

セキュリティ機能ガイド



版	ページNo.	改版内容	改版日
1		制定	2014/7/9
2	全般	機能改良に伴う画像変更	2014/10/29
2	8,11,23,27,28,29,35,37	機能改良に伴い記載内容修正	2014/10/29
2	19	BitLocker暗号化手順追加	2014/10/29
2	25	リモート操作時の注意点4件追加	2014/10/29
2	26	リモートロック実行結果3件追加	2014/10/29
2	30	リモートワイプ実行結果2件追加	2014/10/29
2	34	実行に失敗した時に対処する 対処方法1件追加	2014/10/29
3	全般	機能改良に伴う画像変更	2015/3/26
3	8,11	警告内容追加	2015/3/26
4	全般	機能改良に伴う画像変更	2015/4/30
4	24	端末が30日以上外部ネットワークに接続されない場合の注意事項追記	2015/4/30
4	31	Windows 8.1 Proのリモートワイプからの復旧方法を記載	2015/4/30
4	39	よくあるご質問（FAQ）のリンクを追記	2015/4/30
5	全般	機能改良に伴う画像と文言を修正	2015/9/30
6	7,12,13	注意事項を追記	2015/10/22
6	全般	仕様改良に伴う画像変更	2015/10/22
7	5	OSやエディションによる機能差を「補足事項」として集約	2016/3/24
7	10,15,23,29,30	2016/3/23以前からご利用のお客様へのご案内を追記	2016/3/24
7	全般	機能改良に伴う画像変更	2016/3/24
8	26	注意事項を追記	2016/6/6
9	17,18	機能改良に伴う画像と文言を修正・追加	2016/7/27
9	25	OS側仕様変更に伴う画像の変更	2016/7/27
9	26	手順の追加	2016/7/27
10	42-54	紛失モードについての手順の追加	2016/9/27
10	全般	機能改良に伴う文言の修正	2016/9/27
10	6	注意事項を追記	2016/9/27
11	21,22	機能改良に伴う画像と文言を修正・追加	2016/12/21
12	5,6,10,11,28,30,55,57	リモートロックについての画像の変更と文言の追加	2017/4/27
12	3,48	iPod touch対応に伴う文言の変更	2017/4/27



「セキュリティ機能」操作ガイド



LanScope Anの「セキュリティ」とは？

p.5



1. リモート操作ができる人を社内で決める

p.7



2. 社内のセキュリティ状況を確認する

p.9

3. 第三者に操作されないように、端末にロックをかける

p.28

4. 情報漏えいを防ぐため、端末のデータを削除する

p.34

5. 実行に失敗した時に対処する

p.41

6. パスコードを忘れた場合にパスコードをオフにする
(iOSのみ)

p.42

7. 紛失した端末を探す (iOSのみ)

p.45



よくあるご質問

p.55



制限事項

p.57

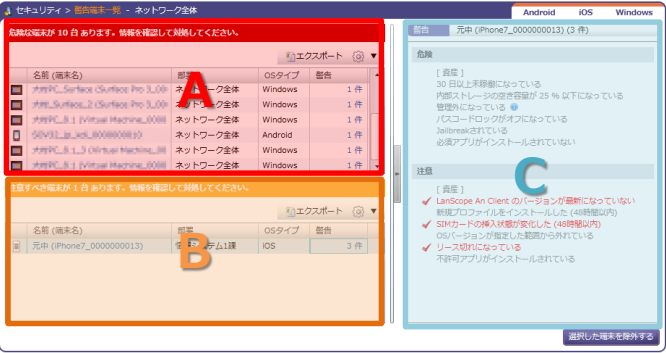
LanScope Anの「セキュリティ」とは？

管理対象の端末の状態確認および、リモートロック・リモートワイプなどのリモート操作を実施できる機能です。紛失や盗難の際にパスワードの設定やデータ消去など、万が一の際の情報漏えい対策に役立ちます。

1. 「警告端末一覧」画面

危険な端末、注意すべき端末を自動で判断します。

【警告端末一覧画面】



- A: 「危険な端末」がどの端末で、どれだけルールに抵触しているのかが分かります。
- B: 「注意すべき端末」がどの端末で、どれだけルールに抵触しているのかが分かります。
- C: 選択した端末が具体的にどのようなルールに抵触しているのかが分かります。

2. 「リモート実行」画面

端末の状態を確認し、対処が必要な端末かどうか判断し実行することができます。

【リモート実行画面】



- A: 選択した端末が、どのルールに抵触しているのかがわかります。
- B: 端末に「リモートロック」「リモートワイプ」「パスコードオフ」「紛失モードオン/オフ」「位置情報取得」を実行できます。
- C: 端末の情報を確認できます。
- D: 端末が現在、どこにあるのか、どのように移動したのかがわかります。
- E: 端末でどのような操作、通話を行ったのかまた資産ポリシーに違反しているのかがわかります。

※操作、通話履歴はAndroidのみ取得可能です。
※「リモートロック」「リモートワイプ」「パスコードオフ」「紛失モードオン/オフ」「位置情報取得」はOS・エディションにより機能差があります。(p.6)

リモートワイプ・パスコードオフ・紛失モード・位置情報取得機能は、OSやエディションにより一部機能差があります。詳細は次のとおりです。

- ・ **リモートロック：**
Android 7.0以降の端末にパスワードが設定されている場合、ロック解除パスワードが設定できません。
- ・ **リモートワイプ：**
LanScope Anで対応しているエディション（別紙『スタートアップガイド for Windows』参照）の内、Windows 8.1 / Windows 10 Homeには対応していません。（リモートロックは対応しています）
※端末側でPINが設定されている場合、リモートワイプはできません。
- ・ **パスコードオフ：**
iOSのみ対応しています。
- ・ **紛失モード：**
iOS 9.3以降で「監視モード」がオンになっている端末のみ対応しています。
※「監視モード」の設定はiOSの機能です。Apple社のApple Configurator を利用して設定するか、Device Enrollment Program（DEP）機能を利用して設定してください（「監視モードに設定する」の項目を有効にしたDEPプロファイルを端末に割当てて、端末をアクティベーションする必要があります）。
- ・ **位置情報取得：**
iOS 9.3以降で「監視モード」と「紛失モード」がオンになっている端末のみ対応しています。

●2016/3/23以前からWindows端末を管理している場合は必ずご確認ください

2016/3/23以前からLanScope AnでWindows端末を管理している場合で、Anクライアントの移行を行っていない端末（*）の場合、OSやエディションによる機能差は次のとおりです。
* 注釈：2016/3/23以前からLanScope AnでWindows端末を管理している場合、Anクライアントの移行が必要です。別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照して移行を完了させてください。（Android・iOSの場合、この作業は不要です）

- ・ **リモートワイプ：**
LanScope Anで対応しているエディション（別紙「スタートアップガイド for Windows 」参照）の内、Windows 8.1 / Windows RT 8.1は対応していません。（リモートロックは対応しています）

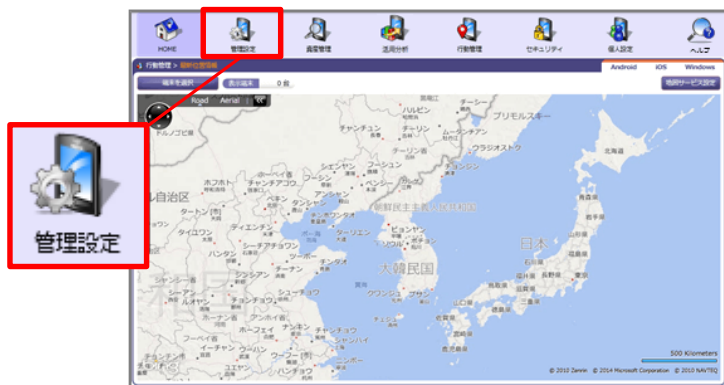
1 リモート操作ができる人を社内で決める

リモートロックやワイプ、紛失モードを実行するために、アカウントに実行権限を付与します。実行権限がないアカウントはリモートロック・ワイプ、紛失モードを実行できません。

1

画面上部にあるメニュー「管理設定」をクリックします。

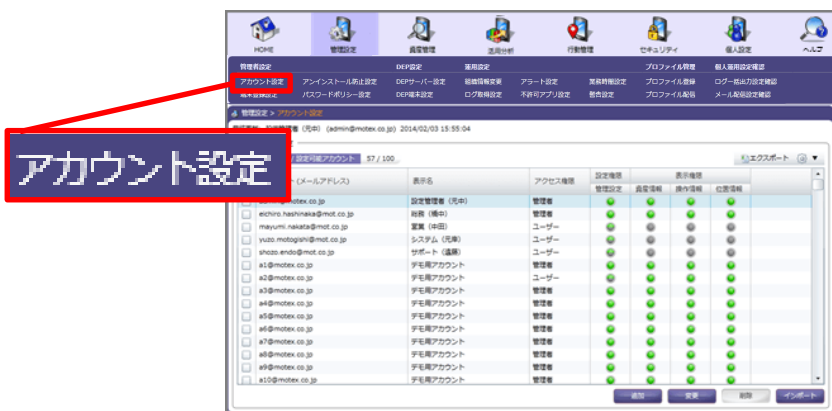
【TOP画面】



2

「アカウント設定」をクリックします。

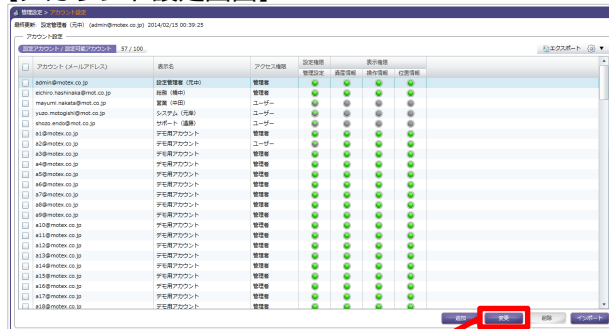
【管理設定画面】



3

リモート操作の実行権限を付与したいアカウントを選択状態にして、「変更」をクリックします。

【アカウント設定画面】



変更

設定権限の「リモートロック・リモートワイプ・紛失モードの実行権限を付与する」にチェックを入れ、「OK」をクリックします。

◆注意◆

「リモートロック・ワイプ、パスコードオフ、紛失モード」の実行は、表示権限が与えられている対象端末に対して実行可能です。また、「紛失モード」の対象端末はiOS端末のみです。

? 新規にアカウントを作成する場合はどうするの？

1

画面上部にあるメニューから「管理設定」をクリックし「アカウント設定」をクリックして、「追加」をクリックします。

2

アカウント（メールアドレス）・表示名・パスワード・パスワードの確認入力を入力し、アクセス権限を設定します。設定権限の「リモートロック・リモートワイプ・紛失モードの実行権限を付与する」と、リモート操作を実行したい端末の表示権限欄にチェックを入れ、「次へ」をクリックします。

3

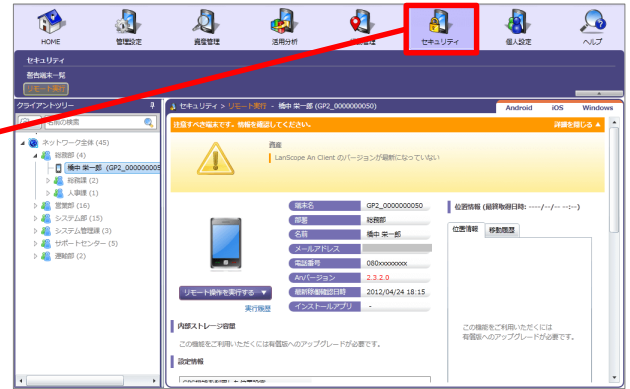
アカウントが追加された旨のメールを送信したい場合は、このあと通知内容の設定を実施します（メールを通知しない設定も可能です）。アカウントが作成され、該当のメールアドレスに通知されます。

日々のセキュリティ状況を定期的に確認することで、万が一何か問題やトラブルが発生した際にも、迅速に対処することができます。

1

画面上部にあるメニュー「セキュリティ」をクリックします。

【セキュリティ画面】



2

「警告端末一覧」をクリックします。

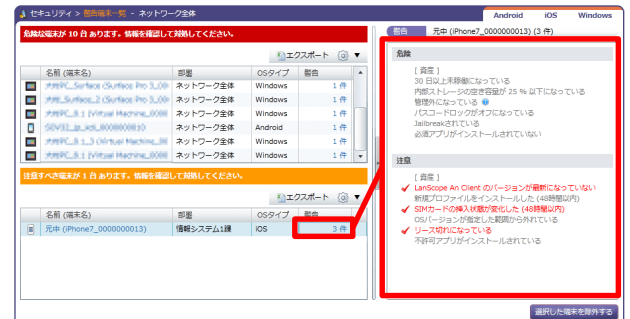
【セキュリティ画面】



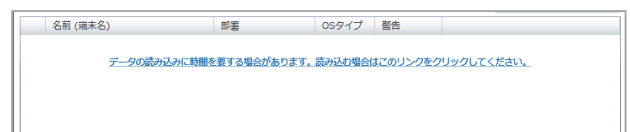
3

「危険な端末」と「注意すべき端末」が表示されます。警告の件数をクリックすると、警告の内容・詳細が表示されます。選択されている部署配下の端末数が500台を超える場合、図のようなリンクを表示します。クリックすると、選択されている部署で警告端末一覧を表示します。

