ezHelp リモートサポートサービス

セキュリティホワイトペーパー

Feb 2017

目次

この資料は、ezHelpのリモートサポート製品の接続セキュリティ関連資料です。コンピュータをリモートで操作することは、安全性がとても重要です。ここに弊社製品のセキュリティ設計と構成について説明し、どのようなセキュリティを施しているのかについて情報の開示を行います。

対象

本資料は、技術的な資料として、ネットワーク管理者の方のために作成されました。この資料で説明されている情報は、技術的な詳細内容です。この資料を通して ezHelp サービスを導入する際のセキュリティについての疑問点を確認・解決するための参考とすることができます。

1. 接続セキュリティについての立場

IOTの技術が発達することによって、企業のリモートによる製品をサポートしたり、または問題を分析するリモートサポートの市場が進化し続けています。多くの企業は、リモートサポートを導入することを検討しており、それに伴うセキュリティへの関心が高まっています。昨今はオンライン状態の製品やオンラインサービスなどが増加しているため、セキュリティとインターネットはさらに密接な関係にある時代に突入しております。しかし、ほとんどのユーザーはオンラインサービスや製品のセキュリティについて、未だに無関心な傾向が続いている状態です。

常に問題になっているオンラインセキュリティの事故を見れば、簡単なパスワードの設定や的確なセキュリティパッチなどをしておらず、または未知のファイルを疑うこともなくダウンロードしたり、実行ファイルをインストールしたりするせいで発生する様々な問題などがあります。このように、ユーザーは、オンラインでのセキュリティについて意識が低くかなり脆弱であるため、違法サイバー攻撃は減っていません。

サイバー攻撃は、技術的な進化でますます加速し、日々進化と変化しており、サイバー攻撃の自動化も増え、インターネットセキュリティは、常にどこからその脅威にさらされています。専門的なネットワーク技術者であっても間違ったファイルをダウンロードしてしまったり、セキュリティパッチの最新更新を怠ってしまったりしまうことによって、企業全体のネットワークがサイバー攻撃からの被害に遭う可能性があります。

ezHelpは、企業がインターネットに接続されているお客様のコンピュータにリモートで接続してサポートをするリモートサポートサービスシステムです。お客様の意識は、たとえ社会的に認知された企業であっても、オペレータにコンピュータを自在に操作されてしまうことはとても不安であり、接続やセキュリティについての心配をすることは事実です。とはいえ、リモートサポートによって顧客自身で解決できない問題を安価でスムーズで目の前でリアルタイムに企業の相談オペレータが解決してくれる利便性も、実は望んでいるのも確かです。

リモートサポートをする場合はezHelpのように、セキュリティ的に信頼の高いリモートソフトウェアを使用する必要があります。ezHelpリモートサポートサービスは、常にネットワークを

