eBook

リモート接続にエンタープライズ レベルのセキュリティ体制を確立する方法

TeamViewer

本書の**目次**

エンタープライズ全体で確立する **セキュリティ体制**

今日の企業は IT 運用の大部分を、リモート接続に大きく依存しています。また、分散した労働力や在宅勤務の増加により、リモート アクセスやコントロール機能への依存度が高まっています。その結果、セキュリティの範囲は多岐にわたるようになりました。

これまで、ＩＴ インフラは企業のファイアウォール内の近接した場所から管理され、少数の運用者やユーザーが一か所からアクセスしていたため、個別のセキュリティの要件によって運用されてきました。しかし、従業員、パートナー、業者がボーダーレスでアクセスする DX への移行により、セキュリティはもはや後から付け足して対応できないものになりました。

このようなコネクテッドなエンタープライズの労働環境は常に進化しています。これらは、人材、技術スタック、ワークフローからなる複雑なエコシステムで構成されています。ほとんどのエコシステムは、多様な ＩＴ システムとネットワーク機器を通じてリモートで管理されています。
組織がリモート接続プラットフォームを活用して、これらの複雑なインフラの管理を行おうとするとき、設定ミスやその他の人為的なミスに起因するセキュリティの問題がしばしば生じます。

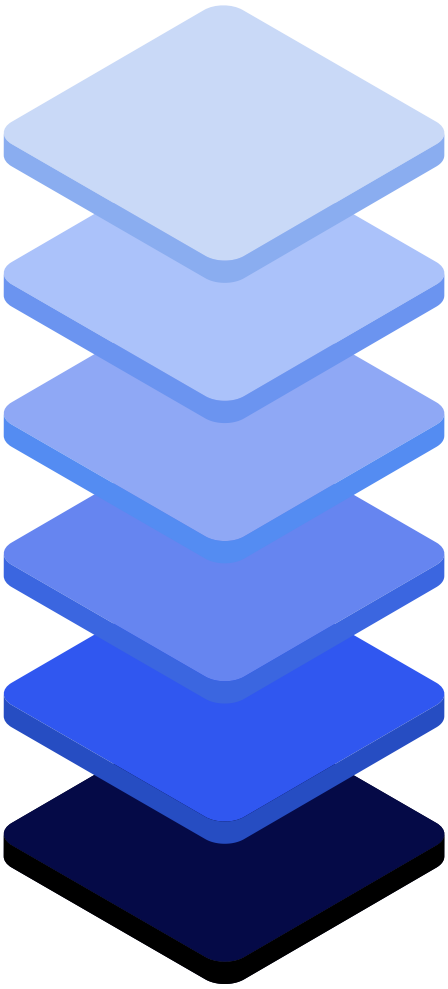
そのため、ネットワークおよびサイバー セキュリティの侵害を最小限に抑える、回復力のあるセキュリティ体制の構築が非常に重要となりました。リモート接続および

今日の労働環境は常に進化し、変化を遂げています

インフラ管理プラットフォーム導入の初期段階にある組織では、このセキュリティ体制を維持するのに役立つアプローチから開始する必要があります。

安全なリモート接続のための フレームワーク

TeamViewer は、リモート接続と強固なセキュリティ体制のフレームワーク確立を通じてビジネスを成功に導く重要性を理解しています。
このフレームワークは 6 つのレイヤーに分割されています :



TeamViewer のセキュリティ フレームワーク

05 **ルール**
安全なリモート接続体験を提供するための黄金ルール

04 **構成**
セキュリティ全般に関わる構成パラメータ

03 **リスク**
防御すべき潜在的なリスク

02 **アクター**
セキュリティ侵害に関係するまたは影響を受ける関係者

01 **期待値**
より安全な接続体験のための期待値設定

00 **コミットメント**
組織全体でのセキュリティ体制の確立

堅牢なセキュリティの体制の確立は、確固としたコミットメントから始まる

エンタープライズ全体に**安全な**リモート接続が重要な理由

IT アプリケーションは従来のメインフレームやデスクトップ ベースのスタンドアロン システムから進化しています。これらのシステムは攻撃に使用する経路が限られていたため、セキュリティ侵害に対する自然な障壁がありました。しかし、労働環境のクラウド化にともない、攻撃をうける領域は著しく増加しました。企業はグローバルに分散する従業員をサポートし、今日のビジネス環境における競争力と俊敏性を維持できるよう、常に利用可能なエンタープライズ ネットワークを持つことを求められています。

増加を続けるアプリケーションや多種多様なデバイス、様々な場所でリモートワークする従業員など、セキュリティへの懸念はますます高まっています。セキュリティ体制の基礎を築くためには、関係者とともにこれらの懸念に対処することが必要です。

レイヤー 1 : セキュリティ体制へのコミットメント

堅牢なセキュリティの体制の確立は、確固としたコミットメントから始まります。このコミットメントは、次のようなイニシアティブを含む、トップダウンの企業責任として推進される必要があります。

セキュリティ関連のニュースやトレンドの最新情報を定期的に提供することで、従業員やスタッフ全体の関心を高めます。

安全なエコシステムを構築し、維持するために外部のパートナーや取引先へ継続的なトレーニングと教育を実施します。

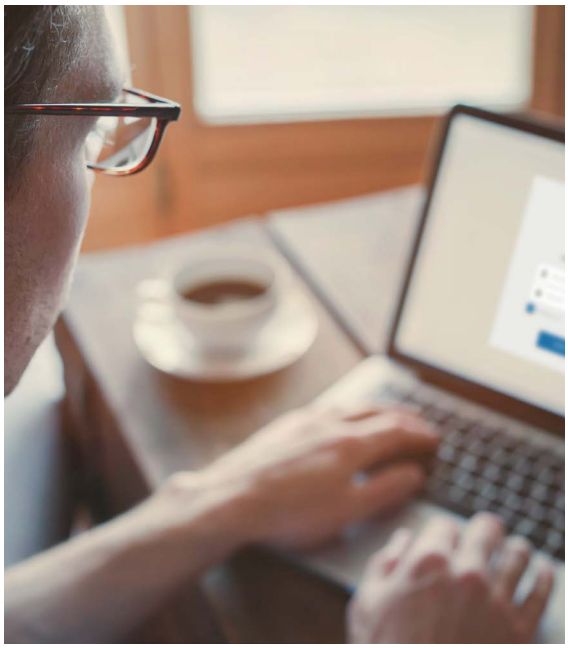
定期的なブリーフィング、コミュニティ フォーラムへの貢献、そして政府機関との協力を通じて、サイバーおよびネットワーク セキュリティのコミュニティにおいて ソートリーダーシップ を確立します。

