

統合ネットワーク (IPCOM VE2) 仕様



SC/LS V01 機能・諸元

仮想マシン仕様

| 仕様 | | |
|--------------------|--|---|
| ソフトウェア名称 | VE2-100 | VE2-220 |
| 割り当てが必要なりソース | | |
| vCPU | 1 | 4 |
| メモリ | 4,096 メガバイト | 8,192 メガバイト |
| サーバーのタイプ(ニフクラ) | h2-small4/h2r-small4 e2-small4/e-small4 ※2 c2-small/4c-small4 ※2 | h2-large8/h2r-large8 e2-large8/e2r-large8/e-large8 ※2 c2-large8/c-large8 ※2 |
| ハードディスク容量 | 100 ギガバイト | |
| ハードディスクのタイプ(ニフクラ) | 標準ディスク/高速ディスク/標準フラッシュドライブ/高速フラッシュドライブ | |
| 最大インターフェース(NIC)数※1 | 8 | 8 |

※1…ニフクラ上ではサーバ作成時に2インタフェースを提供。3インタフェース以上利用する場合は、追加NICでインタフェースを追加可能。

※2…2023年11月1日(水)以降、Type-e、Type-cの新規サーバは作成不可。但し、サーバタイプ変更時には選択可能。

機能一覧

| 対応状況 (●：標準、○：オプション、－：未サポート) | | | | |
|--------------------------------|------------|---------|----|---------|
| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
| ルータ機能 | ● | ● | ● | ● |
| アドレス変換機能 | ● | ● | ● | ● |
| ファイアーウォール機能機能 (L2-7) | ● | ● | ● | ● |
| アノマリ型IPS機能 | ● | ● | ● | ● |
| WAF (Web アプリケーションファイアーウォール) 機能 | － | － | － | ● |
| IPsec-VPN機能 | ● | ● | － | － |
| L2TP/IPsec機能-VPN | － | ● | － | － |
| SSLアクセラレーター機能 | － | ● | ● | ● |
| 帯域制御機能 (L2-7) | － | ● | ● | ● |
| サーバ負荷分散機能 | － | － | ● | ● |
| HTTP/HTTPSコンテンツ圧縮機能 | ● (HTTPのみ) | ● | ● | ● |
| ユーザー認証機能 | ● | ● | ● | ● |
| ネットワークサービス機能 | ● | ● | － | － |
| 高信頼化機能 | ● | ● | ● | ● |
| 運用管理/保守機能 | ● | ● | ● | ● |

共通 (装置全体の上限値)

| 諸元(最大値) | | |
|---|--------------------|-----------|
| ソフトウェアタイプ | VE2-100 | VE2-220 |
| 最大同時セッション数※ (VE2-100 LS PLUSのみ) | 200,000 100,000 | 1,000,000 |
| ※ 同時に制御可能なTCP、UDPフローの最大数 | | |
| 最大同時ノード数※ (VE2-100 LS PLUSのみ) | 200,000 100,000 | 1,000,000 |
| ※ 同時に制御可能なノード (クライアント) の最大数 | | |
| 最大クラスマップ定義数 (Class-map) ※ | 6,000 | 15,000 |
| 最大スケジュールルール定義数 (time-preiod) | 64 | 128 |
| 最大マッチングルール定義数 (match) | 16,000 | 30,000 |
| ※ ファイアーウォール機能、アノマリ型IPS機能、アドレス変換機能、QoS制御機能、サーバ負荷分散機能 で定義しているマッチングルール数の合計。 なお、本装置全体の上限値と別に、機能ごとに定義できるマッチングルール数の上限がある。 | | |
| 最大マッチングルール数/1クラスマップあたり | 30 | |
| 最大アプリケーション識別定義数 (fixup protocol) | 50 | |

ルータ機能

| | | | |
|---------|-----------------|---|-----------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| L2中継 | ブリッジ (MAC学習) | | |
| L3中継機能 | 通信プロトコル | IPv4 | |
| M T U | IPフラグメント、MTU長変更 | | |
| フィルタリング | IPv4 | 送受信IPアドレス、IP Precedence、IP ToS、Protocol (TCP/UDP/ICMP)、ICMP type/code、TCP src/dst port、TCP syn/ack、UDP src/dst port | |

対応状況 (●：標準、○：オプション、－：未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | ● | ● | ● | ● |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|---------------------------|---------|---------|
| レイヤー2中継/レイヤー3中継 | | |
| 最大VLAN定義数 | 32 | 64 |
| 最大DHCPクライアント定義数 | 8 | 8 |
| 最大MAC学習テーブルエントリー数 | 8,000 | 16,000 |
| 最大ARPエントリー数 | 8,000 | 16,000 |
| 最大MAC-VLANエントリー数 | 64 | 128 |
| 最大レイヤー2 フォワードグループ定義数 | 8 | 16 |
| ルーティング制御 | | |
| スタティックルート (IPv4) 最大エントリー数 | 512 | 6,000 |

アドレス変換機能

| | | | |
|--------|--|-------|---------------------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| | | ※ | グローバル側のIPアドレスを変換する場合にはマルチIPサービスの契約が必要 |
| 変換方式 | 送信元IPアドレス (静的変換/動的変換)、送信元IPアドレス/ポート (動的変換/範囲指定可能)、あて先IPアドレス (静的変換/動的変換)、あて先IPアドレス/ポート (動的変換)、アドレス変換除外ルール定義 | | |
| その他の機能 | ダイナミックポート・アプリケーション対応 | | |
| ログ管理 | イベントログ情報 セッションログ ログ転送 (形式) Syslog (IPCOM標準形式、WELF形式) | | |

対応状況 (●：標準、○：オプション、－：未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | ● | ● | ● | ● |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|------------------|---------|---------|
| 最大アドレス変換ルール定義数 | 2,000 | 5,000 |
| 最大マッチングルール定義数 | 6,000 | 10,000 |
| 接続元変換IPアドレス最大定義数 | 1,000 | 2,500 |
| 最大同時セッション数 | 100,000 | 500,000 |
| 最大NBT/ICMPセッション数 | 10,000 | 50,000 |

ファイアウォール機能 (L2-7)

| | | | |
|---------------|---|---------------------|------------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| アクセス制御 | IPv4 | フィルタ条件 | 詳細は参考情報のファイアウォール機能、帯域制御機能を参照 |
| アクション | | 受諾、破棄、拒否、リダイレクト、無効化 | |
| ステートフル・セッション・ | IPv4 | レイヤー2 ~ レイヤー7 | |
| ログ管理 | イベントログ情報 セッションログ ログ転送 (形式) Syslog (IPCOM標準形式、WELF形式) | | |

| | | | | |
|----------------------------|----|---------|----|---------|
| 対応状況（●：標準、○：オプション、－：未サポート） | | | | |
| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
| サポート状況 | ● | ● | ● | ● |

諸元(最大値)

| | | |
|--|---------|-----------|
| ソフトウェアタイプ | VE2-100 | VE2-220 |
| 最大アクセス制御ルール数 | 2,000 | 5,000 |
| アクセス制御ルールの最大マッチングルール定義数 | 10,000 | 20,000 |
| 最大インターフェース・グループ数 | 256 | 256 |
| 1インターフェース・グループに登録可能な最大インターフェース数 | 256 | 256 |
| 最大アクセス制御マップ数※ | 256 | 256 |
| ※ 異なる名前で定義可能な個数。同じ名前でも方向が異なる定義が可能のため、装置全体では1,024個まで可能。 | | |
| アクセス制御マップの最大ルール数 | 2,000 | 5,000 |
| 最大サービス制御マップ数 | 2,000 | 5,000 |
| サービス制御マップの最大ルール数 | 2,000 | 5,000 |
| 同時最大セッション数 | 200,000 | 1,000,000 |
| (VE2-100 LS PLUSのみ) | 100,000 | |

