オフィスまるごとサポートデバイスマネジメント
管理サイト　ユーザーマニュアル
各種設定

最終更新日　2018 年 9 月 14 日

株式会社オプティム

1 はじめに

本マニュアルは、管理サイトのメニュータブにある【証明書管理】、【管理】、【ブラウザー】、【Zone Management】、【設定】の設定に関するマニュアルです。

2 証明書管理

クライアント証明書、CA 証明書の管理を行います。

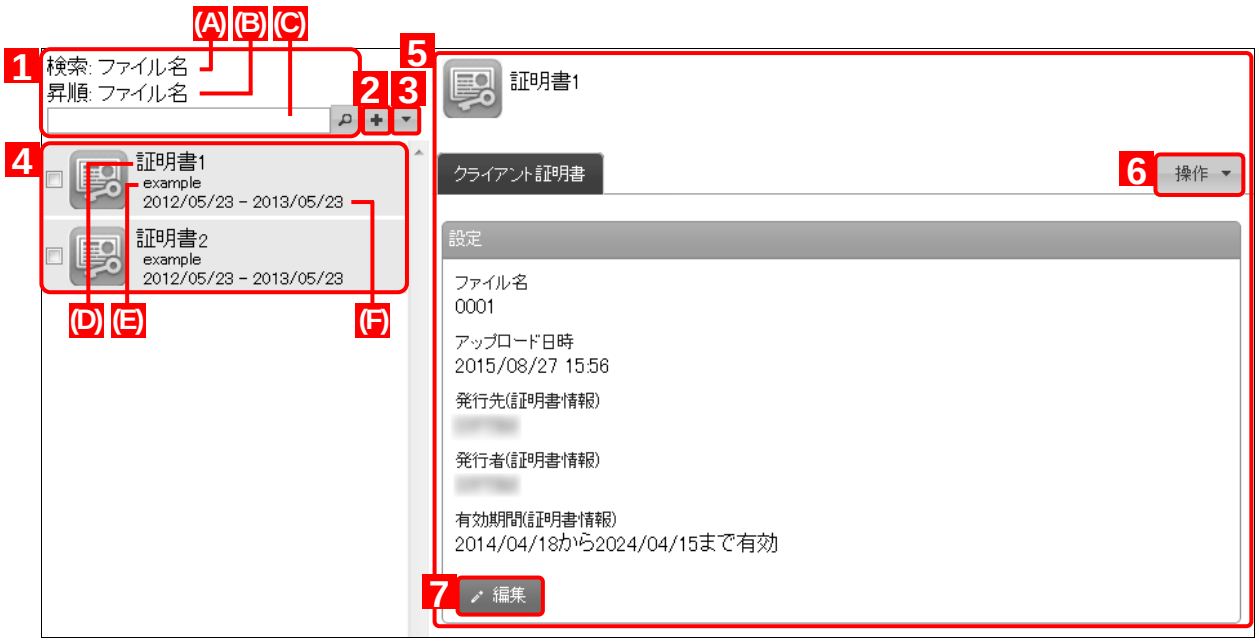
2.1　クライアント証明書管理

クライアント証明書をアップロードする画面です。証明書を 1 ファイルずつアップロードすることができます。当画面でアップロードした証明書は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－Exchange 設定(iOS 機器のみ)」や「管理サイトの操作－機器－VPN 設定(iOS 機器のみ)」で選択可能項目として表示されます。以下の画面は、特定のクライアント証明書を一覧から選択すると表示されます。アップロードした証明書は「機器」画面の「その他」タブの「クライアント証明書」画面から指定可能です。

2.1.1　クライアント証明書管理画面を表示する

クライアント証明書管理画面を表示します。

1．メニュータブをクリックします。
2．[クライアント証明書管理]をクリックします。



項番	対象	説明
1	検索/並び替え	(A)には検索対象項目、(B)には並び替えの対象項目が表示されます。検索する場合は、検索するキーワードを(C)に入力し、[検索]をクリックします。検索後、全ての証明書を再表示するにはブラウザーを再読み込み、または(C)を空欄にし、再度[検索]をクリックします。
2	[新規作成]	クリックすると証明書情報欄に入力欄が表示されます。証明書新規作成方法は 7 ページ「クライアント証明書をアップロードする」を参照してください。
3	[その他の操作]	クリックすると以下のメニューが表示されます。 ・全てにチェックを入れる：全てのチェックボックスにチェックが入ります。 ・全てのチェックをはずす：全てのチェックボックスからチェックを外します。 ・検索対象：検索対象をファイル名、発行先(証明書情報)のいずれかに変更することができます。 ・並び替え 昇順：ユーザー一覧をファイル名、発行先(証明書情報)、有効期間の開始、有効期間の終了のいずれかで昇順に並び替えます。 ・並び替え 降順：ファイル名、発行先(証明書情報)、有効期間の開始、有効期間の終了のいずれかで降順に並び替えます。 ・一括削除：チェックの入った証明書を削除します。詳細は「クライアント証明書をまとめて削除する」8 ページを参照してください。
4	証明書一覧	登録されている証明書一一覧が表示されます。 (D)：証明書ファイル名 (E)：発行先(証明書情報) (F)：有効期間
5	証明書情報	証明書一覧より選択した証明書情報が表示されます。
6	[操作]	クリックすると以下のメニューが表示されます。 ・削除：証明書を削除します。詳細は「クライアント証明書を削除する」8 ページを参照してください。
7	[編集]	登録されている証明書情報を編集することができます。詳細は「クライアント証明書を再アップロードする」7 ページを参照してください。

2.1.2　クライアント証明書をアップロードする

クライアント証明書をアップロードします。入力項目に関しては、「クライアント証明書管理の入力値」8 ページを参照してください。

※クライアント証明書が不正の場合は、エラーメッセージが表示されます。メッセージの案内に沿って、適切な対応を行ってください。

1．クライアント証明書管理画面を表示します。
2．[新規作成]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

2.1.3　クライアント証明書を再アップロードする

アップロード済みの証明書ファイルを差し替えます。入力項目に関しては、証明書をアップロードする場合と同様です。

1．証明書一覧より対象とする証明書をクリックします。
2．[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

2.1.4　クライアント証明書を削除する

アップロード済みのクライアント証明書を削除します。

1．証明書一覧より対象とする証明書をクリックします。
2．[操作]をクリックして操作メニューを表示させます。
3．[削除]をクリックします。
4．確認画面で[OK]をクリックします。

2.1.5　クライアント証明書をまとめて削除する

アップロード済みの証明書を複数指定して削除します。削除したい対象が多数ある場合でも、一度の操作で削除可能です。

1．証明書一覧より対象とする証明書のチェックボックスにチェックを入れます。
2．[その他の操作]をクリックしてその他の操作メニューを表示させます。
3．[一括削除]をクリックします。
4．確認画面で[OK]をクリックします。

2.1.6　クライアント証明書管理の入力値

クライアント証明書管理では以下の入力ルールで設定を行います。

項目名	ルール
【証明書ファイル】	アップロードする証明書を指定します。[参照]をクリックして、アップロードする証明書を選択してください。 なお、アップロードには PKCS #12 形式の証明書を指定してください。
【証明書を保護するパスワード】	パスワードで保護されている証明書アップロードする場合は、設定されているパスワードを入力します。パスワード未設定の場合は入力不要です。 半角英数字のみ入力できます。 255 文字以内で入力してください。 制御文字は入力できません。

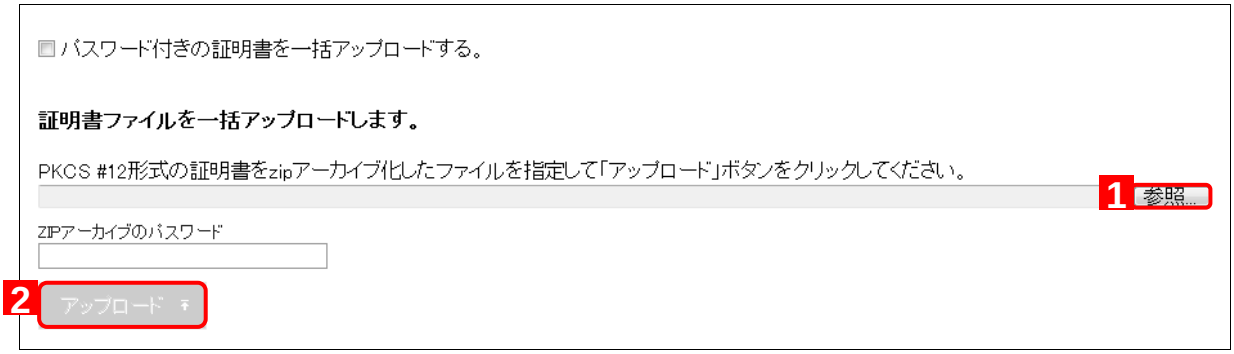
2.2　クライアント証明書一括アップロード

クライアント証明書をアップロードする画面です。複数の証明書を zip ファイルにまとめてアップロードすることができます。当画面でアップロードした証明書は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－Exchange 設定(iOS 機器のみ)」や「管理サイトの操作－機器－VPN 設定(iOS 機器のみ)」で選択可能項目として表示されます。

2.2.1　クライアント証明書一括アップロード画面を表示する

クライアント証明書一括アップロード画面を表示します。

1．メニュータブをクリックします。
2．[クライアント証明書一括アップロード]をクリックします。



項番	対象	説明
1	[参照]	インポートする証明書を指定します。指定したファイル名が左側に表示されます。
2	[アップロード]	指定された証明書をアップロードします。

2.2.2　クライアント証明書を一括アップロードする

zip ファイルにまとめた複数の証明書をアップロードします。

１．証明書一括アップロード画面を表示します。
２．アップロード対象の zip ファイルにパスワードで保護された証明書を含む場合は[パスワード付きの証明書を一括アップロードする]をチェックしてください。また、以降の手順３～手順７は同項目をチェックした場合のみ行ってください。未チェックの場合は、手順６に進んでください。
３．[ダウンロード]をクリックして、任意の場所に証明書パスワード入力用 CSV ファイルを保存してください。
４．ダウンロードした CSV ファイルを Excel やメモ帳で開き、証明書に設定されているパスワードを入力してください。パスワード未設定の証明書に対しては入力不要です。終了したら保存してファイルを閉じてください。拡張子は csv であることが必須です。
５．[参照]をクリックして、保存した CSV ファイルを選択してください。
６．[参照]をクリックして、アップロードする zip ファイルを選択してください。
７．パスワードで保護された zip ファイルを選択した場合は、設定されているパスワードを[ZIP アーカイブのパスワード]に入力してください。
８．[アップロード]をクリックしてください。
９．zip ファイルに含まれる証明書の一覧が表示されます。表示内容に問題がないことを確認してください。アップロード済みの同名証明書を上書きする場合は「同じファイル名の証明書がすでに存在した場合は上書き保存する」をチェックしてください。
１０．　[アップロードを実行]をクリックします。

