ファームウェアバージョン：	V12.00.13.05	
	DFL-260E	A1
	DFL-860E	A1
	DFL-1660	A1
	DFL-2560	A1
	DFL-2560G	A1/A2
	DFL-870	A1
発行日：	2019/9/13	

本リリースノートには、DFL シリーズのファームウェア更新に関する重要な情報が含まれています。ご使用の DFL シリーズに対応するリリースノートであることを確認してください。

DFL シリーズに関する詳細な情報が必要な場合は“ユーザマニュアル”を参照してください。

目次：

変更履歴とシステム要件：

ファームウェアバージョン	リリース日付	モデル	ハードウェアバージョン
V12.00.13.05	2019/9/13	DFL-260E	A1
		DFL-860E	A1
		DFL-1660	A1
		DFL-2560	A1
		DFL-2560G	A1、A2
		DFL-870	A1

アップグレードの手順に関して：

ファームウェアのアップグレード方法には下記の「SCP プロトコルを使用して CLI 経由でのアップグレードを行う方法」と「WEB GIU 経由でのアップグレードを行う方法」の 2 つがあります。

※V2.40.02 より古いファームウェアでは、アップグレード時にコンフィグレーションが正しく更新されないことがある問題が存在します。必ず、アップグレード前に現在のコンフィグを保存し、アップグレード後にリストアを行ってください。
この問題は R11.10.01.06 において修正されていますが、V2.40.02 より古いファームウェア（V2.40.01.08 を含む）からどのバージョンのファームウェアにアップグレードする場合においても、内在する問題となります。
該当バージョン以外のファームウェアバージョンにおきましても、念のためアップグレード前にコンフィグの保存を行うことを推奨します。

R11.10.01.06 以降のバージョンでは、日本語 GUI 言語ファイルが用意されていません。ログイン画面で English を選択してご使用ください。

WEB GUI 経由でのアップグレード方法

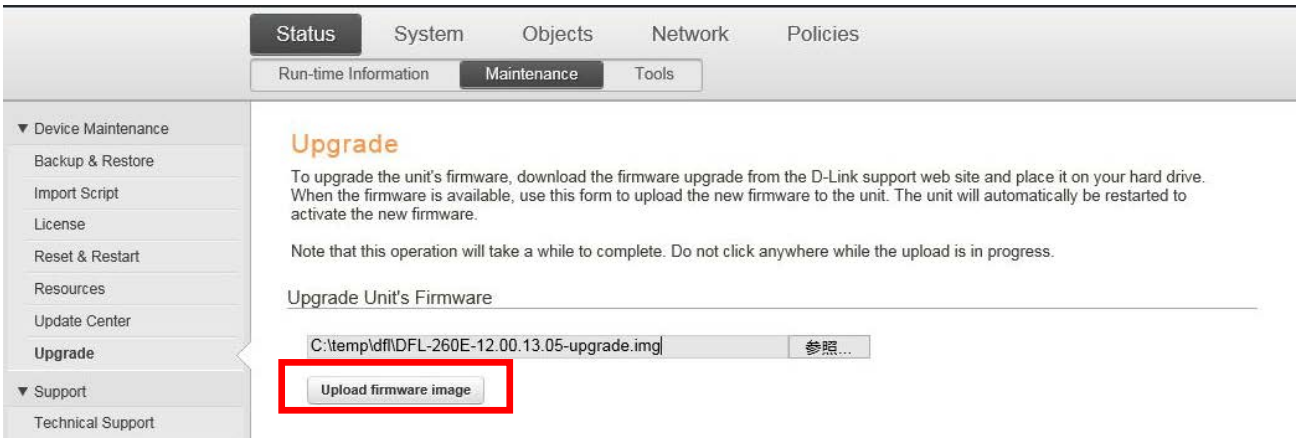
1. 本製品と設定用の PC を接続後、WEB ブラウザを立ち上げ、アドレスバーに WEB GUI の管理画面を表示します。デフォルトのシステム IP アドレスは 192.168.10.1 です。

2. WEB GUI のログイン画面が表示されたら、ユーザ名とパスワードを入力し、ログインしてください。デフォルトのユーザ名およびパスワードは「admin」です。

3. ログイン後、***Status > Maintenance > Upgrade*** の順にメニューをクリックします。

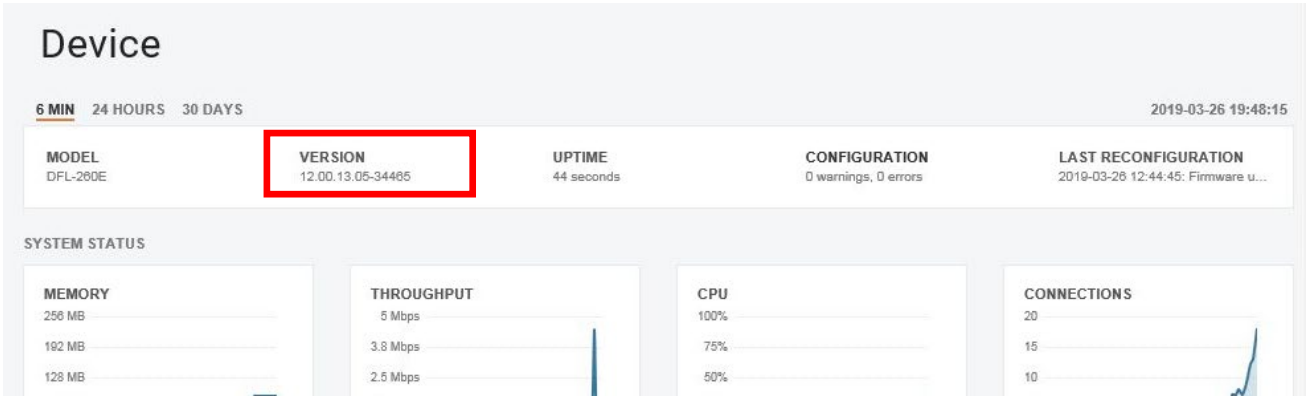
4. 「Upgrade Unit's Firmware」の「参照」ボタンをクリックします。

5. ローカルのハードディスク上に保存したファームウェアファイルを選択し、「Upload firmware image」をクリックします。



6. アップグレード後、DFL への接続が切断されるので、WEB GUI のアドレスに再接続（画面を更新）します。

7. システム概要画面の「Version」にて、最新バージョンになっていることを確認します。



注意：ファームウェアのアップデート中に、電源を切らないでください。アップデート中に電源を切ると、起動に失敗し、正常に起動できなくなることがあります。故障の原因となりますので、ご注意ください。

