

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4821028号
(P4821028)

(45) 発行日 平成23年11月24日(2011.11.24)

(24) 登録日 平成23年9月16日(2011.9.16)

(51) Int.Cl. F I
G06Q 50/00 (2006.01) G O 6 F 17/60 1 5 4
G06F 21/24 (2006.01) G O 6 F 12/14 5 6 0 A

請求項の数 6 (全 12 頁)

<p>(21) 出願番号 特願2007-116247 (P2007-116247)</p> <p>(22) 出願日 平成19年4月25日 (2007. 4. 25)</p> <p>(65) 公開番号 特開2008-276335 (P2008-276335A)</p> <p>(43) 公開日 平成20年11月13日 (2008.11.13)</p> <p>審査請求日 平成21年6月10日 (2009. 6. 10)</p> <p>(出願人による申告) 経済産業省平成18年度原子力発電施設等緊急時対策技術に関する委託に係る研究の成果に係る出願</p>	<p>(73) 特許権者 505374783 独立行政法人日本原子力研究開発機構 茨城県那珂郡東海村村松4番地49</p> <p>(73) 特許権者 596146968 株式会社 N E S I 東京都台東区根岸一丁目2番17号</p> <p>(74) 代理人 100078961 弁理士 茂見 稜</p> <p>(72) 発明者 渡辺 文隆 茨城県那珂郡東海村村松4番地49 独立行政法人日本原子力研究開発機構本部 原子力緊急時支援・研修センター内</p>
--	---

最終頁に続く

(54) 【発明の名称】 情報共有システム

(57) 【特許請求の範囲】

【請求項1】

組織内LANに設置されている情報共有サーバに複数の組織が連携して活動を行う上で必要となる様々な情報が蓄積されるようにし、複数の組織内LANに接続されているPCから当該情報共有サーバへの情報の登録並びに蓄積情報の閲覧を可能にすることにより情報を共有化するシステムにおいて、

前記情報共有サーバに蓄積する情報を、一般に向けて広報を行ってもよい最上位の一般情報、その下位の組織間で全体的に共有する共有情報、更にその下位の組織内だけで共有する内部情報の少なくとも3段階に階層化し、共有情報から一般情報への格上げ/格下げ権限者及び内部情報から共有情報への格上げ/格下げ権限者を階層毎あるいは組織毎に独立に設定可能とし、且つ、前記登録する情報に下書きフラグを付設し、情報共有サーバへの情報の登録に際して下書きフラグをオンにして仮登録の形で行い、下書きフラグをオフにすることで正式登録されるようにすると共に、それぞれの階層で下書きフラグをオンからオフにする下書き解除権限者を所属組織単位で独立に設定可能とし、該下書きフラグをオンにした前記PCを包含する下位の組織では、前記仮登録と前記正式登録の両方の情報を所属組織内に限定して閲覧可能としたことを特徴とする情報共有システム。

【請求項2】

複数の組織内LANにそれぞれ情報共有サーバが設置され、各組織内LANに設置されている情報共有サーバに複数の組織が連携して活動を行う上で必要となる様々な情報が蓄積されるようにし、各組織内LANに接続されているPCから当該情報共有サーバ

への情報の登録並びに蓄積情報の閲覧を可能にすることにより各組織内LANで情報を共有化すると共に、各組織間の共有情報を電子メールの形でインターネット経由でメールサーバにより相互に送受する情報共有システムにおいて、

各情報共有サーバに蓄積する情報を、一般に向けて広報を行ってもよい最上位の一般情報、その下位の組織間で全体的に共有する共有情報、更にその下位の組織内だけで共有する内部情報の少なくとも3段階に階層化し、各情報共有サーバ間で共有情報を連携させることによって該共有情報を複数の組織内LANのPCで全体的に利用可能とし、共有情報から一般情報への格上げ/格下げ権限者及び内部情報から共有情報への格上げ/格下げ権限者を階層毎あるいは組織毎に独立に設定可能とし、且つ、前記登録する情報に下書きフラグを付設し、情報共有サーバへの情報の登録に際して下書きフラグをオンにして仮登録の形で行い、下書きフラグをオフにすることで正式登録されるようにすると共に、それぞれの階層で下書きフラグをオンからオフにする下書き解除権限者を所属組織単位で独立に設定可能とし、該下書きフラグをオンにした前記PCを包含する下位の組織では、前記仮登録と前記正式登録の両方の情報を所属組織内に限定して閲覧可能としことを特徴とする情報共有システム。

10

【請求項3】

複数の組織内LANのうち少なくとも一つはインターネットに接続されていない閉鎖系LANである請求項1又は2記載の情報共有システム。

【請求項4】

内部情報を、組織内情報と最下位のグループ内情報とに更に階層化し、グループ内情報から組織内情報への格上げ/格下げ権限者も所属グループ単位で独立に設定可能とする請求項1乃至3のいずれかに記載の情報共有システム。

