Acronis

ホワイトペーパー

3 省 2 ガイドライン (2G3M)

目次

はじめに

2003 年以来、Acronis は業界をリードするバックアップおよびディザスタリカバリソリューションをあらゆる規模のビジネスに提供している。今日、極めて高いデータ機密性と堅牢なセキュリティ要件を抱え、データ損失やダウンタイムを容認しない数多くの政府機関、金融機関などの組織が、世界中でビジネス上の重要なシステムとデータを保護するために Acronis に信頼を寄せている。

Acronis は、重要なデータ保護ソリューションの設計と実行において、他社を圧倒する経験を有している。Acronis クラウド データセンターは、あらゆる規模のビジネスセクタのために、高度なエンタープライズクラスのセキュリティ、プライバシー、およびコンプライアンスを提供する。このホワイトペーパーでは、Acronis による義務の履行、ならびにカスタマーが Acronis Cyber Protect Cloud を使用し、日本政府の要件に従って医療情報を取り扱う義務を遵守する方法について説明する。

日本国内において、個人を特定できる医療情報（医療 PII）を処理および/または保管するシステムは、2 つの主要なガイドラインに従う必要がある。

- 医療情報システムの安全性管理に関するガイドライン[1]
- 医療情報を取り扱う情報システム・サービスプロバイダーにおける安全性管理ガイドライン[2]

これらのガイドラインは、一般的に「3 省 2 庁ガイドライン（2G3M）」として知られる。Acronis は、カスタマーが 2G3M の義務を満たすためのサポートに注力する。システム構築のための安全な基盤を提供し、システムセキュリティを強化するツールを提供するとともに、これらのツールの有用性を最大限に引き出すための教育リソースをカスタマーに対し提供している。

日本国内における 2G3M 基準への準拠は、主に医療機関の自主規制によって推進されているが、重大な違反があった場合には行政処分が科されることもある。

本ホワイトペーパーは情報提供のみを目的とする。これは法的助言を提供するものではなく、2G3M またはその他の規制に関する特定の懸念事項については、専門家の法的指導を仰ぐことが推奨される。

要求事項

適用範囲

医療情報システムの安全性管理に関するガイドラインは、病院、診療所、助産院、薬局、訪問看護ステーション、介護事業所、医療情報ネットワークなど、幅広い事業者を対象としている。医療個人情報（PII）を取り扱うシステムのユーザに対するコンプライアンス要件を明確にし、日本の医療セクターにおける規制コンプライアンスの基盤としての役割を果たす。

医療情報を取り扱う情報システムサービスプロバイダーにおける安全性管理ガイドラインには、デジタル化された医療個人識別情報を取り扱うシステムおよびサービスを提供する事業者に対する特定のコンプライアンス要件が定められている。このようなインフラストラクチャに統合された場合、これは、Acronis Cloud などのクラウドベースのサービスを含む、ヘルスケア設定で使用されるシステムとサービスの安全な設計、実装、運用を保証するためのフレームワークとして機能する。

[1]医療情報システムの安全性管理に関するガイドライン（第 6.0 版 2023 年版）
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

[2]情報システム・サービスプロバイダーにおける安全性管理ガイドライン（第 1.1 版、2023 年発行）
https://www.soumu.go.jp/main_content/000891033.pdf

リスク管理戦略

医療情報を取り扱う情報システム・サービスプロバイダーにおける安全性管理ガイドラインにおいて、サービスプロバイダーはリスク管理とリスクコミュニケーションの両方への取り組みが義務付けられている。

リスク管理に関しては、ガイドラインでは、サービスプロバイダーが情報の流れを明確にし、リスクを特定して評価し、適切なリスク管理対策を実施することが要求される。Acronisでは利用者ごとに情報の流れが異なるため、各状況に対する対応を提示するのは困難である。このため、Acronis は「別紙 2 統合前ガイドラインにおける対策項目一覧と医療情報安全性管理ガイドライン第 6.0 版の対応表」に従って、互換性マトリクスを作成した。上記の別紙 2 で採用された番号付けと関連する「要求事項の内容」に加えて、Acronis による準拠の方法とAcronis が保有する ISO/IEC 27000 ファミリー認証との表が追加されている。

これらの要件を満たすために必要なリスク管理対策は、以下の 3 つの観点から設計されている。

❶ **人的および組織的**: これらの管理は、組織的安全性と人的安全性に関連するものである。

- **組織的安全性**: 安全性管理を監督するための組織体制を確立し、運用し、文書化することを含む。
- **人的安全性**: 人員が機密情報を守秘し、セキュリティ体制に関するトレーニングを受けることを保証する。

❷ **物理的**:この対策には、関連する施設へのアクセスを規制するための障壁やロックなどの物理アクセス制御の実装が含まれる。

❸ **技術的**:これには、認証、承認、およびアクセス制御を含むデジタルアクセス制御、およびログ記録、暗号化、データ漏洩防止、脆弱性管理、脅威検出などの追加の安全性対策が含まれる。

