(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2004-157697
(P2004-157697A)
(43)公開日　平成16年6月3日(2004.6.3)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/60	G06F	17/60　124	
	G06F	17/60　162C	
	G06F	17/60　512	

審査請求 有　請求項の数 21　ＯＬ　（全 33 頁）

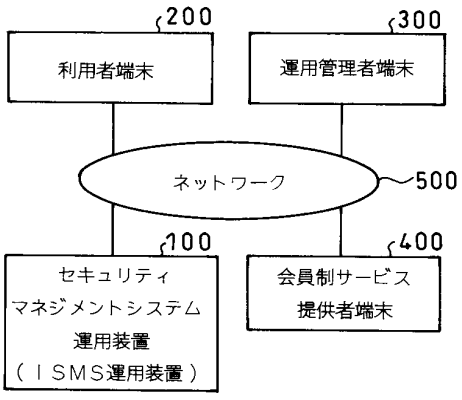
(21)出願番号　特願2002-321923(P2002-321923)
(22)出願日　平成14年11月6日(2002.11.6)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１４年度通信・放送機構「ネットワークセキュリティ監査技術の研究開発」に関する委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　000232092
ＮＥＣソフト株式会社
東京都江東区新木場一丁目１８番６号
(74)代理人　100088890
弁理士　河原　純一
(72)発明者　杉浦　昌
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　山下　昌人
東京都江東区新木場一丁目１８番６号　エヌイーシーソフト株式会社内

(54)【発明の名称】セキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法

(57)【要約】
【課題】経営支援ビジネスの一環として、セキュリティガイドラインの策定からセキュリティチェック等の機能をネットワークを利用した会員制サービスとして実現する。
【解決手段】利用者端末２００は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用者によって使用される。運用管理者端末３００は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者によって使用される。会員制サービス提供者端末４００は、セキュリティマネジメントシステムの会員制サービス提供者によって使用される。セキュリティマネジメントシステム運用装置１００は、利用者端末２００，運用管理者端末３００，および会員制サービス提供者端末４００からのアクセスによりネットワーク５００上でセキュリティマネジメントシステムの運用を可能にする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用者によって使用される利用者端末と、
会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者によって使用される運用管理者端末と、
セキュリティマネジメントシステムの会員制サービス提供者によって使用される会員制サービス提供者端末と、
前記利用者端末，前記運用管理者端末，および前記会員制サービス提供者端末からのアクセスによりネットワーク上でセキュリティマネジメントシステムの運用を可能にするセキュリティマネジメントシステム運用装置と
を有することを特徴とするセキュリティマネジメントシステム。
【請求項２】
前記セキュリティマネジメントシステム運用装置が、利用者機能である申請依頼処理機能と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能と、会員の中でセキュリティマネジメントシステムを利用する一次申請者が最終承認者に対して一次申請者所属部門におけるセキュリティマネジメントに必要な各種作業の状況を報告する際に利用する申請情報データベースと、会員の中でセキュリティマネジメントシステムを利用する最終承認者が運用管理者宛てに申請した申請情報の履歴を登録する履歴データベースと、運用管理者が自分が所属する会員の中の利用者を登録，修正，削除する時に使用する利用者データベースと、運用管理者が自分が所属する会員の中の組織情報を登録，修正，削除する時に使用する組織データベースと、運用管理者が自分が所属する会員の中で使用する申請フォームの雛形をメニューとして登録する申請フォームデータベースと、会員制サービス提供者が会員の会員情報を登録する会員データベースと、会員制サービス提供者がセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するセキュリティガイドラインデータベースとを有することを特徴とする請求項１記載のセキュリティマネジメントシステム。
【請求項３】
前記申請情報データベースのレコードが、申請日，申請者ＩＤ，申請者所属部門コード，申請フォーム区分，申請概要，申請内容，状態フラグ，否認日および否認理由，ならびに承認日および承認者の各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項４】
前記履歴データベースのレコードが、申請者所属部門コード，申請者ＩＤ，申請者／一次承認者所属部門コード，申請者／一次承認者ＩＤ，最終承認者所属部門コード，最終承認者ＩＤ，申請フォーム区分，申請概要，申請内容，および報告日の各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項５】
前記利用者データベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，利用者ＩＤ，パスワード，利用者名，利用者所属部門コード，電子メールアドレス，利用者職制，および申請依頼者設定の各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項６】
前記組織データベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，部門コード，部門名，部門階層，および承認権限設定の各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項７】

前記申請フォームデータベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，申請フォーム区分，および申請フォームの各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項８】
前記会員データベースのレコードが、登録日または最終更新日，企業／団体名，住所，ＴＥＬ／ＦＡＸ，運用管理者ＩＤ，運用管理者パスワード，およびサービス利用形態の各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項９】
前記セキュリティガイドラインデータベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，対応業種，対応企業／団体規模，用途，キーワード，およびセキュリティガイドラインの各フィールドからなることを特徴とする請求項２記載のセキュリティマネジメントシステム。
【請求項１０】
利用者機能である申請依頼処理機能と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する一次申請者が最終承認者に対して一次申請者所属部門におけるセキュリティマネジメントに必要な各種作業の状況を報告する際に利用する申請情報データベースと、会員の中でセキュリティマネジメントシステムを利用する最終承認者が運用管理者宛てに申請した申請情報の履歴を登録する履歴データベースと、会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する会員の中の利用者を登録，修正，削除する時に使用する利用者データベースと、運用管理者が自分が所属する会員の中の組織情報を登録，修正，削除する時に使用する組織データベースと、運用管理者が自分が所属する会員の中で使用する申請フォームの雛形をメニューとして登録する申請フォームデータベースと、会員制サービス提供者が会員の会員情報を登録する会員データベースと、会員制サービス提供者がセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するセキュリティガイドラインデータベースとを有することを特徴とするセキュリティマネジメントシステム運用装置。
【請求項１１】
コンピュータを、利用者機能である申請依頼処理機能と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する一次申請者が最終承認者に対して一次申請者所属部門におけるセキュリティマネジメントに必要な各種作業の状況を報告する際に利用する申請情報データベースと、会員の中でセキュリティマネジメントシステムを利用する最終承認者が運用管理者宛てに申請した申請情報の履歴を登録する履歴データベースと、会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する会員の中の利用者を登録，修正，削除する時に使用する利用者データベースと、運用管理者が自分が所属する会員の中の組織情報を登録，修正，削除する時に使用する組織データベースと、運用管理者が自分が所属する会員の中で使用する申請フォームの雛形をメニューとして登録する申請フォームデータベースと、会員制サービス提供者が会員の会員情報を登録する会員データベースと、会員制サービス提供者がセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するセキュリティガイドラインデータベースとして機能させるためのプログラム。
【請求項１２】
会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用

者によって使用される利用者端末と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者によって使用される運用管理者端末と、セキュリティマネジメントシステムの会員制サービス提供者によって使用される会員制サービス提供者端末と、前記利用者端末，前記運用管理者端末，および前記会員制サービス提供者端末からのアクセスによりネットワーク上でセキュリティマネジメントシステムの運用を可能にするセキュリティマネジメントシステム運用装置とを有するセキュリティマネジメントシステムにおいて、
前記セキュリティマネジメントシステム運用装置の処理が、利用者機能である申請依頼処理機能の処理と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能の処理と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能の処理とを含むことを特徴とする。
【請求項１３】
前記申請依頼処理機能の処理が、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末で会員コーナ内の申請フォームメニューを選択し利用する申請フォーム区分を選択したときに、セキュリティマネジメントシステム運用装置で申請フォーム区分の申請フォームを申請フォームデータベースから抽出する工程と、利用者端末で抽出された申請フォームに申請情報を登録したときに、セキュリティマネジメントシステム運用装置で申請情報データベースに申請概要および申請内容を登録する工程と、利用者端末で申請情報の登録後に申請ボタンをクリックしたときに、セキュリティマネジメントシステム運用装置で利用者データベースを参照し申請者の申請依頼者を抽出し、申請依頼者の電子メールアドレス宛てに申請依頼メールを送信する工程と、他の利用者端末で申請依頼メールを受信後にセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、他の利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、他の利用者端末で会員コーナ内の申請データ承認メニューを選択したときに、セキュリティマネジメントシステム運用装置で組織データベースを参照し承認権限設定情報を抽出し、申請情報データベースを参照し抽出された承認権限設定情報から承認可能な申請情報を抽出する工程と、他の利用者端末で抽出された申請情報が承認されたときに、セキュリティマネジメントシステム運用装置で申請情報データベース内の申請情報に承認フラグ，承認日および承認者を登録し、履歴データベースにも承認したデータを登録する工程と、他の利用者端末で抽出された申請情報を否認し否認理由が登録されたときに、セキュリティマネジメントシステム運用装置で申請情報データベース内の申請情報に否認フラグ，否認日および否認理由を登録し、申請依頼者の電子メールアドレス向けに否認通知メールを送信する工程と、利用者端末でセキュリティマ

ネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末で会員コーナ内の申請否認を選択したときに、セキュリティマネジメントシステム運用装置で利用者が作成した申請情報の中で他の利用者に否認処理されたデータを申請情報データベースから抽出する工程と、利用者端末で否認理由をもとに申請情報を修正したときに、セキュリティマネジメントシステム運用装置で申請情報データベースに修正後の申請概要および申請内容を登録する工程と、利用者端末で申請情報の修正後に申請を実行したときに、セキュリティマネジメントシステム運用装置で利用者データベースを参照し申請者の申請依頼者を抽出し、申請依頼者の電子メールアドレス宛てに申請依頼メールを送信する工程と、利用者端末で申請依頼メールを受信後にセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項１４】

前記利用者マスタ登録・更新・削除機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内の利用者マスタを選択後に新規利用者の登録を選択したときに、セキュリティマネジメントシステム運用装置で新規登録の場合は利用者データベースに利用者ＩＤ，パスワード，利用者名，電子メールアドレス，利用者所属部門コード，利用者職制，および申請依頼者設定の各項目を新規登録する工程と、運用管理者端末で運用管理者コーナ内の利用者マスタを選択後に既存利用者の利用者マスタの修正を選択したときに、セキュリティマネジメントシステム運用装置で利用者ＩＤ，パスワード等の項目を修正することにより利用者データベースが更新される工程と、運用管理者端末で運用管理者コーナ内の利用者マスタを選択後に既存利用者の利用者マスタの削除を選択したときに、セキュリティマネジメントシステム運用装置で削除対象となる利用者ＩＤを指定して削除処理を行うことにより削除した利用者のすべての登録項目が利用者データベースから削除される工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項１５】

前記セキュリティガイドライン策定機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コー

ナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内のセキュリティガイドラインを選択し利用するセキュリティガイドラインの雛形を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインの雛形をセキュリティガイドラインデータベースから抽出する工程と、運用管理者端末でセキュリティガイドラインの雛形をもとにセキュリティガイドラインの作成に着手する工程と、運用管理者端末であらかじめ用意されているヒアリングシートを記入し電子メールに添付して会員制サービス提供者に送信したときに、会員制サービス提供者端末でヒアリングシートに基づきセキュリティガイドラインの雛形の修正内容をアドバイスする工程と、運用管理者端末でセキュリティガイドラインの作成終了後に既にセキュリティガイドラインの雛形上で登録されている対応業種，規模，用途，および検索用キーワードを必要であれば修正し新規登録を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインデータベースに対応業種，対応企業／団体規模，用途，キーワード，およびセキュリティガイドラインを登録する工程と、運用管理者端末でセキュリティガイドラインの修正を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインデータベースからログインした運用管理者が作成したセキュリティガイドラインを抽出する工程と、運用管理者端末でセキュリティガイドラインの修正後にセキュリティガイドラインの修正を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインデータベースに修正後の内容を更新する工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項１６】

