セキュリティを強化した大規模大学向け健康診断システムの開発と評価

藤井　香*　大貫　亮**　齋藤　圭美*
久根木康子*　松本　可愛*　高橋　綾*
清　奈帆美*　小原　佐之*　櫻井　勉*
多川　実佳**　金子　康樹**　押見　淳**
河邊　博史*　齊藤　郁夫*

当大学における旧健康診断システムは，リレーショナルデータベースソフトであるファイルメーカー（FileMaker, Inc.）を中心としたシステム仕様であった。旧システムは，ユーザーである保健師自身でプログラム改修ができ，基準値変更や帳票レイアウトなど多様なニーズに応じた改修が容易であり，また保守費用がライセンス料のみであるため，1990年から2010年までの20年間に渡り，改修と更新を繰り返し利用してきた。しかし，近年，利便性がある反面，下記の問題が生じていた。

1．専門の開発者およびシステム担当者が部署に不在であり，経験や技術のある数人の保健師に改修を依存する状況であるため，職務上の業務分担やセキュリティの確保が困難な状況になってきた。
2．システムへのアクセス者すべてが，直接のデータ編集などシステム内部まで操作できる仕様であり，不備データの投入などのチェック機能が薄いため，年度毎にデータベース保有の項目差異が発生し，データ精度上の問題が生じていた。同時に，システムへのアクセスは共通のパスワードを用いた運用であり，操作者を特定できないという問題もあった。
3．基本情報となる個人情報など，他部署とのデータ交換作業がファイルベースで行われ，データ準備作業に時間がかかるだけでなく，セキュリティ上の問題があった。
4．同一ファイルでの複数年複数レコード管理であり，データ容量が年々増加してしまうことで，バックアップ方法などデータ保管上の運用管理面での問題が生じていた。
5．複数年度，複数回のレコードを維持した構成のため，年度単位でデータ抽出することが難しく，年度毎のバックアップ作業や，年度単位での検査項目や基準値の変更が複雑化していた。過去の書類の再発行や基準値に影響がでることがあり，管理上の問題があった。

そこで，これらの問題，特にセキュリティの強化を目的とした大規模大学向け健康診断シ

* 慶應義塾大学保健管理センター　** 慶應義塾インフォメーションテクノロジーセンター

ステム（IDST：Information and Database of health care Service Tools）を構築し，アプリケーションを実装化したので評価したい。

成　　績

1．システム評価

セキュリティ強化については，ハードウェア，ソフトウェア（アプリケーションの実体，機能），およびデータそのものを対象として設計，構築を行い，約40,000件の学生データを対象に学内基幹データベースとのシームレスな連携[1)]を行った。

1）システム形態

クライアントサーバ型システム，一部WEBサービス（健康診断結果）を展開した。

2）サーバ構成

業務用基幹システムとして統一した環境で構築されているサーバを利用，大学学事システム他と同様のマシン上で稼働させた。

a）ハードウェア

IBM eServer p5 -595（9119-595）

LPAR（Logical Partition）を利用し，CPU x4，メモリ4 GBを割り当てた。

b）OS／ミドルウェア

サーバOSとしてAIX（日本アイ・ビー・エム株式会社）を利用した。さらに，その上でリレーショナルデータベース管理システムであるDB2（日本アイ・ビー・エム株式会社）を利用した。

c）データ蓄積と管理方法における改善点

当年度及び過去6年分を保持し，それより以前のデータについては年度更新処理としてバックアップ領域にて保存した。バックアップ領域はアプリケーションからの参照不可に制限をした。

d）バックアップ方法における改善点

アプリケーションとデータの分離を実装し，データの精度とセキュリティの確保を計った。ADON及びTSM（日本アイ・ビー・エム株式会社）を利用し，毎日夜間の自動取得と70世代を保持するよう設定した。

e）災害対策

本番マシンとは別に災害対策用のマシンを別の建屋に用意し，データについては，非同期（1日遅れ）で本番マシンから転送する仕組みを設けた。

3）クライアント構成

業務用PCとして共通化された基礎構成に加えて，保健管理業務用に特化した専用PCを利用し，使用制限を設けた。アプリケーションについては，専用PC上でのみ利用可能とし，さらに機能レベルでの権限設定を設けることで使用制限によるセキュリティ強化を図った。

a）ハードウェア

富士通 FMV-BIBLO NF/A55(スペック：Core i5，メモリ4 GB)

b）OS／ソフトウェア

クライアントOSとしてWindows7（32bit）（日本マイクロソフト株式会社），実行モジュールとしてVisual Basic6.0（日本マイクロソフト株式会社）で開発したEXE形式のアプリケーションを利用した。また帳票・テンプレートにはOffice2010（日本マイクロソフト株式会社）を利用した。

