サクサ見える化サイト

取扱説明書（ユーザー編）

第8版　２０１９年8月1日

<< 目次 >>

1. はじめに

サクサ見える化サイト（以下、本サイト）は、サクサ UTM/SS1000 のログを Web 上で確認できるサイトです。検知された AV（アンチウイルス）、AS（アンチスパム）、IPS（攻撃系）、DoS（DoS 攻撃）、URL（URL フィルタリング）、ＡＰＣ（アプリケーション制御）の集計数、傾向などを視覚的に確認することができます。

このドキュメントは、本サイトのユーザー向け説明書です。
ユーザー向けのサイト画面では、ユーザーごとのログ集計結果と、ユーザー全体の傾向を確認することができます。

2. サイトを使用するには

本サイトを使用する際は、以下のブラウザをご使用ください。

- Internet Explorer ９．０、１０．０、１１．０
- Firefox （バージョン 25.0 以上）
- Google Chrome （バージョン 30.0.1599.101m 以上）
- Safari
- Microsoft Edge

3. 見える化サイト操作手順

3.1. ログイン

①クライアント PC からブラウザを立ち上げ、アドレス欄に以下の URL を入力し、接続します。

https://www.utmvisible.biz/saxautm/login.aspx

②ログイン画面が表示されます。

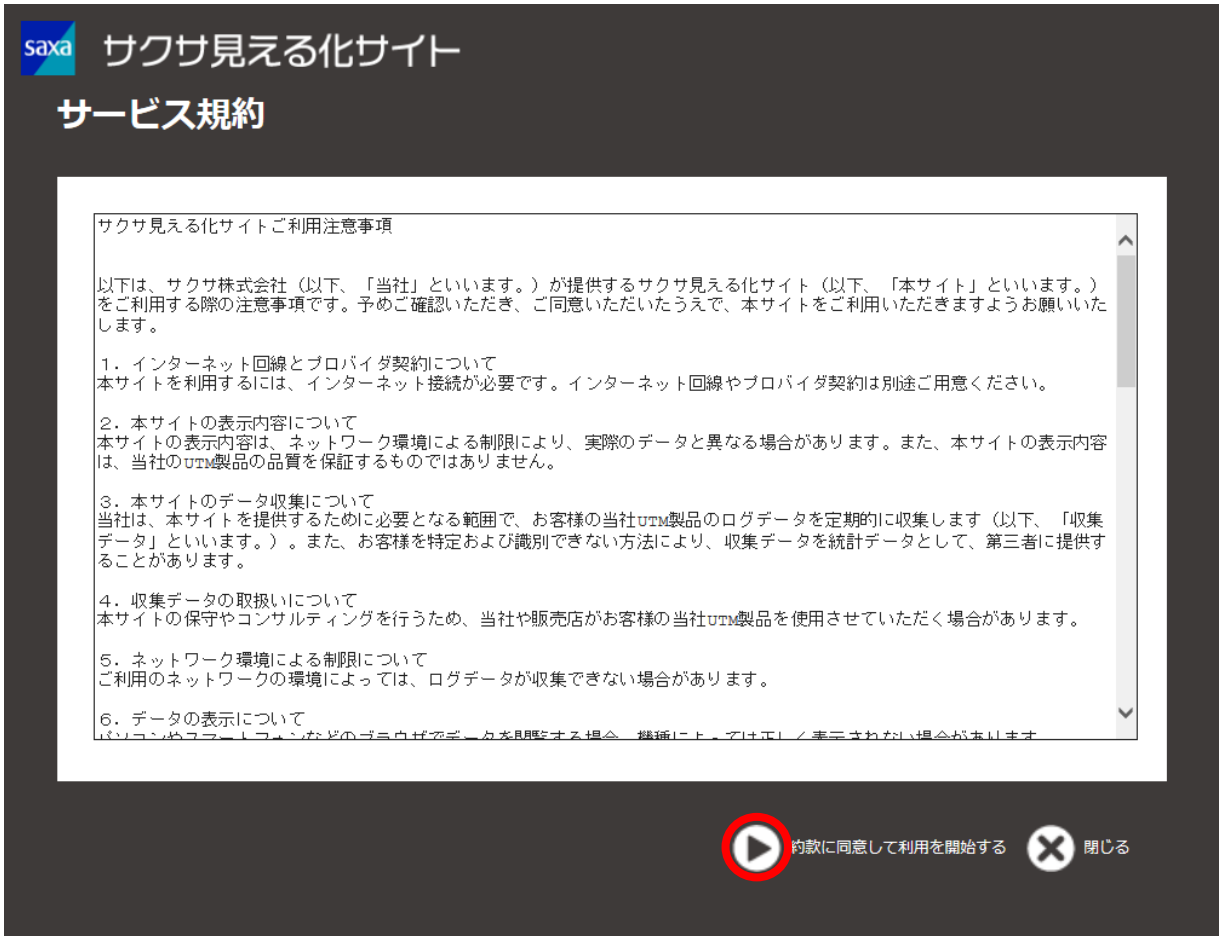
ユーザー名とパスワードを入力し、ログインアイコン（ ログイン ）をクリックします。

※　クリアアイコン（ クリア ）をクリックすると、入力済みの内容を消すことができます。

※　別の ID でログインしている場合は、一旦ログアウトし、画面を閉じてから以降の操作を行ってください。

③ユーザー用のホーム画面が表示されます。

※　初回アクセス時は「サービス規約」画面が表示されますので、サービス規約をご確認いただき、約款に同意して利用を開始する（ ）をクリックしてください。



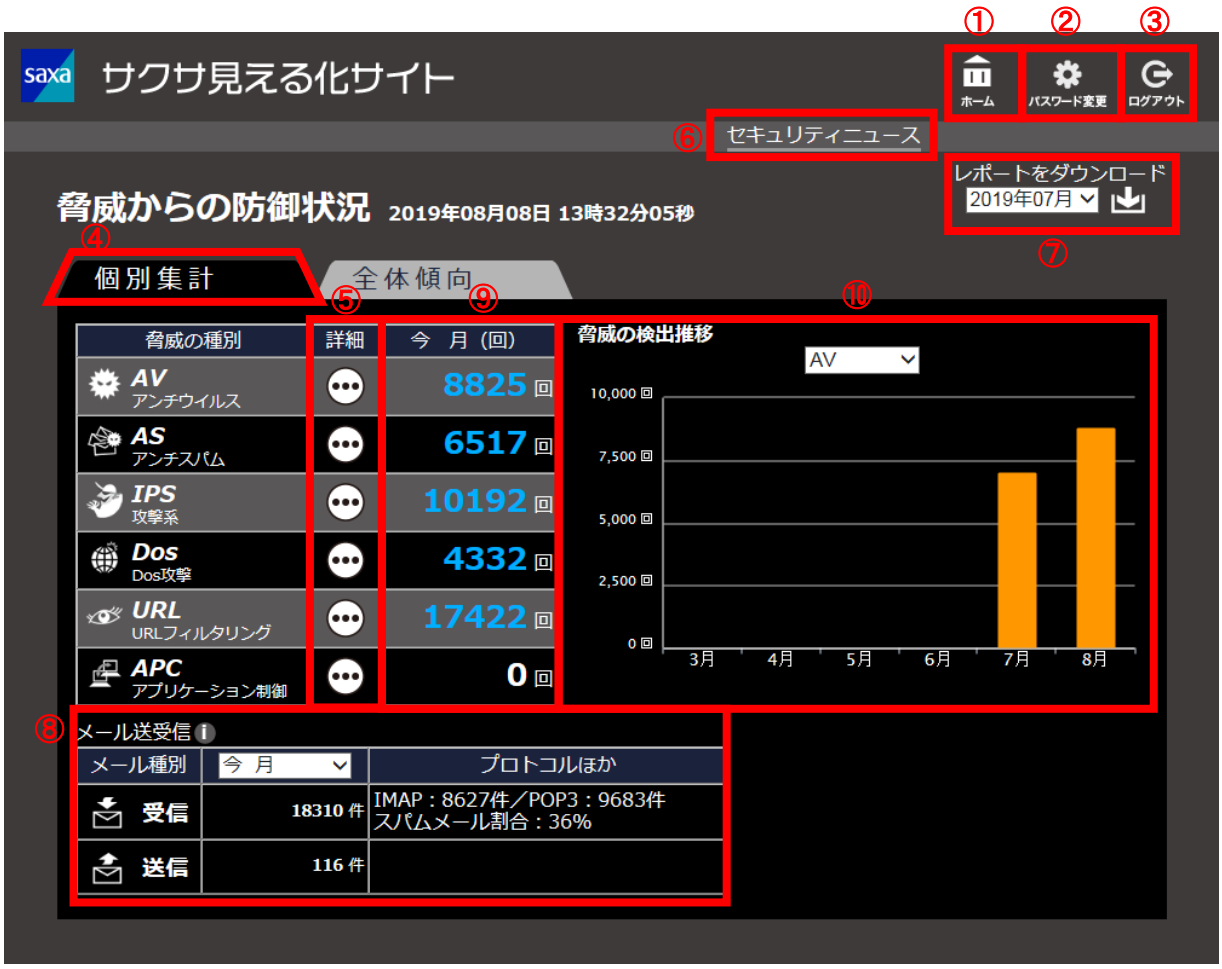
3.2. 集計結果（概要）

ログイン時に表示されるホーム画面では、各ログの集計情報の概要を確認できます。

3.2.1. ホーム画面の「個別集計」画面

ユーザーごとのログ集計結果を表示する画面です。

各脅威の検出合計回数を、今月分と先月分～5 ヶ月前（プルダウンで選択）で比較することができます。



①	ホーム 	画面の再読み込みを行います。
②	パスワード変更 	ユーザーパスワードの変更を行います。
③	ログアウト 	ログアウトし、ログイン画面へ戻ります。
④	個別集計	「個別集計」画面へ表示を切り替えます。
⑤	詳細 	詳細画面の「月別」画面を表示します。
⑥	セキュリティニュース	IPA からリリースされた重要なセキュリティ情報を表示しています。 クリックすると IPA の Web サイトを新しいタブ(またはウィンドウ)で表示します。
⑦	レポートをダウンロード 	プルダウンで選択（先月分～5 ヶ月前）した月のレポート（１ヶ月分）をダウンロードします。
⑧	メール送受信	受信したメールの総数と送信したメールの総数を表示します。 ※SS3000 では非対応のため件数が表示されません。
⑨	ログ集計結果	各脅威の検出合計回数を表示します。
⑩	脅威の検出遷移	各脅威（プルダウンで選択）の検出数を、今月分～5 ヶ月前で比較することができます。

