HOME-UNIT3　クイックガイド

Ver2.0

§ HOME-UNIT3 でできること

1.　HOME-UNIT3 とは

HOME-UNIT3 は、１台で企業のセキュリティレベルを複合的に高め、社外からの様ざまな脅威や、社内からの情報漏えい、セキュリティ事故に備えます。また、その運用管理も HOME コンタクトセンター（以下、HOME-CC といいます）で集中して行いますので、複雑な設定や操作が不要で安心してご利用いただけます。

2.　HOME-UNIT3 の機能

HOME-UNIT3 は、お客様に次の機能を提供します。
※暗号化された通信や IPv6 通信への対応については、下記 URL よりホワイトペーパ「HOME-UNIT3 セキュリティ機能について」をご参照ください。
ホワイトペーパ：https://hmbx.canon.jp/agreement/index.php/wp-unit

■アンチウイルス

電子メールの送受信や Web 閲覧を監視し、万一コンピュータウイルスやスパイウェアが含まれているときはそのウイルスを削除します。また、アンチウイルスソフトの定義ファイル未更新や USB メモリからの感染をきっかけにした外部へのウイルス流出も防ぎ、企業がセキュリティ対策不足による加害者になってしまうケースを未然に防ぎます。

■アンチスパム

日々送信される迷惑メールを差出人や、文面などから判定し、振分等をおこない易いようにタグ付けをします。

■Web フィルタリング

暴力関連のコンテンツが含まれるサイトや、フィッシングなどの被害につながる違法なサイト、アダルトサイトなど業務上不要なサイトの閲覧をカテゴリ単位で禁止します。また、ショッピングやゲームなどのカテゴリの禁止や、特定の URL の閲覧許可などにも対応可能です。仕事上不要なサイトアクセスを制限することで仕事の効率を高め、インターネットを経由した情報漏えいの抑止にも効果的です。

■不正侵入検知／防御

ファイアウォールが許可した通信サービスを、監視カメラのようにチェックして、不適切な通信の可能性や攻撃、不正侵入の試みを判断してブロックします。

■アプリケーションコントロール

社内ネットワークから Winny 等のファイル交換ソフトや、メッセンジャーソフトなどお客様が指定したアプリケーションの通信を遮断し利用を禁止します。

3.　ご利用環境に合わせた設定変更

HOME-UNIT3 の設定は、HOME-CC で実施しますので、お客様が HOME-UNIT を操作することはありません。設定変更をご希望の場合には、HOME-CC にご相談ください。
お客様向けステータス確認サイトから、ご利用中の HOME-UNIT3 の稼働状況や設定情報を確認することができます。詳細は、9.稼働状況の確認をご参照ください。

4.　アンチウイルスの利用

HOME-UNIT3 では、HTTP、FTP、IMAP、POP3、SMTP のプロトコルを利用した通信に対して、アンチウイルス検疫をおこない、脅威の侵入と流出を防ぎます。暗号化された通信については後述ご確認ください。
ウイルスを検知した場合は、感染ファイルを削除し、メールにてお知らせします。（メールによるお知らせは、希望された場合に限ります。）

ただし、標準仕様として以下の通信・データについては、アンチウイルス検疫の対象外となります。

・HTTPS 等の暗号化された通信(※)
・パスワード等でプロテクトされたデータ
・分割されたデータやメール
・HOME-UNIT3 非対応のデータ形式

※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機能を利用できます。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です。(対応プロトコルは、SMTPS/ POP3S です。HTTPS/ FTPS /IMAPS はサポート対象外です。)
なお、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おこなってください。
設定方法の詳細は「クイックガイド(クイックガイド（メール送受信 暗号化 SSL 対応編）)」をご参照ください。
HOME-UNIT4/3/2 管理者向けヘルプ：
https://hmbx.canon.jp/help9a/index.php/unit2_admin
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。

※一般的にウイルスは感染する速度や範囲を考慮し、可搬性が重要視されるため、単一データのサイズは Kbyte～数 Mbyte までとなる傾向にあります。また、一般的に 10MB を超過するファイルはメールでやり取りされることは少なく、ダウンロードが主となります。Web フィルタリング機能によって感染ファイルが配置されている可能性がある有害サイト閲覧を禁止し、不正侵入検知機能で不正な自動ダウンロードを遮断することで、複合的にリスクの低減が可能です。