※事前にアップロード対象とする証明書ファイルを zip ファイルとしてまとめておいてください。

※zip ファイルに含める証明書は PKCS #12 形式の証明書としてください。

2.2.3　クライアント証明書一括アップロードの入力値

クライアント証明書一括アップロードでは以下の入力ルールで設定を行います。

項目名	ルール
【ZIP アーカイブのパスワード】	半角英数字のみ入力できます。 255 文字以内で入力してください。 制御文字は入力できません。

2.3　CA 証明書管理

CA 証明書をアップロードする画面です。以下の画面は、特定の CA 証明書を一覧から選択すると表示されます。

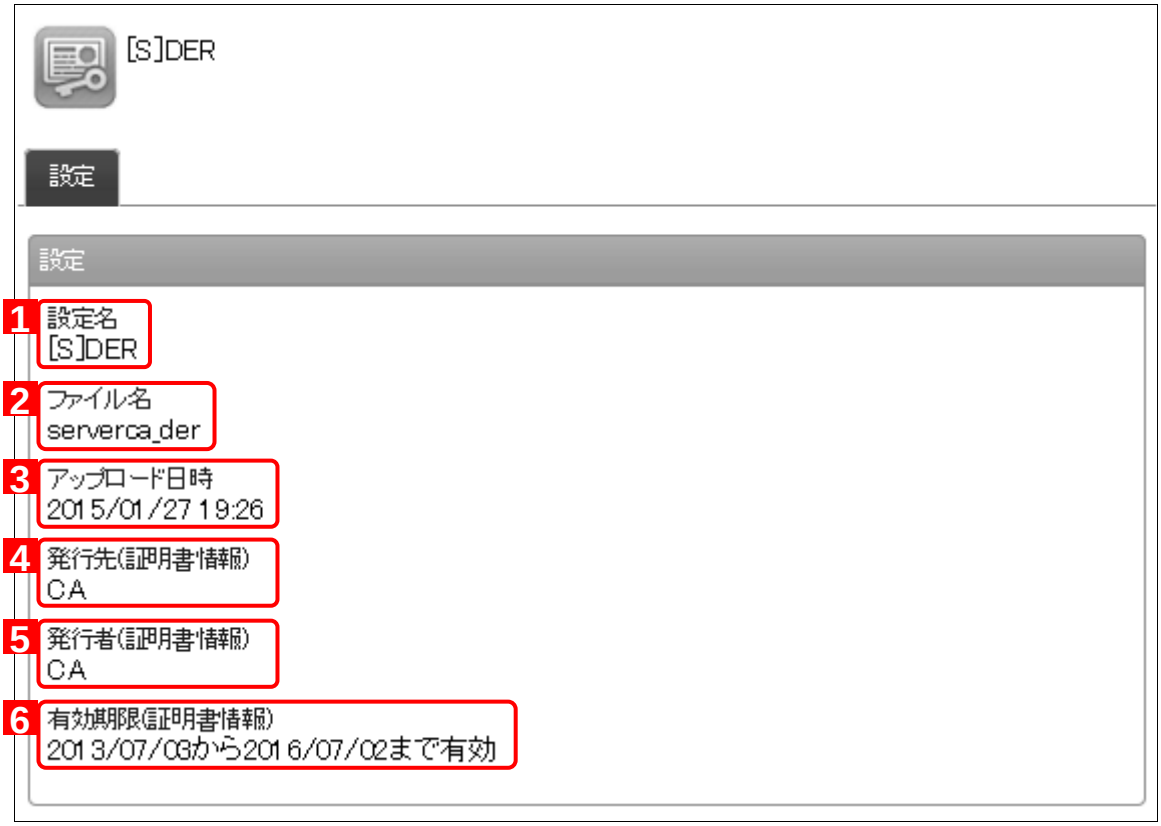
※Android 機器に CA 証明書をインストールするためには、事前に端末側のスクリーンロック設定が必要です。スクリーンロックをしていない場合には、設定を要求するメッセージが表示されます。また、スクリーンロック設定を無効にするには、CA 証明書をアンインストールする必要があります。

※iOS 機器に対しての CA 証明書は、本メニューをご利用いただけません。構成プロファイルとして配信してください。

2.3.1　CA 証明書画面を表示する

CA 証明書画面を表示します。

1．メニュータブをクリックします。
2．[CA 証明書]をクリックします。



項番	対象	説明
1	設定名	CA 証明書管理の設定名が表示します。
2	ファイル名	CA 証明書のファイル名が表示します。
3	アップロード日時	CA 証明書ファイルのアップロード日時を表示します。
4	発行先(証明書情報)	CA 証明書の発行先。
5	発行者(証明書情報)	CA 証明書の発行者。
6	有効期限(証明書情報)	CA 証明書の有効期限。

2.3.2　CA 証明書をアップロードする

CA 証明書をアップロードします。入力項目に関しては、「CA 証明書管理の入力値」12 ページを参照してください。

1．CA 証明書画面を表示します。
2．[新規作成]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

2.3.3　CA 証明書を再アップロードする

アップロード済みの証明書ファイルを差し替えます。入力項目に関しては、証明書をアップロードする場合と同様です。

1．証明書一覧より対象とする証明書をクリックします。
2．[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

2.3.4　CA 証明書を削除する

アップロード済みの CA 証明書を削除します。

1．証明書一覧より対象とする証明書をクリックします。
2．[操作]をクリックして操作メニューを表示させます。
3．[削除]をクリックします。
4．確認画面で[OK]をクリックします。

2.3.5　CA 証明書をまとめて削除する

アップロード済みの証明書を複数指定して削除します。削除したい対象が多数ある場合でも、一度の操作で削除可能です。

1．証明書一覧より対象とする証明書のチェックボックスにチェックを入れます。
2．　[その他の操作]をクリックしてその他の操作メニューを表示させます。
3．[一括削除]をクリックします。
4．確認画面で[OK]をクリックします。

2.3.6　CA 証明書管理の入力値

CA 証明書管理では以下の入力ルールで設定を行います。

項目名	ルール
【設定名】	CA 証明書の名称を指定します。 30 文字以内で入力してください。制御文字は入力できません。
【証明書ファイル】	アップロードする証明書を指定します。[参照]をクリックして、アップロードする証明書を選択してください。なお、アップロードには PEM または DER 形式の証明書を指定してください。

3 管理

ログの確認、アラート、通知設定、ポータル表示、認証制御、アカウントポリシーに関する設定を行います。設定項目は以下のとおりです。

3.1　ログ

ログの確認および、ダウンロードを行うことができます。直近一年間のログを確認できます。保存期間は一年間で、それ以前のログは削除されます。

機器に対する設定や操作が正常に行われたかどうかを確認する場合は、当画面から確認してください。

※[機器]タブから確認するログは、当画面で確認できるログから特定の機器に関するログのみを抽出したものとなります。

3.1.1　ログ画面を表示する

ログ画面を表示します。

1．メニュータブをクリックします。 2．[ログ]をクリックします。

項番	対象	説明
1	検索機能	検索機能を利用し、表示するログを絞り込むことができます。検索したい日時の種類([発生日時](*1)もしくは[受信日時] (*1))を選択し、日時、検索キーワードを入力し[検索]をクリックします。期間のみ入力されている場合は、指定した期間のログが全て表示されます。検索キーワードのみ入力されている場合は、そのキーワードを含むログが全て表示されます。再度全てのログを表示するにはブラウザーを再読み込み、または期間、検索入力欄を空欄にし[検索]をクリックします。 機器：機器名が表示されます。(特定の機器のログを表示している場合のみ表示されます。特定の機器のログの確認方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－管理－機器のログを確認する」を参照してください。) 種別：管理ログ、機器ログ、通知対象のみを選択することができます。 期間：(日時種類)：[発生日時] (*1)もしくは[受信日時] (*1)を選択します。 (日時)：手入力することもできますが(入力例：2011/05/16 01:00)、入力欄をクリックすると表示されるカレンダー画面でも指定することができます。 検索：検索したいキーワードを入力します。 CSV ダウンロード：ログの CSV ダウンロードを行います。詳細は「ログをダウンロードする」15 ページを参照してください。 (*1) 発生日時：該当アクションが発生した際のエージェント(端末)の日時 受信日時：該当アクションが発生し、サーバーで受信した日時
2	ログ	管理サイトの操作ログや、機器の動作ログが表示されます。 【種別】  ：管理サイト操作ログ  ：エージェントの動作ログ 【通知】  ：メール通知済みの場合に表示されます。 ：メール未通知の場合に表示されます。 ※メール通知対象外の場合は何も表示されません

3.1.2　ログの絞り込み表示を行う

表示するログを絞り込みます。ログの絞り込み条件の詳細については、「ログの絞り込み条件」16 ページを参照してください。

1．ログ画面を表示します。
2．絞り込み条件を指定して、[検索]をクリックします。

※ログメール通知に関しては、以下を参照してください。

⇒ログメール通知を新規作成する 21 ページ

3.1.3　ログをダウンロードする

表示されているログを CSV ファイルとしてダウンロードします。

1．ログを表示します。
2．[CSV ダウンロード]をクリックして、任意の場所に CSV ファイルを保存してください。

※最大 100,000 件のログがダウンロード可能です。

※件数によってはダウンロードに時間がかかる場合があります。

3.1.4　ログの絞り込み条件

ログの絞り込み条件の詳細は以下のとおりです。期間のみ入力されている場合は、指定した期間のログが全て表示されます。検索キーワードのみ入力されている場合は、そのキーワードを含むログが全て表示されます。再度全てのログを表示するにはブラウザーを再読み込み、または期間、検索入力欄を空欄にし[検索]をクリックします。

項目名	ルール
種別	種別を指定します。以下のいずれか１つ、または両方を指定してください。 ・管理ログ：管理サイトで行われた操作に関するログを表示します。 ・機器ログ：機器で行われた操作および、機器の挙動に関するログを表示します。管理サイトの操作により、機器で行われた挙動も該当します。
オプション	通知対象のみ：チェックするとログメール通知の対象となっているログのみを表示します。
期間	検索対象の日時の種類を指定します。「発生日時」もしくは、「受信日時」を指定してください。種類を指定後、日時を指定し、絞り込みます。From～To の形式で指定可能です。From のみ、To のみの指定も可能です。 入力欄をクリックするとカレンダーが表示されます。手入力も可能です。
検索	概要で絞り込みます。入力した文字列が概要に含まれるログを表示します。

