

# WatchGuard® Firebox® X Edge e-Series

## Firebox® X Edge e-Series v10.2.8 リリースノート

### 概要

ウォッチガードはこの度、Firebox® X Edge e-Series v10.2.8をリリース致しました。今回のリリースでは、ウォッチガード・ユーザの皆様より報告された問題をいくつか取り上げ、モバイルVPN with SSLやspamBlocker、認証などに関する問題のバグフィックスも用意しました。

詳細については「解決した問題」の欄を参照してください。

### このリリースでサポートしているアプライアス

Firebox® X Edge e-Series v10.2.8は、Firebox® X Edge e-Series製品シリーズでのみご利用頂けます。Edge、SOHO 6、SOHO 6 Wireless、S6、S6 Wireless、SOHO製品シリーズでは機能せずインストールすることができません。

Firebox® X Edge e-Seriesアプライアンスの購入をご検討されている場合は、アカウント・マネージャーまでお問合せください。

### ソフトウェア・ライセンスに関する重要事項

Firebox® X Edge e-Seriesでは、次のソフトウェア・ライセンス規定を実施しています：

- **登録** – LiveSecurityでFirebox X Edge e-Seriesを登録し、フィーチャー・キーを取得してください。有効なフィーチャー・キーがない場合、Edge経由でインターネットへ接続できるのはユーザ1人のみとなります。
- **LiveSecurity** – ソフトウェア・アップグレードをインストールするには、期限の切れていないLiveSecurityサブスクリプションが必要です。
- **WebBlocker** – WebBlockerのサブスクリプションが無効になっている場合、Edgeデバイスは初期設定に従い送信信用のHTTPトラフィックをすべて拒否するようになります。**WebBlocker > Settings** のページでこれを管理することができます。
- **spamBlocker** – spamBlockerのサブスクリプションが無効になった場合、spamBlockerはメール評価を停止し、すべてのメールを許可するようになります。

### インストール

Firebox® X Edge v10.2.8リリースをインストールするには、次の手順を参考にしてください。v10.2.8アプライアンス

ス・ソフトウェアは初期設定により英語でインストールするようになっていますが、**Edge Upgrade Wizard** を使えばEdgeに英語以外の言語パックを1つだけ追加することができます。また、Edgeのウェブ・インターフェイスを使えばAdministration(管理)ページでEdgeのユーザ・インターフェイスを別の言語に変更することも可能です。これについては、次のインストール手順を参考にしてください。

#### Windows XP(またはVista以外のWindows)を使用している場合

1. <http://www.watchguard.com/support> に行き、LiveSecurityユーザ名とパスワードを入力してログインします。次に **Software Downloads** ページへ行き、Edge\_10\_2\_8.exe ファイルをハードディスクに保存してください。
2. Edge v10.2.8にアップグレードする前にEdgeを再起動させておくことをおすすめします。
3. ステップ1でダウンロードしたEdge\_10\_2\_8.exeファイルをダブルクリックし、**Upgrade Wizard** のダイアログ・ボックスに従って手順を完了させてください。
4. 言語パックをインストールしたい場合は、Upgrade Wizardが出ている間に必要な言語を選択してください。Edgeユーザ・インターフェイスの言語を選択するには、Quick Setup Wizardで行うか、Edgeのウェブ・ユーザ・インターフェイスのAdministrationページで設定することができます。

#### Windows Vistaまたはその他のWindowsオペレーティング・システムを使用している場合

1. <http://www.watchguard.com/support> に行き、LiveSecurityユーザ名とパスワードを入力してログインします。次に **Software Downloads** ページへ行き、Edge\_10\_2\_8.zipファイルをハードディスクに保存してください。ファイルを解凍します。
2. Edge v10.2.8にアップグレードする前にEdgeを再起動させておくことをおすすめします。
3. Firebox® X EdgeのSystem Status(システム・ステータス)ページに接続してください。*System Statusに接続するには、使用しているブラウザのアドレス・バーにhttps:// と入力してから、Edgeのトラステッド・インターフェイスのIP アドレスを入力します。初期設定のURLはhttps://192.168.111.1です。*
4. System Statusページの**Update**をクリックします。
5. **Browse(ブラウズ)**をクリックしてください。yakfw.sysa-dlファイルを探し、選択したら**Open(開く)**をクリックします。
6. **Update(アップデート)**をクリックします。インストールを完了させるため、Firebox Edgeを再起動してください。
7. 言語パックをインストールするには、ステップ3からステップ5を繰り返しますが、ステップ4では次のファイルのいずれかを選択してください。

フランス語: lang-fr-10.2.8-arm.wgpkg-dl  
日本語: lang-ja-10.2.8-arm.wgpkg-dl  
簡体字中国語: lang-zh-10.2.8-arm.wgpkg-dl

8. Edgeが再起動したらAdministration(管理)ページに行き、ユーザ・インターフェイスの言語を変更します。

アップデート後、System Statusページには次のように新しいバージョン番号が表示されます:  
10.2.8 March 25 2009 Build 216948