3.2.2. レポートダウンロードについて

[レポートをダウンロード]ボタンをクリックすると、選択した月の PDF レポート（月次セキュリティレポート）と月次詳細レポートをダウンロードすることができます。

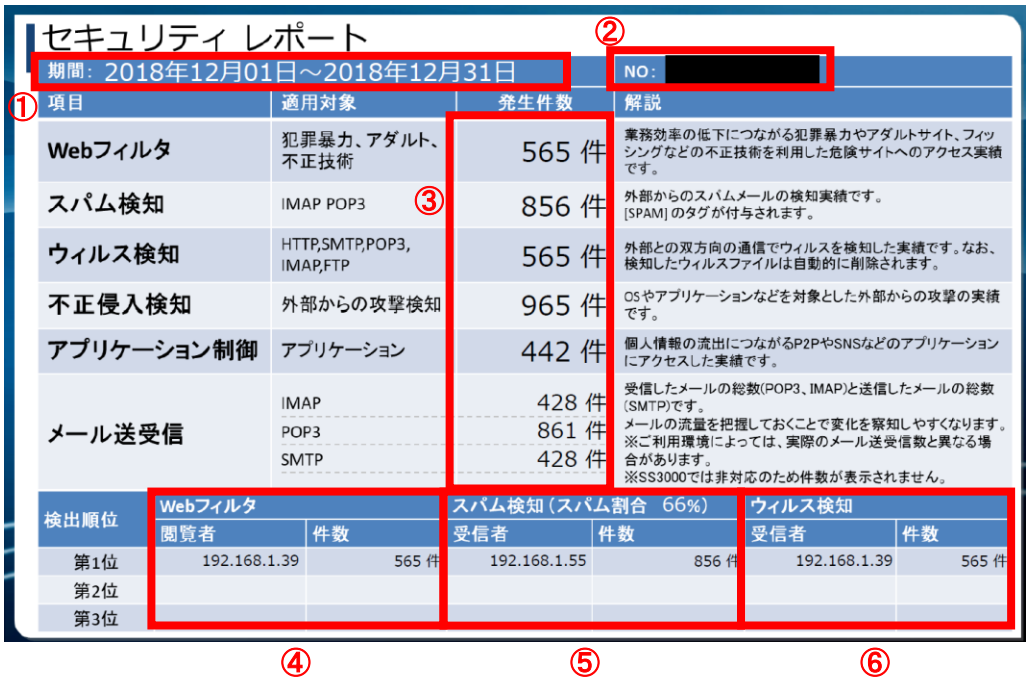
月次セキュリティレポートと月次詳細レポートは zip 形式で圧縮されており、下記の 3 ファイルが格納されています。

※集計期間は指定した月の月初めから月末までです。

月次レポート.pdf	月次セキュリティレポート
月次詳細レポート.xlsm	月次詳細レポート（テンプレート）
Data.csv	月次詳細レポート（データ）

3.2.2.1. 月次セキュリティレポート

○月次セキュリティレポート例

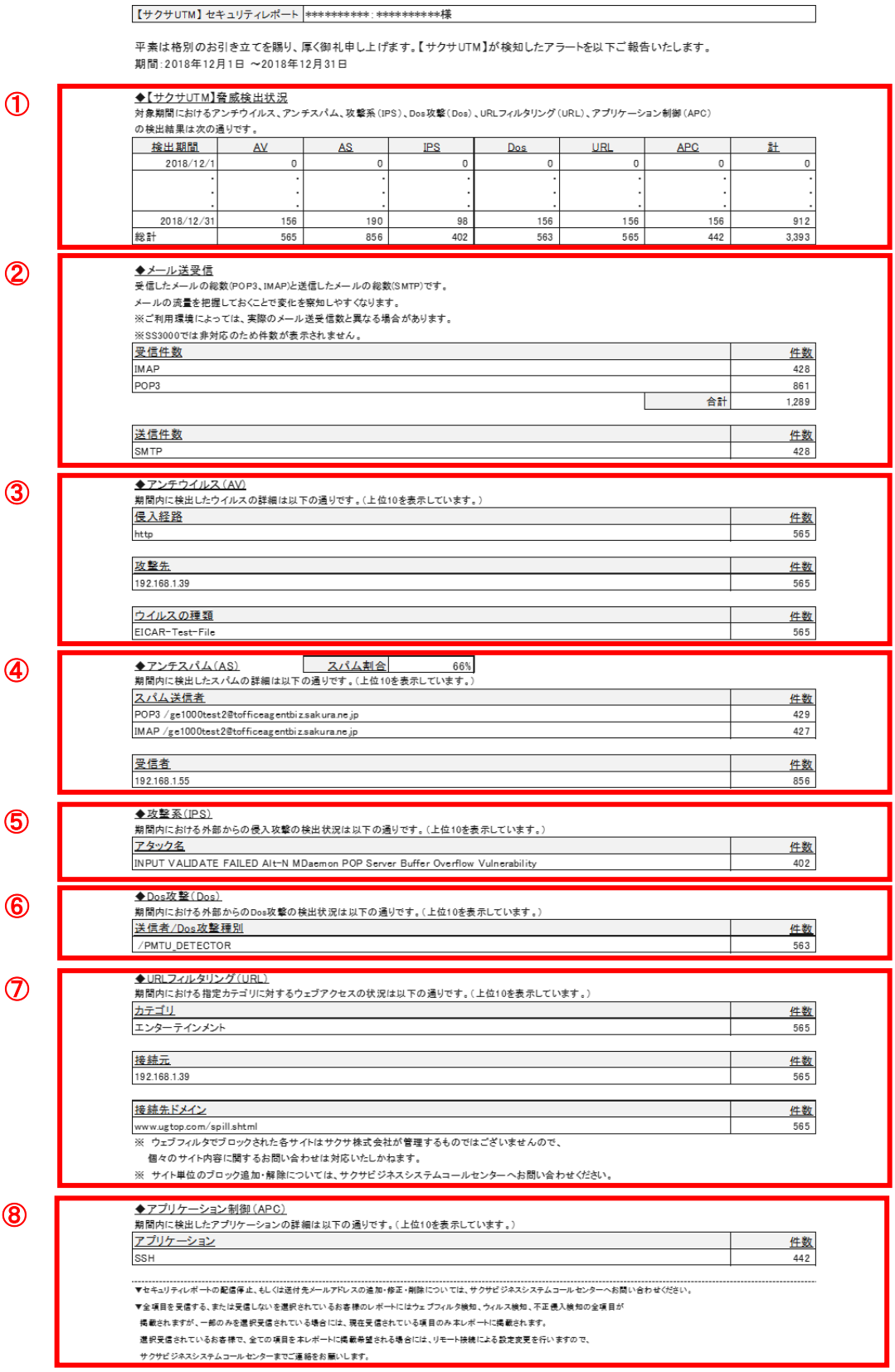


①	期間	指定した月の集計期間を表示します。
②	NO	設定したアカウント ID を表示します。
③	発生件数	各項目の期間中の発生件数を表示します。 Web フィルタ／スパム検知／ウイルス検知／不正侵入検知 ／アプリケーション制御 メール送受信（IMAP／POP3／SMTP） ※不正侵入検知については IPS・DoS の合計件数となります。 ※メール送受信は SS3000 では非対応のため件数が表示されません。
④	Web フィルタ	閲覧者毎の Web フィルタ件数の TOP 3 を表示します。
⑤	スパム検知	受信者毎のスパム件数の TOP 3 を表示します。 受信したメールの総数に対するスパムの割合を表示します。 ※スパム割合は SS3000 では非対応のため割合が表示されません。
⑥	ウイルス検知	受信者毎のウイルス検知の TOP 3 を表示します。

3.2.2.2. 月次詳細レポート

月次詳細レポートは、テンプレート（月次詳細レポート.xlsm）とデータファイル（Data.csv）で構成されており、テンプレートを実行することで生成されます。

○月次詳細レポート例



【サクサUTM】セキュリティレポート　**********：**********様

平素は格別のお引き立てを賜り、厚く御礼申し上げます。【サクサUTM】が検知したアラートを以下ご報告いたします。
期間：2018年12月1日 ～2018年12月31日

①

◆【サクサUTM】脅威検出状況
対象期間におけるアンチウイルス、アンチスパム、攻撃系（IPS）、Dos攻撃（Dos）、URLフィルタリング（URL）、アプリケーション制御（APC）の検出結果は次の通りです。

検出期間	AV	AS	IPS	Dos	URL	APC	計
2018/12/1	0	0	0	0	0	0	0
・	・	・	・	・	・	・	・
・	・	・	・	・	・	・	・
・	・	・	・	・	・	・	・
2018/12/31	156	190	98	156	156	156	912
総計	565	856	402	563	565	442	3,393

②

◆メール送受信
受信したメールの総数(POP3、IMAP)と送信したメールの総数(SMTP)です。
メールの流量を把握しておくことで変化を察知しやすくなります。
※ご利用環境によっては、実際のメール送受信数と異なる場合があります。
※SS3000では非対応のため件数が表示されません。

受信件数	件数
IMAP	428
POP3	861
合計	1,289

送信件数	件数
SMTP	428

③

◆アンチウイルス（AV）
期間内に検出したウイルスの詳細は以下の通りです。（上位10を表示しています。）

侵入経路	件数
http	565

攻撃先	件数
192.168.1.39	565

ウイルスの種類	件数
EICAR-Test-File	565

④

◆アンチスパム（AS）　スパム割合　66%
期間内に検出したスパムの詳細は以下の通りです。（上位10を表示しています。）

スパム送信者	件数
POP3 /ge1000test2@tofficeagentbiz.sakura.ne.jp	429
IMAP /ge1000test2@tofficeagentbiz.sakura.ne.jp	427

受信者	件数
192.168.1.55	856

⑤

◆攻撃系（IPS）
期間内における外部からの侵入攻撃の検出状況は以下の通りです。（上位10を表示しています。）

アタック名	件数
INPUT VALIDATE FAILED Alt-N MDaemon POP Server Buffer Overflow Vulnerability	402

⑥

◆Dos攻撃（Dos）
期間内における外部からのDos攻撃の検出状況は以下の通りです。（上位10を表示しています。）

送信者/Dos攻撃種別	件数
/PMTU_DETECTOR	563

⑦

◆URLフィルタリング（URL）
期間内における指定カテゴリに対するウェブアクセスの状況は以下の通りです。（上位10を表示しています。）

カテゴリ	件数
エンターテインメント	565

接続元	件数
192.168.1.39	565

接続先ドメイン	件数
www.ugtop.com/spill.shtml	565

※　ウェブフィルタでブロックされた各サイトはサクサ株式会社が管理するものではございませんので、
　　個々のサイト内容に関するお問い合わせは対応いたしかねます。
※　サイト単位のブロック追加・解除については、サクサビジネスシステムコールセンターへお問い合わせください。

⑧

◆アプリケーション制御（APC）
期間内に検出したアプリケーションの詳細は以下の通りです。（上位10を表示しています。）

アプリケーション	件数
SSH	442

▼セキュリティレポートの配信停止、もしくは送付先メールアドレスの追加・修正・削除については、サクサビジネスシステムコールセンターへお問い合わせください。
▼全項目を受信する、または受信しないを選択されているお客様のレポートにはウェブフィルタ検知、ウィルス検知、不正侵入検知の全項目が
掲載されますが、一部のみを選択受信されている場合には、現在受信されている項目のみ本レポートに掲載されます。
選択受信されているお客様で、全ての項目を本レポートに掲載希望される場合には、リモート接続による設定変更を行いますので、
サクサビジネスシステムコールセンターまでご連絡をお願いします。