ご存じですか？

- TeamViewerは、インシデント対応担当者のための主要な団体である Forum of Incident Response and Security Teams (FIRST) の監査対象メンバーです。
- TeamViewer は、クラウド ソーシングの代表的なセキュリティ プラットフォームである YesWeHack と協力し、セキュリティ研究者の大規模なコミュニティと連携しています。
- TeamViewer は、サイバーセキュリティ リスクとセキュリティ管理の有効性を評価する独立した第三者企業の BitSight Security Rating によってテック企業のトップ 1% に評価されています。

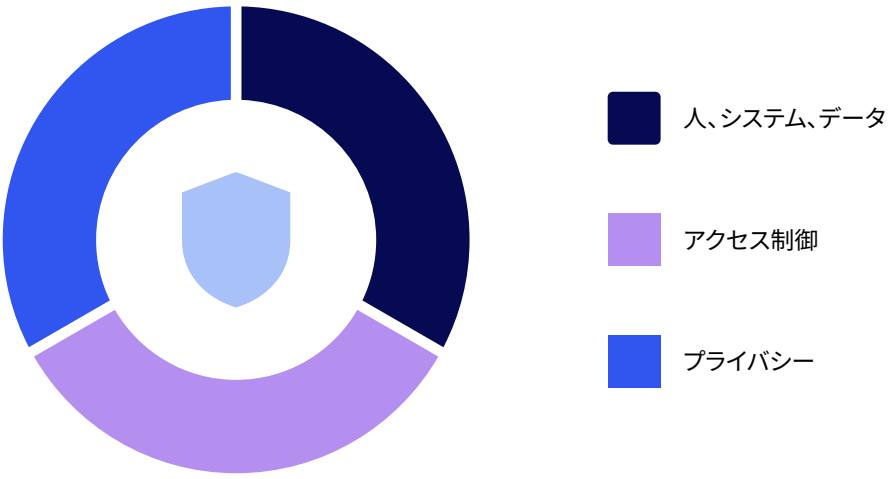
レイヤー 2 : 期待値の設定

理想的なセキュリティ体制に到達する前に、セキュリティへの適切な期待値を設定することは重要です。セキュリティのとらえ方は、人により異なります。しかし、公表された企業の IT セキュリティ侵害のほとんどが、プライバシーやアクセスの問題という形で生じていることは想像に難くありません。



クレジットカードのデータの不正入手であれ、悪意のあるパケットを送信してコンピューターやデバイスを不正に操作するケースであれです。すべてのセキュリティ対策は、プライバシーとアクセス制御のいずれかのカテゴリーに分類されます。これらの対策は、あらゆるセキュリティ体制の基礎となります。

組織は、好ましいワークライフ バランスの奨励に努めています。そのような組織で働く個人は、デジタル ワークスペースに簡単かつ安全にアクセスすることを望んでいます。



基礎的なセキュリティ対策

組織では、プライバシーにより、従業員データ、ビジネス上の機密データ、ビジネス取引や企業秘密などの情報が保護されます。同様にアクセスは、設定、機器の管理、施設、システムの設定と管理を許可された担当者のみに与えられます。

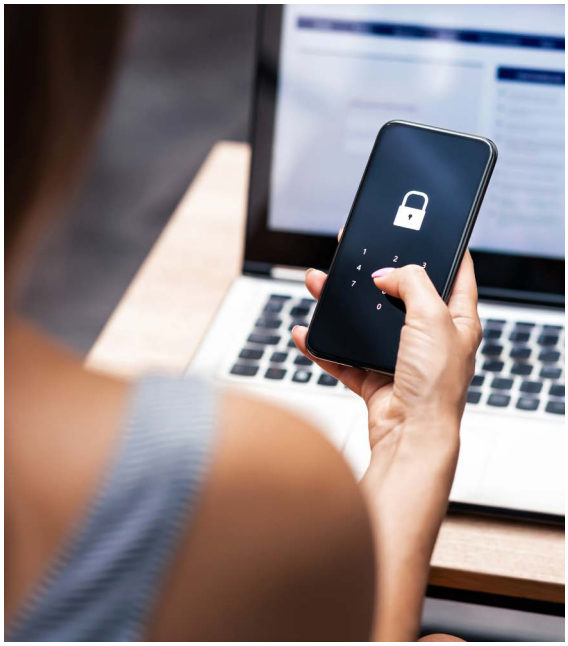
レイヤー 3 : 関係者の明確化

セキュリティの期待値の設定は、関係者を明確にすることによってのみ可能になります。例えば、クレジット カードの詳細が漏洩するプライバシーの侵害は、漏洩したデータに含まれる人すべてに影響します。この場合、クレジット カードの保有者が関係者です。組織の観点からは、これらの関係者は直接的または間接的にセキュリティ関連のインシデントに関与しており、受益者も被害者も含みます。

人
他者と交流し機器を扱う、従業員、パートナー、取引先などの幅広いカテゴリのユーザーです。これらのユーザーは、会社の機能や部門にもとづき、より詳細なグループや役割に分類されます。

機器
コンピューター、サーバー、ネットワーク デバイス、その他のハードウェア、ソフトウェア アセットで、組織のさまざまな利害関係者が日々のビジネスや業務、サービス ワークフローのために使用します。

ボット
最小限の知能を備えた、ユーザーまたは機器の振る舞いを模倣するプログラム可能なハードウェアまたはソフトウェアです。タスクを自動化するために、人間の代わりに働きます。



信頼性のあるリモート接続セキュリティ体制の基礎は、これら 3 つのレイヤーの内部評価から始まります。この評価は、各関係者のセキュリティ期待値を明確に示すものとして機能します。

