ましい。ハニーポットと呼ばれる侵入検知専用の端末を一部設置してマルウェア検出処理を稼働させることで、効率的にマルウェアを検出することが可能と予想される。このため、各端末装置でのマ

ルウェア検出処理を除去して、管理サーバ2との通信による脆弱性通知によってマルウェア対処を行うことで、端末装置に要求される処理能力を小さくして低価格化が可能となる。制御ネットワークにおいては、多数のほぼ同一構成の端末装置が稼働するため、必ずしも各端末装置でパターンマッチングのような高度な検索を実行する必要はない。このように、本実施形態は、単純なウォッチドッグタイマ回路と不揮発性メモリおよびアクセス制御機能を持つシングルマイコンにおいて、大規模マルウェア感染からの自律的回復が可能な端末装置を安価に実現できる。

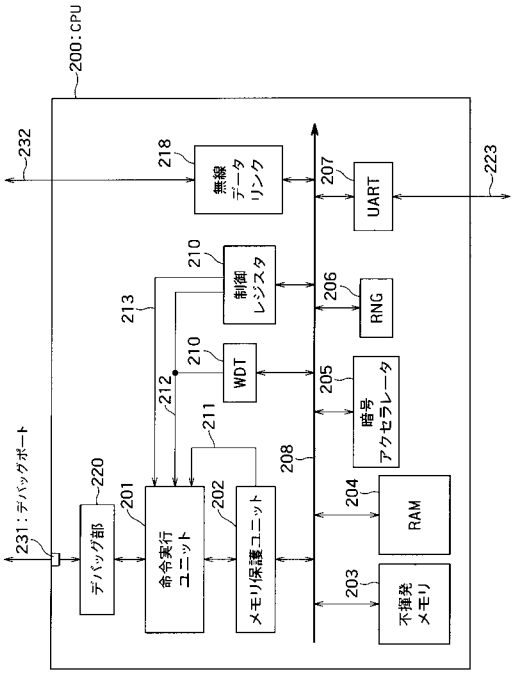
【図１】



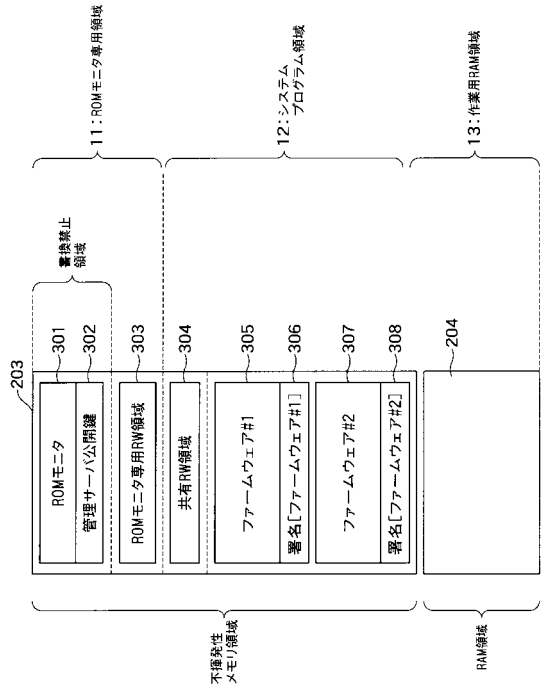
【図２】