リスクコミュニケーションに関しては、提供事業者はリスク管理戦略を医療機関に開示することが義務付けられている。これには、医療機関がサービスを利用する際にリスクを軽減するために講じるべき手順を明確化することが含まる。

共有責任モデル

Acronis は、ベンダの選定を含む自社のクラウドインフラの安全性を確保する責任を負い、カスタマーは、自社の環境の安全性を保護する責任を負う。

共有データセンターとの共有

共同設置されたデータセンターの物理的な安全性は、各データセンターの施設と責任が共有される。

Acronis は、世界中にコロケーション型データセンターを複数運用するためのパートナーシップを確立している。これらの施設は、設備、電力、冷却に関する厳格な基準とコンプライアンス要件に適合している。この手法により、最適な条件と稼働を維持し、基幹のデータを保護する。Acronis はさらに、最も一般的な障害事象の発生率を低下または排除するために、データセンターに厳格な要件を設けている。Acronis は各契約期間中、第三者の安全性制御、サービス提供、契約条件の遵守の定期的な監視およびレビューを行う。

最終カスタマーとの共有

Acronis では以下のように 2 種類のデータを区別している。

- サービス提供（製品使用など）および Acronis のサービス管理に必要なデータ。これは、Acronis がサービスを提供するために、データ管理者として収集および処理するデータである。このようなデータには、アカウント名、Eメールとその他の連絡先情報、請求の詳細、およびサービスを通じて自動収集された一部の情報が含まれる場合があり、個人情報が含まれる可能性がある。詳細については、Acronis の個人情報保護方針を参照のこと。https://www.acronis.com/company/privacy/
- カスタマーのコンテンツデータカスタマーが Acronis のサービスを利用する際に Acronis がデータ処理者（復処理者）として処理する可能性があるデータ。この情報は、特定の製品（バックアップアーカイブ、ファイル、または仮想マシンなど）を利用する際に、カスタマーによって提供される。この種類のデータに関しては、カスタマーが Acronis を通じて保管する情報のカテゴリや内容を Acronis が管理することはない。

カスタマーは自身の法律、コンプライアンスおよび技術に関する義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。

組織的セキュリティ対策

要求事項：	Acronis
プライバシーマーク認証または ISMS 認証を取得していること。	• 情報セキュリティおよびコンプライアンスプログラム。 • 2G3M へのセキュリティ保証。
保管された情報を保管するために使用される情報機器またはデバイスが国内法の対象であることを確認すること。	• データ保護。 • インフラストラクチャとネットワークのセキュリティ。
機器と媒体の所在を定期的に確認すること。	• インフラストラクチャとネットワークのセキュリティ。 • データストレージ。 • アクセスコントロール。
医療機関との役割と責任を明確化すること。	• 共有責任モデル。 • 情報セキュリティおよびコンプライアンスプログラム。 • データ保護。
医療情報内のアクセスおよび操作活動を監視すること。	• インフラストラクチャとネットワークのセキュリティ。 • 人的セキュリティ。 • アクセスコントロール。
個人を特定できる情報（PII）の安全な処理と取り扱い。	• データ保護。 • 情報セキュリティおよびコンプライアンスプログラム。 • アクセスコントロール。
内部監査の実施。	• 情報セキュリティおよびコンプライアンスプログラム。 • 2G3M へのセキュリティ保証。
ICT サプライチェーンのセキュリティ管理。	• サプライヤー関係管理。 • アプリケーションセキュリティ。 • データ保護。 • インシデント管理。
事業継続計画の作成。	• 事業継続およびディザスタリカバリ。 • インシデント管理。
サイバー攻撃によるインシデントへの対応、医療機関への報告。	• インシデント管理。 • 人的セキュリティ。 • 事業継続およびディザスタリカバリ。 • インフラストラクチャとネットワークのセキュリティ。
機器およびソフトウェアの品質管理。	• アプリケーションセキュリティ。 • インシデント管理。
変更に伴う医療機関への影響を最小限に抑えること。	• インフラストラクチャとネットワークのセキュリティ。 • アプリケーションセキュリティ。 • アクセスコントロール。

人的セキュリティ対策

要求事項：	Acronis
すべての人員との間で機密保持契約を締結する。	• 人的セキュリティ。 • サプライヤー関係管理。
医療情報システムおよび類似のサービスの提供に関連する教育および訓練の実施。	• 人的セキュリティ。 • インシデント管理。
セキュリティ対策を導入し、従業員および下請け業者を監督する。	• サプライヤー関係管理。 • 人的セキュリティ。