アナマリ型IPS機能

| | | | |
|---------|--------------------------------------|---------------------------|-----------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| 攻撃防御の種類 | 参考情報のアナマリ型IPS攻撃防御一覧を参照 | | |
| アクション | 検知(通過)、破棄、ブロック | | |
| | ※ 検出対象の攻撃のタイプによっては、ブロックを定義できないものがある。 | | |
| アクセス数規制 | 同一送信元からのセッション数、同一宛先へのセッション数 | | |
| ログ管理 | イベントログ情報 | セッションログ | |
| | ログ転送(形式) | Syslog (IPCOM標準形式、WELF形式) | |

対応状況（●：標準、○：オプション、－：未サポート）

| | | | | |
|----------|----|---------|----|---------|
| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
| サポート状況 | ● | ● | ● | ● |

諸元(最大値)

| | | |
|---------------------|---------|-----------|
| ソフトウェアタイプ | VE2-100 | VE2-220 |
| 最大攻撃防御ルール数 | 256 | 512 |
| 最大マッチングルール定義数 | 10,000 | 20,000 |
| 最大ブロックIPアドレス数 | 10,000 | 50,000 |
| 同時最大セッション数 | 200,000 | 1,000,000 |
| (VE2-100 LS PLUSのみ) | 100,000 | |

WAF (Web アプリケーションファイアーウォール) 機能

| | | | |
|----------------|--|--|-------------------------------|
| IP対応 | : IPv4 | 動作モード | : ブリッジモード(プライベートLANで可)、ルータモード |
| 検知方式 | ブラックリスト(エンジン解析)、ホワイトリスト | | |
| 攻撃防御機能 | リクエストライン規制、HTTPヘッダ規制、メッセージボディ規制、パラメータ規制、ファイル転送規制、改ざん規制、アクセス違反、脆弱性攻撃防御、クロスサイトスクリプティング、SQLインジェクション、XMLインジェクション、Xpathインジェクション、Blind Xpathインジェクション、LDAPインジェクション、OSコマンドインジェクション、SSIインジェクション、ディレクトリトラバース | | |
| 攻撃検知時の動作 | 通過、拒否、エラーページ応答、リダイレクト応答、特定文字に変換 | | |
| クローキング(情報隠蔽)機能 | HTTPレスポンスヘッダの隠蔽、HTTPレスポンスコードの隠蔽、HTMLコメントの隠蔽、クレジットカード番号の隠蔽、マイナンバー | | |
| 学習機能 | クレジットカード種別 | American Express、Diners Club、JCB、MasterCard、VISA | |
| | | パケット採取、パケット解析、学習データベース | |
| 運用管理機能 | 文字コード | ISO8859-1:1987、Shift-JIS、Extended UNIX Code Packed Format For Japanese (EUC)、ISO-2022-JP、UTF-8 | |
| | | 防御状態の表示・解除、統計情報の表示、脆弱性攻撃レポートの保存 | |

| | | |
|------|----------|--------------------------|
| ログ管理 | イベントログ情報 | WAFログ |
| | ログ転送（形式） | Syslog（IPCOM標準形式、WELF形式） |

対応状況（●：標準、○：オプション、－：未サポート）

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | － | － | － | ● |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|--|--------------------|---------|
| 最大WAFコネクション数 | 50,000 | 100,000 |
| 最大サイト数 | 5 | 10 |
| クレジットカードの書式（種類） | | 30 |
| 最大ブラックリスト登録数 | | 4,000 |
| サイト単位設定 | | |
| IPアドレス範囲指定（防御対象IP） | | 5 |
| ポート番号範囲指定（防御対象ポート） | | 10 |
| ホスト名とパス名（防御対象Webサイト） | | 10 |
| HTTPヘッダー・ホワイトリスト/1サイトあたり | | 100 |
| HTTPヘッダー・ホワイトリストに登録可能な HTTPヘッダー名の長さ | | 100バイト |
| HTTPヘッダー・ブラックリスト/1 サイトあたり | | 100 |
| HTTPヘッダー・ブラックリストに登録可能な HTTPヘッダー名の長さ | | 100バイト |
| HTTPヘッダーフィールド置換リスト/1サイトあたり | | 100 |
| 置換する値 | | 100バイト |
| 隠蔽するHTTPステータスコード・リスト/1サイトあたり | | 100 |
| CSRF防御 | | |
| CSRF防御開始URLリスト/サイトあたり | | 100 |
| CSRF防御参照先URLリスト/サイトあたり | | 10 |
| CSRF防御参照元URLリスト/参照先URLあたり | | 10 |
| セッション管理 | | |
| セッション管理開始URLリスト/サイトあたり | | 100 |
| セッション管理参照可能URLリスト/開始 URLリストあたり | | 100 |
| セッション管理終了URLリスト/開始URL リストあたり | | 100 |
| 検知メール送信先アドレス | | 3 |
| 公開URLのホワイトリスト | | 1,000 |
| ホワイトリストに登録可能なURLの長さ | | 1000バイト |
| 公開URLのブラックリスト | | 100 |
| ブラックリストに登録可能なURLの長さ | | 1000バイト |
| ページ単位設定 | | |
| ページ名/1サイトあたり | | 100 |
| HTTPヘッダーのホワイトリスト/1ページあたり | | 50 |
| HTTP ヘッダー・ホワイトリストに登録可能な HTTP ヘッダー名の長さ | | 100バイト |
| cookie名のホワイトリスト/1ページあたり | | 40 |
| cookie 名のホワイトリストに登録可能な cookie 名の長さ | | 100バイト |
| 許可するアップロードファイルの種別数/1ページあたり | | 32 |
| 許可するアップロードファイルの種別の長さ | | 100バイト |
| パラメーター名のホワイトリスト/1ページあたり | | 50 |
| ホワイトリストに登録可能なパラメーター名 の文字数 | | 100バイト |
| cookie 単位 設定 | | |
| cookie 名の定義数/1 ページあたり | | 100 |
| cookie 名の長さ | | 100バイト |
| cookie 値のホワイトリスト | 10（※ただし、全体ページで100） | |
| ホワイトリストに登録可能なcookie 値の文字数 | | 100バイト |

| | | |
|--------------------------|--------|----------------------|
| パラメーター単位 | | |
| パラメーター名の定義数/1 ページあたり | | 100 |
| パラメーター名の長さ | | 100バイト |
| パラメーター値のホワイトリスト | | 10 (※ただし、全体ページで100) |
| ホワイトリストに登録可能なパラメーター値の文字数 | | 100バイト |
| 学習機能 データベース | | |
| サイト単位 | | |
| HTTPレスポンスヘッダーの分析結果 | 記録する長さ | 50 バイト |
| | 記録数 | 50 |
| HTTPレスポンスのステータスコードの分析結果 | 記録する長さ | 3 バイト |
| | 記録数 | 20 |
| コンテンツタイプの分析結果 | 記録する長さ | 80 バイト |
| | 記録数 | 50 |
| ページ単位 | | |
| ページ数 | | 300 |
| 除外されたページ数 | | 600 |
| ページのパス名の長さ | | 1,000 バイト |
| アップロードファイルの種別 | 記録する長さ | 80 バイト |
| | 記録数 | 30 |
| リクエスト単位 | | |
| HTTPメソッド | 記録する長さ | 7 バイト |
| | 記録数 | 10 |
| クエリ部分のパラメーター | 記録する長さ | 200 バイト (※名前と値の合計) |
| | 記録数 | 70 |
| リクエストヘッダー | 記録する長さ | 500 バイト (※名前と値の合計) |
| | 記録数 | 50 |
| cookie | 記録する長さ | 2,000 バイト (※名前と値の合計) |
| | 記録数 | 10 |
| メッセージボディ部のパラメーター | 記録する長さ | 200 バイト (※名前と値の合計) |
| | 記録数 | 70 |
| レスポンス単位 | | |
| ステータスライン | 記録する長さ | 42 バイト (※ライン全体) |
| | 記録数 | 10 |
| レスポンスヘッダー | 記録する長さ | 500 バイト (※名前と値の合計) |
| | 記録数 | 50 |
| 参照するURL | 記録する長さ | 300 バイト |
| | 記録数 | 50 |
| フォーム | 記録する長さ | 300 バイト |
| | 記録数 | 4 |
| フォーム部品 | 記録する長さ | 50 バイト |
| | 記録数 | 100 |