監視して脅威から保護しており、セキュリティリスクに何の心配もなく、顧客サポートをすることができます。

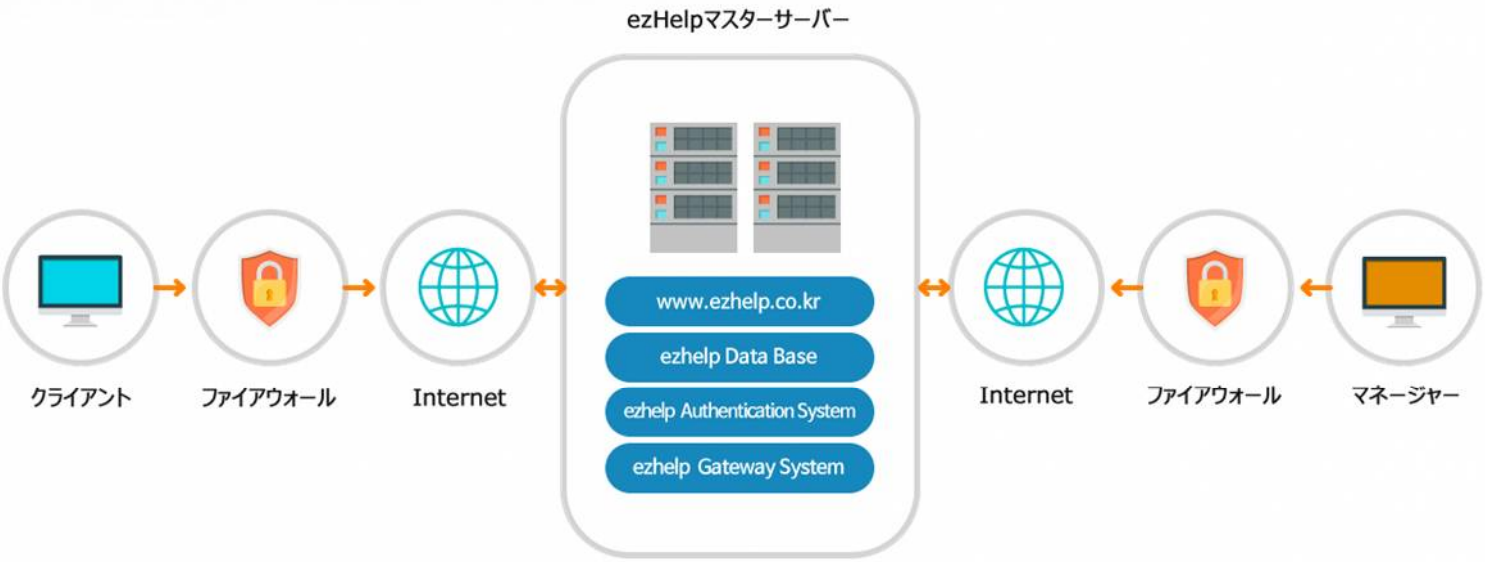
ezHelpは、リモートサポートにおいて、安全なセキュリティとシンプルで快適なサポートと安定的に動作し続けながらリモートサポートサービスの品質を高めるための技術とインフラを構築しています。サービスすべての段階で安全性を考えて設計されており、技術的、物理的なセキュリティ対策を徹底的にしています。

