

# 3 日目 情報システムのセキュリティ対策例

株式会社トスコ  
中桐康隆

1

## 1. 情報システムのセキュリティ対策例

2

### 1. 1 開発事例

情報システム開発時、セキュリティ対策をどのように組み込んで行くか開発事例に基づき説明する。

システム事例

システム名称：某地方自治体「財務会計システム」

システム概要：地方自治体の公会計事務全般を扱うシステム

県職員約 2 万人をユーザとするWebアプリケーションシステム

担当期間：2003年2月～2009年9月

2

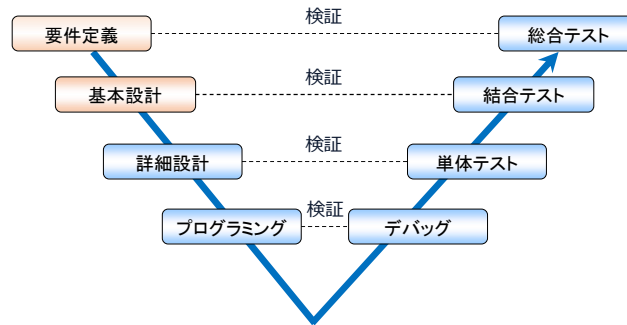
## 1. 情報システムのセキュリティ対策例

3

### 1. 2 開発工程

本講義では、開発工程の上流工程（要件定義、基本設計）で情報システムにセキュリティ対策を組み込んで行く過程を説明する。

ウォーターフォール開発のV字モデル



3

## 2. 要件定義

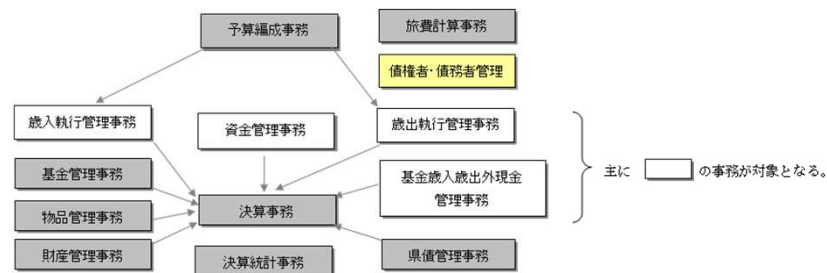
4

### 2. 1 要件定義

#### (1) 要件定義でのアプローチ

財務会計事務において、公金を扱う事務にスポットを当て、内部統制の観点より不正及び誤謬を防止するためのあるべきビジネスプロセスとシステム機能を検討した。ポイントは以下の3点

- A) 業務プロセスとして不正な支出や収入が予防できる、もしくは適切なタイミングで発見できること。
- B) その業務プロセス実現のために、権限が担当職員に適切に付与されていること。
- C) 業務プロセスに即した情報システムでのエラーチェック機能が備わっていること。



4

## 2. 要件定義

5

### (2) 不正および誤謬の定義

#### (A) 不正

不正とは、財務諸表の虚偽記載の原因となる、経営者、従業員又は第三者による意図的な行為であって、次のようなものをいう。

- ・資産の流用
- ・証憑書類の偽造又は改ざん
- ・会計記録からの取引の隠蔽又は除外
- ・実存しない取引の記録
- ・会計基準の不適切な適用

#### (B) 誤謬

誤謬とは、財務諸表の虚偽記載の原因となる意図的でない誤りであって、次のようなものをいう。

- ・財務諸表の基礎となる会計データの収集又は処理上の誤り
- ・事実の見落としまたは誤解に基づく会計上の判断又は見積り
- ・会計基準の適用の誤り

5

## 2. 要件定義

6

### (3) 不正事例の分析

不正、誤謬 の分類	区分	不正手法
不正	1	資産の流用
	2	証憑書類の偽造又は改ざん
	3	会計取引からの取引の隠蔽又は除外情報の改ざん
	4	実存しない取引の記録
	5	会計基準の不適切な適用
	6	システム情報の改ざん
誤謬	7	財務諸表の基礎となる会計データの収集又は処理上の誤り
	8	事実の見落とし又は誤解に基づく会計上の判断又は見積り
	9	会計基準の適用の誤り

不正手法 区分	件数			計
	他自治体	貴庁	会計監査 の観点	
1	1	0	8	9
2	3	0	2	5
3	6	1	8	15
4	3	2	3	8
5	6	0	7	13
6	1	1	2	4
計	20	4	30	54

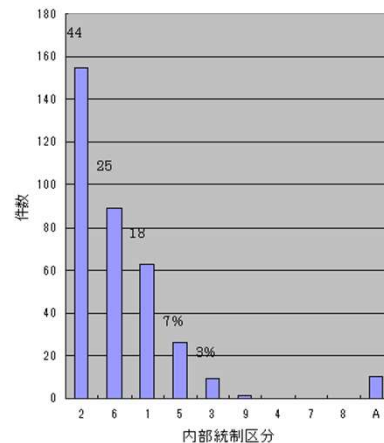
6

## 2. 要件定義

7

### (4) 内部監査事例の分析

内部統制		件数		計	割合 (小数点以下 四捨五入)
区分	内部統制項目	内部監査指摘 事項 (出納管理課)	内部監査指摘 事項 (人事課)		
2	業務分掌	62	93	155	44%
6	突合照合	61	28	89	25%
1	規制の整備	59	4	63	18%
5	承認	1	25	26	7%
3	禁止項目	7	2	9	3%
8	証憑管理	0	0	0	0%
7	人的対策	0	0	0	0%
4	残高確認	0	0	0	0%
9	財産安全管理	1	0	1	0%
A	その他	10	0	10	3%
計		201	152	353	
対応不可		1	0	1	
総合計		202	152	354	