#### 注意:

EdgeでEdge v8.0.x ソフトウェアを使用している場合は、規定のアップグレード・パスに従ってこのリリースをインストールしなければなりません。アップグレード・パスについては次の表を参考にしてください:

現在使用しているバージョン:	この順番でインストールすること:
Edge e-Series v8.0	Edge e-Series v8.0.1 → v8.0.3 → v8.6.2 → v10.2 → v10.2.8
Edge e-Series v8.0.3またはそれ以降のバージョン	Edge e-Series v8.6.2 → v10.2 → v10.2.8

Edgeにインストールしているソフトウェア・バージョンが定かでない場合は、Edgeの管理インターフェイスにログインし、System Statusページを参照してください。Edge e-Series v8.0.3ソフトウェアを入手するには、ウォッチガードのテクニカル・サポートまでお問合せください。

#### Windows用のMobile VPN with SSL v10.2.8クライアントをインストールするには

v10.2.8 Mobile VPN with SSLクライアントは、Edge v10.2.8アプライアンス・ソフトウェアに統合されています。Mobile VPN with SSLユーザには、Edgeからv10.2.8クライアントをダウンロードする方法と、リモート・ユーザがポート4100でFireboxにアクセスすることができない場合に、WatchGuardのウェブサイトからv10.2.8をダウンロードする方法があります。

旧バージョンのクライアント・ソフトウェアを実行しているSSLクライアント・コンピュータが、v10.2.8を使用しているEdgeに接続すると、SSLクライアントをバージョン1.14にアップグレードするように促されます。その場合は、**Yes** をクリックしてMobile VPNクライアントをv10.2.8にアップグレードしてください。ユーザがアップグレードをしない場合でも、Mobile VPN with SSLは機能しますがMobile VPN with SSLクライアントのv10.2.8を対象としたフィックスを受取ることはできません。

#### シングル・サインオン (SSO)ソフトウェアをインストールするには

旧バージョンのSSOインプリメンテーションからアップグレードする場合は、まず既存のSSOエージェントをアンインストールしなければなりません。v10.2.8リリースでは、新しいSSOクライアント・ソフトウェア・パッケージをインストールしてシングル・サインオン・インプリメンテーションの効率性と正確性を向上させることができます。この新しいSSOインプリメンテーションの詳細については、Fireboxのヘルプシステムを参照することをおすすめします。

#### v10.2.8 シングル・サインオン・エージェント・ソフトウェアをインストールするには

- <http://www.watchguard.com/support> に行き、LiveSecurity ユーザ名とパスワードを入力してログインします。Software Downloads ページへ行き、WatchGuard Single Sign-On Agent v10.2.8 をダウンロードしてください。WG-Authentication-Gateway.exe ファイルをハードディスクに保存します。
- Microsoft Windows 2003 や Windows XP、Windows Vista を使用している静的 IP アドレスのドメイン・コンピュータでファイルをインストールし、セットアップ・ウィザードを完了させます。この場合、ドメイン・コントローラにSSOエージェント・ソフトウェアをインストールすることをおすすめします。設定手順の詳細については、製品ヘルプシステムを参照してください。

### v10.2.8 シングル・サインオン・クライアント・ソフトウェアをインストールするには

- <http://www.watchguard.com/support> に行き、LiveSecurity ユーザ名とパスワードを入力してログインします。Software Downloads ページへ行き、WatchGuard Single Sign-On Client v10.2.8 をダウンロードしてください。WatchGuard-Authentication-Client.msi ファイルをハードディスクに保存します。
- SSO クライアント・インストーラーは MSI ファイルであるため、ユーザがドメインにログオンすると自動的にユーザのコンピュータにインストールされるようにすることも可能です。アクティブ・ディレクトリ・グループ・ポリシーを使い、ユーザがドメインにログオンすると自動的にソフトウェアをインストールするように設定することもできます。アクティブ・ディレクトリ・グループ・ポリシー・オブジェクトのソフトウェア・インストール詳細については、<http://www.microsoft.com> を参照してください。Microsoft Windows 2003、Windows XP、Windows Vista を実行しているコンピュータでのみ、クライアント・ソフトウェアをインストールすることができます。

### ローカル WebBlocker と Quarantine Server ソフトウェアをインストールするには

#### 注意:

過去にインストールしたバージョン 10.2 に上乗せする状態に限り、WebBlocker と Quarantine Server v10.2.3 をインストールすることができます。WebBlocker と Quarantine Server のアップデート版は v10.2.8 リリースには含まれていません。

1. <http://www.watchguard.com/support> に行き、LiveSecurity ユーザ名とパスワードを入力してログインします。次に **Software Downloads** ページへ行き、WGEdge10\_2\_3QWB.exe ファイルをハードディスクに保存してください。
2. WebBlocker と Quarantine Server v10.2 がインストールされているコンピュータで WGEdge10\_2\_3QWB.exe を実行してください。画面に表示されるインストール手順に従ってください。

