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	変更箇所
Ver.11.02.04	2021/04/28	修正された問題
		Samba 拡張機能を有効にしても「DICTATTACK: SambaProtocol」のサブメソッドの誤検出が発生しなくなりました。
		BPATTERNS およびカスタムパターンイベントのイベント詳細に、誤検知除外ルールによって削除されたターゲットの数が含まれるようになりました。
		Syslog で破損した IDS イベントを受信すると、IDS イベントの処理が停止していた問題を修正しました。
		チェコ語でのユーザガイドが再度利用できるようになりました。
Ver.11.02.02	2021/03/10	新着情報
		ADS イベントのマッピングに使用される MITRE ATT&CK マトリックスがバージョン 7 からバージョン 8 へ更新されました。 バージョン 8 は、新たに検出されたイベントに対してのみ行われます。今回の更新以前に検出されたイベントは、バージョン 7 に基づいてマッピングされます。
		注釈
		本バージョンには、同日にリリースされた Ver.11.01.05 からの変更点が含まれています（詳細は「過去のリリース - バージョン 11.01.05」をご参照ください）。
		既知の問題点
		日本語のユーザガイドはまだご利用になれません。
Ver.11.02.01	2021/02/25	修正された問題
		イベントを CSV ファイルでエクスポートした際、ヘッダーがずれてしまう問題を修正しました。
		DHCPANOMALY（サブメソッド：ServerChange でのみ発生）において、現在の MAC アドレスが更新されず、イベント詳細に以前と現在で同じ MAC アドレスが表示されていた問題を修正しました。
		注釈
		本バージョンには、Ver.11.01.03 からのパフォーマンスの最適化が含まれています（詳細は「以前のリリース - バージョン 11.01.03」をご参照ください）。
		本バージョンには、同日にリリースされた Ver.11.01.04 からの変更点が含まれています（詳細は「過去のリリース - バージョン 11.01.04」をご参照ください）。
Ver.11.02.00	2021/01/27	新着情報
		解析でのイベントチャートの表示を改良しました。
		イベントチャートが補間曲線で平滑化されるようになりました。
		MITRE ATT&CK の tactics and techniques は、ADS の検出（サブ）メソッドにマッピングされ、ユーザに追加のコンテキストを提供するようになりました。
		ADS の検出イベントに MITRE ATT&CK をマッピングし、ユーザに追加のコンテキストを提供するようになりました。
		最も正確なマッピングを実現するために、文脈的解析が行われます。そのため、同じサブメソッドの異なるイベントに異なる MITRE ATT&CK の tactics and techniques を割り当てることができます。また、イベントの展開状況に応じて、1 つのイベントに複数の tactics and techniques を割り当てることも可能となりました。
		検知方法やサブメソッドの中には、どの MITRE ATT&CK の tactics and techniques にも割り当てられていないものが存在します（例えば、適切な tactics や techniques が存在しない場合や、その方法が構成上の問題を検知する場合など）。
		マッピングは、ATT&CK v7: https://attack.mitre.org/versions/v7/ に対応しています。
		マッピングは過去にさかのぼって行われないため、ADS11.2 へのアップデート前に検出されたイベントは、MITRE ATT&CK のどの tactics and techniques にも割り当てられません。
		JA3 フィンガープリントを用いて、暗号化されたトラフィック解析が可能となりました。
		JA3 フィンガープリントは BLACKLIST メソッドを拡張し、暗号化されたトラフィックに含まれる悪意のある通信を検出するようになりました。
		JA3 フィンガープリントは、新しい JA3 ブラックリストのデータフォーマットを使用して、ローカルまたはリモートのブラックリストとして追加できるようになりました。
		フローレコードには JA3 フィンガープリントのパラメータが必要（Flowmon Probe 提供）であり、JA3 フィンガープリントは Configuration Center で有効にすることが可能： Flowmon Probe ＞ モニタリングポート ＞ 高度な設定＞ TLS JA3 フィールド

