サービス仕様書

Rev.0042

2026 年 1 月 発行

目次

1.　はじめに

本書は、InterSafe GatewayConnection（以下 ISGC）を検討中のお客様、販売店様に対し、サービス概要、注意事項について説明する資料となります。製品機能や使い方につきましては、管理者マニュアルをご参照ください。

2. サービス概要

a. ISGC について

ISGC は、マルチデバイス向けのフィルタリングを提供するセキュア Web ゲートウェイサービスです。クラウドならではの即時性・手軽さでシステム管理者のセキュリティ対策を強力にサポートします。

b. サービス一覧

基本サービス	説明
Web フィルタリングサービス	危険なサイトへのアクセスを遮断し、業務効率とセキュリティを向上させます。
技術サポート　【無償】	メールまたは、電話でのお問い合せが可能です。最新の技術情報やメンテナンス、障害等の情報を掲載する FAQ サイトもご用意しています。
ログ保管サービス　【無償】	アクセスログを 100 日間保存するサービスです。
オプションサービス	**説明**
導入支援サービス　【無償】	導入時に必要な作業をサポートするサービスです。
ログ長期保管サービス	アクセスログの保存期間を 365 日へ延長するサービスです。
ダッシュボードサービス	ISGC のアクセスログを自動で取り込み、端末の利用状況を可視化するクラウドサービスです。（教育委員会・学校法人向け）
Microsoft365 ドメイン配信サービス	Microsoft365 で利用するドメイン情報を配信するサービスです。
アクセス制限オプション	ISGC に関する IP アドレスの情報を提供、または ISGC への接続 IP アドレスを制限するサービスです。 ※　プロキシ接続方式でのみ利用可能なオプションです。
帯域拡張オプション	標準提供の帯域を上位プランへアップグレードするサービスです。 ※　プロキシ接続方式でのみ利用可能なオプションです。
VPN 構成オプション	VPN 接続により組織内のネットワークと同等に接続可能になるサービスです。 ※　プロキシ接続方式でのみ利用可能なオプションです。

c. サービスの申し込みと解約

i. 導入の流れ

検討

概要資料、サービス仕様書(本書) 、InterSafe クラウドサービス利用規約、サポートポリシー、およびクラウドセキュリティホワイトペーパーをご確認ください。

InterSafe クラウドサービス利用規約、サポートポリシー、およびクラウドセキュリティホワイトペーパーは下記 URL よりご覧ください。

https://www.alsi.co.jp/resources/security/licensing/

事前の動作確認には、試用環境をご用意します。弊社営業までご相談いただくか、下記 URL よりお申し込みください。

https://www.alsi.co.jp/trial/isgc/

※ 試用版における制限事項につきましては、本書の「サービスの試用について」をご参照ください。

※ 本書の「注意・制限事項」には、試用の際にもご留意いただきたい内容を掲載しております。動作確認の前にご一読ください。

申し込み

ご利用になるサービス／メニューを選定の上、販売店へお申し込みください。

■サービス／メニュー

Web フィルタリングサービス、各種オプションサービス、
Proxy、ISGC assist、ISGC Agent、スクールライセンス（教育機関向けデバイス）

■販売店から提供される書類

ユーザ情報申請書、注文書

構築

弊社環境にて構築作業を実施します。

■環構築期間

・7 営業日程度（オプションサービスをご利用の場合、遅れる場合があります。）

お客様環境設定

サービス証書と ISGC へ接続するための情報、ログダウンロードサイトのアクセス URL をご連絡します。
お客様環境にて、接続設定を実施してください。

■プロキシ接続方式の場合

ISGC へのプロキシ接続を設定してください。

■VPN 接続方式をご利用の場合

VPN 機器を設置し、VPN 経由で行われる ISGC へのプロキシ接続を設定してください。

■ISGC assist をご利用の場合

ISGC assist iOS 版…

「App Store」からダウンロードし、管理画面からデバイスへ設定ファイルを配布してください。

ISGC assist Android 版…

「Play ストア」からダウンロードし、管理画面からデバイスへ設定ファイルを配布してください。

■ISGC Agent をご利用の場合

ISGC Agent Android 版…

「Play ストア」からダウンロードし、管理画面からデバイスへ設定ファイルを配布してください。

ISGC Agent Windows 版…

管理画面からインストーラをダウンロードし、クライアント PC へインストールしてください。

ISGC Agent ChromeOS 版

「Chrome ウェブストア」からダウンロードし、キッティング用 URL にアクセスしてください。

サービス開始

ISGC をご利用ください。

ii. サービスの試用について

① 試用版は 30 日間ご利用いただけます。設定やログ等は試用期間の終了後に消去されます。

② 試用版の利用可能台数は 10 台までとなります。

③ 正規版と同じ窓口にて、技術サポートをご利用いただけます。お問合せの方法は、お申し込み後にご案内します。

④ 試用版は、申し込み時の接続方式をご利用ください。接続に必要となる情報は、お申し込み後にご連絡します。

※ VPN 接続方式による機能の試用は行えません。VPN 接続テストのみお試しいただけます。

⑤ 試用版のプロキシに接続する際は、アカウント認証を行う必要があります。

⑥ アクセスログは、管理画面で過去 3 日分のダウンロード、および当日分（直近のログ）を最大 10,000 行まで確認することができます。

⑦ 試用版では、下記のメニューを利用できません。

共通アクセス管理 ※ 全てのメニュー
HTTPS 規制設定／ブラウザ規制設定／検索キーワード規制設定／書き込み規制設定／規制画面設定／カテゴリ名設定／規制オプション設定（一部利用可能）

サーバ管理 ※ 全てのメニュー
サーバ設定／認証設定／LDAP サーバ設定／一般設定

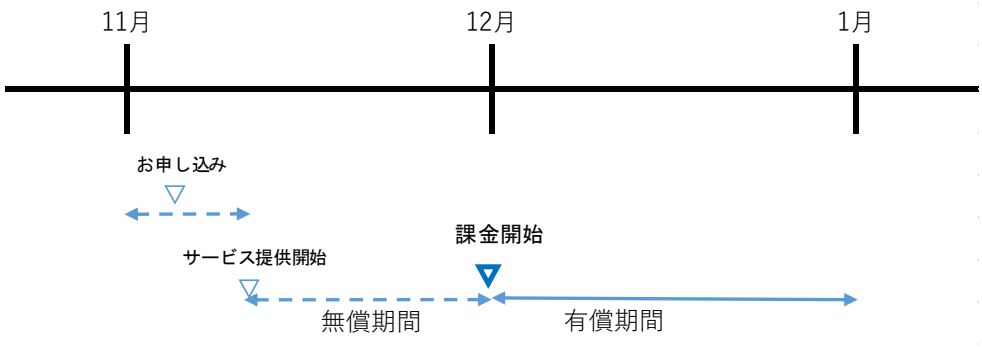
ログ管理
ログ設定

⑧ 試用環境から正規環境への移行（設定やログ等の引継ぎ）は行えません。

※ ISGC Agent のみ利用する（プロキシ接続を利用しない）場合に限り、正規環境への移行が可能です。お申し込み時に弊社営業までご相談ください。

iii. 課金について

サービス開始月は無償期間となり、翌月より課金を開始します。

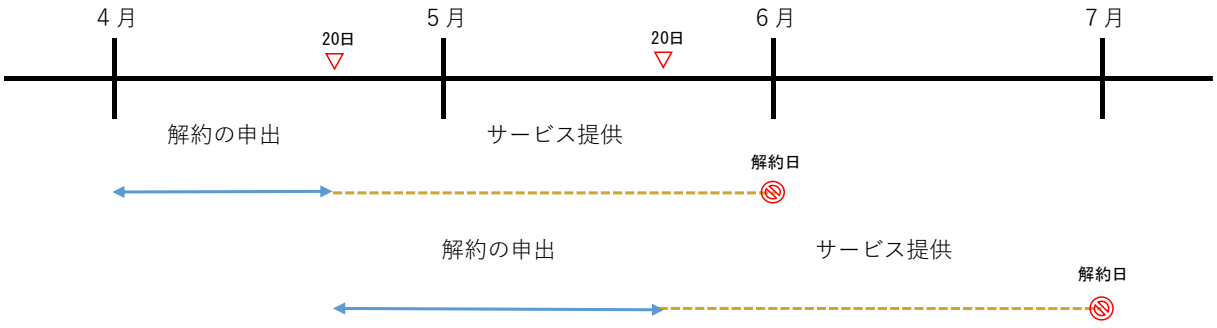


ライセンスはデバイス単位となります。

※ ISGC Agent ChromeOS 版に限りアカウント単位となります。

iv. サービスの解約について

最低利用期間を除き、毎月 20 日までに所定の方法にてお申出いただき、翌月末日をもって解約となります。21 日以降、月末までの解約申出については、翌々月の末日をもって解約となります。



■ 最低利用期間中に解約される場合

残りの月数に月額料金を掛けあわせた金額を一括でお支払いいただきます。

※ 解約日が属する月の月額料金の日割り計算は行いません。

※ 12 ヶ月一括お支払い済みの場合は料金のご返還はいたしません。

■ 最低利用期間後にご解約される場合

1 ヶ月（もしくは申し込みにより 12 ヶ月）を単位とし、自動的に利用期間が延長されるものとします。

d. サービス利用について

① 本サービスは、インターネット上で提供されるため、回線側の機器障害等により通信断が発生する可能性があります。

② ISGC へ接続するインターネット回線は、お客様にてご用意ください。

③ 本サービスの対応プロトコルは、HTTP、HTTPS（※）、FTP over HTTP となります。

※　ISGC Agent（Android/Windows）では、443 ポートを使用しない HTTPS 通信はフィルタリング対象外です。

※　ISGC Agent（Windows）では、FTP over HTTP はフィルタリング対象外です。

④ 選択可能な ISGC への接続方式は、ご利用になるサービスにより異なります。サービスと接続方式の組み合わせにつきましては、次章「3.ISGC の基本構成」をご参照ください。

⑤ 「VPN 構成オプション」をご利用の場合、導入時の接続設定は、サービス開始時に弊社より提供する情報を基に、お客様にて実施をお願いします。

⑥ ISGC の各種設定は、Web の管理画面にて行います。管理画面の対応ブラウザにつきましては、弊社 FAQ サイトに最新情報を掲載しています。
https://www.alsi.co.jp/solution/cybersecurity/isgc/operating/

⑦ アクセスログは、日次で専用のログダウンロードサイトへ保存されます。管理画面では、過去 3 日分のダウンロード、および当日分（直近のログ）を最大 10,000 行まで確認することができます。

⑧ アクセスログには、日付、時刻、プロトコル、接続元 IP アドレス、アカウント、カテゴリ、リクエスト URL 等が記録されます。詳細につきましては、弊社 FAQ サイトをご確認ください。

ISGC Agent … https://alsifaq.dga.jp/faq_detail.html?id=5233

ISGC assist / プロキシ接続 … https://alsifaq.dga.jp/faq_detail.html?id=5168

⑨ ISGC の注意・制限事項の詳細は弊社 FAQ にて公開しています。詳細な情報はログイン後閲覧可能なため、予めログイン ID を取得してください。

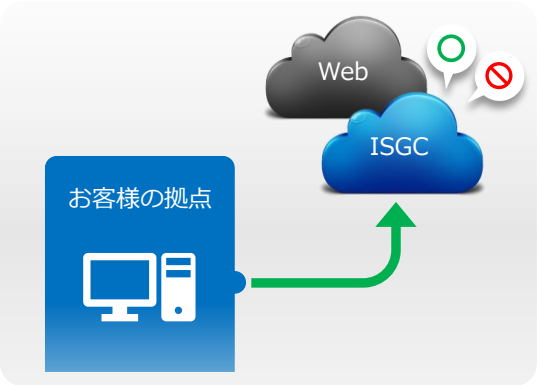
サポートサイト ID 申請サイト　https://www.alsi.co.jp/contact-us/security/supid/