①	【サクサ UTM】脅威検出状況	各項目の日毎の脅威の発生件数を表示します。
②	メール送受信	受信したメールの総数と送信したメールの総数を表示します。 ※メール送受信は SS3000 では非対応のため件数が表示されません。
③	アンチウイルス（AV）	侵入経路、攻撃系、ウイルスの種類の TOP１０を表示します。
④	アンチスパム（AS）	スパム送信者、受信者の TOP１０を表示します。 受信したメールの総数に対するスパムの割合を表示します。 ※スパム割合は SS3000 では非対応のため割合が表示されません。
⑤	攻撃系（IPS）	アタック名の TOP１０を表示します。
⑥	Dos 攻撃（Dos）	送信者／Dos 攻撃種別の TOP１０を表示します。
⑦	URL フィルタリング（URL）	カテゴリ、接続元、接続先ドメインの TOP１０を表示します。
⑧	アプリケーション制御（APC）	アプリケーション名の TOP１０を表示します。

◆月次詳細レポートの参照方法について

※月次詳細レポートを閲覧するには Excel2010,Excel2013 がインストールされている必要があります。

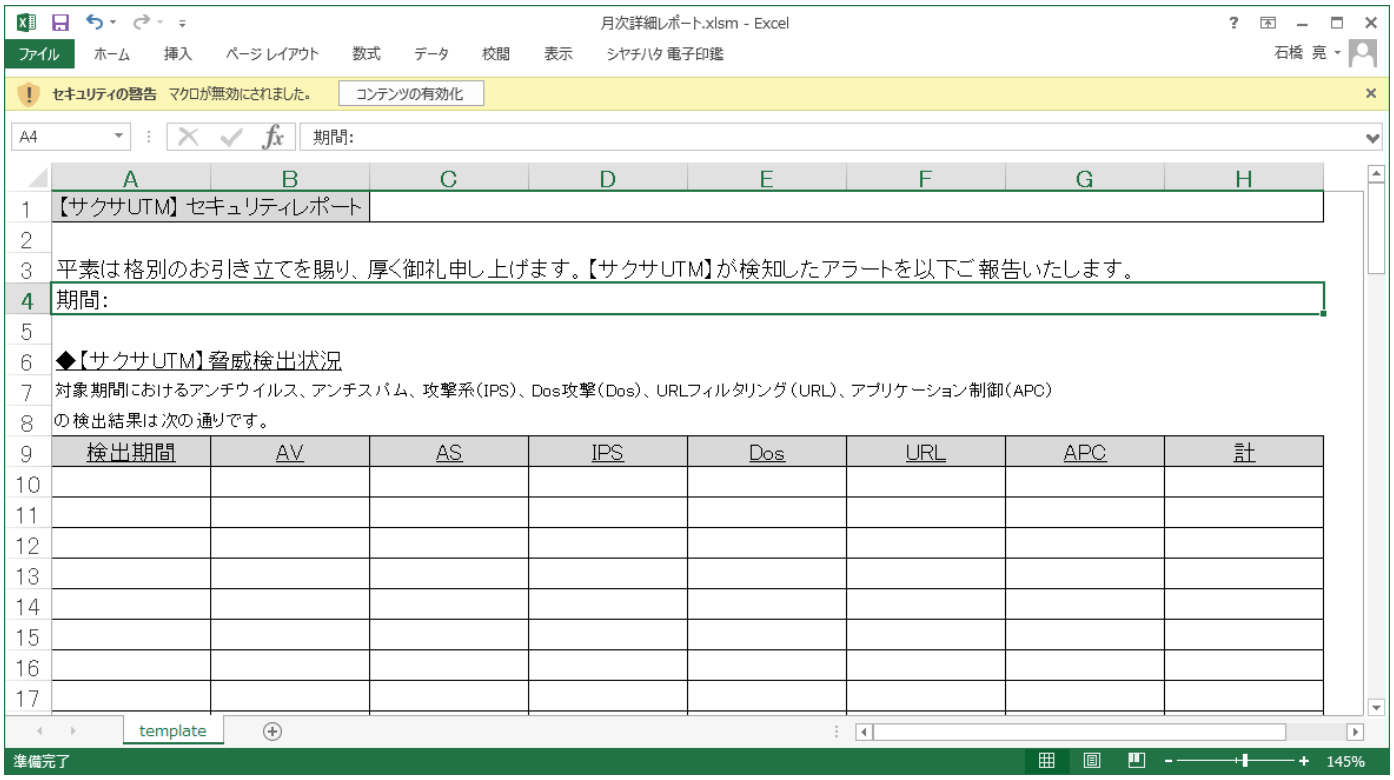
1.圧縮ファイルをパソコンに保存します。

2.保存した圧縮ファイルを解凍します。

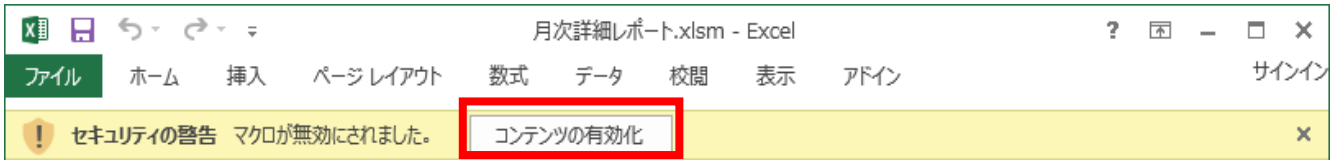
※テンプレートとデータは同じフォルダにある必要があるため、ファイルを移動しないでください。

