勘定奉行Ｖ ERP Standard Edition・運用管理ツール

セキュリティターゲット

2009/03/16

バージョン：1.23

株式会社オービックビジネスコンサルタント

目次

1　ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1　ST 参照

本節では ST の識別情報を記述する。

タイトル　：勘定奉行 V ERP Standard Edition・運用管理ツール　セキュリティターゲット

バージョン：1.23

発行日　　：2009 年 3 月 16 日

作成者　　：株式会社オービックビジネスコンサルタント

1.2　TOE 参照

本節では TOE の識別情報を記述する。

TOE の名称	：勘定奉行 V ERP Standard Edition、運用管理ツール
TOE のバージョン	：勘定奉行 V ERP Standard Edition 運用管理ツールのバージョンはともに 1.05
開発者	：株式会社オービックビジネスコンサルタント

1.3　TOE 概要

1.3.1 TOE 種別および主要セキュリティ機能

TOE は財務会計パッケージソフトウェアである「勘定奉行 V ERP Standard Edition」とセキュリティ管理・ログ管理を担う「運用管理ツール」からなる。

運用管理ツールは勘定奉行 V ERP Standard Edition を購入すると必ず同梱されるものであり、勘定奉行 V ERP Standard Edition と別に購入するものではない。

なお、本 ST では、勘定奉行 V ERP Standard Edition と運用管理ツールの標準機能のみを使った運用を想定しており、アドオン機能の付加などは考慮していない。

また、販売管理パッケージなど他システムとの連携によるリスク、外部ネットワークを利用する際の脅威、企業内 LAN からの攻撃による脅威、OS や DBMS を直接操作する脅威に対しては、別途、運用環境において対策することとし、本 ST が求める TOE の対応範囲外とする。

以下でそれぞれの概要を説明する。

＜勘定奉行 V ERP Standard Edition＞

勘定奉行 V ERP Standard Edition は仕訳処理、各種帳票、財務報告書の作成などの基本機能を持つ。セキュリティ機能としては仕訳伝票データ更新ロック機能を

持ち、財務報告書に関係する金額を業務締めや決算締めのタイミングで確定しロックすることが出来る。

＜運用管理ツール＞

運用管理ツールは利用者管理、ログ管理機能を搭載している。セキュリティポリシーを設定し利用者の管理を行い、勘定奉行 V ERP Standard Edition と運用管理ツールで操作された内容をログに残している。

TOE が搭載するセキュリティ機能

- **利用者識別認証：**

本 TOE の利用者に対する識別と認証を行う機能

- **監査証跡：**

本 TOE での操作のログを作成、参照する機能

- **仕訳伝票データ更新ロック機能：**

指定した期間に対して仕訳伝票データ更新ロックを行い、その期間に含まれる金額データをロックする機能

- **環境設定データ管理：**

環境設定データに対する管理機能

1.3.2 保護資産

TOE の保護資産は以下の通りである。

(1) 会計データ

- 勘定科目マスタ
- 仕訳伝票データ
- キャッシュ・フロー調整金額明細データ
- 期首残高データ

(2) 環境設定データ

TOE のセキュリティ機能を動作させるために必要となる情報。

- 識別認証データ
- 仕訳伝票データ更新ロックデータ
- ログポリシーデータ
- アカウントポリシーデータ
- パスワードポリシーデータ
- 利用者アカウントロックデータ
- 利用者権限データ

1.3.3 TOE 利用環境

[TOE 運用環境]

TOE は、勘定奉行 V ERP Standard Edition サーバープログラム、運用管理ツールサーバープログラム、勘定奉行 V ERP Standard Edition クライアントプログラム、及び運用管理ツールクライアントプログラムである。TOE は、2 つのサーバープログラムがインストールされた奉行 V ERP サーバーと 2 つのクライアントプログラムがインストールされた奉行 V ERP クライアントから構成される。スタンドアロンは対象外である。

奉行 V ERP サーバーPC 及び奉行 V ERP クライアント PC は利用者が作業を行う執務室に設置される。執務室では、経営者、及びすべての管理者、一般利用者を含むその企業に所属する従業員が作業を行う。

サーバー機能は、Windows Server 2003 Standard Edition Service Pack2、SQL Server 2005 Standard Edition、.NetFramework 2.0、及び Internet Explorer 6.0 Service Pack 2 の IT 環境で動作する。

クライアント機能は Windows Vista Business、.NetFramework 2.0、及び Internet Explorer 7.0 Service Pack 2 の IT 環境で動作する。

また、サーバーOS に搭載されたハードディスクの空き容量が物理的に限界値に達するなどの問題が発生し、勘定奉行 V ERP Standard Edition または運用管理ツール上の処理が出来ないという場合は、本 ST の対応範囲外とする。

想定される環境は以下の通りとする。

奉行 V ERP サーバーには勘定奉行 V ERP Standard Edition と運用管理ツールのサーバープログラムが、奉行 V ERP クライアントには勘定奉行 V ERP Standard Edition と運用管理ツールのクライアントプログラムがインストールされている。

保護資産は企業内 LAN に接続する奉行 V ERP サーバーに配置される。

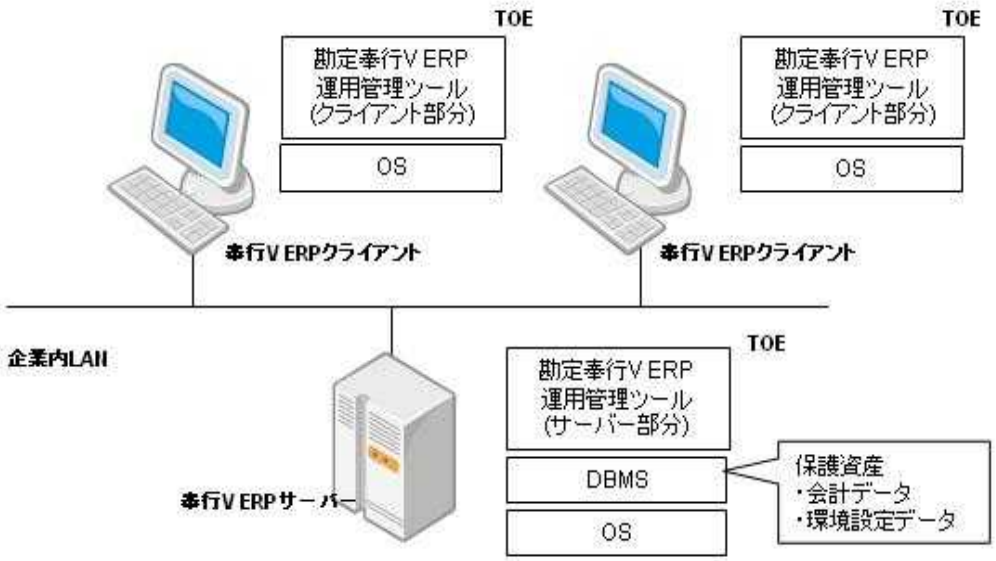

図1.3.3TOE利用環境[TOE運用環境]

1.3.4 TOE 利用方法

TOE の一般的な利用方法は以下の通りである。

① システム管理者は、TOE（奉行 V ERP クライアント）を利用して識別と認証を行う。システム管理者は識別と認証に成功した場合のみ、経営者によって任命されたアカウント管理者・ログ管理者・権限管理者・業務管理者の識別認証データを導入時に登録する。

② ログ管理者は、TOE（奉行 V ERP クライアント）を利用して識別と認証を行う。ログ管理者は識別と認証に成功した場合のみ、TOE（奉行 V ERP クライアント）でどの操作に関するログを取るのかを設定し、対象のログを作成し、参照することが出来る。不適切な操作のログを発見した場合は、適切な対応を行う。

③ アカウント管理者は、TOE（奉行 V ERP クライアント）を利用して識別と認証を行う。アカウント管理者は識別と認証に成功した場合のみ、TOE（奉行 V ERP クライアント）を利用する利用者のアカウントを作成することが出来る。

④ 権限管理者は、TOE（奉行 V ERP クライアント）を利用して識別と認証を行う。権限管理者は識別と認証に成功した場合のみ、TOE（奉行 V ERP クライアント）の一般利用者に対して権限を与えることが出来る。

⑤ 業務管理者は、TOE（奉行 V ERP クライアント）を利用して識別と認証を行う。業務管理者は、識別と認証に成功した場合にのみ、TOE（奉行 V ERP クライアント）のうち勘定奉行 V ERP Standard Edition に対してフルコントロールの権限を持つ。通常の業務では、一般利用者の入力したデータの正確性、

正当性、完全性を確認し承認するなどの会計処理上の操作を行う。データに誤りがある場合には、一般利用者に修正を指示し、問題がなければ承認する。また、決算期には、業務締めが完了した期間に対する仕訳伝票データの更新を禁止するために、TOE（奉行Ｖ ERP クライアント）を利用してその期間の仕訳伝票データをロックすることが出来る。

⑥ 一般利用者は、TOE（奉行Ｖ ERP クライアント）を利用して識別と認証を行う。一般利用者は、識別と認証に成功した場合にのみ、仕訳伝票データの入力や勘定科目マスタの更新、財務情報の集計、財務報告書の作成を行うことが出来る。

奉行Ｖ ERP サーバーはインストール以外で通常利用することはない。

1.3.5 TOE 以外のハードウェア/ファームウェア/ソフトウェア

TOE が動作するための環境をいかに、記述する。

表 1.3.4（1） TOE 以外のハードウェア

ハードウェアの要素	仕様
奉行 V ERP サーバー	- Xeon 2.8GHz - メモリ容量 1GB - HDD 50GB 以上 - ネットワークインタフェース
奉行 V ERP クライアント	- Intel Core 2 Duo 1.80Ghz - メモリ容量 2GB - HDD 50GB 以上 - ネットワークインタフェース

表 1.3.4（2） TOE 以外のソフトウェア

ソフトウェアの要素	製品種別
奉行 V ERP サーバー	・ Windows Server 2003 Standard Edition Service Pack 2 ・SQL Server 2005 Standard Edition ・.NetFramework 2.0 ・Internet Explorer 6.0 Service Pack 2
奉行 V ERP クライアント	・Windows Vista Business ・.NetFramework 2.0 ・Internet Explorer 7.0

1.4 TOE 記述

本章では、TOE の利用者役割、TOE の論理的範囲、及び TOE の物理的範囲について記述する。

1.4.1 TOE 利用者役割

- 経営者
  - 組織すべての活動について最終的な責任を有している。
  - 会計処理の責任者として信頼できるシステム管理者を任命し、権限を委任することが出来る。
  - TOE を攻撃する可能性はない。
- システム管理者
  - TOE 全体を管理する。
  - [システム管理]権限を有する管理者。
  - 導入時にアカウント管理者、ログ管理者、権限管理者、業務管理者を登録する。
  - 以下の管理機能を実施できる。
    - 利用者 ID（システム管理者以外）の管理（問い合わせ、改変、削除、登録）機能
    - パスワードの管理（改変、登録）機能
    - 自身のパスワードの改変機能
    - パスワードポリシーデータ、アカウントポリシーデータの改変機能
    - ログポリシーデータの改変機能
    - 利用者アカウントロックデータの改変機能
    - 利用者権限（[会計担当]権限以外）の管理（問い合わせ、削除 、設定）機能
    - 利用者権限（[会計担当]権限）の管理（問い合わせ、削除、設定）機能
    - 仕訳伝票データ更新ロックデータの問い合わせ、実行機能
  - TOE を攻撃する可能性はない。
- アカウント管理者
  - [利用者管理]権限を有する管理者。
  - 以下の管理機能を実施できる。
    - 利用者 ID（システム管理者以外）の管理（問い合わせ、改変、削除、登録）機能
    - パスワードの管理（改変、登録）機能
    - 自身のパスワードの改変機能

