

表4-2 選択肢について

全項目が重要(問題作成の注意事項に入れるべき)(6名)

ナンセンス肢はないか(4名)

選択肢の長さは適当か

正解を明確に選択できるか(「明らかに最も正しい選択肢」があるか)

統一された疾患名が記載されているか(全大学・学会でのコンセンサスが望ましい)

1つのテーマに集約されているか

選択肢の領域(範疇)が広範囲にまたがっていないか

文章は簡潔明瞭か

無関係な選択肢が入っていませんか

文法的統一性のない選択肢や使用法の誤りを自動的にチェックできるシステムを

「～ことがある」表現の回避

二重否定になっていないこと

選択肢の文字数の制限(超えると自動的に記入不可にする)

表4-3 視覚素材について

講義、論文、講演、シンポジウムなどに使われていないか(2名)	
いずれも重要な項目 順位付けの意図が不明	
視覚素材が不足していないか	
病理写真では染色名を入れる	
矢印や倍率等を画面上に記入する	
同一の視覚素材の過去の使用および今後の使用予定は無いか	
個人情報保護のマスキング(目など)も顔面写真のポイントに入れる	
口腔内所見とX線写真の所見が一致するか	
ファイル形式(JPEG含む)、解像度(dpi、1000 x 800)などデジタルなのは具体的なガイドラインを入れる	
『角度』の項目が理解不能	
ミラー像か否か	
設問に対して、視覚素材は不可欠か	
出題の意図が情報として明確か	
焦点・明るさ・大きさ・天地表裏・中心を一つに 画像サイズを1通りのみに限定	
焦点・明るさ・色調・コントラストは当然と思われるが、チェック項目に必要かは疑問	

別添4

厚生労働科学研究費補助金(医療技術評価総合研究事業)
分担研究報告書

システム構成とセキュリティについての検討

分担研究者 小口春久 日本歯科大学共同利用研究センター 教授

研究要旨

医師・歯科医師国家試験のプール制(試験問題をあらかじめ蓄えておく方式)の早期実現を図るために、全国の委員が作成した試験問題を効率よく集約する方法、特にインターネットを利用した集約方法を模索することを目的とした。

まず、インターネットを介して試験問題を送る際のシステム設計を行った。次に、インターネットを使用する際に常に問題とされる情報漏洩についてのセキュリティについて検討した。新システムにおける処理の流れは以下の通りとなった。①問題作成者がサーバーにログインする。②入力ソフトウェアを自分のコンピュータにダウンロードする。③問題を作成する。④入力した問題(データ)をサーバーにアップロードする。⑤サーバーに登録された問題を取り出し、データベース化する。また、本システムでは、ネットワークセキュリティを確保するため、厚生労働省既設ファイアウォールを利用して、インターネットに接続されたインターネットセグメント、問題登録サーバーを接続するDMZ(非武装地帯)セグメントと管理端末を接続しているDBセグメントの3つのセグメントで構成することとした。

A システムについて

1 機能概要

本システムの利用者は、その利用権限により問題作成者、管理者の2つに分類され、利用できる機能が制限される。

前述2つの利用権限のうち、問題作成者、管理者については、あらかじめ設定されているユーザーIDとパスワードによる認証(ログイン)を行うことにより、該当するユーザーであることを認

証する。ユーザーIDはシステムに設定しているユーザーID、パスワード及び権限に準じて実行される。本システムはユーザーIDを持たない一般ユーザーは利用できないこととする。

機能別に利用者権限を示すと以下の通りとなる。

(問題作成者向け機能)

(1)ログイン機能

問題作成者向け機能にアクセスする

ためのログイン機能。ユーザーID、パスワードを認証する。ユーザー登録機能で問題作成者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。

(2)機能選択機能

問題作成者向け機能を選択する機能。機能選択、問題入力ソフトウェアのダウンロードを行う。

(3)登録問題一覧機能

登録されている問題データを一覧表示する機能。登録済みの問題データの確認、削除を行う。

(4)問題登録機能

問題入力ソフトウェアで作成した問題データをアップロードする機能。

(管理者向け機能)

(1)ログイン機能

管理者向け機能にアクセスするためのログイン機能。

ユーザーID、パスワードを認証する。ユーザー登録機能で管理者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。

(2)機能選択機能

管理者向け機能を選択する機能

(3)ユーザーID一覧機能

登録されているユーザーIDの一覧を表示する機能。ユーザーIDの確認、新規作成、編集を選択することができる。

(4)ユーザー登録機能

ユーザーIDの新規作成、更新時、ユーザーの詳細情報を編集、登録する機能。

(5)登録データの取得機能

登録されているデータを取得する機能。管理端末よりアクセスする。(フリーウェア等のファイル転送ソフトの利用となるので、機能、画面は利用されるファイル転送ソフトに依存する。)

