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19年2月28日** (IT**認証**7137)
認証番号	C0154
認証申請者	**株式会社 インテリジェント ウェイブ**
TOE**の名称**	CWAT3i
TOE**のバージョン**	Ver3.1b_CC
PP**適合**	**なし**
適合する保証パッケージ	EAL2
開発者	**株式会社 インテリジェント ウェイブ**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

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20年4月25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 Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「CWAT3i Ver3.1b_CC」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 はじめに

この認証報告書は、「CWAT3i Ver3.1b_CC」（以下「本TOE」という。）について 株式会社電子商取引安全技術研究所　評価センター（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 インテリジェント ウェイブに報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応する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、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　CWAT3i
バージョン：　Ver3.1b_CC
開発者：　株式会社 インテリジェント ウェイブ

1.2.2 製品概要

CWAT3iは、コンピュータ利用サイトにおいて、ネットワークに接続されるPC端末の端末操作、及びネットワークアクセス操作を監視し、操作に対する監査ログを生成する。さらに、サイトごとに設定したポリシーへの違反操作を検知すると、警告ログを発生させ、その警告ログを集中管理しモニタリングするための機能を提供する。

また、TOEは設定された適切なポリシー情報の配信機能を強化すること、発生した警告ログの送信機能を強化することを実現するため、以下のセキュリティ機能を提供する。

・管理者登録機能
・識別認証機能
・OPDC端末ログオン可能ユーザ識別機能
・アクセス制御機能
・ポリシー配信強化機能
・警告ログ送信強化機能
・セキュリティ管理機能
・監査機能

1.2.3 TOEの範囲と動作概要

(1) TOE動作環境

図1-1にTOEを利用したシステム構成の例を示す。

TOEはファイアウォールの適切な設定によりインターネットなどの外部ネットワークからの攻撃に晒されることのないイントラネットで運用される。このイントラネットは、ネットワーク、サーバ及び端末からなるネットワークコンピューティング環境を導入し、業務システム等を運用していることを想定する。また、この運用環境はネットワークセグメントにより分割された複数のサイト（もしくは単一サイト）、及び各サイトを統括するセグメントエリアにより構成され、サーバ類は物理的に保護されたエリアに設置される。