7

## 2. 要件定義

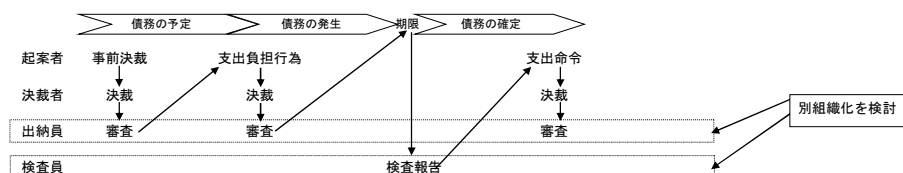
8

### (4) 要件定義要求事項

#### (A) ユーザ認証機能の強化

ユーザIDもパスワードと同様本人しか知りえないIDを付与する。  
ユーザID・パスワードは個人の管理を基本とし、ユーザIDの管理についての職員教育、罰則規定等を併せて実施する。

#### (B) 執行部門の業務分掌強化



#### (C) 地方機関による内部統制の強化

出納員事務と検査員事務が同一者にて行われている執行機関については、人員増を行う。

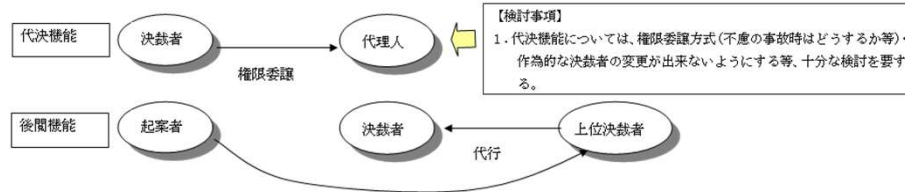
8

## 2. 要件定義

9

### (D) 決裁ワークフローにおける内部統制機能

#### ① 査閲者・決裁者の不在時の事務滞留防止



#### ② 査閲者・決裁者の決裁滞留防止

起案書類の受領から決裁までのリードタイムを設定し、リードタイムを経過すると監査部門と本人及び本人の上席者にアラームメールを送信する機能

9

## 2. 要件定義

10

### (E) 納期管理の強化

#### ① 支出における納期管理

契約書上の債務確定日（検収予定日・納入予定日等）、の履行期限情報を必須入力とし、納期遅延のアラームメールを自動送信

#### ② 収入における納期管理

収入の調定入力時収納予定日を必須入力し、収納未済のものを未収納一覧として各部門長および収納担当者にアラームメールを自動送信

### (F) 検査（債権・債務の確定）を中心にした日付正当性の担保

### (G) 資金前渡に対するセキュリティの強化

#### ① 資金前渡廃止の検討

#### ② 資金前渡・精算事務の牽制機能強化

精算金入力にて戻入還付を同時に行える機能とし、精算金 0 円でも必ず精算処理をしなければ仮払支出残高に残るようシステムの考慮

10

## 2. 要件定義

11

### (H) 債権者登録のセキュリティ強化

債権者登録・変更事務に関しても業務分掌の観点より、支出に関する事務と同等の決裁ワークフローを実施し、最終的に出納員のチェックを経なければ登録できないようにする。

### (I) 債権者情報の重複解消

債権者登録時債権者名、振込口座番号等債権者の一意性を担保する項目を設定し、債権者登録時に重複チェックすることにより、債権者の重複を防止。

### (J) 不正情報の共有

過去にいくつかの不正行為が発覚し、その事実が公表されることにより、一時的に内部規律は高まるが、時間の経過とともに次第に風化していく傾向がある。  
不正を公表することで、内部統制の効力は発揮できるがそれを風化させない工夫

・HPに不正事例を載せる→職員ポータルへのテロップ表示

11

## 3. 基本設計

12

### 3. 1 基本設計でのアプローチ

県セキュリティポリシーに基づき、コンピュータシステムにて考慮すべきセキュリティ対策を検討

脅威	対策区分		対策項目		詳細内容	
	No.	項目	対策No.	項目		
コンピュータシステム障害により、業務またはシステムに障害をきたす	1	ハードウェア対策	(1)	クラスタ構成	サーバをクラスタ構成にし、可用性を高める	
	2		運用管理	(1)	バックアップ	システム障害に備えデータの定期バックアップを行う
				(2)	リストア	障害復旧後データバックアップからの復旧機能を提供する
				(4)	障害監視	サーバの障害監視を行い、障害の通知・分析を行う機能を提供する
				(5)	性能監視	サーバの性能監視を行い、性能劣化に対し早期対応できる機能を提供する
電力の不安定供給により、業務またはシステムに障害をきたす	1	ハードウェア対策	(2)	UPS	UPSの設置により、電力の安定供給を行う	
ソフトウェアのミスにより、業務またはシステムに支障をきたす	3	アプリケーション対策	(1)	トランザクション管理	全てのアプリケーションはトランザクション処理により、同期点によるロールバックを可能とする構造とする	
	(4)		ログ採取	ソフトウェア障害に関しては、障害時に通知を行い、トレースログを採取する		
	2	運用管理	(3)	ソフトウェア配付	障害のあるソフトウェアは、障害箇所の修正後システムを停止することなく入れ替えを可能とする	
データの入力ミスによって、業務またはシステムに支障をきたす	3	アプリケーション対策	(2)	入力チェック	データの入力ミスは未然防止するよう、入力チェックを行う	
操作ミスによって、業務またはシステムに支障をきたす	2		運用管理	(3)	機能	入力ミスを訂正・取消できる機能を提供する
		(4)		ログ採取	データアクセスログを採取し、入力ミス特定する機能を提供する。	
機密性の高いデータが流出する	3	アプリケーション対策	(6)	ジョブスケジューリング	ジョブスケジューリング機能により、バッチ処理の自動化を図りバッチの誤起動・誤操作を防止する	
			(4)	ログ採取	オペレーションログを採取し、誤操作を特定する機能を提供する	
ウィルスに犯され、システムに影響を及ぼす	3	アプリケーション対策	(5)	ユーザ認証機能	システムにログインするとき、ユーザID・パスワードによる利用権のチェックを行い個人の特定をする	
			(6)	アクセス制御	個人ごとにアクセスできるデータに制限を設ける	
			(4)	ログ採取	アクセスログを採取し、不正アクセスの監視を行う	
			(7)	アンチウィルス	サーバにウィルス検出・駆除ソフトを導入し、ネットワーク経由で入ってくるファイルのウィルス検出・駆除を行う	