また、内容の変更・削除等も行わないでください。

3.月次詳細レポート.xlsm を開きます。



4.「コンテンツの有効化」をクリックします。

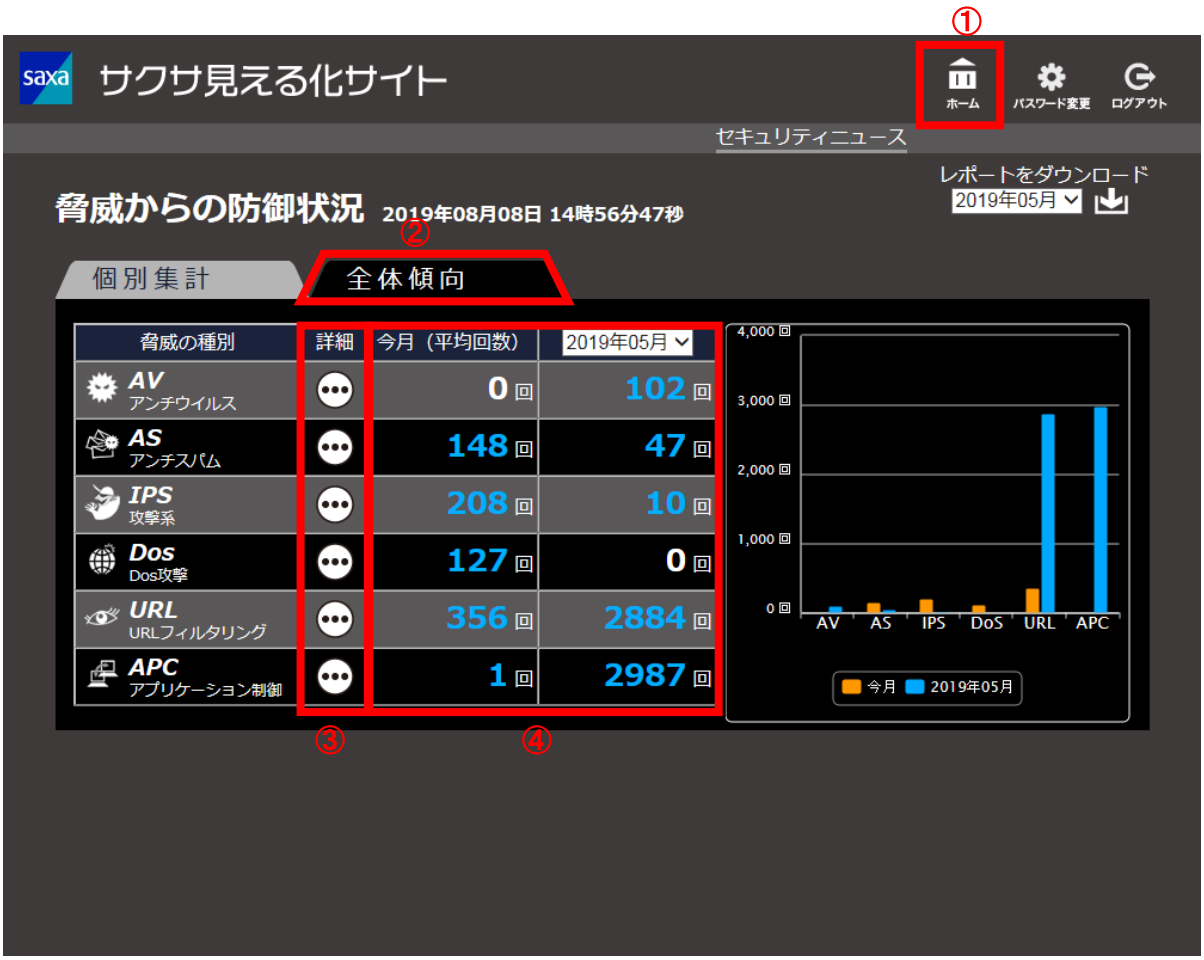


5.月次詳細レポート.xlsm と Data.csv が削除され、月次詳細レポート.xlsx が生成されます。

3.2.3. ホーム画面の「全体傾向」画面

サクサ UTM を使用しているユーザー全体の傾向を表示する画面です。

各脅威の検出傾向（平均回数）を、今月分と先月分～5 ヶ月前（プルダウンで選択）で比較することができます。



以下の項目以外は、個別集計画面と共通です。

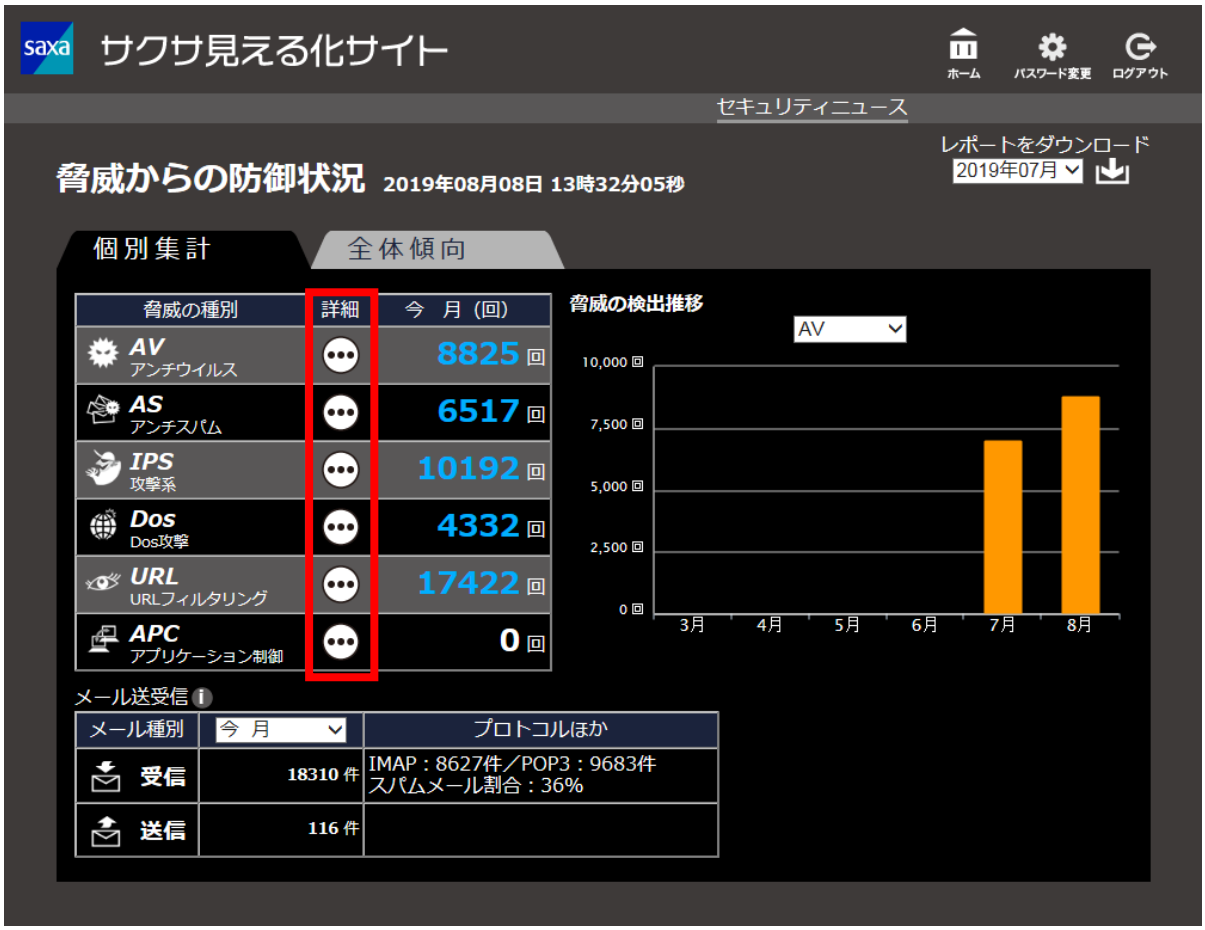
①	ホーム	画面の再読み込みを行い「個別集計」画面を表示します。
②	全体傾向	「全体傾向」画面へ表示を切り替えます。
③	詳細	詳細画面の「月別(全体)」画面を表示します。
④	ログ集計結果	各脅威の検出傾向（平均回数）を、今月分と先月分～5 ヶ月前（プルダウンで選択）で比較することができます。

3.3. 集計結果（詳細）

詳細画面では、各集計結果の詳細（月別／月別の全体傾向／日別／時間別）を確認することができます。

3.3.1. 詳細画面の表示方法

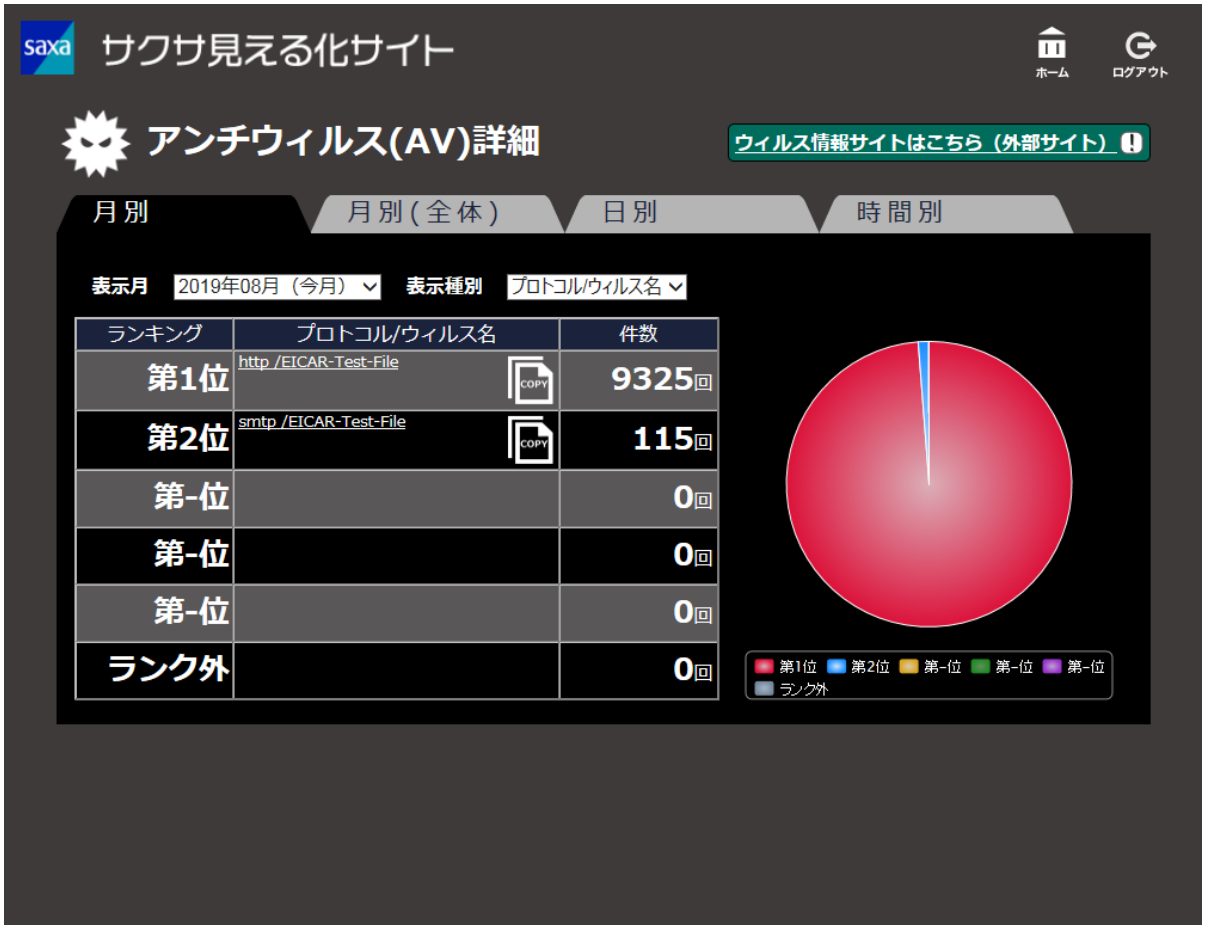
① ホーム画面から詳細アイコン（ ）をクリックします。



② 詳細画面が表示されます。

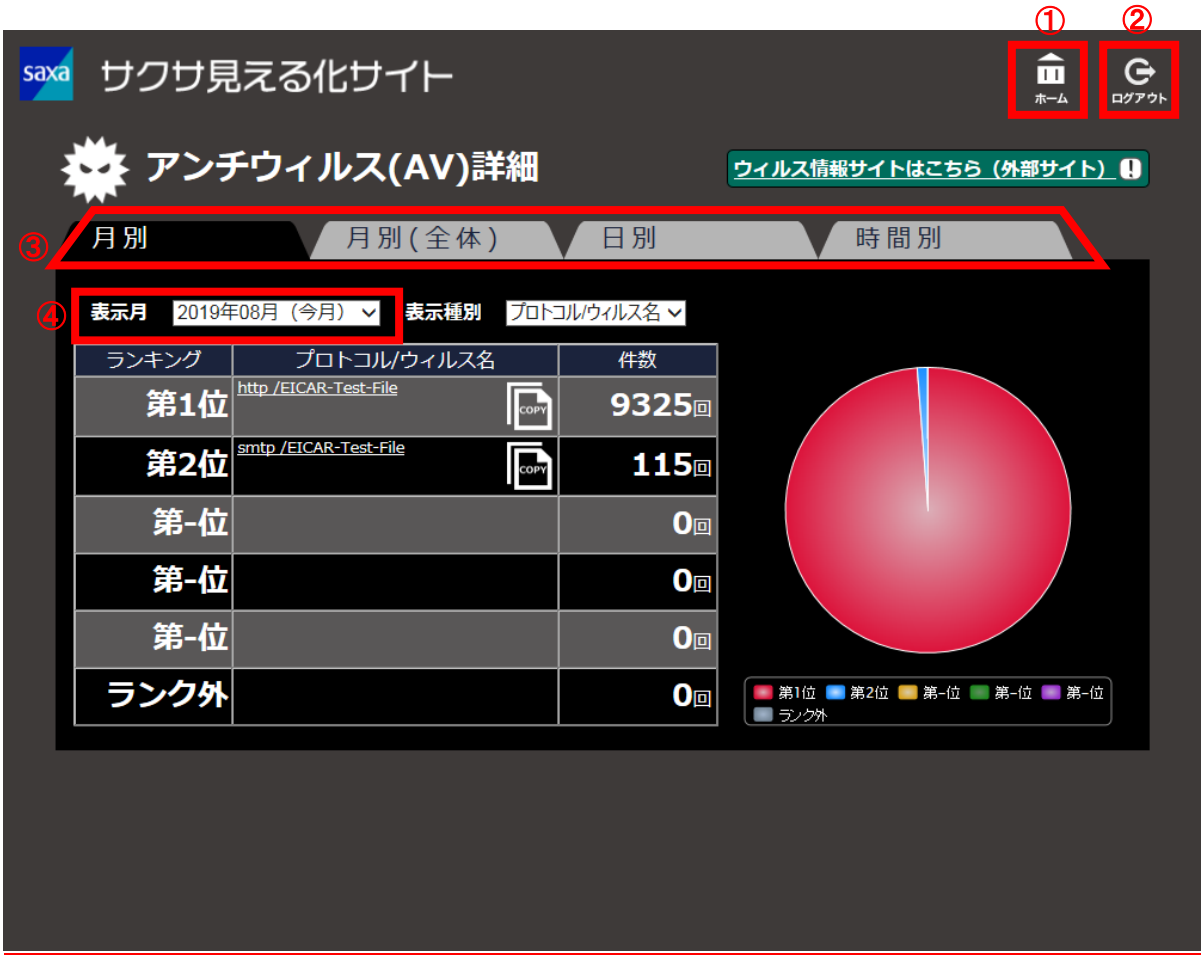
※ 「個別集計」画面で詳細アイコン（ ）をクリックした場合は「月別」画面、「全体傾向」画面で詳細アイコン（ ）をクリックした場合は「月別（全体）」画面が表示されます。

