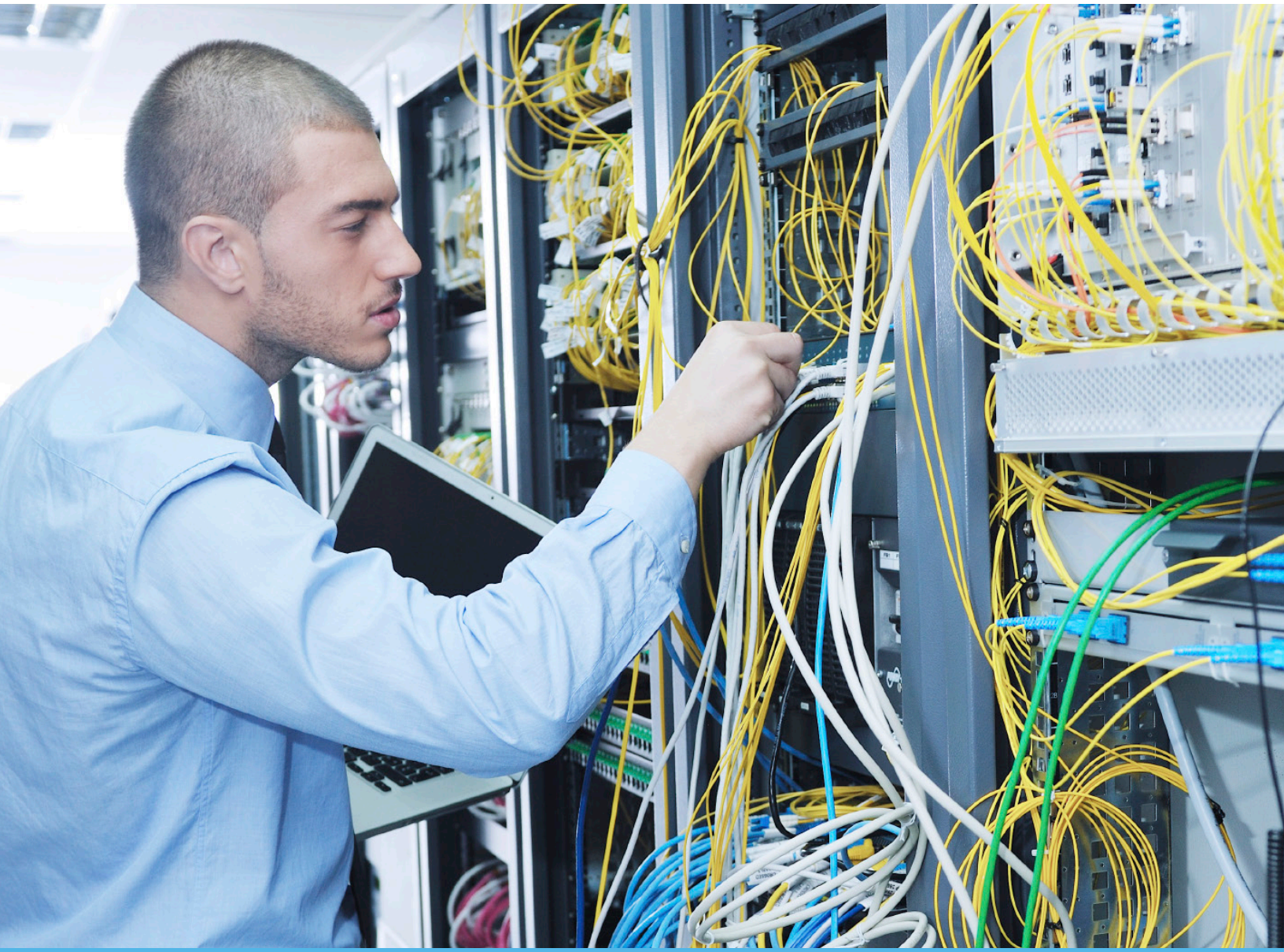
Rescue by LogMeIn

RESCUE のアーキテクチャおよびセキュリティ

概要パンフレット



目次

はじめに

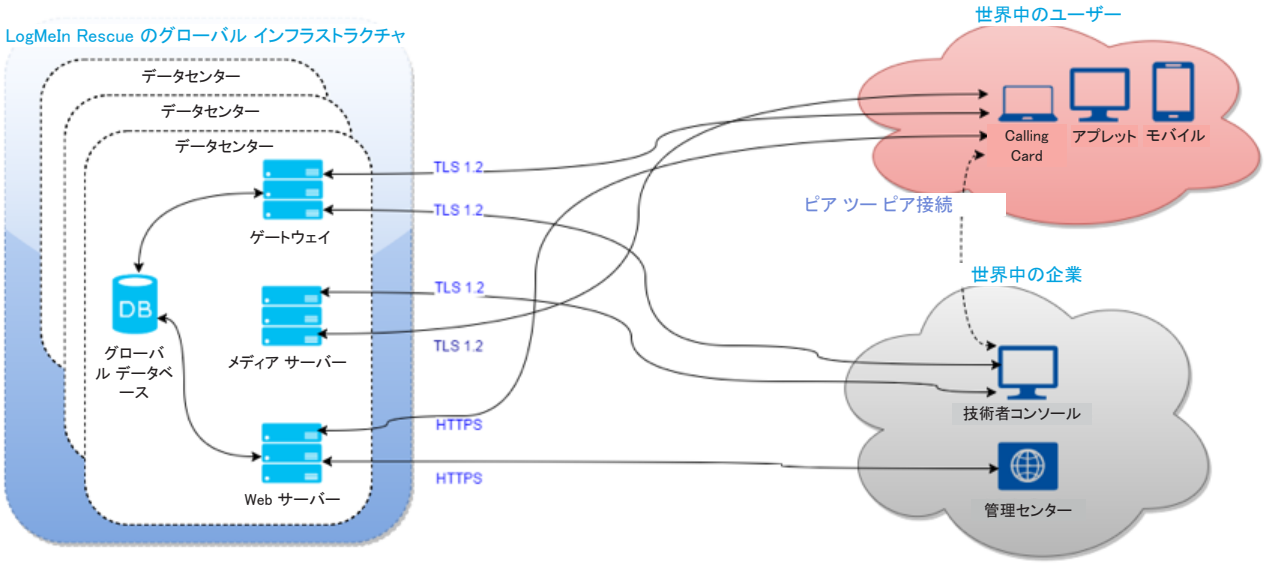
スケーラビリティ、セキュリティ、信頼性、使いやすさ。これら 4 つの特徴は、優れたリモート サポート ソリューションの条件ですが、常にこれらすべての要件が満たされるわけではありません。これらの条件のうち 2 つか 3 つを満たすリモート サポート ソリューションは容易に見つかりますが、4 つすべてを満たすソリューションはまれです。LogMeIn Inc. は、まさにそうしたソリューションを LogMeIn Rescue によって提供しています。