3. ISGC の基本構成

a. 拠点利用 - 社内 LAN から ISGC へ接続

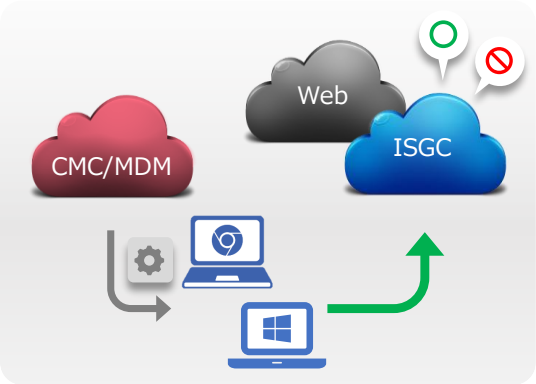
拠点 LAN のゲートウェイから、クラウドの ISGC へプロキシ接続を行う構成です。

拠点からの VPN 接続を利用する場合は、ローカル IP による認証や、ISGC とお客様環境の Active Directory を連携させたアカウント認証も可能です。



b. モバイル利用 - MDM 連携

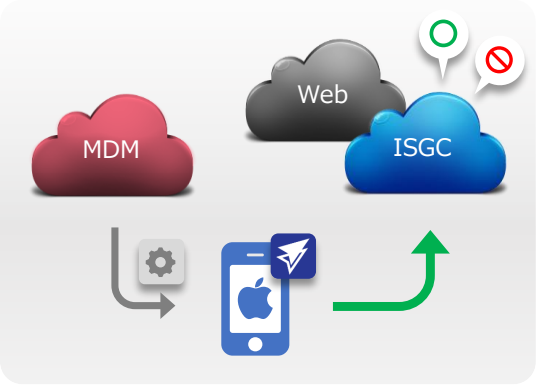
Google 社の Chrome Enterprise（Google 管理コンソール）や MDM（Mobile Device Management）製品で ISGC へ接続するためのプロキシ設定を管理すれば、社内／社外のロケーションを問わず、いつでも ISGC のサービスを利用することができます。



c. モバイル利用 - ISGC assist

Safari 等のアプリの通信を assist で制御し、ISGC へのリクエスト転送もしくは直接 Web サイトに転送します。

MDM（Mobile Device Management）製品等で ISGC へ接続するための設定を管理すれば、社内／社外のロケーションを問わず、いつでも ISGC のサービスを利用することができます。



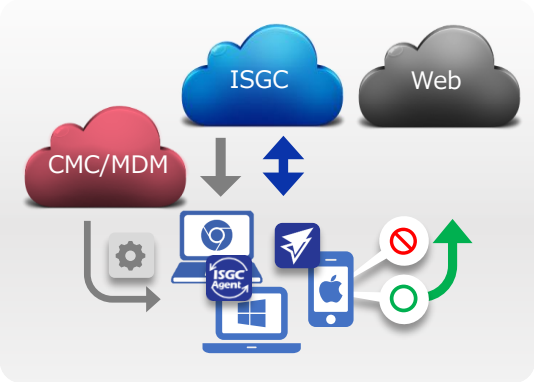
d. モバイル利用 - ISGC Agent

Chrome 等のアプリが Web サイトへアクセスするタイミングで、Agent がその通信をインターセプトしクラウドの ISGC へリクエストを転送します。

ISGC から応答されたフィルタリング判定を基に、Agent が Web アクセスの許可／規制を制御するため、プロキシの設定管理は必要ありません。

e. スクールライセンス - 教育機関向けデバイス

Google 社の Chrome Education（Google 管理コンソール）や MDM（Mobile Device Management）製品を利用して設定を管理すれば、校内／校外のロケーションを問わず、いつでも ISGC のサービスを利用することができます。



※その他の構成をご希望の場合は、弊社営業までご相談ください。

a. 拠点利用 – 社内 LAN から ISGC へ接続

ISGC への接続	プロキシ接続方式	VPN 接続方式
IP アドレス認証	○	任意
対象となる IP	(拠点のグローバル IP)	デバイスのローカル IP
アカウント認証	任意	任意（下記いずれかの方式）
Basic 認証	○	○
NTLM 認証	-	○
Kerberos 認証	-	○
対応デバイス（OS）	Windows iOS iPadOS Android ChromeOS	

※ 対応デバイス毎にプロキシ接続/認証の設定方法や対応状況が異なります。詳細は本章および「7.注意・制限事項」をご参照ください。

i. 拠点からのプロキシ接続

プロキシ接続方式		ISGC へ接続するためのプロキシ設定を、拠点 LAN のゲートウェイ（ルーター/プロキシサーバなど）または、自動構成スクリプト等を利用して個々のデバイスに適用してください。 ※ 接続先のアドレスとポート番号は、ご契約時にご提供します。 ※ 第三者による ISGC への不正アクセスを防止するため、接続元となる拠点のグローバル IP を固定する必要があります（接続元 IP によるアクセス制限を実施）。
IP アドレス認証		拠点内の全てのデバイスが同じグローバル IP を用いて ISGC へ接続するため、IP で個々のデバイス（利用者）を識別することはできません。
アカウント認証	Basic 認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※ 認証情報は Base64 形式の平文で ISGC へ送信されます。

ii. 拠点からの VPN 接続

VPN 接続方式

お客様環境のゲートウェイに VPN 機器を設置し、LAN と ISGC を IPsec で接続する構成です。

暗号アルゴリズム：	AES128
ハッシュ関数：	SHA1
PFS の DH グループ：	2（modp1024）または 5（modp1536）
IPSEC フェイズ 1 鍵有効時間：	28800[s]
IPSEC フェイズ 2 鍵有効時間：	1800[s]
IKE キープアライブ DPD 設定：	有効（インターバル 15[s], タイムアウト 30[s]）
ISGC 側のアクセスポイント：	1 個
ISGC で使用するローカル IP：	最大 16 個（/28）
接続元グローバル IP：	1 個（固定）
接続元ネットワークアドレス：	最大 4 個

※ 接続先のポート番号は、ご契約時にご連絡します。

※ ISGC で使用するローカル IP は、サービス開始時にご連絡します。この IP は、お客様環境の機器と重複しないように運用していただく必要があります。

IP アドレス認証

拠点内のデバイスが VPN 経由で ISGC へアクセスするため、ローカル IP によるデバイス（利用者）の識別も可能です。ISGC 管理画面で IP アドレスのグループ分けを行うことで、デバイス毎のポリシー変更やログ分析が可能になります。

アカウント認証

ISGC にアカウントを登録： Basic 認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。
お客様環境の LDAP サーバと連携： Basic, NTLM, Kerberos 認証	ISGC 側から VPN 経由で LAN 内のサーバへ接続することができるため、お客様環境の LDAP サーバと連携したアカウント認証が可能です。

連携対象となる LDAP サーバ

- Active Directory
  Windows Server 2008 (SP2 推奨), Windows Server 2008 R2 (SP1 推奨) ,
  Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
- OpenLDAP 2.4.35
- Oracle Directory Server Enterprise Edition 11 g R2

※ Windows Server 2008,Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 および Windows Server 2016 では、Active Directory ドメインサービス（AD DS）が必要です。Active Directory ライトウェイトディレクトリサービス（AD LDS）には対応していません。

※ NTLM 認証および Kerberos 認証は Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 が対応しています。

b. モバイル利用 – MDM 連携

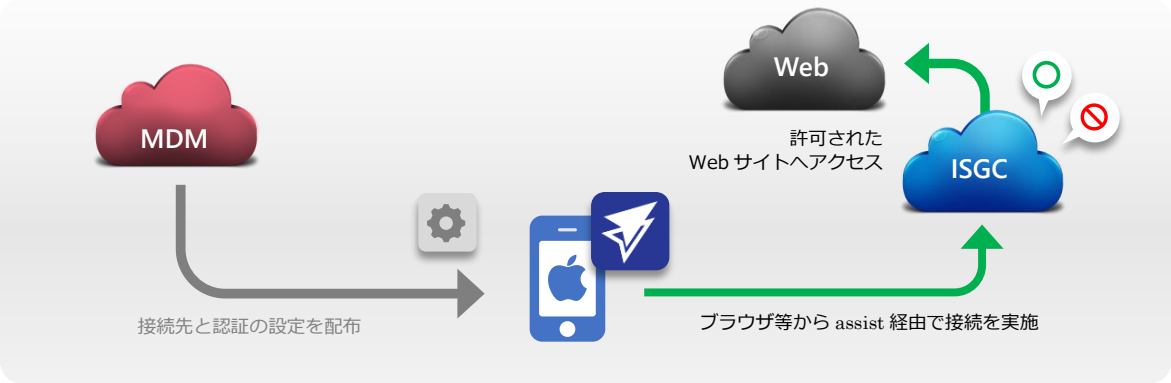
ISGC への接続	プロキシ接続方式
アカウント認証	必須（Basic 認証）
対応デバイス（OS）	Windows　　ChromeOS

※　対応デバイス毎にプロキシ接続/認証の設定方法や対応状況が異なります。詳細は本章および「7.注意・制限事項」をご参照ください。

i. デバイスからの接続

プロキシ接続		MDM（Mobile Device Management）製品等で ISGC へ接続するための設定を管理すれば、社内／社外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 ※　接続先情報は、ご契約時にご連絡します。 ※　第三者による ISGC への不正アクセスを防止するため、プロキシ接続時のアカウント認証が必須となります。平文で情報が送信される Basic 認証をご利用になる場合は、事前に追加規約への同意が必要となります。
アカウント認証	Basic 認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※　認証情報は Base64 形式の平文で ISGC へ送信されます。 ※　ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により表示されていない場合があります）

c. モバイル利用 - ISGC assist



ISGC への接続	独自接続方式
アカウント認証	必須（独自認証方式）
対応デバイス（OS）	iOS　iPadOS　Android

※　ISGC assist では利用における注意事項があります。詳細は「7.注意・制限事項」をご参照ください。

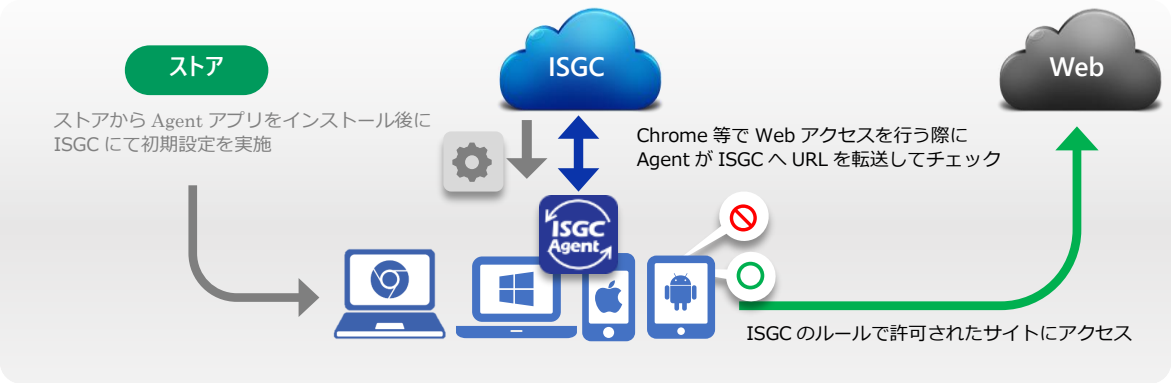
i. デバイスからの接続

ISGC assist		MDM（Mobile Device Management）製品で assist アプリの配布、ISGC へ接続するための設定を管理すれば、社内／社外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 Safari 等のアプリの通信を assist で制御し、ISGC へのリクエスト転送もしくは直接 Web サイトに転送します。 ※　MDM 製品より配信する接続先情報は、ご契約時にご連絡します。
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※　認証時の通信は HTTPS で暗号化されます。 ※　ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により表示されていない場合があります）

ii. フィルタリングキャンセラ

フィルタリングキャンセル URL	ISGC assist とフィルタリング専用サーバを組み合わせて運用する場合には、フィルタリングキャンセラを導入します。 フィルタリングキャンセラを導入すると、社内では既に設置済みのプロキシサーバでフィルタリングを行い、社外へ持ち出したときはフィルタリングを行います。 フィルタリング機能は、自動的に有効／無効が切り替わります。	
準備物	Web サーバ	お客様にて導入環境に Web サーバをご用意ください。 ※　フィルタリングキャンセラは Web 認証に非対応です。
	HTML ファイル	ユーザ様専用ダウンロードサイトより専用 HTML ファイルを取得してください。 ※　HTML ファイルの内容は変更しないでください。
	プロキシサーバ	プロキシサーバをご用意ください。 ※　ISGC assist で利用する場合は、透過プロキシは利用できません。