70 %の組織が

複数のクラウドやオンプレミス環境においてデータを保護できません。

92 %の組織が

社内外のパートナーに新しいクラウド ネイティブの機能を安全に有効化し、拡張することができません。

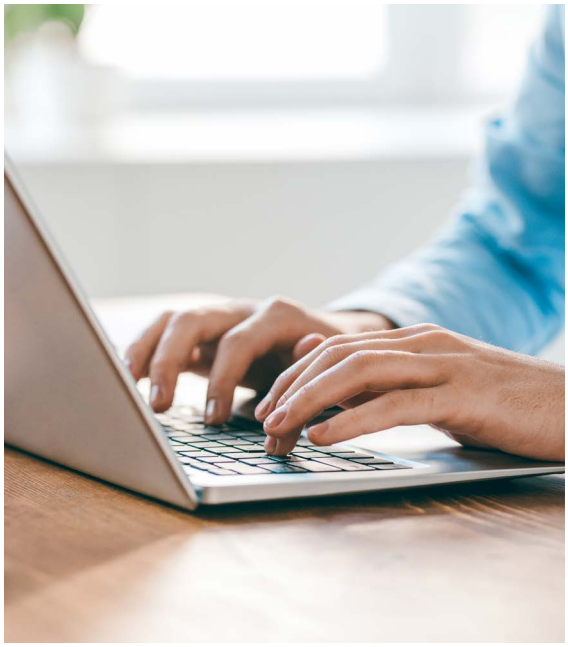
33 %の増加

2020年から 2021年にかけて、脆弱性の悪用によって生じたインシデントの件数です。

出典：IBM, X-Force Threat Intelligence Index 2022

セキュリティ体制の基礎となる前提を主張する

多くの部門や機能にまたがるエンタープライズ全体のIT イニシアティブの管理に役立つ様々な技術があります。同様に、時間や労力を節約し、生産性を高めるのに役立つあらゆる技術が、第三者による悪用やハッキングに使用される可能性もあります。電子メールは依然として企業へのハッキングに最も広く使用されている技術のひとつです。電子メールと同様に、ハッカーは数多くの方法で脆弱性を悪用し、日常業務の妨害を行っており、その試みは今後も続くでしょう。これらは通常、損害を与え、金銭を脅し取り、世間からの評判を棄損するために使用されます。



リモート接続も例外ではありません。しかし、ビジネスにおけるリモート接続の採用は、リスクをはるかに上回る可能性を理解する必要があります。技術者の疲労を軽減し、従業員の生産性を向上させ、オフィスでの作業をスピードアップさせるなどの利点があります。企業は、最初から安全なプラットフォームやソリューションを選択する必要があります。

より多くの組織が、リモート接続によって、人、システム、プロセス、ワークフローにまたがるやりとりや通信を簡単に管理できることを認識するようになっています。

組み込みの**セキュリティ機能**

組み込みのセキュリティ機能が安全なリモート接続セッションを実現します。この保証は、プライバシーとアクセスにも適用されます。すべてのセッションは暗号化されるため、指定された関係者のみがコンテンツを共有し、アクセスできます。

さらに、2 つ以上が関与するあらゆるリモート接続はメカニズムを必要とします。これは、リモートで作業する従業員や移動中の従業員のデバイスへのアクセスを安全に制御し、接続を認証するのに役立ちます。

組み込みのセキュリティ機能は、機密情報を管理するための特別な対策も備えています。これらには、ランダムで予測困難なセキュリティキーを生成するための多様な暗号化技術や、機密セキュリティ情報の交換に使用されるプロトコル (複数形式の鍵交換プロトコル) が含まれます。

組み込みのセキュリティ機能は、機密情報を管理するための特別な機能も備えています。

ご存じですか？

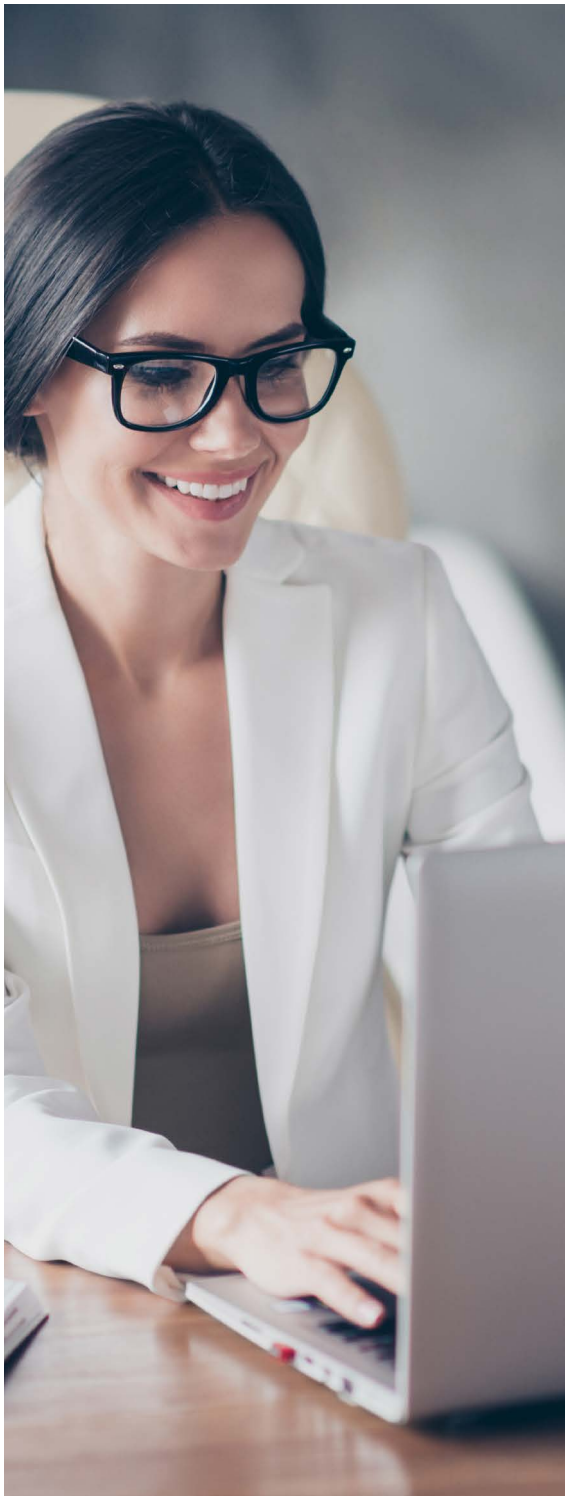
TeamViewer は以下のような組み込みと追加のセキュリティをサポートします。

- 各セッション後のパスワードのランダム化
- デバイス認証 (信頼済みデバイス)
- ワンタイム パスワード (OTP)
- 接続時の多要素認証 (MFA)
- スマート カード リダイレクト
- 条件付きアクセス
- シングル サインオン (SSO)