5.　アンチスパムの利用

HOME-UNIT3 では、POP3、IMAP で受信されるメールに対して迷惑メール判定をします。

POP3/IMAP の場合：（受信）
迷惑メールに判定した際には、件名の頭に“[SPAM]”のタグ付けをおこないます。
広告メールに判定した際には、件名の頭に“[GRAY]”のタグ付けをおこないます。
ブラックリストを設定した場合、デフォルト設定ではブラックリストに合致したメールを受信した場合、当該メールは件名が「[SPAM]The Mail is blocked due to Anti-Spam rules.」に書き換えられ、件名と本文が削除されます。当該メールの件名と本文を削除せず、メールの件名の頭に[SPAM]とタグ付けする設定も選択可能です。ご希望の場合には、HOME-CC にご相談ください。

※Gmail、Yahoo!メール、Hotmail 等、Web ブラウザ上でメール送受信されるウェブメール、Microsoft Exchange を利用されている場合には本機能を利用できません。暗号化された送受信を利用している場合には、以下の制限事項があります。設定をご希望される場合には、HOME-CC にご相談ください。

※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スパム機能を利用することができます。ただし、ご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。
なお、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。
設定方法の詳細は「クイックガイド(暗号化通信(SSL/TLS)対応編)」をご参照ください。
HOME-UNIT4/3/2 管理者向けヘルプ：
https://hmbx.canon.jp/help9a/index.php/unit2_admin

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。設定をご希望される場合には HOME-CC にご相談ください。

6. Web フィルタリングの利用

利用者が閲覧禁止カテゴリに属するサイトにアクセスした場合、HOME-UNIT3 がその閲覧をブロックし、閲覧した記録をメールにて通知します。（メールによるお知らせは、希望された場合に限ります。）
HOME-UNIT3 によりブロックされているサイトを URL 単位で許可したい、またはブロックするサイトを URL 単位で追加したい場合には、HOME-CC へご相談ください。

※URL 単位でブロックを指定した場合、アクセス都度のアラートメールの発行、Security Report for HOME への反映はありません。

※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 HTTP 通信に対しても Web フィルタリング機能を利用することができます。ただし、ご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。
なお、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おこなってください。
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には HOME-CC にご相談ください。

7. 不正侵入検知／防御

社外や社内からの不正な通信を検知した場合は、通信を遮断し、メールにて通知します。（メールによるお知らせは、希望された場合に限ります。）

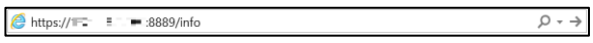
8. アプリケーションコントロール

Winny 等のファイル交換ソフトや、メッセンジャーソフトなどお客様が指定したアプリケーションの社内ネットワークからの通信を遮断し利用を禁止します。

9. 稼働状況の確認

Web ブラウザより、ログイン認証なしで HOME-UNIT3 の稼働状況、設定値を確認する、ステータス確認サイトにアクセスできます。
また、HOME-CC の営業時間外でも、Web フィルタリングやアンチスパムのホワイトリストにお客様自身で URL やメールアドレスを追加いただける機能「ホワイトリストお客様追加機能」で追加された URL につきましても本機能にて確認することができます。
ホワイトリストお客様追加機能の詳細につきましては、下記のいずれかの URL から「クイックガイド（ホワイトリストお客様追加編）」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
HOME-UNIT4/3/2 利用者向けヘルプ
https://hmbx.canon.jp/u0help/index.php/unit2_user

■アクセス方法
ステータス確認サイトを確認する場合、ブラウザの URL 欄に以下を入力し、アクセスしてください。
https://HOME-UNIT3 の IP アドレス:8889/info
例：https://192.168.100.100:8889/info



※HOME-UNIT3 の IP アドレスは「設定内容通知書」に記載されている「管理 IP アドレス」をご参照ください。）
※警告画面が表示された場合は、そのまま続行してください。

■確認できる内容
※上部タブ⇒左側タブの順に選択することで確認可能です。

上部タブ	左側タブ (緑色メニュー) から選択	左側タブ (白メニュー)から選択
ホーム	リソース	CPU、メモリ、内部ストレージ、 USB ストレージ
	インターフェース 状態	結線状態、モード
	ランプ状態	点灯しているランプの状態表示
詳細 設定	システム	時刻
	ネットワーク	モード、インターフェース、 DHCP サーバー、ルーティング、 パケットフィルタリング、プロキシ
	情報漏洩防止	メールポート利用番号、 SSL Inspection、 添付ファイル自動 ZIP 暗号化、 メール誤送信防止、通知メッセージ、 除外 IP アドレス設定
	UTM	UTM 機能、UTM 除外リスト、 WEB フィルタリング、アンチスパム
保守	システム	システム情報、管理
	ログ	ログ設定
	ソフトウェア	一括設定エクスポート