参考：SCP プロトコルを使用した CLI 経由でのアップグレード方法

SCP(Secure Copy)はファイル転送用のコミュニケーション・プロトコルとして広く使用されています。NetDefendOS と共に SCP クライアントを提供していませんが、ほぼ全てのワークステーションのプラットフォームに対応する無料の SCP クライアントを手に入れることができます。
SCP は CLI の処理を補足するもので、管理者のワークステーションと NetDefend ファイアウォール間のファイル転送を安全に行うことができます。NetDefendOS で使用する多様なファイルは SCP を使用してアップロード及びダウンロードを行なうことができます。

この機能の詳細の情報は、ユーザマニュアルの Secure Copy（SCP）に関して記載されている章をご確認下さい。

追加機能：

ファームウェアバージョン	追加機能
V12.00.13.05	1. Web UI のデザインとコンテンツを更新致しました。 2. Threat Prevention カテゴリを追加致しました。Botnet、Scanner、DoS Protection などの新機能のほか、アクセスルール、IDP ルール、Threshold Rule、ZoneDefense など既存の機能も含まれます。 3. IP Reputation 機能に対応致しました。（サブスクリプション機能）（DFL-870/1660/2560/2560G のみ） 4. DoS Protection に対応致しました。 5. スキャンアクティビティを行う送信元 IP から保護する Scanner Protection 機能に対応致しました。 6. Botnet Protection 機能に対応致しました。 7. HTTP/HTTPS 及び SSH 管理接続で IPv6 アドレスに対応致しました。 8. IPsec Status 画面で、より詳細な統計情報の表示に対応致しました。 9. “traceroute”コマンドで UDP/TCP プロトコルオプションに対応致しました。 10. HTTP の接続処理において、持続的な接続（Persistent Connection）に対応致しました。 11. 機密情報が含まれるコンフィグレーションファイルについて、非特定ファイルとしてダウンロードできるように対応致しました。 12. DHCP サーバのログにおいて、受信クライアントのホスト名を出力するように改善致しました。 13. スクリーンに対する“clear”コマンドを追加致しました。 14. ブラックリストの項目名「Time In List」を「Time to Live」に変更致しました。 15. SNMPv3 トラップに対応致しました。 16. ホワイトリスト/ブラックリストでリダイレクト機能に対応致しました。 17. ユーザ定義の Brute Force Protection 設定に対応致しました。 18. WEB コンテンツフィルタリングの再分類設定において、ローカルサブミットフォームではなく外部の再分類ページへのリンクに更新されました。デフォルトの 'ReclassifyURL'と'RestristedSiteNotice'バナーファイルは更新され、カスタムバナーは新しい分類リンクを表示します。 19. Reconfigure や HA アクティベーション後の AV/IDP シグネチャ更新の有効化/無効化設定に対応致しました。 20. システム起動後のパフォーマンスを改善致しました。 21. Email 添付ファイルにおける文字コードのエンコーディングを改善致しました。 22. LW-HTTP エンジンで HTTPS に対応致しました。既存の IP ポリシーの HTTPS 設定は、自動的に更新され、Web プロファイルで使用される際に新しい LW-HTTP エンジンを使用します。 23. サーバロードバランスにおいて、宛先サーバがダウンしていることを検出した場合、Reset（TCP RST/ICMP Port Unreachable）で応答するように対応致しました。 24. TLS 最小バージョンのデフォルト設定を TLS v1.2 に更新致しました。アップグレードされたコンフィグレーションには影響ありません。既存のコンフィグレーションは、最小 TLS バージョンを v1.2 に更新することを推奨致します。 25. Web Profile に HTTP Protocol Upgrade の有効・無効オプションを追加致しました。初期値では、Protocol Upgrade は許可されます。本機能は一般的に Web Socket などで使用されます。 26. ネイバデバイスのステータス画面を追加致しました。 27. DHCP ステータス画面でホスト名、リースアドレスの設定名を表示するように対応致しました。 28. Web ブラウザにおいて、スタティックなオブジェクト（Java スクリプトファイルや画像など）のキャッシュ保持時間を 4 時間から 30 日間に更新致しました。これにより、読み込み時間が改善されます。 29. パケットキャプチャで複数ポート、ポート範囲によるフィルタに対応致しました。 30. Time Server に対し、IPv6 及び FQDN オブジェクトの設定が可能になりました。

31. Intrusion Detection、Threshold Rule、IP ポリシー、トラフィックシェーピング、ポリシーベースルーティングルールで FQDN アドレスオブジェクトの設定に対応致しました。
32. DNS トラフィック種類のモニタと制御に対応致しました。
33. FQDN ポリシーでワイルドカードの使用に対応致しました。
34. Email Control 設定で Non-Managed 設定に対応致しました。
35. WebUI 上の Ping ツールで FQDN/DNS 名が利用できるようになりました。
36. Microsoft Azure VPN 接続用の定義済み IPsec プロファイルに対応致しました。
37. IKE 及び Config Mode で接続している VPN ユーザは、認証がローカルの場合にスタティック IP が割り当てられます。IPsec トンネルプロパティ「ConfigMode」と値「RADIUS」は、CLI で"UserAuth"という項目名に変更されています。（IP の割り当て方式はユーザの認証ルールに応じて異なるため）
38. IPsec トンネルで Proxy ARP インタフェースの設定に対応致しました。
39. スケジュール設定において、開始時刻から 24 時間までアクティブに設定することが可能になりました。これにより、日を跨いで連続した設定が可能となりました。
40. デフォルトの SSL 証明書で SHA-256 に対応致しました。鍵長 512/1024 は使用されません。HTTPS 管理証明書はアップグレード時に自動で置き換わりませんので、脆弱な暗号化（SHA-1 または鍵長 2048 よりも低い）を使用している場合は、新しい証明書を生成することをお奨めします。
41. CLI コマンド結果の「Last Shutdown」項目を「Last Event」という項目名に変更致しました。
42. NTP リクエストに対し、アクティブな HA ノードでは送信元としてシェアードアドレスを使用します。
43. ウイルス検出時に出力される Virus Found ログメッセージについて、すべてのログに Advisory リンクが含まれるように更新致しました。
44. コンフィグレーションファイル及びバックアップファイル生成時、ファイル名にデバイス名を含めるように更新致しました。
45. アンチウイルスのパフォーマンスを改善致しました。
46. IPsec プロファイルにおいて、VPN クライアントと VPN の LAN to LAN トンネルの設定を改善致しました。
47. IPsec トンネルのユーザ認証で IPv6 アドレスに対応致しました。
48. Radius 認証に使用するサーバについて IPv6 アドレスに対応致しました。
49. IKEv2 ローミングクライアントで事前共有鍵によるローカルユーザデータベースを使用した認証に対応致しました。EAP-MSCHAPv2 と EAP-MD5 を使用することができます。
50. IPsec トンネルでのリモート IKEv2 VPN ゲートウェイに対する認証において、EAP-MD5 と EAP-MSCHAPv2 に対応致しました。
51. IPsec クライアントで動作する場合、Config Mode を使用して IP アドレスとネットワークアドレスを割り当てることが可能になりました。
52. IPsec スイートで MOBIKE をサポート致しました。（IKEv2 Mobility and Multihoming Protocol: RFC4555）この機能により、クライアントのローカル IP アドレスが変更された場合や、path を含む NAT デバイスがクライアントの元の IP アドレスを変更した場合に、VPN 接続がオープンした状態を保持することができます。
53. サーバロードバランシング（SLB）機能の Distribution Method のオプションとして、リソース使用率に基づく方式を追加致しました。
54. Config Mode を使用したローミングクライアントに対する IPsec トンネル設定において、接続クライアント IP アドレスが、ユーザ認証に使用されたのと同じ RADIUS サーバにより割り当てることができるようになりました。RADIUS によって割り当てられた IP アドレスは IKEv1 と IKEv2 でサポートされています。
55. High Availability ステータスの SNMP による取得に対応致しました。追加された SNMP 値は、HA Role（マスター/スレーブ）、HA ステート（active/inactive）、最後の Role 変更からの経過時間を設定することができます。
56. サーバロードバランシングにおいて、新しく追加された'slb'コマンドと WEB サーバのステータス画面を使用して、SLB サーバをメンテナンスモードに移行することができます。
57. IPv6 有効化のグローバル設定は削除されました。インタフェースに対してのみ有効化することができます。

