TeamViewer セキュリティ情報

対象グループ

本書は専門のネットワーク管理者を対象にしています。本書に記載する情報はかなり技術的専門性が高く、非常に詳細です。この情報に基づいて、情報 IT の専門家は TeamViewer を使用する前にソフトウェアセキュリティの詳細な概念を入手することができます。考えられるセキュリティ上の問題を解決するために、本書を自由に顧客に配布してかまいません。

自分は対象グループに属さないと思われる方も、「当社/当ソフトウェア」の章のソフトな内容を読まれると、簡単に概要をつかめるでしょう。

当社/当ソフトウェア

当社について

TeamViewer GmbH は南ドイツの都市 Göppingen (Stuttgart 近郊)に拠点を置き、2005 年に設立されました。ウェブベースのコラボレーションのための安全なシステムの開発と販売を専門に行っています。迅速な立ち上げと急成長により、世界中の 200 以上の国々で短期間のあいだに数千万の TeamViewer ソフトウェアがインストールされ、ユーザを獲得するに至っています。本ソフトウェアは 30 以上の言語で提供されています。

セキュリティについての当社の理解

TeamViewer は、インターネットによる簡単のサポートの提供や無人コンピュータへのアクセスのために(たとえば、サーバのリモートサポート)、世界中で数え切れないほど使用されています。TeamViewer の設定に応じて、リモートコンピュータを、実機を操作するのと同じように操作できるのです。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 管理者のいずれであっても、そのコンピュータ上での管理者権限を同様に与えられます。

安全とは思われないインターネットを介したこのような重要な機能を、さまざまな方法で攻撃から守る必要があることは明らかです。実際、セキュリティの話題は当社の他のすべての開発目標の上に位置しています - コンピュータへのアクセスを安全にすると同時に、当社自身の利益を守るために, 世界中の何千万ものユーザは安全なソリューションだけを信頼し、安全なソリューションだけが当社の企業としての長期の成功を保証してくれます。

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理解しています。TeamViewer GmbH は、ISO 9001 の認証を取得した品質管理を実施している、市場では数少ないプロバイダの 1 つです。当社の品質管理は、国際的に認定された規格に従っています。当社は、年間ベースで外部監査機関により品質管理制度の検査を受けています。

外部の専門家の査定

当社のソフトウエア TeamViewer は、Federal Association of IT Experts and Reviewers (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.)により 5 つ星の品質シール(最高値)を授与されています。BISG e.V.の独立した検査官が、資格を満たした製造者の製品の品質、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、ドイツの FIDUCIA IT AG と GAD eG (約 1200 のドイツの銀行のデータ処理センターの運営担当者)によるセキュリティ関連の検査を受け、銀行のワークステーションでの使用を認定されています。

参考資料

現時点で、TeamViewer は 100,000,000 台以上のコンピュータで使用されています。あらゆる種類の業界の(銀行やその他の金融機関などの非常に機密性の高い部門を含めて)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を採用した際の第一印象を知るために、インターネットで当社の参考資料を調べてみてください。ほとんどの会社が - 徹底的な試験を行った後で - 最終的に TeamViewer に決定する前に、同じようなセキュリティ要件と可用性要件を持っていたことに、同意していただけるでしょう。しかしながら、お客様ご自身で独自の印象を得られるよう、以下のパラグラフで技術的な詳細の一部を紹介します。