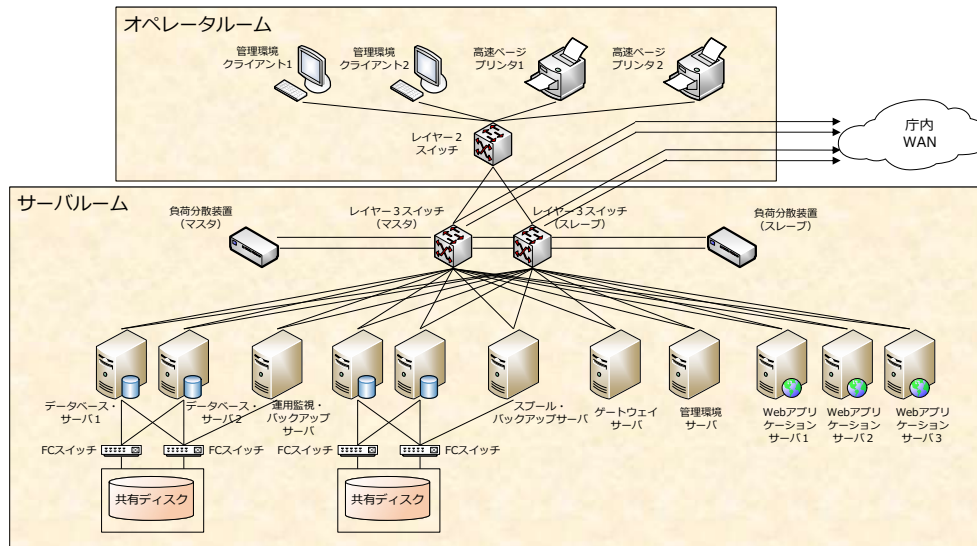
12

### 3. 基本設計

13

#### (1) ハードウェア対策

##### (A) ハードウェア全体構成



13

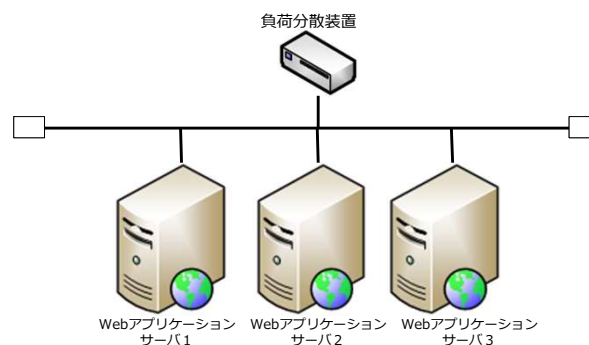
### 3. 基本設計

14

##### (B) WEBアプリケーションサーバ

障害発生時でもサービス提供を継続可能で、且つ、サービス性能を十分に満たせるハードウェア構成とする。

- ① 内蔵ディスクには、基本OS及びミドルウェアを配置し、RAID1（ミラーリング）とする。
- ② CPU障害時の対処として、複数CPUを実装する。
- ③ WEBアプリケーションサーバを3台構成とし、サービス性能を維持する。
- ④ OS及びミドルウェア領域のバックアップのため、直結したバックアップ装置を実装する。