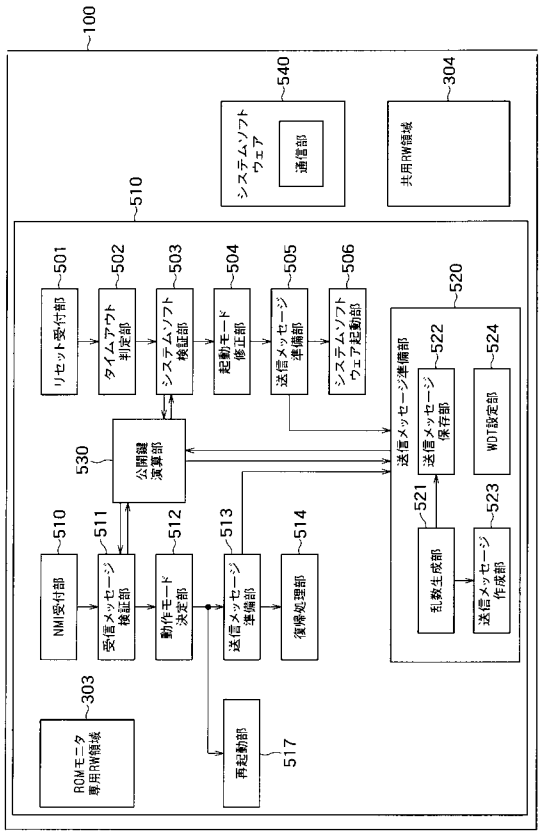
【図３】


200:CPU
232
218
無線データリンク
207
UART
223
213
210
制御レジスタ
206
RNG
210
WDT
212
211
205
暗号アクセラレータ
208
204
RAM
203
不揮発メモリ
231:デバッグポート
220
デバッグ部
201
命令実行ユニット
202
メモリ保護ユニット

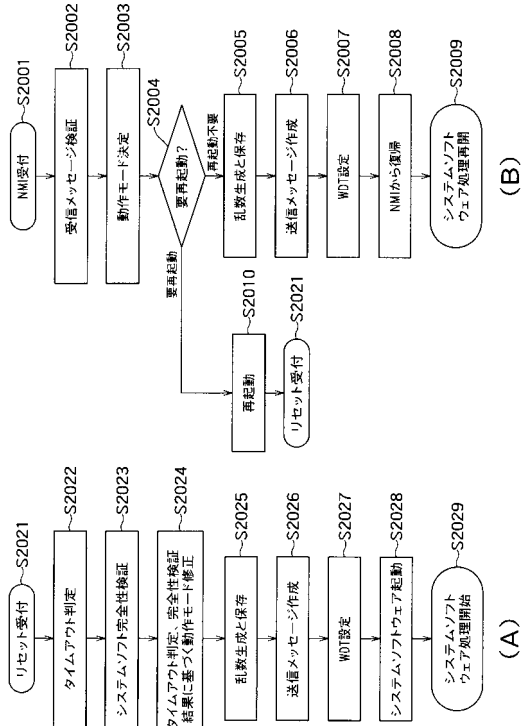
【図４】


11:ROMモニタ専用領域
12:システムプログラム領域
13:作業用RAM領域
書換禁止領域
203
301
302
303
304
305
306
307
308
204
ROMモニタ
管理サーバ公開鍵
ROMモニタ専用RW領域
共有RW領域
ファームウェア#1
署名[ファームウェア#1]
ファームウェア#2
署名[ファームウェア#2]
不揮発性メモリ領域
RAM領域