【警告端末一覧画面】



【端末数が多い場合のリンク】





「危険」や「注意」は、誰が何を基準に決めているの？

どれを「危険」「注意」にするのか設定を変更できます。

◆デフォルト設定◆（警告設定）

区分	カテゴリ	警告判断基準	対象OS
危険	資産	設定期間以上未稼働になっている (※1)	Android,iOS,Windows
		内部ストレージの空き容量が 設定値以下になっている (※1)	Android,iOS,Windows
		未稼働だった必須アプリがある (48時間以内) (※5)	Android
		位置情報サービスが無効になっている	Android
		管理外になっている (※3)	iOS
		パスコードロックがオフになっている	iOS
		必須アプリがインストールされていない	iOS,Windows
		パスワードがポリシーに準拠していない	Android
		リモートワイプが無効になっている	Windows
		Root化されている	Android
		Jailbreakされている	iOS
危険	操作	リモート実行に必要な設定がされていない (※2)	Android
		不許可アプリが起動した (1週間以内)	Android
		SDカードを抜き差しした (1週間以内)	Android
注意	資産	不許可アプリがインストールされている	Android,iOS,Windows
		LanScope An Client のバージョンが最新になっていない	Android,iOS,Windows
		新規プロファイルをインストールした	iOS
		SIMカードの挿入状態が変化した (48時間以内)	Android,iOS
		OSバージョンが指定した範囲から外れている	Android,iOS
		設定日数以内でリース切れになる (※1) (※4)	Android,iOS,Windows
注意	操作	新しくアプリをインストールした (1週間以内)	Android
		不正Webサイトを閲覧した (1週間以内)	Android
		タイムゾーンを変更した (1週間以内)	Android

※1 未稼働日数の設定・空き容量の設定・リース期限切れ何日前にアラートとするかについてはアラート設定で行えます。

※2 リモートロック・ワイプの実行には、Android端末で以下の設定が必要です。

・LanScope An Client のアプリをデバイス管理者に登録

※3 An構成プロファイルが取り除かれた端末を「管理外」として認識します。

※4 リース期限日の設定は「資産情報一覧」の「リース期限」項目で行えます。

※5 Android 7.0未満の端末で利用できます。

●2016/3/23以前からLanScope Anを利用している場合は、次の項目が表示されます

青太字部分は、Anクライアントの移行（*）が完了していれば利用しない項目です。移行完了前の端末でのみ利用します。

* 注釈：2016/3/23以前からLanScope AnでWindows端末を管理している場合、Anクライアントの移行が必要です。
別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照して移行を完了させてください。
（Android・iOSの場合、この作業は不要です）

◆デフォルト設定◆（警告設定）

区分	カテゴリ	警告判断基準	対象OS
危険	資産	設定期間以上未稼働になっている（※1）	Android,iOS,Windows
		内部ストレージの空容量が 設定値以下になっている（※1）	Android,iOS,Windows
		未稼働だった必須アプリがある（48時間以内）（※7）	Android
		位置情報サービスが無効になっている	Android,Windows
		管理外になっている（※3）	iOS,Windows
		パスコードロックがオフになっている	iOS
		必須アプリがインストールされていない	iOS,Windows
		パスワードがポリシーに準拠していない	Android
		Anクライアント（Windowsストア）が稼働していない（※4）	Windows
		Anクライアント（デスクトップ）が稼働していない（※5）	Windows
		リモートワイプが無効になっている	Windows
		Root化されている	Android
		Jailbreakされている	iOS
危険	操作	リモート実行に必要な設定がされていない（※2）	Android
		不許可アプリが起動した（1週間以内）	Android
		SDカードを抜き差しした（1週間以内）	Android
注意	資産	不許可アプリがインストールされている	Android,iOS,Windows
		LanScope An Client のバージョンが最新になっていない	Android,iOS,Windows
		新規プロファイルインストールした	iOS
		SIMカードの挿入状態が変化した（48時間以内）	Android,iOS
		OSバージョンが指定した範囲から外れている	Android,iOS
		設定日数以内にリース切れになる（※1）（※6）	Android,iOS,Windows
注意	操作	新しくアプリをインストールした（1週間以内）	Android
		不正Webサイトを閲覧した（1週間以内）	Android
		タイムゾーンを変更した（1週間以内）	Android

※1 未稼働日数の設定・空き容量の設定・リース期限切れ何日前にアラートとするかについてはアラート設定で行えます。

※2 リモートロック・ワイプの実行には、Android端末で以下の設定が必要です。

・LanScope An Client のアプリをデバイス管理者に登録

※3 以下の条件に該当する端末を管理外として認識します。

・iOS：LanScope An のモバイルデバイス管理ペイロードを含む構成プロファイルが取り除かれた

・Windows：端末上でMDM登録をオフにした

ただし、Anクライアント（Windowsストア）又はAnクライアント（デスクトップ）がインストールされている場合のみ

※4 警告端末を検出するにはAnクライアント（Windowsストア）未稼働のアラート設定をオンにしてください。

※5 警告端末を検出するにはAnクライアント（デスクトップ）未稼働のアラート設定をオンにしてください。

※6 リース期限日の設定は「資産情報一覧」の「リース期限」項目で行えます。

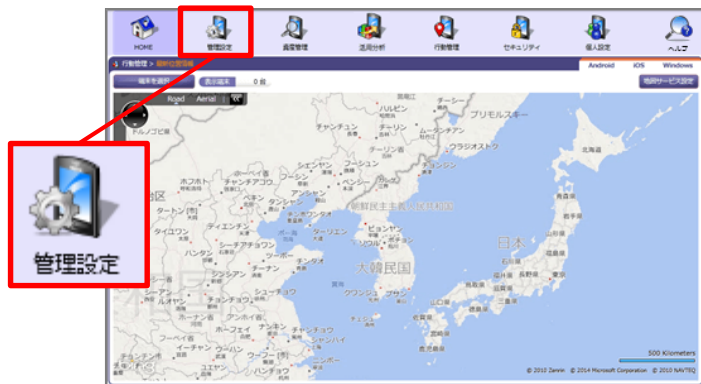
※7 Android 7.0未満の端末で利用できます。

1.「警告設定」を行える権限を設定する

1

画面上部にあるメニュー「管理設定」をクリックします。

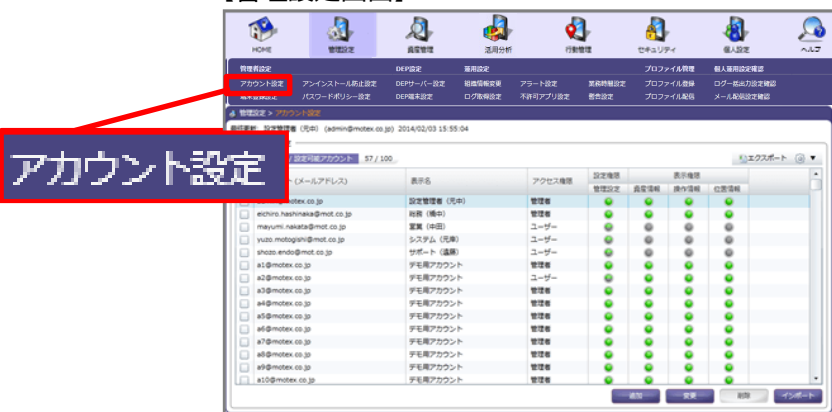
【TOP画面】



2

「アカウント設定」をクリックします。

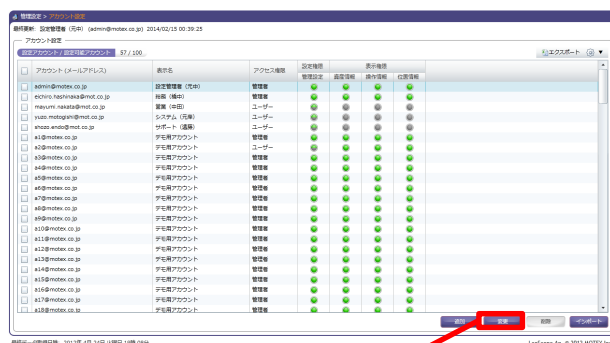
【管理設定画面】



3

警告内容の設定権限を付与したいアカウントを選択状態にして、「変更」をクリックします。

【アカウント設定画面】



4

設定権限の中にある「警告設定を変更する権限を付与する」にチェックを入れ「OK」をクリックします。

【アカウント設定の変更画面】

アカウント設定の変更

アカウント (メールアドレス): its@test.co.jp

表示名: ITS (マニュアル環境)

パスワード:

パスワードの確認入力:

アクセス権限: 管理者権限

設定権限 表示権限

すべてチェック すべてはずす

- ☒ ログ取得設定を変更する権限を付与する
- ☒ アラート設定を変更する権限を付与する
- ☒ 業務時間設定を変更する権限を付与する
- ☒ 不許可アプリ設定を変更する権限を付与する
- ☒ 位置情報を変更する権限を付与する
- ☒ 資産情報を変更する権限を付与する
- ☒ **警告設定を変更する権限を付与する**
- ☒ リモートロック・リモートワイプ・紛失モードの実行権限を付与する
- ☒ プロファイルを登録・配信する権限を付与する
- ☒ 警告レポートメールの配信設定で他のアカウントを宛先に指定する権限を付与する
- ☒ iOSアプリを登録・配信する権限を付与する

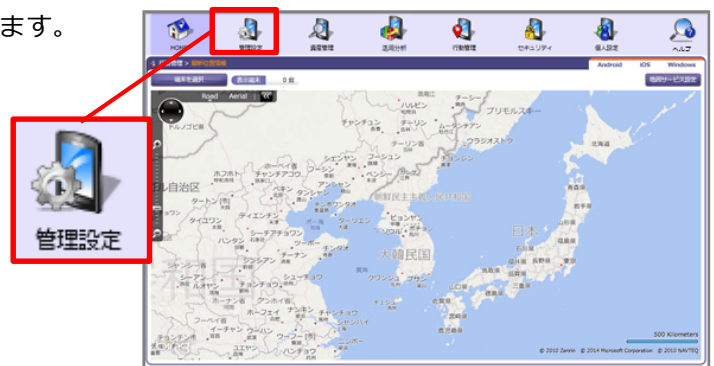
OK キャンセル

2. 「危険」と「注意」の基準を設定する

1

画面上部にあるメニュー「管理設定」をクリックします。

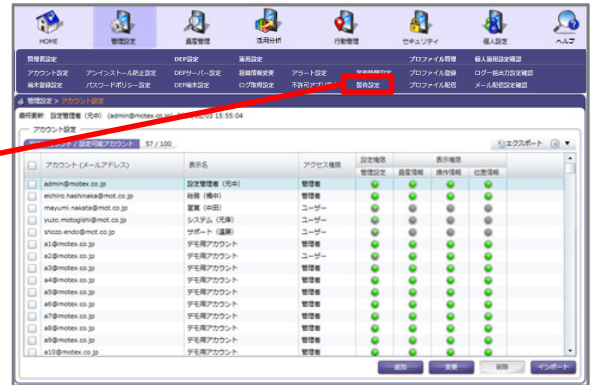
【TOP画面】



2

「警告設定」をクリックします。

【管理設定画面】

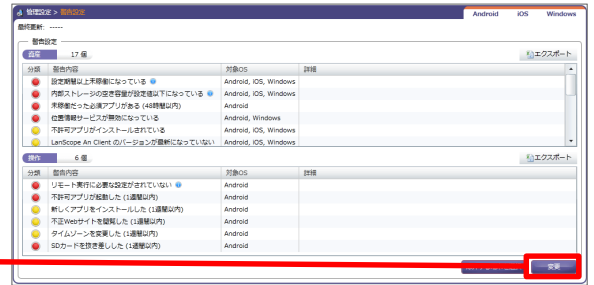


警告設定

3

「変更」をクリックします。

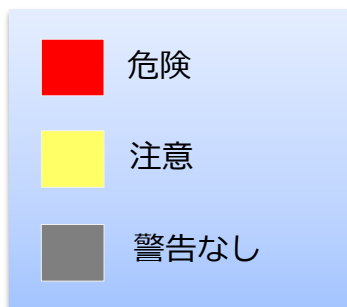
【警告設定画面】



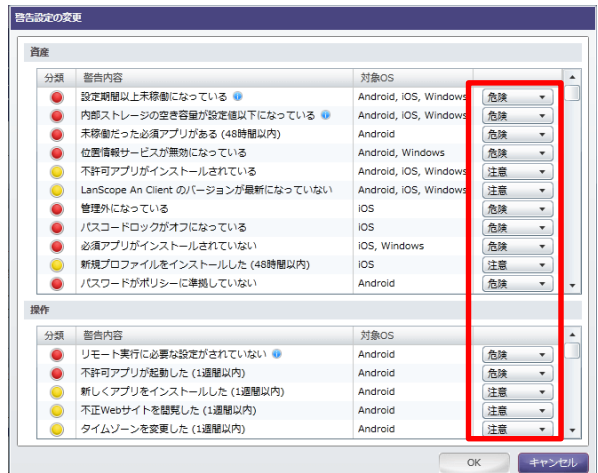
変更

4

警告内容の一覧が表示されるので、それぞれ「危険」「注意」「警告なし」に設定します。



【警告設定の変更画面】



◆注意◆

- ①「警告なし」に設定した警告内容は、「警告端末一覧画面」には表示されません。
- ②「危険」に設定した項目に1つでも該当すると「危険な端末」に分類されます。
- ③以下の内容を警告設定で「危険」「注意」に設定した場合は、「アラート設定」の内容と連動して設定されます。

