バージョンアップリリースノート

Flowmon ADS

注：VerUP 時には再起動、及びファイルチェックが行われる場合があります。

ver.No	リリース日	追加機能
Ver.9.05.08	2019/09/02	誤検知除外機能の動作中にイベントが削除された場合に警告処理が追加されました。
		修正された問題
		Flowmon OS 10.3 の Flowmon ダッシュボードが正しく表示されるようになりました。
		フランス語でのイベントの CSV エクスポートに対応しました。
		新しいパースペクティブに対する評価が改善されました。
Ver.9.05.07β	2019/08/16	誤検知除外機能の統計処理バッチのパフォーマンスが改善されました。
		Flowmon OS による IP アドレスに関する地理情報の表示が改善されました。
		Flowmon OS 10.3 のサポートが可能となりました。
		修正された問題
		イベントの詳細情報内の誤検知除外機能により削除されたターゲット情報が改善されました。
		誤ったタイムゾーンで検索された IDS イベントが改善されました。
		イベント処理中のイベント詳細の表示をブロックしました。
Ver.9.05.06	2019/06/25	より迅速な誤検知と見通しの評価ができるようになりました。
		修正された問題
		期限切れのフロータイムスタンプが誤ったイベントタイムスタンプ正規化する問題を修正しました。
Ver.9.05.05	2019/06/20	新しいイベントの最適化処理が可能になりました
		修正された問題
		IPv6 アドレス ffff：…：ffff がフィルタに存在する場合、イベント処理が機能しない問題を修正しました。
		誤検知ルール使用カウンタの最大値に達したときにイベント処理が機能しない問題を修正しました。
		データ処理用データベースの起動が遅れていた問題を修正しました。
		管理者以外のユーザが CSV ファイルのレポートをエクスポートすることができない問題を修正しました。
Ver.09.05.04	2019/05/24	FlowmonOS　10.2 のサポートが可能となりました。
		修正された問題
		ADS 分散アーキテクチャが有効になっている場合、特殊な環境下において誤検知機能が作動しない問題を修正しました
Ver.9.05.03β	2019/04/17	修正された問題
		Syslog/SNMP イベント報告が遅延する問題を修正。
		仮想ソースが有効になっていると Syslog/SNMP イベントレポートが機能しない問題を修正。
		http ホスト名に基づくブラックリストが機能しない問題を修正。
		イベント詳細ダイアログで、既存のイベント誤検知ルールを評価してしまう問題を修正。
Ver.9.05.02β	2019/03/26	修正された問題
		FMC で NEL/NSEL 拡張が有効になっている場合に間違った国コードになる問題を修正。
		データフィールド All が選択されていると CSV レポートが機能しない問題を修正。
		メールイベントレポートが機能しない問題を修正。
		Flowmon OS 10.1.3 でのイベント証跡の破損を修正。
		メソッドを無効にしたときにメッセージにコロンが表示されない問題を修正。
		注：Syslog Machine Readable Detail は、属性にも統一単位（KiB）を使用します。
		注：Flowmon OS ver.10.01.04 より古いバージョンの Flowmon コンフィグレーションセンターでは、ブランディング機能により PDF レポートのロゴを変更することができません。
Ver.9.05.01β	2019/02/22	修正された問題
		E メールへの送信が失敗するという問題において、PDF のスケジュールされたレポートを修正しました。
		ワイルドカードを使用した False Positive ルールにより処理が停止する問題を修正しました。
		注：PDF レポートのロゴは現在ブランディングでは変更できません

ver.No	リリース日	追加機能
Ver.9.05.00	2019/02/07	ダッシュボードの概要ページを以下の通り再設計しました。 時間内のイベント数とフロー数/秒の新しいグラフを表示。 グラフの下に表示されるイベントの種類は無制限です。 自動更新は更新ボタンで有効にできます。
		誤検知ルールを無効にして再度有効することができます。