## 解決した問題

### 一般

- WAN1 が PPPoE で IP アドレスを取る際、VPN トンネル経由で syslog を有効にしても VPN とコンフィギュレーション・アップデートがフェイルしないようになりました。[29965]
- 中国語のインストーラーが正常に機能するようになりました。[30997]

### NAT

- IPSec VPN トンネル経由で 1-to1 NAT を使いトラフィックをマスカレードすることが可能になりました。[20649][RFE20649]

## ワイヤレス

- ロードが重い状況下でワイヤレス・パフォーマンスに影響していたバグをいくつか修正しました。[34619]  
[34621] [31637]
- カーネル・クラッシュなしにワイヤレス接続でファイルをダウンロードできるようになりました。  
[31132]
- 数時間たった後でもワイヤレス Edge の CPU 使用量が 100%まで行かないようになりました。[34514]

## シングル・サインオン

- SSO エージェントが Windows イベント・メッセージ:EventType clr20r3 でクラッシュしないようになりました。[32775]
- ドメイン・フィルターの空き具合にかかわらず、SSO クライアントが正しいドメイン名を戻すようになりました。
- SSO クライアントとエージェントは、AD ドメイン名情報と NetBIOS ドメイン名情報のどちらも正確に処理できるようになりました。
- SSO クライアントとエージェントは、予期していなかった接続不良が 10 秒以内に発生した場合でも、正確に反応することができるようになりました。

## Mobile VPN with SSL

- Mobile VPN with SSL Mac OS X クライアントが、バウンド IP アドレスとゲートウェイに接続した IP アドレスを正確に表示できるようになりました。[34561]
- Mobile VPN with SSL Mac OS X クライアントが切断されたり終了した場合、検索ドメインと DNS 情報を除去するようになりました。[34564]
- Mobile VPN with SSL Mac OS X クライアントがどちらの WINS アドレスも表示するようになりました。  
[34560] [23635]
- Mobile VPN with SSL Mac OS X クライアントがデフォルトのログ・レベルを低く設定するようになりました。[34563]
- Windows Vista を実行しているコンピュータで Mobile VPN with SSL クライアント・ソフトウェアをインストールした場合、利用可能なネットワーク経路が正しく追加されるようになりました。[34558]

## 既知の問題

### ネットワーク設定

- WAN1 のワイヤレス・クライアント設定用タブは Edge e-Series 製品の全シリーズで表示されるようになっていました。Firebox X Edge e-Series ワイヤレスを使用していない場合は、このタブを使ってワイヤレス設定を変更しないでください。[23910]

## DHCP

- Edge DHCP サーバよりも DHCP リレイ・サーバ設定が優先されることはありません。[16796]
- DHCP のリース・タイムは常にグリニッジ標準時で報告されるようになっていました。[15431]
- レガシーMUVPN を IPsec クライアント・ソフトウェアと使用していて、DHCP 内部クライアント用に Mobile VPN の初期設定経路 (0.0.0.0/0) トンネルを作成する場合、クライアントがその IP アドレスを更新することはできません。また、DHCP リース時間が過ぎれば接続は終了します。この設定を使う場合は、DHCP のリース・タイムアウトを 8 時間以上に設定することをおすすめします。[15912]

## マルチ WAN/ポリシーベース・ルーティング

- WAN1 とリモートの IPsec ゲートウェイが同じサブネットにある場合、BOVPN トンネル・フェイルオーバーが正常に機能しない場合があります。[15935]
- Ping の間隔は設定されている間隔よりも 2 秒長いものとなっています。[15598]
- IPsec トンネルは常に WAN1 を使って交渉しようとします。Edge がマルチ WAN 用に設定されている場合、フェイルオーバーが発生しない限り全ての IPsec トンネルが WAN1 を使用します。[23704]
- マルチ WAN を使用する際、トラフィックが様々なポリシーを使えるよう外部インターフェイスを選択する場合に、ポリシーベースのルーティング機能を使うことができます。標準設定では外部インターフェイスが選択されており、ロード・バランシングが適用されるようになっていました。WAN1 または WAN2 を選択した場合、変更事項が反映されるように Edge を再起動させなければなりません。[23519]
- モデムへの WAN フェイルオーバーを行うように Edge が設定されている場合、IPsec トンネル接続は大量のトラフィックが送信されると正確に re-key することができません。[23560]

## 認証

- **Require user authentication (enable local user accounts)(ユーザの認証が必要: ローカル・ユーザ・アカウントを有効にする)**設定が選択されていない場合、インターネットへのアクセス権を得た匿名ユーザは、「アクティブ・セッション」として分類されませんが利用可能なユーザ・ライセンスを使用します。[26493]
- Windows Vista でシングル・サインオン・エージェントをインストールすると、現ユーザを列挙しようとするリモート・コンピュータが「アクセス拒否」のメッセージを受け取るようになっていました。[23590]
- Edge がシングル・サインオンで設定されていてユーザが Edge に認証しようとした場合、ユーザは