- 利用者アカウントロックデータの改変機能

➢ TOE を攻撃する可能性はない。

・ ログ管理者
  ➢ [ログ管理]権限を有する管理者。ログの参照が出来る。
  ➢ 以下の管理機能を実施できる。
    - ログポリシーデータの改変機能
    - 自身のパスワードの改変機能
  ➢ TOE を攻撃する可能性はない。
・ 権限管理者
  ➢ [権限管理]権限を有する管理者。
  ➢ TOE の利用者に対して権限を付与する。
  ➢ 以下の管理機能を実施できる。
    - 利用者権限（[会計担当]権限）の管理（問い合わせ、削除、設定）機能
    - 自身のパスワードの改変機能
  ➢ TOE を攻撃する可能性はない。
・ 業務管理者
  ➢ [業務管理]権限を有する管理者。
  ➢ 一般利用者に対して、指示や統制を実施する責任を持つ。
  ➢ 月次や四半期など定期的に仕訳伝票データ更新ロック（締処理）を行う。
  ➢ 以下の管理機能を実施できる。
    - 仕訳伝票データ更新ロックデータの問い合わせ、実行機能
    - 自身のパスワードの改変機能
  ➢ TOE を攻撃する可能性はない。
・ 一般利用者
  ➢ [会計担当]権限を有する利用者。
  ➢ 勘定科目マスタの登録、修正、削除、仕訳伝票データの入力、修正、削除、キャッシュ・フロー調整金額明細データの入力、修正、削除、期首残高データの入力を行い、都度内容を出力し確認する。
  ➢ 以下の管理機能を実施できる。
    - 自身のパスワードの改変機能
  ➢ 会計処理上の不正な操作を行う可能性がある。ただし、TOE を介さずに OS や DBMS を直接操作して TOE の保護資産にアクセスすることはできない。
・ 非許可従業員
  ➢ TOE にアカウントが登録されていない従業員。

- 会計処理上の意図的な不正操作を行う可能性がある。
- 財務会計パッケージソフトウェアの標準機能で実行できる範囲で不正操作を試みる可能性がある。ただし、本 ST の意図する運用環境では、企業内 LAN 上の機器から OS や DBMS を直接操作して TOE の保護資産にアクセスすることはできない。

1.4.2 TOE 論理的範囲

本 TOE は、仕訳伝票データを作成し、決算時に財務報告書を作成する財務会計パッケージソフトウェアである「勘定奉行 V ERP Standard Edition」と財務会計パッケージソフトウェアの利用者関連の処理やログを作成・閲覧する「運用管理ツール」である。

提供される機能は以下の機能である。

(1) 基本機能

- 利用者登録機能
- マスタ登録機能（勘定科目や取引先など）
- 仕訳伝票登録機能
- 帳票出力機能
- 財務報告書作成機能

(2) セキュリティ機能

- 利用者識別認証

TOE を利用可能とする前に、TOE の利用者であることを識別認証する必要がある。本 TOE では、利用者 ID・パスワードを使用して、TOE へのアクセスの許可/非許可を判断する。パスワード入力時には、利用者が入力した文字数分の固定文字のみを表示し、パスワードの漏えいのリスクを低減する。

- 監査証跡

TOE 上での操作のログを作成し、閲覧する機能。監査証跡を閲覧できる管理者はシステム管理者とログ管理者のみに限定される。システム管理者とログ管理者は必要なときに必要なログを確認することが出来る。

- 会計データ（勘定科目マスタを除く）アクセス制御

会計データ（勘定科目マスタを除く）のアクセス制御を行なう機能。システム管理者、業務管理者、一般利用者のみに会計データ（勘定科目マスタを除く）へのアクセスを許可する。

- 仕訳伝票データ更新ロック

期間を指定して、TOE 上で仕訳伝票データ更新ロックを行うことで、その期間に含まれる仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データの新規登録、修正、削除が制限され、不正にまたは誤って財務

諸表に関する金額が変わることを防ぐ。

- 環境設定データ管理

利用者識別データ、利用者権限データ、パスワードポリシーデータ、ログポリシーデータなどのTOEのセキュリティ機能に影響を与えるデータを環境設定データとし、その環境設定データを設定・参照できる機能を指す。環境設定データは、導入時に設定するデータや、一度設定したら通常は変更しないデータであるため、むやみに変更が出来ないように設定できる管理者を制限している。ただし、パスワードは定期的な変更が必要なため、システム管理者、アカウント管理者、ログ管理者、権限管理者、業務管理者、一般利用者に変更を許可している。システム管理者、アカウント管理者以外は、自身のパスワードのみ変更ができる。

1.4.3 TOE 物理的範囲

以下の図の破線内に示される部分が TOE の物理的範囲である。

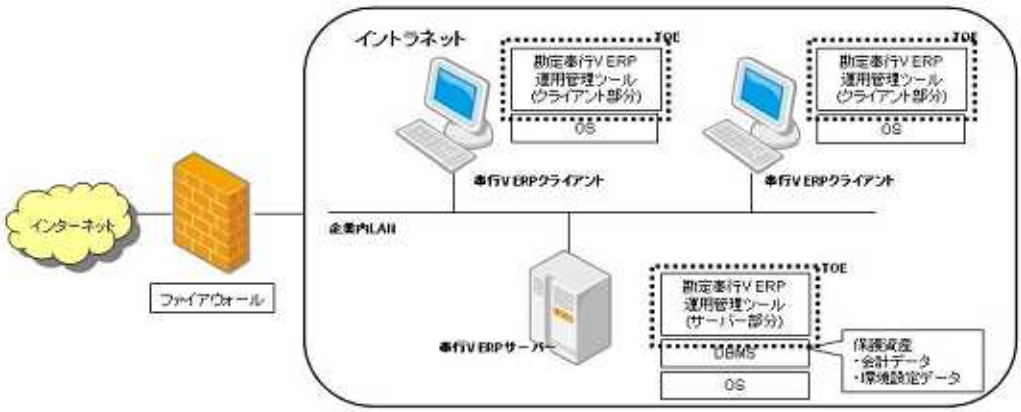

図1.4.3TOE物理的範囲

以下に述べる環境で CC の検証を行った。

(1) ハードウェア構成と概要

① 奉行 V ERP クライアント：

TOE 利用者が TOE にアクセスするために用いる PC。TOE の一部である TOE のクライアント機能（クライアント部分）が搭載される。

OS は Windows Vista Business とする。

② 奉行 V ERP サーバー：

会計データ、環境設定データが格納されているサーバー。主として TOE の一部である TOE のサーバー機能（サーバー部分）が搭載される。

OS は Windows Server 2003 Standard Edition Service Pack2 とする。

③ 企業内 LAN：

企業内に敷設されたローカルエリアネットワーク。奉行 V ERP クライアントと奉行 V ERP サーバーを接続する。

④ ファイアウォール：

インターネットから企業内 LAN までのネットワークに流れる通信を制御している。

(2) ソフトウェア構成と概要

① 勘定奉行 V ERP Standard Edition（バージョン 1.05）：

勘定奉行 V ERP サーバープログラムのインストールされた奉行 V ERP サーバ

ーではクライアントからの要求に対して、仕訳伝票データの登録や勘定科目マスタの更新、財務報告書の作成などのサービスを提供する。
また、勘定奉行Ｖ ERP クライアントプログラムがインストールされた奉行Ｖ ERP クライアントでは、勘定奉行Ｖ ERP に対する操作を行い、奉行Ｖ ERP サーバーに対してその操作に対する結果を要求する。

② 運用管理ツール（バージョン 1.05）：
運用管理ツールサーバープログラムのインストールされた奉行Ｖ ERP サーバーではクライアントからの要求に対して、利用者・ログ関連のサービスを提供する。
また、運用管理ツールクライアントプログラムがインストールされた奉行 Ｖ ERP クライアントでは、運用管理ツールに対する操作を行い、奉行Ｖ ERP サーバーに対してその操作に対する結果を要求する。

③ DBMS：
奉行Ｖ ERP サーバーPC 上で稼動し、会計データ、環境設定データなどを格納するデータベース管理ソフトウェア。DBMS の持つ保護メカニズムによって、DBMS が管理する会計データ、環境設定データへのアクセスに対する TOE 以外からのアクセスを防止する効果を持つ。本 TOE では Microsoft SQL Server 2005 Standard Edition を利用する。

④ OS：
サーバー及びクライアント PC 上で稼動するオペレーティングシステム。OS の持つ保護メカニズムを利用することによって、OS が管理する環境設定データや会計データを含むファイルに対する TOE 以外からのアクセスを防止する効果を持つ。

⑤ その他のソフトウェア：
奉行Ｖ ERP サーバー

- .NetFramework 2.0
- Internet Explorer 6.0 Service Pack 2

奉行Ｖ ERP クライアント

- .NetFramework 2.0
- Internet Explorer 7.0

(3) ガイダンス文書

- 奉行 Ｖ ERP シリーズ　セットアップマニュアル＜ネットワーク対応版＞　平成 20 年 9 月 1 日　初版
- 勘定奉行Ｖ ERP　ガイドブック　平成 20 年 6 月 1 日第 2 版
- 勘定奉行Ｖ ERP　データコンバートマニュアル　平成 20 年 6 月 1 日第 2 版

- 勘定奉行Ｖ ERP　出力帳票集　平成 20 年 6 月 1 日第 2 版
- 奉行Ｖ ERP シリーズ　奉行アップデートサービス　平成 20 年 5 月 15 日第 2 版
- 奉行Ｖ ERP シリーズ　管理者マニュアル　平成 20 年 7 月 1 日第 3 版
- ISO15408 対応ガイダンス　平成 21 年 3 月 16 日初版
- TOE（オンラインマニュアル）－勘定奉行Ｖ ERP
- TOE（オンラインマニュアル）－運用管理ツール

2　適合主張

2.1　CC 適合主張

本 ST および TOE の CC 適合主張は、以下のとおりである。

ST と TOE が適合を主張する CC のバージョン：

●パート１：概説と一般モデル

2006 年 9 月　バージョン 3.1　改訂第 1 版　翻訳第 1.2 版

●パート２：セキュリティ機能コンポーネント

2007 年 9 月　バージョン 3.1　改訂第 2 版　翻訳第 2.0 版

●パート３：セキュリティ保証コンポーネント

2007 年 9 月　バージョン 3.1　改訂第 2 版　翻訳第 2.0 版

CC パート 2 に対する本 ST の適合は、CC パート 2 適合である。

CC パート 3 に対する本 ST の適合は、CC パート 3 適合である。

2.2　PP 主張、パッケージ主張

2.2.1 PP 主張

本 ST が適合している PP はない。

2.2.2 パッケージ主張

EAL1 追加に適合

追加保証コンポーネントは ASE_OBJ.2、ASE_REQ.2 及び ASE_SPD.1 である。

3 セキュリティ課題定義

3.1 前提条件

A.システム・ネットワーク環境

勘定奉行 V ERP および運用管理ツールを利用する環境は企業内 LAN 上に構築する。奉行 V ERP サーバーは、適切に設定したファイアウォールによってシステム管理者が許可したパケットのみを通すよう外部ネットワークからのアクセスを制限し、また、奉行 V ERP サーバーに直接ログインできる利用者をシステム管理者のみに制限する。さらに内部ネットワークは盗聴されないよう暗号装置などを使用して対策を講じる。

A.TOE のセットアップ

TOE のセットアップは、Windows の Administrator もしくは Administrators グループに所属するアカウントを持つシステム管理者が行う。

A.バックアップ

ログ管理者は不測の事態に備えて監査ログのバックアップを実施し、業務管理者は会計データのバックアップを実施する。

A.バックアップ媒体の保護

定期的に実施したバックアップは以下のように管理する。

- 会計データのバックアップについては、業務管理者がバックアップ媒体を施錠出来るキャビネットなどに保管し業務管理者以外アクセスできないようにする。
- 監査ログのバックアップについてはログ管理者がバックアップ媒体を施錠出来るキャビネットなどに保管しログ管理者以外アクセスできないようにする。

A.正確な日付・時刻

TOE を構成する OS はシステム管理者によって正確な日付・時刻が設定されるものとする。

A.Windows のパスワードの設定

TOE がインストールされる PC の OS(Windows)の Administrator または Administrators グループに所属するアカウントのパスワードはシステム管理者によって他人に知られないように管理され、パスワードポリシーは以下の通り設定するものとする。

- 最小パスワード長：8 文字以上
- 文字種類：英大文字・英小文字・数字・記号から 3 種類含む
- パスワードの有効期限：30 日

A.パスワードの設定

管理者（システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者）および一般利用者のパスワードは他人に知られないように管理される。システム管理者は、パスワードポリシーとして以下の通り設定するものとする。