20

【請求項5】

情報共有システムが防災を主目的とする全国規模の緊急時情報共有システムであり、ユーザのシステムへのログイン時、地域選択と事象選択によりユーザが当該事象にアクセスする権限を持つか否かを判断し、その後、ユーザ名とパスワードによりログインの可否を判定し、ログイン後は、ユーザ単位に設定したセキュリティに従い、アクセスできる情報の階層が確定するようにした請求項1乃至4のいずれかに記載の情報共有システム。

【請求項6】

共有情報を事故名称毎に、時間帯軸、組織軸により集計・可視化することができる集計機能を具備している請求項5記載の情報共有システム。

30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、複数の組織が連携して活動を行う上で必要となる様々な情報を階層化し、ユーザがアクセス可能な階層を制限することにより、それらの情報を容易に管理できるようにした情報共有システムに関するものである。この技術は、特に災害発生時に複数の組織が連携して対応活動を行う必要がある緊急時情報共有システムに有用である。

【背景技術】

40

【0002】

緊急時対応活動では、災害規模の拡大と共に複数の組織が相互に連携して活動することが求められ、対応行動の実効性を高める上で、組織間の情報共有が極めて重要となる。例えば、原子力災害対策特別措置法では、災害現地に緊急事態応急対策拠点施設を設置し、原子力事業者をはじめ国、道府県、市町村、警察、消防、自衛隊、原子力専門家等が一堂に会し、事故終息活動、住民の避難防護措置、住民広報、報道対応など災害時の活動に一体となって対応することが定められている。しかしながら、実際の緊急時対応では事実関係の整理と情報共有に手間取る事例が、数多く見受けられる。

【0003】

そこで、切迫した局面においても緊急時対応関係者（防災従事者）が意思疎通を図り、

50

且つそれぞれの役割・機能を有機的に発揮し行動できるように、作業負担に繋がらない迅速な情報共有技術が求められている。このような問題を解決する技術として、緊急時の事実関係の整理と防災従事者の円滑な情報共有を目指し、ネットワーク上で稼働するWEBブラウザベースの緊急時情報共有システムが開発されている（非特許文献1参照）。

【0004】

この情報共有システムは、情報を持ち寄り相互に交換する情報交換所（クリアリングハウス）をネットワーク上に擬似的に実現する構成である。具体的には、全国各所の多数の緊急事態応急対策拠点施設、東京の中央官庁の緊急時対応拠点、茨城県ひたちなか市の原子力緊急時支援・研修センターなどを結ぶ専用回線によって、原子力防災に関わる閉鎖系ネットワークが構築されている。ここで、情報共有システムに係る情報共有サーバは、原子力緊急時支援・研修センター内に設置しているが、ネットワーク上のPCであれば、全国の拠点からWEBブラウザにより、情報の入力、閲覧、検索、印刷などの操作が可能になっている。

10

【0005】

ところで、実際の災害情報には、組織間全体で共有せず、組織内もしくはグループ内だけで共有すべき情報、あるいは組織内、グループ内で確認がとれてから組織間全体で共有すべき情報など、様々な種類の情報が存在する。しかし、従来はこの種の情報共有システムは、蓄積されている災害情報をシステム利用者全体で共有すること（言い換えればシステム利用者の誰もが同じ災害情報を共有すること）を主眼として構築されていた。そのため、上記のような様々な情報について、セキュリティの確保や必要な情報の公開など、各情報を個別に適切に管理することが難しい。特に、全国規模のように組織間ネットワークが広がると、情報管理は一層難しくなる。

20

【非特許文献1】「緊急時の組織間連携の円滑化をねらいとした緊急時情報共有システム」地域安全学会梗概集 No. 12. 2002. 11. p91 - 94

【発明の開示】

【発明が解決しようとする課題】

【0006】

本発明が解決しようとする課題は、様々な種類の情報について、セキュリティの確保や必要な情報の公開など、個別に適切に管理できるようにすることである。本発明が解決しようとする他の課題は、正式に登録すべきか判断が難しい情報、さしあたって登録しておきたい情報なども、とりあえず仮登録し、必要に応じて正式登録することができるようにし、必要な情報の入力漏れが生じ難く、迅速に入力・更新などが行えるようにすることである。本発明が解決しようとする更に他の課題は、防災を主目的とする全国規模の緊急時情報共有システムであっても、ユーザセキュリティを強化できるようにすることである。本発明の他の課題は、複数の関係組織が、どの時点でどのような活動を行ったのか、どの情報を得たのかを明らかにできるようにすること、訓練の事後評価においても、それらのことを明らかにできるようにすることである。

30

【課題を解決するための手段】

【0007】

本発明は、組織内LANに設置されている情報共有サーバに複数の組織が連携して活動を行う上で必要となる様々な情報が蓄積されるようにし、複数の組織内LANに接続されているPCから当該情報共有サーバへの情報の登録並びに蓄積情報の閲覧を可能にすることにより情報を共有化するシステムにおいて、前記情報共有サーバに蓄積する情報を、一般に向けて広報を行ってもよい最上位の一般情報、その下位の組織間で全体的に共有する共有情報、更にその下位の組織内だけで共有する内部情報の少なくとも3段階に階層化し、共有情報から一般情報への格上げ/格下げ権限者及び内部情報から共有情報への格上げ/格下げ権限者を独立に設定可能としたことを特徴とする情報共有システムである。