◆「個別集計画面」で AV の詳細アイコンをクリックした場合



3.3.2. 詳細画面の表示内容

- 集計結果は、件数ごとに上位５位までの詳細を表示し、その他の結果は「ランク外」とします。
- ５位までの項目については、集計種別によって以下の内容が表示されます。
  - AV（アンチウイルス）…… 検出したプロトコル / ウィルス名
  - AS（アンチスパム）…… 検出したプロトコル / スパム発信元のメールアドレス
  - IPS（攻撃系）…… 検出した攻撃種別
  - DoS（DoS 攻撃）…… 検出した DoS 攻撃種別 / 発信元
  - URL（URL フィルタリング）…… 検出したアクセス先 URL
  - APC（アプリケーション制御）…… 検出したアプリケーション名

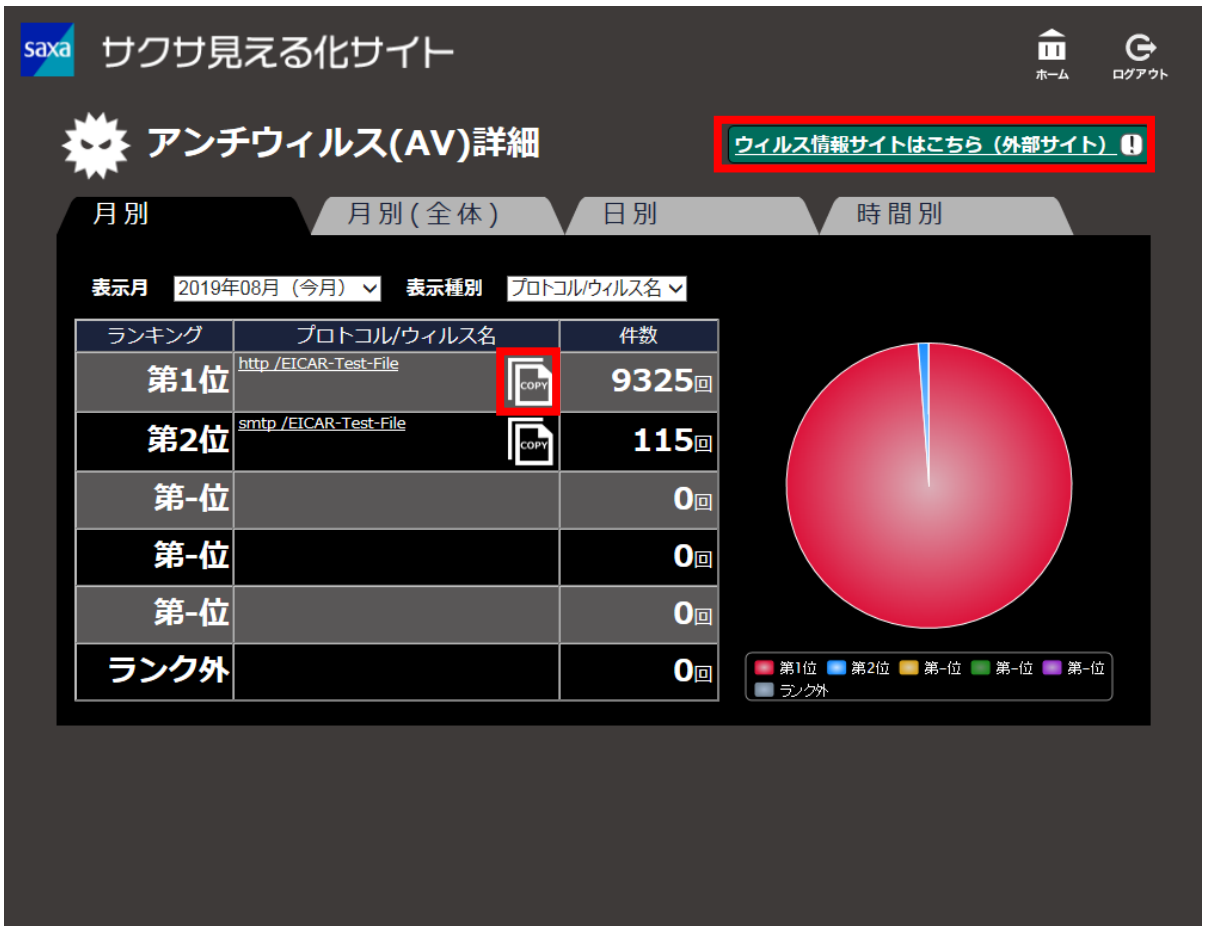


①	ホーム	ホーム画面の「個別集計」画面に戻ります。
②	ログアウト	ログアウトし、ログイン画面へ戻ります。
③	月別／月別（全体）／日別／時間別	各集計画面へ表示を切り替えます。
④	表示月	画面に表示される月を切り替えます。 表示する月を選択します。

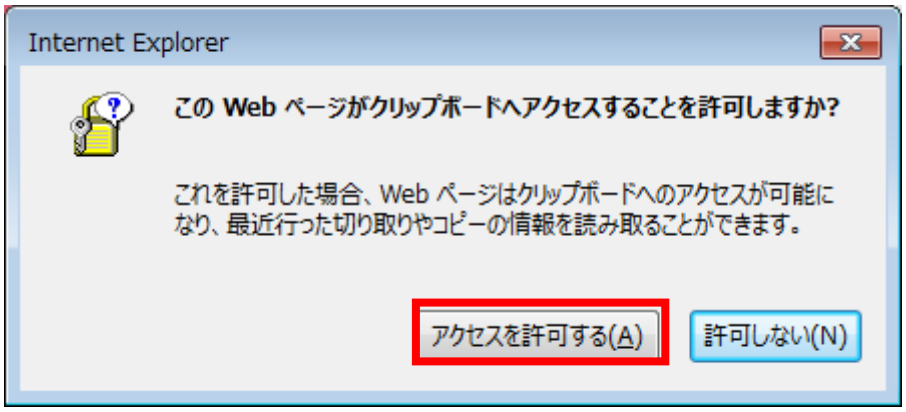
◆ウイルス情報サイトについて

アンチウイルス（AV）の詳細画面にある「ウィルス情報サイトはこちら（外部サイト）」をクリックすると、Kaspersky Lab の Web サイトを新しいタブ（またはウィンドウ）で表示します。

プロトコル/ウィルス名にある COPY アイコン（  ）をクリックすることで、表示されているウィルス名がクリップボードにコピーされますので、Kaspersky Lab サイトでの検索時にご利用ください。



