KDSec セキュリティ監視システム

Web ポータル操作マニュアル

バージョン 1.5

改訂履歴

バージョン	更新日	内容
1.0	2021/03/26	新規作成
1.1	2021/08/05	ログフォーマット変更に伴う変更
1.2	2022/02/01	サービス機能追加に伴う変更
1.3	2022/05/19	ログの時刻についての記述を追加
1.4	2022/06/29	チケットについての記述を追加
1.5	2023/02/10	サービス機能追加に伴う変更、ページ番号追加

目次

1.はじめに

本書は KDSec セキュリティ監視システムの Web ポータルの操作説明書です。Web ポータルは以下サービスご利用のお客様において共通で使用します。

・Prisma Access for Clean Pipe（以下 CleanPipe）
・セキュアインターネット（以下 SIG）
・ゲートウェイセキュリティ powered by Prisma Access（以下 IP-Sec）
・KDDI クラウドプラットフォームサービス（以下 KCPS）
・Wide Area Virtual Switch 2（以下 WVS2）

Webポータルでは、Paloalto PrismaAccess、PA-5260やPAシリーズから出力されたログの分析結果を確認することができる他、サービスオペレータとのQ&Aなどに使用するチケットや、よくある質問(FAQ)に対する回答、およびレポートがご利用いただけます。
Webポータルのメイン画面となるダッシュボードは、お客様の必要な情報を選択して自由に配置することができます。

本書に記載されているシステム名、製品名、会社名などの固有名詞は、一般にその開発元の商標、または登録商標です。本書では、弊社製品の使用方法を説明する目的においてのみ、これらの固有名詞を利用しており、その商標権を侵害する目的や意思はございません。なお、本文中では、TM、©、及び®を明記していない場合があります。

1.1. 免責

本書を KDDI デジタルセキュリティ株式会社の許可無く、KDSec セキュリティ監視システム以外の用途に二次利用することを禁止します。
本書に記載されている仕様、及び製品に関する情報は、必要に応じて予告なしに変更されることがあることをあらかじめご了承ください。

1.2. 用語説明

本書で使用する用語について説明します。

表 1.3-1 用語一覧

用語	説明
CSV	データをカンマや改行で区切って並べたファイルフォーマットで、Web ポータルから情報をダウンロードするときに使用している。
FAQ	よくある質問のこと。Frequently Asked Questions の略語。
PDF	電子文書のためのフォーマットで、月次レポート等に使用している。
PIN	ワンタイムパスワードと同義。6 桁の番号のこと。
KDSec MSS	本書では本サービスを管理・運用するオペレータが所属する組織を指す。
アナリスト	攻撃手法やセキュリティ上の脅威に関する豊富な知識を持ち、インシデントの分析を行うセキュリティ技術者のこと。
アラート	ログを分析した結果、セキュリティに対する懸念がある場合に出される通知のこと。
チケット	お客様と KDSec MSS のコミュニケーションを記録するための機能のことで、開始(オープン)から終了(クローズ)までの一連のコミュニケーションをそれぞれが記入することができる。
デバイス	セキュリティデバイスを短縮した表記で、セキュリティ監視サービスの対象機器のこと。ネットワーク通信を自動的に分析して機器固有のアラートを出すことができるが、誤報が多い。
センサ	デバイスと同義。センサ監視サービスなど、サービス名やサービスの説明部分で使用している。
ログ	セキュリティデバイスが通信内容を分析した結果として出力するテキストデータのこと。
ワンタイムパスワード	ログイン時にパスワード以外に入力が必要な、短時間のみ有効なパスワード(6 桁の数字)のこと。

1.3. 文中の表記に関して

本書における、各書式の意味を下記表に示します。

表 1.3-1 書式説明

書式	意味
太字	操作箇所を示す。
[括弧付き]	必要に応じて、選択する箇所を示す。

2. ログイン

サービスプロバイダから連絡された所定のアドレスに Web ブラウザでアクセスすると、Web ポータルのログイン画面が表示されます。

図 2-1 ログイン画面

Web ポータルがサポートしているブラウザは以下の通りです。各ブラウザは、最新のセキュリティ対策が講じられている最新版をお使いください。PC だけではなく、iPhone と Android スマートフォンの標準ブラウザもサポートしています。

表 2-1 対応ブラウザ

対応ブラウザ名
・ Google Chrome ・ Microsoft Edge ・ Apple Safari

2.1. ログイン

初回ログイン時と、パスワードリセット直後の管理者アカウントでのログイン時には、パスワード変更画面が表示されますので、任意のパスワードを設定してください。パスワードは、**スペース以外の記号が使用でき、英語の大文字と小文字と数字を含む、10 文字以上72文字以下**にする必要があります。

ログイン画面でユーザ ID とパスワードを正しく入力すると、Web ポータルのメイン画面であるダッシュボードが表示されます。

5 回連続でログインに失敗すると、アカウントロックされます。アカウントロックは 1 時間で自動的に解除されますので、再びログインを試行することができます。

2.2. ワンタイムパスワード

ワンタイムパスワードを使った、よりセキュリティ強度の高い二段階認証も可能です。二段階認証を使うように設定したアカウントの場合、ユーザ ID とパスワードを入力すると初回ログイン時に限り、以下の QR コード画面が表示されます。

無償提供されているスマートフォン用の二段階認証アプリである Google Authenticator を使用して QR コードを読み込むことで、二段階認証の準備ができます。

図 2.2-1 QR コード画面

QR コードを読み込んで**完了**ボタンを押すと、PIN コード入力画面になります。

二段階認証を使うユーザのログインが 2 度目以降の場合には、QR コード画面は表示されず、PIN コード入力画面が表示されます。

ワンタイムパスワードは、6 桁の数字からなる PIN コードです。
二段階認証アプリである Google Authenticator に表示される PIN コードを入力すると、ログインすることができます。PIN コードは 30 秒間に限り有効なため、入力タイミングによっては認証に失敗することがあります。この場合は、二段階認証アプリに表示されている最新の PIN コードを再度入力してください。
入力後に**次へ**ボタンを押すと、ダッシュボード画面が表示されます。エンター(改行)キーは押さないでください。

図 2.2-2 PIN コード入力画面

3. ダッシュボード

本分析サービスの状況を表示する、カスタマイズ可能な画面です。

3.1. Web ポータルメニューの構成

まず、Web ポータルの左側に常に表示されているメニューについて説明します。
メニュー内のアイコン上で、マウスを押すと各機能の画面に遷移します。

ダッシュボード画面に遷移 ・・・・・・・・・ 本章で説明

センサ監視 分析結果画面に遷移 ・・・・ 5 章で説明

お知らせ一覧画面に遷移 ・・・・・・・・・ 6 章で説明

チケット一覧画面に遷移 ・・・・・・・・・・ 7 章で説明

レポート画面に遷移 ・・・・・・・・・・・・・ 10 章で説明

ログ表示画面に遷移 ・・・・・・・・・・・・・・ 8 章で説明

FAQ 画面に遷移 ・・・・・・・・・・・・・・・・・ 9 章で説明

ウィジェット画面に遷移 ・・・・・・・・・・・ 4 章で説明

プロファイル画面、
メール通知画面に遷移 ・・・・・・ 11,12,13 章で説明

ログアウト ・・・・・・・・・・・・・・・・・ 14 章で説明

図 3.1-1 Web ポータルメニュー

3.2. ダッシュボードの構成

Web ポータルメニューの**ダッシュボード**を押すと、ダッシュボード画面が表示されます。

初期状態は、お客様へのお知らせのみが表示されます。
ウィジェットを追加して、お客様が必要とする情報を簡単に確認できるようにカスタマイズしてください。ウィジェット追加方法については、次章を参照してください。

お客様へのお知らせに表示されているお知らせの行を選択すると、選択した項目の詳細内容が表示されます。なお、詳細内容がないお知らせを選択しても、詳細内容は表示されません。3 日以内に更新されたお知らせは、”NEW”が表示されます。右上にある「**一覧を表示**」を押すと、お知らせ一覧画面に遷移します。

チケット一覧に表示されているチケットの行を選択すると、選択したチケットの詳細が表示されます。チケット一覧のウィジェットの右上にある「**一覧を表示**」を押すと、チケット一覧画面に遷移します。

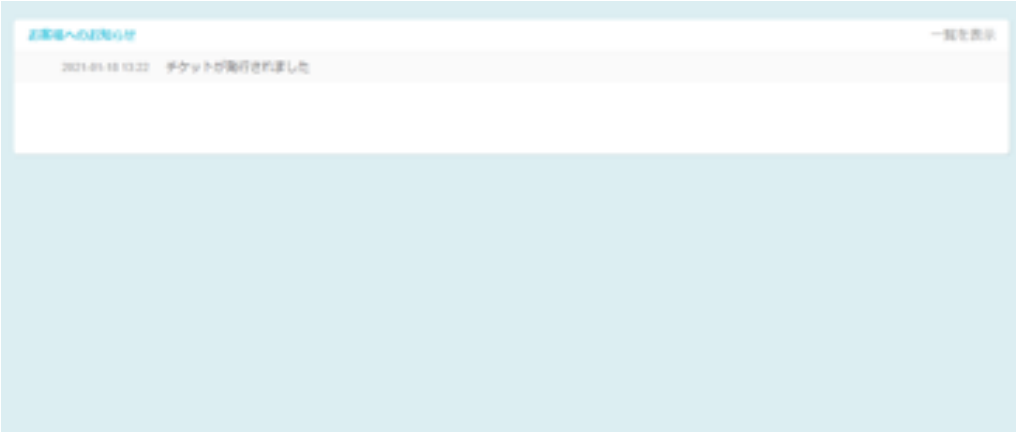


図 3.2-1 ダッシュボードの初期画面

ダッシュボードをカスタマイズした一例を下図に示します。このように、必要な情報をすぐに確認できるよう、表示するウィジェットを選択し、任意の位置に配置することができます。
ただし、ダッシュボード画面最上部の、お客様へのお知らせの部分は位置を固定していますので、移動できません。

グラフウィジェットに限り、右下の 」マークを押してドラッグすることで拡大、縮小することが可能です(後述の「4.2.ウィジェット拡大・縮小」を参照ください)。

ご利用のサービス内容や、確認したい内容に応じて表示内容や表示位置をカスタマイズしてお使いください。
ウィジェットの種類・内容、および追加に関する操作は、次章を参照してください。

図 3.2-2 ダッシュボードのカスタマイズ例

4. ウィジェット

ウィジェットとは、小さいプログラムの意味で、ダッシュボードに複数のウィジェットを表示して、本分析サービスの状況を確認することができます。ご利用のサービス内容や、確認したい内容に応じて表示内容や表示位置をカスタマイズすることができます。

Web ポータルの左側に表示されている**ウィジェット**を押すと、ウィジェット設定画面が表示されます。ダッシュボード画面とほぼ同様に見えますが、移動できない「お客様へのお知らせ」の部分がグレーアウトされており、右下に ＋ マークのボタンが表示されます。