40

【0008】

また本発明は、複数の組織内LANにそれぞれ情報共有サーバが設置され、各組織内L

50

A Nに設置されている情報共有サーバに複数の組織が連携して活動を行う上で必要となる様々な情報が蓄積されるようにし、各組織内LANに接続されているPCから当該情報共有サーバへの情報の登録並びに蓄積情報の閲覧を可能にすることにより各組織内LANで情報を共有化すると共に、各組織間の共有情報を電子メールの形（添付ファイルも含む）でインターネット経由でメールサーバにより相互に送受する情報共有システムにおいて、各情報共有サーバに蓄積する情報を、一般に向けて広報を行ってもよい最上位の一般情報、その下位の組織間で全体的に共有する共有情報、更にその下位の組織内だけで共有する内部情報の少なくとも3段階に階層化し、各情報共有サーバ間で共有情報を連携させることによって該共有情報を複数の組織内LANのPCで全体的に利用可能とし、共有情報から一般情報への格上げ/格下げ権限者及び内部情報から共有情報への格上げ/格下げ権限者を独立に設定可能としたことを特徴とする情報共有システムである。

10

【0009】

これらにおいて、「格上げ/格下げ権限者」とは、格上げ機能のみの権限者、格上げと格下げの両方に対応できる権限者、格下げ機能のみの権限者も含まれるものとする。複数の組織内LANのうち少なくとも一つはインターネットに接続されていない閉鎖系LANであってよい。更に必要があれば、内部情報を、組織内情報と最下位のグループ内情報とに更に階層化し、グループ内情報から組織内情報への格上げ/格下げ権限者も独立に設定できるようにする。

【0010】

また、登録する情報に下書きフラグを付設し、情報共有サーバへの情報の登録に際して下書きフラグをオンにして仮登録の形で行い、下書きフラグをオフにすることで正式登録されるようにすると共に、それぞれの階層で下書きフラグをオンからオフにする下書き解除権限者を独立に設定可能とする。

20

【0011】

情報共有システムが防災を主目的とする全国規模の緊急時情報共有システムの場合は、ユーザのシステムへのログイン時、地域選択と事故事象選択によりユーザが当該事故事象にアクセスする権限を持つか否かを判断し、その後、ユーザ名とパスワードによりログインの可否を判定し、ログイン後は、ユーザ単位に設定したセキュリティに従い、アクセスできる情報の階層が確定するように構成するのが好ましい。なお、共有情報を事故名称毎に、時間軸、組織軸により集計・可視化することができる集計機能を具備していることが望ましい。

30

【発明の効果】**【0012】**

本発明に係る情報共有システムは、情報共有サーバに蓄積する様々な情報を、一般に向けて広報を行ってもよい最上位の一般情報、その下位の組織間で全体的に共有する共有情報、更にその下位の組織内だけで共有する内部情報というように階層化し、下位の階層から上位の階層への格上げ/格下げ権限者を独立に設定できるように構成しているため、複数の組織で共通の情報共有サーバを利用する場合でも、あるいは複数の組織にそれぞれ情報共有サーバを設置して互いに連携させて利用する場合であっても、様々な種類の情報を、セキュリティの確保や必要な情報の公開などを含めて個別に適切に管理できる。必要があれば、内部情報を、組織内情報と最下位のグループ内情報とに更に階層化でき、グループ内情報から組織内情報への格上げ/格下げ権限者も独立に設定することで、より一層細かな情報管理が行える。

40

【0013】

また、登録する情報に下書きフラグを付設し、情報共有サーバへの情報の登録に際して下書きフラグをオンにして仮登録の形で行い、下書きフラグをオフにすることで正式登録されるようにし、それぞれの階層で下書きフラグをオンからオフにする下書き解除権限者

50

を独立に設定可能にすると、正式に登録すべきか判断が難しい情報、さしあたって登録しておきたい情報なども、とりあえず仮登録しておくことができ、必要な情報の入力漏れが生じ難く、迅速な情報の入力・更新が行える。

【0014】

更に、ユーザのシステムへのログイン時、地域選択と事故事象選択によりユーザが当該事故事象にアクセスする権限を持つか否かを判断し、その後、ユーザ名とパスワードによりログインの可否を判定し、ログイン後は、ユーザ単位に設定したセキュリティに従い、アクセスできる情報の階層が確定するように構成すると、防災を主目的とする全国規模の緊急時情報共有システムであっても、ユーザセキュリティを強化できる。

【実施例】

【0015】

図1は、本発明に係る情報共有システムの一例を示す構成図である。ここでは、図面と説明を簡略化するため、主に2つの閉鎖系LAN(A組織LANとB組織LAN)で情報連携を行う場合を示しているが、同様の構成と同様の手順により、3つ以上の閉鎖系LAN間での情報連携を行うことができることは言うまでもない。このような構成は、特に緊急時情報共有システムとして有用である。

