TeamViewer セキュリティ保護方針

本書をお読み頂く前に

本セキュリティ保護方針の記載内容には専門性を必要とする高度な技術情報が含まれており、主にネットワーク管理者を対象にしております。TeamViewer をご利用頂く前に本書を参照いただくことで、システム管理者の方々に本ソフトウェアのセキュリティの詳細をご理解いただけるようになっております。また、エンドユーザー様がセキュリティに関してご不明点がある場合に配布していたくことも可能です。

尚、システム管理者でない方々には、次の「当社 / 当ソフトウェア」をお読みいただきますと当社ソフトウェアの概要をご理解いただけるようになっております。

当社/当ソフトウェア

会社概要

TeamViewer GmbH は 2005 年に設立されました。ドイツ南部のゲッピンゲン(シュトゥットガルト近郊)に本社があり、オーストラリアとアメリカ合衆国に支社があります。設立以来の継続した成長により、世界中でのインストール回数は既に 2 億回を超え、約 200 カ国に及ぶ国々にてご利用いただいており、ご利用可能な言語数は 30 カ国語を超えます。

ソフトウェアの開発はドイツ国内のみで行われています。

セキュリティについての当社の理解

TeamViewerは、世界中で何百万回も使用されています。無人コンピュータ(サーバーのリモートサポート等)にアクセスしてインターネット上で自動サポートを提供し、オンライン会議をホストします。TeamViewer では、設定に応じて遠隔地にある端末を実際に目の前にあるようにスムーズかつ簡単に操作することが可能です。リモートコンピュータにログオンしているユーザが Windows、Mac、Linux 端末の管理者のいずれであっても、そのコンピュータ上で管理者権限を持った状態で操作可能です。

このような重要機能をインターネットを介して使用する場合、不正な攻撃を阻止できるよう十分な対策が重要となります。セキュリティに関する課題は当社での製品開発目標の中でも最重要課題として扱っています。リモートコントロールソフトウェアの使用に当たり、世界中の何千万ものユーザーが信頼できるのはセキュアなソリューションのみであり、セキュアなソリューションのみが長期的なビジネスとして成り立つことを理解しています。

品質管理

当社では、セキュリティ管理は確立された品質管理抜きでは考えられないと考えています。TeamViewer GmbH は、市場でも数少ない ISO 9001 に添った認証された品質管理を実施しているプロバイダの 1 つです。当社では、国際的に認定された規格に準じた品質管理を行っており、毎年外部監査機関による品質管理システムの監査を受けています。

外部専門家による査定

当社のソフトウェア TeamViewer は、Federal Association of IT Experts and Reviewers (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.)より 5 つ星の品質シール(最高値)を授与しています。BISG e.V.は独立した検査官を認定製造元へ派遣し、製品品質、セキュリティ、およびサービス品質を検査します。

セキュリティ関連の検査

TeamViewerは、ドイツ企業の FIDUCIA IT AG 社と GAD eG 社 (ドイツ国内に 1200 以上のデータ処理センターを所有するドイツの共同組合金融システムにおける最大の IT サービスプロバイダー) によるセキュリティに関連する検査を受けた後、銀行機関のワークステーションでの使用できるソフトウェアとして認定されています。

ご利用企業

現在 TeamViewer は 2 億台を越えるコンピュータ上にてインストールされ、多様な業界に及ぶ国際的にも知名度の高い大手企業に TeamViewer をご利用いただいております。銀行やその他金融機関、またヘルスケア企業や政府機関などの情報に高い機密性の求める機関を含む国際的なトップ企業が、TeamViewer を活用しています。

当社のソリューションの採用して頂いた企業様の導入の際の印象を、弊社ウェブサイト上にて掲載しております。大半の導入企業が同様のセキュリティ要件と可用性要件の評価にあたり、徹底的な検証を行った後、最終的に TeamViewer の採用に至ったことをご理解いただけることでしょう。次項では、実際にお客様ご自身にて概要を理解いただけるよう、技術的な詳細の一部を紹介しています。

TeamViewer セッション

セッションの生成と接続の種類

セッションを生成する時に、TeamViewer は最適なタイプの接続を選択します。マスタサーバを介した応答確認後、70%の場合に UDP または TCP にての直接接続を使用した接続が確立されます(一般的なゲートウェイ、NAT、およびファイアウォールの背後でも)。残りの接続は、TCP または HTTP トンネル経由で当社の冗長なルータネットワークを介してルーティングされます。TeamViewer の使用に当たり、ポートの開放は不要です。