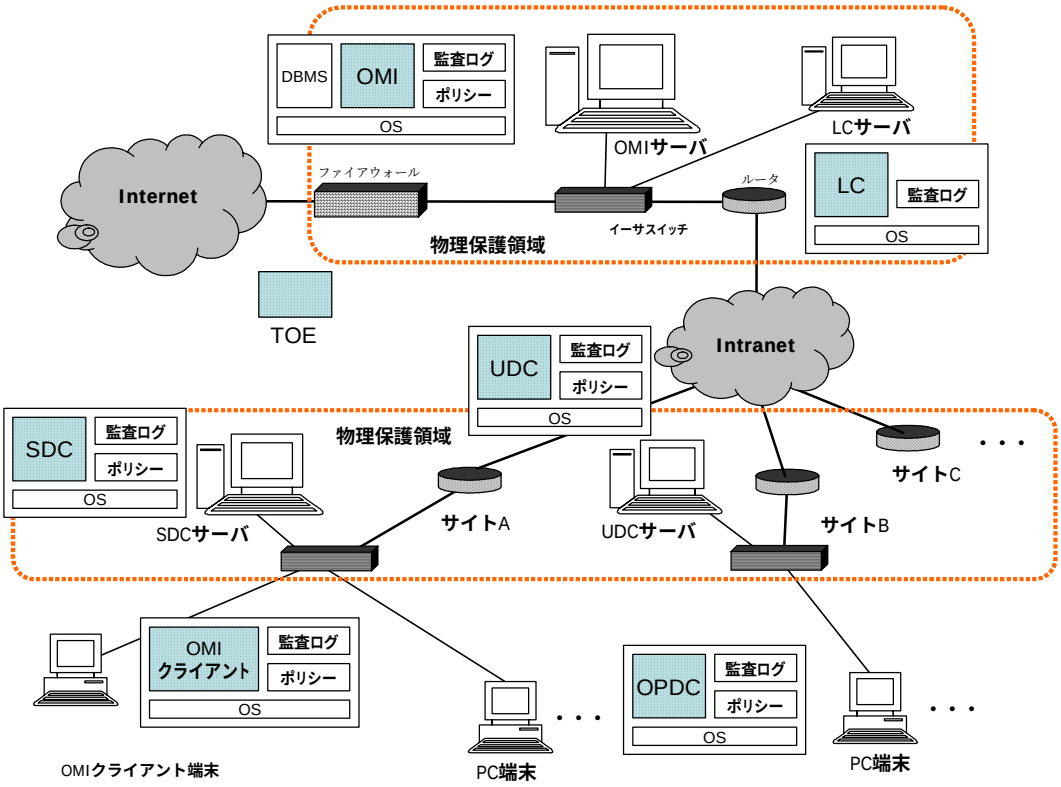


図1-1　TOEシステム構成例

以下に、システムを構成する各要素について説明する。

【OMIサーバ】
OMI（オーガナイゼーション モニタ インターナショナル）が動作するサーバマシンであり、設定された各種ポリシーの管理、各ノードへの配信、及び各ノードから通知される警告情報の集中監視等を行う機能を提供する。設定したポリシーや収集した警告情報は、DBMSにて管理し、OMIはこのDBMSで管理するDBへのアクセス手段を提供する。OMIサーバは不正な物理的アクセスから保護されたエリア（物理保護領域）に設置される。物理保護領域に入ることができるTOEの関係者はシステム管理者、CWAT管理者、サイト管理者のみである。

【LCサーバ】
LC（ログ コレクタ）が動作するサーバマシンであり、SDC、UDC及びOPDCで生成された監査ログを自動収集し閲覧・出力するための機能を提供する。LCサーバもOMIサーバと同様に物理保護領域に設置される。

【SDCサーバ】
SDC（セグメント ディフェンス コントローラ）が動作するサーバマシンであり、ポリシーに基づき、サイトのネットワークアクセス操作を監視する機能を提供する。SDCサーバは必要に応じてサイトごとに導入され、不正な物理的アクセスから保護されたエリア（物理保護領域）に設置される。

【UDCサーバ】
UDC（アンノウンターミナル ディフェンス コントローラ）が動作するサーバマシンであり、ポリシーに基づき、サイトの不正に接続された端末と、その動作を検知する機能を提供する。UDCサーバは必要に応じてサイトごとに導入され、不正な物理的アクセスから保護されたエリア（物理保護領域）に設置される。

【OMIクライアント端末】
OMIクライアントが動作する端末であり、OMIが提供する機能の一部（ポリシー設定機能、その他各種設定機能等）をOMIサーバ外から利用できる機能を提供する。OMIクライアント端末は物理保護領域の外に設置されるが、運用によりシステム管理者、CWAT管理者、及びサイト管理者のみが使用可能となるように管理される。

【PC端末】
一般利用者が使用する端末であり、OPDC（オペレーション ディフェンス コントローラ）が動作する端末である。PC端末上での操作の監視、ポリシー違反の

検出がOPDCにより実施される。

(2) TOEの範囲

図1-1に示すとおり、TOEは各サーバマシン、PC端末に搭載されるソフトウェア製品全体であり、下記のコンポーネントにより構成される。

・OMI（オーガナイゼーション モニタ インターナショナル）
・LC（ログ コレクタ）
・SDC（セグメント ディフェンス コントローラ）
・UDC（アンノウンターミナル ディフェンス コントローラ）
・OMIクライアント
・OPDC（オペレーション ディフェンス コントローラ）

(3) TOEの関係者

TOEでは、以下の関係者及び役割（TOEのセキュリティ機能に関連するものを抜粋）を想定する。以降、システム管理者、CWAT管理者、及びサイト管理者を総称して管理者とする。

1．システム管理者
・運用環境のネットワーク管理
・TOEのインストール、設定、及びシステム管理
・OM認証アカウント、サイト管理認証アカウントの登録、更新、削除
2．CWAT管理者
・サイト管理者の登録、更新、削除
・サイト情報の登録、更新、削除
3．サイト管理者
・監視サイトのセキュリティポリシー設定
4．端末利用者
・TOEにより操作が監視される端末の一般利用者

1.2.4 TOEの機能

本TOEは以下に示す機能を提供する。

(1) 統合監視コンソール機能
(2) 端末不正操作検出機能
(3) ネットワークアクセス監視機能
(4) 不正接続端末監視機能
(5) 監査ログ収集機能
(6) セキュリティ機能

今回のセキュリティ評価は「(6) セキュリティ機能」に対し実施された。以下では各機能の概要について説明する。

(1) 統合監視コンソール機能

OMI、及びOMIクライアントにより提供され、下記に示す各種設定、情報監視に関する機能により構成される。

・サイト、ノード、ユーザ登録機能
・ポリシー設定機能（設定されるポリシーは下記の通り）
  - ユーザログオンポリシー
  - 端末使用ポリシー
  - 未登録・盗難端末ポリシー
  - ネットワークポリシー
  - 外部接続機器ポリシー
  - ユーザオペレーションポリシー
  - メッセンジャーポリシー
・警告情報、ユーザ、端末の集中監視機能
・監査情報、警告情報の閲覧機能
・警告情報への対処機能
・警告情報の出力機能

(2) 端末不正操作検出機能

端末における不正操作を検出するための機能であり、OPDCにより提供される。本機能は設定されたポリシーに従い、端末における下記操作（主なもののみ提示）を実行する。

・端末の電源ON/OFF、ログオン/オフ状況の監視、自動遮断
・外部接続バス、MO、CD等への書き出し、プリンタ印刷、アプリケーション起動、ファイル操作の監視、自動遮断
・登録されたモバイル機器を持ち出した場合に、持ち出し中のモバイル機器に対する操作を監視し、再接続時に不正操作を報告
・ノードごと、ユーザごとの不正挙動、不審操作（特異挙動）の監視
・操作ログ自動取得、保存
・アラート状態のスクリーンショットの取得