【0016】

A組織LANとB組織LANとに、それぞれ情報共有サーバ10a, 10bが設置されている。各情報共有サーバ10a, 10bには、同じ組織内LANに接続されている複数のPC(ここではそれぞれ1個のみ、即ち12aと12bのみ描いてあるが、通常はそれぞれ複数個接続されている)からアクセス可能である。これにより、各組織(A組織及びB組織)の情報がそれぞれの情報共有サーバ10a, 10bに集約される。例えば、A組織LANに組み込まれている複数のPC12aから同じA組織LANに組み込まれている情報共有サーバ10aに対して緊急時対応活動を行う上で必要となる様々な情報が登録され蓄積されるようにし、それらのPC12aで当該情報共有サーバ10aの蓄積情報を閲覧することにより、そのA組織内で情報を共有化できる。B組織でも同様である。

【0017】

情報共有サーバ内におけるデータベース構造の好ましい一例を図2に示す。情報共有サーバに蓄積する情報を、一般に向けて広報を行ってもよい最上位の一般情報、その下位の組織間で全体的に(防災関係者全体で)共有する共有情報、更にその下位の組織内だけで共有する内部情報の3段階に分ける。ここでは更に、内部情報を上位の組織内情報、最下位のグループ内だけで共有するグループ内情報に分ける。これによって、緊急時対応活動を行う上で必要となる様々な情報は、4段階に階層化される。なお、組織内にグループが無く全ての情報を共有するのであれば、内部情報を組織内情報とグループ内情報とに階層化する必要はなく、一般情報、共有情報、内部情報の3段階のみの階層化でもよい。このような情報の階層化に伴い、各情報の階層を変更する仕組みを設ける。

【0018】

更に、このような情報の階層化とは別次元の手法として、一般情報を除く各階層の情報に対して下書きフラグを付設する。この下書きフラグは、各情報の一つの属性である。情報共有サーバへの情報の登録に際して、下書きフラグをオンにして仮登録の形で行い、下書きフラグをオフにすることで正式登録される。下書きフラグを付け登録された情報は、同じ組織またはグループに所属するユーザだけが閲覧できる情報となる。

【0019】

緊急時対応活動では、災害規模の拡大と共に複数の組織が相互に連携して活動することが求められ、対応行動の実効性を高める上で、組織間の情報共有が極めて重要となる。そこで、各組織内LANの情報共有サーバ間で蓄積情報を連携させ、それによって他の組織の蓄積情報も利用可能とする。そのため図2に示すように、各情報共有サーバの共有情報の階層についてのみ相互に情報連携を図り、それらを全体共有情報として、A, B両組織LANのPC12a, 12bで利用できるようにする。このようにすることで、複数の組織に複数の情報共有サーバが併存する場合でも、必要な情報を組織をまたいで全組織で共

10

20

30

40

50

有することができ、災害時に複数の組織がそれぞれに連携をはかりながら適切且つ有効な防災活動を行うことができる。

【 0 0 2 0 】

前記のように情報の階層化に伴い、各情報の階層を変更する仕組みを設ける。情報共有サーバにおける各情報の階層変更は、共有情報を一般情報へ、内部情報を共有情報へ、グループ内情報を組織内情報へ、それぞれの格上げ/格下げである。階層間の格上げ/格下げは、予めそれぞれの格上げ/格下げについて独立に設定されている権限者、即ち共有情報から一般情報への格上げ/格下げ権限者（一般的には広報担当の責任者）、内部情報から共有情報への格上げ/格下げ権限者（一般的には各組織の情報担当の責任者）、及びグループ内情報から組織内情報への格上げ/格下げ権限者（一般的にはグループの責任者）のみが行えるように制限され、それによって各階層の情報を個別に管理できる仕組みを採用している。因みに、共有情報から一般情報への格上げ/格下げ権限者でも、内部情報から共有情報への格上げ/格下げ権限者とは限らない。

10

【 0 0 2 1 】

アクセス権限の設定画面の一例（要部のみ）を図3に示す。一般ユーザ権限としては、階層毎に更新権限、閲覧権限の設定（但し、一般情報については全ユーザで閲覧可）があり、更新権限の中には更に下書き権限の設定、取り消し権限の設定もある。情報責任者権限としては、各段階において情報の格上げ/格下げ権限があり、それとは別に下書き権限が独立に存在する。これらは、システムの利用状況に合わせて画面上で四角枠にチェックを入れることで任意に設定できる。同様にサーバ間連携を行う共有情報を設定できるサーバ間情報連携権限も別途設定できる。更に管理者権限も設定でき、その他、任意の権限設定も追加できる。このように各情報共有サーバ内における蓄積情報を階層化し、各階層間での情報の格上げ/格下げ権限を制限することにより、複数の情報共有サーバが併存する複雑な組織体制下でも、情報を個別に管理することが容易となる。

