認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成20年7月28日** (IT**認証**8228)
認証番号	C0211
認証申請者	**株式会社オービックビジネスコンサルタント**
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**	1.05
PP**適合**	**なし**
適合する保証パッケージ	EAL1**及び追加の保証コンポーネント**ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
開発者	**株式会社オービックビジネスコンサルタント**
評価機関の名称	**みずほ情報総研株式会社 情報セキュリティ評価室**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成21年3月26日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版 (翻訳第2.0版)

評価結果：合格

「勘定奉行V ERP Standard Edition、運用管理ツール」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約 1
1.1 はじめに 1
1.1.1 評価保証レベル 1
1.1.2 PP適合 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 2
1.2.3 TOE範囲とセキュリティ機能 2
1.3 評価の実施 5
1.4 評価の認証 6
2 TOE概要 7
2.1 セキュリティ課題と前提 7
2.1.1 脅威 7
2.1.2 組織のセキュリティ方針 8
2.1.3 操作環境の前提条件 8
2.1.4 製品添付ドキュメント 10
2.1.5 構成条件 10
2.2 セキュリティ対策 11
3 評価機関による評価実施及び結果 15
3.1 評価方法 15
3.2 評価実施概要 15
3.3 製品テスト 15
3.3.1 開発者テスト 15
3.3.2 評価者独立テスト 15
3.3.3 評価者侵入テスト 18
3.4 評価結果 19
3.4.1 評価結果 19
3.4.2 評価者コメント/勧告 19
4 認証実施 20
5 結論 21
5.1 認証結果 21
5.2 注意事項 21
6 用語 22
7 参照 24

1 全体要約

1.1 はじめに

この認証報告書は、「勘定奉行V ERP Standard Edition、運用管理ツール」（以下「本TOE」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である株式会社オービックビジネスコンサルタントに報告するとともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、市販される本TOEを購入する一般消費者を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL1追加である。
追加の保証コンポーネントはASE_OBJ.2、ASE_REQ.2、ASE_SPD.1である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称： 勘定奉行V ERP Standard Edition
バージョン： Ver1.05
開発者： 株式会社オービックビジネスコンサルタント

1.2.2 製品概要

本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、その運用管理を行うソフトウェアである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。

勘定奉行V ERP Standard Editionでは、仕訳処理、各種帳票、財務報告書の作成等の基本機能、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をする仕訳伝票データ更新ロック機能、及び利用者の権限に従った会計データの操作の制御を行う会計データアクセス制御機能を提供する。

また、運用管理ツールでは、セキュリティ機能の動作に関わる設定を行う機能、利用者の管理を行う利用者管理機能、及び勘定奉行V ERP Standard Editionと運用管理ツールで操作された内容をログとして記録するログ管理機能を提供する。