前記申請フォーム作成機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内の申請フォームを選択後に新規フォームを画面上で作成したときに、セキュリティマネジメントシステム運用装置で新規登録の場合は申請フォームを申請フォームデータベースに新規登録する工程と、運用管理者端末で運用管理者コーナ内の申請フォームを選択後に申請フォームの修正または削除を画面上で選択したときに、セキュリティマネジメントシステム運用装置で申請フォームデータベースからログインした運用管理者が作成した申請フォームを抽出する工程と、運用管理者端末で申請フォームの修正後に申請フォームの修正を選択したときに、セキュリティマネジメントシステム運用装置で申請フォームデータベースに修正後の内容を更新する工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項１７】

前記ワークフロー滞留監視機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログ

イン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内のワークフロー滞留監視を選択したときに、セキュリティマネジメントシステム運用装置で運用管理者が所属する会員におけるワークフローの滞留状況を集計する工程と、運用管理者端末で集計されたワークフローの滞留状況をチェックし、ワークフローが滞留している部門の部門長宛てに電子メールで処理の促進を督促したときに、利用者端末で運用管理者から自部門のワークフローの滞留状況の報告を電子メールで運用管理者とやりとりする工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項１８】

前記履歴参照機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内の履歴参照を選択後にチェックする部門を選択したときに、セキュリティマネジメントシステム運用装置で選択された部門の履歴のみを履歴データベースから抽出する工程と、運用管理者端末で抽出された履歴情報から参照したいデータを選択し参照する工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項１９】

前記会員マスタ登録・更新・削除機能の処理が、会員制サービス提供者端末でセキュリティマネジメントシステム運用装置上のメンテナンス機能にアクセスし会員マスタを選択したときに、セキュリティマネジメントシステム運用装置で新規登録の場合は会員データベースに企業／団体名，住所，ＴＥＬ／ＦＡＸ，運用管理者ＩＤ，運用管理者パスワード，および会員制サービス利用形態を新規登録する工程と、会員制サービス提供者端末で会員マスタを選択後に会員マスタの修正を選択したときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤ，運用管理者パスワード等の項目の修正により会員データベースが更新される工程と、会員制サービス提供者端末で会員マスタを選択後に会員マスタの削除を選択したときに、セキュリティマネジメントシステム運用装置で削除対象となる運用管理者ＩＤを指定して削除処理を行うことにより削除した会員のすべての登録項目が会員データベースから削除される工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項２０】

前記セキュリティガイドライン雛形登録・修正・削除機能の処理が、会員制サービス提供者端末でセキュリティマネジメントシステム運用装置上のメンテナンス機能にアクセスしセキュリティガイドラインを選択したときに、セキュリティマネジメントシステム運用装置で新規登録の場合はセキュリティガイドラインデータベースに対応業種，対応する企業の規模，用途，検索用キーワード，およびセキュリティガイドラインの雛形を登録する工程と、会員制サービス提供者端末でセキュリティガイドラインを選択後にセキュリティガイドラインの雛形の修正を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインの雛形の内容等の項目の修正によりセキュリティガイドライ

ンデータベースが更新される工程と、会員制サービス提供者端末でセキュリティガイドラインを選択後にセキュリティガイドラインの雛形の削除を選択したときに、セキュリティマネジメントシステム運用装置で削除対象となるセキュリティガイドラインの雛形を指定して削除処理を行うことにより削除したセキュリティガイドラインの雛形に付随したすべての登録項目がセキュリティガイドラインデータベースから削除される工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【請求項２１】

前記利用状況参照機能の処理が、会員制サービス提供者端末でセキュリティマネジメントシステム運用装置上のメンテナンス機能にアクセスし利用状況ログファイルを選択したときに、セキュリティマネジメントシステム運用装置で契約した会員ごとに蓄積された利用状況ログファイルを抽出する工程と、会員制サービス提供者端末で抽出した利用状況ログファイルに対し自動集計を選択したときに、セキュリティマネジメントシステム運用装置で日，週，月単位の利用時間合計や最も利用している時間帯の集計等を行い表示する工程とを含むことを特徴とする請求項１２記載のセキュリティマネジメントサービス提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法に関し、特に経営支援ビジネスとしてのセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法に関する。

【０００２】

【従来の技術】

従来のセキュリティマネジメントシステムでは、情報セキュリティポリシーおよび対象システムと管理・監査プログラムとを対応づけたセキュリティ・監査プログラムデータベースを設け、操作者により指定された情報セキュリティポリシーおよび対象システムの範囲に対応する管理・監査プログラムを検索し、自動的に実行するようになっていた（例えば、特許文献１参照）。

【０００３】

また、従来のセキュリティマネジメントシステムの他の例では、ポリシーデータベース，情報セキュリティポリシーおよび対象システムと管理・監査プログラムとを対応付けたセキュリティ管理・監査プログラムデータベース，ポリシー・設定情報マッピングテーブル，ならびに設定情報格納データベースを設け、操作者により指定された情報ポリシーおよび対象システムの範囲に対応する管理・監査プログラムを検索し、自動的に実行するようになっていた（例えば、特許文献２参照）。

【０００４】

【特許文献１】

特開２００１－２７３３８８号公報（第６－７頁、図２）

【特許文献２】

特開２００２－２４７０３３号公報（第６－７頁、図２）

【０００５】

【発明が解決しようとする課題】

上述した従来のセキュリティマネジメントシステムでは、以下の３つの問題点があった。

【０００６】

第１の問題点は、セキュリティマネジメントシステムを企業が導入するのに多大な時間と費用（コンサルテーション費用，ＩＴ（Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ）投資，要員教育等）がかかることである。また、システムの維持および管理についても多くの費用や専門知識を有した運用要員が必要である。このことは、セキュリティマネジメントシステムの企業への導入が一部の大企業にしか普及しないということであり、企業の大半を占める中小企業のセキュリティ対応状況の改善を阻む大きな要因であった。

【０００７】
第２の問題点は、セキュリティマネジメントシステムを導入しても、業務ワークフローと連動していないため、運用が十分行われなかったということである。
【０００８】
第３の問題点は、セキュリティガイドラインの質が策定者の技能レベルによって左右される問題があり、一定の品質を保つための方策が必要であったということである。
【０００９】
本発明の第１の目的は、経営支援ビジネスの一環として、セキュリティガイドラインの策定からセキュリティチェック等の機能をネットワークを利用した会員制サービスとして実現するようにしたセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法を提供することにある。
【００１０】
また、本発明の第２の目的は、会員制サービスが、複数の会員が同一システムを利用できる仕組みとすることやセキュリティガイドライン策定の支援を顧客である会員を直接訪問することなく、すべてネットワークを介して実現できるようにしたセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法を提供することにある。
【００１１】
さらに、本発明の第３の目的は、セキュリティガイドライン策定支援には、業種や規模別に作成されたヒアリングシートとセキュリティガイドラインデータベースとを利用し、策定までに要する時間の大幅短縮を実現するようにしたセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法を提供することにある。
【００１２】
さらにまた、本発明の第４の目的は、業種や規模別に作成されたセキュリティガイドラインデータベースを利用してセキュリティガイドラインを策定できることで、セキュリティガイドラインの質の低下や策定者の技能レベルに質が左右されることを防ぐようにしたセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法を提供することにある。
【００１３】
また、本発明の第５の目的は、クライアントの機器にはインターネットブラウザと電子メールソフトのみあれば、その他の特別なソフトウェアをインストールすること無しに利用できるようにしたセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法を提供することにある。
【００１４】
さらに、本発明の第６の目的は、Ｗｅｂと電子メールを利用したワークフロー機能を有するため、運用の効率化を実現できるようにしたセキュリティマネジメントシステムおよびセキュリティマネジメントサービス提供方法を提供することにある。
【００１５】
【課題を解決するための手段】
本発明のセキュリティマネジメントシステムは、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用者によって使用される利用者端末と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者によって使用される運用管理者端末と、セキュリティマネジメントシステムの会員制サービス提供者によって使用される会員制サービス提供者端末と、前記利用者端末，前記運用管理者端末，および前記会員制サービス提供者端末からのアクセスによりネットワーク上でセキュリティマネジメントシステムの運用を可能にするセキュリティマネジメントシステム運用装置とを有することを特徴とする。
【００１６】
また、本発明のセキュリティマネジメントシステムは、前記セキュリティマネジメントシステム運用装置が、利用者機能である申請依頼処理機能と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機

能，ワークフロー滞留監視機能，および履歴参照機能と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する一次申請者が最終承認者に対して一次申請者所属部門におけるセキュリティマネジメントに必要な各種作業の状況を報告する際に利用する申請情報データベースと、会員の中でセキュリティマネジメントシステムを利用する最終承認者が運用管理者宛てに申請した申請情報の履歴を登録する履歴データベースと、会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する会員の中の利用者を登録，修正，削除する時に使用する利用者データベースと、運用管理者が自分が所属する会員の中の組織情報を登録，修正，削除する時に使用する組織データベースと、運用管理者が自分が所属する会員の中で使用する申請フォームの雛形をメニューとして登録する申請フォームデータベースと、会員制サービス提供者が会員の会員情報を登録する会員データベースと、会員制サービス提供者がセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するセキュリティガイドラインデータベースとを有することを特徴とする。

【００１７】

さらに、本発明のセキュリティマネジメントシステムは、前記申請情報データベースのレコードが、申請日，申請者ＩＤ，申請者所属部門コード，申請フォーム区分，申請概要，申請内容，状態フラグ，否認日および否認理由，ならびに承認日および承認者の各フィールドからなることを特徴とする。

【００１８】

さらにまた、本発明のセキュリティマネジメントシステムは、前記履歴データベースのレコードが、申請者所属部門コード，申請者ＩＤ，申請者／一次承認者所属部門コード，申請者／一次承認者ＩＤ，最終承認者所属部門コード，最終承認者ＩＤ，申請フォーム区分，申請概要，申請内容，および報告日の各フィールドからなることを特徴とする。

【００１９】

また、本発明のセキュリティマネジメントシステムは、前記利用者データベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，運用管理者ＩＤ，利用者ＩＤ，パスワード，利用者名，利用者所属部門コード，電子メールアドレス，利用者職制，および申請依頼者設定の各フィールドからなることを特徴とする。

【００２０】

さらに、本発明のセキュリティマネジメントシステムは、前記組織データベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，部門コード，部門名，部門階層，および承認権限設定の各フィールドからなることを特徴とする。

【００２１】

さらにまた、本発明のセキュリティマネジメントシステムは、前記申請フォームデータベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，申請フォーム区分，および申請フォームの各フィールドからなることを特徴とする。

【００２２】

また、本発明のセキュリティマネジメントシステムは、前記会員データベースのレコードが、登録日または最終更新日，企業／団体名，住所，ＴＥＬ／ＦＡＸ，運用管理者ＩＤ，運用管理者パスワード，およびサービス利用形態の各フィールドからなることを特徴とする。

【００２３】

さらに、本発明のセキュリティマネジメントシステムは、前記セキュリティガイドラインデータベースのレコードが、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，対応業種，対応企業／団体規模，用途，キーワード，およびセキュリティガイドラインの各フィールドからなることを特徴とする。

