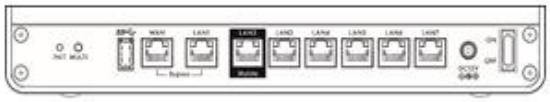
HOME-UNIT3 のセキュリティ機能について

HOME-UNIT3 は、HOME においてサクサ社製 UTM「HOME-UNIT2」の後継となる標準 UTM です。

◎本体外観

(本体前面)



(本体背面)

◎本体性能

※HOME-UNIT3/HOME-UNIT3 Pro については、本体は同一筐体で、許諾された収容 IP 端末数のみが異なります。

機種	HOME-UNIT3	HOME-UNIT3 Pro
メーカ	SAXA	SAXA
外形寸法	29.1×17.7×4.3	29.1×17.7×4.3
重量	2.3kg	2.3kg
消費電力	15W	15W
雷サージ電流対策　(※1	○	○
バイパスポート	○	○
LAN ポート数	6	6
同時セッション数	非公開	非公開
新規セッション/秒	非公開	非公開
収容 IP 端末数(ライセンス許諾数)	30 台	100 台
導入形態	ブリッジ	ブリッジ
リモートアクセス　(※2	○	○
ＶＰＮ（他拠点接続）　(※2	○	○
UTM 機能	○（ブリッジ型）	○（ブリッジ型）
アンチウイルス	○	○
エンジン	Kaspersky	Kaspersky
検出方式	プロキシベース	プロキシベース
ヒューリスティック　(※3	○	○
サンドボックス　(※3	○	○
スキャンサイズ上限 ※初期値	なし ※10MB 以上は先頭 10MB のみ検疫	なし ※10MB 以上は先頭 10MB のみ検疫
スループット	200Mbps	200Mbps
対応プロトコル	HTTP、FTP、IMAP、POP3、SMTP POP3s、SMTPs(※4	HTTP、FTP、IMAP、POP3、SMTP POP3s、SMTPs(※4
Web フィルタリング	○	○
エンジン	ALSI	ALSI
HTTPS 対応	○	○
カテゴリ数	144	144

標準選択カテゴリ　（※5	犯罪暴力コンテンツ アダルトコンテンツ 違法コンテンツ ゲームサイト ショッピング・オークション ウェブメール ギャンブルサイト チャットサイト ダウンロードサイト 出会い系サイト 転職サイト SNS サイト P2P ファイル共有サイト	犯罪暴力コンテンツ アダルトコンテンツ 違法コンテンツ ゲームサイト ショッピング・オークション ウェブメール ギャンブルサイト チャットサイト ダウンロードサイト 出会い系サイト 転職サイト SNS サイト P2P ファイル共有サイト
アンチスパム（※6	○	○
検出方式	**タグ付**	**タグ付**
エンジン	**Kaspersky**	**Kaspersky**
対応プロトコル	**SMTP、POP3、IMAP POP3s、SMTPs(※4**	**SMTP、POP3、IMAP POP3s、SMTPs(※4**
IPS	○	○
エンジン	**メーカオリジナル**	**メーカオリジナル**
アプリケーションコントロール	○	○
エンジン	**メーカオリジナル**	**メーカオリジナル**
禁止選択カテゴリ	**ゲームサイト インスタンスメッセージ P2P ファイル共有サイト SNS サイト ウェブメール**	**ゲームサイト インスタンスメッセージ P2P ファイル共有サイト SNS サイト ウェブメール**
稼働監視　（※7	○	○
レポート　（※8	○	○
月次レポートのメール送信	○	○
生ログ送付	×	×
レポートサイト	○	○
ローカルログ閲覧	×	×
アラート通知	○（日本語）	○（日本語）
LED 通知	○	○
情報漏洩防止機能（※9	○	○
添付ファイル自動 ZIP 暗号化	○	○
誤送信防止	○	○
カスタマイズ対応	○	○
IP アドレスグループ等によるダブルポリシー	○	○
Web フィルタリングの閲覧許可／ログ設定	○	○
Web フィルタリングのカテゴリ追加	○（※10	○（※10
Web フィルタリング・アンチスパム ホワイトリストお客様追加機能	△（※11	△（※11