(3) ネットワークアクセス監視機能

設定されたポリシーに従い、サイトのネットワークアクセスを監視するための機能であり、SDCにより提供される。本機能は下記に示す監視機能により構成される。

・ネットワークパケット情報の監視・防御機能

・ネットワークログ（ネットワークパケット情報）自動取得・保存機能

(4) 不正接続端末監視機能

設定されたポリシーに従い、サイトのネットワークに不正に接続された端末とその動作を検知する、またはネットワークへの接続を拒否する機能であり、SDC及びUDCにより提供される。

(5) 監査ログ収集機能

SDC、UDC、OPDCで生成された監査ログを自動収集し閲覧・CSV出力するための機能でLCにより提供される。また下記機能より構成される。

・監査ログ自動収集機能
・監査ログ閲覧・CSV出力機能

(6) セキュリティ機能

本TOEは下記セキュリティ機能を提供する。

a.管理者登録機能

管理者が管理者共通アカウント（OM認証アカウント）及び、CWAT管理者用アカウント（サイト管理認証アカウント）の登録、削除等を行うための管理機能。

b.識別認証機能

CWAT管理者、及びサイト管理者が使用する機能を利用可能とする前に、それぞれの管理者であることを識別、認証する機能。この識別認証機能は、両管理者の共通機能へのログオン時に使用されるOM認証、それぞれの管理者の識別認証を行うサイトログオン認証、及びサイト管理認証により構成される。

c.アクセス制御機能

各種統計情報へのアクセス、及びポリシー等に対する各種操作をその権限を有する管理者に制限する機能。

d.OPDC端末ログオン可能ユーザ識別機能

OPDC端末にログオン可能ユーザが設定されている場合、端末にログオンしようとする利用者がログオン可能ユーザであることを識別する機能。

e.ポリシー配信強化機能

設定されたポリシー情報をサイト内の各ノードに配信する際に発生し得る、ネットワーク障害による未配信のリスクを軽減させるための機能。

f.警告ログ送信強化機能

SDC、UDC、OPDCで発生した警告ログをOMIに送信する際に発生し得る、ネットワーク障害による未配信のリスク軽減、またネットワーク非接続状態の

端末において発生した警告ログを再接続時にOMIに送信するための機能。

g.セキュリティ管理機能
識別認証機能による識別認証の手順を経た後に、TOEの運用に必要となる、管理者向け各種管理機能を提供する。

h.監査機能
識別認証、及び管理画面へのアクセスに関わる監査記録を生成する機能。

尚、上記セキュリティ機能については、「1.5.4 セキュリティ機能」において詳細に説明する。

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「CWAT3i（Ver3.1b_CC）セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]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・製造・出荷環境がCCパート3（[7][10][13]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、「CWAT3i (Ver3.1b_CC)評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

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20年4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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL2適合である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、高度な専門知識を持たず、攻撃用の特別なツールを利用することも無い低レベルの攻撃者に対抗することが意図されているため、SOF-基本で十分である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

(1) 管理者登録機能

システム管理者が、OMIサーバ、OMIクライアント端末上で登録コマンド（cwlogon_write.exe）を実行することにより、下記アカウントを登録する機能。登録するアカウントの種別はコマンドの引数により区別する。

・OM認証アカウント登録機能

OM認証アカウントは、IDとパスワードが記入された設定ファイルを引数に登録コマンドを実行することにより生成される。パスワードの桁数は8文字以上、32文字以下である必要がある。また、設定ファイルの内容を変更してコマンドを実行することにより、アカウントの削除、変更を行うことができる。

・サイト管理認証アカウント登録機能

サイト管理認証アカウントは、IDとパスワードが記入された設定ファイルと、本アカウントであることを示す引数と共に登録コマンドを実行することにより生成される。パスワードの桁数は8文字以上、32文字以下である必要がある。また、設定ファイルの内容を変更してコマンドを実行することにより、アカウントの削除、変更を行うことができる。

(2) 識別認証機能

TOEの管理者が使用する機能を利用可能とする前に、本人であることを識別・認証する機能であり、OMIサーバ上、及びOMIクライアント上で実行される。本機能は下記に示す3種類の認証機能により構成される。また、本機能を使用するTOEの管理者は、CWAT管理者、及びサイト管理者であり、いずれの管理者も、それぞれの管理者機能にログオンする前にOM認証されていなければならない。図1-2に各認証機能の関係を示す。

・OM認証機能

CWAT管理者、及びサイト管理者がサイトモニタ画面にログオンしようとするときに、サイト管理認証やサイトログオン認証の前に、登録してあるOM認証アカウント所持者であることを識別し、許可を得ている主体であることを認証するものである。この認証で使用されるアカウントは上記管理者登録機能により生成される。