	58. Log、Event、Mail Alerting 機能を個別のセクションとしました。 59. SNMP について、置き換えられた接続数/秒のカウンタを追加致しました。許可された接続数の上限に達した場合、不正なトラフィックの可能性として示されます。 60. アプリケーションコントロールライブラリを更新致しました。 61. GeoIP データベースが更新されました。

CLI の変更点：

ファームウェアバージョン	変更点
V12.00.13.05	1. “connection”コマンドで extend 情報、データ量によるフィルタに対応致しました。 2. "memory"コマンドでサイズ、説明、割り当て数による出力ソートに対応致しました。 3. “traceroute”コマンドで UDP/TCP プロトコルオプションに対応致しました。

MIB の変更点：

ファームウェアバージョン	変更点
V12.00.13.05	1. DNS ALG カウンタを追加致しました。 2. Threat Prevention Blacklist カウンタを追加致しました。 3. High Availability Status オブジェクトを追加致しました。

※V11.10.01.06 以降では、管理インタフェースから MIB ファイルをダウンロードすることが可能です。
（***Status > Maintenance > Resources***）

修正した問題点：

ファームウェアバージョン	修正した問題点
V12.00.13.05	1. DNS サーバの設定を有効化/無効化した場合に該当エントリのキャッシュが更新されない問題を修正致しました。 2. IPsec 接続時、デバイスの OS 更新などで IKE 接続のプロポーザル数が増加した場合にネゴシエーションが失敗する問題を修正致しました。 3. L2TPv3 インタフェースが誤った MAC アドレスで応答する問題を修正致しました。 4. Reconfigure 実行時にパケットロスが発生する問題を修正致しました。（DFL-870 のみ） 5. Poll Offloading 機能を有効化している場合、システムがクラッシュすることがある問題を修正致しました。 6. Email のウイルススキャン実行時に CPU 負荷が高くなる問題を修正致しました。 7. デバイスやインタフェースのタイプにより、起動時に Gratuitous ARP が送信されない場合がある問題を修正致しました。 8. IDP またはアンチウイルス更新時に予期せぬ再起動が稀に発生することがある問題を修正致しました。 9. インタフェースが Transparent モードの場合、予期せぬ再起動が稀に発生することがある問題を修正致しました。 10. DHCP サーバ有効化時、稀に ARP テーブルが正しく更新されない事がある問題を修正致しました。 11. フラグメント化されたトラフィックを処理している際に、予期せぬ再起動が発生することがある問題を修正致しました。 12. キャラクタセット/言語が含まれない MIME のファイル名が正しく解析されない問題

	を修正致しました。 13. HTTP ALG で処理されたトラフィックを受信する際に、予期せぬ再起動が発生することがある問題を修正致しました。 14. TFTP ALG 経由の TFTP トラフィックを受信する際に、予期せぬ再起動が発生することがある問題を修正致しました。 15. HTTP ALG を使用し、ユーザが特定の Web サーバに接続した際に、稀に予期せぬ再起動が発生することがある問題を修正致しました。 16. 工場出荷時設定のコンフィグのアップグレードにおいて、Strong Password 設定が正しく処理されない問題を修正致しました。 17. 特定のコンフィグ設定において、IPsec ネゴシエーション時に予期せぬ再起動が発生することがある問題を修正致しました。 18. SMTP アンチウイルス設定において、感染ファイルが一部しかブロックされない問題を修正致しました。 19. IPsec トンネルの Auto Establish 機能において、リモートエンドポイントの応答がない場合に一度しか接続を試みない問題を修正致しました。 20. Time Sync サーバ構成で IP アドレスがルーティングテーブルを参照して到達不可の場合、他の IP アドレスが到達可能であっても同期が失敗する問題を修正致しました。 21. 受信 ESP パケットによってポートの変更が必要になった場合、ハードウェアアクセラレータによって IKEv1 SA のポート更新が失敗する問題を修正致しました。 22. IKE レスポンダとして動作する場合、クライアントに送信された Config Mode IP がクライアントの最初のトラフィックセレクタに一致するかどうか検証されない問題を修正致しました。 23. アクティブな SSL VPN ユーザが存在している場合、予期せぬ再起動が発生することがある問題を修正致しました。 24. 多数のトンネル接続がセットアップされた後に、IPsec EAP トンネルが動作を停止する問題を修正致しました。 25. VLAN インタフェースの詳細情報を表示する VLAN コマンドで、IPv6 アドレスの情報が含まれない問題を修正致しました。 26. スクリプト読み込み後、コンフィグレーションのエラーが読み取れない問題を修正致しました。 27. Transparent モードにおいて、パケットに元の送信元 MAC アドレスが保持されないことがある問題を修正致しました。 28. L2TP/PPTP インタフェースにおいて、RADIUS 認証を使用したルートに対するルートモニタリングが失敗した際に、稀に予期せぬ再起動が発生することがある問題を修正致しました。 29. 時刻フィールドが 0 で不正なタイムスタンプとなっている場合に、不正な SNMP 値「HOST-RESOURCES-MIB::hrSystemDate」が生成される問題を修正致しました。 30. OSPF インタフェースのルータプライオリティについて、不正な単位が表示される問題を修正致しました。 31. FQDN でエンドポイントに接続する際に、IPsec トンネルで古いライフタイムの IP アドレスが使用される問題を修正致しました。本バージョンでは、最新の IP アドレスが使用されるように修正されています。 32. 設定されたルーティングテーブルがメインルーティングテーブルと異なる場合、指定 IP アドレスへの接続試行時、SNMPv3 イベントレシーバで指定のルーティングテーブルが使用されない問題を修正致しました。 33. IPsec ConfigModePool オブジェクト変更時に Reconfig を実施後、予期せぬ再起動が発生することがある問題を修正致しました。 34. OSPF インタフェースがインタフェースとして IPsec トンネルを参照し、ネットワークが設定されていない場合、システムのアップグレードにより再起動のループが発生する場合がある問題を修正致しました。 35. 一部の IP ポリシーにおいて、SNMP 統計が利用できない問題を修正致しました。 36. クラスタピアから SA をインポートした HA クラスタノードによって IPsec rekey がトリガされない問題を修正いたしました。 37. DHCP リレーの自動保存タイマが使用されない問題を修正致しました。 38. DNS クライアント設定画面の IPv4/IPv6 設定の区切りが表示されない問題を修正致しました。 39. DHCP リレーPPM 制限が、リクエストとリスポンス両方に対して不正に適用される