	警告内容	アラート設定	OS (※)
資産	設定期間以上未稼働になっている	端末が一定の期間以上稼働しなかったらアラートとする	A,i,W
	内部ストレージの空き容量が設定値以下になっている	空き容量が少なくなったらアラートとする	A,i,W
	未稼働だった必須アプリがある（48時間以内）	必須アプリが稼働していなかったらアラートとする	A
	位置情報サービスが無効になっている	位置情報サービスが無効だったらアラートとする	A,W
	管理外になっている	端末が管理外となっていたらアラートとする	i
	パスコードロックがオフになっている	パスコードロックがオフになっていたらアラートとする	i
	不許可アプリがインストールされている	不許可アプリがインストールされていたらアラートとする	A,i,W
	必須アプリがインストールされていない	必須アプリがインストールされていなかったらアラートとする	i,W
	新規プロファイルをインストールした（48時間以内）	新規プロファイルをインストールしたらアラートとする	i
	パスワードがポリシーに準拠していない	パスワードがポリシーに準拠していなかったらアラートとする	A
	リモートワイプが無効になっている	リモートワイプの実行条件を満たしていなかったらアラートとする	W
	Root化されている	Root化されていたらアラートとする	A
	Jailbreakされている	Jailbreakされていたらアラートとする	i
	SIMカードの挿入状態が変化した（48時間以内）	SIMカードの挿入状態が変化したらアラートとする	A,i
	OSバージョンが指定した範囲から外れている	OSバージョンが指定の値以外の時にアラートとする	A,i
	設定日数以内にリース切れになる	リース有効期限が近づいたらアラートとする	A,i,W
操作	不許可アプリが起動した（1週間以内）	不許可アプリが起動したらアラートとする	A
	不正Webサイトを閲覧した（1週間以内）	不正なWebサイトを閲覧したらアラートとする	A
	新しくアプリをインストールした（1週間以内）	新しくアプリをインストールしたらアラートとする	A
	タイムゾーンを変更した（1週間以内）	タイムゾーン設定を変更したらアラートとする	A
	SDカードを抜き差しした（1週間以内）	SDカードを抜き差ししたらアラートとする	A

※ 対応OSの表記 : A…Android / i…iOS / W…Windows

※ 未稼働日数、内部ストレージの空き容量、リース期限切れ何日前にアラートとするかについては「アラート設定」で設定可能です。

●2016/3/23以前からLanScope Anを利用している場合は、次の項目が表示されます

青太字部分は、Anクライアントの移行（*）が完了していれば利用しない項目です。移行完了前の端末でのみ利用します。

* 注釈：2016/3/23以前からLanScope AnでWindows端末を管理している場合、Anクライアントが必要です。
別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照して移行を完了させてください。
（Android・iOSの場合、この作業は不要です）

	警告内容	アラート設定	OS (※)
資産	設定期間以上未稼働になっている	端末が一定の期間以上稼働しなかったらアラートとする	A,i,W
	内部ストレージの空き容量が設定値以下になっている	空き容量が少なくなったらアラートとする	A,i,W
	未稼働だった必須アプリがある（48時間以内）	必須アプリが稼働していなかったらアラートとする	A
	位置情報サービスが無効になっている	位置情報サービスが無効だったらアラートとする	A,W
	管理外になっている	端末が管理外となっていたらアラートとする	i,W
	パスコードロックがオフになっている	パスコードロックがオフになっていたらアラートとする	I
	不許可アプリがインストールされている	不許可アプリがインストールされていたらアラートとする	A,i,W
	必須アプリがインストールされていない	必須アプリがインストールされていなかったらアラートとする	i,W
	新規プロファイルをインストールした（48時間以内）	新規プロファイルをインストールしたらアラートとする	I
	パスワードがポリシーに準拠していない	パスワードがポリシーに準拠していなかったらアラートとする	A
	Anクライアント（Windowsストア）が稼働していない	Anクライアント（Windowsストア）が稼働していなかったらアラートとする	W
	Anクライアント（デスクトップ）が稼働していない	Anクライアント（デスクトップ）が稼働していなかったらアラートとする	W
	リモートワイプが無効になっている	リモートワイプの実行条件を満たしていなかったらアラートとする	W
	Root化されている	Root化されていたらアラートとする	A
	Jailbreakされている	Jailbreakされていたらアラートとする	i
	SIMカードの挿入状態が変化した（48時間以内）	SIMカードの挿入状態が変化したらアラートとする	A,i
	OSバージョンが指定した範囲から外れている	OSバージョンが指定の値以外の時にアラートとする	A,i
	設定日数以内にリース切れになる	リース有効期限が近づいたらアラートとする	A,i,W
操作	不許可アプリが起動した（1週間以内）	不許可アプリが起動したらアラートとする	A
	不正Webサイトを閲覧した（1週間以内）	不正なWebサイトを閲覧したらアラートとする	A
	新しくアプリをインストールした（1週間以内）	新しくアプリをインストールしたらアラートとする	A
	タイムゾーンを変更した（1週間以内）	タイムゾーン設定を変更したらアラートとする	A
	SDカードを抜き差しした（1週間以内）	SDカードを抜き差ししたらアラートとする	A

※ 対応OSの表記：A…Android / i…iOS / W…Windows

※ 未稼働日数、内部ストレージの空き容量、リース期限切れ何日前にアラートとするかについては「アラート設定」で設定可能です。



「修理中の端末や利用を一時的に停止している端末」を警告対象から除外したい時

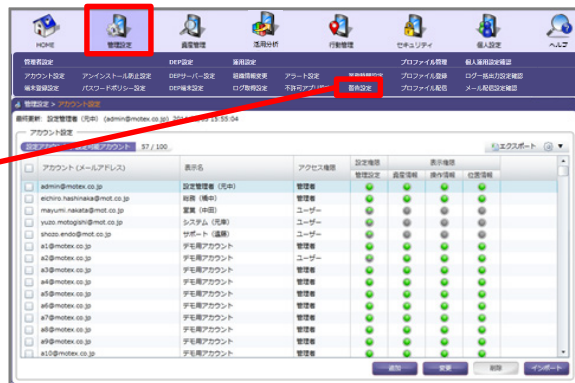
除外設定方法 その1

～設定時に除外したい時～

1

画面上部にあるメニュー「管理設定」をクリックし、「警告設定」をクリックします。

【TOP画面】

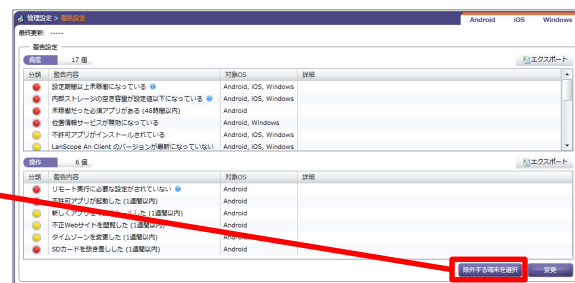


警告設定

2

「除外する端末を選択」をクリックします。

【警告設定画面】

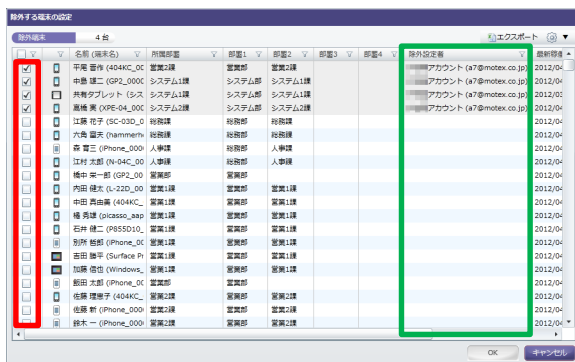


除外する端末を選択

3

警告対象から除外する端末にチェックを入れ、「OK」をクリックします。

【除外する端末の設定画面】



◆ポイント

除外設定をした「表示名（メールアドレス）」が除外設定者列に表示されます。

除外設定方法 その2

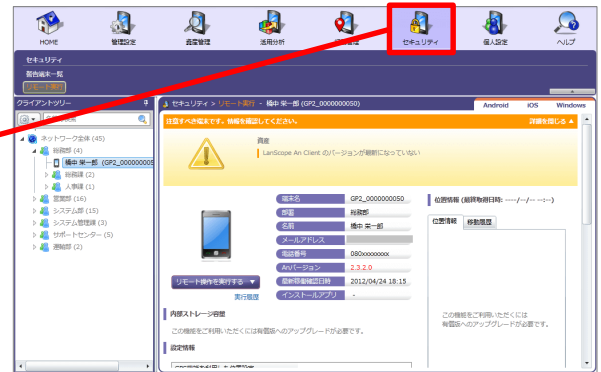
～日々の運用の中で除外したい時～

1

画面上部にあるメニュー「セキュリティ」をクリックします。



【TOP画面】



2

「警告端末一覧」をクリックします。

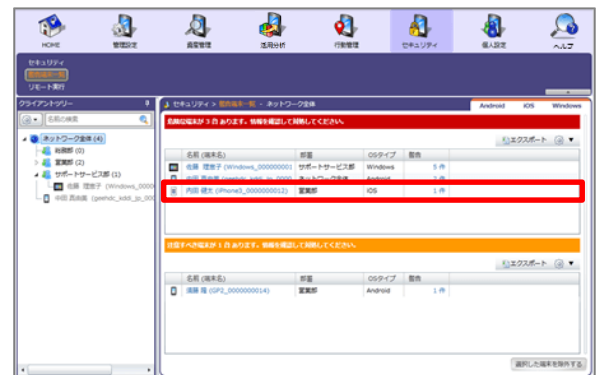
【セキュリティ画面】



3

除外したい端末行を選択します。

【警告端末一覧画面】



◆注意◆

- 端末行を選択する際は、「名前（端末名）」列以外の、「部署」「OSタイプ」「警告」を選択します。
- 部署を選択した場合、選択されている部署配下の端末数が500台を超えたときに図のようなリンクを表示します。クリックすると、選択されている部署で警告端末一覧を表示します。

【端末数が多い場合のリンク】



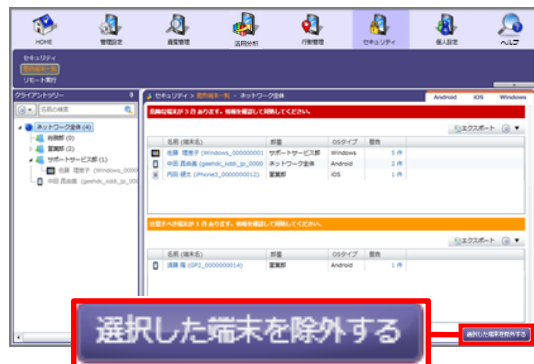
4

「選択した端末を除外する」をクリックします。

◆注意◆

一度に複数の端末を除外設定することが可能です。
ただし、「危険一覧」にある端末と「注意一覧」にある端末を同時に選択および除外することはできません。

【警告端末一覧画面】

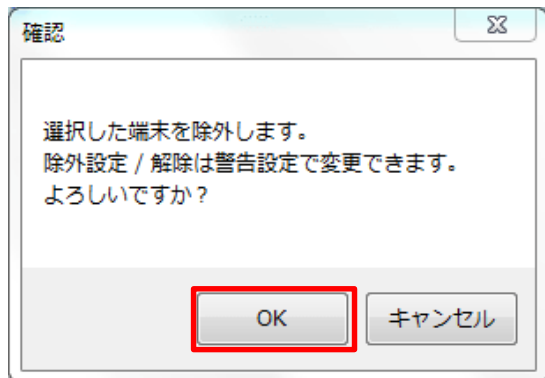


選択した端末を除外する

5

確認画面が表示されるので、問題がなければ「OK」をクリックします。

【確認画面】



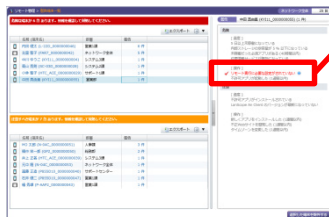


「リモート実行に必要な設定がされていない」という警告がある場合、どうするの？

※Android端末の場合のみ

「リモート実行に必要な設定がされていない」という警告がある場合、リモートロックやワイプを実行することはできません。つまり、端末を紛失・盗難した際に迅速に対応することができません。日頃から各端末のセキュリティ状況を確認するようにしましょう。

