Complete Security

信頼から生まれる力を提供します

- 強固な企業セキュリティのフレームワークによってリスクを軽減し、最新のベストプラクティスに準拠しながら世界規模での運用を行います
- 事業継続性、災害復旧、ベンダー管理、インシデント管理、サードパーティのPENテストによる脆弱性管理、専任のデータプライバシー担当者による情報プライバシープログラムなど、情報セキュリティ管理のすべての面に対応します
- 世界の多国籍クライアントとサードパーティによるセキュリティおよびコンプライアンスの定期的な監査を実施します

情報セキュリティチーム

当社には、業界で累計100年以上の経験とISO 27001、ISO 10012、, *CBCP, CISSP, CISA, CISM, CEH, GCIH, GCIA, GAWN, GPE, GXPN, GSEC, GREM, GCC, GNFA, SSCP, CAPM, GSE, OSCP, GPEN, GWAPT* を含むプロフェッショナルな情報セキュリティ認定を持つ専任のグローバル情報セキュリティチームがいます。

データセンター

セキュリティガード、カメラ、生体認証を含むマルチレイヤーの物理的なセキュリティが当社の施設へのアクセスを制限します。

- ラスベガス
- トロント
- ロンドン
- フランクフルト
- パリ
- チューリッヒ
- 香港
- 上海
- 東京

セキュアなクライアントエクスペリエンスを提供することでグローバルに広がる当社のクライアントのニーズに応えるため、Consilioは強固で世界的な企業セキュリティのフレームワークに投資し、それを展開してきました。さらにそのフレームワークを採用しているテクノロジー、インフラストラクチャーおよびチームの間に完全統合しました。

Consilioセキュリティ認定

弊社の総合的なeDiscoveryソリューションは、認定を受けたセキュアなデータセンターに物理的に配置されています。

- ISO\IEC 27001:2013年認証取得
- HITRUST認定
- ITAR準拠
- Cyber Essentials Plus認定
- GDPR準拠
- CCPA準拠
- EU-米国間およびスイス-米国間 のプライバシーシールド原則*に準拠

セキュリティの特徴

- 建物はISO 27001/SAS 70またはType II/SSAE 16認定を受け、年中無休のセキュリティ、アラーム、動作検知、生体認証、マントラップ付き入口ドア、施錠ケージにより保護されています。
- データセンターを火災、水害、自然災害から守るための環境管理を行っています
- 各地理的地域にある災害復旧施設間でほぼリアルタイムのデータ複製を行っています
- データセンター、ネットワーク、システムへの厳戒な最小権限のアクセス制御
- すべてのデータはクライアントやプロジェクトごとに必然的に分けられます。
- AES-XTS 256ビットの暗号化によるデータの保管
- TLS 1.2および1.3のみを使用し、128ビットないし256ビットの対称暗号アルゴリズムを使用したデータの移動
- マルチレイヤー、マルチベンダー、MITRE ATT&CKフレームワークへの冗長カバレッジによる重複セキュリティモデル
- 採用前のバックグラウンドチェックおよび秘密保持契約の締結
- 年次の従業員セキュリティトレーニング、継続的なフィッシング意識テストの実施
- 強化されたリモートのユーザーセキュリティであるMFAを使用したセキュアな仮想文書レビューのインフラストラクチャー

EU圏はプライバシー原則を撤廃しましたが、米国商務省は未だ米国企業に同省の原則に準ずるよう求めています。privacyshield.gov.のFAQs項目を参照してください。

Consilio

法務関連のコンサルティングとサービスの世界的リーダー

jp.consilio.com

Consilio
jp.consilio.com

ConsilioはeDiscovery、ドキュメントレビュー、リスク管理、法務コンサルティングサービスを提供します。当社は法律および規制業界の専門知識や専用のツールを扱う多国籍の法律事務所と企業をサポートします。Consilioの一連のComplete Securityには資格を持ったセキュリティのエキスパートチームが含まれ、認定されたベストプラクティスを実践します。