d. モバイル利用 - ISGC Agent



ISGC への接続	独自接続方式
アカウント認証	必須（独自認証方式）
対応デバイス（OS）	Android　Windows　ChromeOS

※　対応デバイス毎に導入方法が異なります。詳細は後述をご参照ください。

※　導入時期に応じて Windows のアップデート方法が異なります。詳細は「7.注意・制限事項」をご参照ください。

※　ISGC Agent の利用おける注意事項があります。詳細は「7.注意・制限事項」をご参照ください。

※　Agent Android 版は 2025 年 6 月に新規販売を終了しました。

i. Android からの接続

ISGC Agent		ストアからインストールした Agent アプリに認証情報（ライセンスとアカウント）を適用するため、利用開始時に各デバイスで初期設定をすれば、社内／社外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 利用開始後は、ブラウザ等のアプリが Web サイトへアクセスするタイミングで、Agent が通信をインターセプトし、クラウドの ISGC へリクエストを転送します。ISGC から応答されたフィルタリング判定結果を基に、Agent が Web アクセスの許可／規制を制御します。
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※ 認証時の通信は HTTPS で暗号化されます。 ※ ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により表示されていない場合があります）

ii. Windows からの接続

ISGC Agent		管理画面から取得したインストーラでインストール後、利用開始時に初期設定をすれば、社内／社外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 コマンドオプションを使用することで、アカウントの自動登録かつ指定グループへの登録が可能です。 利用開始後は、ブラウザ等のアプリが Web サイトへアクセスするタイミングで、Agent が通信をインターセプトし、クラウドの ISGC へリクエストを転送します。ISGC から応答されたフィルタリング判定結果を基に、Agent が Web アクセスの許可／規制を制御します。
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※ 設定ファイルで初期設定した場合、認証情報は管理画面で作成した任意のアカウントを利用します。 ※ コマンドオプションで導入した場合、認証情報は導入時のデバイス名（コンピュータ名）を利用します。 ※ 認証時の通信は HTTPS で暗号化されます。 ※ ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により表示されていない場合があります）

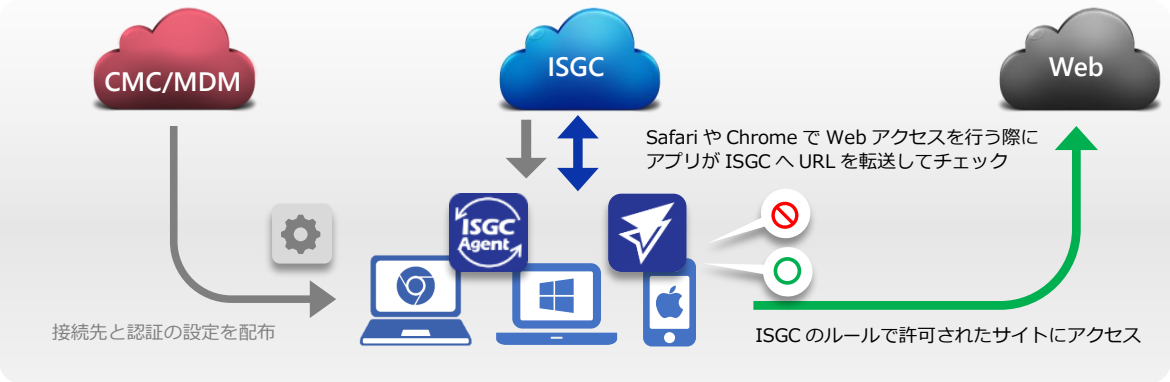
iii. ChromeOS からの接続

ISGC Agent	Google 社の Chrome Enterprise（Google 管理コンソール）を利用して Agent を配布管理すれば、社内／社外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 利用開始後は、Chrome ブラウザが Web サイトへアクセスするタイミングで、Agent が通信をインターセプトし、クラウドの ISGC へリクエストを転送します。ISGC から応答されたフィルタリング判定結果を基に、Agent が Web アクセスの許可／規制を制御します。	
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※ 認証情報は G Suite アカウントを利用します。 ※ 認証時の通信は HTTPS で暗号化されます。 ※ ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により表示されていない場合があります）

iv. フィルタリングキャンセラ

フィルタリングキャンセル URL	ISGC Agent とフィルタリング専用サーバを組み合わせて運用する場合には、フィルタリングキャンセラを導入します。 フィルタリングキャンセラを導入すると、社内では既に設置済みのプロキシサーバでフィルタリングを行い、社外へ持ち出したときはフィルタリングを行います。 フィルタリング機能は、自動的に有効／無効が切り替わります。 ※ ISGC Agent は Windows 版および ChromeOS 版で利用可能です。	
準備物	Web サーバ	お客様にて導入環境に Web サーバをご用意ください。 ※ フィルタリングキャンセラは Web 認証に非対応です。
	HTML ファイル	ユーザ様専用ダウンロードサイトより専用 HTML ファイルを取得してください。 ※ HTML ファイルの内容は変更しないでください。
	プロキシサーバ	プロキシサーバをご用意ください。

e. スクールライセンス - 教育機関向けデバイス



ISGC への接続	独自接続方式
アカウント認証	必須（独自認証方式）
対応デバイス（OS）	iOS　iPadOS　Windows　ChromeOS

※　スクールライセンスは GIGA スクールライセンスも含まれます。

※　対応デバイス毎に利用するアプリ、導入方法が異なります。詳細は後述をご参照ください。

※　スクールライセンスでは Web フィルタリングの一部機能を利用できません。詳細は「7.注意・制限事項」をご参照ください。

※　ISGC assist および ISGC Agent の利用おける注意事項があります。詳細は「7.注意・制限事項」をご参照ください。

i. iOS および iPadOS からの接続

ISGC assist		MDM（Mobile Device Management）製品で assist アプリの配布、ISGC へ接続するための設定を管理すれば、校内／校外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 利用開始後は、Safari 等のアプリが Web サイトへアクセスするタイミングで、Agent が通信をインターセプトし、クラウドの ISGC へリクエストを転送します。ISGC から応答されたフィルタリング判定結果を基に、Agent が Web アクセスの許可／規制を制御します。 ※　MDM 製品より配信する接続先情報は、ご契約時にご連絡します。
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※　認証時の通信は HTTPS で暗号化されます。 ※　ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により選択不要の場合があります）

ii. Windows からの接続

ISGC Agent		管理画面から取得したインストーラでインストール後、利用開始時に初期設定をすれば、校内／校外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 コマンドオプションを使用することで、アカウントの自動登録かつ指定グループへの登録が可能です。 利用開始後は、ブラウザ等のアプリが Web サイトへアクセスするタイミングで、Agent が通信をインターセプトし、クラウドの ISGC へリクエストを転送します。ISGC から応答されたフィルタリング判定結果を基に、Agent が Web アクセスの許可／規制を制御します。
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※ 設定ファイルで初期設定した場合、認証情報は管理画面で作成した任意のアカウントを利用します。 ※ コマンドオプションで導入した場合、認証情報は導入時のデバイス名（コンピュータ名）を利用します。 ※ 認証時の通信は HTTPS で暗号化されます。 ※ ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により選択不要の場合があります）

iii. ChromeOS からの接続

ISGC Agent		Google 社の Chrome Education（Google 管理コンソール）を利用して Agent を配布管理すれば、校内／校外のロケーションを問わずいつでも ISGC のサービスを利用することができます。 利用開始後は、Chrome ブラウザが Web サイトへアクセスするタイミングで、Agent が通信をインターセプトし、クラウドの ISGC へリクエストを転送します。ISGC から応答されたフィルタリング判定結果を基に、Agent が Web アクセスの許可／規制を制御します。
アカウント認証	独自認証	アカウント名を ISGC 管理画面に登録してグループ分けを行うことで、利用者毎のポリシー変更やログ分析が可能になります。 ※ 認証情報は G Suite アカウントを利用します。 ※ 認証時の通信は HTTPS で暗号化されます。 ※ ISGC 管理画面上では、アカウント認証の方式に「Basic 認証」を選択してください。（ご利用の環境により選択不要の場合があります）

iv. フィルタリングキャンセラ

フィルタリングキャンセル URL		ISGC Agent と ISGC assist、フィルタリング専用サーバを組み合わせて運用する場合には、フィルタリングキャンセラを導入します。 フィルタリングキャンセラを導入すると、校内では既に設置済みのプロキシサーバでフィルタリングを行い、校外へ持ち出したときはフィルタリングを行います。 フィルタリング機能は、自動的に有効／無効が切り替わります。 ※　ISGC Agent は Windows 版および ChromeOS 版で利用可能です。
準備物	Web サーバ	お客様にて導入環境に Web サーバをご用意ください。 ※　フィルタリングキャンセラは Web 認証に非対応です。
	HTML ファイル	ユーザ様専用ダウンロードサイトより専用 HTML ファイルを取得してください。 ※　HTML ファイルの内容は変更しないでください。
	プロキシサーバ	プロキシサーバをご用意ください。 ISGC assist で利用する場合は、透過プロキシは利用できません。

4. Web フィルタリングサービス

a. HTTPS デコード

i. ご利用になる前に

HTTPS デコードを利用する際のリスクについて、予めサービス利用規約をお読みいただき、お客様ご自身で、妥当性、必要性、リスクおよび効果を充分に検討し、適切であると判断いただいた上でご利用ください。

ii. 機能概要

HTTPS デコードは、暗号化された HTTPS 通信を解析し、フィルタリングを実施します。HTTPS デコードを有効にした場合のみ、HTTPS 通信のドメイン部以降のディレクトリやファイル名まで含めたフィルタリングが可能です。

従来のドメイン単位フィルタリング

https://www.alsi.co.jp/homepage https://www.alsi.co.jp/webmail https://www.alsi.co.jp/job https://www.alsi.co.jp/bbs	カテゴリ判定不可 一律、IT カテゴリ	許可	“/”（スラッシュ）以下が判断できず、すべて同一のフィルタリングポリシーとなる。

HTTPS デコードを利用

https://www.alsi.co.jp/homepage	ホームページサービス	許可	“/”（スラッシュ）以下をそれぞれ異なるカテゴリで判断できるため、異なるフィルタリングポリシーが設定可能
https://www.alsi.co.jp/webmail	コミュニケーション	規制	
https://www.alsi.co.jp/job	就職・転職	警告	
https://www.alsi.co.jp/bbs	掲示板	許可	

HTTPS サイトにデータを送信したことを判断でき、書き込み操作やデータアップロードを禁止することが可能です。

5. オプションサービス

a. 導入支援サービス

i. 概要

導入支援サービスは、本契約済みのお客様が ISGC を導入する上で、ISGC の設定提案や同居アプリケーションの調査を実施します。

本サービスは 100 ライセンス以上を契約済み、かつ契約開始前のお客様が対象となります。最長 1 ヶ月の作業期間となるため、契約開始月 1 ヶ月前より実施できるよう、充分な期間をご準備ください。

ii. 導入支援の作業内容

本サービスでは、お客様もしくは販売店様に対して、弊社技術員が問い合わせ窓口を介して対応します。オンサイト対応は本サービスの対象外です。

本サービスでは、お客様もしくは販売店様で実施いただく作業があります。

■ 弊社技術員の作業内容

① お客様もしくは販売店様へのヒアリングシート送付

お申し込み時に申請いただいた連絡先へヒアリングシートを送付します。

② ISGC 側の設定提案・反映、利用サイトやアプリケーションの調査

記載済みヒアリングシートを基に、弊社技術員が作業します。作業期間中、お客様へ内容確認のためのご連絡をする場合があります。

ISGC 管理画面でグループ/ユーザの登録、フィルタリングルールの設定を完了後、調査を実施します。調査時にフィルタリングルールの追加・変更を実施する場合があります。