【警告端末一覧画面】



✓ リモート実行に必要な設定がされていない

チェックポイント

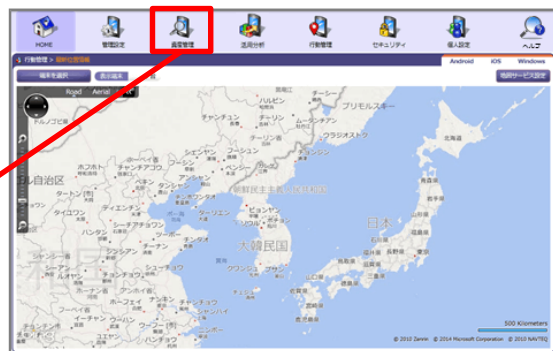
- ① 「デバイス管理者」にLanScope An Clientが登録されている
- ② 「Google Play ストア」がインストールされている
- ③ Google アカウントが端末に設定されている
(Android OS 4.0.4未満の場合)

1. 「デバイス管理者」にLanScope An Clientが登録されているか確認する

1

画面上部にあるメニュー「資産管理」をクリックします。

【TOP画面】

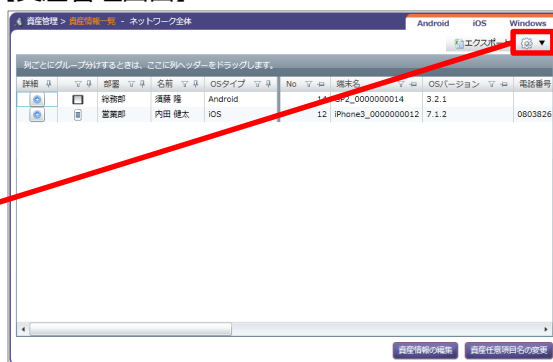


資産管理

2

画面右上の  をクリックします。

【資産管理画面】



3

「表示項目の設定」をクリックします。

【資産管理画面】



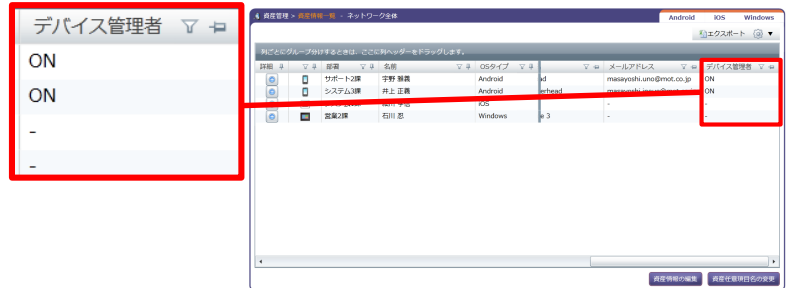
4

「デバイス管理者 (Android)」にチェックを入れます。



5

再度、「資産情報一覧」画面を確認します。「デバイス管理者」列が追加され、「デバイス管理者」が有効な端末にのみ「ON」と表示されています。



6

端末にインストールされているLanScope An Clientの「デバイス管理者」が無効だった場合、有効に設定してください。

◆注意◆

デバイス管理者の設定が無効のままの場合、右の手順1の画面が表示され続けます。

- ※「使用履歴へのアクセス」は、Android 5.0以上の場合のみ表示されます。
- ※「アクセス設定」、「電池の最適化 例外設定」は、Android 6.0以上の場合のみ表示されます。
- ※「ユーザー補助」は、Android 5.0以上の場合のみ表示され、管理コンソールの設定が必要です。詳細は『ユーザーズガイド for Android』を参照してください。



「デバイス管理者」をタップします。



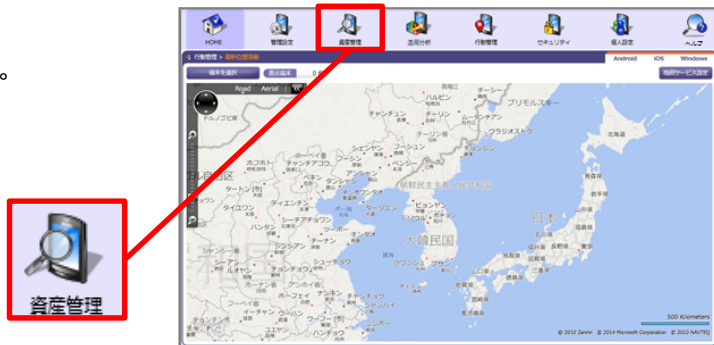
「有効にする」をタップします。

2. 「Google Play ストア」 がインストールされているか確認する

1

画面上部メニューの「資産管理」をクリックします。

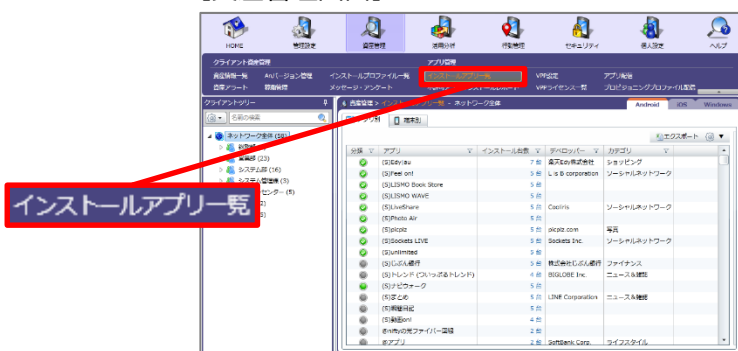
【TOP画面】



2

「インストールアプリ一覧」をクリックします。

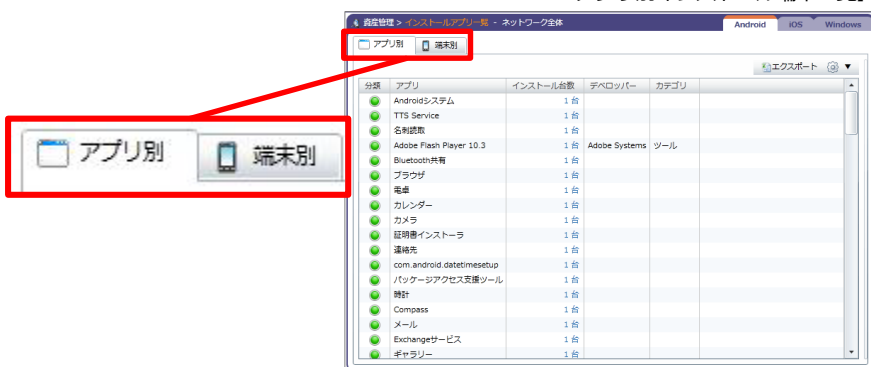
【資産管理画面】



3

「アプリ別」が選択されていることを確認します。

【インストールアプリ一覧画面・アプリ別インストール端末一覧】



「Google Play ストア」のインストール台数をクリックします。



【インストールアプリ一覧画面・
アプリ別インストール端末一覧】

アプリ別	インストール台数	デベロッパー	カテゴリ
ダウンロード	1 台		
DRM保護されたコンテンツの保存	1 台		
メディアストレージ	1 台		
ストレージの設定	1 台		
モバイルネットワークの設定	1 台		
User Dictionary	1 台		
設定	1 台		
セットアップウィザード	1 台		
音声レコーダー	1 台		
システムUI	1 台		
Google Playストア	1 台		
マーケット更新ツール	1 台		
Androidライブ壁紙	1 台		
com.android.wallpaper.holospiral	1 台		
Live Wallpaper Picker	1 台		
Documents To Go	1 台	Dataviz, Inc.	ビジネス
Evernote	1 台	Evernote Corp.	仕事効率化

「Google Play ストア」がインストールされているか端末が一覧で表示されます。

【インストールアプリ一覧画面・
アプリ別インストール端末一覧】

アプリ別	インストール台数	デベロッパー	カテゴリ
ダウンロード	1 台		
DRM保護されたコンテンツの保存	1 台		
メディアストレージ	1 台		
ストレージの設定	1 台		
モバイルネットワークの設定	1 台		
User Dictionary	1 台		
設定	1 台		
セットアップウィザード	1 台		
音声レコーダー	1 台		
システムUI	1 台		
Google Playストア	1 台		
マーケット更新ツール	1 台		
Androidライブ壁紙	1 台		
com.android.wallpaper.holospiral	1 台		
Live Wallpaper Picker	1 台		
Documents To Go	1 台		

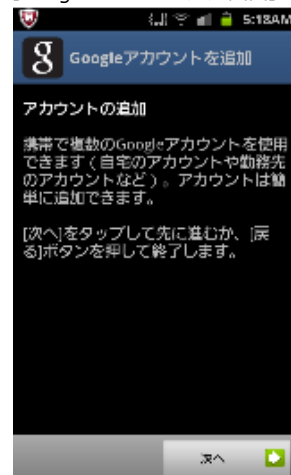
3. Google アカウントが端末に設定されているか確認する

Android 4.0.4未満の端末をお使いの場合は、Google アカウントの設定が必須です。

Googleアカウントが設定されているか確認してください。
設定されていない場合は、端末で設定を行ってください。

※機種により画面が異なる場合があります。

【Googleアカウント追加画面】





「管理外端末のためリモート操作が実行できません」という警告がある場合どうするの？

■iOS端末の場合

「An構成プロファイル」が端末にインストールされていません。別紙『スタートアップガイド for iOS』を参照して正しく構成プロファイルがインストールされていることを確認してください。

●2016/3/23以前からWindows端末を管理している場合はご確認ください

2016/3/23以前からLanScope AnでWindows端末を管理している場合で、Anクライアントの移行を行っていない端末（*）の場合、次の対処方法があります。

* 注釈：2016/3/23以前からLanScope AnでWindows端末を管理している場合、Anクライアントの移行が必要です。別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照して移行を完了させてください。（Android・iOSの場合、この作業は不要です）。

■Windows端末の場合

端末上でMDMの登録（デバイス管理）がオフになっています。別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照してAnクライアントを移行してください。



「リモートワイプ有効」が「無効」と表示されている場合、どうするの？

※Windowsのみ

※リモートワイプ機能はOS・エディションにより機能差があります。詳細は「補足事項」（p.6）を参照してください。

Windows端末に「リモートワイプ」を実行するには、端末上で「BitLocker」を設定しておく必要があります。「BitLocker」を設定した上で「リモートワイプ」を実行すると、復旧手順を踏まなければデータを確認することができないようになります。

設定箇所の詳細について、以下のようにメッセージが表示されます。

- ・BitLocker を使用してシステムドライブが暗号化されていない
- ・BitLocker 暗号化に TPM が利用されていない
- ・BitLocker 暗号化に回復キーが利用されていない