3.2　アラート

アラートが検出された機器の一覧及び、管理外機器の一覧を表示します。

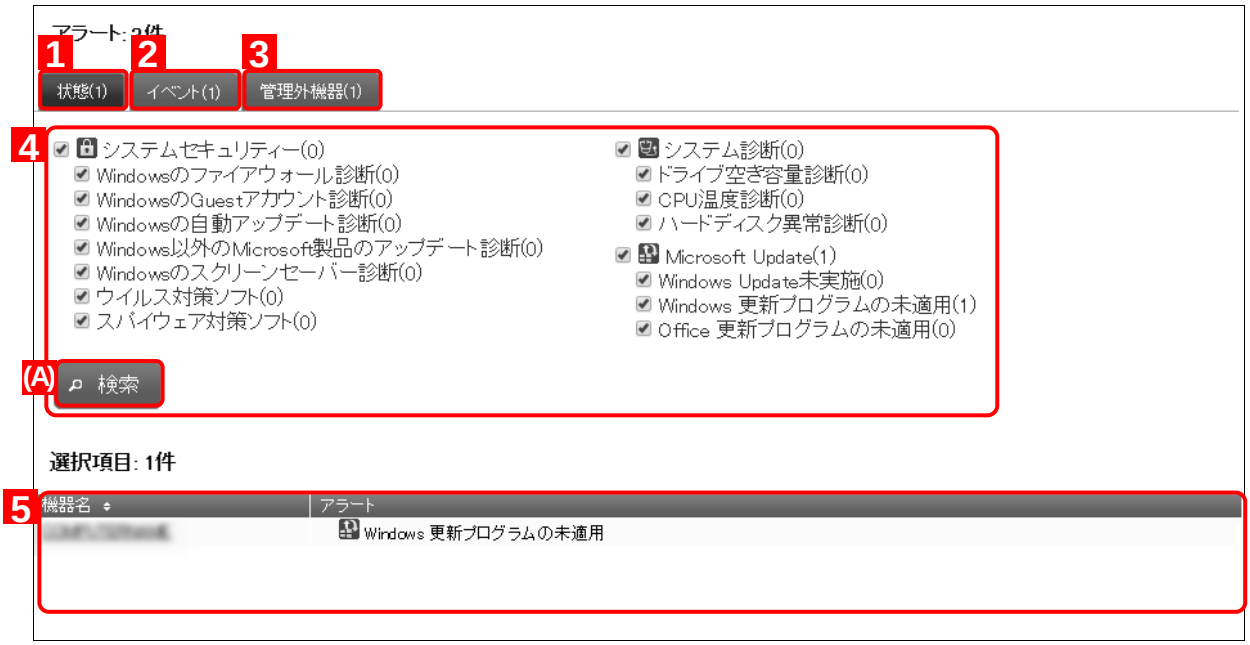
3.2.1　アラート画面を表示する

アラート画面を表示します。

1．メニュータブをクリックします。 2．[アラート]をクリックします。

【状態タブ】

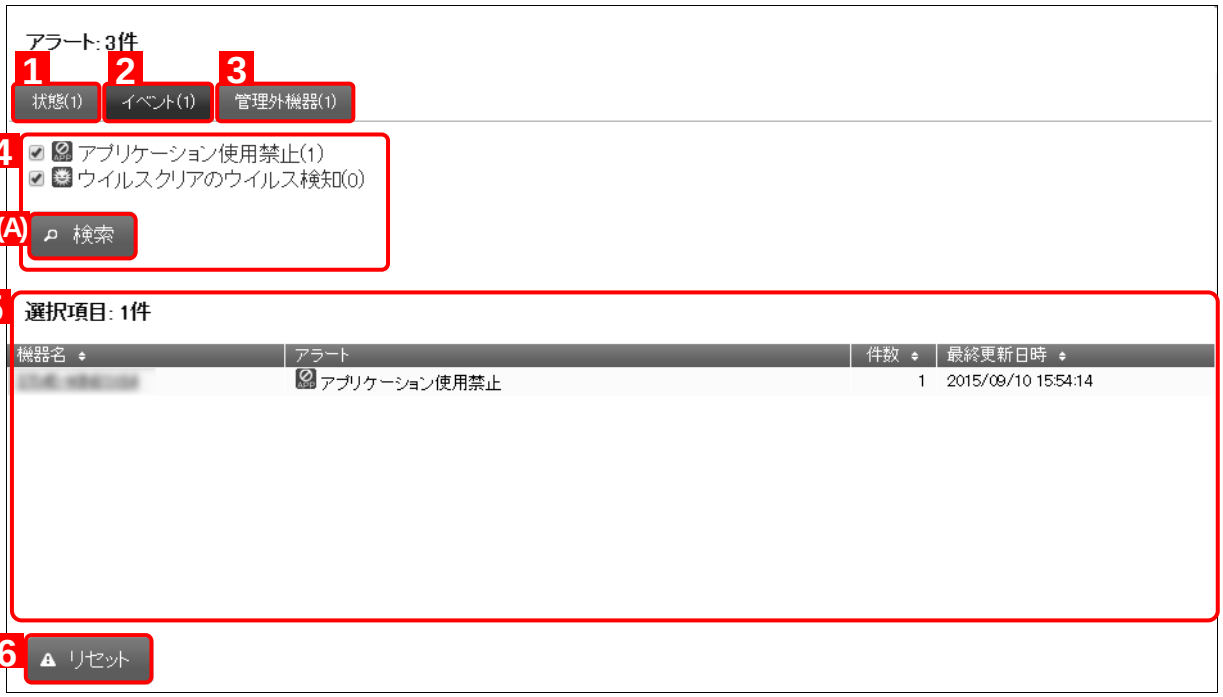
システムセキュリティー、システム診断、Microsoft Update に関するアラートが検出された機器の一覧を表示します。チェックボックスを有効にして検索をおこなうと、各アラートが検出された機器の一覧が表示されます。



項番	対象	説明
1	「状態」タブ	状態アラートが検出された機器の総数が()内に表示されます。
2	「イベント」タブ	イベントアラート画面に移動します。詳細は、18 ページ【イベントタブ】を参照してください。
3	「管理外機器」タブ	管理外機器一覧画面に移動します。詳細は、18 ページ【管理外機器タブ】を参照してください。
4	アラート検索	検索するアラートのチェックボックスを選択し、[検索](A)をクリックします。 アラート名の隣の()内には該当のアラートが検出された機器の総数が表示されます。
5	検索結果	4「アラート検索」で選択したアラートが検出された機器の一覧が表示されます。

【イベントタブ】

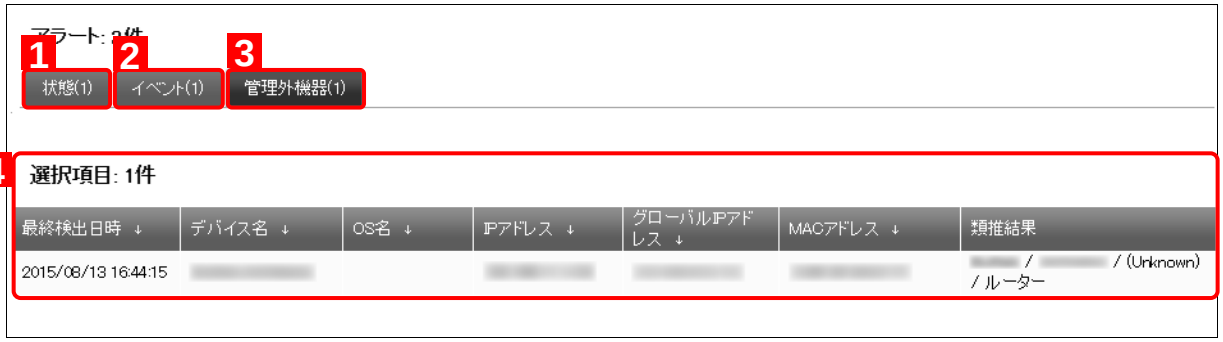
アプリケーション使用禁止もしくは、ウイルスクリアのウイルス検知のアラートが検出された機器の一覧を表示します。チェックボックスを有効にして検索をおこなうと、各アラートが検出された機器の一覧が表示されます。



項番	対象	説明
1	「状態」タブ	状態アラート画面に移動します。詳細は、17 ページ【状態タブ】を参照してください。
2	「イベント」タブ	イベントアラートが検出された機器の総数が()内に表示されます。
3	「管理外機器」タブ	管理外機器一覧画面に移動します。詳細は、18 ページ【管理外機器タブ】を参照してください。
4	アラート検索	検索するアラートのチェックボックスを選択し、[検索](A)をクリックします。 アラート名の隣の()内には該当のアラートが検出された機器の総数が表示されます。
5	検索結果	検索したアラートが表示されます。
6	リセット	5「検索結果」に表示された機器のアラートをリセットします。以降は該当機器に対する該当のアラートが検出されなくなります。

【管理外機器タブ】

検出された管理外機器の一覧が表示されます。管理外機器の詳細については、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－マップ－機器の種類」を参照してください。



項番	対象	説明
1	「状態」タブ	状態アラート画面に移動します。詳細は、17 ページ【状態タブ】を参照してください。
2	「イベント」タブ	イベントアラート画面に移動します。詳細は、18 ページ【イベントタブ】を参照してください。
3	「管理外機器」タブ	検出された管理外機器の総数が()内に表示されます。
4	管理外機器一覧	検索された管理外機器の一覧が表示されます。

3.2.2　アラートの検索を行う

アラートが検出された機器の検索を行います。

１．アラート画面を表示します。
２．「状態」タブもしくは、「イベント」タブをクリックします。
３．検索するアラートのチェックボックスを選択し、[検索]をクリックします。

※検索可能なアラートは以下のとおりです。

「状態」タブ：
- システムセキュリティー
  - Windows のファイアウォール診断
  - Windows の Guest アカウント診断
  - Windows の自動アップデート診断
  - Windows 以外の Microsoft 製品のアップデート診断
  - Windows のスクリーンセーバー診断
  - ウイルス対策ソフト
  - スパイウェア対策ソフト
- システム診断
  - ライブ空き容量診断
  - PU 温度診断
  - ハードディスク異常診断
- Microsoft Update
  - WindowsUpdate 未実施
  - Windows 更新プログラムの未適用
  - ffice 更新プログラムの未適用

「イベント」タブ：
- アプリケーション使用禁止
- ウイルスクリアのウイルス検知

3.2.3　アラート表示のリセットを行う

「イベント」タブのアラートのリセットを行います。リセット後は、該当機器に対する該当のアラートは検出されなくなります。

１．アラート画面を表示します。
２．[イベント]タブをクリックします。
３．リセットを行うアラートを表示させ、[リセット]をクリックします。

3.2.4　管理外機器を確認する

管理外機器の一覧を表示します。

１．アラート画面を表示します。
２．[管理外機器]タブをクリックします。

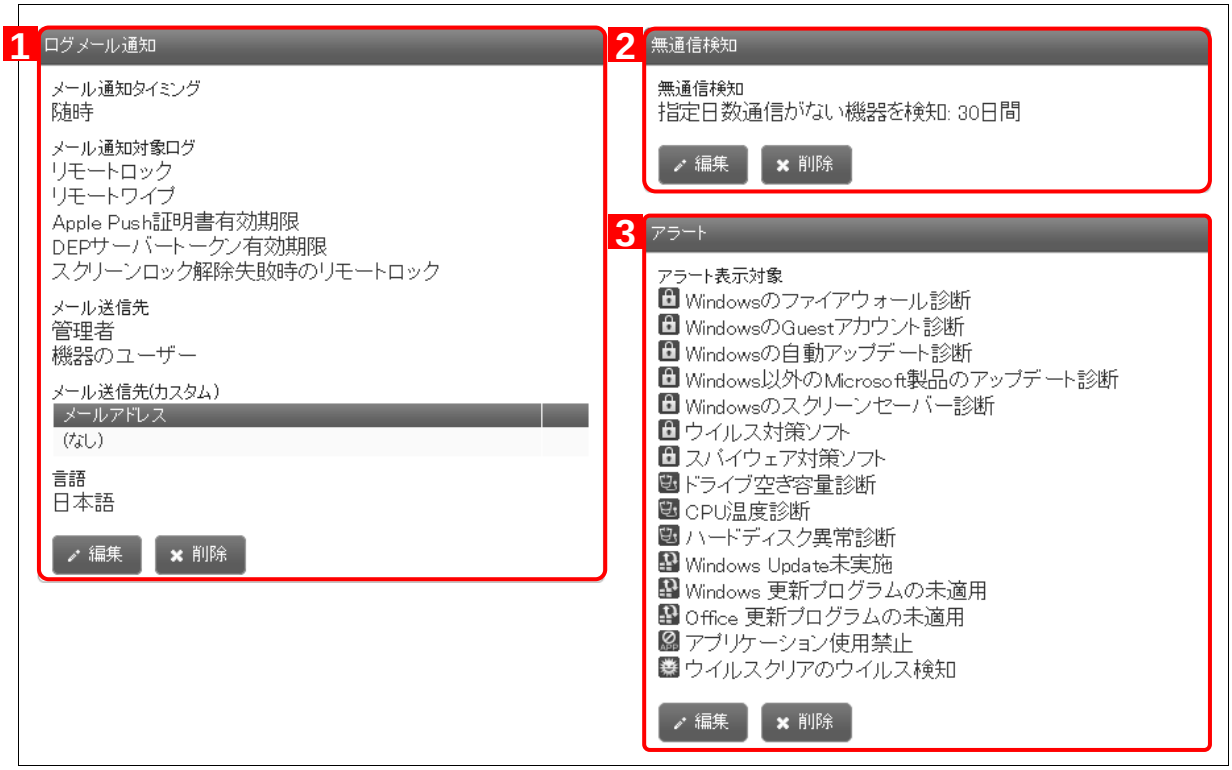
3.3　通知設定

一部のログはメールで通知することが可能です。当画面ではメール通知に関する設定を行います。また、通知可能なログの 1 つである無通信検知やアラートに関する設定を行います。