COPY アイコンクリック時に、以下の確認画面が表示された場合は、「アクセスを許可する」をクリックしてください。



※「許可しない」を選択した場合、クリップボードへウィルス名はコピーされません。

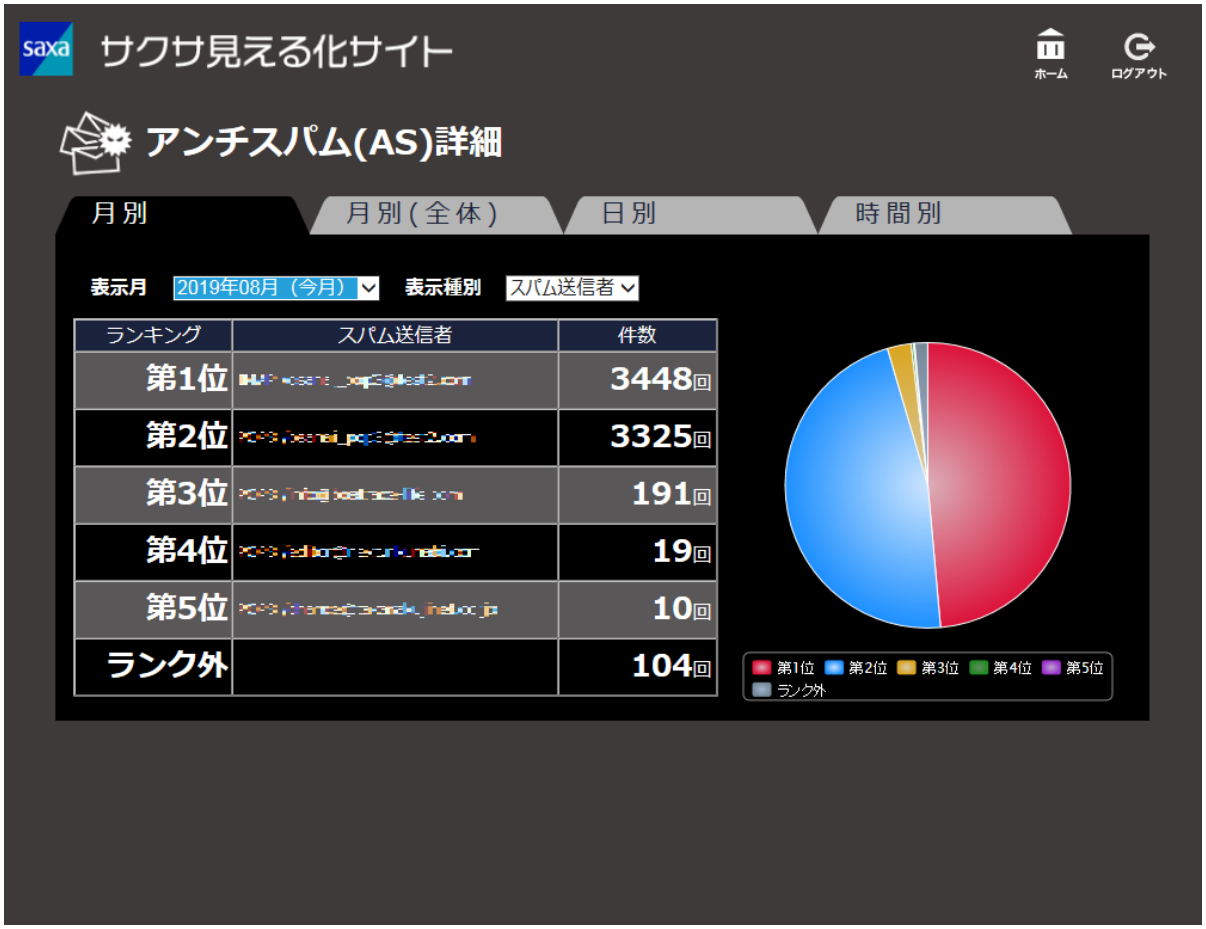
◆Kaspersky Lab サイト

検索ウィンドウに確認したいウイルス名を入力することで、詳細な情報を確認することが出来ます。

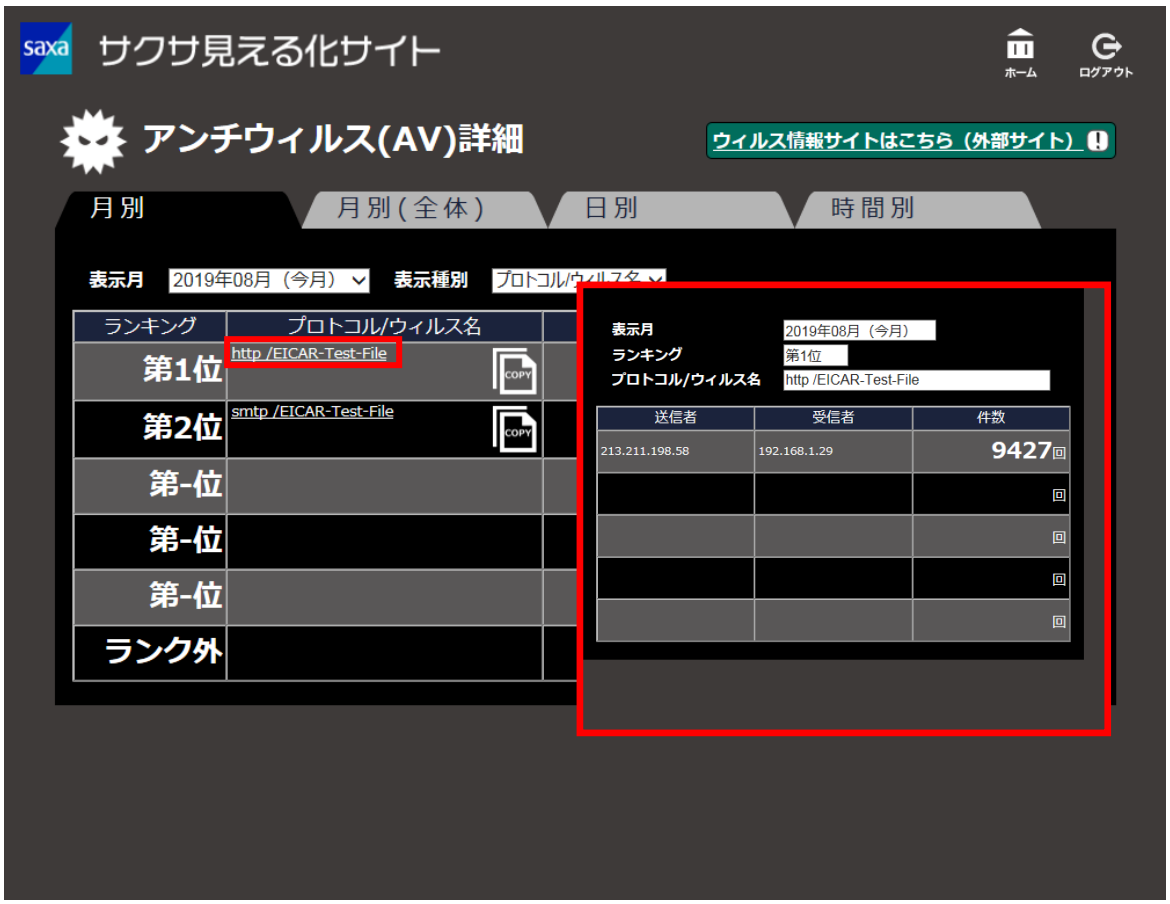
3.3.3. 詳細画面の「月別」画面

ユーザー自身の集計結果を月別に表示する画面です。

◆「個別集計画面」で AS の詳細アイコンをクリックした場合



○検知内容の詳細表示

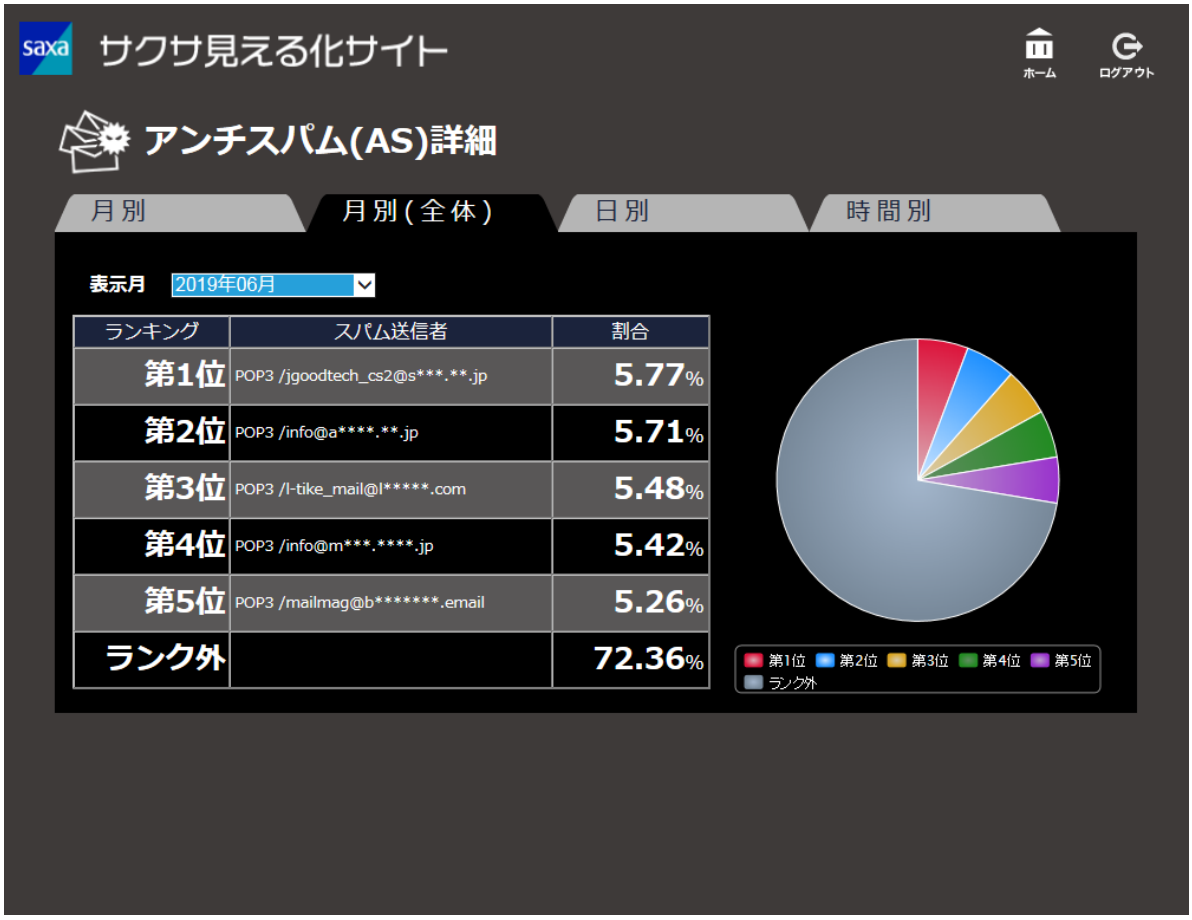


AV、URL、APC の月別表示では、検知した対象のリンクをクリックすることで、
選択した表示種別ごとに、詳細情報が別ウィンドウで表示されます。

3.3.4. 詳細画面の「月別（全体）」画面

サクサ UTM を使用しているユーザー全体の集計結果を表示する画面です。

◆「全体傾向画面」で AS の詳細アイコンをクリックした場合



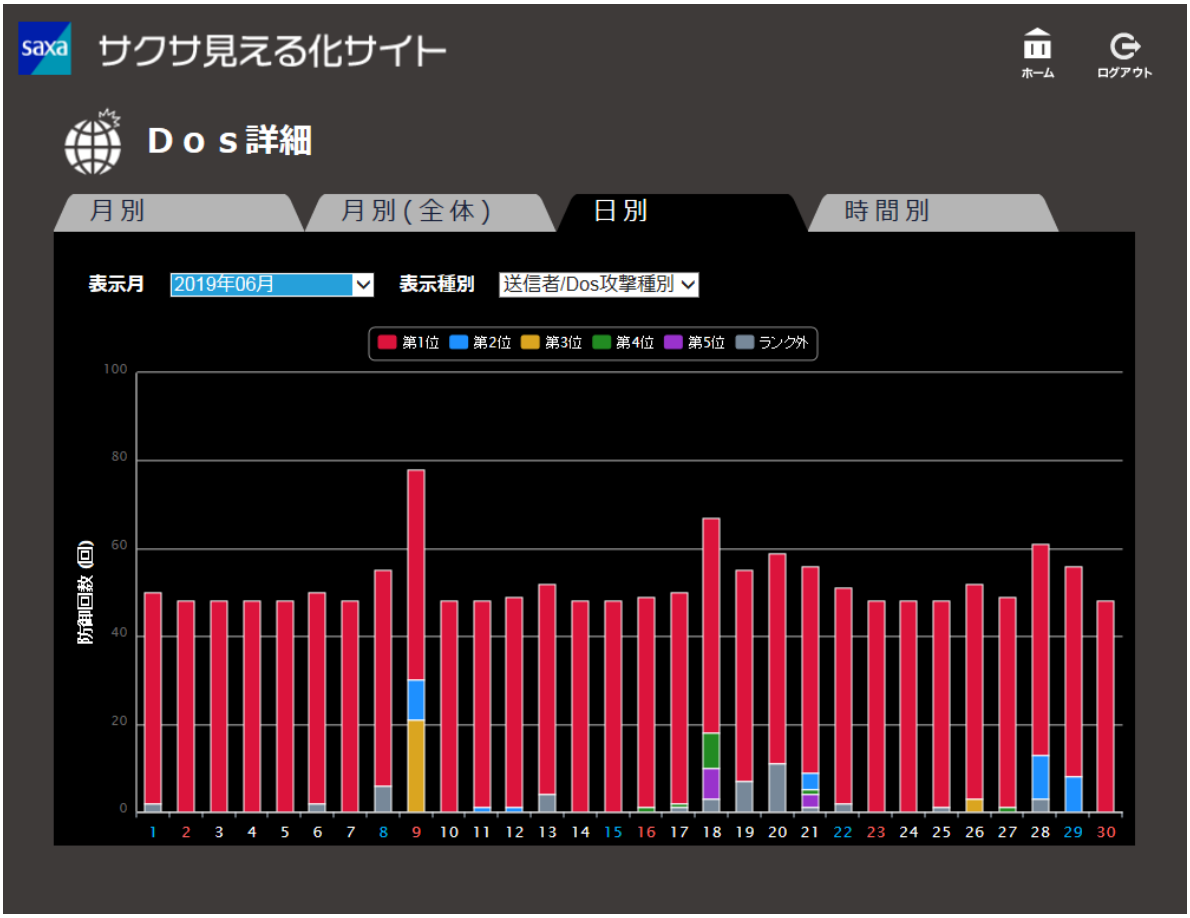
※　AS の詳細（全体傾向）に関しては、スパム発信元のアドレスの@以降は、最初の文字とピリオド、最後のドメインを除いてアスタリスク（＊）に置き換えて表示されます。