図 4-1 ウィジェット

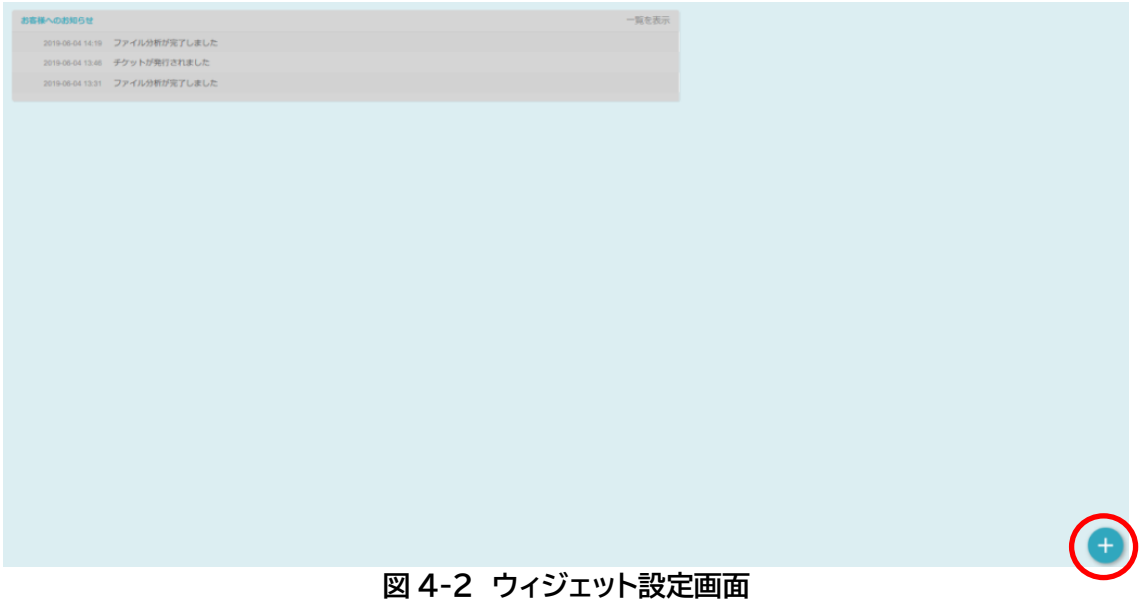


図 4-2 ウィジェット設定画面

4.1. ウィジェット追加

ウィジェット設定画面で右下の+マークのボタンを押すと、ウィジェット追加画面が表示されます。

この画面で、ウィジェットの分類、ウィジェットの種類や表示方法などを、プルダウンメニューで選択します。

選択した後に**追加**ボタンを押すと、ウィジェット設定画面の最下部に選択したウィジェットが追加されます。

利用できるウィジェットの種類と、選択方法については、次項で説明します。

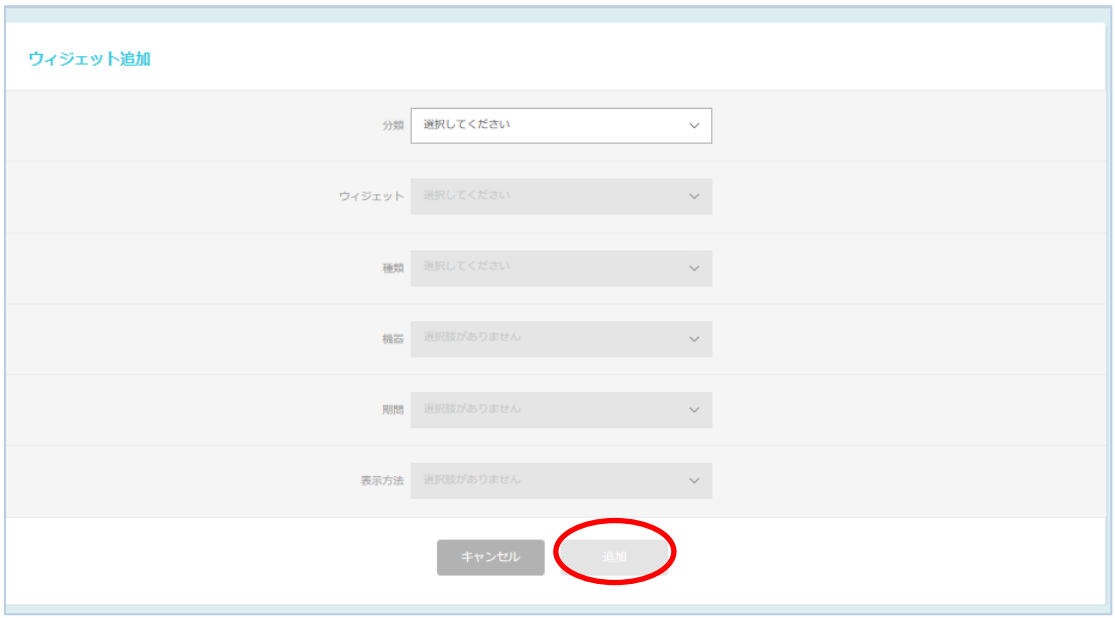


図 4.1-1 ウィジェット追加画面

4.1.1. ウィジェット一覧

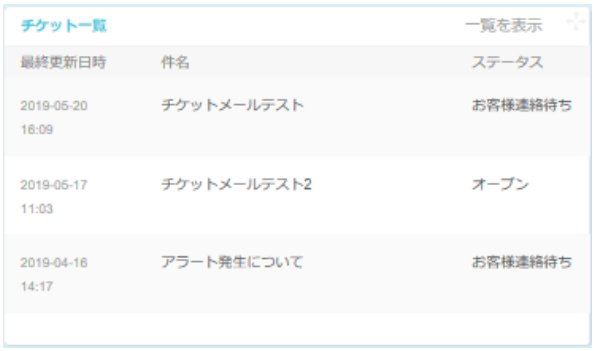
利用可能なウィジェットは以下の通りです。

表 4.1.1-1 ウィジェット一覧

ウィジェット	種類	説明
チケット一覧	チケット一覧	チケットの一覧を表示します
サービス状況	アラート発生状況	アラート発生状況を表示します
	ログ処理状況	ログ処理の状況を表示します
	センサ別ステータス一覧	センサ別のステータス一覧を表示します
アラート一覧	アラート一覧	アラートの一覧を表示します
アラート件数	今日のアラート件数	今日検知したアラート件数を表示します
	アラート件数（全体）	指定した期間内に検知したアラート件数を表示します
	アラート重要度別件数	指定した期間内に検知したアラートの需要度別の件数を表示します
	アラート重要度別占有率	指定した期間内に検知したアラートの需要度別占有率を表示します
	アラート概要別件数	指定した期間内に検知したアラートの概要別に件数を表示します
	アラート概要別占有率	指定した期間内に検知したアラートの概要別占有率を表示します
ログ件数	今日のログ件数	今日のログ件数を表示します
	今月のログ件数	今月のログ件数を表示します
	ログ件数（全体）	指定した期間内における全機器のログ件数を表示します
	ログ件数（センサ別）	指定した期間内におけるセンサ別のログ件数を表示します
ログ処理量	今日のログ処理量	今日のログ処理量を表示します
	今月のログ処理量	今月のログ処理量を表示します
	今日のログ処理量と基準値	今日のログ処理量と基準値を対比表示します
	今月のログ処理量と契約量	今月のログ処理量と契約量を対比表示します
	センサ監視状況付き ログ処理グラフ（全体）	センサ監視状況付きログ処理グラフを表示します
	センサ監視状況付き ログ処理グラフ（センサ別）	センサ監視状況付きログ処理グラフを表示します
	ログ処理量（全体）	指定した期間のログ処理量を表示します
	ログ処理量（センサ別）	指定した期間のセンサ別のログ処理量を表示します
ログダウンロード保存量	ログダウンロード保存量	ログダウンロード保存量を表示します

各ウィジェットの概要と追加方法を以下に記します。
一部のウィジェットでは、「**一覧を表示**」を押すと、対応する項目の一覧が表示されます。
なお、【期間】および【表示方法】については選択肢の一例をあげています。

・チケット一覧:チケットの一覧を表示します。



追加方法
【分類】>【UTM サービス】
【ウィジェット】>【チケット一覧】
【種類】>【チケット一覧】

図 4.1.1-1 チケット一覧

・アラート発生状況:アラート発生状況を表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【サービス状況】
【種類】>【アラート発生状況】

図 4.1.1-2 アラート発生状況

・ログ処理状況:ログ処理の状況を表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【サービス状況】
【種類】>【ログ処理状況】

図 4.1.1-3 ログ処理状況

・センサ別ステータス一覧:センサ別のステータス一覧を表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【サービス状況】
【種類】>【センサ別ステータス一覧】

図 4.1.1-4 センサ別ステータス一覧

・アラート一覧:アラートの一覧を表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート一覧】
【種類】>【アラート一覧】

図 4.1.1-5 アラート一覧

・今日のアラート件数:今日検知したアラート件数を表示します。

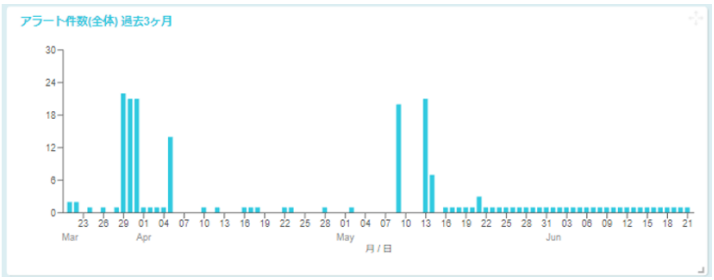
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート件数】
【種類】>【今日のアラート件数】

図 4.1.1-6 今日のアラート件数

・アラート件数(全体):指定した期間内に検知したアラート件数を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、棒グラフまたは折れ線グラフを選択できます。
グラフ型ウィジェットの場合、グラフ上にマウスカーソルを合わせると、吹き出しのようなツールチップが表示され、詳細な数値情報を確認することができます。



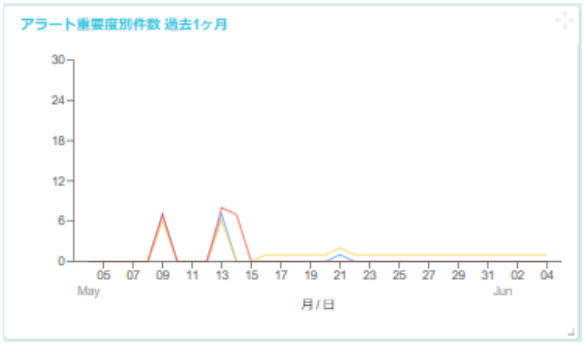
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート件数】
【種類】>【アラート件数グラフ全体】
【期間】>【過去 3 ヶ月】
【表示方法】>【棒グラフ】

図 4.1.1-7 アラート件数(全体)

・アラート重要度別件数:指定した期間内に検知したアラートの重要度別件数を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、折れ線グラフまたは積み上げ棒グラフを選択できます。



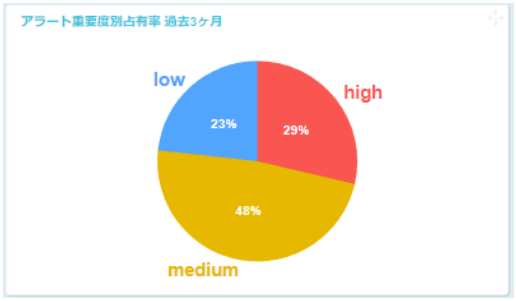
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート件数】
【種類】>【アラート件数グラフ重要度別件数】
【期間】>【過去 1 ヶ月】
【表示方法】>【折れ線グラフ】

図 4.1.1-8 アラート重要度別件数

・アラート重要度別占有率:指定した期間内に検知したアラートの重要度別占有率を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、円グラフまたはドーナツグラフを選択できます。



追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート件数】
【種類】>【アラート件数グラフ重要度別占有率】
【期間】>【過去 3 ヶ月】
【表示方法】>【円グラフ(割合)】

図 4.1.1-9 アラート重要度別占有率

・アラート概要別件数:指定した期間内に検知したアラートの概要別に件数を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

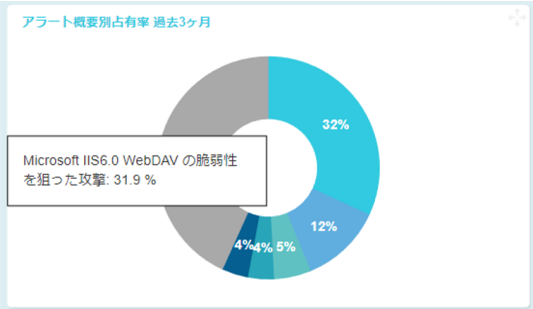
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート件数】
【種類】>【アラート件数グラフ概要別件数】
【期間】>【過去 1 ヶ月】

図 4.1.1-10 アラート概要別件数

・アラート概要別占有率:指定した期間内に検知したアラートの概要別占有率を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、円グラフまたはドーナツグラフを選択できます。
グラフ上にマウスカーソルを合わせると、吹き出しのようなツールチップが表示され、各分類のアラート概要が表示されます。



追加方法
【分類】>【UTM サービス】
【ウィジェット】>【アラート件数】
【種類】>【アラート件数グラフ概要別占有率】
【期間】>【過去 1 ヶ月】
【表示方法】>【円グラフ(上位 5 件とその割合)】

図 4.1.1-11 アラート概要別占有率

・今日のログ件数:今日のログ件数を表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ件数】
【種類】>【今日のログ件数】

図 4.1.1-12 今日のログ件数

・今月のログ件数:今月のログ件数を表示します。

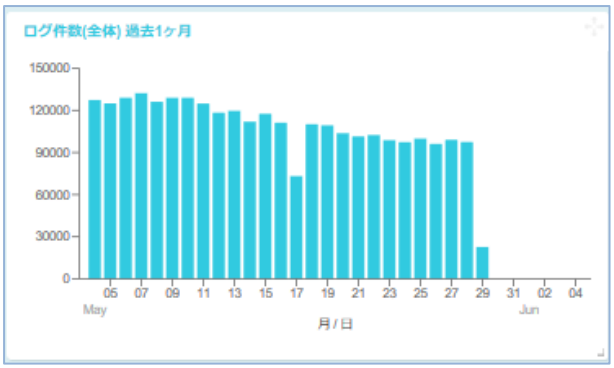
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ件数】
【種類】>【今月のログ件数】

図 4.1.1-13 今月のログ件数

・ログ件数(全体):指定した期間内のログ件数を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、棒グラフまたは折れ線グラフを選択できます。



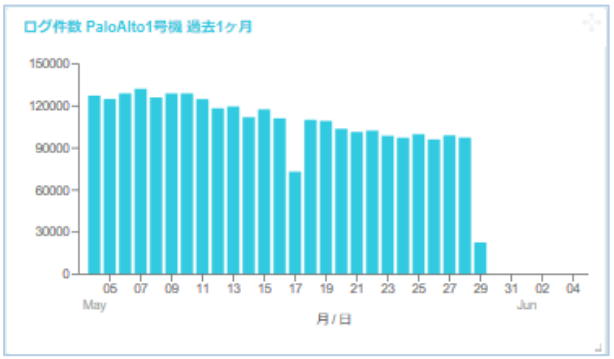
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ件数】
【種類】>【ログ件数グラフ全体】
【期間】>【過去 1 ヶ月】
【表示方法】>【棒グラフ】

図 4.1.1-14 ログ件数(全体)

・ログ件数(センサ別):指定した期間内におけるセンサ別のログ件数を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、棒グラフまたは折れ線グラフを選択できます。



追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ件数】
【種類】>【ログ件数グラフセンサ別】
【機器】>【登録した機器】
【期間】>【過去 1 ヶ月】
【表示方法】>【棒グラフ】

図 4.1.1-15 ログ件数(センサ別)

・今日のログ処理量:今日のログ処理量を表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】>【今日のログ処理量】

図 4.1.1-16 今日のログ処理量

・今月のログ処理量:今月のログ処理量を表示します。

月間契約量と契約量比も表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】>【今月のログ処理量】

図 4.1.1-17 今月のログ処理量

・今日のログ処理量と基準値:今日のログ処理量と基準値を対比表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】
>【今日のログ処理量と基準値との対比表示】

図 4.1.1-18 今日のログ処理量と基準値

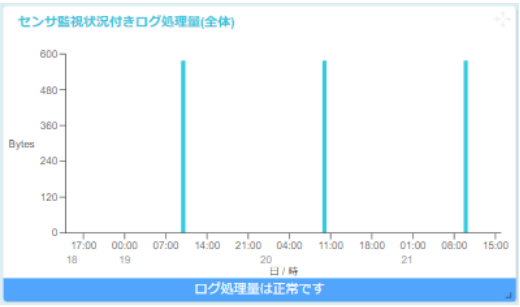
・今月のログ処理量と契約量:今月のログ処理量と契約量を対比表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】
>【今月のログ処理量と契約量との対比表示】

図 4.1.1-19 今月のログ処理量と契約量

・センサ監視状況付きログ処理量グラフ(全体):センサ監視状況付きログ処理量を表示します。

表示方法は、棒グラフまたは折れ線グラフを選択できます。

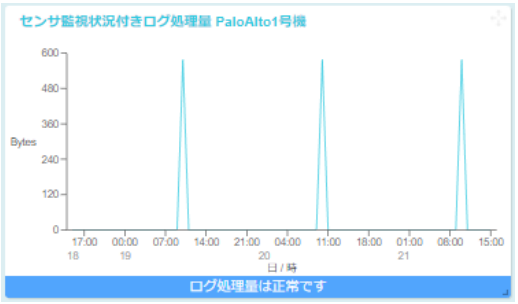


追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】
>【センサ監視状況付きログ処理量グラフ全体】
【表示方法】>【棒グラフ】

図 4.1.1-20 センサ監視状況付きログ処理量グラフ(全体)

・センサ監視状況付きログ処理量グラフ(センサ別):センサ監視状況付きログ処理量を表示します。

表示方法は、棒グラフまたは折れ線グラフを選択できます。



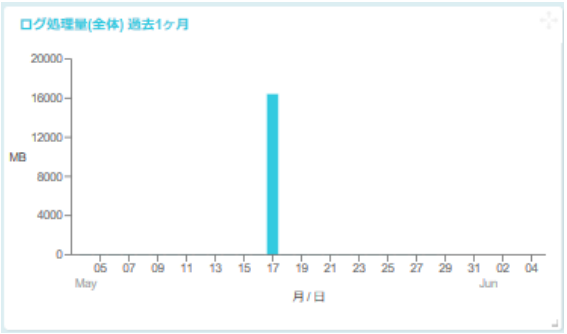
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】
>【センサ監視状況付きログ処理量グラフセンサ別】
【機器】>【登録した機器】
【表示方法】>【折れ線グラフ】

図 4.1.1-21 センサ監視状況付きログ処理量グラフ(センサ別)

・ログ処理量(全体):指定した期間のログ処理量を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、棒グラフまたは折れ線グラフを選択できます。



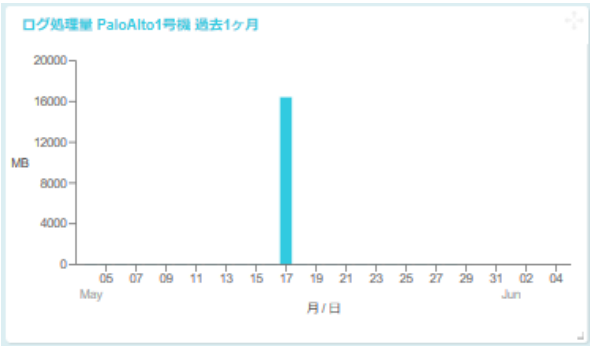
追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】>【ログ処理量グラフ全体】
【期間】>【過去 1 ヶ月】
【表示方法】>【棒グラフ】

図 4.1.1-22 ログ処理量グラフ(全体)

・ログ処理量(センサ別):指定した期間のセンサ別のログ処理量を表示します。

期間は以下の7種類から選択できます。
過去 1 日/過去 3 日/過去 1 週間/過去 1 か月/過去 3 か月/過去 6 か月/過去 12 か月

表示方法は、棒グラフまたは折れ線グラフを選択できます。



追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログ処理量】
【種類】>【ログ処理量グラフセンサ別】
【機器】>【登録した機器】
【期間】>【過去 1 ヶ月】
【表示方法】>【棒グラフ】

図 4.1.1-23 ログ処理量グラフ(センサ別)