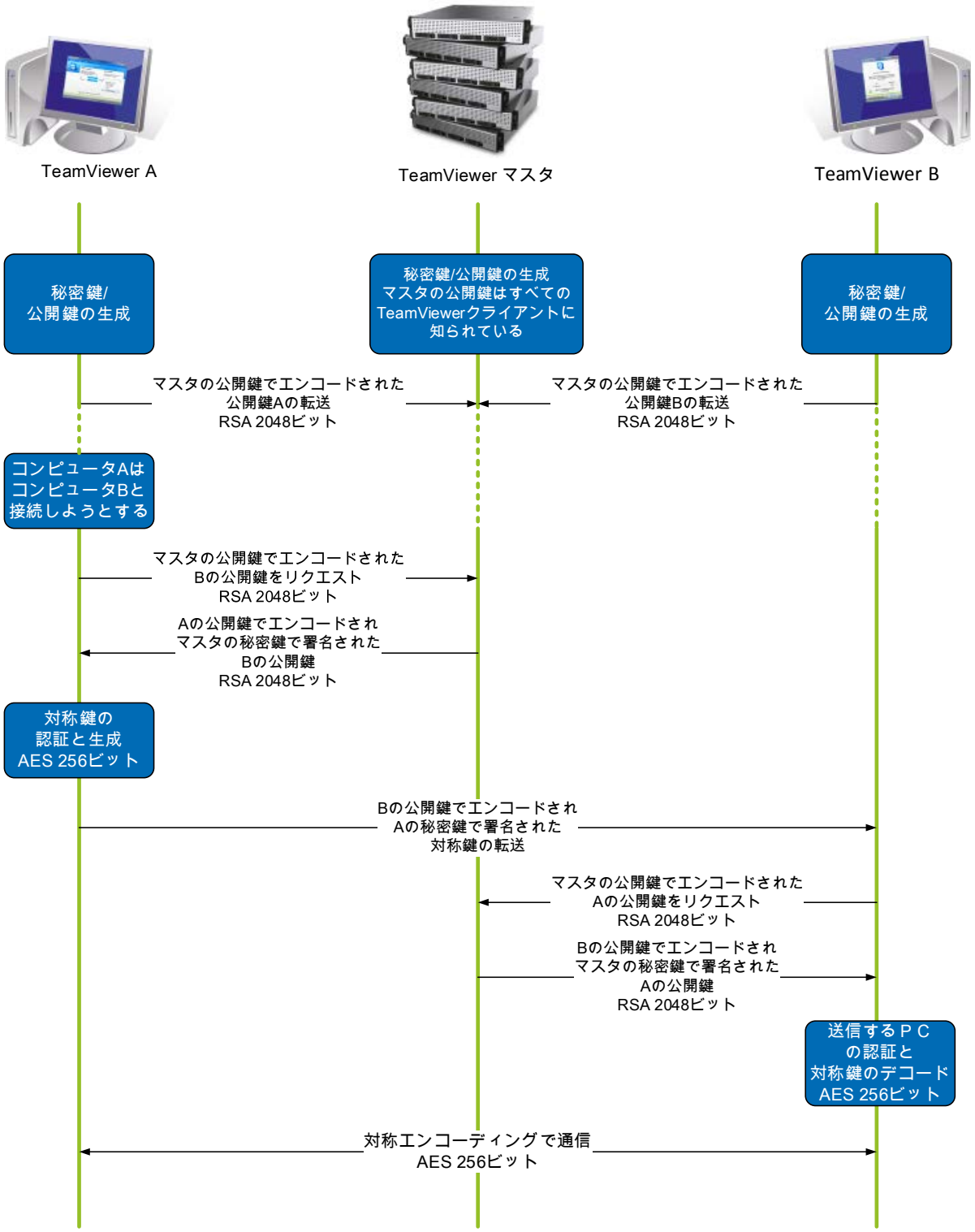
次項目の「暗号化と認証」にて記載のように、ルーティングサーバのオペレータである当社でさえも、暗号化されたデータトラフィックを読み取ることはできません。

暗号化と認証

TeamViewer Traffic はセキュアな RSA 公開/秘密鍵交換と AES (256 ビット)セッション暗号化を使用しています。この技術は https/SSL 用の同等の形式で使用されており、今日の基準で完全に安全であると見なされています。秘密鍵はクライアントから外部へ出ることはないため、TeamViewer ルーティングサーバを含む相互接続されているコンピュータのデータストリームを解読することは不可能であり、完全に保護されています。

各 TeamViewer クライアントはすでにマスタクラスタの公開鍵を実装しているので、マスタクラスタへのメッセージを暗号化して、署名済みメッセージをチェックすることができます。
PKI (公開鍵インフラ)が効率的に「中間者攻撃」を防止します。暗号化に加え、パスワードの送信は直接送信ではなく、チャレンジレスポンス方式でのみ送信され、ローカルコンピュータにのみ保存されます。

認証中は、Secure Remote Password (SRP)が使用されているため、パスワードが直接転送されることはありません。パスワード検証機能がローカルコンピュータに保存されるだけです。



