WatchGuard® System Manager　Firebox X Core & Firebox III 対象

WSM v7.5 (Build 2063) リリースノート

v7.5 の新機能と強化点について

「WSM v7.5」は、Firebox III 及び Firebox X Core アプライアンスをサポートする最新の WFS ソフトウェアです。

WSMv7.5 の新機能は次の通りです:

- IKE Phase 2 での AES-CBC 128/192/256 ビット暗号化をサポートします。
- 「GAV for Email」サービスをご利用のユーザーに、動的 GAV エンジンのアップデートを提供します。

WSMv7.5 の強化点は次の通りです（先にリリースしたホットフィックスの内容も含む）：

- 改正された米国/カナダの夏時間をサポートするようになりました。
- ゲートウェイ・ウィルス対策エンジンを「Clam 0.88.7」にアップデート。主なバグ修正や「Clam 0.88」バージョンで報告された脆弱性を修正しました。
- 最新のセキュリティ脅威に対し、効果的に措置を講じるため SMTP プロキシーの「拒否する添付ファイルのタイプ」というディフォルト・リストを新しいコンフィギュレーションにアップデートします。
- SMTP プロキシー設定に RFC822 や RFC2231 特定のコントロールを含む「RFC Compliance（RFC 準拠）」という新しいタブを追加しました。
- モバイル・ユーザーVPN と PPTP ユーザー間の切断を強制するメニュー・オプションを管理者に提供。【FSM】→【Front Panel（フロント・パネル）】、又は【FSM】→【Authentication List（認証リスト）】に行き、リモート・ユーザー・トンネルを選択し、右クリックでメニューを引き出します。
- IPSEC トンネル設定において、IP データグラムでサービス(TOS)ビットのタイプをセットしたり、クリアにしたりするオプションを提供します。
- ディフォルト・パケット処理のダイアログボックスで、ユーザーが ICMP レートの制限を特定できるようにする新しいグラフィック・ユーザー・インターフェイスのオプションを追加しました。
- Firebox X Core の FB X500 や X700 におけるトラフィック・バンド幅が、より良いパフォーマンスを提供できるように改善しました。
- Firebox X Core ユーザーを対象とした「SpamScreen」「GAV」「WebBlocker」などのサービス・サブスクリプションが無効になった状況が変わりました。

注意： このソフトウェアは WSM 8.X や 9.0 ではご利用頂けませんのでご注意下さい。「WSM v7.5」は、WSM 7.X のみを対象としています。WFS アップデートのサポートは、WSM 9.0 リリースにあります。

WSM7.4.1 対象のWebBlockerサーバーを既にインストールしている場合は、新しいバージョンのWSM7.5 は必要ありません。

テクニカル・サポート

技術サポートをご利用のお客様は、弊社技術サポートまでお電話、又はウェブサイト <http://www.watchguard.com/support>よりお問い合わせ下さい。その際は、ご登録済みのLiveSecurityキー番号、シリアル番号、又はパートナーIDの確認をさせて頂きますので、ご了承下さい。

	電話番号
米国のお客様	877-232-3531
日本のお客様	005-31-11-4950
弊社認定の販売代理店	005-31-11-4950

インストールとアップグレードについて

WSM ソフトウェアをインストールする前に、このリリースノートの「既知の問題」欄に目を通して下さい。

WSM v7.5 管理ソフトウェアをインストールするには：

1. 使用しているコンフィギュレーション・ファイルのバックアップを取ります。
2. アプリケーションを全て閉じます。
3. ダウンロードしたアプリケーションを開始し、画面に表示される手順に従って下さい。
4. WebBlocker サービスを使用している場合は、WSM 7.5 ソフトウェア用に WebBlocker を別にインストールする必要がある場合もあります。その場合は、この欄の最後にある手順を参照して下さい。