Edge からログオフすることができません。[23708]

### 回避方法

必要であれば Enable automatic session termination (セッション自動終了を有効にする) 設定で短期間の認証セッションを実施することも可能です。

- ・ シングル・サインオンを使うには Active Directory 認証を使用しなければなりません。LDAP 認証は、シングル・サインオンでサポートされていません。

### プロキシ

- ・ POP3 プロキシ設定の Deny unsafe URL patterns (安全ではない URL パターンを拒否する) は正確ではありません。Deny unsafe file name patterns (安全ではないファイル名パターンを拒否する) が正しい表示です。
- ・ BitTorrent の初期接続は TCP-UDP (送信) プロキシで問題なく阻止されますが、その後 BitTorrent が TCP ポート 80 を使って接続しようとした場合、HTTP プロキシや HTTP フィルター・ポリシーで許可されます。[27474]
- ・ 安全ではないファイル名パターンを使用する HTTP プロキシの機能では、ファイル名パターンはフル URI が使われ、リダイレクトもいくつか阻止する場合があります。[23758]

### 回避方法

安全ではないファイル・タイプを許可しコンテンツのタイプ別ブロック方法を使うか、問題が発生した際にデフォルト・リストから安全ではないファイル名パターンを除去する方法があります。

- ・ 送信プロキシを有効にすると、送信 SIP 接続が SIP プロキシに正確に送信されません。[23546, 全プラットフォーム]

### 回避方法

SIP 接続を直接処理できるように SIP プロキシを設定してください。

- ・ 外部 PBX を使って同じ Firebox の内側から 1 つのトラステッド・エンドポイントから別のトラステッド・エンドポイントを呼び出すことはできません。これは NAT「ヘアピンング」として知られています。[23872]
- ・ SMTP プロキシは Uuencode や BinHex の添付ファイルを完全に遮断しません。そのような添付ファイルのヘッダーの一部は拒否されたメッセージと共にメール本文に残ります。[22989]
- ・ VoIP デプロイメントは複雑であることが多く、様々なスタンダードおよび専用のプロトコルを使用します。ベーシック・ボイスやビデオ・トランスファー用の現プロキシでは、H.323 と SIP プロトコルを使用するスタンダードベースのトラフィックのみをサポートしています。VoIP の業界用語では、そうした新しいプロキシをより正確に表すため、アプリケーション・レイヤー・ゲートウェイ (ALG) と呼ばれています。データ・ファイル転送 (チャット、whiteboarding、ファックス送信など)、トラフィック・コントロール (QoS)、各

プロトコルでその制限が記されているものなど、ALG 機能やサービス、設定の中にはサポートされていない機能もあります。こうした理由から、プロダクション・デプロイメントに入る前に自己環境下で互換性と相互運用性をテストすることを強くおすすめします。

- H.323 プロキシはボイス・アンド・ビデオトラフィックで NAT トラバーサルをサポートします。H.323 ゲートキーパー (PBX ホスティング/トランキング) と T.120 マルチメディアは今回のリリースでサポートされていません。このため、ビデオ会議のようなポイント・ツー・ポイントでのプロキシ使用には制限があります。互換性や相互運用性を保証することはできませんが、ポイント・ツー・ポイントのオーディオやビデオ接続に関しては一般的なソフトウェア・クライアントやビデオ会議用のハードウェアで実証されています。

- トランスペアレント SIP プロキシは、ボイストラフィックやビデオトラフィックで NAT トラバーサルをサポートします。通常スタンドアロン、SIP レジストラ・プロキシの PBX レジストレーション機能を提供していませんが、SIP トラフィックに対しトランスペアレントなアプリケーション・レイヤー・ゲートウェイを提供しています。このトランスペアレント SIP プロキシは、PBX トラフィックのパススルーをサポートしますが、こうした接続をルートするには自分のレジストラ・プロキシ・サーバが必要となります。今回のリリースでは、Firebox (トランキングではなくホスト状態) の外部セグメントにある PBX でのみ、トランスペアレント SIP プロキシがテストされています。互換性や相互運用性を保証することはできませんが、ポイント・ツー・ポイントのオーディオやビデオ接続に関しては一般的なソフトウェア・クライアントで実証されています。また、ホステッド・オーディオの接続も様々な電話ハンドセットで実証済みです。

### WebBlocker

- WebBlocker 設定により HTTPS 接続が正しく阻止された場合、クライアントに拒否メッセージが送信されません。阻止された HTTPS 接続はログ・ファイルに記録されます。[22515]