1.2.3 TOE範囲とセキュリティ機能

1) TOEに関係する役割

① 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できる。

② システム管理者

TOE全体の管理を行う。勘定奉行V ERP Standard Editionと運用管理ツールに対するフルコントロール権限を有している。

③ アカウント管理者

利用者(アカウント)を登録・削除する権限を有している。

④ ログ管理者

取得するログの種類の設定やログの参照を行う権限を有している。

⑤ 権限管理者

登録済みの一般利用者に勘定奉行V ERP Standard Edition上での操作権限の設定を行う権限を有している。

⑥ 業務管理者

会計業務の管理を行う。勘定奉行V ERP Standard Edition上でのすべての操作権限を有している。

⑦ 一般利用者

勘定奉行V ERP Standard Editionにおいて、以下の操作をする権限を有している。

・ 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

⑧ 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

2) TOEの範囲と利用方法
TOEの利用環境を図1-1に示す。

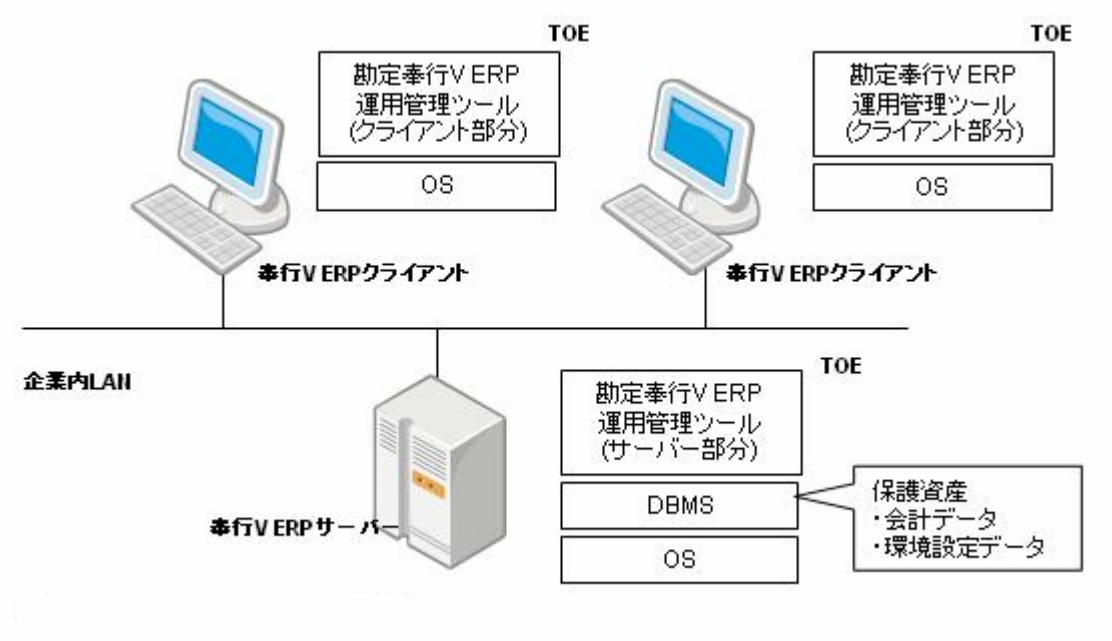

図1-1　TOEの利用環境

TOEは、奉行V ERPサーバーにインストールされる勘定奉行V ERP Standard Editionと運用管理ツールのサーバープログラム、及び奉行V ERPクライアントにインストールされる勘定奉行V ERP Standard Editionと運用管理ツールクライアントプログラムである。
奉行V ERPサーバー、及び奉行V ERPクライアントは企業内LANに接続した状態で利用を想定しており、スタンドアロンでの利用は評価の対象外である。
また、保護資産は企業内LANに接続する奉行V ERPサーバーに保存される。

TOEの利用方法は以下のとおりである。

① システム管理者は、TOE（奉行V ERPクライアント）を操作して識別と認証を行う(システム管理者は、本TOEにおけるビルトインアカウントである)。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・業務管理者のアカウント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）を操作して識別と認証

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、参照することができる。不適切な操作や誤った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）を操作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できる。

④ 権限管理者は、TOE（奉行V ERPクライアント）を操作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）のアカウント管理者によりアカウントを作成された一般利用者に対して権限を与えることができる。

⑤ 業務管理者は、TOE（奉行V ERPクライアント）を操作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）のうち運用管理ツールを除く勘定奉行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等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できる。

⑥ 一般利用者は、TOE（奉行V ERPクライアント）を操作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、権限管理者の設定した権限に従い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できる。

⑦ 奉行V ERPサーバーはインストール以外で操作することはない。

3) TOEのセキュリティ機能

TOEが搭載するセキュリティ機能は以下のとおりである。

① 利用者識別認証機能

本TOEのすべての利用者に対する識別と認証を行う機能。本機能によって許可されていない利用者によるなりすましを防ぐことができる。

② 監査証跡機能

本TOEでの操作のログを作成し、許可されていない利用者によるなりすましや、承認されていないデータの修正等の一般利用者による不正操作や誤操作を検出することができる。また、システム管理者、及びログ管理者のみに対してログの参照を提供する。

③ 仕訳伝票データ更新ロック機能

システム管理者、及び業務管理者が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、伝票日付がその期間に含まれる場合金額データをロックする機能。本機能によって一般利用者による指定された期間内の伝票日付を持つ仕訳伝票データ、キャッシュ・フロー調整金額明細データ、期首残高データの不正操作、または誤操作を防ぐことができる。

④ 会計データアクセス制御機能

環境設定データの設定内容に応じて、許可された役割を持った利用者のみが会計データを操作できるように制御する機能。本機能によって、許可されていない利用者による会計データの不正操作を防ぐことができる。