	問題を修正致しました。 40. IPsec トンネルの Auto Establish 機能により、IPsec SA の重複及び（または）ネゴシエーションの失敗が発生する問題を修正致しました。 41. IPsec エンジンのエラーにより予期せぬ再起動が発生することがある問題を修正致しました。 42. HA 同期ユーザの削除により、非アクティブノードでトラフィックが転送されることがある問題を修正致しました。 43. SMTP または IMAP ALG でメール処理を行う際、予期せぬ再起動が発生することがある問題を修正致しました。 44. IPsec サブシステムにより、稀に予期せぬ再起動が発生することがある問題を修正致しました。 45. デフォルトのコンフィグレーションを使用している場合、システムのアップグレード時に Strong Password のチェックが行われず、管理者ユーザが無効化されログインできなくなる問題を修正致しました。本バージョンでは、ロックアウトを防ぐため、デフォルトコンフィグを使用している場合はファームウェアアップグレード時に Strong Password 機能が無効化されます。 46. end-of-email マーカーの直前に非常に長い padding が含まれる Email の場合、SMTP や POP3 ALG においてストールが発生する問題を修正致しました。 47. POP3 または SMTP 使用時、アンチウイルスが Single-part メッセージに対する想定動作とならない問題を修正致しました。 48. Rekey または HA フェイルオーバ時、同じピア、同じ認証に対する複数の IKE SA でトラフィックが破棄される場合がある問題を修正致しました。 49. Web コンテンツフィルタリングのログ画面で、ログが存在するにもかかわらず「No Logs」メッセージが表示される問題を修正致ました。 50. 特定 Web ページに対する HTTP ALG による HTTP 応答が不正となり到達不可となる問題を修正致しました。 51. IPsec の Informational メッセージ交換中、稀にメモリ破損が発生する問題を修正致しました。 52. CVE-2018-8753 の脆弱性を修正致しました。 53. WebGUI の memlog において、IPsec インタフェース名が項目欄に表示されず、テキストラインで表示される問題を修正致しました。 54. IPsec ログメッセージにおけるパラメータ名（source_ip と dest_ip）をより汎用的な名称に更新致しました。 55. WebUI ログイン時、REST API に対する多数のユーザ認証リクエストを受信した際に、予期せぬ再起動が発生することがある問題を修正致しました。 56. ARP Cache による認証ユーザが、ダッシュボードのマウスオーバ時のポップアップに表示されない問題を修正致しました。 57. IPsec Lifetime の KiloBytes を超過した場合、複数の IPsec rekey が開始されることがある問題を修正致しました。 58. HA フェイルオーバ後、不正な分類によりアプリケーションコントロールの接続が動作を停止する問題を修正致しました。 59. Reconfigure 後、OSPF が更新を送信せず他の OSPF ノードにも影響を与える問題を修正致しました。 60. WebUI のチェックボックスが正しく動作しない問題を修正致しました。 61. High Availability ウィザードの表示上のエラーによりコンボボックスを選択しづらくなる問題を修正致しました。 62. ネイバーキャッシュのエントリが残り続けることがある問題を修正致しました。 63. IP Reputation ライセンスがインストールされていない場合、IP Reputation に依存するサービスを設定した際に警告メッセージが表示されない問題を修正致しました。 64. アプリケーションルール画面を小さくした際にスクロールバーが表示されない問題を修正致しました。 65. Gratuitous ARP クエリが Transparent モードで正しく転送されない問題を修正致しました。 66. 特別に作成した HTTP ヘッダを処理する場合に予期せぬ再起動が発生することがある問題を修正致しました。 67. SMTP における DIGEST-MD5 認証が完全にはサポートされていなかった問題を修正致しました。

	68. ALG によりオープンした通信において、Thershold ルールが予期せずトリガされる問題を修正致しました。 69. HA クラスタのクラスタ ID 変更により、クラスタメンバ間でステータス同期が失敗し、メンバが再起動するまで継続する問題を修正致しました。 70. DHCP ホスト名に特殊文字が使用された場合、DHCP サーバのステータス画面が正常にレンダリングされない問題を修正致しました。 71. ログメッセージに特殊文字が含まれている場合、システムログ画面が正常にレンダリングされない問題を修正致しました。 72. CLI コマンドのセッションマネージャを使用して IPv6 セッションを切断できない問題を修正致しました。 73. 1000 以上のルールまたはポリシーが存在する場合、“rules”コマンドを実行すると 999 個より大きい値のインデックスについては”…”と表示される問題を修正致しました。 74. SSH サーバで CBC モードの AES 暗号化のみサポートされる問題を修正致しました。 75. 暗号化された SNMP（AuthPriv モードの SNMPv3）により統計を取得することができない問題を修正致しました。（DFL-260E/860E） 76. 送信フォルダにコピーを保存する設定の一部の Email クライアントに対して IMAP ALG 経由で Email が送信されない問題を修正致しました。 77. IPsec トランスポートモードトンネルに、フラグメント化された IP パケットが送信された場合、ESP パケットが再フラグメント化され、レシーバによって破棄されることがある問題を修正致しました。 78. L2TP/Client 動作時、IPsecTunnel の“Host”設定に対して”SetupSAPer”の指定が必要となる問題を修正致しました。 79. IP アドレスが ID として使用されている場合、IKE ネゴシエーションから RADIUS サーバにパスされた ID が不正なフォーマットとなる問題を修正致しました。 80. DHCP サーバにより、一部リクエストに対して重複した NAK（と稀に不正なオプション）が送信されることがある問題を修正致しました。 81. ローカルユーザデータベースのユーザに対して設定された netobject に対する変更が、再起動後に反映されない問題を修正致しました。 82. DHCPv6 サーバとクライアントにより DUID が opaque 値として処理されず、新しい UUID タイプを使用するデバイスとの動作が正常に行われない問題を修正致しました。 83. MIB の一部項目に、未署名の integer タイプの不正な変数が含まれる問題を修正致しました。 84. IPsec EAP ネゴシエーションにおいて、稀にシステムが再起動する場合がある問題を修正致しました。 85. 複数のユーザに対し、同じ IP/インタフェースを異なるユーザ名で認証することができてしまう問題を修正致しました。 86. UseUniqueSharedMac が有効である場合、すべてのリンクアグリゲーションインタフェースで同じ MAC アドレスが使用される問題を修正致しました。 87. Address Folder オブジェクトの Address 列で、High Availability オブジェクトに対して 1 つのアドレスしか表示されない問題を修正致しました。 88. IKEv2 トンネルの不要なトンネル deletion において、Rekey の際のパケットロスが発生する問題を修正致しました。 89. PFS グループとして「None」が設定されている場合、ピアが 1 つの PFS グループを提案しているにもかかわらず PFS なしで応答する問題を修正致しました。エンドポイント両端で NetDefendOS が使用されている場合、片方のシステムのみ本ファームウェアバージョンへアップグレードされている場合、正しく動作しない可能性があります。アップグレード後も適切なトンネル動作となるには、両方のエンドポイントをアップグレードするか、両方のピアで同じ値を持つ PFS グループが設定されている必要があります。 90. “connections”コマンドを使用して IPv6 接続情報を表示しようとすると、データ利用状況や identified アプリケーションなどの詳細接続情報が表示されない問題を修正致しました。 91. エージェントとして RADIUS の UserAuthRule を使用した IPsec EAP ネゴシエーションの際、ネゴシエーションが Reconfiguration 時に発生した場合、稀にメモリ破損を引き起こすことがある問題を修正致しました。 92. ブラックリストのアンブロックを強制する CLI コマンドにより、誤ったエントリまた