### spamBlocker

- Quarantine Server (検疫サーバ) > Edit-Auto Remove Rule (自動ルール削除の編集) のダイアログ・ボックスで、Auto Remove messages with specific text in the subject (件名にある特定のテキストによりメッセージを自動削除) ルールへの変更事項が Quarantine Server で保存されません。ユーザ・インターフェイスではそのルールが削除されていると表示されますが、実際にはまだ有効となっています。Auto Remove messages with specific text in the subject のボックスのチェックを外すことがそのルールを無効にする唯一の方法です。[26796]
- Virus Outbreak Detection (VOD) を使った spamBlocker を有効にしている、Gateway AV でメールをスキャンしている場合に SMTP プロキシがスパム兼ウィルスのメールを検出すると、SMTP プロキシは VOD のメッセージ対応設定に従います。特に、VOD アクションが Strip で設定されていて添付ファイルがメッセージから除去され、それを回復することができない場合に見られます。VOD アクションが Lock で設定されている場合、添付ファイルは検疫されたメッセージ内でロックされた状態になります。  
[23709, 23711]
- Virus Outbreak Detection (VOD) がメールを検出したことに spamBlocker が気付くと、メールの添付ファイルは全て取り除かれるか検疫されます。メールが HTML 形式で送信されていた場合は、メール

本文もその対象になります。

- 感染したメールから複数の添付ファイルが(埋め込まれたメール本文など)検出され、spamBlocker が **Strip** アクションを実行するように設定されていた場合、添付ファイルで拒否されたメッセージと共に添付ファイルのメール・ヘッダーの一部が受信した添付ファイル内に残ります。ただし、ウイルスの中身は常に取り除かれるようになっています。[23550]
- Edge がプライマリの DNS サーバに到達できない場合、spamBlocker は機能しません。[18159]

### Gateway AV/IPS

- シグネチャ・アップデートのログ・メッセージはタイムゾーンを変更後、これまでの時間と日付情報を表示するようになっています。Edge を再起動させるまで、ログ・メッセージでは正しいタイムゾーンが使われません。[17754]

### ワイヤレス

- ワイヤレス・クライアント・ハードウェアやソフトウェアにおいては、クライアントがすでに接続したことがある場合、利用可能なワイヤレス・ネットワーク全てを表示しない場合もあります。別の Edge ワイヤレス・ネットワークに接続する必要がある場合は、ワイヤレス・ネットワーク・アダプターを無効にしてから再び有効にしなければならない場合があります。
- WAN1 インターフェイスがワイヤレス・クライアントとして設定されている場合、Traffic Control(トラフィック・コントロール)は正常に機能しません。[23757]
- Windows XP SP1 を使用しているワイヤレス・クライアントは、ワイヤレス認証に “WPA2 ONLY” を使うように設定している Edge に接続できない場合があります。[23808]
- Edge の前面にある WAP ライトは、Edge がワイヤレス・アクセス・ポイントとして設定されている場合や、外部 WAN1 インターフェイスがワイヤレス・クライアントとして設定されている場合に点灯します。  
[23121]
- Wireless Guest(ワイヤレス・ゲスト)アカウントを有効にしている Edge を再起動した場合、Edge DHCP サーバが 3 回停止する場合があります。DHCP サーバは Edge が再起動すると 2 分以内に正常に機能するようになります。[23792]
- XBOX 360 ワイヤレス・クライアントを使って Edge にワイヤレス接続を設立することはできません。[27481]
- 旧バージョンの Wireless Guest Services (ワイヤレス・ゲスト・サービス)(Edge v8.0 から Edge v8.5)を Edge で使用している場合は、Edge v10.2.8 にアップグレードした後 Guest Services を再設定しなければなりません。

### VPN

- IKE 再交渉が頻繁に行われるように設定されている場合、Edge は通常より多くのメモリを消費し Edge 管理の接続が遅くなる原因となります。初期設定の IPSec 設定を変更した場合は、トンネルが毎時間 2 回以上キーを交換しないようにしてください。[24221]
- WSM Centralized Management の環境下で v8.6.2 を入れている Edge は、キーが交換されてから1つのトラフィックもトンネルを通過していない場合、有効時間をベースに新しいキーを交換したトンネルが赤い感嘆符 (!) で表示されます。このトンネル経由でトラフィックが送信されると、赤い感嘆符は消え、トンネルは正常に機能するようになります。[22412]
- Cisco VPN Client を使用している場合、Edge 経由の Mobile VPN with IPSec の送信用接続が正常に機能しないことがあります。[19183]

### Mobile VPN with SSL

- Mobile VPN with SSL クライアントの初期接続後に Mobile VPN with SSL 設定で行った変更は、Windows Vista SP1 クライアントとの接続問題の原因になります。クライアントは正常に接続しているように見えますが、クライアントはフラッシュに失敗した ARP テーブルのログ・メッセージを送信します。[29621]

#### 回避方法

この問題を回避する方法は 2 つあります。

1. Vista PC の User Account Control (UAC)を無効にしてください。
  2. Program Files(プログラム・ファイル) > WatchGuard > WatchGuard Mobile VPN with SSL に行き、wgsslvpcn を右クリックしてください。次に **Run as Administrator(管理者として実行)** を選択します。
- Edge に SSL が接続していて管理者が Mobile VPN with SSL 設定を変更した場合、SSL クライアントは Edge から切断されません。各ユーザは手動で接続を切断してから、新しい SSL 設定ファイルを取り入れるために再接続してください。[23921]
  - Windows 2000 Professional を入れているコンピュータで Mobile VPN with SSL クライアントをインストールすることはできません。[23667]
  - Mobile VPN with SSL クライアントがトラステッド・ネットワークから Edge に接続することはできません。[22547]