⑤ 環境設定データ管理機能

環境設定データに対する管理を適切な管理者に制限する機能。本機能によってTOEを利用する利用者の設定(利用者アカウントの設定や権限の付与等)、ログの取得規則、及び会計データや環境設定データ自身を保護するために会計データと環境設定データへのアクセス制御の規則を設定することができる。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「株式会社オービックビジネスコンサルタント 勘定奉行V ERP Standard Edition・運用管理ツール Ver.1.05 セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「勘定奉行V ERP、運用管理ツール 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成21年3月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	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 ・ 確定後の勘定科目マスタの不正な修正、削除 ・ 確定後の仕訳伝票データの不正な修正、削除 ・ 確定後のキャッシュ・フロー調整金額明細データの修正、削除 ・ 確定後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

2.1.2 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表2-2に示す。

表2-2 組織のセキュリティ方針

識別子	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。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-3に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表2-3 TOE使用の前提条件

識別子	前提条件
A.システム・ネットワーク環境	勘定奉行V ERP、及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等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できるキャビネット等に保管し業務管理者以外アクセスできないようにする。

	・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できるキャビネット等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とお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)、及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とお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とお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等)までログをと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。 ※この前提は1.2.3小節のTOEに関する役割に示された一般利用者に対する権限のみを与えることを意味する。
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行わない。 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しなければならない。 ログ管理者は、定期的にログを確認し、不正な痕跡、及び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。

(注)パスワードポリシー、アカウントポリシー、ログポリシーとは本TOEによって提供される機能であり、パスワードポリシーは最小パスワード長、文字種類、パスワードの有効期限を、アカウントポリシーはログイン失敗時の累積回数、ロックアウト解除時間を、ログポリシーは記録するログの種類を設定するものである。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

- 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

2.1.5 構成条件

本TOEは、奉行V ERPサーバー上、及び奉行V ERPクライアント上で稼動するソフトウェアである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

奉行V ERPサーバー、奉行V ERPクライアントのハードウェア構成を表2-4に示す。また、TOE以外のソフトウェア構成を表2-5に示す。

表2-4　TOE以外のハードウェア構成

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2-5　TOE以外のソフトウェア構成

ソフトウェアの要素	製品名称
奉行 V ERP サーバー	・ Windows Server 2003 Standard Edition Service Pack2 ・ SQL Server 2005 Standard Edition ・ .NET Framework 2.0 ・ Internet Explorer 6.0 Service Pack 2
奉行 V ERP クライアント	・ Windows Vista Business ・ .NET Framework 2.0 ・ Internet Explorer 7.0

2.2　セキュリティ対策

TOEは、2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たすために以下のセキュリティ機能を具備する。

(1) 「T.非許可従業員による不正使用」に対抗するためのセキュリティ機能

本脅威は、許可されてい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する可能性を想定している。

本TOEでは、以下の機能を保持することによって、本脅威に対抗している。

・本TOEは、TOEのセキュリティ機能の動作に関わる環境設定データを管理する機能(以上、「環境設定データ管理機能」)を保持する。この機能で本TOEの利用を許可する利用者のアカウントの登録や会計データを作成することができる権限の付与等のアカウントの管理、及び取得するログの種類の設

定を行う。以下に示す利用者識別認証機能、会計データアクセス制御機能、及び監査証跡機能と合わせて許可されていない利用者が本TOEにログインすること、及び会計データが不正に作成されることを防いでいる。

・本TOEは、本TOEを利用する際に利用者を識別認証する機能(以上、「利用者識別認証機能」)を保持する。この機能で、許可されていない利用者(環境設定データ管理機能でアカウントが登録されていない利用者)が不正に本TOEにログインすることを防いでいる。

・本TOEは、環境設定データの設定内容に応じて、会計データへのアクセスを制御する機能(以上、「会計データアクセス制御機能」)を保持する。この機能で、会計データを作成することができる利用者を制限することによって、不正に会計データが作成されることを防いでいる。