ver.No	リリース日	変更箇所
		Flowmon Collector ＞ FMC 設定 ＞ フローのデータベースフィールド＞ TLS JA3 フィールド
		JA3 フィンガープリントを使用すると、正当なアプリケーションと悪意のあるアプリケーションの JA3 フィンガープリントが衝突する可能性があるため、誤検出の原因となる可能性があります。ユーザは以下のリンクから JA3 ブラックリストをダウンロードし、ローカルのブラックリストとして追加すると、必要に応じて編集することができます。ブラックリストをリモートで設定した場合、ブラックリストの内容をローカルで設定した場合のように自由に編集することはできませんが、リモートでは JA3 フィンガープリントのブラックリスト提供者から自動的にリストを取得/更新します。
		JA3 のブラックリストはこちらから入手可能となります：https://services.flowmon.com/reputation/ja3malware/list.csv
		脅威情報共有プラットフォームの MISP に対応するようになりました。
		MISP インスタンスをリモートブラックリストとして ADS に接続することで、MISP の IoC フィードからブラックリストを自動的に作成し、悪意のある通信を検知できるようになりました。
		BPATTERNS の 1 秒あたりのフロー（fps）性能が向上しました。
		ADS Business 以上のモデルをお持ちのすべてのお客様に、パフォーマンスの向上をもたらします。
		最大パフォーマンスが 15k から 25kfps に向上しました（Enterprise と Ultimate モデルで有効）。
		詳細は Flowmon ADS スペックシートをご参照ください。
		“サービスタイプ”のブラックリストで、任意のプロトコルに対してキーワードに“ANY”を使用できるようになりました。
		P2P Supernodes のブラックリストは、利用時に制限があるため削除しました。
		修正された問題
		VPN のイベントでソース IP を持たない場合エラーが発生し、ADS が動作しなくなることがある問題を修正しました。
Ver.11.01.05	2021/03/10	新着情報
		イベントフローの解析を改善するために、「イベント詳細」の「イベント証跡」に「フロー受信時間」が追加されました。「フロー受信時間」は、Configuration Center＞ FMC 設定＞ フローのデータベースフィールド＞ コレクタが受信したタイムスタンプフロー、のチェックが有効になっている場合のみ表示されます。
		フローペアリングのタイムアウトを 60 秒から 75 秒に変更し、反対方向のフローの遅延による誤検出を減らしました。
		修正された問題
		サーバからの応答がない場合、クライアントが「DHCPANOMALY: FakeServer」のサブメソッドから DHCP サーバに通信しようとする際の検出を除外しました。
		“App タグ”列が空欄の場合、「イベント証跡」に表示されないように修正されました。
Ver.11.01.04	2021/02/25	修正された問題
		設定＞ 処理＞ パースペクティブ設定で、データフィードが正しくソートされるようになりました。
		高負荷のアプライアンス上で非常にまれに ADS の機能が停止してしまう問題を修正しました。
		イベント証跡の'Data feed IP'の項目名を'Flow source IP'に変更し、Monitoring Center の用語と一致するように修正しました。（※英語版のみの対応です。）
Ver.11.01.03	2021/02/15	新着情報
		様々なパフォーマンスの最適化により、「イベント詳細」と「イベント証跡」のダウンロード時間が短縮され、複数のイベントを分析する際のシステムの応答性が向上されました。
		イベント詳細とそれに対応するイベント証跡のダウンロード時間を短縮し、特にイベント証跡の中で期間が長くフロー量が多いイベントのダウンロード時間が短縮されました。
		イベント詳細で対応するタブを開いた後に、イベント証跡がダウンロードされるようになりました。
		イベント証跡 は、開始時刻ではなく受信時刻に従って Monitoring Center から最初の 1000 (変更可能なデフォルト値) のフローを取得できるようになりました。この修正により、フローの読み込みが非常に速くなりましたが、フローの数が制限値を超えた場合、開始時刻に応じて Monitoring Center でソートされたフローのリストと比較すると、遅延したフローがイベントの証跡として表示されなくなることがあります。