下記の手順に沿って、Windows端末で「BitLocker」を設定してください。

1

【コントロールパネル】 - 【BitLockerドライブ 暗号化】を開きます。

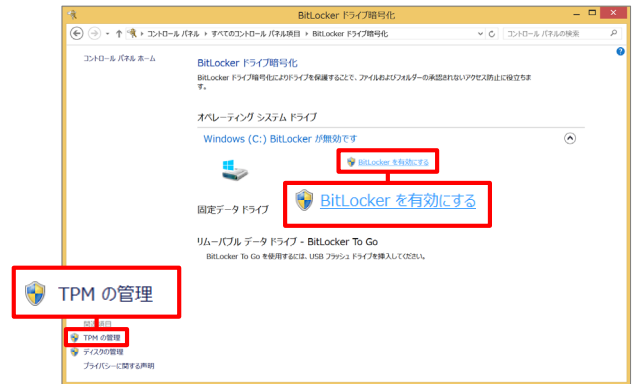


2

左下に「TPM の管理」が表示されていることを確認し、BitLocker を有効化にします。

◆注意

「TPM の管理」が表示されていない場合、その Windows 端末は TPM 非搭載機種であるため、リモートワイプは実行できません。

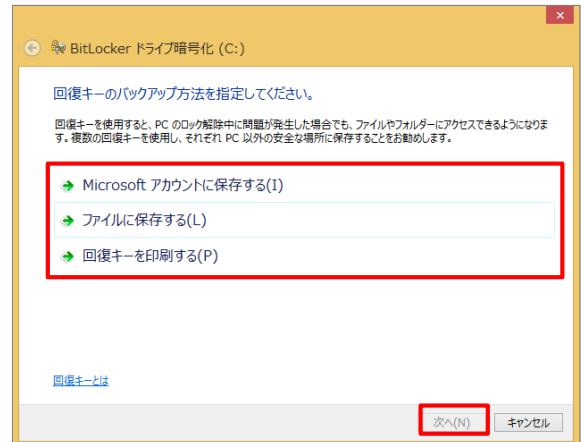


3

端末へのワイプを実行した後、端末を復旧させたい場合に必要になる回復キーのバックアップ方法を設定します。

保存形式は特に問いません。

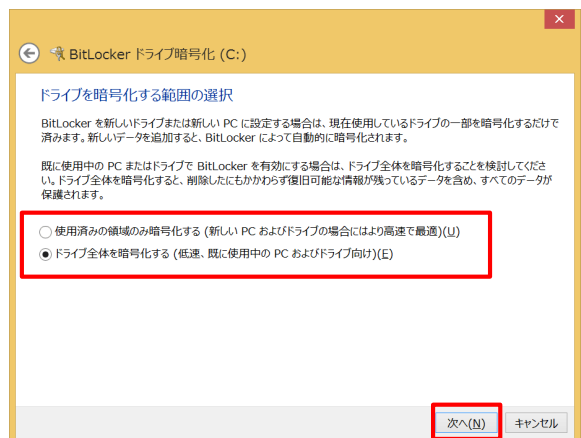
バックアップが完了したら「次へ」をタップします。



4

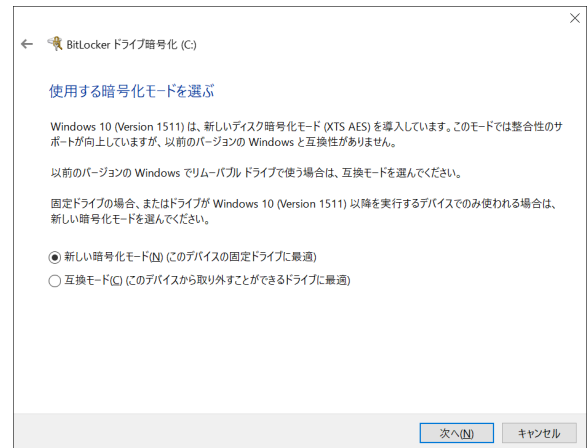
ドライブを暗号化する範囲を設定します。暗号化の範囲は特に問いませんが、「ドライブ全体を暗号化する」を選択することで安全性が高まります（ただし、暗号化に時間がかかることがあります）。

設定したら「次へ」をタップします。



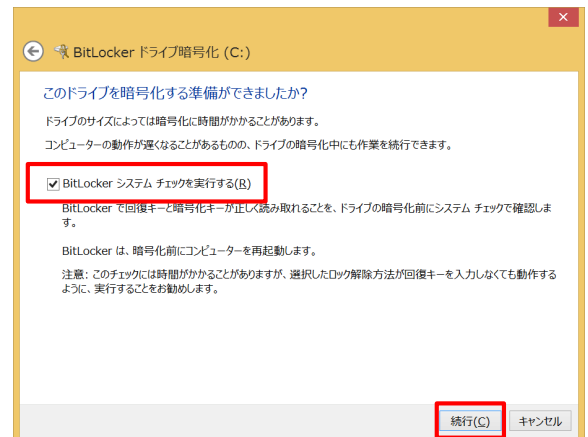
5

「使用する暗号化モードを選ぶ」画面が表示された場合は、任意の暗号化モードを選択して「次へ」をタップします。



6

BitLockerのシステムチェックを実行するかどうかを選択します。選択の有無は問いませんが、「BitLocker システム チェックを実行する」にチェックを入れたほうが安全性が高まります（ただし、端末再起動の実施が必要です）。



7

暗号化が行われます。完了のダイアログが表示されたら「閉じる」をタップします。



選択したドライブに「BitLockerが有効です」と表示されたことを確認します。



3 第三者に操作されないように、端末にロックをかける

端末に遠隔でパスワードロックを実行し、ロック状態にできます。

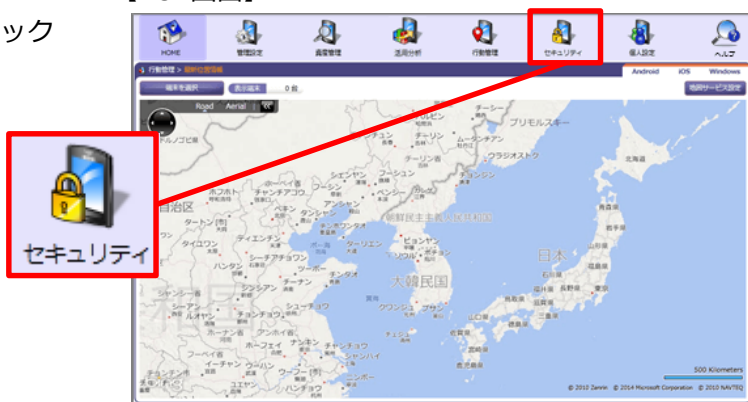
◆注意◆

- ・iOS端末・Windows端末の場合、端末にパスワード（パスコード）設定がされていなければ、リモートロックを実行しても、画面はパスワード入力必要無しのロック画面になります。あらかじめパスワード設定を行ってください。
- ・**Android 3.xのOSで、かつ今までに英数字のパスワードを一度も設定したことがない場合、リモートロックに失敗します。初期状態でも4文字のパスワードが設定されていますが、その後、手動で設定されている必要があります。**
- ・Android 3.0以降かつ「パスワードポリシー設定」（別紙「ユーザーズガイド for Android」参照）の「スリープ開始までの最大許容時間」が設定されている端末にリモートロックを実行すると、一時的に「スリープ開始までの最大許容時間」の設定が外れます。それ以外の「パスワードポリシー設定」が外れることはありません。なお、端末起動から12時間ごとのタイミング、もしくは、端末を再起動したタイミングで「スリープ開始までの最大許容時間」の設定が再度適用されます。
- ・すでにパスワードが設定されているAndroid 7.0以降の端末の場合、リモートロック実行時に入力したパスワードは設定されません。

1

画面上部にあるメニュー「セキュリティ」をクリックします。

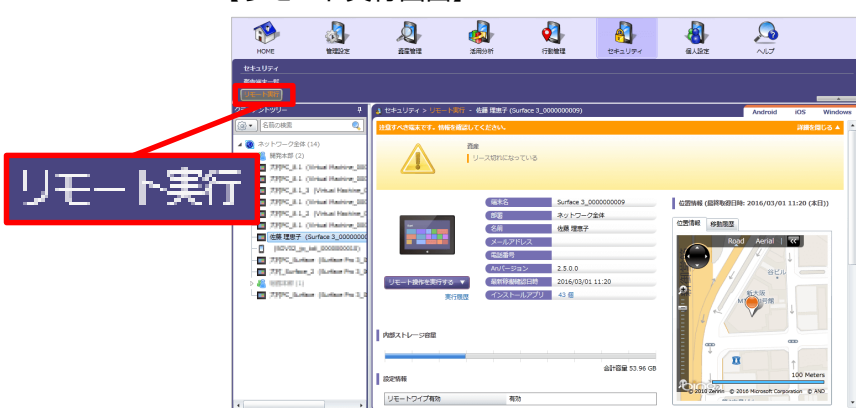
【TOP画面】



2

「リモート実行」をクリックします。

【リモート実行画面】

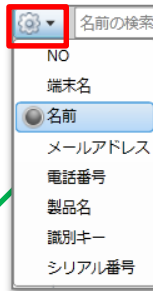


3

左のツリーからロックを実行する端末を選択してクリックします。

★ポイント★

電話番号やメールアドレスから実行端末を検索することができます。



【リモート実行画面】



4

「リモート操作を実行する」をクリックします。

リモート操作を実行する ▼

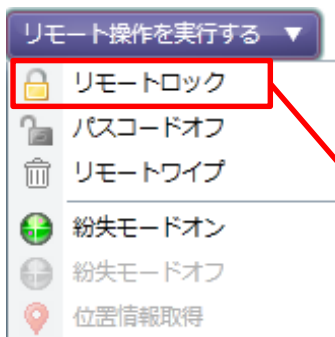
【リモート実行画面】



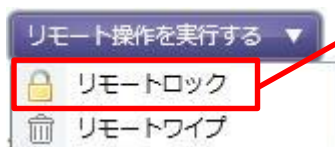
5

「リモートロック」をクリックします。

iOSの場合



Android/
Windowsの場合



【リモート実行画面】



6

Androidの場合

パスワードと確認用パスワードを入力し、実行をクリックします。

iOS/Windowsの場合

そのまま実行をクリックします。

※端末が紛失モードオンの場合、または紛失モードオン実行中の場合はリモートロックを行うことができません。

◆注意◆

Android 7.0以降の端末にパスワードが設定されている場合、ロック解除パスワードが設定できません。

※Androidの場合

※iOS/Windowsの場合

7

「実行履歴」をクリックします。

実行履歴

【リモート実行画面】

8

「実行履歴」画面が表示されます。

「更新」ボタンをクリックすると、実行履歴が再読み込みされ、最新の情報に更新されます。

◆注意◆

端末の電源がOFFになっている場合や、通信ができない状態の場合、端末が通信可能な状態になるまで「実行中」や「待機中」（実行中から30秒経過後）になります。

※状態が「実行中」や「待機中」の場合、90日間は処理を「キャンセル」できます。

【実行履歴】

実行結果

リモートロックの実行に成功した場合、次のような画面が表示されます。

※機種により画像は異なる場合があります。

【端末側の画面】



●2016/3/23以前からWindows端末を管理している場合は必ずご確認ください

2016/3/23以前からLanScope AnでWindows端末を管理している場合で、Anクライアントの移行を行っていない端末(*)の場合、次の注意事項があります。

* 注釈：2016/3/23以前からLanScope AnでWindows端末を管理している場合、Anクライアントの移行が必要です。
別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照して移行を完了させてください。
（Android・iOSの場合、この作業は不要です）。

◆注意◆

Windows端末は定期的に外部ネットワークに接続し、LanScope Anの管理サーバーと通信を行う必要があります。

LanScope AnではWindows端末との通信の際、Windowsプッシュ通知サービス（WNS）を利用しています。

このサービスの仕様上、端末が30日以上外部ネットワークに接続されず、LanScope Anの管理サーバーと通信を行わなかった場合、通信に必要な通知チャネルの有効期限が切れてしまい、端末にプッシュ通知が届かなくなるため、資産情報の取得、リモートロックができなくなります。

30日以上通信がとれなかった端末は、別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照してAnクライアントを移行してください。



リモート操作時の注意点

以下のいずれかに該当している場合、「リモート操作を実行する」ボタンはクリックできません。

OS	原因	対処方法
全OS	管理コンソールにログインしているアカウントに、リモートロック・ワイプの実行権限がない	現在ログインしているアカウントに実行権限を付与する（p.7）か、実行権限をもつユーザーでログインしなおしてください。
Android	端末のLanScope An Clientで「デバイス管理者」の設定が有効になっていない	端末側で「デバイス管理者」の設定を有効にしてください。（p.21）
	端末にGoogle Playストアがインストールされていない	2012年以降に発売の端末にはプリインストールされています。2012年以前に発売の端末で「AndroidMarket」がインストールされている場合は、端末をネットワークに接続すると自動的に「Google Play ストア」にアップデートされます。
	端末のLanScope An Clientのバージョンが1.1.0.0未満である	リモート操作を実行するには、LanScope An Clientのバージョンが1.1.0.0以上である必要があります。『バージョンアップガイド for Android』を参照してバージョンアップしてください。
	Googleアカウントが端末に設定されていない（Android4.0.4未満の場合のみ）	Android4.0.4未満の端末にリモート操作を実行するには、端末にGoogleアカウントが設定されている必要があります。端末にGoogleアカウントを設定してください。
iOS	An構成プロファイルが端末にインストールされていない	リモート操作を実行する場合、端末にAn構成プロファイルがインストールされている必要があります。『スタートアップガイド for iOS』を参照してインストールしてください。

●2016/3/23以前からWindows端末を管理している場合にご確認ください

2016/3/23以前からLanScope AnでWindows端末を管理している場合で、Anクライアントの移行を行っていない端末（*）の場合、次の条件下でもボタンがクリックできなくなります。

* 注釈：2016/3/23以前からLanScope AnでWindows端末を管理している場合、Anクライアントの移行が必要です。別紙『Anクライアント（デスクトップ）移行ガイド for Windows』を参照して移行を完了させてください。（Android・iOSの場合、この作業は不要です）

原因： 端末のMDM登録が解除されている

対処方法： 端末側で再度MDM登録を行う必要がありますが、2016/3/24以降はMDMの登録ができなくなるため、上記のとおり別紙を参照してAnクライアントを移行してください。