【００２４】

さらにまた、本発明のセキュリティマネジメントシステム運用装置は、利用者機能である

申請依頼処理機能と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する一次申請者が最終承認者に対して一次申請者所属部門におけるセキュリティマネジメントに必要な各種作業の状況を報告する際に利用する申請情報データベースと、会員の中でセキュリティマネジメントシステムを利用する最終承認者が運用管理者宛てに申請した申請情報の履歴を登録する履歴データベースと、会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する会員の中の利用者を登録，修正，削除する時に使用する利用者データベースと、運用管理者が自分が所属する会員の中の組織情報を登録，修正，削除する時に使用する組織データベースと、運用管理者が自分が所属する会員の中で使用する申請フォームの雛形をメニューとして登録する申請フォームデータベースと、会員制サービス提供者が会員の会員情報を登録する会員データベースと、会員制サービス提供者がセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するセキュリティガイドラインデータベースとを有することを特徴とする。

【００２５】

一方、本発明のプログラムは、コンピュータを、利用者機能である申請依頼処理機能と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能と、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する一次申請者が最終承認者に対して一次申請者所属部門におけるセキュリティマネジメントに必要な各種作業の状況を報告する際に利用する申請情報データベースと、会員の中でセキュリティマネジメントシステムを利用する最終承認者が運用管理者宛てに申請した申請情報の履歴を登録する履歴データベースと、会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する会員の中の利用者を登録，修正，削除する時に使用する利用者データベースと、運用管理者が自分が所属する会員の中の組織情報を登録，修正，削除する時に使用する組織データベースと、運用管理者が自分が所属する会員の中で使用する申請フォームの雛形をメニューとして登録する申請フォームデータベースと、会員制サービス提供者が会員の会員情報を登録する会員データベースと、会員制サービス提供者がセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するセキュリティガイドラインデータベースとして機能させることを特徴とする。

【００２６】

他方、本発明のセキュリティマネジメントサービス提供方法は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用者によって使用される利用者端末と、会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者によって使用される運用管理者端末と、セキュリティマネジメントシステムの会員制サービス提供者によって使用される会員制サービス提供者端末と、前記利用者端末，前記運用管理者端末，および前記会員制サービス提供者端末からのアクセスによりネットワーク上でセキュリティマネジメントシステムの運用を可能にするセキュリティマネジメントシステム運用装置とを有するセキュリティマネジメントシステムにおいて、前記セキュリティマネジメントシステム運用装置の処理が、利用者機能である申請依頼処理機能の処理と、運用管理者機能である利用者マスタ登録・更新・削除機能，セキュリティガイドライン策定機能，申請フォーム作成機能，ワークフロー滞留監視機能，および履歴参照機能の処理と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能，セキュリティガイドライン雛形登録・修正・削除機能，および利用状況参照機能の処理とを含むことを特徴とする。

【００２７】
また、本発明のセキュリティマネジメントサービス提供方法は、前記申請依頼時の処理が、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末で会員コーナ内の申請フォームメニューを選択し利用する申請フォーム区分を選択したときに、セキュリティマネジメントシステム運用装置で申請フォーム区分の申請フォームを申請フォームデータベースから抽出する工程と、利用者端末で抽出された申請フォームに申請情報を登録したときに、セキュリティマネジメントシステム運用装置で申請情報データベースに申請概要および申請内容を登録する工程と、利用者端末で申請情報の登録後に申請ボタンをクリックしたときに、セキュリティマネジメントシステム運用装置で利用者データベースを参照し申請者の申請依頼者を抽出し、申請依頼者の電子メールアドレス宛てに申請依頼メールを送信する工程と、他の利用者端末で申請依頼メールを受信後にセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、他の利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、他の利用者端末で会員コーナ内の申請データ承認メニューを選択したときに、セキュリティマネジメントシステム運用装置で組織データベースを参照し承認権限設定情報を抽出し、申請情報データベースを参照し抽出された承認権限設定情報から承認可能な申請情報を抽出する工程と、他の利用者端末で抽出された申請情報が承認されたときに、セキュリティマネジメントシステム運用装置で申請情報データベース内の申請情報に承認フラグ，承認日および承認者を登録し、履歴データベースにも承認したデータを登録する工程と、他の利用者端末で抽出された申請情報を否認し否認理由が登録されたときに、セキュリティマネジメントシステム運用装置で申請情報データベース内の申請情報に否認フラグ，否認日および否認理由を登録し、申請依頼者の電子メールアドレス向けに否認通知メールを送信する工程と、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、利用者端末で会員コーナ内の申請否認を選択したときに、セキュリティマネジメントシステム運用装置で利用者が作成した申請情報の中で他の利用者に否認処理されたデータを申請情報データベースから抽出する工程と、利用者端末で否認理由をもとに申請情報を修正したときに、セキュリティマネジメントシステム運用

装置で申請情報データベースに修正後の申請概要および申請内容を登録する工程と、利用者端末で申請情報の修正後に申請を実行したときに、セキュリティマネジメントシステム運用装置で利用者データベースを参照し申請者の申請依頼者を抽出し、申請依頼者の電子メールアドレス宛てに申請依頼メールを送信する工程と、利用者端末で申請依頼メールを受信後にセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程とを含むことを特徴とする。

【００２８】

さらに、本発明のセキュリティマネジメントサービス提供方法は、前記利用者マスタの登録，更新，削除時の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内の利用者マスタを選択後に新規会員の登録を選択したときに、セキュリティマネジメントシステム運用装置で新規登録の場合は利用者データベースに利用者ＩＤ，パスワード，利用者名，電子メールアドレス，利用者所属部門コード，利用者職制，および申請依頼者設定の各項目を新規登録する工程と、運用管理者端末で運用管理者コーナ内の利用者マスタを選択後に既存利用者の利用者マスタの修正を選択したときに、セキュリティマネジメントシステム運用装置で利用者ＩＤ，パスワード等の項目を修正することにより利用者データベースが更新される工程と、運用管理者端末で運用管理者コーナ内の利用者マスタを選択後に既存利用者の利用者マスタの削除を選択したときに、セキュリティマネジメントシステム運用装置で削除対象となる利用者ＩＤを指定して削除処理を行うことにより削除した利用者のすべての登録項目が利用者データベースから削除される工程とを含むことを特徴とする。

【００２９】

さらにまた、本発明のセキュリティマネジメントサービス提供方法は、前記セキュリティガイドラインの策定の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内のセキュリティガイドラインを選択し利用するセキュリティガイドラインの雛形を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインの雛形をセキュリティガイドラインデータベースから抽出する工程と、運用管理者端末でセキュリティガイドラインの雛形をもとにセキュリティガイドラインの作成に着手する工程と、運用管理者端末であらかじめ用意されているヒアリングシートを記入し電子メールに添付して会員制サービス提供者に送信したときに、会員制サービス提供者端末でヒアリン

グシートに基づきセキュリティガイドラインの雛形の修正内容をアドバイスする工程と、運用管理者端末でセキュリティガイドラインの作成終了後に既にセキュリティガイドラインの雛形上で登録されている対応業種，規模，用途，および検索用キーワードを必要であれば修正し新規登録を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインデータベースに対応業種，対応企業／団体規模，用途，キーワード，およびセキュリティガイドラインを登録する工程と、運用管理者端末でセキュリティガイドラインの修正を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインデータベースからログインした運用管理者が作成したセキュリティガイドラインを抽出する工程と、運用管理者端末でセキュリティガイドラインの修正後にセキュリティガイドラインの修正を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインデータベースに修正後の内容を更新する工程とを含むことを特徴とする。

【００３０】

また、本発明のセキュリティマネジメントサービス提供方法は、前記申請フォームの作成の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内の申請フォームを選択後に新規フォームを画面上で作成したときに、セキュリティマネジメントシステム運用装置で新規登録の場合は申請フォームを申請フォームデータベースに新規登録する工程と、運用管理者端末で運用管理者コーナ内の申請フォームを選択後に申請フォームの修正または削除を画面上で選択したときに、セキュリティマネジメントシステム運用装置で申請フォームデータベースからログインした運用管理者が作成した申請フォームを抽出する工程と、運用管理者端末で申請フォームの修正後に申請フォームの修正を選択したときに、セキュリティマネジメントシステム運用装置で申請フォームデータベースに修正後の内容を更新する工程とを含むことを特徴とする。

【００３１】

さらに、本発明のセキュリティマネジメントサービス提供方法は、前記ワークフロー滞留監視機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば自部門のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内のワークフロー滞留監視を選択したときに、セキュリティマネジメントシステム運用装置で運用管理者が所属する会員におけるワークフローの滞留状況を集計する工程と、運用管理者端末で集計されたワークフローの滞留状況をチェックし、ワークフローが滞留している部門の部門長宛てに電子メールで処理の促進を督促したときに、利用者端末で運用管理者から自部門のワークフローの滞留状況の報告を電子メールで運用管理者とやりとりする工程とを含むことを特徴とする。

【００３２】
さらにまた、本発明のセキュリティマネジメントサービス提供方法は、前記履歴参照機能の処理が、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤおよびパスワードが会員データベースに存在するかどうかをチェックし、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末でセキュリティマネジメントシステム運用装置上の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインしたときに、セキュリティマネジメントシステム運用装置で利用者ＩＤおよびパスワードが利用者データベースに存在するかどうかをチェックし、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする工程と、運用管理者端末で運用管理者コーナ内の履歴参照を選択後にチェックする部門を選択したときに、セキュリティマネジメントシステム運用装置で選択された部門の履歴のみを履歴データベースから抽出する工程と、運用管理者端末で抽出された履歴情報から参照したいデータを選択し参照する工程とを含むことを特徴とする。

【００３３】
また、本発明のセキュリティマネジメントサービス提供方法は、前記会員マスタ登録・更新・削除機能の処理が、会員制サービス提供者端末でセキュリティマネジメントシステム運用装置上のメンテナンス機能にアクセスし会員マスタを選択したときに、セキュリティマネジメントシステム運用装置で新規登録の場合は会員データベースに企業／団体名，住所，ＴＥＬ／ＦＡＸ，運用管理者ＩＤ，運用管理者パスワード，および会員制サービス利用形態を新規登録する工程と、会員制サービス提供者端末で会員マスタを選択後に会員マスタの修正を選択したときに、セキュリティマネジメントシステム運用装置で運用管理者ＩＤ，運用管理者パスワード等の項目の修正により会員データベースが更新される工程と、会員制サービス提供者端末で会員マスタを選択後に会員マスタの削除を選択したときに、セキュリティマネジメントシステム運用装置で削除対象となる運用管理者ＩＤを指定して削除処理を行うことにより削除した会員のすべての登録項目が会員データベースから削除される工程とを含むことを特徴とする。

【００３４】
さらに、本発明のセキュリティマネジメントサービス提供方法は、前記セキュリティガイドライン雛形登録・修正・削除機能の処理が、会員制サービス提供者端末でセキュリティマネジメントシステム運用装置上のメンテナンス機能にアクセスしセキュリティガイドラインを選択したときに、セキュリティマネジメントシステム運用装置で新規登録の場合はセキュリティガイドラインデータベースに対応業種，対応する企業の規模，用途，検索用キーワード，およびセキュリティガイドラインの雛形を登録する工程と、会員制サービス提供者端末でセキュリティガイドラインを選択後にセキュリティガイドラインの雛形の修正を選択したときに、セキュリティマネジメントシステム運用装置でセキュリティガイドラインの雛形の内容等の項目の修正によりセキュリティガイドラインデータベースが更新される工程と、会員制サービス提供者端末でセキュリティガイドラインを選択後にセキュリティガイドラインの雛形の削除を選択したときに、セキュリティマネジメントシステム運用装置で削除対象となるセキュリティガイドラインの雛形を指定して削除処理を行うことにより削除したセキュリティガイドラインの雛形に付随したすべての登録項目がセキュリティガイドラインデータベースから削除される工程とを含むことを特徴とする。