◎仕様詳細

各種機能の競合について

HOME-UNIT3 と他のセキュリティ製品を合わせて利用する場合、機能の競合により、アンチスパム機能などが正常に動作しない場合があります。正常動作が確認できない場合は、ご利用開始後に HOME-CC にご相談ください。

IPv6 環境での利用について

IPv6 の環境において HOME-UNIT3 をご利用いただくことはできますが、通信の内容や種類によっては検疫がなされない場合があります。お客様都合により IPv4 から IPv6 への環境変化が生じた場合、提供機能の差異評価等のサポートはいたしかねます。
なお、IPv4 over IPv6 通信については、HOME-UNIT3 配下の通信は IPv4 で行いますので、IPv4 環境同様に本機能が利用できます。

- **メーカによる動作確認結果**

機能	対応	注意事項
アンチウイルス	○	通信の内容/種類によっては検疫されない場合があります。
Web フィルタリング	×	接続先のサイトによっては検疫ができる場合があります。
アンチスパム	○	通信の内容/種類によっては検疫されない場合があります。
IPS	○	通信の内容/種類によっては検疫されない場合があります。
アプリケーションコントロール	○	通信の内容/種類によっては検疫されない場合があります。
添付ファイル自動 ZIP 暗号化機能 **メール誤送信防止機能**	**－**	利用不可
POP3S/SMTPS に対する **SSL インスペクション機能**	**－**	利用不可

- **IPv6 環境でご利用する際の注意点**
  - IPv6 環境下では IP アドレス指定での検疫除外ポリシー等が利用頂けません。IPv4 から IPv6 への切替された場合、ポリシーを踏襲できない場合があります。
  - IPv6 環境下では NAT モードでの利用はできません。（HOME-UNT3 を使った拠点間 VPN、リモートアクセスをご利用いただくことはできません。）

(※1：雷サージ電流対策

HOME-UNIT3 は IEC61000-4-5 に準拠した試験をクリアしており、落雷等で生じるサージ電流の対策が実施されています。
※ただし、落雷によって本体が故障しないことを保証するものではありません。

(※2：リモートアクセス／ＶＰＮについて

レンタルモデルの HOME-UNIT3 ではリモートアクセス／ＶＰＮ機能をご利用いただけます。
ただし、IPv6 環境ではご利用になれません。

(※3： ヒューリスティック／サンドボックスについて

HOME-UNIT3 はアンチウイルスエンジンである Kasperskey のヒューリスティック検知とサンドボックス機能を利用することでゼロデイ攻撃に対してもダブルチェックで対応できます。

※ヒューリスティック検知とは、プログラムの構造や動作（振る舞い）を解析することでウイルス判定する検知方式です。
※サンドボックス機能とは、仮想環境内で、不審なプログラムを動作させ、ウイルス判定する機能です。
※ゼロデイ攻撃とは、セキュリティホールが「一般的に知られる前/対策が施される前」にハッカーやクラッカーがおこなう攻撃です。

(※4：POP3S/SMTPS、STARTTLS に対する SSL インスペクション機能について

SSL インスペクション機能を有効化することで、SSL/TLS で暗号化されたメール通信に対してアンチウイルス検疫、アンチスパム検疫、添付ファイル自動 ZIP 暗号化機能、誤送信防止機能を利用することができます。ただし、利用にはクライアント端末への証明書のインポート作業やメーラの設定変更などの作業が必要となります。
本機能を有効化した場合、推奨ユーザー数の低減や通信速度の低減が見込まれます。設定を希望する場合は、HOME-CC にご相談ください。
また、証明書のインストールや各種設定作業はお客様ご自身で実施いただきます。