- 最小パスワード長：8 文字以上
- 文字種類：英大文字・英小文字・数字・記号から 3 種類含む
- パスワードの有効期限：30 日

A.アカウントポリシーの設定

システム管理者は、アカウントのポリシーとして以下の通り設定するものとする。

- ログイン失敗時の累積回数：3 回以下
- ロックアウト自動解除時間：0（「解除しない」）

A.ログポリシーの設定

ログ管理者は、認証ログ、メニューログ、アクションログを取り、さらにアクションログの中でも詳細（新規登録や修正登録など）までログを取るように設定するものとする。

A.一般利用者の権限

一般利用者の権限は、権限管理者によって設定され、締処理に関する権限以外の権限を与えられる。

A.OS タイムスタンプ

TOE が稼動する OS は、高信頼のタイムスタンプを提供する。

A.管理者の前提

システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者は TOE のセキュリティ機能に関する必要な知識を持ち、悪意を持った不正をおこなわない。

システム管理者は、勘定奉行 V ERP サーバーに繋がる勘定奉行 V ERP クライアントの台数を管理し､勘定奉行 V ERP サーバーのディスク容量を管理しなければならない。

ログ管理者は、定期的に監査証跡を確認し、不正な痕跡、または誤った操作が発見された場合適切な処置を取らなければならない。

3.2 脅威

T.非許可従業員による不正使用

許可のない利用者が正当な利用者になりすまし、不正にログインして会計データを作成してしまうかもしれない。

T.一般利用者による不正操作または誤操作

一般利用者による TOE を使用した以下の不正操作または誤操作により財務報告書の金額や勘定科目の正確性を損なうかもしれない。

<不正操作>

- 業務管理者により承認されていない勘定科目マスタの登録
- 業務管理者により承認されていない仕訳伝票データの入力
- 業務管理者により承認されていないキャッシュ・フロー調整金額明細データの入力
- 業務管理者により承認されていない期首残高データの入力

- 既存の勘定科目マスタの不正な修正、削除
- 既存の仕訳伝票データの不正な修正、削除
- 既存のキャッシュ・フロー調整金額明細データの不正な修正、削除
- 既存の期首残高データの入力

<誤操作>
- 勘定科目マスタの登録、修正、削除における誤操作
- 仕訳伝票データの入力、修正、削除における誤操作
- キャッシュ・フロー調整金額明細データの入力、修正、削除における誤操作
- 期首残高データの入力における誤操作

3.3　組織のセキュリティ方針

P.内部統制の構築・整備

経営者は業務執行を直接監督する仕組み、及び会計帳簿や計算書類等の適正性を確保するための仕組みとして、内部統制を構築・整備するために、職務分掌を実現する。TOE においても、システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者・一般利用者というように役割をわけて運用している。

4　セキュリティ対策方針

4.1　TOE のセキュリティ対策方針

O.利用者識別認証

TOE は、利用者が TOE を利用するときは、以下に示す機能を実施しなければならない。

- TOE は、利用者が TOE を利用するときは、必ず識別認証されることを保証し、指定された回数以内に識別認証に成功した利用者のみ TOE の利用を許可する。ただし、システム管理者は例外であり、指定された回数以内に識別認証に成功しなくても識別認証にさえ成功すれば TOE の利用を許可する。
- TOE は、指定された回数識別認証に失敗した場合は、そのシステム管理者以外の利用者をロックし、ロック後はその利用者からの識別認証を拒否する。システム管理者またはアカウント管理者によるロックの解除が実施された場合、ロックを解除する。
- TOE は、利用者がパスワードを入力している間は、固定された文字を表示する。
- TOE は、パスワードが指定された品質尺度を満たしていることを保証しなければならない。

O.監査証跡

TOE は、以下の監査事象を監査ログとして、記録、及び管理する。

＜会計データ＞

- 勘定科目マスタの登録、修正、削除の成功、失敗
- 仕訳伝票データの入力、修正、削除の成功、失敗
- キャッシュ・フロー調整金額明細データの入力、修正、削除の成功、失敗
- 期首残高データの入力の成功、失敗

＜環境設定データ＞

- 利用者 ID の改変、削除、登録
- パスワードの登録
- 仕訳伝票データ更新ロックデータの実行の成功、失敗
- ログポリシーデータの改変の成功、失敗
- アカウントポリシーデータの改変の成功、失敗
- パスワードポリシーデータの改変の成功、失敗
- 監査記録の参照の成功、失敗
- パスワード認証の成功、失敗
- 利用者 ID 識別の成功、失敗
- 利用者権限の削除、設定の成功、失敗

・ 利用者アカウントロックデータの改変の成功、失敗

また、監査ログに関しては、以下に示す機能を実施しなければならない。

- TOE は、監査ログの参照をシステム管理者、ログ管理者に制限する。また、参照する場合は、指定された条件によって監査ログを抽出する。監査ログに対する操作は、参照以外提供しない。
- TOE は、監査ログを記録する場合は、事象の日付・時刻、事象の種別、メニュー情報、及び事象の結果を記録する。また、監査機能の起動、及び終了を記録する。

O.仕訳伝票データ更新ロック

TOE は、システム管理者または業務管理者により承認された会計データに対し仕訳伝票データ更新ロックをすることで、ロックした仕訳伝票データ、キャッシュ･フロー調整金額明細データ、期首残高データの操作を制限しなければならない。

- 許可された利用者プロセスの権限が[システム管理]権限もしくは[業務管理]権限もしくは[会計担当]権限でかつ､仕訳伝票データ更新ロックが実行されていない場合、仕訳伝票データの入力・修正・削除・参照、キャッシュ・フロー調整金額明細データの入力・修正・削除・参照、期首残高データの入力・参照を許可する。
- 許可された利用者プロセスの権限が[システム管理]権限もしくは[業務管理]権限もしくは[会計担当]権限でかつ、仕訳伝票データ更新ロックが実行された場合、仕訳伝票データの参照、キャッシュ・フロー調整金額明細データの参照、期首残高データの参照を許可する。

O.環境設定データ管理

TOE は、環境設定データに関して権限のある管理者のみが操作をすることを制限しなければならない。

- TOE は、利用者 ID （システム管理者以外）の問い合わせ・改変・削除・登録をシステム管理者、アカウント管理者に制限する。
- TOE は、パスワード（システム管理者以外）の登録をシステム管理者、アカウント管理者に制限する。TOE は、システム管理者、アカウント管理者がパスワードの登録するときは、定義された品質尺度に一致した場合、登録を許可する。
- TOE は、利用者自身のパスワードの改変をシステム管理者、アカウント管理者、ログ管理者、業務管理者、権限管理者、一般利用者に制限する。なお、TOE はシステム管理者、及びアカウント管理者によるすべての利用者のパスワードの改変を許可する。TOE は、システム管理者、アカウント管理者、ログ管理者、業務管理者、権限管理者、一般利用者がパスワードの改変をするときは、定義された品質尺度に一致した場合、改変を許可する。
- TOE は､パスワードポリシーデータとアカウントポリシーデータの改変をシステム

管理者に制限する。この設定はパスワードの登録・改変にも適用される。

- TOE は、ログポリシーデータの改変をシステム管理者、ログ管理者に制限する。ログポリシーデータの設定に従い、TOE でログが作成される。
- TOE は、利用者のアカウントロックデータの改変をシステム管理者、アカウント管理者に制限する。
- TOE は、利用者権限データ（アカウント管理者・ログ管理者・権限管理者・業務管理者）の問い合わせ・削除・設定をシステム管理者に制限する。
- TOE は、利用者権限データ（一般利用者）の問い合わせ・削除・設定をシステム管理者、権限管理者に制限する。

4.2 運用環境のセキュリティ対策方針

OE.プルーフリスト確認

業務管理者は、一般利用者が勘定科目マスタ、仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データに対する操作をした際に、都度登録内容をプルーフリストとして出力し、前回出力したプルーフリストとの差分を確認し、その結果を記録・保管し、経営者に報告しなければならない。

OE.操作履歴確認

ログ管理者は、会計上の不正や誤謬が発生していないか、TOE の認証ログ、メニューログ、アクションログを利用して操作された内容を定期的に確認しなければならない。また、不正や誤謬が発見された場合は、企業の内部統制にしたがって適正な方法で是正し、経営者に報告しなければならない。

OE.システム・ネットワーク環境

勘定奉行 V ERP および運用管理ツールを利用する環境は企業内 LAN 上に構築する。奉行 V ERP サーバーは、適切に設定したファイアウォールによってシステム管理者が許可したパケットのみを通すよう外部ネットワークからのアクセスを制限し、また、奉行 V ERP サーバーに直接ログインできる利用者をシステム管理者のみに制限しなければならない。さらに内部ネットワークは盗聴されないよう暗号装置などを使用して対策を講じなければならない。

OE.TOE のセットアップ

TOE のセットアップは、Windows の Administrator もしくは Administrators グループに所属するアカウントを持つシステム管理者が実施しなければならない。

OE.定期的なバックアップ

業務管理者は会計データのバックアップを、ログ管理者は監査ログのバックアップを定期的に実施しなければならない。

OE.バックアップ媒体の管理

定期的に実施したバックアップは以下のように管理しなければならない。

- 会計データのバックアップについては、業務管理者がバックアップ媒体を施錠出来るキャビネットなどに保管し業務管理者以外アクセスできないようにしなければならない。
- 監査ログのバックアップについてはログ管理者がバックアップ媒体を施錠出来るキャビネットなどに保管しログ管理者以外アクセスできないようにしなければならない。

OE.正確な日付・時刻

日付・時刻は利用する OS のシステム日付・時刻を利用するが、システム日付・時刻が正しい状態であるかシステム管理者が管理する。

OE.Windows のパスワードの設定

TOE がインストールされる PC の OS(Windows)の Administrator または Administrators グループに所属するアカウントのパスワードは、システム管理者が他人に知られないように管理し、さらにシステム管理者は当該アカウントのパスワードポリシーを以下のように設定しなければならない。

- 最小パスワード長：8 文字以上
- 文字種類：英大文字・英小文字・数字・記号から 3 種類含む
- パスワードの有効期限：30 日

OE.パスワードの設定

システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者および一般利用者はパスワードが他人に知られないように管理しなければならない。すべての利用者は、パスワードを以下のように設定しなければならない。

- 最小パスワード長：8 文字以上
- 文字種類：英大文字・英小文字・数字・記号から 3 種類含む
- パスワードの有効期限：30 日

OE.アカウントポリシーの設定

システム管理者は、アカウントのポリシーとして以下の通り設定しなければならない。

- ログイン失敗時の累積回数：3 回以下
- ロックアウト解除時間：0（「解除しない」）

OE.ログポリシーの設定

ログ管理者は、認証ログ、メニューログ、アクションログを取り、さらにアクションログの中でも詳細（新規登録や修正登録など）までログを取るように設定しなければならない。

OE.一般利用者の権限

一般利用者の権限は、権限管理者によって設定され、締処理に関する権限以外の権限を与えられる。

OE.OS タイムスタンプ

TOE が稼動する OS は、高信頼のタイムスタンプを提供できなければならない。

OE.管理者の選任と管理

経営者は、システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者に信頼できる者を選任し管理・指導することによりシステム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者が会計処理において不正を行わないことを確実にしなければならない。

また、システム管理者は、奉行Ｖ ERP サーバーに繋がる奉行Ｖ ERP クライアントの台数を管理すること､奉行Ｖ ERP サーバーのディスク容量を管理しなければならない。

4.3　セキュリティ対策方針根拠

表 4.3セキュリティ対策方針根拠　脅威、環境、セキュリティ対策方針

セキュリティ環境 / セキュリティ対策方針	A.システム・ネットワーク環境	A.TOEのセットアップ	A.バックアップ	A.バックアップ媒体の保護	A.正確な日付・時刻	A.Windowsのパスワードの設定	A.パスワードの設定	A.アカウントポリシー	A.ログポリシーの設定	A.一般利用者の権限	A.OSタイムスタンプ	A.管理者の前提	T.非許可従業員による不正使用	T.一般利用者による不正操作または誤操作	P.内部統制の構築・整備
O.利用者識別認証													○		
O.監査証跡													○	○	○
O.仕訳伝票データ更新ロック														○	
O.環境設定データ管理													○	○	○
OE.プルーフリスト確認														○	○
OE.操作履歴確認												○	○	○	○
OE.システム･ネットワーク環境	○														
OE.TOEのセットアップ		○													
OE.定期的なバックアップ			○												
OE.バックアップ媒体の管理				○											
OE.正確な日付･時刻					○										
OE.Windowsのパスワードの設定						○									
OE.パスワードの設定							○								
OE.アカウントポリシーの設定								○							
OE.ログポリシーの設定									○						
OE.一般利用者の権限										○					
OE.OSタイムスタンプ											○				
OE管理者の選任と管理												○			