セキュリティ基準と認証

セキュリティ基準と認証は、あらゆるプラットフォームにおけるセキュリティ コンプライアンスと期待への基礎を築きます。

リモート接続プラットフォームでは、いくつかの主要な基準と認証があります。

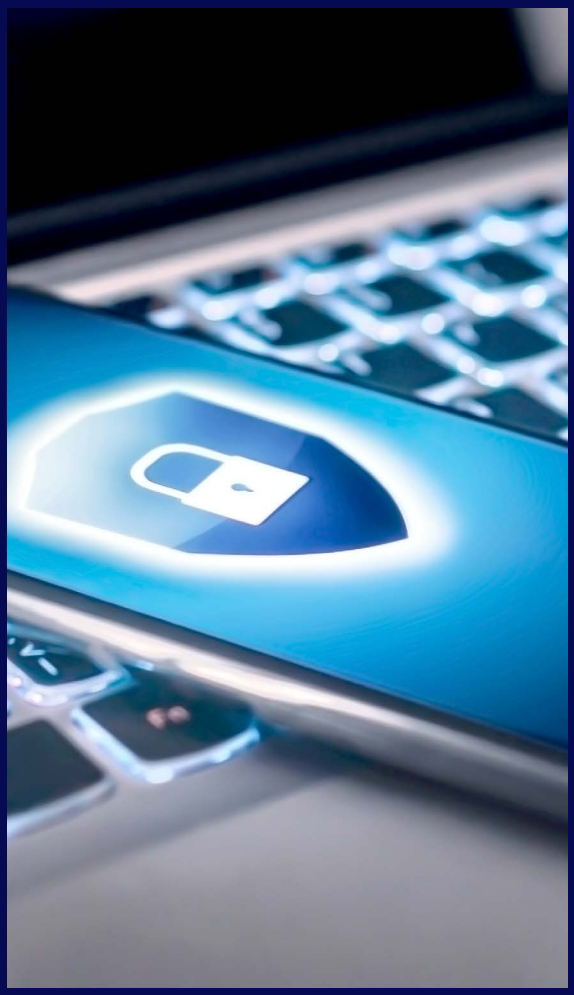


暗号化基準
情報暗号化のメカニズムを定義します。AES (Advanced Encryption Standard) と RSA (Rivest, Samir, Adleman) は、リモート接続セッションにおいてデータの暗号化と情報の交換に使用される一般的な 2 つの標準規格です。

セキュリティ フレームワーク
法的、物理的、技術的な管理を含む組織レベルのポリシーを定義し、すべての情報システムとそれらによって生成されたデータへのアクセスを規制します。ISO 27001 と GDPR はもっとも有名なセキュリティとプライバシー フレームワークの例です。

コード署名
ファイルやソフトウェア実行ファイルの改ざんや破損を防ぐことで、そのオリジナル性や完全性を保証する、デジタル認証のメソッドです。

セキュリティは終わりのない**課題です**



ご存じですか？

TeamViewer は以下にサポートされています。

- エンドツーエンドの 4096 ビット RSA キー暗号化と 256 ビット AES 暗号化セッション
- GDPR、HIPAA / HITECH、TISAX、SOC 2、SOC 3、ISO 27000 準拠
- クラス最高のセキュリティ体制 - 独立した第三者サイバー セキュリティ評価企業 BitSight による評価
- IAPP ゴールド メンバーシップ
- デジタル リスク プロテクション

セキュリティの継続的な**改善**

セキュリティは終わりのない課題です。歴史的に、素晴らしい技術革新のすべてがビジネスを合理化し、ワークフローやプロセスを加速させる一方で、電子メールやインスタント メッセージなどの技術は悪用され、企業への攻撃に使用されることもありました。AI やその他の技術革新も同様に、システムのハッキングやデータの盗用に使用されています。

その結果、すべてのリモート接続プラットフォームを新たなセキュリティの脅威からの保護する安全対策を施し、定期的に更新する必要が生じています。しかし、これらの脅威を予測することは困難です。そのため、サイバー セキュリティとネットワーク セキュリティ分野の最新情報を常に把握することが大切です。

脆弱性の公表
セキュリティ上の脆弱性の可能性について透明性を保つことは、セキュリティホールの悪用を遅らせる最善の方法です。これにより特定のプラットフォームを使用しているエンタープライズは、リモート接続かどうかにかかわらず、十分な情報を得ることができます。

バグ報償金プログラム
脆弱性を認識し、その報告を提出した個人に企業から報償金を支払う、バグ報償金もひとつの方法です。

セキュリティの ソートリーダーシップ
企業は、最先端のセキュリティに対して発言力を発揮するために、テクノロジーに関する ソートリーダーシップ に参加する必要があります。それを可能にするいくつかのチャネルがあります。セキュリティ領域および関連分野に興味を持つ、さまざまなメディアの出版物、コミュニティ、および団体が、このようなイニシアティブを推進するための最適な協力源です。

ご存じですか？

TeamViewer は、シーメンス、SAP、ボッシュなどドイツのわずか 9 社の CNA と、世界 178 社のベンダーが参加する認定 CVE 番号付与機関 (CNA) です。TeamViewer は、業界をリードするサイバー セキュリティへの取り組みと姿勢に加え、製品とサービスをより良くするために責任ある情報公開を実施しています。

その一環として、バグやセキュリティ エクスプロイトの発見に挑戦するための VDP (脆弱性開示方針) を提供することで、倫理的なハッカーに明確な指針を提供しています。

さらに詳しく
vdp.teamviewer.com/p/Send-a-report

セキュリティ体制を強化

エンタープライズ全体でのセキュリティ体制の基礎を確立したら、セキュリティ強化のための要素に注意を払うことも重要です。これらは、アプリケーション レベルでカスタム可能なセキュリティ構成に関係しています。

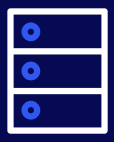
戦略 : セキュリティを軸にリスクと構成を組み合わせる

構成は、2人以上の通信を保護する追加レイヤーを提供します。サポート エージェントがリモート ワーカーに接続するシナリオ、技術者がリモート デバイスにログインしてリモートでサポートを提供するシナリオ、問題を修正するシナリオなどがあります。構成ミスが招く、企業環境への潜在的なセキュリティ リスクを理解することが重要です。

レイヤー 4 : **エンタープライズ アプリケーション**のセキュリティ リスクの理解

サイバーおよびネットワーク セキュリティの現在のトレンドにもとづき、エンタープライズ アプリケーションに 4 種類のセキュリティ リスクを挙げることができます。

侵入型リスク



偶発的リスク

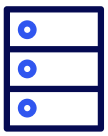
内在的リスク

相互依存型リスク

内在的セキュリティ リスク
内在的セキュリティ リスクは、ときに組織の基本的なセキュリティ ポリシーの遵守を怠っていたことにより生じます。一般的な例としては、暗号化または認証メソッドを用いていないために、データ転送中にプライバシー リスクが発生したり、安全なサポート体験をリモート ワーカーに提供できなかったりすることが挙げられます。