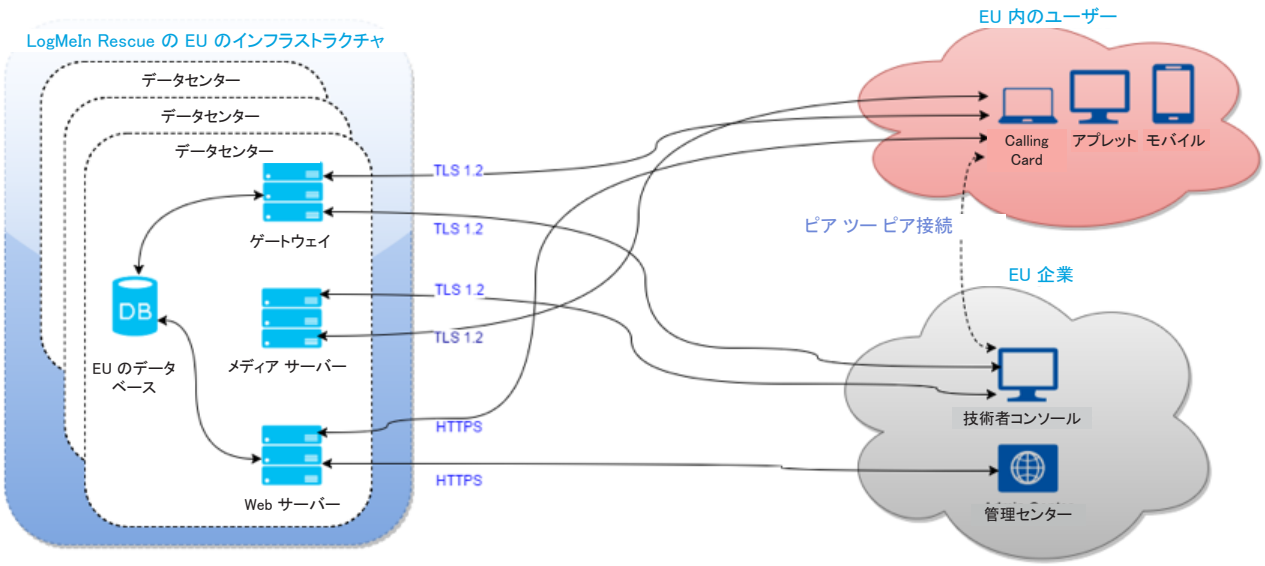
スケーラビリティ。サポートを担当するのがたった 1 人の技術者であっても、10,000 人の従業員を擁するコール センターであっても、Rescue は効果を発揮します。

セキュリティ。サポート セッションは、エンドツーエンドの 256 ビット AES 暗号化で保護されます。サポートの操作は、エンドユーザーの許可なしに技術者が実行することはできません。サポート セッションのログは、暗号化された形でデータベースに保存され、後で参照できます。リモート制御セッションはビデオ ファイルに記録できます。

信頼性。Rescue は、完全に冗長化されたインフラストラクチャを持つ、通信事業者レベルの 6 つのデータ センターによってホストされます。

使いやすさ。わずか数時間で技術者との接続が確立され、サポート体制が整います。サポートを受けるエンド ユーザーは、数回のクリックでヘルプ情報を取得できます。どちらの側でもソフトウェアのインストールは一切不要です。





データの機密性

多くの場合、セキュリティはデータの機密性と、データの機密性は暗号化と同一視され、暗号化は使用する対称暗号とその鍵の長さによって特徴付けられます。これらの誤った認識が「256 ビット AES は安全」という根拠のない表現につながっています。いうまでもなく、これは誤解です。

安全なオンライン　システムは、必ず次の条件を満たしている必要があるからです。

- 通信を行う当事者の認証
- 中間者による傍受が起こらない暗号鍵のネゴシエーション
- メッセージ交換の機密化
- 通信中に変更されたメッセージの検出機能

SSL/TLS（Secure Sockets Layer および Transport Layer Security）　は、上記の手順をサポートするために設計されています。元々 1990 年代半ばに Netscape Communications 社によって作成されたもので、その後、インターネット上の安全な通信のためのデファクト　スタンダードとなり、Visa、MasterCard、および American Express にも支持されています。

LogMeIn Rescue で使用されている SSL 実装は OpenSSL（http://www.openssl.org）です。LogMeIn は常に、利用可能な最新のバージョンを使用しています。この文書の刊行時点で Rescue が採用しているバージョンは 1.0.2j です。

鍵の合意

サポート　セッションが開始され、サポートを受けるユーザーと技術者の間に接続が確立される際には、両者のコンピュータがセッション中に使用する暗号化アルゴリズムと対応する鍵について合意する必要があります。この手順の重要性はよく見過ごされますが、それも無理はありません。単純明解でごく平凡な作業のように思われるからです。

しかし、実際には単純どころではありません。ここでも、いわゆる中間者攻撃（コンピュータ A と B の間に位置するコンピュータ C が A と B の双方に対してそれぞれ B、A のふりをするというもの）に対抗するために、証明書を使用する必要があります。技術者とエンド　ユーザーのどちらのコンピュータにもサーバー ソフトウェアや SSL 証明書がインストールされていないため、両者は LogMeIn Rescue サーバーの 1 つにアクセスし、このコンピュータとの鍵の合意の初期フェーズを実行します。技術者コンソールとエンド ユーザー アプレットの双方が証明書を検証することで、Rescue サーバーのみがこのプロセスを仲介できることが保証されます。