TeamViewer セッションの作成と操作

セッションおよび接続タイプの作成

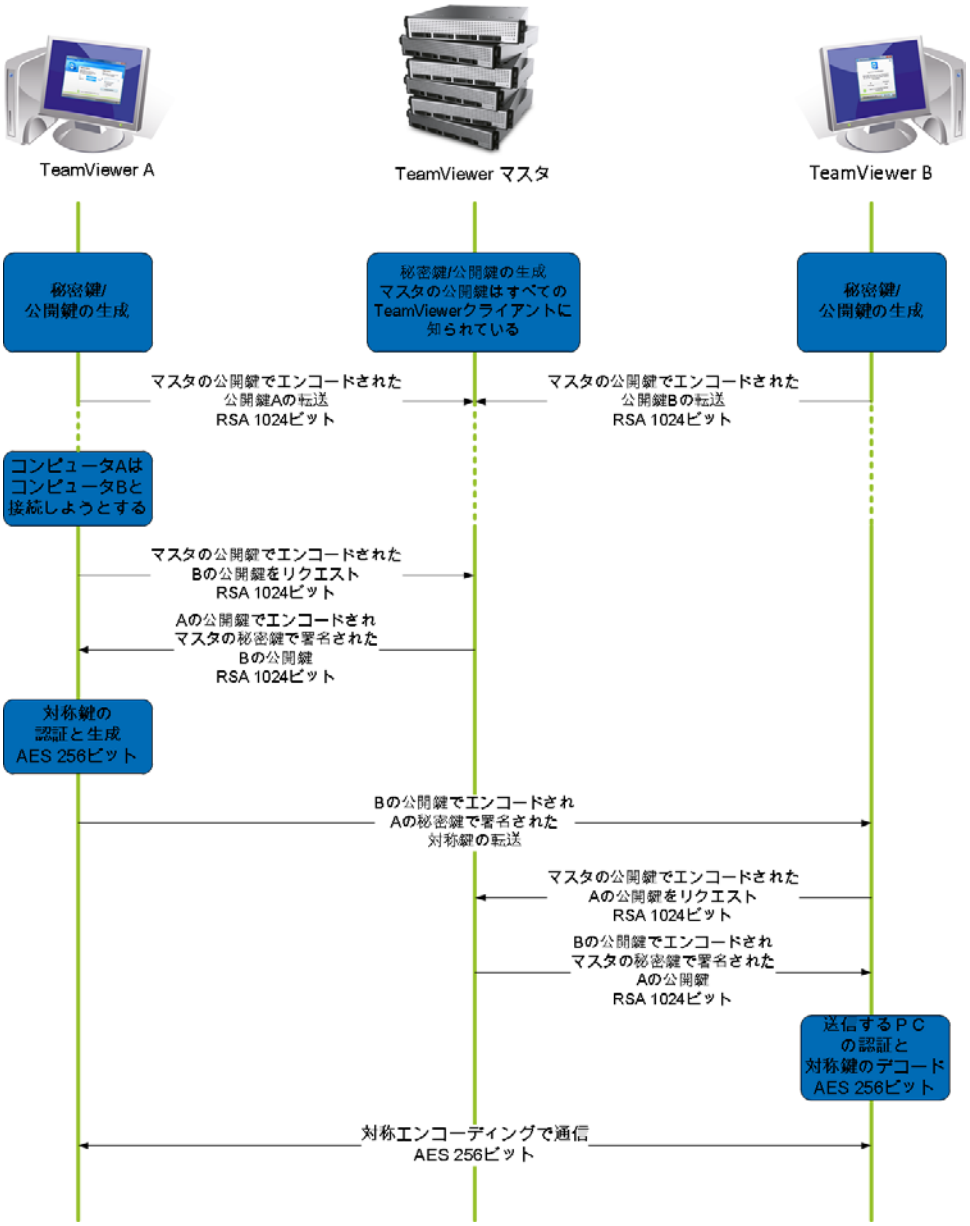
セッションを作成する時に、TeamViewer は接続の最適なタイプを決定します。マスタサーバを介した応答確認後、70%の場合に、UDP または TCP を介したダイレクト接続が確立されます(標準ゲートウェイ、NAT、およびファイアウォールの後ろにも)。残りの接続は、TCP または http トンネルを介して当社の高度に冗長化されたルータネットワークで経路指定されます。TeamViewer を使用するためにポートを開ける必要はありません!

パラグラフ「暗号化と認証」で後述するように、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 は、RSA 公開/秘密鍵交換と AES (256 ビット)セッション符号化に基づく完全な暗号化を使用します。このテクノロジは https/SSL 用の同等の形式で使用され、現在の規格により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コンピュータの外に出ることはないため、相互接続されているコンピュータ - TeamViewer ルーティングサーバを含めて - がデータストリームを解読できないことが、この手順により保証されます。

各 TeamViewer クライアントにはすでにマスタクラスタの公開鍵が実装されているため、それぞれでマスタサーバのメッセージを暗号化し、マスタの署名をチェックできます。PKI (公開鍵インフラ)が効率的に「中間者攻撃」を防止します。暗号化されているにもかかわらず、パスワードはダイレクトには送信されず、チャレンジレスポンス手順でのみ送信され、ローカルコンピュータにのみ保存されます。



TeamViewer の暗号化と認証

TeamViewer ID の検証

TeamViewer ID は、ハードウェアの特性に基づいて TeamViewer 自身により自動的に生成されます。TeamViewer サーバは、偽の ID の生成、使用を防止するために、接続の前に毎回、ID の有効性をチェックします。

総当り攻撃からの保護

見込みのある顧客が TeamViewer のセキュリティについて問い合わせてくる場合、必ず暗号化について質問します。当然のことながら、最も恐れられているのは、第三者が接続内容をのぞき見するリスクや、TeamViewer のアクセスデータが盗聴されるリスクです。実際、ほとんどの場合に危険なのは非常に原始的な攻撃です。

コンピュータのセキュリティに関しては、総当たり攻撃ではしばしば、保護対象のリソースを保護しているパスワードをトライアルアンドエラーによって推測することが試みられます。標準のコンピュータの計算力が向上するにつれ、より長いパスワードの推測に必要な時間さえも大幅に短縮されつつあります。