#### 回避方法

オプション・ネットワークから Edge に接続できるように Mobile VPN with SSL クライアントを設定してください。

- Mobile VPN with SSL Mac OS X クライアントは、Firebox との接続が切断ではなく失われた場合に、その設定をチェックしません。VPN 接続を再び確立するには、接続を切断してから再接続する必要があります。[23109]

### SNMP

- SNMP v3 を使えるように Edge を設定する場合のパスワードの長さは 8 文字、またはそれ以上の長さにしなければ正常に機能しません。[23531]

### Traffic Control

- IPSec の Traffic Control は、大方見られる特定のルールではなく VPN-ANY ルールを使用します。[24206]

### ロギングとリアルタイム監視

- Edge System の Status ページを見ると、次のようなエラーがログ・ファイルで見られる場合があります。httpd doInclude:INCLUDE failed for "lang.inc" result code was -1. このログ・メッセージは情報提供をしているものなので無視して構いません。[27322]
- レガシー WatchGuard Security Event Processor Log Server (セキュリティ・イベント・プロセッサ、ログ・サーバ) に Edge がログ・メッセージを送信すると、ログ・メッセージは途中で途切れたかのように見えます。[27430]
- トラストド・ネットワークとオプション・ネットワーク間のトラフィックがイベント・ログ・ファイルで表示されません。[15611]
- Network (ネットワーク) > Traffic Control ページで Log traffic prioritization (ログ・トラフィックの優先順位) を有効にした場合、プロキシ・ポリシーによって生成されるログ・メッセージに優先順位付けが含まれません。[23164]

### 工場出荷時設定に Edge を設定しなおすには

- 工場出荷時設定に戻した場合、設定ファイルが削除されません。[15174]

### 回避方法

Edge を工場出荷時設定に戻す場合は、Firebox X Edge e-Series のリセット・ボタンを 45 秒間押し続けることで設定ファイルを消去してください。

### ユーザ・インターフェイス

- Quick Setup Wizard (クイック・セットアップ・ウィザード) を使用中にフィーチャー・キーを入力すると、2 回目のログインが促されます。[21994]
- 新しいユーザ・インターフェイスや新機能を見るには、v8.x から v10.x に Edge をアップデートした後、ブラウザのキャッシュメモリをクリアにしなければならない場合があります。[20457]
- Internet Explorer 7 や Mozilla Firefox 3 で Firebox X Edge e-Series を管理している場合、Certificate Security (証明書セキュリティ) 警告が表示されます。この警告が表示されるのは、Firebox X Edge がデフォルトで使う自己署名証明書にネットワークの正確な情報が入っていないためです。こうしたブラウザの旧バージョンでも似たような警告は表示されますが、新しいバージョンで見られる警告ではその語調が特

に強くなっています。インターネット・エクスプローラを使用している場合は、警告メッセージを無視して作業を続行して構いませんが、Firefox を使用している場合は、各クライアント・コンピュータで Firebox X Edge に証明書を例外として追加しなければなりません。[14434]

## ユーザガイド

Edge v10.2.8 リリースでのユーザガイド変更事項は、ヘルプシステム(英語) [www.watchguard.com/help/documentation](http://www.watchguard.com/help/documentation) で説明しています。今回のリリースでは Edge ユーザガイドのアップデート版はありません。

## テクニカル・サポート

技術に関する御質問はウォッチガードのテクニカル・サポートへお電話、またはウェブサイト <http://www.watchguard.com/support> よりお問合せください。テクニカル・サポートにお問合せの際は、ご登録されている製品のシリアル番号と LiveSecurity キー、またはパートナーID を予めご用意ください。

	電話番号
米国エンドユーザ	877.232.3531
海外のエンドユーザ	+1 206.613.0456
ウォッチガードの代理店	206.521.8375

## Edge v10.2.x で解決した問題

この欄では、参考までに 10.2.x バージョンまでのリリースノートで解決した問題をリストにしています。各リリースのインストール手順や技術情報、既知の問題については必要なバージョンのリリースノートをダウンロードしてください。

### Edge v10.2.1 で解決した問題

#### 一般

- ・ 設定がアップデートされた場合に Allowed MAC (許可した MAC) アドレスを Edge で保存できるようになりました。[27242]

- Advanced(アドバンス)タブの Mobile VPN with SSL 設定ページで UDP ポート 80 が選択されていても SSL VPN Protocol/Port (udp:80) conflicts with HTTP というエラー・メッセージが発生しないようになりました。[27702]
- SSL VPN と同じセカンダリ IP アドレスやポート/プロトコルを使用し、Edge が 1-to-1 NAT 用にも設定されていても Mobile VPN with SSL を有効にすることができるようになりました。[27863]