メッセージ交換

TLS ではさまざまな暗号スイートを使用でき、通信する当事者どうしは双方がサポートしている暗号スキームについて合意することができます。これには主に 2 つの目的があります。1 つは、下位互換性を失うことなくプロトコルを新しい暗号スイートに拡張できるようにすること、もう 1 つは暗号上の弱点の存在が知られているスイートのサポートを新しい実装で中止できるようにすることです。

LogMeIn Rescue 通信システムの 3 つのコンポーネントはすべて LogMeIn の管理下にあるため、これらのコンポーネントで使用される暗号スイートは常に同じものです。RSA　鍵合意による暗号ブロック連鎖モードの AES256-SHA がそれです。これは以下のことを意味します。

- 暗号鍵の交換は RSA 秘密/公開鍵ペアを使用して行われる（前のセクションを参照）。
- AES（Advanced Encryption Standard）が暗号化/復号化アルゴリズムとして使用される。
- 暗号鍵の長さは 256 ビットである。
- SHA-2 がメッセージ認証コード（MAC）の基盤として使用される。MAC　とはメッセージの認証に使用される短い情報である。MAC　の値は、通信を行う当事者がメッセージの変更を検出できるようにすることで、メッセージの整合性と信頼性の両方を保護する。
- 暗号ブロック連鎖（CBC）モードでは、暗号文の各ブロックがそれ以前の平文のブロックに依存し、同じメッセージでもネットワーク上で識別することはできなくなる。

以上のことから、サポートを受けるエンド ユーザーと技術者の間でやりとりされるデータがエンドツーエンドで暗号化されること、またそれぞれの当事者だけがメッセージ ストリーム内に含まれる情報にアクセスできることが保証されます。

認証と承認

LogMeIn Rescue の認証と承認は 2 種類の目的を果たします。

認証は、Rescue システムにログインしている技術者または管理者が実際に名乗っているとおりの人物であることを保証します。Rescue では、認証は非常に直接的な方法で処理されます。技術者には、ログイン ID（通常は各自のメール アドレスに一致）と対応するパスワードが管理者によって割り当てられます。これらの資格情報は、技術者が勤務する日の業務開始時に LogMeIn Rescue Web サイトのログイン フォームに入力されます。

LogMeIn Rescue では、まず Rescue システムの認証が 2048 ビットのプレミアム RSA SSL 証明書を用いて技術者（厳密には、技術者の Web ブラウザ）に対して行われます。これにより、技術者が自らのユーザー名とパスワードを適切な Web サイトに入力することが保証されます。続いて、技術者は自らの資格情報を用いてシステムにログインします。

LogMeIn Rescue ではパスワードを保存しません。代わりに scrypt を使ってパスワードのハッシュを作成し、これを Rescue データベースに保存します。固有のパスワードごとに CSPRNG を使って 24 文字のソルトを生成し、ハッシュに適用します。

LogMeIn Rescue は、管理者に対してパスワード ポリシーに関する数々の選択肢を提供します。

- 管理者は最低限必要なパスワードの長さを強制できる。組み込みのメーター表示によって管理者および技術者は選択したパスワードの長さを知ることができる。
- 技術者に対して、次回ログイン時に Rescue パスワードの変更を強制できる。
- マスタ管理者は組織のメンバーに対して、次回 Rescue へのログイン時に 2 段階検証を強制できる。

LogMeIn Rescue では、管理者によるシングル サインオン（SSO）ポリシーの実装も可能です。Security Assertion Markup Language（SAML）が採用されています。この言語は、認証および承認データをセキュリティ ドメイン間（ID の提供者とサービス プロバイダの間）で交換するための XML 規格です。この場合、技術者はあらかじめ決められたアプリケーションにしかアクセスできませんが、1 つの SSO ID でそれらのアプリケーションにログインできます。技術者の SSO ID はスイッチ操作で無効にできます。