総当たり攻撃に対する防御手段として、TeamViewer は接続の試みと試みの間の待ち時間を大幅に増やしています。24 回試みると、既に 17 時間がかかります。待ち時間は、正しいパスワードが正常に入力されないとリセットできません。

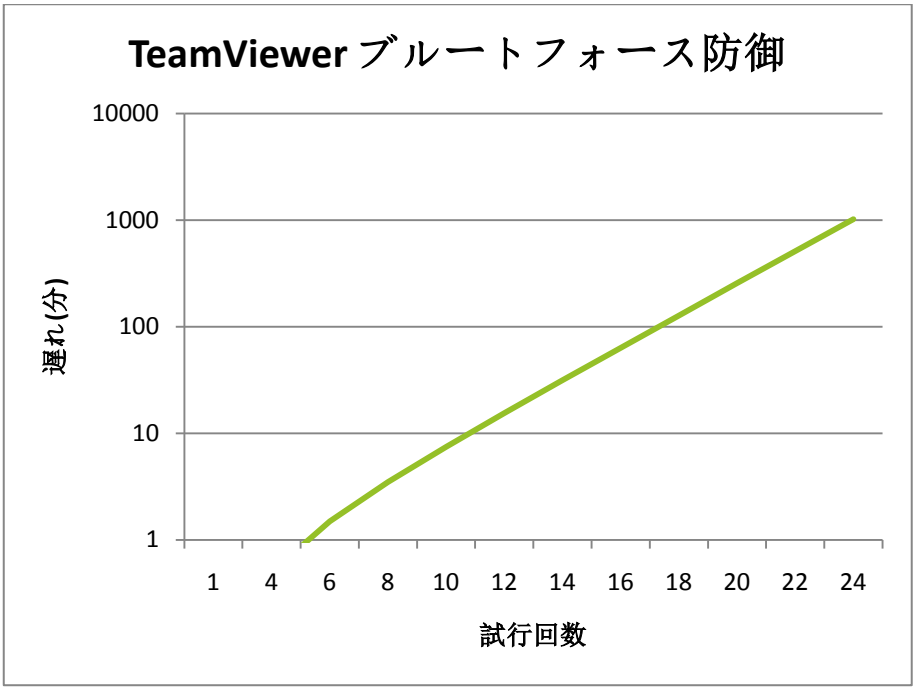


図: 総当り攻撃中に接続が n 回試みられた後の経過時間

コード署名

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。このため、ソフトウェアの発行者は常に確実に識別できます。後からソフトウェアが変更されると、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、作成中にダイナミックに署名されています。

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。中央 TeamViewer サーバは、多冗長化キャリア接続と冗長化電源を備えた最新のデータセンターに置かれています。使用されているのは、信頼できる会社のハードウェアだけです(Cisco、Foundry、Juniper)。

データセンターへのアクセスは、1 つだけのエントランスゲートを介した徹底的な身元チェック後に初めて可能になります。CCTV、進入検出、24 時間 365 日の監視、およびオンサイトのセキュリティ要員により、当社のサーバは攻撃に対して内部から守られています。

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補修に使用する場合(即ち、TeamViewer を Windows サービスとしてインストールする場合など)、他のすべてのセキュリティメカニズムに加えて、当該コンピュータへのアクセスを複数の特定のクライアントに制限することが可能です。

許可リスト機能により、どの TeamViewer ID に当該コンピュータへのアクセスを許可するかを明示的に示し、ブロックリスト機能によって特定の TeamViewer ID をブロックすることができます。

ステルスモードなし

TeamViewer を完全にバックグラウンドで実行するための機能はありません。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、TeamViewer はシステムトレイ内のアイコンによって常に表示されています。

接続の確立後は、システムトレイの上部に常に小さいコントロールパネルが表示されます – そのため、TeamViewer はコンピュータや従業員を内密に監視するには意図的に不向きになっています。

パスワード保護

簡単なカスタマサポートのために、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。カスタマからパスワードを伝えられたら、ID とそのパスワードを入力してカスタマのコンピュータに接続できます。カスタマ側で TeamViewer を再起動すると、カスタマから明示的に指示された場合にだけカスタマのコンピュータに接続できるよう、新しいセッションパスワードが生成されます。

TeamViewer を(サーバなどの)無人のリモートサポート用に展開する場合は、当該コンピュータへのアクセスをセキュアにする個別の固定パスワードを設定します。

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コンピュータを、着信接続ができないよう設定することができます。

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。

さらにご質問がありますか?

さらにご質問がありましたら、いつでも(JP) + 81 (0) 345 780 488 にお電話くださるか、nihon@teamviewer.com までメールをお寄せください。

お問い合わせ先

TeamViewer GmbH
Kuhnbergstr. 16
D-73037 Göppingen
ドイツ
nihon@teamviewer.com

管理者: Holger Felgner
登録: Ulm HRB 534075