4）ネットワーク環境

（図1 Keio Intercampus Network）

a）業務用LAN（有線）ネットワークを利用した。WEBサービス用には別途グローバルネットワークを利用，一部地区にてRIS（Radiology Information System）用ネットワークとの健診時にデータ連携する仕様とした。複数地区同時での健診実施および事後処理を想定したパフォーマンスのテストを行い，実装した。

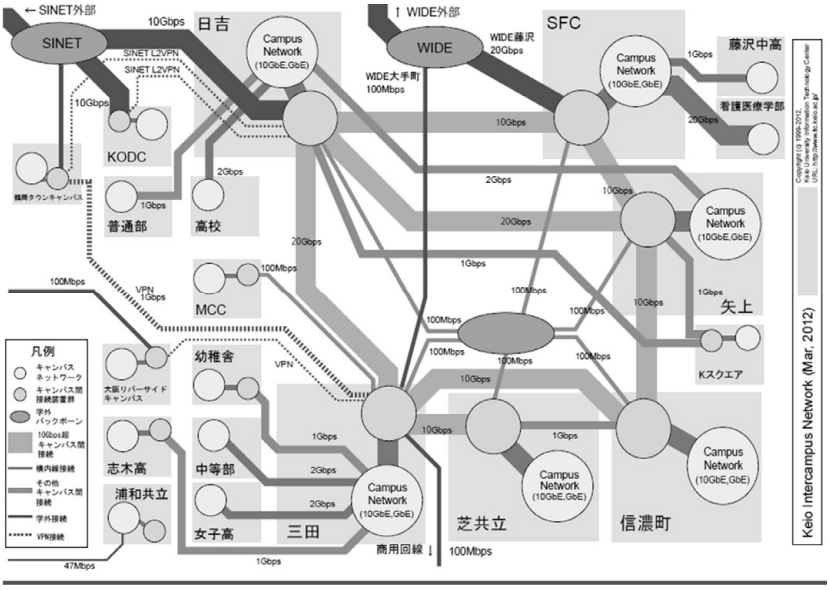

図 1　Keio Intercampus Network

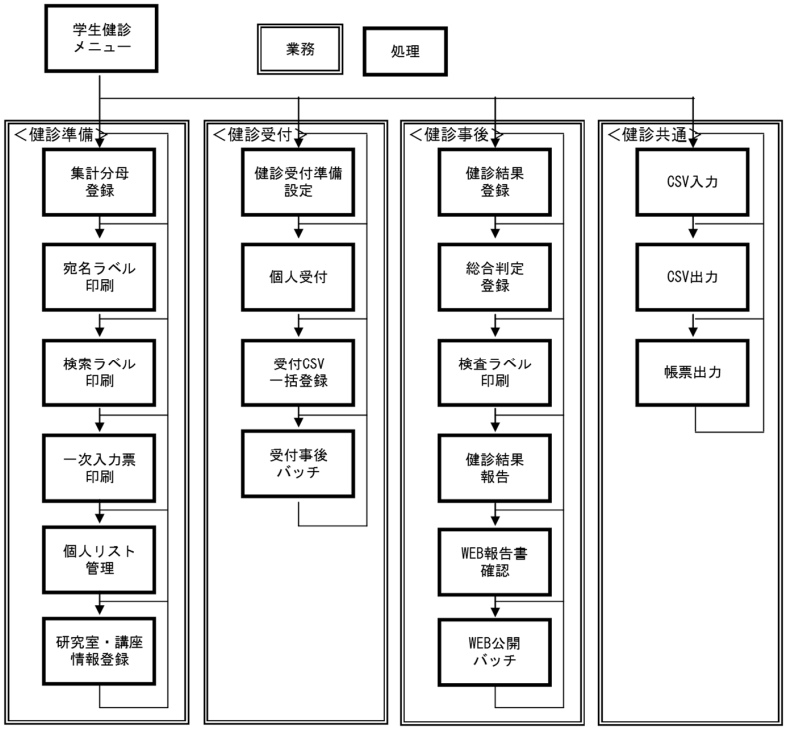

図 2　業務，処理フロー

b）セキュリティ対策

ファイアウォールでのネットワーク制限，アカウント管理（サーバ／クライアント双方）による認証，クライアント PC への Antivirus ソフトの導入を行った。

2．業務，処理フローの整理（図 2）

学生健診，教職員健診，特定業務従事者健診，雇入時健診の業務，処理フローを統一化し，操作ミスを防止した。また，単年度管理をベースにしたデータベースの設計とアプリケー