2 段階検証は、選択した組織のメンバーに ID を確認するための追加方法の設定を求め、LastPass Authenticator を使って Rescue アカウントに第 2 の保護レイヤを提供する機能です。以下のいずれかの場合に、認証アプリを設定します。

- 選択したメンバーが安全な web サイトで Rescue アカウントにログインを試みる場合
- 選択したメンバーが技術者コンソール デスクトップ アプリにログインを試みる場合
- 選択したメンバーが Rescue のパスワードを変更しようとする場合

LastPass 技術ホワイトペーパー: https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper-3.pdf

一方、承認の処理は非常に頻繁に（どんなリモート サポート セッションでも少なくとも 1 回は）発生します。サポートを受けるエンド ユーザーは、サポート用アプレットをダウンロードして実行した後、技術者からの連絡を待ちます。技術者は、このアプレットを介してエンド ユーザーとチャットできますが、それ以上の操作（ファイルの送信、エンド ユーザーのデスクトップの閲覧など）を行うにはユーザーからの明示的な許可が必要です。「単一の確認メッセージ」を実装することもできます。これは、セッションの途中でユーザーが不在になる可能性がある長期的なリモート サポート作業を想定したものです。このフラグが技術者グループに対して有効になっている場合、そのグループの技術者は、「グローバルな」権限をユーザーに対して要求でき、その権限が与えられたときには、エンド ユー

ザーからそれ以上の承認を受けなくても、システム情報の閲覧、リモート制御セッションへの参加といった操作を実行することができます。

また、管理者は技術者に対して IP アドレス制限を課すことができます。この制限を選択すると、利用可能な IP アドレスをごく少数のアドレスに制限できます。その場合、特定のタスクに割り当てられた技術者は、そのタスクであらかじめ承認された IP アドレスからしか Rescue にアクセスできなくなります。

また、技術者グループの管理者は、管理センターの特定の機能を無効にすることもできます。たとえば、技術者グループのメンバーによる、エンド ユーザーからのファイルの受信を禁止できます。次に、管理者が許可または禁止できる権限の例を示します。

- リモート制御の起動
- 再起動
- デスクトップ閲覧の起動
- セッションの記録
- ファイルの送受信
- プライベート セッションの開始
- ファイル マネージャの起動
- Windows 資格情報の要求
- URL の送信
- クリップボード同期の許可
- システム情報の閲覧
- スクリプトの展開
- 単一の確認メッセージですべての許可を適用
- セッションの転送
- ユーザーとの画面共有を許可

Rescue システムの認証は、サポートを受けるエンド ユーザーに対しても行われます。ユーザーがダウンロードして実行するアプレットは、LogMeIn のコード署名証明書を用いて（2048 ビットの RSA 鍵に基づいて）署名されます。通常、こうした情報は、ユーザーがソフトウェアを実行しようとするときに Web ブラウザによって表示されます。

サポートを受けるユーザーは認証されません。ユーザーがだれであるか、チャットと電話のどちらでやりとりするかの判断は、技術者に委ねられます。Rescue システムには認証に類似したメカニズム（固有の PIN コードなど）が用意されていますが、これらはサポート セッションを適切な専用または共有のキューに振り分けるために使用されるものであり、認証システムと見なすのは適切ではありません。

監視とログ

あらゆるリモート サポート ソリューションは、アカウンタビリティ（説明責任）を非常に重視する必要があります。LogMeIn Rescue には 2 種類の監査機能があります。

まず、いわゆる「チャット ログ」が Rescue データベースに保存されます。「チャット ログ」は、技術者コンソールによって Rescue サーバーにリアルタイムで送信され、そこにはイベントや特定のサポート セッションに関連するチャット メッセージが記録されています。たとえば、ログ ファイルには、リモート制御セッションがいつ開始されて終了したか、また技術者がいつファイルをエンド ユーザーに送信したかが記録されます。メタデータ（送信されたファイルの名前や MD5 ハッシュ拇印など） が付随する場合には、それらもログに含められます。「チャット ログ」データベースに対する問い合わせは管理センターから実行できます。この文書の刊行時点では、LogMeIn のデータ保持ポリシーによって、ログの内容がそのリモート サポート セッションの終了から 2 年間はオンラインで参照できること、さらにその後 2 年間はアーカイブとして保存されることが規定されています。CRM システムとの統合を容易にするために、LogMeIn Rescue ではセッションの詳細を URL に送信できます。管理者は、こうした詳細情報からチャットのテキストを除外できるようにするかどうかを選択できます。また、技術者とエンド ユーザーとの間のチャット テキストのすべての記録を Rescue データ センターに保存されるセッションの詳細から自動的に除外することもできます。