A.システム・ネットワーク環境

OE.システム・ネットワーク環境により、勘定奉行Ｖ ERP および運用管理ツールを利用する環境は企業内 LAN 上に構築する。奉行Ｖ ERP サーバーは、適切に設定したファイアウォールによってシステム管理者が許可したパケットのみを通すよう外部ネットワークからのアクセスを制限し、また、奉行Ｖ ERP サーバーに直接ログインできる利用者をシステム管理者のみに制限しなければならない。さらに内部ネットワークは盗聴されないよう暗号装置などを使用して対策を講じなければならないとされていることから、A.システム・ネットワーク環境を満たしている。

A.TOE のセットアップ

OE.TOE のセットアップにより、TOE をセットアップするのはシステム管理者に制限され、システム管理者が Windows の Administrator もしくは Administrators グループに属するアカウントであることが保証されていることから、A.TOE のセットアップを満たしている。

A.バックアップ

OE.定期的なバックアップにより、業務管理者が会計データのバックアップを、ログ管理者が監査ログのバックアップを定期的に作成することから A.バックアップを満たしている。

A.バックアップ媒体の保護

OE.バックアップ媒体の管理により、会計データのバックアップについては、業務管理者がバックアップ媒体を施錠出来るキャビネットなどに保管し業務管理者以外アクセスできないようにすること、および監査ログのパックアップについては、ログ管理者がバックアップ媒体を施錠出来るキャビネットなどに保管しログ管理者以外アクセスできないようにすることから A.バックアップ媒体の保護を満たしている。

A.正確な日付・時刻

OE.正確な日付・時刻により、システム管理者によって TOE を利用するマシンの正確な日付・時刻が保たれていることから A.正確な日付・時刻を満たしている。

A.Windows のパスワードの設定

OE.Windows のパスワードの設定により、システム管理者によって最小パスワード長 8 文字、文字種類は英大文字・英小文字・数字・記号から 3 種類含む、パスワードの有効期限 30 日と設定していることから A.Windows のパスワードの設定を満たしている。また、OE.Windows のパスワードの設定により、システム管理者によってパスワードが他人に知られないように管理されていることから、A.Windows のパスワードの設定を満たしている。

A.パスワードの設定

OE.パスワードの設定により、最小パスワード長 8 文字、文字種類は英大文字・英小文字・数字・記号から 3 種類含む、パスワードの有効期限 30 日と設定していることから A.パスワードの設定を満たしている。また、OE.パスワードの設定により、システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者および一般利用者によってパスワードが他人に知られないように管理されていることから、A.パスワードの設定を満たしている。

A.ログポリシー

OE.ログポリシーにより、ログ管理者は、認証ログ、メニューログ、アクションログの詳細設定を取るように設定する。このことから A.ログポリシーを満たしている。

A.一般利用者の権限

OE.一般利用者の権限により、一般利用者の権限は、権限管理者によって設定され、締処理に関する権限以外の権限を与えられることから、A.一般利用者の権限を満たしている。

A.OS タイムスタンプ

OE.OS タイムスタンプにより、TOE を利用する PC にインストールされている OS は信頼

できる日付・時刻を提供することから、A.OS タイムスタンプを満たしている。

A. 管理者の前提

OE.管理者の選任と管理により、システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者は会計処理において不正を行わないことを確実にしている。またシステム管理者は、奉行Ｖ ERP サーバーに繋がる奉行Ｖ ERP クライアントの台数を管理し、奉行Ｖ ERP サーバーのディスク容量を管理する。

また、OE.操作履歴確認により、ログ管理者は、定期的に監査証跡を確認し、不正な痕跡、または誤った操作が発見された場合適切な処置を取る。以上により、A.管理者の前提を満たしている。

T.非許可従業員による不正使用

非許可従業員は、O.利用者識別認証により識別認証されなければ、TOE を利用することができないため脅威を軽減している。O.環境設定データ管理により環境設定データに関しては、許可された利用者にのみ操作を限定しているため、O.利用者識別認証を破りさらには、許可された利用者でログインしない限りは不正に操作することはできない。つまり脅威を軽減している。また、非許可従業員が、TOE の識別認証に対して、不正な試行を行った結果は、O.監査証跡により監査証跡として保管され、この監査証跡を OE.操作履歴確認によりログ管理者が定期的に操作履歴を確認することにより、不正な試みを確認し注意喚起等による牽制を行うことが出来るため脅威を緩和できる。

以上の対策方針により、T.非許可従業員による不正使用に対抗できる。

T.一般利用者による不正操作または誤操作

業務管理者が、期間を指定して O.仕訳伝票データ更新ロックを定期的に実行することにより、その期間の財務報告書に関する仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データをロックすることが出来る。ロックすることにより、不正操作または誤操作を防ぐことが出来るため脅威を軽減している。また、O.環境設定データ管理により環境設定データに関しては、許可された利用者にのみに操作を限定しているため環境設定データを不正に操作することはできない。つまり脅威を軽減している。

たとえ、不正操作または誤操作が起こってしまった場合でも O.監査証跡でログ（認証ログ・メニューログ・アクションログ）を確認することで一般利用者が操作した詳細なログを把握することが出来る。さらに OE.操作履歴確認によりログ管理者が定期的に操作履歴を確認することで、不正な試み、または誤った操作を確認し注意喚起等による牽制を行うことが出来る。つまり、脅威を緩和している。

また、業務管理者が OE.プルーフリストにより勘定科目マスタ、仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データのプルーフリストを操作完了時に都度登録内容をプルーフリストとして出力し、前回出力時との差分を比較確認することによって勘定科目マスタ、仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データに対する操作を把握することが出来、不正操作や誤操作に気づくことが出来るため

脅威を緩和している。
以上のことから、T.一般利用者による不正操作または誤操作に対抗できる。

P.内部統制の構築・整備

経営者は、システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者・一般利用者というように権限ごとに利用者をわけることで職務分掌を実現する。TOE 上では、利用者権限データに対する権限のある管理者のみが利用者権限を操作することが O.環境設定データ管理により担保されている。権限を設定した際のログは O.監査証跡により監査証跡として保管される。
職務分掌を実現した結果、会計業務に関する TOE 上の会計処理は一般利用者が実施する。一般利用者が作成した会計帳簿や計算書類等の適正性は OE.操作履歴確認でログ管理者が、OE.プルーフリスト確認で業務管理者が確認することにより担保される。
職務分掌を実施し、会計データや財務情報に関する IT 統制の一環として TOE を使用した会計処理の業務執行を監督する仕組み、及び会計帳簿や計算書類等の適正性を確保するための仕組みを実現することで、P.内部統制の構築･整備は満たされる。

5　拡張コンポーネント定義

本 ST は拡張コンポーネントを定義しない。

6　セキュリティ要件

6.1　セキュリティ機能要件

● セキュリティ監査（FAU）

FAU_GEN.1 監査データ生成

下位階層：なし

依存性：FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1

TSF は、以下の監査対象事象の監査記録を生成できなければならない。

a) 監査機能の起動と終了；

b) 監査の[選択：*最小*、*基本*、*詳細*、*指定なし*：から一つのみ選択]レベルのすべての監査対象事象；及び

c) [割付：*上記以外の個別に定義した監査対象事象*]

[選択：*最小*、*基本*、*詳細*、*指定なし*：から一つのみ選択]：指定なし

[割付：*上記以外の個別に定義した監査対象事象*]：

表 6.1 の監査対象事象、及び勘定科目マスタの登録、修正、削除の成功と失敗

表　6.1 セキュリティ機能要件　監査事象リスト

TOE にて選択した機能要件	CCPart2 で規定された監査対象	監査対象事象
FAU_GEN.1	予見される監査対象事象はない	なし
FAU_SAR.1	基本：監査記録からの情報の読み出し。	監査記録の参照の成功と失敗
FAU_SAR.3	詳細：閲覧に使用されるパラメタ	なし
FDP_ACC.1	予見される監査対象事象はない	なし
FDP_ACF.1	最小：SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 基本：SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求 詳細：アクセスチェック時に用いられる特定のセキュリティ属性。	・仕訳伝票データの入力、修正、削除の成功と失敗 ・キャッシュ・フロー調整金額明細データの入力、修正、削除の成功と失敗 ・期首残高データの入力の成功と失敗

TOE にて選択した機能要件	CCPart2で規定された監査対象	監査対象事象
FIA_AFL.1	最小：不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション（たとえば端末の停止）、もし適切であれば、正常状態への復帰（たとえば端末の再稼動）	なし
FIA_ATD.1	予見される監査対象事象はない	なし
FIA_SOS.1	最小：TSF による、テストされた秘密の拒否 基本：TSF による、テストされた秘密の拒否または受入 詳細：定義された品質尺度に対する変更の識別	なし
FIA_UAU.2	最小：認証メカニズムの不成功になった使用 基本：認証メカニズムのすべての使用	・パスワード認証の成功と失敗
FIA_UAU.7	予見される監査対象事象はない	なし
FIA_UID.2	最小：提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 基本：提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用	・利用者 ID 識別の成功と失敗
FIA_USB.1	最小：利用者セキュリティ属性のサブジェクトに対する不成功結合（たとえばサブジェクトの生成） 基本：利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗（たとえば、サブジェクトの生成の成功または失敗）	なし

TOE にて選択した機能要件	CCPart2 で規定された監査対象	監査対象事象
FMT_MSA.1（1）	基本：セキュリティ属性の値の改変すべて	・システム管理者による[利用者管理]権限、[ログ管理]権限、[権限管理]権限、[業務管理]権限の削除、設定の成功と失敗
FMT_MSA.1（2）	基本：セキュリティ属性の値の改変すべて	・システム管理者または権限管理者による[会計担当]権限の削除、設定の成功と失敗
FMT_MSA.1（3）	基本：セキュリティ属性の値の改変すべて	・システム管理者または業務管理者による仕訳伝票データ更新ロックの実行の成功と失敗
FMT_MSA.3	基本: 許可的あるいは制限的規則のデフォルト設定の改変 基本: セキュリティ属性の初期値の改変すべて	なし
FMT_MTD.1（1）	基本：TSF データの値のすべての改変	・システム管理者またはアカウント管理者による利用者 ID（システム管理者以外）の改変、削除、登録の成功と失敗
FMT_MTD.1（2）	基本：TSF データの値のすべての改変	・システム管理者またはアカウント管理者によるパスワード（システム管理者以外）の登録の成功と失敗
FMT_MTD.1（3）	基本：TSF データの値のすべての改変	なし
FMT_MTD.1（4）	基本：TSF データの値のすべての改変	・システム管理者によるパスワードポリシーデータ（最小パスワード長、文字種類、パスワードの有効期限)、アカウントポリシーデータ（ログイン失敗時の累積回数、ロックアウト解除時間（0：解除しない））の改変の成功と失敗

TOE にて選択した機能要件	CCPart2 で規定された監査対象	監査対象事象
FMT_MTD.1（5）	基本：TSF データの値のすべての改変	・システム管理者またはログ管理者によるログポリシーデータ（認証ログ、メニューログ、アクションログ）の改変の成功と失敗
FMT_MTD.1（6）	基本：TSF データの値のすべての改変	・システム管理者またはアカウント管理者による利用者のアカウントロックデータの改変の成功と失敗
FMT_SMF.1	最小：管理機能の使用	なし
FMT_SMR.1	最小：役割の一部をなす利用者のグループに対する改変 詳細：役割の権限の使用すべて	なし

FAU_GEN.1.2

TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）；及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付：*その他の監査関連情報*]。

[割付：*その他の監査関連情報*]：なし

FAU_SAR.1 監査レビュー

下位階層：なし

依存性：FAU_GEN.1 監査データ生成

FAU_SAR1.1

TSF は、[割付：*許可利用者*]が、[割付：*監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

[割付：*許可利用者*]：システム管理者、ログ管理者

[割付：*監査情報のリスト*]：事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）

FAU_SAR1.2

TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

FAU_SAR.3 選択可能監査レビュー
下位階層：なし
依存性 FAU_SAR.1 **監査レビュー**
FAU_SAR.3.1
TSF **は、[割付：*論理的な関連の基準*]に基づいて、監査データの[割付：*選択方法、及び/または並べ替え方法*]を適用する能力を提供しなければならない。**
[割付：*論理的な関連の基準*]：選択された項目（日付・アカウント名・メニュー名・アクション区分）の論理積
[割付：*選択方法、及び/または並べ替え方法*]：選択方法