・サイト管理認証機能

個別サイト詳細画面にログオンしようとする者が、登録してあるCWAT管理者であることを識別し、本人であることを認証する。この認証で使用されるアカウントは上記管理者登録機能により生成される。

・サイトログオン認証機能

サイトごとの設定機能にアクセスし、ポリシー設定、各種配信インターバル、警告再送最大件数等を更新しようとする者が、登録してあるサイト管理者であることを識別し、本人であることを認証する。この認証で使用されるアカウントはサイト管理者によりセキュリティ管理機能を使用して登録される。

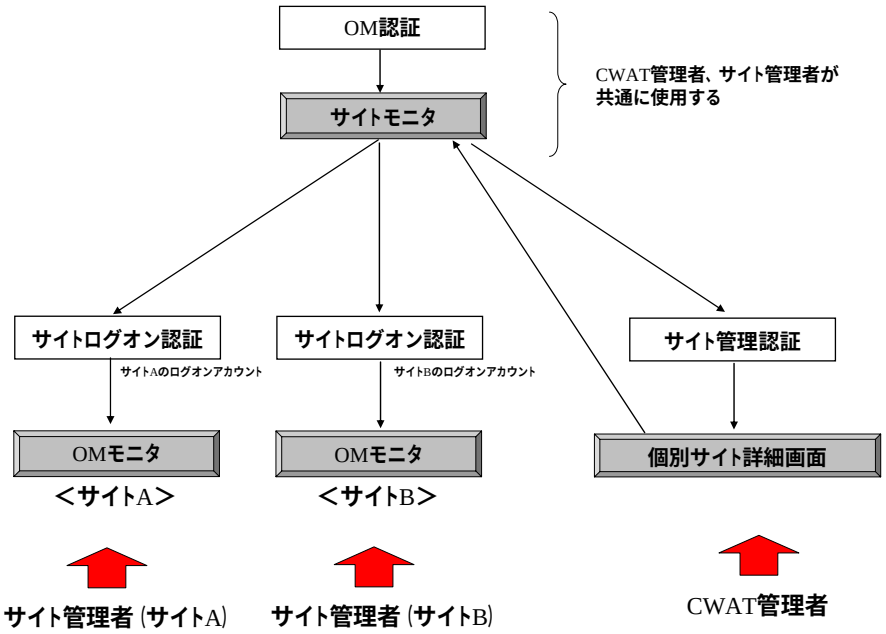


図1-2　各認証機能の関係

(3) OPDC端末ログオン可能ユーザ識別機能

本機能は、当該端末にログオン可能ユーザが設定されている場合、OPDC端末のOSにログオンしようとするユーザのアカウントIDがログオン可能ユーザリストに存在しなければそのアカウントIDによるログオンを拒否する機能である。

(4) アクセス制御

各種統計情報へのアクセス、及びポリシー等に対する各種操作をその権限を有する管理者に制限する機能であり、権限ごとに下記3種類のアクセス制御が行われる。

・サイトの統計情報へのアクセス制御

監視対象サイトの統計情報へのアクセス（参照のみ）をOM認証アカウント所持者のみに制限する機能である。統計情報は主に下記情報により構成される。

- サイトID
- サイト名称
- 構成端末に関する情報（端末数、電源状況、Logon状況）
- 発生警告に関する情報（発生件数、発生時刻、レベル、対応状況）

・サイトの管理情報へのアクセス制御

監視対象サイトの管理情報へのアクセス（登録、更新、削除、参照）をサイト管理認証に成功したCWAT管理者のみに制限する機能である。管理情報は主に下記により構成される。

- サイト関連情報（ID、名称、場所）
- 担当者関連情報（担当者名、電話番号、担当部署、メールアドレス）
- サイト管理者（アカウント管理）

・サイトの詳細情報へのアクセス制御

サイトの詳細情報（ポリシー情報、警告ログ、配信用ポリシー情報ファイル）へのアクセス（登録、更新、削除、参照、更新の反映、出力、通常配信）を、当該サイトのサイトログオン認証に成功したサイト管理者のみに制限する機能である。配信用ポリシー情報ファイルとは、設定されたポリシー情報を元に生成された実際に各ノードに配信されるファイル自体のことであり、このファイルに対する配信操作を行う。警告ログは、各ノードから実際に通知され、データベースにおいて管理されているログ自身であり、画面上の参照操作、及びファイルへの出力操作を行うことができる。

(5) ポリシー配信強化機能

サイト管理者が管理するサイトに対して、最新バージョンの配信用ポリシー情報ファイルをサイト内のノードに適用するための機能であり、下記の機能により構成される。本機能により、設定されたポリシー情報をサイト内の各ノードに配信する際に発生し得る、ネットワーク障害による未配信のリスクを軽減させることが可能

