

Secure Filtering (ISGC) 初期設定手順について

Ver1.4 2026/9/14

株式会社AXSEED





本資料では、**Secure Filtering(ISGC)**に関する初期設定の手順について、記載します。

なお、設定手順は**ISGC**側の仕様変更に伴い、予告なく変更される場合があります。予めご了承ください。



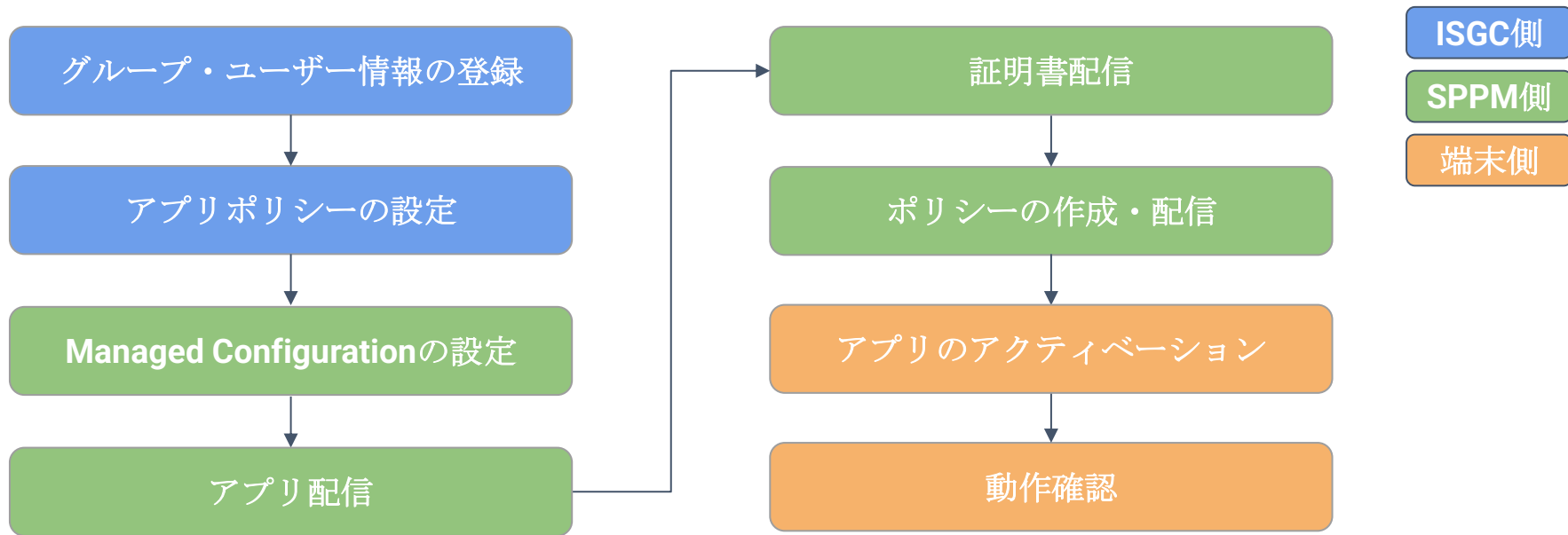
- **Android設定**
 - [フロー図](#)
 - [Managed Configurationの設定](#)
 - [アプリ配信](#)
 - [証明書配信](#)
 - [ポリシーの作成・配信](#)
- **iOS設定**
 - [フロー図](#)
 - [ManagedAppConfigurationの設定](#)
 - [アプリ配信](#)
 - [プロファイルの作成・配信](#)
- **キッティング**
 - [ISGC assist キッティング](#)

Android設定





Android設定フロー図



本資料では、MDM側の設定箇所となる「**Managed Configurationの設定**」「**アプリ配信**」「**証明書配信**」「**ポリシー作成・配信**」について記載します。
その他の設定については、**ISGC**のマニュアルをご参照ください。

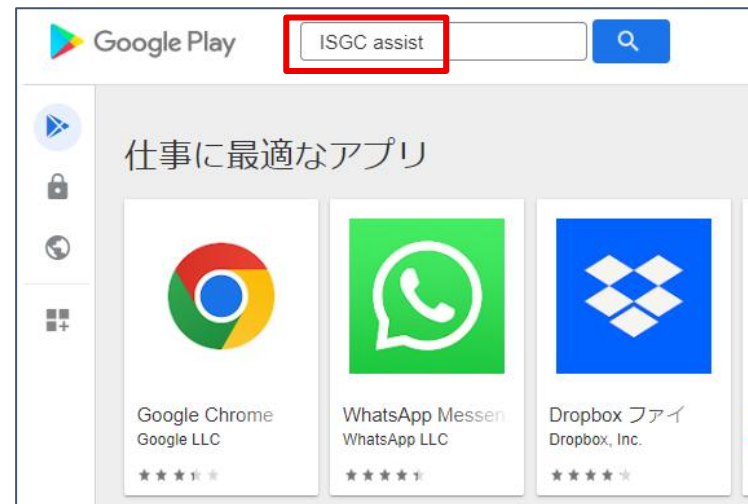
ユーザー様専用ダウンロードサイト>端末初期設定手順>**ISGC assist** を利用の方
>**ISGC assist** 初期設定手順書 (Android 版)