※ステータス確認サイトでは、稼働状況や設定情報の確認、設定値の一括エクスポート、再起動のみ実施可能です。

■ホワイトリストに追加された URL やメールアドレスの確認方法
① 画面上部の「詳細設定」タブを押下します。

② 画面左側に表示された「UTM」を押下し、プルダウンリストを表示させます。

以降の手順はアンチスパムと WEB フィルタリングで手順が異なりますので、それぞれの手順に沿って操作してください。

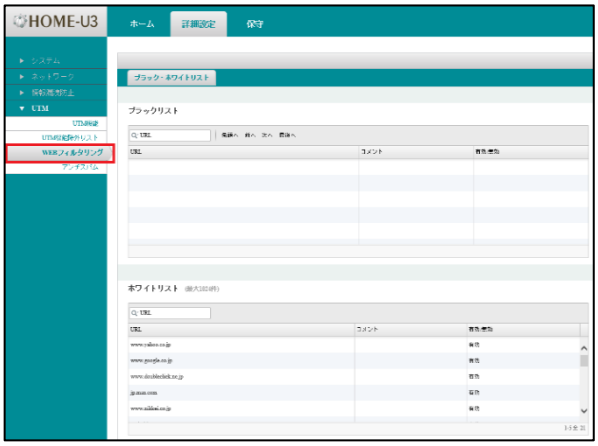
■アンチスパム

③　「アンチスパム」を押下します。

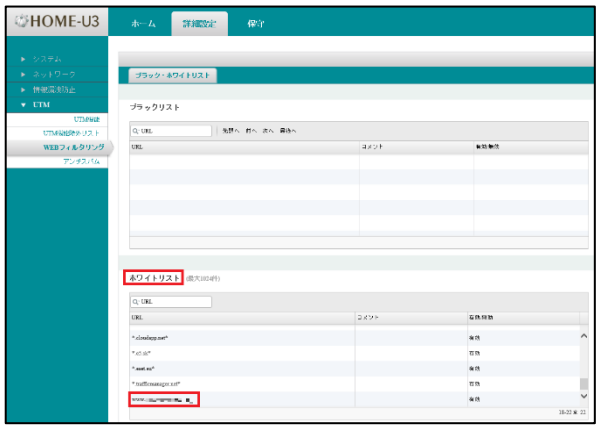
④　「送信者ホワイトリスト」タブの「メールアドレス」に追加したアドレスが反映されていることが確認できます。

■WEB フィルタリング

③　「WEB フィルタリング」を押下します。



④　「ブラック・ホワイトリスト」タブの「ホワイトリスト」をスクロールすると、リストの末尾に追加した URL が反映されていることが確認できます。



§ HOME-UNIT3 を利用した迷惑メール対策（受信）

1． ご利用に際して

HOME-UNIT3 は、受信メールが迷惑メールであると判定した場合、そのメールの件名の頭に“[SPAM]”の文字を自動的に付加し、そのまま PC に送信されます。（広告メールであると判定したメールには、そのメールの件名の頭に“[GRAY]”の文字を付加します。）

そのため、ご利用者ご自身の PC で受信したメールを迷惑メールフォルダに振り分ける必要があります。

※お客様ご自身にとって必要なメールが迷惑メールとして判定されることがあります。かならず、フォルダーに一旦振り分けていただき、内容を確認してから削除するようにしてください。

次章以降の内容を参照し、お客様ご自身でメール振分の設定をおこなってください。

2． Microsoft Outlook 2016 の場合の振分設定

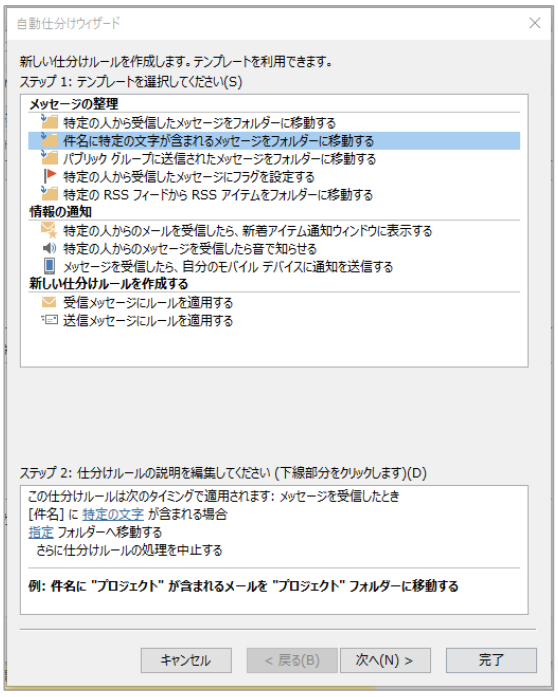
Microsoft Outlook 2016 を起動し、以下の設定をおこないます。