となる。

・自動配信機能

各ノードのTOE（UDC、SDC、OPDC）が上位NM（配信元となる上位ノード）のIPアドレスに対して、設定された配信インターバル（デフォルト60分）でポリシー情報のバージョン問い合わせを実施し、その結果により必要に応じて上位NMからポリシー情報を受信し、自身に反映させる機能。

・強制配信機能

サイト管理者が、セキュリティ管理機能を使用してサイト内の各ノードに反映されているポリシー情報バージョンを確認し、必要に応じて指定ノードに対して最新バージョンのポリシーファイルを強制的に配信させる機能。

(6) 警告ログ送信強化機能

UDC、SDC、OPDCの各ノードで発生した警告ログ（ポリシー違反操作に対する通知）をOMIに送信する際に使用される機能であり、下記の機能により構成される。本機能により、警告ログ送信時に発生し得る、ネットワーク障害による未送信のリスクを軽減させること、及びネットワーク切断状態にある端末上で発生した警告ログを、再接続されたタイミングでOMIに確実に送信することが可能となる。

・異なる方式を併用した警告ログ送信機能

各ノードのTOE（UDC、SDC、OPDC）において不正操作の警告イベントが検知された場合、OMIのIPアドレスに対して即時性の高いプロトコル（UDP）を使用して警告ログを送信する。その後、設定された配信インターバルで警告ログを再送する（再送処理はOMIとの通信成功が確認できるまでリトライする）。

・モバイル状態の警告ログ送信機能

ネットワーク非接続状態にあるOPDC端末上において発生した警告ログを端末内で管理し、ネットワーク再接続時にOMIに対して送信する機能。蓄積された警告ログが、一度に送信できる件数（セキュリティ管理機能で設定）よりも多い場合は、上記配信インターバルのタイミングで全ての警告ログを順次送信する。

(7) セキュリティ管理機能

CWAT管理者、及びサイト管理者が使用するTOEのセキュリティに関連する各種設定機能である。使用する管理者ごとに下記機能に分類される。

・CWAT管理者セキュリティ管理機能

サイト管理認証に成功したCWAT管理者が、個別サイト詳細画面（図1-2参照）より使用する機能で、監視対象となるサイトに関する管理（新規登録、情報更新、登録削除）、及びサイトごとのサイトログオン認証アカウントの管理（登録、内容変更、削除）を行う。

・サイト管理者セキュリティ管理機能

サイトログオン認証に成功したサイト管理者が、OMモニタ画面（図1-2参照）より使用する機能で、サイト内各ノードの属性管理（各端末へのログオン可能ユーザ設定、各ノードのポリシー情報のバージョン参照等）、及び通信関連属性の管理（ポリシー・警告ログ配信インターバルの設定、最大送信件数設定等）を行う。

(8) 監査機能

本機能は、CWAT管理者、及びサイト管理者の識別認証、及び管理画面へのアクセスに関わる監査記録を生成する機能である。OMI上での各管理者の操作を操作ログとして記録し、DBMSが管理するデータベースに保存する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1　想定する脅威

識別子	脅　威
T.EVIL_POLICY_VIA_SERVER（サーバ経由の不正なポリシーの設定）	サーバ設置場所に入室許可を与えられた者のうちTOEの管理者の役割を持たない者がOMIサーバ端末に不正にログオンすることにより、不正なポリシー情報の設定を行うかもしれない。
T.EVIL_POLICY_VIA_OPDC（OPDC端末経由の不正なポリシーの設定）	TOEの管理者としての役割を持たない者が、OPDC端末からTOEを使用せずにポリシー情報へのアクセスを試み、不正なポリシー情報の設定を行うかもしれない。
T.FAIL_SEND_POLICY（ポリシー配信の失敗）	通信パケットの破損もしくは一時的なネットワーク障害により、OMIからDCへのポリシー情報の配信が失敗し、最新のバージョンのポリシー情報がDCに届かないかもしれない。
T.LOSS_WARNING_LOG（警告情報の消失）	攻撃者がOPDCで発生した警告ログをOMIサーバに送信しないようPC端末をネットワークから切り離したり、DCで発生した警告ログが一時的なネットワーク障害により喪失することにより、OMIが警告ログを正しく受信しモニタリングすることができなくなるかもしれない。
T.STOP_OPDC_INTENTIONALLY（サービスの停止）	攻撃者が、PC端末上で稼動しているOPDCのプロセスを不正に停止させることにより、OPDCのサービスが停止するかもしれない。

1.5.6 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1-2に示す。

表1-2 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.AUDIT （監査記録の生成）	TOEの管理者の識別認証、及び管理画面へのアクセスに関わる監査記録を生成できなければならない。
P.SITE_POLICY （サイトのセキュリティ方針）	サイトのポリシー情報、警告ログ、及びそれに付随するデータ（サイトの統計情報、サイトの管理情報）は、そのサイトの管理・監視の責任を持つサイト管理者の操作に制限できなければならない。