		選択したオプションで誤検知ルールが作成された場合、イベントを削除できます。
		ADS 分散アーキテクチャがアクティブな場合、Syslog/SNMP は、マスターノードから送信されます。
		Flowmon Traffic Recorder ver.10(アダプティブバッファ)に対応し、履歴の記録を開始できます。
		修正された問題
		グラフにイベントが表示されないという問題において、[イベント]ページの集計ビューが修正されました。
		DNSREVERSE メソッドの遅延イベントを修正しました。
		注：Syslog マシンの読み取り可能な詳細は一時的に変更されます（単位は以前のように統一されていません）。
Ver.9.04.02	2018/11/9	データフィード設定のバグを修正しました。 （バージョン 9.04.01 で「仮想ソースとしてのチャンネル」オプションが変更された場合）
		最新のユーザガイド（日本語）を搭載しました。
Ver.9.04.01		無効な XML 設定のインポートを修正しました（データフィードセクション）
		分散アーキテクチャモードでのデータフィードの予期しない無効化を修正しました。
Ver.9.04.00		ADS 分散アーキテクチャ設定ウィザード（kads-wizard.py）を追加しました。
		アトミックフィルタをリレーショナルに変換するための新しい関数。
		既存のデータフィードをすべての検出方法に割り当てるための新機能。
		データフィードページで欠けているプロフィール/チャンネルのシグナル伝達を改善しました。
		ADS イベントデータベースに関する稀な問題を修正しました。
Ver. 9.03.00		Flowmon OS 10 に対応いたしました。
Ver.9.02.02	2018/10/24	Flowmon OS 9.01.06 で ADS の以前のバージョンをアップグレードする機能が追加されました。 （Flowmon ADS は、Flowmon OS がバージョン 9.02.01 以降にアップグレードされるまで無効になります）
		MAC アドレスの検出（イベントソース IP として 127.0.0.1 の場合）が修正されました。
		Flowmon OS 9.02.02 以降のイベント報告を修正（動作していない）しました。
		Flowmon OS 9.02.02 以降のブラックリストの表示を修正（予期しないエラー）しました。
Ver.9.02.01β		イベント詳細の詳細およびソース MAC アドレスを使用した syslog レポートが拡張されました。
		syslog メッセージの変更点： - 新しいフィールドを追加しました smac = XX：XX：XX：XX：XX：XX
Ver.9.02.00β		削除された機能「脅威（集約されたイベント）」。
		新しい言語（ドイツ語、フランチャイズ、スペイン語）のサポートを追加。
		ユーザグループ（FCC ロール、ADS タブ）に ADS 管理者権限を与える機能を追加。
		簡単にフォーム設定を複製するための「名前を付けて保存」機能が新しく追加されました。
		計算データベース（セキュリティパッチ）が更新されました。
		BPATTERNS - 新しいパラメータ "Activation"（新しく追加されたパターンのデフォルトステータス）が追加されました。
		CSV ファイルへのエクスポートを修正しました（最大イベント数）。
Ver.9.01.03	2018/5/24	電子メールレポートに GPG 暗号化/署名のサポートを追加（FM 9.01.03 より）しました。
		拡張された RESTful API：カスタムスクリプトとレポート
		長い章名を持つ PDF レポートの構成エクスポートを修正しました（間違った名前切り捨てにより、インポート後に依存関係が失われる不具合を修正）。
		ADS ライセンスを下位モデルに変更した時の、データフィードのアクションの不具合を修正しました。
		HONEYPOT メソッドの IgnoreAccessFrom パラメータを修正しました。
		今後の FM 10.00.00（NoDataException）との互換性が修正されました。
Ver.9.01.01	2017/11/1	Flowmon OS 9.00.04 以上でのイベントエビデンスへのフローロードが改善されました。

ver.No	リリース日	追加機能
Ver.9.01.00β		新しい検出方法 DICTATTACK（辞書攻撃の一般的な検出）