【リモート実行画面】



！ リモートロックを実行後、次のような結果が表示されます

Androidの場合は以下のとおりです。

メッセージ	対処方法
リモート操作の送信に成功しました。	リモート操作の送信に成功しています。「OK」をクリックし、実行結果を「実行履歴」画面から確認してください。(p.30)
リモート操作の送信に失敗しました。 LanScope Anクライアントのアプリがインストールされていない可能性があります。インストール状況を確認して再度実行してください。	リモート操作の対象となる端末にLanScope An Clientがインストールされているか確認してください。
予期しないエラーが発生しました。	時間をおいて再度実行いただき、それでも同じ結果になる場合は、サポートセンター (p.57) にお問い合わせください。
端末が通信できない状況の可能性があります。 時間をおいて再度実行してください。	サポートセンター (p.57) にお問い合わせください。

iOS/Windowsの場合は以下のとおりです。

メッセージ	対処方法
リモート操作の設定が完了しました。	リモート操作の設定が完了しています。「OK」をクリックし、実行結果を「実行履歴」画面から確認してください。(p.30)
リモート操作の設定に失敗しました。	「OK」をクリックするとリモートロックの実行画面に戻る ので、再度リモート操作を実行してください。 それでも同じ結果になる場合は、サポートセンター (p.57) にお問い合わせください。
すでに紛失モードオンが実行されています。 リモートロックを実行するには、[リモート 操作] - [実行履歴] からキャンセルし、再度 リモートロックを実行してください。	「OK」をクリックし、「実行履歴」画面から紛失モードを キャンセルしてから再度リモートロックを実行してください。 紛失モードについては、「7. 紛失した端末を探す (iOSのみ) 」 (p.45) を参照してください。

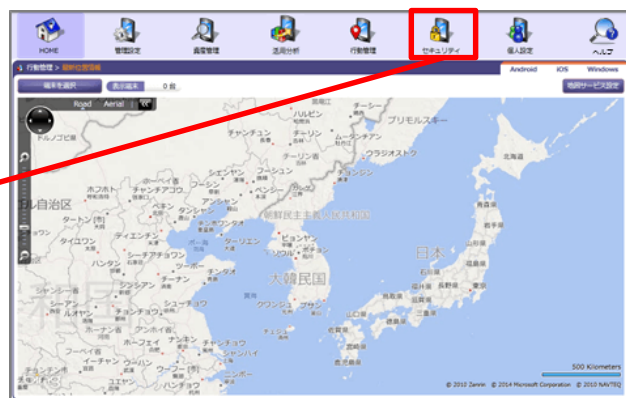
端末が紛失や盗難など危機的状況に陥った際、Android/iOS端末を工場出荷状態に戻すことができます。Windows端末の場合は、端末に保存されたデータにアクセスできなくなります（アクセスするには回復キーの入力などの手順が必要です）。

※リモートワイプ機能はOS・エディションにより機能差があります。詳細は「補足事項」（p.6）を参照してください。

1

画面上部にあるメニュー「セキュリティ」をクリックします。

【TOP画面】

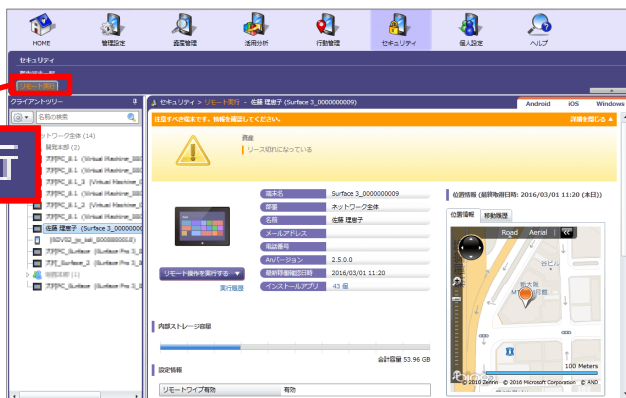


2

「リモート実行」をクリックします。

【リモート実行画面】

リモート実行



3

左のツリーからリモートワイプを実行したい端末をクリックします。

【リモート実行画面】



4

リモート実行画面から、「リモート操作を実行する」をクリックします。



【リモート実行画面】



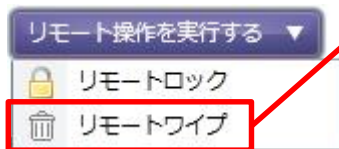
5

「リモートワイプ」をクリックします。

iOSの場合



Android/
Windowsの場合



【リモート実行画面】



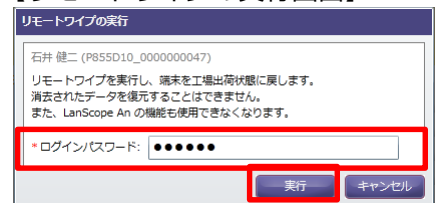
※Windows端末で、リモートワイプの実施に必要なAnクライアント（デスクトップ）がインストールされていない場合、リモートワイプは選択できません。

6

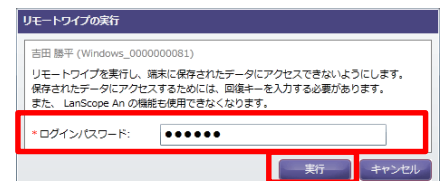
操作ミスを防ぐために、ワイプ実行前にLanScope Anの管理画面への「ログインパスワード」を入力してください。

【リモートワイプの実行画面】

Android/iOSの
場合



Windowsの場合



「実行履歴」をクリックします。

実行履歴

【リモート実行画面】



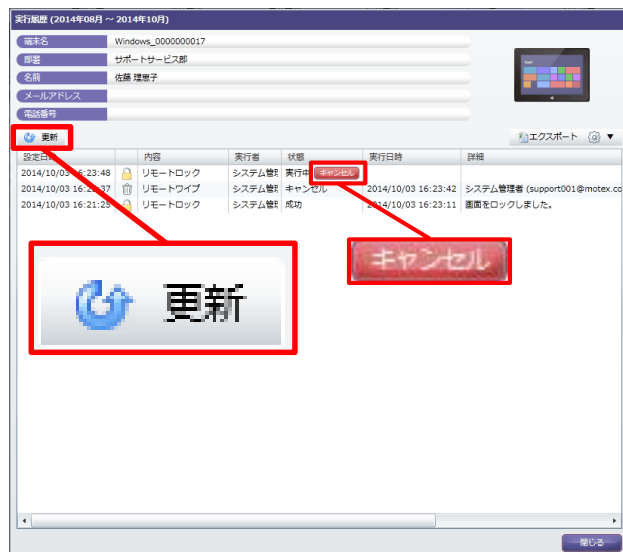
「実行履歴」画面が表示されます。
「更新」ボタンをクリックすると、実行履歴が再読み込みされ、最新の情報に更新されます。

◆注意◆

端末の電源がOFFになっている場合や、通信ができない状態の場合、端末が通信可能な状態になるまで「実行中」や「待機中」（実行中から30秒経過後）になります。

※状態が「実行中」や「待機中」の場合、90日間は処理を「キャンセル」できます。

【実行履歴】



実行結果

リモートワイプの実行に成功すると、Android/iOS 端末は工場出荷状態に戻ります。

Windows端末の場合は、端末に保存されたデータにアクセスできなくなります（アクセスするには回復キーの入力などの手順が必要です）。

！ リモートワイプを実行後、次のような結果が表示されます

Androidの場合は以下のとおりです。

メッセージ	対処方法
リモート操作の送信に成功しました。	リモート操作の送信に成功しています。「OK」をクリックし、実行結果を「実行履歴」画面から確認してください。（p.36）
リモート操作の送信に失敗しました。 LanScope Anクライアントのアプリがインストールされていない可能性があります。インストール状況を確認して再度実行してください。	リモート操作の対象となる端末にLanScope An Clientがインストールされているか確認してください。
予期しないエラーが発生しました。	時間を置いて再度実行いただき、それでも同じ結果になる場合は、サポートセンター（p.57）にお問い合わせください。

iOS/Windowsの場合は以下のとおりです。

メッセージ	対処方法
リモート操作の設定が完了しました。	リモート操作の設定が完了しています。「OK」をクリックし、実行結果を「実行履歴」画面から確認してください。（p.36）
リモート操作の設定に失敗しました。	「OK」をクリックするとリモートワイプの実行画面に戻りますので、再度リモート操作を実行してください。 それでも同じ結果になる場合は、サポートセンター（p.57）にお問い合わせください。

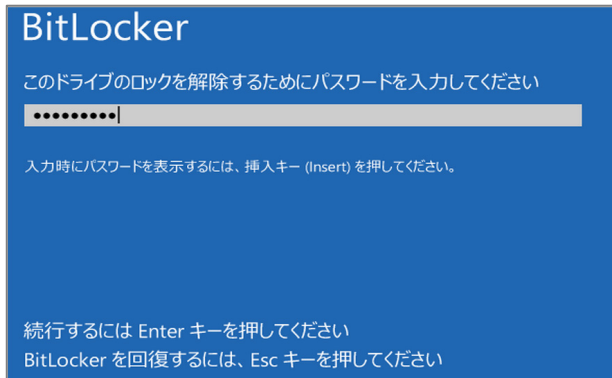
！ リモートワイプ実行後、復旧する場合の手順は次のとおりです

※Windows 8.1 Proの場合の手順です。

1

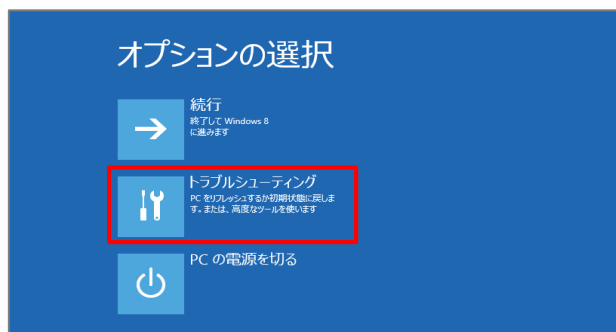
電源ボタンを押すと、右記画面が表示されるので、保存していたパスワード（回復キー）を入力し「Enter」キーを押します。

※次の「オプションの選択」画面が表示されず、ログインできる場合があります。
その場合、再起動後の右記画面で「Esc」キーを押してから、パスワード（回復キー）を入力します。



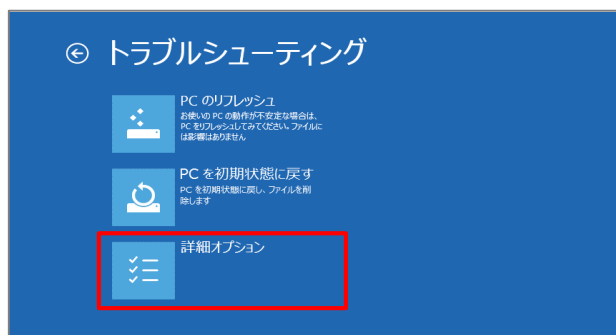
2

「オプションの選択」画面が起動するので、「トラブルシューティング」をタップします。



3

「詳細オプション」をタップします。



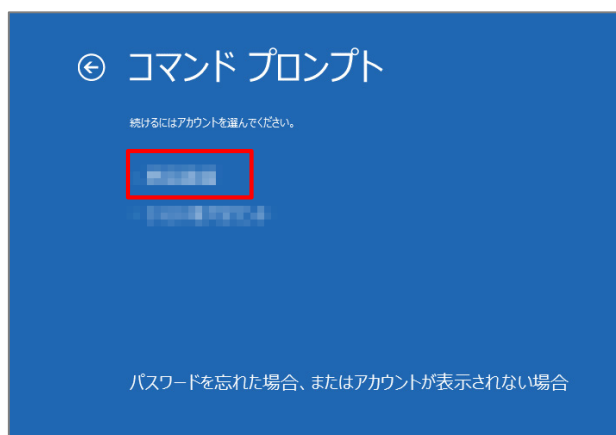
4

「コマンドプロンプト」をタップします。



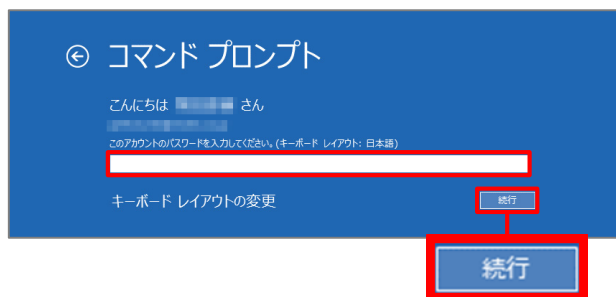
5

アカウント選択画面が起動するので、起動させるアカウントを選択します。



6

選択アカウントのログインパスワード入力画面が表示されるので、ログインパスワードを入力し「続行」をタップします。



7

コマンドプロンプトが起動するので、コマンドラインに「manage-bde.exe c: -off」と入力し「Enter」キーを押します。



8

回復処理が開始されるので、コマンドラインに「manage-bde.exe c: -status」と入力し「Enter」キーを押します。

```
暗号化の解除は現在実行中です。

C:\Windows\system32>manage-bde.exe c: -status
BitLocker ドライブ暗号化: 構成ツール Version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

ボリューム C: [ ]
[OS ボリューム]

サイズ: 59.66 GB
BitLocker のバージョン: 2.0
変換状態: 暗号化の解除を実行中です
暗号化された割合: 32.5%
暗号化の方法: AES 128
保護状態: 保護はオフです
ロック状態: ロック解除
識別子フィールド: 不明
キーの保護機能:
    パスワード
    数字パスワード
```

