技術概要

TeamViewer のセキュリティ

はじめに

このセキュリティに関する技術ドキュメントは、TeamViewer のセキュリティ基準とプロトコルの概要を理解したい IT プロフェッショナルおよびネットワーク管理者に向けて書かれたものです。セキュリティについての懸念を解消するために、顧客や同僚の方へ本書を自由に共有してください。

ネットワーク管理者以外の方は、「TeamViewer : 当社およびソフトウェアについて」で、セキュリティについての当社のコミットメントと方針の概要をご確認ください。

TeamViewer : 当社およびソフトウェアについて

TeamViewer について

TeamViewer GmbH は、2005年にドイツのゲッピンゲンで設立されました。ドイツ ゲッピンゲンに本社を置き、米国、オーストラリア、アジアの各地にオフィスを構えています。安全なリモートアクセスとサポートのためのリモート接続ソフトウェア、IoT ソリューション、カスタマーエンゲージメント、そして産業用の拡張現実ワークフローの開発および販売をしています。短期間のうちに無料バージョンの TeamViewer は急速に世界中に普及しました。世界 200 か国以上、2 億を超えるユーザーがおり、利用デバイスは 25 億台以上におよびます。ソフトウェアは 30 か国語を超える言語でご利用いただけます。

TeamViewer セキュリティの基礎

TeamViewer は、1日に 4500万人以上のユーザーが同時に使用しています。これらのユーザーは、インターネットを介したリモートサポートのスポット提供や、無人コンピュータへのアクセスとサポート (サーバーのリモートサポートなど)、オンラインミーティングなどを行っています。設定次第では、TeamViewer はコンピュータのマウスやキーボードをリアルタイムで遠隔操作し、あたかも自分がその場にいるかのように使用することができます。

Windows、Mac、Linux の管理者がリモートコンピュータにログインした場合、その人にはそのコンピュータの管理者権限も付与されます。インターネットを介してこのような強力な機能を使う際には、当然ながら厳重なセキュリティプロトコルで保護する必要です。ゆえに、当社ではすべての中心にセキュリティを位置付けてソフトウェアを設計 (セキュリティ バイ デザイン) し、開発を行っています。

当社のゴールは、安全なコンピュータアクセスを提供することです。セキュリティは当社の最優先事項であり、ユーザーは安全なソリューションのみを信頼します。当社では顧客が長期的なビジネスの成功を維持するための安全なソリューションを提供することに全力を尽くします。

品質管理

セキュリティ管理のためには、品質管理システムの確立は欠かせません。TeamViewer GmbH は、ISO 9001 の認証を受けた品質管理システム (QMS) を持つ、市場をリードするグローバルベンダーです。当社の品質管理は、国際的に認められた規格に準拠しており、毎年、外部の監査機関によってレビューされています。

外部の専門家による評価

TeamViewer ソフトウェアは、ドイツ IT 鑑定士査定人協会 (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.) によって最高評価の 5つ星の品質評価を受けています。BISG e.V.の独立した審査員が、品質、セキュリティ、サービス特性について、認定メーカーの製品を審査します。

参考

金融サービス、ヘルスケア、政府機関、その他機密性の高いデータを扱う組織など、様々な業界の大手グローバル企業が、安全なリモートアクセスやサポート、カスタマーエンゲージメント、IoT、産業用拡張現実ソリューションのために TeamViewer を利用しています。

TeamViewer がそれぞれのお客様の組織でどのように利用されているかは、Web サイト teamviewer.com/customersで公開されているお客様の事例をご覧ください。

TeamViewer の接続

リモート接続とセッション

リモートセッションを確立する際、TeamViewer は最適な接続タイプを判断します。当社のマスターサーバーを通してハンドシェイクした後、標準的なゲートウェイ、NAT、ファイアウォールを経由した場合でも、すべてのケースの 70 %で、UDP（ユーザ データグラム プロトコル）またはTCP（トランスミッション コントロール プロトコル）による直接接続が確立されます。残りの接続は、TCP または HTTP トンネリングで、冗長性が非常に高いルーターネットワークを経由してルーティングされます。TeamViewer を使用するためにポートを開放する必要はありません。次の「安全な接続」セクションに記載されるように、ルーティングサーバーを運用している TeamViewer であっても、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。

