

情報漏えい対策システム「CWAT（シーワット）」の 最新バージョン CWAT V5.3 を発売

－2014年12月1日から出荷開始－

2014年 11月 25日

株式会社インテリジェント ウェーブ（本社東京都中央区新川 1-21-2、代表取締役社長 山本祥之）は、情報漏えい対策システム「CWAT（シーワット）」の最新版「CWAT Version5.3」を2014年12月1日に出荷開始します。

「CWAT」は、PCなどの情報端末（クライアント）のファイル操作、アプリケーション起動、メール送信、Web操作や外部メディアへの書き込み、接続を監視し、セキュリティポリシーに基づいてデータやファイルの不正な持ち出しを未然に防ぐ情報漏えい対策システムです。

クライアントの操作履歴を記録した「監査ログ」、セキュリティポリシーに違反した操作履歴を「警告ログ」として管理ができるので、企業の情報管理と内部統制を強化するシステムとしても高く評価されています。

最新バージョン「CWAT Version5.3」では、社内でセキュリティポリシーを設定するための申請、承認の業務フローをシステム化した、申請・承認ワークフローオプション『w-GRID(ダブルグリッド)』や、大量の監査ログデータを高速検索するオプション『Q-GRID(エルグリッド)』、未許可の無線LANアクセスポイントへの接続を防ぐ監視機能『PowerNe(パワーエヌ)』（機能拡張）、PCリモートコントロール機能、クライアント監視エージェントの仮想化環境(XenDesktop/VMware)対応といった多くの新機能を実装し、企業の情報漏えい対策を大幅に強化しています。

CWAT Version5.3 の特長

1. 新しいIT環境へ対応

- (1) Microsoft SQL Server 2014 対応
- (2) デスクトップ仮想化(XenDesktop/VMware) 対応

2. 強化オプションの追加と拡張

- (1) 申請、承認 ワークフロー機能(w-GRID) 新規開発
担当者からのセキュリティポリシー変更申請を、直接承認者に送信することができるようになりました。承認者は許可、却下の選択をするだけなので、ポリシー管理業務がこれまでより簡単かつ柔軟に運用できるようになりました。
- (2) 監査ログ高速検索機能(Q-GRID) 新規開発
“大規模データ用分散処理フレームワーク”と“高速検索エンジン”2つのOSSテクノ

ロジックを活用して、膨大な CWAT 監査ログから目的のデータを高速検索することができます。

- (4) 未登録無線 LAN アクセスポイント監視機能 (PowerNe) 機能拡張
未登録のアクセスポイントが接続先候補に表示されることを防ぎ、脆弱なフリースポットへのネットワーク接続を監視します。
- (5) 新規通信プロセス監視機能 (PowerNe) 機能拡張
特定のアプリケーションが、企業の外部へと新規に通信プロセスを開始した際に、リアルタイムに監視、通信を遮断 (プロセス強制停止) することが可能です。無断通信 (成りすまし通信) での漏えい動作を遮断できます。

3. 標準搭載機能の追加 新規開発

- (1) PC リモートコントロール機能
OM Web 画面から、監視エージェント導入済み PC にボタン一つでログインし、遠隔操作が可能となります。
- (2) OM 管理画面改善
より使いやすい画面、より効果的な運用を追求して、管理画面の改善を行いました。

<動作環境>

OM

導入先：専用サーバ

OS：Microsoft Windows Server 2008 R2 (Enterprise/Standard) x64 SP1

Microsoft Windows Server 2012 (Standard) x64

Microsoft Windows Server 2012 R2 (Standard) x64

動作条件：Microsoft .NET Framework 4.5

Microsoft SQL Server 2008 R2 (Enterprise/Standard) x64 SP2 及び SP3

Microsoft SQL Server 2012 (Enterprise/Standard) x64 SP1

Microsoft SQL Server 2014 (Enterprise/Standard) x64

Microsoft Internet Information Services 7.5/8.0/8.5

OPDC ※1

導入先：クライアント端末

OS：Microsoft Windows Vista (Business/Enterprise) x86, x64 SP1 及び SP2 ※2

Microsoft Windows 7 (Professional/Enterprise) x86, x64 SP1

Microsoft Windows 8 (Professional/Enterprise) x64

Microsoft Windows 8.1 (Professional/Enterprise) x64

対応仮想環境：Citrix XenDesktop7.5

VMWare Horizon View6

※1：OM Version5の監視環境で、OPDC Version5とOPDC Version4のハイブリッド運用が可能です。

※2：Windows VistaはVersion4のみ対応しています。

<<株式会社インテリジェント ウェイブ>>

株式会社インテリジェント ウェイブは、カードビジネス事業、システムソリューション事業、セキュリティシステム事業を行っています。特にカードビジネス事業では、自社開発パッケージによるクレジットネットワークシステムおよび集配信システムの提供で大手クレジット会社の多くのシェアを占めています。この金融業界で培った技術はセキュリティ技術に応用され、カード不正対策システムや内部情報漏えい対策システムに活かされています。