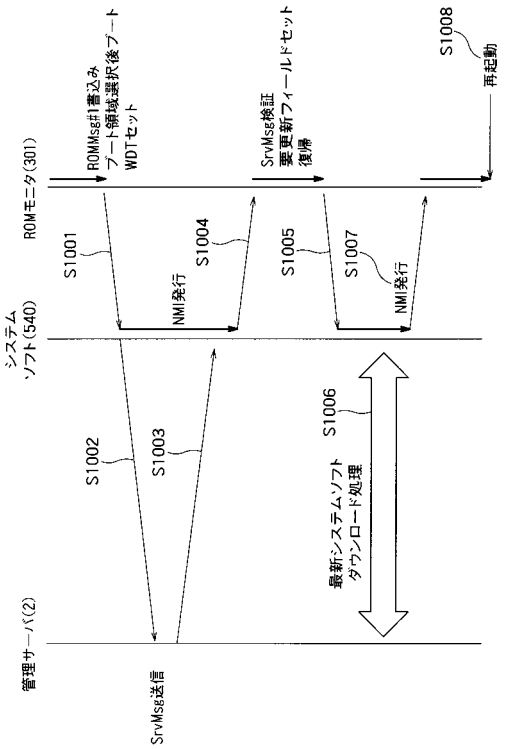
【図５】


100
510
540
システムソフトウェア
通信部
304
共用RW領域
501
リセット受付部
502
タイムアウト判定部
503
システムソフト検証部
504
起動モード修正部
505
送信メッセージ準備部
506
システムソフトウェア起動部
520
送信メッセージ準備部
522
送信メッセージ保存部
524
WDT設定部
530
公開鍵演算部
521
乱数生成部
523
送信メッセージ作成部
510
NMI受付部
511
受信メッセージ検証部
512
動作モード決定部
513
送信メッセージ準備部
514
復帰処理部
303
ROMモニタ専用RW領域
517
再起動部

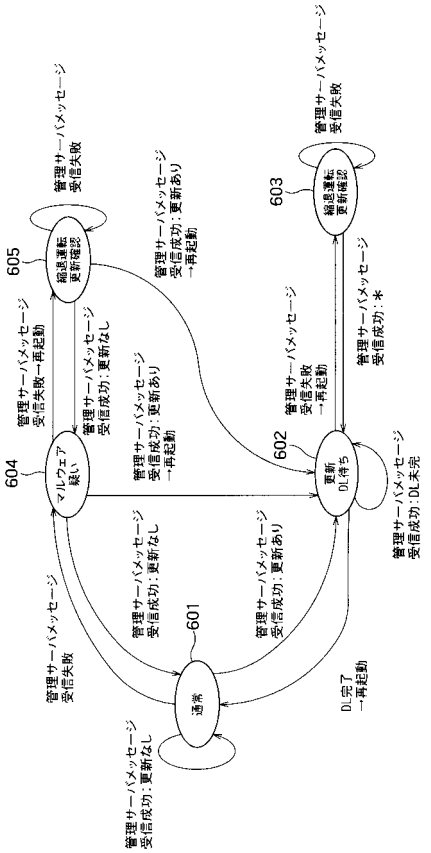
【図６】


S2001
NMI受付
S2002
受信メッセージ検証
S2003
動作モード決定
S2004
要再起動?
再起動不要
S2005
乱数生成と保存
S2006
送信メッセージ作成
S2007
WDT設定
S2008
NMIから復帰
S2009
システムソフトウェア処理再開
(B)
要再起動
S2010
再起動
S2021
リセット受付
S2021
リセット受付
S2022
タイムアウト判定
S2023
システムソフト完全性検証
S2024
タイムアウト判定、完全性検証結果に基づく動作モード修正
S2025
乱数生成と保存
S2026
送信メッセージ作成
S2027
WDT設定
S2028
システムソフトウェア起動
S2029
システムソフトウェア処理開始
(A)

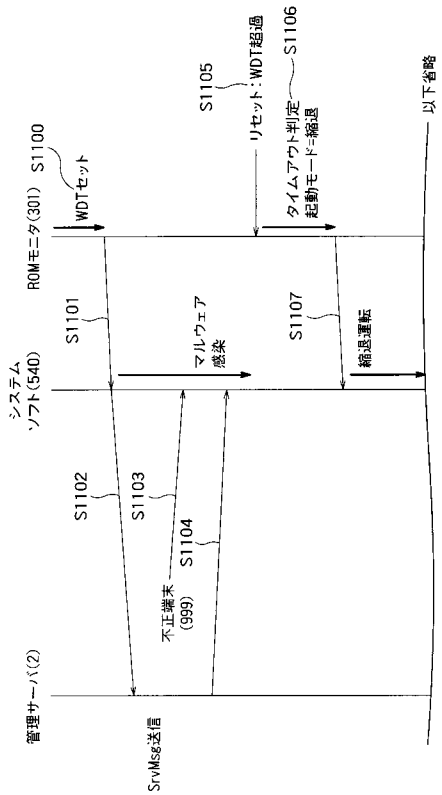
【図７】


ROMモニタ(301)
システムソフト(540)
管理サーバ(2)
S1001
S1002
S1003
S1004
S1005
S1006
S1007
S1008
ROMMsg書込み
ブート領域選択後ブート
WDTセット
NMI発行
SrvMsg検証
要更新フィールドセット
復帰
NMI発行
再起動
最新システムソフト
ダウンロード処理
SrvMsg送信

