つかえるITを、世界から。

ISL Online
パブリック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

isl_securityinfo-241212

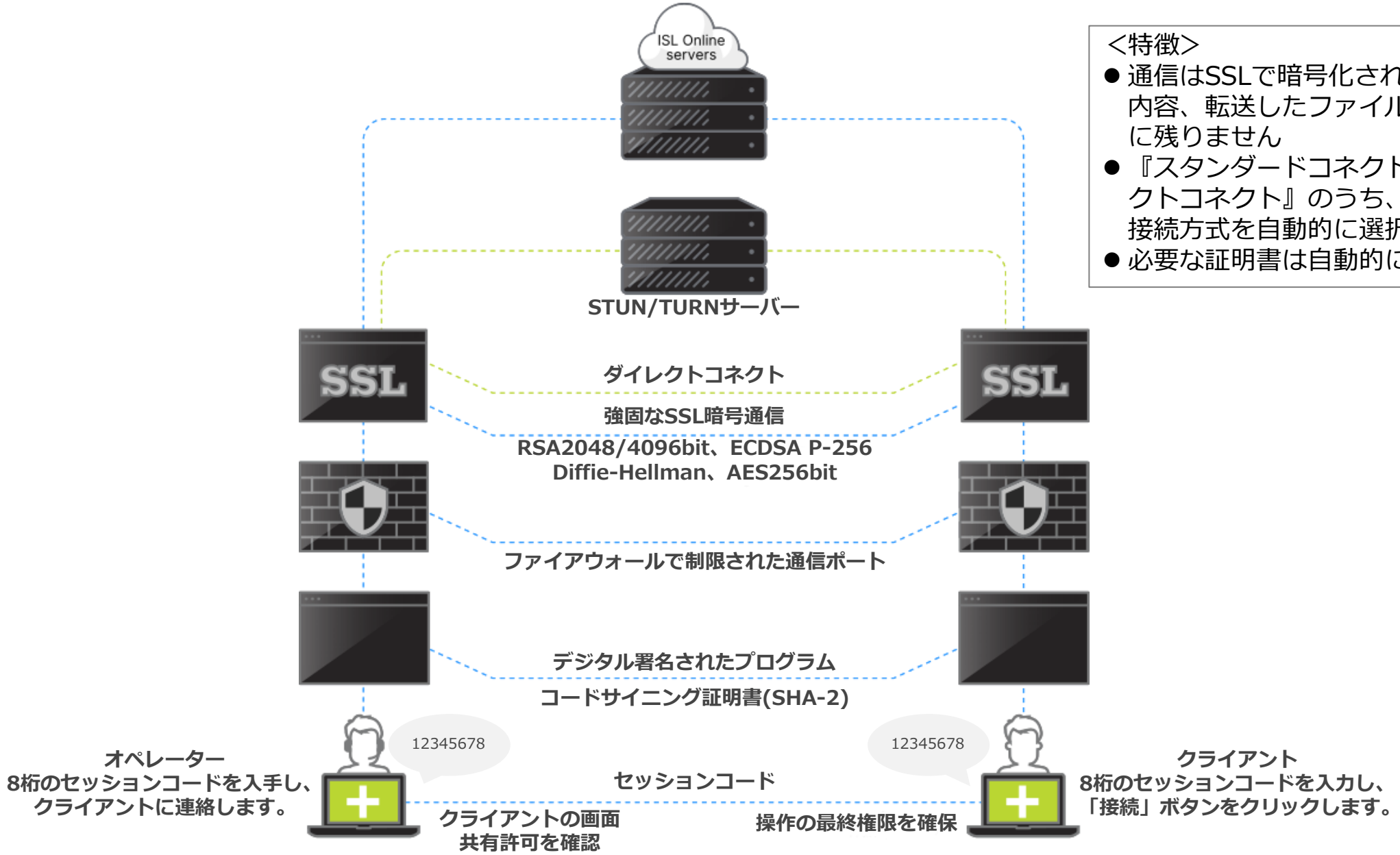
ISL Online のしくみ

- 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

ISL Online パブリッククラウド『セキュリティ基本概要』

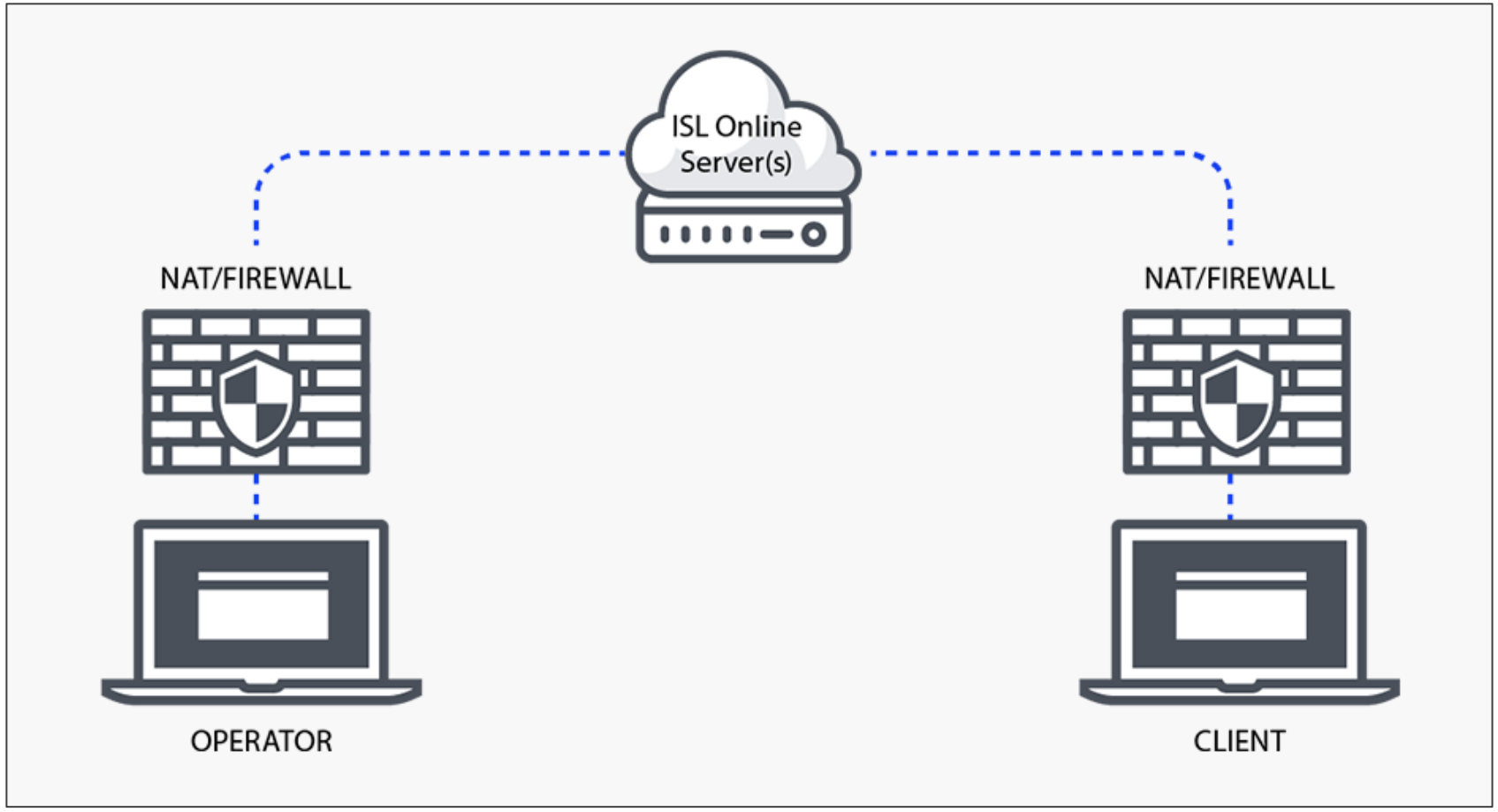