20

【 0 0 2 2 】

情報共有システムが、防災を主目的とする緊急時情報共有システムの場合、一般に全国に展開したネットワーク上での利用を考慮したシステムとなる。そのためユーザのログイン時、ユーザ名、パスワードを選択する前に、地域の選択を行うようにする。また地域の選択後には、その地域で利用可能な事故対象名からログインしたい事故名称を選択し、その後、具体的に組織名、グループ名、ユーザ名、及びパスワードの入力を行う仕組みとする。そのようなユーザセキュリティの自動設定の処理フローを図4に示す。通常のようなシステムのようなユーザ認証だけでなく、地域および事故名称を絞り込むことにより、その時点でそのユーザがログインしようとする事故名称にアクセスする権限を持つかを判断する。そのため、ユーザ名およびパスワードを正しく入力しても、その事故名称にアクセスする権限を持っていない場合には、ログインを行うことができない。ユーザのセキュリティ権限を確認しシステムにログインした後は、ユーザ単位に設定されたセキュリティに従い、閲覧もしくは入力・更新できる情報の階層が確定する。各ユーザのセキュリティ権限については、予めセキュリティ情報を登録しておき、その情報をユーザ登録時に選択するようにしており、毎回ユーザ毎に細かいセキュリティ設定を行わなくてもよい仕組みとなっている。

30

40

【 0 0 2 3 】

ところで、一般にデータベースの情報を交換するには、データベースエンジンが持つ機能を利用する。しかし、これをインターネット経由で行おうとすると、各組織内LANのファイアウォールにより通信が遮断され、情報交換が行えない。そのため、専用回線を用いざるをえないが、専用回線費が高くなること、組織LANの増加や減少に柔軟に対応し難いことなどデメリットが大きい。また本発明では、一般向けに広報を行う一般情報が含まれている。そこで、インターネット経由で電子メールの形（添付ファイルも含む）で情報を送受信する方式を採用している。電子メールを利用する情報交換は、次のような利点がある。まず、組織内LANのファイアウォールにより通信が遮断される可能性が殆どなく、システム管理者にファイアウォールの設定変更を要求する必要がないこと、簡単にシ

50

システムを拡大・縮小できること、更にそれぞれの組織LAN間を専用回線で接続しなくても良いため、専用回線費が不要となること、などである。

【0024】

しかし、一般的に閉鎖系LANに接続されたPCからは、インターネットに接続されたPCに対してメールの送受信を行うことはできない。これは、閉鎖系のネットワークが物理的に切り離されているので当然である。閉鎖系LANは、基本的にセキュリティを高めることを目的としているため、インターネット経由で情報の送受信を行う場合でもセキュリティを確保する必要がある。ネットワークで一般的に利用されているプロトコルは、TCP/IPであり、IP接続を基本とする以上、セキュリティを確保することは困難である。そこで本実施例では非IP接続による通信を採用している。

10

【0025】

図1に立ち戻って説明すると、必要な情報を電子メールの形(添付ファイルも含む)にし、A組織LAN側のメールサーバ14aとインターネット接続のメールサーバ16aを経て、インターネット経由で送受するように構成する。そして、A組織LAN側のメールサーバ14aとインターネット接続のメールサーバ16aとの間は、非IP接続(例えばRS-232CやIEEE1284(セントロニクス仕様)等:点線で示す)で行う。B組織LAN側も同様であり、メールサーバ14bとインターネット接続のメールサーバ16bを経て、インターネット経由で送受するように構成し、B組織LAN側のメールサーバ14bとインターネット接続のメールサーバ16bとの間は、非IP接続で行う。情報共有サーバ10a,10b間で共有情報の連携を行う場合は、このような経路で行う。一般情報を情報共有サーバ10a,10bから広報情報公開サーバ18に送る場合も、インターネット環境下のPC20から情報共有サーバ10a,10bに情報を送る場合も、同様である。閉鎖系LAN側のメールサーバ14a,14bとインターネット接続のメールサーバ16a,16bとの間での非IP通信により、閉鎖系LAN環境下のPCとインターネット環境下のPCとの間で安全に情報の送受が行えるようになる。

20

【0026】

閉鎖系のA組織LANからインターネット経由でB組織LANに至る共有情報の流れを図5に示す。A組織LANの情報共有サーバ10aの共有情報がメールサーバ14aに送られる。共有情報を受信したメールサーバ14aは、専用のメールソフトでメールサーバ16aに送信する。この送信は、前記のように非IP接続で行われる。メールサーバ16aは、受信メールをインターネット経由で発信し、メールサーバ16bにメールが着信する。メールを受信したメールサーバ16bは、B組織LANのメールサーバ14bにメールを送信する。この送信も非IP接続で行われる。情報共有サーバ10bは、B組織LANのメールサーバ14bに着信したメールを受信する。閉鎖系のB組織LANの情報共有サーバからインターネット経由でA組織LANの情報共有サーバに共有情報を送る場合も同様である。

30

【0027】

閉鎖系LANの情報共有サーバ10a,10bからインターネット接続の広報情報公開サーバ18への一般情報の流れ、インターネット接続のPC20から閉鎖系LANの情報共有サーバ10a,10bへの情報の流れ、及びインターネット接続のPC20から閉鎖系LANのPC12a,12bへの情報の流れも、基本的には同様である。