相互依存型セキュリティ リスク
相互依存型のセキュリティ リスクはセキュリティの概念そのものを弱体化する機密情報の露出から生じます。例えば、ワークステーションへのユーザー ログイン情報が露出してしまうと、そのワークステーションはセキュリティの侵害を受けやすくなります。

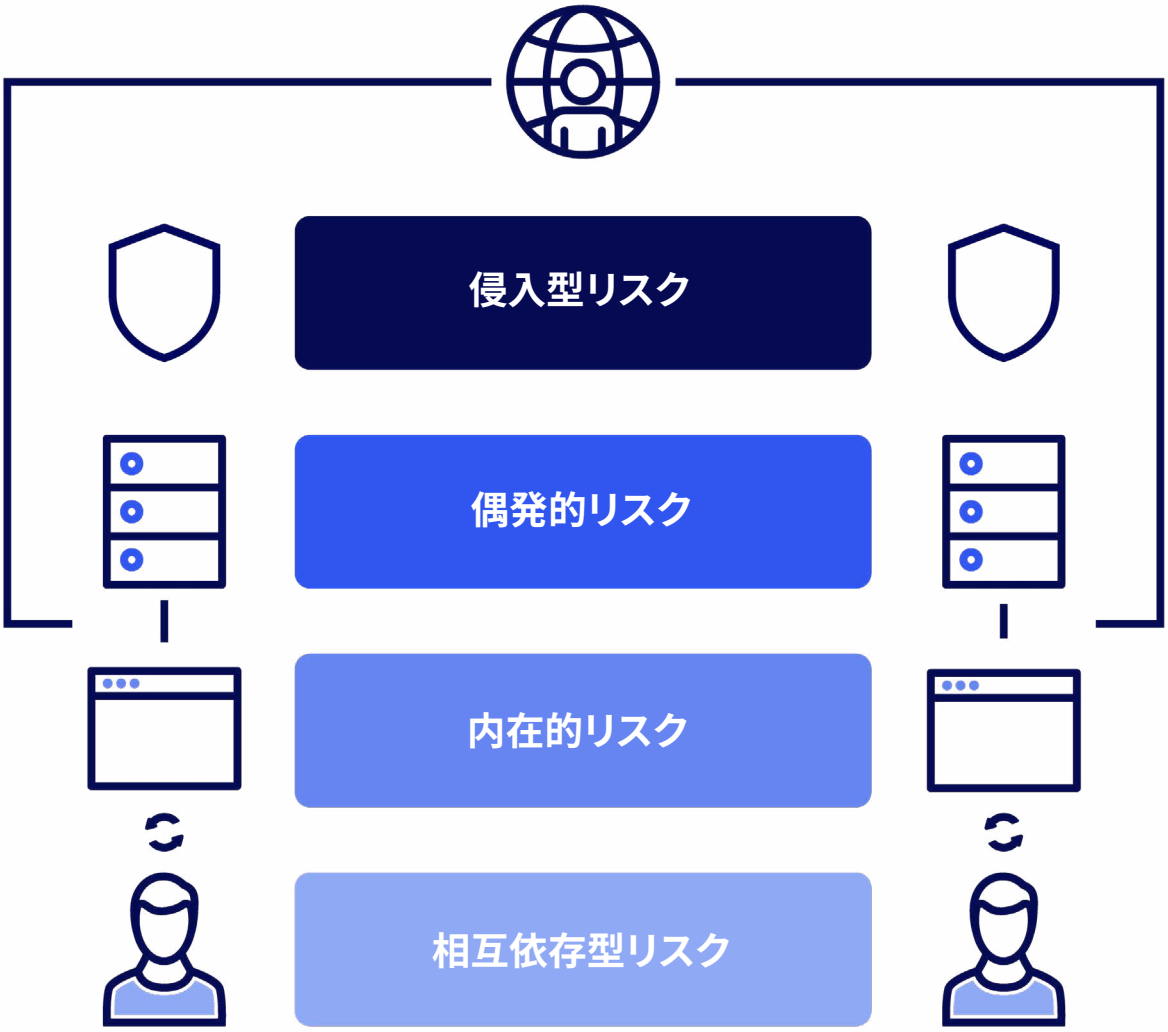
ログイン情報は、機密情報の組み合わせの一部で、特定の関係者間でのみ共有されるものです。この例では、ユーザーとワークステーションがそれにあたります。パスワード、証明書、暗号化キーなど、さまざまな形式の機密情報がありますが、それらは 2 人以上の間で安全な接続を確立するために交換される必要があります。相互依存はセキュリティを実現するための基本的な考え方です。



偶発的セキュリティ リスク
偶発的セキュリティ リスクは、安全な通信に関与する仲介者に関係するものです。例えば、ファイアウォールはトラフィックをフィルタリングして特定のアプリケーションに対する特定のパケットのみを許可します。ファイアウォールの設定を誤ると無許可のトラフィックを通過させてしまい、セキュリティが損なわれる結果を招きます。同様に、VPN のゲートウェイや認証

サーバー、ストレージなど、関係者間の安全な通信の管理に関与する様々な仲介者があります。これら仲介者のいずれかの侵害によって、セキュリティは危険にさらされる可能性があります。

侵入型セキュリティ リスク
セキュリティはアクセス提供機能の一環でもあります。提供されるアクセス メカニズムが多いほど、複数の攻撃対象領域へより多くの侵入の機会が与えられることになります。いくつかの場合、このリスクは相互依存型または偶発的セキュリティ リスクとよく似ており、パスワードの露出やデバイスの設定ミスによって、攻撃対象領域を増やす結果を招きます。



エンタープライズ ネットワーク☒における 4 種類のセキュリティ リスク

レイヤー 5：主要なセキュリティ**構成対象**

セキュリティ体制強化の目的はこれら 4 種類のリスクを軽減することです。

それを達成するためにいくつかの重要なセキュリティ指標があります。それらは、リモート接続プラットフォームのセキュリティを強化するための一要素として構成する必要があります。