1.5.7 構成条件

図1-1の構成において、TOEの動作に必要となるオペレーティングシステム（OS）及びソフトウェアを、TOEを構成するモジュールごとに表1-3に示す。ハードウェアに関しては下記OS、ソフトウェアが動作するマシンが構成条件となる。

表1-3 TOE動作環境

モジュール	動作環境
OMI	OS: Microsoft Windows Server 2003 日本語版 動作条件: Microsoft.NET Framework Version 1.1 以上 高度暗号化パックまたはIE5.5 以降 Microsoft SQL Server 2000 以上
OMIクライアント	OS: Microsoft Windows Server 2003 日本語版、 Microsoft Windows XP 英語版 動作条件: Microsoft.NET Framework Version 1.1 以上 高度暗号化パックまたはIE5.5 以降
OPDC	OS: Microsoft Windows XP 日本語版 Microsoft Windows Server 2003 日本語版 Microsoft Windows XP 英語版 動作条件:

	高度暗号化パックまたはIE5.5 以降 Microsoft Office 2000 以上
SDC	OS: Microsoft Windows Server 2003 日本語版 動作条件: 高度暗号化パックまたはIE5.5 以降
UDC	OS: Microsoft Windows XP 英語版 動作条件: 高度暗号化パックまたはIE5.5 以降
LC	OS: Microsoft Windows Server 2003 日本語版 動作条件: 高度暗号化パックまたはIE5.5 以降

1.5.8 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1-4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1-4 TOE使用の前提条件

識別子	前提条件
A.ADMIN （システム管理者の信頼性）	システム管理者は信頼できる人物であり、TOEのシステム管理者として実施すべき職務を遂行するものとする。
A.CWAT_ADMIN （CWAT管理者の信頼性）	サイト管理認証アカウント所有者はCWAT管理者として与えられた役割を遂行するものとする。
A.SITE_ADMIN （サイト管理者の信頼性）	サイトログオン認証アカウント所有者はサイト管理者として、自身が属するサイトの管理における与えられた役割を遂行するものとする。また、TOEの運用に対して脅威となる行為は行わない。
A.INSTALL （インストールの信頼性）	各専用サーバへのOMI、SDC、UDC及びLCのインストール・設定・アンインストール、各PC端末へのOPDCのインストール・設定・アンインストールは、システム管理者の管理の下に実施されるものとする。
A.PC_USER_ROLE	OPDCが動作するPC端末を利用する管理者以外の端末利

（PC端末利用者の権限）	用者は、システム管理者によって各PC端末のOSであるWindows上に設定されたUsers権限グループのみに属するアカウントを使用する。各PC端末のUsers権限グループ以外のアカウントは、システム管理者のみが利用可能となるような設定を維持することとする。 OMIクライアントが動作するPC端末は、上記のシステム管理者のOSアカウントのほか、TOEの管理者としてその端末の利用を許可するCWAT管理者もしくはサイト管理者のOSアカウントを設定する。
A.PASSWORD_MANAGEMENT （パスワード管理）	TOEにアクセスするためのアカウント（OM認証、サイト管理認証、サイトログオン認証）のパスワードは、主体以外の他者に知られないように主体によって管理する。パスワードは推測・解析されにくいものが設定され、時間経過とともに適正な間隔で変更する。
A.PHYSICAL_PROTECTION （サーバ設置場所の保護）	OMI、SDC、UDC及びLCをインストールする各専用サーバは、コンピュータセンターなど、その組織で運用するシステムの管理・運用のために許可された者のみが入室可能な物理的に保護された区域に設置する。また、OMI機能、SDC、UDC、LCの操作は、サーバが設置された区域でのみ可能となるようにTOEの操作環境を設定する。物理的に保護された区域以外からOMI機能を使用する場合は、端末にOPDCをインストールした上でOMIクライアントをインストールするものとする。
A.NETWORK_RELIABILITY （ネットワークの信頼性）	外部ネットワークからの攻撃はネットワーク機器等の適切な設定により防御されるものとする。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを表1-5、表1-6に示す。

表1-5 日本語版ドキュメント

ドキュメント名称	シリアル番号
CWAT セキュリティマニュアル <セキュリティ構築・設定編>	初版 JP-080229-3.1b_CC_Pro
CWAT インストレーションマニュアル Windows編	2 版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル	初版 JP-070130-3.1b_Pro

Part1 監視編	
CWAT アドミニストレーションマニュアル Part2 ノード・ユーザ管理	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part3 ポリシー管理編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part4 警告・監査情報管理編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part5 CWAT 管理コンソール編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part6 アドミニストレーション編	2 版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part7 TOOL 編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part8 暗号編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part9 盗難端末オプション編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part10 印刷オプション編	初版 JP-070130-3.1b_Pro
CWAT アドミニストレーションマニュアル Part11 CPS 編	初版 JP-070130-3.1b_Pro

