TeamViewer は **データの保護**を真剣に考慮しています。

ドイツの企業である当社は、高い要件のドイツのセキュリティ基準を満たすことに専念しています。当社では、お客様のデータセキュリティ、作業環境のプライバシー、そして不正防止のために、さまざまな対策を講じています。TeamViewer では暗号化やコードサイニング、2 要素認証などが背後で働くことによってセキュリティが保たれています。さらに日々の仕事の中でもセキュリティを維持する便利な機能も提供しています。

TeamViewer **セキュリティ**

TeamViewer ID
TeamViewer ID はデバイスごとに割り振られる 固有の ID です。自動的に生成され、個別のセッションの前にチェックされます。

世界で最も高いセキュリティ基準
当社のメインのデータセンターは、ISO 27001 産業セキュリティ基準を満たしています。

ブルートフォース攻撃からの保護
TeamViewer は、ログイン試行の失敗間隔が指数関数的に増加した後に正しいパスワードが入力されたとき、パスワードをリセットします。リモートアクセスデバイスまたは接続パートナーも他の攻撃から保護されます。

TeamViewer パスワード
TeamViewer は、TeamViewer サービスが再起動するたびに、自動的に新たな動的セッションパスワードを生成します。ただし、セッション終了ごとに自動的に新たな動的セッションパスワードを生成するオプション設定もあります。このパスワードは、標準で 6 文字のアルファベットを使用します。つまり、21億通りを超えるの組み合わせが可能です。

セキュアリモートプロトコル (SRP)
TeamViewer では認証とパスワード保護のために SRP プロトコルを使用しています。パスワードは暗号化されるうえにインターネットに送信されることも決してありません。外部アクセスから最適に保護されます。パスワードはバックエンド暗号化も受け付けます。

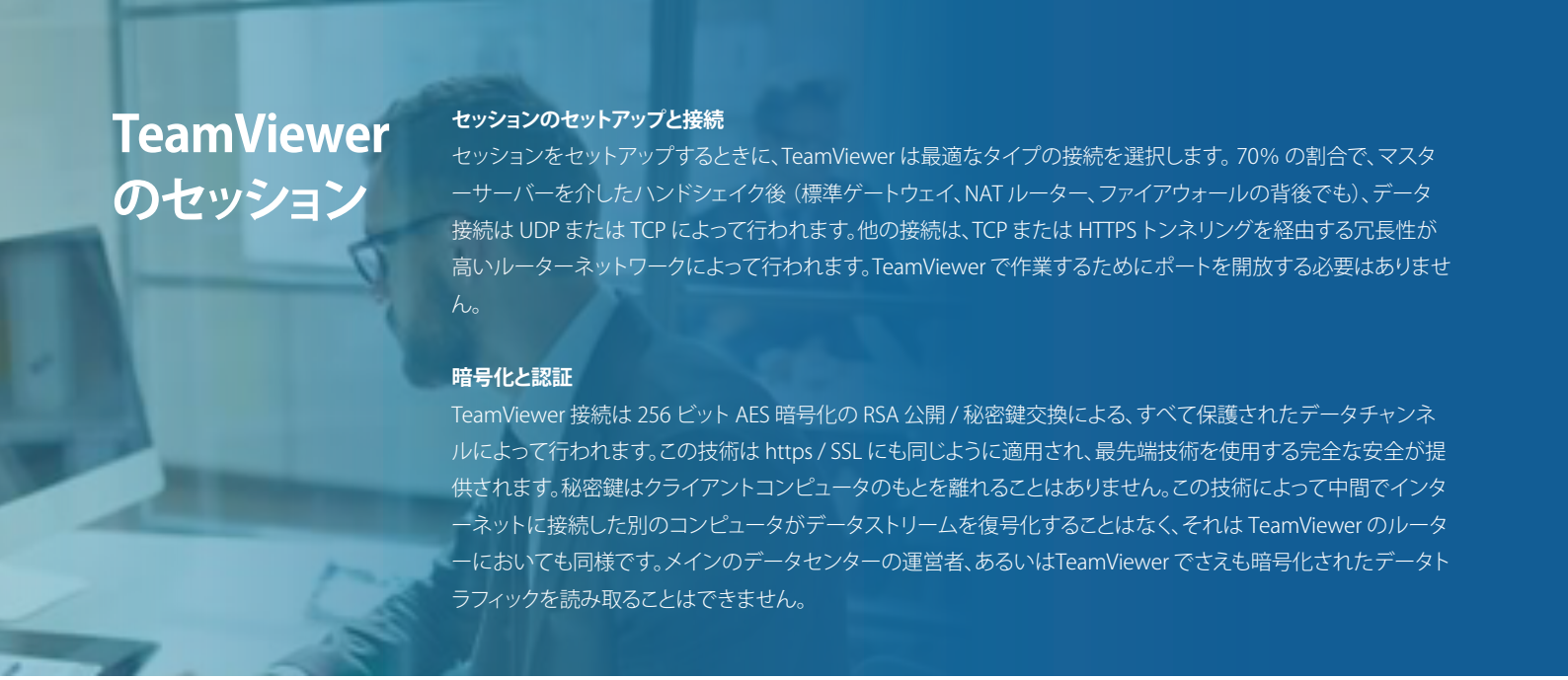
暗号化
ファイル転送、VPN、チャットなどを含む、TeamViewer でのすべての操作は、2048 ビット RSA 公開 / 秘密鍵のエンドツーエンド暗号化によって保護されます。