<<本件に関するお問い合わせ先>>

株式会社インテリジェント ウェイブ

営業本部

TEL：03-6222-7300 FAX：03-6222-7301

E-Mail：cwatsales@iwi.co.jp

URL：http://www.iwi-security.com/

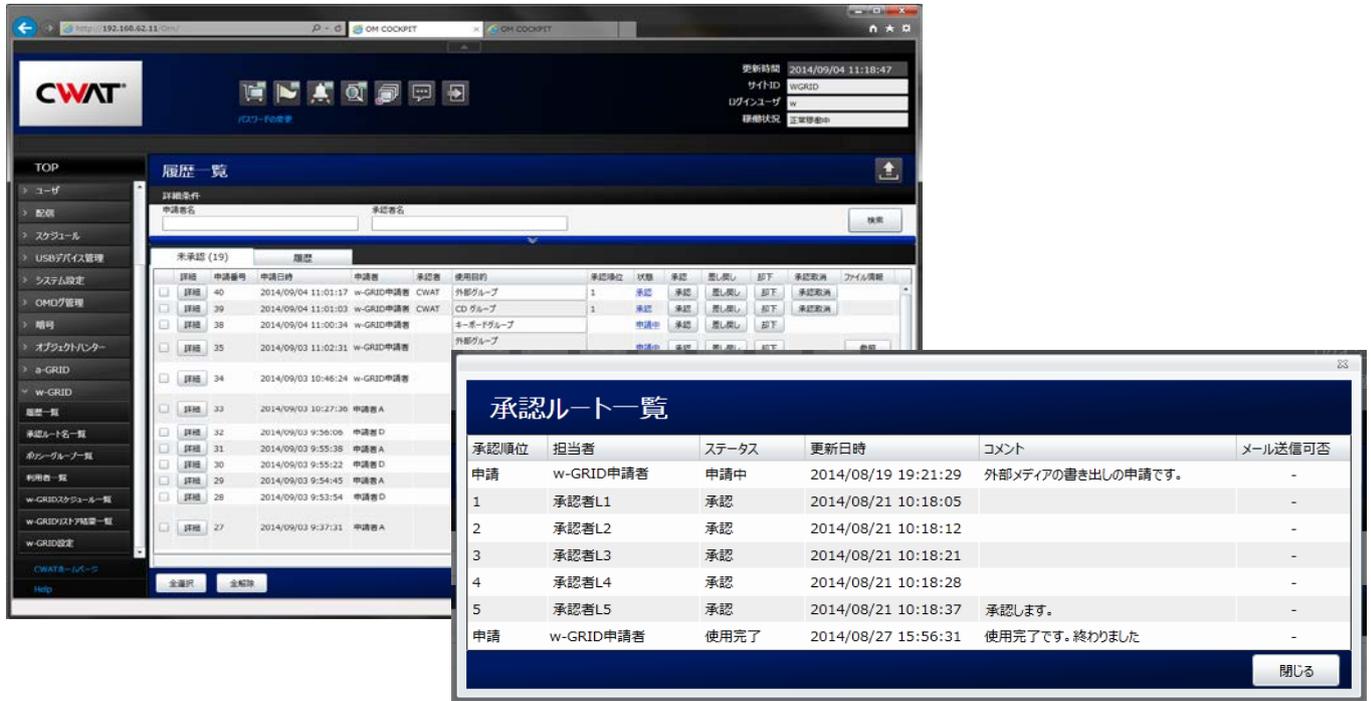
<<商標・著作権について>>

「CWAT」は株式会社インテリジェント ウェイブの日本国またはその他の国における商標または登録商標です。記載の会社名および商品名、ウェブサイトのURLなどは、本リリース発表時点のものです。