【００３５】
さらにまた、本発明のセキュリティマネジメントサービス提供方法は、前記利用状況参照機能の処理が、会員制サービス提供者端末でセキュリティマネジメントシステム運用装置上のメンテナンス機能にアクセスし利用状況ログファイルを選択したときに、セキュリティマネジメントシステム運用装置で契約した会員ごとに蓄積された利用状況ログファイルを抽出する工程と、会員制サービス提供者端末で抽出した利用状況ログファイルに対し自

動集計を選択したときに、セキュリティマネジメントシステム運用装置で日，週，月単位の利用時間合計や最も利用している時間帯の集計等を行い表示する工程とを含むことを特徴とする。

【００３６】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００３７】

［第１の実施の形態］

図１を参照すると、本発明の第１の実施の形態に係るセキュリティマネジメントシステムは、セキュリティマネジメントシステム運用装置（以下、ＩＳＭＳ運用装置と記載する）１００と、利用者端末２００と、運用管理者端末３００と、会員制サービス提供者端末４００と、これらを相互に接続するインターネット等のネットワーク５００とから、その主要部が構成されている。

【００３８】

本実施の形態に係るセキュリティマネジメントシステムの利用者は、大きく分けて会員制サービスを提供する会員制サービス提供者と、会員制サービスを契約した会員（企業または団体）とに分けられる。上記会員内には、自らが所属する企業または団体のシステム運用全般を管理する運用管理者（一般的には情報システム部門）と、企業または団体の組織内において会員制サービス提供者が提供する機能を利用する利用者Ａおよび利用者Ｂとの３者が存在する（３者が承認階層によって増える場合もある）。利用者Ａは利用者端末Ａを、利用者Ｂは利用者端末Ｂを利用し、利用者Ａと利用者Ｂとの関係は企業または団体内組織における申請者（部下）と承認者（上司）との関係にある。

【００３９】

ＩＳＭＳ運用装置１００は、ネットワーク５００上でセキュリティマネジメントシステムの運用を可能にするための装置で、ワークステーション，サーバ等の情報処理装置によって構成される。

【００４０】

図２を参照すると、ＩＳＭＳ運用装置１００は、利用者機能である申請依頼処理機能１１１と、運用管理者機能である利用者マスタ登録・更新・削除機能１１２，セキュリティガイドライン策定機能１１３，申請フォーム作成機能１１４，ワークフロー滞留監視機能１１５，および履歴参照機能１１６と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能１１７，セキュリティガイドライン雛形登録・修正・削除機能１１８，および利用状況参照機能１１９と、利用者が申請したデータを申請情報として登録する申請情報データベース１２１と、申請情報を履歴として登録する履歴データベース１２２と、運用管理者が利用者ＩＤ（ＩＤｅｎｔｉｆｉｃａｔｉｏｎ），パスワード，社員情報などを登録する利用者データベース１２３と、組織情報，承認権限情報などを登録する組織データベース１２４と、申請フォームを登録する申請フォームデータベース１２５と、会員制サービス提供者が会員情報を登録する会員データベース１２６と、ヒアリングシートおよびセキュリティガイドラインを登録するセキュリティガイドラインデータベース１２７とを有する。なお、その他、特には図示しなかったが、会員単位に毎月の利用請求額を計算し請求書を発行する請求額計算・請求書発行機能等がＩＳＭＳ運用装置１００に含まれている。

【００４１】

申請情報データベース１２１は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用者Ａ（一次申請者）が利用者Ｘ（最終承認者）に対して利用者Ａ所属部門におけるセキュリティマネジメントに必要な各種作業（パーソナルコンピュータ内ソフトウェアのバージョン情報チェックやパーソナルコンピュータのウイルスチェック等）の状況を報告する際に利用するデータベースである。ここでは、利用者Ａ所属部門内に最終承認者が利用者Ｂという２階層の承認階層を想定して説明しているが、利用者データベース１２３および組織データベース１２４の設定によっては３階層以上の承

認階層の設定も可能である。

【００４２】

利用者Ａが申請登録したデータは、上位承認者（利用者Ａおよび利用者Ｂしか存在しない場合は利用者Ｂ）が否認処理しない限りは利用者Ａは修正できない（利用者Ａ，Ｂ，Ｃが存在する場合は、利用者Ｂは利用者Ａに対する承認および否認権限とデータ修正権限とを有し、利用者Ｃは利用者Ｂに対する承認および否認権限とデータ修正権限とを有する）。申請データを承認者が否認する場合は、必ず否認理由を登録することとし、申請者は否認理由を参照の上、下位申請者に否認として差し戻すか、その場で内容修正して再度、承認者宛に申請することになる。申請データは、最終承認者によって承認されて始めて当該部門の申請情報として正式に運用管理者宛に通知され全社情報として扱われる。

【００４３】

申請情報データベース１２１のレコードは、申請日（最新の申請日），申請者ＩＤ（申請者の利用者ＩＤ），申請者所属部門コード，申請フォーム区分（申請フォームデータベース１２５上の区分番号），申請概要（５０字程度の概要），申請内容（最終承認者に報告した内容），状態フラグ（各申請データに対する未申請，承認，否認の状態および滞留状況），否認日（申請データに対して否認処理を行った日）および否認理由，ならびに承認日および承認者（最終承認まで複数の承認がある場合は、それぞれの承認日および承認者）の各フィールドからなる。

【００４４】

履歴データベース１２２は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを利用する利用者Ｘが運用管理者宛てに申請した申請情報の履歴を登録するデータベースである。

【００４５】

履歴データベース１２２のレコードは、申請者所属部門コード，申請者ＩＤ（申請者の利用者ＩＤ），申請者／一次承認者所属部門コード，申請者／一次承認者ＩＤ（申請者／一次承認者の利用者ＩＤ），最終承認者所属部門コード，最終承認者ＩＤ（最終承認者の利用者ＩＤ），申請フォーム区分，申請概要，申請内容，および報告日（利用者Ｘが承認し運用管理者に報告した日。利用者Ｘの承認日と同じ日付）の各フィールドからなる。なお、承認階層が３階層以上の場合は、それに対応して承認者所属部門コードおよび承認者ＩＤが増えることになる。

【００４６】

利用者データベース１２３は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する企業または団体の中の利用者を登録，修正，削除する時に使用するデータベースである。ちなみに、運用管理者自らのＩＤとシステムを利用するすべての利用者のＩＤとは、利用者データベース１２３に登録されていることがシステム利用における必須条件となる。

【００４７】

利用者データベース１２３のレコードは、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，運用管理者ＩＤ（運用管理者のＩＤ），利用者ＩＤ（申請者／一次承認者／最終承認者等の運用管理者以外の利用者向けＩＤ），パスワード（運用管理者および利用者のシステム利用時のパスワード。初回は運用管理者が登録、それ以降の変更は自らが行う），利用者名，利用者所属部門コード，電子メールアドレス，利用者職制（主任，課長，部長等），および申請依頼者設定（だれが申請承認を行うのかを設定）の各フィールドからなる。

【００４８】

組織データベース１２４は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する企業または団体の中の組織情報を登録，修正，削除する時に使用するデータベースである。システムを利用する利用者の組織情報は、所属部門コードおよび所属部門名としてすべて組織データベース１２４に登録されていなければならない。また、下部組織に対する上位組織の設定等も、組織

データベース１２４上で登録される。

【００４９】

組織データベース１２４のレコードは、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，部門コード，部門名，部門階層（下位に位置する部門の部門コード情報），および承認権限設定（例えば、Ａ部門の部長はＡ部門配下の課のすべてを承認対象とするなど）の各フィールドからなる。なお、承認権限は、設定された部門コードの下位に位置する部門コードに対してもすべて承認権限を持つものとする。

【００５０】

申請フォームデータベース１２５は、会員制サービスを契約した会員の中でセキュリティマネジメントシステムを運用および管理する運用管理者が自分が所属する企業または団体の中で使用する申請フォームの雛形をメニューとして登録するデータベースである。システムを利用する利用者は、メニューとして登録された申請フォームを利用して、セキュリティマネジメントシステムの運用に必要な各種作業（パーソナルコンピュータ内ソフトウェアのバージョン情報チェックやパーソナルコンピュータのウイルスチェック等）の状況を承認者に申請（報告）する。また、新規申請フォームを登録機能を利用して申請フォームデータベース１２５に登録すると、申請フォーム区分というフォーム識別コードがシステム上で自動付与される。

【００５１】

申請フォームデータベース１２５のレコードは、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，申請フォーム区分（システムで自動付与），および申請フォーム（登録した申請フォームがセキュリティアップデート，セキュリティ監査等のメニューになる）の各フィールドからなる。

【００５２】

会員データベース１２６は、会員制サービス提供者が会員制サービスを契約した会員の会員情報を登録するデータベースである。運用管理者は、会員データベース１２６に運用管理者ＩＤおよびパスワードの登録が無いと、運用管理者向け機能のある運用管理者コーナへのログインができない。

【００５３】

会員データベース１２６のレコードは、登録日または最終更新日，企業／団体名，住所，ＴＥＬ／ＦＡＸ，運用管理者ＩＤ（複数付与可能），運用管理者パスワード（上記に対応し複数付与が可能），およびサービス利用形態（この利用形態により月額の請求額が変わる）の各フィールドからなる。

【００５４】

セキュリティガイドラインデータベース１２７は、会員制サービス提供者が会員制サービスを契約した会員向けにセキュリティガイドライン策定支援向けサービスとしてセキュリティガイドラインの雛形および運用管理者が作成したセキュリティガイドラインを登録するデータベースである。セキュリティガイドラインデータベース１２７は、業種，企業規模，用途によってカテゴライズしてセキュリティガイドラインの雛形を登録でき、検索対応としてキーワード登録も可能な構造である。

【００５５】

セキュリティガイドラインデータベース１２７のレコードは、登録日または最終更新日，登録または最終更新した運用管理者ＩＤ，対応業種，対応企業／団体規模，用途，キーワード（検索用キーワード、複数登録化），およびセキュリティガイドラインの各フィールドからなる。なお、会員制サービス提供者が登録したセキュリティガイドラインの雛形には、運用管理者ＩＤ欄に会員制サービス提供者固有のＩＤが登録される。

【００５６】

利用者端末２００は、ネットワーク５００上でセキュリティガイドラインに沿ったセキュリティマネジメントを行う利用者により使用される、パーソナルコンピュータ等の情報処理装置である。

【００５７】

運用管理者端末３００は、ネットワーク５００上でセキュリティマネジメントシステムの運用管理者によって使用される、パーソナルコンピュータ等の情報処理装置である。

【００５８】

会員制サービス提供者端末４００は、ネットワーク５００上で会員制サービス提供者によって使用される、パーソナルコンピュータ等の情報処理装置である。

【００５９】

図３を参照すると、利用者端末ＡおよびＢは、運用管理者から発行された利用者ＩＤおよびパスワードを用いネットワーク５００上を経由してセキュリティマネジメントシステム上の会員コーナにログインできる。利用者端末Ａは、会員限定コーナにログイン後、セキュリティアップデート，セキュリティ監査，セキュリティ簡易アセスメント等の申請依頼処理機能１１１を利用し、事前にマスタ上で設定された上司が利用する利用者端末Ｂに対してワークフロー機能を利用して申請を行うことができる。利用者端末Ａが申請すると、承認依頼が利用者端末Ｂに電子メールで届き、その通知により利用者端末Ｂは会員コーナにログイン後、申請内容について承認または否認を行うことができる。