安全な接続

TeamViewer のトラフィックは、RSA 4096 公開鍵/秘密鍵交換および AES 256 ビットによるセッション暗号化を使用してセキュリティ保護されます。このテクノロジーは、HTTPS/TLS と同等の形式で使用されており、今日の基準では完全に安全と見なされています。秘密鍵がクライアントコンピュータから外に出ることがないため、TeamViewer のルーティングサーバーも含めて、相互接続されるコンピューターがデータストリームを解読することは不可能です。

各 TeamViewer クライアントはマスタークラスタの証明書を持ち、TeamViewer システムの証明書を検証することができます。これらの証明書は、TeamViewer ネットワークの参加者間のハンドシェイクで使用されます。

図1 簡略化したハンドシェイクによる鍵交換の概要

図 1 : このハンドシェイクで得られたセッションキーは、当事者間の通信を AES で暗号化するために使用される。

パスワード認証

TeamViewer ではパスワードの認証プロセスにセキュア リモート パスワード (SRP) プロトコル バージョン 6 を使用し、そのプロセス中にパスワードに相当するデータが共有されることはありません。パスワード ベリファイアのみローカルコンピュータに保存されます。詳しくは「TeamViewer アカウント」セクションをご参照ください。

TeamViewer ID の検証

TeamViewer は、ハードウェアおよびソフトウェアのさまざまな特徴に基づき、TeamViewer ID を自動で生成します。
TeamViewer サーバーは、これらの ID の有効性を検証します。

ブルートフォース攻撃からの保護

TeamViewer のセキュリティの話題となると、暗号化についての質問をされることがよくあります。当然ながら、そのような質問をする方は TeamViewer アクセスデータの盗聴や、第三者による監視などがないかということを強く懸念しています。TeamViewer ではブルートフォース攻撃へのセキュリティプロトコルを備え、接続の安全性とプライバシーを確保しています。

コンピュータ セキュリティの世界では、リソースを保護するパスワードをトライ & エラーを大量に繰り返すことで推測する攻撃手法をブルートフォース攻撃と呼んでいます。コンピュータの計算能力は向上しており、長いパスワードの推測に要する時間は大幅に短縮されています。

TeamViewer では、パスワード入力を失敗するたびに、再試行するまでの待ち時間を指数関数的に増加させることで、ブルートフォース攻撃に備えています。例えば、24 回失敗すると、待ち時間は 17 時間かかります。正しいパスワードを入力するまで、これをリセットすることができないのです。

TeamViewer は特定の 1 台のコンピュータによる攻撃から顧客を保護するだけではありません。大量のコンピュータを制御して特定のコンピュータにアクセス (ボットネットを使用するなど) しようとする攻撃者からも保護するメカニズムを備えています。

コードサイニング

さらなるセキュリティレイヤーとして、当社のすべてのソフトウェアはデジサート コードサイニングによって署名されています。これによって、ソフトウェアの発行元は常に容易に特定できるようになっています。後にソフトウェアが変更された場合、電子署名は自動的に無効になります。

データセンターおよびバックボーン

TeamViewer のサービスに関して、最大限のセキュリティと可用性を提供するため、TeamViewer のすべてのサーバーは、ISO 27001 に準拠し、マルチキャリア接続と電源の冗長化を備えたデータセンターに設置されています。さらに、業界グレードのハードウェアのみを使用し、重要なデータを保存するすべてのサーバーは、ドイツまたはオーストリアに設置されています。

ISO 27001認定を受けているということは、個人のアクセス制御、ビデオカメラ監視、モーション検出、年中無休の監視、および現場のセキュリティ担当者により認証を受けた人物のみデータセンターにアクセスできること、そしてハードウェアとデータセキュリティに関して最大限に保証されていることを意味しています。また、データセンターに設けられている入口は 1 カ所だけで、入念な ID チェックが行われています。

TeamViewer アカウント

TeamViewerアカウントは、専用 TeamViewer サーバーにホストされます。アクセス制御に関する情報については、「データセンターとバックボーン」セクションをご参照ください。認証には、セキュア リモート パスワードプロトコル (SRP) バージョン 6 を使用します。このプロトコルは、従来のパスワード保存方法の利点を組み合わせたものです。許可されていない第三者がアカウントによる認証に使用する可能性のある情報は、サーバーに保存しません。また、認証のためにパスワードが当社のサーバーに送信されることもありません。TeamViewer では、認証実行一回限りに有効な、再使用されない独自の認証プロセスを使用しています。