アイデンティティ (ID)
関係者を明確に特定できる一意のシグネチャを確立します。

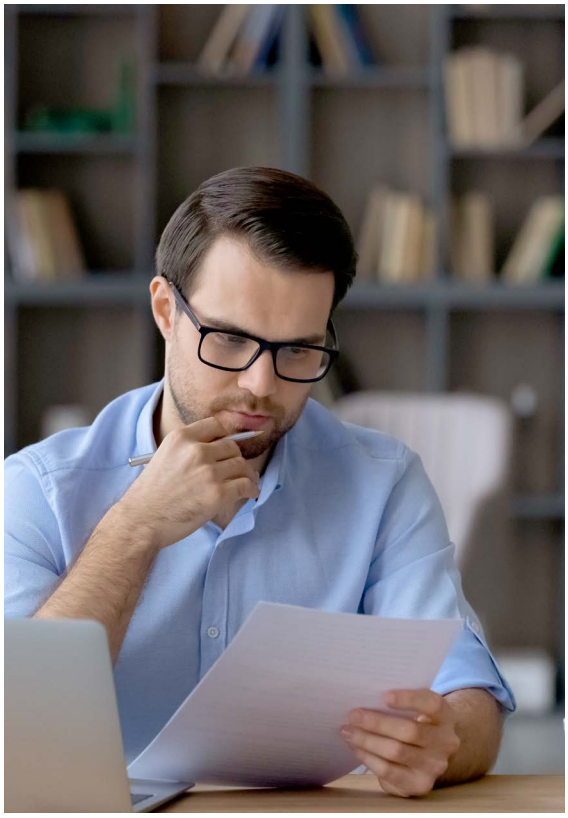
安全な通信の多くでは、実際の ID は常に秘匿され、関連付けられた一時的な ID が使用されています。

TeamViewer は、Active Directory または TeamViewer 会社プロフィールを元にユーザー ID を作成する柔軟なオプションを提供しています。

認証情報
これは、2人の間で確立される前に、接続を検証するために使用されます。

これは、相互認証や、両者間で交換される情報をコード化してメッセージを難読化するために使用することができます。

パスワードと 2 要素認証とは別に、TeamViewer はユーザーのシングル サインオン (SSO) とリモート デバイスへの無人アクセスをサポートし、侵入型セキュリティ リスクに対する完全な保護を保証します。



ポリシー
リクエストに含まれる特定のパラメーターにもとづいてアクセス リクエストを審査するための一連の基本原則を定義します。例えば、ファイアウォール ポリシーではリクエスト パケットの IP アドレスとポート番号にもとづいて、パケットの受け入れ許可及び拒否を判断するためのポリシーを構成します。機器やシステムへのアクセス管理についても、誰が、どこから、いつアクセスするかにもとづいて、同様にポリシーが考案されています。

ユーザーやグループにもとづく一般的なアクセス制御ポリシーとは別に、TeamViewer はまた、多くの形式の相互依存型セキュリティ リスクに対処するために柔軟なポリシー オプションをサポートしています。特定の時間枠、ホストのプロフィールにもとづいて設定する条件付きアクセスを提供します。

接続性
これには、安全なエンドツーエンドを確立する仮想の接続コンテキストが含まれます。例えば、HTTPS を使用するすべての Web サイトは、すべての HTTP トラフィックに対して SSL レイヤーを使用して、Web サーバーとブラウザ間の通信を保護しています。同様に、VPN 接続は接続のコンテキストに IP をカプセル化する IPIP トンネル接続を使用しています。

TeamViewer は、ネットワークに依存しないエンドツーエンドの安全なシステムにより、リモート アクセスのユースケースに VPN よりも高い信頼性の接続を提供します。これは、VPN ネットワークと同等レベルの内在的セキュリティの軽減を実現します。

導入
アプリケーションの継続的なセキュリティ保護に関わる、導入関連のパラメーターを管理します。

鍵交換、ソフトウェア更新、パッチ管理、不審なイベント管理のメカニズムは導入の範囲に含まれます。

TeamViewer は、ネットワークに依存しないエンドツーエンドの安全なシステムにより、リモート アクセスのユースケースに VPN よりも高い信頼性の接続を提供します。

セキュリティ体制の強化

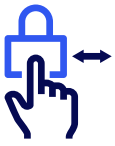
セキュリティの設定を重ねていくことによって、セキュリティリスクに対処する多くのオプションが提供されます。しかし、理想的なセキュリティ設定に到達するには大変な作業があるように思えるでしょう。セキュリティの強化によってユーザー体験を損い、日々の業務を困難にさせ、摩擦をおこすようなことがあってはいけません。

プロセス
様々な複雑な構成とリスクの組み合わせの可能性にかかわらず、セキュリティ意識向上のプロセスを確立するために、いくつかの主要なルールがあります。

レイヤー 6 : セキュリティの黄金ルール

これらのルールは、あらゆるエンタープライズのリモート接続をサポートする、最善のセキュリティ体制に到達するためのガイダンスを提供します。これらのルールは、ユーザー アカウントの設定と導入後にあらゆるシステムへ迅速に展開することを推奨します。

多要素認証



アクセスの容易性

許可リスト

強力なパスワード

更新

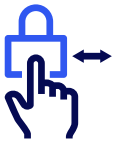
バックアップ

多要素認証

多要素認証 (MFA) は、認証情報の漏洩に起因した侵入型セキュリティ侵害に対処する追加の認証レイヤーを提供します。単一要素認証は、ユーザーの既存の認証情報を使用します。これらの認証情報が漏洩した場合、迅速な復旧は不可能です。そこで、この場限りの 2 つ目の要素を生成し、一時的な追加の認証情報として使用します。これはメール、SMS、電話などの別の通信チャネルで共有して、[redacted]関係者[redacted]が追加の安全対策のステップとして使用することができます。

2 要素認証 (2FA) は最も推奨される多要素認証 (MFA) 方法です。しかし重要性を考慮して、一時的なパスワード、コード、秘密の質問といった追加の要素を構成して一時的な認証情報を有効化する必要があります。

TeamViewer は、銀行や金融機関のような高度に規制された分野で業務を行う企業向けに、ワンタイム パスワード (OTP) や、スマート カード リダイレクト メカニズムをサポートし、より安全な認証を実現しています。



アクセスの容易性

同じシステムに繰り返しアクセスするとき、追加の手順を何度も行う必要があるため、ときにセキュリティは負担となります。この場合、関係者は日々の業務において機器を操作します。

例えば、使用後に自動でロックがかかるよう、会社のポリシーによって設定されたデバイスに、日常業務のためにアクセスするオペレーターがいます。

簡易アクセスは、複雑なセキュリティ プロセスを経ることなく日々の業務を行えるよう、関係者と機器をペアリングするために優れたメカニズムを提供します。日常業務では、無人アクセスや自動化などのいくつかの利点を活用することができます。