Managed Configuration の設定 - 概要

ISGC assist アプリを**Play**ストアアプリとして登録後、「アプリ設定」から各アプリパラメータを設定します。

Managed Configuration の設定 - 手順1/7



②検索画面に「ISGC assist」と入力の上、検索を行い、検索結果に表示される「ISGC assist」を選択

①管理画面「アプリ」>Android「Playストアアプリ」
>「アプリ登録・削除」



Managed Configuration の設定 - 手順2/7



③画面内の「選択」を押下することでPlayストアアプリ一覧内に「ISGC assist」が追加されます



☐	ISGC assist		アルプスシステムインテグレーション株式会社	2024/08/09 10:38	しない	
--------------------------	-------------	---	-----------------------	---------------------	-----	--

Managed Configuration の設定 - 手順3/7

	ISGC assist		アルプスシステムインテグレーション株式会社
--	-----------------------------	---	-----------------------



- ④Playストアアプリ一覧画面内の「ISGC assist」を選択の上、画面右下にある「アプリ設定」を選択



Managed Configuration の設定 - 手順4/7

- ⑤ 「アプリパラメータ設定」において、「設定区分」を「設定する」、「配布区分」を「個別設定」に設定の上、
【入力フォーマット出力】を選択し、CSVファイルをダウンロードする

アプリパラメータ設定

設定区分

☐ 設定しない ☒ 設定する

配布区分

☐ 一括設定 ☒ 個別設定

入力フォーマット出力

タイトル	key	入力値	型	説明
version	version	string	hidden	制約指定でサポートしているキー種別を定義するためのバージョン
host	icaphost	string	string	サービスサーバーのホストを指定します。
port	icapport	string	integer	サービスサーバーのポートを指定します。
group	group	string	string	アプリインストールのManaged Configurations情報の表示に沿って指定を行ってください。
account	account	string	string	任意ユーザのアカウント名を指定します。
password	password	string	string	任意ユーザのパスワードを指定します。
agreement	agreement	TRUE or FALSE	bool	サービス利用規約に同意済みかを表すフラグ
unreached_block	unreached_block	TRUE or FALSE	bool	クラウド通信不可時の動作を定義するフラグ
hide_restart	hide_restart	TRUE or FALSE	bool	再起動機能非表示フラグ
hide_log	hide_log	TRUE or FALSE	bool	ログ確認機能非表示フラグ
service_proxy_port	service_proxy_port	string	integer	内部プロキシの待ち受けポートを指定する

アプリ設定CSV

ファイルを選択

選択されていません

OK

キャンセル

Managed Configuration の設定 - 手順5/7

CSVに設定内容を記載してください。（アプリ設定項目の詳細は[SPPMオンラインマニュアル](#)をご参照ください。）

account,password

account: アプリ設定を行うISGCのユーザーのユーザー名を入力します。
password: アプリ設定を行うISGCのユーザーのパスワードを入力します。
※ISGCのユーザー名は端末毎に異なる値である必要があります。

service_proxy_port

「15123」と入力します。

記載例：

処理区分	tel	serial	version	icaphost	icaproduct	icaproduct	group	account	password	agreement	unreached_block	hide_restart	hide_log	service_proxy_port
1		xxx0000000000000000		xxx.com			グループA	xxx0000000000000000	password					15123

処理区分

操作の有無を選択します。
行いたい操作によって、
以下を入力してください。

- ・ 追加,変更を行う：1
- ・ 追加,変更を行わない：0
- ・ 設定を解除：3

tel,serial

「tel」と「serial」は、どちらか一方のみ入力してください。
両方入力した場合は、「tel」の内容が優先して登録されます。
tel：電話番号を入力します。
serial：シリアルを入力します。

※telを使用する場合は、デバイス一覧画面に表示される「電話番号1」列の電話番号を記載してください。serialを使用する場合は、デバイス一覧画面に表示される「シリアル」列のシリアル番号を記載してください。

Managed Configuration の設定 - 手順6/7

CSVに設定内容を記載してください。

ISGC管理画面ホームの「アプリインストール」 >

「ISGC assist Android Managed Configurations 情報」の各項目をコピーしCSVにペーストします。

記載例：

処理区分	tel	serial	version	icaphost	icappport	group	account	password	agreement	unreached_block	hide_restart	hide_log	service_proxy_port
1		xxx0000000000000000		xxx.com	xxx	グループA	xxx0000000000000000	password					15123

▶ ISGC assist Android Managed Configurations情報

構成	host	
	port	
	group	
	account	※任意ユーザのアカウント名を指定します。
	password	※任意ユーザのパスワードを指定します。



Managed Configuration の設定 - 手順7/7

⑥CSV入力後、画面左下の「アプリ設定CSV」からCSVをアップロードの上、「OK」を選択します。

*Excelで編集を行った場合、シリアル番号等の数値が指数になっていることがあります。

数値になっているかCSVを確認の上、アップロードしてください。

アプリパラメータ設定

設定区分

☐ 設定しない ☒ 設定する

配布区分

☐ 一括設定 ☒ 個別設定

入力フォーマット出力

タイトル	key	入力値	型	説明
version	version	string	hidden	制約指定でサポートしているキー種別を定義するためのバージョン
host	icaphost	string	string	サービスサーバーのホストを指定します。
port	icapport	string	integer	サービスサーバーのポートを指定します。
group	group	string	string	アプリインストールのManaged Configurations情報の表示に沿って指定を行ってください。
account	account	string	string	任意ユーザのアカウント名を指定します。
password	password	string	string	任意ユーザのパスワードを指定します。
agreement	agreement	TRUE or FALSE	bool	サービス利用規約に同意済みかを表すフラグ
unreached_block	unreached_block	TRUE or FALSE	bool	クラウド通信不可時の動作を定義するフラグ
hide_restart	hide_restart	TRUE or FALSE	bool	再起動機能非表示フラグ
hide_log	hide_log	TRUE or FALSE	bool	ログ確認機能非表示フラグ
service_proxy_port	service_proxy_port	string	integer	内部プロキシの待ち受けポートを指定する