		修正された問題
		ICMPANOM メソッドの一部でセグメンテーションエラーが発生し、システムに高負荷がかかっていた問題を修正しました。
Ver.11.01.02	2021/1/21	新着情報
		フィルタの操作が大幅に高速化されました。
		脅威インテリジェンスのデータが拡張されたため、クォータの管理で ADS が要求するディスクの下限値が増加しました。
		修正された問題
		多数のイベントの処理中にフィルタが複数回編集された場合に、アプリケーションが数分間フリーズする問題が修正されました。
		誤検知除外の設定を設定ファイルから正しくインポートされるように修正しました。
Ver.11.01.01	2020/12/03	新着情報
		正しく一度に複数のフィルタに IP アドレスを追加できるようになりました。
		Flowmon OS 11.1.0 との互換性を追加しました。
		Flowmon OS 11.1 以降をご利用の場合、GUI 上で新しい Rest API ガイドを利用できるようになりました。
		チェコ語と日本語のユーザガイドを追加しました。
		修正された問題

ver.No	リリース日	変更箇所
		データフィードが設定ファイルから正しくインポートされるようになりました。
		クライアントとサーバのタイムゾーンが同じではない場合、解析ページにはサーバの設定時刻が表示されます。
		解析の優先度別イベントの各イベントの「IP をフィルタに追加」にて、事前に設定した情報が表示されない問題を修正しました。
		解析の優先度イベントが表示される前にグラフが表示されていた問題を修正しました。
		既知の問題点
		バージョン 11.1 で導入された変更は、チェコ語と日本語のユーザガイドに反映されていません。
Ver.11.01.00	2020/09/30	新着情報
		ストリーム処理において、プロキシ相関が再実装されました。詳細については、ユーザガイドの「データフィード」の章を参照してください。
		イベントの視覚化の Adobe Flash は、Javascript D3 ライブラリをベースにした新しいものに置き換えられました。
		誤検出エンジンが刷新されました。 イベントが複数の誤検知除外ルールに一致した場合に、誤検知除外ルールが適切に適用されるようになりました。
		ユーザは、指定されたターゲットで誤検知除外のタイムスタンプを定義することができなくなりました。
		使用統計情報が簡素化されました。
		プロファイル'live'の名前が'All Sources'に変更され、FMC の命名規則に対応するようになりました。
		プロファイルのグループ名がデータフィードの編集画面に表示されるようになりました。
		修正された問題
		文字 '&' が CSV エクスポートで正しく表示されるようになりました。
		データフィードの名前は、UI 内のすべての場所で適切に翻訳されるようになりました。
		syslog メッセージのフォーマットが CEF 標準に一致するように調整されました。
		既知の問題点
		日本語のユーザガイドはまだご利用できません。
Ver.11.00.11	2020/12/01	修正された問題
		SIP フローの処理中に SIP データフィードの再起動につながるバグを修正しました。
		フィルタを使用した誤検知除外の設定を設定ファイルから正しくインポートされるように修正しました。
		BROKENSEN メソッドが膨大な CPU を使用しデッドロックが発生する問題を修正しました。
		実行時に使用可能なマシン メモリが変更されたために、データ フィードが再初期化されない問題を修正しました。
Ver.11.00.10	2020/10/09	新着情報
		Flowmon のサブライセンスに対応しました。
		修正された問題
		Hyper-V プラットフォームでデータフィードが実行されない問題を修正しました。
		既知の問題点
		イベントが複数の誤検知除外ルールに該当した場合、一部の誤検知除外ルールが適用されない場合があります。 （Flowmon ADS 11.1 で修正されました）
Ver.11.00.09	2020/09/30	新着情報
		データベースが最大サイズに達した場合、バックエンドエンジンが適切に復旧し、処理停止を防ぐようになりました。
		日本語のユーザガイドを公開しました。
		修正された問題
		IP アドレスのコンテキストメニューから「IDS イベントの閲覧」が正しく開かない問題を修正しました。
		既知の問題点
		イベントが複数の誤検知除外ルールに該当した場合、一部の誤検知除外ルールが適用されない場合があります。 （Flowmon ADS 11.1 で修正予定）
Ver.11.00.08	2020/08/31	新着情報