文中では、TM、(R)マークは原則として明記しておりません。その他記載されている会社名、製品名は各社の商標または登録商標です。

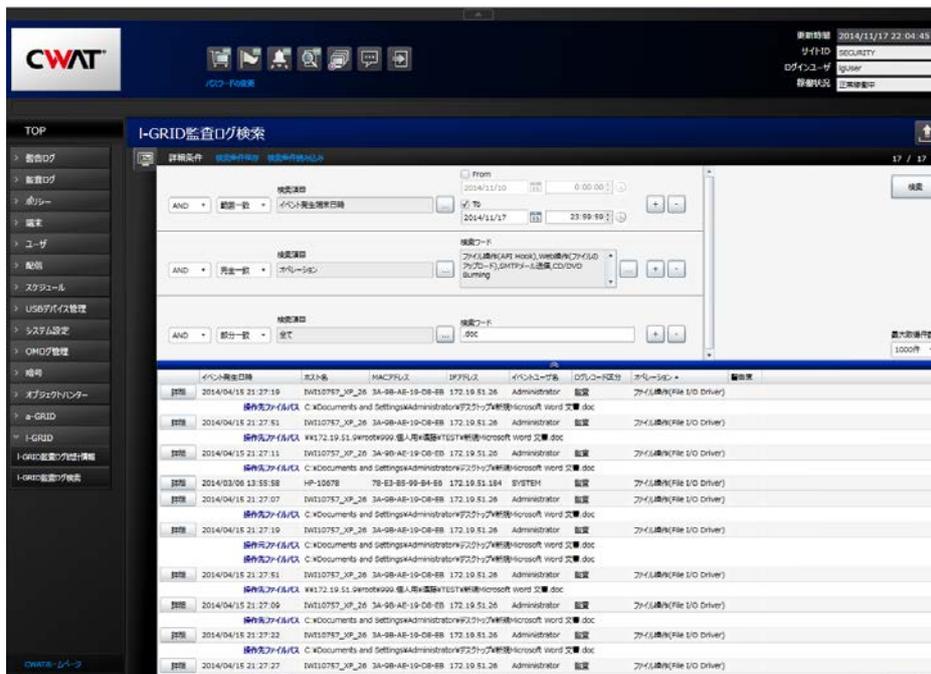
(参考)

* 申請/承認 ワークフロー機能『w-GRID(ダブルグリッド)』画像



(参考)

* 監査ログ高速検索機能『l-GRID(エルグリッド)』画像



(参考)

* 未登録無線 LAN アクセスポイント監視機能『PowerNe(パワーエヌ)』画像

ポリシー作成画面



ネットワーク監視ポリシー詳細

ポリシー名: 未承認アクセスポイントへの接続
 ポリシーID: 1000003

監視対象時間
 終日監視
 指定時間監視
 監視開始時間: 00 時 00 分 監視終了時間: 24 時

説明

検知時動作

自動対処
 オペレーション中止
 監査ログに出力する
 警告を発信する
 スナップショットを出力する
 ポップアップメッセージを出力する
 警告: アクセスポイント名が詐称されている危険なアクセスポイントです。 接続を切断します。

警告通知メール設定
 警告通知メールを送信する

検知条件

ネットワーク監視ポリシー種類
 通信 新規通信プロセス 無線LANアクセスポイント

検知対象除外アクセスポイント
 検知対象除外アクセスポイント(SSID)を指定する
 接続許可アクセスポイント
 上記指定ブック内容を除外する
 上記指定ブック内容以外を除外する

監視対象オプション
 検知対象除外MACアドレス(BSSID)を指定する
 接続許可アクセスポイント
 上記指定ブック内容を除外する
 上記指定ブック内容以外を除外する

更新 キャンセル

警告ログ詳細画面



警告ログ詳細

警告情報共通

警告ID: 274
 警告度: High
 警告種類: オペレーション警告
 オペレーション: ネットワーク監視(無線LAN接続)
 操作番号
 操作番号フラグ: 無効
 検知日時: 2014/10/31 17:17:23
 警告検知端末日時: 2014/10/31 17:17:31
 警告受信日時: 2014/10/31 17:17:57
 詳細/編集/削除: TOP&W

警告個別情報

アクセスポイント名: CWAT
 接続先MACアドレス: CC-E1-D5-0A-41-5A
 測定方法: 三角測量
 緯度: 35.65117
 経度: 140.03742