アプリ設定CSV

ファイルを選択

選択されていません

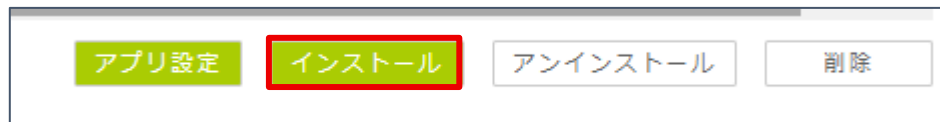
OK

キャンセル



アプリの配信 - 手順1/2

	ISGC assist		アルプスシステムインテグレーション株式会社
--	-----------------------------	---	-----------------------



- ①Playストアアプリ一覧画面内の「ISGC assist」を選択の上、画面右下にある「インストール」を選択



アプリの配信 - 手順2/2

サイレントインストール

アプリのサイレントインストールを行います。
各項目を入力して、OKボタンを押してください。

アプリ名	ISGC assist
説明文	
デバイス選択	☒ デバイス一覧から選択 ☐ CSVで指定 選択
適用スケジュール	☒ 即時適用 ☐ スケジュール適用

OK

キャンセル

②対象端末および適用スケジュールを選択の上、
「OK」を選択

③順次端末にアプリがインストールされます。



証明書配信 - 手順1/2



- ① 予めISGC管理画面において、「共通アクセス管理」の「HTTPS規制設定」を選択して、HTTPS規制設定画面に遷移の上、「認証局設定」にある「認証局証明書のダウンロード」をクリックし、「cacert.cer」を保存してください。
- ② 管理画面「プロフィール」> **Android**「証明書」>「新規登録」



証明書配信 - 手順2/2

③「設定名」を入力の上、CA証明書「する」を選択し、保存した証明書ファイルをアップロード

- ※保存した証明書をそのままアップロードすると、エラーが発生し、アップロードに失敗します。Windowsコマンドプロンプト等を使用し、Base64エンコード形式に変換した証明書を登録する必要があります。

Windowsコマンドプロンプトでの変換手順：

- Windowsキー>[d]キー>[o]キー>[s]キーと押下し、右図が表示された後[Enter]を押下

最も一致する検索結果

コマンド プロンプト
システム

以下の通り「正常に完了しました」と表示されれば成功です。この場合はWindowsのダウンロードフォルダにcacert.b64.cerという証明書ファイルができます。このファイルをアップロードしてください。

以下のコマンドを入力して[Enter]を押下

- ※ どちらのファイル名もフルパスで指定してください。

certutil -encode "元ファイル名" 変換後ファイル名"

```
Microsoft Windows [Version 10.0.19045.5198]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Yax>certutil -encode "C:\Users\Yax\Downloads\cacert.cer"
"C:\Users\Yax\Downloads\cacert.b64.cer"
入力長 = 946
出力長 = 1360
CertUtil: -encode コマンドは正常に完了しました。

C:\Users\Yax>
```

④「配布対象デバイス」および「適用スケジュール」を選択の上、「OK」を選択



ポリシーの作成・配信 - 手順1/3



**ポリシー登録
プリセットパターン選択**

選択したパターンがプリセットされた状態から、ポリシーの登録を行います。
ポリシーの設定内容は、自由に変更可能です。

「プリセットなし」以外のパターンから作成する場合は、すでに「パスコード・制限・アプリ制御」の機能制御が作成されているため、「Wi-Fi設定・Wi-Fi設定（証明書）」、「SIM変更検知設定」を混合して作成することはできません。
また、work profile、COPEは対象外となります。
work profile、COPEで作成したい場合は「プリセットなし」を選択してください。

「Wi-Fi設定・Wi-Fi設定（証明書）」、「SIM変更検知設定」を作成したい場合は「プリセットなし」を選択するか、一度「パスコード・制限・アプリ制御」ペイロードの右上の「－」ボタンを押下して削除を行ってから作成してください。

プリセットパターン選択

プリセットパターン ? プリセットなし ▼

[プリセット内容説明用ファイルへのリンク](#) **OK** キャンセル

①管理画面「プロフィール」>**Android**「ポリシー」
>「新規登録」

②「プリセットなし」のまま、「**OK**」を選択



ポリシーの作成・配信 - 手順2/3

③ポリシー名を入力する。

ポリシー登録

Android Enterprise

Android

Android Enterprise のポリシー作成をおこないます。(*がついている項目は、必須入力項目です。)
Wi-Fi設定以外の設定はデバイスに1つしか適用されず、複数適用した場合には最新のポリシーが有効となります。
ポリシーは「パスコード・制限・アプリ制御」の機能制御、「Wi-Fi設定・Wi-Fi設定（証明書）」、「SIM変更検知設定」、「発着信番号制限」を混在して作成することはできないため、項目ごとに作成してください。
また、「Wi-Fi設定」と「Wi-Fi設定（証明書）」を混在して作成することもできないため、項目ごとに作成してください。

✓ 一般	一般
☐ パスコード	ポリシー名*
☐ 制限	種別* ☒ fully managed device ☐ work profile ☐ COPE
☐ アプリ制御	説明
☐ Wi-Fi設定	
☐ Wi-Fi設定(証明書)	