Firebox III 及び Firebox X を WFS v7.5 にアップグレードするには：

1. 使用している Firebox のコンフィギュレーションのバックアップを取ります。
2. WSM v.7.5 ソフトウェアが管理ステーションにインストールされていない場合は、前述のソフトウェア・インストール手順を参照して下さい。
3. WFS Policy Manager を使い、Firebox III 又は Firebox X のコンフィギュレーション・ファイルを開きます。
4. 「File（ファイル）」→「Save（保存）」→「To Firebox（Firebox に）」まで行きます。Firebox のドロップダウン・リストを使って Firebox を選択します。コンフィギュレーション・パスフレーズを入力し「OK」をクリックします。コンフィギュレーション・ファイルがローカルのハードディスクに保存され、次に Firebox のフラッシュ・ディスクの主要エリアに保存されます。

注意：SpamScreen v7.2.1 又はそれ以前のバージョンを実行している Firebox III をアップグレードする場合は、Policy Manager にある既存の SpamScreen ライセンス・キーを再入力して下さい。これを怠ると、SpamScreen が正常機能しません。

WSM7.5 ソフトウェア対象の WebBlocker サーバーをインストールするには：

1. WebBlocker サービスを停止します。
2. ダウンロードしたアプリケーション・ファイル(WSM75_wbserver.exe)を開始し、画面の手順に従います。

注意：WebBlocker サーバーのインストールが完了したら、再び WebBlocker データベースをフル・ダウンロードして下さい。

修正点

パケット・フィルター/ NAT

- **ダブル NAT 強化点サポート-**
  トラステッド・ネットワーク上にいるホストが、Firebox の外部インターフェイスのパブリック IP アドレスを使ってオプショナル・ネットワークのサーバーにアクセスすることができるようになりました。そうする場合、管理者は、送信先の「External_IP」→「Optional_Server_IP」として静的（スタティック）NAT エントリーを追加しなければなりません。この場合、2 つの制限があるので注意して下さい。
  - Firebox の外部 IP やネットワーク・アドレスが、動的 NAT 設定で特定されたソース・ネットワークと対立のないようにして下さい。
  - 2 つめの制限については例を用いて説明します。例えば、トラステッド・ネットワーク上のホストが、Firebox の外部 IP アドレスを使ってオプショナル・ネットワークにあるサーバーに接続したいとします。上述したように、その場合は送信用の静的 NAT エントリーを作成しなければなりません。しかし、「Trusted（トラステッド）→ External（外部）」というタイプの動的 NAT エントリーが既にある場合は、「Trusted（トラステッド）→ External IP（外部 IP）」というタイプの動的 NAT の例外を追加し、ダブル NAT が正常に機能するようにする場合もあります。

    似たように、オプショナル・ネットワークからトラステッド・ネットワークへの接続状況に適した動的 NAT 例外を設定する必要がある場合もあります。

- TCP NAT接続の高数値がFireboxがロックアップしてしまう問題の原因となっていましたが、これを修正しました。128/256 MBにおいてのみ、この修正は適用されています。[14770]
- HPUXマシーン間の‘remsh’接続を正確にFireboxが許可するようになりました。[14770]

WebBlocker

- WebBlocker のカスタム拒否メッセージに、ある無効の文字列が正しく解析されることで Policy Manager が Firebox に接続できなかった問題を修正しました。[14767]
- URL ベースの WebBlocker にある例外ダイアログ下の URL 欄が、正規のドメイン名のみを許可するようになりました。サブフォルダーで例外を規定するには、ディレクトリー・パターンを使わなければなりません。[14824]

SMTP

- SMTP プロキシーがファイル名のない添付ファイルを GAV スキャン・エンジンに送信するようになりました。[14332]
- 本文に別の電子メールを含んでいるメールを SMTP プロキシーが正しく処理するようになりました。[17360]
- スタンダードではない MIME エンコードを使った添付ファイルをブロックする、新しいグラフィック・ユーザー・インターフェイス（GUI）を追加しました。[13988]
- SMTP プロキシー設定が RFC2231 構文解析を有効/無効にすることができる、新しいオプションを提供します。[16864]
- SMTP プロキシーのコンフィギュレーション・ページで、ユーザーが SMTP グリーティング（Ready）メッセージを設定することができるようになりました。[14805]
- Firebox からのNAT送信用FINパケットが失敗する原因であったSMTPプロキシー問題を修正しました。[14766]

