セキュリティドキュメント

TÜV SÜD ISO 9001

目次

最も重要な事項の要約

コンテンツセキュリティ

データ圧縮と暗号化	会議の参加者と共有されたすべてのコンテンツは、独自の圧縮アルゴリズムで圧縮されています。この圧縮されたコンテンツは、適切な Mikogo 参加者ソフトウェアのみにより解読されます。Mikogo はクリアテキストで会議の内容を送信しません。256 ビットの AES 暗号化方式を使ってすべてのデータを暗号化しています。
ウェブサイトの暗号化	Mikogo のウェブサイトは SSL（Secure Sockets Layer）を使用した 128 ビットの暗号化で保護されています。SSL（Secure Sockets Layer）はセキュリティー重視の Web データ通信に最も広く採用されているインターネット標準です。ベリサイン/ Thawte 社によって署名されてた SSL Web サーバ証明書があります。

ユーザーインターフェイスのセキュリティ

セッション ID とセッションパスワード	一意的にセッションを識別できる、ランダムに生成された 9 桁のセッション ID が主催者に割り当てられます。更なるセキュリティーのためにセッション・パスワードが準備されます。セッション参加にはこれらのセッション ID とセッションパスワードが必要です。
役割と責任	Mikogo セッションにはいくつかの役割があります。主催者、発表者、そして参加者です。主催者にはユーザー名とパスワードが必要であり、主催者は唯一セッションを開始する権限を持ちます。 発表者はデータをシェアする権限を持ちます。発表者はセッション中にどのデータがシェアされてよいかの決定ができ参加者のアクセスの度合いを決めることもできます。発表者の権限を他に渡すこともできます。発表者になる前に、参加者が自分のコンピュータの画面を送信することに明確に同意する必要があります。遠隔操作の権限を与える時も同じく明確な同意を必要とします。 発表者の明確な同意なしに、コンピュータの画面を表示したり、制御することはできません。

インフラのセキュリティ

第三者のアクセスの防止	M Mikogo は最先端のファイアウォール、ネットワーク監視、侵入検知、のツールを採用しています。 厳格な変更管理が採用されており、内部セキュリティポリシーと手順が随時強化されています。
セッションデータは保存されていません	Mikogo セッション中に表示されたセッションの内容は発表者のコンピュータのみから発信されています。参加者は、このデータの再生表示を見ているに過ぎません。セッションが終わるとこれらの再生表示データは消滅します。

詳細

グローバルなオンラインコラボレーションソリューションプロバイダー (http://www.BeamYourScreen.com),が提供する、Mikogo は、販売、マーケティング、トレーニング、プロジェクト管理、顧客サポートのために使用される革新的なデスクトップ共有ツールです。企業からの厳しいセキュリティー要望に Mikogo が応えらえるよう BeamYourScreen は努力しています。ネットワーク、プラットフォーム、サービスについてのデザイン、開発、維持管理において、Mikogo はデータセキュリティーを最も高い優先順位を割り当てています。この文書の目的は、Mikogo で利用可のであり、基盤となる通信インフラに内在するデータセキュリティ機能に関する情報を提供することです。この文書に記載されている以下の項目について説明します：アプリケーション、ファイアウォールの互換性、コンテンツセキュリティ、ユーザ・インタフェース・セキュリティ、およびインフラストラクチャのセキュリティ。

アプリケーション

Mikogo ソフトウェアは、独自のプロトコルとデータ交換方法を使用して、北米とヨーロッパにある Mikogo サーバーと通信します。Mikogo ソフトウェアと Mikogo サーバー間の緊密な連携なしで Mikogo セッションに参加することは不可能です。 Mikogo セッション内のデータは、Mikogo サーバとの接続を確立するソフトウェアを使用して共有されます。これらのセキュリティ機能は、セッション全体に内在しています。各セッションは動的であり、Mikogo ソフトウェアと Mikogo サーバ間のハンドシェイクを伴い、これらのコンポーネント間の通信は、既定の圧縮、符号化、暗号化されています。

ファイアウォールの互換性

Mikogo ソフトウェアは、信頼性と安全な接続を確立するために、Mikogo サーバと交信します。セッションが開始されると、Mikogo ソフトウェアは通信のための最良の方法を決定します。Mikogo ソフトウェアは、ポート 80 または 443 で TCP または HTTP / HTTPS プロトコルを使用して Mikogo サーバーに接続します。TCP 接続が遮断された場合に、Mikogo ソフトウェアは、HTTP / HTTPS を使用してすべての通信をトンネルを通します。セッションが開始されたときに確立された接続のタイプにかかわらず、Mikogo セッションを可能にするようにファイアウォールを特別に構成する必要はありません。

主催者は、積極的に遠隔操作の権限を要求することができます。発表者は、常に遠隔操作権限を与えることに明示的に同意する必要があります。これは、発表者の明示的な同意なしにコンピュータを操作することができないからです。主催者と発表者はお互いの表示方向を切り替えることができます。しかし、参加者は最初に発表者になることと、自分のコンピュータ画面の表示を明示的に同意する必要があります。セッション中参加者が初めて発表者になった以後、主催者は発表する権利を取り戻し、参加者の同意なくして発表者に再度なることができます。しかし、画面の表示方向を切り替える際、主催者が常に発表者になることを明示的に同意しなければなりません。

品質管理：ISO 9001 認証

A Mikogo セッションを活用しているすべてのユーザーだけでなく、セッションに参加している皆さん、Mikogo が ISO9001 の認証を授与されたことを喜んでいただけることでしょう。国際的に知られている品質管理の要件の一つとして、ISO 9001 認証は、組織の品質管理システムが、高い顧客満足度とその適用される法令および規制要件を満たすことを強化する製品とサービスを一貫して提供する能力を持っていることを認めています。