ポリシーの作成・配信 - 手順3/3

☒ 一般	制限
☒ パスコード	
☒ 制限	機能 アプリ ポーリング間隔時間: 60分 ▼ 制限メッセージ*: ご不明な点がある場合は、IT管理者にお問い合わせください。
☒ アプリ制御	
☐ Wi-Fi設定	☐ カメラを禁止
☐ Wi-Fi設定(証明書)	☐ Wi-Fiを禁止
☐ SIM変更検知設定	☐ ユーザによるWi-Fi設定変更を禁止
☐ 発着番号制限	☐ VPNの設定変更を禁止
	☐ Bluetoothを禁止
	☐ Bluetooth設定変更を禁止
	☒ 外部ストレージを禁止
	☐ デザリング&モバイルホットスポットの設定変更を禁止
	☐ 位置情報共有設定を禁止
	位置情報取得方法: 高精度 ▼
	位置情報の取得: ☐ 取得する 取得間隔: しない ▼ ☒ 取得しない
	☐ スクリーン・キャプチャーを禁止
	☒ 開発者モード(デバッグ機能)を禁止する
	☐ 開発者モードを設定する
	☐ USBデバッグをオンにする

④「制限」の「作成」を押下の上、各項目を設定する。

⑤「制限」項目内の一番下にある「プロキシの設定を有効にする」をチェックを入れ、

左入力欄「127.0.0.1」

右入力欄「15123」

を入力する

⑥必要情報入力後、画面右下の「設定確認」を選択

⑦対象端末および適用スケジュールを選択の上、「OK」を選択

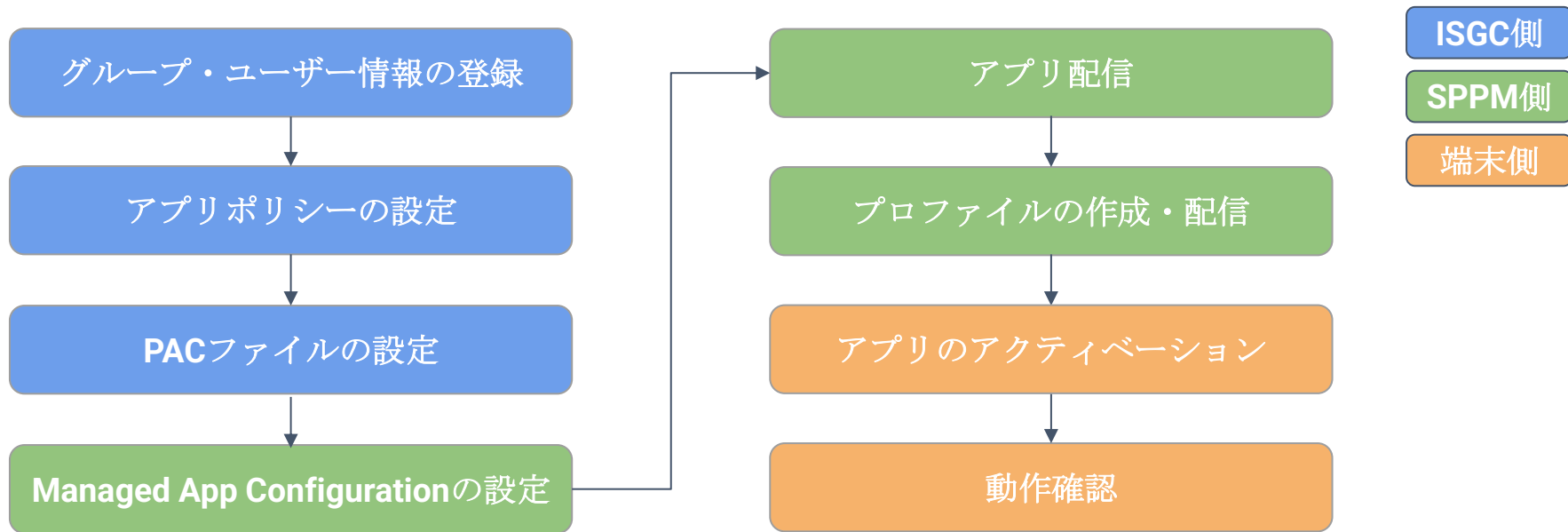
☒ プロキシの設定を有効にする			
プロキシサーバとポート	127.0.0.1	:	15123

iOS設定





iOS設定フロー図



本資料では、MDM側の設定箇所となる「**Managed App Configurationの設定**」「**アプリ配信**」「**プロファイルの作成・配信**」について記載します。
その他の設定については、**ISGC**提供のマニュアルをご参照ください。

ユーザー様専用ダウンロードサイト>端末初期設定手順>**ISGC assist** を利用の方
>**ISGC assist** 初期設定手順書 (iOS 版)

ISGC assist アプリを **Managed Apps** に新規登録する際、併せて「**Configuration**」項目に専用の値を設定します。

Managed App Configuration の設定 - 手順1/5



①管理画面「アプリ」>iOS「Managed Apps」>「新規登録」

アプリ種別*	☐ エンタープライズApp ☐ App Store (無償) ☒ 購入済App iOS9
アプリケーション名*	ISGC assist
説明文	
アイコン	 ファイルを選択 選択されていません
アプリケーション指定*	ISGC assist ▼
アプリカタログに表示*	☐ 表示する ☒ 表示しない
アプリのリモート配布*	☒ 配布する ☐ 配布しない