パスワード、キー、チャットログなどのアカウントに保存される情報は、RSA と AES の組み合わせによって暗号化され、暗号化のためのルートキーはユーザーのパスワードから取得されます。これにより、パスワードがなければアカウントに保存されたデータにアクセスできないようになっています。

管理コンソール

TeamViewer 管理コンソールは、ユーザー管理、接続レポート、コンピュータおよびパートナー管理のための Web ベースのプラットフォームです。このツールは、ISO:27001 認証を取得した HIPAA 準拠のデータセンターにホストされています。すべてのデータ転送は、安全なインターネット ネットワーク接続の標準である TLS (Transport Security Layer) 暗号化を使用するセキュアなチャネルを経由して行われます。重要なデータは AES/RSA 256 ビットで暗号化して保存されます。TeamViewer アカウントで説明したものと同じメカニズムで暗号化と認証を行います。

ポリシーベースの設定

ユーザーは、TeamViewer 管理コンソール内から、自分に所属するデバイス上の TeamViewer ソフトウェアインストールの設定ポリシーを定義、配布、実行することができます。設定ポリシーは、これを生成するアカウントによって電子署名されます。これにより、デバイスにポリシーを割り当てる許可を受けたアカウントのみ、デバイスが所属するアカウントであることが保証されます。

TeamViewer のアプリケーションセキュリティ

ブロックリストと許可リスト

特に、TeamViewer を無人コンピュータの保守とサポート (リモートコンピュータのそばに人員が不在で、接続要求の受付操作をできない環境など) に使用するとき、許可リストがそのセキュリティを高めます。TeamViewer ID またはアカウントを許可リストに追加することで、指定したマシンにアクセスする相手を、明示的に指定した ID またはアカウントに制限することができます。さらに、パスワードの紛失や漏洩があっても、許可されていない第三者がそのデバイスにアクセスすることはできません。指定した TeamViewer ID または TeamViewer アカウントのみがコンピュータへリモートアクセスできるように設定できます。許可リストは、「管理コンソール」セクションに記載したポリシーを使用して管理できます。

ブロックリストを使用すると、特定のパートナーまたはデバイスが自分のコンピュータへの接続を確立するのを防ぐことができます。ブロックリストに登録された TeamViewer アカウントまたは TeamViewer ID はそのコンピュータに接続することはできません。

注意 : ブロックリストに登録されたパートナーに対して、TeamViewer の発信セッションを確立することはできます。

チャット

チャットメッセージとその履歴は、エンドトゥエンドで暗号化され、「TeamViewer アカウント」のセクションに記載された RSA/AES を使用して TeamViewer アカウントに保存されます。チャットルームの参加者または 1 対 1 のチャット相手のみがメッセージと履歴にアクセスできます。

ステルスモードなし

TeamViewer をバックグラウンドで検知されずに動作させる機能はありません。アプリケーションが Windows サービスとしてバックグラウンドで動作する場合であっても、システムトレイにアイコンが表示され、TeamViewer を常に確認することができます。接続が確立すると、システムトレイの上に小さなコントロールパネルが必ず表示されます。このように、TeamViewer は、コンピュータや社員をひそかに監視するには不向きなツールとして意図的に作られています。これによりユーザーは、重要なデータや機密データが TeamViewer セッション中に画面に表示されるのを防ぐことができます。

信頼済みデバイス

信頼済みデバイスは、2要素認証に代わるもので、TeamViewer アカウントにさらなるセキュリティレイヤーを提供します。

2 要素認証を設定しない場合、信頼済みデバイスが自動的に適用されます。これはアカウントのセキュリティを確保するための予防的な方法です。新しいデバイスやブラウザから初めて TeamViewer アカウントにアクセスするときは、手動で認証する必要があります。