		Flowmon ADS Standard ライセンスのデータフィードの最大数が 1 から 3 に増加しました。
		修正された問題
		50 チャネル以上割り当てられたデータフィードで BPATTERNS が処理されない問題を修正しました。
		Flowmon ADS 11 よりも前に生成されたイベントに対して、イベント証跡が適切に動作するようになりました。
		既知の問題点
		イベントが複数の誤検知除外ルールに該当した場合、一部の誤検知除外ルールが適用されない場合があります。 （Flowmon ADS 11.1 で修正予定）
		「データフィードの編集」画面の「FPS の上限値/下限値の設定」項目でフロー数は 0～200,000 の範囲であると説明されていますが、正しくは 0～100,000 です。
		日本語のユーザガイドはまだご利用できません。
Ver.11.00.07	2020/08/04	修正された問題

ver.No	リリース日	変更箇所
		Flowmon ADS ログのローテーションを妨げる問題を修正しました。（ディスク上のスペースを確保するために古いログを削除します。）
Ver.11.00.06β	2020/07/22	新着情報
		「タイムスタンプ」という用語は、実際の意味を反映するために「検出時間」という用語に置き換えられました。（英語版のみ）
		規格外のフロー期間を持つエクスポータからのフローは、処理をしない代わりに 300 秒に短縮して処理されるようになりました。
		以前のバージョンからの無効なカスタムパターン設定が処理されるとユーザに適切に通知されるようになりました。
		修正された問題
		11.0.5 にアップグレードした後、新しいパラメータの無効なデフォルト値によって生じた不正なタイムスタンプのレポートを修正しました。
		集約されたイベントおよび関連イベントをすべてのモーダルウィンドウから開くことができるようになりました。
		ICMP プロトコルに基づくメソッドのトラフィックの記録フィルタを修正しました。
		既知の問題点
		日本語のユーザガイドはまだご利用できません。
		その他：
		カスタムパターン設定で正規表現が許可されなくなりました。
		データフィード設定で「アクティブなプロキシ」オプションが有効になっている場合、v11 より古いバージョンの Flowmon ADS からのアップグレードができなくなりました。
Ver.11.00.05β	2020/07/08	修正された問題
		イベントターゲットの誤検知除外ルールが正しく評価されるようになりました。
		既存の Flowmon ADS レポートの Flowmon Dashboard and Reports への移行は、すべてのケースで機能するようになりました。
		Flowmon Dashboard and Reports の CSV エクスポートに関する問題を修正しました。
		VPN の使用を検出する VPN メソッドが機能するようになりました。
		フローチャートと集約ビューに、以前のバージョンの Flowmon ADS のデータが正しく表示されるようになりました。
		集約ビューをイベントターゲットから開くことができるようになりました。
		検出エンジンは、パケット数が 0 のフローを処理できるようになりました。
		イベント証跡に表示されるフローの時間範囲を修正しました。
		既知の問題点
		日本語のユーザガイドはまだご利用になれません。
		その他
		イベント処理のパフォーマンスが向上しました。
		メソッド検出の問題を回避するために、規格外のフロー期間（300 秒を超える）のフローは処理されない場合があります。
		データフィード設定で「アクティブなプロキシ」オプションが有効になっている場合、v11 より古いバージョンの Flowmon ADS からのアップグレードができなくなりました。
		イベントあたりの最大ターゲットは 1000 に制限されています。
Ver.11.00.04β	2020/06/03	新機能
		新しいストリーム処理
		トラフィックの処理性能（1 秒あたりのフロー）が全体的に大幅に向上しました。
		振る舞い検知がより速くなりました。
		5 分毎のバッチ処理から Flow を受信するとリアルタイムに分析されるように変更されました。
		検出されたイベントは遅延なく通知されます。
		限界のない幅広い時間帯でのフローデータ分析により、検出の質が向上しました。
		振る舞いが継続して検出されている場合は、再度新しいイベントを作成するのではなく、既存のイベントを継続的に更新するように変更されました。
		正しいイベントソースを特定するために通信イニシエータの識別を改善しました。