3.3.1　通知設定画面を表示する

通知設定画面を表示します。

1．メニュータブをクリックします。
2．[通知設定]をクリックします。



項番	対象	説明
1	ログメール通知	ログのメール通知に関する設定が表示されます。
2	無通信検知	無通信検知に関する設定が表示されます。
3	アラート	アラートに関する設定が表示されます。

3.3.2　ログメール通知を新規作成する

ログメール通知を行うための設定を新規に作成します。入力項目に関しては、「通知設定入力値」24 ページを参照してください。

1．通知設定画面を表示します。
2．ログメール通知の[新規作成]をクリックします。
3．通知条件を指定して、[保存]をクリックします。

3.3.3　ログメール通知を編集する

作成済みのログメール通知を編集します。入力項目に関しては、ログメール通知を新規作成する場合と同様です。

1．通知設定画面を表示します。
2．ログメール通知の[編集]をクリックします。
3．通知条件を指定して、[保存]をクリックします。

3.3.4　ログメール通知を削除する

作成済みのログメール通知を削除します。

1．通知設定画面を表示します。
2．ログメール通知の[削除]をクリックします。
3．確認画面で[OK]をクリックします。

3.3.5　無通信検知を新規作成する

無通信検知を行うための設定を新規に作成します。無通信検知とは、指定した間隔で管理サーバーと通信が行われていない機器を検知する機能です。検知した場合はログに出力されます。また、機器画面に表示している通信日時が赤字となります。検知対象は「指定した間隔で管理サーバーと通信が行われているか？」で判断しているため、機器の通信状態が良好でも管理サーバーと通信を行っていなければ検知対象となります。また、一般的なメールやインターネットの利用も管理サーバーと通信を行っていることにはなりません。入力項目に関しては、「通知設定入力値」24ページを参照してください。

1．通知設定画面を表示します。
2．無通信検知の[新規作成]をクリックします。
3．検知条件を指定して、[保存]をクリックします。

3.3.6　無通信検知を編集する

作成済みの無通信検知を編集します。入力項目に関しては、無通信検知を新規作成する場合と同様です。

1．通知設定画面を表示します。
2．無通信検知の[編集]をクリックします。
3．検知条件を指定して、[保存]をクリックします。

3.3.7　無通信検知を削除する

作成済みの無通信検知を削除します。

1．通知設定画面を表示します。
2．無通信検知の[削除]をクリックします。
3．確認画面で[OK]をクリックします。

3.3.8　アラートを新規作成する

アラートの表示設定を新規作成します。ここで表示対象に指定すると、機器画面のアラート(「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－アラート」を参照)にアラート状態が表示されます。

1．通知設定画面を表示します。
2．アラートの[新規作成]をクリックします。
3．アラート表示対象を指定して、[保存]をクリックします。

3.3.9　アラートを編集する

作成済みのアラートを編集します。

1．通知設定画面を表示します。
2．アラートの[編集]をクリックします。
3．アラート表示対象を指定して、[保存]をクリックします。

3.3.10 アラートを削除する

作成済みのアラートを削除します。

1．通知設定画面を表示します。
2．アラートの[削除]をクリックします。
3．確認画面で[OK]をクリックします。

3.3.11 通知設定入力値

通知設定では以下の入力ルールで設定を行います。

項目名	ルール
【メール通知タイミング】	メール通知のタイミングを指定します。以下のいずれか 1 つを指定してください。 ・随時：10 分ごとにメール通知を行います。 ・1 日 1 回：午前 3 時にメール通知を行います。 ・一時停止：メール通知を行いません。
【メール通知対象ログ】	通知対象とするログを指定します。複数指定が可能です。以下に記載がないログについては、メール通知が行えません。 ・リモートロック：リモートロックに関するログ。 ・リモートワイプ：リモートワイプに関するログ。 ・重要な iOS バージョンのリリース：重要な iOS バージョンのリリースに関するログ。 ・スクリーンロック設定のパスワード変更：スクリーンロック設定のパスワード変更に関するログ。 ・無通信検知：無通信検知に関するログ。 ・root 化状態検知：root 化状態検知に関するログ。 ・Jailbreak 状態検知：Jailbreak 状態検知に関するログ。 ・管理外検知：管理外検知に関するログ。 ・Microsoft Update 未実施：Microsoft Update 未実施に関するログ。 ・Office 更新プログラムの未適用：Office 更新プログラムの未適用に関するログ。 ・Windows 更新プログラムの未適用：Windows 更新プログラムの未適用に関するログ。 ・ウイルス対策ソフト：ウイルス対策ソフトに関するログ。 ・スパイウェア対策ソフト：スパイウェア対策ソフトに関するログ。 ・アプリケーション検知：アプリケーション検知に関するログ。 ・機器検出：機器検出に関するログ。 ・Apple Push 証明書有効期限：Apple Push 証明書の有効期間が一定の日数以内となった際に出力するログ。通知タイミングは、60 日前、30 日前、14 日前、7 日前～有効期限前日まで毎日。 ・DEP サーバートークン有効期限：DEP サーバートークンの有効期間が一定の日数以内となった際に出力するログ。通知タイミングは、60 日前、30 日前、14 日前、7 日前～有効期限前日まで毎日。 ・スクリーンロック解除失敗時のリモートロック･ワイプ：スクリーンロックのロック解除失敗に関するログ。 ・Windows のファイアウォール診断：Windows のファイアウォール診断に関するログ。 ・Windows の Guest アカウント診断：Windows の Guest アカウント診断に関するログ。 ・Windows の自動アップデート診断：Windows の自動アップデート診断に関するログ。 ・Windows 以外の Microsoft 製品のアップデート診断：Windows 以外の Microsoft 製品のアップデート診断に関するログ。 ・Windows のスクリーンセーバー診断：Windows のスクリーンセーバー診断に関するログ。 ・システムセキュリティの Office 設定結果：システムセキュリティによる Office への変更適用に関するログ。 ・システムセキュリティのブラウザー設定結果：システムセキュリティによるブラウザーへの変更適用に関するログ。 ・ドライブ空き容量診断：ドライブ空き容量診断に関するログ。 ・CPU 温度診断：CPU 温度診断に関するログ。 ・ハードディスク異常診断：ハードディスク異常診断に関するログ。 ・コンテンツ配信：コンテンツ配信に関するログ。 ・アカウントのロックアウト：アカウントのロックアウトに関するログ。 ・アプリケーション使用禁止：アプリケーション使用禁止に関するログ。 ・外部デバイス・CD/DVD/ブルーレイ禁止：外部デバイス・CD/DVD/ブルーレイ禁止に関するログ。 ・位置情報設定の変更：位置情報設定の変更に関するログ。 ・デバイス管理者権限の無効化：デバイス管理者権限変更時（有効/無効）に関するログ。 ※「Jailbreak 状態検知」は iOS エージェントがインストールされていない場合は表示されません。 ※「管理外検知」とは、プロファイルをアンインストールした iOS 機器を検知する機能です。検知した場合はログに出力されます。また、機器画面に表示している通信日時に「管理外」の文字が付与され、赤字となります。検知対象は「プロファイルをアンインストールしたか？」で判断しているため、リモートワイプなど、アンインストール以外の方法でプロファイルを削除しても検知対象となりません。
【メール送信先】	メール通知の送信先を指定します。複数指定が可能です。 ・管理者：ユーザー種別が管理者として登録されているユーザーのメールアドレスに送信します。 ・機器のユーザー：機器に登録されているユーザーのメールアドレスに送信します。

項目名	ルール
【メール送信先(カスタム)】	自由にメールアドレスを指定できます。「メール送信先」との併用が可能です。 255 文字以内で入力してください。 半角英数字・記号のみ入力できます。 @の前後にそれぞれ 1 文字以上入力してください。 ※をクリックすることで、最大 30 件まで入力行が追加されます。 をクリックすることで、入力行が削除されます。
【言語】	通知されるメールは、“ログ内容”と“その他の文言”(件名やフッターなど)の組み合わせで構成されています。当項目では、“その他の文言”に用いる言語を指定できます。プルダウンメニューに表示される言語より選択してください。
【無通信検知】	無通信と判断する間隔を指定します。以下のいずれか 1 つを指定してください。 ・指定時間通信がない機器を検知：時間を合わせて指定します。半角数字のみ入力できます。1 以上 23 以下で入力してください。 ・指定日数通信がない機器を検知：日数を合わせて指定します。半角数字のみ入力できます。1 以上 365 以下で入力してください。 ・なにもしない：無通信検知を行いません。
【アラート】	アラート表示対象を下記より選択します。 ・Windows のファイアウォール診断 ・Windows の Guest アカウント診断 ・Windows の自動アップデート診断 ・Windows 以外の Microsoft 製品のアップデート診断 ・Windows のスクリーンセーバー診断 ・ウイルス対策ソフト ・スパイウェア対策ソフト ・ドライブ空き容量診断 ・CPU 温度診断 ・ハードディスク異常診断 ・WindowsUpdate 未実施 ・Windows 更新プログラムの未適用 ・Office 更新プログラムの未適用 ・アプリケーション使用禁止 ・ウイルスクリアのウイルス検知

3.4　ポータル表示設定

ポータルメニュー(機器から直接、ユーザーや機器カスタム項目の選択等を行うための機能)の表示/非表示の設定を行うことができます。OS(Android / iOS / Windows)ごとに表示設定を行い、設定を保存した時点で企業管理下にあるすべての機器に対して設定を適用します。機器単位での設定は行えません。

※設定が機器に反映されるまでの時間は、サーバーや機器の通信状態に依存します。

3.4.1　ポータル表示設定画面を表示する

ポータル表示設定画面を表示します。

1．メニュータブをクリックします。
2．[ポータル表示設定]をクリックします。

項番	対象	説明
1	Android ポータル	Android ポータルの設定が表示されます。
2	iOS ポータル	iOS ポータルの設定が表示されます。
3	Windows ポータル	Windows ポータルの設定が表示されます。

3.4.2　ポータル表示設定を編集する

ポータル表示設定を編集します。入力項目に関しては、「ポータル表示設定の入力値」27 ページを参照してください。

1．ポータル表示設定画面を表示します。
2．[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

3.4.3　ポータル表示設定の入力値

ポータル表示設定では以下の入力ルールで設定を行います。

項目名	ルール
【Android ポータル】	Android ポータルの表示/非表示を指定します。 ・表示：Android ポータルを表示します。 ・非表示：Android ポータルを表示しません。
【iOS ポータル】	iOS ポータルの表示/非表示を指定します。 ・表示：iOS ポータルを表示します。 ・非表示：iOS ポータルを表示しません。
【Windows ポータル】	Windows ポータルの表示/非表示を指定します。 ・表示：Windows ポータルを表示します。 ・非表示：Windows ポータルを表示しません。

3.5　認証制御設定

エージェントのライセンス認証を行う際、事前に認証待ち機器としての登録が必要かどうかを設定します。本機能を用いることにより、管理者が許可した端末以外はエージェントのライセンス認証が行えないように制限を設けることが可能です。設定を保存した時点で有効となります。OS ごとの設定は行えません。

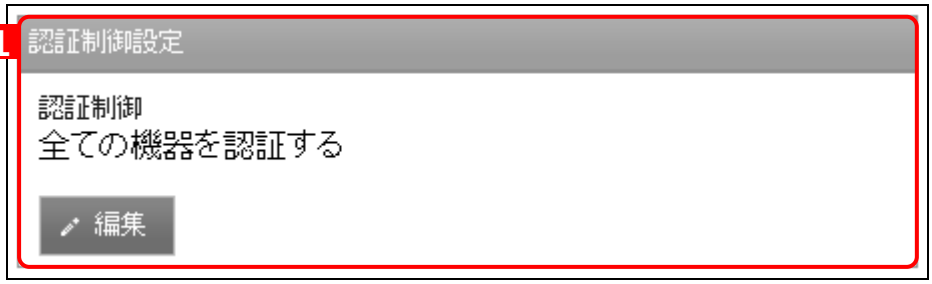
※機器の事前登録については以下を参照してください。
⇒「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－表示－機器を新規作成する」