認証プロセスの一環で、E メールが TeamViewer アカウントに関連付けられたメールアドレスに送信されます。信頼済みデバイスとしてデバイス、ブラウザ、IP を追加しない限り、ログインすることができません。ログインを認証するには、メールの受信トレイへのアクセスも必要となるため、他者によるアカウントへのログインを防ぐことができます。

信頼済みデバイスと信頼済みデバイスの管理の詳細は、TeamViewer ナレッジベースをご参照ください。

1. 信頼済みデバイス: https://community.teamviewer.com/Japanese/kb/articles
2. 信頼済みデバイスの管理 : https://community.teamviewer.com/Japanese/kb/articles

パスワード保護

スポットの顧客サポートでは、TeamViewer と TeamViewer QuickSupport は随時変更可能なランダムパスワードを生成します。接続パートナーやサポート依頼者からパスワードを提供されるときは、相手の ID とパスワードを使用してコンピュータへ接続することができます。設定に応じて、再起動の後、セッションの後、手動で要求されたときに、TeamViewer は新しいパスワードを生成します。TeamViewer QuickSupport は起動時とユーザーによる要求時に、常に新しいパスワードを生成します。

無人デバイスのリモートサポート (サーバーへのアクセスと保守など) で TeamViewer を利用する際は、次のことを推奨します。

- 安全な無人サポートを提供するために、パスワード不要の簡易アクセスを設定する。https://community.teamviewer.com/Japanese/kb/articles 可リストにデバイスを定義する。

2 要素認証と組み合わせて、これらのセキュリティ機能を使用することで、許可された相手のみが特定のデバイスへアクセスできるようにすることができます。

すべてのパスワードは、「TeamViewer アカウント」セクションに記載した SRP プロトコルによって認証されます。

受信と発信のアクセス制御

TeamViewer の接続モードは個々に設定することができます。例えば、リモートサポートやミーティング用のコンピュータは、接続を受信できないように設定することができます。

機能を実際に必要なものに制限することは、侵害や攻撃などの潜在的なリスクを低減する効果があります。

2 要素認証

TeamViewer は、企業の HIPAA および PCI コンプライアンス要件を支援します。2 要素認証によって、TeamViewer アカウントを不正アクセスから保護するため、セキュリティレイヤーが追加されます。

ユーザーが認証されるには、ユーザー名とパスワードに加えて、コードを入力する必要があります。そのコードは短時間のみ有効で、Time-based One-time Password (TOTP) アルゴリズムによって時間に基づいて生成されます。

2 要素認証と許可リストへデバイスを登録してアクセスを制限することで、TeamViewer は HIPAA と PCI 準拠に必要なすべての要件を満たします。

セキュリティテスト

TeamViewer のインフラストラクチャとソフトウェアには、定期的に侵入テストが行われています。このテストは、セキュリティテストを専門とする独立した会社によって実施されます。

ご質問は?

詳しくは、TeamViewer ジャパン株式会社、**03-4563-9650** または teamviewer.com/support からオンラインでお問合せください。

お問い合わせ先

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 10F

TeamViewer について

チームビューワーはリモート接続プラットフォームのグローバルリーダーとして、デジタル化を推進するあらゆる規模の企業を支援しています。リモート接続ソリューションである『TeamViewer』は、PC、モバイル端末、工場の機械やロボットなどのデバイスと人、そして場所や時間を問わず世界のユーザーとの接続を可能にし、セキュリティの高いリモートアクセス、サポート、コントロール、コラボレーション機能がいかなるオンライン上のエンドポイントでも利用可能です。個人向けには無償で提供しており、現在62万人以上が登録。法人は中小企業から大企業まで多様な業種で利用されています。チームビューワーはデバイスの分散化、自動化、ニューノーマルといった環境の変化に柔軟に対応しながらAR、IoT、AIの分野でのDXやイノベーションを主導しています。会社設立以来、『TeamViewer』がダウンロードされているデバイスは現在25億台に達しています。
会社設立は2005年。本社はドイツのゲッピンゲン、従業員は全世界で約1,500名。2021年度の売上は約5億4,800万ユーロ。TeamViewer AG（TMV）はフランクフルト証券取引所に上場しており、MADAX株式指数構成銘柄となっています。TeamViewerジャパン株式会社はTeamViewerの日本法人として2018年に設立されました。

Stay Connected

www.teamviewer.com