- 状況に該当するRFC準拠に従うよう、SMTPプロキシーが正しくMIMEバウンドリー文字列を解析するようになりました。これは余分な改行スペースを作っていましたが、この問題は解消されました。[16140]

管理（マネージメント）

- Firebox がトラフィック・ロードの多い状況下でコンフィギュレーションを保存しようとする際に、必要のない再起動ステップを取り除くため、実行中のプロセスを数回に渡り再起動しようとするようになりました。[15920]
- サービスがスタートした後でも WSEP ログ・サーバーのユーザー・インターフェイスが、消えないようになりました。[15121]
- 「Policy Manager（ポリシー・マネージャー）」が 8 文字列以下の DVCP クライアントの共有シークレットを許可しないようになりました。[6524]
- 「VPN Manager（VPN マネージャー）で VPN トンネルを作成した場合、「ANY」サービスの自動作成を無効にすることが可能になりました。[14811]

モバイル・ユーザーVPN

- 30 日を過ぎるとブロックされていた MUVPN クライアントの認証問題を修正しました。[18760]
- Fireboxは証明書が無効になったMUVPNユーザーが接続できないようにします。[14804]

ブランチ・オフィス VPN

- NATトラバーサルの使用時に見られたCisco PixとのIPSEC相互運用性問題を修正しました。[14804]

ポリシーとプロキシー

- HTTPプロキシーが内容を変更せず正確に応答をサーバーに返すようになりました。[14772]
- ポリシーは無効でも HTTP プロキシーが設定されているなど、コンフィギュレーションにおける小さな変更においては Firebox を再起動させる必要がなくなりました。[14942]
- 特定の状況で構築されたテスト環境において、HTTPプロキシーがHTTPリクエストに失敗せずにキャッシュするようになりました。（‘¥r¥n’で停止）[14773]

ロギング/ レポート

- Firefox で「Historical Reports（履歴のレポート）」を表示することが可能になりました。[18226]
- 管理者が「Historical Reports（履歴レポート）」を通して、サブフォルダーで帰納的にレポートを確認することができるようになりました。そうするには「Historical Reports（履歴レポート）」→「Report Properties（レポート・プロパティ）」→「Setup（セットアップ）」のボックスをチェックして下さい。[14983]
- IPSEC の「Routing Policy（ルーティング・ポリシー）」を有効にする新しいユーザー・インターフェイスを追加しました。[14807]
- 送信用のブロードキャスト・パケットのロギングが、新しい設定用にはディフォルトで有効にされるようになりました。[14777]
- 「Roll Log（ロール・ログ）」機能がロールされたログ・ファイルで、常にバックアップ・スクリプトを実行するようになりました。[5686]

- 「Logging Scheduler（ロギング・スケジューラー）」機能が、新しい年に続く次回のログ・ロールの日付を正確に更新するようになりました。[16070]

その他

- Fireboxがノン・ゼロバイトで隙を埋めると、NICカードが60バイト以下のイーサーネット・パケットの受理に失敗する問題を修正しました。[17290]
- 既存及び新設定に対し、ディフォルト・パケット処理がステートフルICMPをディフォルトで有効にするようになりました。[15978]
- サービス・ベースの送信用静的NATのサポートを追加しました。[14806]

既知の問題

管理（マネージメント）

- ロードの多い状況下で、Fireboxにコンフィギュレーションを保存しようとするとエラーが表示されることがあります。その場合は、トラフィック・ロードが落ち着いてから再びコンフィギュレーションを保存してみて下さい。[19449]
- ログ・メッセージに見られるGAVイベントに関する情報は「Historical Reports（履歴のレポート）」で表示されないことがあります。[18440]
- HAクラスターにおいてプライマリーのFireboxにコンフィギュレーションの変更を保存した場合、スタンバイ用のFireboxに自動的に保存されません。[14743]