②アプリ種別等、必要項目を登録する*

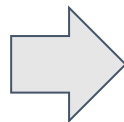
*「アプリのリモート配布」は「配布する」を選択してください



ユーザー情報の登録の際の注意事項

ISGC側でユーザーの登録を行う際は、SPPM管理画面上で取得できる以下の値のいずれかをアカウント名およびパスワードに設定してください。

管理画面の場所	SPPM管理画面項目
デバイス> デバイス一覧> デバイス名> デバイスタブ	デバイス名
	UDID(デバイス識別番号)
	シリアル
	IMEI



いずれかの情報を
アカウント名、パスワードとしてユ
ーザーを作成してください。



Managed App Configuration の設定 - 手順2/5

Configuration

☐ なし ☒ あり

Key	Value (値)
例) host を入力	例) 対応する値 を入力

追加

Key と Value については
次ページをご参照ください

Configuration

Key	Value (値)	
host		削除
port		削除
group		削除
account		削除
password		削除

③ 「**Configuration**」を「あり」に変更し、**Key** と **Value** に値を1つずつ入力し、
都度「追加」ボタンを押下する

Managed App Configuration の設定 - 手順3/5

▶ ISGC assist iOS Managed App Configuration情報

	識別子	
構成	host	
	port	
	group	
	account	※任意ユーザのアカウント名を指定します。
	password	※任意ユーザのパスワードを指定します。

登録する「Key」は以下の通りです。

host
port
group
account
password

「account」と「password」の
Value 値については
次ページをご参照ください

「host」「port」「group」に対応する **Value** 値は、
ISGC 管理画面の下記箇所に表示されております。

「ホーム」>「アプリインストール」>
「ISGC assist iOS Managed App Configuration情報」

Managed App Configuration の設定 - 手順4/5

Key	Value (値)
Key	Value (値)
host	
port	
group	
account	{Serial}
password	{Serial}

account と **password** の **Value** 値には、原則変数を入力します。

使用できる変数は以下の通りです。

管理画面の場所	SPPM管理画面項目	変数
デバイス> デバイス一覧> デバイス名> デバイスタブ	デバイス名	{Device_Name}
	UDID(デバイス識別番号)	{Udid}
	シリアル	{Serial}
	IMEI	{Imei}

account と **password** は、それぞれ異なる変数であっても左の画像の様に同一の変数であっても問題ありません。

※端末を識別する役割のため、値が原則変動しない **{Serial}** や **{Imei}** のご利用を推奨します。

Managed App Configuration の設定 - 手順5/5

デバイス選択	☒ デバイス一覧から選択 ☐ CSVで指定
	選択
適用スケジュール	☐ 通常適用 ☒ 即時適用 ☐ スケジュール適用 即時適用を選択すると、配信キャンセルができなくなります。
OK	

④デバイスは選択せずに「OK」を押下する

アプリカタログに表示	表示しない
アプリのリモート配布	配布する
再配布	再配布しない
デバイス登録時アプリ配信	デバイス登録時アプリ配信しない
配布対象	設定登録：即時適用
OK	

⑤確認画面にて内容を確認の上、再度「OK」を押下する



アプリの配信 - 手順1/2

	ISGC assist	なし		購入済App (AppStore)
---	-----------------------------	----	---	----------------------



- ①Managed Apps一覧画面内の
「ISGC assist」を選択の上、画面右下にある
「登録変更」を選択



アプリの配信 - 手順2/2

デバイス選択	☒ デバイス一覧から選択 ☐ CSVで指定
	選択
適用スケジュール	☒ 通常適用 ☐ 即時適用 ☐ スケジュール適用 通常適用を選択すると、10分後に配信され、その間配信キャンセルができます。
<input checked="" type="button" value="OK"/> キャンセル	

②対象端末および適用スケジュールを選択の上、「OK」を選択

※その他の設定については、必要に応じてご設定ください

③順次端末にアプリがインストールされます。



構成プロファイルの作成・配信 - 概要

ISGC assist アプリの設定にあたっては以下 **3 種**の構成プロファイル、および ISGC の認証局証明書のインストールが必要となります。

1. 端末制限構成プロファイル
2. コンテンツフィルタ構成プロファイル
3. グローバル HTTP プロキシ構成プロファイル
(証明書ペイロードに **ISGC** の認証局証明書を含める)

※それぞれ別のプロファイルで作成の上、1つずつプロファイル配信を実施する必要があります



構成プロファイルの作成 - 手順1/13



①管理画面「プロファイル」>iOS「かんたん一括設定」



構成プロファイルの作成 - 手順2/13

かんたん一括設定 プリセットパターン

選択したパターンがプリセットされた状態から、構成プロファイルの登録を行います。
構成プロファイルの設定内容は、自由に変更可能です。

構成プロファイルには、デバイスが監理モードの場合に効果を発揮する監理モード専用項目 (SV) があります。

また、Apple社の仕様により、「パスコード」のペイロード設定(①)した構成プロファイルを、パスコードの変更を禁止する「制限」ペイロードが設定(②)されているデバイスに対して適用すると、初回は配布成功になりますが、それ以降の変更を受け付けなくなり、エラーステータスとなります。①・②を一枚の構成プロファイルにまとめて適用した場合も同様です。
構成プロファイル登録の際にはご注意ください。

詳細は画面下部の「プリセット内容説明用ファイルへのリンク」をご覧ください。

プリセットパターン選択

プリセットパターン ?