2 ハードウェア性能・容量

ハードウェアとしては、CPU(Celeron D2.53GHzx1 256KB L2以上)、メモリ(1GBメモリ以上)、ディスク(80GB)を必要とする。

3 問題登録アプリケーション性能

ログイン性能は問題作成者200名が1日(8時間)ログインしたと仮定し、0.5件/分以上のログインアクセスを可能とした。1ファイルのアップロードサイズは4MBまでとした。

4 起動方法

本システムは<https://dkoubo.newpass.jp>のURLより起動する。本システムはあらかじめ設定されているユーザーIDとパスワードによる認証を経てユーザーIDに対応した利用者の利用者権限により該当するトップページへと遷移し、機能を利用することが可能となる。

5 処理の流れ

本システムにおける処理の流れを図1に示す。公募問題入力ソフトウェアは問題登録サーバーからダウンロードし問題を作成する。問題作成結果の入力データはインターネット上の問題登録サーバーにて登録する。

6 システム構造の概要

本システムの概要を図2に示す。ファイアウォールを通った情報が問題登録サーバーに送られる。サーバーには各種アプリケーション(現在検討中)、サーバー証明書、データベース、サーバーソフトウェアが搭載されている。

B セキュリティ

1 セキュリティシステムの内容

セキュリティシステムのハードウェア構成を図3に示す。本システムでは、ネットワークセキュリティを確保するため厚生労働省既設ファイアウォールを利用して、①インターネットに接続されたインターネットセグメント、②問題登録サーバーを接続するDMZ(非武装地帯)セグメントと③管理端末を接続しているDBセグメントの3つのセグメントで構成した。基本的なセグメント間通信の考え方は次の通りである。

- (1) ファイアウォールで、不要な通信を可能な限り遮断する。
- (2) 通信可能な方向を決める。
インターネットセグメントからDMZセグメントへの通信、DMZセグメントからDBセグメントへの通信を許すが、インターネットセグメントからDBセグメントへの直接通信は許さない。インターネットセグメントからDBセグメントへ通信する場合は、必ずDMZセグメントを経由して通信する必要がある。
- (3) それぞれのセグメント間で通信が可能なプロトコルを制限する。各セグメント間で可能な通信プロトコルを最小限にする。
- (4) セグメント間を流れる通信は、プロトコル毎に発信可能なサーバーと受信可能なサーバーを制限する。

通常、各サーバーは想定されるプロトコルに対する防御は強いが、想定外のプロトコルに対する通信には防御が弱いいため可能な限りファイアウォールで不要なプロトコルを流さなくする様にした。

2. システム監視機構

本システムは、インターネットに公開するシステムであるため、安定かつ安全な運用を実現するため、次のシステム監視支援の機構を設ける。

1)改ざん検証

Tripwireを導入し、システムファイルの改ざんをチェックする。

2)ディスク監視

logwatchを導入し、ディスク容量をチェックする。

3)Syslog監視

Syslog監視を行うためのswatchを導入し、システムエラーをチェックする。

4)エラーログ監視

エラーログ監視を行うためのswatchを導入し、システムエラーをチェックする。

5)バックアップ

週1回データベース、登録ファイルのバックアップをサーバーのバックアップディレクトリにバックアップする。

2 セキュリティについての課題

セキュリティに関しては、サーバー機器、

開発アプリケーションに関わるソフトウェア的な脆弱性に関する処置、確認試験については、三菱電機に委託する。しかし、システムの運用時における登録データ(問題入力データ、ユーザーID、パスワード)の管理に関してはユーザー側の責任となる。

現段階で最も心配されるのは、問題作成委員が自分のパーソナルコンピュータのハードディスクに問題を一時的に保存した場合のセキュリティをどうするかという点である。これについては、①個人で徹底的に管理してもらい、②リアルタイムでデータを逐次送信してハードディスクには残らないシステムにする、などの対処が考えられるが、今後の検討課題としたい。