9

手順8 のコマンド実行時に表示される「暗号化された割合」を確認し、0%になるまで待機します（約10分程度かかります）。

```
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>manage-bde.exe c: -status
BitLocker ドライブ暗号化: 構成ツール Version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

ボリューム C: [ ]
[OS ボリューム]

サイズ: 59.66 GB
BitLocker のバージョン: なし
変換状態: 暗号化は完全に解除されています
暗号化された割合: 0.0%
暗号化の方法: なし
保護状態: 保護はオフです
ロック状態: ロック解除
識別子フィールド: なし
キーの保護機能: 見つかりません

C:\Windows\system32>exit
```

10

手順9 の項目が 0% になっていることを確認し、コマンドラインに「exit」と入力して「Enter」キーを押し、コマンドプロンプトを終了します。

11

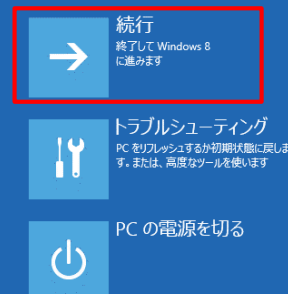
オプションの選択画面で「続行」をタップして完了です。

◆注意◆

本手順を実行することで「BitLocker暗号化」が解除されるため、「リモートワイプ有効」が「無効」と表示されます。

「BitLocker」を再設定する場合、p.24からの手順を参照してください。

オプションの選択



「実行履歴」画面に次の結果が表示された場合、それぞれ対処を行ってください。



表示されるメッセージと対処方法は以下のとおりです。

メッセージ	対処方法
LanScope An Clientのアプリがデバイス管理者に登録されていません。登録してから再度、実行してください。 ※Androidのみ	p.21を参照して、LanScope An Clientのアプリをデバイス管理者に登録してください。
リモート操作の実行に失敗しました。	<ul style="list-style-type: none"> Android 3.x以降4.x未満の端末 今までに英数字のパスワードを一度も設定したことがない場合、「リモートロック」の実行に失敗します。 上記以外の端末の場合 時間をおいて再度実行いただき、それでも同じ結果になる場合は、サポートセンター（p.57）にお問い合わせください。

【実行履歴】

実行履歴 (2014年08月 ~ 2014年10月)

端末名

Windows_0000000017

部署

サポートサービス部

名前



佐藤 理恵子

メールアドレス

電話番号

更新

エクスポート

設定日時	内容	実行者	状態	実行日時	詳細
2014/10/03 16:23:48	 リモートロック	システム管理	実行中		
2014/10/03 16:23:37	 リモートワイプ	システム管理	キャンセル	2014/10/03 16:23:42	システム管理者 (support001@motex.co.jp)
2014/10/03 16:21:25	 リモートロック	システム管理	成功	2014/10/03 16:23:11	画面をロックしました。

閉じる

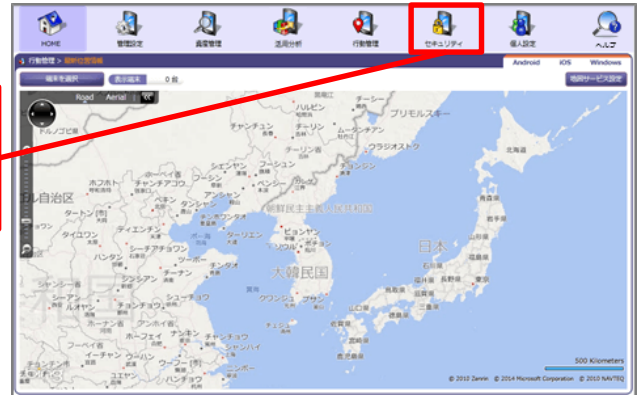
※iOSのみ

端末使用者がパスコードを忘れてしまった場合に、パスコードをオフにしてロックを解除します。

1

画面上部にあるメニュー「セキュリティ」をクリックします。

【TOP画面】

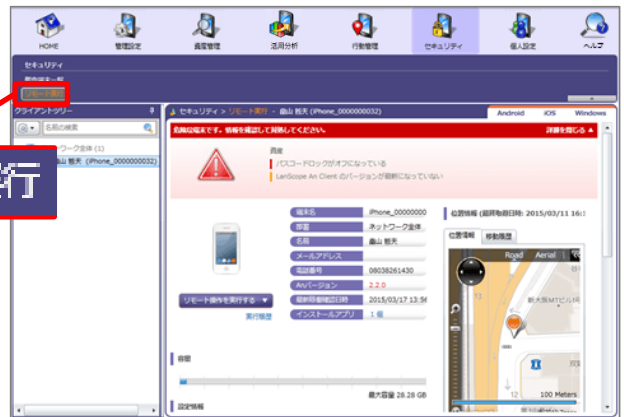


2

「リモート実行」をクリックします。

【リモート実行画面】

リモート実行



3

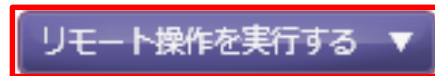
左のツリーからパスコードをオフにしたい端末を選択してクリックします。

【リモート実行画面】



4

リモート実行画面から、「リモート操作を実行する」をクリックします。



【リモート実行画面】



5

「パスコードオフ」をクリックします。



【リモート実行画面】

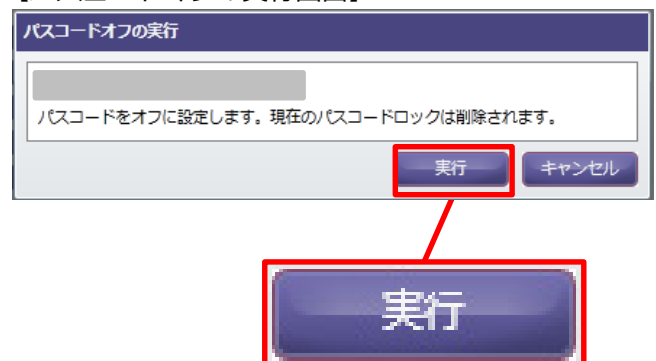


6


「実行」をクリックすると、パスコードロックをオフにする処理が実行されます。

なお、パスコードオフが実行されると、端末に現在設定されているパスコードロックの設定は削除されます。パスコードを再度有効化したい場合は、端末側で設定してください。

【パスコードオフの実行画面】



！ パスコードオフを実行後、次のような結果が表示されます

 表示されるメッセージと対処方法は以下のとおりです。

メッセージ	対処方法
リモート操作の設定が完了しました。	リモート操作の設定が完了しています。「OK」をクリックし、実行結果を「実行履歴」画面から確認してください。
リモート操作の設定に失敗しました。	「OK」をクリックするとリモート実行の画面に戻るので、再度リモート操作を実行してください。 それでも同じ結果になる場合は、サポートセンター（p.57）にお問い合わせください。



「紛失モード」とは？

「紛失モード」とは、iOS端末を紛失してしまった場合に、ロック解除不可能な状態に設定し、ロック画面上に任意のメッセージを表示することができる機能です。

LanScope Anでは、次の機能が利用できます。

- ・ 紛失モードをオンに設定する／オフに設定する
- ・ 紛失モード起動中の位置情報取得

また、紛失モードを使用できる端末は次のとおりです。

- ・ iOS端末で、OSバージョンが9.3以降であるもの
- ・ 「監視モード」がオンになっているもの



紛失モードをオンにした時の注意点

- 端末がオフラインの場合、オンラインになったタイミングで紛失モードがオンになります。
- 端末の紛失モードの状態がオンの場合、次の挙動になります。
 - ・ リモートロックが行えません。
 - ・ 紛失モードをオフにするまで端末のロック画面を解除できません。
 - ・ 紛失モードがオンになっている場合でも、パスコードオフは実行できます。ただし、パスコードオフ実行後の画面は紛失モードオフ後に確認できます。
 - ・ リモートワイプを行うことはできます。ただし、リモートワイプ後、紛失モードはオフになり再アクティベート可能な状態になります。
 - ・ Anクライアント（アプリ）はバックグラウンドで動作できません。そのため、標準位置情報サービスの取得、メッセージ・アンケートの通知の表示ができません。
- 次の操作は、紛失モードがオフになるまで適用されません。
 - ・ アプリ、ブックのインストール操作（App Store / In-House / VPP Store）
アプリ配信のリトライは12時間ごとのため、紛失モードオフが適用されてから、最大12時間以内に端末に配信されます。
 - ・ VPP利用ユーザーの招待
VPP利用ユーザーの招待のリトライは12時間ごとのため、紛失モードオフが適用されてから、最大12時間以内に招待が行われます。
- 管理コンソールから紛失モードオンの端末を削除すると、その端末を紛失モードオフにすることができなくなり、ロックを解除することができず、端末が利用できなくなります。
管理コンソールから紛失モードオンの端末を削除する場合、必ず端末の紛失モードをオフにしてから端末を削除してください。



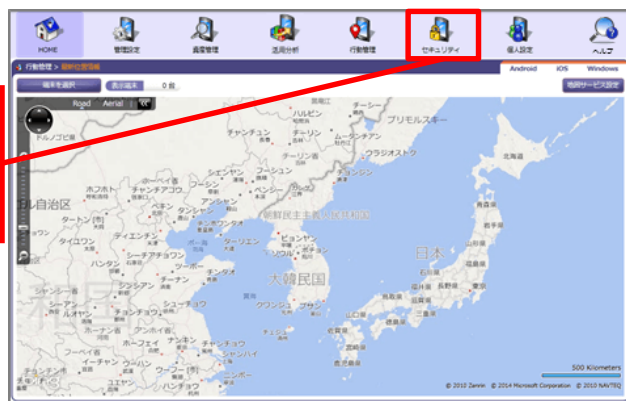
紛失モードをオンにする

※iOSのみ

端末使用者が端末を紛失してしまった場合に、紛失モードをオンにして外部からの操作を防ぎます。

1

画面上部にあるメニュー「セキュリティ」をクリックします。

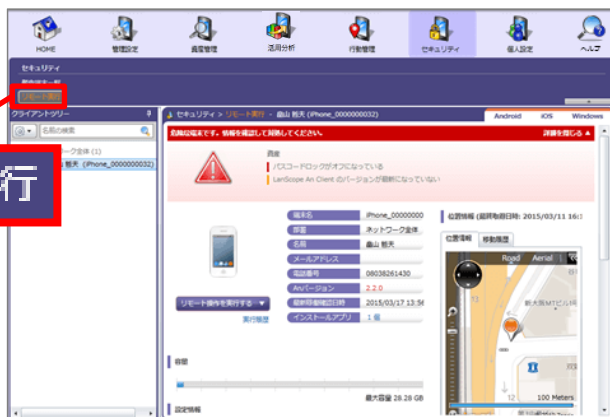


2

「リモート実行」をクリックします。

【リモート実行画面】

リモート実行



3

左のツリーから紛失モードをオンにしたい端末を選択してクリックします。

【リモート実行画面】



4

リモート実行画面から、「リモート操作を実行する」をクリックします。

リモート操作を実行する ▼

【リモート実行画面】



5

「紛失モードオン」をクリックします。



【リモート実行画面】



6

「紛失モードオンの実行」が開きます。
「メッセージ」、「電話番号」、「脚注」を入力し、
「実行」をクリックすると紛失モードの設定が完了します。

※「メッセージ」、「電話番号」、「脚注」についての詳細は次のページを参照してください。

【紛失モードオンの実行画面】

紛失モードオンの実行

飯田 太郎 (iPhone_000000026)

紛失モードをオンにします。
オフにするまで端末のロック画面を解除することはできません。
また、メッセージ、電話番号、脚注を変更することはできません。

メッセージ:

ロック画面の上段に表示されます。

電話番号:

ロック画面の中段に表示されます。

脚注:

ロック画面の下段に表示されます。 ※「脚注」のみを設定することはできません。

※紛失モードをオンにすると、「リモート操作を実行する」メニューの「位置情報取得」が実行できます。
端末の位置情報サービス設定がオフの場合や LanScope An Client がインストールされていない場合でも、
リモートで位置情報が取得できます。

実行 キャンセル

実行

●紛失モードの「メッセージ」、「電話番号」、「脚注」について

紛失モードの実行画面で、端末側のロック画面に表示させる「メッセージ」、「電話番号」、「脚注」を任意に設定することができます。

設定後、紛失モードをオフにするまで文言を変更することはできません。変更したい場合は、紛失モードをオフにしてから変更し、再度紛失モードをオンにする必要があります。

それぞれの詳細については、次のとおりです。

・「メッセージ」について

ロック画面の上段に表示されます。入力可能な文字数は、半角50文字、全角25文字です。

※「メッセージ」を設定せずに「電話番号」を設定した場合、「メッセージ」と同じ位置に「持ち主に連絡」という文言がiOSの仕様により自動的に表示されます。

※iOSが対応していないフォントで「メッセージ」を設定した場合、端末側で文字化けします。

・「電話番号」について

ロック画面の中段に表示されます。入力可能な文字数は、半角数字のみの15文字です。「-（ハイフン）」は入力できません。また、「発信」ボタンが表示されて設定した番号に発信することができます。