	はすべてのエントリが削除されることがある問題を修正致しました。 93. High Availability クラスタ構成の場合、特定の状況下において、多数の認証ユーザによって CPU 使用率が高くなる問題を修正致しました。 94. RADIUS プロトコルパケットの NAS-Identifier フィールドが String 値に Null ターミネーション文字を誤って送信する問題を修正致しました。 95. ネゴシエーションに失敗した IKEv2 トンネルにおいて、IKE SA におけるリークが発生し、max_ike_sa_reached がログに出力される問題を修正致しました。本問題が発生した場合、IKE トンネルは確立されません。 96. 特定のインタフェースに対して SSH リモート管理が設定されている場合、該当インタフェースのコア IP アドレス以外からは SSH サーバに接続することができない問題を修正致しました。 97. IPsec によりメモリリークが発生する場合がある問題を修正致しました。（DFL-1660/2560/2560G のみ） 98. DHCP クライアントによりリンクダウンイベントが正しく処理されない問題を修正致しました。クライアントはひとつ前の値を完全にリセットせずに discovery ステートに移行します。 99. File Control プロファイルのファイル拡張子リストで長いリストを処理できない問題を修正致しました。 100. Web Profile の IP Policy を使用した Websocket などの HTTP プロトコルアップグレードが許可されない問題を修正致しました。本バージョンではデフォルトでプロトコルアップグレードが許可されます。 101. RSA または DSA がホストキーとして設定されている RemoteManagementSSH オブジェクトの設定が不正に許可される問題を修正致しました。 102. 一部の CLI コマンドでシステムのステータス変更に管理者権限が不要となっていた問題を修正致しました。次のコマンドは auditor 権限で実行不可となります： arp - flush, nd -flush, time - set, route -flushl3cache, zonedefense -blockip/blockenet, ike -delete, dhcp –lease renew/release, dhcp6 -lease renew/release, ha -activate/deactivate, ldap -reset 103. FQDN が IPv4 と IPv6 どちらでも解決可能である場合、IPv4 アドレスが IPv6 アドレスで上書きされてしまい、テーブル内の不正なエントリとなる問題を修正致しました。 104. ユーザ認証ルールの MAC/ARP 認証に対して、イーサネットアドレスの上位・下位どちらを送信するかを選択できない問題を修正致しました。 105. "HAStatusRole"、"HAStatusState"、"HAStatusTimeWithinState"のレポートされた SNMP 値のタイプが誤ったデータタイプに更新される問題を修正致しました。 106. アドレスフォルダに設定されたアドレスのスイッチを検査できない問題を修正致しました。 107. WebUI において、アドレスグループのメンバを選択する際に、無効化されているオブジェクトが選択可能となる問題を修正致しました。 108. RFC の例に基づき、IPv6 サービスの ICMP サービスの名前を IPv6-ICMP から ICMPv6 に修正致しました。 109. アンチウイルスを使用していない場合にアンチウイルスに関するエラーメッセージが出力される問題を修正致しました。 110. Date-time ピッカーを使用した場合に正しく動作しない場合がある問題を修正致しました。 111. SMTP ALG の設定により、予期せぬ再起動が発生することがある問題を修正致しました。 112. HTTP ALG により、ZIP 形式の特定のファイルタイプがブロックされることがある問題を修正致しました。 113. アンチウイルススキャンから ipa ファイルを除外した場合、すべての ZIP ファイルがスキャンから除外される問題を修正致しました。 114. ローカルユーザデータベースのユーザ設定時のパスワード文字数チェックにおいて、サポートされる最大文字数を超過した場合に誤ったメッセージが表示される問題を修正致しました。 115. SIP ALG 使用時、特定の SIP トラフィックによりメモリリークが発生することがある問題を修正致しました。 116. DNS クエリを表示する CLI コマンドを実行すると、誤ったアドレスが表示される問