・ログダウンロード保存量:ダウンロードできるログの保存量を表示します。

契約量と契約量比も表示します。

追加方法
【分類】>【UTM サービス】
【ウィジェット】>【ログダウンロード保存量】
【種類】>【ログダウンロード保存量】

図 4.1.1-24 ログダウンロード保存量

4.2. ウィジェット拡大・縮小

ウィジェットの右下にマウスカーソルを合わせドラッグすることで拡大・縮小します。
ウィジェットの拡大・縮小はグラフのウィジェットのみ可能です。スペースがある場合のみ、拡大できます。

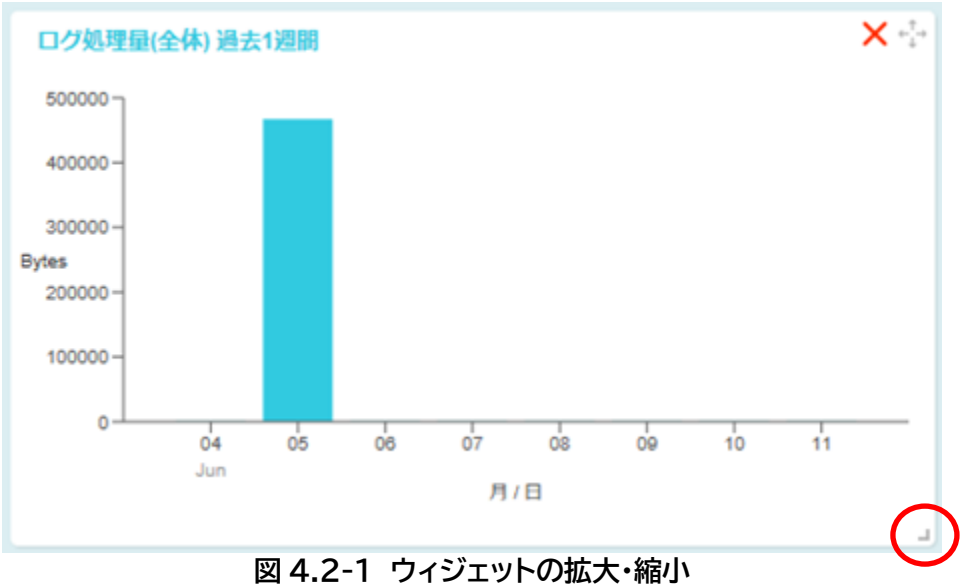


図 4.2-1 ウィジェットの拡大・縮小

4.3. ウィジェット移動

ウィジェットの右上にマウスカーソルを合わせドラッグすることで移動します。
移動先のスペースが空いていない場合ウィジェットの移動はできません。

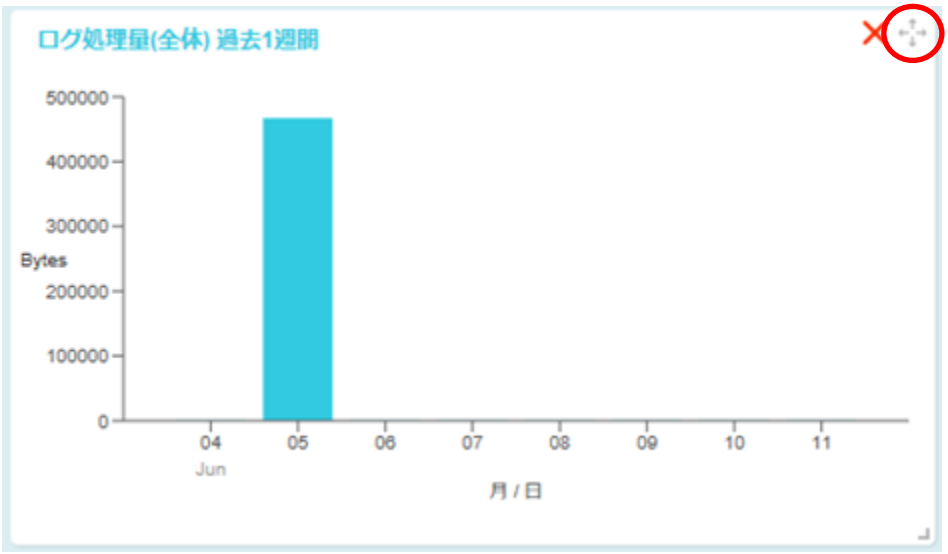


図 4.3-1 ウィジェットの移動

4.4. ウィジェット削除

ウィジェットの右上にあるバツ印を押すことで削除します。

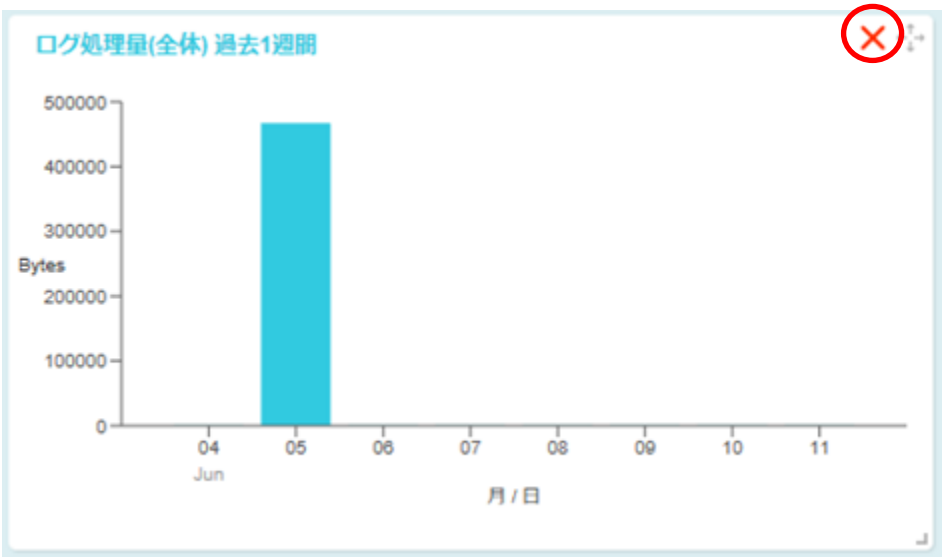


図 4.4-1 ウィジェットの削除

5. センサ監視

5.1. 分析結果一覧

Web ポータルの左側メニューの**センサ監視**を押すと、センサ監視の分析結果一覧が表示されます。項目名を押すことで**検知日時**、**重要度**、**対応**のいずれかで並び替えることができます。また、各分析結果を押すと、アラートの詳細情報が表示されます。

初期状態は過去 1 か月のセンサ監視分析結果を表示します。過去 1 か月以前のセンサ監視分析結果を表示したい場合は、虫眼鏡ボタンを押し、検索画面を開きます（5.3 参照）。

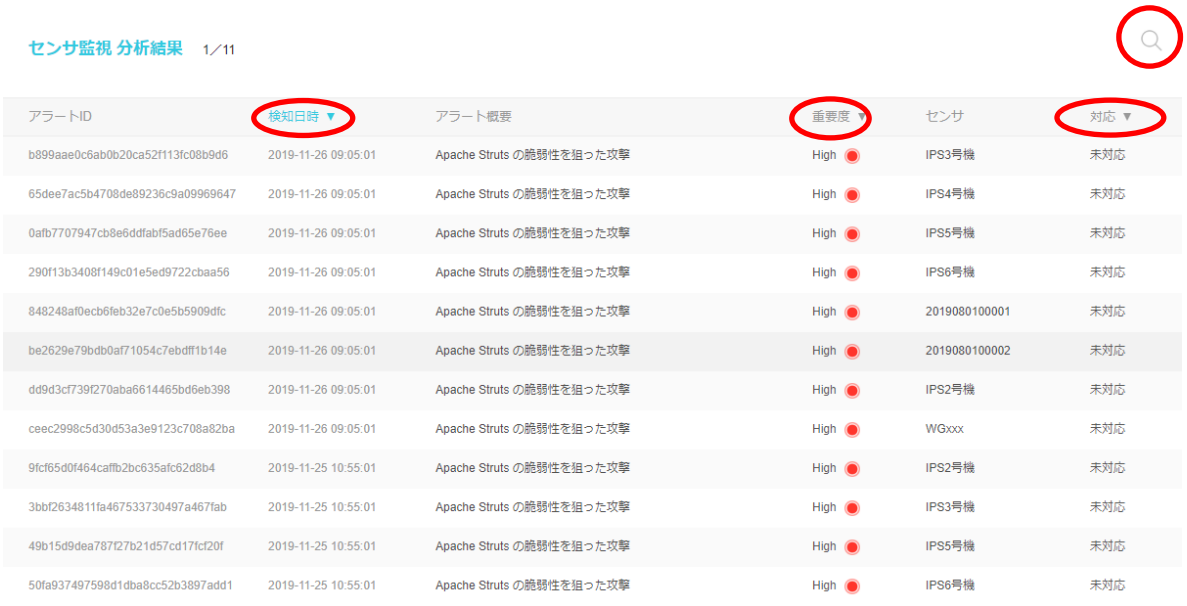


図 5.1-1 センサ監視 分析結果一覧

5.2. アラート詳細

センサ監視分析結果画面から任意の行を選択すると、アラート詳細画面が表示されます。

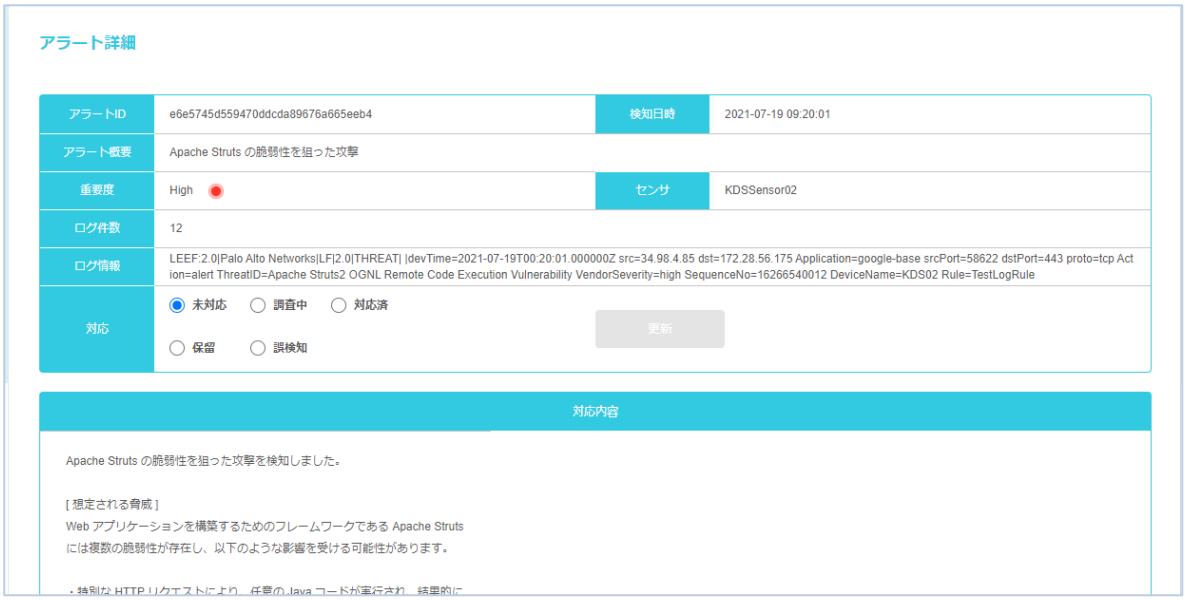


図 5.2-1 アラート詳細画面

アラート詳細画面の表示項目は以下のとおりです。

表 5.2-1 アラート詳細情報

項目	内容
アラート ID	アラート固有の識別番号。
検知日時	アラートを検知した日時。
アラート概要	アラートの概要。
重要度	重要なものから順に、High, Medium, Low の 3 段階で表示する。
センサ	アラートを検知したセンサの名称。
関連チケット番号	アラートに関連したチケットを発行した時のみ、関連チケット番号を表示する。
ログ件数	アラートを検知したログ数。同じアラートを同日に大量に検知した場合、アラートは 1 件に集約しログ件数に集約した数を表示する。
ログ情報	アラートを検知したログデータ。集約したときには、最初に検知したログを表示する。
対応内容	アナリストによるアラートの原因についての説明、推奨する対処方法、調査するときに必要な参考情報の URL などを表示する。

センサ監視アラートは、お客様の対応状況を設定することが可能です。下記表の項目から選択して設定してください。初期状態は未対応となっています。

表 5.2-2 対応の設定

対応項目	状況
未対応	初期状態。
調査中	調査や対策を検討している状態。
対応済	対応が完了した状態。
保留	対応の優先度が低いと思われるときなど。
誤検知	正常な通信をアラートとして検知していると考えられるときや、使用していないソフトに対する攻撃アラートなど。

対応内容に記載している情報を元に、対処を検討することができます。深刻なアラートが多く検出される場合には、弊社の C119 取次サービスなどの専門機関に相談されることをお勧めします。

アラートに関し、不明点がある場合、アラート詳細画面下部の**チケット発行**ボタンを押し、質問事項を記載してください。KDSec-MSS オペレータが回答します。

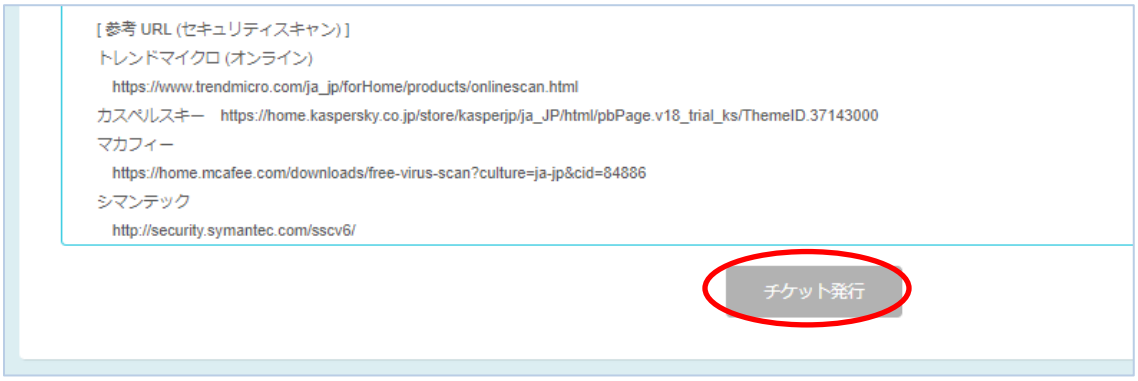


図 5.2-2 アラート詳細画面 チケット発行

チケット発行の詳細については、7 章を参照してください。

5.3. 分析結果検索

図 5.1-1 の画面で右上の**虫眼鏡ボタン**を押すと、図 5.3-1 のような検索画面が表示されます。検索画面では検知日、重要度、センサ、対応、アラート概要、アラート詳細の項目について絞り込みを行うことができます。各項目を入力後、**適用**ボタンを押すと検索条件に一致した分析結果一覧が表示されます。**クリア**ボタンを押すと検索項目の設定を初期設定に戻します。

誤検知に設定したアラートと同様のアラートは 30 日間分析結果一覧に表示されなくなりますが、検索画面の対応の項目で**抑止**にチェックを入れることで確認できるようになります。