※ 利用サイト、アプリケーションの調査結果は通信除外リストにてご案内します。

※ 弊社環境で確認できない利用サイトおよびアプリケーションの調査は対象外です。

※ 調査期間は 1～5 営業日程度となりますが、作業内容により時間を要する場合があります。

③ デバイスのキッティング時に必要な情報の送付

ISGC 管理画面の設定情報、デバイスのキッティング時に必要な設定情報をご案内します。キッティング時の設定情報は、MDM 製品等の連携を行っている場合に、連携先で指定する設定情報となります。

※ MDM 製品側に登録する ISGC の設定情報の送付が対象となります。MDM 製品側の操作案内は行っておりません。

■　弊社技術員の対象外作業内容

① ヒアリングシートの記載

ISGC 管理画面のグループ/ユーザの情報やカテゴリ設定や例外 URL 設定などのフィルタリングルール、利用サイトの URL 情報、アプリケーション情報を記載してください。

② MDM 製品等の他社製品の設定作業

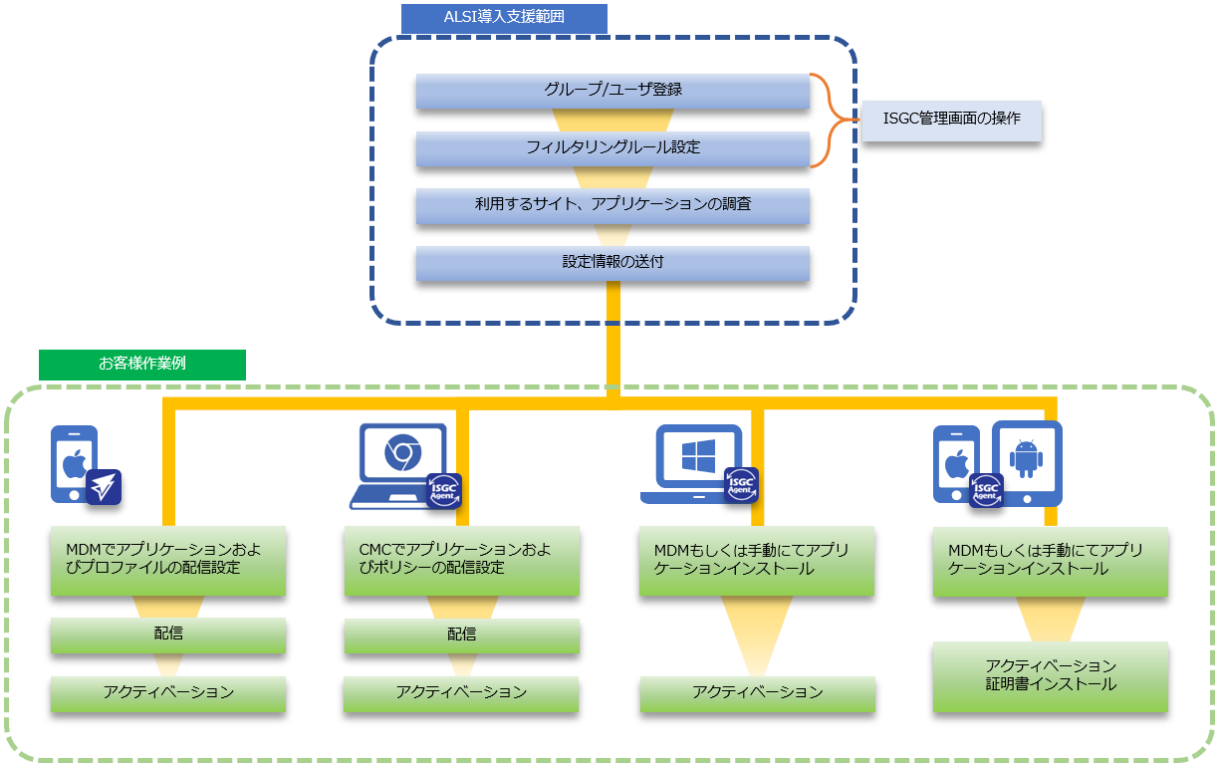
サービス証書や初期設定手順書、調査結果を参考に、連携先となる MDM 製品等の設定作業を実施してください。

③ 検証デバイスでの動作確認

導入デバイスに適用する前に、検証デバイスでキッティングを実施し、フィルタリング動作や利用サイト、同居アプリケーションが正常に動作するかをご確認ください。

④ デバイスのキッティング作業

動作確認が完了後、導入デバイスに対してキッティング作業を実施してください。



iii. 導入支援の流れ

本サービスは、以下の流れで実施します。

	作業担当	作業内容
1.	弊社技術員	弊社技術員からヒアリングシートをメールにて送付します。
2.	お客様	ISGC の設定情報、運用開始後の利用サイトやアプリケーションの情報をヒアリングシートに記入し、メールにて送付します。
3.	弊社技術員	ISGC 管理画面からの設定反映、利用サイトやアプリケーションの調査をします。
4.	弊社技術員	デバイスのキッティング時に必要な情報を送付します。
5.	お客様	送付情報を参考にフィルタリングや利用サイト、アプリケーションを動作確認します。
6.	お客様	導入デバイスのキッティング作業をします。
7.	弊社技術員	運用開始（契約開始）のタイミングで導入支援を終了します。

※　ヒアリングシート送付後、5 営業日以降もご連絡をいただけない場合は本サービスを終了します。終了時の案内はございません。

iv. 問い合わせ

本サービスを利用している際の問い合わせ窓口は、技術サポート窓口と共通です。個別の問い合わせ窓口の設置、受付時間の変更は行いません。

本サービスの終了後、製品についての問い合わせは技術サポートにて対応します。

b. ログ長期保管サービス

i. 概要

ログ長期保管サービスは、基本サービスである「ログ保管サービス」の保管期間を 365 日へ延長するサービスです。

c. ダッシュボードサービス

i. 概要

ダッシュボードサービスは、InterSafe GatewayConnection からアクセスログを自動で取り込み、簡単操作で Web アクセスの状況や傾向、端末の利用状況をレポート表示することができるクラウドサービスです。（教育委員会・学校法人向け）

ii. 機能概要

1. 自動取り込み：InterSafe GatewayConnection のアクセスログを自動で取り込みます。
2. 各種レポート機能：アクセスサマリー、日別レポート、時間帯別レポート等、様々な形式のレポートでアクセスログを可視化します。

※その他詳細機能及び注意事項については、InterSafe GatewayConnection ダッシュボードサービス のマニュアルをご参照ください。 https://netstar-inc.github.io/isgc-dashboard-manual/

iii. 問い合わせ

本サービスを利用している際の問い合わせは技術サポート窓口と共通です。

d. Microsoft365 ドメイン配信サービス

i. 概要

Microsoft365 ドメイン配信サービスは、Web サービスである Microsoft365 を利用する際にフィルタリング許可が必要なドメイン情報を定期的にメール配信で提供します。

ii. 配信の内容

メール配信では Microsoft365 全てのアプリケーションで利用しているドメイン、および Microsoft365 で定めているサービス分類別でのドメイン情報の 2 種類を提供します。

提供するドメイン情報は前回提供したドメイン情報の差分情報も含まれます。

また、ドメイン情報は管理画面の設定である、アプリポリシー設定の「フィルタリング無効ホスト」や ISGC assist の「PAC_BYPASS_HOST」もしくは「PROXY_BYASS_HOST」の登録形式に合わせた形で提供します。

iii. 問い合わせ

本サービスを利用している際の問い合わせは技術サポート窓口と共通です。

e. アクセス制限オプション

i. 概要

アクセス制限オプションは、ISGC に関する IP アドレスの情報を提供、または ISGC への接続 IP アドレスを制限するサービスです。

ii. 問い合わせ

本サービスを利用している際の問い合わせは技術サポート窓口と共通です。

f. 帯域拡張オプション

i. 概要

帯域拡張オプションは、標準提供の帯域を上位プランへアップグレードするサービスです。一部通信先を除き、除外対応が不要となります。

ii. 問い合わせ

本サービスを利用している際の問い合わせは技術サポート窓口と共通です。

g. VPN 構成オプション

i. 概要

VPN 構成オプションは、VPN 接続により組織内のネットワークと同等に接続可能になるサービスです。

※本サービスは、新規構築時の同時申込みが条件となります。

ii. 問い合わせ

本サービスを利用している際の問い合わせは技術サポート窓口と共通です。

6. 連携ツール

a. ログ分析/レポートツール InterSafe LogNavigator

i. 製品概要

InterSafe LogNavigator は、InterSafe GatewayConnection からアクセスログを自動で取り込み、簡単操作でログ検索・レポート表示することができるログ分析ソフトです。

ii. 機能概要

1. 自動取り込み：InterSafe GatewayConnection のアクセスログを自動で取り込みます。
2. 各種レポート機能：ユーザレポート、デイリーレポート、ドリルダウンレポート等、様々な形式のレポートでアクセスログを可視化します。
3. アラート警告機能：しきい値を設定して、アラート警告を行います。
4. アクセスログ検索：アクセスログを様々な条件で検索します。
5. 自動レポート送信：一部のグラフレポートにて、メールによる自動配信を行います。

※その他詳細機能及び注意事項については、InterSafe LogNavigator のマニュアルをご参照ください。

iii. 問い合わせ

本ツールを利用している際の問い合わせは技術サポート窓口と共通です。

7. 注意・制限事項

a. サービス全般

i. Web アクセス

1. 提供する情報や設定ファイルなどは、お客様固有の情報を含みます。第三者へ提供しないようご留意ください。
2. 提供サービスを利用する場合、各構成で ISGC の CA 証明書をクライアントにインストールする必要があります。
3. 拠点、モバイル利用でのプロキシ接続および ISGC assist で利用する場合、「ISGC 管理画面」、「イントラサイト」、「大量のトラフィックが発生する Web サービス」、「OS がバックエンドで行うシステム通信」および、ISGC の通信制御処理でエラーとなるサイトのアドレスは、下記の設定でフィルタリングの処理対象から除外してください。
   除外設定の詳細につきましては、弊社 FAQ サイト（要ログイン）をご参照ください。 http://support.alsi.co.jp/

   - フィルタリングの対象外とするサイト ⇒ ISGC へ接続する機器のプロキシ例外
     または ISGC assist の「PAC_BYPASS_HOST」
   - フィルタリング処理に伴う通信エラー ⇒ ISGC へ接続する機器のプロキシ例外
     または ISGC assist の「PAC_BYPASS_HOST」
   - プロキシ認証処理に伴う通信エラー ⇒ ISGC へ接続する機器のプロキシ例外
     または「リクエスト別認証設定」
   - HTTPS デコード処理に伴う通信エラー ⇒ 「HTTPS デコード除外設定」

   ※ Web 通話サービスやストレージサービス、Windows Update、iOS Update などの通信は大量のトラフィックが発生します。予めフィルタリング対象外となるようにしてください。

   ※ プロキシ例外は、お客様環境のファイアウォール、プロキシ、または個々のデバイスにて行う設定です。個々のデバイスへのプロキシ例外設定には、プロキシ自動設定（PAC）の使用を推奨します。