規制 ConsilioはISO\IEC 27001:2013標準規格で認定されており、その最も厳格な要件を満たして機密データを適切に取り扱います。Consilioのすべてのコロケーションデータセンターは ISO 27001あるいはSOC 2 Type 2の認定を受けています。ConsilioはITAR規制、EU-米国間およびスイス-米国間のプライバシーシールド原則（米国では引き続き適用）、EU一般データ保護規則 (GDPR)、カリフォルニア州消費者プライバシー法 (CCPA)、その他多数の世界中のデータプライバシーの規則に準拠します。Consilioは現在2021年のHITRUST認定の取得手続き中であり、当社のHITRUSTベンダーとのギャップ評価フェーズを完了しています。

情報セキュリティプログラムおよびポリシー 当社のISO 27001認定で求められる通り、Consilioは世界中の拠点における当社のセキュリティに対する態勢を標準化する包括的なセキュリティポリシーおよび手順を維持します。企業の情報セキュリティポリシーおよび手順は経営陣によって適切に精査され、Consilioの従業員に与えられています。ポリシーおよび手順はConsilio Information Security Governance Council (ISGC) によって承認された上で、すべての従業員に通知されており、毎年レビューされます。当社のポリシーにより、Consilioは保有するすべてのデータが現地のデータ保護規則に準拠して取り扱われ、世界各地にある当社の拠点によって異なる法的および契約上の要件に基づいています。これらの要件に準拠しているか否かはISO監査人を含む社内外の担当者によって定期的に監視および監査されます。

当社の認定においては、当社のポリシーがリスク管理、インシデント管理、ベンダー管理、災害復旧および事業継続性、ネットワークセキュリティ、アクセス制御、人事セキュリティ、資産管理、変更管理やその他を含む当社が保有するデータの保護に関連したすべてのセキュリティエリアに対応することが求められています。

情報セキュリティの構造 Consilioの情報セキュリティ部長が引率する高いレベルの認定を受けた当社の情報セキュリティチームが、情報セキュリティに関する組織のすべての活動を管理します。この情報セキュリティチーム内には、セキュリティオペレーション、コンプライアンス、リスク専門の個別のチームがあります。さらに、高度なセキュリティ機能のため、当社は第三者に管理されたセキュリティプロバイダーを用い、EU圏に拠点を置く担当者によってEU関連の法律およびコンプライアンスの懸念に対しての専門知識を補完するようしています。また、Consilioのさまざまな事業部の幹部からなるConsilio ISGCが情報セキュリティに対するイニシアチブの監督およびサポートを行っています。ISGC半年ごとに召集され、Consilioの情報セキュリティに対する態勢のレビューと監査を行います。

ベンダーリスク管理 リスク管理はConsilioによるセキュリティへの包括的アプローチの一部です。Consilioのベンダー管理プログラムの一環として、当社のすべてのベンダーは、Consilioまたは当社のクライアントに対し不必要なセキュリティのリスクをもたらすことのないよう、必ず詳細に調査されます。Consilioの災害復旧および事業継続性のプログラムの監査は定期的に決められたスケジュールで実施されます。内部監査はConsilioのグローバル情報セキュリティチームによって実施されます。データのバックアップは継続的に更新され、当社の第1データセンターから物理的に離れた建物内にある第2データセンターで保管されます。

ネットワークセキュリティ Consilioのコンピューティングネットワークは DMZおよび複数のファイアウォールと伴って設定され、インターネット接続が可能なネットワークセグメントを機密データ保管セグメントから分離します。当社のネットワークは厳重なファイアウォール、第三者による監視サービス、侵入者検知および予防ソフトウェア、アンチウィルスソフトウェア、厳しいアクセス制御ポリシーによって保護されています。ユーザー許可手順は最小権限の原則に従うもので、各ネットワークセグメントへのアクセスは適切な権限によって正式に承認されなければなりません。ITインフラストラクチャーへの変更は正式な変更管理手順に従います。ソフトウェアは定期的かつ適切なタイミングでパッチ処理され、実装前の正式なレビューおよび承認の対象となります。