		検出されたイベントの理解を深めるための新しい説明を追加しました。
		利用可能なすべての言語のイベント詳細テキストの翻訳を追加しました。
		メソッドにサブタイプを追加しました。これにより、1 つの検出方法から様々なイベントを識別できるようになりました。
		イベント属性の表示を追加しました。属性は、UI でローカライズされたイベント詳細を構築するために使用されます。
		すべての検出メソッドが再構築されました。
		TEAMVIEWER メソッドの機能を改善しました。
		アプリケーションの起動とデスクトップの共有を区別できるようになりました。
		DHCPANOM メソッドの機能を改善しました。
		DHCP サーバの MAC アドレスの変更を検出できるようになりました。
		DHCP サーバを過負荷にしているサーバを IP アドレスによって検出できるようになりました。

ver.No	リリース日	変更箇所
		DHCP サーバを過負荷にしているクライアントを MAC アドレスによって検出できるようになりました。
		BROKENSEN メソッドを再設計しました。
		旧式のメソッドである ICGUARD、LATENCY、DNSREVERSE、INSTMSG を削除しました。
		DNSANOMALY メソッドから旧式の大きな UDP パケットを検出する機能を削除しました。
		動作パターン(BPATTERNS)を処理するための新しい下位互換エンジンを導入しました。
		より長いドメインを持つブラックリストに対応しました。（31 文字から 63 文字に拡張）
		PDF/CSV レポートとダッシュボードウィジェットを Flowmon ADS モジュールから Flowmon Dashboard and Reports に移動しました。
		データフィードの設定からアクティブなプロキシ設定を削除しました。
		SuperFast 機能とフィルタブースタ機能を削除しました。
		パースペクティブの高度なフォーム設定から「部分文字列」が削除され、「サブメソッド」から選択する方式に替わりました。
		既知の問題
		日本語のユーザガイドはまだご利用になれません。
		Flowmon Dashboard and Reports
		レポートに以下のチャプターを使用して「CSV としてエクスポート」を実施しても CSV にエクスポートされません。 ● 優先度別のイベント概要 ● タイプ別のイベント概要 ● 優先度とイベント数による上位 10 件のイベントタイプ ● Security status
		イベントマトリックスのチャプターを使用したレポートで「CSV としてエクスポート」を実施した場合に、イベント数が正しくない／イベントの送信元フィールドが欠落していることがあります。
		チャプター「タイプ別イベント概要」で、表示されるメソッドが検出された数より少ない場合があります。
		Flowmon ADS のダッシュボードから「集約されたイベント」を選択しても、集計されたイベント画面が開かない場合があります。
		誤検知除外ルールが有効になるまでに数分程度時間が掛かることがあります。
		注意事項
		イベントの概念が新しくなったため、誤検知除外機能の動作が変更されました。
		新しい誤検知除外ルールを追加すると、すべてのアクティブなイベントに影響を与えます。
		つまり履歴から始まり、まだ更新されているイベントは、新しい誤検知除外によって削除される可能性があります。
		新しい誤検知除外ルールにより ADS からのアクティブなイベントが消失することは、想定動作であることに注意してください。
		DA(Distributed Architecture)モードで Flowmon ADS の旧バージョンからアップグレードする場合は、Flowmon サポート（support@flowmon.com）にお問い合わせ頂くことをお勧めします。
Ver.10.01.01	2020/06/24	修正された問題
		PDF スケジュール レポートがタイムアウトしないようになりました。
		「対話型のイベント視覚化」画面の [関連イベント]と[集約されたイベント]がオプションメニューから正常に動作するようになりました。
		長い名前のデータ フィードが存在する場合にも、デフォルト レポートの作成が正常に行えるようになりました。
		新規に開いたモーダルウィンドウが常にフォアグラウンドに表示されるようになりました。
		Syslog メッセージに出力されるイベントからは IP アドレスのルーティングプレフィックスを表示しなくなりました。
Ver.10.01.00β	2020/04/21	修正された問題
		FlowmonOS バージョン 11 に対応しました。
Ver.10.00.06	2020/06/23	修正された問題