   ※ iOS 版の ISGC Agent アプリでは、OS の仕様に合わせて通信処理性能が制限されるため、画像や動画のコンテンツが多数掲載された Web ページ等で接続数超過によるアクセスエラーが起こる場合があります。iOS が Apple 社のサーバへ接続するシステム通信や、よく閲覧される Web サイト等の IP 除外を推奨します。
4. 「ヘッダ編集設定」は Web ブラウザでアクセスした際に、Web サービスのアクセス制御が行われることを確認しております。Web サービス専用のアプリケーションでは正常に動作しない場合があります。
5. 本サービスを利用すると、通信に対して様々なフィルタリング処理を適用するため、利用前に比べて通信速度が低下します。また、HTTPS デコード設定等のお客様の適用する各種設定やご利用の OS によっても影響の度合いが異なります。
   しかしながら各種設定を適用した場合も、ご利用のネットワークが十分な速度を確保できていれば、一般的な Web 利用や動画視聴等は問題なくご利用いただけます。
   なお、高速通信が必要な特定のサイトやサービスにおいて影響がある場合で、フィルタリング処理やアクセスログの取得が不要であれば、フィルタリング処理の除外設定を使用して、高速通信を確保することも可能です。
6. 検索キーワード設定、書き込みキーワード設定では、GET / POST データに対してキーワードマッチングを行うため、ユーザが検索 / 書き込んだ内容以外でも GET / POST データにキーワードが含まれると制御対象及びアラートメールが送信されますのでご注意ください。

ii. HTTPS デコード

1. HTTPS デコード有効時、Web アクセスのパフォーマンスが低下する可能性があります。
2. 独自通信を利用するサイトやクライアント証明書を利用するサイト、デバイス管理ツールの通信は正常に動作しません。「除外ホスト設定」機能を使用して、対象通信を対象から除外してください。
3. デバイスにインストールされている他社製品が正常に動作しない場合があります。「除外ホスト設定」機能を使用して、対象通信を対象から除外してください。

iii. クラウドプラットフォーム

1. 本サービスは冗長構成にて提供しておりますが、万一の障害発生時はサーバ切替えに伴う通信断が発生します。
2. サーバリソースの枯渇等でパフォーマンス改善が必要となった場合は、緊急メンテナンスの実施に伴う通信断が発生します。
3. 基本構成の帯域は共有型の 100Mbps ベストエフォートでの提供となり、トラフィック急増時等にアクセス遅延が起こる場合があります。
4. ISGC 側の帯域状況により、事前告知なしで帯域制限もしくは特定宛先へのアクセス制限を実施する場合があります。

   過度な帯域利用（転送量）が確認された際には、過多となった通信先のフィルタリング除外設定を案内します。

   案内後も改善が見られない場合には、超過分の請求、契約ライセンスの見直しを実施する場合があります。

iv. その他

1. アカウント名とパスワードは 64 文字以内の半角英数字で入力してください。下記の半角記号も使用できます。（ご利用の環境により入力可能文字数が異なる場合があります。）

   ! # $ % & ' ( ) = ` ~ { + } _ - ^ @ . * / < > |
2. ISGC の導入時、MDM 製品や Google 管理コンソールなどの管理ツールを利用する場合、他社製品の機能および設定方法についての問い合わせはサポート対象外となります。
3. 管理画面は Google Chrome、Microsoft Edge(Chromium 版)に対応しています。
4. ログファイルのダウンロードは、事前にメールアドレスを登録する必要があります。詳細は「ログダウンロードマニュアル」をご参照ください。
5. Youtube エクスポーターで抽出した URL や YouTube チャンネル ID または Youtube ビデオ ID を例外 URL 設定の規制対象として登録した場合、規制対象の動画のサムネイルにカーソルを合わせるとサムネイル上で映像のみが再生されてしまいます。
6. Youtube エクスポーターで抽出した URL や YouTube チャンネル ID を例外 URL 設定の規制対象として登録した場合、Youtube サイト上の検索での遷移や再生リスト経由で規制対象の動画が再生できてしまいます。
7. HTTP リクエストが発生しない場合、フィルタリングによる判定は行われません。例えば、アンカー付きのリンクで同ページ内を移動した場合は Web サイトに対して HTTP リクエストが発生しないためフィルタリングが行われずアクセス可能となります。

b. プロキシ対応状況

i. Windows

1. ISGC に接続するブラウザの動作実績は以下の通りです。
   - Microsoft Edge（Microsoft）
   - Firefox（Mozilla）
   - Chrome（Google）
2. NTLM 認証を行う場合は、Firefox , Chrome の利用を推奨します。

ii. iOS / iPadOS

1. ISGC に接続するブラウザの動作実績は以下の通りです。
   - Safari（Apple）

   ※ 動作確認は、iPhone, iPad にて実施しています。
2. Wi-Fi のプロキシ設定にて ISGC へ接続した場合の、HTTP および HTTPS プロトコルのみ対象となります。
3. Basic 認証を行う場合、アカウント名とパスワードをデバイスに保存できないため、接続の度にアカウント名とパスワードを手入力する必要があり運用が困難です。

iii. Android

1. ISGC に接続するブラウザの動作実績は以下の通りです。
   - Chrome（Google）
2. Wi-Fi のプロキシ設定にて ISGC へ接続した場合の、HTTP および HTTPS プロトコルのみ対象となります。
3. ユーザ認証を行う場合は、IP アドレス認証の利用を推奨します。

iv. ChromeOS

1. Google 管理コンソールの [Chrome 管理]–[ユーザとブラウザの設定] にて行なったプロキシの設定は、Wi-Fi、モバイルデータ、イーサネット接続のいずれでも有効になります。
2. Google 管理コンソールの [Chrome 管理]–[ユーザとブラウザの設定] にて行なったプロキシの設定は、「デバイス」ではなく「Google アカウント」に対して適用されます

   ※ Chromebook 以外のデバイスで当該の Google アカウントにログインした際も、プロキシの設定が有効になります。プロキシを適用する必要がない場合は、別の Google アカウントを使用してください。

   ※ Chromebook のゲストユーザにはプロキシの設定が適用されません。ゲストユーザによる利用は許可しないことを推奨します。
3. Chrome ブラウザの起動時にプロキシ認証のポップアップが表示されます。認証情報を繰り返し入力させたくない場合は、認証情報を保持するために Google 管理コンソールの [Chrome 管理]–[ユーザとブラウザの設定]–[セキュリティ]でパスワードマネージャを有効にすることを推奨します。

4. Chrome の機能を利用する際に Google 社のサーバと行われる通信が、ISGC の通信制御処理でエラーとなります。ログイン制御を実施するホスト以外の通信先ホストは Google 管理コンソールにて当該のアドレスをプロキシ設定のプロキシバイパスリストに登録してください。

Google 社のサーバと通信する機能の例：

google.com	ポータル
*.google.com	各種サービス
*.googleapis.com	システムコンテンツ
*.google.co.jp	検索ポータル、ニュース
*.youtube.com	YouTube
*.gstatic.com	システムコンテンツ
*.googleusercontent.com	システムコンテンツ
.gvt.com	システムコンテンツ、ビーコン
*.doubleclick.net	システムコンテンツ
*.google-analytics.com	Google Analytics
*.googlevideo.com	システムコンテンツ

c. 拠点利用

1. お客様環境のプロキシサーバ（ISGC の下位プロキシ）で HTTPS デコードを行っている場合、Web アクセス時に SSL 証明書のセキュリティ警告が発生することがあります。お客様環境のプロキシサーバに、ISGC 管理画面からダウンロードした CA 証明書をインストールしてください。

i. 拠点からのプロキシ接続

1. [サーバ管理]－[認証設定] の設定は変更しないでください。
2. お客様環境にプロキシサーバ（ISGC の下位プロキシ）が設置されている場合は、下位プロキシで「x-forwarded-for」を無効に設定し、ISGC へローカル IP が転送されないようにしてください。
3. 同一環境でモバイル利用をする場合、モバイル利用では、IP アドレスでの認証ができないため、アカウント認証用のアカウントを作成して利用してください。
4. 複数拠点（複数のグローバル IP アドレス）からの利用をご希望の場合は、申込書にその旨を記載ください。
5. 接続元として登録可能なグローバル IP は、お客様自身で契約されたアドレスに限ります。同一環境でモバイル利用や ISGC assist、ISGC Agent を利用する場合、IP アドレスでの接続元制限は実施できません。
6. 接続元グローバル IP アドレスによるアクセス制限は、管理画面へのアクセスにも適用されます。拠点外から ISGC の設定管理を行うことはできません。

ii. 拠点からの VPN 接続

1. サービス利用開始後の VPN 接続設定（ネットワーク変更、サーバ IP 変更等）については、技術サポートの対象外となります。

   ※　VPN 接続の設定変更を行う場合は、担当営業までご相談ください。

2. 管理画面へのアクセスも、拠点から VPN 経由で実施してください。拠点外から ISGC の設定管理を行うことはできません（管理画面の Web サービスは HTTP で提供されます）。
3. [サーバ管理]－[認証設定] の「第一階層グループ毎にアカウントの管理をする」の設定は変更しないでください。
4. ISGC にてユーザ認証を行う構成で、お客様環境にプロキシ（ISGC の下位プロキシ）が設置されている場合は、下記の設定を行ってください。

   ISGC で IP アドレス認証を実施　⇒ 下位プロキシから ISGC へ X-Forwarded-For ヘッダを送信

   ISGC で Basic 認証を実施　⇒ 下位プロキシで Basic 認証を実施し、ISGC に認証ヘッダを転送

   ISGC で NTLM／Kerberos 認証を実施　⇒ 下位プロキシではアカウント認証を行わないように設定

5. NTLM／Kerberos 認証を使用する場合、認証結果が一定時間キャッシュされます。1 台の PC を複数のアカウントで共有している環境では、キャッシュ時間を短く設定するなど留意してください。
6. 同一環境でモバイル利用の併用はできません。
7. VPN 接続は 1 拠点のみとなります。複数拠点での接続は実施しません。
8. 弊社クラウド環境とお客様の拠点における VPN 接続は死活監視対象に含まれません。お客様にて実施してください。
9. サービスの利用にはライセンス上限があります。

d. モバイル利用

1. [サーバ管理]－[認証設定] の設定は変更しないでください。
2. IP アドレスでの認証ができないため、アカウント認証用のアカウントを作成してください。
3. アクセスログに出力されるクライアント IP アドレスはプロキシ接続および ISGC Agent ChromeOS 版を除き、一律「0.0.0.0」となります。
4. 予めシステムで利用する通信や業務で利用するコンテンツは除外設定をしてください。
5. 導入デバイスでは接続方式を複数利用ができません。導入デバイスでは ISGC のプロキシ設定と ISGC assist/ISGC Agent の設定を同時に行わないでください。
6. デバイスのキッティングが完了する前に、必ず ISGC 管理画面でアカウント登録をしてください。登録が完了していない場合、一律認証エラーとなり Web アクセスが制限されます。
7. IP アドレスでの接続元制限は実施できません。
8. キッティング完了デバイス一覧に登録されるデバイス情報は、初回キッティング時のみ登録されます。ISGC Agent Windows および ChromeOS の場合は、ユーザ切り替えが発生した際にも登録されます。

   プロキシ接続および ISGC Agent iOS 版、Android 版は対応していません。

i. フィルタリングキャンセラ

1. フィルタリングキャンセラは ISGC assist および ISGC Agent Windows 版、ChromeOS 版が対応となります。
2. フィルタリングキャンセラは Web 認証に対応していません。Web 認証が不要な Web サーバをご用意ください。
3. フィルタリングキャンセラで利用する HTML ファイルは編集しないでください。編集後、正常にフィルタリングキャンセラが動作しない場合があります。
4. フィルタリングキャンセラは ISGC を導入した端末と同一ネットワークに配置する必要はありません。アクセス可能であれば、異なるネットワーク環境の Web サーバで導入することができます。
5. ISGC assist で利用する場合、透過プロキシは対応していません。明示的なプロキシ指定が可能なプロキシサーバをご用意ください。

e. ISGC assist iOS 版

1. iOS および iPadOS の対応バージョンは、原則、最新を含む 2 世代のメジャーバージョンとしております。新しいメジャーバージョンがリリースされた際は、2 ヶ月後を目安に対応を開始します。
2. Wi-Fi および VPN のプロキシ設定と併用はできません。
3. Shared iPad には対応していません。
4. ISGC の IP アドレス情報は公開しておりません。接続先 IP アドレスでアクセス制限を行っている場合、正常に動作しないことがあります。
5. MDM 製品等をご利用の場合、iOS 制限設定（構成プロファイル「Restrictions」ペイロード）で下記の操作が無効化されていると、設定ファイルの展開が行なえません。この制限を解除してからファイルを展開してください。
   - 管理対象外出力先で管理対象ソースからの書類を許可
   - 管理対象出力先で管理対象外ソースからの書類を許可
6. ISGC assist に設定したアカウント情報と管理画面に登録したアカウント情報に差異が生じた場合、ISGC assist での認証が失敗し、認証に失敗した旨のメッセージポップが表示され、ISGC assist が利用できません。