## プロキシ

- SMTP プロキシや POP3 プロキシ・ポリシーを通して BinHex 添付ファイルを許可できるようになりました。[27927]
- SMTP プロキシと POP3 プロキシが、base64-encoded メッセージからのエクストラ・パディング文字列の入った添付ファイルを遮断しないようになりました。[27445]

## spamBlocker

- spamBlocker の例外リストに 80 件までのエントリを追加できるようになりました。[27098]

## Edge v10.2.2 で解決した問題

### 一般

- Quick Setup Wizard のヘルプ・リンクが正しく機能するようになりました。[23489]
- 中国語、フランス語、日本語用の Edge\_10\_2\_2.exe インストーラーを使用した際に見られたエラー・メッセージの原因となっていた問題を解決しました。[28121]

### VPN

- Edge v10.2.2 や Fireware v10.2.2 での BOVPN 標準設定が同じになりました。[28389]

### Mobile VPN with SSL

- NAT を使用している Edge で Mobile VPN with SSL を使用することができるようになりました。[27844]

## Edge v10.2.3 で解決した問題

### 一般

- v8.6.2 またはそれ以前のバージョンからアップグレードした場合に、VPN-ANY ポリシーを作成できないようにしていたアップグレード問題を解決しました。[29321]

- Mobile VPN with IPsec で Dead Peer Detection を有効にすることができるようになりました。[23498]

### Mobile VPN with SSL

- Mobile VPN with SSL クライアントが Window Vista SP1 をサポートするようになりました。[27901]
- Mobile VPN with SSL クライアントとゲートウェイが中間者攻撃から保護するようになりました。IP アドレスが Firebox の外部インターフェイスに指定された場合、Mobile VPN with SSL ゲートウェイは自己署名による x.509 証明書を生成します。v10.2.3 クライアントの初回接続時にゲートウェイはこの証明書を提示しますが、証明書が自己署名であるため Mobile VPN with SSL の全ユーザが最初に Firebox に接続すると、不審な証明書に関する警告メッセージが表示されます。ユーザには、その証明書を信頼しローカルに保存するオプションが与えられます。その証明書を信頼できるものとして許可すると、証明書が変更され中間者攻撃の可能性が出た場合に Mobile VPN with SSL クライアントはユーザに対し警告することができます。[27304]

### 検疫サーバ

.HTML 形式やリッチテキスト形式で検疫サーバに送信されたメールが、検疫サーバから解放された後にプレーンテキスト形式で表示されないようになりました。[28058]

### SMTP プロキシ

▪ spamBlocker の例外にマッチしたメールを検疫するように spamBlocker を設定している場合、SMTP プロキシが 200 サクセス・メッセージを送信するようになりました。スパム、大量メール、不審メール、VOD として分類されたメールを検疫するように spamBlocker が設定されている場合も、200 サクセス・メッセージは送信されます。送信メールクライアントに 200 サクセス・メッセージを送り返すことで、検疫サーバでのメール重複を防げることが可能です。[29332] [29333]

### シングル・サインオン

▪ ドメイン名に見られる ASCII ではない文字が、Malformed “list” response from SSO Agent というログ・メッセージで認証を失敗させる原因にならないようになりました。[27198]

## Edge v10.2.4 で解決した問題

### 一般

- このリリースには v10.2.3 やそれ以前のバージョンを実行している Firebox X Edge に見られる認証バイパスの脆弱性を修正するフィックスが含まれています。この脆弱性の詳細については [www.watchguard.com/archive/broadcasts.asp](http://www.watchguard.com/archive/broadcasts.asp) を参照してください。
- 言語パックが正確にインストールされるようになりました。[29986]
- ポート 4100 での認証が SSLv2 をサポートしないようになり、Payment Card Industry (PCI) のスタンダ

ードに準拠するようになりました。[29794]

- PPPoE 認証リトライ・タイムアウトを設定できるようになりました。[29829]

## HTTPS プロキシ

- HTTPS プロキシのアイドル・タイムアウトがセッション・タイムアウトとして処理されないようになりました。[28706]

## マルチ WAN/ポリシーベース・ルーティング

- ポリシーベースのルーティングにマッチするトラフィックが、常に正確なポリシー・ルーティング・アクションに従うようになりました。[27601] [27602] [25791]
- マルチ WAN を使用している場合、WAN2(ETH3)経由で送信された送信パケットすべてが、初期のインターフェイス ETH1(トラステッド用)や ETH2(オプション用)から送信されたものとしてログ・ファイルに表示されないようになりました。[27519]

## シングル・サインオン

- シングル・サインオン・ソリューションは v10.2.4 リリースで改善されました。シングル・サインオン・クライアントは、ネットワークの各コンピュータにインストールできるようになり、認証している人物の正確性を向上させることができます。詳細情報については上記のクライアント・インストール手順を参照してください。