物理的セキュリティ

要求事項：	Acronis
アクセス制御管理。	• アクセスコントロール。 • インフラストラクチャとネットワークのセキュリティ。 • 情報セキュリティおよびコンプライアンスプログラム
機器の盗難対策。	• インフラストラクチャとネットワークのセキュリティ。 • アクセスコントロール。
地震、洪水、落雷、火災、および付随する停電への対策。	• サプライヤー関係管理。 • 人的セキュリティ。
媒体の安全な処分。	• データストレージ。 • インフラストラクチャとネットワークのセキュリティ。

技術的なセキュリティ対策

要求事項：	Acronis
ユーザ認証の実装。	• アクセスコントロール。 • インフラストラクチャとネットワークのセキュリティ。
アクセス権の管理。	• アクセスコントロール。
ログの取得と検証。	• インシデント管理。 • アクセスコントロール。 • アプリケーションセキュリティ。 • エンドポイントセキュリティ。
悪意のあるプログラムへの対策。	• エンドポイントセキュリティ。 • インシデント管理。
端末とサーバの強化およびアップデート。	• エンドポイントセキュリティ。 • インフラストラクチャとネットワークのセキュリティ。 • アプリケーションセキュリティ。
脆弱性管理。	• アプリケーションセキュリティ。 • 情報セキュリティおよびコンプライアンスプログラム
ネットワークのアクセス制御。	• インフラストラクチャとネットワークのセキュリティ。 • アクセスコントロール。
登録されていない電子媒体接続の制限。	• エンドポイントセキュリティ。
暗号化および電子署名の使用。	• インフラストラクチャとネットワークのセキュリティ。 • データストレージ。 • アクセスコントロール。
バックアップと復元の管理。	• エンドポイントセキュリティ。

Acronis Cyber Protect Cloud のセキュリティ

アクロニスは継続的なリスク評価に基づいた物理的環境、技術の管理のための包括的な情報セキュリティとコンプライアンスプログラムを提供します。Acronis の情報セキュリティポリシーおよびプロセスは、ISO/IEC 27000 シリーズや米国国立標準技術研究所（NIST）などの一般に受け入れられている国際セキュリティ標準に基づいており、また、関連する地域の規制フレームワーク（日本の個人情報保護法（APPI）や欧州連合の一般データ保護規則（GDPR）など）の要求事項を考慮している。

情報セキュリティおよびコンプライアンスプログラム

当社は、情報セキュリティをプロセス、ツールおよびポリシーを管理するための一連の体系的な戦略としてではなく、個々の果たす役割が重要であり、情報が主要な役割を担う複数のプレイヤーによる継続的なプロセスとして捉える。

Acronis の情報セキュリティ管理システム（ISMS）は、業界標準となっている情報セキュリティの ISO/IEC 27001 フレームワークに従い、独立した第三者監査人によって認証されている。従来のシステムに加えて、クラウドにおけるセキュリティ要件に対応するために、クラウドセキュリティの実践に関する ISO/IEC 27017 と、クラウドにおける個人を特定できる情報（PII）のセキュリティを保証するために ISO/IEC 27018 を取得し、ISMS の拡充と認証を行った。

さらにセキュリティ慣行に関するさらなる保証を提供するために、Acronisはサービス組織向けの システムおよび組織管理2(SOC 2®) 報告書の取得を追求している。この規格は、カスタマーのデータを管理する組織に対してトラストサービス基準および要求事項を適用する。

また、日本の個人情報保護法（APPI）、EU 一般データ保護規則（GDPR）、米国の医療保険の相互運性と責任に関する法律（HIPAA）、フランスの健康データホスティング（HDS）など、ローカルのプライバシーおよびデータ保護規制に関連するカスタマーの要件にも対応している。

Acronis は、企業レベルのセキュリティをカスタマーに保証するために、オンプレミスおよびクラウド情報セキュリティソリューションの他社製品と比較して、膨大なリソースを投入している。Acronisは継続的に 一貫性のあるサービスを確保し、適切な水準のセキュリティを維持するべく、資産のトラッキング、資産のプロファイリング、アクセス制御、脆弱性管理を継続的に改善している。Acronis は、一般に認められた情報セキュリティ規格とベストプラクティスに対するコンプライアンスを積極的に追求している。当社の情報セキュリ

ティ対策はすべて、Acronis のビジネス継続性管理プログラムと統合され、調整されており、これにより、セキュリティに対する脅威、自然災害、人的災害を最小限に抑えている。

情報セキュリティおよびコンプライアンスプログラムの適切な導入を確保するため、Acronis は、情報セキュリティおよびデータ処理に関する確立された要求事項に対するコンプライアンスを確認するため、内部および外部監査を継続的に実施および監視している。これにより、Acronis は、プログラム実施の程度を適切に測定し、新しい情報セキュリティリスクの発生を検出し、対応することが可能となる。