図1 処理の流れ

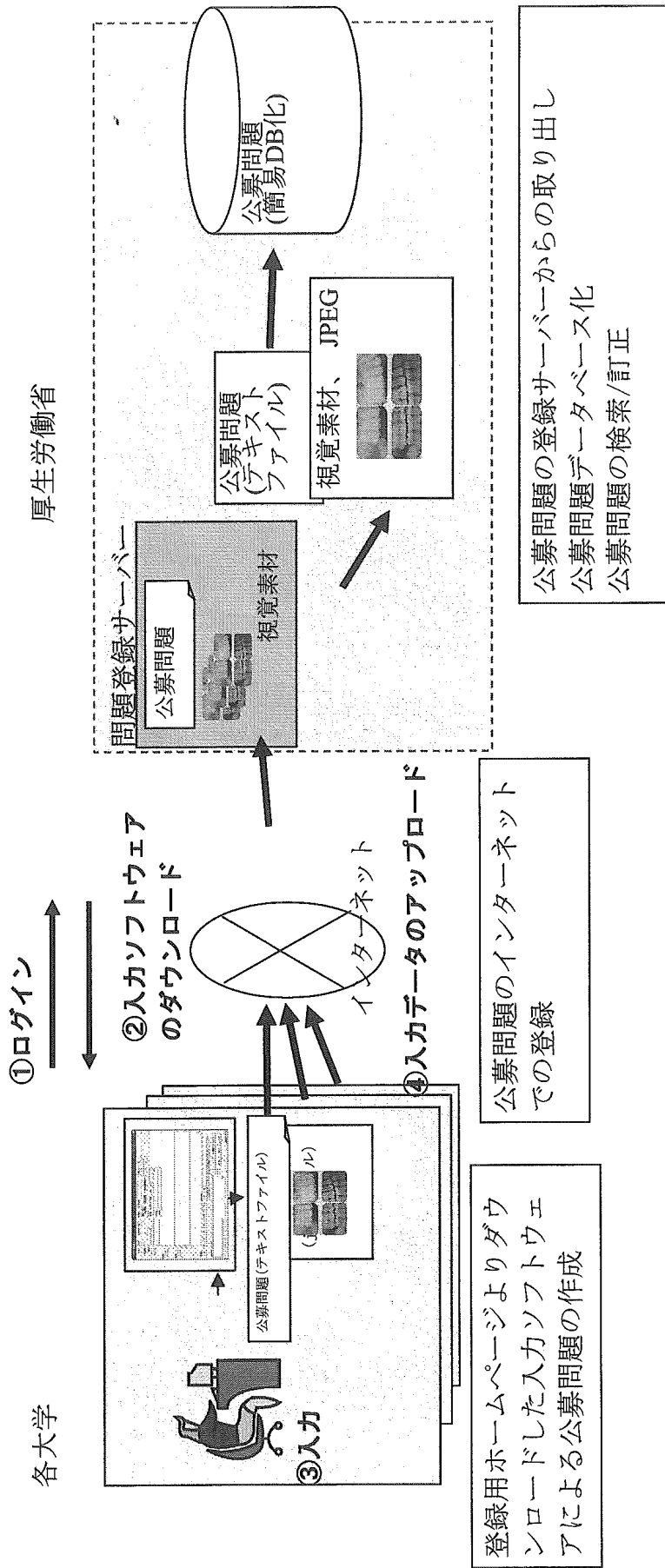


図2 システム構造概要図

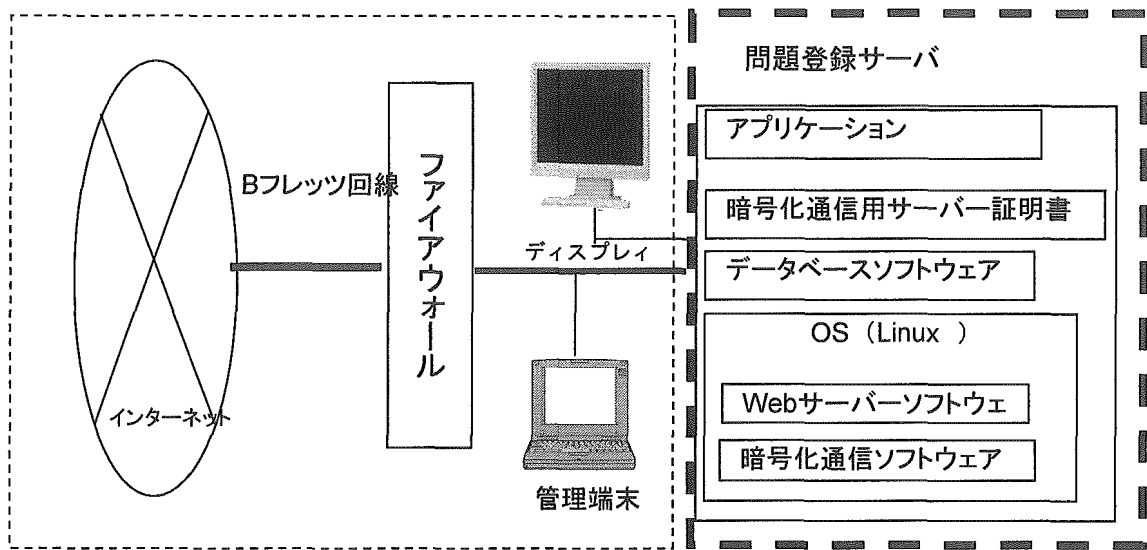
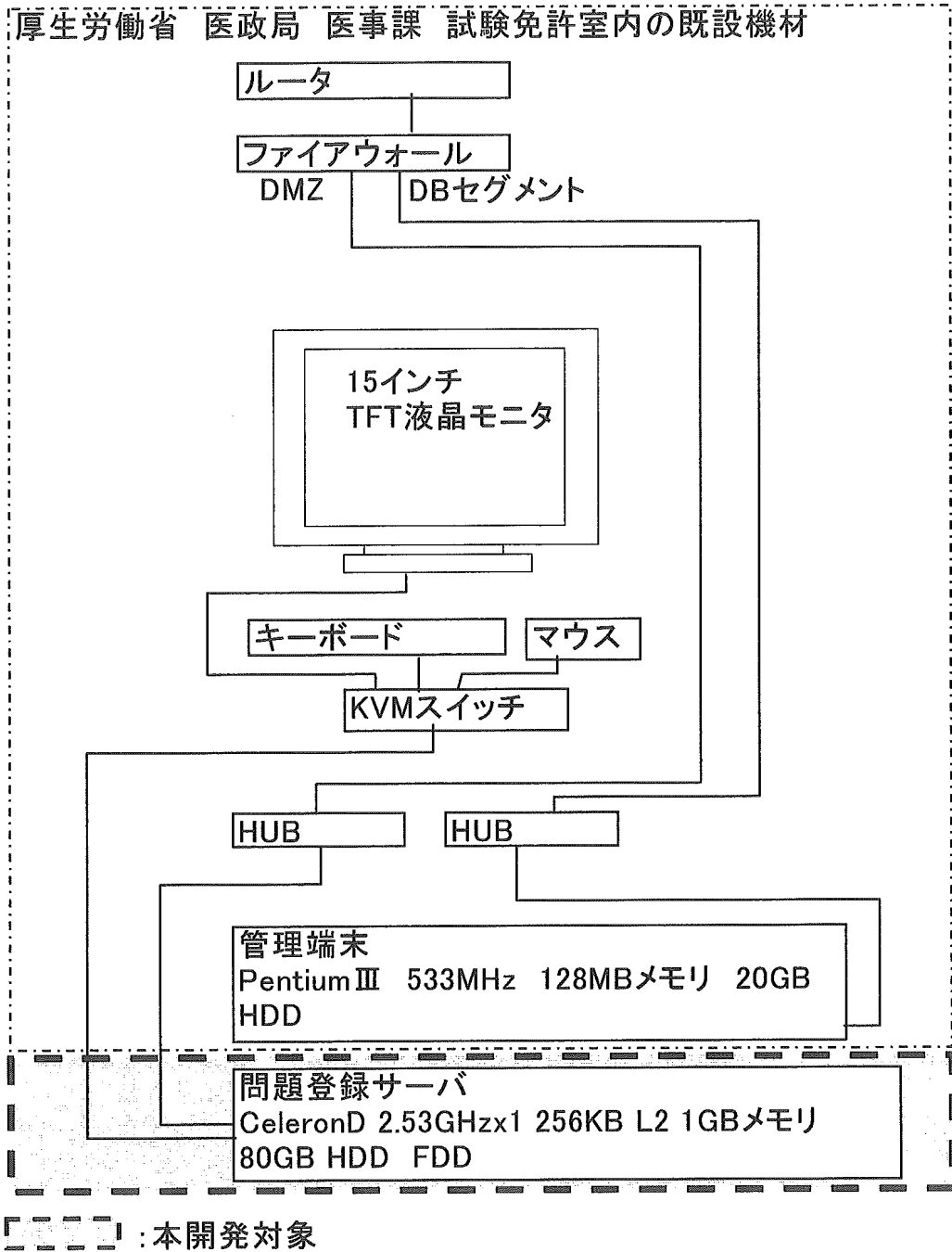


図3 ハードウェア構成図



厚生労働科学研究費補助金(医療技術評価総合研究事業)

分担研究報告書

入力画面のデザインと確認メッセージの検討

久光 久

分担研究者 昭和大学歯学部 齶蝕・歯内治療学講座 教授

研究要旨

医師・歯科医師国家試験のプール制(試験問題をあらかじめ蓄えておく方式)の早期実現を図るために、全国の委員が作成した試験問題を効率よく集約する方法、特にインターネットを利用した集約方法を模索することを目的とした。

まず、インターネットを介して試験問題を送るための、ハード面におけるシステム整備と画面設定を検討した。

入力の際の各画面については、可及的に使いやすく、混乱の生じないように考慮した。今後は、試験委員から提出されたチェックリスト項目をどのように画面に挿入するか、また、複数の視覚素材を必要とする問題の送付方法の改良が課題である。

A 各画面の詳細

各画面の構成を表1と図1に示す。

1. 問題作成者向け画面

1)ログイン画面

問題作成者向け機能にアクセスするためのログイン画面。ユーザー登録機能で問題作成者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。