■振分フォルダーの作成

① フォルダーを作成したい親フォルダー選択し、『フォルダー』タブに移動し、一番左にある「新しいフォルダー」を選択し、『新しいフォルダーの作成』画面を開きます。
② 適当なフォルダー名（例：迷惑メール）を入力し迷惑メールを格納するフォルダーを作成します。

■振分ルールの作成

① メニューバーの「ファイル」をクリックし、「仕分けルールと通知の管理」をクリックし、表示された画面の［新しい仕分けルール］をクリックします。
② 『自動仕分けウイザード』の画面が開きますので、ステップ 1 の欄で「件名に特定の文字が含まれるメッセージをフォルダーに移動する。」をクリックします。



③ “[件名]に特定の文字が含まれる場合“の青文字をクリックします。『文字の指定』画面が開きますので、入力欄に “SPAM”（半角アルファベット 4 文字）と入力し、「追加」をクリックし、単語の登録をおこない「OK」をクリックします。
④ 次に、“指定フォルダーへ移動する”の青文字をクリックし、作成した振分フォルダーを指定します。
⑤ 任意の名称（例：HOME）で作成したルールを保存します。

広告メールも振り分けをおこなう場合は、同様に振分フォルダーおよび振分ルールの作成をおこなってください。

以上で、設定は終了です。

3． Mac Mail の場合の振分設定

MacMail を起動し、以下の設定をおこないます。

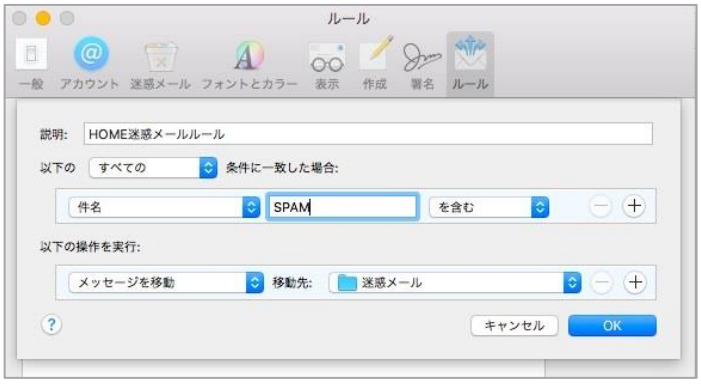
■振分フォルダーの作成

① メニューの「メールボックス」から「＋」を選択します

② 保存場所を選択し、適当なフォルダー名（例：迷惑メール）を入力し迷惑メールを格納するフォルダーを作成します。

■振分ルールの作成

① [環境設定]から[ルール]タブを開きます。
② [ルールの追加]をクリックします。
③ 任意の名称で[説明]（例:HOME）を入力し、[いずれかの]条件に一致した場合、「件名」に[SPAM]（半角アルファベット 4 文字）[を含む]を指定します。
④ 実行する操作で[メッセージを移動]を選択し、先ほど作成した任意のフォルダーを選んで[OK]をクリックします。