次に、LogMeIn Rescue では、デスクトップ閲覧またはリモート制御のセッション中に発生するイベントを技術者がビデオ ファイルに記録することができます。これは説明責任および法的責任に関する理由から非常に重要な機能です。記録ファイルは技術者が指定したディレクトリに保存されます。大規模なサポート組織の場合、この保存場所はネットワーク サーバー上にする必要があります。こうした記録に必要なディスク領域は、サポートを受けるエンド ユーザーのデスクトップの内容 （および圧縮性） のみに依存して大きく変わってきます。LogMeIn の技術を利用している何百万というリモート制

御セッションの分析に基づくと、1 分間のリモート制御データの保存に必要な平均ディスク領域は 372 ～ 1024 KB です。記録データは AVI 形式で直接保存されるか、LogMeIn 独自の中間形式で保存されます。この独自形式は、help.logmein.com からダウンロード可能なアプリケーション「Rescue AVI Converter」によって標準の AVI ファイルに変換できます。この LogMeIn 独自形式は RCREC と呼ばれ、記録サイズを約 10% 削減できます。

データ センターのアーキテクチャ

LogMeIn Rescue は、次のような機能を備える、最先端で安全なデータセンターによってホストされます。

- 多重のセキュリティ制御手順、バイオメトリクス入退室管理システム、および年中無休 24 時間稼働の有線ビデオおよび警報による監視機能
- 無停電の冗長化された AC、DC 電源、オンサイトの予備発電機
- 高床式で換気を行う HVAC 冗長化設計により、温度を最適にコントロール
- 煙検知システムを高床の上と下に設置、二重連動/プリアクション/ドライパイプによる消火

次のように、LogMeIn Rescue はインフラストラクチャ自体が非常に高い安全性と信頼性を備えています。

- サーバー コンポーネント レベルの冗長性：冗長化された電源および冷却ファン、RAID-1 ミラーリングされたハードディスク
- サーバー レベルの冗長性：役割に応じたアクティブ/パッシブまたはアクティブ/アクティブ クラスタ
- データセンター レベルの冗長性：準即時的なフェイルオーバー機能を備えた 6 つのデータセンター（米国の西海岸、中央部、南中部、東海岸、英国のロンドン、ドイツのフランクフルト）
- 80 番および 443 番ポートだけをオープンした二重化されたファイアウォール
- アクティブ/パッシブ データベース クラスタ
- SSL を含む冗長化された負荷分散装置
- 負荷分散式の冗長化された Web およびアプリケーション サーバー クラスタ
- 負荷分散式の冗長化されたゲートウェイ サーバー クラスタ

RESCUE のゲートウェイ移管プロセスの概要

デジタル署名された Rescue アプレットがコンピュータ上で開始されたとき：

- アプレットにはセッション認証 GUID（グローバルー意識別子）が含まれている。この GUID は、アプレットのダウンロード時にサイトによって .exe ファイル内にリソースとして埋め込まれる。
- アプレットが利用可能なゲートウェイのリストを secure.logmeinrescue.com からダウンロードする。
- アプレットがリストからゲートウェイを選択し、TLS を使用してそのゲートウェイに接続する。このゲートウェイの認証は、アプレットによってその SSL 証明書を用いて行われる。
- ゲートウェイがデータベース内のアプレットを GUID を用いて認証し、ユーザーが技術者を待っていることを登録する。

Rescue の技術者コンソールでセッションが選択されたとき：

- 技術者コンソールとクライアント アプレットとの接続を中継するために、要求とセッション認証 GUID がゲートウェイに送信される。
- ゲートウェイが接続の認証を行い、転送レベルでデータの中継を開始する（中継データの復号化は行わない）。