表示項目は、タイトル、ユーザーID、パスワード、ログインボタンである。

ログインボタン：問題作成者として登録したユーザーID、パスワードが入力された場合のみ(Ss1) 機能選択画面へ遷移する。

2)機能選択画面

問題作成者向け機能を選択する画面。選択機能と問題入力ソフトウェアのダウンロードのリンクが有る。

表示項目はタイトル、登録問題一覧画面、問題登録画面、入力ソフトウェアダウンロード、戻るボタン、ログアウト、操作マニュアルである。

3)登録問題一覧画面

ログインした問題作成者が自分で登録した問題入力データの一覧を表示する画面。登録済みの問題入力データの確認、削除が行える。

管理者によって、ユーザーIDを変更された場合は、前回のユーザーIDで登録したデータの一覧は表示されない。

管理者が登録データ取得機能にて、データの削除を行った場合は、削除されたデータは表示されない。

表示項目はタイトル、登録ファイル名、コメント、操作マニュアル、ログアウトボタン、戻るボタン、削除ボタン、問題登録画面である。

4)問題登録画面

問題入力ソフトウェアで作成した問題データをアップロードする画面。参照で指定できるファイルは1ファイルである。送信できるファイルは1回に1ファイルである。コメントの選択は必須である。送信されたファイルはサーバー上にユーザー毎にディレクトリ分けされ保存される。

表示項目はタイトル、送信データ添付コメント、問題文、視覚素材、問題番号視覚素材種別、参照、送信、戻る、ログアウト、操作マニュアル、登録問題一覧画面である。

2. 管理者向け画面

1)ログイン画面

問題作成者向け機能にアクセスするためのログイン画面。ユーザー登録機能で問題作成者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。管理者用のログイン画面は問題作成者向けの画面とは別URLで起動する。

表示項目はタイトル、ユーザーID、パスワード、ログインボタンである。

2)機能選択画面

管理者向け機能を選択する画面である。

表示項目はタイトル、ユーザーID一覧画面、戻るボタン、ログアウトボタンである。

3)ユーザーID 一覧画面

登録されているユーザーIDの一覧を表示する画面。ユーザーIDの新規作成、編集を選択できる。

表示項目は、タイトル、ユーザーID、パスワード、委員名、グループ番号、委員番号、有効期限、権限、備考、編集ボタン、新規ボタン、削除ボタン、ログアウトボタン、戻るボタンである。

4)ユーザー登録画面

ユーザーIDの新規作成、更新時、ユーザーの詳細情報を編集、登録する画面である。

表示項目はタイトル、ユーザーID、パスワード、グループ番号、委員番号、委員名、有効期限、権限、備考、登録ボタン、キャンセルボタン、ログアウトボタンである。

5)登録データの取得画面

登録されているデータを取得する画面。本画面は管理端末にインストールされたフリーウェア等のファイル転送ソフトの画面となる。開発ソフトウェアではないため、画面の変更はできない。(利用するファイル転送ソフトウェアに依存する。)

表示項目(例)としては、ファイル転送ソフト「FFFTP」を利用の場合、A:管理端末のハードディスク内と B:問題登録サーバー内の登録ファイル一覧である。

B 確認メッセージ

各画面での操作に誤りがある場合や、入力方法に誤りがある場合にはエラーメッセージが自動的に送信される。メッセージの一覧を表2に示す。

C 今後の課題

問題登録一覧画面で示されているが、一つの問題に、本文(テキストファイル)と数個の視覚素材(JPEGファイル)とが含まれる場合、それぞれにファイルを分けて送らなくてはならない。今後の課題としては、それら数個のファイルを1つのファイルとしてまとめて、かつ試験で実際に出題された場合をシミュレートできる(一つの画面で全ての情報が視覚的に分る)システムを付加する必要がある。

表1 画面一覧

1.問題作成者向け画面 【権限：問題作成者】

画面番号	画面名	画面概要
Sg1	ログイン画面	問題作成者向け機能にアクセスするためのログイン画面。ユーザー登録機能で問題作成者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。
Ss1	機能選択画面	問題作成者向け機能を選択する画面。 選択機能と問題入力ソフトウェアのダウンロードのリンクが有る。
S11	登録問題一覧画面	登録されている問題データを一覧表示する画面。 登録済みの問題データの確認、削除が行える。
Su1	問題登録画面	問題入力ソフトウェアで作成した問題データをアップロードする画面。