- **利用者データ保護**（FDP）

FDP_ACC.1 サブセットアクセス制御
下位階層：なし
依存性：FDP_ACF.1 **セキュリティ属性によるアクセス制御**
FDP_ACC.1.1
TSF **は[割付：*サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して、[割付：*アクセス制御 SFP*]を実施しなければならない。**
[割付：*サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]：
サブジェクト：許可された利用者プロセス
オブジェクト：仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データ
SFP **で扱われるサブジェクトとオブジェクト間の操作のリスト：**

- **許可された利用者プロセスによる仕訳伝票データの入力、修正、削除、参照**
- **許可された利用者プロセスによるキャッシュ・フロー調整金額明細データの入力、修正、削除、参照**
- **許可された利用者プロセスによる期首残高データの入力、参照**

[割付：*アクセス制御 SFP*]：
会計処理操作アクセス制御 SFP

FDP_ACF.1 セキュリティ属性によるアクセス制御
下位階層：なし
依存性：FDP_ACC.1 **サブセットアクセス制御**

FMT_MSA.3 静的属性初期化

FDP_ACF.1.1
TSF は、以下の[割付：*示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付：*アクセス制御 SFP*]を実施しなければならない。

[割付：*示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]：
サブジェクト：許可された利用者プロセス
サブジェクトのセキュリティ属性：権限
オブジェクト：仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データ
オブジェクトのセキュリティ属性：仕訳伝票データ更新ロックデータ
[割付：*アクセス制御 SFP*]：
会計処理操作アクセス制御 SFP

FDP_ACF.1.2
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない：[割付：*制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付：*制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]：

- 許可された利用者プロセスが権限（=[システム管理]権限）で関連付けられ、仕訳伝票データ更新ロックが実行されない場合、仕訳伝票データの入力・修正・削除・参照、キャッシュ・フロー調整金額明細データの入力・修正・削除・参照、期首残高データの入力・参照を許可する。
- 許可された利用者プロセスが役割（=[業務管理]権限）で関連付けられ、仕訳伝票データ更新ロックが実行されない場合、仕訳伝票データの入力・修正・削除・参照、キャッシュ・フロー調整金額明細データの入力・修正・削除・参照、期首残高データの入力・参照を許可する。
- 許可された利用者プロセスが役割（=[会計担当]権限）で関連付けられ、仕訳伝票データ更新ロックが実行されない場合、仕訳伝票データの入力・修正・削

除・参照、キャッシュ・フロー調整金額明細データの入力・修正・削除・参照、期首残高データの入力・参照を許可する。

- 許可された利用者プロセスが役割（=[システム管理]権限）で関連付けられ、仕訳伝票データ更新ロックが実行されている場合、仕訳伝票データの参照、キャッシュ・フロー調整金額明細データの参照、期首残高データの参照を許可する。
- 許可された利用者プロセスが役割（=[業務管理]権限）で関連付けられ、仕訳伝票データ更新ロックが実行されている場合、仕訳伝票データの参照、キャッシュ・フロー調整金額明細データの参照、期首残高データの参照を許可する。
- 許可された利用者プロセスが役割（=[会計担当]権限）で関連付けられ、仕訳伝票データ更新ロックが実行されている場合、仕訳伝票データの参照、キャッシュ・フロー調整金額明細データの参照、期首残高データの参照を許可する。

FDP_ACF.1.3
TSF は、次の追加規則、[割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。
[割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]：
なし

FDP_ACF.1.4
TSF は、[割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]：
なし

- 識別の認証（FIA）

FIA_AFL.1 認証失敗時の取り扱い
下位階層：なし
依存性：FIA_UAU.1 認証のタイミング

FIA_AFL.1.1
TSF は、[割付：認証*事象のリスト*]に関して、[選択：*[割付：正の整数値]*、*[割付:許容*

可能な値の範囲]内における*管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。
[割付：認証*事象のリスト*]：
・アカウント管理者認証操作における最後の認証成功以降の不成功認証試行
・ログ管理者認証操作における最後の認証成功以降の不成功認証試行
・権限管理者認証操作における最後の認証成功以降の不成功認証試行
・業務管理者認証操作における最後の認証成功以降の不成功認証試行
・一般利用者認証操作における最後の認証成功以降の不成功認証試行
[*割付:許容可能な値の範囲*]：
・システム管理者が設定した累積認証失敗回数（0～999 回）

FIA_AFL.1.2
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：*アクションのリスト*]をしなければならない。
[割付：*アクションのリスト*]：
対象利用者をロックアウトする。

FIA_ATD.1 利用者属性定義
下位階層：なし
依存性：なし

FIA_ATD.1.1
TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。：[割付：*セキュリティ属性リスト*]
[割付：*セキュリティ属性リスト*]：
利用者権限（[システム管理]権限、[利用者管理]権限、[ログ管理]権限、[権限管理]権限、[業務管理]権限、[会計担当]権限）

FIA_SOS.1 秘密の検証
下位階層：なし
依存性：なし

FIA_SOS.1.1
TSF は、秘密（システム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者・一般利用者のパスワード）が[割付：*定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。

[割付：*定義された品質尺度*]：
以下の事項を設定可能
※設定が出来るのは、システム管理者のみ

- 最小文字数設定（0~14）
- 文字種類（記号、数字など）

FIA_UAU.2 アクション前の利用者認証
下位階層：FIA_UAU.1 認証のタイミング
依存性：FIA_UID.1 識別のタイミング

FIA_UAU.2
TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

FIA_UAU.7 保護された認証フィードバック
下位階層：なし
依存性：FIA_UAU.1 認証のタイミング

FIA_UAU.7.1
TSF は、認証を行っている間、[割付：*フィードバックのリスト*]だけを利用者に提供しなければならない。
[割付：*フィードバックのリスト*]：
入力されたパスワードの文字数分の固定文字

FIA_UID.2 アクション前の利用者識別
下位階層：FIA_UID.1 識別のタイミング
依存性：なし

FIA_UID.2.1
TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功すること要求しなければならない。

FIA_USB.1 利用者・サブジェクト結合
下位階層：なし
依存性：FIA_ATD.1 利用者属性定義

FIA_USB.1.1

TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。: [割付：*利用者セキュリティ属性のリスト*]

[割付：*利用者セキュリティ属性のリスト*]：

- 利用者 ID
- 利用者権限

FIA_USB.1.2

TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付：*属性の最初の関連付けの規則*]

[割付：*属性の最初の関連付けの規則*]：

識別した利用者の利用者 ID と、関連付けられる権限を、その利用者プロセスに関連付ける。

表　6.1　セキュリティ機能要件　FIA_USB.1.2 属性の最初の関連付けの規則

利用者	利用者を代行するサブジェクト	利用者セキュリティ属性	利用者セキュリティ属性の取りうる値
利用者	利用者プロセス	利用者権限	[システム管理]権限 [利用者管理]権限 [ログ管理]権限 [権限管理]権限 [業務管理]権限 [会計担当]権限

FIA_USB.1.3

TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付：*属性の変更の規則*]

[割付：*属性の変更の規則*]：

なし

- セキュリティ管理（FMT）

FMT_MSA.1（1）セキュリティ属性の管理（会計担当者以外の権限管理）

下位階層：なし

依存性：[FDP_ACC.1 サブセットアクセス制御、
または FDP_IFC.1 サブセット情報フロー制御]

FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1（1）
TSF はセキュリティ属性[割付：*セキュリティ属性のリスト*]に対し、[選択：*デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*]をする能力を[割付：*許可された識別された役割*]に制限する[割付：*アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付：*セキュリティ属性のリスト*]：
利用者権限（[利用者管理]権限、[ログ管理]権限、[権限管理]権限、[業務管理]権限）
[選択：*デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*]：
問い合わせ、削除、*[割付：その他の操作]*
[割付：その他の操作]：
設定（権限の付与）
[割付：*許可された識別された役割*]：
システム管理者
[割付：*アクセス制御 SFP、情報フロー制御 SFP*]：
会計処理操作アクセス制御 SFP

FMT_MSA.1（2）セキュリティ属性の管理（会計担当者の権限管理）
下位階層：なし
依存性：[FDP_ACC.1 サブセットアクセス制御、
または FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1（2）
TSF はセキュリティ属性[割付：*セキュリティ属性のリスト*]に対し、[選択：*デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*]をする能力を[割付：*許可された識別された役割*]に制限する[割付：*アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付：*セキュリティ属性のリスト*]：
利用者権限（[会計担当]権限）
[選択：*デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*]：
問い合わせ、削除、*[割付：その他の操作]*
[割付：その他の操作]：

設定（権限の付与）
[割付：*許可された識別された役割*]：
システム管理者、権限管理者
[割付：*アクセス制御 SFP*、*情報フロー制御 SFP*]：
会計処理操作アクセス制御 SFP

FMT_MSA.1（3）セキュリティ属性の管理（仕訳伝票データ更新ロックの管理）
下位階層：なし
依存性：[FDP_ACC.1 サブセットアクセス制御、
　　または FDP_IFC.1 サブセット情報フロー制御]
　　FMT_SMR.1 セキュリティの役割
　　FMT_SMF.1 管理機能の特定

FMT_MSA.1.1（3）
TSF はセキュリティ属性[割付：*セキュリティ属性のリスト*]に対し、[選択：*デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*]をする能力を[割付：*許可された識別された役割*]に制限する[割付：*アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付：*セキュリティ属性のリスト*]：
仕訳伝票データ更新ロックデータ
[選択：*デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*]：
問い合わせ、*[割付：その他の操作]*
[*割付：その他の操作*]：
実行
[割付：*許可された識別された役割*]：
システム管理者、業務管理者
[割付：*アクセス制御 SFP、情報フロー制御 SFP*]：
会計処理操作アクセス制御 SFP

FMT_MSA.3 静的属性初期化
下位階層：なし
依存性：FMT_MSA.1 セキュリティ属性の管理
　　FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1
TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択: 制限的、

許可的、[割付: その他の特性]: から 1 つのみ選択]デフォルト値を与える[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。
[選択: 制限的、許可的、[割付: その他の特性]：
[割付: その他の特性]：
仕訳伝票データ更新ロックが実行されていない
[割付：*アクセス制御 SFP*、*情報フロー制御 SFP*]：
会計処理操作アクセス制御 SFP

FMT_MSA.3.2
TSF は、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。
[割付：許可された識別された役割]：
なし（仕訳伝票データ更新ロックデータに対して、FMT_MSA.3.2 が要求する処理を実現する必要がないため）

FMT_MTD.1（1）TSF データの管理
下位階層：なし
依存性：FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1（1）
TSF は、[割付：*TSF データのリスト*]を[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]する能力を[割付：*許可された識別された役割*]に制限しなければならない。
[割付：*TSF データのリスト*]：
利用者 ID （システム管理者以外）
[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]：
問い合わせ、改変、削除、 [割付：*その他の操作*]
[割付：*その他の操作*]：
登録
[割付：*許可された識別された役割*]：
システム管理者、アカウント管理者

FMT_MTD.1（2）TSF データの管理
下位階層：なし
依存性：FMT_SMR.1 **セキュリティの役割**
FMT_SMF.1 **管理機能の特定**

FMT_MTD.1.1（2）
TSF **は、[割付：***TSF データのリスト***]を[選択：***デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]***]する能力を[割付：***許可された識別された役割***]に制限しなければならない。**
[割付：*TSF データのリスト***]：**
パスワード（システム管理者以外）
[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]***]：**
[割付：*その他の操作***]**
[割付：*その他の操作***]：**
登録
[割付：*許可された識別された役割***]：**
システム管理者、アカウント管理者

FMT_MTD.1（3）TSF データの管理
下位階層：なし
依存性：FMT_SMR.1 **セキュリティの役割**
FMT_SMF.1 **管理機能の特定**

FMT_MTD.1.1（3）
TSF **は、[割付：***TSF データのリスト***]を[選択：***デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]***]する能力を[割付：***許可された識別された役割***]に制限しなければならない。**
[割付：*TSF データのリスト***]：**
パスワード
[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]***]：**
改変
[割付：*許可された識別された役割***]：**
システム管理者、またはアカウント管理者、または当該パスワードの所有者