IPsec-VPN機能

| | | | |
|-----------|------------------------|--|--|
| IP対応 | ： IPv4 | 動作モード | ： ルータモード |
| IPsec/IKE | セキュリティプロトコル | | AH、ESP |
| | IPsec通信方式 | | トンネルモード、トランスポートモード (L2TP/IPsec時) |
| | SA管理 | | マニュアル方式、 IKEv1方式 (IKEオートスタート、メインモード、アグレッシブモード、PFS) |
| | セレクト (フィルター条件) | | IPアドレス、IPサブネット、プロトコル、ポート番号 (TCP/UDP)、 ホスト名 (FQDN) |
| | 暗号化アルゴリズム | | NULL暗号 (暗号なし)、DES-CBC (56bits)、3DES-cbc (168bit)、Rijndael (AES) -CBC (128/192/256bits) |
| | 認証アルゴリズム | | HMAC-MD5、HMAC-SHA-1、 HMAC-SHA-2 (SHA-256/SHA-384/SHA-512) |
| | IKE認証方式 | | 事前共有鍵 (Pre-shared key)、RSA署名 (512-4096bits) |
| | DH(Diffie-Hellman)グループ | MODP768 (DH-Grp1)、MODP1024 (DH-Grp2)、 | |
| | | MODP1536 (DH-Grp5)、MODP2048 (DH-Grp14) | |

| | |
|--------|--|
| その他の機能 | ポリシーベースIPsec-VPN、Hub and Spoke中継、パスMTUディスカバリ/MSS書換え、IPフラグメント、Ipsecトンネル分散（リンク負荷分散連携）、障害時のSA自動復旧、Ipsecマルチホーミング、ダイナミックネットワークのサポート、IKE Commitビット同時接続最大数制限、NATトラバース |
|--------|--|

対応状況（●：標準、○：オプション、－：未サポート）

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | ● | ● | － | － |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|--|---------|---------|
| 最大相手装置数 | 500 | 2,000 |
| 最大SA数 | 1,500 | 6,000 |
| 最大IPsecトンネル数 | 500 | 2,000 |
| 自装置の最大秘密鍵/証明書数 | 256 | 256 |
| 自装置の最大CA証明書数 | 1 | 1 |
| 相手装置の最大CA証明書数 | 2,048 | 2,048 |
| 最大事前共有鍵定義数 | 500 | 2,000 |
| 最大IKEルール定義数 | 500 | 2,000 |
| 最大IPsecルール定義数※ | 500 | 2,000 |
| ※ ipsec ruleとipsec ping-keep-alive-ruleとipsec dynamic-ruleの合計数 | | |
| 最大monitor route定義数 | 512 | 6,000 |
| 最大set-peer定義数/1つのIPsecルールあたり | 32 | 64 |

L2TP/IPsec-VPN機能

IP対応 : IPv4 動作モード : ルータモード

| | |
|------------|--|
| L2TP/IPsec | 認証機能 |
| | 接続認証 |
| | IKE（事前共有鍵（Pre-shared key）、RSA署名（512-4096bits）） |
| | ユーザー認証 |
| | PAP、CHAP、MS-CHAP-V2、EAP |
| | パスワード変更機能 |
| | MS-CHAP-V2（認証データベースとしてRADIUS or ローカルデータベースを利用の場合） |
| | クライアントOS |
| | Windows 8.1(32bit/64bit)、Windows 10(32bit/64bit)、iOS 5.x/6.x/7.x/8.x/9.x/10.x/11.x/12.x/13.x ^{※1} 、Android 2.x/3.x/4.x/5.x/6.x/7.x/8.x/9.x ^{※1} 、OS X 10.11 ^{※2} 、macOS Sierra 10.12 ^{※2} 、macOS High Sierra 10.13 ^{※2} 、macOS Mojave 10.14 ^{※2} 、macOS Catalina 10.15 ^{※2} |
| | ※1 ユーザー認証に証明書を使用するEAP認証（拡張認証プロトコル）、およびMSCHAP-V2認証を使用した際のパスワード変更機能はサポートしていません。 |
| | ※2 接続認証に証明書を使用することはサポートしていません。 |
| | 監視機能 |
| | L2TPキーブアライブ機能、無通信監視機能 |

その他の機能との連携
ファイアウォール連携、アドレス変換連携、IPsec-VPN連携、アンチウィルス機能連携、Webコンテンツ・フィルタリング機能連携

対応状況（●：標準、○：オプション、－：未サポート）

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | － | ● | － | － |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|--|---------|---------|
| 最大同時接続ユーザー数※ | 500 | 2,000 |
| 最大IPsecトンネル数※ | 500 | 2,000 |
| ※ IPsec-VPN 機能でIPsec トンネルを消費すると、この上限値は消費された分、減少。 | | |
| 最大リモートアクセス・ルール数 | 128 | 256 |
| 最大ユーザーロール・プロパティ数 | 64 | 128 |
| /1リモートアクセス・ルールあたり | | |
| 最大ユーザーロール・プロパティ数/装置あたり | 1,024 | 1,024 |

SSLアクセラレータ機能

| | | | |
|---------------|---|---|-------------------------------|
| IP対応 | : IPv4 | 動作モード | : ブリッジモード(プライベートLANで可)、ルータモード |
| アクセラレーション方式 | サーバサイド・アクセラレーション方式 | | |
| 暗号/復号 | プロトコル | SSL v3.0、TLS v1.0、TLS v1.1、TLS v1.2、TLS v1.3 | |
| 暗号スイート | 鍵交換 | RSA、ECDHE_RSA、ECDHE_ECDSA | |
| ※ 優先度付け定義が可能 | 暗号化 | 3DES_CBC、AES_CBC、RC4、AES_GCM、ChaCha20-Poly1305 | |
| | ハッシュ | MD5、SHA1、SHA256、SHA384 | |
| | 暗号スイート | 詳細は参考情報の暗号スイート（SSL/TLS プロトコル）を参照 | |
| サービス中継 | HTTPS、SMTPS、NNTPS、LDAPS、TELNETS、IMAPS、POP3S | | |
| HTTPリクエストヘッダー | 書き換え | Locationヘッダー、Set-Cookieヘッダー（Secure Cookie） | |
| | 設定と追加 | プロトコル種別、暗号スイート名、クライアントIPアドレス、クライアント証明書全体、クライアント証明書の特定情報 | |
| | 削除 | ヘッダー名+値 | |
| その他の機能 | クライアント認証、フォールバック動作防止 | | |

対応状況 (●：標準、○：オプション、－：未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | － | ● | ● | ● |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|---------------------------|---------|---------|
| 最大仮想SSLサーバ定義数 | 256 | |
| 最大サーバアドレス登録数/1仮想SSLサーバあたり | 32 | |
| 最大CA証明書登録数 | 2,048 | |
| 最大CA証明書グループ数 | 256 | |
| 最大CA証明書数/1CA証明書グループあたり | 256 | |
| 最大CRL数/1CA証明書グループあたり | 256 | |
| 最大CRLのURI数/1CA証明書グループあたり | 256 | |
| CA証明書の最大チェーン数 | 8 | |
| 最大サーバ証明書登録数 | 256 | |
| 同時最大SSLコネクション数 | 10,000 | 100,000 |
| 最大HTTP中継ルール数 | 8,192 | |
| 最大HTTP中継ルール数/1仮想SSLサーバあたり | 300 | |