14

### 3. 基本設計

15

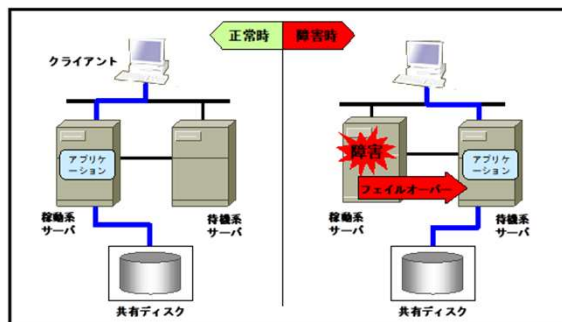
#### (C) データベースサーバ

データベースサーバは、障害発生時でもサービス提供を継続可能で、且つ、サービス性能を十分に満たせるハードウェア構成とする。

①内蔵ディスクには、基本OSのみを配置することを原則とし、RAID1（ミラーリング）とする。

②CPU障害時の対処及びサービス性能を満たすため、複数CPUを実装する。

③サービス提供維持のため、データベースサーバは2重化構成とし障害発生時にもサービス提供を維持する。



④データベースの共有を行うため、データベースファイルは共有ディスクの中に配置する。

⑤OS領域のバックアップのため、直結したバックアップ装置を実装する。

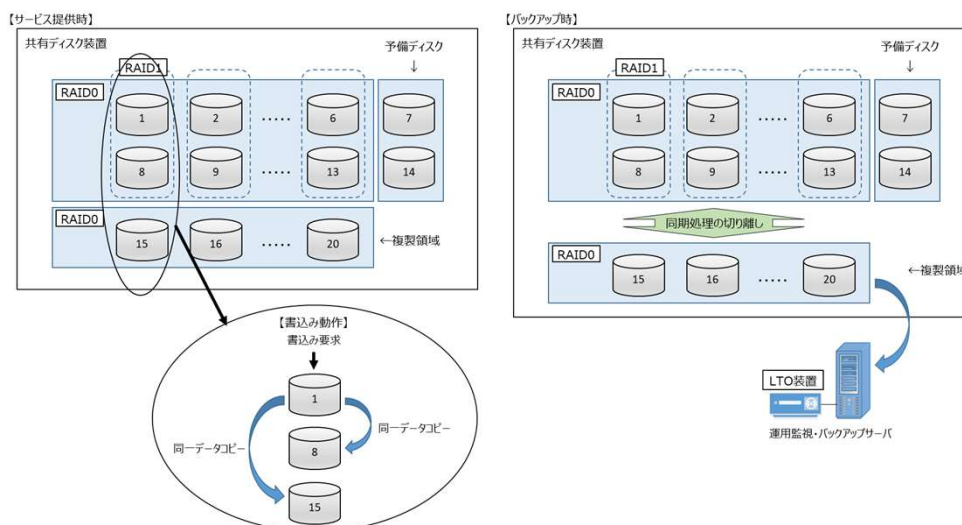
15

### 3. 基本設計

16

#### (D) 共有ディスク装置（データベースサーバ用）

ディスク障害発生時の対策としてRAID構成はRAID1+0を採用し、予備ディスクの搭載により障害発生時に自動的にRAID構成の再構築が図れる構成とする。



16



3．基本設計

17

(2) 運用管理

監視項目	監視内容
ハードウェアの監視	CPU使用率、メモリー使用率、ディスク使用率、OS固有のシステムログファイル（イベントログ）、ハードウェアデバイスの状態等を監視する。
ネットワークの監視	ネットワーク上のサーバに対し定期的に稼働確認問い合わせを実施し、応答があるか否かにより、ハードウェア／OSのダウンによる無応答状態を検出する。 ネットワークのトラフィック量、イーサネットのパフォーマンス、エラーを監視する。
アプリケーションの監視	Webアプリケーション、またはそれらを構成するミドルウェアから出力されるログ情報を監視し、管理・保守用端末に表示する。 <ul style="list-style-type: none"><li>エラーログファイルを監視し、アプリケーションのエラーメッセージを検出する。</li><li>特定アプリケーションの起動状態(プロセスの存在)を監視する。これによりアプリケーションの異常終了によりプロセスが存在していない事象を検出する。</li><li>システム全体の稼働状況を監視し、しきい値超過を検出すると管理者に通知する。</li><li>トランザクションレスポンスタイム、プリンタ出力量を監視する。</li></ul>
バッチジョブの監視	<ul style="list-style-type: none"><li>バッチジョブの処理時間、処理件数、処理結果を監視する。</li><li>異常終了時はメールにて運用保守ベンダ、運用管理チーム、システム主管課（当該バッチ処理担当）に通知する。</li></ul>
セキュリティの監視	<ul style="list-style-type: none"><li>庁内利用者が、権限以外のサービスを利用できないようにサービスごとにアクセス権を設定する。</li><li>庁内利用者がアクセスするサーバにウィルス対策ソフトを導入しウィルスの監視を行う。</li><li>誰がいつ利用したかログを採取し監視する。</li></ul>

17

3．基本設計

18

(A) ハードウェア／アプリケーションの監視

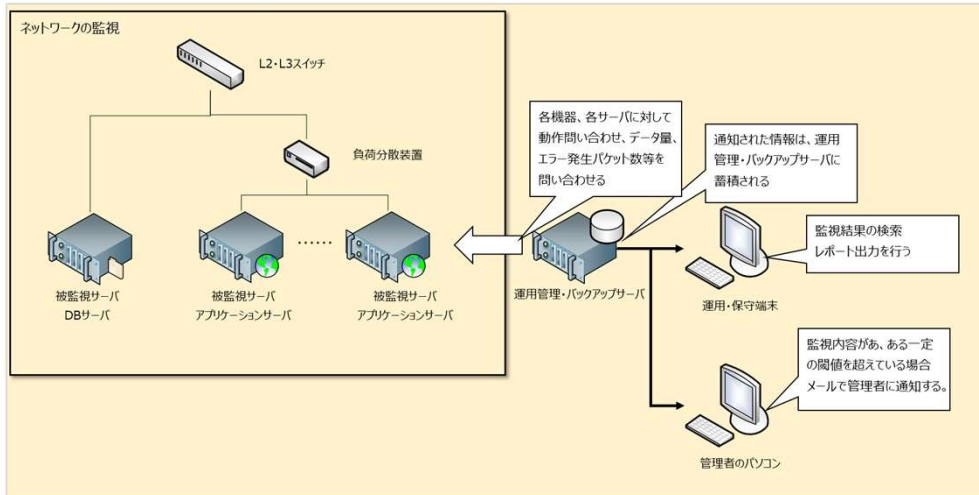
The diagram illustrates the monitoring workflow for hardware and applications. It starts with '被監視サーバ Webアプリケーションサーバ等' (Monitored Servers, Web Application Servers, etc.) on the left. An arrow points to '運用管理・バックアップサーバ' (Operation Management / Backup Server) in the center. A callout box above this arrow states: 'エージェントにより CPU使用率、各種ログが監視され、運用管理・バックアップサーバに通知される' (Monitored by agents, CPU usage, various logs are monitored and notified to the operation management/backup server). From the central server, an arrow points to '運用・保守端末' (Operation/Maintenance Terminal) on the right. A callout box above this arrow states: '通知された情報は、運用管理・バックアップサーバに蓄積される。' (Notified information is accumulated in the operation management/backup server). From the terminal, an arrow points to '管理者のパソコン' (Administrator's PC) at the bottom right. A callout box above this arrow states: '監視結果の検索レポート出力を行う' (Perform search and report output of monitoring results). Another callout box next to the administrator's PC states: '監視内容があ、ある一定の閾値を超えている場合メールで管理者に通知する。' (If monitoring content is present or exceeds a certain threshold, notify the administrator via email).

18

### 3. 基本設計

19

#### (B) ネットワークの監視



19

### 3. 基本設計

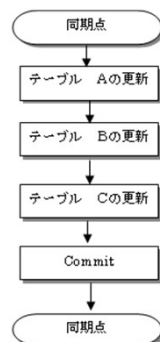
20

#### (3) アプリケーション対策

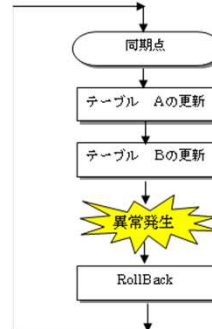
##### (A) トランザクション管理

トランザクションとは、一連のデータ処理を1つの単位として管理すること。  
 例えば、入金処理において「領収番号を新たに発番する」、「入金票を出力する」、「請求残高を差し引く」という一連の処理は、複数の処理を含む1つのトランザクションである。  
 一連の処理は、正常に処理が完了するか異常終了するかに係らず、処理結果のデータは整合性が保証されなければならない。

【正常ケース】



【異常ケース】



20

### 3. 基本設計

21

#### (3) アプリケーション対策

##### (B) 入力チェック

全てのデータ入力アプリケーションは、データの入力ミス未然に防止するため、入力データの更新を行う前には、考えられる全ての項目について入力チェックを行わなければならない。