2. 管理者向け画面 【権限：管理者】

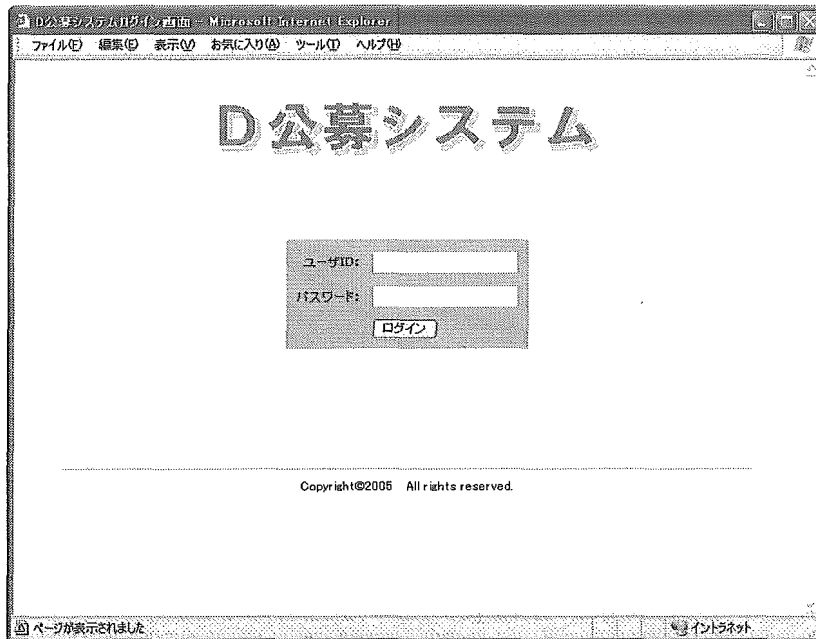
画面番号	画面名	画面概要
Klg1	ログイン画面	管理者向け機能にアクセスするためのログイン画面。 ユーザー登録機能で管理者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。
Ks1	機能選択画面	管理者向け機能を選択する画面。
K11	ユーザーID一覧画面	登録されているユーザーIDの一覧を表示する画面。ユーザーIDの新規作成、編集を選択することができる。
Ku1	ユーザー登録画面	ユーザーIDの新規作成、更新時、ユーザーの詳細情報を編集、登録する画面。
—	登録データの取得画面	登録されたデータを取得する画面。管理端末上で起動する。(フリーウェア等ファイル転送ソフトの利用となるので、画面は利用されるファイル転送ソフトに依存する。)

図1 画面詳細

(1) 問題作成者向け画面、【権限：問題作成者】

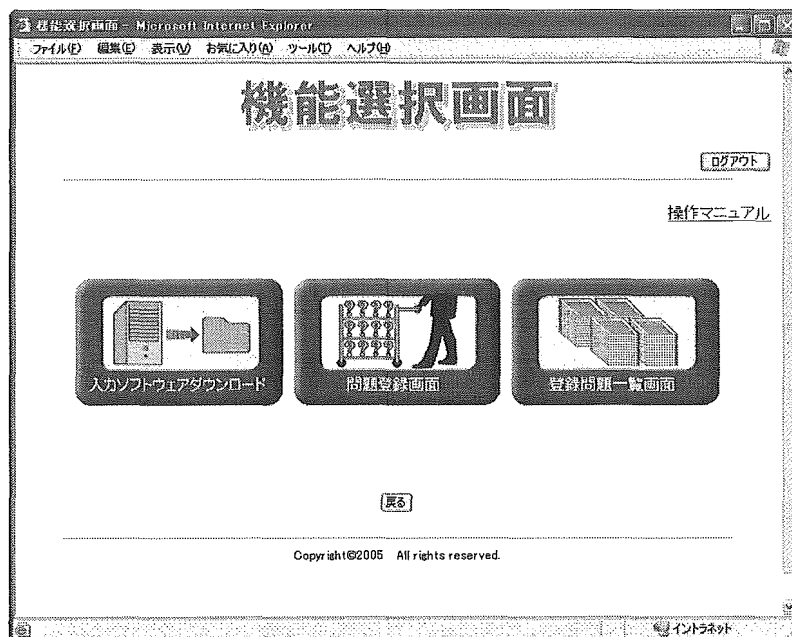
(S1g1)ログイン画面

問題作成者向け機能にアクセスするためのログイン画面。ユーザー登録機能で問題作成者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。