・本TOEは、環境設定データの設定内容に応じて、本TOEを操作した内容をログとして記録し、参照する機能(以上、「監査証跡機能」)を保持する。この機能で、本TOEに対する不正なログインの試みをログとして記録することができるため、ログ管理者が不正な試みを確認し、注意喚起による牽制を行うことで、許可されていない利用者が不正に本TOEにログインすることを防いでいる。

(2) 「T.一般利用者による不正操作または誤操作」に対抗するためのセキュリティ機能

本脅威は、一般利用者がTOEを使用して会計データに対して不正操作や誤操作をすることにより、財務報告書の金額や勘定科目の正確性が損なわれる可能性を想定している。

・本TOEは、環境設定データ管理機能を保持する。この機能で会計データや環境設定データ自身を操作することができる権限の付与等のアカウントの管理、及び取得するログの種類の設定を行う。以下に示す利用者識別認証機能、仕訳伝票データ更新ロック機能、会計データアクセス制御機能、及び監査証跡機能と合わせて会計データに対する不正操作や誤操作を防いでいる。

・本TOEは、利用者識別認証機能を保持する。この機能で環境設定データ管理機能により設定された利用者の役割を識別認証した利用者に対応付ける。このことによって、会計データのロック、及び会計データの操作、ログの参照を付与された役割に従って実施する。以下に示す仕訳伝票データ更新ロック機能、会計データアクセス制御機能、及び監査証跡機能と合わせて会計データに対する不正操作や誤操作を防いでいる。

・本TOEは、業務管理者が指定した期間内の伝票日付を持つ会計データ(勘定

科目マスタを除く)をロックする機能(以上、「仕訳伝票データ更新ロック機能」)を保持する。以下に示す会計データアクセス制御機能と合わせて、指定した期間内の伝票日付を持つ会計データ(勘定科目マスタを除く)に対する不正操作や誤操作を防いでいる。

・本TOEは、会計データアクセス制御機能を保持する。この機能で、仕訳伝票データ更新ロック機能によりロックされた会計データ(勘定科目マスタを除く)に対して参照以外の操作を禁止することによって、会計データ(勘定科目マスタを除く)に対する不正操作や誤操作を防いでいる。

・本TOEは、監査証跡機能を保持する。この機能で、会計データに対する操作をログとして記録することができるため、不正操作や誤操作が起こってしまったとしても、ログ管理者が不正操作を確認して注意喚起による牽制を行う、または誤った操作を確認して一般利用者に修正指示を行うことで、会計データに対する不正操作や誤操作を防いでいる。

※仕訳伝票データ更新ロックの対象として勘定科目マスタは対象外であるため、勘定科目マスタについてはTOEのセキュリティ機能では十分に脅威に対抗していない。勘定科目マスタに対する不正操作や誤操作への対策としては、会計データを操作した際にプルーフリストが出力されるので、出力されたプルーフリストと前回会計データを操作した際に出力されたプルーフリストの差分を業務管理者が比較することによって、勘定科目マスタに対して不正操作が行われていないかを確認し、注意喚起による牽制を行う。よって、勘定科目マスタについては、脅威に十分に対抗するためにTOEのセキュリティ機能ではなくTOEの運用によって対抗する。

※一般利用者による誤操作への対策として、上記に示した監査証跡機能では会計データの誤操作を検知できない場合が考えられる。会計データの誤操作への対策としては、会計データを操作した際に出力されるプルーフリストと、前回会計データを操作した際に出力されたプルーフリストの差分を業務管理者が比較して会計データの操作内容を確認し、誤操作が行われていないかを確認し、一般利用者に修正指示を行う。よって、会計データの誤操作については、監査証跡機能だけではなく、TOEの運用と合わせて対抗する。

(3) 「P.内部統制の構築・整備」を満たすためのセキュリティ機能

本組織のセキュリティ方針は、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(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・一般利用者に役割を分類)する方針である。

・本TOEは、環境設定データ管理機能を保持する。この機能で、本TOEを利用する役割をシステム管理者・アカウント管理者・ログ管理者・権限管理者・業務管理者・一般利用者に分類することができる。よって、本機能は本組織のセキュリティ対策を満たすことにつながる。

・本TOEは、監査証跡機能を保持する。この機能で、各利用者にどの役割を付与したかについてのログが記録されるため、利用者毎に付与されている役割を管理することができる。よって、本機能は本組織のセキュリティ方針を満たすことにつながる。