- ① 入力項目のタイプチェック  
入力項目のタイプに合致するかどうかのチェックを行う。  
入力項目のタイプは、データベースの論理設計にて論理ドメインとして定義する。  
また、本システムはHTMLベースの入力を行うため、クロスサイトスクリプティングの脆弱性対策として、入力項目全てに対し特殊文字(< & ' " 等)の混在チェックをサーバサイドで行うものとする。
- ② 入力項目の論理チェック  
入力項目のマスタ上の存在チェック等、項目単体の論理的な妥当性をチェックする。
- ③ 入力項目の相関チェック  
入力項目間の相関性をチェックする。  
ツリー構造のデータ構造を持つ項目がある場合、親の項目により子の項目の取りうる範囲が変わるような場合の範囲チェックなどが考えられる。

21

### 3. 基本設計

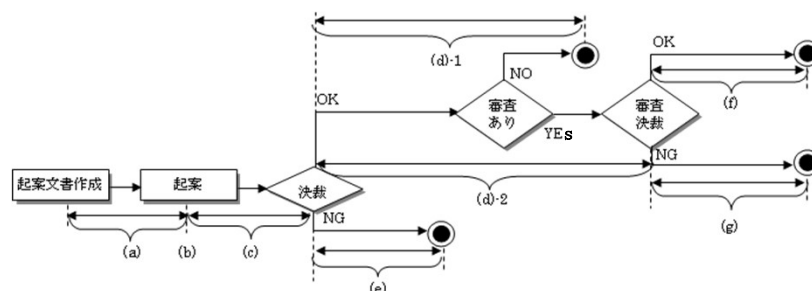
22

##### (C) 訂正・取消機能

入力チェック機能を充実しても、利用者の入力ミスを完全に防止することはできない。入力ミスが発覚した時点で、速やかに入力ミスを訂正・取消することができなければならない。

また、訂正・取消機能によりデータの整合性・妥当性を保証するためには、そのデータの時間的狀態（ステータスの遷移）により以下のパターンを考慮する必要がある。

**パターン例：会計伝票の起票等、電子決裁を経てデータが更新されるパターン**  
決裁ステータスにより訂正・取消の可否を判断する。



22

### 3. 基本設計

23

- (a) 起案文書作成～電子決裁起案での案件の訂正・取消  
 決裁ステータス : 未処理  
 入力ミスの訂正方法 : 1) 起案文書作成画面より、当該起案文書を呼び出し訂正・取消を行う。
- (b) 電子決裁起案画面での案件の訂正・取消  
 決裁ステータス : 起案待ち  
 入力ミスの訂正方法 : 1) 当該起案文書を「廃案」にすることで、決裁ステータスが「未処理」となる。  
 2) 起案文書作成画面より、当該起案文書を呼び出し訂正・取消を行う。
- (c) 電子決裁起案～決裁での案件の訂正・取消  
 決裁ステータス : 決裁回付中  
 入力ミスの訂正方法 : 1) 起案者が電子決裁の「引き戻し」機能により、当該起案文書を引き戻す。  
 または、回付途中の者が電子決裁の「差し戻し」機能により、当該起案文書を差し戻す。  
 2) 当該起案文書を「廃案」にすることで、決裁ステータスが「未処理」となる。  
 3) 起案文書作成画面より、当該起案文書を呼び出し訂正・取消を行う。

23

### 3. 基本設計

24

- (d) - 1. 電子決裁完了後の案件の訂正（支出負担行為等の出納員審査を伴わない場合）  
 決裁ステータス : 決裁完了  
 入力ミスの訂正方法 : 決裁完了後の決裁文書は原則訂正・取消できない。  
 決裁完了後に決裁後の文書訂正の必要性が生じた場合は、以下の手順で変更注4を行うこととする。  
 1) 変更・取消対象の案件の決裁文書番号を指定し、当該案件の変更の伺いを所定の書式によるWord等の電子文書により起案し、電子決裁により決裁を受ける。  
 （取消対象の決裁文書との関連付けが必要）  
 2) システム管理者に連絡し、当該起案文書を強制的に「保留」状態にもらう。  
 このとき、起案文書は起案者に差し戻されるが、起案～最終決裁権者にはメールで決裁済の文書が差し戻された旨を通知する。  
 3) 起案者は電子決裁の起案画面より、当該起案文書を呼び出し「変更起案」を行う。  
 4) 「変更起案」の決裁が完了した時点で、内部では元の起案文書を取消し新しい枝版で決裁文書を作成する。

24

## 3. 基本設計

25

### (D) ログ採取

#### (a) ログの種類

アプリケーションで採取するログの種類を以下に示す。

種 類	内 容	出力が必要となるケース
トレースログ	アプリケーションで検知した障害情報及び、アプリケーションの稼働情報等 outputs する。	障害を検知した場合、又はプログラム単位で処理を行った件数や正常終了時に内容確認を行うための情報を出力しておきたい場合。
パフォーマンスログ	アプリケーションの稼働情報を出力する。	プログラム単位でのタイムスタンプ（開始／終了時間）を採取する場合。 ＜パフォーマンスログが必要なケース＞ ・業務システムのレスポンス低下時、調査が必要になると思われるバッチプログラム全て。 ・原因追求のため必要となる可能性のある全てのデータを当ログに出力する。
認証ログ	ユーザ認証の際、認証結果等の情報を出力する。	利用者認証を行う場合。
アクセスログ	データへのアクセスの際、アクセスした情報を出力する。	・機密性の高いデータにアクセスする場合。 ・データを更新する場合。
オペレーションログ	システム管理者によるシステム操作の際、操作内容等の情報を出力する。	システム管理者権限でシステム操作を行う場合。

25

## 3. 基本設計

26

### (b) トレースログ

#### (i) ログの用途・目的

- ・アプリケーションにて検知した障害の詳細を迅速に把握する。
- ・処理の稼働情報を出力することにより、障害原因及び障害箇所の追求を迅速に行う。
- ・監視コンソールに出力された障害メッセージを基にログを参照し、障害発生箇所の発見を迅速に行う。