ezHelpの導入で業務の効率化と生産性を向上させることができ、顧客サポートによるコストの削減でもすることができます。

2. ezHelpの アーキテクチャー

1) アーキテクチャー

ezHelpが設計したセキュリティメカニズムを説明する前に、ezHelpサービスのアーキテクチャーをまず説明します。



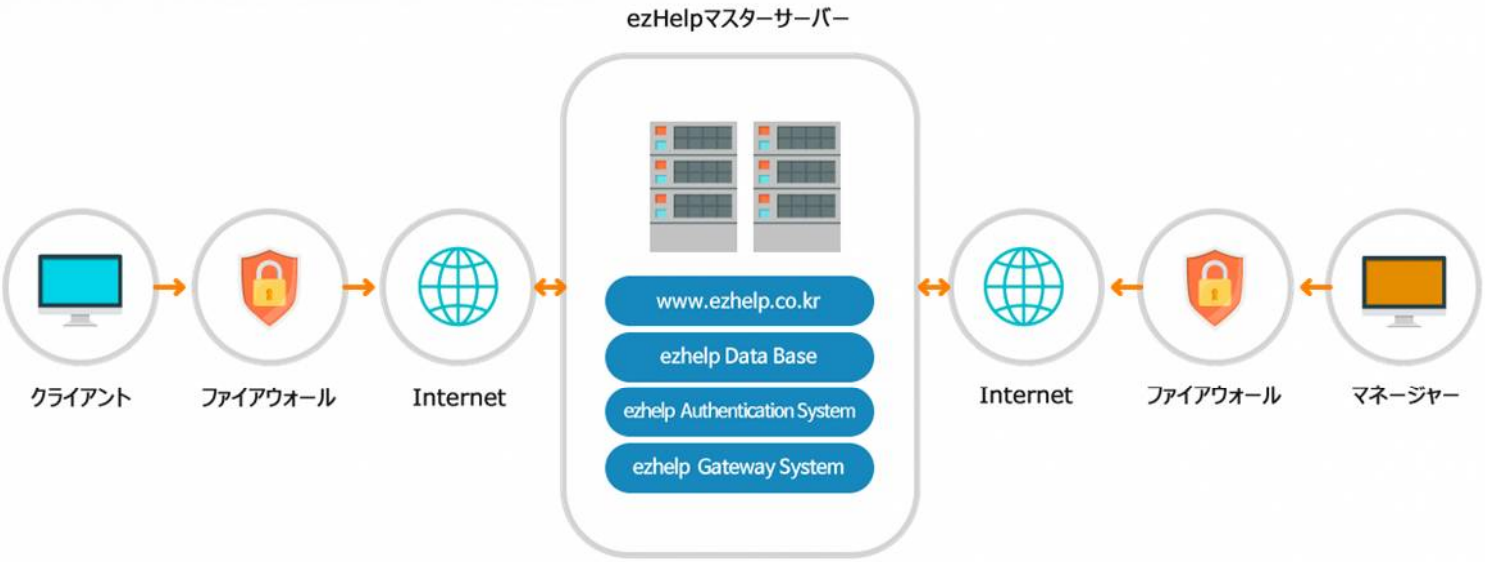
<図 1. ezHelpアーキテクチャー>

ezHelp アーキテクチャーは、リモートアクセスのセッションに関連するエンティティ（ENTITY）が3つあります。 クライアントPCは、リモートサポートを受ける人、またはコンピュータです。 ezHelpマネージャーは、接続しているコンピュータまたはそのコンピュータのezHelpホストソフトウェアです。 ezHelpマスターサーバーは、クライアントPCとezHelpマネージャーとの間の認証及びトラフィックを仲介しています。

2) 設計原理

ezHelpは、重要なリソースとしてリモートアクセスを信頼できないネットワークを経由しても安全に実行できるように設計されています。利便性よりもセキュリティ性により重点的に設計しました。