【００６０】

図４を参照すると、運用管理者端末３００は、会員制サービス提供者から発行された運用管理者ＩＤおよびパスワードを用いネットワーク５００上を経由してセキュリティマネジメントシステム上の運用管理者コーナにログインできる。運用管理者端末３００は、運用管理者用として利用者マスタ（利用者ＩＤ，パスワード，組織情報，社員情報，電子メールアドレス，承認権限情報）登録・変更・削除機能１１２と、セキュリティガイドライン策定機能１１３と、申請フォーム登録・変更・削除機能１１４と、ワークフロー滞留監視機能１１５と、過去のセキュリティチェック状況を参照できる履歴参照機能１１６とを利用することができる。

【００６１】

図５を参照すると、会員制サービス提供者端末４００は、会員情報，企業名，住所，ＴＥＬ，運用管理者端末向けＩＤおよびパスワード等を登録，変更，削除する会員マスタ登録・更新・削除機能１１７と、セキュリティガイドライン策定のためのヒアリングシートを登録，変更，削除したりセキュリティガイドラインを登録，変更，削除したりセキュリティガイドライン策定に関する問い合わせに対して回答を返したりするセキュリティガイドライン雛形登録・修正・削除機能１１８と、契約した会員単位のサービス利用状況を参照する利用状況参照機能１１９とを利用することができる。

【００６２】

次に、このように構成された第１の実施の形態に係るセキュリティマネジメントシステムの動作について、図１ないし図５および図６ないし図１６のフローチャートを参照して詳細に説明する。

【００６３】

（１）　申請依頼処理機能１１１の処理（図６～図８参照）

【００６４】

利用者端末Ａで、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＡ１０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ１０１）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ１０２）。

【００６５】

利用者端末Ａで、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＡ１０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ１０３）、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力して

ログイン不可とする（ステップＣ１０４）。
【００６６】
利用者端末Ａで、会員コーナ内の申請フォームメニューを選択し利用する申請フォーム区分を選択すると（ステップＡ１０３）、ＩＳＭＳ運用装置１００では、選択された申請フォーム区分の申請フォームを申請フォームデータベース１２５から抽出する（ステップＣ１０５）。
【００６７】
利用者端末Ａで、抽出された申請フォームに申請情報を登録すると（ステップＡ１０４）、ＩＳＭＳ運用装置１００では、申請情報データベース１２１に申請概要および申請内容を登録（この時、申請日，申請者ＩＤ，申請者所属部門コード，および申請フォーム区分も同時に登録）する（ステップＣ１０６）。
【００６８】
利用者端末Ａで、申請情報の登録後に申請ボタンをクリックすると（ステップＡ１０５）、ＩＳＭＳ運用装置１００では、利用者データベース１２３を参照し申請者の申請依頼者を抽出し（ステップＣ１０７）、申請依頼者の電子メールアドレス宛てに申請依頼メールを送信する（ステップＣ１０８）。
【００６９】
利用者端末Ｂで、申請依頼メールを受信後、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＢ１０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ１０９）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ１１０）。
【００７０】
利用者端末Ｂで、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＢ１０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ１１１）、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ１１２）。
【００７１】
利用者端末Ｂで、会員コーナ内の申請データ承認メニューを選択すると（ステップＢ１０３）、ＩＳＭＳ運用装置１００では、組織データベース１２４を参照し承認権限設定情報を抽出し（ステップＣ１１３）、申請情報データベース１２１を参照し抽出された承認権限設定情報から承認可能な申請情報を抽出する（ステップＣ１１４）。
【００７２】
利用者端末Ｂで、抽出された申請情報を承認すると（ステップＢ１０４）、ＩＳＭＳ運用装置１００では、申請情報データベース１２１内の申請情報に承認フラグ，承認日および承認者を登録し（ステップＣ１１５）、履歴データベース１２２にも承認したデータを登録（登録する項目は履歴データベース１２２に存在する項目すべて）する（ステップＣ１１６）。
【００７３】
一方、利用者端末Ｂで、抽出された申請情報を否認し否認理由を登録すると（ステップＢ１０５）、ＩＳＭＳ運用装置１００では、申請情報データベース１２１内の申請情報に否認フラグ，否認日および否認理由を登録し（ステップＣ１１７）、申請依頼者の電子メールアドレス向けに否認通知メールを送信する（ステップＣ１１８）。
【００７４】
利用者端末Ａで、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＡ１０６）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどう

かをチェック（企業／団体チェック）し（ステップＣ１１９）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ１２０）。

【００７５】

利用者端末Ａで、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＡ１０７）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ１２１）、存在すれば自部門のみ利用できる会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ１２２）。

【００７６】

利用者端末Ａで、会員コーナ内の申請否認を選択すると（ステップＡ１０８）、ＩＳＭＳ運用装置１００では、利用者Ａが作成した申請情報の中で利用者Ｂに否認処理されたデータを申請情報データベース１２１から抽出する（ステップＣ１２３）。

【００７７】

利用者端末Ａで、否認理由をもとに申請情報を修正すると（ステップＡ１０９）、ＩＳＭＳ運用装置１００では、申請情報データベース１２１に修正後の申請概要および申請内容を登録（この時、申請日の更新も自動で行われる）する（ステップＣ１２４）。

【００７８】

利用者端末Ａで、申請情報の修正後に申請を実行すると（ステップＡ１１０）、ＩＳＭＳ運用装置１００では、利用者データベース１２３を参照し申請者の申請依頼者を抽出し（ステップＣ１２５）、申請依頼者の電子メールアドレス宛てに申請依頼メールを送信する（ステップＣ１２６）。

【００７９】

利用者端末Ｂで、申請依頼メールを受信後、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＢ１０６）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ１０９）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ１１０）。

【００８０】

このように、第１の実施の形態に係るセキュリティマネジメントシステムによれば、利用者は、運用管理者から発行されたＩＤおよびパスワードを利用してセキュリティマネジメントシステムにログインできる。

【００８１】

また、利用者（部下）は、ログイン後のメニューからセキュリティアップデート，セキュリティ監査，セキュリティ簡易アセスメント等の申請を選択して利用できる。

【００８２】

さらに、利用者（部下）がセキュリティマネジメントシステムから申請を行うと、申請した利用者の上司宛に承認依頼が電子メールで届き、その通知により利用者（上司）は、会員コーナにログイン後、申請内容について承認または否認を行うことができる。

【００８３】

（２）　運用管理者機能の処理（図９～図１３参照）

【００８４】

▲１▼利用者マスタ登録・更新・削除機能１１２の処理（図９参照）

【００８５】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＤ１０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ２０１）、存在すれば会員

コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ２０２）。

【００８６】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＤ１０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ２０３）、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ２０４）。

【００８７】

運用管理者端末３００で、運用管理者コーナ内の利用者マスタを選択後、新規利用者の登録を選択すると（ステップＤ１０３）、ＩＳＭＳ運用装置１００では、新規登録の場合は利用者データベース１２３に利用者ＩＤ，パスワード，利用者名，電子メールアドレス，利用者所属部門コード，利用者職制，および申請依頼者設定の各項目が新規登録（この時、登録日および登録した運用管理者の運用管理者ＩＤは自動登録となる）される（ステップＣ２０５）。

【００８８】

運用管理者端末３００で、運用管理者コーナ内の利用者マスタを選択後、既存利用者の利用者マスタの修正を選択すると（ステップＤ１０４）、ＩＳＭＳ運用装置１００では、利用者ＩＤ，パスワード等の項目の修正により利用者データベース１２３が更新（この時、更新日および更新した運用管理者の運用管理者ＩＤは自動登録となる）される（ステップＣ２０６）。

【００８９】

運用管理者端末３００で、運用管理者コーナ内の利用者マスタを選択後、既存利用者の利用者マスタの削除を選択すると（ステップＤ１０５）、ＩＳＭＳ運用装置１００では、削除対象となる利用者ＩＤを指定した削除処理により削除した利用者のすべての登録項目が利用者データベース１２３から削除される（ステップＣ２０７）。

【００９０】

▲２▼セキュリティガイドライン策定機能１１３の処理（図１０参照）

【００９１】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＤ２０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ３０１）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ３０２）。

【００９２】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＤ２０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ３０３）、存在すれば自部門のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ３０４）。

【００９３】

運用管理者端末３００で、運用管理者コーナ内のセキュリティガイドラインを選択し利用するセキュリティガイドラインの雛形を選択すると（ステップＤ２０２）、ＩＳＭＳ運用装置１００では、選択されたセキュリティガイドラインの雛形をセキュリティガイドラインデータベース１２７から抽出する（ステップＣ３０５）。

【００９４】

運用管理者端末３００で、抽出されたセキュリティガイドラインの雛形をもとにセキュリ

ティガイドラインの作成に着手する（ステップＤ２０４）。

【００９５】

運用管理者端末３００で、あらかじめ用意されているヒアリングシートを記入し電子メールに添付して会員制サービス提供者に送信（この時、作成に関わる質問があればそれも電子メールで会員制サービス提供者とやりとり）すると（ステップＤ２０５）、会員制サービス提供者端末２００では、ヒアリングシートに基づきセキュリティガイドラインの雛形の修正内容をアドバイス（質問が来ている場合それに対する回答も含めて電子メールで運用管理者とやりとり）する（ステップＥ１０１）。

【００９６】

運用管理者端末３００で、セキュリティガイドラインの作成終了後、既にセキュリティガイドラインの雛形上で登録されている対応業種，規模，用途，および検索用キーワードを必要であれば修正し新規登録を選択すると（ステップＤ２０６）、ＩＳＭＳ運用装置１００では、セキュリティガイドラインデータベース１２７に対応業種，対応企業／団体規模，用途，キーワード，およびセキュリティガイドラインを登録（この時、登録日および登録した運用管理者のＩＤも自動登録）する（ステップＣ３０６）。

【００９７】

運用管理者端末３００で、セキュリティガイドラインの修正を選択すると（ステップＤ２０７）、ＩＳＭＳ運用装置１００では、セキュリティガイドラインデータベース１２７からログインした運用管理者が作成したセキュリティガイドラインを抽出する（ステップＣ３０７）。

【００９８】

運用管理者端末３００で、セキュリティガイドラインの修正後、セキュリティガイドラインの修正を選択すると（ステップＤ２０８）、ＩＳＭＳ運用装置１００では、セキュリティガイドラインデータベース１２７に修正後の内容を更新（この時、更新日と更新した運用管理者のＩＤも自動更新）する（ステップＣ３０８）。

【００９９】

▲３▼申請フォーム作成機能１１４の処理（図１１参照）

【０１００】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＤ３０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ４０１）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ４０２）。

【０１０１】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＤ３０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ４０３）、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ４０４）。

【０１０２】

運用管理者端末３００で、運用管理者コーナ内の申請フォームを選択後、新規フォームを画面上で作成すると（ステップＤ３０４）、ＩＳＭＳ運用装置１００では、新規登録の場合は申請フォームデータベース１２５に申請フォームが新規登録（この時、登録日，登録した運用管理者の運用管理者ＩＤ，および申請フォーム区分は自動登録）される（ステップＣ４０５）。