接続の中継が開始されると、通信する各当事者がピアツーピア (P2P) 接続の確立を試みる。

- アプレットが Windows によって割り当てられたポートで TCP 接続待ちの状態になる。
- TCP 接続を制限時間 (10 秒) 内に確立できなかった場合は、ゲートウェイの支援を得て UDP 接続の確立を試みる。
- TCP 接続と UDP 接続のどちらかが確立された場合、通信する各当事者は P2P チャネルの認証を (セッション認証 GUID を用いて) 行い、中継された接続からトラフィックを引き継ぐ。
- UDP 接続が確立された場合は、TCP のエミュレーションが UDP データグラム上で XTCP を使用して行われる。XTCP は BSD TCP スタックに基づいた LogMeIn 独自のプロトコルである。

すべての接続は TLS プロトコル (AES256 暗号化と SHA256 MAC を使用) によってセキュリティ保護されます。セッション認証 GUID は 128 ビットの暗号化されたランダムな整数値です。

データベース

- 機密情報が含まれるデータは 256 ビットの AES 暗号で保護されます (チャット ログおよびカスタム フィールド)。
- Rescue データベースは、24 時間に一度の間隔で自動的にバックアップされます。バックアップ データベースは、元のデータベースと同じ暗号を使ってデータセンターに保存されます。
- Rescue では、エンド ユーザーのデータを EU (フランクフルト、ロンドン) に保存するか、米国に保存するかを選択できます。データの保存先として EU を選択した場合は EU 内のデータセンターにのみ接続され、ユーザーのデータは選択された地域内にのみ保持されます。EU 内のデータセンターと米国内のデータセンターの間に接続はありません。

RESCUE メディアのアーキテクチャ

Rescue メディア サービスは、Rescue Lens ビデオ ストリーミングを処理する WebRTC ベースのスタンドアロン サービスです。このサービスは、Lens 機能を使う Rescue セッションのために、いわゆる「会議」を管理します。会議の出席者 (ピア) は会議への参加と退出を行い、クライアントはビデオと音声をストリームで送信して他の参加者が試聴できるようにします。Lens は、ビデオ コンテンツを Lens アプレットから技術者コンソールまでの一方向のストリームで送信します。

メディア サービスには、MediaSDK、セッション マネージャ、およびストリーミング サーバーの 3 つの主なコンポーネントがあります。これらのコンポーネントは、会議の作成 / 破棄および参加 / 退出のプロセスを管理します。各コンポーネントは、技術者コンソールと Web サイトとの間、および Lens アプリと Web サイトとの間の既存のセキュアな接続を使って通信します。

MediaSDK

メディア サービスは、WebRTC コード ベースを薄いラッパーで覆うことにより、WebRTC を基盤として構築されました。このいわゆる MediaSDK は、技術者コンソールとモバイル Lens アプリで使用されます。

セッション マネージャ

セッション マネージャは、負荷分散型のシンプルな Web サイトで、会議の管理 (作成 / 破棄 / 参加 / 退出) のために REST API を提供します。セッション マネージャは、この Web サイトからの要求のみを受け付けます。

ストリーミング サーバー

メディア サービスは、Jitsi オープン ソース ストリーミング サーバー ソリューションを使って、ピア (技術者コンソールと Lens アプリ) 間のストリームを処理しています。技術者コンソールと Lens アプリは、どちらもストリーミング サーバーに接続され

ます。Lens アプリは、ビデオ コンテンツをストリーミング サーバーにストリームで送信します。技術者コンソールは、このサーバーからビデオ コンテンツをストリームで取得します。Jitsi は、ピア間のリレー サーバーのように動作します。Lens セッションには、2 つのストリーム（送信されるストリームと受信されるストリーム）があります。

LOGMEIN RESCUE が順守する業界標準

SOC 2

LogMeIn Rescue はサービス オーガニゼーション コントロール 2（SOC 2）の認定を受けており、顧客の大切なデータを守るために適切な制御を使用していることを保証します。