3) サービスのフロー



<図 1.1. ezHelpアーキテクチャー>

① ezHelp マネージャーは ezHelp 認証システムにユーザー認証を使用してログインし、接続コード 6 桁を与えられます。

② 接続コード 6 桁をクライアント PC に伝えた後、その接続コードを介して ezHelp マネージャーとリモート接続を実行します。

③ クライアント PC は、ezHelp 認証システムを介して ezHelp マネージャーとの接続タイプを判別します。

④ 直接接続が可能な場合には、クライアント PC と ezHelp マネージャー互いに直接接続を決定して、リモート接続が実行されます。

⑤ もし、直接接続が困難な環境の場合には、ezHelp ゲートウェイシステムを仲介して、リモート接続が実行されます。

3. 技術的なセキュリティ

1)　リモート接続と接続タイプ

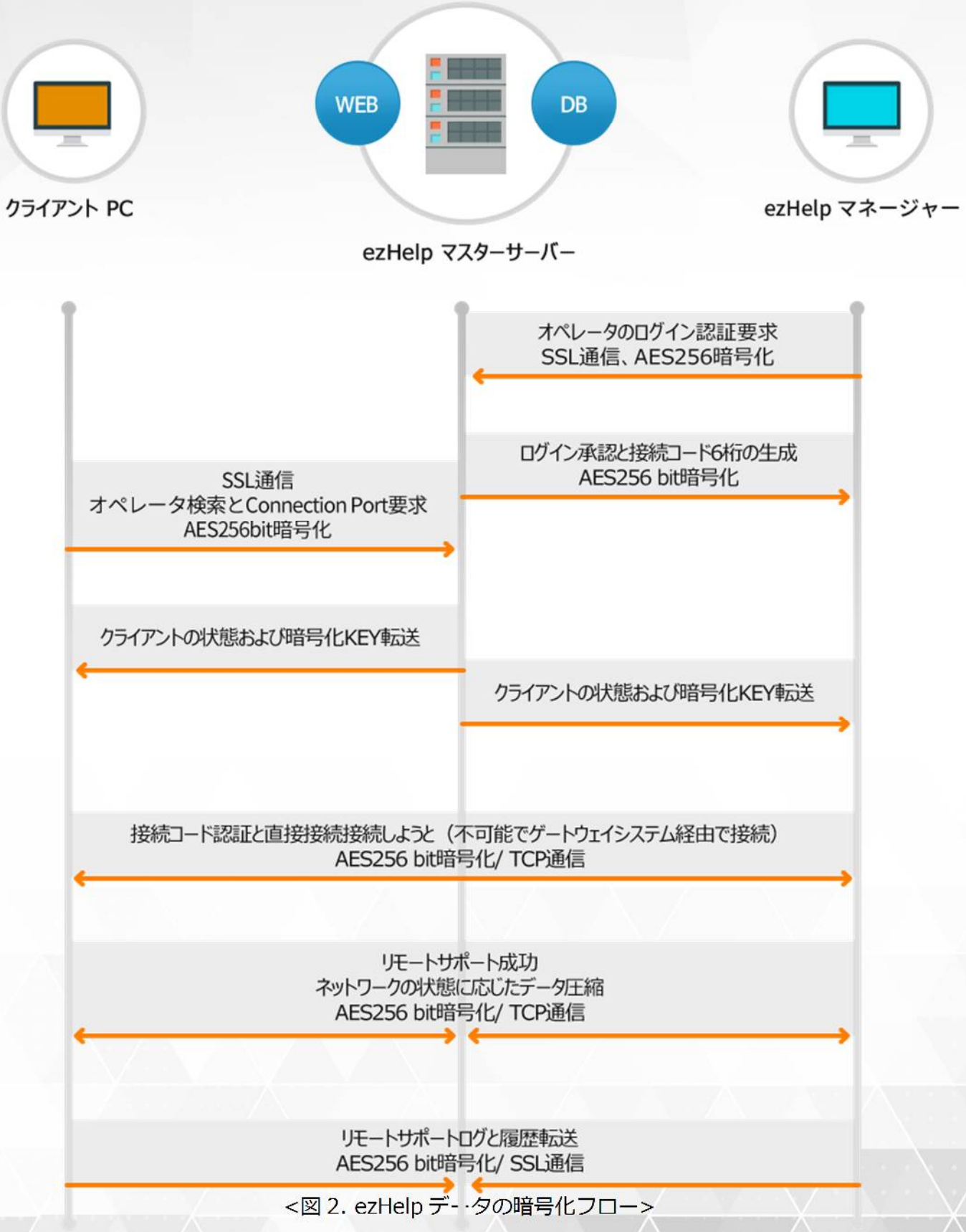
ezHelpのリモートアクセスの認証に使用される接続コードはランダムに6桁の数字で提供されて、生成された接続コードは、ezHelpマネージャーとのリモート接続のために使用され、第3者の任意のアクセスは、徹底的に許可しません。また、ezHelpマネージャーを再起動すると、新しい接続コードが生成されるため、接続コードを案内されたクライアントPCのみ接続することができます。

リモート接続を行う場合、ezHelpが最適で接続タイプを決定します。ほぼすべてに対し、ezHelp認証システムを経由した後、TCPを介して直接接続が確定されます。また、すぐに接続が困難な場合は、TCPを介してezHelpゲートウェイシステムを経由して接続されます。

2) データの暗号化

リモートアクセス情報を暗号化処理せずに平文で送信すれば中間者攻撃（MITM：Man in the Middle）への脅威を受けることができてしまいます。安全なデータ転送のためには、クライアントPC上で1次暗号化を介して送信されるデータのセキュリティ処理をする必要があります。ezHelpは、すべてのリモートアクセスで転送されるデータをEnd-to-Endで256bit AESセッションの暗号化を介して転送します。

ezHelpデータトラフィックは、256bit AESセッションの暗号化を利用して保護されます。この技術は、https/ SSLと同じ形式で利用されて、現在の基準でもっとも安全な方法です。また、毎回生成される暗号化キーを使用して完全に保護されるので、悪意のある攻撃者のスニッフィング（Sniffing）攻撃にも解読が不可能な状態で安全にデータを転送して保護されます。



<図 2. ezHelp データの暗号化フロー>

3) ネットワークセキュリティ

ezHelpは、ネットワークされたユーザーのデータを保護するために強力な業界標準の技術を使用しています。SSL（Secure Socket Layer）のデータ暗号化は、ezHelpシステムとezHelpマネージャーとクライアントPCとの間の安全な接続を作成します。リモート接続の接続時に強力な2048-bit SSL暗号化通信を提供して、クライアントPCとezHelpシステム間で転送されるすべてのデータについては、暗号化通信を提供することにより、悪意のある攻撃者のスニッフィング（Sniffing）攻撃にも解読が不可能な状態で安全にデータを送信します。

ezHelpは、リモートサービスサイトへのアクセス時にHTTPS通信を使用して、安全なウェブアクセスを提供し、リモートサポートのウェブサーバーは、外部からアクセス可能なページには、重要なデータを保存しません。ezHelpシステムに最新のセキュリティパッチを適用し、メッセージ / 要求 / 応答などのセッションで正しくない再送信攻撃を防止するための方針を適用しています。