【０１０３】

運用管理者端末３００で、運用管理者コーナ内の申請フォームを選択後、申請フォームの修正または削除を画面上で選択すると（ステップＤ３０４）、ＩＳＭＳ運用装置１００で

は、申請フォームデータベース１２５からログインした運用管理者が作成した申請フォームを抽出する（ステップＣ４０６）。

【０１０４】

運用管理者端末３００で、申請フォームの修正後、申請フォームの修正を選択（削除の場合は削除対象の申請フォームを選択）すると（ステップＤ３０４）、ＩＳＭＳ運用装置１００では、申請フォームデータベース１２５に修正後の内容を更新（この時、更新日および更新した運用管理者のＩＤも自動更新。削除の場合は削除対象となっている申請フォームが申請フォームデータベース１２５から削除）する（ステップＣ４０７）。

【０１０５】

▲４▼ワークフロー滞留監視機能１１５の処理（図１２参照）

【０１０６】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＤ４０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ５０１）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ５０２）。

【０１０７】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＤ４０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ５０３）、存在すれば自部門のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ５０４）。

【０１０８】

運用管理者端末３００で、運用管理者コーナ内のワークフロー滞留監視を選択すると（ステップＤ４０３）、ＩＳＭＳ運用装置１００では、運用管理者が所属する企業または団体におけるワークフローの滞留状況を集計する（ステップＣ５０５）。

【０１０９】

運用管理者端末３００で、集計されたワークフローの滞留状況をチェックし、滞留している部門の部門長宛てに電子メールで処理の促進を督促すると（ステップＤ４０４）、利用者端末Ｂでは、運用管理者から自部門のワークフローの滞留状況の報告を電子メールで運用管理者とやりとりする（ステップＢ２０１）。

【０１１０】

▲５▼履歴参照機能１１６の処理（図１３参照）

【０１１１】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の会員コーナにアクセスし運用管理者ＩＤおよびパスワードでログインすると（ステップＤ５０１）、ＩＳＭＳ運用装置１００では、入力された運用管理者ＩＤおよびパスワードが会員データベース１２６に存在するかどうかをチェック（企業／団体チェック）し（ステップＣ６０１）、存在すれば会員コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ６０２）。

【０１１２】

運用管理者端末３００で、ＩＳＭＳ運用装置１００上の自社コーナ内の会員コーナにアクセスし利用者ＩＤおよびパスワードでログインすると（ステップＤ５０２）、ＩＳＭＳ運用装置１００では、入力された利用者ＩＤおよびパスワードが利用者データベース１２３に存在するかどうかをチェック（利用者チェック）し（ステップＣ６０３）、存在すれば運用管理者のみ利用できる運用管理者コーナにログイン可とし、存在しなければエラーメッセージを出力してログイン不可とする（ステップＣ６０４）。

【０１１３】

運用管理者端末３００で、運用管理者コーナ内の履歴参照を選択後、チェックする部門を画面上で選択すると（ステップＤ５０３）、ＩＳＭＳ運用装置１００では、選択された部門の履歴のみを履歴データベース１２２から抽出する（ステップＣ６０５）。

【０１１４】

運用管理者端末３００では、抽出された履歴情報から参照したいデータを選択し参照する（ステップＤ５０４）。

【０１１５】

このように、運用管理者は、会員制サービス提供者から発行されたＩＤおよびパスワードを利用しセキュリティマネジメントシステムにログインできる。

【０１１６】

また、運用管理者は、ログイン後のメニューからマスタ（利用者ＩＤ，パスワード，組織情報，社員情報，承認権限情報）の更新を選択し、システムを利用する利用者情報，組織情報，申請データの承認権限情報等を登録し利用者に対する利用者ＩＤおよびパスワードの発行を行う。

【０１１７】

さらに、運用管理者は、ログイン後のメニューからセキュリティガイドライン策定のためのメニューを選択し、ネットワーク５００を通して会員制サービス提供者との間でセキュリティガイドラインの策定を行う。

【０１１８】

さらにまた、会員制サービス提供者は、セキュリティガイドライン策定に関する運用管理者からの質問等に対してネットワーク５００を介して回答を行うことができる。

【０１１９】

また、運用管理者は、ログイン後のメニューから申請フォームの更新機能を選択し、自社のセキュリティマネジメントシステムの運用に必要な申請フォームの登録を行う。

【０１２０】

さらに、運用管理者は、ログイン後のメニューからワークフローの滞留監視機能を選択し、セキュリティマネジメントシステムの運用が滞留している組織がないかどうかの監視を行うことができる。

【０１２１】

さらにまた、運用管理者は、ログイン後のメニューから希望する組織の過去のセキュリティチェック状況を参照行うことができる。

【０１２２】

（３）　会員制サービス提供者利用機能の処理（図１４～図１６参照）

【０１２３】

▲１▼会員マスタ登録・更新・削除機能１１７の処理（図１４参照）

【０１２４】

会員制サービス提供者端末２００で、ＩＳＭＳ運用装置１００上のメンテナンス機能にアクセスし会員マスタを選択（メニューから会員マスタの新規登録を選択）すると（ステップＥ２０１）、ＩＳＭＳ運用装置１００では、新規登録の場合は会員データベース１２６に企業／団体名，住所，ＴＥＬ／ＦＡＸ，運用管理者ＩＤ，運用管理者パスワード，および会員制サービス利用形態を新規登録（この時、登録日および運用管理者向け運用管理者ＩＤは自動登録）する（ステップＣ７０１）。

【０１２５】

会員制サービス提供者端末２００で、会員マスタを選択後、会員マスタの修正を選択すると（ステップＥ２０２）、ＩＳＭＳ運用装置１００では、運用管理者ＩＤ，運用管理者パスワード等の項目の修正により会員データベース１２６が更新（この時、登録日が更新した日に自動更新）される（ステップＣ７０２）。

【０１２６】

会員制サービス提供者端末２００で、会員マスタを選択後、会員マスタの削除を選択すると（ステップＥ２０３）、ＩＳＭＳ運用装置１００では、削除対象となる運用管理者ＩＤ

を指定して削除処理を行うことにより削除した会員のすべての登録項目が会員データベース１２６から削除される（ステップＣ７０３）。

【０１２７】

▲２▼セキュリティガイドライン雛形登録・修正・削除機能１１８の処理（図１５参照）

【０１２８】

会員制サービス提供者端末２００で、ＩＳＭＳ運用装置１００上のメンテナンス機能にアクセスしセキュリティガイドライン（選択メニューからアクセスしセキュリティガイドラインの雛形の新規登録）を選択すると（ステップＥ３０１）、ＩＳＭＳ運用装置１００では、新規登録の場合はセキュリティガイドラインデータベース１２７に対応業種，対応する企業の規模，用途，検索用キーワード，およびセキュリティガイドラインの雛形を登録（この時、登録日および会員制サービス提供者向け運用管理者ＩＤは自動登録）する（ステップＣ８０１）。

【０１２９】

会員制サービス提供者端末２００で、セキュリティガイドラインを選択後、セキュリティガイドラインの雛形の修正を選択すると（ステップＥ３０２）、ＩＳＭＳ運用装置１００では、セキュリティガイドラインの雛形の内容等の項目の修正によりセキュリティガイドラインデータベース１２７が更新（この時、登録日が更新した日に自動更新）される（ステップＣ８０２）。

【０１３０】

会員制サービス提供者端末２００で、セキュリティガイドラインを選択後、セキュリティガイドラインの雛形の削除を選択すると（ステップＥ３０３）、ＩＳＭＳ運用装置１００では、削除対象となるセキュリティガイドラインの雛形を指定して削除処理を行うことにより削除したセキュリティガイドラインの雛形に付随したすべての登録項目がセキュリティガイドラインデータベース１２７から削除される（ステップＣ８０３）。

【０１３１】

▲３▼利用状況参照機能１１９の処理（図１６参照）

【０１３２】

会員制サービス提供者端末２００で、ＩＳＭＳ運用装置１００上のメンテナンス機能にアクセスし利用状況ログファイル（図示せず）を選択すると（ステップＥ４０１）、ＩＳＭＳ運用装置１００では、契約した会員ごとに蓄積された利用状況ログファイルを抽出する（ステップＣ９０１）。

【０１３３】

会員制サービス提供者端末２００で、抽出した利用状況ログファイルに対し自動集計を選択すると（ステップＥ４０２）、ＩＳＭＳ運用装置１００では、日，週，月単位の利用時間合計や最も利用している時間帯の集計等を行い表示する（ステップＣ９０２）。

【０１３４】

このように、会員制サービス提供者は、会員制サービスの契約を結んだ会員の会員情報を登録し、ＩＤおよびパスワードを発行することで会員制サービスの利用を可能とすることができる。

【０１３５】

また、会員制サービス提供者は、必要に応じてヒアリングシートやセキュリティガイドラインの更新を行うことができる。

【０１３６】

さらに、会員制サービス提供者は、会員制サービスを契約した会員の利用状況の参照を行うことができる。

【０１３７】

以上説明したように、第１の実施の形態によれば、セキュリティガイドラインの策定からセキュリティチェック等のセキュリティマネジメントシステムをネットワークを利用した会員制サービスとして安価な利用料で提供することができる。

【０１３８】

また、会員制サービスは、複数の会員が同一システムを利用できる仕組みとすることやセキュリティガイドライン策定の支援を顧客に直接訪問することなく、すべてネットワークを介して実現することで安価な利用料を実現できる。

【０１３９】

さらに、セキュリティガイドライン策定支援には、業種や規模別に作成されたヒアリングシートとセキュリティガイドラインデータベースとを利用し、策定までに要する時間の大幅短縮を実現できる。

【０１４０】

さらにまた、業種や規模別に作成されたセキュリティガイドラインデータベースを利用してセキュリティガイドラインを策定できることで、セキュリティガイドラインの質の低下や策定者の技能レベルに質が左右されることを防止することができる。

【０１４１】

また、会員制サービスを実現するシステムは、クライアントの機器にはインターネットブラウザと電子メールソフトのみあれば、その他の特別なソフトウェアをインストールすること無しに利用できる。

【０１４２】

さらに、会員制サービスを実現するシステムは、Ｗｅｂと電子メールを利用したワークフロー機能を有するため、セキュリティマネジメントシステムの運用効率化を実現することができる。

【０１４３】

［第２の実施の形態］

図１７は、本発明の第２の実施の形態に係るセキュリティマネジメントシステムの構成を示すブロック図である。本実施の形態に係るセキュリティマネジメントシステムは、図１に示した第１の実施の形態に係るセキュリティマネジメントシステムに対して、ＩＳＭＳ運用装置１００にセキュリティマネジメントプログラム１０００を付加するようにした点だけが異なる。したがって、その他の特に言及しない部分には同一符号を付してそれらの詳しい説明を省略する。

【０１４４】

セキュリティマネジメントプログラム１０００は、コンピュータでなるＩＳＭＳ運用装置１００に読み込まれ、ＩＳＭＳ運用装置１００の動作を、利用者機能である申請依頼処理機能１１１と、運用管理者機能である利用者マスタ登録・更新・削除機能１１２，セキュリティガイドライン策定機能１１３，申請フォーム作成機能１１４，ワークフロー滞留監視機能１１５，および履歴参照機能１１６と、会員制サービス提供者機能である会員マスタ登録・更新・削除機能１１７，セキュリティガイドライン雛形登録・修正・削除機能１１８，および利用状況参照機能１１９と、申請情報データベース１２１と、履歴データベース１２２と、利用者データベース１２３と、組織データベース１２４と、申請フォームデータベース１２５と、会員データベース１２６と、セキュリティガイドラインデータベース１２７として制御する。セキュリティマネジメントプログラム１０００の制御によるＩＳＭＳ運用装置１００の動作は、第１の実施の形態におけるＩＳＭＳ運用装置１００の動作と全く同様になるので、その詳しい説明を割愛する。