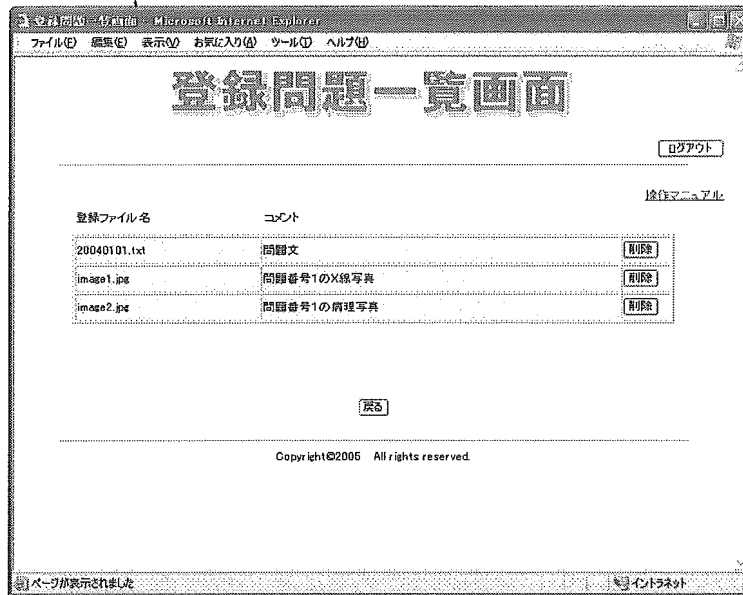
(Ss1)機能選択画面

問題作成者向け機能を選択する画面。選択機能と問題入力ソフトウェアのダウンロードのリンクが有る。



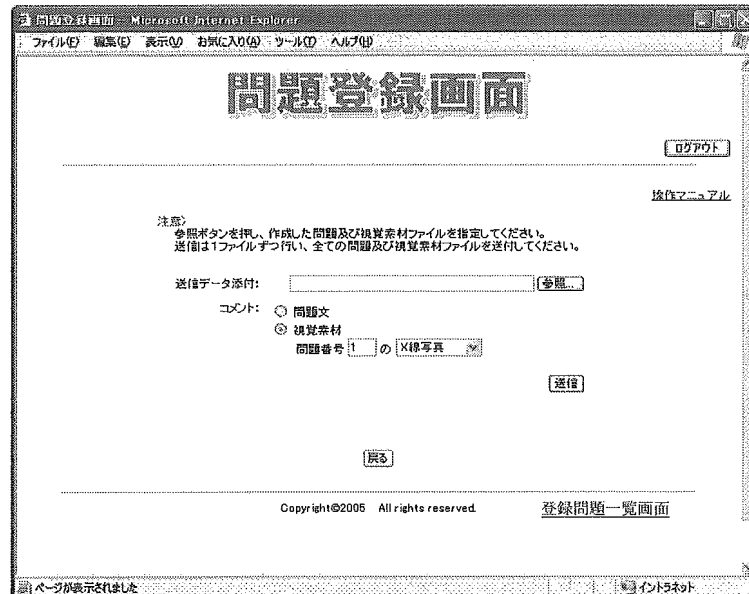
(S11)登録問題一覧画面

ログインした問題作成者が自分で登録した問題入力データの一覧を表示する画面。登録済みの問題入力データの確認、削除が行える。



(Su1)問題登録画面

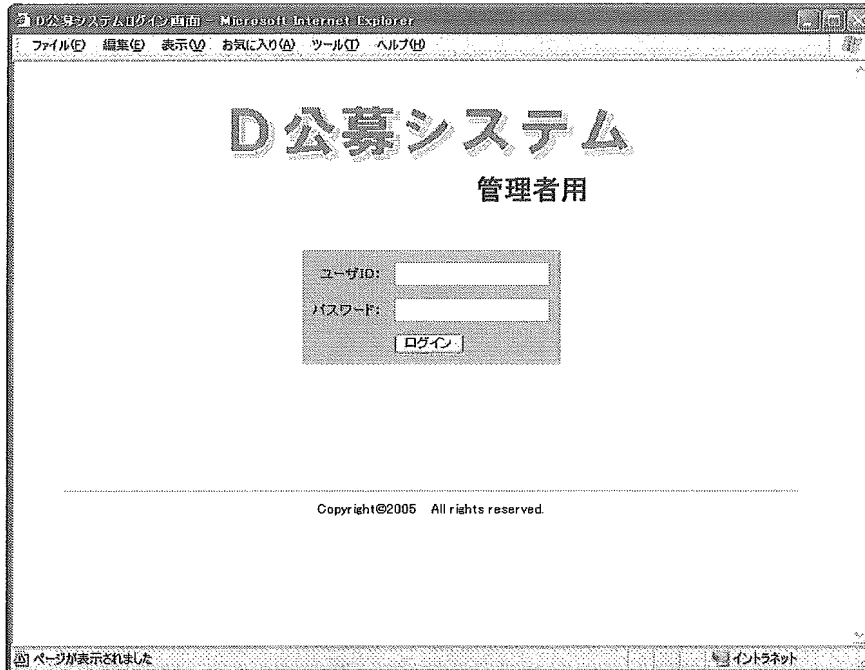
問題入力ソフトウェアで作成した問題データをアップロードする画面。参照で指定できるファイルは1ファイルである。送信できるファイルは1回に1ファイルである。コメントの選択は必須である。送信されたファイルはサーバー上にユーザー毎にディレクトリ分けされ保存される。



(2)管理者向け画面 【権限：管理者】

(Klg1)ログイン画面

問題作成者向け機能にアクセスするためのログイン画面。ユーザー登録機能で問題作成者として登録したユーザーID、パスワードが入力された場合のみ、次画面に遷移する。管理者用のログイン画面は問題作成者向けの画面とは別URLで起動する。