帯域制御機能 (L2-7)

| | | | |
|-------------|---------------------------------------|--|-----------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| トラフィック分類 | 参考情報のファイアウォール機能、帯域制御機能を参照 | | |
| 方向 | アウトバウンド、インバウンド | | |
| 均等割当て | セッション単位、ノード単位、転送元IPアドレス単位、転送先IPアドレス単位 | | |
| アドミッション制御 | IPv4 | 拒否、破棄、受け入れ、リダイレクト、SIPビジー制御 | |
| パケットサイズの最適化 | IPv4 | IPフラグメンティング、IPフラグメントの無効化、TCPセグメンティング (MSS値書き換え) | |
| マーキング | IPv4 | VLANユーザプライオリティ・マーキング、ToSマーキング | |
| マッピング機能 | IPv4 | IEEE 802.1p/ToSマッピング | |
| その他の機能 | IPv4 | 優先転送、最低帯域保証、最大帯域幅 (帯域制限)、最大キューサイズのカスタマイズ、仮想回線の階層化、ポリシースケジューリング、トラフィックディスカバリー、帯域仮想専用線、フェールオーバー・マネジメント、フラグメント無効化 | |

対応状況 (●：標準、○：オプション、－：未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | － | ● | ● | ● |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|---------------|---------|---------|
| 最小制御単位 | 1kbps | 1Kbps |
| QoSフロー最大定義数 | 256 | 1,000 |
| QoSクラス最大定義数 | 2,000 | 8,000 |
| 最大マッチングルール定義数 | 4,000 | 20,000 |

| | | |
|--|--------------------|-----------|
| 最大QoSクラス階層数※ ※ QoSクラスは、最大7階層（QoSフローを含めると8階層）まで定義可能。 | 7 | 7 |
| 同時最大セッション数(WAF機能未使用時) (VE2-100 LS PLUSのみ) | 200,000 100,000 | 1,000,000 |
| 最大同時ノード数(WAF機能未使用時) (VE2-100 LS PLUSのみ) | 200,000 100,000 | 1,000,000 |
| 同時最大SIPコネクション数 | 100,000 | 250,000 |
| 最大P2Pノード管理エントリ数 | 10,000 | 60,000 |
| AudioGalaxy 同時最大ノード数 | 5,000 | 10,000 |
| BitTorrent 同時最大ノード数 | 5,000 | 10,000 |
| DirectConnect 同時最大ノード数 | 5,000 | 10,000 |
| eDonkey 同時最大ノード数 | 5,000 | 10,000 |
| FastTrack 同時最大ノード数 | 5,000 | 10,000 |
| Gnutella 同時最大ノード数 | 5,000 | 10,000 |
| Groove 同時最大ノード数 | 5,000 | 10,000 |
| Hotline 同時最大ノード数 | 5,000 | 10,000 |
| Manolito 同時最大ノード数 | 5,000 | 10,000 |
| Napster 同時最大ノード数 | 5,000 | 10,000 |
| PeerCast 同時最大ノード数 | 5,000 | 10,000 |
| PerfectDark 同時最大ノード数 | 5,000 | 10,000 |
| Share 同時最大ノード数 | 5,000 | 10,000 |
| Skype 同時最大ノード数 | 5,000 | 10,000 |
| SoftEther1 同時最大ノード数 | 5,000 | 10,000 |
| SoftEther2 同時最大ノード数 | 5,000 | 10,000 |
| SoulSeek 同時最大ノード数 | 5,000 | 10,000 |
| WinMX 同時最大ノード数 | 5,000 | 10,000 |
| Winny 同時最大ノード数 | 5,000 | 10,000 |
| 最大トラフィックディスクバリ定義数 | 12 | 12 |
| トラフィックディスクバリでの未知のTCP サービス 最大検出数 | 1,024 | 1,024 |
| トラフィックディスクバリでの未知のUDPサービス 最大検出数 | 1,024 | 1,024 |

サーバ負荷分散機能（L2-7）

| | | | |
|------------------|-----------------|--|--|
| IP対応 | ： IPv4 | 動作モード | ： ブリッジモード(プライベートLANで可)、ルータモード ※ グローバル側に負荷分散の仮想IPアドレスを設ける場合にはマルチIPサービスの契約が必要 |
| 負荷分散 | 転送方式 | IPアドレス変換、MACアドレス変換 | |
| | コンテンツ単位分散 方式 | URLベース負荷分散、HTTPヘッダー負荷分散 | |
| | サーバ分散方式 | ラウンドロビン、静的な重み付け、最小コネクション数、単純な最小コネクション数、最小ノード数、単純な最小ノード数、最小データ通信量、最小応答時間、最小サーバ負荷（CPU負荷率、メモリ使用率） | |
| | 分散対象サービス | WEBサーバ（HTTP/HTTPS）、FTPサーバ、メールサーバ（POP3/IMAP）、メールゲートウェイ（SMTP）、LDAPサーバ、TELNETサーバ、NNTPサーバ、RADIUSサーバ、プロキシサーバ、ストリーミングサーバ（PNA/RTSP/MMS）、その他TCP/UDPベースのアプリケーション | |
| | 一意性保証 | ノード単位（IPアドレス単位）、ノード単位（ネットマスク単位）、コネクション単位、cookie単位（クライアントID挿入方式、サーバID挿入方式、セッションID参照方式）、cookie・URLリライト単位、HTTPヘッダー情報単位、HTTP認証ヘッダー単位、SSLセッションID単位、APS.NETセッションID単位 | |
| サーバファーム内 故障監視 | 監視方式 | バックLAN監視（レイヤー1/2レベル・ヘルスチェック） | |
| | | 装置監視（レイヤー3レベル・ヘルスチェック） | |
| | | サービス監視（レイヤー4レベル・ヘルスチェック） | |
| | | アプリケーション監視（レイヤー7レベル・ヘルスチェック） | |
| | 故障監視オプション 機能 | URLリダイレクト 可変URLリダイレクト | URLリダイレクトのHTTPレスポンス通知 httpからhttpsに変更したURLリダイレクト のHTTPレスポンス通知 |