データ保管 すべてのクライアントデータはConsilioの企業データからは物理的かつ論理的に分離され、クライアントデータはクライアントおよびプロジェクトごとに分けられます。データはクライアント契約上同意された期間保管され、プロジェクト完了時にはConsilioは正式なデータ破棄ポリシーに準じます。データを破棄する前にクライアントは正式なデータ破棄または移動フォームに署名する必要があります。そしてConsilioはデータが破棄された後にデータ破棄証明を発行します。

資産管理 すべての設備はConsilioの資産管理ポリシーを通して追跡および管理されます。一連の管理文書化および保管はクライアントの設備とメディアのすべてについて追跡されます。クライアントのメディアは安全で施錠された場所に保管され、認証されたデータ管理スタッフのみによりアクセスされます。

認定およびコンプライアンス

ConsilioはISO\IEC 27001:2013標準規格で認定されており、その最も厳格な要件を満たして機密データを適切に取り扱います。Consilioのすべてのコロケーションデータセンターは ISO 27001あるいはSOC 2 Type 2の認定を受けています。ConsilioはITAR規制、EU-米国間およびスイス-米国間のプライバシーシールド原則* (米国では引き続き適用) 、EU一般データ保護規則 (GDPR)、カリフォルニア州消費者プライバシー法 (CCPA)、その他多数の世界中のデータプライバシーの規則に準拠します。Consilioは現在HITRUST認定の取得手続き中であり、当社のHITRUSTベンダーとのギャップ評価フェーズを完了しています。HITRUST認定は2021年に完了予定です。

*注：EU-米国間のプライバシーシールドのフレームワークはEU司法裁判所により無効とされましたが、Consilioは引き続きこのフレームワークが施行された時のすべてのプライバシー関連の契約要件を敬意をもって継続します。プライバシーシールドに代わって適用される新しい規則が作られた場合は、Consilioは適用されるすべての法律に準拠します。

プライバシー

Consilioのプライバシーポリシーおよび実践はデータセキュリティの国際的なベストプラクティスに準拠し、多くの場合それを上回るものです。当社の企業プライバシー構造およびポリシーは各プロジェクトおよびデータのある場所に基づき、国際的かつ局所的なプライバシー規則の要件を確実に満たしています。これらには、GDPR、HIPAA、ITAR、CCPAおよびその他の類似規則などが含まれます。

当社のプライバシー標準規格の実行は認可されたデータプライバシー担当者によって監視されます。Consilioの情報分類ポリシーは確実にすべてのデータがその機密性に基づき適切に保護されます。クライアントデータへのアクセス制限はクライアントの依頼に基づくか、現地の規則およびクライアントとの契約要件の順守のために設けられます。

物理的なセキュリティ

Consilioのコロケーションデータセンターはデータセンターの場所によってISO 27001:2013標準規格に認定されているか、あるいはSOC 2 Type 2保証監査を完了しています。Consilioは世界中さまざまな拠点にコロケーションデータセンターを持ち、その法域における当社のクライアントのデータセキュリティ要件に取り組みます。Consilioは、コロケーションデータセンター運用ベンダーとの厳密な契約と機密保守文書の内容を遂行し、当社のデータと設備のセキュリティおよび機密性を確実にします。

データセンター内では、厳重な物理的および論理的セキュリティ制御が運用されており、Consilioの資産がデータセンター内のその他の資産から適切に分離され、かつ当社の各クライアントの資産がそれぞれ分離されるようにします。Consilioサーバーはコロケーション施設内の専用のConsilio IT装置内で物理的に隔離されています。Consilio ITチームの認可された従業員のみがそのサーバーエリアに物理的にアクセスすることができます。すべてのConsilioデータセンターサーバー室へのすべての出入りはログ管理され、追跡することができます。ビデオカメラが建物内とその周辺での物理的な動きを継続的に記録しているため、複数地点での監視映像を入手することができます。