プリセットなし

OK

キャンセル

② 「プリセットなし」のまま、「OK」を選択

かんたん一括設定

構成プロファイルの簡易作成機能です。
(*がついている項目は、必須入力項目です。)

プロフィール設定

設定確認

デバイス選択

✓ 一般

☐ パスコード

☐ 制限

☐ Wi-Fi

☐ VPN

☐ Web クリップ

☐ 証明書

☐ Googleアカウント

一般

プロフィール名称*

組織名*

株式会社AXSEED

説明

デバイスでの
プロフィール削除*

SV

許可しない ▼

プロフィールの
スケジュール削除*

しない ▼

③ 「プロフィール名称」を入力する

*プロフィールを3つ作成するため、区別が付くような
名称にてご設定ください

次ページ以降でプロフィール別の操作になります



構成プロファイルの作成 - 手順3/13

1. 端末制限構成プロファイルについて

かんたん一括設定 構成プロファイルの登録作成機能です。

プロフィール設定 ▶ 設定確認 ▶ デバイス選択

- ☒ 一般
- ☐ パスコード
- ☒ 制限**
- ☐ Wi-Fi
- ☐ VPN
- ☐ Web クリップ
- ☐ 証明書
- ☐ Googleアカウント
- ☐ Exchange ActiveSync
- ☐ メール
- ☐ グローバルHTTPプロキシ
- ☐ DNSプロキシ
- ☐ コンテンツフィルタ
- ☐ モバイル通信

制限
構成

クリア 設定確認へ

④操作①～③を実施の上、「制限」の項目を選択し、画面内の「構成」を押下



構成プロファイルの作成 - 手順4/13

1. 端末制限構成プロファイルについて

制限

機能 アプリケーション メディアコンテンツ

- ☒ カメラの使用を許可
- ☒ FaceTimeを許可 SV
- ☒ スクリーンショットと画面収録を許可
- ☒ AirPlay、"クラスルーム"による画面の閲覧、および画面共有の許可 iOS12 SV
☐ "クラスルーム"にプロンプトなしでのAirPlayと"画面を表示"の実行を許可 SV
- ☒ AirDropを許可 SV
- ☒ iMessageを許可 SV
- ☒ Apple Musicを許可 SV
- ☒ Radioを許可 SV
- ☒ デバイスのロック中も音声ダイヤルを許可
- ☒ Siriを許可
 - ☒ デバイスのロック中もSiriを許可
 - ☐ Siriの不適切な単語フィルタを有効にする SV
 - ☒ Siriにユーザ生成コンテンツを表示 SV
- ☒ Siriの検索候補を許可
- ☒ Apple Booksを許可 SV
- ☒ Appのインストールを許可 SV
 - ☒ App StoreからのAppのインストールを許可 iOS9 SV
 - ☒ Appの自動ダウンロードを許可 iOS9 SV
- ☒ Appの削除を許可 SV
- ☒ システムAppの削除を許可 SV
- ☒ App Clipを許可 SV
- ☒ App内課金を許可
- ☐ 購入時に常にiTunes Store/パスワードを要求

⑤以下の項目について、それぞれ設定を行ってください。

- スクリーンタイムを許可（監視対象のみ）
→チェックを入れない
- 管理対象外出力先で管理対象ソースからの書類を許可
→チェックを入れる
- 管理対象出力先で管理対象外ソースからの書類を許可
→チェックを入れる

※その他は任意の設定にて、問題ございません。

⑥設定完了後、画面右下の「設定確認へ」>「デバイス選択画面へ」を選択



構成プロファイルの作成 - 手順5/13

1. 端末制限構成プロファイルについて

構成プロファイル登録

構成プロファイルの登録およびデバイスへの適用をおこないます。
各項目を入力して、OKボタンを押してください。
(*がついている項目は、必須入力項目です。)

構成プロファイル設定

構成プロファイル*

ファイルを選択 選択されていません
検証テスト.mobileconfig

個別設定*

☐ あり ☒ なし

デバイス選択

☒ デバイス一覧から選択 ☐ CSVで指定 ☐ AppleID一覧で指定(※共有iPadのみ)

選択

ポリシー違反時プロファイル自動削除

セキュリティポリシー違反検知に伴いプロファイルを削除します。

プロファイル自動削除

☐ あり ☒ なし

スケジュール設定

適用スケジュール

☒ 即時適用 ☐ スケジュール適用

その他設定

メモ欄

OK

キャンセル

⑦設定は変更せず、「OK」を選択

⑧続いて表示される確認画面でも「OK」を選択

※デバイスは選択しないでください。



構成プロファイルの作成 - 手順6/13

2. コンテンツフィルタ構成プロファイル

一般

☐ パスコード

☐ 制限

☐ Wi-Fi

☐ VPN

☐ Web クリップ

☐ 証明書

☐ Googleアカウント

☐ Exchange ActiveSync

☐ メール

☐ グローバルHTTPプロキシ

☐ DNSプロキシ

コンテンツフィルタ

☐ モバイル通信

コンテンツフィルタ SV

構成

クリア 設定確認へ

⑨操作①～③を実施の上、「コンテンツフィルタ」の項目を選択し、画面内の「構成」を押下



構成プロファイルの作成 - 手順7/13

2. コンテンツフィルタ構成プロファイル

コンテンツフィルタ

フィルタ・タイプ	プラグイン (他社製App)
フィルタ名*	
識別子*	
サービスのアドレス	
組織	
ユーザ名	
パスワード	
証明書 証明書ペイロードを指定してください	証明書ペイロードに証明書を追加
トラフィックフィルタ	☒ WebKitトラフィックをフィルタ ☐ ソケット・トラフィックをフィルタ