3.3.5. 詳細画面の「日別」画面

ユーザー自身の集計結果を日別に表示する画面です。

検出回数が増える期間や曜日などの傾向を確認することができます。

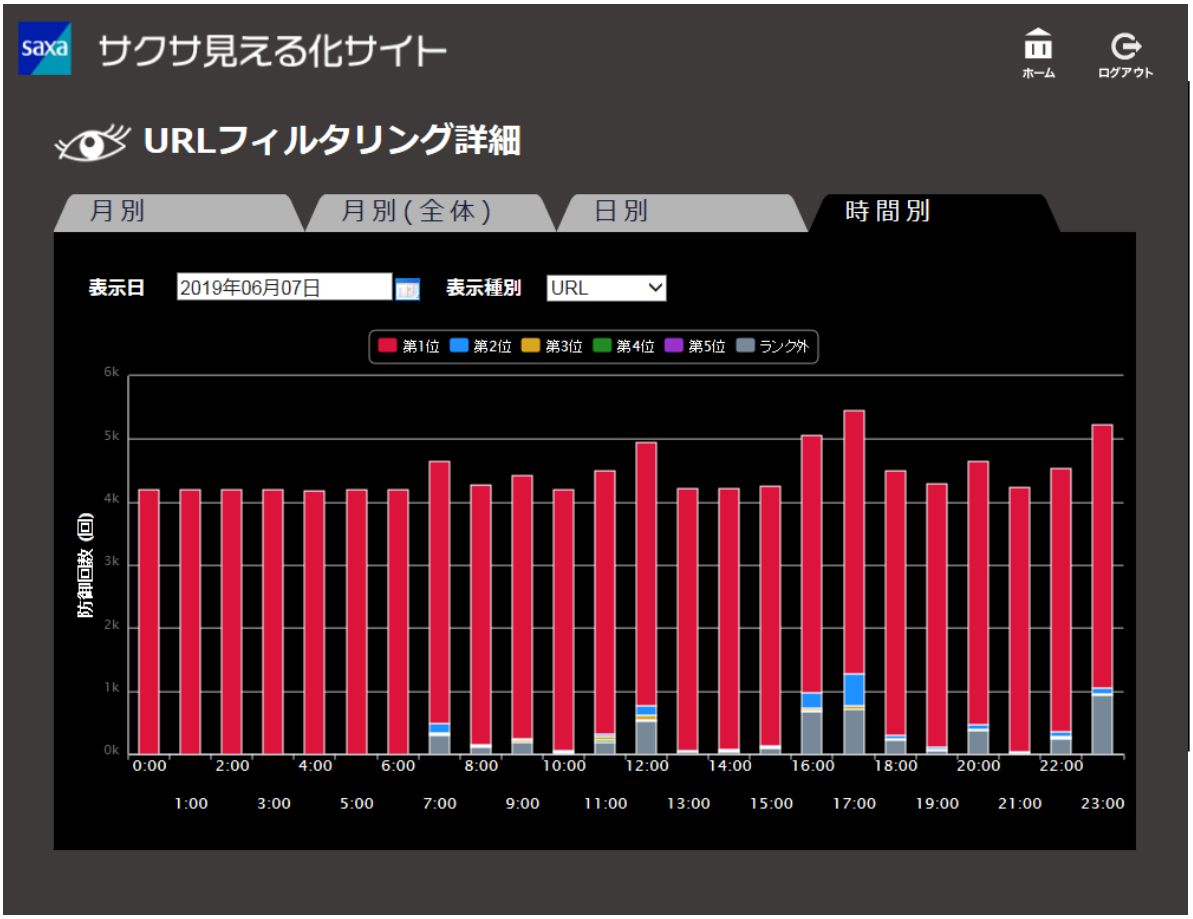
◆DoS 詳細で日別をクリックした場合



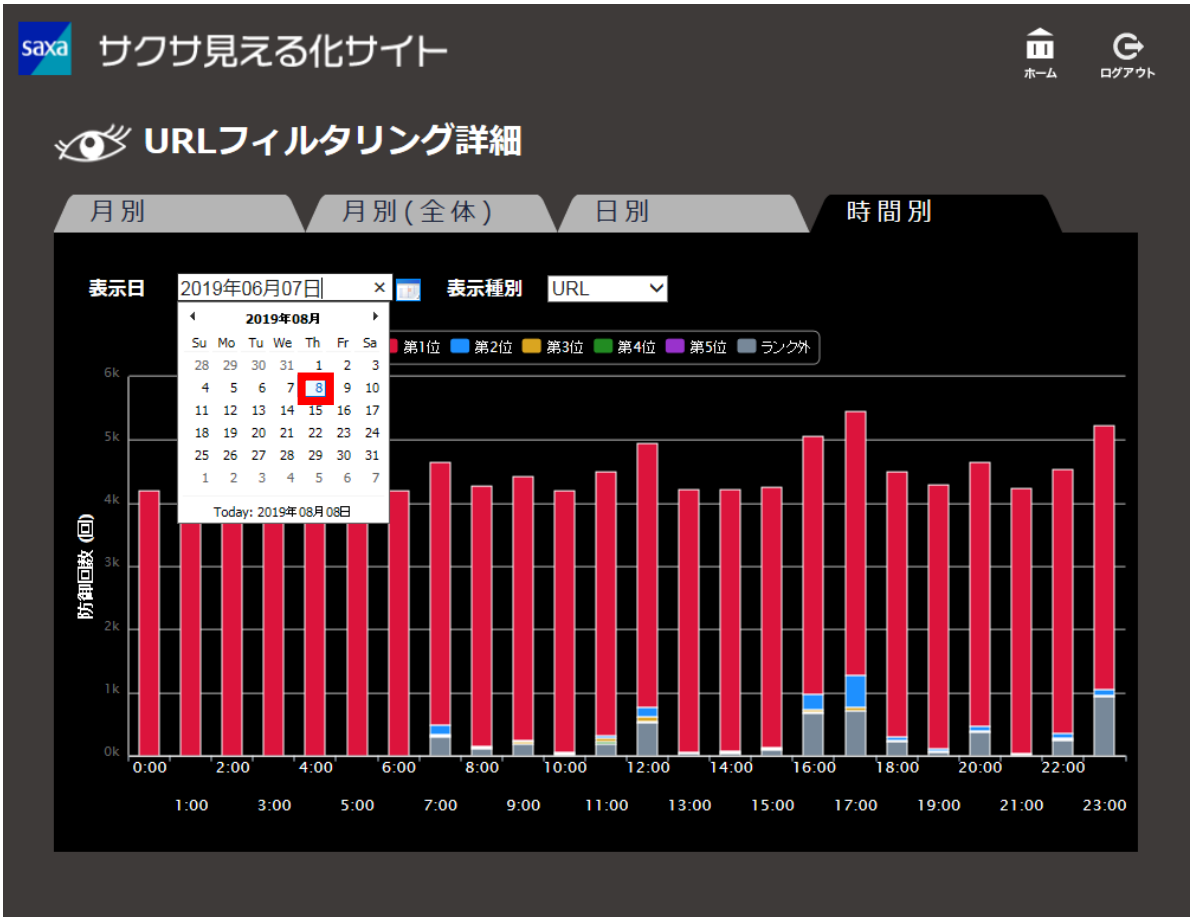
3.3.6. 詳細画面の「時間別」画面

ユーザー自身の集計結果を時間別に表示する画面です。
時間帯ごとの検出傾向を確認することができます。

◆URL フィルタリング詳細で時間別をクリックした場合

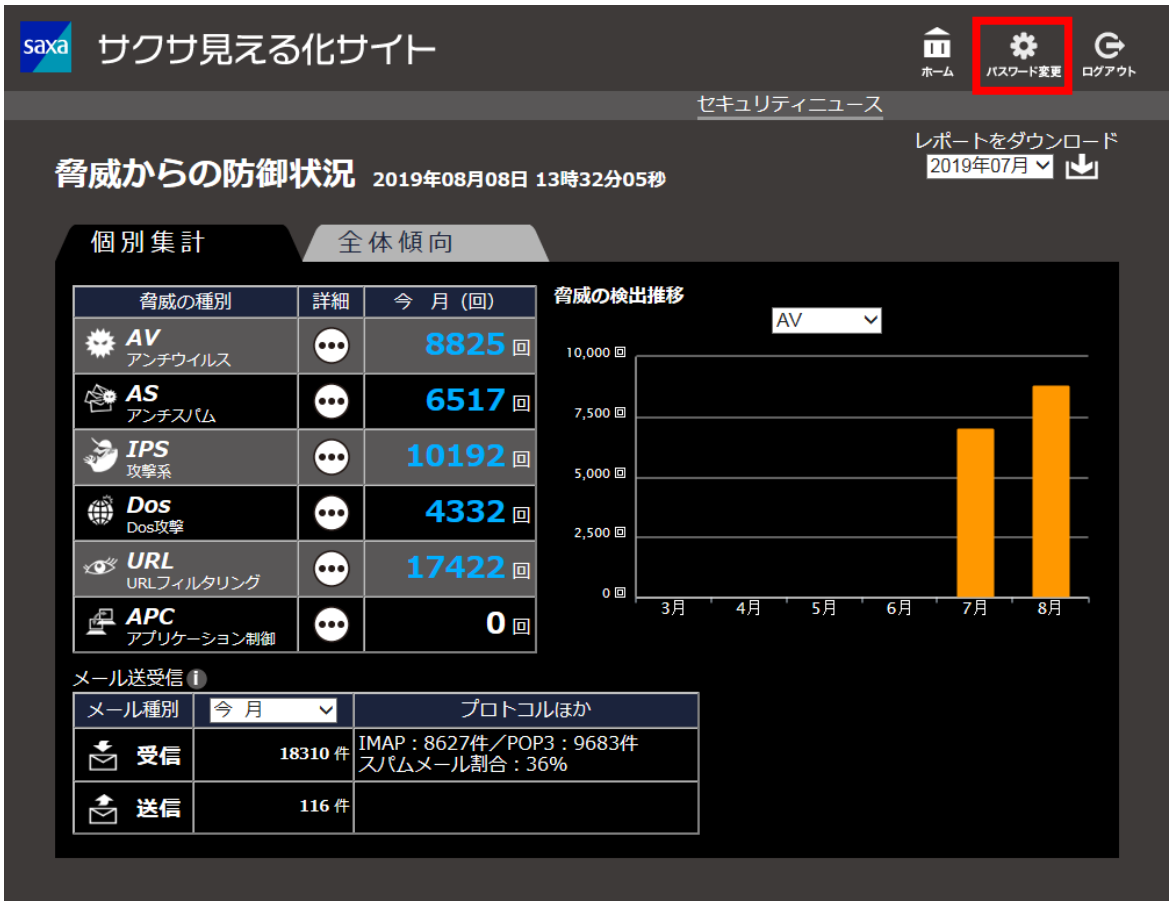


※　表示日を切り替えるには日付部分をクリックして表示されたカレンダーで表示したい日付を選択します。

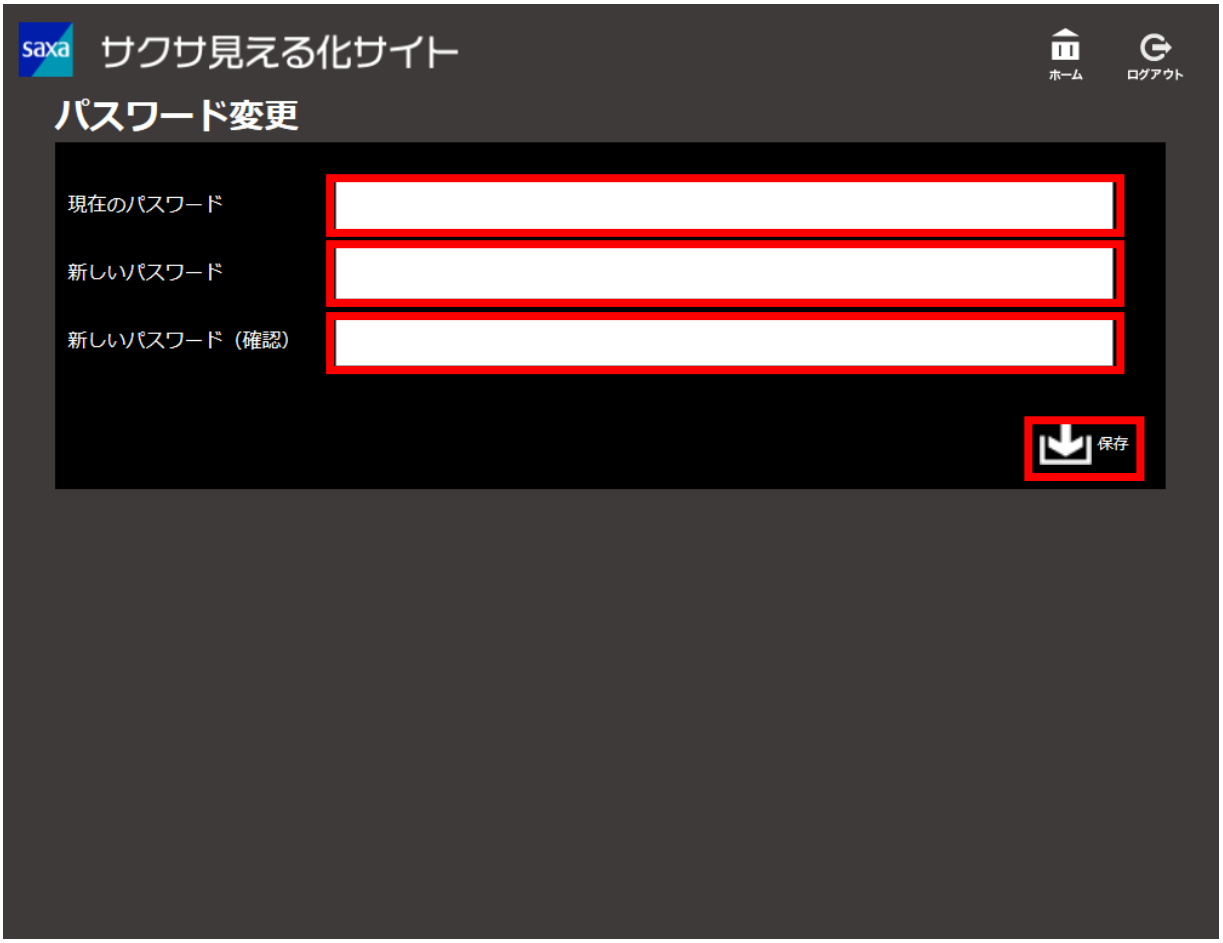


3.4. ユーザーのログインパスワードを変更する

① ホーム画面から、パスワード変更アイコン（  ）をクリックします。



② 現在のパスワードと新しいパスワードを入力し、保存アイコン（  ）をクリックします。

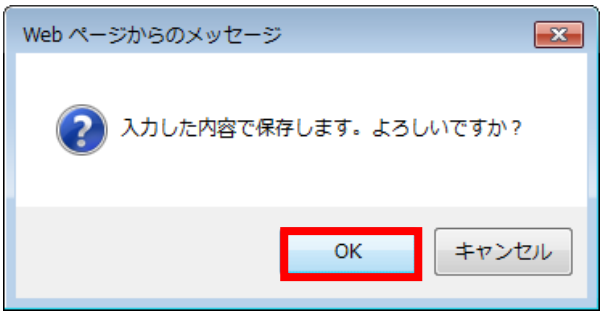


※ パスワードは、半角英数字記号 1～20 文字以内で設定する必要があります。

※ ホームアイコン（  ）をクリックすると、ホーム画面の「個別集計」画面を表示します。

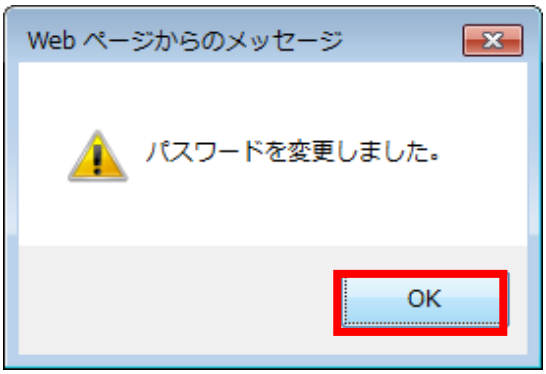
※ ログアウトアイコン（  ）をクリックすると、ログアウトしてログイン画面に戻ります。

③　確認メッセージが表示されますので、 OK ボタンをクリックします。



※　 キャンセル ボタンをクリックするとパスワード変更画面へ戻ります。