TeamViewer の暗号化と認証

TeamViewer ID の検証

TeamViewer ID は、多様なハードウェアとソフトウェアの特性に基づき自動的生成されます。TeamViewer サーバは、接続確立前に ID の有効性を確認するため、偽 ID の生成や使用は不可能となっています。

ブルートフォース対策

TeamViewer 導入をご検討中のお客様より多くお問い合わせ頂くセキュリティに関しての質問に、暗号化があります。大半のお客様が恐れるリスクとして、第三者による接続内容の盗聴や、TeamViewer のアクセスデータの盗聴があります。しかし実際に最も危険なのは、非常に原始的なタイプの攻撃です。

コンピュータのセキュリティでは、情報を保護するパスワードを推測するトライアルアンドエラー方法をブルートフォースアタックと言います。一般的なコンピュータの計算能力が向上するにつれ、長いパスワードの推測に必要とする時間も大幅に短縮されつつあります。

ブルートフォースアタックに対する防御対策として、TeamViewer は接続試行の間の待ち時間が大幅するようになっています。例えば 24 回無効なパスワードにてアクセスを試みた場合では、次に接続が可能となるまでに 17 時間掛かる計算となります。この待ち時間は、正しいパスワードが正常に入力されるまでリセットできません。

TeamViewer は、特定のコンピュータからの攻撃だけでなく、ボットネットとして知られる、特定の TeamViewer-ID にアクセスしようとする複数のコンピュータからの攻撃から顧客を守る機能を備えています。

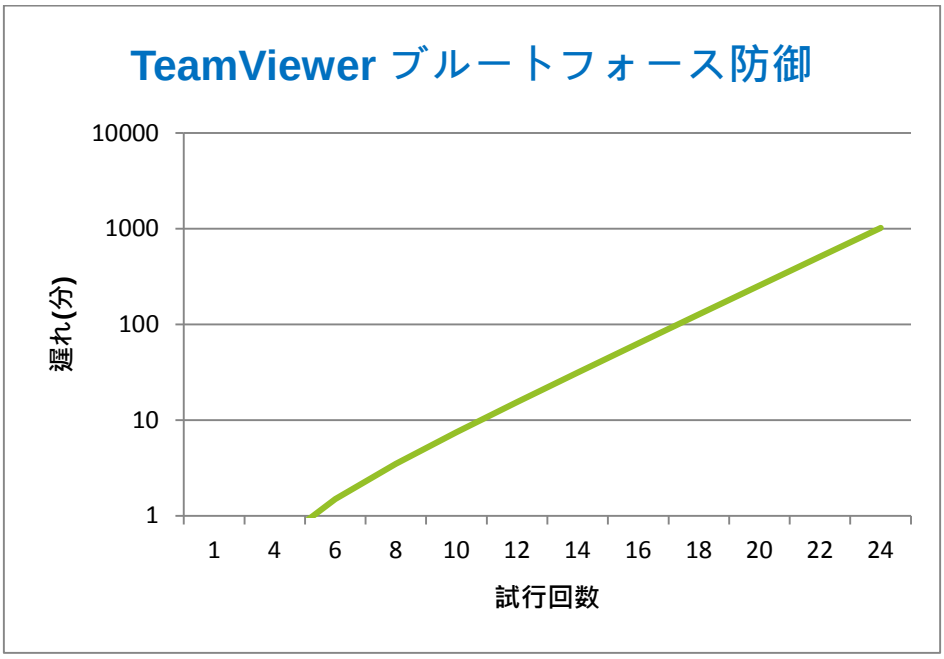


図: ブルートフォースアタックにより接続が n 回試みられた後の経過時間

コードサイニング

その他のセキュリティ機能として、当社のすべてのソフトウェアはベリサインコードサイニングにより署名されています。これにより、ソフトウェアの発行元を常に確実に識別可能です。ソフトウェアに変更があった場合、デジタル署名は自動的に無効になります。カスタマイズ可能な TeamViewer モジュールも、生成過程で動的に電子署名されるようになっています。

データセンターとバックボーン

この 2 つの項目は、可用性とセキュリティの両方に関係しています。TeamViewer のセントラルサーバは、マルチキャリア接続方式と冗長化電源を備えた ISO27001 認証の最新データセンターに置かれています。さらに、TeamViewer では信頼できる製造元のハードウェアのみを使用しています。

データセンターではアクセス制御、監視カメラ、モーションセンサー、24 時間 365 日の監視に加え、データセンターのセキュリティ担当者に許可された人のみに付与されるデータセンターへのアクセス権を設けることで、ハードウェアとデータ保護のための最善のセキュリティが保証しています。またデータセンターに設けられている入り口は 1 つのみで、詳細に渡る身元確認の後初めてセンター内へ入ることが許可されるようになっています。