		非常にまれなケースで電子メールレポートを送信できない問題を修正しました。
		イベント属性のオーバーフローが原因でバッチ処理が失敗する問題を修正しました。
		CSV レポートで、チャプタの構成で指定されたすべてのフィルタが考慮されるようになりました。
		イベント証跡画面でフィルタに指定した整数値が適切に機能するようになりました。
		イベント画面の[簡易リスト]、[ホスト別]の検索結果でソースとターゲットを選択時にオプションメニューが表示されるようになりました。
Ver.10.00.05	2020/03/23	Syslog メッセージに含まれる詳細メッセージ部の区切り文字をカンマ区切りからセミコロン区切りに変更しました。
		修正された問題
		Syslog メッセージの重要度を表す数値がユーザガイドの記載と異なっていた問題を修正しました。 優先度：変更前 → 変更後 ---------- 重要 : 2 → 10 高 : 4 → 8 中 : 6 → 6（※変更なし） 低 : 8 → 4

ver.No	リリース日	変更箇所
		情報　：10　→　2
		「レポートのスケジューリング」においてカスタムインターバルの「終了」時間が「00:00」になっていた問題を「23:59」になるように修正しました。
		イベントマトリックスのチャプターを「レポートの作成」で CSV にエクスポートした際、正しい日付でイベントが表示されない問題を修正しました。
		英語表示以外の UI においてデフォルトレポートが作成できない問題を修正しました。
		チャネルを仮想データフィードとして使用する設定をした際、設定画面とダッシュボードでの表記が異なる問題を修正しました。
Ver.10.00.04	2020/02/03	データベースサイズの大きいアプライアンスにおけるダッシュボードの読み込み速度が改善されました。
		修正された問題
		IP アドレスのメニュー項目[一般情報]に誤ったブラックリスト名が表示される問題を修正しました。
		仮想データフィードからのイベントがパースペクティブに正しく割り当てられない問題を修正しました。
		仮想データフィードが有効な場合において、Syslog メッセージが適切に送信されない問題を修正しました。
		[説明]が記載されていないカスタムブラックリストをアップロードできない問題を修正しました。
		プラグインの再起動後にカスタムブラックリストが正しく機能しない問題を修正しました。
		イベント処理の失敗を引き起こす可能性のあるイベント解析の問題を修正しました。
		既知の不具合
		[デフォルトレポートの作成]ボタンは日本語では正常に動作しません。
		制限事項
		Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、Flowmon OS をバージョン 10.3.2 以上にアップグレードしてください。
		Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。
Ver.10.00.03	2020/01/06	[HIGHTRANSF]メソッドのしきい値の最大値を増加しました（1GB から 1TB）。
		ユーザガイドに小規模な改善を実施しました。
		修正された問題
		仮想データフィードのイベントが適切に表示されない問題を修正しました。
		Flowmon ADS 10.0 にアップグレードする前に Flowmon IDS Collector がインストールされたアプライアンスで、IDS イベントブラウザが動作するようになりました。
		ユーザガイドの日本語版の全文検索が正しく機能するようになりました。
		Flowmon OS のローカルディスクのカスタムブラックリストは、Windows の行末記号（CRLF）を使用して CSV でインポートできるようになりました。
		欠落していた翻訳を追加しました。
		構成の変更後にページが自動で更新されるようになりました。
		制限事項
		Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、Flowmon OS を少なくともバージョン 10.3.2 にアップグレードしてください。
		Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。
Ver.10.00.02β	2019/12/04	日本語のユーザガイドが利用可能になりました。
		ダッシュボードに送信元 IP アドレスの国旗とドメイン名が表示されるようになりました。
		修正された問題
		ダッシュボードとイベント画面で正しいタイムゾーン（サーバー側）が使用されるようになりました。
		[IP の一般情報]が正しく機能するようになりました。