対応コメント一覧

更新日時	コメント	オペレータ

警告対応状況一覧

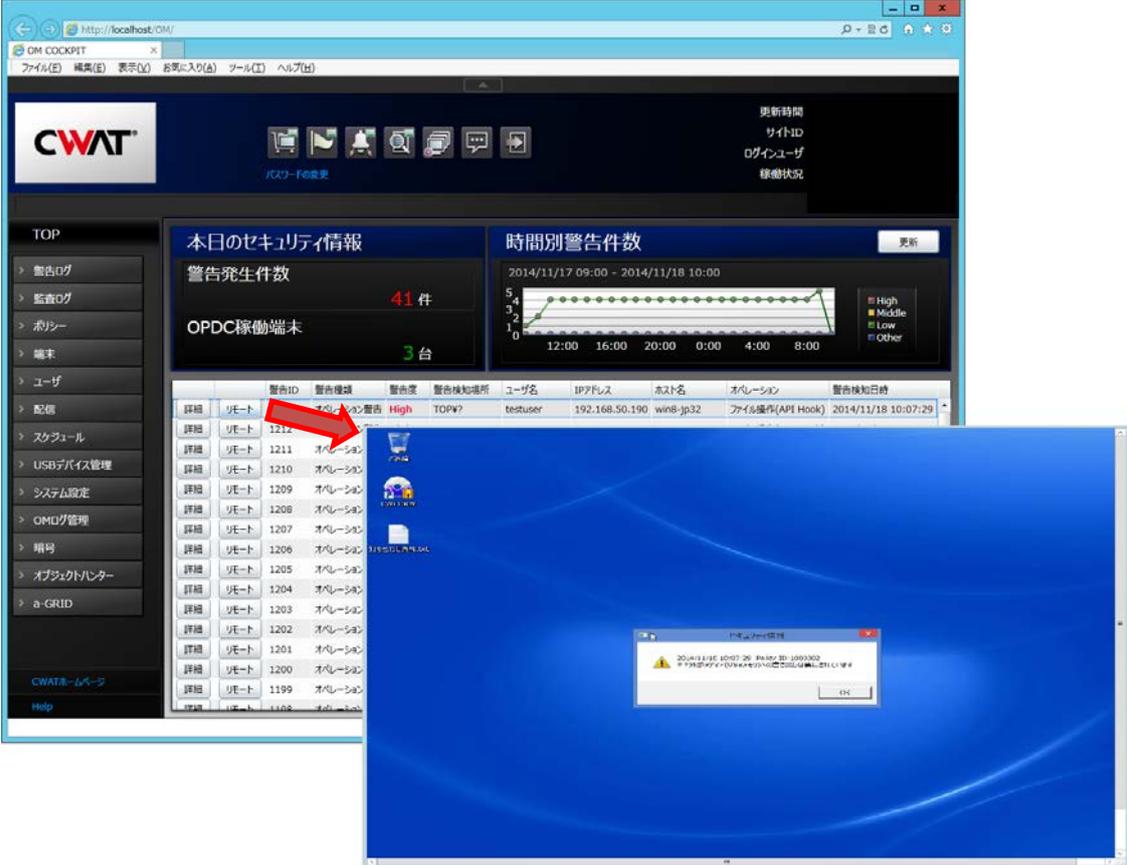
更新日時	警告対応状況	オペレータ
2014/10/31 17:17:57	未対応	System

端末対処/OPDC制御履歴一覧

更新日時	対処/制御区分	対処/制御内容	対処/制御状況	オペレータ
2014/10/31 17:17:57	自動対処	オペレーションの中止	成功	System
2014/10/31 17:17:57	自動対処	オペレーションの中止	開始	System
2014/10/31 16:00:31	自動対処	オペレーションの中止	成功	System
2014/10/31 16:00:31	自動対処	オペレーションの中止	開始	System

閉じる

* PC リモートコントロール機能 (標準搭載機能)



The screenshot displays the CWAT OM COCKPIT interface. The main dashboard shows security information for the current day, including 41 alerts and 3 OPDC team terminals. A table lists various alerts, with a red arrow pointing to the first entry. A graph shows the number of alerts over time. A remote control window is overlaid on the bottom right, showing a Windows desktop with a system message box.

詳細	リモート	警告ID	警告種別	警告種別	警告種別場所	ユーザ名	IPアドレス	ホスト名	オペレーション	警告種別日時
詳細	リモート	1212	オペレーション警告	High	TOPW?	testuser	192.168.50.190	win8-jp32	ファイル操作(API Hook)	2014/11/18 10:07:29
詳細	リモート	1211	オペレーション							
詳細	リモート	1210	オペレーション							
詳細	リモート	1209	オペレーション							
詳細	リモート	1208	オペレーション							
詳細	リモート	1207	オペレーション							
詳細	リモート	1206	オペレーション							
詳細	リモート	1205	オペレーション							
詳細	リモート	1204	オペレーション							
詳細	リモート	1203	オペレーション							
詳細	リモート	1202	オペレーション							
詳細	リモート	1201	オペレーション							
詳細	リモート	1200	オペレーション							
詳細	リモート	1199	オペレーション							
詳細	リモート	1198	オペレーション							