FMT_MTD.1（4）TSF データの管理

下位階層：なし

依存性：FMT_SMR.1 **セキュリティの役割**

FMT_SMF.1 **管理機能の特定**

FMT_MTD.1.1（4）

TSF **は、**[**割付：***TSF データのリスト*]**を**[**選択：***デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]**する能力を**[**割付：***許可された識別された役割*]**に制限しなければならない。**

[**割付：***TSF データのリスト*]**：**

パスワードポリシーデータ

- **最小パスワード長**
- **文字種類**
- **パスワードの有効期限**

アカウントポリシーデータ

- **ログイン失敗時の累積回数**
- **ロックアウト自動解除設定**

[**選択：***デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]**：**

改変

[**割付：***許可された識別された役割*]**：**

システム管理者

FMT_MTD.1（5）TSF データの管理

下位階層：なし

依存性：FMT_SMR.1 **セキュリティの役割**

FMT_SMF.1 **管理機能の特定**

FMT_MTD.1.1（5）

TSF **は、**[**割付：***TSF データのリスト*]**を**[**選択：***デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]**する能力を**[**割付：***許可された識別された役割*]**に制限しなければならない。**

[**割付：***TSF データのリスト*]**：**

ログポリシーデータ

- **認証ログ**
- **メニューログ**
- **アクションログ**

[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]：
改変
[割付：*許可された識別された役割*]：
システム管理者、ログ管理者

FMT_MTD.1（6）TSF データの管理
下位階層：なし
依存性：FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1（6）
TSF は、[割付：*TSF データのリスト*]を[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]する能力を[割付：*許可された識別された役割*]に制限しなければならない。
[割付：*TSF データのリスト*]：
利用者のアカウントロックデータ
[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]：
改変
[割付：*許可された識別された役割*]：
システム管理者、アカウント管理者

FMT_SMF.1 管理機能の特定
下位階層：なし
依存性：なし

FMT_SMF.1.1
TSF は、以下の管理機能を実行することができなければならない。：[割付：*TSF によって提供される管理機能のリスト*]
[割付：*TSF によって提供される管理機能のリスト*]：

- システム管理者、アカウント管理者による利用者 ID（システム管理者以外）の管理（問い合わせ、改変、削除、登録）機能
- システム管理者、アカウント管理者によるパスワードの管理（登録）機能
- システム管理者、アカウント管理者、当該パスワードの所有者によるパスワードの改変機能
- システム管理者、アカウント管理者によるパスワードの改変機能
- システム管理者によるパスワード、アカウントポリシーの改変機能

- システム管理者、ログ管理者によるログポリシーの改変機能
- システム管理者、アカウント管理者による利用者アカウントロックの改変機能
- システム管理者による利用者権限（[会計担当]権限以外）の管理（問い合わせ、削除、設定）機能
- システム管理者、権限管理者による利用者権限（[会計担当]権限）の管理（問い合わせ、削除、設定）機能
- システム管理者、業務管理者による仕訳伝票データ更新ロックデータの問い合わせ、実行機能

FMT_SMR.1 セキュリティの役割
下位階層：なし
依存性：FIA_UID.1 **識別のタイミング**

FMT_SMR.1.1
TSF **は、役割[割付：*許可された識別された役割*]を維持しなければならない。**
[割付：*許可された識別された役割*]：
システム管理者、アカウント管理者、ログ管理者、権限管理者、業務管理者、一般利用者、当該パスワードの所有者

FMT_SMR.1.2
TSF **は利用者を役割に関連付けなければならない。**

6.2　セキュリティ保証要件

本TOEの評価保証レベルは、EAL1追加（追加する保証コンポーネントはASE_SPD.1、ASE_OBJ.2、ASE_REQ.2）であり、TOEセキュリティ保証要件は以下のとおりである。

表　6.2セキュリティ要件　クラス、保証コンポーネント

クラス	保証コンポーネント	
ADV;開発	ADV_FSP.1	基本機能仕様
AGD;ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ALC;ライフサイクルサポート	ALC_CMC.1	TOEのラベル付け
	ALC_CMS.1	TOEのCM範囲
ASE;セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE要約仕様
ATE;テスト	ATE_IND	独立テスト・準拠
AVA;脆弱性評定	AVA_VAN.1	脆弱性調査

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

以下に TOE のセキュリティ要件根拠を示す。各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対応している。

表 6.3.1セキュリティ機能要件根拠

セキュリティ機能要件 ＼ セキュリティ対策方針	O.利用者識別認証	O.監査証跡	O.仕訳伝票データ更新ロック	O.環境設定データ管理
FAU_GEN.1		○		
FAU_SAR.1		○		
FAU_SAR.3		○		
FDP_ACC.1			○	
FDP_ACF.1			○	
FIA_AFL.1	○			
FIA_ATD.1	○			
FIA_SOS.1	○			○
FIA_UAU.2	○			
FIA_UAU.7	○			
FIA_UID.2	○			
FIA_USB.1	○			
FMT_MSA.1(1)				○
FMT_MSA.1(2)				○
FMT_MSA.1(3)			○	
FMT_MSA.3			○	
FMT_MTD.1(1)				○
FMT_MTD.1(2)				○
FMT_MTD.1(3)				○
FMT_MTD.1(4)				○
FMT_MTD.1(5)				○
FMT_MTD.1(6)				○
FMT_SMF.1				○
FMT_SMR.1	○		○	○

(1) O.利用者識別認証

すべての利用者が TOE を利用する前に、システム管理者、アカウント管理者、ログ管理者、権限管理者、業務管理者、一般利用者であることの識別と認証が成功することを要求すればよい。

A) TOE の使用を許可する前に TOE 利用者の識別認証を実施

TOE では、識別認証が成功しない限りいかなる操作も許可しない。識別認証に成功した場合は、TOE が維持する利用者 ID、利用者権限を、利用者を代行して動作するサブジェクトに関連付ける。

これに該当するセキュリティ機能要件は、FIA_ATD.1、FIA_UID.2、FIA_UAU.2、FIA_USB.1、FMT_SMR.1 である。

B) パスワード品質を保証

TOE ではパスワードポリシーを設定し、各 TOE 利用者はそのポリシーに沿ったパスワードを持つ。強固なパスワードポリシーを設定することでパスワードを試行入力する攻撃が成功する可能性を減少させている。

これに該当するセキュリティ機能要件は、FIA_SOS.1 である。

C) パスワードの暴露防止

TOE で認証を行っている間、入力されたパスワードの文字数分の固定文字のみをフィードバックし、パスワードの暴露の機会を減少させている。

これに該当するセキュリティ機能要件は、FIA_UAU.7 である。

D) 指定回数以上識別認証に失敗した場合の利用者の無効化

識別認証時に指定回数以上失敗すると、TOE の正当な利用者ではないとみなす必要がある。そのため指定回数以上識別認証に失敗した場合には TOE 利用者の利用者 ID を無効化し、TOE へのログインを制限する。いったん無効化された利用者 ID はシステム管理者またはアカウント管理者が無効化を解除するまで識別認証が拒否される。

これに該当するセキュリティ機能要件は FIA_AFL.1 である。

したがって、これらの要件の組み合わせることにより「O.利用者識別認証」を実現する。

(2) O.監査証跡

「O.監査証跡」では、監査記録の取得とその保護について求める。監査記録は操作ログを事後的に確認するためのものであり、必要なときに必要な情報を権限のある管理者が確認する。監査記録はあらかじめ設定したログポリシーに沿って作成され、改ざんは一切出来ないものとする。

A) 監査データの取得

TOE では、以下の事象が発生した場合、事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果を監査証跡として保管する。6.1 セキュリティ機能要件の FAU_GEN.1 で取得する監査証跡は「指定なし」を選択しているが、これはそのほかのセキュリティ対策方針である O.識別認証機能、O.仕訳伝票データ更新ロック機能、O.環境設定データ管理の実現をかんがみて、「指定なし」で十分とする。

また取得した監査証跡は、TOE 上から改変・削除は出来ないため、不正な改変・削除から保護される。

＜会計データ＞

- 勘定科目マスタの登録、修正、削除の成功、失敗
- 仕訳伝票データの入力、修正、削除の成功、失敗
- キャッシュ・フロー調整金額明細データの入力、修正、削除の成功、失敗
- 期首残高データの入力の成功、失敗

＜環境設定データ＞

- 利用者 ID の改変、削除、登録の成功、失敗
- パスワードの登録の成功、失敗
- 仕訳伝票データ更新ロックデータの実行の成功、失敗
- ログポリシーデータの改変の成功、失敗
- アカウントポリシーデータの改変の成功、失敗
- パスワードポリシーデータの改変の成功、失敗
- 監査記録の参照の成功、失敗
- パスワード認証の成功、失敗
- 利用者 ID 識別の成功、失敗
- 利用者権限の削除、設定の成功、失敗
- 利用者アカウントロックデータの改変の成功、失敗

これに該当するセキュリティ機能要件は FAU_GEN.1 である。

B) 監査データの利用者・記録の読み出し方法

取得した監査証跡を読み出しできる利用者を制限する。その利用者以外は監査証

跡に関する権限は一切持たない。
これに該当するセキュリティ機能要件は FAU_SAR.1 である。
また取得した監査証跡を検索ししぼりこんで必要な監査証跡のみを確認することが出来る。
これに該当するセキュリティ機能要件は FAU_SAR.3 である。
したがって、これらの要件の組み合わせにより「O.監査証跡」を実現するのに十分である。

(3) O.仕訳伝票データ更新ロック
「O.仕訳伝票データ更新ロック」を実現するためには、システム管理者または業務管理者によりロックされた仕訳伝票データ・キャッシュ・フロー調整金額明細データ・期首残高データを、それ以降、入力、修正、削除を禁止する機能を提供すればよい。
A) アクセス制御規定の実施
仕訳伝票データ・キャッシュ・フロー調整金額明細データ・期首残高データに対しての操作が許可された利用者と許可された操作を示す。また仕訳伝票データ・キャッシュ・フロー調整金額明細データ・期首残高データに関しては仕訳伝票データ更新ロックというセキュリティ属性があり、それが実行された場合は操作が制限される。以下に具体的な操作を示す。

＜仕訳伝票データ更新ロックが実行された場合＞
- システム管理者の仕訳伝票データに対する参照
- システム管理者のキャッシュ・フロー調整金額明細データに対する参照
- システム管理者の期首残高データに対する参照
- 業務管理者の仕訳伝票データに対する参照
- 業務管理者のキャッシュ・フロー調整金額明細データに対する参照
- 業務管理者の期首残高データに対する参照
- 一般利用者の仕訳伝票データに対する参照
- 一般利用者のキャッシュ・フロー調整金額明細データに対する参照
- 一般利用者の期首残高データに対する参照

＜仕訳伝票データ更新ロックが実行されていない場合＞
- システム管理者の仕訳伝票データに対する入力･修正・削除・参照
- システム管理者のキャッシュ・フロー調整金額明細データに対する入力・修正・削除・参照
- システム管理者の期首残高データに対する入力・参照
- 業務管理者の仕訳伝票データに対する入力･修正・削除・参照

・ 業務管理者のキャッシュ・フロー調整金額明細データに対する入力・修正・削除・参照
・ 業務管理者の期首残高データに対する入力・参照
・ 一般利用者の仕訳伝票データに対する入力･修正・削除・参照
・ 一般利用者のキャッシュ・フロー調整金額明細データに対する入力・修正・削除・参照
・ 一般利用者の期首残高データに対する入力・参照

これに該当するセキュリティ機能要件は FDP_ACC.1、FDP_ACF.1、FMT_MSA.3 である。

B) 仕訳伝票データ更新ロック実施者の限定

仕訳伝票データ更新ロックを実行することで、保護資産である会計データに対するアクセス制御を実現することが出来るが、仕訳伝票データ更新ロックを問い合わせ・実行できる利用者も限定する必要がある。

仕訳伝票データ更新ロックを問い合わせ・実行できる利用者をシステム管理者と業務管理者に制限することで不正を行わない確かな管理者に仕訳伝票データ更新ロックの権限を委ねる。