カスタムデータ

キー	値

Per-App Web Content Filter

☐ ※アプリ毎のコンテンツフィルタを利用するには、ManagedAppsでの設定が必要となります。

⑩以下の項目について、それぞれ設定を行ってください。

キー	値
フィルタ・タイプ	プラグイン(他社製App)
フィルタ名	任意の名称
識別子	jp.co.alsi.isgc.assist
WebKit トラフィックをフィルタ	チェックを入れる
ソケットトラフィックをフィルタ	チェックを入れない



構成プロファイルの作成 - 手順8/13

2. コンテンツフィルタ構成プロファイル

⑪カスタムデータについて、それぞれ以下の設定を行ってください。

カスタムデータ キー (Key)	値 (Value)
SERVICE_PROXY_PORT	ISGC assist PAC配信で表示される「ローカルプロキシポート番号」で設定したポート番号を指定してください。
SERVICE_PORT	PACサーバの待ち受けポートを指定します。定義自体の省略が可能です。省略した場合は8080です。 他アプリとのポートバッティング等が発生しない限り、変更する必要はありません。
BYPASS_HOST_SEPARATOR	PROXY_BYPASS_HOSTにて指定するホスト名の区切り文字を指定します。定義自体の省略が可能です。 省略された場合カンマ (,) です。文字列が指定された場合は対象の文字列を区切り文字として判定します。 ※ワイルドカード (*) を含む文字列は指定しないでください。
UNREACHED_BLOCK	通信を規制する場合はtrueを指定してください。指定すると、以下の場合に通信を規制します。 ● ISGC assistがISGCサーバへの接続に失敗したとき ● Ver. 1.1.11未満からアップデートを実施する、あるいはVer. 1.1.11以降で新規キittingしたあと、アプリを起動して情報取得へ同意するまでの間、定義自体の省略が可能です。省略された場合はfalseです（通信が許可されます）。



構成プロファイルの作成 - 手順9/13

2. コンテンツフィルタ構成プロファイル

構成プロファイル登録

構成プロファイルの登録およびデバイスへの適用をおこないます。
各項目を入力して、OKボタンを押してください。
(*がついている項目は、必須入力項目です。)

構成プロファイル設定

構成プロファイル*

ファイルを選択

選択されていません

検証テスト.mobileconfig

個別設定*

☐ あり ☒ なし

デバイス選択

☒ デバイス一覧から選択 ☐ CSVで指定 ☐ AppleID一覧で指定(※共有iPadのみ)

選択

ポリシー違反時プロファイル自動削除

セキュリティポリシー違反検知に伴いプロファイルを削除します。

プロファイル自動削除

☐ あり ☒ なし

スケジュール設定

適用スケジュール

☒ 即時適用 ☐ スケジュール適用

その他設定

メモ欄

OK

キャンセル

⑫設定完了後、画面右下の「設定確認へ」>「デバイス選択画面へ」を選択

⑬設定は変更せず、「OK」を選択

⑭続いて表示される確認画面でも「OK」を選択

※デバイスは選択しないでください。



構成プロファイルの作成 - 手順10/13

3. グローバル HTTP プロキシ構成プロファイル

⑮操作①～③を実施の上、「グローバル HTTP プロキシ」の項目を選択し、画面内の「構成」を押下



構成プロファイルの作成 - 手順11/13

3. グローバル HTTP プロキシ構成プロファイル

グローバルHTTPプロキシ

プロキシタイプ	自動 ▼
プロキシPACのURL*	
PACが到達不能の場合に直接接続を許可	☐
キャプティブネットワークにアクセスするためプロキシのバイパスを許可	☐

⑯以下の項目について、それぞれ設定を行ってください。

キー	値
プロキシタイプ	自動
プロキシPACのURL	ISGC管理画面 「PACファイル設定」内に 表示されるダウンロードURL
PACが到達不能の場合に直接接続を許可	チェックを入れない
キャプティブネットワークにアクセスするためプロキシのバイパスを許可	チェックを入れない (※) 認証を用いる公衆Wi-Fiを利用するケースではチェックする必要があります。



構成プロファイルの作成 - 手順12/13

3. グローバル HTTP プロキシ構成プロファイル

- ⑰ 予めISGC管理画面において、「共通アクセス管理」の「HTTPS規制設定」を選択して、HTTPS規制設定画面に遷移の上、「認証局設定」にある「認証局証明書のダウンロード」をクリックし、「cacert.cer」を保存してください。
- ⑱ 「証明書」の項目を選択の上、画面内の「構成」を押下
- ⑲ 保存した証明書を選択の上、「登録」を押下
- ※ 「証明書名」は登録押下後、自動で入力されます。パスワードの入力は不要です。

☒ 一般	証明書	
☐ パスコード	証明書*	ファイルを選択 選択されていません 登録
☐ 制限	証明書名	CSV
☐ Wi-Fi	パスワード	CSV
☐ VPN		
☐ Web クリップ		
☒ 証明書		



構成プロファイルの作成 - 手順13/13

3. グローバル HTTP プロキシ構成プロファイル

構成プロファイル登録

構成プロファイルの登録およびデバイスへの適用をおこないます。
各項目を入力して、OKボタンを押してください。
(*がついている項目は、必須入力項目です。)

構成プロファイル設定

構成プロファイル*

ファイルを選択

選択されていません

検証テスト.mobileconfig

個別設定*

☐ あり ☒ なし

デバイス選択

☒ デバイス一覧から選択 ☐ CSVで指定 ☐ AppleID一覧で指定(※共有iPadのみ)