40

【0028】

情報共有サーバに蓄積する様々な情報には、複数のファイルを添付できる。添付ファイルは、必要に応じてパスワード付き圧縮ファイル(例えばZIPファイルなど)とすることができる。パスワード付加により暗号化した添付ファイルは、情報一覧表示画面においても他の添付ファイルとは異なったアイコンで表示されるようにし、ユーザが一目で暗号化された添付ファイルと認識できる仕組みとするのが好ましい。添付ファイルをパスワード付き圧縮ファイルにすると、その文が万一盗み見されても添付ファイルだけはパスワードがわからない限り見ることができないため、セキュリティを確保することができる。情報共有サーバに蓄積する様々な情報にファイルを添付する場合の処理フローを図6に示す

50

【 0 0 2 9 】

本発明では、情報に階層化の考え方を組み込んだことから、情報を複雑に管理することができるようになる。しかし、ユーザ側からみると複雑になったために使い難くなった面もある。その一つが情報の公開先の確認である。グループはともかく、組織や関係者というのは、どこを（誰を）指しているのか不明なことがある。この問題を解決するために、内部情報一覧表示画面において、表タイトルの「組織」や「関係者」にマウスを移動すると、半透明のウィンドウがポップアップし、そこにマウスで指した「組織」ないしは「関係者」がどこを（誰を）指しているのか一覧表示する仕組みを導入するのが好ましい。但し、この機能は、システムにログインする時に指定する事故情報にアクセス権限が割り振られている時に利用できるようにしている。

10

【 0 0 3 0 】

更に、情報共有サーバに蓄積されている情報を、ユーザが見易い、もしくは評価に利用できる形式で出力するための集計機能を組み込んでいる。この集計機能で出力することができる表としては、例えば全体時系列表や組織別時系列表がある。全体時系列表は、任意の事故名称に登録された情報を事実日時で昇順に並べ替えをして出力した表である。これは、全体の流れを見直すために便利な表である。それに対して組織別時系列表は、各組織が同じ時間帯にどのような動きをしていたのかを確認するために利用できる表である。この表は、縦軸に時間軸（例えば10分単位）、横軸を組織とし、それぞれの時間帯に各組織から入力された情報を出力して作成する。縦軸を単に時間とした場合は、ほぼ同じ時間帯に複数の事象が発生しないことから、1行に1情報しか入力されず、結果的に縦長の資料となり、全体の動きを追いかけるのに見易い資料とはなり得ない。そこで、縦軸を時間帯として幅を持たせたことにより、その時間帯に各組織において複数の動きがあることがわかり、全体の動きをより把握し易くなる。

20

【 0 0 3 1 】

集計結果の一例を図7に示す。これは、各組織が同じ時間帯にどのような動きをしていたのかを確認するために利用できる。任意の事故名称に対して、縦軸に時間軸（本例では10分単位）、横軸を組織とし、それぞれの時間帯に各組織から入力された情報を出力して作成する表形式のシートである。縦軸は、a)のように任意の時間間隔を設定でき、横軸は、b)のように組織を任意の順に並び替えることができる。また、事実事象に添付ファイルがある場合には、d)のようにハイパーリンクとして添付ファイルを簡単に見える仕組みとしている。添付ファイルは、WEBシステム同様ファイルの種類によりアイコン表示を行い、一見しただけでファイルの種類がわかるようにし、さらに、c)に示すように、1セル内に複数の添付ファイルをアイコン状態で横に並べることにより見やすさを確保している。

30

【 0 0 3 2 】

図8は、集計機能の具体的な処理手順を示したものである。まず、図示していないが、集計する対象の事故名称ほか、データベースの任意の出力したい項目を選択し、出力する事故名称テーブルの指定を行う（S1）。次に、指定した事故名称のデータを抽出し（S2）、抽出されたデータを指定された順に登録組織の並び替え（S3）、その登録組織単位に事実情報を集計し（S4）、その後、表形式の（例えばExcel：商品名）シートを作成し（S5）、事実情報を時間間隔毎にグループ化して表形式のシート上へ出力する（S6）。更に、各事実情報毎に添付ファイルの有無を確認し（S7）、添付ファイルが「あり」の場合には、所定の添付ファイルをデータベースからプログラムを実行しているPCにコピーし（S8）、ハイパーリンクを設定して（S9）、垂直、水平方向のポイント指定等のアイコンの位置補正を行なう（S10）。添付ファイルありの処理が終了あるいは添付ファイルがないときには、各事実情報の重要度に合わせて該当セルの背景色の色分けを行なう（S11）。このような処理を行なうことで、事故名称毎の事実情報収集表を作成することができる。

40

【 0 0 3 3 】

50

いずれにしても本発明の情報共有システムは、情報共有サーバに蓄積する様々な情報を階層化し、階層間で情報の格上げ/格下げを行える者を予め設定した特定の格上げ/格下げ権限者に制限するように構成しているため、複数の組織で共通の情報共有サーバを利用する場合でも、あるいは複数の組織にそれぞれ情報共有サーバを設置して互いに連携させて利用する場合であっても、様々な種類の情報を、セキュリティの確保や必要な情報の公開などを含めて個別に適切に管理することが可能となる。上記の実施例は最も簡単な2つの組織内LANの連携であるが、多数の組織内LAN間の情報連携も同様の手法で行えることは明らかである。複数の情報共有サーバで情報連携を行う場合、インターネット経由で電子メールの形式で行うのが好ましいが、専用回線を利用することも可能である。なお、本発明は緊急時における情報共有の他、日常的に複数の組織間で情報を共有したい場合にも適用できることは言うまでもない。