2G3M へのセキュリティ保証

2G3M に準拠する必要がある Acronis のカスタマーにとって最も関連性の高い第三者認証は以下のものである。

ISO/IEC 27001 シリーズ 情報セキュリティ管理システム（ISMS）の確立、実装、維持、および継続的改善の要求事項を定める、国際的に認められた規格。このソリューションは、情報セキュリティリスクの特定、評価、管理を体系的に実行することで、組織がデータを保護し、潜在的なセキュリティ脅威に対して保護するのに役立てることができる。リスクベースのアプローチの重要性を強調し、組織に対して、情報セキュリティコントロールを特定のビジネスニーズとリスクプロファイルに合わせて調整するよう要求する。

Acronis の ISO/IEC 27001 への準拠は、情報セキュリティのベストプラクティスに対する当社のコミットメントを示し、カスタマーから信頼と信用を得るうえで重要である。これにより、機密データの管理とセキュリティリスクの軽減を行うための構造化されたフレームワークが提供され、業界における企業の信頼性と評判が向上する。この規格に準拠することで、Acronis はカスタマー情報の機密性、整合性、可用性を確保し、信頼性と信頼に基づく長期的な関係を構築することができる。さらに、ISO/IEC 27001 への準拠により、Acronis は進化するサイバーセキュリティの脅威に先んじて対応し、新たな課題に対して継続的な改善と適応性を確保することができる。

ISO/IEC 27017 シリーズ は、クラウドサービス提供事業者に特に適した有益なガイダンスを提供し、効果的なクラウドセキュリティ対策を実装するためのフレームワークを提供する。この規格に準拠することで、Acronis はクラウドベースのデータとサービスの保護に対する取り組みを示し、クラウドソリューションを信頼するカスタマーに信用を与えることにつながる。

ISO/IEC 27018 シリーズ は、Acronis のようなクラウドサービス提供事業者に対して包括的なガイドラインを提供し、クラウド上で保管および処理される個人情報のプライバシーと保護を保証する。この規格を採用することで、Acronis は個人のプライバシー権利を保護し、関連するデータ保護規制を遵守することに対する取り組みを示している。

SOC 2 Type II 報告書は、クラウドサービス提供事業者のセキュリティ、可用性、処理の完全性、機密性、プライバシーに関連する内部統制を評価するために独立した監査人によって実施される包括的な評価である。通常 6〜12 ヵ月の指定期間にわたって、これらの統制が効果的に設計され、効率的に機能しているかどうかを検証する。

SOC 2 Type II 報告書を取得することで、Acronis は堅牢なセキュリティ慣行を維持し、カスタマーデータの可用性、完全性、機密性を確保することへの取り組みを示している。

インフラストラクチャとネットワークのセキュリティ

Acronis は、信頼性の高いデータセンター（米国、英国、フランス、ドイツ、日本、シンガポール、スイスおよびその他の複数のロケーション）において、データとクラウド製品をホストしている。詳細は、Web サイト (https://www.acronis.com/data-centers/)を参照のこと。

カスタマーは、データを保管する地域またはデータセンターを選択できる。このため、GDPR、APPI（2G3M によって要求される）、その他のプライバシーおよびデータ保護に関する現地の規制の場合と同様に、データ配置に関する地域の要件を満たすことができる。

データセンター提供事業者とデータセンターのロケーションを選択する際には、施設の機能、現在の脅威評価（建設、技術、環境、政治など）、特定の地域の相対的な魅力と事業要件を考慮し、提供事業者を全面的に評価している。

データセンタープロバイダーの信頼性を確認し、その情報のセキュリティ、可用性、機密性、および整合性を維持する能力を保証するため、当社のデータセンター提供事業者は、信頼できる独立組織によって定期的に監査を受けている。

Acronis はデータセンターに対して、物理アクセスの不正防止とカスタマーデータの安全性確保に最高水準の物理セキュリティ基準を採用するよう要求している。厳格なアクセス制御措置と監視カメラ（CCTV）による監視に基づいて、データセンターには許可された専任スタッフのみがアクセスできる。侵入者からの保護水準は、中小企業が単独で導入可能な水準をはるかに上回る。

データセンターの電力系統は、インフラストラクチャ全体に 24 時間年中無休で無停電電源装置を提供するように設計されている。データセンターは、少なくとも 2 つの独立した電源から給電されている。自動無停電電源装置の使用は、電力線を切り替える場合に発生する電力サージから保護し、ディーゼル発電機への切り替え中に電力サポートを提供する。

高可用で冗長化されたインフラストラクチャは、付随するリスクを最小限に抑え、単一障害点を排除するように設計されている。Acronisは、インフラストラクチャのすべてのハードウェア層で冗長性を高めるために、ニーズプラス1（N+1）のアプローチに従う。これによりハードウェア層のコンポーネントで障害が発生した場合でも、Acronis のカスタマーに影響することはない。