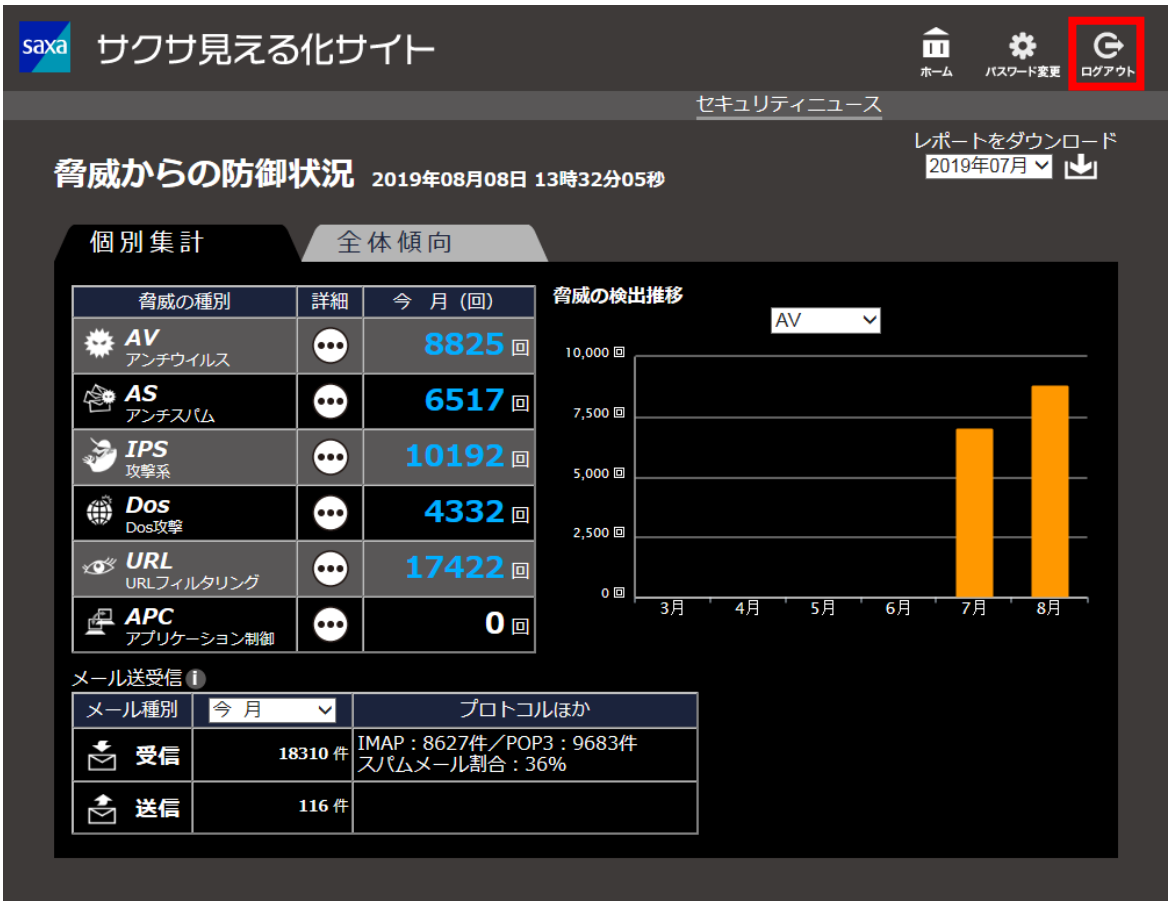
④　変更完了メッセージが表示されますので、 OK ボタンをクリックします。



⑤　ホーム画面に戻ります。次回以降のログイン時は新しいパスワードを使用します。

3.5. ログアウト

① ログイン中、画面右上部に常に表示されているログアウトアイコン（ ）をクリックします。



② ログイン画面に戻ります。

3.6. 月次レポートメール

月上旬に先月分のセキュリティレポートのサマリーをメールで送信します。

月次レポートメールには、月次詳細レポートが添付されます。

月次詳細レポートの参照方法は「◆月次詳細レポートの参照方法について」(12 ページ)をご確認ください。

送信例)

題名：セキュリティレポート[XXXXXXXXXX]

サクサＵＴＭ
『サクサ見える化サイト』レポート配信
発行元：サクサ株式会社

＊本メールは「サクサ見える化サイト」のレポート
配信機能をご依頼されたお客様へ送付しております。
心あたりが無い方は、本メール末尾のサクサビジネスシステム
コールセンターにご連絡ください。

サクサＵＴＭ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。

■お客様名：AAAA

■対象期間：yyyy/mm/dd　～　yyyy/mm/dd

■脅威検出状況：

◎Ｗｅｂフィルタ　　X　件

◎アンチスパム　　X　件

◎アンチウイルス　　X　件

◎不正侵入/検知　　X　件

◎ＡＰＣ制御　　X　件

脅威検出の詳細内容を確認したい場合は、
以下の『サクサ見える化サイト』をご利用ください。

【URL】https://www.utmvisible.biz/saxautm/login.aspx

※サービス開始時に登録されましたメールアドレスに送信されます。

※試用ユーザーアカウントでは送信されません。

４４３５　０６８０　００－８