◎HOME-UNIT3 SSL インスペクション機能 動作確認 OS 及びメールソフト ※2020 年 1 月 29 日時点

OS	バージョン	メールソフト
Windows	8.1	Outlook2016/Outlook2013/Thunderbird
	10	Outlook2016/Outlook2013/Thunderbird
Mac OS X	10.12 (Sierra)	Mac 標準メールソフト(v10.x)
	10.13 (High Sierra)	Mac 標準メールソフト(v11.x)
	10.14 (Mojave)	Mac 標準メールソフト(v12.x)
	10.15 (Catalina)	Mac 標準メールソフト(v13.x)
iOS	10	iOS 標準メールアプリ
	11	
	12	
	13	
Android	7	Android 標準メールアプリ
	8	
	9	
	10	

(※5：Web フィルタリング機能 標準選択カテゴリについて

HOME-UNIT3 では、Web 登録時に 14 のカテゴリについて、Web フィルタリング適用指定が可能です。
主要なカテゴリが網羅されていますので、オプションの必要性が最小化します。

●追加で選択可能なオプション扱いのカテゴリ一覧

金融・経済指数・マーケット情報、保険商品の申込、金融商品・サービス、保険、銀行
ローン・決済、ポイント・マイレージ、会員権、不動産、質問サイト、ブログ、メーリングリスト
メールマガジン、ウェブアーカイブ・キャッシュ、オンライン辞書・テキスト翻訳、ウェブページ翻訳
フリー百科事典、ブックマーク・リンク集、URL 転送・変換サービス、動画配信、ライブ動画
ストレージサービス、クチコミ・評価・コメント、位置情報、ドメインパーキング、ウェブアプリケーション
更新ファイル・ドライバ、IT、プロバイダ、ポータルサイト、検索、ホスティング、ビジネスセミナー・交流会
ビジネス・経済情報、ビジネス・経済団体、サイドビジネス、アルコール製品・タバコ
成人向け遊技・飲食、その他の青年・成人向け、テレビ・ラジオ、映画・演劇、音楽
書籍・雑誌、漫画・アニメ、タレント・ミュージシャン・著名人、グラビア・水着、ファッション・美容
コスプレ、占い・診断、スポーツ・レジャー、ペット・動物、玩具・模型、アミューズメント、DIY・園芸
懸賞・プレゼント、趣味と娯楽総合、その他の趣味と娯楽、交通、自動車・オートバイ、その他の乗り物
地図サービス、宿泊・旅行、ライフライン、郵便・物流、暮らし・地域情報、生活関連商品
生活関連サービス、イベント、公共施設、文例・テンプレート、食事・料理・食品、結婚紹介
冠婚葬祭、妊娠・出産・育児、宗教、病気・医療、介護・福祉、ヘルスケア・リラクゼーション
美容整形、メンタルヘルス、学校・教育、学習、学術・開発・研究、資格・語学・カルチャースクール
文化・芸術・工芸、美術館・博物館、行政・地方自治体、政党・政治家、外交・国際機関
軍事・防衛、政治評論・情報、広告・マーケティング、オンライン広告・バナー、迷惑メールリンク
ニュース、天気・災害情報、司法・法律・行政書士、経理・税金・年金、興信所、デザイン
コンサルティング、翻訳・通訳、その他のサービス、農林水産、建設、製造、その他の産業

(※6：アンチスパムのタグ付けについて

HOME-UNIT3 のアンチスパム機能では、スパム判定時に“[SPAM]”、”[GRAY]”と 2 種類のタグ付けをおこないます。

判定	タグ	件名／本文への処理
迷惑メール	[SPAM]	変更しない
広告メール	[GRAY]	変更しない
任意ブラックリスト	[SPAM]The Mail is Blocked due to Anti-Spam rules.	削除

タグの変更や、任意ブラックリスト判定時の処理の変更をご希望の場合には、HOME-CC にご相談ください。

(※7： 監視機能について

●死活監視

HOME-UNIT3 のネットワーク機器としての死活監視を実施します。1 時間以上連続して稼働が確認できない場合は、HOME-CC による状況確認の上、お客様へご連絡する場合があります。