TeamViewer アカウント

TeamViewer アカウントは、専用の TeamViewer サーバーでホストされています。アクセス制御に関する情報については、上の Datacenter & Backbone を参照してください。 認証とパスワード保護に関しては、Secure Remote Password protocol (SRP)、強化された password-authenticated key agreement (PAKE)プロトコルが使用されます。侵入者は十分な情報を得ることができないので、総当り攻撃ができません。つまり、弱いパスワードを使用していても強いセキュリティを確保できます。クラウド記憶域のログイン情報等の TeamViewer アカウントの大切なデータは、AES/RSA 2048 ビットで暗号化されて保存されます。

Management Console

TeamViewer Management Console は、ユーザー管理、接続の報告、コンピュータ&パートナーの管理のための Web ベースのプラットフォームです。ISO-27001 を取得しています。すべてのデータ転送は、セキュアなインターネット接続の標準である SSL (Secure Sockets Layer)暗号化を使用したセキュアなチャンネルで行われます。大切なデータは AES/RSA 2048 ビットで暗号化されて保存されます。認証とパスワード暗号化では Secure Remote Password プロトコル(SRP)が使用されます。SRP は、強固で安定したセキュアなパスワードに基づく認証であり、2048 ビットの係数を使用した鍵交換方式です。

ポリシーに基づいた設定

TeamViewer Management Console から、ユーザーは各自のデバイスへの TeamViewer ソフトウェアのインストールの設定ポリシーを、定義、配布、強化することができます。設定ポリシーは、生成したアカウントによってデジタル署名されます。これにより、デバイスにポリシーを割り当てるアカウントは、デバイスが属するアカウントだけになります。

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

TeamViewer を無人コンピュータのメンテナンスに使用する場合 (TeamViewer を Windows サービスとしてインストールする場合等) 、さらなるセキュリティ設定として、該当するコンピュータへ指定するクライアントからのみ接続を許可するよう設定することが可能です。

許可リスト機能では、該当するコンピュータへのアクセスを許可する TeamViewer ID を明示的に指定することができ、また、ブロックリスト機能では特定の TeamViewer ID からのアクセスをブロックすることができます。中央許可リストは、「Management Console」で記述された「ポリシーに基づいた設定」の一部として利用できます。

チャットおよび動画の暗号化

チャット履歴は使用中の TeamViewer アカウントと関連付けられて、見出し「TeamViewer アカウント」で記述されたのと同じ AES/RSA 2048 ビット暗号化セキュリティを使用して保存されます。すべてのチャットメッセージと動画のトラフィックは AES (256 ビット)セッション暗号化を使用して完全に暗号化されます。

ステルスモードなし

TeamViewer には完全にバックグラウンドで実行することを可能とす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実行されている場合でも、システムトレイ内にアイコンが表示されるので TeamViewer が実行されていることが一目で分かります。

接続が確立すると、システムトレイ上部に TeamViewer のコントロールパネルが必ず表示されます。これにより、TeamViewer はコンピュータや従業員の内密な監視には意図的に不向きとなっています。

パスワード保護

簡単なカスタマサポートを行うために、TeamViewer (TeamViewer QuickSupport)はセッションパスワード(ワンタイムパスワード)を生成します。顧客にパスワードを確認し、ID とそのパスワードを入力することで顧客のコンピュータに接続できます。顧客側で TeamViewer を再起動するとパスワードが新たに生成されるため、顧客にパスワードを得られた場合にのみ接続を確立することができるようになっています。

サーバなどに対し無人リモートサポート用に TeamViewer を展開する場合は、当該コンピュータへのアクセスをセキュアにするために個別で固定パスワードを設定することが可能です。

着信と発信のアクセス制御

TeamViewer の接続モードを個別に設定することができます。たとえば、リモートサポートやプレゼンテーションに使用するコンピュータには、リモート着信接続ができないよう設定することも可能です。

機能を実際に必要な機能に制約することで常に、潜在的な攻撃に対する考えられる弱点が制約されます。

2 段階認証

TeamViewer は、企業が HIPAA および PCI コンプライアンス要件を満たすのをお手伝いします。2 段階認証はセキュリティレイヤーを追加して、TeamViewer アカウントを不正アクセスから保護します。さらに TeamViewer は、許可リストによるアクセスコントロールと組み合わせて HIPAA と PCI を準備します。

2 段階認証では、TeamViewer アカウントにサインインするにはユーザー名とパスワードの他に、モバイルデバイスで生成されたコードが必要です。コードは時間ベースのワンタイムパスワード(TOTP)アルゴリズムで生成されます。

さらにご質問がありますか?

その他ご不明な点等ございましたら、03 4578 0488 までお電話にてお問い合わせいただくか、support@teamviewer.com までメールにてお気軽にお問い合わせください。

お問い合わせ先

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Germany
service@teamviewer.com

管理者: Holger Felgner

登録: Ulm HRB 534075