   管理画面でアカウントのパスワードを変更した場合も同様の動作となります。パスワードを変更した際は設定ファイルを再作成し、ISGC assist を再度アクティベーションしてください。
7. ISGC assist のアクティベーションは構成プロファイルの配信前に実施します。アクティベーション前に構成プロファイルを配信した場合、HTTP 通信および HTTPS 通信が強制的に規制される動作となります。

   この動作はアクティベーション後に解消されますが、MDM 通信も規制対象となるため、アクティベーションされるまで MDM 製品のリモート操作ができない状態となります。

   アクティベーション前に構成プロファイルを配信する場合は、必ずコンテンツフィルタ構成プロファイルで MDM 通信の通信先ホストを「PAC_BYPASS_HOST」に登録した上で配信してください。
8. グローバル HTTP プロキシ構成プロファイルで「PAC が到達不能の場合に直接接続を許可」のチェックボックスをオンにした場合、以下の挙動が発生する場合があります。
   - 正規の順序が前後し、グローバル HTTP プロキシ構成プロファイルを初めにインストールすると、フィルタリングが開始されない
   - プロキシ接続に失敗し直接接続を開始した後、一定時間プロキシを参照しない

   機内モード・Wi-Fi・4G の切り替え等でネットワークを切り替えることで再度プロキシを参照するようになります。
9. グローバル HTTP プロキシ構成プロファイルで「PAC が到達不能の場合に直接接続を許可」のチェックボックスをオフにした場合、以下の挙動が発生する場合があります。
   - 単一でグローバル HTTP プロキシ構成プロファイルが適用されている状態で、外部通信が全遮断される
   - ISGC assist のアップデート時に、外部通信が全遮断される
10. ISGC assist が起動完了前のタイミングで通信が発生した場合や ISGC assist が ISGC への接続に失敗した場合、対象の通信はフィルタリング対象外となり、直接接続を行います。以下が起動完了前のタイミングとなります。
    - デバイスの再起動直後
    - ISGC assist の再起動直後
    - デバイスのスリープ復帰直後

    フィルタリング対象外の通信をフィルタリングする（規制する）場合は、以下の設定を検討してください。

    ISGC assist の起動完了前にフィルタリング対象外となる対策
    - グローバル HTTP プロキシ構成プロファイルで「PAC が到達不能の場合に直接接続を許可」のチェックボックスをオフにする

    ISGC assist が ISGC への接続に失敗した際にフィルタリング対象外となる対策
    - コンテンツフィルタ構成プロファイルで「UNREACHED_BLOCK」を設定する

11. Managed App Configuration を利用する場合、MDM 製品で配布する前に、必ず ISGC 管理画面でアカウント登録をしてください。登録が完了していない場合、一律認証エラーとなり Web アクセスが制限されます。

12. Managed App Configuration でアカウント名とパスワードを MDM 製品で任意の文字列に指定する場合、ISGC での入力制限文字を利用しないようにしてください。

13. Managed App Configuration でアカウント名とパスワードを配布した際に、ISGC 管理画面に登録したアカウント情報と差異がある場合、ISGC assist での認証が失敗し、認証に失敗した旨のメッセージポップが表示され、ISGC assist が利用できません。

    ISGC 管理画面のアカウント情報を修正、もしくは MDM 製品側で Managed App Configuration の設定を修正してください。

    ※ MDM 製品の仕様により Managed App Configuration の設定変更後、アプリの再配布が必要な場合もあります。

14. Managed App Configuration を利用する場合、Managed App Configuration の設定情報が優先されます。設定ファイルで設定情報の上書きをすることはできません。

    また、設定ファイルでアクティベーション済みのデバイスは Managed App Configuration での設定を配信した場合、ISGC assist を起動時に上書きされます。

15. iOS13 および iPadOS13 以降、ISGC assist をアクティベーション済みのデバイスにおいて、以下の VPN 方式は VPN 接続に失敗し利用できません。

    - IPsec（IKEv1）
    - L2TP（L2TP/IPsec）

16. iOS13 および iPadOS13 以降で、デバイスの再起動直後に極稀に ISGC assist が停止し、ISGC への接続に失敗する場合があります。現象が確認された場合はデバイスを再起動してください。

17. Apple のポリシーに従い、Ver. 1.1.11 よりアプリ起動後に情報取得の同意が必要となります。以下の場合に情報取得の同意が求められます。同意されるまでフィルタリングは開始されません。

    - 新規キッティング
    - Ver. 1.1.10 以前からアップデート

18. iOS13 および iPadOS13 以降では以下の構成プロファイル設定を無効にしてください。

    - 構成プロファイル「WebContentFilter」ペイロード
        - ソケットトラフィックをフィルタ

    設定が無効となっていない場合、以下の挙動などが発生します。

    - ISGC assist のアプリアップデートに失敗する
    - 社内サイト接続用のクライアント VPN の接続が確立しない

19. Ver. 1.1.11 以前は「アプリポリシー設定」での機能および自動同期に対応していません。

    - 共通設定
    - ISGC assist 設定

20. コンテンツフィルタ構成プロファイルのカスタムデータで指定した設定値を「アプリポリシー設定」で配信する場合は、同期対象をすべての設定に変更してください。

    同期対象の設定でデバイスに反映される対象

    - すべての設定

      共通設定および ISGC assist 設定の設定値がデバイスに反映されます。「SERVICE_PROXY_PORT」および「SERVICE_PORT」は引き続きコンテンツフィルタ構成プロファイルのカスタムデータで指定する必要があります。

    - エージェント設定ファイルに含まれる設定項目は同期しない

      「フィルタリングキャンセル URL」および「フィルタリングキャンセル代替プロキシ」の設定値のみがデバイスに反映されます。

コンテンツフィルタ構成プロファイルの設定値と「アプリポリシー設定」は併用することができません。すでにコンテンツフィルタ構成プロファイルで設定値を指定している場合は、「アプリポリシー設定」へ設定を移行してください。

コンテンツフィルタ構成プロファイルから「アプリポリシー設定」に切り替える場合に、設定移行が必要な項目

- PAC_BYPASS_HOST → PAC バイパスホスト
- PROXY_BYPASS_HOST → フィルタリング無効ホスト
- HIDE_RESTART → 再起動機能
- UNREACHED_BLOCK → クラウド通信不可時動作

21. フィルタリングキャンセラを利用する場合、「フィルタリングキャンセル URL」および「フィルタリングキャンセル代替プロキシ」の両設定が必須となります。「フィルタリングキャンセル代替プロキシ」は明示指定で利用可能なプロキシサーバを指定してください。
22. フィルタリングキャンセラを利用する場合、プロキシサーバ宛の通信は、以下の設定に含まれない宛先が対象となります。

    コンテンツフィルタ構成プロファイルの場合

    - PAC_BYPASS_HOST
    - PROXY_BYPASS_HOST

    アプリポリシー設定の場合

    - フィルタリング無効ホスト
    - PAC バイパスホスト
23. 以下の設定で IPv6 アドレスを登録する場合、完全表記/省略表記を全て記載する必要があります。

    コンテンツフィルタ構成プロファイルの場合

    - PAC_BYPASS_HOST
    - PROXY_BYPASS_HOST

    アプリポリシーの場合

    - フィルタリング無効ホスト
    - PAC バイパスホスト

    例 1) 同一アドレスであるが、すべて登録が必要です。

    [2404::a:0:0:1]　[2404:0:0:0:a::1]　[2404:0:0:0:a:0:0:1]

    例 2）ワイルドカード「*」を使用時もすべて登録が必要です。

    [2404::a:*]　[2404:0:0:0:a:*]
24. ISGC assist iOS の下記バージョンにおいて、フィルタリング無効ホストに以下文字列が含まれていると ISGC assist のサービス起動に失敗し、インターネット通信ができない状態となる場合があります。
    この場合、アプリの再インストールが必要となりますのでご注意ください。
    詳細は弊社 FAQ サイト(http://support.alsi.co.jp/ ※要ログイン)をご参照ください。

    - v1.4.x 以前、v1.5.1
25. 以下の環境ではインターネットにアクセスができないネットワークに接続して利用するアプリやサービスは利用できません。

    - グローバル HTTP プロキシの「PAC 到達不能時の直接接続を許可」しない場合
26. iOS17 以降で、ISGC assist をインストールした直後に iOS 側でサービスを発見/起動までの処理が正しくできず、インターネットに接続できなくなる事象が発生する場合があります。現象が確認された場合はデバイスを再起動してください。
27. 2024 年 9 月 17 日の Jamf Pro のアップデートにより、コンテンツフィルタ構成プロファイルに以下のカスタムデータを指定しても反映されません。

    - UNREACHED_BLOCK

- HIDE_LOG
- HIDE_RESTART

MDM 製品として Jamf Pro を利用している環境で ISGC の管理画面の「アプリポリシー設定」ではなく、構成プロファイルでカスタムデータの指定を行う環境の場合、以下のように設定してください。

・コンテンツフィルタ構成プロファイルのカスタムデータの値に true を指定したい場合は、true および false 以外の値を指定する。

記述例）

UNREACHED_BLOCK = block

HIDE_LOG = hide

HIDE_RESTART＝hide

f. ISGC assist Android 版

1. AndroidOS の対応バージョンは、原則、最新を含む 3 世代のメジャーバージョンとしております。新しいメジャーバージョンがリリースされた際は、3 ヶ月後を目安に対応を開始します。

2. MDM 製品との連携が前提となります。
2025 年 12 月現在、動作確認できているものは下記製品になります。最新情報は FAQ サイトよりご確認ください。
（https://alsifaq.dga.jp/faq_detail.html?id=6106）

   - Microsoft Intune
   - SOTI MobiControl
   - SPPM 3.0
   - ビジネス・コンシェル デバイスマネジメント
   - BizMobile Go!
   - LINC Biz emm
   - OPTiM Biz
   - Workspace ONE

3. ISGC assist に設定したアカウント情報と管理画面に登録したアカウント情報に差異が生じた場合、ISGC assist での認証が失敗し、認証に失敗した旨のメッセージポップが表示され、ISGC assist が利用できません。管理画面でアカウントのパスワードを変更した場合も同様の動作となります。

4. MDM 製品でアプリケーションを配布する前に、必ず ISGC 管理画面でアカウント登録をしてください。登録が完了していない場合、一律認証エラーとなり Web アクセスが制限されます。

5. Managed Configurations でアカウント名とパスワードを配布した際に、ISGC 管理画面に登録したアカウント情報と差異がある場合、ISGC assist での認証が失敗し、認証に失敗した旨のメッセージポップが表示され、ISGC assist が利用できません。ISGC 管理画面のアカウント情報を修正、もしくは MDM 製品側で Managed Configurations の設定を修正してください。

6. Wi-Fi 接続直後は www.google.com へのアクセスが数秒間許可され、その後はポリシーに応じて制御されるようになります。これは Android の仕様により当該 URL にアクセスが必要なためです。予めご了承ください。

7. フィルタリングキャンセラ機能を利用時、予め指定したキャンセル URL へアクセスできる社内/構内環境において、何らかの障害により代替プロキシサーバが応答しないような場合は、タイムアウトまで接続を試みるため、Web サイトへアクセスするまでに数分程度時間がかかる場合があります。