※HOME-UNIT3 の UTM 各機能の正常稼働を監視するものではありません。万が一、UTM 機能が正常に動作していないとお気づきの場合には、HOME-CC へご相談ください。

●ステータス確認

2020 年 4 月 1 日以降、ステータス確認サイトで HOME-UNIT3 の稼働状況、設定情報を確認できます。アクセス方法や機能についての詳細は以下のリンク先より、[クイックガイド（管理者向け）]をご確認ください。

HOME-UNIT4/3/2 管理者向けヘルプ：https://hmbx.canon.jp/help9a/index.php/unit2_admin

(※8：レポート機能について

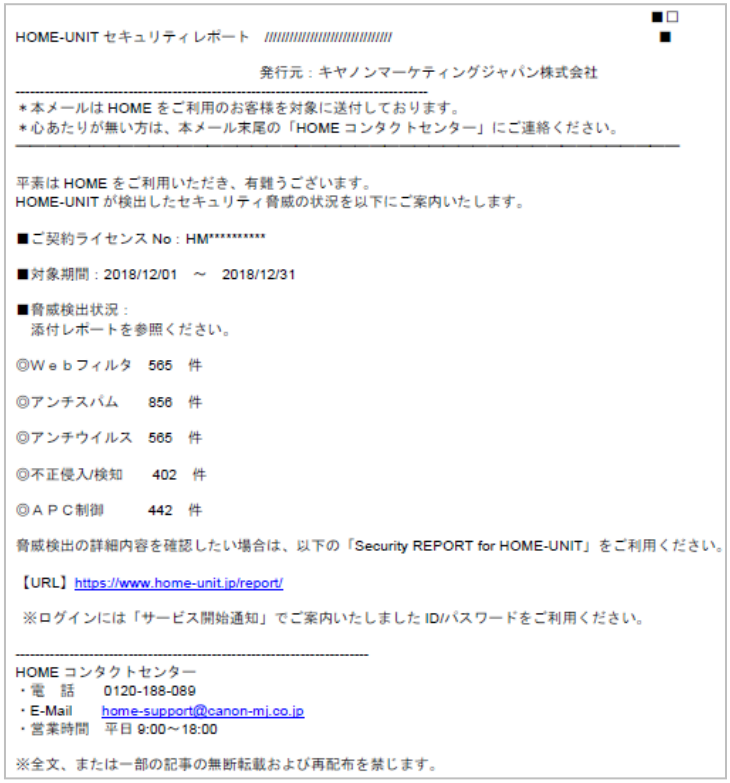
HOME-UNIT3 には、以下のレポート機能を提供します。

●月次レポート

本文に期間中の脅威検出状況を記載したメールを送付します。

詳細は本文内 URL リンクから「Security Report for HOME-UNIT」にアクセスすることで確認できます。

※ログイン ID/パスワードは管理者向け「サービス開始通知」に記載されています。ご不明の場合は HOME-CC までお問い合わせください。



HOME-UNIT セキュリティレポート ////////////////////////

発行元：キヤノンマーケティングジャパン株式会社

＊本メールは HOME をご利用のお客様を対象に送付しております。
＊心あたりが無い方は、本メール末尾の「HOME コンタクトセンター」にご連絡ください。

平素は HOME をご利用いただき、有難うございます。
HOME-UNIT が検出したセキュリティ脅威の状況を以下にご案内いたします。

■ご契約ライセンス No：HM**********

■対象期間：2018/12/01 ～ 2018/12/31

■脅威検出状況：
添付レポートを参照ください。

◎Ｗｅｂフィルタ 565 件

◎アンチスパム 856 件

◎アンチウイルス 565 件

◎不正侵入/検知 402 件

◎ＡＰＣ制御 442 件

脅威検出の詳細内容を確認したい場合は、以下の「Security REPORT for HOME-UNIT」をご利用ください。

【URL】https://www.home-unit.jp/report/

