

# ALSI クラウド型 多層セキュリティゲートウェイサービス 「InterSafe GatewayConnection」を提供開始

## サイバー攻撃対策と Web フィルタリングで出口対策を実現

アルプス システム インテグレーション株式会社(本社:東京都大田区、代表取締役社長:永倉 仁哉、以下ALSI〔アルシー〕)は、クラウド型 多層セキュリティゲートウェイサービス「InterSafe GatewayConnection」(インターセーフ ゲートウェイコネクション)を2016年10月末より提供開始することを発表いたします。

サービス名	クラウド型 多層セキュリティゲートウェイサービス「InterSafe GatewayConnection」
提供開始日	2016年10月末
主なターゲット	国内企業 300~3,000 ユーザー規模
主な機能	サイバー攻撃対策、Web フィルタリング
提供価格 (税別)	300 ユーザーの場合 (月額・1 ユーザーあたり) サイバー攻撃対策サービス: 550 円 / Web フィルタリングサービス: 450 円
販売目標	2017年度末 28,000ライセンス
詳細情報 URL	<a href="http://www.alsi.co.jp/security/isgc/new/">http://www.alsi.co.jp/security/isgc/new/</a>

### ■新サービス 提供開始の背景

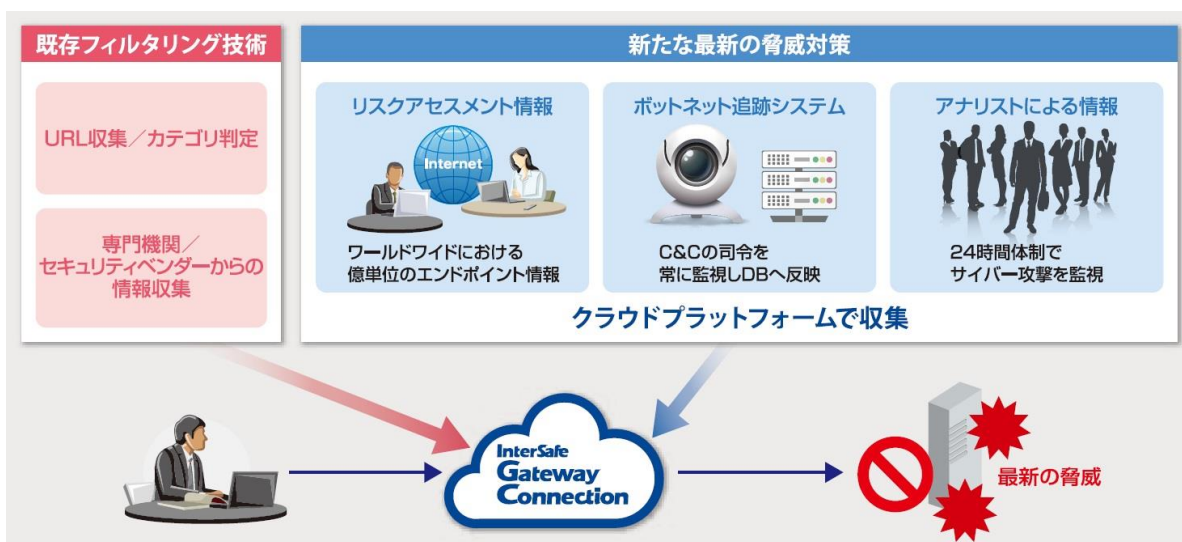
現在、多くの企業や組織が標的型サイバー攻撃を受け、被害が拡大しております。加速度的に広がり続ける最新の脅威に対して、これまでは「侵入させない」ことを目的とした入口対策に重点が置かれていました。しかし、サイバー攻撃の巧妙化により入口対策での完全な防御は限界となり、「侵入を防ぐことはできない」ことを前提とした出口対策を講じることが重要となってきています。

万が一サイバー攻撃を受けてしまったとしても、多層セキュリティにより出口対策を強化することで、機密情報の漏洩を防ぎ、不正な通信を遮断することが可能となります。

この度 ALSI が提供を開始する新サービス「InterSafe GatewayConnection」は、クラウド上に多層セキュリティを設置し、出口における情報のリスクコントロールと、運用負荷を軽減することができるクラウドサービスです。高精度のリスクアセスメント情報とワールドワイドで収集した脅威情報データベースにより、最新の脅威に対するアクセスブロックを実現します。

### ■「InterSafe GatewayConnection」の特長

「InterSafe GatewayConnection」は、クラウド上に多層セキュリティを設置し、情報の出口でのリスクコントロールと運用負荷を軽減するクラウドサービスです。この度、Layer1「サイバー攻撃対策」、Layer2「Web フィルタリング」を提供し、今後、Layer3「データ暗号化対策」、Layer4「個人情報漏洩対策」を順次提供する予定です。