#### (ii) 対象

- ・障害を検知し、運用者に通知するロジックを実装するプログラム全て。

#### (iii) トレースログ格納場所の規定

- ・アプリケーションは規定されたディレクトリに、トレースログを作成する。

#### (iv) トレースログ出力フォーマットの規定

No.	項目	内容
1	キーワード	以下のいずれかとし固定とする。 ・inform : アプリケーション稼働情報 ・error : エラー情報（自システム内の要因でエラー発生の場合） ・fatal : エラー情報（他システム、環境など 自システム外の要因でエラー発生の場合）
2	日付	YYYYMMDD形式で出力
3	時刻	HHMMSS形式で出力
4	戻り値	プログラム内にて判定している戻り値（exit値）
5	内容	処理の内容、処理データ等を記述

26

3．基本設計

27

(b) トレースログ

サーバシステム

アプリケーション

①障害発生

②メッセージ出力 (障害通知)

③障害ログ作成

④ログ書き込み

```
inform *20020601 *162955 *0 *sts=0000000
error *20020601 *163001 *1 *DB ACCESS ROUTINE
ABNORMAL . STS=000001011 :xxxxxxxxxxxxx
xxxxxxxxxxxx xxxxxxxx
```

本番環境でキーワード(inform)をトレースログに出力するには、外部環境ファイル内のデバッグモードを “O n” に設定することで可能となる。  
(通常の場合は“O f f”に設定しておく)

27

3．基本設計

28

(c) パフォーマンスログ

(i) ログの用途・目的

- ・アプリケーションにて急激なレスポンス低下が発生した場合の原因追求を行う。
- ・本番導入後のシステム評価で、設計段階でのレスポンスとの差異を把握する。

(ii) 対象

- ・アプリケーション全て。

(iii) パフォーマンスログ格納場所の規定

- ・アプリケーションは規定されたディレクトリに、パフォーマンスログを作成する。

(iv) パフォーマンスログ出力フォーマットの規定

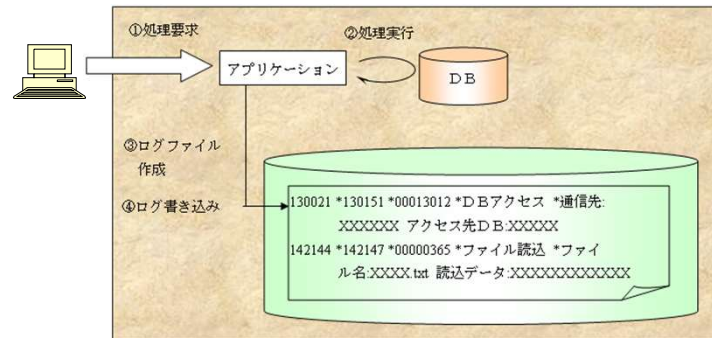
No.	項目	内容
1	開始時刻	HHMMSS形式で出力
2	終了時刻	HHMMSS形式で出力
3	処理時間	HHMMSSmm※形式で出力 ※mm = ミリ秒
4	採取ポイント	プログラム内でのレスポンスデータ出力箇所を出力
5	レスポンス出力情報	レスポンスデータの詳細情報を出力 →通信先サーバ名 →送信データ →アクセス先DB名 等

28

### 3. 基本設計

29

(c) パフォーマンスログ



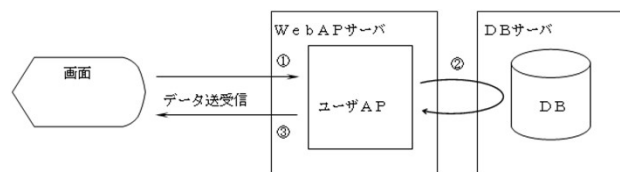
29

### 3. 基本設計

30

(viii) パフォーマンスログ採取のタイミング

- パフォーマンスログを採取するには、各アプリケーション側にてタイムスタンプを出力する仕組みを考慮する。タイムスタンプを出力するタイミングとして、以下が考えられる。



- ①画面からのデータ受信時
- ②ユーザアプリケーションからDBへのアクセス（開始／終了）時
- ③画面へのデータ送信時

以上の出力タイミングから、アプリケーション側で必要と思われる時点でのタイムスタンプを出力し、システム評価及び障害切り分け時のレスポンスデータとする。  
パフォーマンスログを採取するには、共通フレームワークで提供されているAPIを使用する。

本番環境でパフォーマンスログ（レスポンスデータ）の評価を行う場合は、共通フレームワークで提供されている外部環境ファイル内のレスポンス採取機能を“On”に設定することで可能となる。

（通常の場合は“Off”に設定しておく）

30

### 3. 基本設計

31

#### (d) 認証ログ

##### (i) ログの用途・目的

- ・ログの追跡を行うことにより、システムの不正利用（パスワード試行攻撃等）を検知する。

##### (ii) 対象

- ・財務会計システムにログインする利用者全て。

##### (iii) 認証ログ格納場所の規定

- ・アプリケーションは規定されたディレクトリに、認証ログを作成する。

##### (iv) 認証ログ出力フォーマットの規定

認証ログは、ログイン/ログアウトのタイミングで出力する。

認証ログにおけるログイン/ログアウト時の出力フォーマットは以下の通り。

##### ①ログイン時の認証ログ

No	項目	内容
1	利用者 I D	
2	区分	ログイン/ログアウトの区分 ログイン . . . login
3	ログイン日付	YYYYMMDD形式で出力
4	ログイン時刻	HHMMSS形式で出力
5	認証結果	利用者 I D パスワードの認証結果 ログイン成功 . . . 0 ログイン失敗 . . . 1