この冗長インフラストラクチャにより、Acronis はサービスの中断なしに、ほとんどの種類の予防・保守アクティビティを実行することができる。定期メンテナンスとインフラストラクチャの変更は、製造元の仕様および内部文書化された変更管理手順に従って実施される。すべての機器が保証対象であり、インフラストラクチャのすべての要素は各ベンダの SLA の対象である。すべてのベンダの保守契約は、専任チームによって管理され、年次改訂が行われる。チームは、インフラストラクチャの可用性を向上し、運用・保守コストを削減するために設計された標準化されたメンテナンスアプローチに従う。

Acronis は、新規または既存の脆弱性に関する最新情報を入手するために、すべての公式リポジトリおよび公式掲示板を監視している。セキュリティと重要なアップデートは最優先で迅速にインストールされる。アップデートは実装前に十分にテストされる。Acronis は、インフラストラクチャのあらゆるレベルで熟練した技術者や専門家を雇用し、問題の解決に向けて第三者のベンダと積極的に協力している。

Acronis は、すべてのコンポーネントと構成にセキュリティ上の問題がないことを確認するために、第三者によるセキュリティ監査を実施している。

Acronis は、重要なインフラを毎日スキャンし、すべてのネットワーク セキュリティコンポーネントの構成を定期的に確認している。

Acronis は、新しいサービスのセキュリティとこれらのサービスとのネットワークインタラクションのアーキテクチャについて、企業のネットワークに統合する前にレビューしている。

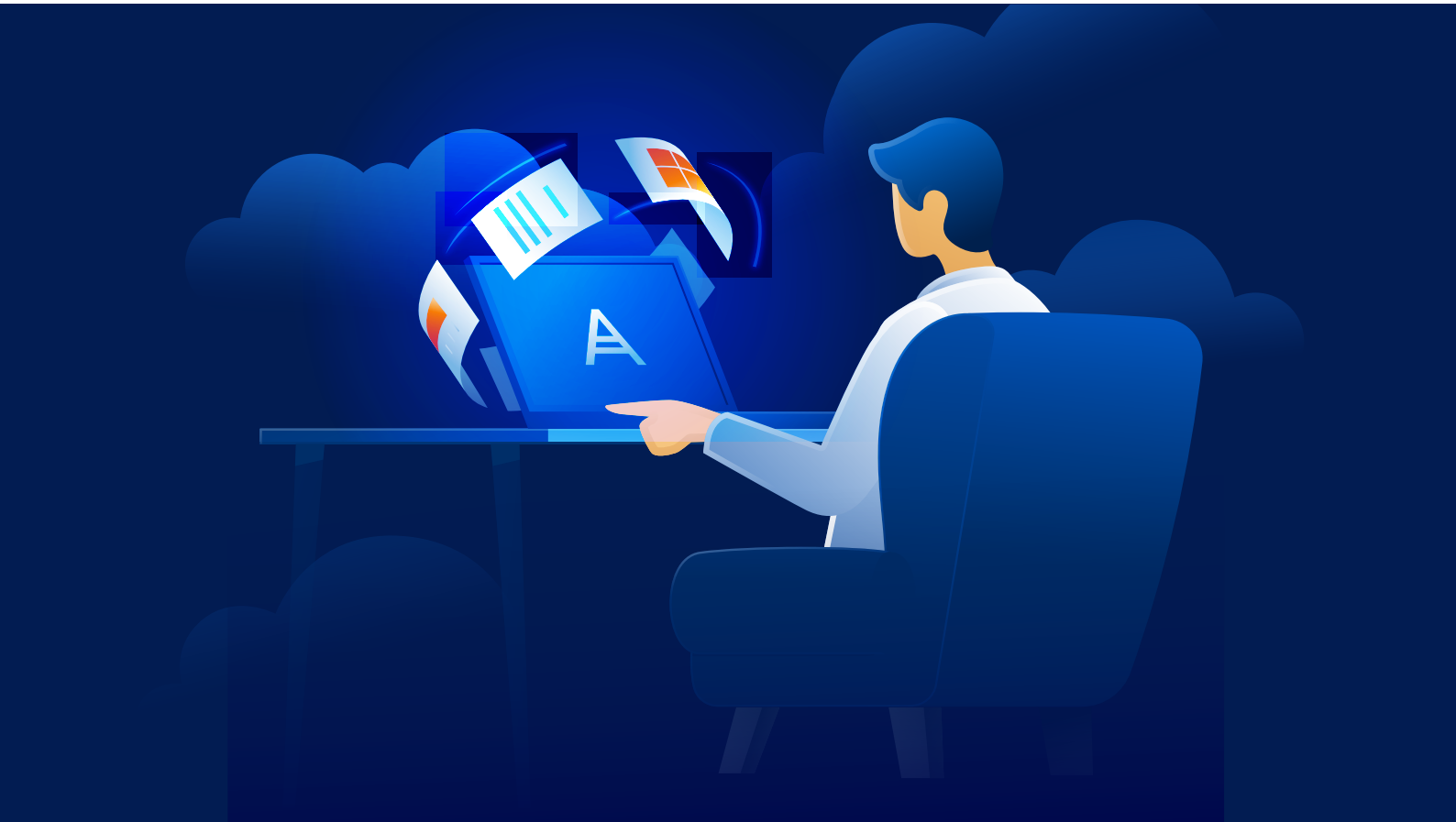
Acronis のネットワークは、多層構造かつゾーンベースである。管理対象のネットワーク機器は、内部、外部およびカスタマーの環境を分離・隔離し、ネットワークプロトコルおよびパケットのルーティングおよびフィルタリングを提供する。