SOC 2 は複数の原則と基準に基づく包括的な監査方法で、データ処理に使用される制御システムのや、これらのシステムで処理される情報の機密性について確認するものです。SOC 2 への順守が維持されていることを確認するため、毎年見直しを行う必要があります。ソフトウェア会社にとって至適基準である SOC 2 は米国内のさまざまな業種間で広く認識されていますが、 SOC 2 保証の獲得と維持はセキュリティやプライバシーに対する当社の取り組みのほんの一例です。

GDPR

一般データ保護規則（GDPR）は、欧州連合（EU）内における個人データやプライバシー保護に関する欧州連合の規則です。GDPR の主な目的は、市民や住民が自身の個人データを制御できるようにすることや、EU 内の規制環境を簡素化することです。LogMeIn Rescue のユーザーは、LogMeIn Rescue が代行保存しているデータを制御でき（内容はサービス規約の定義に基づく）、GDPR の準備を効率的に行いながら中核業務に集中できます。

- Rescue のユーザーは、管理センターのレポート機能や Rescue API を使用してデータをエクスポートできる。
- Rescue のユーザーは、LogMeIn Rescue サーバーに保存されたデータを削除できる。
  - サポート技術者に関連するすべてのデータの削除
  - ユーザーに関連する個人データやユーザーに結び付いた個人データなど、サポート セッションに関連するすべてのデータの削除

LogMeIn Rescue のこれらの機能により、ユーザーは GDPR の基準や要件を満たすことができます。

GDPR の詳細については、LogMeIn GDPR のサイトをご欄ください。

HIPAA

LogMeIn はユーザーによって共有されたコンテンツをサポート セッション中に制御することはできませんが、LogMeIn Rescue サービスは厳しいセキュリティ規格を満たすように設計されているため、HIPAA によって規制される組織は関連する規制ガイドラインを順守できます。

アクセス制御

- 権限ベースのアクセスを詳細に定義できる（リモート閲覧の使用は許可するが、リモート制御は許可しない、など）。
- リモート デバイスのデータは LogMeIn データセンター サーバーに一切保存されない（前述のように、セッションおよびチャット ログのみが保存される）。また、チャット テキストのログはセッションの詳細から削除できる。
- 技術者がファイルを転送できないように権限を設定することで、技術者はリモート デバイスからファイルを持ち出せなくなる。
- エンド ユーザーはリモート デバイスの前にいて、リモート アクセスを許可する必要がある。
- エンド ユーザーは制御を維持し、セッションをいつでも終了できる。

- エンド ユーザーが技術者に明示的に権限を付与するまで、技術者はその機能を使用できない （リモート制御、デスクトップ閲覧、ファイル転送、システム情報、再起動と再接続など）。
- アクセス権はセッションの終了時に自動的に消滅する。
- 操作がないままあらかじめ定められた時間が経過すると自動的にログオフする。
- 通信事業者レベルの冗長化されたデータ センターによってホストされ、データ センターへのアクセスには制限とセキュリティ対策が施されている。

監査の制御

- セッションの記録を強制的に実行し、監査ファイルを安全な共有ネットワーク上に保存できる。
- 技術者のセッションおよびリモート セッション活動は、セキュリティの確保と品質制御の維持のためにホスト コンピュータにログとして記録される （ログインの成功と失敗、リモート制御の開始と終了、リブートの開始、ログアウト）。
- 個人または組織の認証。
- 技術者の ID は固有のメール アドレスまたは SSO ID によって定義され、技術者は認証を受ける必要がある。
- ログインの失敗が続くと、アカウントがロックされる。
- 技術者は、承認された IP アドレスからのログインのみが許可される。

通信のセキュリティ

- エンドツーエンドの 256 ビット AES ですべてのデータが暗号化される。
- MD5 ハッシュによってファイル転送の追跡可能性が強化される。

まとめ

リモート サポート ソリューションを選択する際には、多くの場合、機能と価格が決め手になります。この文書をお読みになっているということは、LogMeIn Rescue がこうしたカテゴリでお客様のニーズを満たしているということでしょう。これまでに記した情報により、Rescue の基盤となるアーキテクチャが適切なレベルのスケーラビリティ、セキュリティ、および使いやすさを備えていることをご理解いただけたと思います。