▲「InterSafe GatewayConnection」サービス概要イメージ

## 【Layer 1】サイバー攻撃対策

クラウドプラットフォームでワールドワイドから最新の脅威情報を収集したリスクアセスメント情報、ボットネット追跡システム、経験豊富なアナリスト集団からの最新情報に基づいて、C&C サーバ<sup>(※1)</sup>など標的型攻撃に用いられる脅威サイトへの通信を遮断します。

クラウド型のセキュリティゲートウェイサービスのため、上位プロキシに設定するだけで、既存のネットワーク構成を変更する必要がなく、複雑なポリシーの設定なども不要です。手軽に導入することができ、初期費用も抑えることができるため、サイバー攻撃対策をこれから検討する企業・組織に適した新しいセキュリティサービスとなります。

### ①リスクアセスメント情報

最新のリスクアセスメント情報をクラウド上でリアルタイム収集

ワールドワイドに散らばる億単位のエンドポイントから収集した情報を基準としたリスクアセスメント情報を、クラウドプラットフォーム上でリアルタイムに収集するため、常に最新の脅威情報データベースの提供が可能です。

### ②ボットネット遮断システム

金融機関を標的とするボットネットの約 99%をカバーする追跡システムが監視

現在主流となっているネットワーク攻撃は、ボットネットを使って組織化されています。「InterSafe GatewayConnection」は、オンライン決済システムやネットバンキングシステムなど、金融機関を標的にするボットネットの約 99%をカバーするボットネット追跡システムを構築しています。ボットネットの動作を追跡し、C&C サーバの指令を常に監視し、脅威情報データベースに反映します。

### ③アナリストによる 24 時間 監視体制

世界で実績を持つアナリスト集団が 24 時間体制でサイバー攻撃を監視

世界中のAPT、標的型攻撃を発見、レポートしてきたアナリスト集団から最新の脅威情報の提供、実績豊富なアナリストによる24時間監視体制と連携することで、データベースの信頼性をさらに向上し、脅威へのアクセスブロックを強化します。

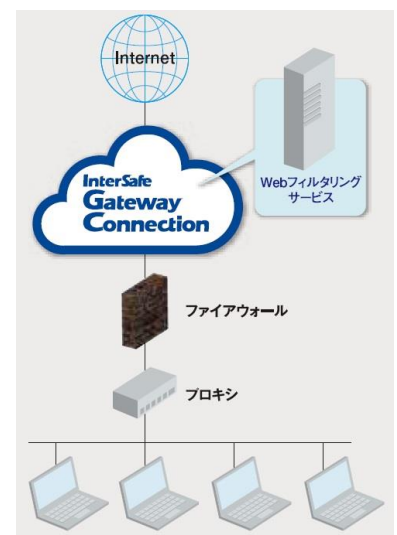


▲リスクアセスメント情報のイメージ

## 【Layer 2】Webフィルタリング

Web フィルタリングは、12 年連続マーケットシェア 1 位<sup>(※2)</sup>の「InterSafe WebFilter(インターセーフ ウェブフィルター)」と同等の機能をクラウド上で提供するサービスです。

携帯キャリア採用率100%の高精度URLデータベースに基づいて、クライアントPC の Web アクセスをコントロールします。不正なサイトへのアクセスや書き込みを防止し、情報漏洩防止・ウイルス感染防止・私的利用防止による業務効率向上を実現します。



▲Web フィルタリングのイメージ

※掲載されている会社名及び商品名は各社の商標または登録商標です。

※1: command and control server(コマンド&コントロールサーバー);サイバー攻撃などにおいて、マルウェアに感染してボットと化したコンピュータ群(ボットネット)に指令を送り、制御の中心となるサーバ。

※2: 出典 IDC Japan 2016 年 8 月「国内情報セキュリティ製品市場予測、2016 年～2020 年」(Report#JPJ40602516)、富士キメラ総研 2015 年 11 月「2015 年ネットワークセキュリティビジネス調査総覧」(Webフィルタリングツール 2014 年度金額ベース。富士キメラ総研「2015 年ネットワークセキュリティビジネス調査総覧」を基に当社作成。

### 【このリリースに関するお問い合わせ・取材受付先】

アルプス システム インテグレーション株式会社

URL: <http://www.alsi.co.jp/>

〒145-0067 東京都大田区雪谷大塚町 1-7

TEL: 03-5499-8043 FAX: 03-3726-7050

広報担当: 桑野 宏子 (kuwano@alsi.co.jp)