| | | |
|---|---|---|
| | HTTPエラーメッセージ転送 | ソーリメッセージ通知でソーリーサーバ代替 |
| | コネクション・リセット | サーバ異常検出時にTCPコネクションをリセットする |
| | コネクション・ページ | サーバ異常検出時にUDP仮想コネクションを即時に解放し、UDP通信を振り分ける |
| 拡張型故障監視 | 任意の装置の動作状況監視 | |
| | 監視方式 | サービス監視方式（レイヤー4レベル・ヘルスチェック） アプリケーション監視方式（レイヤー7レベル・ヘルスチェック：HTTP） |
| 故障復旧時の組込方式 | 自動、手動 | |
| 透過デバイス負荷分散 | 透過型キャッシュサーバ、透過型ファイアウォール、透過型SSLアクセラレーター | |
| HTTP Keep-Alive | WebサーバのKeep Alive 設定を有効にした状態で負荷分散を行う機能 | |
| 負荷分散 | 配置方法 | 透過型配置 |
| | 転送方式 | IP アドレス変換方式 |
| | HTTPメソッドの対応 | GET、POST、HEAD、PUT、TRACE、DELETE、OPTIONS |
| | WebDAVメソッドの対応 | PROPFIND、PROPPATCH、MKCOL、COPY、MOVE、LOCK、UNLOCK |
| | tcp-advance | パケットロスト多発や、高遅延、広帯域などのネットワーク環境下で、通信サービスの品質低下を抑制 |
| ※ 透過デバイス負荷分散、セッション・リカバリー機能、BackToBack 機能、Web アクセラレーション機能とは併用不可。 | | |
| BackToBack | サーバファーム内の分散対象サーバがクライアントとなり、自身が属するサーバファームの | |
| 負荷分散 | 仮想IPv4アドレスあての通信を負荷分散する機能 | |
| | 配置方法 | 透過型配置 |
| | 転送方式 | IP アドレス変換方式 |
| ※ 透過デバイス負荷分散、HTTP Keep-Alive 負荷分散との併用不可。 | | |
| Webアクセラレーション | 事前に本装置とサーバファーム内のWeb サーバとの間にTCPコネクションを確立することで、Web サーバの負荷を軽減する機能 | |
| | Webサーバ | HTTP/1.1 |
| | 配置方法 | 透過型配置 |
| | 転送方式 | IP アドレス変換方式 |
| | HTTP メソッドの対応 | GET、POST、HEAD、PUT、TRACE、DELETE、OPTIONS |
| | WebDAVメソッドの対応 | PROPFIND、PROPPATCH、MKCOL、COPY、MOVE、LOCK、UNLOCK |
| | tcp-advance | パケットロスト多発や、高遅延、広帯域などのネットワーク環境下で、Webアクセラレーション機能の通信サービスの品質低下を抑制 |
| ※ 透過デバイス負荷分散およびセッション・リカバリー機能との併用不可。 | | |
| セッションリカバリー | 一定回数再試行されてもサーバ未応答の場合は、サーバ異常またはサーバ高負荷と判断し、別の正常なサーバに転送し直す機能 | |
| | HTTP 応答に含まれるステータスコードを検査し、エラーを検出すると、別のサーバに転送する機能 | |
| ※ Web アクセラレーション機能、HTTP Keep-Alive負荷分散との併用不可 | | |
| ポート多重制御 | 1台の物理サーバ上で動作しているポート番号の異なるアプリケーションのそれぞれを仮想的なサーバと見なして負荷分散を行う機能。 | |
| | 転送方式 | IP アドレス変換方式 |
| サーバ保守制御 | 保守対象のサーバを利用者に被害を与えることなくスムーズにサーバファームから切り離す機能 | |
| | 保守への移行 | 手動（コマンド） 保守開始／保守移行時間／保守終了 自動（スケジュール） メンテナンス期間の登録 |
| | オプション機能 | URLリダイレクション、可変URLリダイレクション、HTTPエラーメッセージ転送、コネクション・リセット、コネクション・ページ |
| アクセス制限 | サーバファーム単位、分散対象サーバ単位に受け入れ可能な「コネクション数」や「ノード数」を設定 | |
| | 制限可能なアクセス数 | ノード数、コネクション数 |
| | オプション機能 | URLリダイレクション、可変URLリダイレクション、HTTPエラーメッセージ転送 |
| バックアップ・サーバ | 稼働中の分散対象サーバが指定された台数分だけ故障または高負荷状態になると、1台のバックアップ・サーバが分散対象に組み込まれて動作。複数台のバックアップ・サーバは優先度で制御。 | |
| スロースタート制限 | サーバの負荷状況を監視しながら、約30秒でほかの分散対象サーバ同等の振り分け状態になるように負荷を分散 | |

| 対応状況（●：標準、○：オプション、－：未サポート） | | | | |
|----------------------------|----|---------|----|---------|
| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
| サポート状況 | － | － | ● | ● |

| 諸元(最大値) | | |
|------------------------|---|---------|
| ソフトウェアタイプ | VE2-100 | VE2-220 |
| 最大サーバファーム数 | 16 | 128 |
| 最大サーバ数 | 256 | 1,024 |
| 最大マッチングルール数 | 16,000 | 30,000 |
| 最大仮想ポート数 | コマンドにより、[ポート数/プロトコル] の書式でポート設定を行う。文字列が950文字（カンマを含む）に納まる範囲でポート数設定可能。 | |
| 最大実ポート数 | コマンドにより、[ポート数/プロトコル] の書式でポート設定を行う。文字列が950文字（カンマを含む）に納まる範囲でポート数設定可能。 | |
| バックLAN監視最大数(分散対象サーバごと) | 4 | 4 |

HTTP/HTTPSコンテンツ圧縮機能

| | | | |
|--------|---|---|-------------------------------|
| IP対応 | ： IPv4 | 動作モード | ： ブリッジモード(プライベートLANで可)、ルータモード |
| 利用通信 | HTTP通信、HTTPS通信（SSLアクセラレーター機能と連携） | | |
| サポート機能 | 圧縮データ形式 | gzip、deflate | |
| | 圧縮フィルター条件 | リクエストURI、ユーザーエージェント、コンテンツタイプ、最小コンテンツサイズ | |
| 統計情報 | HTTPレスポンス総計、圧縮HTTPレスポンス数（HTTP 1.0/HTTP 1.1レスポンス数）、非圧縮HTTPレスポンス数（HTTP解析エラー、フィルター条件、その他エラー）、コンテンツタイプごとのHTTP圧縮レスポンス統計（圧縮前バイト総数、圧縮後バイト総数、圧縮率） | | |

| 対応状況（●：標準、○：オプション、－：未サポート） | | | | |
|----------------------------|-----------|---------|----|---------|
| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
| サポート状況 | ●(HTTPのみ) | ● | ● | ● |

| 諸元(最大値) | | |
|---|---------|---------|
| ソフトウェアタイプ | VE2-100 | VE2-220 |
| コンテンツ圧縮ルール数 | 30 | |
| 1圧縮フィルター条件に登録可能な圧縮対象、非圧縮対象の最大数（圧縮対象、非圧縮対象の合計） | 50 | |
| 仮想HTTP圧縮サーバ定義数 | 256 | |
| 最大同時HTTPコンテンツ圧縮コネクション数（HTTP） | 125,000 | |
| 最大同時HTTPSコンテンツ圧縮コネクション数（HTTPS） | 10,000 | 100,000 |

ユーザー認証機能 ※装置管理のユーザー認証で利用可能

| | | | |
|-----------|---|-------|-----------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| 認証方式 | 固定パスワード（PAP方式）、固定パスワード（CHAP方式）、固定パスワード（MS-CHAP-V2方式（L2TP/AO952/IPsec時）、EAP方式（L2TP/I957かつRADIUSサーバ連携時） | | |
| ユーザー認証/管理 | ローカル認証、RADIUSサーバ連携、LDAPサーバ連携、TACACS+サーバ連携 | | |
| その他の機能 | 認証許可条件検証（ユーザ有効期間、パスワード有効日数、ロックアウト）、ユーザー正当性検証、ユーザーロール選択条件検証（ユーザーロール有効期限、クライアントのIPアドレス）、ユーザーロールベースのアクセス制御、パスワードポリシー設定 | | |

| 対応状況（●：標準、○：オプション、－：未サポート） | | | | |
|----------------------------|----|---------|----|---------|
| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
| サポート状況 | ● | ● | ● | ● |