10

【図面の簡単な説明】

【0034】

【図1】本発明に係る情報共有システムの一例を示す構成図である。

【図2】情報共有サーバ内の情報蓄積構造の一例を示す説明図。

【図3】アクセス権限の設定状況を示す説明図。

【図4】ユーザセキュリティの自動設定の処理フロー図。

【図5】A組織LANからB組織LANに至る共有情報処理のフロー図。

【図6】情報共有サーバに蓄積する様々な情報にファイルを添付する場合の処理フロー図

20

。【図7】集計結果の一例を示す説明図。

【図8】集計機能の具体的な処理手順を示す説明図。

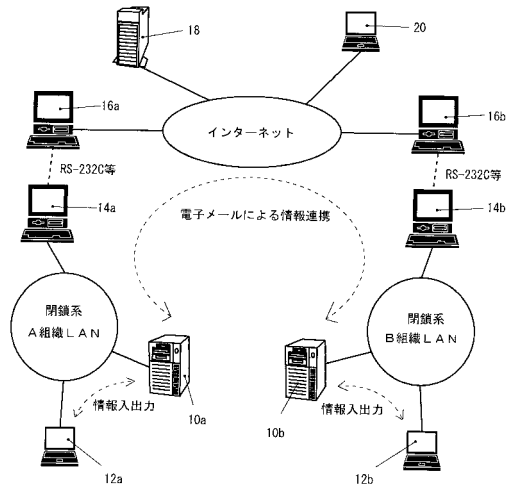
【符号の説明】

【0035】

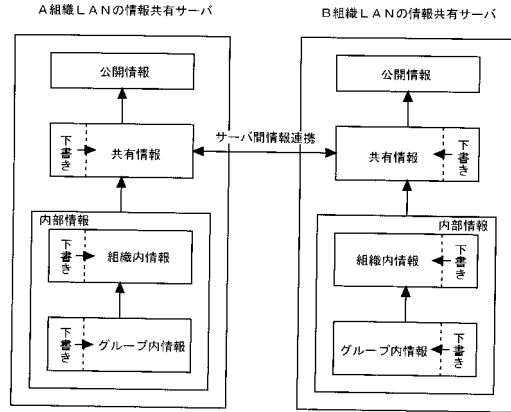
- 10 a , 10 b 情報共有サーバ
- 12 a , 12 b 閉鎖系LANのPC
- 14 a , 14 b 閉鎖系LAN側のメールサーバ
- 16 a , 16 b インターネット接続のメールサーバ
- 18 広報情報公開サーバ
- 20 インターネット接続のPC

30

【図1】



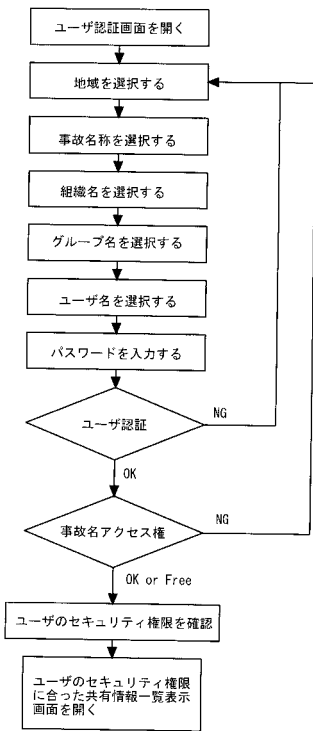
【図2】



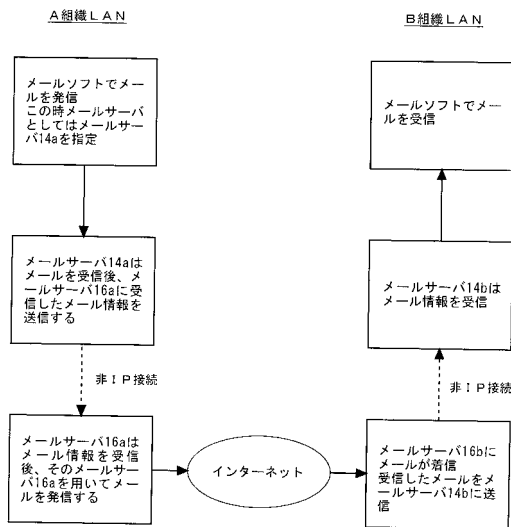
【図3】

アクセス権の設定	一般ユーザ権限	全てのユーザが閲覧可能
	一般情報	<input type="checkbox"/> 更新権限 (□下書き、□取り消し) <input type="checkbox"/> 閲覧権限のみ
	共有情報	<input type="checkbox"/> 更新権限 (□下書き、□取り消し) <input type="checkbox"/> 閲覧権限のみ
	内部情報	<input type="checkbox"/> 更新権限 (□下書き、□取り消し) <input type="checkbox"/> 閲覧権限のみ
	情報責任者権限	
	情報責任者	<input type="checkbox"/>
	サーバ間の情報連携権限	<input type="checkbox"/>
	情報の格上げ権限	<input type="checkbox"/> 一般情報 <input type="checkbox"/> 共有情報 <input type="checkbox"/> 組織内情報 <input type="checkbox"/> グループ内情報
管理者権限		
システム管理者	<input type="checkbox"/>	