図 5.3-1 センサ監視　分析結果検索

6. お知らせ

6.1. お知らせ一覧

Web ポータル左側メニューの**お知らせ**を押すと、サポートセンターからのお知らせ一覧が表示されます。

お知らせの最大表示件数は 25 件と 50 件から選択できます。

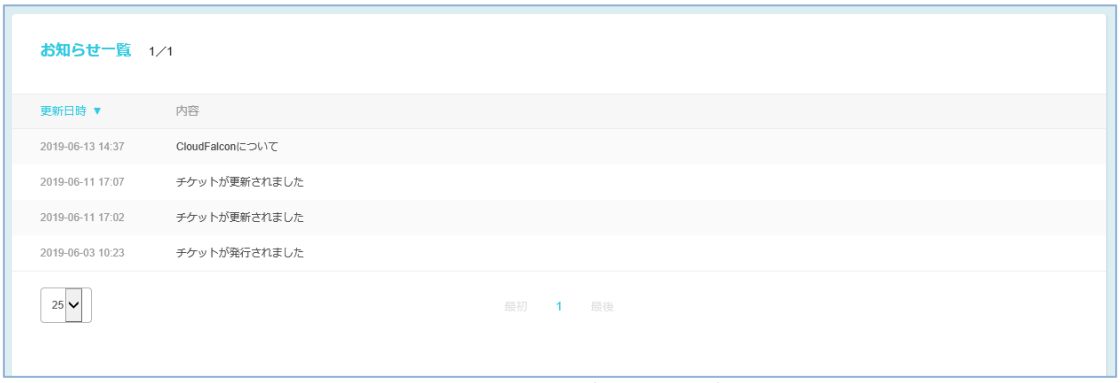


図 6.1-1 お知らせ一覧

6.2. お知らせ詳細

お知らせには詳細情報があるものとないものの 2 種類があります。詳細情報のあるお知らせを一覧画面で選択したときには、お知らせ詳細画面に遷移します。

なお、お知らせ種別が「チケット」であるものはチケット詳細画面に遷移します。

詳細情報のないお知らせを一覧画面で選択したときは、遷移はせず画面は変わりません。

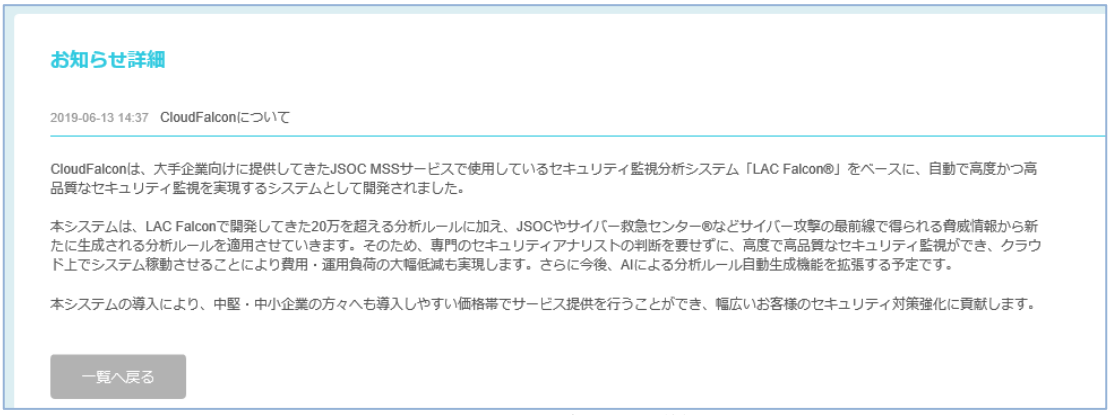


図 6.2-1 お知らせ詳細

7. チケット

本サービスの動作について不明な点がある場合、アラート内容や FAQ の内容についてご質問がある場合には、チケットを発行して問い合わせることができます。

チケットの発行は Web ポータルからいつでも可能ですが、KDSec-MSS オペレータの対応時間は、平日 9:00～17:00 となります。(土日祝日、年末年始、弊社休業日を除く)
そのため、回答が翌営業日以降となる場合があります。

チケットには、以下のような状態があります。

表 7-1 チケットステータスの説明

項目	説明
オープン	お客様がチケットを作成した直後の状態。
SOC 対応中	オペレータが回答を準備中の状態。
お客様連絡待ち	オペレータが回答し、お客様が確認する前の状態。
クローズ	お客様が内容を確認し、解決された状態。

質問開始からチケット完了までの流れは、以下の通りです。
KDSec-MSS オペレータからの回答で不明な点がある場合、何度でも質問をすることができます。
KDSec-MSS オペレータの回答によって不明な点が解決した場合、チケットをクローズしてください。

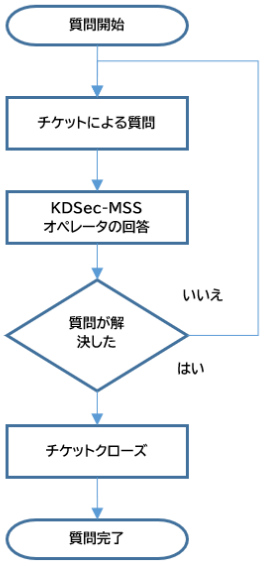


図 7-1 質問完了までの流れ

7.1. チケット一覧

Web ポータル左側メニューの**チケット**を押すと、チケット一覧が表示されます。最新のチケットが一番上に表示されます。チケットを選択するとチケット詳細に遷移します。最終更新日が過去 1 か月以前のチケットを表示したい場合は、右上の虫眼鏡ボタンを押し、検索画面に遷移し、最終更新日を指定して検索を行います。

チケットの最大表示件数は 25 件と 50 件から選択できます。

図 7.1-1　チケット一覧

7.2. チケット発行

チケット一覧画面の右上にある**チケット発行**ボタンを押すと、以下のチケット発行画面が表示されます。

チケットの件名を件名欄、質問内容をコメント欄に記入し、**発行**ボタンを押すとチケットを発行できます。また、アラート詳細画面からもチケット発行画面へ遷移できますので、特定のアラートに関する質問はこちらから発行してください。

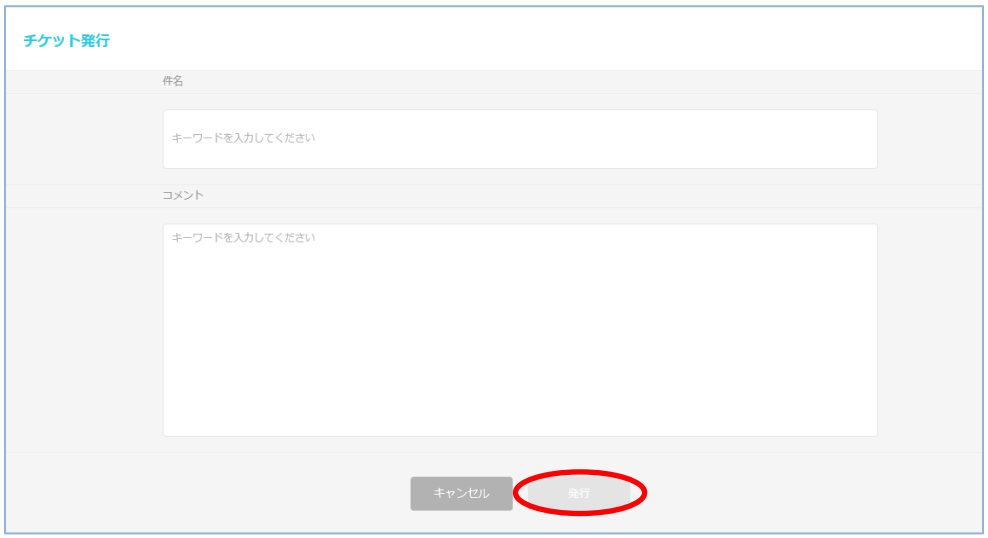


図 7.2-1　チケット発行

7.3. チケット詳細

チケット一覧からチケットを選択することで、下図のチケット詳細画面が表示されます。
対応履歴の欄に、お客様と KDSec-MSS オペレータ間の対話の履歴が表示されます。

図 7.3-1 チケット詳細

さらに質問がある場合には、質問内容をコメント欄に記載して、**更新**ボタンを押すと質問ができます。**更新**ボタンを押すことにより、チケットステータスが SOC 対応中に変更されます。
コメント欄に記載した後に、チケット更新を行わずにキャンセルする場合には、ブラウザの戻るボタンでチケット一覧画面に戻ることができます。

KDSec-MSS オペレータの回答によって不明な点が解決した場合、**チケットクローズ**ボタンを押してクローズしてください。このチケットは解決された状態になり、ステータスがクローズに変わります。

7.4. チケット検索

チケット一覧画面の右上の**虫眼鏡ボタン**を押すと、検索用の画面が表示されます。

図 7.4-1　チケット検索

下図の画面にて、検索条件を指定し、**適用**ボタンを押すことでチケットを検索することができます。

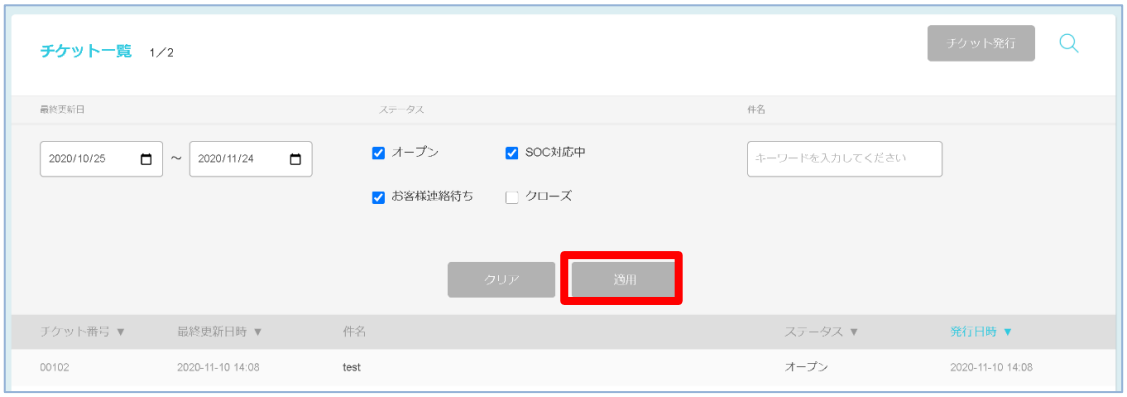


図 7.4-2　チケット検索条件

チケットの検索条件は以下の通りです。適用を押すことで、指定した条件で検索を行います。

表 7.4-1　チケット検索条件

項目	説明
更新日時(開始)	最終更新日の期間指定において、開始日を設定する。 カレンダーから日付を選択するか、手入力により年月日を設定する。
更新日時(終了)	最終更新日の期間指定において、終了日を設定する。 カレンダーから日付を選択するか、手入力により年月日を設定する。
ステータス	チケットのステータスを設定する。
件名	チケット件名の一部を入力して検索する(部分一致検索)。

チケット検索が完了すると条件に合致したチケットの一覧が表示されます。検索結果は、更新日時が最新のものから順に表示されます。 なお、表示されるチケットの件数は最大 50 件です。

8. ログ表示・検索

本システムの分析したログデータを表示、検索することができます。

8.1. Firewall ログ

Web ポータル左側メニューの**ログ表示**を押すと、ログ検索用の設定項目と Firewall ログ一覧が表示されます。デフォルト状態では、ログは 1 ページに 25 件まで表示されます。

8.1.1. Firewall ログ一覧

ログ一覧の左下のプルダウンメニューから 25 または 50 を選択することで、1 ページに表示するログ数を、25 件または 50 件に切り替えることができます。

また、ログ一覧の下に表示されているページ番号を押すと、選択したページに遷移します。全ページ合わせて 1000 件まで表示することができます。

本システムにおける Firewall ログの分析対象は Deny ログのため、ログ表示画面における Firewall ログの表示は Deny ログのみとなります。

デバイス名	日時 ▼	送信元IP	ポート	宛先IP	ポート	プロトコル	ICMP Type	Policy No	アクション	メッセージ
PrismaAccess 001	2021-07-21 22:05:01	34.98.31.161	58622	172.28.168.216	443	TCP	-1	-1	Deny	LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC| |devTime=2021-07-21T13:05:01.000000Z src=34.98.31.161 dst=172.28.168.216 Application=g...
PrismaAccess 002	2021-07-21 21:55:01	34.98.148.68	58622	172.28.229.225	443	TCP	-1	-1	Deny	LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC| |devTime=2021-07-21T12:55:01.000000Z src=34.98.148.68 dst=172.28.229.225 Application=g...
PrismaAccess 001	2021-07-21 21:55:01	34.98.162.223	58622	172.28.240.155	443	TCP	-1	-1	Deny	LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC| |devTime=2021-07-21T12:55:01.000000Z src=34.98.162.223 dst=172.28.240.155 Application=...
PrismaAccess 001	2021-07-21 21:55:01	34.98.106.100	58622	172.28.169.132	443	TCP	-1	-1	Deny	LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC| |devTime=2021-07-21T12:55:01.000000Z src=34.98.106.100 dst=172.28.169.132 Application=...
PrismaAccess 001	2021-07-21 21:55:01	34.98.173.22	58622	172.28.246.36	443	TCP	-1	-1	Deny	LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC| |devTime=2021-07-21T12:55:01.000000Z src=34.98.173.22 dst=172.28.246.36 Application=go...

図 8.1.1-1 Firewall ログ一覧

ログ一覧の各行を選択すると、選択したログの内容を確認することができます。

ログの内容で表示される時刻はログ収集サーバによって標準時間が異なりますのでご注意ください。

標準時間 UTC：Prisma Access 又は PA-5260 のログを受信するログ収集サーバ

標準時間 JST：PA シリーズ（WVS2、KCPS）のログを受信するログ収集サーバ

図 8.1.1-2 Firewall ログの内容確認

8.1.2. Firewall ログ検索

ログ表示画面の上部には、ログ検索用の設定項目が表示されます。画面の右上の**虫眼鏡ボタン**を押すことで非表示にすることもできます。ログの検索条件は以下の表の通りです。

適用ボタンを押すことで、指定した条件で検索を行います。**クリア**ボタンを押すと、検索項目の設定が初期設定に戻ります。

図 8.1.2-1 Firewall ログ検索

表 8.1.2-1 Firewall ログ検索条件

項目	説明
日時(開始)	検索対象ログの開始日時を設定する。 カレンダーから日付を選択するか、手入力により設定する。
日時(終了)	検索対象ログの終了日時を設定する。 カレンダーから日付を選択するか、手入力により設定する。
送信元 IP アドレス	送信元 IP アドレスを入力して検索する(完全一致検索)。 ドット付き 10 進表記で入力する。
(送信元)ポート	送信元 IP アドレスの右隣りにある入力項目。送信元ポート番号を入力して検索する(完全一致検索)。数値以外の検索は無効。
宛先 IP アドレス	宛先 IP アドレスを入力して検索する(完全一致検索)。 ドット付き 10 進表記で入力する。
(宛先)ポート	宛先 IP アドレスの右隣りにある入力項目。送信元ポート番号を入力して検索する(完全一致検索)。数値以外の検索は無効。
プロトコル	プロトコルを検索条件として指定する。 すべて/TCP/UDP/ICMP から選択できる。
アクション	ルールアクションを検索条件として指定する。 すべて/Allow/Deny から選択できる。

8.1.3. 検索結果取得

検索**適用**ボタンの右にある**検索結果取得**ボタンを押すことで検索結果の csv ファイルをダウンロードすることができます。一度に 1000 件までログを取得することができます。

8.2. IPS ログ

Firewall ログ表示画面上部にある Firewall･IPS 切り替えタブの IPS タブを押すと、ログ検索用の設定項目と IPS ログ一覧が表示されます。デフォルト状態では、ログは 1 ページに 25 件まで表示されます。