選択

ポリシー違反時プロファイル自動削除

セキュリティポリシー違反検知に伴いプロファイルを削除します。

プロファイル自動削除

☐ あり ☒ なし

スケジュール設定

適用スケジュール

☒ 即時適用 ☐ スケジュール適用

その他設定

メモ欄

OK

キャンセル

②⑩設定完了後、画面右下の「設定確認へ」>「デバイス選択画面へ」を選択

②⑪表示される画面で設定は変更せず、「OK」を選択

②⑫続いて表示される確認画面でも「OK」を選択

***デバイスは選択しないでください。**



構成プロファイルの配信 - 手順1/3

【注意】

作成したプロファイルを配信する際は、必ず以下の順で配信を行ってください。

また、1つのプロファイルの配信が成功したことを必ず確認したうえで、次のプロファイルの配信を実施してください。

1. 端末制限構成プロファイルの配信指示



プロファイルの配信が成功した事を確認



2. コンテンツフィルタ構成プロファイルの配信指示



プロファイルの配信が成功した事を確認



3. グローバル HTTP プロキシ構成プロファイルの配信指示

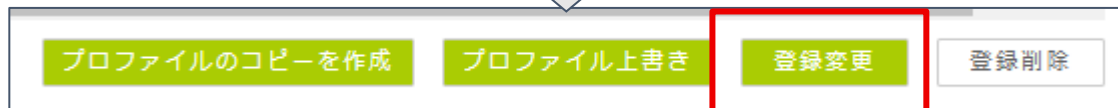
※アンインストール時は3→2→1の順番で削除を行ってください



構成プロファイルの配信 - 手順2/3



	プロフィール名	共通設定ファイル
☒	ISGC用機能制限プロフィール	ISGC用機能制限プロフィール.mobileconfig



②対象のプロファイルを選択の上、
画面右下「登録変更」を選択

①管理画面「プロフィール」>iOS「構成プロフィール一覧」
を選択



構成プロファイルの配信 - 手順3/3

構成プロファイル変更

構成プロファイル登録内容の変更をおこないます。
各項目を入力して、OKボタンを押してください。

構成プロファイル設定

プロファイル名	ISGC用機能制限プロファイル		
構成プロファイル	ISGC用機能制限プロファイル.mobileconfig	ファイル出力	かんたん一括設定編集
個別設定	なし		
デバイス選択	☒ デバイス一覧から選択 ☐ CSVで指定 ☐ AppleID一覧で指定(※共有iPadのみ) 選択		

ポリシー違反時プロファイル自動削除

セキュリティポリシー違反検知に伴いプロファイルを削除します。

プロファイル自動削除	☐ あり ☒ なし
------------	--

スケジュール設定

適用スケジュール	☒ 即時適用 ☐ スケジュール適用
----------	--

その他設定

メモ欄

OK

キャンセル

③配布対象および適用スケジュールを選択の上、**OK**を選択

④確認画面にて内容を確認の上、再度「**OK**」を押下する

⑤適宜プロファイルが配信されます

※iOS構成プロファイルは端末側で画面ロックが解除されたタイミングで配信されます

※構成プロファイルは、端末への配信が完了したことを必ず確認した上で、次のプロファイルの配信を行ってください

配信状況は以下の手順で確認可能です

管理画面「プロファイル」>iOS「構成プロファイル一覧」を選択
>該当の構成プロファイル名を選択

キッティング





ゼロタッチキットティングであつという間に利用開始が可能！

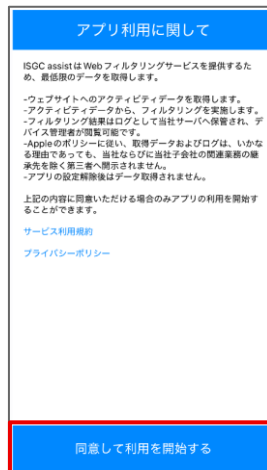
①プロフィール/証明書配信

SPPMよりアプリ/
各種プロフィール/
証明書をプッシュ配信



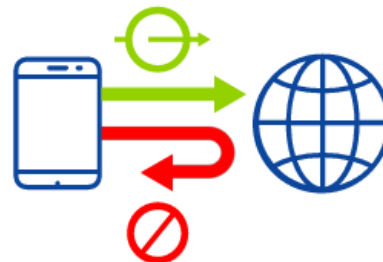
②端末設定

端末で「ISGC assist」
アプリを開き
「同意して利用を開始する」
をタップ



③制御開始

フィルタリング制御開始



※MDMのアプリケーション設定配信機能を利用します。



キッティング完了デバイス確認

キッティングが完了したデバイス情報は一覧で確認可能
条件絞り込みやCSVでの一括出力にも対応

キッティング完了デバイス一覧

▶ 絞り込み条件

アプリ名	(指定なし) ▼	osタイプ	(指定なし) ▼	アカウント名	
ホスト名					
検索/再表示				エクスポート	

表示件数: 15 ▼ 件

◀ ◀ 1 ▼ /1ページ (全6件) ▶ ▶

削除

完了日時 ▼	アプリ名	osタイプ	アカウント名	ホスト名	☐
2024/08/09 16:11:47	Agent Windows	Windows	kainuma	LAPTOP-4B110Q7M	☐
2024/08/06 16:59:54	assist iOS	iOS	P94JVKMG6J	iPhone	☐
2024/07/07 20:54:41	assist iOS	iOS	P94JVKMG6J	iPhone	☐
2024/07/07 20:32:09	assist iOS	iOS	T695D63WQH	iPhone	☐
2024/07/04 19:38:28	assist iOS	iOS	T695D63WQH	iPhone	☐

AXSEED