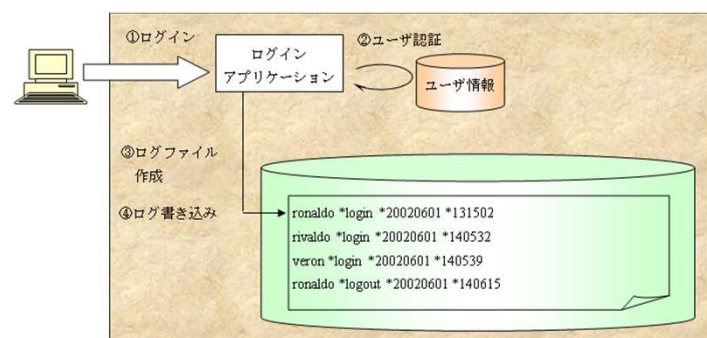
31

### 3. 基本設計

32

#### ②ログアウト時の認証ログ（正常にログインした時のみ出力）

No	項目	内容
1	利用者 I D	
2	区分	ログイン/ログアウトの区分 ログイン . . . login ログアウト . . . logout
3	ログアウト日付	YYYYMMDD形式で出力
4	ログアウト時刻	HHMMSS形式で出力



32



3. 基本設計

33

(e) アクセスログ

(i) ログの用途・目的

・ログの追跡を行うことにより、システムの不正利用（DBへの不正アクセス等）を検知する。

(ii) 対象

・アプリケーション全て。

(iii) アクセスログ格納場所の規定

・アプリケーションは規定されたディレクトリに、認証ログを作成する。

(iv) アクセスログ出力フォーマットの規定

No.	項目	内容
1	利用者 I D	
2	アクセス日付	HHMMSS形式で出力
3	アクセス時刻	HHMMSS形式で出力
4	アクセス対象名	アクセスしたデータ、プログラムの名前・場所等を出力する

33

3. 基本設計

34

(e) アクセスログ

```
graph TD
    App[アプリケーション] -- "①処理実行" --> DB[(DB)]
    DB -- "②ログファイル作成" --> Log[(Log Storage)]
    Log -- "③ログ書き込み" --> Log
    subgraph LogContent [Log Content]
        direction TB
        L1[zidane *20020601 *120215 *DB-NAME:XXXXXXXX *0]
        L2[neuville *20020601 *184439 *CONNECT:XXXXXXXX *1]
    end
```

34

### 3. 基本設計

35

- (f) オペレーションログ
- (i) ログの用途・目的
- ・ログの追跡を行うことにより、業務システムにおける管理者権限の誤操作・不正利用を検知する。
- (ii) 対象
- ・業務システムにおける管理者ユーザ用処理を実装しているプログラム全て。
- (iii) オペレーションログ出力フォーマットの規定
- オペレーションログは、業務システムにおける管理者 I D でログインし、ログアウトするまでの間に実行された処理の履歴を出力する。
- 管理者 I D でのログイン/ログアウト時及び処理実行時のフォーマットは以下の通り。

#### ①ログイン時のフォーマット

No	項目	内容
1	管理者 I D	財務会計システムの管理者 I D を出力
2	区分	ログイン/ログアウトの区分 ログイン . . . login
3	ログイン日付	YYYYMMDD形式で出力
4	ログイン時刻	HHMMSS形式で出力

35

### 3. 基本設計

36

#### ②処理実行時のフォーマット

No	項目	内容
1	管理者 I D	財務会計システムの管理者 I D を出力
2	実行した処理内容	

#### ③ログアウト時のフォーマット

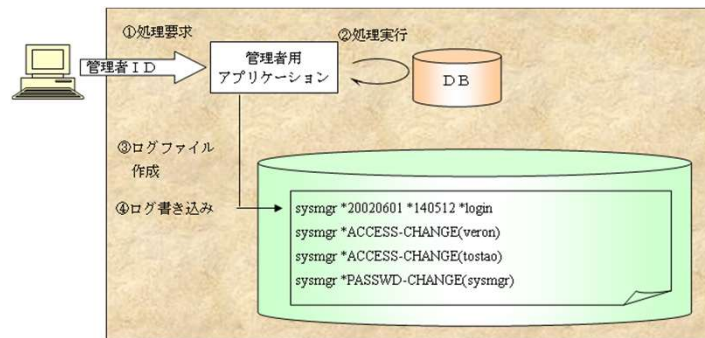
No	項目	内容
1	管理者 I D	財務会計システムの管理者 I D を出力
2	区分	ログイン/ログアウトの区分 ログイン . . . logout
3	ログアウト日付	YYYYMMDD形式で出力
4	ログアウト時刻	HHMMSS形式で出力

36

### 3. 基本設計

37

(f) オペレーションログ



37

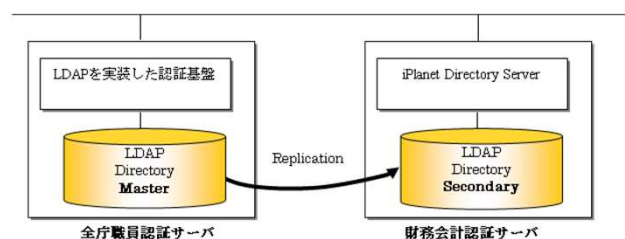
### 3. 基本設計

38

(E) ユーザ認証機能

(a) 財務会計システムのユーザ認証機能の位置付け

財務会計システムの認証機能は、全庁認証用のLDAP Directoryを使用する。  
財務会計システムの認証機能は、職員認証システムのセカンダリーサーバとして機能する位置付けとする。