		ユーザガイドのチェコ語版での検索が、すべての場合に機能するようになりました。
		既知のバグ
		日本語版のユーザガイドの全文検索のインデックスに一部の単語が欠落していますが、次のバージョンで修正される予定です。
		制限事項
		Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、少なくとも Flowmon OS を ver.10.3.2 にアップグレードしてください。
		Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。
Ver.10.00.01β	2019/11/18	チェコ語のユーザガイドが利用可能になりました。
		PDF 形式で完全なユーザガイドをダウンロードできるようになりました。
		FTR トラフィックレコードの起動に失敗した際のエラーメッセージを改善しました。
		修正された問題

ver.No	リリース日	変更箇所
		ダッシュボードからのドリルダウン調査のイベント数の概要が正しく表示されない問題を改善しました。
		すべての Flowmon ADS 9.5 バージョンからのアップグレードが可能になりました。
		PDF フォーマットでスケジュールされたレポートが正しく生成されない問題を修正しました。
		ブラックリストの更新時間が正しく表示されない問題を修正しました。
		[ADS 管理者]ロールを持つユーザがログページを表示できるようになりました。
		既知のバグ
		チェコ語版のユーザガイドの検索が正しく機能しない場合があります。
		制限事項
		ユーザガイドは英語版とチェコ語版でのみ利用可能です。
		Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、少なくとも Flowmon OS を ver.10.3.2 にアップグレードしてください。
		Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。
Ver.10.00.00β	2019/10/31	ユーザインターフェイスが分析に重点を置いて完全に再設計されました。また、簡単な微調整を実施しました。
		新しいフィルタ管理機能の追加、独自の評価フィードの実装、利用できる外部サービスを拡張しました。
		Syslog メッセージ機能がデータフィードとパースペクティブインジケータによって拡張されました。
		IDS コレクタを搭載しました。
		ユーザガイドを HTML で入手できるようになりました。Flowmon ADS ユーザインターフェイスからアクセス可能で、全文検索をサポートしています。
		制限事項
		ユーザガイドは英語版のみで利用可能です。
		Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能が制限される場合があります（Flowmon OS バージョン 10.3.2 で対処されます）。
		Flowmon ダッシュボードのレポート機能において、Flowmon ADS が制限される場合があります（Flowmon OS のバグ修正で処理されます）。
		既知のバグ
		ダッシュボードからのドリルダウン調査のイベント数の概要が正しく表示されない場合があります。
Ver.9.05.11	2019/10/21	Syslog および SNMP 経由のイベントレポートのパフォーマンスが最適化されました。
		修正された問題
		SCANS メソッドのフローが欠落する問題を修正しました。
Ver.9.05.09	2019/09/23	修正された問題
		多数のイベント処理に対応するために、誤検知除外機能に使用するカウンタのサイズを増やしました。
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

ver.No	リリース日	変更箇所
		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.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。

ver.No	リリース日	変更箇所
		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.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

ver.No	リリース日	変更箇所
		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.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)