＜特徴＞

- 通信はSSLで暗号化され、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
- 『スタンダードコネクト』か『ダイレクトコネクト』のうち、最も効果的な接続方式を自動的に選択します
- 必要な証明書は自動的に更新されます

ISL Online パブリッククラウド『スタンダードコネクト』

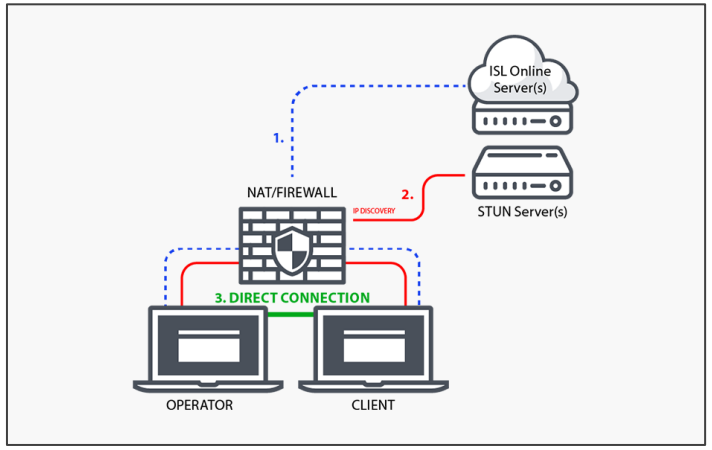
- 「スタンダードコネクト」は、すべての通信が中継サーバーを経由する接続方式です。