これに該当するセキュリティ対策方針は FMT_MSA.1（3）である。

以上のことからこれらの要件の組み合わせにより、「O.仕訳伝票データ更新ロック」を実現するのに十分である。

(4) O.環境設定データ管理

TOE のセキュリティ機能を動作させるために必要となる環境設定データを環境設定データに対する操作権限のある管理者が設定する。

A) 環境設定データの管理

環境設定データに対して権限を持つ管理者による環境設定データに対する操作の管理を実現する。

＜利用者権限データ＞

TOE はシステム管理者に、利用者権限（[会計担当]権限以外）の問い合わせ、削除 、設定を許可する。（FMT_MSA.1(1)）

TOE はシステム管理者、及び権限管理者に、利用者権限（[会計担当]権限）の問い合わせ、削除 、設定を許可する。（FMT_MSA.1(2)）

＜識別認証データ＞

識別認証データに関しては、以下の通りとする。

表　6.3.1（4）識別認証データに関する操作、役割の関係

TSF データ	操作	役割
利用者 ID（システム管理者以外）	問い合わせ、改変、削除、登録	システム管理者 アカウント管理者
パスワード（システム管理者以外）	登録	システム管理者 アカウント管理者
パスワード	改変	システム管理者 アカウント管理者 当該パスワードの所有者

TOE は、システム管理者、アカウント管理者に利用者 ID（システム管理者以外）の問い合わせ、改変、削除、登録を許可する。（FMT_MTD.1(1)）
TOE は、システム管理者、アカウント管理者にパスワード（システム管理者以外）の登録を許可する。（FMT_MTD.1(2)、FIA_SOS.1）
TOE は、システム管理者、またはアカウント管理者、または当該パスワードの所有者にパスワードの改変を許可する。（FMT_MTD.1(3) 、FIA_SOS.1）
＜パスワードポリシーデータ・アカウントポリシーデータ＞
TOE はシステム管理者にパスワード、アカウントポリシーの改変を許可する。（FMT_MTD.1(4)）
＜ログポリシーデータ＞
TOE はシステム管理者及びログ管理者にログポリシーの改変を許可する。（FMT_MTD.1(5)）
＜利用者アカウントロックデータ＞
TOE はシステム管理者及びアカウント管理者に利用者アカウントロックの改変を許可する。（FMT_MTD.1(6)）
TOE は、TOE の動作に影響する管理機能を特定し、役割を維持する。これにより、セキュリティ属性、TSF データの管理を行う。（FMT_SMF.1、FMT_SMR.1）

上記管理機能を満たし、この機能は TOE 識別認証時から終了時まで維持される。これに該当するセキュリティ機能要件は、FIA_SOS.1、FMT_MSA.1（1）、FMT_MSA.1（2）、FMT_MTD.1（1）、FMT_MTD.1（2）、FMT_MTD.1（3）、FMT_MTD.1(4)、FMT_MTD.1(5)、FMT_MTD.1(6)、FMT_SMR.1、FMT_SMF.1 である。

以上のことからこれらの要件の組み合わせにより、「O.環境設定データ管理」を実現するのに十分である。

6.3.2 依存性の検証

表 6.3.2依存性の検証

セキュリティ機能要件	Part2の依存性	本TOEにて満たすべき依存性
FAU_GEN.1	FPT_STM.1	*1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1、FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	なし	N/A
FIA_SOS.1	なし	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_UID.2	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1(1)	[FDP_ACC.1、または FDP_IFC.1]、FMT_SMR.1、FMT_SMF.1	FDP_ACC.1、FMT_SMR.1、FMT_SMF.1
FMT_MSA.1(2)	[FDP_ACC.1、または FDP_IFC.1]、FMT_SMR.1、FMT_SMF.1	FDP_ACC.1、FMT_SMR.1、FMT_SMF.1
FMT_MSA.1(3)	[FDP_ACC.1、または FDP_IFC.1]、FMT_SMR.1、FMT_SMF.1	FDP_ACC.1、FMT_SMR.1、FMT_SMF.1
FMT_MSA.3	FMT_MSA.1、FMT_SMR.1	FMT_MSA.1*2
FMT_MTD.1(1)	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_MTD.1(2)	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_MTD.1(3)	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_MTD.1(4)	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_MTD.1(5)	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_MTD.1(6)	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_SMF.1	なし	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2

表 6.3.2 により、セキュリティ機能要件は、後述する例外を除いて必要な依存関係をすべて満たしている。

例外については、依存関係を満たさなくても問題がない根拠を以下に示す。

*1　本 TOE では、製品内の時刻は、OE.OS タイムスタンプにより、TOE 外となる OS 機能を使用することから、依存関係は不要である。

*2　本 TOE では、セキュリティ属性に対して、FMT_MSA.3.2 が要求する処理を実現する必要がないことから、依存関係は不要である。

6.3.3 セキュリティ保証要件根拠

本 TOE の運用環境は、企業内 LAN を使用することが想定されているため、外部からの攻撃はないものと考える。

脅威エージェントは、TOE 一般利用者と非許可従業員であり、運用環境の対策により直接 OS や DBMS を使用して保護資産へのアクセスを行うことができず、TOE に対して低レベルの攻撃しか行わないことを想定する。つまり、想定される利用環境から低レベルの攻撃者を想定しており、EAL1 追加（追加する保証要件は、ASE_SPD.1、ASE_OBJ.2、ASE_REQ.2）を評価保証レベルとするのが妥当である。

また、これらのすべてのセキュリティ保証要件は依存性を満たしている。

7　TOE 要約仕様

7.1　TOE セキュリティ機能

TOE セキュリティ機能とセキュリティ機能要件（SFR）との対応関係について示す。ここで示されるとおり、本節で説明するセキュリティ機能は、すべての SFR を満たすものである。

7.1.1 利用者識別認証

TOE にアクセスする利用者を識別し、登録されている利用者本人であることを確認するための機能を提供する。以下では、識別認証機能について、SFR の実現方法という観点から説明する。

＜対応する SFR の実現方法＞

(1) FIA_AFL.1 認証失敗時の取り扱い

TOE は、利用者（システム管理者以外）が最後の認証成功後に一定回数以上認証に失敗した場合にロックアウトしその利用者 ID を無効化することが出来る。また、システム管理者もしくはアカウント管理者がロックアウトされた利用者の解除を実行するまでは、その利用者の識別認証試行を拒否することができる。

上記、機能の実装により FIA_AFL.1 を実現する。

(2) FIA_ATD.1 利用者属性定義

TOE は、利用者の識別認証時に、利用者のセキュリティ属性である利用者権限（[システム管理]権限・[利用者管理]権限・[ログ管理]権限・[権限管理]権限・[業務管理]権限・[会計担当]権限）と利用者 ID を結びつけ、TOE 利用中はその権限を維持する。

上記、機能の実装により FIA_ATD.1 を実現する。

(3) FIA_SOS.1 秘密の検証

TOE は、パスワードポリシーを設定することが出来、そのポリシーに則したパスワードしか設定することが出来ない。また、パスワードポリシーの設定はシステム管理者のみ運用管理ツールの[セキュリティ管理] - [セキュリティポリシー]で設定することが出来る。

品質尺度は、以下の値である。

- 最小パスワード長：0～14
- 文字種類：英大文字・英小文字・数字・記号から 3 種類含む必要がある／ない

パスワードポリシーは前提条件（A.パスワードの設定）により以下の値が設定される。

- 最小パスワード長：8 文字以上
- 文字種類：英大文字・英小文字・数字・記号から 3 種類含む
- パスワードの有効期限：30 日

上記制限はすべての利用者に適用され、システム管理者とアカウント管理者が運用管理ツールの[セキュリティ管理] - [利用者登録]でパスワードを登録、変更する際、ログイン画面から自身のパスワード変更をする際に、品質の尺度を満たした場合パスワードの操作（登録、変更）が許可される。
上記、機能の実装により FIA_SOS.1 を実現する。

(4) FIA_UID.2 アクション前の利用者識別、FIA_UAU.2 アクション前の利用者認証

TOE は TOE を利用する前に必ず利用者の識別認証を行う。利用者 ID が無効化されていないこと、利用者 ID の識別に成功し、パスワードの認証に成功して初めて TOE 上で操作が許される。
上記、機能の実装により FIA_UID.2、FIA_UAU.2 を実現する。

(5) FIA_UAU.7 保護された認証フィードバック

TOE は、利用者がパスワードを入力する際、入力された文字に対して盗みられることないようアスタリスクを表示する。
上記、機能の実装により FIA_UAU.7 を実現する。

(6) FIA_USB.1 利用者・サブジェクト結合

TOE は、識別認証された利用者が TOE を利用するために、利用者のセキュリティ属性である利用者権限、利用者 ID と許可された利用者プロセスの関連付けを行う。
上記、機能の実装により FIA_USB.1 を実現する。

(7) FMT_SMR.1 セキュリティの役割

パスワードの識別認証に成功すると、利用者 ID と権限が関連付けられる。利用者 ID に関連付けられる権限は以下の通りである。

- [システム管理]権限
- [利用者管理]権限
- [ログ管理]権限
- [権限管理]権限

・ [業務管理]権限
・ [会計担当]権限

上記の権限を利用者 ID と関連付け、維持する。
上記、機能の実装により FMT_SMR.1 を実現する。

7.1.2 監査証跡

監査証跡の機能は、TOE に対して行ったすべての処理をログという形で記録しておくことが出来る。記録したログの中から必要な情報を検索して確認することが出来るため、不正なアクセスがあった場合でも探し出すことが出来る。
また、ログを閲覧する権限はシステム管理者とログ管理者に限定されるので、不正に閲覧されることもなく、ログの内容は画面で確認するため不正に改ざんされることなく正確性を保つことが出来る。

＜対応する SFR の実現方法＞

(1) FAU_GEN.1 監査データ生成

TOE で操作された内容はログとして運用管理ツールの[ログ管理] - [ログビューア]で監査データを生成し、確認することができる。
生成されるログは、アクションログ・メニューログ・認証ログの 3 種類に分類される。また、[ログ管理] - [ログビューア]の検索機能を利用することによって必要なデータだけを絞り込みログの内容を確認することができる。
この SFR で求められている監査記録は、以下の通りである。

・ 監査機能の起動と終了
・ 監査記録の参照の成功と失敗
・ 仕訳伝票データの入力、修正、削除の成功と失敗
・ キャッシュ・フロー調整金額明細データの入力、修正、削除の成功と失敗
・ 期首残高データの入力の成功と失敗
・ 勘定科目マスタの登録、修正、削除の成功、失敗
・ パスワード認証の成功と失敗
・ 利用者 ID 識別の成功と失敗
・ システム管理者による[利用者管理]権限、[ログ管理]権限、[権限管理]権限、[業務管理]権限の削除、設定の成功と失敗
・ システム管理者または権限管理者による[会計担当]権限の削除、設定の成功と失敗
・ システム管理者または業務管理者による仕訳伝票データ更新ロックの実行の成功と失敗
・ システム管理者またはアカウント管理者による利用者 ID（システム管理者以

外）の改変、削除、登録の成功と失敗
- システム管理者またはアカウント管理者によるパスワード（システム管理者以外）の登録の成功と失敗
- システム管理者によるパスワードポリシーデータ（最小パスワード長、文字種類、パスワードの有効期限）、アカウントポリシーデータ（ログイン失敗時の累積回数、ロックアウト解除時間（0：解除しない））の改変の成功と失敗
- システム管理者によるログポリシーデータ（認証ログ、メニューログ、アクションログ）の改変の成功と失敗
- システム管理者またはアカウント管理者による利用者のアカウントロックデータの改変の成功と失敗

上記の操作に対して事象の日付・時刻（OS から取得したタイムスタンプ情報を使用する）、事象の種別、サブジェクト識別情報（利用者 ID）、事象の結果（成功または失敗）を記録する。
上記、機能の実装により FAU_GEN.1 を実現する。

(2) FAU_SAR.1 監査レビ ュー
TOE は取得したログをわかりやすい形式で出力し、ログに関する権限のあるシステム管理者とログ管理者のみが参照できる機能を提供する。システム管理者とログ管理者は運用管理ツールの[ログ管理] - [ログビューア]で事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）をキーワードとし、ログを確認することが出来る。
上記、機能の実装により FAU_SAR.1 を実現する。

(3) FAU_SAR.3 選択可能監査レビュー
TOE では、ログに関する権限のあるシステム管理者またはログ管理者がログの内容から日付、アカウント名、メニュー名またはアクション区分を指定して必要なログのみ選択して[ログ管理] - [ログビューア]の画面上で確認することが出来る。
上記、機能の実装により FAU_SAR.3 を実現する。