TeamViewer では、ユーザー向けのシングル サインオン (SSO) や信頼済みデバイスへの無人アクセスなど、複数の組み込みメカニズムを使って、アクセスの簡易性を提供しています。

許可リスト

許可リストは、特定の関係者のみがシステムへアクセスできるようにポリシーを定義します。これは、システムのアクセス ポリシーの一部です。全員を許可するワイルドカードではなく、関係者を限定するルールを備えた簡潔な許可リストを使用することを推奨します。

TeamViewerは、会社プロフィール全体のようなワイルドカード エントリのサポートも含め、アカウントとプロファイルをもとにコンピュータへの接続許可または禁止を管理する、個別の許可リストとブロック リストを提供します。

強力なパスワード
パスワードは、安全な通信のために最も広く使用されている認証方式です。したがって、組織内で強力なパスワードを選択するように啓蒙することが不可欠です。

強力なパスワードのための主な要素は以下のとおりです。

- 辞書にある単語、名前、誕生日など公表済みの情報、ソーシャル エンジニアリングによって容易に推測できる情報を含まない、固有のパスワードであること
- 大文字小文字、数字、記号を含む長いパスワードであること
- 最低でも 3 つの単語を使用し、よくあるアルファベット、数字、隣接したキーワードの組み合わせを避けるためにランダム化すること

パスワードは定期的な変更が推奨されます。さらに、ほとんどのシステムではパスワード ポリシーを保有しており、ルールにもとづいて強力なパスワードを設定するように強制されます。

- TeamViewer は、各セッション後のパスワードのランダム化をサポートします。さらに、ゼロ知識のアカウント回復方法を使用してアカウントを回復することも可能です。

更新
サードパーティのアプリケーションと OS にソフトウェア更新を適用できます。古いバージョンはハッカーの格好の標的となり、組織のセキュリティ上の弱点となります。

大規模なパッチ管理では、人為的なミスを回避し、システムを常に最新状態に保つよう、ソフトウェア更新の手順を自動化する必要があります。

TeamViewer は、導入済みのすべてのハードウェアとソフトウェアの最新情報を提供して、古く、脆弱性のあるソフトウェアに自動でパッチを適用し、修正を行います。

バックアップ
バックアップは、情報のコピーを作成して他のデバイスやクラウド ストレージへ保存するアプリケーションです。更新と同様に、バックアップも自動化して常に最新の情報が保存されるようにする必要があります。

TeamViewer では、単一の画面から最高水準セキュリティのクラウド データ ストレージによるバックアップとデータ復元をあらゆるデバイス向けに行え、災害からの復旧シナリオに完璧なソリューションを提供します。

TeamViewer：**リモート IT 管理**のためのセキュリティを重視した接続プラットフォーム

TeamViewerは、成長する企業や、大規模に事業を展開しているエンタープライズがその関係者にリモートアクセス、サポート、制御を提供することを可能にするセキュリティ重視のリモート接続プラットフォームです。バリューチェーン全体、さまざまなビジネス部門、あらゆる地域やタイムゾーンで活動する、従業員、パートナー、顧客を簡単にサポートできます。これにより、安全な方法で生産性と俊敏性が向上します。

TeamViewer は、4096 ビット RSA キー暗号化、256 ビット AES セッション暗号化に加え、情報セキュリティ管理のために ISO/IEC 27001 認証基準を使用しており、内在的セキュリティ リスクをネットワーク レベルで最小化することを保証します。アプリケーション レベルでは、TeamViewer は、あらゆる相互依存型セキュリティ リスクに対処して最大限の保護を保証するシングル サインオン (SSO) などのアプローチを通じてアクセスの容易性を促進し、アクセス管理のために多くのセキュリティ代替モジュールをサポートします。

さらに、TeamViewer は、アクセス制御を管理する多くのアドオンのセキュリティ機能を提供します。これらの機能はまた、重要なネットワーク リソースの保護も強化します。例えば、デバイス識別子、時間枠、有効期限を含む条件付きアクセス ルールは、アクセス制御のための追加のセキュリティ レイヤーとして機能します。さらに、多要素認証 (MFA) 、生体認証にもとづくセキュリティ機能を利用することもできます。これらすべてのオプションは、あらゆるセキュリティ リスクの可能性を退け、リモート サポート セッションを安全にするよう、設計されています。

コンプライアンス

> “Bühler は 2020年 ISO 27001 準拠の認証を取得しました。特にセキュリティの領域において、当社は TeamViewer Tensor によってこの認証に向けた重要なステップを踏み出すことができました。”
>
> — **Roland Isler,** Bühler 社 上級システム管理者

リモート接続は、従業員や多様な関係者に安全で俊敏なデジタル エコシステムの提供を望む企業にとって重要な要素です。

当社のお客様は、アプリケーションとデータにアクセスする従業員の管理や保護のためのソリューションとして、TeamViewer を信頼しています。

その信頼には以下のことが求められます。

- 当社のサービスが最も認知された認証や規制の要件を満たしていること
- 当社のお客様がその業界のセキュリティの認証や規制を満たすのを支援すること

TeamViewer サービス **認証**

TeamViewer は、さまざまな認証に準拠しています。コンプライアンスや規制の環境は常に変化します。最新のリストはこちらからご確認いただけます。
www.teamviewer.com/ja/trust-center/industry-leading-security/

御社のコンプライアンス要件に対応
TeamViewer は、有効な国際的なコンプライアンス要件の大半に準拠し、認定されています。

SOC2
Service Organization Controls 2 (SOC2) は、受託企業に関するレポーティング フレームワークであり、5 つの信頼提供原則 (TSP) に関する非財務的な内部統制に関して報告します。システム セキュリティ、可用性、処理の完全性、機密性、プライバシーがその原則に含まれています。

HIPAA/HITECH
TeamViewer は、リモート アクセス、リモート サポート、オンライン コラボレーション機能を、HIPAA 準拠に必要なレベルのセキュリティとプライバシーとともに提供します。