※設定が機器に反映されるまでの時間は、サーバーや機器の通信状態に依存します。

3.5.1　認証制御設定画面を表示する

認証制御設定画面を表示します。

1．メニュータブをクリックします。
2．[認証制御設定]をクリックします。



項番	対象	説明
1	認証制御設定	認証制御設定が表示されます。

3.5.2　認証制御設定を編集する

認証制御設定を編集します。入力項目に関しては、「認証制御設定の入力値」28 ページを参照してください。

1．認証制御設定画面を表示します。
2．[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

3.5.3　認証制御設定の入力値

認証制御設定では以下の入力ルールで設定を行います。

項目名	ルール
【認証制御】	ライセンス認証制限の有無を指定します。 ・全ての機器を認証する：全ての機器でライセンス認証が行えます。認証待ち機器としての事前登録は不要です。 ・管理者が登録した機器のみを認証する：認証待ち機器として事前登録されている機器でのみライセンス認証が行えます。

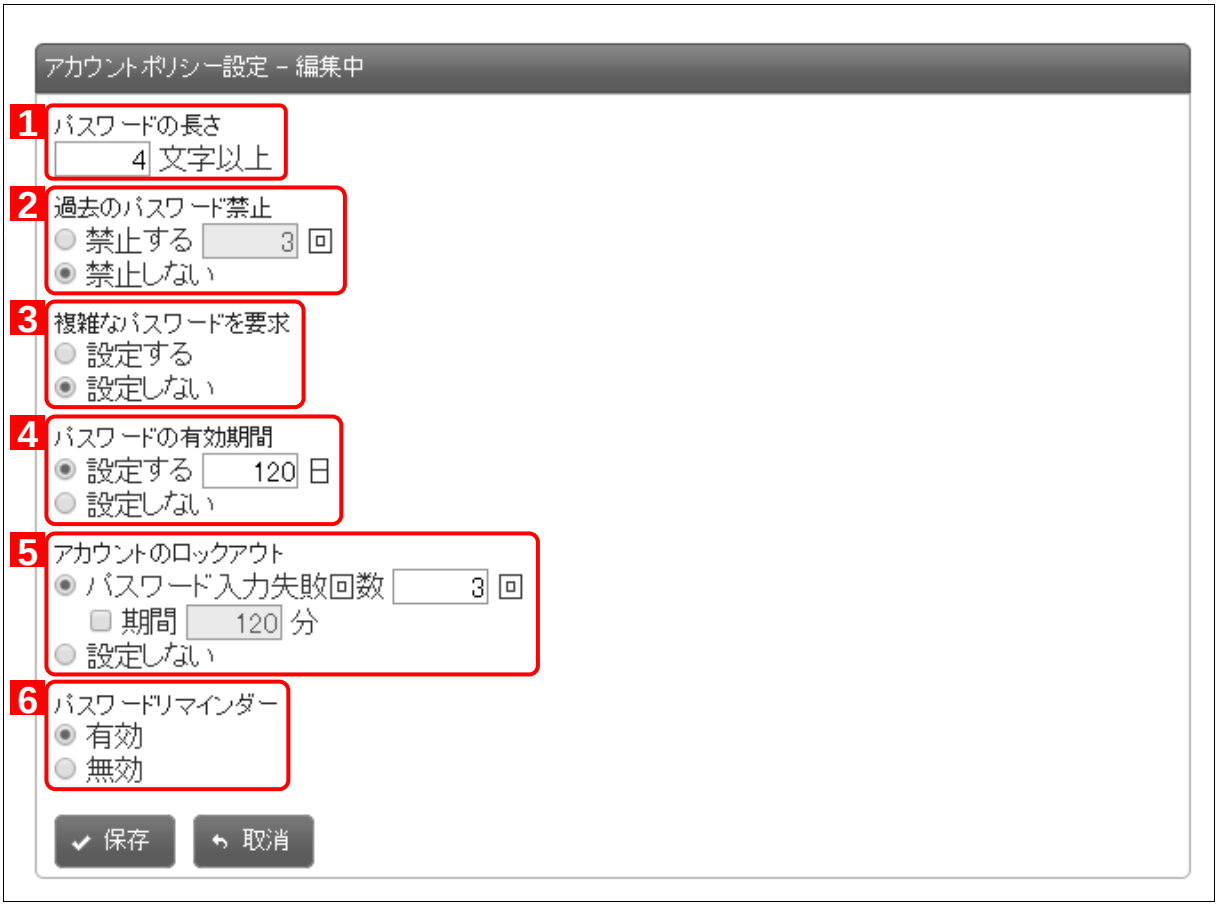
3.6　アカウントポリシー設定

セキュリティに関連するアカウントポリシーを設定します。

3.6.1　アカウントポリシー設定画面を表示する

アカウントポリシー設定画面を表示します。

1．メニュータブをクリックします。
2．[アカウントポリシー設定]をクリックします。



項番	対象	説明
1	パスワードの長さ	管理サイトへのログインパスワードのパスワード長を指定します。
2	過去のパスワード禁止	・禁止する：一度使用したパスワードを再利用できるまでに必要なパスワード変更回数を設定し、指定した変更回数を超えない限り、以前使ったことがあるパスワードの使用を禁止します。 ・禁止しない：以前使ったことがあるパスワードの再利用を禁止しません。同一パスワードを即座に再利用可能です。
3	複雑なパスワードを要求	・設定する：複雑なパスワードの規則を適用します。 ・設定しない：複雑なパスワードの規則を適用しません。 設定した場合、新しく設定するパスワードは、複雑さの要件を満たす必要があります(ユーザーのアカウント名またはメールアドレスに含まれる連続文字を使用しない / 8 文字以上 / 英大文字、英小文字、10 進数の数字 (0 から 9) アルファベット以外の文字 (!、$、#、% など)の 4 つの文字カテゴリの内、3 つのカテゴリを必ず使用する)。
4	パスワードの有効期間	・設定する：パスワードの有効期間を日数で指定します。 ・設定しない：パスワードの有効期間を指定しません。 設定した場合、パスワードの有効期間が切れるとログイン時にパスワード再設定画面が表示されますので、新しいパスワードを設定してください。 詳細は、「管理サイト ユーザーマニュアル 付録」の「付録－期限切れパスワードの更新」を参照してください。
5	アカウントのロックアウト	・パスワード入力失敗回数：パスワードの入力失敗時にアカウントをロックアウト(ログインできない状態にすること)します。ロックアウトまでの連続ログイン失敗回数を指定します。「期間」にチェックを入れると、自動でロックアウトが解除されるまでの分数を指定できます。チェックを入れない場合は、自動でロックアウトの解除は行われません。手動でロックアウトの解除を行ってください。 ・設定しない：パスワードの入力を失敗してもアカウントをロックアウトしません。 ロックされたアカウントの解除方法については、「管理サイト ユーザーマニュアル 組織/ユーザー」の「ユーザー－ユーザー－ロックアウトされたユーザーの解除を行う」を参照してください。
6	パスワードリマインダー	・有効：ログイン画面に「初めてご利用の方、パスワードを忘れた方はこちら」リンクが表示されます。リンク先からパスワード設定用のメールを送信することができます。 ・無効：ログイン画面に「初めてご利用の方、パスワードを忘れた方はこちら」リンクを表示しません。 詳しくは「管理サイト ユーザーマニュアル 付録」の「付録－新規パスワードの発行・パスワードの再設定」を参照してください。

3.6.2　アカウントポリシー設定を編集する

アカウントポリシー設定を編集します。入力項目に関しては、「アカウントポリシー設定の入力値」31 ページを参照してください。

1．アカウントポリシー設定画面を表示します。
2．[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

3.6.3　アカウントポリシー設定の入力値

アカウントポリシー設定では以下の入力ルールで設定を行います。

項目名	ルール
パスワードの長さ	パスワード長を指定します。32 文字までの指定が可能です。 4～32 の整数で入力してください。
過去のパスワード禁止	以前使ったことがあるパスワードの使用を禁止します。指定回数は以前に使用したパスワードが、再度使用できるようになるまでに必要な「新しいパスワードの設定回数」となります。例えば 3 回とした場合、3 回新しいパスワードが設定されるまでそのパスワードは再利用することが出来なくなります。 以下より選択します。 ・禁止する ・禁止しない 「禁止する」を選択した場合、回数を 1～100 の整数で入力してください。
複雑なパスワードを要求	以下より選択します。 ・設定する ・設定しない 設定した場合、新しく設定するパスワードは、以下の複雑さの要件を満たす必要があります。 ・ユーザーのアカウント名またはメールアドレスに含まれる 3 文字以上連続する文字列を使用しない。 ・長さは 8 文字以上。 ・次の 4 つのカテゴリのうち 3 つから文字を使う。 英大文字 (A から Z) 英小文字 (a から z) 10 進数の数字 (0 から 9) アルファベット以外の文字 (!、$、#、% など)
パスワードの有効期間	パスワードの有効期間を指定します。以下より選択します。 ・設定する ・設定しない 「設定する」を選択した場合、日数を 1～999 の整数で入力してください。
アカウントのロックアウト	パスワードの入力失敗時にアカウントをロックアウトするかどうか指定します。指定する場合は、ロックアウトまでの連続ログイン失敗回数を指定します。この失敗回数の上限を超えるとアカウントがロックアウトされます。ロックされたアカウントの解除については、「管理サイト ユーザーマニュアル 組織/ユーザー」の「ユーザー－ユーザー－ロックアウトされたユーザーの解除を行う」を参照してください。 また、ロックアウトされた場合に、自動でロックアウトが解除されるまでの時間を指定します。 以下より選択します。 ・パスワード入力失敗回数～回 ・設定しない 「パスワード入力失敗回数～回」を選択した場合、回数を 1 以上、10 以下にしてください。 「パスワード入力失敗回数～回」を選択した場合、「期間～分」が記入可能になります。期間は 1～99999 の整数で入力してください。
パスワードリマインダー	有効にすると、ログイン画面に「初めてご利用の方、パスワードを忘れた方はこちら」リンクが表示されます。 以下より選択します。 ・有効 ・無効

4 ブラウザー

ブラウザーの設定および、設定セットの作成を行います。作成した設定セットは一括機器設定および、機器ごとの設定にて適用してください。作成可能な設定セットは以下のとおりです。

※iOS 端末の管理サイトへの通信のタイミングにより、iOS のブラウザーに対する設定セットの反映まで最大 30 分ほどの時間が必要な場合があります。

※端末に DM Browser をインストールする前に、必ずエージェント認証を行ってください。エージェントが認証されていない場合、DM Browser をインストールしても Web フィルタリング、Web 閲覧履歴、お気に入りなどのブラウザー関連機能を使用することはできません。

4.1 Web フィルタリング

標準ブラウザーおよびDM Browser利用時のWeb閲覧を制限する機能です。閲覧できるWebサイトのURL指定、もしくは、閲覧できないWeb サイトのURL 指定のいずれかを行うことができます。Web サイトの閲覧が禁止された場合には、禁止された旨のポップアップメッセージを表示します。

※本機能は、Android の場合、標準ブラウザーおよびDM Browser のみ、iPhone/iPad の場合は、DM Browser のみ有効です。
Android 6.x 以降の場合、本機能は DM Browser のみで有効です。