コロケーションデータセンター施設での物理的なセキュリティ対策に含まれるもの

- フェンスや入口ゲートを含む周辺のセキュリティ
- 年中無休のセキュリティガード
- PINコードと生体認証スキャンによって保護された施錠機能を備えた施設および機械室へのアクセス制御付きドア
- データセンター内のConsilio IT設備のための分離ラックスペースおよび施錠ケージ
- CCTV監視および映像のバックアップ保管
- 訪問者管理プロセス
  - データセンターへの未認可スタッフの立ち入りを禁止する。
  - 訪問者は事前承認を受け、データセンターに立入る際には認可されたスタッフが同行する。
- UPS、HVAC、防火、バックアップ作成などの環境的な管理を行う。

データセキュリティ

クライアントデータの取り扱いのためのConsilioのポリシーは、Consilioが保有する間、データおよびデバイスを安全に保管し、認可されていないアクセスから保護します。クライアントデータは、含まれるデータが個人情報 (PII) や保護医療情報 (PHI) か、または単なる私的情報かどうかに関わらず、すべて機密データとして取り扱われます。

物理的および論理的なセキュリティ管理には厳重な認証管理、強力なパスワード、データ分離、クライアントデータの他の組織データからの隔離、最小権限の原則に基づいた役割ベースアクセスが含まれます。クライアントのプロジェクトデータへのアクセス付与のための社内手順は、Consilio独特のクライアントとのビジネスエンゲージメントの性質、クライアントの契約上の要件、現地規約の順守、特定の状況におけるセキュリティ考慮に基づいています。クライアントデータへのアクセスは正式な認可を受け、かつ職務を実行するためにアクセスが必要な者にのみ付与されます。クライアントには自身のデータやプロジェクトへのアクセス付与について完全な決定権があります。

セキュアなデータの取り扱いポリシーは、データがクライアントに返却されるか破棄されるまで有効なデータ管理認証を維持することを含め、eDiscoveryプロジェクトのライフサイクル全体において施行されます。プロジェクトは、Consilioによるデータの収集、データ取込みの実施、当社の専用のシステムでの処理、Consilio管理またはクライアント管理でのセキュアなデバイスを使ったドキュメントレビューの実施から開始されます。プロジェクトの完了時には、クライアントはConsilioにデータを返却してもらうか、データ (物理的メディアも含む) を破棄して破棄の認証を受けるかを選択することができます。技術上、運用上、管理上の制御はデータの全ライフサイクルを通してデータセキュリティの要件に準拠するようにします。

Consilioはクライアントデータを混合しません。当社は、特定のクライアントおよびプロジェクト専用の仮想サーバーを当社のセキュアなテクノロジーインフラストラクチャー内に作成します。当社は、クライアント契約内で特定されている期間のみクライアントのデータを保管し、その後、クライアントの指示に基づきデータを破棄または返却します。

ネットワークセキュリティ

インターネット接続可能なすべてのシステムはセキュアなファイアウォールで保護されたDMZネットワーク内に配置されています。すべてのクライアントデータは第2の同様のファイアウォールで保護されたセキュアなネットワーク内に保管されます。この2つのファイアウォールは両方とも最小限のアクセスだけを許可するよう構成されています。このセキュアなネットワークへはインターネットからの直接のトラフィックは許可されません。これらのネットワーク間での通信は256ビットSSL暗号を使用して暗号化され、いかなるデータ (ログイン認証データも含む) も公共のネットワークを介してプレーンテキスト形式で受信されないことを保証します。

Consilioのネットワークセキュリティ制御は次の通りです。

1. インターネット接続されたすべての地点は完全な冗長構成でデプロイされたファイアウォール、侵入者検知システムおよび侵入者予防システム (IDS/IPS) インフラストラクチャー、セキュリティ情報およびイベント管理 (SIEM) ソフトウェアで保護されます。Consilioネットワークに出入りするすべてのトラフィックは管理されたセキュアなエントリポイントを通って横断しなければなりません。