【０１４５】

【発明の効果】

第１の効果は、セキュリティガイドラインの策定からセキュリティチェック等のセキュリティマネジメントシステムをネットワークを利用した会員制サービスとして安価な利用料で提供できることである。

【０１４６】

第２の効果は、会員制サービスが、複数の会員が同一システムを利用できる仕組みとすることやセキュリティガイドライン策定の支援を顧客に直接訪問することなくすべてネットワークを介して実現することで、安価な利用料で実現できることである。

【０１４７】

第３の効果は、セキュリティガイドライン策定支援には、業種や規模別に作成されたヒアリングシートとセキュリティガイドラインデータベースとを利用し、策定までに要する時間の大幅短縮を実現できることである。

【０１４８】

第４の効果は、業種や規模別に作成されたセキュリティガイドラインデータベースを利用してセキュリティガイドラインを策定できることで、セキュリティガイドラインの質の低下や策定者の技能レベルに質が左右されることを防止できることである。

【０１４９】

第５の効果は、会員制サービスを実現するシステムが、クライアントの機器にはインターネットブラウザと電子メールソフトのみあれば、その他の特別なソフトウェアをインストールすること無しに利用できることである。

【０１５０】

第６の効果は、会員制サービスを実現するシステムが、Ｗｅｂと電子メールを利用したワークフロー機能を有するため、セキュリティマネジメントシステムの運用効率化を実現できることである。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係るセキュリティマネジメントシステムの構成を示すブロック図である。

【図２】図１中のＩＳＭＳ運用装置の構成を示すブロック図である。

【図３】第１の実施の形態に係るセキュリティマネジメントシステムにおける申請依頼時の動作を説明する図である。

【図４】第１の実施の形態に係るセキュリティマネジメントシステムにおける利用者マスタの登録，更新，削除時等の動作を説明する図である。

【図５】第１の実施の形態に係るセキュリティマネジメントシステムにおける会員マスタの登録，更新，削除時等の動作を説明する図である。

【図６】第１の実施の形態に係るセキュリティマネジメントシステムにおける申請依頼処理機能の処理の前部を示すフローチャートである。

【図７】第１の実施の形態に係るセキュリティマネジメントシステムにおける申請依頼処理機能の処理の中部を示すフローチャートである。

【図８】第１の実施の形態に係るセキュリティマネジメントシステムにおける申請依頼処理機能の処理の後部を示すフローチャートである。

【図９】第１の実施の形態に係るセキュリティマネジメントシステムにおける利用者マスタ登録・更新・削除機能の処理を示すフローチャートである。

【図１０】第１の実施の形態に係るセキュリティマネジメントシステムにおけるセキュリティガイドライン策定機能の処理を示すフローチャートである。

【図１１】第１の実施の形態に係るセキュリティマネジメントシステムにおける申請フォーム作成機能の処理を示すフローチャートである。

【図１２】第１の実施の形態に係るセキュリティマネジメントシステムにおけるワークフロー滞留監視機能の処理を示すフローチャートである。

【図１３】第１の実施の形態に係るセキュリティマネジメントシステムにおける履歴参照機能の処理を示すフローチャートである。

【図１４】第１の実施の形態に係るセキュリティマネジメントシステムにおける会員マスタ登録・更新・削除機能の処理を示すフローチャートである。

【図１５】第１の実施の形態に係るセキュリティマネジメントシステムにおけるセキュリティガイドライン雛形登録・更新・削除機能の処理を示すフローチャートである。

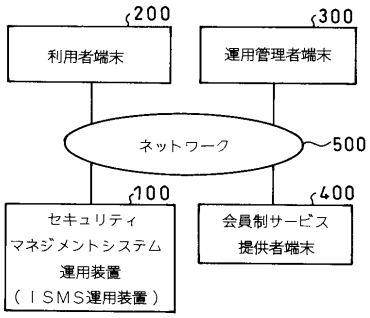
【図１６】第１の実施の形態に係るセキュリティマネジメントシステムにおける利用状況参照機能の処理を示すフローチャートである。

【図１７】本発明の第２の実施の形態に係るセキュリティマネジメントシステムの構成を示すブロック図である。

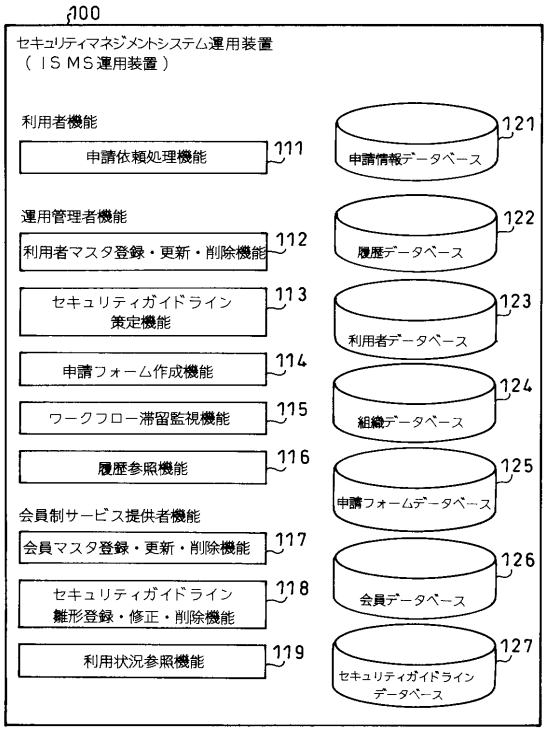
【符号の説明】

１００　セキュリティマネジメントシステム運用装置（ＩＳＭＳ運用装置）
申請依頼処理機能１１１
１１２　利用者マスタ登録・更新・削除機能
１１３　セキュリティガイドライン策定機能
１１４　申請フォーム作成機能
１１５　ワークフロー滞留監視機能
１１６　履歴参照機能
１１７　会員マスタ登録・更新・削除機能
１１８　セキュリティガイドライン雛形登録・修正・削除機能
１１９　利用状況参照機能
１２１　申請情報データベース
１２２　履歴データベース
１２３　利用者データベース
１２４　組織データベース
１２５　申請フォームデータベース
１２６　会員データベース
１２７　セキュリティガイドラインデータベース
２００　利用者端末
３００　運用管理者端末
４００　会員制サービス提供者端末
５００　ネットワーク
１０００　セキュリティマネジメントプログラム