表1-6　英語版ドキュメント

ドキュメント名称	シリアル番号
CWAT Security Manual <Security Configuration and Setup>	First edition EN-022908-3.1b_CC_Pro
CWAT Installation Manual (Windows Version2)	Second edition EN-013007-3.1b_pro
CWAT Administration Manual Part1 Monitoring	First edition EN-013107-3.1b_pro
CWAT Administration Manual Part2 Node and User Management	First edition EN-122606-3.1a_pro
CWAT Administration Manual Part3 Policy Management	First edition EN-013107-3.1b_pro
CWAT Administration Manual Part4 Alert and Audit Log Search	First edition EN-013107-3.1b_pro
CWAT Administration Manual	First edition

Part5 CWAT Manger	EN-013107-3.1b_pro
CWAT Administration Manual Part6 Administration	First edition EN-013107-3.1b_pro
CWAT Administration Manual Part7 Administrative Tools	First edition EN-013107-3.1b_pro
CWAT Administration Manual Part8 Encryption Function	First edition EN-122606-3.1a_pro
CWAT Administration Manual Part9 Anti-Theft Option	First edition EN-122606-3.1a_pro
CWAT Administration Manual Part10 Print Option	First edition EN-122606-3.1a_pro
CWAT Administration Manual Part11 CWAT Plat Server	First edition EN-103106-3.1a_pro

2 評価機関による評価実施及び結果

2.1 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。

2.2 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19年3月に始まり、平成20年4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19年12月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成19年12月、及び平成20年1月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び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。

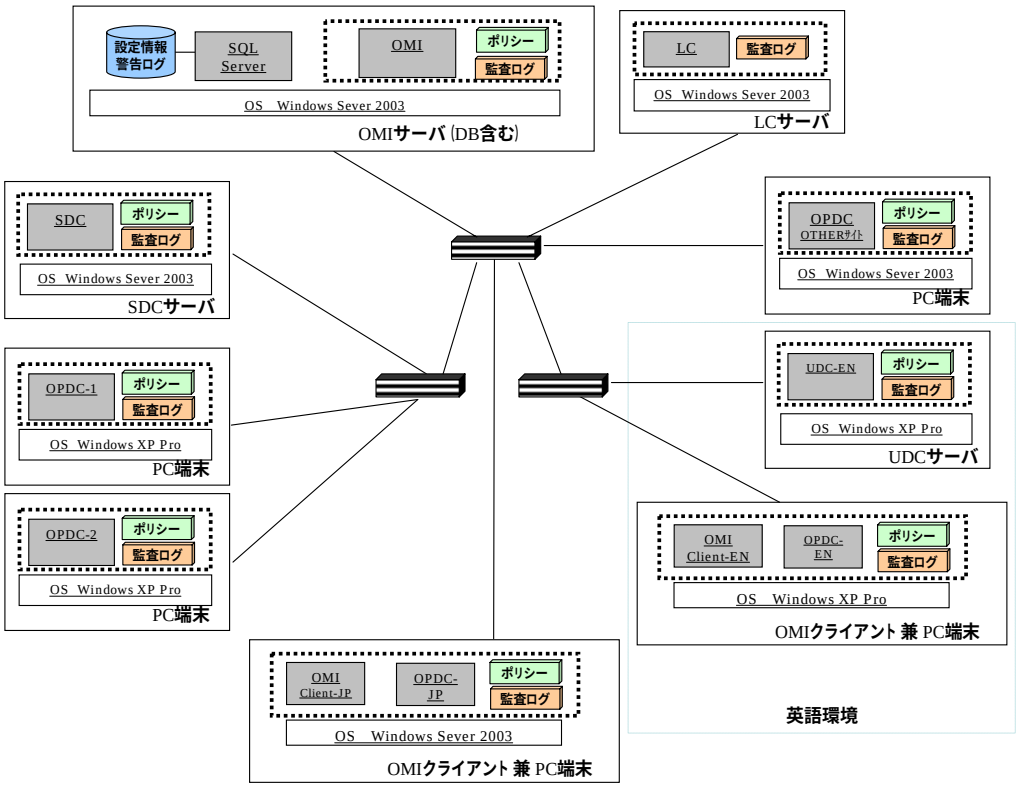
2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。



※ テスト環境は、Firewallによって外部からのアクセスが制限されている

図2-1　開発者テストの構成図

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストは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。

b.テスト手法

テストには、以下の手法が使用された。

①TSFIテスト

コマンド、及び画面インタフェースにより構成されるTSFIを刺激し、表示されるメッセージ内容、画面遷移の状況、設定ファイルの変更状況等を確認することにより、セキュリティ機能のふるまいを観察するテスト