3 評価機関による評価実施及び結果

3.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年7月に始まり、平成21年3月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年10月、平成20年11月、及び平成21年3月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、必要と判断された評価者テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

本評価において、開発者テストは保証要件には含まれない。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成を図3-1に示す。評価者テストは本STにおいて

識別されているTOE構成と同一のTOEテスト環境で実施されている。

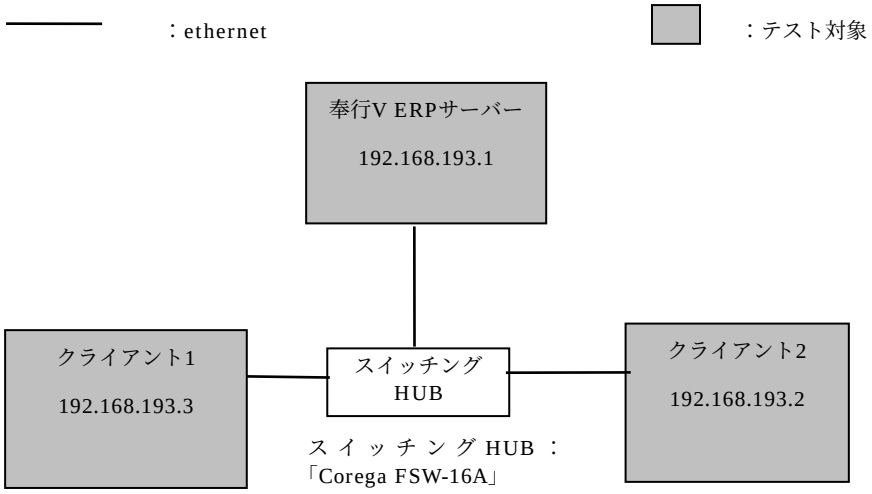

図3-1　評価者独立テストの構成図

図3-1において、使用している機器の構成を表3-1に示す。

表3-1 テスト環境の機器構成

端末・装置名	製品	
	種別	名称
奉行V ERPサーバー	ハード	DELL PowerEdge 1750
	プロセッサ/ メモリ/HDD	Intel Xeon 2.8GHz /2GB/68GB
	OS	Windows Server 2003 Standard Edition Service Pack 2
	DBMS	SQL Server 2005 Standard Edition
	Web ブラウザ	Internet Explorer 6.0 Service Pack 2
	アプリケーション実行環境	.NetFramework 2.0
	アプリケーションソフトウェア	勘定奉行 V ERP Standard Edition V1.05（サーバープログラム） 運用管理ツール　V1.05（サーバープログラム） 上記は、TOE の構成要素である。
クライアント1 (奉行V ERPクライアント)	ハード	DELL OPTIPLEX 745
	プロセッサ/ メモリ/HDD	Intel Core 2 2.40Ghz /2GB/150GB
	OS	Windows Vista Business
	Web ブラウザ	Internet Explorer 7.0
	アプリケーション	.NetFramework 2.0

端末・装置名	製品	
	種別	名称
	実行環境	
	アプリケーション ソフトウェア	勘定奉行 V ERP Standard Edition V1.05（クライアント部分） 運用管理ツール　V1.05（クライアント部分） 上記は、TOE の構成要素である。
クライアント2 (奉行V ERPクライアント)	ハード	HP dx7300
	プロセッサ/ メモリ/HDD	Intel Core 2 1.86Ghz /2GB/150GB
	OS	Windows Vista Business
	Web ブラウザ	Internet Explorer 7.0
	アプリケーション 実行環境	.NetFramework 2.0
	アプリケーション ソフトウェア	勘定奉行 V ERP Standard Edition V1.05（クライアント部分） 運用管理ツール　V1.05（クライアント部分） 上記は、TOE の構成要素である。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、すべてのTSFIに対するブラックボックステストを考案した。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

① 本評価では機能仕様書レベルの情報のみが利用可能であるため、すべてのTSFIにおいて、ブラックボックステストを実施した。

② 実施した独立テストの概要を以下に示す。

- 利用者の識別認証に関するふるまいを確認する。
- 権限に応じた仕訳伝票データ更新ロック、会計データ、及び環境設定データの操作に関するふるまいを確認する。
- 仕訳伝票データ更新ロックの状況に応じた会計データの操作に関するふるまいを確認する。
- 会計データ、環境設定データの操作に関するログが取得されていることを確認する。
- ログの参照に関するふるまいを確認する。