(Ks1)機能選択画面

管理者向け機能を選択する画面。



(K11)ユーザーID一覧画面

登録されているユーザーIDの一覧を表示する画面。ユーザーIDの新規作成、編集を選択できる。

ユーザーID	パスワード	委員名	グループ番号	委員番号	権限	有効期限	備考	新規
1 ID2	Password1	ユーザ名1	01	01	管理者	2005/03/31		<input type="button" value="編集"/> <input type="button" value="削除"/>
2 ID2	Password2	ユーザ名2	01	02	問題作成者	2005/03/31		<input type="button" value="編集"/> <input type="button" value="削除"/>
3 ...	Password3	ユーザ名3	01	03	問題作成者	2005/03/31		<input type="button" value="編集"/> <input type="button" value="削除"/>

(K11)ユーザー登録画面

ユーザーIDの新規作成、更新時、ユーザーの詳細情報を編集、登録する画面。

ユーザーID :

パスワード :

グループ番号 :

委員番号 :

委員名 : 山本 太郎

権限 :

有効期限 : 2005 / 03 / 31

備考 : 厚生労働省

登録データの取得画面

登録されているデータを取得する画面。本画面は管理端末にインストールされたフリーウェア等のファイル転送ソフトの画面となる。開発ソフトウェアではないため、画面の変更はできない。利用するファイル転送ソフトウェアに依存する。

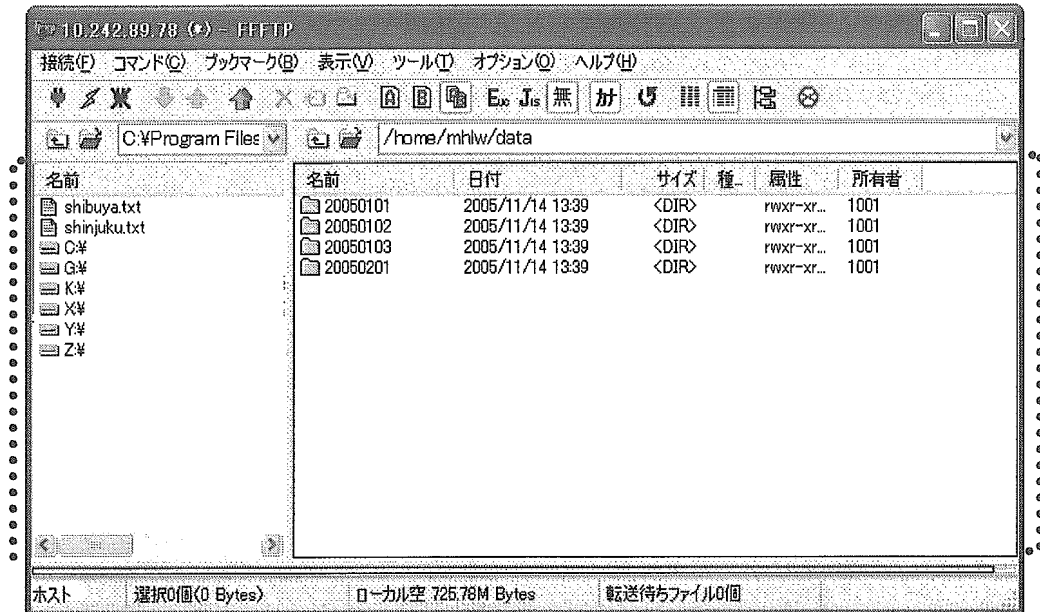


表2 確認メッセージ

(1) 問題作成者向け画面 【権限:問題作成者】

(Slg1)ログイン画面 入力エラーメッセージ
ユーザーIDまたはパスワードが違います。再度正しいユーザーID、パスワードを入力し、ログインしてください。 <ul style="list-style-type: none"> ・大文字、小文字に誤りはありませんか？ ・入力は半角英数で入力してください。

(Sll)登録問題一覧画面 確認メッセージ
登録ファイルを削除します。よろしいですか？

(Su1)問題登録画面 エラーメッセージ
送信ファイルを指定してください。

(2) 管理者向け画面 【権限:管理者】

(Klg1)ログイン画面 入力エラーメッセージ
ユーザーIDまたはパスワードが違います。再度正しいユーザーID、パスワードを入力し、ログインしてください。 <ul style="list-style-type: none"> ・大文字、小文字に誤りはありませんか？ ・入力は半角英数で入力してください。

(Kll)ユーザーID一覧画面 確認メッセージ
登録ファイルを削除します。よろしいですか？

(Kul)ユーザー登録画面 入力エラーメッセージ
ユーザーIDは入力必須です。
パスワードは入力必須です。
グループ番号は入力必須です。
委員番号は入力必須です。
委員名は入力必須です。
権限は入力必須です。
ユーザーIDは半角10文字以内で入力して下さい。
パスワードは半角16文字以内で入力して下さい。
有効期限は日付として適切ではありません。
備考は128文字以内で入力して下さい