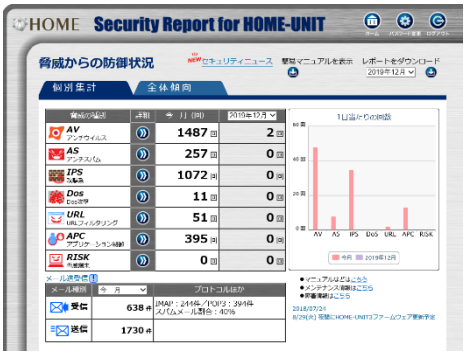
※ログインには「サービス開始通知」でご案内いたしました ID/パスワードをご利用ください。

HOME コンタクトセンター
・電 話 0120-188-089
・E-Mail home-support@canon-mj.co.jp
・営業時間 平日 9:00～18:00

※全文、または一部の記事の無断転載および再配布を禁じます。

※　検出のログのご提供を希望する場合は、HOME-CC にご相談ください

●レポートサイト
HOME-UNIT3 が検出した脅威は、見える化サイト「Security Report for HOME-UNIT」から確認できます。
「Security Report for HOME-UNIT」では当月と過去 5 か月分と脅威検出状況をグラフで確認したり、過去の検出状況を印刷したりすることができます。なお、HOME-UNIT3 自身へアクセスしログを確認する、といった機能は提供されません。



●アラート通知について
HOME-UNIT3 が検出した脅威は、日本語で通知されます。アラート通知は 10 分毎もしくは 30 件蓄積毎に送信されます。

-アンチウイルス

イベント1 (2019-02-14 15:47:46)：
ウイルスが検出された為、駆除いたしました。

[タイプ] LAN-Client-home_av
HTTP eicar.com EICAR-Test-File Block

[送信元アドレス／ポート番号]
[送信先アドレス／ポート番号]

イベント2 (2019-02-14 15:49:26)：
ウイルスが検出された為、駆除いたしました。

[タイプ] LAN-Client-home_av
HTTP eicar.com EICAR-Test-File Block

[送信元アドレス／ポート番号]
[送信先アドレス／ポート番号]

－Web フィルタリング

イベント2 (2019-02-14 16:52:25)：
禁止されてるURLに対するアクセスが検出された為、ブロックいたしました。

[タイプ] home_web
m/ Pornography

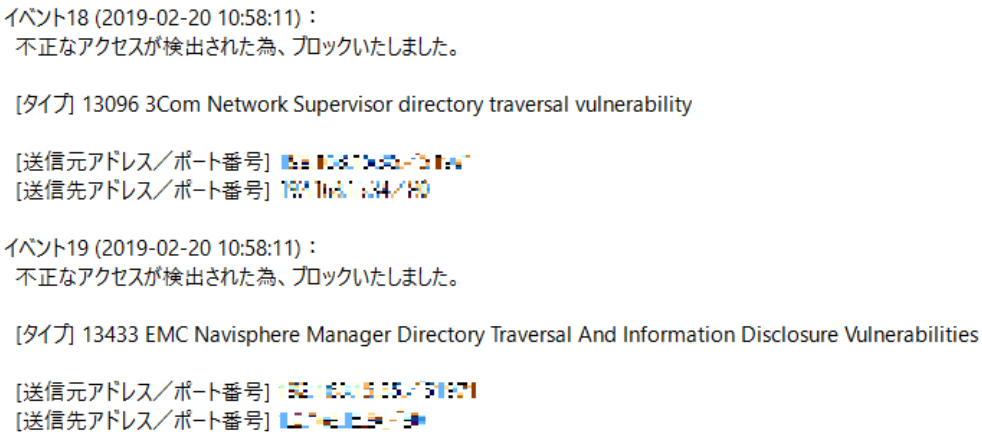
[送信元アドレス／ポート番号]
[送信先アドレス／ポート番号]

