OceanBridge

つかえるITを、世界から。

ISL Online
プライベートクラウドライセンスのセキュリティについて

株式会社オーシャンブリッジ

2018年7月13日

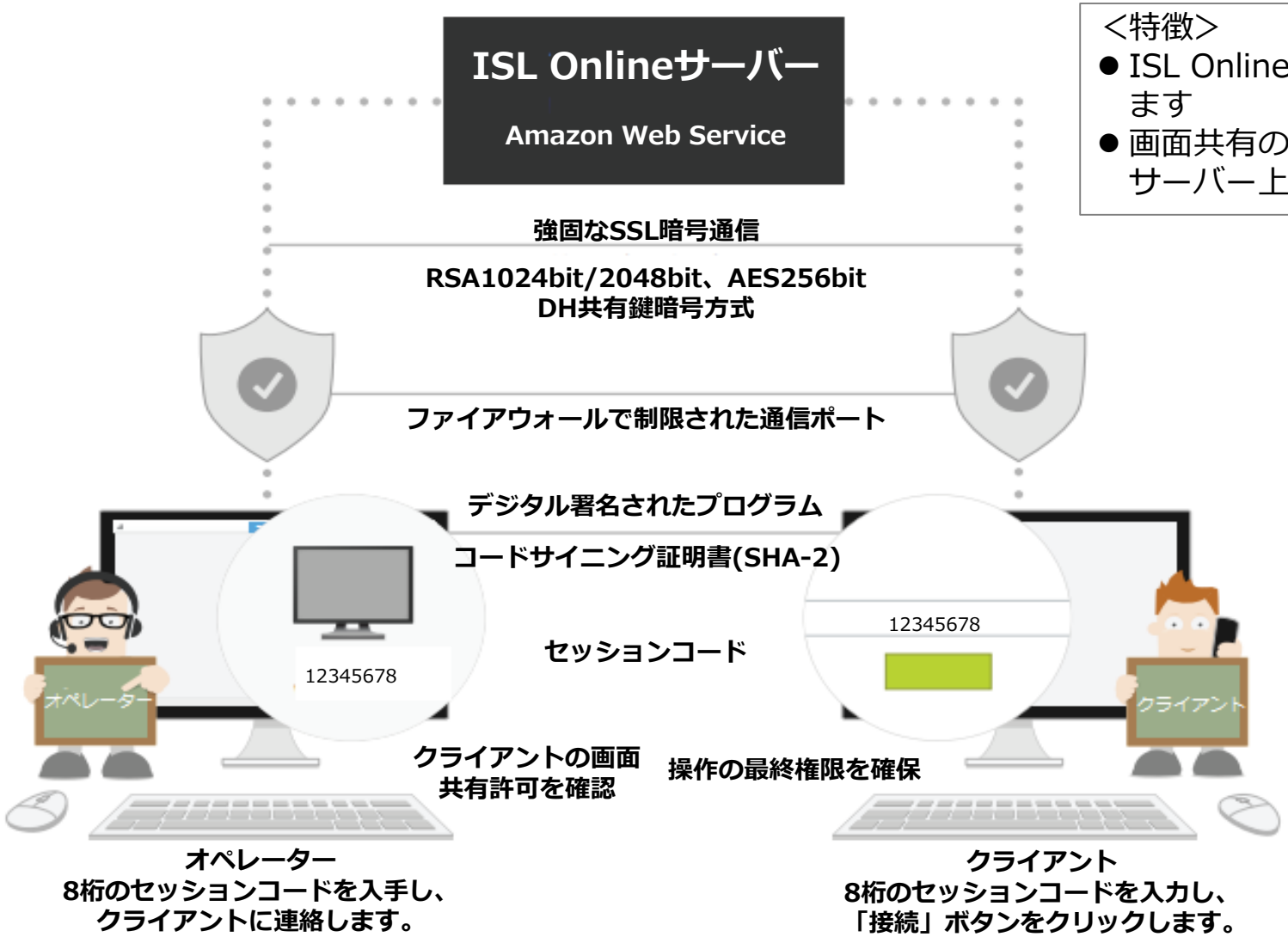
ISL Online の仕組みについて

- ISL Onlineは中継サーバー型のリモートコントロールツールです。
- すべての通信が『**中継サーバー**』を経由するため、**「オペレーター端末が単独でクライアント端末に接続できない」**仕組みです。**接続状況や接続履歴を中継サーバー上で確認できます。**
- 内向きのポートを開放する必要がないため、**セキュア**なリモートアクセスを行うことができます。

ISLリモコンエンジン提供内容	
プログラム	ワンタイム型リモコン
	常駐型リモコン
	Web会議
サービス	データベース
	Webサービス

OceanBridge

ISL Online セキュリティ基本概要



＜特徴＞
- ISL Onlineの通信はSSLで暗号化されます
- 画面共有の内容、転送したファイルはサーバー上に残りません

プライベートクラウドライセンスの安全性と安定性について

1. Amazon Web Service（以下、AWS）上でのサーバー運用
   - ISL Onlineのプライベートクラウドライセンスでは、AWS上にシングルテナントで契約企業様のみがご利用いただけるActive/Active構成のサーバーを構築します。
   - AWSは50以上のセキュリティコンプライアンスに準拠しています（ISO 27001、ISO 27017、ISO 27018、PCI DSS レベル1、SOC 1-3等）
   - AWSのデータセンターは外部からはそれとはわからないように設計され、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。
   - AWSのビルトインファイアーウォール、およびサーバーのオペレーティングシステム（CentOS 7）の設定により、接続許可ポート、SSH接続のアクセス元IPアドレスを制限し、不正アクセス対策を施しています。
   - サービスが停止するほどのサーバー障害が発生した場合や、システムの脆弱性の存在が発覚した場合には、契約企業様のご了承のもと、弊社または開発元によるパッチの適用や遠隔メンテナンスを実施いたします。