※Android の場合：DM Browser とは、Android 端末の標準ブラウザーとは別にインストールする無償ブラウザーです。
Android4.0 以降に搭載されている標準ブラウザーの機能の 1 つであるシークレットモードで Web 閲覧をすると、管理サイトの Web フィルタリング機能で禁止しているページであっても、閲覧をすることができてしまいます。そのため、この DM Browser を Android 端末にインストールし、DM Browser のみの使用に制限することで(管理サイトのアプリケーション禁止機能を使用)、シークレットモードでのブラウザー閲覧を防ぎ、Web フィルタリングの抜け道をなくします。ご利用状況により DM Browser の利用をご検討ください。

※DM Browser の使用方法については、以下を参照してください。
Android の場合⇒「Android ユーザーマニュアル」
iPhone/iPad の場合⇒「iOS ユーザーマニュアル」

※Web フィルタリングを利用する場合は、ブラウザー設定で javascript を有効にしてください。

※Web フィルタリングを設定すると、Android の場合は、標準ブラウザーおよび DM Browser のお気に入りから、
iPhone/iPad の場合は、DM Browser のお気に入りからフィルタリング対象となる URL のお気に入りが削除されます。

※本製品のご利用を解約いただいても、機器に対して行った設定はそのまま保持されるのでご注意ください。解約の際は事前に各種設定セットに「設定なし」を適用してください。

4.1.1　Web フィルタリング画面を表示する

Web フィルタリング画面を表示します。

1．メニュータブをクリックします。
2．[Web フィルタリング]をクリックします。

項番	対象	説明
1	設定名	お好きな名前を入力します。
2	URL フィルタリング設定	・許可する URL を指定する : URL 一覧で設定した Web サイトのみ閲覧できるようにします。 ・禁止する URL を指定する : URL 一覧で設定した Web サイトは閲覧できないようにします。
3	URL 一覧(先頭部分の一致による比較)	・URL : 制限対象となる URL を入力します。(入力する URL は完全一致していなくても、前方一致で適用されます) ※[追加] をクリックすると、入力欄が追加されます。 ※[削除] をクリックすると、入力欄が削除されます。 ※URL を 31 個以上登録した場合、ご使用の端末によっては Web フィルタリングに時間がかかる場合がございます。 ※すべての URL へのアクセスを禁止したい場合は、「URL フィルタリング設定」から「許可する URL を指定する」を選択し、「URL 一覧」の[削除] で全ての URL を削除してから保存してください。すべての URL へのアクセスが禁止されます。

※新規作成、編集、削除、複製方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－設定セット作成方法」を参照してください。

4.1.2　Web フィルタリングの設定セット入力値

Web フィルタリングの設定では以下の入力ルールで設定を行います。

項目名	ルール
【設定名】	設定セットの名称を指定します。1 文字～30 文字で入力してください。
【URL フィルタリング設定】	閲覧する URL の使用禁止条件を以下より選択します。 ・許可する URL を指定する (指定されていない URL は禁止)：ホワイトリスト形式。 ・禁止する URL を指定する (指定されていない URL は許可)：ブラックリスト形式。
【URL 一覧 (先頭部分の一致による比較)】	フィルタリングする URL を入力します。「https」から始まる URL も指定可能です。入力必須です。 設定内で重複はできません。 200 文字以内で入力してください。 半角英数字、記号のみで入力してください。 先頭は「http://」か「https://」にしてください。 ※  をクリックすると、URL 情報を追加します。1000 件まで登録可能です。

4.2　Web 閲覧履歴

標準ブラウザーおよび DM Browser 利用時の Web 閲覧履歴を取得し、管理サイトのログに表示する機能です。また、ブラウザーに保存されている、Web 閲覧履歴を削除することができます。上記操作は、同期のタイミングで定期的に実行されます。

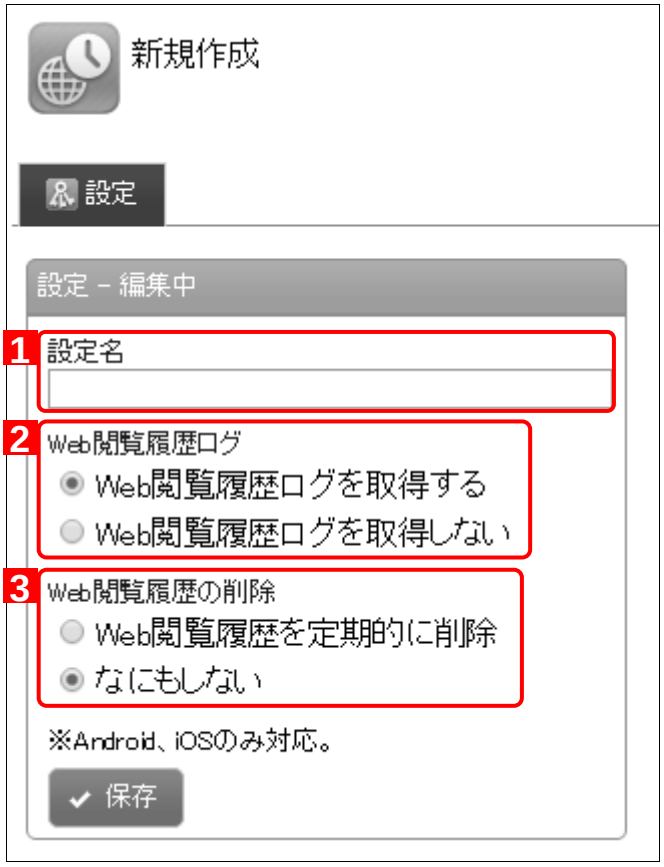
※本機能は、Android の場合、標準ブラウザーおよび DM Browser のみ、iPhone/iPad の場合は、DM Browser のみ有効です。
Android 6.x 以降の場合、本機能は DM Browser のみで有効です。

※DM Browser の使用方法については、以下を参照してください。
Android の場合⇒「Android ユーザーマニュアル」
iPhone/iPad の場合⇒「iOS ユーザーマニュアル」

4.2.1　Web 閲覧履歴画面を表示する

Web 閲覧履歴画面を表示します。

1．メニュータブをクリックします。
2．[Web 閲覧履歴]をクリックします。



※新規作成、編集、削除、複製方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－設定セット作成方法」を参照してください。

項番	対象	説明
1	設定名	お好きな名前を入力します。
2	Web 閲覧履歴ログ	・Web 閲覧履歴ログを取得する：Web サイトの閲覧履歴を取得しログ画面に表示します。 ・Web 閲覧履歴ログを取得しない：Web サイトの閲覧履歴の取得を行いません。
3	Web 閲覧履歴の削除	・Web 閲覧履歴を定期的に削除：Web サイトの閲覧履歴を同期のタイミングで削除します。 ・なにもしない：Web サイトの閲覧履歴の削除を行いません。

4.2.2　Web 閲覧履歴の設定セット入力値

Web 閲覧履歴の設定では以下の入力ルールで設定を行います。

項目名	ルール
設定名	設定セットの名称を指定します。 1 文字～30 文字で入力してください。
Web 閲覧履歴ログ	Web 閲覧履歴取得の有効/無効の設定を以下より選択します。 ・Web 閲覧履歴ログを取得する：端末の Web 閲覧履歴取得を「取得する」に設定します。 ・Web 閲覧履歴ログを取得しない：端末の Web 閲覧履歴取得を「取得しない」に設定します。
Web 閲覧履歴の削除	取得した Web 閲覧履歴を定期的に削除するように設定します。 ・Web 閲覧履歴を定期的に削除：Web 閲覧履歴の定期削除を有効にします。 ・なにもしない：Web 閲覧履歴の操作をなにもしないに設定します。

4.3　お気に入り

機器のブラウザーに対して、お気に入りの追加や、ホームページ設定を行う機能です。ホームページ設定は、Windows 機器のみ行えます。

※本機能は、Android の場合は、標準ブラウザーおよび DM Browser のみ、iPhone/iPad の場合は、DM Browser のみ、Windows の場合は、Internet Explorer 9-11 のみ有効です。Android6.x 以降の場合、本機能は DM Browser のみで有効です。

※DM Browser の使用方法については、以下を参照してください。
Android の場合⇒「Android ユーザーマニュアル」
iPhone/iPad の場合⇒「iOS ユーザーマニュアル」

4.3.1　お気に入り画面を表示する

お気に入り画面を表示します。

1．メニュータブをクリックします。
2．[お気に入り]をクリックします。

項番	対象	説明
1	設定名	お好きな名前を入力します。
2	お気に入り	タイトル：お気に入りに登録する Web サイトのタイトルを入力します。(タイトルはお好きなものを入力してください。) URL：お気に入りに登録する Web サイトの URL を入力します。 ※[追加] をクリックすると、入力欄が追加されます。 ※[削除] をクリックすると、入力欄が削除されます。
3	ホームページ	ブラウザーのホームページを設定します。ホームページとして設定するサイトの URL を入力してください。 ※ホームページの設定は Windows のみ適用されます。

※新規作成、編集、削除、複製方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－設定セット作成方法」を参照してください。

4.3.2　お気に入りの設定セット入力値

お気に入りの設定では以下の入力ルールで設定を行います。

大項目名	小項目名	ルール
【設定名】	設定セットの名称を指定します。1 文字～30 文字で入力してください。	
【お気に入り】	タイトル	お気に入りのタイトル名を設定します。 100 文字以内で入力してください。 半角英数字、「-」、「_」、「@」のみで入力してください。
	URL	お気に入り先 URL 情報を設定します。 200 文字以内で入力してください。 半角英数字、記号のみで入力してください。 先頭は「http://」か「https://」にしてください。 ※をクリックすると、URL 情報を追加します。300 件まで登録可能です。
【ホームページ】	ブラウザーのホームページを設定します。ホームページとして設定するサイトの URL を入力してください。 200 文字以内で入力してください。 半角英数字、記号のみで入力してください。 先頭は「http://」か「https://」にしてください。 ※ホームページの設定は Windows のみ適用されます。 ※「お気に入り」の設定は行わず、「ホームページ」の設定のみ行う場合は、お気に入りの入力欄は削除をクリックして削除した後に、[保存]をクリックしてください。	

5 Zone Management

Zone Management に関する情報の確認、追加、削除、編集を行うことができます。

作成可能な設定セットは以下のとおりです。

5.1　ゾーン

Zone Management を利用することで、特定のネットワーク・位置・時間帯に該当する機器に対して、設定セットを適用することが可能です。接続先のネットワーク・位置情報・時間帯の組み合わせを「ゾーン」として定義することで、条件に一致する機器に対して複数の設定セットを適用することが可能です。まず、「ゾーン」でネットワークを指定し、次に「ポリシー」で設定セットを指定します。その後、その 2 つをゾーンポリシー構成で組み合わせます。作成したゾーンポリシー構成は、一括機器設定および、機器ごとの設定にて適用してください。
本章では、「ゾーン」についての説明を行ないます。