		レポートに CSV 形式のエクスポートを追加
		カスタムパターンの強化された機能（Having 節、イベントソースの選択、ヘルプの追加）
		フィルタ、パースペクティブ、データフィードの削除に関連するすべてのアクションに関する警告が改善されました。
		SNMP イベントレポートの改善（複数のレポート、FCC SNMP ターゲットグループのサポート）
		ダッシュボードページにデータロードの信号を追加（ドリルダウン）
		ADS Ultimate ライセンスのサポートを追加
		修正された syslog イベントレポート形式（Syslog UDP 送信者が使用されている場合、ホスト名が不明）
		脅威のリスニングイベント（rest / ads / threats / <id> / events はコード 302 を返すことがある）のための固定 RESTful API クエリ
		イベントの詳細でのトラフィック記録ファイルのダウンロードを修正しました（「同じイベント間隔」が設定されている場合）
Ver.9.00.01β		多数のフロー・ソースに対する最適化された処理パフォーマンス（統計的オーバーヘッドを削減）
		アップグレード後に固定フローソースが停止する（「実行していない」状態が表示される）
		Flowmon モバイルダッシュボードアプリケーションのウィジェット表示を修正しました
		固定イベントの有効期限（Delete Events After パラメータで定義された時間より前に発生する可能性があります）
		すべてのフローソースまたはフィルタを削除した後のユーザインターフェイスの問題を修正しました。
		改善されたユーザガイド（検出方法の再編成、オペレーティングシステムテーブルのカスタムパターンへの追加）
Ver.9.00.00β		Flowmon OS 9.x プラットフォーム（データ処理、システムサービスなどの新しいデータベース）に最適化されています。
Ver.8.02.05	2017/7/27	日本語版ユーザガイドをアップデートしました。
Ver.8.02.04	2017/2/16	Flowmon OS バージョン 8.03 以上でのイベント証拠の表示を修正しました。 ・MAC アドレスコンテキストメニューの固定ラベル ・特殊な記号を使用した外部 IP サービス URL の修正
		IP アドレス割り当て（望ましくない IP 部分文字列一致）に対する DNS 名を修正しました。
		イベントエビデンスでのフィルタリングのパフォーマンスが向上しました。
Ver.8.02.03	2017/1/18	特別な場合の UPLOAD メソッドの検出を修正しました（pairwise オプションを無効にしました）
		ダッシュボードの概要図の月の名前の翻訳が修正されました
		SCANS – RST / ACK スキャンの実験的検出を削除。
Ver.8.02.02		ブラックリストイベントベースのホスト名の詳細を修正 (変換するバイト数の合計)
Ver.8.02.01 β		データ処理のデータベースの起動処理を修正
		長文の DNS レコードの表示を修正
		自動 IP アドレス名前変換が無効になったとき、誤検知除外処理の修正
		双方向フローに関連した、検知メソッドの修正 (IPV6TUNNEL, SRVNA, DNSANOMALY,)
		BLACKLIST - "malware domains" の情報で、"malware activities" を変更しました。
Ver.8.02.00 β		パフォーマンスの改善 (双方向フローに切り替え)
		フローサンプリングの拡張 (ペアフローの対策)
		フローの重複の解析拡張 (異なるソースからのフローのみを比較)
		逆引き DNS レコードの取り込みメソッドを変更 (ページレンダリング中にリアルタイム処理)
		MULTICAST - MAC アドレスベースの検知を追加
		REFLECTDOS - 新規 TFTP 攻撃の検知を追加 (TrivialFTP パラメータ)
		SMTPANOMALY - 新規パラメータ IgnoreSYNflows 追加 (検知から SYN フローを除外)
		SYSCHECK - 新規パラメータ DeactivateOnFlood 追加 (大量のイベント発生時に無効にするメソッド)
Ver.8.01.02		SNMP 経由のイベントレポートの修正
		存在しないプロファイル/チャネルでフローソースの設定の保存処理を修正