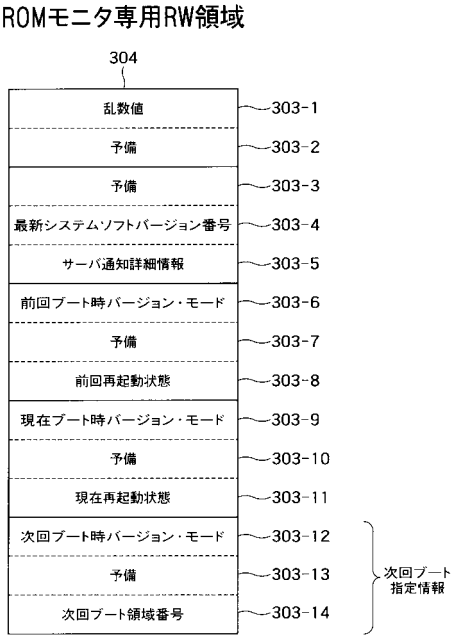
【図８】


601
通常
602
更新
DL待ち
603
縮退運転
更新確認
604
マルウェア
疑い
605
縮退運転
更新確認
管理サーバメッセージ
受信失敗
管理サーバメッセージ
受信成功:更新なし
管理サーバメッセージ
受信成功:更新あり
→再起動
管理サーバメッセージ
受信失敗
→再起動
管理サーバメッセージ
受信成功:＊
管理サーバメッセージ
受信成功:DL未完
DL完了
→再起動

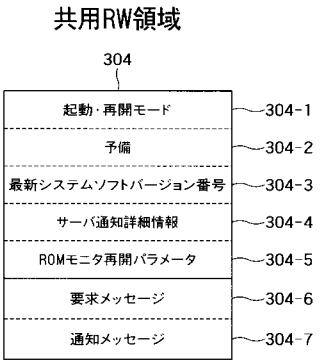
【図９】


ROMモニタ(301)
システムソフト(540)
管理サーバ(2)
S1100
S1101
S1102
S1103
S1104
S1105
S1106
S1107
WDTセット
マルウェア
感染
不正端末
(999)
リセット:WDT超過
タイムアウト判定
起動モード=縮退
縮退運転
以下省略
SrvMsg送信

【図１０】


ROMモニタ専用RW領域
304
乱数値
303-1
予備
303-2
予備
303-3
最新システムソフトバージョン番号
303-4
サーバ通知詳細情報
303-5
前回ブート時バージョン・モード
303-6
予備
303-7
前回再起動状態
303-8
現在ブート時バージョン・モード
303-9
予備
303-10
現在再起動状態
303-11
次回ブート時バージョン・モード
303-12
予備
303-13
次回ブート領域番号
303-14
次回ブート
指定情報

【図１１】


共用RW領域
304
起動・再開モード
304-1
予備
304-2
最新システムソフトバージョン番号
304-3
サーバ通知詳細情報
304-4
ROMモニタ再開パラメータ
304-5
要求メッセージ
304-6
通知メッセージ
304-7

フロントページの続き

(72)発明者　橋　本　幹　生
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　山　中　晋　爾
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　宮司　卓佳

(56)参考文献　特開２００２－３１８６３２（ＪＰ，Ａ）
特開２００１－０１４２２０（ＪＰ，Ａ）
特開２００４－１６４３５１（ＪＰ，Ａ）
特開２００４－０４６４３５（ＪＰ，Ａ）
特表２００７－５２８０８３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６