2. BGP、MPLS、IPSecネットワークセキュリティプロトコルによって、ネットワークトラフィックはConsilioネットワーク、サーバー、エンドユーザーセグメント内を安全に横断することができます。Consilioにはネットワーキング用に分離したシステムおよびウェブまたはウェブサービス、データベース、ストレージアクティビティ用のサーバークラスの設備があります。

3. 強力な認証管理 (強力なパスワード、多要素認証、データセグメント化、役割ベースアクセスなど) をConsilioネットワーク環境内で施行することによって、クライアントデータへの適切なアクセス制御を確実にします。Active Directory LDAPサーバーに対しては社内認証が実行されます。

    1. 一意のユーザーIDおよび強力なパスワードがすべてのユーザーに求められます。

    2. Consilioはサードパーティのツールを使用してActive Directoryアカウント用のパスワードポリシーに確実に準拠します。すべてのベンダーのデフォルトパスワードおよびアカウントは最初に使用する際に変更または削除する必要があります。

4. ConsilioはAES、3DES、RSA、IDEA、などの標準的な暗号アルゴリズムを使用して、保管中のデータ (AES-XTS 256ビット認定暗号) および移動中のデータ (TLS 1.2および1.3のみ、128ビット/対称暗号アルゴリズムには256ビット暗号) を保護します。一続きの暗号はMozillaの中間相換性標準規格ごとに構成されます。

5. すべてのConsilioシステムをConsilioのベースライン強化ポリシーに準じて強化することによって、未使用のポートはロックされ、接続ストリングが既知のサーバーおよびサービスでのみ確立されるようにします。
6. すべてのConsilioサーバーおよびワークステーションには承認されたアンチウイルスおよびアンチマルウェアソフトウェアがインストールされています。最新のエンドポイント脅威検知ソフトウェアおよびモバイルデバイス管理ソリューションがすべてのConsilioエンドポイントに実装されています。
7. 情報技術に関するあらゆる変更やアプリケーションの開発は制作環境に実装される前に適切にレビューおよび承認されます。
8. アプリケーションおよびネットワークの脆弱性評価およびペネトレーションテストが定期的に実施されます。社内外の脆弱性スキャンおよびペネトレーションテストが信頼できる第三者のチームによって半年ごとに実施され、社内チームによってもより頻繁に実施されます。
9. Consilioによるソフトウェア開発のライフサイクルにはセキュアな開発フレームワークが含まれます。開発、テスト、制作環境は当社のシステムおよびデータのセキュリティと統合性を確実にするために分離されます。

ドキュメントレビュー

Consilioは当社のセキュアな仮想レビュー (SVR) プラットフォームを通してセキュアなドキュメントレビューサービスをオンサイトおよびリモートで提供します。Consilioのドキュメントレビュープロジェクト（オンサイト、リモートに関わらず）のすべてのユーザーは厳戒なセキュリティ制御付きの独自のネットワーク構成内で分離されたConsilioのセキュアな仮想環境へのアクセスを認証される必要があります。

- ドキュメントレビューシステムは分離されたVLAN環境内に配置されています。
- レビュー施設はドキュメントレビュープロジェクトのセットアップ用に特別に必要とされるソフトウェアユーティリティのみを許可するように構成された、ロックされたセキュアなシンクライアントシステムで提供されます。
- Consilioのセキュアなドキュメントレビューシステムはウェブコンテンツ、印刷、Eメール機能をクライアントのプロジェクト仕様に準じて制限します。
- ConsilioのセキュアなドキュメントレビューシステムではWi-Fi、インスタントメッセージツール、取り外し可能なメディアドライブ、プリンターアクセスの使用はプロジェクトクライアントによって特別に依頼されるか、またはセキュアな仮想レビューのためでない限り、許可されません。
- ユーザーベースのグループアクセスポリシーはドキュメントレビューアーのアカウントに適用され、承認されたドキュメントレビューシステムにのみアクセスするように制限されています。
- 役割ベースのアクセス制御ポリシーはドキュメントレビューアーに適用され、クライアントが要請する場合は多要素認証も含まれます。