※「ポリシー」に関しては以下を参照してください。
⇒ポリシー　45 ページ

※「ゾーンポリシー構成」に関しては以下を参照してください。
⇒ゾーンポリシー構成　47 ページ

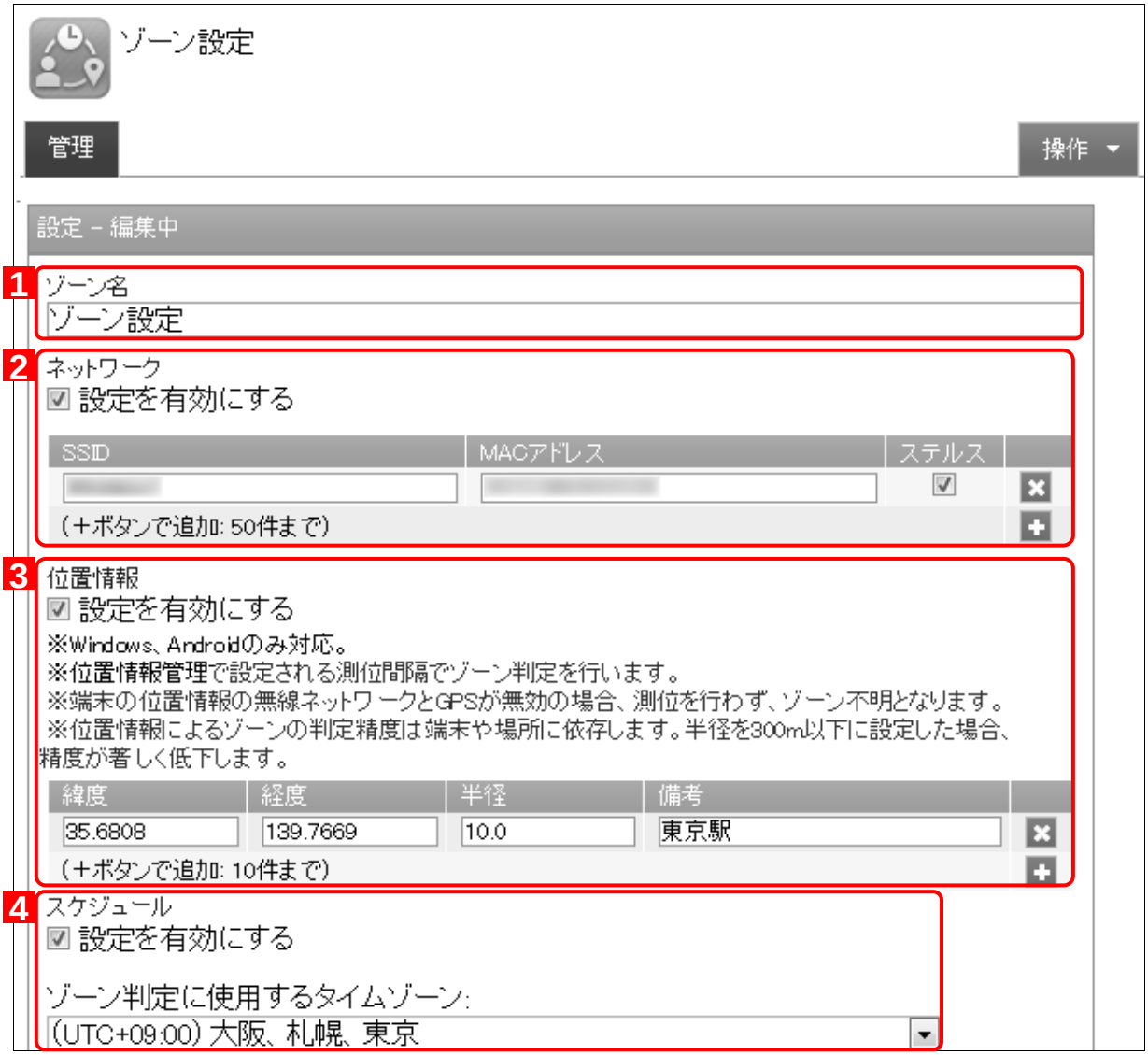
※一括機器設定に関しては以下を参照してください。
⇒「管理サイト ユーザーマニュアル 機器」の「機器－一括機器設定－一括して複数の機器に設定セットを適用する」

※機器ごとの設定に関しては以下を参照してください。
⇒「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－設定－機器に設定テンプレートを適用する」

5.1.1　ゾーン画面を表示する

ゾーン画面を表示します。

1．メニュータブをクリックします。
2．[ゾーン]をクリックします。


ゾーン設定
管理
操作
設定 - 編集中
1
ゾーン名
ゾーン設定
2
ネットワーク
設定を有効にする
SSID
MACアドレス
ステルス
(+ボタンで追加: 50件まで)
3
位置情報
設定を有効にする
※Windows、Androidのみ対応。
※位置情報管理で設定される測位間隔でゾーン判定を行います。
※端末の位置情報の無線ネットワークとGPSが無効の場合、測位を行わず、ゾーン不明となります。
※位置情報によるゾーンの判定精度は端末や場所に依存します。半径を300m以下に設定した場合、精度が著しく低下します。
緯度
経度
半径
備考
35.6808
139.7669
10.0
東京駅
(+ボタンで追加: 10件まで)
4
スケジュール
設定を有効にする
ゾーン判定に使用するタイムゾーン:
(UTC+09:00) 大阪、札幌、東京

項番	対象	説明
1	ゾーン名	お好きな名前を入力します。
2	ネットワーク	ゾーンに設定するアクセスポイントの SSID と MAC アドレスを登録します。 ・設定を有効にする ネットワークによるゾーン管理を有効にします。「設定を有効にする」チェックボックスは設定編集画面でのみ有効です。 ・SSID：SSID を入力します。 ・ステルス：ESS-ID ステルスを有効としたネットワークの場合はチェックボックスをオンにします。 ・MAC アドレス：アクセスポイントの MAC アドレスを入力します。 ※[追加] をクリックすると、入力欄が追加されます。 ※[削除] をクリックすると、入力欄が削除されます。 ※1 ゾーンに対して、登録できる SSID は 50 件です。 ※ステルス機能を利用したアクセスポイントを登録する場合、端末側にネットワークプロファイルを登録し、「自動的に接続する」を有効にする必要があります。
3	位置情報	ゾーンに設定する位置情報を登録します。 ・設定を有効にする 位置情報による Zone Management を有効にします。「設定を有効にする」チェックボックスは設定編集画面でのみ有効です。 ・緯度 ・経度 ・半径 ・備考 ゾーンに該当するエリアの緯度と経度、またゾーンの広さを半径で指定します。経度と緯度に指定された位置情報を中心に、指定された長さの半径で円を形成します。この円の中身が「ゾーン内」となります。 例：緯度が 90°、経度が 120.0°半径が 500m で指定された場合、緯度 90°経度 120.0°を中心とした半径 500m の円で囲まれた領域がゾーン内となります。 ※[追加] をクリックすると、入力欄が追加されます。 ※[削除] をクリックすると、入力欄が削除されます。 ※1 ゾーンに対して、登録できる位置情報は 10 件です
4	スケジュール	ゾーンに設定するスケジュールを登録します。 ・設定を有効にする 特定の日時による Zone Management を有効にします。「設定を有効にする」チェックボックスは設定編集画面でのみ有効です。 ・曜日 ・開始時刻 ・終了時刻 ゾーンに該当する曜日と時刻を指定します。開始時刻は 00:00～23:59、終了時刻は 00:00～35:59 が指定可能です。終日に設定する場合は、00:00～24:00 を指定します。 ※[追加] をクリックすると、入力欄が追加されます。 ※[削除] をクリックすると、入力欄が削除されます。 ※1 ゾーンに対して、登録できるスケジュールは 10 件です

※単一のゾーンに対して複数の SSID を設定した場合、いずれかの SSID が検知された場合に「ゾーン内」となります。また複数の位置情報とスケジュール設定も、いずれかの設定が満たされた場合に「ゾーン内」となります。

SSID と位置情報、SSID とスケジュールなど異なる設定を複数組み合わせる場合は、全ての設定を満たされた場合に「ゾーン内」となります。

【複数組み合わせた場合】

場所：SSID1、 SSID2、 SSID3

時間：月曜 17:00～18:00、土曜 16:00～17:30

□上記のゾーン設定では SSID が「SSID1」「SSID2」「SSID3」の**いずれか**に一致し、**かつ**日時が「月曜 17:00～18:00」「土曜 16:00～17:30」の**いずれか**に一致した場合に「ゾーン内」となります。

※Android8 の場合は、Wi-Fi の SSID 情報及び位置情報の取得が 1 時間に 1 回程度へ制限されます。ゾーンの切り替えを即時検知することができず、約 1 時間程度のタイムラグが発生します。

※新規作成、編集、削除方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－設定セット作成方法」を参照してください。

5.1.2　ゾーンの入力値

ゾーンの設定では以下の入力ルールで設定を行います。

項目名	ルール	
【ゾーン名】	ゾーン名を入力します。入力必須です。 設定内で重複はできません。 制御文字は入力できません。 30 文字以内で入力してください。 [S]から始めることはできません。	
【ネットワーク】	ゾーンに設定するネットワークの SSID、MAC アドレスの設定を行います。 ネットワークは 50 件以下にしてください。 SSID と MAC アドレスは重複しないものを入力してください。	
	設定を有効にする	特定の日時による Zone Management を有効にします。 チェックボックスをオンにして設定を有効にします。
	SSID	SSID 名を入力します。入力必須です。 32 文字以内で入力してください。 半角英数字、「-」、「_」、「@」のみで入力してください。 ※1 ゾーンに対して、登録できる SSID は 50 件です。
	MAC アドレス	アクセスポイントのMACアドレスを入力します。「XX:XX:XX:XX:XX:XX」(X は大文字の16 進数)という形式で入力してください。
	ステルス	ESS-IDステルスを有効としたネットワークの場合はチェックボックスをオンにします。
【位置情報】	ゾーンに設定する位置の緯度と経度、エリアの範囲を指定します。位置情報は10件以下にしてください。 ※端末の位置情報の無線ネットワークとGPSが無効な場合、または管理サイトの時刻と端末時刻の間に大幅な差がある場合は、測位を行わず「ゾーン不明」となります。「ゾーン不明」と判定された端末に特定のポリシーを適用することが可能です。詳細は「ゾーンポリシー構成」(47ページ)を参照してください。 ※エージェントの位置情報取得が「許可しない」の場合、位置情報を取得しません ※Windows、Androidのみ対応。位置情報の測位間隔については、以下を参照してください。 ・「管理サイト ユーザーマニュアル Windows」の「Windows－位置情報管理」 ・「管理サイト ユーザーマニュアル Android」の「Android－位置情報管理」	
	設定を有効にする	位置情報によるZone Managementを有効にします。チェックボックスをオンにして設定を有効にします。ゾーンに該当するエリアの緯度と経度、またゾーンの広さを半径で指定します。
	・緯度	-90から90の値で入力してください。
	・経度	-180から180の値で入力してください。
	・半径	1から20037500の値で入力してください。
	・備考	備考を入力します。30文字以内で入力してください。
【スケジュール】	ゾーンに設定するスケジュールを登録します。 スケジュールは10件以下にしてください。	
	設定を有効にする	特定の日時によるZone Managementを有効にします。 チェックボックスをオンにして設定を有効にします。
	・ゾーン判定に使用するタイムゾーン	判定に使用するタイムゾーンをプルダウンメニューから選択します。
	・曜日	スケジュール設定を有効にする曜日のチェックボックスをオンにします。
	・開始時刻	00:00～23:59 の間で指定します。
	・終了時刻	00:00～35:59 の間で指定します。 ※土曜日に日跨りで Zone Management を設定する場合は、xx:xx～24:00 までの設定と、日曜日 0:00～35:59 までの設定の 2 つを実施することで、日跨り後の制御が可能となります。

5.2　ポリシー

Zone Management におけるポリシー画面では、ゾーン(41 ページ)に適用するポリシー(設定セットの束)を指定します。

※リモートロックのポリシーは現在 Android のみ対応しています。

※Zone Management に関しては以下を参照してください。

⇒ゾーン 41 ページ

5.2.1　ポリシー画面を表示する

ポリシー画面を表示します。

1．メニュータブをクリックします。
2．[ポリシー]をクリックします。

項番	対象	説明
1	ポリシー名	お好きな名前を入力します。
2	機能タブ	【Android 設定】Android 機器に対してポリシー単位での機器設定を行います。
		【Windows 設定】Windows 機器に対してポリシー単位での機器設定を行います。

※新規作成、編集、削除方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－設定セット作成方法」を参照してください。