  回避策：
  プライマリーとスタンバイ用のFireboxは、同じサブネットでIPアドレスを設定することでコンフィギュレーションの変更を共用します。又、ハートビートをパスするように、プライマリーとスタンバイ用のFireboxはそれぞれクロスオーバー・ケーブルなどで、物理的にもお互いと繋がっていなければなりません。物理的に繋がっていない場合は、ハートビートに使っていない別のインターフェイスでスタンバイ用のIPアドレスを設定して下さい。

- 場合によって、すぐにFirebox Xのアップグレード・キーが適用されず、Firebox X LCDパネルに新しいFirebox Xモデル番号が表示されないことがあります。

  回避策：
  手作業でFirebox Xを再起動させ、モデル・アップグレードを完了させて下さい。

- Firebox Xに3-Port &ハイ・アベイラビリティを適用後、WSMのトラフィックを表示する3つのポートのトライアングル・ビューが、すぐに6ポート・ビューに変更されません。

  回避策：
  6ポートのトラフィック・ビューを更新するにはWSMを一旦閉じてから、再び開いて下さい。

- 同じ管理ステーションにある別のディレクトリーに、2つの異なるバージョンのWSMをインストールする場合、アンインストール時に問題が発生することがあります。2つのバージョンをインストールし、その内1つをアンインストールする場合は、残されたバージョンが正確に機能しなくなることがあります。それは、共有するレジストリー・キーが除去されたためです。2つめのバージョンもアンインストールすると、ファイルがうまく外されなかったことを示すエラーが表示されます。

  回避策：
  全てのバージョンのWSMをアンインストールして下さい。使用を希望するバージョンのみ、インストールします。

- SpamScreen では、スパムのルールを新しいバージョンにアップグレードし、元のオリジナル・ルールセットに戻ろうとすると SpamScreen が正確に機能しません。

  回避策：
  問題なく元のルールセットに戻すには、最初にインストールされていたWFS/WSMソフトウェアを再度インストールします。「untitled.cfg」は、ルールのアップデートがまだ実行されていないインストールに使われることがあります。

- Fireboxは、特定の場合においてPolicy Manager（ポリシー・マネージャー）が新しいコンフィギュレーション・ファイルを保存することができない場合に「Error connecting to Firebox」「unable to sync」「error parsing command output」「Unknown return value」「CAN'T SYNC (Success) [OK]」などのエラー・メッセージを送信することがあります。[15785]

  回避策：
  再度、Fireboxにコンフィギュレーションを保存して下さい。

認証

- SecurID Radiusでアクセス・リクエストとの相互運用性問題があります。[13636]

  回避策：

  Steel-Belted RADIUSがService-Type=8（認証のみ)のアクセス・リクエストを受けると、ディフォルトにより、アクセス受理の返答でいかなる属性も戻しません。この問題を修正するには「radius.ini」ファイルを編集し、次の値をコンフィギュレーションの欄に追加します（ファイルにある手順を参照）。

  AuthenticateOnly=0

  次にSteel-Belted RADIUS/RSA RADIUSを再スタートさせます。この値はディフォルト・アクションを無効にします。詳細についてはRSAの「a29647」を参照して下さい。

WebBlocker

- WebBlocker は、時によって WebBlocker データベース以外のウェブサイトに、ユーザーがアクセスできないようにすることがあります。これは、URL 内の特定のリンクが、ユーザーを分類されていないサイトにリダイレクトさせる場合に発生します。[13217]
- データベースを除去せずに、旧バージョンの WebBlocker をアンインストールする場合、新しいバージョンを別のハードディスクにインストールすると、WebBlocker はスタートに失敗することがあります。これは、データベースのない新しいディレクトリーをチェックしているために発生します。