※表示されている「電話番号」への発信は、SIMカード利用のiPhoneのみ対象です。

iPad / iPod touchでは「発信」ボタンが表示されません。

・「脚注」について

ロック画面の下段に表示されます。入力可能な文字数は、半角50文字、全角25文字です。

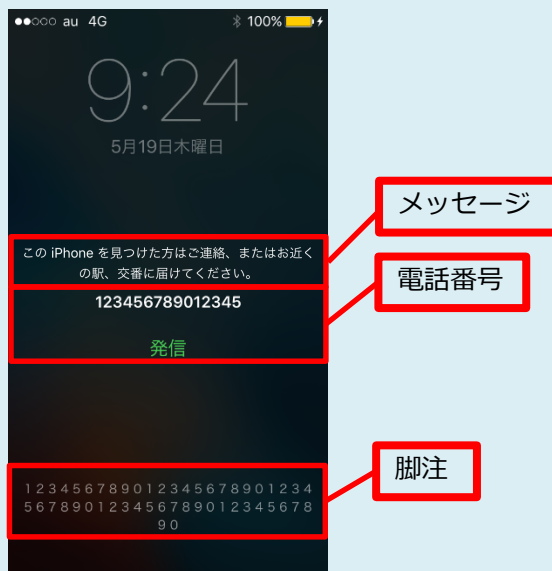
また、下記の文字が含まれている場合、iOS 端末側で「脚注」が表示されません。

- ・全角文字（例：あいう）
- ・半角カナ（例：ｶﾅ）
- ・「/（スラッシュ）」（例：/abc）

※iOSの仕様により、「脚注」のみを設定して端末側で表示することはできません。

「メッセージ」もしくは「電話番号」と併せて設定する必要があります。

【iPhone5の紛失モードロック画面例】



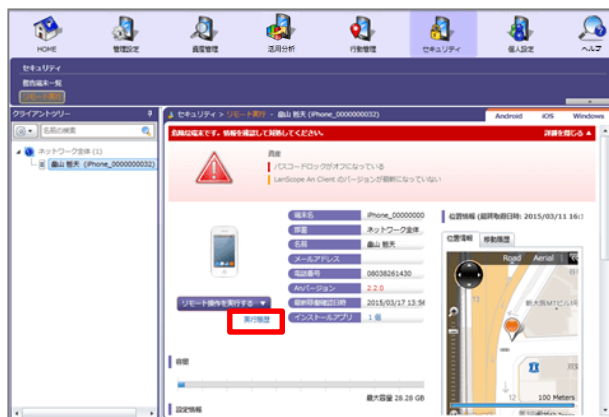
！ 紛失モードの実行結果を確認する

紛失モードが実行されているかどうかを確認します。

1

リモート実行画面で、「実行履歴」をクリックして開きます。

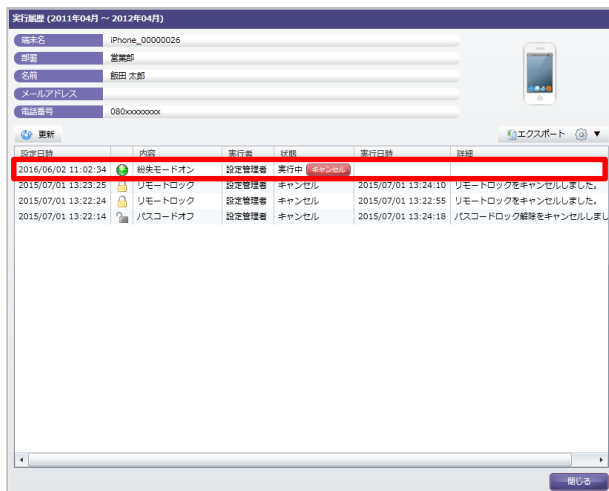
【リモート実行画面】



2

紛失モードの実行結果を確認します。

【実行履歴画面】

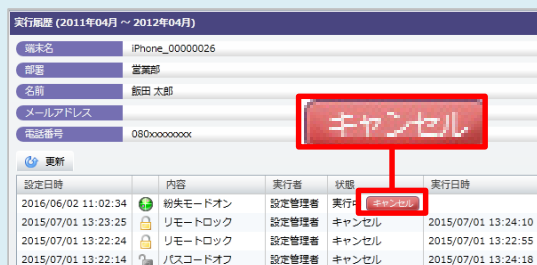


●紛失モードのキャンセル

紛失モードが実行中の場合、「実行履歴」画面から紛失モードをキャンセルすることができます。

実行をキャンセルする場合、「状態」項目の「キャンセル」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、確認画面が表示されたのち、結果ダイアログが表示されます。

【実行履歴画面】



●実行履歴画面の状態表示について

紛失モードオンの場合、実行履歴画面の状態表示には、次のステータスが表示されます。

リモート操作	状態	詳細
紛失モードオン	成功	紛失モードをオンに設定しました。
	待機中	端末が通信できる状態になればリモート操作を実行します。
	キャンセル	紛失モードオンをキャンセルしました。
	失敗	リモート操作の実行に失敗しました。
		90 日間端末から応答がありませんでした。



紛失モードをオンにした時のエラーと対処方法

紛失モードをオンにした時に次のエラーが表示された場合、それぞれ対処を行ってください。



表示されるメッセージと対処方法は以下のとおりです。

メッセージ	対処方法
<p>すでに紛失モードオンが実行されています。</p> <p>改めて実行するには、【リモート操作】 - 【実行履歴】 からキャンセルし、再度紛失モードオンを実行してください。</p>	<p>「紛失モードの実行結果を確認する」(p.49)を参照し、紛失モードをキャンセルしてから、再度紛失モードをオンにします。</p>



紛失モード実行中に位置情報を取得する

1. 位置情報の取得について

端末が紛失モードオンであれば、次の場合でも位置情報が取得できます。

- ・ログ取得設定で「位置情報を取得する」設定が有効になっていない場合
- ・iOS端末の位置情報サービス設定がオフの場合
- ・Anクライアント（アプリ）をインストールしていない場合

取得した位置情報は、最新位置情報画面に反映されます。移動履歴画面には反映されません。

2. 位置情報の取得設定

1

リモート実行画面から、「リモート操作を実行する」をクリックします。

リモート操作を実行する ▼

【リモート実行画面】



2

「位置情報取得」をクリックします。



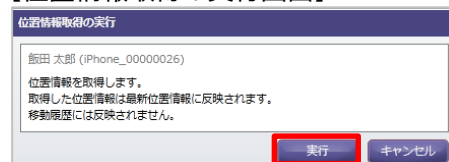
【リモート実行画面】



3

「位置情報取得の実行」画面が表示されます。
「実行」ボタンをクリックします。

【位置情報取得の実行画面】



3.「位置情報」画面の表示について

リモート実行画面から「位置情報取得」を有効にした紛失モード実行中の端末の位置情報は、「最新位置情報」画面で確認できます。

紛失モード実行中の端末は、図のように現在地アイコンのマークとピンを灰色で表示し、通常の状態の端末と区別しています。

※通常の端末は赤色で表示されます。

【最新位置情報画面】





紛失モードをオフにする

※iOSのみ

紛失した端末が発見できた場合、紛失モードをオフにします。

※紛失モードをオフにする設定は、管理コンソールからのみ実行できます。

1

リモート実行画面から、「リモート操作を実行する」をクリックします。

リモート操作を実行する ▼

【リモート実行画面】



2

「紛失モードオフ」をクリックします。



【リモート実行画面】



3

「紛失モードオフの実行」画面が開きます。
「実行」をクリックすると、紛失モードオフの設定が完了します。

【紛失モードオフの実行画面】



●実行履歴画面の状態表示について

紛失モードオフの場合、実行履歴画面の状態表示には、次のステータスが表示されます。

リモート操作	状態	詳細
紛失モードオフ	成功	紛失モードをオフに設定しました。
	待機中	端末が通信できる状態になればリモート操作を実行します。
	キャンセル	紛失モードオフをキャンセルしました。
	失敗	リモート操作の実行に失敗しました。
		90 日間端末から応答がありませんでした。

?

モバイル回線、Wi-Fi回線のどちらでもリモート操作はできますか？

01

はい、どちらかが有効で通信が可能な状態であれば、リモート操作は実行可能です。

?

リモート操作に失敗するとどうなりますか？

02

端末が通信可能になるまで「実行中」や「待機中」（実行中から30秒経過後）ステータスになります。端末が通信可能になればリモート操作に成功しますが、90日経過後も成功しない場合は「失敗」になります。

?

ロック解除方法を「パターン」形式で設定している場合、リモートロックは可能ですか？（Android端末のみ）

03

可能です。その場合は、自動的に「パスワード」形式に変換されます。

?

「リモート実行画面」で、位置情報に「データがありません」と表示されます。何が原因ですか？

04

位置情報の表示権限がない場合、位置情報は表示されません。また位置情報に限らず表示権限がない情報は、表示されません。

?

同じ端末に複数回、リモートロックを実行した場合はどうなりますか？

05

リモートロックを実行するたびに、端末がロックされます。ロックを解除するには、最後にリモートロックを実行した際に設定したパスワードでロックを解除します。
※すでにパスワードが設定されているAndroid 7.0以降の端末の場合、リモートロック実行時に入力したパスワードは設定されません。

?

LanScope An Clientの「デバイス管理者」を強制的に有効にできますか？

06

Android OSの仕様上、自動で有効にすることはできません。ただし、有効になっていない場合、設定を有効にするよう促す画面が表示され、設定するまで他の操作が行えない状態になります。



リモートワイプを実行した場合、SDカードの情報も消去されますか？

07

機種によって制限事項があります。詳細はお問い合わせください。



LanScope An Clientの「デバイス管理者」を利用者が無効にした場合、管理者は気づくことができますか？

08

Android端末の場合、「警告端末一覧」画面にリモート操作が実行できない旨のアラートが表示されるので、管理者の方は、気づくことが可能です。また「デバイス管理者」が無効の場合、「資産情報一覧」画面の「デバイス管理者」列が「OFF」と表示されるため、一覧で確認ができます。

さらに「デバイス管理者」を無効にしたログを操作ログ画面から確認することもできます。

なお無効にした場合、設定を有効にするよう促す画面が表示され、設定するまで他の操作が行えない状態になります。



LanScope An Clientの「デバイス管理者」を利用者が無効にした場合、端末側で何か変更はありますか？

09

「デバイス管理者に登録されていません」という警告が、端末上に表示されます。詳細な画面は、p.21をご覧ください。（Android端末のみ）



「警告端末一覧」画面で「選択した端末を除外する」ボタンが表示されません。何が原因ですか？

10

除外設定には、「警告設定を変更する権限を付与する」の設定が必要です。手順は、p.12をご覧ください。



「警告設定」で危険や注意の警告内容を部署ごとに設定することはできますか？

11

部署ごとの設定はできません。1つの設定が全端末に反映されます。

その他よくあるご質問（FAQ）については下記のURLをご参照ください。

https://faq.motex.co.jp/?site_domain=an

- ※ Android端末のリモート操作の実行には「Google Play ストア」のインストールが必要です。2012年以降に発売された端末であればプリインストールされています。
2012年より前に発売されたAndroid端末には、出荷状態では「Google Play ストア」ではなく「AndroidMarket」がインストールされている場合があります。「AndroidMarket」はネットワークに接続されると自動的に「Google Play ストア」にアップデートされます。
 - ※Android 4.0.4 未満の端末に対して、リモート操作を実行するには、端末にGoogleアカウントが設定されている必要があります。
 - ※Android OS 3.x 以降4.0未満のバージョンかつ、今までに英数字のパスワードを一度も設定したことが無い場合はリモートロックに失敗します。事前に英数字のパスワードを設定してください。
 - ※iOS端末への命令は、Apple社のPush通知サーバであるAPNsを使用しています。このAPNsの処理能力（仕様未公開）により、Push通知に遅延が発生することがありますが、その場合リモート実行が設定後すぐに実行されないことがあります。
 - ※端末の通信環境が特殊な状況下（ネットワーク環境が不安定であったり、接続/切断が繰り返されるような状況）においてリモート実行を行った場合、実行履歴が「待機中」のまま変わらないことがあります。この場合、実際に実行もされておらず、実行命令も途中で無効になっています。明らかに端末がネットワークに接続されているにもかかわらず、履歴が「待機中」のまま変わらない場合は、再度リモート実行を行ってください。
 - ※すでにパスワードが設定されているAndroid 7.0以降の端末の場合、リモートロック実行時に入力したパスワードは設定されません。
- その他、機種によって制限事項があります。詳細はお問い合わせください。

■ 製品に関するご相談は、次のWebフォームよりお問い合わせください。

- ご購入後の機能・操作に関するお問い合わせ
<https://go.motex.co.jp/l/320351/2017-06-21/ffyl?>
- ご購入に関するお問い合わせ
<https://go.motex.co.jp/l/320351/2017-11-27/7d5pg?>

■ よくあるご質問（FAQ）については下記URLを参照してください。

https://faq.motex.co.jp/?site_domain=an