イベント3 (2019-02-14 16:52:34)：
禁止されてるURLに対するアクセスが検出された為、ブロックいたしました。

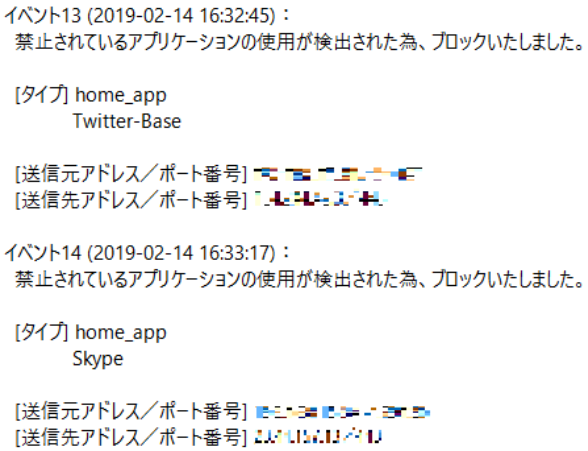
[タイプ] home_web

[送信元アドレス／ポート番号]
[送信先アドレス／ポート番号]

－IPS



－アプリケーション制御



●LED 通知

HOME-UNIT3 ではアンチウイルス機能等で脅威を検知した際に、筐体前面の LED ランプが流れるように点灯することで脅威の可視化が可能です。

(※9： 情報漏洩防止機能について

HOME-UNIT3 では、情報漏洩防止機能として、以下 2 つの機能が利用できます。(オプション機能となります。)
※各種機能の詳細は、ホワイトペーパ「HOME-UNIT3 添付ファイル自動 ZIP 暗号化サービス」「HOME-UNIT3 メール誤送信防止サービス」をご参照ください。
ホワイトペーパ：https://hmbx.canon.jp/agreement/index.php/wp-unit

※IPv6 でのメール送信に対しては、本機能は動作しません。IPv4 over IPv6 通信の場合、HOME-UNIT3 配下の通信は IPv4 行いますので、IPv4 環境同様に本機能が利用できます。
※SMTP サーバとの認証において CRAM-MD5 及び DIGEST-MD5 を利用されている場合、クライアント端末側の設定変更をご案内する場合があります。

●添付ファイル自動 ZIP 暗号化機能

HOME-UNIT3 を経由して送付されるメールの添付ファイルを自動的に ZIP 暗号化します。

●メール誤送信防止機能

HOME-UNIT3 を経由して送付されるメールを一定時間本体内に保留させます。
設定された URL にアクセスし保留されたメールを削除することが可能です。
一定時間経過後、または設定された URL にアクセスし送信ボタンをクリックすることでメールが送付されます。

メールサーバ側と通信において 465 ポートを利用した SSL/TLS で暗号化された通信(SMTPS)で通信している場合にはクライアント端末への証明書のインポート作業及び HOME-UNIT3 の設定変更が必要になります。
また、587 ポートを使用した STARTTLS 通信を使用している場合にはクライアント端末でご利用中のメーラの設定を平文通信に変更する作業と HOME-UNIT3 の設定変更が必要になります。
本機能を有効化した場合、推奨ユーザー数の低減や通信速度の低減が見込まれます。設定をご希望の場合には、HOME-CC にご相談ください。
また、証明書のインストールや各種設定作業はお客様ご自身で実施いただきます。