ションレベルでの機能実装により，年度または検査種類でのデータを検索，抽出することが可能となった。また，健診種類別に単年度ベースでの複数年度にわたる健診データの管理が可能となったことに加え，年度ごとの基準値や帳票レイアウトの保持も可能となった。

3．キャンパス内複数システムとの情報共有化（図 3）

保健管理センターは，人事部，学生部が主管部署である個人属性データを利用しており，旧システムでは手作業が多く，操作ミスもみられた。今回のシステムでは，学内基幹サーバを利用し，アプリケーションとデータの分離により，基幹サーバ内の学事データベース上の学生データとの連携が可能となった。これにより，更新するタイミングが多い学生情報の自動更新を実装することが出来，健康診断証明書発行のための健診結果データの自動転送も可能となった。

4．権限グループ管理（図 4），アクセス権

IDST 内で権限グループ管理をするシステムを構築した。システム管理者はセキュリティ上，地区にて選出された職員数名のみに限定し，保健管理担当，一般担当の 3 つのカテゴリーで使用可能メニューを制限した。メニュー制限により，画面に表示されるボタン（機能）は自動的に表示を制御する仕様とした。所属ユーザーのアクセス権はシステム管理者が管理し，登録と初回パスワード付与，削除を行うこととした。

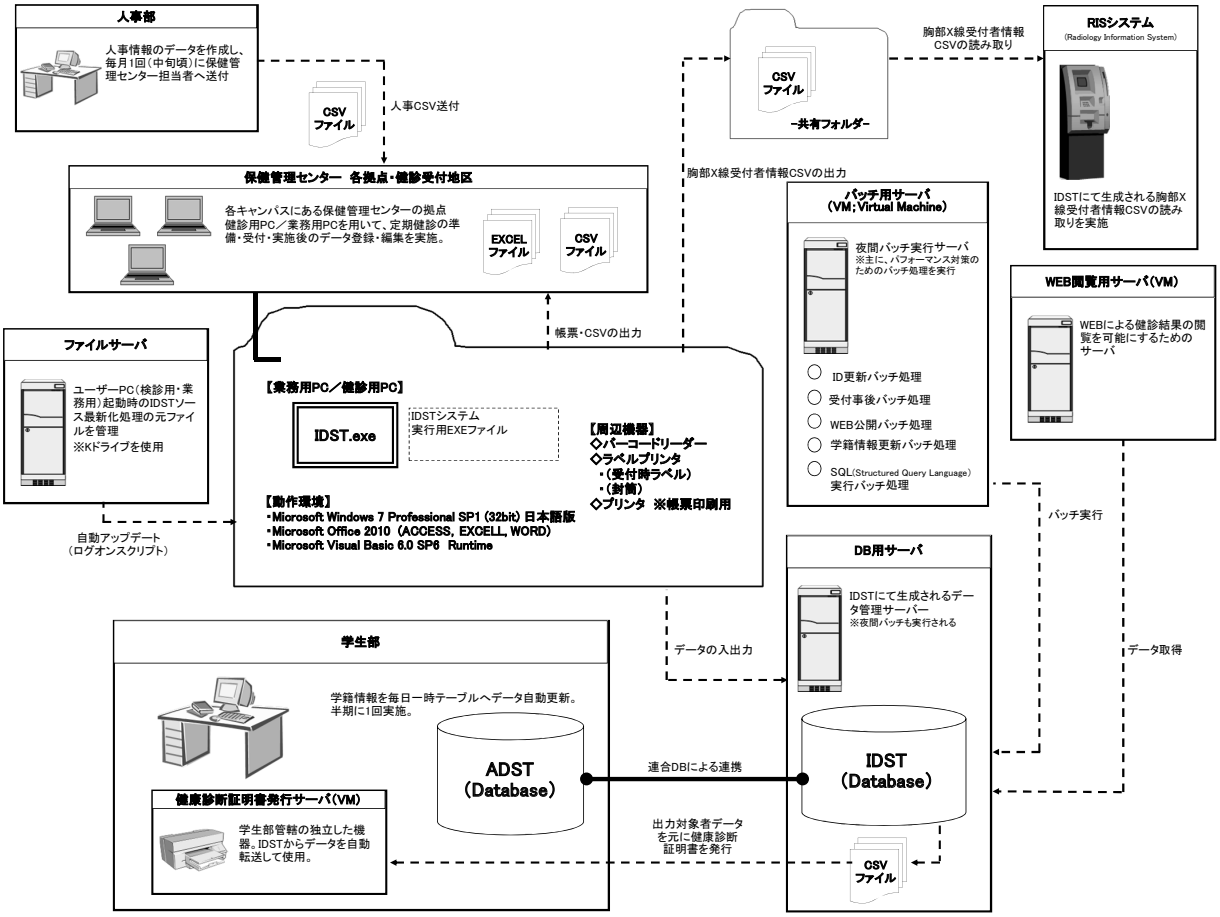

図 3　キャンパス内複数システムとの情報共有化

図 4　権限グループ管理

考　　察

今回，IDST の設計，構築により，旧システムと比較して大幅にセキュリティ環境は改善された。旧システムでは，サーバ機器の維持管理も保健管理センターが主管となった管理体制であり，専門のシステム担当者が不在のまま運用していたが，IDST に移行後は基幹システムの一部となり，専用のネットワーク利用，業務用 PC の利用，アクセス権の設定など，複数のゲートを設けることでセキュリティ管理上の大きな安心感が生まれた。基幹システム内部で堅牢に保護されている安心感はあるが，不慮の故障や個人情報の流出を避けるためには，今後はパフォーマンスとのバランスを見つつ，内部データ自体の暗号化も検討したい。