Acronis は、転送されるすべてのデータをリアルタイムで暗号化する。Acronis は、HTTPS、TLS、SSH、OpenVPN などのセキュアなデータ転送プロトコルを使用し、強力な暗号化アルゴリズムを使用して、データの転送時に暗号化されたデータを保護する。また、Diffie-Hellman、RSA などの暗号鍵交換のセキュリティを提供し、転送されたデータへの不正アクセスおよび鍵情報の漏洩リスクを低減する。

Acronis は、持続的標的型攻撃(APTs)やサイバー攻撃から保護するために、IT インフラ全体のセキュリティを継続的に監視する。Acronis は、自己の境界、DMZ ネットワーク、VPN およびリモート接続、内部フローをコントロールおよび監視する。Acronis は、人的介入を防ぐために自動化ツールを組織的統制と組み合わせて使用している。

SQL インジェクション攻撃から保護するために、すべてのデータベースクエリのために専用のプリペアドステートメントライブラリを使用している。このアプローチにより、ユーザーの入力が安全にパラメータ化され、SQL コマンドの不正な操作を防止できる。また、カスタマー向けに構築されたクライアントサイドフレームワークには、クロスサイトスクリプティング（XSS）攻撃に対するビルトイン保護機能が備わっている。

このフレームワークは、安全でない文字を自動的に公開し、ユーザーのブラウザで実行される前に有害な可能性のあるスクリプトを無効化する。



当社は、ユーザーが閲覧権限を持つデータにのみアクセスできるようにするために、独自のテナントモデルに基づいて厳密にデータアクセス制御を実施する内部サーバー側コンポーネントを開発した。

このテナントモデルにより、各ユーザーのアクセスが割り当てられたスコープに厳密に制限され、それにより他のユーザーやテナントに属するデータへのアクセスを防止する。当社のシステム内のすべてのサーバー側コンポーネントは、この中央機関を呼び出して許可を解決するように求められるため、プラットフォーム全体で一貫したセキュリティが確保される。

データ保護

グローバルな事業展開をしている国際企業は、世界的なプライバシー保護の展開に合わせてさまざまなコンプライアンスへの準拠を求められる。Acronis は、適用される地域のデータ保護規制への準拠に尽力している。

個人情報保護法（APPI）は、プライバシー規制として日本において 20 年以上にわたって施行されており、Acronis は、日本の APPI の要件を含む適用されるデータ保護規制の遵守に努めている。当社ではデータ保護を念頭に置いて製品およびサービスを設計している。Acronis は情報を安全に保つために尽力しており、プライバシーの保護をより一層向上させるため、セキュリティ対策を定期的に監視し、アップデートしている。Acronis は、適用される義務を遵守するためのポリシーと手順を策定している。APPI の対象となる個人は、複数のプライバシー権利を有している。Acronis は、プライバシーに関する要求に対応し、適宜対処する。

Acronis のデータ処理に関する詳細情報については、よくあるご質問（FAQ）および Acronis のプライバシー保護方針を参照のこと。

データ ストレージのセキュリティ

Acronis Acronis Cyber Cloud 環境はマルチテナント環境であるため、クラウドサービスのアーキテクチャは、カスタマーのデータを物理的および論理的に分離し、規定の処理目的に応じて最小限のデータのみを処理するように設計されている。

アクロニスは、独自のソフトウェア定義ストレージソリューションである Acronis CloudRAID テクノロジー装備した Acronis Cyber Infrastructure を使用してカスタマーデータを保存する。Acronis Cyber Cloud Infrastructureは、高速、汎用、保護済み、効率的、実績のあるストレージを提供し、ブロック、ファイル、およびオブジェクト ワークロードを統合する。

AcronisCyber Infrastructureは、独自のイレージャコーディングアルゴリズムを使用して信頼性を高め、障害から保護する。スケーラブルで効率的な自己回復メカニズムを備え、データリスクを最小化する。さらに、Acronis Cyber Infrastructureは、すべてのカスタマーのデータ完全性を保護するために完全冗長アーキテクチャを利用している。