広告メールも振り分けをおこなう場合は、同様に振分フォルダーおよび振分ルールの作成をおこなってください。

以上で、設定は終了です。

4． Mozilla　Thunderbird の場合の振分設定

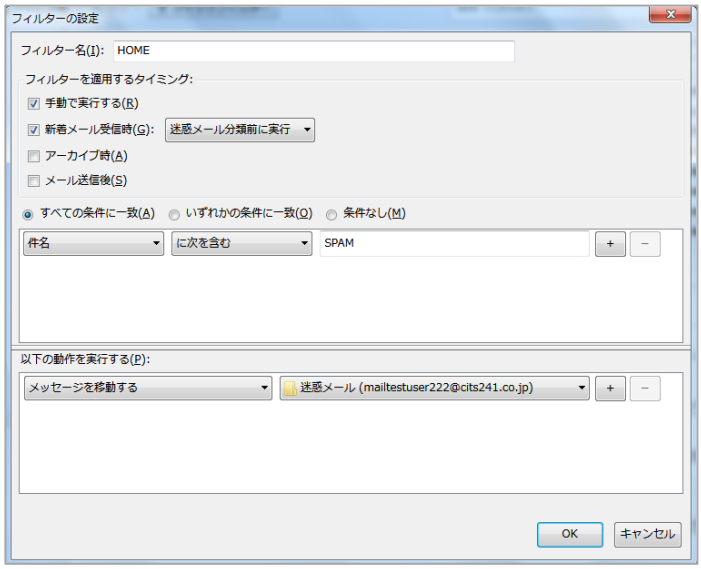
Mozilla Thunderbird を起動し、以下の設定をおこないます。

■振分フォルダーの作成

① メニューの「ファイル」から「新規作成」、「フォルダー」を選択し、『新しいフォルダー』画面を開きます。
② 任意の作成先を指定し、適当なフォルダー名（例：迷惑メール）を入力し迷惑メールを格納するフォルダーを作成します。

■振分ルールの作成

① メニューの「ツール」から「メッセージフィルター」を選択し、『メッセージフィルター』画面を開きます。「新規...」をクリックし、『フィルターの設定』画面を開きます。
② 任意の名称でフィルター名（例:HOME）を入力し、「件名」に「次を含む」を選択後、入力欄に“SPAM”（半角アルファベット 4 文字）と入力します。



③ 動作を設定する欄で、「メッセージを移動する」を選択後、作成した振分フォルダーをプルダウンで選択し、「OK」をクリックします。

広告メールも振り分けをおこなう場合は、同様に振分フォルダーおよび振分ルールの作成をおこなってください。

以上で、設定は終了です。

§ アラートメールの解説と確認方法

1. HOME-UNIT3 アラートメールについて

サービス申込時にお客様にご要望いただいた場合に限り、ご指定のメールアドレスに HOME-UNIT3 からアラートメールが自動送信されます。
※10 分間隔または 30 件アラートがたまったタイミングで送信されます。

送信するアラートメール

◎ ウイルス検知 通知
◎ Web フィルタリングブロック検知 通知
◎ 不正侵入検知 通知
◎ アプリケーションコントロール検知 通知

なお、このメールの設定はサービスご利用中に停止／再開のご相談をいただくことで変更が可能です。

2. アラートメール文面例

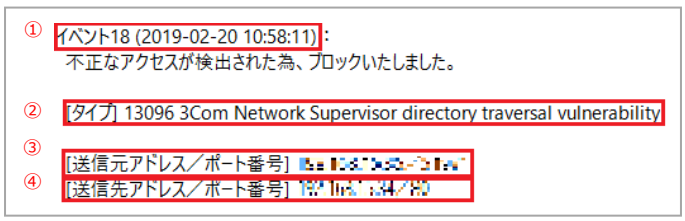
HOME-UNIT3 で検知されたログは、以下のようなメール文面でご登録いただいたメールアドレス宛に送信されます。
代表的なメール文面をご紹介します。

件名はすべて「HOME-UNIT3 アラートメール」になります。

■ウイルス検知アラートメール

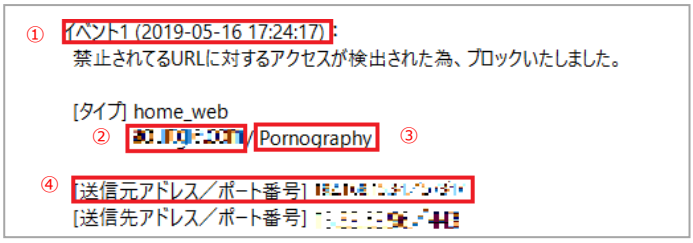
・①の日時に
・③から④に送信されたファイルに
・②のウイルスに感染した可能性のある添付ファイルを検知したためブロックした。

■不正侵入検知通知アラートメール



・①の日時に
・③の IP アドレスのユーザーが
・④の IP アドレスから②のタイプの侵入攻撃を受けたためブロックした。

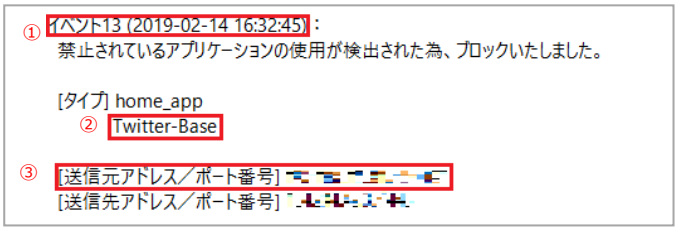
■Web フィルタブロック通知アラートメール



・①の日時に
・④の IP アドレスのユーザーが
・アクセスしたインターネットサイト（②）が
・コンテンツフィルタで「許可しない」の設定をしたカテゴリ（③）のサイトであったため閲覧をブロックした。