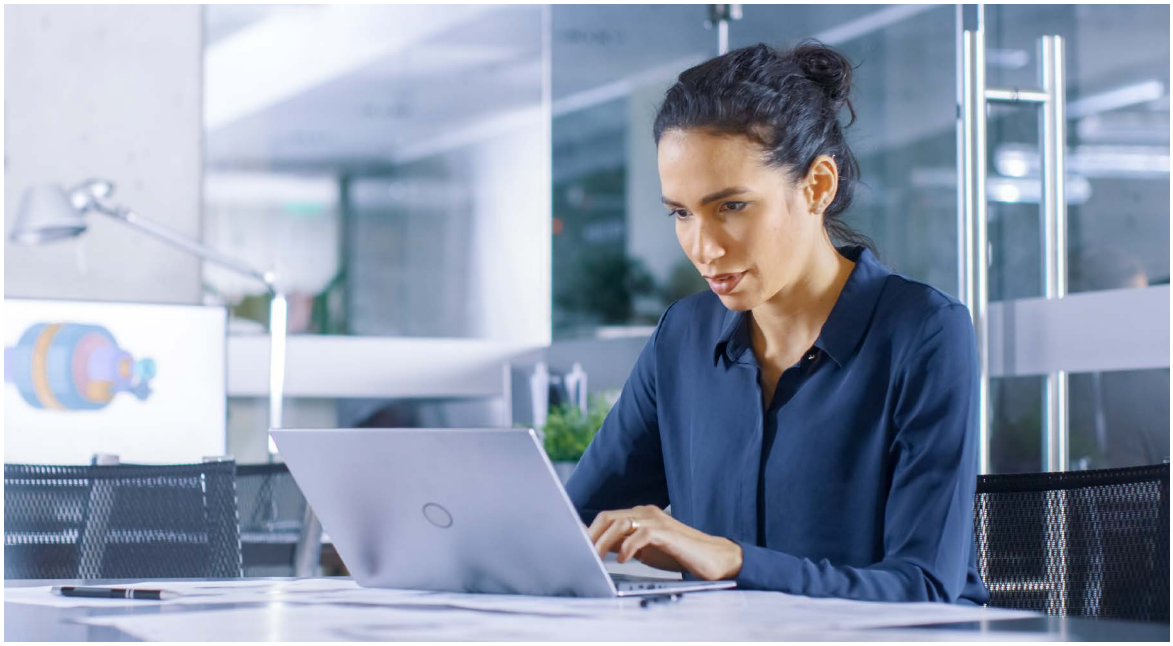
TeamViewer は、顧客の個人情報とその従業員と業務内容を GDPR に従って適切に扱う国際的な組織です。TeamViewer のデータ プライバシー コミットメントと GDPR に関する詳細は、当社ナレッジ ベースの TeamViewer と GDPR のページをご覧ください。

TeamViewer が使用するすべてのデータ センターは、情報セキュリティ マネジメント システムおよびセキュリティ コントロールの国際規格である ISO/IEC 27001 認証を取得しています。
データセンターには、個人のアクセス制御、ビデオ カメラによる監視、動作感知装置、24 時間 365 日対応の監視といった最先端のセキュリティ対策が導入されています。データ センターへのアクセスが承認された人物のみが現場のセキュリティを担当するとともに、ハードウェアとデータに対する最高のセキュリティを保証します。また、データセンターにある 1 カ所のみの入り口で ID チェックが行われています。

ISO 9001 : 2015 は、品質マネジメントシステム (QMS) の要件を定めている世界的に認められた規格です。組織は顧客や規制要件を満たす製品やサービスを一貫して提供できる能力があることを証明するために、この規格を使用します。TeamViewer は、総合的な品質管理や顧客重視だけでなく、作業のさらなる効率化や製品とサービスの品質向上への継続的なプロセス改善を献身的に行っていることを、ISO 9001:2015 の認証によって実証しました。

DigiCert Code Signing を介した署名により、当社のすべてのソフトウェアにはさらなるセキュリティ レイヤーが提供されています。これにより、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。

TeamViewer は、ISO 27001 にもとづいて自動車業界における高品質な IT セキュリティの評価を合理化するように設計された TISAX ラベルを取得しています。



追加資料

セキュリティ資料

セキュリティ ハンドブック :
community.teamviewer.com/Japanese/kb/articles/108686-welcome-and-introduction

6 つのセキュリティ黄金ルール
community.teamviewer.com/Japanese/kb/articles/108694-six-golden-security-rules

多要素認証

2 要素認証の有効化
community.teamviewer.com/Japanese/kb/articles/66-activate-two-factor-authentication

アクセス管理

条件付きアクセスと管理者が着信および発信接続を制御する方法
community.teamviewer.com/Japanese/kb/articles/57261-get-started-conditional-access

パスワードに加えて物理的なセキュリティ キーを使用してアカウントを保護する方法
community.teamviewer.com/Japanese/kb/articles/109554-security-key-redirection

シングル サインオン (SSO)

SSO による時間と労力の削減
https://community.teamviewer.com/Japanese/kb/articles/30784-single-sign-on-sso

コンプライアンスと監査

TeamViewer が遵守するコンプライアンスと国際標準
community.teamviewer.com/Japanese/kb/articles/108692-compliance-international-standards

可監査性 :
ビジネスを保護し、社内で発生したサポート体験を追跡
community.teamviewer.com/Japanese/kb/articles/54970-auditability-event-log

TeamViewer コミュニティとナレッジ ハブ

英語 (EN)	community.teamviewer.com/English
ドイツ語 (DE)	community.teamviewer.com/German
日本語 (JP)	community.teamviewer.com/Japanese
フランス語 (FR)	community.teamviewer.com/French
スペイン語 (ES)	community.teamviewer.com/Spanish
ポルトガル語 (PT)	community.teamviewer.com/Portuguese
中国語 (CN)	community.teamviewer.com/Chinese

詳しい内容をお知りになりたいですか？

Web サイトに移動 :
www.teamviewer.com/ja/

TeamViewer

TeamViewer について

世界的なテクノロジー企業として、TeamViewer はあらゆるプラットフォームのあらゆるデバイスに、どこからでもアクセス、制御、管理、監視、サポートできる安全なリモート接続プラットフォームを提供しています。60 万以上のお客様にご利用いただいている TeamViewer は、個人用途・非商用目的であれば無料で使用でき、25 億台以上のデバイスにインストールされています。TeamViewerは、リモート接続、拡張現実、IoT、デジタル・カスタマー・エンゲージメントの分野で継続的に革新を続けています。あらゆる業界の企業がシームレスな接続を通じてビジネスクリティカルなプロセスをデジタルに変革できるよう支援しています。

2005 年に設立され、ドイツのゲッピンゲンに本社を置く TeamViewer は、全世界で約 1,400 名の従業員を擁する株式公開企業です。TeamViewer AG（TMV）はフランクフルト証券取引所に上場している、MDAX の構成銘柄です。

www.teamviewer.com/support

TeamViewer Germany GmbH
Bahnhofsplatz 2 73033 Göppingen Germany
+49 (0) 7161 60692 50

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
03 4563 9650

Stay Connected

www.teamviewer.com/ja/