Acronis Cyber Cloudのすべてのデータは、Advanced Encryption Standard（AES）により 256 ビットのキーを使用して暗号化され保存される。

Acronis のデータセンターのストレージ容量は、過去数年で数百テラバイトから数十ペタバイトに向上した。また同時に、Acronis Storage の柔軟性とスケーラビリティにより、この急激な成長がカスタマーの重要なデータに影響を及ぼすことはない。

データの保存および/または処理が実行される Acronis Cyber Infrastructureドライブおよび装置は故障、修理のために交換、または廃止される可能性がある。この場合、Acronis は NIST SP 800- 88 に従ってディスクからデータを完全に消去し、機器の内部メモリから残留データを削除する措置を講じる。情報を消去（削除）できない場合、そのようなデータを読み取り、復元することができないように、機器を物理的に破壊する。

人的セキュリティ

データセキュリティを維持するには、人的対策が不可欠である。組織の最も重要な資産は従業員である一方で、Acronis は従業員に関連する主要なセキュリティ上の懸念を理解している。企業全体でセキュリティ文化を確立しない限り、どのようなシステムやインフラも完全に保護されることはない。

Acronis の全社員は、自己の職務機能と割り当てられたロールに適した情報セキュリティ、プライバシー保護、およびデータ処理に関する認識教育および訓練を受ける。

Acronis は、適用される現地の法律、法令、および倫理に従って、採用候補者の適切な身元確認チェックを実施し、人選に特別な注意を払っている。すべての Acronis の従業員は、Acronis の機密保持、ビジネス倫理、および行動規範ポリシーに従うことが求められるとともに、雇用契約終了後も有効な機密保持契約（NDA）に署名することが求められる。

エンドポイントセキュリティ

エンドポイントデバイスのセキュリティを確保することは、機密データを保護し、不正アクセスを防止し、マルウェアやデータ損失などのサイバー脅威から保護するうえで不可欠である。Acronis は、エンドポイントデバイスを保護するために独自のソリューションである Acronis Cyber Protect Cloud を使用して、以下の対策を講じている。

- 脅威インテリジェンスフィード、フォレンジックインサイト、パッチ管理、分析された攻撃のブロック、ポリシー管理を使用して、セキュリティ脆弱性を解消する。
- 自動化された振る舞い検知およびシグネチャベースのエンジン、URL フィルタリング、新たな脅威インテリジェンスフィード、イベント相関を使用して、セキュリティ関連イベントを継続的に監視する。
- ワークロードへのセキュアなリモート接続を使用したり、バックアップに自動保存されたフォレンジックデータを確認して不審なアクティビティを調査し、フォローアップ監査を実行する。

アクセスコントロール

Acronis は、職務に従って、情報リソースおよびデータへのアクセスを制限するために、企業向けゼロトラストアクセス制御ポリシーを導入している。

Acronisは、すべての職務において、職務分掌、知る必要性、最小権限の原則に準拠する。これにより、すべてのユーザがジョブを完了するために必要な最小限の権限を与えられ、すべての重要な業務が管理され、責任が追跡可能になる。データセンター環境には、最高レベルの許可を受けたスタッフのみがアクセスできる。

内部アクセス制御手順により、Acronis システムおよびデータへの不正アクセスを検出し、防止する。Acronis は、不正アクセスの可能性を最小限に抑えるために、アクセス時に、セキュリティ保護されたメカニズムと認証プロトコル（LDAP、Kerberos、SSH 証明書、802.1xなど）、ユーザ ID、強力なパスワード、多要素認証メカニズム、および制限付きの制御アクセスリストを使用した、集中管理型のゼロトラストアクセス制御システムを使用している。

さらに、すべてのアクセスはシステムの監査ログに記録され、変更を防止され、定期的に確認される。

論理アクセス制御と保存時暗号化に加え、Acronis は、カスタマーがデータを完全に管理できるよう、カスタマーのパスワードから生成されたキーに基づいてデータを暗号化する機能を提供する。