図 8.2-1 Firewall･IPS 切り替えタブ

8.2.1. IPS ログ一覧

ログ一覧の左下のプルダウンメニューから 25 または 50 を選択することで、1 ページに表示するログ数を、25 件または 50 件に切り替えることができます。

一覧の下に表示されているページ番号を押すと、選択したページに遷移します。全ページ合わせて 1000 件まで表示することができます。

本システムにおける IPS ログの分析対象は THREAT ログとなります。

分析対象（THREAT ログ）以外のログ（file ログ、URL ログ他）の場合、シグネチャ名が空欄で表示されます。

デバイス名	日時 ▼	シグネチャ名	重要度	送信元IP	ポート	宛先IP	ポート	プロトコル	遮断
PrismaAccess 003	2021-07-21 22:10:01	Windows BAT(52128)	low	34.98.150.237	58622	172.28.123.135	443	TCP	なし
PrismaAccess 001	2021-07-21 22:10:01	Suspicious DNS Query (generic:track.motormobile.com) (208655604)	medium	34.98.204.240	58622	172.28.50.23	443	TCP	なし
PrismaAccess 001	2021-07-21 22:10:01	HTTP OPTIONS Method(30520)	informational	34.98.110.212	58622	172.28.193.94	443	TCP	なし
PrismaAccess 001	2021-07-21 22:05:01	JSIG-WEB_STRUTS2-CONTENT-TYPE-XML-PROCESSBUILDER-2(42243)	medium	34.98.172.48	58622	172.28.244.140	443	TCP	なし

図 8.2.1-1 IPS ログ一覧

ログ一覧の各行を選択すると、選択したログの内容を確認することができます。
　ログの内容で表示される時刻はログ収集サーバによって標準時間が異なりますのでご注意ください。
　標準時間 UTC：Prisma Access 又は PA-5260 のログを受信するログ収集サーバ
　標準時間 JST：PA シリーズ（WVS2、KCPS）のログを受信するログ収集サーバ

図 8.2.1-2　IPS ログの内容確認

8.2.2. IPS ログ検索

ログ表示画面の上部には、ログ検索用の設定項目が表示されます。画面の右上の**虫眼鏡ボタン**を押すことで非表示にすることもできます。検索条件は以下の表の通りです。

適用ボタンを押すことで、指定した条件で検索を行います。**クリア**ボタンを押すと、検索項目の設定が初期設定に戻ります。

図 8.2.2-1 IPS ログ検索

表 8.2.2-1 IPS ログ検索条件

項目	説明
日時(開始)	検索対象ログの開始日時を設定する。 カレンダーから日付を選択するか、手入力により設定する。
日時(終了)	検索対象ログの終了日時を設定する。 カレンダーから日付を選択するか、手入力により設定する。
送信元 IP アドレス	送信元 IP アドレスを入力して検索する(完全一致検索)。 ドット付き 10 進表記で入力する。
(送信元)ポート	送信元 IP アドレスの右隣りにある入力項目。送信元ポート番号を入力して検索(完全一致検索)。数値以外の検索は無効。
宛先 IP アドレス	宛先 IP アドレスを入力して検索する(完全一致検索)。 ドット付き 10 進表記で入力する。
(宛先)ポート	宛先 IP アドレスの右隣りにある入力項目。送信元ポート番号を入力して検索する(完全一致検索)。数値以外の検索は無効です。
プロトコル	プロトコルを検索条件として指定する。 すべて/TCP/UDP/ICMP から選択できる。
遮断有無	遮断状況を検索条件として指定する。 すべて/あり/なしから選択する。
重要度	重要度を検索条件として指定する。 すべて/critical/high/medium/low/informational/- から選択できる。

8.2.3. 検索結果取得

検索**適用**ボタンの右にある**検索結果取得**ボタンを押すことで、検索結果の csv ファイルをダウンロードすることができます。一度に 1000 件までログを取得することができます。

9. FAQ

よくある質問と回答（FAQ：Frequently Asked Questions）を Web ポータル上で確認することができます。本分析サービスについて不明な点がありましたら、まず FAQ をご参照ください。

9.1. FAQ 一覧

Web ポータル左側メニューの **FAQ** を押すと FAQ 一覧が表示されます。

FQA は、1 ページ最大 50 件まで表示されます。一覧の下に表示されているページ番号を押すと、選択したページに遷移します。

図 9.1-1 FAQ 一覧

9.2. キーワード検索

FAQ 画面右上の**虫眼鏡ボタン**を押すと、キーワードとカテゴリによる検索が可能な画面が表示されます。

図 9.2-1 FAQ キーワード検索

この画面でキーワードを入力し、**適用**ボタンを押すと、FAQ 一覧の中から質問文を対象にしたキーワード検索を実行できます。**クリア**ボタンを押すと検索項目の設定が初期設定に戻ります。

9.3. カテゴリでの絞り込み

FAQ のカテゴリでの絞り込みをすることも可能です。プルダウンメニューから検索したいカテゴリを選択し、**適用**ボタンを押すことにより選択したカテゴリの FAQ だけを表示することができます。**クリア**ボタンを押すと検索項目の設定が初期設定に戻ります。

図 9.3-1 FAQ カテゴリ絞り込み画面

9.4. FAQ 詳細

FAQ の一覧で確認した点が見つかった場合には、その行を押すことで詳細画面が表示され、質問に対する回答を確認することができます。

図 9.4-1 FAQ 詳細画面

10. レポート

本サービスでは、ログ分析の結果から日次レポートまたは月次レポートを作成することができます。

10.1. 日次レポート

Web ポータルのレポート画面の左側メニューの**レポート**を押すと、日次レポートと月次レポートの選択画面が表示されます。

日次レポートの下にあるプルダウンメニューで、レポート出力対象日（過去 30 日間）を選択し、ダウンロードボタンを押すと、PDF 形式のレポートファイルをダウンロードすることができます。

図 10.1-1 日次レポート PDF ダウンロード

日次レポートの内容は、以下のとおりです。

表 10.1-1 日次レポートの内容

章	節	内容
1.アラート一覧	(1)当日のアラート一覧	一覧表形式。
	(2)重要度 High のアラート詳細	アラート詳細。
2.アラートサマリー	(1)重要度別アラート件数推移	重要度別アラート件数の 7 日間の推移グラフ。
	(2)重要度別件数集計表	重要度別アラート件数の 7 日間の集計表。
3.ログ件数サマリー	(1)センサ別ログ件数推移	センサ別ログ件数の 7 日間の推移グラフ。
	(2)センサ別ログ件数集計表	センサ別ログ件数の 7 日間の集計表。
4.ログ処理量サマリー	(1)センサ別ログ処理量推移	センサ別ログ処理量の 7 日間の推移グラフ。
	(2)センサ別ログ処理集計表	センサ別ログ転送量の 7 日間の集計表。

10.2. 月次レポート

レポート画面の月次レポートの下にあるプルダウンメニューで、レポート出力対象月（直近 3 年以内）を選択し、「レポート取得」下のダウンロードボタンを押すと、PDF 形式のレポートファイルをダウンロードすることができます。また、「csv の取得」下のダウンロードボタンを押すと、CSV 形式のファイルをダウンロードすることができます。

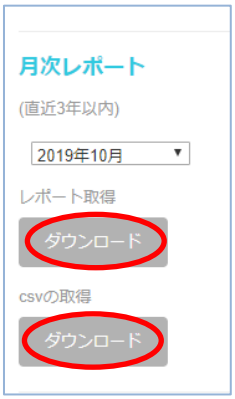


図 10.2-1 月次レポート ダウンロード

PDF の月次レポートは、以下の内容で構成されます。

表 10.2-1 月次レポートの内容

章	節	内容
1.アラート一覧	(1)当月のアラート一覧	一覧表形式。
	(2)重要度 High のアラート詳細	アラート詳細。
2.アラートサマリー	(1)重要度別アラート件数推移	重要度別アラート件数の 4 か月(月単位)の折れ線グラフ。
	(2)重要度別件数集計表	重要度別アラート件数の 4 か月(月単位)の集計表。
3.ログ件数サマリー	(1)センサ別ログ件数推移	センサ別ログ件数の 4 か月(月単位)の折れ線グラフ。 センサ別ログ件数の 1 か月(日単位)の折れ線グラフ。
	(2)センサ別ログ件数集計表	センサ別ログ件数の 4 か月(月単位)の集計表。
4.ログ処理量サマリー	(1)センサ別ログ処理量推移	センサ別ログ処理量の 4 か月(月単位)の折れ線グラフ。 センサ別ログ処理量の 1 か月(日単位)の折れ線グラフ。
	(2)センサ別ログ処理量集計表	センサ別ログ処理量の 4 か月(月単位)の集計表。
	(3)全センサのログ処理量	全センサのログ処理量の 1 か月(日単位)の折れ線グラフ。
5.チケット一覧		最終更新日が選択月のチケットの一覧。
6.チケットサマリ		ステータス別チケット件数。

CSV の月次レポートは、以下の内容で構成されます。

表 10.2-2 月次レポート CSV ファイルの内容

項目	内容
アラート ID	アラートの識別番号。
検知日時	アラートを検知した日時(分まで)。
アラート概要	アラートの概要説明。
重要度	アラートの重要度（ High, Medium, Low の 3 段階 ）。
対応	アラートへの対処状況。
ログ件数	同日の同じアラートを検知した数。
センサ	監視対象デバイスの識別子。

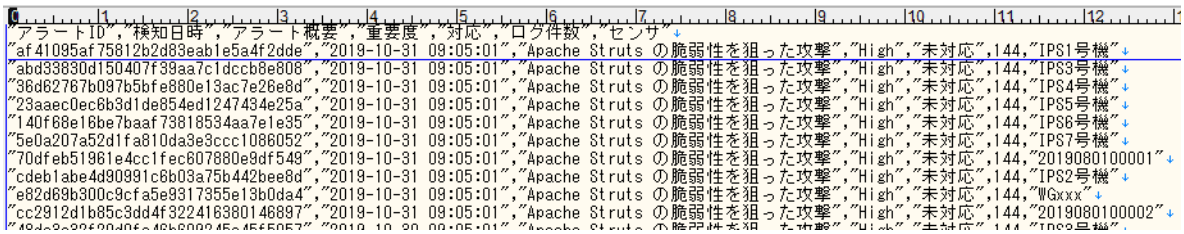


図 10.2-3 CSV ファイル

10.3. ログダウンロード

プルダウンメニューで対象年月日を選択後、ダウンロードボタンを押すと、zip 形式で圧縮したログファイルをダウンロードすることができます。
1 日のログダウンロード回数の上限は 100 回です。

図 10.3-1 ログダウンロード

ログダウンロードファイルの仕様は下記のとおりです。
・対象日の日本時間 0 時から翌 0 時までにログ収集サーバで受信したすべてのログが対象です。Firewall の Allow ログなど、分析対象以外のログも含まれます
・ログダウンロードファイルは zip 形式で圧縮されます。
・ログダウンロードファイルは、タイムスタンプ順でのソートを行いません。
・ログダウンロードファイルは最大 1,000,000 行までとし、超えた部分は別ファイルになります。
・圧縮後の zip 形式ファイルに格納する圧縮前ログファイル数は、2 ファイルまでとします。
・1 日のログファイル行数が 3,000,000 行を超えた場合、圧縮後の zip 形式ファイルが 2 ファイル以上となり、ダウンロードログプルダウンメニューに、日付と枝番が表示されます。

図 10.3-2 ログダウンロードプルダウン日付と連番

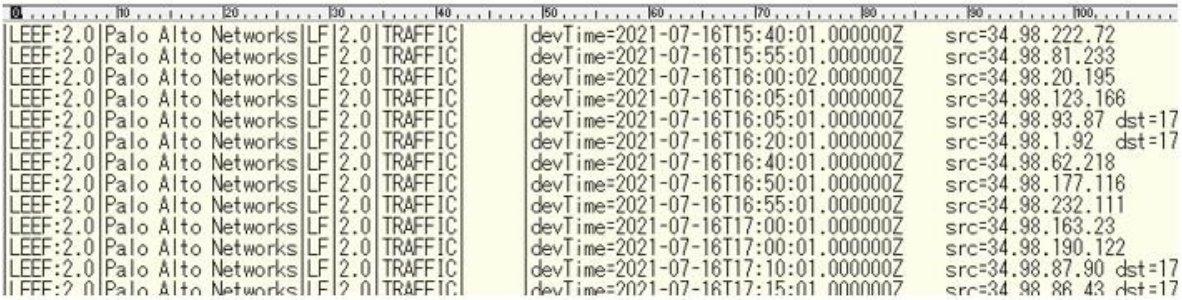
ダウンロード用のログファイルは、契約時に設定したログダウンロード保存量まで保存されます。実際のログダウンロード保存量が、契約ログダウンロード保存量(初期設定 10GB、10GB 単位で増加可能、最大 100GB)を超えた場合、契約ログダウンロード保存量を超えなくなるまで、過去の日付から日付単位でダウンロード用ログファイルを削除します。ただし、前日分のログは削除を行いません(最低保持日数 1 日)。

ダウンロードした zip ファイルを展開すると、以下のサンプルのようなテキストファイル(.log 形式)でログ内容を確認できます。

なお、ログの内容で表示される時刻はログ収集サーバによって標準時間が異なりますのでご注意ください。

標準時間 UTC:Prisma Access 又は PA-5260 のログを受信するログ収集サーバ
標準時間 JST:PA シリーズ(WVS2、KCPS)のログを受信するログ収集サーバ

※WVS2 ご利用のお客様へ
各ログ項目の詳細につきましては「【別紙】【WVS2 ご契約者様向け】KDSec セキュリティ監視システム Web ポータル操作マニュアル_ログ項目一覧」をご参照ください。



```
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T15:40:01.000000Z	src=34.98.222.72
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T15:55:01.000000Z	src=34.98.81.233
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:00:02.000000Z	src=34.98.20.195
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:05:01.000000Z	src=34.98.123.166
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:05:01.000000Z	src=34.98.93.87 dst=17
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:20:01.000000Z	src=34.98.1.92  dst=17
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:40:01.000000Z	src=34.98.62.218
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:50:01.000000Z	src=34.98.177.116
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T16:55:01.000000Z	src=34.98.232.111
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T17:00:01.000000Z	src=34.98.163.23
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T17:00:01.000000Z	src=34.98.190.122
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T17:10:01.000000Z	src=34.98.87.90 dst=17
LEEF:2.0|Palo Alto Networks|LF|2.0|TRAFFIC|	devTime=2021-07-16T17:15:01.000000Z	src=34.98.86.43 dst=17
```

図 10.3-3 ダウンロードログサンプル

11. プロファイル

Web ポータルの左側メニューの**アカウント**を押すとアカウント画面が表示されます。

管理者アカウントでログインしている場合、アカウント画面に契約者情報及びアカウント情報が表示されます。

図 11-1　アカウント画面初期表示（管理者アカウント）

アカウント画面は 3 種類あります。
・プロファイル　お客様に関する情報
・サービス管理　契約サービスに関する情報
・メール通知　　メール通知に関する情報

プロファイル、サービス管理、メール通知の各タブを押すことで画面を切り替えることができます。

図 11-2　アカウント画面タブ切り替え

担当者アカウントでログインしている場合、アカウント画面にログイン中のアカウントの情報のみ表示されます。画面切り替えタブは非表示となり、サービス管理、メール通知画面への切り替えはできません。