4) デジタル署名されたアプリケーション

ezHelpで配布するすべてのソフトウェアは、最も強力で安全なデジタル署名（VeriSign Secured）がされてプライベートキーがなければどのような個人も、変更または更新をすることができません。後でソフトウェアが変更されると、デジタル署名が自動的に無効にされて、セキュリティリスクから安全を保証します。

5) データセンターのセキュリティ

ezHelp は日本国内のデータセンターをベースに ezHelp 専用のネットワークを構成しており、このネットワークに基づいてサービスを運営、管理します。また、システム構成をミラー化して、天災でシステム障害が発生しても、代替システムを介して信頼性の高いサービスの提供が可能です。また、個人アクセス制御、CCTV 監視、指紋アクセスコントロールなど 365 日、24 時間の監視と現場保安要員を介して認証された人だけに、データセンターの出入りを許可しています。

4. アプリケーションのセキュリティ

6 桁の接続コードを使用

ezHelp は、リモート接続の安全性を確保するためにリモート接続をする場合は、接続コードを使用することができます。ezHelp マネージャーが遠隔接続のために、6 桁の接続コードを伝えます。クライアント PC は、ezHelp マネージャーから受けた接続コード以外のコードでは、リモート接続を許可することができません。6 桁のの接続コードは、ezHelp マネージャーの固有のコードであり、ezHelp マネージャーが新たにログインすると、毎回接続コードは変更されます。

ステルスモード不可

ezHelp は、リモート接続中のクライアントに必ずリモートサポートという表示をクライアント PC に表示するようになっています。これは、現在の ezHelp マネージャーが正常にリモート接続中であることを知らせるためです。したがって、ezHelp マネージャーがクライアント PC に潜入して監視したり、不適切なプログラムをインストールすることは一切できません。

リモートの権限回収

ezHelp のリモートサポートは ezHelp マネージャーがリモートでクライアント PC を制御しているが、もし ezHelp マネージャーがクライアント PC の機密情報を事前の同意なしに修正/削除したり、悪意のあるプログラムをインストールしようとするときに、クライアントは ezHelp マネージャーからリモート制御をすぐに回収して、不要なリモート接続をブロックすることができます。

指定された IP ログイン

ezHelp サービスを利用する管理者 ID は、オペレータが指定したコンピュータ以外のコンピュータからお客様のコンピュータをリモートサポートすることを不可能にします。管理者は、オペレータの IP アドレスをリストで管理して追加 / 削除をすることができます。

接続ログ

ezHelp はオペレータが ezHelp マネージャーにログインをした記録とクライアント PC へのリモート接続を実行した記録をすべてログに保存するため、オペレータがいつ、どのような顧客に遠隔接続をしたのか、問題はなかったのかなどをチェックすることができます。また、遠隔接続のログは、グラフの統計で提供します。