5.2.2　ポリシー単位で機器設定を行う

ポリシー単位で設定セットの適用を行います。指定したポリシーに属する全ての機器に適用されます。

1．ポリシー一覧より対象とするポリシーをクリックします。
2．目的の機器設定タブをクリックします。
3．[編集]をクリックします。
4．プルダウンメニューから適用する設定セットを選択します。
5．[保存]をクリックします。編集をキャンセルする場合は[取消]をクリックします。

※デフォルトの「所属組織に従う」を選択した場合、上位組織の設定が継承されます。
※上位組織が設定されていない場合に「所属組織に従う」を選択した場合、「設定なし」を選択した場合と同じ動きとなります。
※「機器の設定に従う」を選択した場合、ゾーンポリシー以外で設定されている設定が継承されます。

5.2.3　ポリシーの入力値

ポリシーの設定では以下の入力ルールで設定を行います。

タブ名	項目名	ルール
管理	【ポリシー名】	ポリシーの名称を指定します。入力必須です。 設定内で重複はできません。 制御文字は入力できません。 30 文字以内で入力してください。 [S]から始めることはできません。
Android 設定 /Windows 設定	【設定】	ポリシーにおける設定セットの使用設定を行います。 適用する設定セットを選択します。設定変更の必要がない機能に対しては初期値である「(設定なし)」のままで結構です。 ※デフォルトの「所属組織に従う」を選択した場合、上位組織の設定が継承されます。 ※上位組織が設定されていない場合に「所属組織に従う」を選択した場合、「設定なし」を選択した場合と同じ動きとなります。 ※「機器の設定に従う」を選択した場合、ゾーンポリシー以外で設定されている設定が継承されます。

5.3　ゾーンポリシー構成

Zone Management におけるゾーンポリシー構成画面では、ゾーン(41 ページ)とポリシー(45 ページ)を組み合わせ、ネットワーク単位での設定セットの割り当てを実現します。
作成したゾーンポリシー構成は、一括機器設定および、機器ごとの設定にて適用してください。

※Zone Management に関しては以下を参照してください。
⇒ゾーン 41 ページ

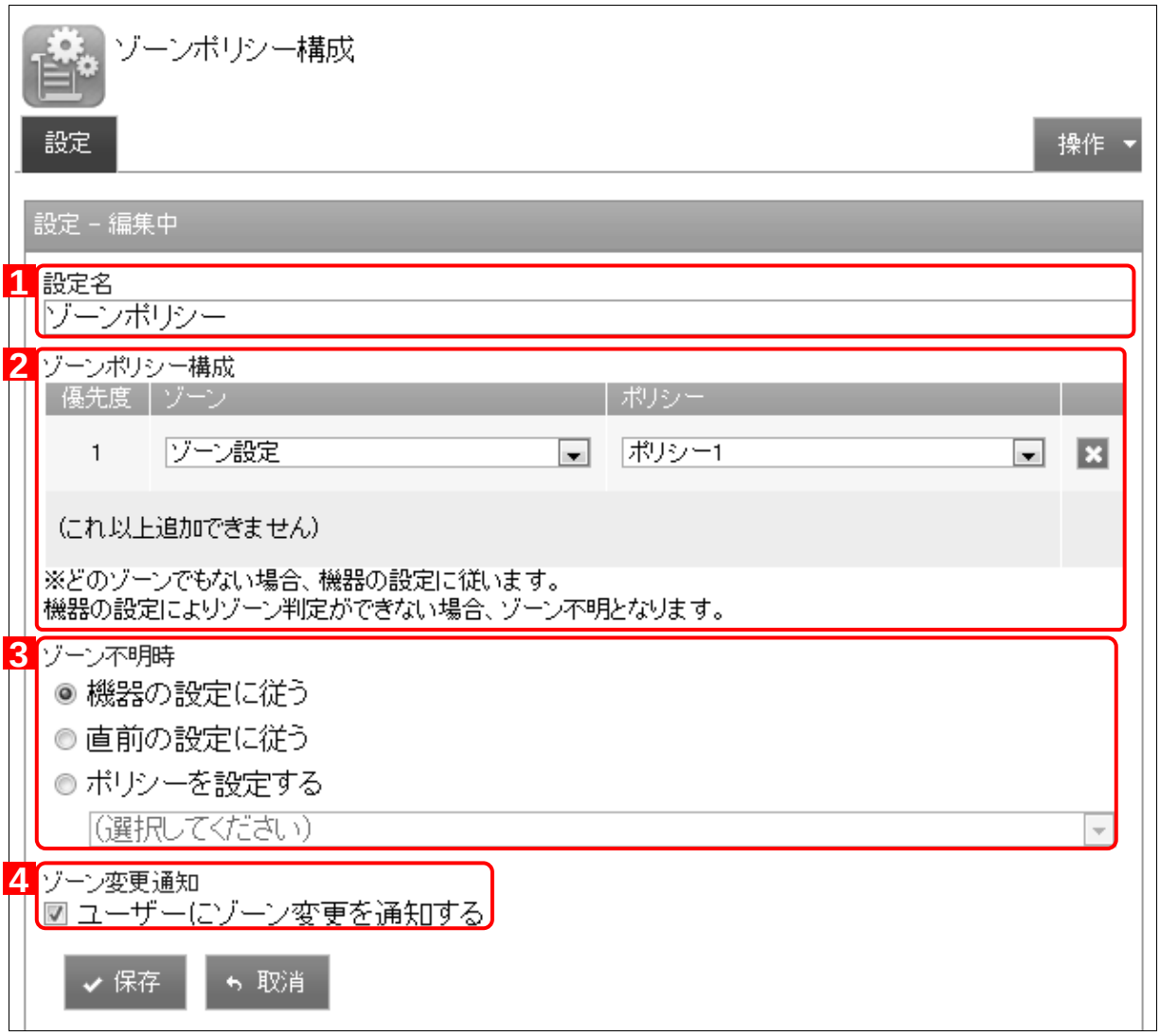
※一括機器設定に関しては以下を参照してください。
⇒「管理サイト ユーザーマニュアル 機器」の「機器ー一括機器設定ー一括して複数の機器に設定セットを適用する」

※機器ごとの設定に関しては以下を参照してください。
⇒「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作ー機器ー設定ーーの機器に設定テンプレートを適用する」

5.3.1　ゾーンポリシー構成画面を表示する

ゾーンポリシー構成画面を表示します。

1．メニュータブをクリックします。
2．[ゾーンポリシー構成]をクリックします。



項番	対象	説明
1	設定名	お好きな名前を入力します。
2	ゾーンポリシー構成	ゾーンに設定するゾーン優先度、ゾーン、ゾーンポリシーを登録します。 ・ゾーン優先度：ゾーン優先度を入力します。 ・ゾーン：ゾーンを選択します。 ※ゾーンについての詳細は、41 ページを参照してください。 ・ポリシー：ゾーンポリシーを選択します。 ※ポリシーについての詳細は、45 ページを参照してください。 ※[追加] ✚をクリックすると、入力欄が追加されます。 ※[削除] ✖をクリックすると、入力欄が削除されます。 ※1 ゾーンポリシー構成に対して、登録できるゾーンは 10 件です
3	ゾーン不明時	ゾーン不明と判定された場合に適用される設定を選択します。「機器の設定に従う」、「直前の設定に従う」、「ポリシーの設定する」から選択できます。「ポリシーを設定する」を選択する場合は、不明時に適用するポリシーを選択できます。 ※コンピューターの Wi-Fi スイッチが切られている場合、Wi-Fi が機器設定により OFF に設定されている場合、サーバー時刻と端末の時刻が著しく異なる場合、無線ネットワークまたは GPS が OFF の場合には、端末は「ゾーン判定不可」を検知して、ゾーン不明というステータスを管理サイトに送信します
4	ゾーン変更通知	端末のゾーンが変更された際に、端末上に通知を表示します。 ※Android 端末では通知領域、Windows 機器ではステータスバー上のバルーンに通知が表示されます。 ※スケジュールと位置情報によるゾーン設定によっては、大量の通知が発生する可能性がございます。過度な情報通知により、ユーザーの利便性を下げてしまう可能性があるので慎重に設定してください。

※新規作成、編集、削除、複製方法は、「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－設定セット作成方法」を参照してください。

5.3.2　ゾーンポリシー構成の設定セット入力値

ゾーンポリシー構成の設定では以下の入力ルールで設定を行います。

項目名		ルール
【設定名】		設定セットの名称を指定します。入力必須です。 設定内で重複はできません。 制御文字は入力できません。 30 文字以内で入力してください。 [S]から始めることはできません。
【ゾーンポリシー構成】※	作成したゾーンとポリシーを紐付け、さらにゾーンに関して優先度を設定を行います。 最大 10 件のゾーンとポリシーの組み合わせをゾーンポリシー構成に追加することが可能です。	
	ゾーン	機能ごとに適用するゾーンセットを選択します。 ※ゾーンを重複することは出来ません。
	ゾーン不明時	ゾーン不明と判定された場合に適用するポリシーを選択します。
	ポリシー	機能ごとに適用するゾーンポリシーを選択します。
	ゾーン変更通知	このオプションが有効な場合は、端末のゾーンが変更された際に、端末上の通知領域に通知を表示します。

※ゾーンポリシー構成で作成するゾーンとポリシーの組み合わせは 10 件以下にしてください。

6 設定

管理サイトにログイン中のユーザー自身が保持する項目の、確認および編集を行います。

設定項目は以下のとおりです。

6.1　個人設定

当画面では管理サイトの環境設定を行います。ここで行う設定は、設定変更を行ったユーザー自身にのみ有効であり、別のユーザーでログインした際には反映されません。ユーザー種別が閲覧者のユーザーでも設定変更が可能です。

6.1.1　個人設定画面を表示する

個人設定画面を表示します。

1．メニュータブをクリックします。
2．[個人設定]をクリックします。

項番	対象	説明
1	環境	表示言語に関する設定が表示されます。
2	パスワード	パスワードに関する設定が表示されます。
3	アプリケーションメモ	アプリケーションメモに関する設定が表示されます。

6.1.2　表示言語を変更する

管理サイトの表示言語を変更します。入力項目に関しては、「個人設定入力値」52 ページを参照してください。

1．個人設定画面を表示します。
2．環境の[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

6.1.3　パスワードを変更する

管理サイトへログインするためのパスワードを変更します。入力項目に関しては、「個人設定入力値」52 ページを参照してください。

1．個人設定画面を表示します。
2．パスワードの[編集]をクリックします。
3．必要事項を入力して、[保存]をクリックします。

6.1.4　アプリケーションメモを削除する

アプリケーションメモを削除します。アプリケーションメモとは、アプリケーション禁止機能の設定にて利用できる、入力補助の仕組みです。アプリケーション禁止機能の[メモから追加]をクリックした際にアプリケーション一覧に表示されます。

1．個人設定画面を表示します。
2．アプリケーションメモの[クリア]をクリックします。
3．確認画面で[OK]をクリックします。

※アプリケーションメモの追加に関しては、以下を参照してください。
⇒「管理サイト ユーザーマニュアル 管理サイトの操作」の「管理サイトの操作－機器－アプリ－アプリケーションメモに追加する(Android 機器)」

6.1.5　個人設定入力値

個人設定では以下の入力ルールで設定を行います。

項目名	ルール
【言語】	管理サイトの表示言語をプルダウンメニューより選択します。
【現在のパスワード】	現在のパスワードを入力してください。入力必須です。 4 文字以上、20 文字以下にしてください。 半角英数字のみ入力できます。
【新規パスワード】	変更後のパスワードを入力してください。入力必須です。 4 文字以上、20 文字以下にしてください。 半角英数字のみ入力できます。
【新規パスワード(再入力)】	【新規パスワード】と同じ値を入力してください。