コンディショナル アクセス*
コンディショナルアクセスを使用し、未承認のアクティビティを防ぎ、セキュリティのガイドラインを調整するためにリモートアクセスのルールを強化することができます。

2 要素 認証
2 要素認証では、ログインごとに新たなパスワードが使用されます。パスワードはアルゴリズムによって毎回異なったものがモバイルデバイスから提供されます。

*TeamViewer Tensor で使用可能です。諸条件が適用されます。

AICPA SOC
A-LIGN HIPAA
südcert ISO 9001
VeriSign Trusted
ISO ISO/IEC 27001



TeamViewer のセッション

セッションのセットアップと接続

セッションをセットアップするときに、TeamViewer は最適なタイプの接続を選択します。70% の割合で、マスターサーバーを介したハンドシェイク後（標準ゲートウェイ、NAT ルーター、ファイアウォールの背後でも）、データ接続は UDP または TCP によって行われます。他の接続は、TCP または HTTPS トンネリングを経由する冗長性が高いルーターネットワークによって行われます。TeamViewer で作業するためにポートを開放する必要はありません。

暗号化と認証

TeamViewer 接続は 256 ビット AES 暗号化の RSA 公開 / 秘密鍵交換による、すべて保護されたデータチャンネルによって行われます。この技術は https / SSL にも同じように適用され、最先端技術を使用する完全な安全が提供されます。秘密鍵はクライアントコンピュータのもとを離れることはありません。この技術によって中間でインターネットに接続した別のコンピュータがデータストリームを復号化することはなく、それは TeamViewer のルーターにおいても同様です。メインのデータセンターの運営者、あるいはTeamViewer でさえも暗号化されたデータトラフィックを読み取ることはできません。

コンプライアンスとデータ保護

信頼されているデバイス

信頼されてるデバイスではない、新しいデバイスが既存の TeamViewer アカウントへログインを試みると、初回のみ認証が要求されます。

データの整合性

データの整合性は、サイバー犯罪からの保護を提供します。システムは、ユーザーアカウントのあらゆる異常な動きを継続的にチェックし、検出された際には自動でパスワードリセットを発動します。

許可リスト / ブロックリスト

この機能は、監視されていない状態で保守されているコンピュータに TeamViewer がインストールされている場合に特別な保護を提供します。許可リストは、アクセスを許可するクライアントを決めるために使用します。ブロックリストは、ブロックする TeamViewer ID とアカウントを決めるために使用します。

コードサイニング

すべての TeamViewer プログラムは VeriSign によってデジタル署名されており、発行者は固有の ID によっていつでも識別可能です。

ISO/IEC 27001

当社のデータセンターは ISO/IEC 27001 標準の認定を受けています。これは、セキュリティ管理と制御の国際標準であるということを表しています。

ISO 9001:2015

TeamViewer はまた、品質管理システム (QMS) の 9001:2015 認定も受けています。

EU 一般データ保護規則 (GDPR)

2018年 5月 25日、EU 一般データ保護規則（GDPR）が施行されました。これには、デジタル化が進行する世界におけるデータ保護の重要性が反映されています。TeamViewer はグローバルに展開している組織であるため、お客様と当社の社員の個人情報を GDPR に準拠して扱うことは重要です。TeamViewer のデータプライバシー保護への取り組みと GDPR への準備に関する詳細は、当社のナレッジベースをご覧ください。

HIPAA, HITECH、SOC2 認証

TeamViewer は、米国全域にわたるセキュリティとコンプライアンスプロバイダである A-LIGN から HIPAA、HITECH、SOC2 の認証を受けました。

医療機関にとっては、機密データや保護された健康情報（PHI）の機密性と安全性を確保するために、HIPAA と HITECH の認証が不可欠です。SOC2は、サービス提供組織が財務以外の内部統制を報告する手段を確立し、信頼されるサービスの 5 つの原則（TSP）の実施状況を顧客に理解してもらうための必須の報告フレームワークとなっています。

TeamViewer

TeamViewerジャパン株式会社
東京都千代田区丸の内1-5-1 新丸の内
ビルディング EGG JAPAN 10 F
Tel: 03-4563-9650

快適な接続を