5. 総評

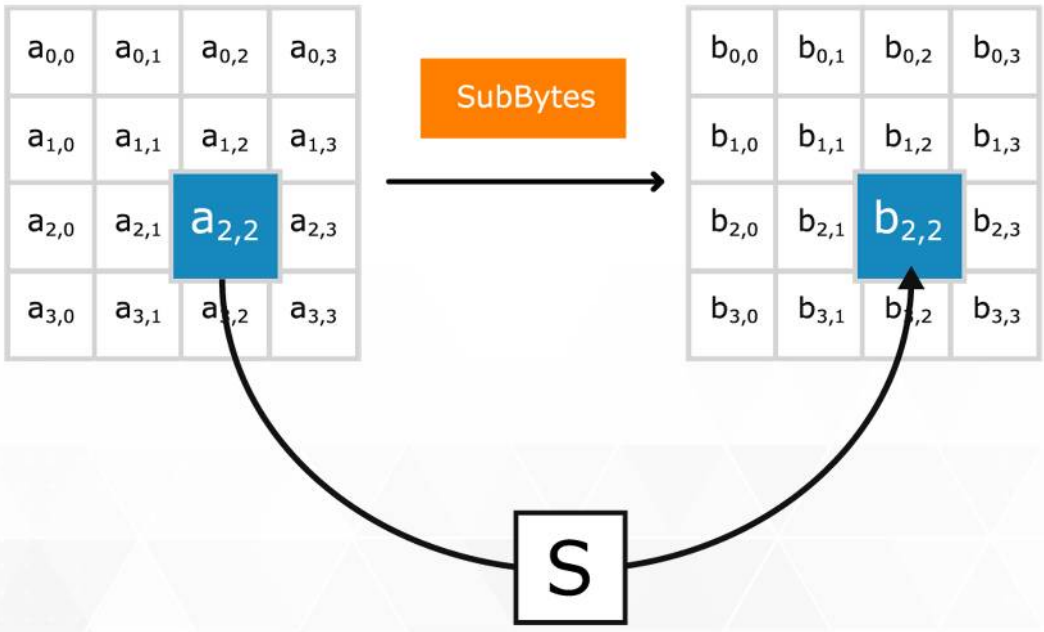
ezHelpリモートサポートサービスは、最高のネットワークセキュリティチームによって設計されており、最先端の暗号技術と認証技術を導入しました。これらのセキュリティ設計に基づいて、最適なリモートサポートサービスをしており、ネットワークのセキュリティシステムがリアルタイムで常にデータを保護監視しています。また、ezHelpは、独自のセキュリティプロトコルを含む国際セキュリティ基準を満たしており、これを徹底的に遵守しています。製品のセキュリティは、継続的な投資と支援、そしてグローバルレベルの環境が整ってなければ、完全なセキュリティが可能です。ezHelpは、お客様の安全のために、常に万全の準備をしています。

6. APPENDIX

用語の説明

AES (Advanced Encryption Standard)

アドバンス暗号化標準（AES）は、2001年に米国標準技術研究所（NIST）によって制定された暗号化方式です。AESは、アメリカ政府が採用した以来、世界中で広く使用されており、1977年に公表されたDESを取り替えたAESは、暗号化と復号化の過程で、同じキーを使用して対称鍵アルゴリズムです。AESは、ISO/ IEC18033-3規格に含まれており、複数の暗号化パッケージで使用されています。AESはまた、アメリカ国家安全保障局によって1級秘密（TOP Secret）に使用できるように、承認されたアルゴリズムの中で最初に公開されているアルゴリズムです。



SSL (Secure Socket Layer)

SSLは、ネットワーク内でメッセージ転送の安全性を管理するために、Netscapeによって作成されたプログラムのレイヤーです。

ネットスケープの考えは、秘密が保証されるべきメッセージを引き受けたプログラムはウェブブラウザやHTTPなどのアプリケーションとインターネットのTCP/ IPレイヤーの間に入らなければならな

いというものです。ここで言う「ソケット」とは、データをネットワーク上のクライアントとサーバーのプログラム間または同じコンピュータ上のプログラムレイヤー同士やりとりソケット方式を指します。

SSLは、クライアントとサーバーの間で情報を暗号化して、万が一ハッキングを介して情報が流出されることが起こらないよう、情報の内容を保護することができます。SSLはウェブ製品だけでなく、ファイル転送プロトコル（FTP）などの他のTCP/ IPアプリケーションに適用することができ、認証暗号化機能とデータの暗号化など、インターネット上の脅威から保護することができます。

SHA-2ベースのSHA-256ハッシュアルゴリズム

SHAは、安全なハッシュアルゴリズム（Secure Hash Algorithm）は、アメリカ国立標準技術研究所のNISTが標準で採用したことで、互いに関連している暗号ハッシュ関数の集合です。その中SHA-2に基づくSHA-256は、32ビットのワードを使用しているハッシュ関数であり、SHA-1、SHA-0よりも攻撃により安全であると知られています。

MITM (man in the middle attack, 中間者攻撃)

中間者攻撃は、ネットワーク通信を操作して通信内容を盗聴したり、操作する攻撃テクニックである。中間者攻撃は、通信を接続する二人の間に中間者が侵入して、二人は相手に接続したと思うが、実際には2人は中間子に接続されており、中間子が片側から渡された情報を盗聴や操作した後、反対側転送する方法です。