OceanBridge

プライベートクラウドライセンスの安全性と安定性について

2. ISL Conference Proxy（サーバーソフトウェア）の運用
   - グリッド技術を採用したサーバーの耐障害性
     Active-Activeバックアップによりシステムを冗長化しています。接続サーバーが故障しても別のサーバーが自動で継続運用します。また、一部サーバーに負荷が偏った場合でも、全体で分散処理し効率運用を実現します。

   - ISL Conference Proxyの管理者ページへのアクセスは、以下の通り制限されています。
     - アクセス元IPアドレスを制限
     - 64桁のログインパスワードによる保護
       ※基本的には弊社および開発元もバージョンアップ、ライセンスファイルの更新のため管理者ページにログインできる形になりますが、お客様がログインパスワードを変更した場合、それらの作業をお客様側で行っていただく形になります

   - ISL Online製品の利用（プロダクトログインページへのアクセスやセッションコードの取得）をIPアドレスにより制限することが可能です。

OceanBridge

プライベートクラウドライセンスの安全性と安定性について

3. 通信データ
   - ISL Onlineのセッションはオペレーター PCとクライアントPCのデスクトップ共有やファイル転送を実現しています。
   - デスクトップ共有はイメージの転送によって実現するもので、中継サーバーにファイルは蓄積されません。
   - ファイル転送機能を使用する際も、送信先PCに保存先が指定される方式をとりますので、PC間でやり取りされたいかなるファイルもサーバーに蓄積されることはございません。
     ※Web会議（ISL Groop）では、サーバー上にファイルをアップロードし、ファイル共有を行う機能がございますが、アップロードしたファイルは権限を持つユーザーが削除可能です。

4. 通信データの暗号化
   - ISL Online製品では、ファイル転送時を含めた全セッションを通じSSL 256bit-AESの暗号化を行っております。
     ※ISL Online製品のプログラムには、デジタル署名（SHA-2）が付与されています。

OceanBridge

プライベートクラウドライセンスの安全性と安定性について

5. 操作上の許可確認
   - ISL Onlineのセッションは「両者合意のもとで」リモートセッションを行うことを基本としています。
   - デスクトップ共有を開始する前に、オペレーターがクライアントPCの画面表示および操作の許可を求める「許可確認画面」を表示することで、クライアントの許可を得た後にデスクトップ共有が開始される環境を実現しています。

6. デスクトップ共有時の操作権限
   - デスクトップ共有をオペレーターに許可した後も、マウスを動かすだけで、クライアントはいつでもオペレーターの操作を一時的に停止することができます。
   - その他にも、画面操作を停止し画面表示のみとしたり、テキストチャットモードのみ許可することも可能ですので、クライアントが安心して利用できます。

OceanBridge

SSLとは

- SSLとは：
  SSL（Secure Sockets Layer）とは、ネットワークを介したコンピューター同士の通信を安全にやり取りするための技術で、OSI参照モデルにおけるセッション層ならびにトランスポート層において機能するプロトコル。遠隔地のコンピューター同士がネットワークを介して情報をやり取りする際の、認証や暗号化による安全な通信実現のためのプロトコルや技術の総称です。

- SSLによって防ぐことのできるリスク：「盗聴」「成りすまし」「改ざん」「否認」など

- ISL Onlineで使用するSSL通信について：
  AES-256bit ⇒ データ通信の暗号化、256bit暗号データを解読することは現在の技術では現実的に不可能です。
  RSA-1024bit ⇒ セッション開始時に行うデータ交換方式で、1024bit暗号データを解読することは現在の技術では現実的に不可能です。なお2018年7月現在、各プログラムがRSA-2048bit暗号化通信を行うよう順次アップグレードしております。

OceanBridge

管理機能

ISL Online プライベートクラウドライセンスの管理設定で、セキュリティの強化を実現できます。

機能名	機能概要
オペレーター作成	管理者はオペレーターを無制限に作成できます。
オペレーターパスワード変更	管理者による操作でオペレーターのパスワードを変更できます。
利用機能制限	オペレーターごとにファイル転送、遠隔プリント、音声・ビデオチャットの使用を禁止できます。
利用履歴	IPアドレス、接続時間、送受信を行ったファイル名のログを保持し、管理画面から閲覧できます。
アカウント利用停止	オペレーターの利用を停止することができます。
オペレーター利用制限	オペレーター単位で、IPアドレスまたはMACアドレスによる利用制限を行うことができます。
二段階認証	ログイン時に、Google Authenticator、Eメールのいずれかの方法によるセキュリティコードを使用した認証を行うことができます。

OceanBridge

OceanBridge

つかえるITを、**世界から。**

製品、サービス、その他ご質問やご不明な点などございましたら
下記までお問い合わせください

体験版ユーザー様はこちら:　sales@oceanbridge.jp
ご購入ユーザー様はこちら：　isl-support@oceanbridge.jp

株式会社オーシャンブリッジ

150-0043　東京都渋谷区道玄坂1-20-8　寿パークビル7F
www.oceanbridge.jp