(b) LDAP Directoryで保有する情報

LDAP Directoryでは、以下の情報が保有されている。

1. 職員コード (ユーザID)
2. 職員名称
3. パスワード
4. 職責
5. 所属コード
6. 兼務情報
7. メールアドレス

38

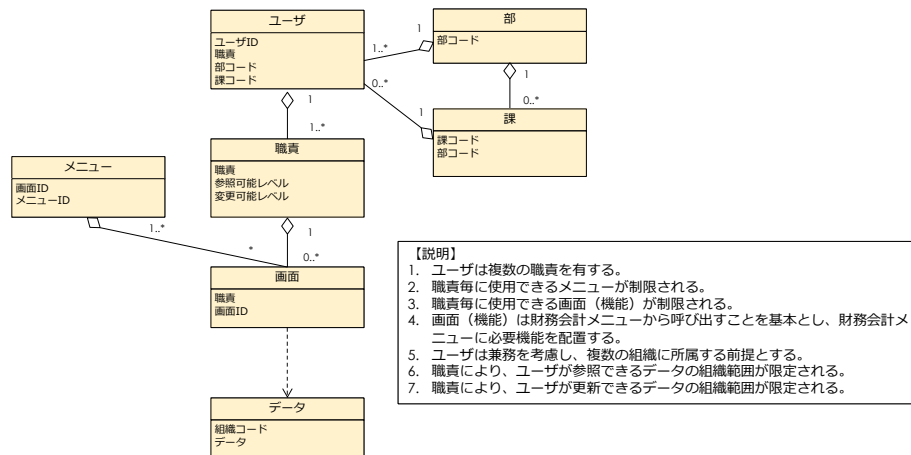
### 3. 基本設計

39

#### (F) アクセス制御

機密性の高いデータの流出防止、不正アクセスの防止を目的とし、個人の職責に応じ以下のアクセス制限を加える。

##### (a) セキュリティ関連図



39

### 3. 基本設計

40

#### (b) 利用機能制限

利用機能制限は、ユーザの職責によりメニューに表示される機能を制御することで実現する。メニューのイメージを下記に示す。

財務会計システム

ユーザー: 財務次郎

メニュー毎に、表示する画面IDが設定できる。

ユーザの職責によりメニューに表示する画面ID（機能）を制限する。

40

3．基本設計

41

(c) データアクセス権

(i) 情報の重要性分類にて、財務会計システムで扱う情報の重要性を分類する。

重要度レベル	情報種別	重要性
4	セキュリティの侵害が、住民及び職員の生命、財産、プライバシー等への重大な影響を及ぼす情報	高い ↑ ↓ 低い
3	セキュリティの侵害が、行政事務の執行等に重大な影響を及ぼす情報	
2	セキュリティの侵害が、行政事務の執行等に軽微な影響を及ぼす情報	
1	行政事務の執行等にほとんど影響を及ぼさない情報	

No.	情報種別	情報内容	重要性	備考
1	歳入金情報	歳入金の予算執行情報	4	
2	歳出金情報	歳出金の予算執行情報	4	
3	複式伝票情報	複式勘定元帳に記帳する貸借がバランスした勘定科目と金額を含む複式伝票情報	3	
4	予算編成情報	予算編成中の予算情報	3	
5	予算執行情報	確定予算と執行状況の情報 勘定科目、予算額、執行額、調定額、事前決裁額、支出負担行為額、支払の管理を行う	3	
6	複式勘定元帳情報	B/S,P/L,C/S,M/Wを作成するための元帳情報 決算調整等の特別な取引以外は、単式勘定元帳記帳時に自動的に作成される。	3	
7	契約情報	当該取引の、納期、契約額、契約先等の契約内容が記載された伝票。	4	契約情報は個人情報を含むため、プライバシーの保護が必要

3．基本設計

42

No.	情報種別	情報内容	重要性	備考
8	財産台帳情報	複式勘定元帳の「固定資産の部」に載る評価額、取得原価及び資産情報をもつ台帳 現行の公有資産及び物品データが対象となる	3	
9	歳入計画情報	資金管理で使用する歳入計画	3	
10	歳出計画情報	資金管理で使用する歳出計画	3	
11	県債情報	県債の起債単位の償還予定と実績が記載される台帳	3	
12	決算整理情報	決算書中の備考欄表記で使用する	3	
13	旅費情報	旅費の申請単位の明細情報。 ( ) 内は「何い」「精算（不足金）」「精算（剰余金）」等の文言を明記する。	4	公安委員会の情報は、他部門からは参照不可とする。
14	職員情報	人事・給与から連動する職員情報を管理する。 ( ) 内は特に明記が必要な場合は「職責」「支払先口座」「パスワード」「メールアドレス」・・・等を記述する。	4	
15	基金情報	各種基金の契約情報、運用情報を管理する	3	
16	債権者・債務者情報	債権者・債務者を一括管理するマスタ。	4	
17	不動産契約台帳情報	財産の貸借事務及び目的外使用事務において、公有財産の賃貸借契約情報を管理する台帳	4	契約情報は個人情報を含むため、プライバシーの保護が必要
18	用度情報	用度会計で使用するマスタ情報、及び指定物品、指定供用物の請求データを管理する台帳 マスタ情報、指定物品、指定供用物等の情報を含む	4	

3．基本設計

43


(d) 参照データ制限

職責に対応する「参照可能組織レベル」を設定することで、当該職責が参照可能なデータの組織範囲を制御する。  
尚、EUC機能（注）に関しては本制限の対象外とし、EUC機能で事前に設定された参照可能項目は、全てのユーザが平等な「参照可能レベル”0”」の参照権限を持つこととする。

参照可能組織レベル 0：全てのデータを参照可能  
1：当該ユーザが所属する部コードを持つデータを参照可能  
2：当該ユーザが所属する局コードを持つデータを参照可能  
3：当該ユーザが所属する課コードを持つデータを参照可能

【例】

人事 太郎  
職責：課長  
参照可能組織レベル：3  
所属：経営管理部 人事課



部	局	課	データ
経営管理部	人事課	人事課	00000001000020010010101010
経営整備部	企画管理課	建設技術室	0230012023030403005875732890-
経営管理部	人事課	人事課	000030302010575759238-2-030458
経営管理部	文書法務室	文書法務室	0009837298000038171-77381-3871-183747-
経営整備部	砂防課	砂防課	92-2-179438-98900000302008187201-38
経営管理部	人事課	人事課	6637810-091-98730-68926440936187-1-63974165
経営管理部	管財課	管財課	33582670027631-927672-19837103346730128236

(注) EUC(End User Computing)

情報システムを利用して現場で業務を行う従業員や部門(エンドユーザ、ユーザ部門)が、自らシステムやソフトウェアの開発・構築や運用・管理に携わること。

3．基本設計

44

(e) 更新データ制限

職責に対応する「更新可能組織レベル」を設定することで、当該職責が更新可能なデータの組織範囲を制御する。

更新可能組織レベル 0：全てのデータを更新可能  
1：当該ユーザが所属する部コードを持つデータを更新可能  
2：当該ユーザが所属する局コードを持つデータを参照可能  
3：当該ユーザが所属する課コードを持つデータを更新可能