大学内の複数部署の複雑化した IT 基盤をいかにシンプル，かつセキュアで，効率よく運用するかは重要であり，保健管理センターと学生部のデータ連携による大きな利点は，業務としての作業効率向上だけでなく，無駄な外部ファイル出力が不要となったことである。外部ファイル出力したデータを受け渡すといった運用がなくなるため，データ漏洩のリスクも軽減された。ただし現段階では，すべてのデータが連携できているわけでなく，一部残存している学内および外部業者とのファイルベースでのデータ交換の運用については，改善する必要がある。

また，旧システムでは，同一ファイルでの複数年複数レコード管理により，データ容量が年々増加しており，ハード面での解決が望まれた。しかし，今回のシステムでは，蓄積されるデータについては，容量増加に伴うパフォーマンス低下の問題が解決されず，保持する年度を 6 年で区切っているため，さらにそれより遡っての横断検索や経年分析が難しい状況である。将来的には，柔軟性の高い医療クラウド・アーキテクチャの利用も検討すべきである。

データ管理と利活用の観点からみると，今回のシステム構築に伴い，正規化，最適化されたデータベースにおいては，様々な角度から結果データの検索や抽出が可能となり，健康診断を実施するだけのシステムではなく，集計や傾向分析といったデータ活用が可能になった。その反面，IDST では検査項目ごとに CSV 出力を行う機能があるが，マージできる仕組みがなく，データ活用がしにくい状況である。また，IDST では出力ジョブにユーザー ID が付与されていないことや，IDST 利用頻度が少ない教員が職員へ出力を依頼するというようなヒューマンエラーを生じさせる可能性もあり，この点では，危機管理上，セキュリティが十分に確保されているとはいえない。安全性と利便性をバランスよく確保することは，研究機関である保健管理センターの大きな課題である。

総　括

1．新健康診断システムである IDST は，業務用基幹システム環境の利用，アプリケーションとデータの分離，アプリケーション機能上の権限管理等により，それぞれ独立したセキュリティを設けることができたため，セキュリティ強化ができた。ただし，運用上必ず発生する外部業者等とのデータ授受については外部要因も多く，視野を広げた検討が必要である。

2．膨大なデータの蓄積に伴うパフォーマンス問題やバックアップ運用については技術的な観点を含め，継続検討が必要である。

文　献

1）IBM 連合データベース・テクノロジー：http://www.ibm.com/developerworks/jp/data/library/ds/techdoc/federateddb.html