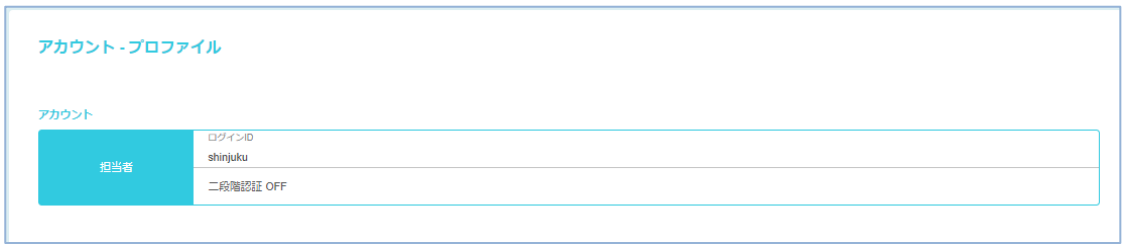


図 11-3　アカウント画面初期表示（担当者アカウント）

11.1. 契約者情報

管理者アカウントでログインしている場合、上部に契約者に関する情報が表示されます。
担当者アカウントでログインしている場合、契約者情報は表示されません。

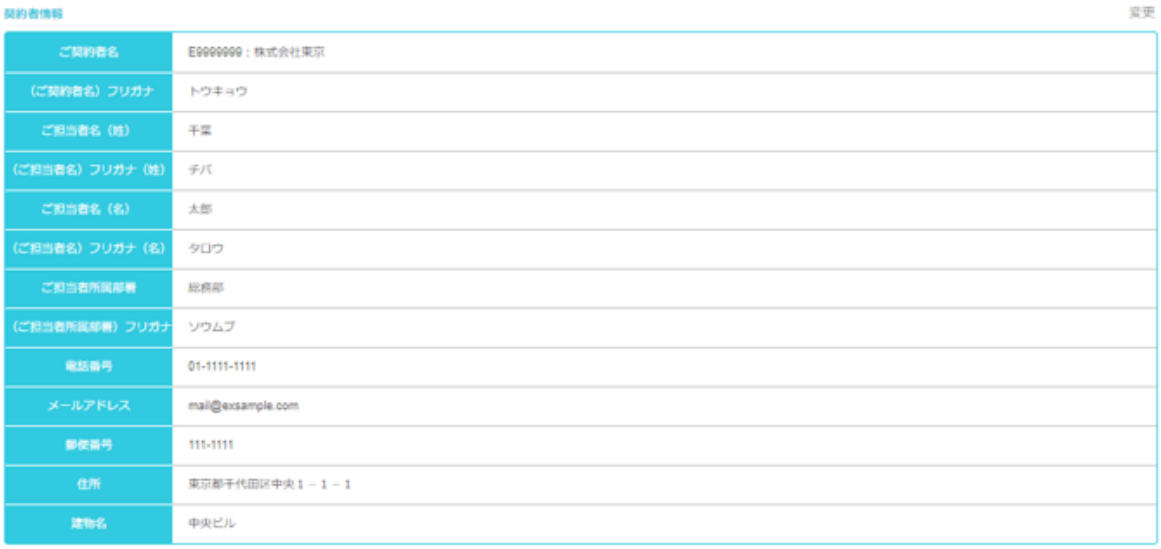


図 11.1-1 契約者情報

右上にある**変更**を押すことでプロファイル変更画面が表示されます。
項目を変更後、変更ボタンを押すと変更することができます。

なお、「ご契約者名」の欄には本システムで提供しているサービスを識別するため、会社名の前に識別子が付与されております。
こちらの識別子の変更・削除は行わないでください。

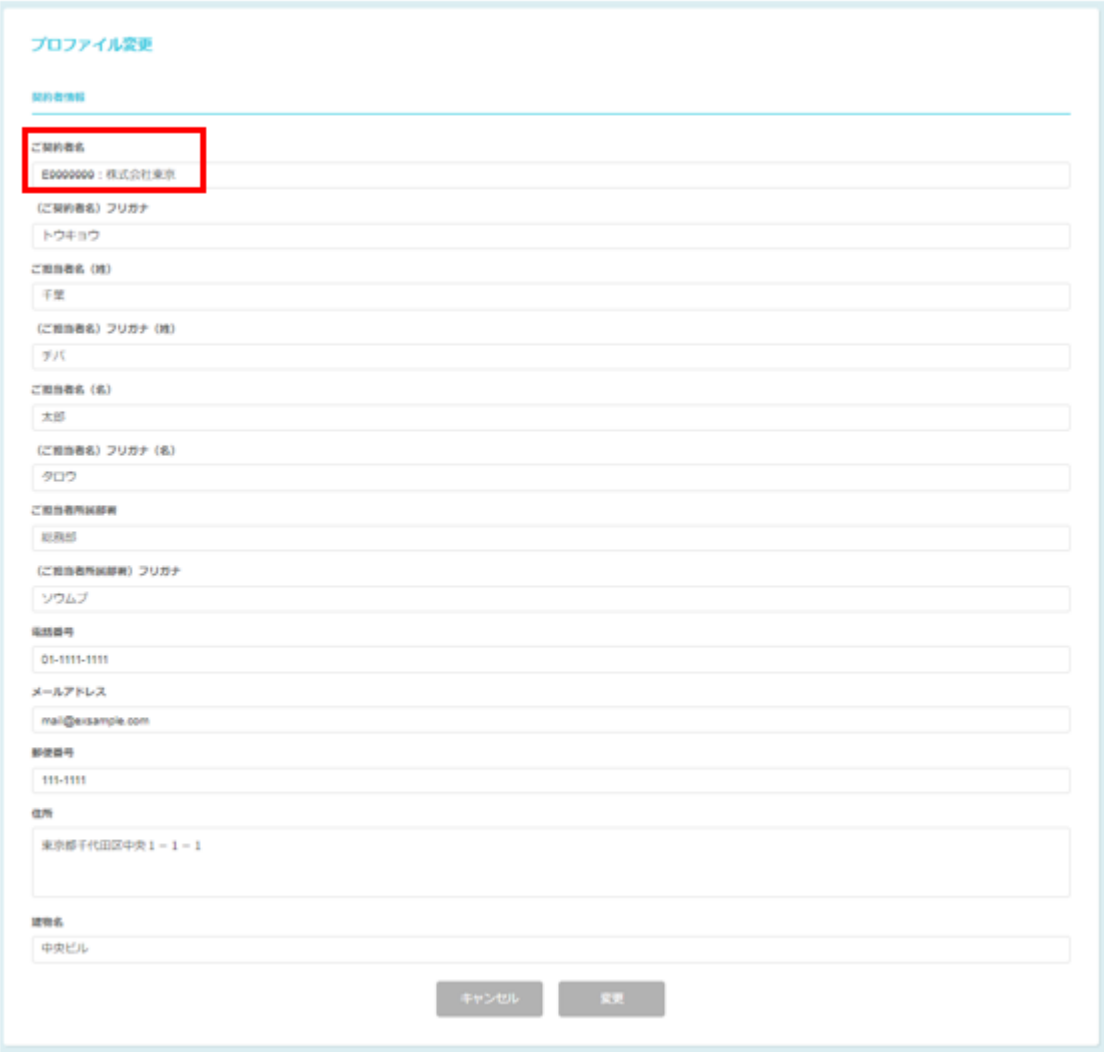


図 11.1-2　プロファイル変更画面（契約者情報）

11.2. アカウント管理

11.2.1. 表示

画面下部にアカウント情報(ログイン ID、二段階認証設定)が表示されます。
管理者アカウントでログインしている場合、全てのアカウントに関する情報が表示されます。

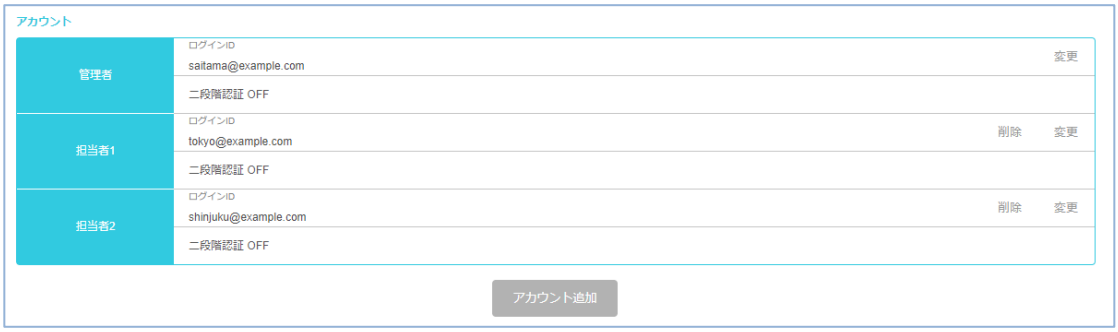


図 11.2.1-1 アカウント画面初期表示(管理者アカウント)

管理者アカウントでログインしている場合、下記を行うことができます。
・登録されている全てのアカウントに関する情報表示
・登録されている全てのアカウントの設定変更
・ログイン中の管理者アカウントのパスワード変更
・担当者アカウントの追加・削除・設定変更

担当者アカウントでログインしている場合、ログイン中のアカウントの情報が表示されます。

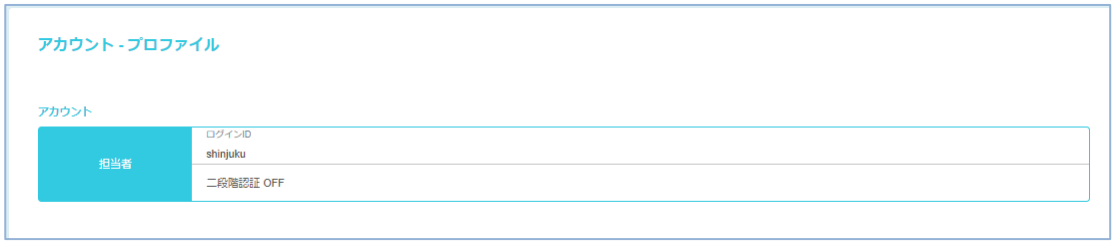


図 11.2.1-2 アカウント画面初期表示(管理者アカウント)

担当者アカウントでログインしている場合、下記を行うことができます。
・ログイン中の担当者アカウントに関する情報の表示
・ログイン中の担当者アカウントの設定変更・パスワード変更

担当者アカウントでは、アカウント情報の追加、変更、削除はできません。

同じ契約者であれば、管理者アカウントでログインしても、担当者アカウントでログインしても、アラート、チケット等の内容は同じです。ただし、ダッシュボード画面の表示内容は、アカウント(ポータル ID)ごとに異なります。

11.2.2. 設定変更

管理者アカウントでログインしている場合、登録されているすべてのアカウント情報を変更することができます。

管理者アカウント右側にある**設定変更**を押すと、管理者アカウント用のアカウント設定変更画面が表示されます。

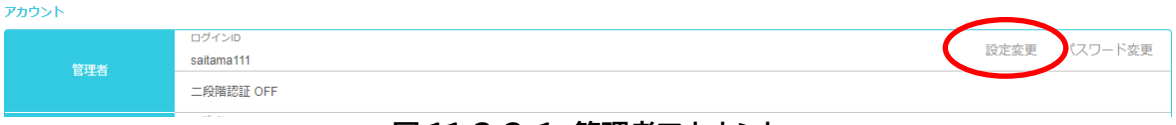


図 11.2.2-1　管理者アカウント

管理者アカウントのログイン ID、二段階認証(ON/OFF)を変更することができます。
ログイン ID は、**英数と記号(※)が使用でき、3 文字以上 100 文字以下の文字列を設定できます。**
ただし、既に本システムへ登録済みのログイン ID を重複して設定することはできません。
二段階認証 ON が推奨です。
(※)使用できる記号は以下となります。
ハイフン　　：-
アンダーバー　：_
ドット　　：.

変更後、**更新**ボタンを押してください。

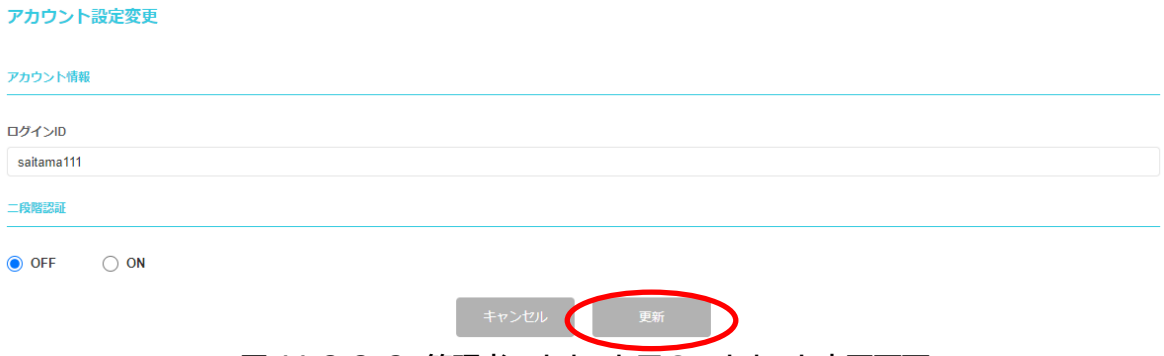


図 11.2.2-2　管理者アカウント用のアカウント変更画面

担当者アカウント右側にある**設定変更**を押すと、担当者アカウント用のアカウント設定変更画面が表示されます。

図 11.2.2-3　担当者アカウント

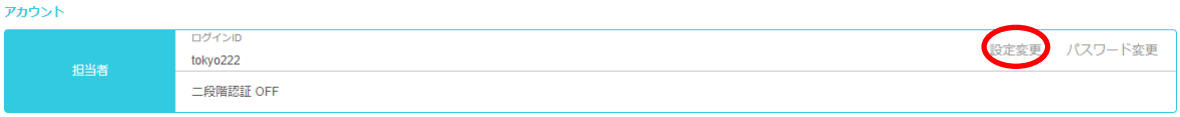
担当者アカウントのログイン ID、二段階認証(ON/OFF)を変更することができます。
ログイン ID は、**英数と記号(※)が使用でき、3 文字以上 100 文字以下の文字列を設定できます。**
ただし、既に本システムへ登録済みのログイン ID を重複して設定することはできません。
二段階認証 ON が推奨です。
(※)使用できる記号は以下となります。
ハイフン　　：-
アンダーバー　：_
ドット　　：.