③　特にテストツールは使用されていない。

c.　結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

3.3.3　評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1)　評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a.　懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

①　仕訳伝票データ更新ロックに関連する会計データに対する同時アクセスにより会計データの正確性が損なわれてしまう可能性がある。

②　SQLインジェクションによりTOEが予期しない動作をしてしまう可能性がある。

③　セキュリティ機能がバイパスされることにより権限外の操作を実行されてしまう可能性がある。

④　ネットワークケーブルの遮断/再接続によりTOEが予期しない動作をしてしまう可能性がある。

⑤　奉行V ERPサーバーのポートへの直接攻撃によりTOEが予期しない動作をしてしまう可能性がある。

b.　実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。なお、侵入テストを実施したテスト環境は3.3.2小節に示す評価者独立テスト環境と同じ構成である。

脆弱性①：クライアント1、及びクライアント2を使用して、会計データの操作中に当該会計データに対して仕訳伝票データ更新ロックが操作できないことを確認する。また、会計データに対して仕訳伝票データ更新ロックの操作中に当該会計データを操作できないことを確認する。

脆弱性②：クライアント2を使用して、TOEへのログイン画面にてSQL文

を入力し、SQLインジェクションが成功しないことを確認する。

脆弱性③：クライアント2を使用して、クライアント2上に保存されているTOEの実行ファイル(*.exe)を直接実行し、セキュリティ機能がバイパスできないことを確認する。

脆弱性④：TOEへログイン中にクライアント1に接続されているネットワークケーブルを切断し、再接続した際に認証された状態が維持されていないことを確認する。

脆弱性⑤：クライアント2と奉行V ERPサーバー間に流れるパケットを分析し、奉行V ERPサーバーのポートへの攻撃が成立させることができないことを確認する。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

4 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本ST及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL1及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1に対する保証要件を満たすものと判断する。

5.2 注意事項

- 本TOEでは、TOEの不正使用、不正操作のみを脅威の対象としており、TOEを介さないHDDやDBMSへの直接攻撃、HDDの持ち出しによる脅威は想定していない。
- 本TOEでは、キーロガーによるパスワード入手等クライアントへの攻撃は、TOE固有の問題ではなく、ウイルス対策ソフトの導入等ネットワークを使用する環境で一般に行われる対策で対応すべきものであると判断し、TOEの保証外としている。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation(セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義を以下に示す。

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・印刷等の情報を確認することができる。
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、期首残高データの総称。
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であり、以下のデータを指す。 ・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
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等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。
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ー、ファイアウォール等を設備し、企業内のサーバー等で保管・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。
期首残高データ	各勘定科目の期首残高データ。
キャッシュ・フロー調整金額明	キャッシュ・フロー計算書を作成するためのデータ。

細データ	
誤操作	一般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： ・仕訳伝票データの金額を間違えて登録する。 ・正しい仕訳伝票データ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。
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わる情報であり、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(賃借対照表、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)を広告するために取りまとめた報告書類。
仕訳伝票データ	企業において発生した会計に係わる取引について、複式簿記における賃借の勘定科目に分類したデータ。
仕訳伝票データ更新ロック	勘定奉行V ERP Standard Edition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。
認証ログ	勘定奉行V ERP Standard Edition、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、アカウント名等の情報を確認することができる。
プルーフリスト	会計データに対してどのようなデータを入力したかを、一覧表として作成したもの。記録と共に、照合チェックや重複データ、紛失データの発見、修復等に使用される。
保護資産	会計データ、及び環境設定データ
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、メニュー終了日時等の情報を確認することができる。

7 参照

[1] 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　2009年3月16日　株式会社オービックビジネスコンサルタント

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001　(平成19年3月翻訳第1.2版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002　(平成20年3月翻訳第2.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003　(平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] 勘定奉行V ERP Standard Edition、運用管理ツール 評価報告書 第2版 平成21年3月18日 みずほ情報総研株式会社 情報セキュリティ評価室