スタッフ

すべてのConsilioの社員および契約社員は雇用される前にバックグラウンドスクリーニングを完了する必要があります。Consilioの従業員には次のことが求められます。

- 従業員の雇用期間中の秘密保守および機密情報同意書に署名をする。
- 雇用期間中は情報セキュリティ認識トレーニングを毎年完了する。
- Consilioのセキュリティポリシーに準ずることに同意する。
- 職務に関連したトレーニングを維持する。
- 役職についての•e認定を受け、適用される教育認定を雇用期間中維持する。

Consilio
jp.consilio.com

ベンダーリスク管理

Consilioのベンダーリスク管理評価ポリシーは、Consilioのベンダーおよび第三者のサプライヤーが Consilioのための業務を開始する前に適切に調査および承認され、Consilioによるセキュリティ監査を定期的に受けることを求めています。Consilioとベンダーとの契約上の同意には、Consilioとクライアントの情報を保護する機密情報の条項が含まれます。Consilioはベンダーのリスク評価を少なくとも年に1回実施します。

また、明らかになりつつあるサプライチェーンの脆弱性に対応するためにConsilioはベンダーを監視し、新しい問題が特定された場合はベンダーとのフォローアップを行います。

インシデント管理

Consilioのインシデント管理ポリシーにおいて、当社は積極的に対策を講じ、セキュリティインシデントの予防および報告、その影響の緩和を確実に行います。Consilioはクライアント契約で求められている期間内で発生したクライアントデータに関わるすべてのインシデントを公開します。Consilioのインシデント応対手順は経営陣、クライアント、該当する場合は外部規制機関へのエスカレーションと報告のプロセスを含む社内エスカレーションプロトコルにも対応しています。

Consilioのインシデント応対チームは緊急事態時に迅速なアクションを取ることができる年中無休のセキュリティ運用ベンダーによって補強されています。ベンダーは潜在的なインシデントが示唆された際に問題のあるエンドポイントまたはユーザーを迅速に隔離し、危険にさらされている可能性のあるエンドポイントからそのインデントの影響がさらに拡散していかないようにします。

災害復旧および事業持続性

Consilioの災害復旧および事業持続性のポリシーにおいては、Consilioが当社のデータセンターまたはオフィスでビジネスオペレーションに障害が起こる可能性のある災害シナリオを用意することが求められています。自然災害、パンデミックシナリオ、ユーティリティの断絶、人員不足、人員やビジネスリソースに影響を起こす可能性のあるその他の出来事などに対応するための計画です。

Consilioの災害復旧プランは当社の初期対応および災害後の評価から、当社スタッフおよびクライアントの移動手段および連絡手段、サービスの復旧、適切な機能の検証、事業の再開、中間オペレーション、通常業務への復帰のステップに及びます。Consilioの災害復旧および事業継続性計画は、リスク管理、法的および規則的要件、災害後にどのようにクライアントへのサービスを再開するかについて検討しています。

文書化されたConsilioの復旧時間の目標はIT資産やアプリケーションによって異なります。特定のアプリケーション、データ、プロジェクトのための具体的な復旧時間の目標は、各プロジェクトのConsilioのクライアントサービス担当から入手できます。復旧時間の目標はすべての資産とアプリケーション用に文書化および追跡され、Consilio年次の災害復旧および事業継続性テストによって試されます。

データのバックアップ

Consilioのデータバックアップポリシーでは、当社がデータの複製、日次の増分バックアップ、週次のクリティカルデータのフルバックアップを実行することが求められています。Consilioの第1および第2データセンター施設は40㎞離れて位置し、ひとつのデータセンターで起こった災害がもう一方のデータセンターを機能不全にしないようにしています。

詳細のお問い合わせ先
jp.consilio.comをご覧いただくか、Eメール(info@consilio.com)でお問い合わせください。