※：カテゴリ別の代表的な表記
・犯罪暴力：Violence、Illegal Drug
・アダルト：Nudity、Pornography
・不正技術：Malware、Phishing & Fraud

■不正アプリケーション検知アラートメール



・①の日時に
・③の IP アドレスのユーザーが使用した
・②のアプリケーションアプリケーション制御で
・「禁止」の設定をしたアプリーションであったため使用をブロックした。

§ Security Report for HOME の利用

1． Security Report for HOME について

HOME-UNIT3 が検知した直近 6 か月間の脅威を視覚的に確認することができます。

※7 か月以前のログを確認することはできません。
※本ツールの詳細な利用方法は、「4.トップ画面の説明」の「⑨ 各種リンク」に含まれる「マニュアルなどはこちら」から、HOME-UNIT4/3/2 管理者向けヘルプページに移動し、「Security Report for HOME-UNIT ユーザーマニュアル」を参照ください。

2．ログ確認 PC の動作条件

以下のブラウザを推奨します。

Internet Explorer 11 以降

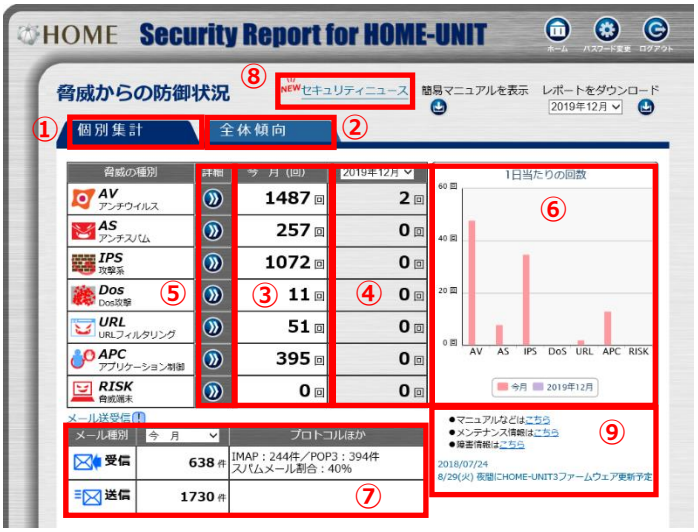
※その他のブラウザでも閲覧は可能ですが、表示速度が遅い、画面が崩れる等の不具合が出る場合があります。
※ Microsoft Edge を利用の場合、互換表示設定により正常に表示されない場合があります。その場合には互換表示機能を有効/無効をお試しください。

3． 管理サイトへのログイン

任意の PC から、ブラウザを起動し、
URL 欄に「https://www.home-unit.jp/report/」を入力しログインボタンを押下します。
※ユーザー名(ログイン ID)は管理者向け「サービス開始通知」に記載されています。パスワードの初期値は、本体裏面シール記載の MAC アドレス「MAC:●●●●●●●●●●●●(12 桁)」の下 8 桁です。ご不明の場合は HOME-CC までお問い合わせください。

4． トップ画面の説明

ログイン直後は以下のような表示となります。



①個別集計
HOME-UNIT3 がお客様環境で検出した脅威の状況をご確認いただけます。
②全体傾向
市場で稼働しているすべての HOME-UNIT3 が検出した脅威の状況を確認できます。
③今月の検出状況
今月のお客様環境における脅威検出状況を確認できます。
④過去の検出状況
過去のお客様環境における検出状況を確認できます。
⑤詳細確認
お客様環境における検出内容の詳細を確認できます。
⑥検出状況のグラフ表示
お客様環境における検出結果を視覚的にグラフ表示します。
⑦メール送受信
お客様環境における合計のメール送受信数を確認できます。
⑧セキュリティニュース
IPA が発行する情報セキュリティのニュースを参照できます。
⑨各種リンク
HOME の障害情報やメンテナンス情報、各種マニュアルサイトへのリンクが利用できます。

以上

ご不明な点がありましたら、
HOME コンタクトセンター (フリーダイヤル) 0120-188089
まで、お問い合わせください。