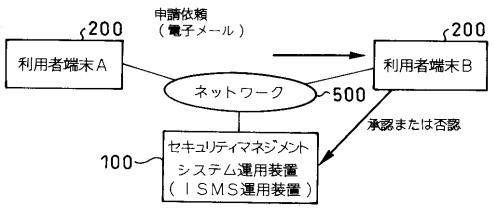
【図１】



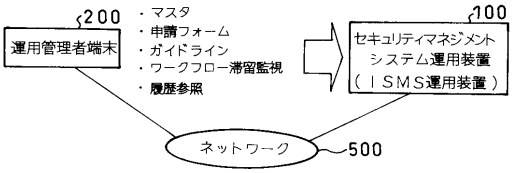
【図２】



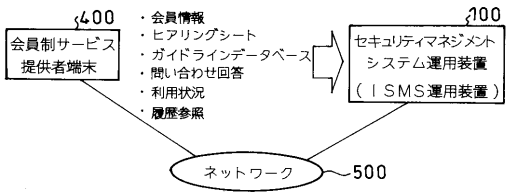
【図３】



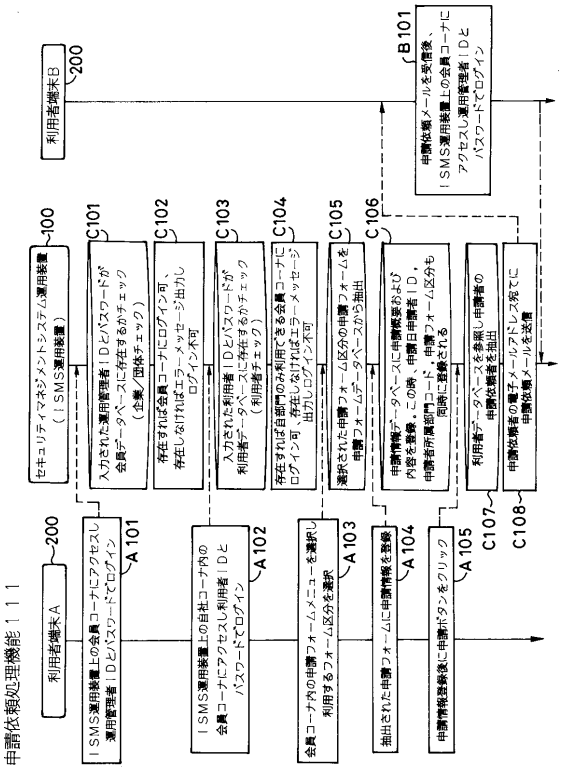
【図４】



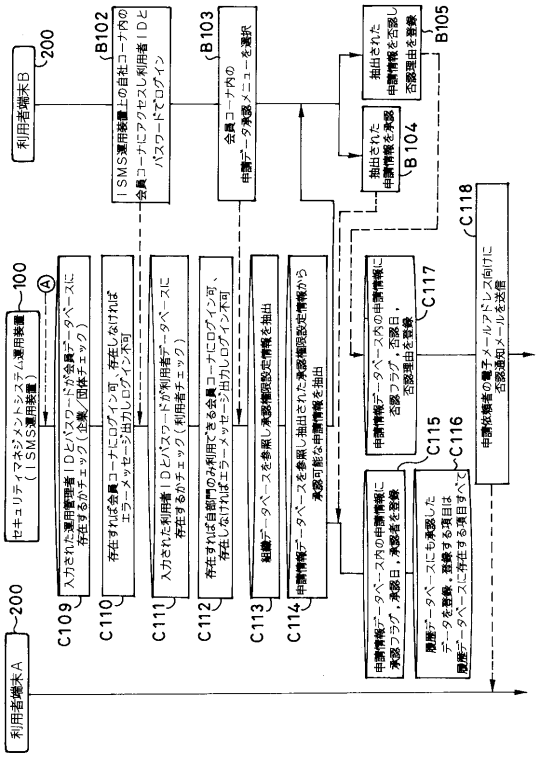
【図５】



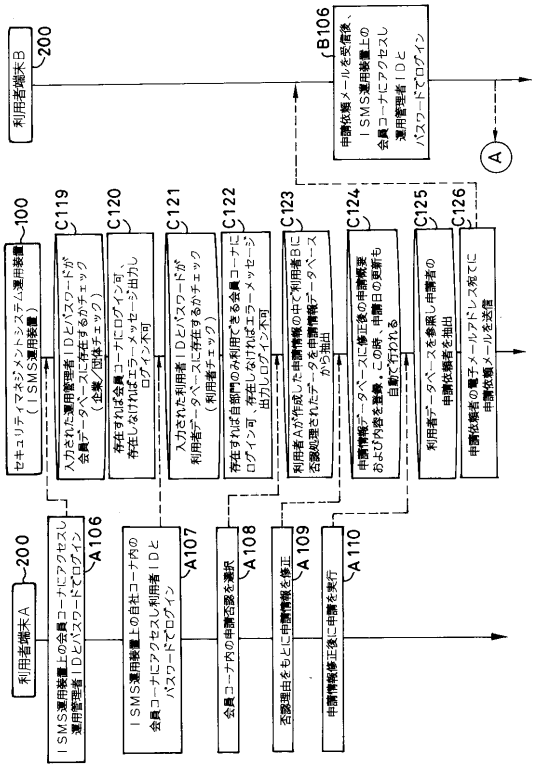
【図６】



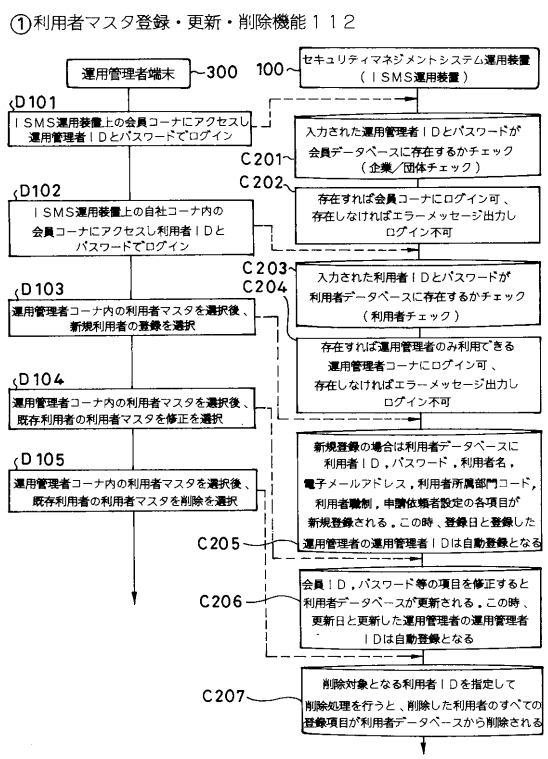
【図７】



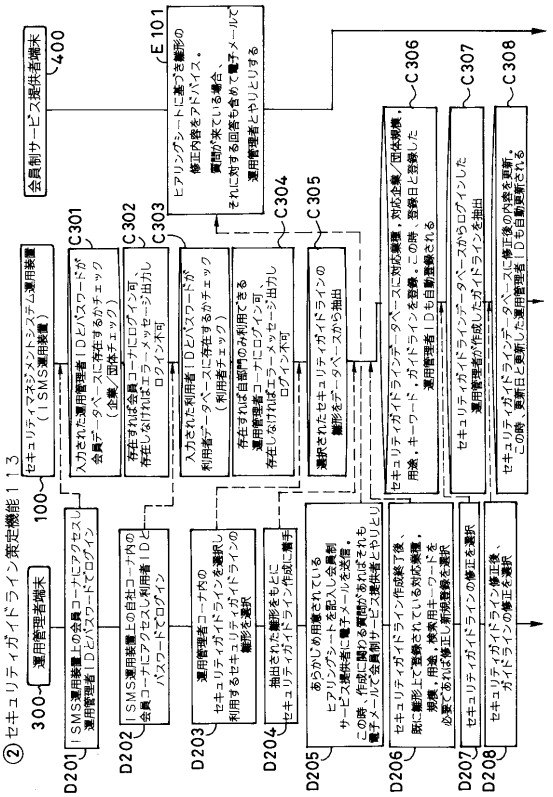
【図８】



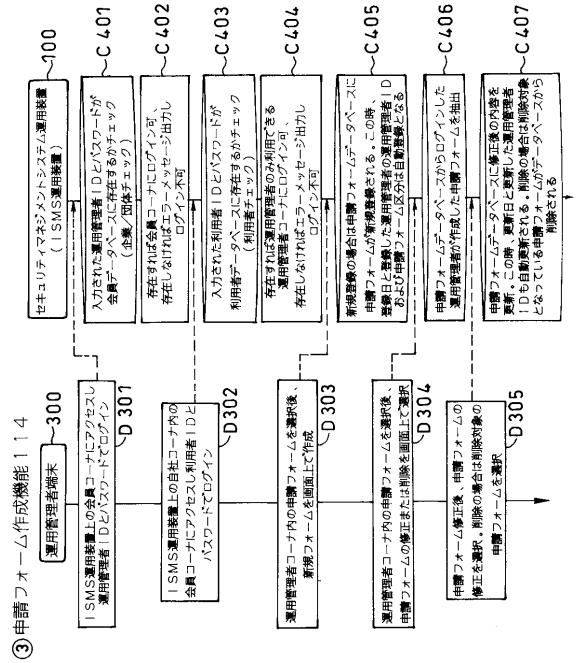
【図９】



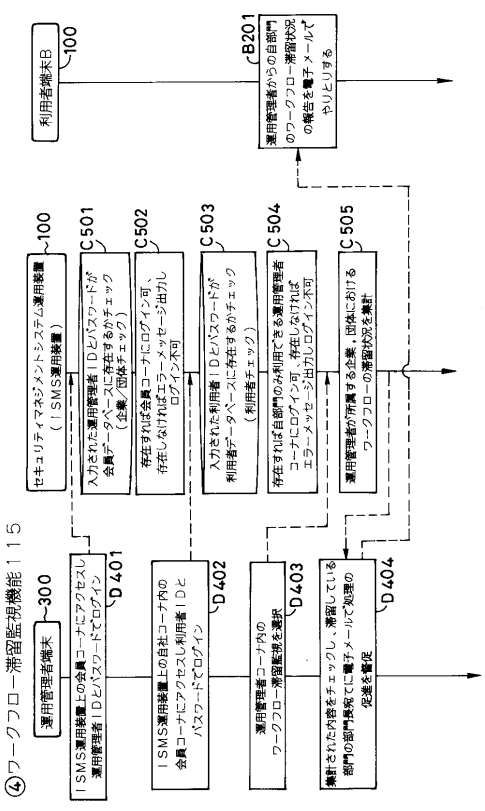
【図１０】



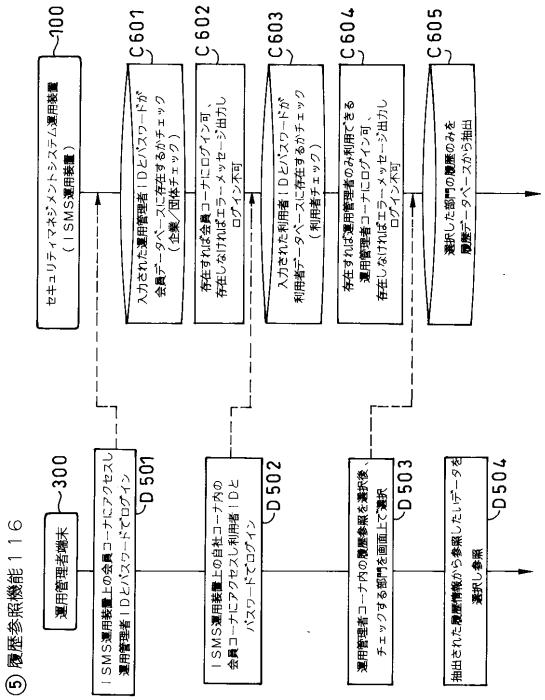
【図１１】



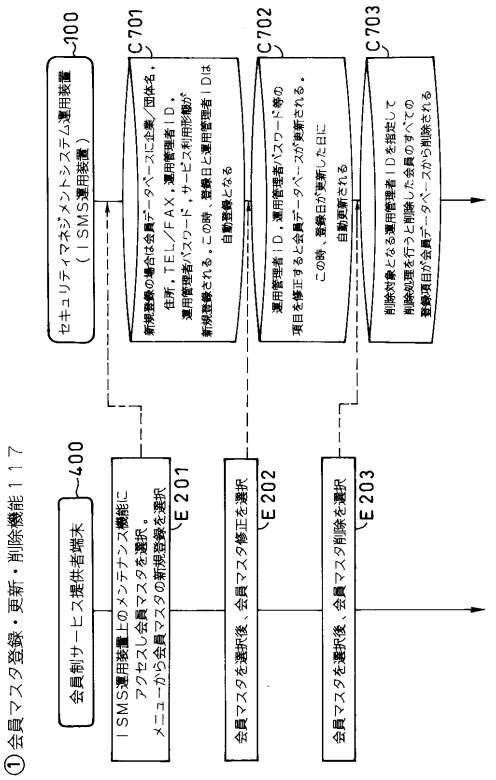
【図１２】



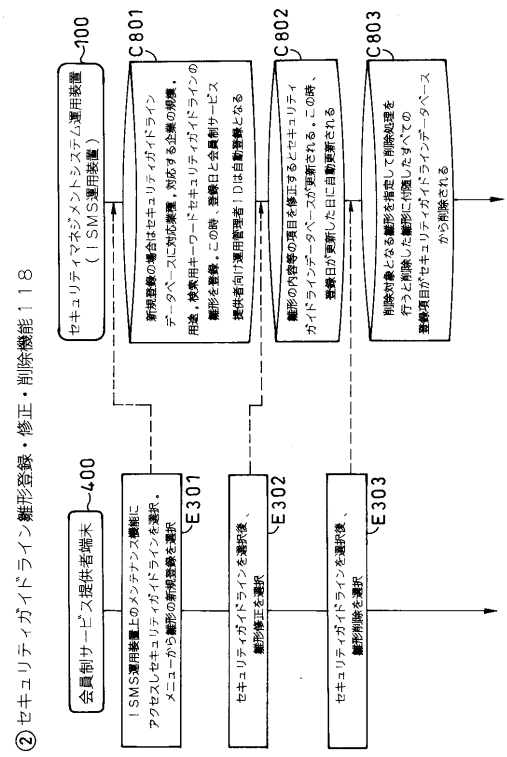
【図１３】



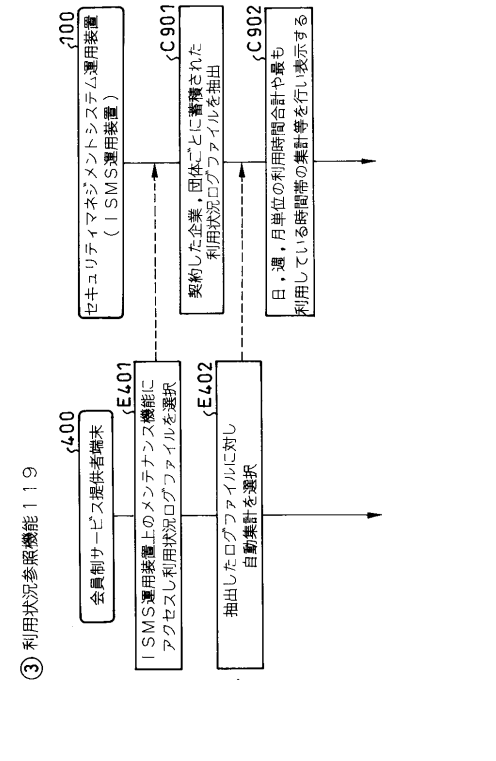
【図１４】



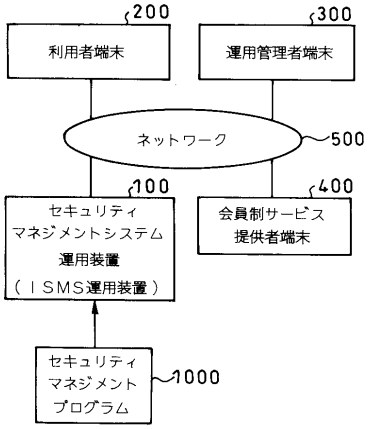
【図１５】



【図１６】



【図１７】


200
利用者端末
300
運用管理者端末
ネットワーク
500
100
セキュリティ
マネジメントシステム
運用装置
（ＩSMS運用装置）
400
会員制サービス
提供者端末
セキュリティ
マネジメント
プログラム
1000