| 諸元(最大値) | | | |
|---|-----------------------|-----------------------|---------------------------|
| ソフトウェアタイプ | VE2-100 SC/SC PLUS | VE2-220 SC/SC PLUS | VE2-100/220 LS/LS PLUS |
| 最大ユーザー定義数 (user) ※ admin ユーザーは、最大ユーザー定義数に含まない。 | 1,000 | 2,000 | 100 |
| 最大ユーザーロール定義数 (user-role) | 1,000 | 2,000 | 16 |
| 最大ユーザーグループ定義数 (user-group) | 500 | 1,000 | 16 |
| 最大スケジュールマッチングルール定義数 /1ユーザーあたり | 10 | 10 | 10 |
| 最大ユーザーマッチングルール定義数※ /1ユーザーロールあたり ※ administratorやremoteのユーザーロールに定義されたmatch user adminは含まない。 | 255 | 255 | 31 |
| 最大ユーザーグループマッチングルール定義数 /1ユーザーロールあたり | 128 | 128 | 16 |
| 最大スケジュールマッチングルール定義数 /1ユーザーロールあたり | 10 | 10 | 10 |
| 最大接続元IPマッチングルール定義数 /1ユーザーロールあたり | 10 | 10 | 10 |
| 最大ユーザーマッチングルール定義数 /1ユーザーグループあたり | 255 | 255 | 31 |
| 最大ユーザーグループマッチングルール定義数 /1ユーザーグループあたり | 127 | 127 | 15 |
| 最大ユーザーグループ階層数 | 3 | | 3 |
| 最大ユーザーマッチングルール定義数/装置あたり | 3,000 | 6,000 | 200 |
| 最大ユーザーグループマッチングルール定義数 /装置あたり | 1,000 | 2,000 | 100 |
| 最大認証データベース定義数 | 64 | 64 | 64 |
| 最大正規表現ユーザー定義数 /1認証データベースあたり | 10 | 10 | 10 |
| 最大IPアドレスプール定義数 | 500 | 2,000 | - |
| コマンドリスト定義数/1ユーザーロールあたり | 256 | 256 | 256 |
| コマンドリスト定義数/装置あたり | 1,000 | 1,000 | 1,000 |

ネットワークサービス機能

IP対応 : IPv4 動作モード : ブリッジモード(プライベートLANで可)、ルータモード
機能 DHCPサーバ、DNSサーバ、DNSリレー

対応状況 (● : 標準、○ : オプション、- : 未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | ● | ● | - | - |

| 諸元(最大値) | | |
|-------------------------------|--------------|--------------|
| ソフトウェアタイプ | VE2-100 | VE2-220 |
| DNSサーバ/DNSリレー | | |
| 最大ゾーン定義数 | 32 | 64 |
| ゾーンあたりの最大サブドメインのネームサーバ 定義数 | 64 | 128 |
| ゾーンあたりの逆引きゾーンの最大定義数 | 8 | 8 |
| 逆引きゾーンの子階層最大参照数 | 31 | 63 |
| ゾーンあたりの最大ホスト定義数 | 256 | 512 |
| キャッシュサイズ上限値 | 10,240 キロバイト | 10,240 キロバイト |
| 最大転送先ネームサーバ (DNSサーバ) 定義数 | 10 | 10 |

高信頼化機能

| | | | |
|----------|------|----------------|---------------------------------|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| ホットスタンバイ | | 構成 | 2台での冗長構成 (Active-Sutandby) |
| | | 監視プロトコル | VRPベースの独自 |
| | | 付加機能 | 上位アプリケーション維持、RIP制御 (仮想IPでRIP送信) |
| | | ※プライベートLANのみ | |
| その他の機能 | | ゲートウェイ・フェールセーフ | |

対応状況 (●：標準、○：オプション、－：未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | ● | ● | ● | ● |

運用管理/保守機能

| | | | |
|---------------|------|---|---|
| IP対応 | IPv4 | 動作モード | ブリッジモード(プライベートLANで可)、ルータモード |
| コンソール | | 日本語Web-GUI (HTTPS)、CLI (SSHv2、Telnet) | |
| Webコンソール | | サポートOS | Windows 8.1 (32/64bit)、Windows 10 (32/64bit)、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 |
| | | Webブラウザ | Internet Explorer 11(32bit) |
| 構成定義 | | インターフェースの動的定義変更、構成定義複数世代管理、定義情報退避・復元、コンフィグドライブ | |
| 保守インターフェース | | ニフクラ コンソール、Telnetサーバ、SSHサーバ、SSHクライアント、FTPクライアント、HTTPサーバ機能 | |
| 保守形態 | | ニフクラ コンソール、remote | |
| 運用管理 | | NTP | クライアント |
| | | ※ NTP Version3、またはNTP Version4をサポートしたNTPサーバに接続可能 (最大4台) | |
| | | Syslog送信 | クライアント ※ 最大3台の異なるSyslogサーバに転送可能 |
| | | イベント通知 | メール転送、SNMPトラップ転送、ログファイル転送 |
| | | ログ解析 | テキストファイル出力 (IPCOM標準形式)、レポートングツール (Security Reporting Center) との連携 (WELF形式) |
| | | ログ解析ツール | IPCOM標準形式のログ情報の解析 (メッセージ数のカウント) |
| | | 管理ツール | Systemwalker Centric Manager連携 |
| 保守機能 | | IPホスト機能 | ping、traceroute |
| | | ログ情報 | エラーログ、メッセージログ、トラップログ、コマンドログ、アカウントログ、セッションログ、ウイルスログ、プロキシログ |
| | | ※ 各ログの詳細フォーマットは保守ガイドに記載されています。 | |
| | | 保守情報採取 | メモリダンプ、プロセスダンプ、ファンクショントレース、ネットワークトレース (IPCOMでのSSLの復号直後・暗号直前)、プロトコルイベントトレース、ローグ一括採取機能 |
| | | リアルタイムモニタ | システム情報モニタ、ネットワークモニタ (インタフェース、ARPキャッシュ、ブリッジ、DHCPクライアント、PPPoE、ネイバーキャッシュ)、サーバ負荷分散モニタ、QoSモニタ、ファイアウォール、ルートモニタ、IPsecVPNモニタ、P2Pモニタ、DHCPサーバモニタ、TCPゲートウェイモニタ、DHCPサーバモニタ、TCPゲートウェイモニタ、リンク負荷分散モニタ、アンチウイルスモニタ、Webコンテンツ・フィルタリングモニタ、シグネチャー型IPSモニタ、ログ情報モニタ |
| SNMPエージェント | | プロトコル | SNMPv1、SNMPv2c、SNMPv3 |
| | | SMI | SMIv2 (SMIv1を一部含む) |
| | | MIB | 標準 MIB (MIB- II)、snmpV2 MIB、拡張 MIB (Private MIB) |
| | | ※ SNMPv3の認証および暗号アルゴリズムのサポート範囲 | 認証アルゴリズム HMAC-MD5-96、HMAC-SHA-96 暗号アルゴリズム DES-CBC、AES128-CFB |
| 簡易ロギングユーティリティ | 機能 | syslogサーバツール (受信フィルター機能、ファイル管理機能、ビューア機能) | |
| | | サポートOS(32bit) | Windows 8.1 (32/64bit)、Windows 10 (32/64bit)、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 |
| | | Syslogメッセージ形式 | RFC3164 The BSD Syslog Protocol準拠 |

対応状況 (● : 標準、○ : オプション、- : 未サポート)

| ソフトウェア名称 | SC | SC PLUS | LS | LS PLUS |
|----------|----|---------|----|---------|
| サポート状況 | ● | ● | ● | ● |