変更後、**更新**ボタンを押してください。

図 11.2.2-4　担当者アカウント用のアカウント変更画面

担当者アカウントでログインしている場合は、ログイン中の担当者アカウント情報の設定変更ができます。

担当者アカウント右側にある**設定変更**を押すと、担当者アカウント用のアカウント設定変更画面が表示されます。



担当者アカウントの二段階認証(ON/OFF)を変更することができます。
二段階認証 ON が推奨です。

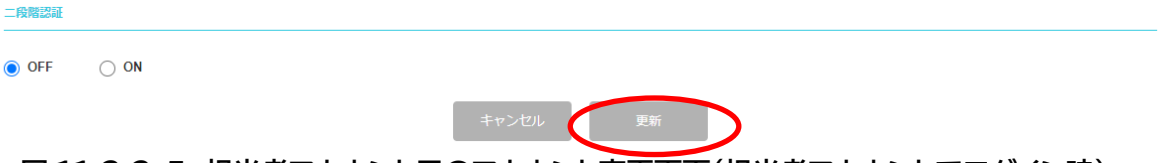


図 11.2.2-5 担当者アカウント用のアカウント変更画面(担当者アカウントでログイン時)

11.2.3. パスワード変更

管理者アカウントでログインしている場合、登録されている管理者アカウントのパスワード変更をすることができます。

管理者アカウントでは、担当者アカウントのパスワードは変更することができません。担当者アカウントでログインしてパスワード変更をしてください。

管理者アカウント右側にある**パスワード変更**を押すと、管理者アカウント用のパスワード変更画面が表示されます。

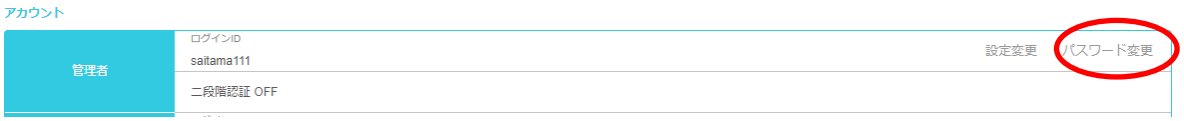


図 11.2.3-1 管理者アカウント

管理者アカウントのパスワードを変更することができます。

パスワードは、**スペース以外の記号が使用でき、英語の大文字と小文字と数字を含む、10 文字以上 72 文字以下にする必要があります。**現在のパスワード、新しいパスワード、新しいパスワード(確認)ともに必須入力です。

変更後、**更新**ボタンを押してください。

図 11.2.3-2 管理者アカウント用のアカウント変更画面

担当者アカウントでログインしている場合は、登録されている担当者アカウントのパスワード変更をすることができます。

担当者アカウント右側にある**パスワード変更**を押すと、担当者アカウント用のパスワード変更画面が表示されます。

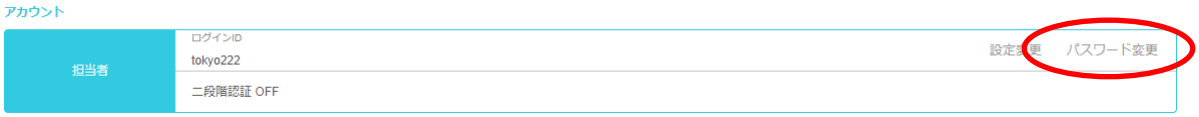


図 11.2.3-3 担当者アカウント

担当者アカウントのパスワードを変更することができます。
パスワードは、**スペース以外の記号が使用でき、英語の大文字と小文字と数字を含む、10 文字以上 72 文字以下にする必要があります。**現在のパスワード、新しいパスワード、新しいパスワード(確認)ともに必須入力です。

変更後、**更新**ボタンを押してください。

図 11.2.3-4 担当者アカウント用のアカウント変更画面

11.2.4. 追加

管理者アカウントでログインした場合、担当者アカウントを最大 4 アカウントまで作成することができます。

アカウント追加ボタンを押すと、アカウント追加画面が表示されます。

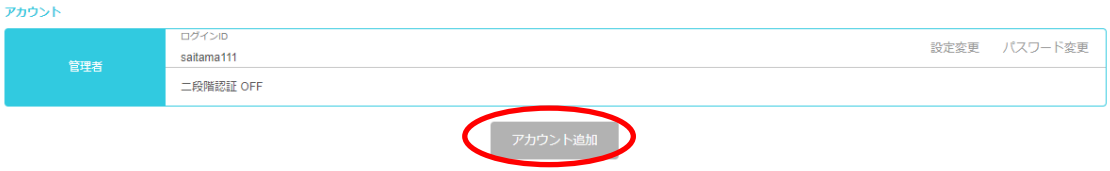


図 11.2.4-1 アカウント追加ボタン

アカウント追加画面で、下記を入力します。入力後、**変更**ボタンを押してください。

・追加する担当者アカウントのログイン ID
・追加する担当者アカウントのパスワード
・追加する担当者アカウントの二段階認証設定

ログイン ID は、**英数と記号(※)が使用でき、3 文字以上 100 文字以下の文字列を設定できます。**
ただし、既に本システムへ登録済みのログイン ID を重複して設定することはできません。
パスワードは、**スペース以外の記号が使用でき、英数 10 文字以上 72 文字以下で、小文字、大文字、数字を必ず 1 文字以上を含めてください。**
二段階認証 ON が推奨です。
(※)使用できる記号は以下となります。
ハイフン　：-
アンダーバー　：_
ドット　：.

図 11.2.4-2 アカウント追加画面

追加するログイン ID が重複している場合はエラーになります。
エラーになった場合は、別の ID で作成してください。

図 11.2.4-3 アカウント追加時エラー画面

11.2.5. 削除

管理者アカウントでログインした場合、担当者アカウントの右側にある**削除**を押すと、担当者アカウントを削除することができます。管理者アカウントは削除できません。

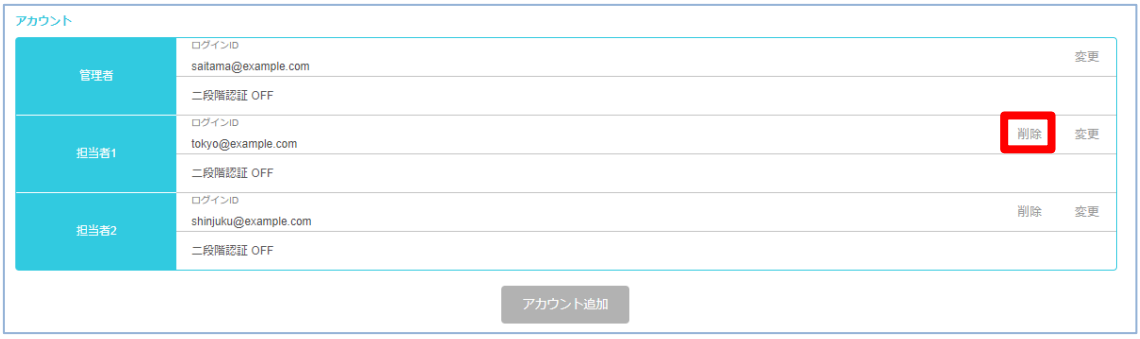


図 11.2.5-1　アカウント画面

12. サービス管理

アカウント画面の左上の**サービス管理**タブを押すと、サービス管理画面が表示されます。

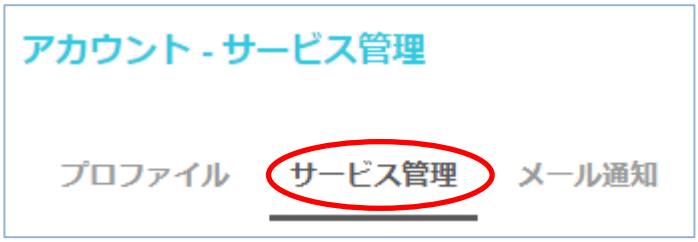


図 12-1 サービス管理タブ

サービス管理画面では、お客様がご契約中のサービス内容を確認することができます。

表 12-1 サービス管理画面

項目	説明
ご契約中のプラン	お客様のご契約中のプランが表示される。
センサ監視サービス	センサ監視サービスのご契約状況が表示される。

12.1. ご契約中のプラン

お客様のご契約中のプランをご確認いただけます。

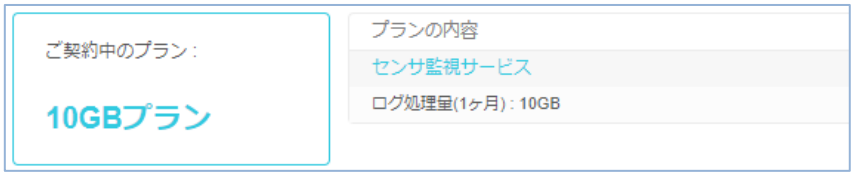


図 12.1-1 ご契約中プランの表示例

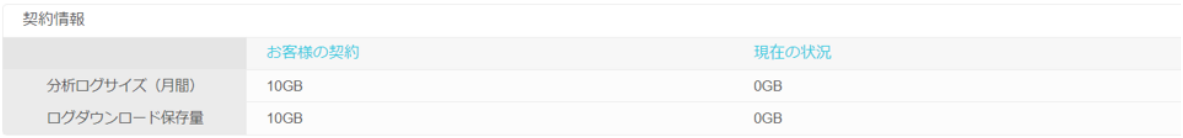
12.2. センサ監視サービス

契約情報とセンサ登録情報が表示されます。

12.2.1. 契約情報

ご契約内容に基づく月間の分析可能なログサイズと、ログダウンロード最大保存量を表示します。

また、当月 1 日から現在までの累積ログ分析サイズと、ログダウンロードのために保存されているサイズを表示します。



契約情報

	お客様の契約	現在の状況
分析ログサイズ（月間）	10GB	0GB
ログダウンロード保存量	10GB	0GB

図 12.2-1 契約情報の表示例

12.2.2. センサ登録情報

監視対象として登録されているセンサの機種、識別子、表示名を一覧表示します。

ここで設定されている表示名が、センサ監視分析結果画面のセンサ、PDF レポートのセンサ、ログ表示画面のデバイス名で使用されます。

センサ登録情報

番号	機種	識別子	表示名	状況
1	PrismaAccessLEEF	DeviceName-01	センサ-01	SOC確認中
2	PrismaAccessLEEF	DeviceName-02	センサ-02	SOC確認中

図 12.2-2 センサ登録情報の表示例

12.3. 監視システム内部 IP アドレス

セキュリティセンサのログ分析では、組織のネットワークを定義し、外部からの攻撃通信や、内部のウイルス感染端末からの外部サーバーへの通信を検出します。

通常のプライベート IP アドレスは設定済みですが、社内または組織内として判定すべきお客様固有の IP アドレスレンジがある場合には、この項に設定してください。

13. メール通知

アラート検知時、ログ処理量が所定の値を超えた時など、特定の条件でメール通知を行います。通知設定はメール通知設定画面で行います。アカウント画面の左上のメール通知タブを押すと、メール通知画面が表示されます。

図 13-1 メール通知

設定項目の左側のチェックボックスにチェックを入れるとメール通知が行われます。通知メールが必要のないものは、チェックボックスのチェックを外してください。

図 13-2 メール通知設定画面

13.1. E-mail 設定

プロファイルのメールアドレスで設定したアドレス以外に 4 つのメールアドレスを指定できます。

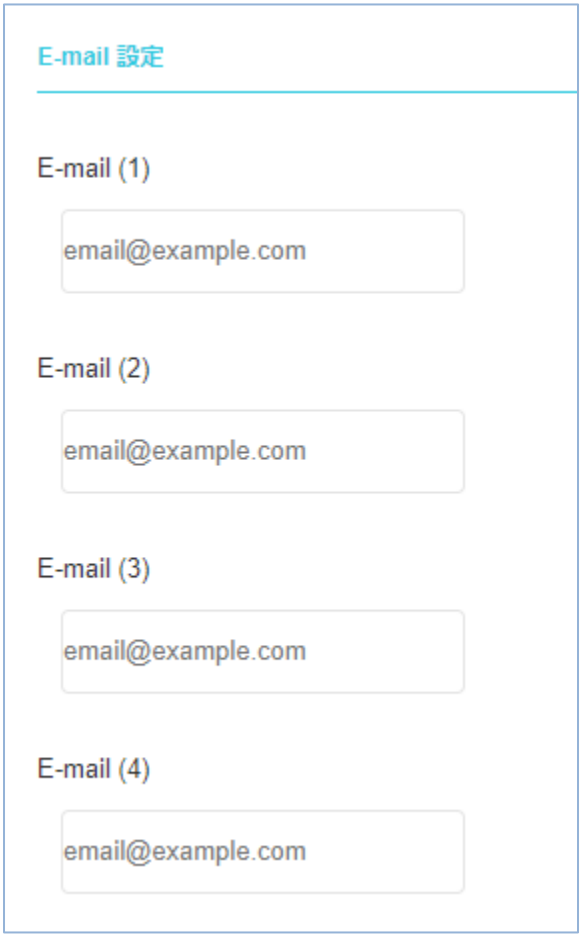


図 13.1-1 E-mail 設定

13.2. センサ監視サービス

登録済みのセンサからアラートを検知し、そのアラートが設定した重要度以上の場合に通知メールを送信します。また、センサログの分析量が一定量に達した場合の通知と、前日の分析状況通知設定も行うことができます。

13.2.1. アラート通知設定

アラート通知を受け取る場合は、ドロップダウンリストから重要度を **Medium 以上**または **High のみ**を選択してください。アラート通知が不要の場合は、左側のチェックボックスのチェックを外してください。

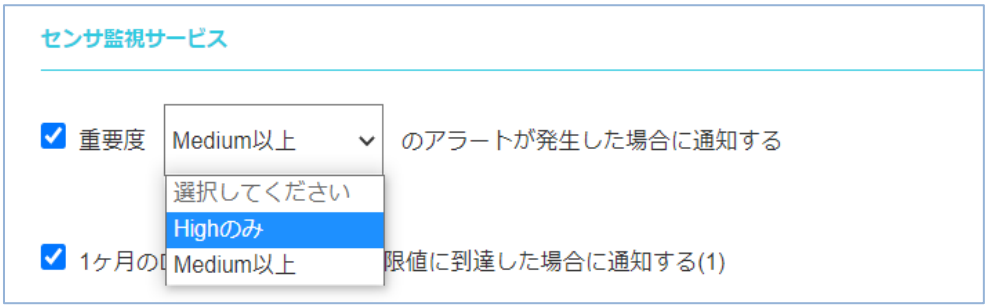


図 13.2.1-1 アラート通知設定

13.2.2. ログ処理量通知

月間ログ分析処理量がログ分析処理契約量に到達すると分析が止まるため、事前にアラートするための通知機能です。ログ処理量が一定量に到達した場合の通知を 2 段階で設定します。

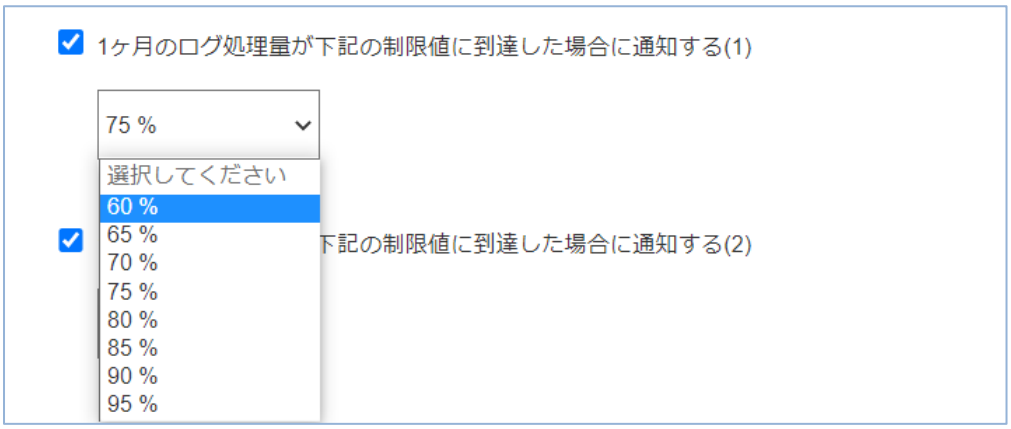


図 13.2.2-1 ログ処理量通知（1）

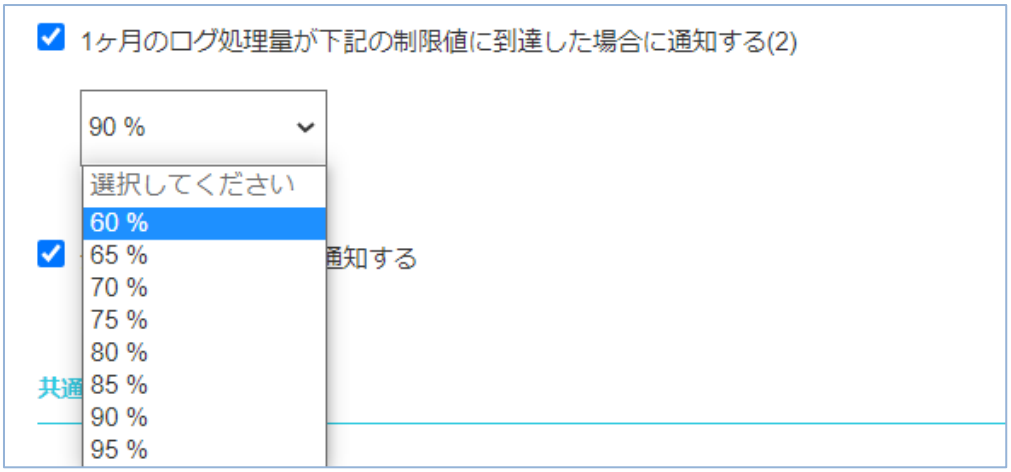


図 13.2.2-2 ログ処理量通知（2）

「1 日もしくは月間のログ処理量が上限値に到達した場合に通知する」を有効にすると、1 日のログ処理量が制限値に到達した場合、又は月間ののログ処理量が制限値に到達した場合に通知を行います。