ISL Online パブリッククラウド『ダイレクトコネクト』

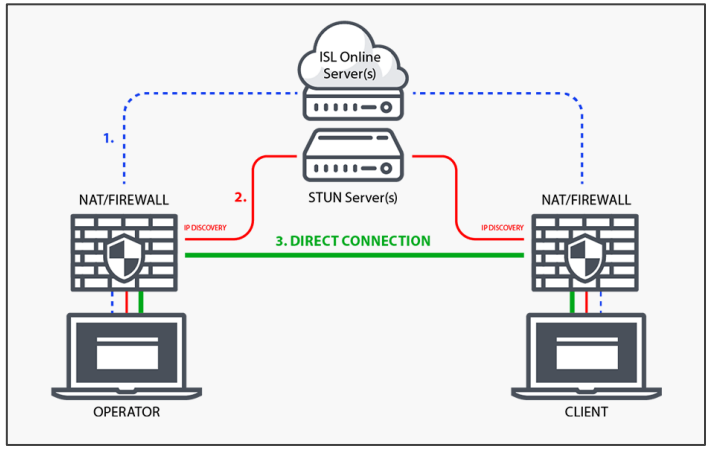
- 「ダイレクトコネクト」は、セッション制御のための中継サーバーとの接続はアクティブのまま、エンドポイント同士の暗号化された直接接続に通信データをオフロードする接続方式です。以下の候補から最適なルートを自動的に選択します。

ホスト候補



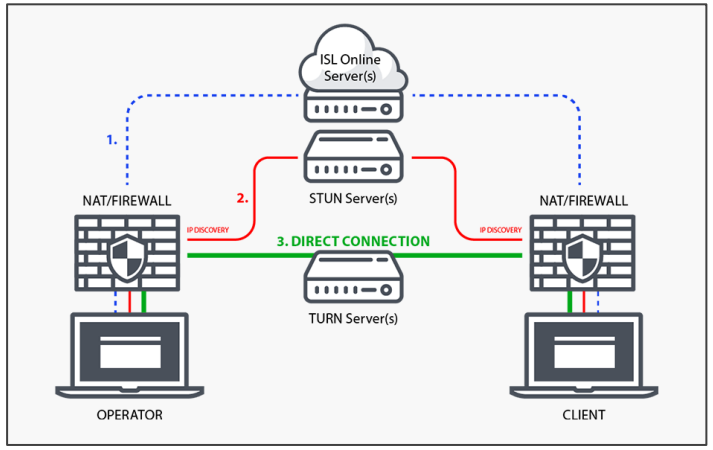
両端末が同じローカルネットワーク上にある場合に使用されます。

サーバーリフレクティブ候補



両端末がSTUNサーバーを通じて、ローカルネットワーク外との通信を確立します。

リレー候補



両端末がSTUNサーバーを通じ、さらにTURNサーバーを経由して通信を確立します。ファイアウォールやNATの制限等により直接通信ができない場合に使用されます。

ダイレクトコネクトを利用するには、最新バージョンの製品を利用している必要があります。
ISL Light 4.4.2332.175 ～／ISL Light Client 4.4.2332.31 ～／ ISL AlwaysOn 4.4.2332.78 ～

ISL Online パブリッククラウドの安全性と安定性について

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。

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。

ISL Online パブリッククラウドの安全性と安定性について

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。

ISL Online パブリッククラウドの安全性と安定性について

OCEANBRIDGE

5. 信頼のおける管理会社での運用
   - 日本に置かれたISL Online製品の接続を可能にするグリッドサーバーは、信頼のおけるサーバー管理会社の管理下で運用されています。
   - 不正アクセスの対策として、SSH等でグリッドサーバーに接続を行う場合のアクセス元を制限しております。
   - ログの取得を行うと同時に、脆弱性が存在する場合にはパッチの適用を行うなど、情報漏えいを防止する為に最善の対策を実施しております。

6. グリッド技術を採用したサーバーの耐障害性
   - ISL Onlineのパブリッククラウドは世界中に点在したグリッドサーバーにより支えられています。
   - これらグリッドサーバーは最先端グリッド技術により連結されており、接続サーバーの偶発的トラブルにも他のサーバーがセッションを維持する機能を備えております。こうして、安定したサービスを提供しております。

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-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。

管理機能

ISL Online パブリック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、SMS、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