8. ISGC assist Android がインストールされている環境では、Web 認証を行う公共交通機関や商業施設などの公衆 Wi-Fi へ接続する際は、予め Web 認証の接続先ホストをフィルタリング無効ホストに登録しておく必要があります。なお、Wi-Fi サービスによってはローカル IP を登録しないと回避できない場合があり、その場合はご利用になれませんので予めご了承ください。
※Web 認証とは、Wi-Fi サービスに接続する際に表示される Web 画面での認証や利用登録を指します。

g. ISGC Agent

1. ISGC Agent では「フィルタリングバイパス設定」は利用できません。（プロキシ接続／VPN 接続向けの機能です）
2. ISGC Agent のみ利用する場合は、下記の機能を利用できません。
   - Geo スコープ
   - HTTPS デコード機能の除外カテゴリ設定, パス部ログ出力設定
   - 例外 URL 自動削除
   - クライアント IP アドレス制限
   - ログ設定
3. ISGC Agent のみ利用する場合は、下記の機能が有効状態で提供されます（無効化および設定値の変更はできません）。
   - 高度分類クラウド（IWCC）　※ 当該のアクセスログはカテゴリ名に[IWCC]を付与
   - HTTP 接続禁止ポート設定　※ 25, 110 ポートへの接続を禁止
   - リクエスト別認証設定　※ OS の行うシステム通信の一部などをルートグループで認証
4. 違反検知時に管理者へ送信するアラートメールの宛先は 1 件のみ設定できます。複数名でアラートを受信する場合はメーリングリスト等を使用してください。
5. ISGC の IP アドレス情報は公開しておりません。接続先 IP アドレスでの制限している場合、正常に動作しないことがあります。
6. ご利用の環境により、以下の事象が発生する場合があります。
   - 管理画面や規制画面 URL がアクセスログに出力される
   - 規制画面の「あなたがリクエストした URL」に規制画面 URL が表示される
7. Web 認証を行う公共交通機関や商業施設など公衆 Wi-Fi へ接続する際に、予め Web 認証の接続先ホストをフィルタリング無効ホストに登録しておく必要があります。なお、Wi-Fi サービスによってはローカル IP を登録しないと回避できない場合があり、その場合はご利用になれませんので予めご了承ください。
   ※Web 認証とは、Web 画面で認証や利用登録を行う必要がある Wi-Fi サービスを指します。

i. Android 版の Agent

1. デバイスに Wi-Fi のプロキシ設定がある場合でも、ISGC Agent が行う通信はプロキシを経由しません。
2. ISGC 管理画面から取得した設定ファイルを Web ポータル等のサイトにアップロードした場合、サイト側の仕様によりファイルの展開に失敗する場合があります。
3. Wi-Fi で LAN に接続した際などに、同一セグメント内で行われる通信（デフォルトゲートウェイを経由しない通信）は、Web フィルタリングの対象外となります。
4. Wi-Fi で LAN に接続し、ローカルエリアのサーバにアクセスする場合、ホスト名によるリクエスト（NetBIOS による名前解決）は行えません。IP アドレスでリクエストを行ってください。
5. Agent は、デバイス内部で「169.254.81.16」のローカル IP を使用します。Wi-Fi 等で接続した LAN 上に、このアドレスを使用するサーバが存在した場合、そのサーバとの通信は行えません。
6. LINE 等の音声通話アプリを利用する場合、アプリの通信先となるサーバを Agent の「除外 IP リスト」に登録する必要があります。

   ※　音声通話アプリの仕様によっては、IP 除外を実施しても正常に動作しない可能性があります。

7. モバイルネットワークと Wi-Fi の切り替え時など、接続先ネットワークが変更されるタイミングで音声通話アプリの通信が途切れる場合があります。

8. AppleTV、EZCastPro 等で画面ミラーリングを行う場合、画面の転送先となる機器でインターネット接続が無効になっている時は Web フィルタリングが行われません。

9. Agent を利用中のデバイスでテザリングを有効にした場合、テザリング配下のデバイス（子機側）では Web フィルタリングが行われません。

10. 「アプリポリシー設定」の「フィルタリング無効ホスト」はワイルドカード（*）での指定はできません。完全修飾ドメイン名を指定してください。

11. 2022 年 1 月 31 日より「エージェント設定配布」の「VPN 設定情報」は非表示となりました。

12. マルチユーザ機能を利用しているデバイスはサポート対象外です。

13. 電源管理アプリ（デバイスの省電力機能）が有効な場合、Agent が強制停止される場合があります。動作影響が疑われる場合は、Agent を電源管理の対象外に設定してください。

14. Chrome の圧縮プロキシ機能が有効な場合、Web フィルタリングが行われません。「proxy.googlezip.net」を Web フィルタリングの規制対象に設定する、または Google 管理コンソールで当該機能を無効化することを推奨します。

15. Agent を導入したデバイスでテザリングを利用する場合、「エージェント設定配布」の「除外 IP リスト」に「192.168.43.0/24」と登録した設定ファイルをデバイス側で再読み込みしてください。機種仕様により、登録する IP アドレスが異なる場合もあります。

16. Ver. 1.0.3 以前は「アプリポリシー設定」での機能および自動同期に対応していません。

    - 共通設定

    - ISGC Agent iOS/Android 設定

17. フィルタリング無効ホストに登録したホスト名が複数の IP を持ち、DNS 名前解決後の IP が時間によって変化する場合は正常に除外できない場合があります。

18. ISGC Agent Android は、VPN を介した接続機能を利用しています。しかし、LINE などの音声通話アプリのように、VPN を経由すると通信できないアプリも存在します。これらのアプリを使用する際には、Android OS の VPN 機能をバイパスするように、アプリの通信先を「フィルタリング無効 IP アドレス」または「フィルタリング無効ホスト」に登録する必要があります。なお、「フィルタリング無効ホスト」は内部で IP アドレスに変換されますが、ホストによっては複数の IP アドレスに変換されることがあります。この処理により、VPN を経由する IP アドレスの数が Android OS の VPN 機能の上限を超えると、ISGC Agent Android アプリが正常に動作しない可能性があります（例：フィルタリングが行えない）。この機能は Android OS の仕様に依存しているため、必ず事前に動作確認を行ってください。また、安定動作させるため「フィルタリング無効ホスト」の登録数は 25 件を目安にしてください。ただし、登録するホストによっては 25 件未満でも ISGC Agent アプリの動作に影響がある可能性がありますので、正常に動作しない場合は登録数を減らすなどの対応をお願いします。

ii. Windows 版の Agent

1. 導入時のインストーラにより、導入後の管理方法が異なります。

   Ver. 1.2.x 以上の場合

   コマンドオプション利用でインストール

   - アカウントの管理

     認証単位はデバイス単位となります。ユーザ管理のアカウントにデバイス情報が ISGC に登録されます。

     インストール後、デバイス名（コンピュータ名）でアカウントを自動登録します。（アカウント自動登録が完了後、任意のグループで管理してください。）

     インストール後、デバイス名を変更しても、以前のデバイス名をアカウント情報として利用します。インストール前にデバイス名を決定してください。

デバイス名は一意の値としてください。デバイス名が重複した際は、同一アカウントとして識別されます。

設定ファイル利用でインストール

- アカウントの管理

  認証単位は Windows ログオンユーザ単位となります。ユーザ管理のアカウントにデバイス情報は ISGC に登録されません。

  ISGC に作成した任意のアカウントで認証します。Windows ログオンユーザ毎に ISGC の認証アカウントを切り替えて利用します。（事前に ISGC 管理画面でアカウントおよび設定ファイルの作成が必要です。）

Ver. 1.1.11 以下の場合

EXE ファイル形式のインストーラ（旧バージョンはユーザ様専用ダウンロードサイトより、最新版は ISGC 管理画面より取得）

- アカウントの管理

  認証単位は Windows ログオンユーザ単位となります。デバイス情報は ISGC に登録されません。

  ISGC に作成した任意のアカウントで認証します。Windows ログオンユーザ毎に ISGC の認証アカウントを切り替えて利用します。（事前に ISGC 管理画面でアカウントおよび設定ファイルの作成が必要です。）

- モジュールアップデート

  自動アップデート機能もしくは手動でのアップデートがサポート対象となります。

MSI ファイル形式のインストーラ（ISGC 管理画面より取得）

- アカウントの管理

  認証単位はデバイス単位となります。デバイス情報が ISGC に登録されます。

  MSI でインストール後、デバイス名（コンピュータ名）でアカウントを自動登録します。（アカウント自動登録が完了後、任意のグループで管理してください。）

  インストール後、デバイス名を変更すると、アカウントの自動登録が再実施されます。インストール前にデバイス名を決定してください。

- モジュールアップデート

  自動アップデート機能もしくは手動でのアップデートがサポート対象となります。

2. POST データのフィルタリングはデータサイズが大きい場合に、デバイスの通信負荷がかからないよう一律フィルタリング対象外としています。そのため、以下のフィルタリングは機能しません。

   - 検索キーワード規制（POST データの場合のみ規制対象外）
   - 書き込みキーワード規制（一律規制対象外）

3. 解析可能なプロトコルは HTTP 通信および HTTPS 通信となります。FTP over HTTP には対応していません。

4. Google サービスなどで利用される HTTP/2 および HTTP/3（QUIC）プロトコルはフィルタリング対象となりません。

   HTTP/2 を制限する場合は Agent を導入後、ブラウザのキャッシュを削除してください。

   HTTP/3 を制限する場合は Chrome ブラウザを起動後、「chrome://flags/」より「Experimental QUIC protocol」を Disable にしてください。

5. Agent が実施している認証およびフィルタリングなどの各種通信は、認証必須のプロキシサーバを導入している環境に対応していません。プロキシサーバ側で特定 User-Agent「ISGC Agent」を部分一致で判定もしくは接続先ホスト「*.iss.netstar-inc.com」（「*」はワイルドカード）で判定し、認証を実施しないといった設定を実施してください。

6. ISGC 管理画面でアカウントを削除した場合、一律認証エラーとなり Web アクセスが制限されます。アカウントを削除後に再度利用したい場合は、デバイスへの再インストールが必要となります。

7. Ver. 1.0.21 をご利用の場合、Ver. 1.2.x へのアップデートパスがありません。Ver. 1.2.x へアップデートは Ver. 1.1.11 へのアップデートが完了後に可能となります。

8. Ver. 1.1.11 の MSI インストーラおよび Ver. 1.2.x のコマンドオプション利用で導入したデバイスは、アカウントが自動登録されます。アカウントは所定のグループ（「第 1 階層グループ」もしくは「自動登録ユーザ」）に登録されます。

9. Ver. 1.1.11 の MSI インストーラで導入したデバイスおよび Ver. 1.2.x のコマンドオプション利用で導入したデバイスでは、自動登録されたアカウント名が変更できません。

10. 自動登録されたアカウントに登録されるユーザ名はログオンしていたアカウント付与されます。ログオンアカウントに Microsoft アカウントを利用している場合、正常に表示されません。（先頭 5 文字のみ表示）

11. 自動登録されたアカウントに登録されるユーザ名は同一デバイスにログオンするユーザが変わる際に更新されます。

12. 自動登録されたアカウントはアカウントの CVS ファイルでの一括削除対象に含まれません。

13. Ver. 1.1.11 の MSI インストーラで導入したデバイスでは、HTTPS フィルタリングが強制有効となります。

14. Ver. 1.1.11 の MSI インストーラで導入したデバイスでは、「エージェント設定配布」の「除外 IP リスト」は利用できません。

15. Active Directory で導入したデバイスでは、ISGC の自動アップデート機能は無効にしてください。アップデートに失敗する場合があります。また Active Directory で導入したデバイスが自動アップデート機能でアップデートされた場合、 Active Directory 経由でアンインストールを実行する際に、導入したバージョンのレジストリ情報を Active Directory で付与する必要があります。

16. Intune を用いて MSI インストーラで導入したデバイスでは、ISGC の自動アップデート機能は無効にしてください。自動アップデート機能でアップデートされた場合、Intune 経由でアンインストールができません。

    Intune にてアンインストール管理をする場合、アップデートは Intune 上で実施してください。

    Intune を用いて MSI インストーラで導入したデバイスでは、Intune 経由でアンインストール操作をした際に、即時反映されない場合があります。

17. Ver. 1.1.11 以前の EXE インストーラで導入したデバイスで Ver. 1.2.x のコマンドオプション利用でアップデートした場合、「エージェント設定配布」で指定した「フィルタリング情報設定」の指定値が削除されます。アップデートした場合は「アプリポリシー設定」で再設定し、同期対象としてください。

18. Microsoft Entra ID（旧 AzureAD）連携機能を利用する際には、7.g. ii Windows 版の Agent ※Microsoft Entra ID（旧 AzureAD）利用時に記載の制限事項がありますのでご注意ください。