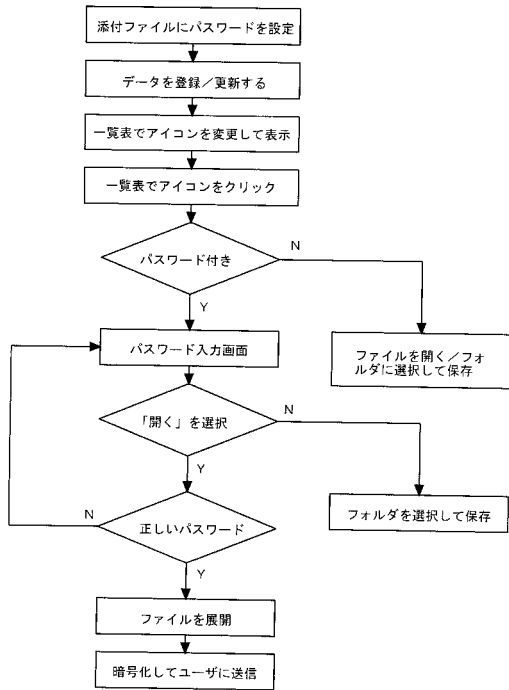
【図4】



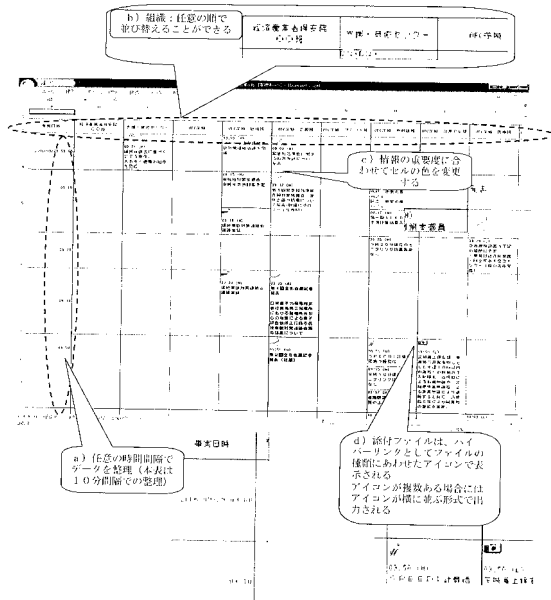
【図5】



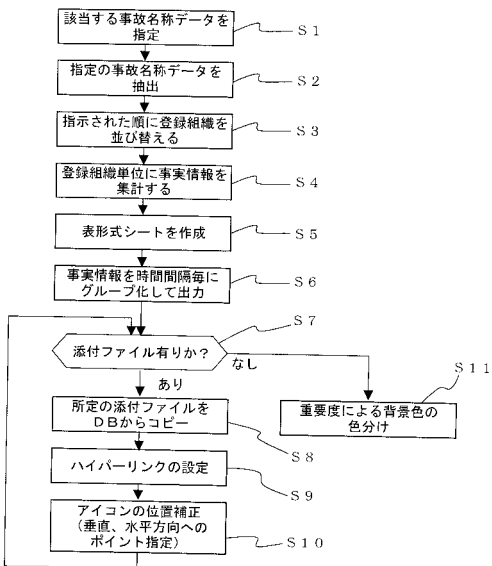
【図6】



【図7】



【図8】



フロントページの続き

- (72)発明者 山本 一也
茨城県那珂郡東海村村松4番地49 独立行政法人日本原子力研究開発機構本部 原子力緊急時支援・研修センター内
- (72)発明者 佐治木 健二郎
茨城県那珂郡東海村村松4番地49 独立行政法人日本原子力研究開発機構本部 原子力緊急時支援・研修センター内
- (72)発明者 安 貞憲
茨城県ひたちなか市新光町38 ひたちなかテクノセンター4階 株式会社NESI情報システムセンター内
- (72)発明者 竹内 義人
茨城県ひたちなか市新光町38 ひたちなかテクノセンター4階 株式会社NESI情報システムセンター内
- (72)発明者 平山 勇一
茨城県ひたちなか市新光町38 ひたちなかテクノセンター4階 株式会社NESI情報システムセンター内

審査官 田付 徳雄

- (56)参考文献 特開2004-318034(JP,A)
特開2002-269094(JP,A)
特開2005-327081(JP,A)
特開2004-246537(JP,A)
特開2007-034447(JP,A)
関正秀, ブログのビジネス活用 どこまで使えるか・どこまで安全か?, N+I NETWORK K, 日本, ソフトバンクパブリッシング株式会社, 2005年 3月 1日, 第5巻, 第3号, 第54-61頁

(58)調査した分野(Int.Cl., DB名)

G06Q 10/00 - 50/00
G06F 21/24