## Edge v10.2.5 で解決した問題

### 一般

- このリリースには v10.2.3 やそれ以前のバージョンを実行している Firebox X Edge に見られる認証バイパスの脆弱性を修正するフィックスが含まれています。この脆弱性の詳細については <https://www.watchguard.com/archive/showhtml.asp?pack=78373> を参照してください。
- 言語パックが正確にインストールされるようになりました。[29986]
- ポート 4100 での認証が SSLv2 をサポートしないようになり、Payment Card Industry (PCI) のスタンダードに準拠するようになりました。[29794]
- PPPoE 認証リトライ・タイムアウトを設定できるようになりました。[29829]

## HTTP プロキシ

- セキュリティ機能がどちらにおいても有効になっている場合、HTTP プロキシが IPS と Gateway AV のためのボディ・スキャンを実行しないようになりました。Gateway AV と IPS がどちらも有効になっている

場合、Gateway AV においてのみボディ・スキャンが実行されるので、スループットが改善されます。  
[28002]

### HTTPS プロキシ

- HTTPS プロキシのアイドル・タイムアウトがセッション・タイムアウトとして処理されないようになりました。  
[28706]

### BOVPN

- Edge ローカル・ネットワーク(例: リモート・ネットワーク 10.0.0.0/8、Edge ローカル・ネットワーク 10.0.2.0/24)とオーバーラップするリモート・ネットワークでブランチ・オフィス VPN が設定されている場合、トラステッド・インターフェイスへの管理アクセスを Edge が阻止しないようになりました。  
[28352] [27106]

### Mobile VPN with SSL

- Edge v10.2.4 にアップグレードした後に発生していた Mobile VPN with SSL クライアントがフェイルする問題を解決しました。  
[30951]
- Firebox Users ページで“Default”グループを編集した場合、**Allow remote access with Mobile VPN with SSL (Mobile VPN with SSL でリモートアクセスを許可する)**ボックスのチェックが表示されなくなりました。  
[23449]

### Multi-WAN/ポリシーベース・ルーティング

- ポリシーベースのルーティングにマッチするトラフィックが、常に正しいポリシー・ルーティング・アクションに従うようになりました。  
[27601] [27602] [25791]
- マルチ WAN を使用している場合、WAN2(ETH3)経由で送られた送信パケットすべてが、初期のインターフェイス ETH1(トラステッド用)や ETH2(オプション用)から送信されたものとしてログ・ファイルに表示されないようになりました。  
[27519]
- ポリシー・ベース・ルートと BOVPN トンネルが BOVPN トンネル経由でルートしないようにするトラフィック・マッチング問題を解決しました。  
[31015]

### シングル・サインオン

- シングル・サインオン・ソリューションは v10.2.5 で改善されました。v10.2.4 シングル・サインオン・クライアントは、ネットワークの各コンピュータにインストールできるようになり、認証している人物の正確性を向上させることができます。詳細情報については上記のクライアント・インストール手順を参照してください。

## Edge v10.2.6 で解決した問題

### 一般

- PPPoE の再認証時に ISP から最初の CHAP フェイル・メッセージを受信した後、Edge が認証リクエストを送信し続けなくなりました。[29564]
- フランス語、日本語、中国語の言語パックを使用すると Schedule Reboot(スケジュールの再起動)オプションを使用することができます。[29361]

## BOVPN

- 動的外部インターフェイスがあり、動的 DNS を使用している 2 台の Edge 間の BOVPN トンネルは、どちらか 1 台または両方で外部 IP アドレスが変更した後でも正確に交渉できるようになりました。[28100]
- H.323 を使用するアバイア電話機が BOVPN トンネル経由で H.323 トラフィックを送信しても、Edge がクラッシュしないようになりました。[24191]

## Mobile VPN with SSL

- Edge が認証中に Mobile VPN with SSL ユーザのパスワードを含むログ・メッセージを送信しないようになりました。[27572]
- Mobile VPN with SSL クライアントをスタートさせると、そのコンピュータの DNS クライアント・サービスが停止し、Mobile VPN with SSL クライアント設定で提供されている DNS サーバの IP アドレスをコンピュータが使うようにアップデートするため、再起動させます。[28120]

## NAT

- 他の受信用ポリシーと同じポートを使う受信用ポリシーで 1-to-1 NAT が適用された場合に正常に機能するようになりました。[31243]

## Edge v10.2.7 で解決した問題

### 一般

- 設定機能をより正確に説明するため、HTTP プロキシ設定の **Deny unsafe file name patterns** オプションが **Deny unsafe URL patterns** に書き換えられました。[23758]

### spamBlocker

- spamBlocker の例外制限が 150 件の例外までサポートするようになりました。[28385]

## Mobile VPN with SSL

- Windows SSL VPN クライアントを Windows XP でインストールする場合に、Runtime Error メッセージが表示されインストールに失敗することがなくなりました。[31932]
- コンピュータの節電モードが解除された後に Windows SSL VPN クライアントが正しく機能するように

なりました。[31523]

## 認証

- Active Directory グループ・メンバーシップをベースにした SSL VPN ユーザ認証を Edge が正確に実施するようになりました。[27363]