  回避策：
  WebBlockerデータベースを再びダウンロードして下さい。

- Windows XP や Windows 2003 サーバーに WebBlocker をインストールすることが可能です。WebBlocker データベースを提供する Surf Control は、Windows XP や Windows 2003 サーバーを公式にサポートしていませんが、そうしたオペレーティング・システムでも普通に機能します。
- WebBlocker サーバーをインストールし、データベースをダウンロードしない場合、WebBlocker サーバー・サービスはスタートに失敗します。

  回避策：
  WebBlockerサーバーをインストールし、データベースをダウンロードしたら管理ステーションを再起動させて下さい。WebBlocker サーバー・サービスが開始します。

仮想プライベート・ネットワーク

- MD5 認証アルゴリズムが「Phase1」で使用されている場合、証明書ベースの手動 IPSec トンネルが構築されないことがあります。[19309]
- DVCPクライアントの「Unique Name or ID（ユニーク名又はID）」が、13 文字列以上に設定されている場合、リモート管理のSOHOが失敗します。[17213]
- トラステッド又はオプショナル・ネットワークから、同じFireboxの外部インターフェイスにPPTPトンネルを構築すると、トンネルはルートされたモードでは正常に機能しませんが、ドロップイン・モードでは正常に動きます。[16895]
- クライアント・コンピューターが MUVPN トンネル経由で SOHO に接続し、その SOHO が VPN 経由で全てのインターネット・トラフィックを Firebox に送信するように設定されていた場合、SOHO のプライベート・ネットワークに送信されるようになっていたトラフィックは全て Firebox に送信されます。

  回避策：
  SOHOからMUVPNトンネルをFireboxに動かし、MUVPNトンネルからSOHOのプライベート・ネットワークへのトラフィックを許可するように、サービスを設定して下さい。

- 「Advanced Mobile User VPN Configuration（アドバンス・モバイル・ユーザーVPN設定）」のダイアログボックスで「Allow MUVPN connects from all interfaces（全インターフェイスからのMUVPN接続を許可する）」というオプションを有効にした場合、Fireboxを再起動させるかFSMからのIPsecをリブートさせて下さい。Fireboxは、自動的に再起動しません。[17951]
- Fireboxの外部インターフェイスが静的PPPoEアドレスを使用し、Basic DVCPからVPN Managerにアップグレードした場合、エラーが発生します。VPN Managerは、動的IPアドレスを使うFirebox X EdgeやFirebox SOHO製品に接続することができません。[17479]

  回避策：
  Firebox DVCPサーバーをアップグレードしてから、Firebox X Edge又はFirebox SOHOのコンフィギュレーション・ページを開きます。次に、コンフィギュレーションとステータス・パスフレーズをセットします。スモール・オフィスのディバイスをVPN Managerに設定します。詳細については、Firebox X Edge又はSOHOのユーザーガイドを参照して下さい。

- **仮想アダプター**
  MUVPNのクライアント・ポリシー(*.wgx ファイル)で仮想アダプター（VA）がオフになっていると、クライアントがトンネルを構築できない可能性があります。この問題が発生した場合、手作業で行うトンネル接続も機能しないかもしれません（MUVPNのアイコンを右クリックし、Connect（接続）をクリック）。[17260]

  回避策：
  システムトレイのMUVPNアイコンを右クリックし「Security Policy Editor（セキュリティ・ポリシー編集）」をクリックします。仮想アダプターのドロップダウン・リストで「Required（必要条件）」を選択します。

  1. 「File（ファイル）」→「Save（保存）」をクリックしてセキュリティ・ポリシーを保存します。次に「File（ファイル）」→「Exit（終了）」をクリックして MUVPN ポリシー編集を終了します。
  2. MUVPN のアイコンを右クリックし「Deactivate Security Policy（セキュリティ・ポリシーを無効にする）」を選択します。
  3. MUVPN のアイコンを右クリックし「Reload Security Policy（セキュリティ・ポリシーのリロード）」を選択します。
  4. MUVPN のアイコンを右クリックし「Activate Security Policy（セキュリティ・ポリシーを有効にする）」を選択します。