諸元(最大値)

| ソフトウェアタイプ | VE2-100 | VE2-220 |
|--|--------------------|-----------|
| ニフクラ コンソール/CLI 最大同時接続数 | 1 | |
| コマンド操作端末 (LAN接続/CLI) 最大同時接続数※ ※ 最大同時接続数はtelnet接続とssh接続とWebブラウザ接続とダウンロード版モニタ接続の合計数です。 | 4 | 6 |
| Webブラウザ端末/ダウンロード版モニタ端末 (LAN接続/GUI) 最大同時接続数※ ※ 最大同時接続数はtelnet接続とssh接続とWebブラウザ接続とダウンロード版モニタ接続の合計数です。 | 4 | 6 |
| 最大一時保存構成定義ファイル数 | 6 | |
| 最大同時ログファイル保存数 | 3 | |
| 最大同時ファンクショントレースファイル保存数 | 3 | |
| 最大同時プロトコルイベントトレース自動書き出しファイル保存数 | 3 | |
| 最大同時プロトコルイベントトレース手動書き出しファイル保存数 | 3 | |
| 最大同時ネットワークトレースファイル保存 | 3 | |
| 最大CLI履歴管理数 | 100 | |
| 最大ログ情報表示可能数 | 最新1,000件 | |
| 最大ログ情報保存件数※1 | | |
| エラーログ最大保存件数 | 64,000 | |
| アカウントログ最大保存件数 | 64,000 | |
| コマンドログ最大保存件数 | 64,000 | |
| トラップログ最大保存件数 | 64,000 | |
| メッセージログ最大保存件数 | 800,000 | |
| セッションログ最大保存件数 | 6,400,000 | |
| ウイルスログ最大保存件数 | 35,000 | |
| プロキシログ最大保存件数 | 5,592,000 | |
| WAFログ最大保存件数 | 1,600,000 | |
| 再送待ちログ最大保存件数※2 | 4,096,000 | |
| ※1 装置に保存できるイベントログの最大件数。 それぞれのイベントログ情報は文字数 (バイト数) が異なるので、この件数 (1メッセージあたり256バイトで換算。プロキシログ、ウイルスログについては1メッセージ当り300バイトで換算) は、目安として見る。最大保存件数を超えるイベントログ情報は、古いイベントログ情報から順番に最新のイベントログ情報で上書きする。 | | |
| ※2 それぞれの再送待ちログ情報は文字数 (バイト数) が異なるので、この件数 (1メッセージあたり256 バイトで換算) は、目安として見る。最大保存件数を超える再送ログ情報は、保存せず破棄する。 | | |
| ログ保存容量 | | |
| エラーログ最大保存容量 | 16,384,000 バイト | |
| アカウントログ最大保存容量 | 16,384,000 バイト | |
| コマンドログ最大保存容量 | 16,384,000 バイト | |
| トラップログ最大保存容量 | 16,384,000 バイト | |
| メッセージログ最大保存容量 | 204,800,000 バイト | |
| セッションログ最大保存容量 | 1,638,400,000 バイト | |
| ウイルスログ最大保存容量 | 10,500,000 バイト | |
| プロキシログ最大保存容量 | 1,638,400,000 バイト | |
| WAFログ最大保存容量 | 409,600,000 バイト | |
| 再送待ちログ最大保存容量 | 1,048,576,000 バイト | |
| 最大ファンクショントレースメモリサイズ | 1,024-10,240 キロバイト | |
| 最大プロトコルイベントトレース自動書き出しメモリサイズ | 1,024 キロバイト | |
| 最大プロトコルイベントトレース手動書き出しメモリサイズ | 1,024 キロバイト | |
| 最大ネットワークトレースメモリサイズ | 16 メガバイト | 128 メガバイト |
| 最大NTPサーバ定義 (登録) 数 | 4 | |
| 最大ロギングルール (rule logging) 定義数 | 10 | |

ファイアウォール機能、帯域制御機能

フィルター条件

| | |
|------|---|
| IPv4 | 隣接ルータのIPv4アドレス、隣接ルータのホスト（IPv4アドレス）、接続先IPv4アドレス、接続先のインターフェースIPv4アドレス、接続元IPv4アドレス、接続元のインターフェースIPv4アドレス、接続先または接続元のIPアドレス、接続先または接続元のインターフェースIPv4アドレス、接続先ホスト（IPv4アドレス）※、接続元ホスト（IPv4アドレス）、接続元ホスト（IPv4アドレス）、接続先または接続元ホスト（IPv4アドレス）、ICMPセッション、DNSクエリホスト名、ユーザーロール、Sun RPC、MS RPC、P2Pアプリケーション、メディアタイプ、ストリーミング・アプリケーション バイナリパターン、仮想インターフェース名、あて先MACアドレス、送信元MACアドレス、転送先および転送元MACアドレス（または範囲）、転送先のインターフェースMACアドレス、転送元のインターフェースMACアドレス、転送先および転送元のインターフェースMACアドレス、受信物理インターフェース、受信仮想インターフェース、VLAN識別子、VLANプライオリティ、接続先のインターフェースIPv4アドレス、接続元のインターフェースIPv4アドレス、接続先または接続元のインターフェースIPv4アドレス、接続先のホストグループ、接続元のホストグループ、接続先または接続元のホストグループ、接続先ポート、接続元ポート、プロトコル、接続先または接続元のポート、サービスタイプ（ToS）、HTTPメソッド、FTPコマンド、POP3コマンド、SMTPコマンド、HTTPバージョン番号、HTTP URI、HTTPヘッダーのタグ、HTTPボディ部のタグ、HTTP URLの長さ、メールヘッダーのタグ、メールボディ部のタグ、アドレスファミリー、接続先サーバ名、ダイナミックポート・アプリケーション、フィルタ条件グループ、アプリケーション辞書、国名コード |
|------|---|

※ ホスト名にはFQDNを設定出来ます。なお、ホスト名にワイルドカード文字（*）として指定出来ます。（DNSパケットを解析出来る環境の場合に限ります。）

ダイナミックポートアプリケーション

| | |
|------|---|
| IPv4 | FTP、TFTP、H.323、SIP/RTP、RTSP/RTP、MMS、PNA、CUseeMe、StreamWorks、RSH、SUN-RPC、MS-RPC、SQL*Net V2 |
|------|---|

メディアタイプ

| | |
|------|--|
| IPv4 | H.323、SIP/RTP、FNA on TCP/IP、FNLAN、TN6680、TN3270、TN5250 |
|------|--|

ストリーミングアプリケーション

| | |
|------|---|
| IPv4 | MS-MMS/HTTP、RN-RTSP-RDT/HTTP、MM-RTMP/TCP、MM-RTMP/HTTP |
| | <ul style="list-style-type: none"> ・ MMS : Microsoft Media Service Protocol ・ RDT : RealNetworks Real Data Transport Protocol ・ RTMP : Macromedia Real Time Messaging Protocol |

P2Pアプリケーション

| | | |
|------|---------------|--|
| IPv4 | e-Donky | eMule、eDonky2000プロトコル互換P2Pアプリケーション |
| | FastTrack | KaZaA、KaZaA Lite、KaZaA Lite K++、iMesh、Weraz P2P |
| | Gnutella | Shareaza、Gnucleus、XoloX、LimeWire、BearShare、Morpheus、NeoNapster、Gnotella、Ares Gold、Cabos、LemonWire、Gnutellaプロトコル互換P2Pアプリケーション |
| | Napster | Xnap、WinMX（OpenNap）、Napsterプロトコル互換P2Pアプリケーション |
| | WinMX | WinMX 3.x |
| | Winny | Winny2 |
| | SoftEther1.0 | SoftEther1.0 |
| | SoftEther2.0 | PacketiX VPN2.0、PacketiX VPN3.0 |
| | Share | Share |
| | Soulseek | Soulseek |
| | BitTorrent | BitTorrent、Shareaza、Azureus、BitComet、µTorrent、BitSpirit、Turbo Torrent、BitBuddy、eXeem |
| | PeerCast | PeerCast |
| | PerfectDark | PerfectDark 1.07 |
| | Skype | Skype1.x、Skype2.x、Skype3.x、Skype 4.x、Skype5.0.x、Skype5.3.x |
| | AudioGalaxy | AudioGalaxy Rhapsody |
| | DirectConnect | DirectConnect、DC++ |
| | Groove | Groove Workspace |
| | HotLine | Hotline Connect、SilverWing、Hotline互換P2Pアプリケーション |
| | Manolite | Blubster、Piolet |

| アプリケーション辞書詳細 ※2021年6月現在 | | | |
|---|--------|--------------------------------|-------|
| グループ名 | グループ番号 | | 種類 |
| Networking | 10 | ネットワーキング | 500 |
| Business System | 20 | ビジネス・システム、アプリケーション | 295 |
| Management | 30 | マネージメント・プロトコル、アプリケーション | 386 |
| Security | 40 | セキュリティ・プロトコル、アプリケーション | 159 |
| General Internet | 50 | コラボレーション・システム、アプリケーション | 827 |
| Multimedia | 60 | マルチメディア・プロトコル、アプリケーション | 614 |
| Others | 70 | その他 | 0 |
| Custom Application | 90 | ユーザー定義のカスタムアプリケーション辞書が使用するグループ | 0 |
| 合計 | | | 2,781 |
| アプリケーション辞書の更新 SupportDesk-Web（お客様専用ホームページ）から入手し、反映が可能 | | | |

| | | | |
|---|---------|----------------|--|
| 国/地域別 IPアドレスリスト ※2021年6月現在 | | | |
| 国/地域別 IP アドレスリスト数 | 国/地域数 | 241 | |
| | IPアドレス数 | IPv4 : 113,387 | |
| 国/地域別 IP アドレスリストの更新 SupportDesk-Web（お客様専用ホームページ）から入手し、反映が可能 | | | |