題を修正致しました。
117. “blacklist”コマンドにデフォルトアクションが設定されていない問題を修正致しました。
118. コマンドラインで最初の設定を変更した後、デフォルトのパスワードを使用した管理者がロックされる場合がある問題を修正致しました。
119. IKEv2 の IPsec トンネルにおいて Local 及び Remote Network の設定が不可となる設定がある問題を修正致しました。
120. IPsec トンネルセットアップが”out of memory”により失敗する問題を修正致しました。
121. SNMP トラップで、” ifOperStatus"に対して誤った値が返されることがある問題を修正致しました。
122. IKE/ESP パケットが他の IPsec トンネルに送信された場合、パケットが破棄される問題を修正致しました。
123. ZoneDefense スイッチの検証が動作しない問題を修正致しました。
124. ローカルユーザデータベースからのユーザの固定 IP アドレス割り当てが想定通りに動作しない問題を修正致しました。
125. IPsec インタフェースと Config Mode で IP プールを使用できない問題を修正致しました。
126. IPv6 に対する Traceroute が想定通りに動作しない問題を修正致しました。
127. DHCP リレー機能において、DHCP メッセージのリレーに失敗することがある問題を修正致しました。
128. IKE SA ネゴシエーション処理中の IPsec インタフェースに対し Reconfiguration を実行すると、IKE SA ネゴシエーションが失敗する場合がある問題を修正致しました。
129. HTTP ALG 及び NAT を使用している場合、メモリリークが発生する問題を修正致しました。
130. FQDN アドレスを 512 個より多く使用することができない問題を修正致しました。
131. LACP の Protocol Data Units が、標準仕様よりも長い問題を修正致しました。
132. Domain Verification を含む Email プロファイルを使用し、DNS サーバが設定されていない場合に警告メッセージが表示されない問題を修正致しました。
133. REST API を使用してスペースを含む、またはグループリストの最後に改行文字を含む新しい認証ユーザを追加した場合、認証が失敗する問題を修正致しました。
134. アンチウイルスを使用している場合に、誤って'out of memory'のログが出力される場合がある問題を修正致しました。
135. Email プロファイルのホワイトリスト/ブラックリストにおいてメモリリークが発生する問題を修正致しました。
136. SMTP、POP3、IMAP ALG においてメモリリークが発生する問題を修正致しました。
137. IDP Rule Action または Treshold Action において、Dynamic Black Listing の「Block service only」を有効化している場合、確立した接続がクローズしない問題を修正致しました。
138. アップロードされた DER 証明書により IPsec コンフィグレーションのアクティブ化に失敗することがある問題を修正致しました。
139. 事前定義済みの時刻同期間隔を修正致しました。
140. Userauth REST API の制限を 9999 から 1000000000 に修正致しました。
141. トラフィックが高負荷となっている場合に、予期せぬ再起動が発生することがある問題を修正致しました。（DFL-260E/860E のみ）
142. CRL ルックアップに対し、以前応答がなかった CA サーバが再度応答し始めた場合、IPsec トンネルセットアップ中に予期せぬ再起動が発生することがある問題を修正致しました。
143. REST API を使用したユーザの再認証において、“idle_timeout”が更新されない問題を修正致しました。
144. "userauth -list"コマンドにおいて、少数ユーザのみ表示されているにも関わらず多数のユーザが認証されている場合、トラフィックの割り込みが発生することがある問題を修正致しました。本バージョンでは、コマンドによって表示されたユーザのみを処理するように最適化されています。
145. トンネルモニタを有効化した状態で IPsec トンネルの Reconfigure を実行すると、トンネルステータスが更新されないことがある問題を修正致しました。
146. “hostmon”コマンドを”num”オプションで実行した場合に、指定エントリ数が正しく表

	示されない問題を修正致しました。 147. IPsec トンネルの両端のピアが IKE SA セットアップを同時に開始した場合、重複した IPsec/IKE SA で片方のエンドポイントが終了し、トンネル内のトラフィックに影響を与える問題を修正致しました。 148. トンネルが Config Mode クライアントとして設定され、Remote Network が all nets 以外に設定されている場合、IPsec Rekey が失敗する場合がある問題を修正致しました。 149. “pcapdump”コマンド実行時、複数のインタフェースを設定できない問題を修正致しました。 150. リンクアグリゲーショングループに対し、定義済み DHCP クライアントのインタフェースを追加すると、失敗する場合がある問題を修正致しました。 151. Microsoft Edge 利用時、ログ画面の「Download Logs」ボタンがブラウザでサポートされていないにも関わらず表示される問題を修正致しました。 152. DNS ルックアップが失敗した際に、DNS キャッシュによる FQDN アドレスの更新が停止する場合がある問題を修正致しました。 153. システム起動時に ZoneDefence ログイベントが誤って生成される問題を修正致しました。 154. 複数のルールセットの中で IP ポリシーに同じ名前を使用できてしまう問題を修正致しました。 155. IPsec トンネル上の Local Network または Remote Network に設定された複数のネットワークにおいて、Rekey が失敗し、IPsec SA 再作成中にパケットが破棄されることがある問題を修正致しました。 156. ブラックリストに含まれる IP アドレスの E メールにもかかわらずヘッダ変換失敗によりブラックリストとして処理されない問題。 157. Email コントロール機能において、ブラックリストに設定された IP アドレスを含む E メールが適切に処理されない問題を修正致しました。 158. 証明書に適切なフォーマットのプライベート鍵が含まれない場合、11.04.00 より古いファームウェアからのアップグレードにおいて再起動のループが発生することがある問題を修正致しました。本バージョンでは、不正な証明書及びそれに依存するオブジェクトを無効とします。オブジェクトを再度有効化するには、証明書を再度アップロードする必要があります。 159. OSPF を実行しているシステムで、OSPF ネイバの Reconfigure 中に予期せぬ再起動が発生することがある問題を修正致しました。 160. Diagnostics Console 画面でエラーが発生しログが表示されない場合がある問題を修正致しました。 161. IP ルールにおいて、アクティブ化されている IP ポリシーより前に配置された IP ポリシーが追加/有効化/削除/無効化された場合、トラフィックが停止する場合がある問題を修正致しました。 162. IPsec 上の OSPF インタフェースが、起動状態にも関わらず Down としてタグ付けされる問題を修正致しました。 163. 機能毎に MAC アドレスのフォーマットが異なる問題を修正致しました。 164. 空のログファイルをダウンロードした場合、受信ファイルには Web 画面のソースコードが含まれ、”Logs.txt”という名前のファイルとなる問題を修正致しました。本バージョンでは、”Empty log”というテキストが含まれ、ログデータが含まれるログファイルと同様に、ファイル名に日時が含まれます。 165. Reconfigure 後にダイナミックブラックリストのエントリがタイムアウトした場合、システムが無応答になる場合がある問題を修正致しました。 166. Reconfigure 中、ブラックリストファイルの読み込み・保存の度にログエントリが生成される問題を修正致しました。 167. IMAP 経由で転送された Email に対するアンチウイルス検査実行時に、一部のメール接続がストールする場合がある問題を修正致しました。 168. RADIUS サーバから取得したクライアント IP アドレスを IPsec トンネル経由で割り当てる際、RAIUS アカウンティングサーバが使用されていると、IP アドレスが取得できない場合がある問題を修正致しました。 169. NAT によって UDP カプセル化 ESP パケットのポートが変更された場合、NAT された IPsec クライアントのトラフィックが停止する場合がある問題を修正致しました。（DFL-2560/DFL-2560G のみ）