		誤検知除外処理の修正 (名称に特殊なフィルタ記号が含まれる場合)
		イベントエビデンスタブ上のメニューオーバレイの修正
		イベントの集約表示の拡大表示を修正
Ver.8.01.01		AdBlock browser プラグインによるブロックされた機能 "Show filters for IP"の修正
		"Edit user"表示中の "Renamer settings"の保存を修正

ver.No	リリース日	追加機能
Ver.8.01.00		新分散アーキテクチャ (複数の ADS がインストール環境のリンクの可能性)
		大規模ブラックリストのサポートを追加 (C&C ドメインリスト
		メールイベントレポート中の日付フォーマットの選択オプションの追加
		PDF チャプタ"Events by priority"中のイベントソートのためのオプションの追加
		メインメニューの表示の更新
		ロングテーブルでの新フローティングヘッダー表示
		新機能 "Show filters for IP" (IP アドレスの文章メニュー)
		"Event detail" 拡張表示 (メソッドインスタンスの名称追加)
		最新のダウンロードされたブラックリストの表示拡張 (ページを追加)
		"Event Evidence" テーブルの拡張 (新規のフィールド、apptag コードからアプリケーション名変換)
		NATDET - IP アドレスの背後の NAT の発見する新たなメソッドの追加
		BLACKLIST - イベント詳細の拡張 (ブラックリストされたドメインの表示)
Ver.8.00.05		syslog メッセージの SNTPANOMALY メソッドの説明が消える問題の修正
Ver.8.00.04		スケジュールド PDF レポートの修正(送信)
		プロキシ相関関係の修正と拡張(設定ミスについての注意を追加)
Ver.8.00.03		HTML イベントレポートの拡張 (イベント詳細に関連する IP アドレスの代わりにホスト名を利用)
		アップグレード中、SCANS メソッドの DetectOnlyKnown のオプション設定が上書きされる問題の修正
Ver.8.00.02		翻訳のミスを修正 (アップグレード後のキャッシュのリフレッシュ)
		バックグランドで起動する ADS データベースの修正(システム起動がブロックされた)
Ver.8.00.01		ADS ソース編集フォームでプロファイル/チャネルの表示を修正
Ver.8.00.00		関連フィルタの追加 (関連情報でのフィルタ込み入ったフィルタの定義を許可)
		誤検知除外ページの IP アドレス表示の拡張
		PDF レポート用の新規チャプタ "Events by type"を追加 (タイプによる TOP 10)
		PDF レポートのパーミッションの再設定(オーナー設定機能を追加)
		IgnoreInternal パラメータの追加(内部ローカルセグメントの通信を無視)
		BLACKLIST - DNS トラフィックでブラックリストされたドメイン名を検出するを新規に追加(Flowmon 独自 DNS フィールド設定)
		DOS - syn flood と fin2-wait 攻撃を検出する機能を新規に追加
		MULTICAST - 高トラフィックを検出する機能を新規に追加(データ合計もしくは秒間での高パケットレート)
		REFLECTDOS - portmap サービス経由の攻撃を検出する機能を新規に追加
		SCANS - ARP scans 検出する機能を新規に追加
		SCANS - DetectThesePorts パラメータにポートレンジ入力可
		OUTSPAM メソッドを SMTPANOMALY メソッドに名称変更
		BTTORENT MinSeeds パラメータの意味を変更 (すべてのイベントに適用)
		CSV へフィルタをエクスポート 機能を削除 (重複のため、FCC コンフィグレーションのインポート/エクスポートでリプレース)
		空き容量のアラートを削除(クォータ管理に定義された推奨されないデータ領域)
		syslog メッセージの変更
		短いメソッドコード後にメソッド名が長い場合の問題を修正
		INVEA-TECH の社名変更に伴う、会社名記述を Flowmon Networks に変更
		いくつかのメソッドのイベント推奨詳細を変更(例：MULTICAST)