5. MUVPN のアイコンを右クリックし「Connect（接続する）」を選択します。

クライアントがトンネルを作成します。トンネルが機能したらセキュリティ・ポリシー編集に戻ります。「Disabled（無効）」を選択するには、仮想アダプターのドロップダウン・リストから「Disabled（無効）」を選択して下さい。ステップ 1 から 5 を繰り返します。

Gateway AntiVirus for E-mail

- ゲートウェイ・ウィルス対策が bin hex の添付ファイルをスキャンしません。[1533]
- GMT（グリニッジ標準時）以外にタイムゾーンを設定してもGAV/SpamScreen統計をGMTとして表示します。[1851]
- 外部とオプショナル・インターフェイス間でクロスオーバー・ケーブルが接続していて「Sys A - Loopbackモード」にあった場合、Fireboxは再起動します。[1873]
- 「Gateway AntiVirus for E-mail」のライセンス・キーを持っていない場合でも「Security Service（セキュリティ・サービス）」タブにある 2 つのリンクは機能しているように見えますが、実際には使用できません。[17893]
  - シグネチャー・リンクが機能し、コンフィギュレーション・パスフレーズのプロンプトが表示されます。
  - 「Clear Statistics」のリンクが入力を受け、コンフィギュレーション・パスフレーズのプロンプトが表示されます。
- GAV for E-mail 機能のヘルプは、最新の変更事項を正確に反映させないことがあります。[18856, 18996]
- 「Security Service（セキュリティ・サービス）」タブで「Clear Stats」をクリックする度にコンフィギュレーション・パスフレーズのプロンプトが表示されます。[17828]

その他

- **PPPoE アイドル・タイムアウト**
  アイドル接続のタイムアウトを使用していて、アイドル・タイムアウトが発生した場合、サーバー側の PPP 接続は、LCP Echo タイムアウトが過ぎるまで終了しない可能性があります。アイドル接続のタイムアウト機能を使用する場合は、LCP Echo タイムアウトをなるべく小さい値に設定しておきましょう。LCP Echo タイムアウトのディフォルト値の使用をお勧めします。

- **リンク・スピードとデュプレックスの謝ったログ・メッセージ**
  状況によって、リンク・スピードに関連するログ・メッセージが正確でないことがあります。この場合、ユニットは正確に機能しますがログに不正確な点があります。
  - Policy Manager の設定にかかわらず Firebox X NIC リンクが「100/10 Mbps full-duplex」で交渉する場合、「10Mbs half-duplex operation Link OK（10Mbs ハーフ・デュプレックス・オペレーション・リンク OK）」というメッセージが表示されます。
  - Firebox III が特定のスピードで機能するように設定されていても「Auto-negotiation enabled（自動交渉　有効）」というメッセージが表示されます。

- **データ・チャンネル　ログ・メッセージ**
  ICSA 準拠に追加されたログ・メッセージ「data channel created from（データ・チャンネルの作成先）」がログで頻繁に表示されていました。これはディフォルトでオフにしましたが、ログ・メッセージを表示することができます。そうするには、コンフィギュレーション・ファイルを編集し、次のコンフィギュレーション・プロパティを追加します。

    services.<your service>.proxies.ftp.incoming.log.data_channel: 1

services.<your service>.proxies.ftp.outgoing.log.data_channel: 1

- **Windows 2000/2003 認証**
  Policy Manager でWindows 2000/2003 のドメイン認証が有効になっている場合、認証アプレットが「authentication succeeded, but no access granted for user（認証には成功しましたがユーザーへのアクセス許可は与えられていません）」というメッセージを表示することがあります。これは、「Local（ローカル）」と「Global（グローバル）」グループを誤って選択していることを意味しています。[17911]

  回避策：
  ネイティブ・モードでインストールされているWindows 2000/2003 ドメイン・コントローラーでNTサーバー認証を使用するにはFAQを参照して下さい。
  <https://www.watchguard.com/support/advancedfaqs/auth_2k3natv.asp >