	170. LW-HTTP ALG でメモリリークが発生する問題を修正致しました。 171. PPPoE インタフェース経由で送信されるパケットがパケットキャプチャ機能でキャプチャされない問題を修正致しました。 172. フラグメント化された SYN パケット及び/またはペイロードを送信する SYN パケットが破棄されるオプションを追加致しました。初期設定：「drop and log」 173. 7bit の Transfer Encoding を含む HTTP persistent 接続に対して HTTP ALG が使用された場合、後続のメッセージが同じエンコーディングを使用して処理される問題を修正致しました。 174. アプリケーションコントロールサブシステムにおいて、アプリケーション識別子がログ出力されない問題を修正致しました。 175. ルートロードバランシングセットアップの一部としてルートが使用される接続が、Reconfigure 時に不正にクローズされることがある問題を修正致しました。 176. 感染 URL について、ユーザに情報を提示する前にブロックされ HTTP 接続が終了することがある問題を修正致しました。 177. XAuth の IPsec トンネルが開始された際に不正な認証方式がピアに対して送信される問題を修正致しました。 178. File Control の Fail-Mode 設定が File Control と紐づいておらずアンチウイルスプロファイルに移動される問題を修正致しました。既存の設定は変換され、設定済みの値を使用します。 179. ZoneDefense 設定の同期が原因で、Reconfigure 中に HA メンバが予期せぬ再起動をすることがある問題を修正致しました。 180. Traffic Shaping において、TCP 接続により、稀に予期せぬ再起動が発生することがある問題を修正致しました。 181. HTTP を使用した音楽ストリームについて、Web Content Filter または File Control と一緒に使用している場合、破棄される場合がある問題を修正致しました。 182. DHCP サーバがリッスンしているインタフェースが main ルーティングテーブルに存在しない場合、IPv4 DHCP サーバが応答しない問題を修正致しました。 183. High Availability の Out-of-buffer カウンタが正常にインクリメントされない場合がある問題を修正致しました。 184. WebUI 上で IPsec ステータスボタンが表示されない問題を修正致しました。 185. WebUI で侵入検知ルールを追加し特定の設定を除外した際に、メインステータス画面に移動してしまう問題を修正致しました。 186. TLS ALG のアイドルタイムアウト設定により、一部アプリケーションでタイムアウトの問題が発生する問題を修正致しました。本設定は 30 秒から 5 分に拡張されました。 187. 不正な MIME 形式の Email が IMAP コンテンツスキャンを通過できない問題を修正致しました。 188. DNS サーバへのルートを取得できない場合、DNS サブシステムがバックオフし、最初の試行失敗の後に FQDN アドレスを解決できない問題を修正致しました。 189. スケジュール化されたアンチウイルスの更新が失敗または停止する場合がある問題を修正致しました。 190. プライベートネットワークで IMAP の Email Control が使用された場合、一部の機能が動作しない場合がある問題を修正致しました。 191. エンコードされた長いタイトルヘッダを含む Email において、IMAP コンテンツスキャン時にメッセージが破損する場合がある問題を修正致しました。 192. Updatecenter WCF サーバへの接続において、接続クローズを受信後、リストの次のサーバへの試行を行わず、同じサーバが試行される問題を修正致しました。 193. IMAP 事前認証が想定通りに動作しない問題を修正致しました。 194. HTTP ALG 使用時に一部 URL が接続不可となる問題について、“Content-Type”の HTTP ヘッダフィールドの上限を 64 文字を 256 文字に拡張し、修正致しました。 195. HTTP を使用したホストモニタリングで、提供された Expected Response パラメータを含む受信データに一致しない問題を修正致しました。 196. SSH サーバにより、稀にメモリ使用率が増加し予期せぬ再起動が発生する問題を修正致しました。 197. PPPoE インタフェースに対してソースインタフェースとしてリンクアグリゲーションインタフェースを選択できない問題を修正致しました。 198. Light-weight HTTP ALG において、接続 Web ページがポリシーでブロックされた際

	に、稀に適切なブロック画面が表示されない場合がある問題を修正致しました。 199. メイン画面のアプリケーションカウントで正確な数値が表示されない問題を修正致しました。 200. 新しいステートに対し、ステートフル NAT プールで利用の少ない IP が使用されない問題を修正致しました。 201. データ転送中に IMAP 接続がどちらかの側で予期せずクローズした場合、適切な処理が行われない問題を修正致しました。 202. 大容量の添付ファイルを含む Email が、稀にアンチウイルススキャンを通過できない問題を修正致しました。 203. POP3 タグのアンチスパムが稀に想定通りに動作しない問題を修正致しました。 204. Email の圧縮添付ファイルが、Drop 設定にも関わらず転送されることがある問題を修正致しました。 205. 稀にアンチウイルススキャンで ZIP ファイルのスキャンに失敗する問題を修正致しました。 206. WebUI のルーティングテーブル表の Gateway 及び Local IP 列のツールチップが正しく動作しない問題を修正致しました。 207. RADIUS 共有シークレット設定において、99 文字以上の入力が可能であるにも関わらず、使用されるのは 99 文字までとなる問題を修正致しました。本バージョンでは、入力及び使用可能な最大文字数は 128 文字となっています。 208. マルチキャストアドレス変換使用時、一部 UDP フラグメントのデータが不正に変換される問題を修正致しました。 209. Mail Alerting が設定されている場合、新しい設定をアクティブ化した際に警告メッセージが表示されない問題を修正致しました。 210. Local Console Idle Timeout 設定が、SSH Idle Timeout という誤った名称となっていた問題を修正致しました。 211. “virus”の URL が検出された場合、memlog エントリのアドバイザリリンクが誤った URL となる問題を修正致しました。 212. Atomic IPv6 フラグメントの送信をトリガすることが可能であった問題を修正致しました。 213. アンチウイルス URL スキャンを実行しキャッシュ URL が検出された場合、HTTP_ALG において、URL ではなくファイルとしてログ出力され、誤ったアドバイザリリンクが生成される問題を修正致しました。 214. 設定からすべての IPsec トンネルインタフェースを削除した場合、設定の更新反映に 1 分程度要する問題を修正致しました。 215. 複数のインタフェースで DHCPv6 クライアントを設定し、いずれかのインタフェースがリースを取得できない場合、成功したインタフェースのリースを使用し始めるまで半永久的に待機する問題を修正致しました。 216. Email Control の Malicious Link Protection 機能で HTTPS を処理できない問題を修正致しました。 217. Web Content Filter Memlog において、ログエントリがあった場合でも、Web Content Filter ALG のログが出力されない問題を修正致しました。 218. IPsec トンネルで Config mode プールを使用した場合、Reconfigure 後に割り当て済みの IP が他のクライアントに配布される問題を修正致しました。 219. IMAP コンテンツスキャナで非 Multipart メッセージが正しくスキャンされない問題を修正致しました。 220. High Availability 構成において、同期ケーブルが抜かれた場合に CPU 使用率が増加する問題を修正致しました。 221. Reconfigure 後、ピアがメッセージに応答するにも関わらず IKEv2 削除メッセージが再送される問題を修正致しました。 222. CRL Distribution Point (CDP) が、ゲートウェイ証明書には含まれず Certification Authority (CA) 証明書に含まれる場合、Certificate Revocation List (CRL) ルックアップが失敗する問題を修正致しました。 223. WebUI から IKE SA を削除できない問題を修正致しました。 224. 現在のコンフィグに、名前のない Route オブジェクト及び子要素の Monitored Host オブジェクトが含まれる場合、“script-create”コマンドで誤ったスクリプトが生成される問題を修正致しました。 225. IMAP 使用時、一部スパム Email で正しくタグ付けが行われない問題を修正致しまし