アノマリ型IPS攻撃防御一覧

| 攻撃防御種類一覧 | |
|----------|---|
| IPv4 | 不正IPパケット（不正なIPヘッダー長、不正なIPヘッダー長、不正なIPバージョン番号、不正なIP チェックサム値、不正な送信元IPアドレス、不正な送信先IP アドレス、未定義なプロトコル番号、未定義なオプション）、不正IPオプション（不正な形式のIPオプション、許可されないIPオプション）、不正ARPパケット（不正なARPパケット長、不正なARPパケット形式）、ネットワークアドレス攻撃 不正TCPパケット（不正なTCPヘッダー長、不正なTCPチェックサム値、不正なTCPポート番号、不正なTCP SYNパケット、不正なTCP制御フラグの組み合わせ、不正なTCPオプション、許可されないTCPオプション、不正なTCP シーケンス）、不正UDPパケット（不正なUDPヘッダー長、不正なUDPチェックサム値、不正なUDPポート番号）、不正ICMPパケット（不正なICMPパケット長、不正なICMPチェックサム値）、TCPポートスキャン、UDPポートスキャン、ホストスキャン、SYN Flood攻撃、ICMP Flood攻撃、UDP Flood攻撃、UDP Bomb攻撃、Very Small IP Fragment攻撃、Too Many IP Fragment 攻撃、Fragmented ICMP攻撃、Fragmented IGMP攻撃、Empty Fragment攻撃、Overlapped Fragment攻撃、Large ICMP攻撃、Ping of Death攻撃、IP Spoofing攻撃、Land攻撃、Smurf攻撃、Unrequested ICMP Echo Reply攻撃、Fraggle攻撃、FTP Bounce 攻撃、Snork攻撃、WinNuke攻撃、URL Overflow攻撃、Spam Mail攻撃、MIME Overflow 攻撃、Very Small TCP Segment攻撃、未知の攻撃/探索（利用者指定のトラップ） |

暗号スイート（SSL/TLS プロトコル）

| SSL v3.0の暗号スイート | | | |
|--------------------------------------|-------------------|------------|---------|
| 暗号スイート名称 | 鍵交換 | 暗号化 | メッセージ認証 |
| SSL_RSA_WITH_3DES_EDE_CBC_SHA | RSA (4096) | 3DES (168) | SHA1 |
| SSL_RSA_WITH_RC4_128_MD5 | RSA (4096) | RC4 (128) | MD5 |
| SSL_RSA_WITH_RC4_128_SHA | RSA (4096) | RC4 (128) | SHA1 |
| SSL_RSA_WITH_AES_128_CBC_SHA | RSA (4096) | AES (128) | SHA1 |
| SSL_RSA_WITH_AES_256_CBC_SHA | RSA (4096) | AES (256) | SHA1 |
| SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDHE_RSA (384) | AES (128) | SHA1 |
| SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDHE_RSA (384) | AES (256) | SHA1 |
| SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | ECDHE_ECDSA (384) | AES (128) | SHA1 |
| SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | ECDHE_ECDSA (384) | AES (256) | SHA1 |
| TLS v1.0の暗号スイート | | | |
| 暗号スイート名称 | 鍵交換 | 暗号化 | メッセージ認証 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | RSA (4096) | 3DES (168) | SHA1 |
| TLS_RSA_WITH_RC4_128_MD5 | RSA (4096) | RC4 (128) | MD5 |
| TLS_RSA_WITH_RC4_128_SHA | RSA (4096) | RC4 (128) | SHA1 |

| | | | |
|--------------------------------------|----------------------|-----------|------|
| TLS_RSA_WITH_AES_128_CBC_SHA | RSA (4096) | AES (128) | SHA1 |
| TLS_RSA_WITH_AES_256_CBC_SHA | RSA (4096) | AES (256) | SHA1 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDHE_RSA (384) | AES (128) | SHA1 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDHE_RSA (384) | AES (256) | SHA1 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | ECDHE_ECDSA (384) | AES (128) | SHA1 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | ECDHE_ECDSA (384) | AES (256) | SHA1 |

TLS v1.1の暗号スイート

| 暗号スイート名称 | 鍵交換 | 暗号化 | メッセージ認証 |
|--------------------------------------|----------------------|------------|---------|
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | RSA (4096) | 3DES (168) | SHA1 |
| TLS_RSA_WITH_RC4_128_MD5、 | RSA (4096) | RC4 (128) | MD5 |
| TLS_RSA_WITH_RC4_128_SHA | RSA (4096) | RC4 (128) | SHA1 |
| TLS_RSA_WITH_AES_128_CBC_SHA | RSA (4096) | AES (128) | SHA1 |
| TLS_RSA_WITH_AES_256_CBC_SHA | RSA (4096) | AES (256) | SHA1 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDHE_RSA (384) | AES (128) | SHA1 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDHE_RSA (384) | AES (256) | SHA1 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | ECDHE_ECDSA (384) | AES (128) | SHA1 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | ECDHE_ECDSA (384) | AES (256) | SHA1 |

TLS v1.2の暗号スイート

| 暗号スイート名称 | 鍵交換 | 暗号化 | メッセージ認証 |
|---|----------------------|------------------|---------|
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | RSA (4096) | 3DES (168) | SHA1 |
| TLS_RSA_WITH_RC4_128_MD5、 | RSA (4096) | RC4 (128) | MD5 |
| TLS_RSA_WITH_RC4_128_SHA | RSA (4096) | RC4 (128) | SHA1 |
| TLS_RSA_WITH_AES_128_CBC_SHA | RSA (4096) | AES (128) | SHA1 |
| TLS_RSA_WITH_AES_256_CBC_SHA | RSA (4096) | AES (256) | SHA1 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 | RSA (4096) | AES (128) | SHA256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | RSA (4096) | AES (256) | SHA256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 | RSA (4096) | AES_GCM (128) | AEAD |
| TLS_RSA_WITH_AES_256_GCM_SHA384 | RSA (4096) | AES_GCM (256) | AEAD |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDHE_RSA (384) | AES (128) | SHA1 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDHE_RSA (384) | AES (256) | SHA1 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDHE_RSA (384) | AES (128) | SHA256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDHE_RSA (384) | AES (256) | SHA384 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDHE_RSA (384) | AES_GCM (128) | AEAD |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDHE_RSA (384) | AES_GCM (256) | AEAD |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | ECDHE_ECDSA (384) | AES (128) | SHA1 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | ECDHE_ECDSA (384) | AES (256) | SHA1 |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | ECDHE_ECDSA (384) | AES_GCM (128) | AEAD |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | ECDHE_ECDSA (384) | AES_GCM (256) | AEAD |

●仕様は改良のため予告なく変更することがありますので予めご了承ください。