コンテンツセキュリティ

Mikogo は、セッション中に無意識にデータを共有しないようにするいくつかのコントロールを用意しています。発表者は自分の機密ファイルを調べるとき、いつでも画面を隠すことができます。発表者はデスクトップの壁紙、デスクトップ内容、およびタスクバーを非表示にすることができます。

データ圧縮と暗号化

発表者がセッションで参加者と共有するすべてのコンテンツは元データの表現です。また、セッションで参加者と共有されているすべてのコンテンツは、独自の圧縮アルゴリズムで圧縮されています。この圧縮されたコンテンツは、適切な Mikogo の接続ソフトウェアによってのみ解読できます。さらに、Mikogo はセッションの内容をクリアテキストの状態で送信をしていません。256 ビットの AES 暗号化（高度暗号化規格）を使用してすべてのデータの暗号化をしています。

ウェブサイトの SSL 暗号化

Mikogo のウェブサイトは SSL（Secure Sockets Layer）を使用した 128 ビットの暗号化で保護されています。SSL（Secure Sockets Layer）はセキュリティー重視の Web データ通信に最も広く採用されているインターネット標準です。ベリサイン / Thawte 社によって署名されてた SSL Web サーバ証明書があります。

デジタル署名されたソフトウェア

Mikogo が提供するすべてのソフトウェアコンポーネントは、先端の認証権威であるベリサイン / Thawte の証明書を用いてデジタル署名されています。

ユーザーインターフェイスのセキュリティ

Mikogo ユーザー・インタフェースを介して公開される様々なメカニズムを通じて Mikogo セキュリティは強化されています。使用可能なオプションは、セッション参加者が想定する担当に依存します。

役割と責任

Mikogo にはいくつかの担当があります：主催者、発表者、参加者です。
主催者は、ユーザー名とパスワードを必要とし、セッションを開始できる唯一のユーザーです。
参加者は、セッションに参加することができます。
主催者と参加者の両方が発表者になれます、そして自分の画面を表示することができます。

セッションパラメータ

主催者は、9 桁のセッション ID を指定したり、セッションを一意に識別するために、ランダムに生成された 9 桁のセッション ID を使用することができます。セッションパスワードは、追加のセキュリティのために定義することができます。セッションに参加するにはセッション ID を手動で入力するか、メール招待状かインスタントメッセージに記載されている参加用 URL をクリックします。いずれの場合でも、主催者がセッションの開催日時を電話または電子メールで参加者に通知することをお勧めします。

主催者、発表者、参加者の権限

唯一、主催者のみが、特有なユーザー名と強力なパスワードを使用して Mikogo セッションを開始できます。主催者は、セッションでの最高のレベルの操作権限を持ちます。主催者と発表者は Mikogo セッション中いつでも主催者と各発表者のいずれの画面を表示するか（表示方向）の切り替えができます。この際、参加者の明確な同意を必要とします。発表者はデータを共有することができます。発表者はセッション中に何を共有可能にするかの決定ができ、参加者がセッション中にアクセス可能な範囲の決定もできます。

発表者は遠隔操作の権限を付与することができます。セッション中の任意の時点で発表者は参加者の遠隔操作の権限を取り消すこともできます。二つの方法があります。キーボードの Ctrl+ F12 キー（Windows や Linux）を（Mac の場合は Ctrl+ Esc キーで）押す方法と、システムトレイにある M アイコンをクリックして遠隔操作無効を選択する方法があります。これにより、遠隔操作中に起こり得ることを充分に制御することができます。

主催者は、積極的に遠隔操作の権限を要求することができます。発表者は、常に遠隔操作権限を与えることに明示的に同意する必要があります。これは、発表者の明示的な同意なしにコンピュータを操作することができないからです。主催者と発表者はお互いの表示方向を切り替えることができます。しかし、参加者は最初に発表者になることと、自分のコンピュータ画面の表示を明示的に同意する必要があります。セッション中参加者が初めて発表者になった以後、主催者は発表する権利を取り戻し、参加者の同意なくして発表者に再度なることができます。しかし、画面の表示方向を切り替える際、主催者が常に発表者になることを明示的に同意しなければなりません。
主催者とプレゼンターのいずれもがいつでもセッションを終了することができます。

インフラのセキュリティ

Mikogo は、高速スイッチング・サーバーの分散ネットワークを維持しています。
発表者の機器から発信されたデータと参加者の機器が受信するデータは、Mikogo のスイッチング・サーバー・ネットワークを介して ー 全く格納されずに ー 切り替わります。セッションデータは Mikogo サーバーに格納されることはありません。

セッション開始前にコンテンツを Mikogo サーバにアップロードする必要はありません。
Mikogo のセッション中に表示される活発なセッションコンテンツは発表者の機器のみから発信されます。
参加者はこのデータの表示を見ているのです。セッションの終了時にこれらの表示は消滅します。
Mikogo セッションから残るものは会話記録そのものでなく課金記録のような補助的情報です。

BeamYourScreen は Mikogo サービスの安全な環境の開発、導入、維持のために多大な時間とエネルギーの投資をしています。私たちは最先端のファイアーウォール、ネットワーク監視、侵入検知ツールを採用しています。
厳格な変更管理を採用し、追加の内部セキュリティポリシーと手順が強化されています。

結論

BeamYourScreen は、Mikogo の基盤とサービスの設計と運用において、セキュリティ原則と基準の融合に細心の注意を払っています。 Mikogo のデータセキュリティは、BeamYourScreen の最高の優先順位です。
このことは Mikogo が効率的で安全なオンラインリアルタイム通信サービスを提供する目標を達成し続けることを可能にしています。

http://www.mikogo.come からダウンロードしてオンライン会議を企画してください。