	た。 226. IDP ルールにおいて、"Invalid hex encoding"が drop ルールとして設定されている場合、一部 Email が転送されない問題を修正致しました。 227. File Control 設定で特定の組み合わせが設定されている場合、一部のメッセージが IMAP コンテンツスキャナーによって誤ってブロックされる問題を修正致しました。 228. 同じ Email に対して別の方式を使用してスパムが検出された場合、IMAP ALG のスパムカウンタが正しくカウントされない問題を修正致しました。 229. FQDN グループがサポートされていない IP-、Goto-、Return-、Routing-ルールで選択可能である問題を修正致しました。 230. HA 構成において、ZoneDefense ブロックエントリの詳細情報が非アクティブノードに対して正しく同期されない問題を修正致しました。 231. アプリケーションコントロールが IPv6 TCP パッケージに対してのみ実行される問題を修正致しました。 232. キャッシュの IP アドレスが適切であるにも関わらず DNS キャッシュが DNS サーバからエラーを示すメッセージを受信した場合、FQDN エンドポイントを使用した IPsec トンネルが予期せず終了する問題を修正致しました。 233. IPv4 エンドポイントの IPsec トンネルなどを介した IPv6 パケットの送信により、ハードウェアアクセラレータでパケットが破棄される問題を修正致しました。（DFL-2560/DFL-2560G） 234. Mail Alerting で SMTP サーバとして FQDN アドレスを使用した場合、動作しない問題を修正致しました。 235. 感染ファイルが添付された一部のメールが転送されない問題を修正致しました。

既知の問題：

ファームウェアバージョン	既知の問題
V12.00.13.05	1. IDP コンテンツスキャンが稀に誤った結果となることがある問題。 2. IDP コンテンツスキャン処理において、IDP シグネチャで指定されたパターンの検出とレポートに失敗することがある問題。 3. Web Profile Fail Mode 設定が正しく動作しない問題。 4. リンクアグリゲーションを設定したインタフェースでパケットキャプチャを行った場合に、入力パケットがキャプチャされない問題。 5. IDP コンテンツスキャンにおいて、トリガとなるコンテンツが複数パケットに分割されている場合、正しく処理されない問題。 6. PPTP を設定している場合、稀に予期せぬ再起動が発生する場合がある問題。 7. High Availability および IPsec を設定している場合、reconfigure 処理中に予期せぬ再起動が発生することがある問題。 8. DNS 応答パケットの長さが 512bytes を超える場合、または EDNS0 の UDP ペイロードサイズが含まれる場合、DNS ALG によりパケットが破棄される問題。 9. セットアップウィザードに不要な項目が含まれている問題。 10. セットアップウィザードに前の画面へ戻るボタンが表示されていない問題。 11. 古いアップグレードパッケージフォーマットの場合、パッケージ検証が失敗する問題。 12. AutoEstablish が設定された IPsec トンネルの Remote Endpoint に対してルートが存在しない場合、reconfigure 処理中にシステムが無応答となり予期せぬ再起動が発生することがある問題。 13. IPsec サブシステムのエラーにより、reconfigure 処理後に予期せぬ再起動が発生することがある問題。 14. リンク速度を 10Gbps に設定できてしまう問題。 15. IP Reputaion の更新を行った場合、メモリ消費が増加する問題。 16. 「Save and Activate」実行時の接続性確認までの時間が長く設定されている問題。 17. WEB コンテンツフィルタにおける再分類 URL が誤っている問題。 18. REST API のユーザ認証リストの groups プロパティについて、255 文字までに制限

	される問題。 19. IPsec ユーザが XAuth または EAP を使用してログインしている場合に、アクティブ状態であるにも関わらず"Idle Timeout"後にログアウトされる問題。 20. Android 端末において、HTTP 認証で DHCP サーバを使用している場合、WiFi 接続が切れた後に再度認証が必要となる問題。 21. IDP 設定画面の構成が他の画面の仕様と異なる問題。 22. VLAN インタフェースで DHCP クライアントが有効化されている場合、ステータス画面に割り当て IP の詳細が表示されない問題。 23. High Availability のフェイルオーバ後、IPsec トンネルが動作を停止することがある問題。 24. L2TP サーバを使用している場合、稀に予期せぬ再起動が発生する場合がある問題。 25. Transparent Mode に設定されたインタフェースでトラフィックが処理される際に、稀に予期せぬ再起動が発生する場合がある問題。 26. IPsec トラフィックの処理中に、予期せぬ再起動が発生する場合がある問題。 27. DNS リゾルバにおいて一部の圧縮済みメッセージが解析できず、アンチスパム処理のパフォーマンス低下などを招く場合がある問題。 28. Web 画面上の ON/OFF 設定の幅が狭い場合がある問題。 29. HA モードにおいて、透過モードのステート同期が行われずループが発生する問題。 30. HA モードにおいて、アプリケーションレイヤゲートウェイでステート同期行われない問題。クラスタが他のピアにフェイルオーバするとき、ALG によって処理されるすべてのトラフィックがフリーズします。ただし、クラスタが 30 秒程度で元のピアへフェイルバックした場合、フリーズしたセッション（及び関連する送信）は再度処理を開始します。新しい設定がアップロードされる度、このようなフェイルオーバ（及びフェイルバック）が発生します。 31. HA クラスタの非アクティブノードが、IPsec、PPTP、L2TP および GRE トンネル経由で到達不可となる問題。これらのトンネルはアクティブノードへ/から確立します。 ・非アクティブな HA メンバはトンネルを介してログイベントを送信できません。 ・非アクティブな HA メンバはトンネルを介して管理/監視できません。 ・OSPF：クラスタメンバがブロードキャストインタフェースを共有せずに、非アクティブノードが OSPF ステートについて学習する場合、トンネル経由の OSPF フェイルオーバはアクセラレータされたフェイルオーバ（<1s）ではなく、通常の OSPF フェイルオーバを使用します。デフォルト設定で 20-30 秒、より積極的な同期 OSPF タイミングでも 3-4 秒かかります。 32. HA モードにおいて、L2TP 及び PPTP トンネルでステートが同期されない問題。フェイルオーバ時には、トンネルが動作していないとみなされた後に、次のクライアントでトンネルを再確立します。タイムアウトは一般的に 30～120 秒の範囲です。 33. HA モードにおいて、IDP シグニチャステートが同期しない問題。 34. トランスポートモードの 2 つの DFL ファイアウォール間で、IPsec L2TP/L2TPv3 トンネルを確立できない問題。 対処方法：クライアントサイトの WAN IP アドレスに対して"local endpoint"を指定する