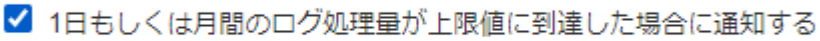


図 13.2.2-3 ログ処理量上限値到達通知

13.2.3. 分析状況通知

この項目にチェック入れた場合、前日の分析状況を毎朝通知します。通知メールには登録デバイス、分析対象日、ログ分析量、アラート件数が表示されます。

希にしかアラートが発生しない状況で、分析処理が正しく動作していることを確認するために利用することを想定しています。

13.3. 共通

チケット更新時に通知を受け取る場合は、「**サポートセンターチケットが更新した場合に通知する**」の左側にあるチェックボックスにチェックを入れてください。

13.4. その他のメール通知

メール通知設定画面で説明した通知メール以外でも、メールが通知される場合があります。

13.4.1. 監視センサとの初回接続時

お客様が登録したセンサから初めてログを検出した場合、監視対象デバイスの設定が完了し、分析サービスを開始したことを通知します。

13.4.2. 管理者がパスワードリセットした時

Web ポータルの管理者アカウントのパスワードを忘れた場合、パスワードリセットを行うことができます。

Web ポータルのログイン画面下部の「**パスワードをお忘れの場合**」を押し、ログイン ID を入力すると、登録中のメールアドレス宛にリセット用の URL が送付されます。

リセット用の URL に接続すると、パスワードがリセットされたことと、初期パスワードが登録中のメールアドレスにメールで通知されます。

ログイン ID と初期パスワードで再ログインすると、パスワード変更画面が表示されますので、ここでパスワードを設定してください。

なお、担当者アカウントは、本機能が使用できません。

13.4.3. アカウント情報を変更した時

契約者情報、管理者アカウント、担当者アカウント、監視システム内部 IP アドレスの変更、メール通知設定の変更があった場合、メール通知します。

14. ログアウト

Web ポータルの左側メニュー最下段にある、ログアウトを押すことでログアウトします。

図 14-1 ログアウト

15. 補足

本項では、補足説明が必要なウィジェットと、スマートフォンでの利用について説明します。

15.1. ウィジェットの補足説明

表示内容が分かりにくいウィジェットについて説明します。

15.1.1. ログ処理状況

ログ処理状況を緑・黄・赤の 3 色で表示します。
3 時間以上 1 日未満、1 件もログが受信できない場合は、ログが受信できていない累計の時間を図 15.1.1-1 のように表示します。

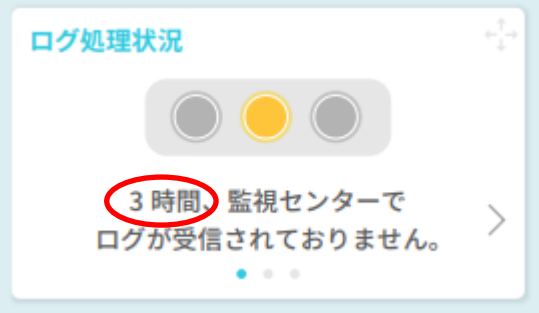


図 15.1.1-1 ログ未受信

ログ処理量が増加傾向にある場合は図 15.1.1-2 のようになります。直近 1 時間のログ処理量が増加傾向の場合に、ログ処理量が増加傾向であることを表示します。

図 15.1.1-2 ログ処理量増加傾向

直近 1 時間のログ処理量が急増した場合に、ログ処理量が急増したことを図 15.1.1-3 のように表示します。

図 15.1.1-3 ログ処理量急増

ログ処理量が月間ログ処理契約量の 90%を超えた場合、図 15.1.1-4 のように表示します。

図 15.1.1-4 ログ受信契約量到達直前

ログ処理量がログ受信契約量に到達した場合は、図 15.1.1-5 のように表示します。

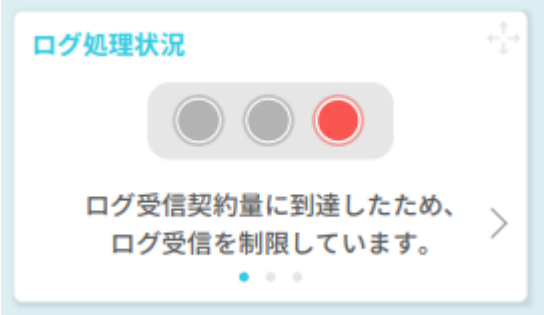


図 15.1.1-5 ログ受信契約量到達

15.1.2. アラート概要別グラフ

アラート概要別グラフは、アラートの内容に着目したグラフです。アラート概要別件数やアラート概要別占有率を確認することで、検知したアラートの傾向を知ることができます。

アラート概要別件数は指定した期間内に検知したアラートの内、件数が上位 5 件のアラート概要と件数を下図のように表示します。

図 15.1.2-1 アラート概要別件数

アラート概要別占有率は、同一のアラート概要が全体のアラート件数に占める割合を上位 5 件とその他で分類してグラフに表示します。
ウィジェットに表示されたアラート概要別占有率は図 15.1.2-2 のようになります。

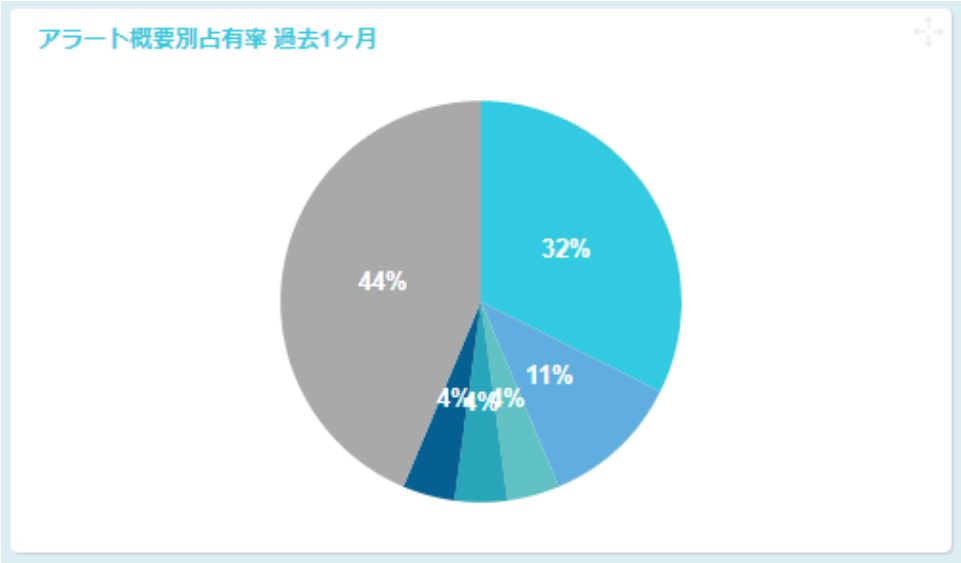


図 15.1.2-2 アラート概要別占有率（例 1）

また、グラフの上にマウスカーソルを移動させると、該当するアラート概要が図 15.1.2-3 のように表示されます。

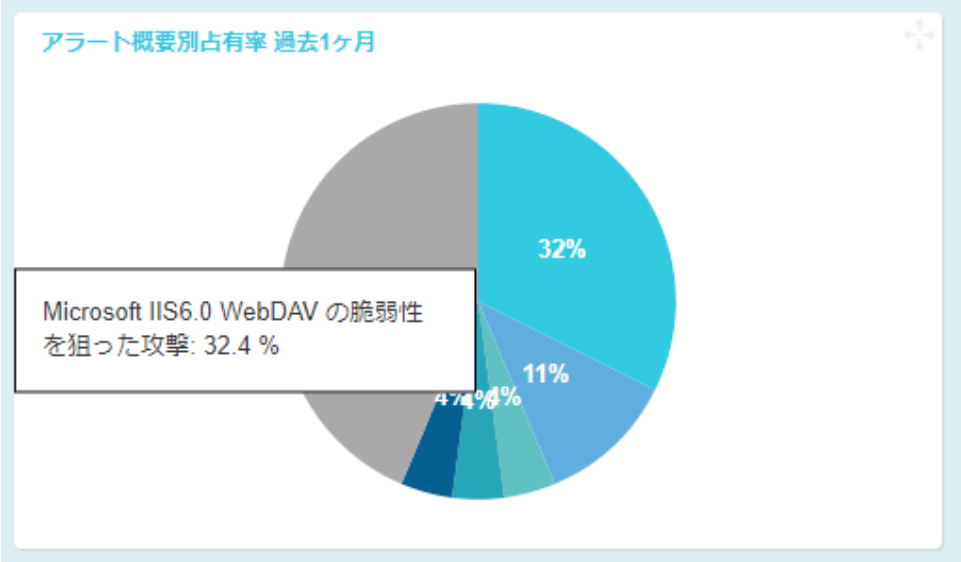


図 15.1.2-3 アラート概要別占有率（例 2）

15.1.3. センサ別ステータス一覧

センサ別ステータス一覧では、センサ別のログ処理量の状況とアラート発生状況が確認できます。

センサ別ステータス一覧の各項目の説明を表 15.1.3-1 に示します。

表 15.1.3-1 センサ別ステータス一覧の項目説明

項目	説明
センサ	センサ名を一覧表示する。
センターとの通信	センサ別に監視センターとの接続状況を表示する。
ログ処理量超過	センサ別のログ処理状況を表示する。 「今日のログ処理量」と「今月のログ処理量」の内、ログ処理量が上限値であるログ処理契約量に近い方の状況を表示する。
インシデント	アラート発生状況を表示する。 センサ別に「アラート発生状況」と同じ判断基準で表示する。

センサ別ステータス一覧の一例を図 15.1.3-1 に記します。

図 15.1.3-1 センサ別ステータス一覧（例 1）

当月 1 日から現在までのログ処理量が、ログ処理契約量の 90%以上に達した場合、図 15.1.3-2 のようにウィジェット下部が赤くなり、注意喚起が表示されます。

図 15.1.3-2　センサ別ステータス一覧（例 2）

15.2. スマートフォンでの利用

基本的な機能は PC ブラウザと同様ですが、PC と異なる機能もあります。以下で相違点について説明します。

ブラウザは各スマートフォンの標準ブラウザを使用してください。

スマートフォンのブラウザでログインすると、以下のようなダッシュボード画面が表示されます。

図 15.2-1 スマートフォンのダッシュボード画面

15.2.1. PC とスマートフォンで異なる機能

スマートフォンでの Web ポータル利用において、PC と異なる機能は以下の通りです。

・メニュー画面の表示

PC 用画面では常時左側に表示されているメニューがスマートフォンでは表示されません。下図、**右上部のマーク**をタッチすることで、PC 画面の左側に表示されているメニューと同様の内容を含むメニュー画面を表示します。

図 15.2.1-1 スマートフォンでのメニュー画面の表示

図 15.2.1-2 スマートフォンでのメニュー画面

・ウィジェットの移動
スマートフォンでは、ウィジェットは縦一列に配置されます。上下方向での配置のみをカスタマイズすることができます。
ウィジェットの**上部または下部のマーク**をタッチすることで、隣接したウィジェットと入れ替わりますので、お好みの位置に配置ください。

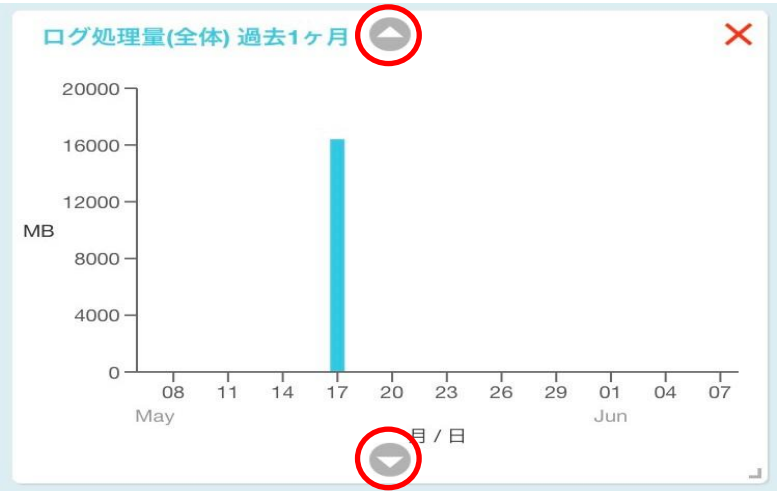


図 15.2.1-3 スマートフォンでのウィジェットの移動

15.2.2.スマートフォンで利用できない機能

スマートフォンにおいて利用できない機能は以下の通りです。

・二段階認証の登録

2.2 章で説明した、ワンタイムパスワードを用いた二段階認証を登録することができません。
スマートフォンでは、以下のような警告が表示されます。
PC でログインして、登録を行ってください。

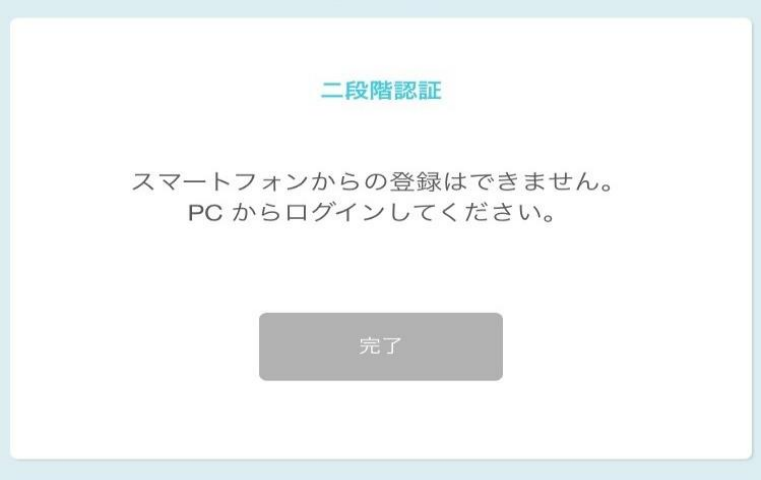


図 15.2.2-1 スマートフォンでの二段階認証登録時の警告画面

・ウィジェットでの拡大・縮小

スマートフォンでは、ダッシュボードの横幅に合わせてウィジェットサイズを固定しているため、ウィジェットの拡大・縮小を行うことができません。

・アラート概要の表示

スマートフォンでは 15.1.2 章で説明した、グラフにマウスカーソルを重ねて、該当するアラート概要を表示させる機能を利用することができません。

16. トラブルシューティング

- パスワードを忘れ、ログインできない（担当者アカウント）
  管理者にアカウントの削除と再度のアカウント追加を依頼してください。同じアカウント名で作成した場合でも、ダッシュボードのレイアウトなどが初期化されますので、お手数ですが再設定をお願いします。

- スマートフォンを変えたため、二段階認証ができない（担当者アカウント）
  管理者ユーザに依頼して、プロファイル画面で該当するユーザの二段階認証を**リセット**してください。次回ログイン時に、再び QR コードが表示されますので、新しいスマートフォンの認証アプリで読み込んでください。

- パスワード忘れや二段階認証ができなくなり、管理者アカウントでログインできない
  ログイン画面で、**初回ログインまたはパスワードをお忘れの場合**を押してパスワードをリセットしてください。ご登録いただいているメールアドレスにメールが届きます。このメールに記された、初期パスワードを使ってログインしてください。二段階認証の登録もリセットされますので、新規のワンタイムパスワード設定が必要になります。

17. 別冊文書

本サービスの関連文書として、以下の文書があります

1. 【別紙】【WVS2 ご契約者様向け】KDSec セキュリティ監視システム Web ポータル操作マニュアル_ログ項目一覧