19. ISGC Agent Windows については、HTTPS デコード除外カテゴリ設定はご利用になれません。HTTPS デコード除外設定を行う場合は、[共通アクセス管理] > [HTTPS 規制設定] >「対象ホスト設定」をご利用ください。

iii. Windows 版の Agent ※Microsoft Entra ID（旧 AzureAD）利用時

1. Microsoft Entra ID において、ISGC のグループ名に使用できない文字を使用したグループを同期できません。
   同期対象の Microsoft EntraID では、グループ名に以下の文字列を使用しないようお願いいたします。

   - Tab（キーボード上の Tab ボタンで入力できるスペース）
   - 半角記号（「¥」,「/」,「:」,「;」,「?」,「<」,「>」,「|」,「"」）
   - 全角記号（「￥」,「／」,「：」,「；」,「？」,「＜」,「＞」,「｜」,「”」）

2. Microsoft Entra ID 上から削除済みのアカウントで端末にログインした場合、AgentWindows のアカウント名と ISGC 管理画面上のアカウント名の不一致が生じ、Web 閲覧およびフィルタリングルールの更新ができません。
   Microsoft Entra ID（旧 AzureAD）で削除済みのアカウントでは、端末へログインしないようお願いいたします。

3. Microsoft Entra ID（旧 AzureAD）連携で 100 件以上のグループを取り込むことが出来ません。ISGC については、1 グループに登録できるグループ数の上限が 100 までとなるため、Microsoft Entra ID グループの配下に登録できるグループ数は 99 です。

4. Microsoft Entra ID（旧 AzureAD）連携で大量のアカウント取り込みを行った場合に時間がかかります。Microsoft Entra ID 側のプロビジョニングに時間がかかり、アカウント登録を 1 件ずつ処理する仕様のため、大量のアカウント取り込みを行う場合に時間がかかります。（1 万件あたり約 8 時間程度）

iv. ChromeOS 版の Agent

1. Google 管理コンソールでの制限を必須としているため、Google 管理コンソールでの配布を推奨します。

2. Agent を配布する Google アカウントでは Chrome 同期を利用してください。
Agent の設定情報は Google アカウントに紐づき、同期データの対象となります。Google 管理コンソールでの配信対象から Agent を削除すると、同期データが削除されます。

3. Google 管理コンソールで配布する際、以下のポリシーを設定してください。

   ユーザとブラウザの設定

   - キッティング URL のブックマーク配信

     デバイス側でアクティベーションする際に必須となります。

     （json ポリシーでキッティングする場合は不要です。）

   - シークレットモードを無効

     シークレートモードでは Agent の利用が強制できないため、シークレットモードの利用は制限してください。

   - 一時的ログインモードを無効

     Agent の設定情報はローカルデータに保存されるため、ローカルデータ削除を削除すると、Agent が初期化されます。

   - Chrome タスクマネージャーでのプロセス終了をユーザに禁止する

   デバイスの設定

   - 強制的に再登録する

   - ローカルユーザデータを削除しない

   アプリと拡張機能

   - ユーザに他のアプリや拡張機能のインストールを許可しない

     ChromeOS 版 Agent は Chrome ブラウザのみがフィルタリング対象となるため、Play Store よりダウンロードするアプリケーションはフィルタリング対象外になります。

     許可されないアプリ/拡張機能はデフォルトアプリも対象となります。事前に許可アプリ/拡張機能を許可対象として登録してください。

4. HTTPS フィルタリングは強制有効となります。HTTPS デコードが無効の場合にも、パス付き URL 情報でのフィルタリングとなります。

5. Google 管理コンソールで Agent を配布されているアカウントは他 OS の Chrome でログインしないでください。他 OS の Chrome もフィルタリング対象となります。Agent は ChromeOS での利用のみが動作保証となります。

6. 以下の HTTP ヘッダのいずれかが含まれたリクエスト URL は、対象サイトに正常にアクセスすることができないため、フィルタリング対象外になります。

   - X-frame-Options

- Content-Security-Policy（frame-ancestors/frame-action/child-src/frame-src のいずれか）

上記リクエスト URL をフィルタリング対象に含める場合は、非同期リクエストのフィルタリング対象ドメインに追加してください。

サイトの構成により、フィルタリング対象に含めることで正常にアクセスできない場合があります。

7. YouTube のチャンネルホーム画面に表示された自動再生動画およびミニプレーヤーにて再生される動画はフィルタリング対象外になります。

   非同期リクエストのフィルタリング対象ドメインに YouTube を登録することで規制可能となりますが、ページ遷移などができない場合があります。

8. キッティング完了デバイス一覧の「ホスト名」は Google Enterprise および Google Education にて管理デバイスとなっている場合、かつ「デバイスのネットワークホスト名テンプレート」を設定している場合に表示されます。

   ChromeOS のバージョンが 85.x 未満の場合、適切な API が利用できないため、デバイス一覧に表示されません。

9. セーフサーチロックを有効化している場合も以下の操作で Youtube 動画へ直接アクセスした場合は、Youtube の制限付きモードが強制されません。

   - ブラウザのアドレスバーに Youtube 動画再生ページの URL を入力して直接アクセスする
     （共有用の短縮リンクからのリダイレクトを含む）

   - Youtube 動画再生ページ上部から検索を行う

   Youtube の制限付きモードを強制する場合は、以下の設定を検討してください。

   - Google 管理コンソール側で［YouTube の制限付きモード］を[YouTube で制限付きモードを強制的に適用する］に変更する。

   セーフサーチロックを有効化している場合、セーフサーチロックの仕様上、Youtube へのログイン状態が維持されません。Youtube へログインした状態でページ読み込みボタンを押下するとログアウトされてしまいます。
   Youtube からログアウトされてしまった場合は、ブラウザのキャッシュ削除を行うことで対処してください。

h. スクールライセンス

1. アクセスが集中する時間帯では、トラフィックの急増によりアクセス遅延が発生する場合があります。予めシステムで利用する通信や授業で利用するコンテンツは必ず除外設定をしてください。除外対象となるホスト情報は弊社 FAQ サイト（要ログイン）をご参照ください。 http://support.alsi.co.jp/

   除外を実施する OS

   - iOS / iPadOS：除外方法「PAC_BYPASS_HOST もしくは PROXY_BYPASS_HOST」（コンテンツフィルタ）
   - ChromeOS：除外方法「Google 管理コンソールでのプロキシバイパスリスト」（プロキシ利用時）

   除外を実施する通信

   - MDM 製品の通信
   - Apple 製品の通信
   - Microsoft 365 の通信
   - Google サービスの通信
   - 学習支援コンテンツ
   - Web 会議アプリケーションの通信

2. スクールライセンスでは、一部機能の利用、または設定変更ができません。詳細は弊社 FAQ サイト（要ログイン）をご参照ください。 http://support.alsi.co.jp/

   利用できない機能：

   - Geo スコープ
   - HTTPS デコード機能の除外カテゴリ設定, パス部ログ出力設定
   - 規制解除申請
   - 例外 URL 自動削除
   - クライアント IP アドレス制限
   - ログ設定

   設定変更が出来ない機能（常に有効）：

   - 高度分類クラウド（IWCC） ※ 当該のアクセスログはカテゴリ名に[IWCC]を付与
   - HTTP 接続禁止ポート設定 ※ 25, 110 ポートへの接続を禁止
   - フィルタリングバイパス設定 ※ OS の行うシステム通信の一部などを除外
   - リクエスト別認証設定 ※ OS の行うシステム通信の一部などをルートグループで認証

3. ISGC の IP アドレス情報は公開しておりません。接続先 IP アドレスでの制限している場合、正常に動作しないことがあります。
4. アクセスログに出力されるクライアント IP アドレスは ChromeOS を除き、一律「0.0.0.0」となります。
5. 特定サイトやコンテンツはアクセスログに出力されません。対象コンテンツは弊社 FAQ サイト（要ログイン）をご参照ください。
6. デバイスのキッティングが完了する前に、必ず ISGC 管理画面でアカウント登録をしてください。登録が完了していない場合、一律認証エラーとなり Web アクセスが制限されます。
7. 各デバイスでの注意・制限事項については「e.ISGC assist」および「g.ISGC Agent」の項目をご確認ください。

i. オプションサービス

i. 導入支援サービス

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。
2. オンサイト対応は本サービスに含まれません。
3. アカウントのグループ移動は本サービスに含まれません。
4. 作業期間は最長 1 ヶ月となります。期間延長は実施しておりません。
5. 契約前（運用開始前）のお客様を対象としております。契約開始（運用開始）より本サービスは終了となります。
6. 本サービスは ISGC 管理画面での設定作業および同居アプリケーションの調査が対象となります。デバイスのキッティング作業および他社製品の設定作業は対象外となります。

ii. ログ長期保管サービス

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。
2. 365 日以上の保管期間の延長はできません。
3. 本サービス適用以降のログが対象となります。

iii. ダッシュボードサービス

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。
2. 本サービスは、Google 社が提供する「BigQuery」および「LookerStudio」を使用しております。
3. 本サービスのご利用には、Google アカウントが必要です。
4. 組織ポリシーとして LookerStudio の利用を制限している場合、本サービスへのアクセスができません。ご使用前に予めご確認ください。
5. 管理画面は Google Chrome に対応しています。
6. 表示するログは、当月+過去 2 ヶ月分です。*
7. ログの取り込みは日次で行います。*

   (*)表示するログ期間について・・・2025/4/10 にダッシュボードサービスにアクセスした場合には、2025/2/1～2025/4/9 までのログをご確認いただけます。
8. サービスのアップデートに伴い、提供するサービス URL が変更となる場合があります。
9. グループ名が長い場合や、グループが階層構造になっている場合、サービス画面上でグループ名が見切れることがあります。
10. 例外 URL や未分類 URL は、カテゴリ分類「-(ハイフン)」として出力されます。
    https://alsifaq.dga.jp/faq_detail.html?id=6613

iv. Microsoft365 ドメイン配信サービス

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。

2. メール配信は月末に実施します。

3. 差分情報の設定反映は自動では行われません。メールの内容を確認後、適時登録してください。

v. アクセス制限オプション

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。

2. 「モバイル利用」および「スクールライセンス」のお客様はご利用できません。

3. IP アドレスに関する 2 種類のサービスを提供します。

   ISGC 宛の通信アクセス制限

   ISGC 宛の通信（ISGC の管理画面/プロキシポート）へアクセスを社内からの IP アドレスのみに限定したい場合に指定の IP アドレスを設定して制限を行います。

   ※許可登録できる IP アドレスは 5 つまで

   固定 IP アドレス提供

   企業で契約しているクラウドサービスにアクセスを ISGC 経由のみに限定できるようにします。
   ISGC のグローバル IP アドレスをクラウドサービスに登録することで自宅端末や未認証端末からのアクセスを制限します。
   ※提供する IP アドレスはサーバ障害、サーバの増設や増強、帯域拡張オプション利用開始時等により変わる可能性がありますので、予めご了承下さい。変更時には適宜連絡致します。
   ※弊社オプションでは IP アドレスの提供のみです。各クラウドサービスの設定等に関するお問い合わせは対象外となります。

vi. 帯域拡張オプション

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。

2. 「スクールライセンス」のお客様はご利用できません。

3. 本サービスはベストエフォートでの提供となります。

4. WindowsUpdate/Apple/MDM 等の一部の通信は除外対象として下さい。

5. 帯域変更時にはメンテナンス作業が発生する為、作業中は通信断等が発生する可能性があります。

vii. VPN 構成オプション

1. 本サービスは、ISGC のご利用を前提としたオプションサービスです。

2. 「モバイル利用」および「スクールライセンス」のお客様はご利用できません。

3. お客様側の VPN ルーターの設定はお客様自身での実施となります。

4. 「プロキシ利用 PAC 配信」機能は利用できません。

8. 問い合わせ先

ISGC および本仕様書に関するお問い合わせは、下記までご連絡ください。

問い合わせフォーム	https://alsifaq.dga.jp/support_form.html
メールアドレス	support@alsi.co.jp

午前10時～正午、午後1時～午後5時

土曜日、日曜日、祝祭日および弊社指定休日は休業させていただきます。

InterSafe GatewayConnection　サービス仕様書

2026 年 1 月 第 42 版

作成 / 発行 / 企画　　アルプスシステムインテグレーション株式会社
〒145-0067 東京都大田区雪谷大塚町 1-7