7.1.3 仕訳伝票データ更新ロック
仕訳伝票データ更新ロックの機能は、指定した期間に対してロックを実行することによって、その期間の財務諸表に関する金額データ（仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データ）を新規登録・修正・削除することを制限する。この機能は仕訳伝票データ更新ロックに権限のあるシステム管理者・業務管理者のみ問い合わせ・実行することが出来る。

＜対応する SFR の実現方法＞

(1) FDP_ACC.1 サブセットアクセス制御、 FDP_ACF.1 セキュリティ属性によるアクセス制御、FMT_MSA.3 静的属性初期化

TOE では業務締めや決算締めのタイミングで、勘定奉行 V ERP の[決算処理] - [締処理] - [締処理]で期間を指定して締処理を実行することが出来る。締処理を実行すると保護資産である仕訳伝票データの入力・修正・削除、キャッシュ・フロー調整金額明細データの入力・修正・削除、期首残高データの入力を制限することが出来る。仕訳伝票データ更新ロックデータは、仕訳伝票データ更新ロックが実行されていない属性とする。

「仕訳伝票データ更新ロックが実行されない場合」

以下のアクセスを許可する。

- システム管理者の仕訳伝票データの入力・修正・削除・参照
- システム管理者のキャッシュ・フロー調整金額明細データの入力・修正・削除・参照
- システム管理者の期首残高データの入力・参照
- 業務管理者の仕訳伝票データの入力・修正・削除・参照
- 業務管理者のキャッシュ・フロー調整金額明細データの入力・修正・削除・参照
- 業務管理者の期首残高データの入力・参照
- 一般利用者の仕訳伝票データの入力・修正・削除・参照
- 一般利用者のキャッシュ・フロー調整金額明細データの入力・修正・削除・参照
- 一般利用者の期首残高データの入力・参照

「仕訳伝票データ更新ロックが実行されている場合」

以下のアクセスを許可する。

- システム管理者の仕訳伝票データの参照
- システム管理者のキャッシュ・フロー調整金額明細データの参照
- システム管理者の期首残高データの参照
- 業務管理者の仕訳伝票データの参照
- 業務管理者のキャッシュ・フロー調整金額明細データの参照
- 業務管理者の期首残高データの参照
- 一般利用者の仕訳伝票データの参照
- 一般利用者のキャッシュ・フロー調整金額明細データの参照
- 一般利用者の期首残高データの参照

上記、機能の実装により FDP_ACC.1、FDP_ACF.1、FMT_MSA.3 を実現する。

(2) FMT_MSA.1（3）セキュリティ属性の管理、FMT_SMR.1 セキュリティの役割

TOE は、仕訳伝票データ・キャッシュ・フロー調整金額明細データ・期首残高データをロックする仕訳伝票データ更新ロックの問い合わせ・実行をシステム管理者と業務管理者に限定する。

上記、機能の実装により FMT_MSA.1（3）、FMT_SMR.1 を実現する。

7.1.4 環境設定データ管理

環境設定データの管理機能を権限のある管理者に限定する。

(1) FMT_MSA.1（1）、FMT_MSA.1 （2）セキュリティ属性の管理、FMT_SMR.1 セキュリティの役割

TOE は、環境設定データである利用者権限データに対する管理機能を持つ。具体的な操作は以下に示す。

表　7.1.4 セキュリティ属性の管理

セキュリティ属性	操作	役割
[利用者管理]権限 [ログ管理]権限 [権限管理]権限 [業務管理]権限	問い合わせ 削除 設定	システム管理者
[会計担当]権限	問い合わせ 削除 設定	システム管理者 権限管理者

運用管理ツールの画面より、利用者権限（[利用者管理]権限、[ログ管理]権限、[権限管理]権限、[業務管理]権限）の問い合わせ、削除、設定操作をシステム管理者ができる。（FMT_MSA.1（1））

運用管理ツールの画面より、利用者権限（[会計担当]権限）の問い合わせ、削除、設定操作をシステム管理者、及び権限管理者ができる。（FMT_MSA.1（2））

上記、機能の実装による FMT_MSA.1（1）、FMT_MSA.1 （2）、FMT_SMR.1 実現する。

(2) FMT_MTD.1（1）、FMT_MTD.1（2） 、FMT_MTD.1 （3） 、FMT_MTD.1（4）、FMT_MTD.1（5）、FMT_MTD.1（6）TSF データの管理、FMT_SMR.1 セキュリティの役割

TOE は、環境設定データである以下の表に示す TSF データに対する管理機能を持つ。具体的な操作は以下に示す。

表　7.1.4 TSF データの管理

TSF データ	操作	役割	インターフェース
利用者 ID（システム管理者以外）	問い合わせ、改変、削除、登録	システム管理者 アカウント管理者	利用者登録 （FMT_MTD.1（1））
パスワード（システム管理者以外）	登録	システム管理者 アカウント管理者	利用者登録 （FMT_MTD.1（2））
パスワード	改変	システム管理者 アカウント管理者 当該パスワードの所有者	利用者登録 パスワード変更 （FMT_MTD.1（3））
パスワードポリシーデータ アカウントポリシーデータ	改変	システム管理者	パスワードポリシー アカウントポリシー （FMT_MTD.1（4））
ログポリシーデータ	改変	システム管理者 ログ管理者	ログポリシー （FMT_MTD.1（5））
アカウントロックデータ	改変	システム管理者 アカウント管理者	利用者登録 （FMT_MTD.1（6））

上記、機能の実装による FMT_MTD.1（1）、FMT_MTD.1（2）、FMT_MTD.1（3）、FMT_MTD.1（4）、FMT_MTD.1（5）、FMT_MTD.1（6）、FMT_SMR.1 実現する。

(3) FMT_SMF.1 管理機能の特定

TOE は以下に示すセキュリティ管理機能を提供する。

- システム管理者、アカウント管理者による利用者 ID（システム管理者以外）の管理（問い合わせ、改変、削除、登録）機能
- システム管理者、アカウント管理者によるパスワード（システム管理者以外）

の管理（登録）機能

- システム管理者、アカウント管理者、当該パスワードの所有者によるパスワードの改変機能
- システム管理者によるパスワード、アカウントポリシーの改変機能
- システム管理者、ログ管理者によるログポリシーの改変機能
- システム管理者、アカウント管理者による利用者アカウントロックの改変機能
- システム管理者による利用者権限（[会計担当]権限以外）の管理（問い合わせ、削除、設定）機能
- システム管理者、権限管理者による利用者権限（[会計担当]権限）の管理（問い合わせ、削除、設定）機能
- システム管理者、業務管理者による仕訳伝票データ更新ロックの問い合わせ、実行機能

上記、機能の実装による FMT_SMF.1 実現する。

8　付録　用語の定義

8.1　用語

表 8.1　用語

用語	定義内容
システム管理者	TOE 全体の管理者。 アカウント管理者、ログ管理者、権限管理者、業務管理者の登録（権限の付与）を行う。 ※運用管理ツールのビルとインアカウントである SecAdmin と勘定奉行 V ERP のビルトインアカウントである AcAdmin、を指す。現 ST におけるシステム管理者。
[システム管理]権限	運用管理ツールと勘定奉行 V ERP に対するフルコントロール権限
アカウント管理者	[利用者管理]権限を有する管理者
[利用者管理]権限	利用者（アカウント）を登録・削除する権限
ログ管理者	[ログ管理]権限を有する管理者
[ログ管理]権限	ログポリシーの設定やログの参照を行う権限
権限管理者	[権限管理]権限を有する管理者
[権限管理]権限	登録済みの一般利用者にメニュー操作の操作権限の設定を行う権限。
業務管理者	[業務管理]権限を有する管理者
[業務管理]権限	勘定奉行 V ERP 上の業務に関するすべてのメニューを操作できる権限
一般利用者	[会計担当]権限を有する利用者。
[会計担当]権限	システム管理者または権限管理者により付与される権限。 以下のメニューを操作することができる。 ・勘定科目マスタの登録、修正、削除、参照 ・仕訳伝票データの入力、修正、削除、参照 ・キャッシュ・フロー調整金額明細データの入力、修正、削除、参照 ・期首残高データの入力、参照
当該パスワードの所有者	改変するパスワードの所有者（システム管理者、アカウント管理者、ログ管理者、権限管理者、業務管理者または一般利用者）
管理者	システム管理者、アカウント管理者、ログ管理者、権限管理者、業務管理者をあわせて管理者と称する。
非許可従業員	TOE にアカウントが登録されていない従業員
保護資産	会計データ、環境設定データ
会計データ	勘定科目マスタ、仕訳伝票データ、調整金額明細データ、期首残高データ
環境設定データ	TOE のセキュリティ機能を動作させるために必要となる識別認証データ、仕訳伝票データ更新ロックデータデータ、ログポリシーデータ、アカウントポリシーデータ、パスワードポリシーデータ、利用者アカウントロックデータ、利用者権限データ
勘定科目マスタ	勘定奉行 V ERP で複式簿記の仕訳や財務諸表などに用いる表示金額の名目を表す勘定科目として、どのような名目を定義するのかを集約したマスタデータ。一般利用者によって勘定奉行 V ERP で作成・修正・削除される。

用語	定義内容
仕訳伝票データ	企業において発生した会計に係る取引について、複式簿記における貸借の勘定科目に分類したデータのこと。一般利用者によって勘定奉行 Ｖ ERP で作成・修正・削除される。
キャッシュ･フロー調整金額明細データ	キャッシュ・フロー計算書を作成するためのデータ。
期首残高データ	各勘定科目の期首残高データ。
仕訳伝票データ更新ロック	勘定奉行 Ｖ ERP の締処理機能を利用することで、指定した期間に含まれる仕訳伝票データがロックされ、その期間に含まれる仕訳伝票の入力・修正・削除、調整金額の入力・修正・削除、期首残高の入力が制限される。この機能のことを仕訳伝票データ更新ロックと呼ぶ。
企業内 LAN	企業内に敷設されたローカルエリアネットワーク。企業外アブのネットワークとの間に通信パケットの流れを制御するルータ、ファイアウォール等を配備し、企業内サーバー等で保管・維持されるデータに対して所定の保護が行えるよう外部ネットワークと区別した管理が行われる。
財務会計パッケージソフトウェア	企業内の財務情報、会計データを管理するためのアプリケーション機能を提供する市販ソフトウェアの総称。
財務情報	財務報告書を作成するために整理された財務報告書の構成要素に係る情報であり、予算・実績管理や各種分析用の集計処理も含む。財務会計パッケージソフトウェアを使用して一般利用者により集計される。
財務報告書	企業が利害関係者に対して一定期間の経営成績や財務状態等を明らかにするために複式簿記に基づき作成される書類（決算書と呼ばれる）について、会社法により株式会社にその作成が義務付けられる計算書類（貸借対照表、損益計算書、株主資本等変動計算書、個別注記表等の財務諸表）を公告するために取りまとめた報告書類。財務会計パッケージソフトウェアを使用して一般利用者により作成される。
誤操作	利用者がオペレーションミスをして故意ではなく意図しない内容を登録してしまうこと。 例： ・仕訳伝票の金額を間違えて登録する。 ・正しい仕訳伝票を誤って修正してしまう。 ・勘定科目マスタを誤って登録する。

用語	定義内容
認証ログ	勘定奉行Ⅴ ERP または運用管理ツールへの認証ログ。つまり、ログイン画面でのログイン（認証）と製品終了時にログアウト情報、ログイン日時やログインしたコンピュータ名、アカウント名などの情報を確認することが出来る。
メニューログ	メニューを起動した際のログ。メニュー起動日時やメニュー名、メニュー終了日時などの情報を確認することが出来る。
アクションログ	各メニューの中での操作のログ。新規登録・修正・削除・実行・印刷などの情報を確認することが出来る。
アクション区分	各メニューでの以下のアクションを指す。 新規・修正・削除・登録・実行・印刷・プレビュー・転送・受入
承認	会計業務のワークフローにおける「承認」を意味しており、TOE の機能ではありません。一般利用者が会計データを入力などする際には事前に業務管理者の会計業務上の「承認」をもらいます。

8.2 略語

表 8.2 略語

略語	正式名称
CC	Common Criteria
PP	Protection Profile
EAL	Evaluation assurance level
ID	identification data
IT	information technology
LAN	local area network
OS	operating system
PC	personal computer
SFP	security function policy
ST	security target
TOE	target of evaluation
TSF	TOE security functionality