②サブシステム間インタフェーステスト

設定されたポリシーに違反する操作を端末上で実施した上で、ツールを使用してサブシステム間を流れるデータをキャプチャすることにより、警告ログの通知状況を確認するテスト

c.実施テストの範囲

テストは開発者によって333項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1に示す。評価者テストは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。

b.テスト手法

開発者テストにおいて不適切な手法がないと評価者は判断し、テストは開発者テストと同じ手法が使用された。さらに侵入テストにおいては、TSFI以外からのTOEセキュリティ機能へのアクセスの可否を確かめるため、OSのインタフェース（各種ファイル、実行オブジェクトへの直接アクセス）を使用したテストが実施された。

c.実施テストの範囲

評価者が独自に考案したテストを25項目、開発者テストのサンプリングによるテストを71項目、計96項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストにおいて不足していると判断されるテスト項目（特に異常系に関するテスト項目）
② TOEの全てのセキュリティ機能を網羅するテスト項目
③ 開発者テストからは仕様通りに動作することが疑われるセキュリティ機能
④ 脆弱性分析において懸念される事項に関するテスト項目

d.結果

実施したすべての評価者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。

2.4 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 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 当該所見報告書でなされた指摘内容が妥当であること。
② 当該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、ST及び評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された評価報告書、当該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EAL2に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。

ADV_HLD.1.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.1.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確に対応していることを確認している。

ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。

AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

本TOEにおける下記機能は、本評価認証においてセキュリティ機能としての評価対象にはなっていないことに読者は注意されたい。

・ネットワーク監視機能
・端末操作監視機能

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用されたTOE特有の略語を以下に示す。

DC	ディフェンス コントローラ SDC、UDC、OPDCを総称する場合、DCと記載する。
LC	ログコレクタ SDC、UDC 及びOPDC で生成された監査ログを自動収集し閲覧・出力するための機能を提供する。
OMI	オーガナイゼーション モニタ インターナショナル ポリシーを設定し、設定したポリシーをサイトの各ノード（OPDC、SDC またはUDC が動作するサーバまたはPC 端末）へ配信する機能、及びこれらのノードから発生する警告情報の集中監視を行なう機能を提供する。サーバおよびクライアントで動作する。
OPDC	オペレーション ディフェンス コントローラ PC 端末の操作に関する監査ログを生成し、不正操作を検出した場合は警告ログを発生させる機能を提供する。
SDC	セグメント ディフェンス コントローラ ポリシーに基づき、サイトのネットワークアクセス操作を監視する機能を提供する。その他はUDC と同等機能を提供する。

UDC	アンノウンターミナル ディフェンス コントローラ ポリシーに基づき、サイトのネットワークに不正に接続された端末とその動作を検知する機能を提供する。

本報告書で使用された用語を以下に示す。

TOEの管理者	CWAT管理者、サイト管理者の総称
外部接続機器ポリシー	外部機器の接続や外部メディアへのデータ書き込みを監視するための諸条件を設定する。
管理者	システム管理者、CWAT管理者、サイト管理者の総称
警告ログ	ポリシーに基づき不正操作や不審操作が検出されるとDCからOMIに送信されるメッセージ。OMIでモニタリングするために必要な情報を含む。
個別サイト詳細画面	サイトの登録、更新、削除及びサイトの管理情報を設定する画面。
サイト	CWAT3iが監視の対象とするネットワーク及びノードからなるグループを示す概念であり、企業や組織の拠点など、指定した所定のポリシーが求められる単位で設定する。
サイトモニタ画面	CWAT3iの各監視サイトのサマリー情報（サイト一覧情報）を表示する画面。
上位NM（Network Manager）	DCに対し、ポリシーやDC設定情報の配信元となるSDC/UDC、または、OMIのこと。上位NMには、さらに、上位NMを配置するといった多段階の構成をとることが可能である。
端末使用ポリシー	端末使用状況を監視するための対象ノード、ユーザ端末使用行為などを設定する。
ネットワークポリシー	ネットワークのアクセス、ポート番号などを設定する（SDCが必要）。
ポリシー	CWAT3iが監視する不正操作やネットワーク操作に関する条件の集合。
未登録端末	管理サイトにおいて、未登録・盗難端末ポリシーマネージャにて登録されたポリシーに合致しなかった端末。
未登録・盗難端末	未登録端末、盗難端末を監視するための諸条件を設定する

ポリシー	（SDCまたはUDCが必要）。
メッセンジャーポリシー	MSN Messenger/Windows Messenger/ Windows Live Messengerを監視するための諸条件を設定する。
ユーザオペレーションポリシー	ユーザ操作によるファイル操作、使用アプリケーション、画面ハードコピーなどを監視するための諸条件を設定する。
ユーザログオンポリシー	ユーザログオンを監視するための対象ノード、有効期間などを設定する。

6 参照

[1] CWAT3i（Ver3.1b_CC）セキュリティターゲット バージョン 0.39
（2008年4月15日）株式会社インテリジェントウェイブ

[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 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[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2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0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: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0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: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 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2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] CWAT3i（Ver3.1b_CC）評価報告書 第1.1版 2008年4月16日
株式会社 電子商取引安全技術研究所 評価センター