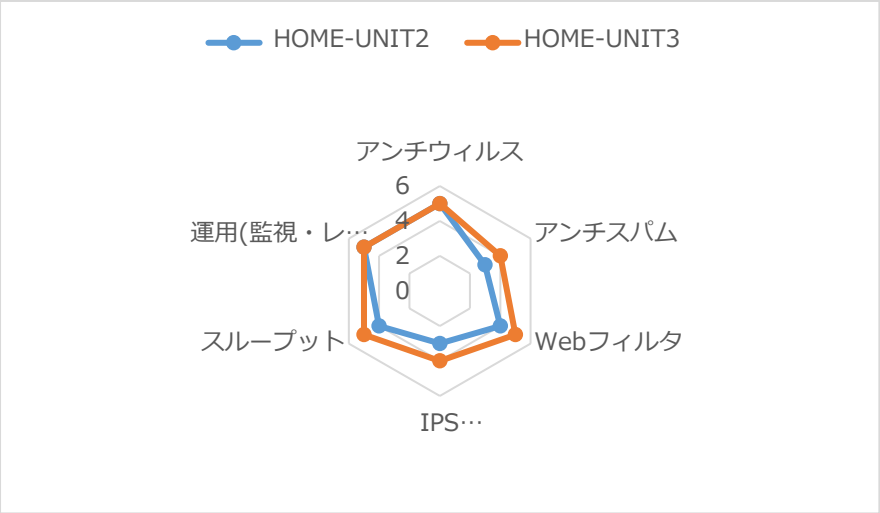
◎HOME-UNIT3 情報漏洩防止機能 動作確認 OS 及びメールソフト ※2020 年 1 月 29 日時点

OS バージョン	メールソフト
Windows 10	Outlook2016 Outlook2013 Thunderbird
Windows 8.1	Outlook2016 Outlook2013 Thunderbird
Mac OS X 10.15 (Catalina)	Mac 標準メールソフト(v13.x)
Mac OS X 10.14 (Mojave)	Mac 標準メールソフト(v12.x)
Mac OS X 10.13 (High Sierra)	Mac 標準メールソフト(v11.x)
Mac OS X 10.12 (Sierra)	Mac 標準メールソフト(v10.x)
Mac OS X 10.11 (El Capitan)	Mac 標準メールソフト(v9.x)

(※10：カスタマイズ対応について
複数のプロファイルを併用する場合は、有償カスタマイズが必要となります。詳細は HOME-CC へご相談ください。

◎旧機種との比較について

	HOME-UNIT3(SS5000)	HOME-UNIT2(SS3000)
全般	LAN 内の端末同士の通信であっても、各種セキュリティ機能によって検疫が行われます。	LAN 内の端末同士の通信にはセキュリティ検疫がかかりません。
アンチウイルス	検出率の観点から世界トップ水準の「Kaspersky」を採用。ヒューリスティック、サンドボックス機能の利用によりゼロデイ攻撃にも対応。	検出率の観点から世界トップ水準の「Kaspersky」を採用。ヒューリスティック、サンドボックス機能の利用によりゼロデイ攻撃にも対応。
アンチスパム	検出率の観点から世界トップ水準の「Kaspersky」を採用。	多くの UTM に採用される米メーカ「CYREN」のエンジンを採用
Web フィルタリング	国内シェア No.1 の「ALSI」のエンジンを採用し、より日本国内のお客様に最適な Web フィルタリングを提供。	アンチスパム同様「CYREN」のエンジンを採用。HTTPS サイトにも対応。
IPS **アプリケーション制御**	メーカオリジナル。3000 種類以上にアプリケーションに対応(2018 年 1 月現在)。	メーカオリジナル。1000 種類以上のアプリケーションに対応(2018 年 1 月現在)。
運用 ※死活監視・レポート	死活監視を標準で提供(1 時間の無通信検知)、レポートサイト、月次配信に対応。	死活監視を標準で提供(1 時間の無通信検知)、レポートサイト、月次配信に対応。



(※11 Web フィルタリング・アンチスパムホワイトリストお客様追加機能について

2020 年 4 月 1 日以降、一部のお客様にて Web フィルタリングでブロックされた URL やアンチスパムでスパム判定されたメールアドレスに対して、ホワイトリスト追加ができる、「ホワイトリストお客様追加機能」を利用できます。HOME-CC の営業時間外でも、Web フィルタリングのブロック画面やスパム判定されたメールに下部に記載された URL から、お客様にてホワイトリストへの追加が可能です。
詳細は、「クイックガイド(ホワイトリストお客様追加編)」をご参照ください。

HOME-UNIT4/3/2 利用者向けヘルプ：https://hmbx.canon.jp/u0help/index.php/unit2_user

以上