



つかえるITを、世界から。

ISL Online プライベートクラウド / オンプレミスライセンスの セキュリティについて

株式会社オーシャンブリッジ

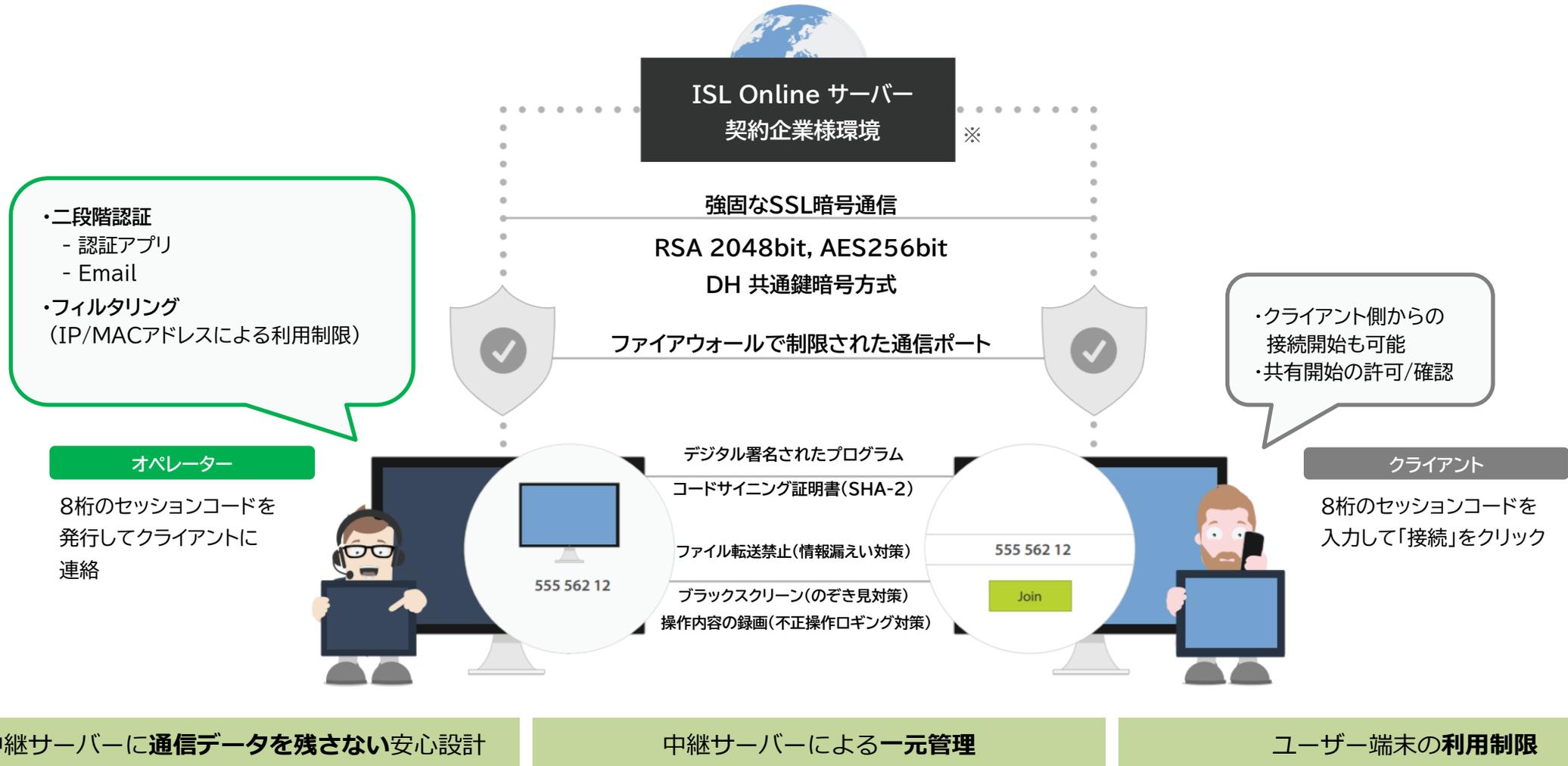
islmpc_securityinfo-241212

- ISL Onlineは、すべてのセッションが『**中継サーバー**』で管理され、「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。
- オペレーターとクライアント端末間で最適な通信方式を自動で判断し、セキュアな接続を実現します。



ISL Onlineでは、デスクトップ画面を「画像データ」として転送します。画面共有の内容、転送したファイルは中継サーバーに蓄積されません。

※2024年11月現在、チャット (ISL Pronto) はオンプレミス・プライベートクラウドライセンスでご利用可能です



※オンプレミスライセンスでは、社内ネットワークやお客様が契約している IAAS に中継サーバーを設置して、よりセキュアなリモートメンテナンスサービスを構築できます。

※プライベートクラウドライセンスでは、Microsoft AzureまたはAWS(Amazon Web Services)上に、契約企業様専用の中継サーバーをご用意します。

1. 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ありません。
※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。

2. 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。

3. 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。

4. 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。

1. 契約企業様専用インスタンス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、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構成のサーバー構築を以下のサービスからお選びいただけます。

AWS (Amazon Web Service)

Microsoft Azure

- AWS (Amazon Web Service) およびMicrosoft Azureは以下に代表される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
- サーバーOS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。

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（製品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。

- 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-2048bit ⇒ セッション開始時に行うデータ交換方式で、2048bit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。

ISL Online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、認証アプリ（Google Authenticator・Microsoft 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。 |



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

〒107-0051 東京都港区元赤坂一丁目5番12号 住友不動産元赤坂ビル7階
www.oceanbridge.jp