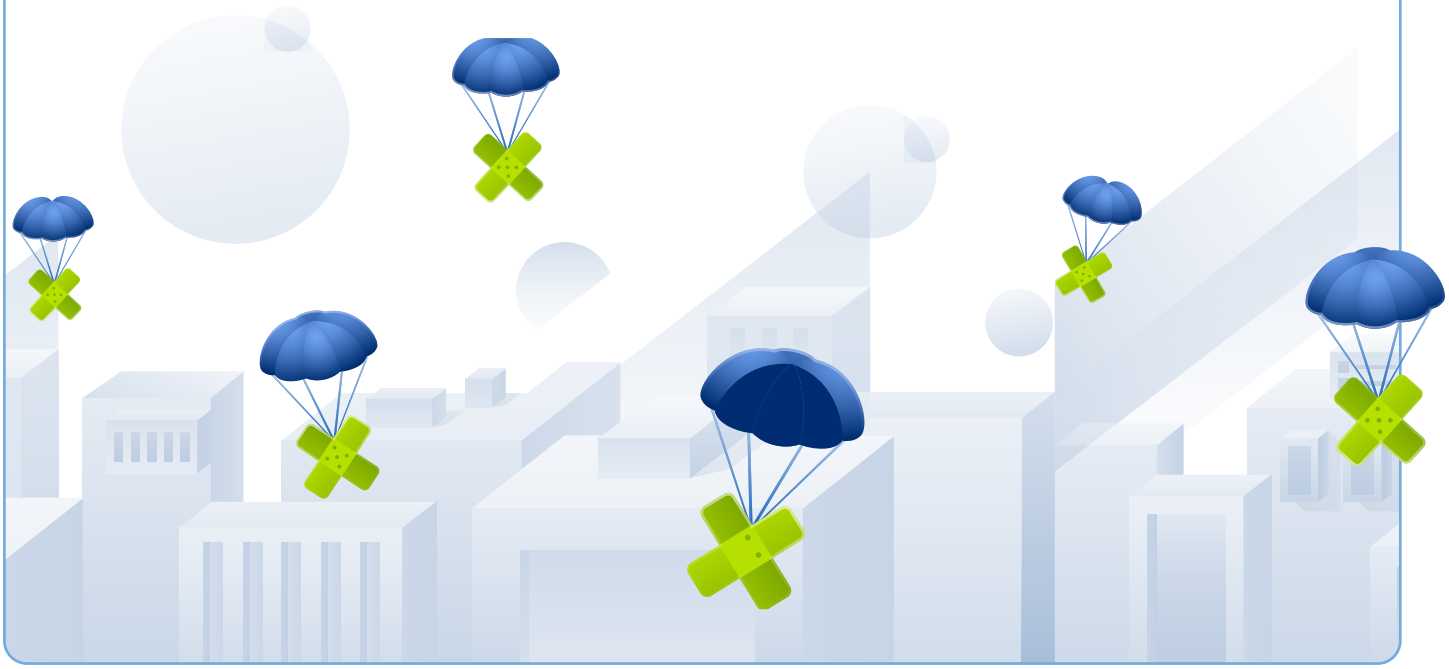
アプリケーションセキュリティ

Acronis は、最新バージョンのソフトウェアを使用し、オペレーティングシステム、ソフトウェア、フレームワーク、ライブラリを定期的にアップデートしている。Acronis のソフトウェア慣行によって、すべてのデータの機密性、完全性、可用性が保護される。

第三者のコンポーネント（オープンソースを含む）は、メインソフトウェアにリンクする前に、内部の Acronis リポジトリに複製される。すべてのコンポーネントは開発部門と情報セキュリティ部門によってレビューされ、開発プロセスでの使用の承認を受けている。また、ソフトウェア開発で使用するコンポーネントについて、企業の技術リーダーシップにも報告が与えられる。セキュリティチームは、使用中のコンポーネントに対して定期的にアップデートを監視し、脆弱性の修正が含まれているアップデートがあれば、レビューのうえ、内部リポジトリを更新する。

当社の標準的なソフトウェアセキュリティ慣行には、以下が含まれる。

- セキュアなソフトウェア開発ライフサイクルの各ステージでセキュリティを組み込むために、厳格なセキュリティポリシーと一般に知られたセキュリティのベストプラクティスに従う。
- アーキテクチャのセキュリティレビュー、機能および最終ソリューションの設計。情報セキュリティおよび品質保証チームをセキュリティレビューを実施する。これには、既知の脆弱性やオープンポートなどのアプリケーションのスキャンが含まれる。また、Acronisは、独立した第三者による外部レビューも実施している。
- 製品開発の方向性とガイダンスを提供するために、セキュリティの弱点、脆弱性、およびコード品質についてソースコードの定期的なレビュー（手動および静的コードアナライザーを使用）を実施する。開発中にソースコードが変更された場合、その特定のソフトウェアの専門家とエンジニア 2 名によるレビューが行われる。提出された変更はすべて、Acronis が使用するタスク管理システムのチケットにリンクされる。
- 開発者に迅速なフィードバックを提供するために、ソフトウェアの継続的なデリバリー（CI/CD）パイプラインの一部として、静的アプリケーションセキュリティテスト（SAST）ツールによるコード評価を実施する。この処理は自動化されており、すべてのアクティビティが Acronis 情報セキュリティチームの将来の監査のために記録される。
- 全チームに対してセキュリティ文化を構築および維持し、既知の脆弱性や現在の情報セキュリティ脅威に対する注意を継続させる。
- この取り組みをサポートするために、Acronis は 2018 年から HackerOne で脆弱性報告に対する報奨金制度を実行している。Acronis は、セキュリティコミュニティと緊密に連携し、製品の最適化に貢献する研究者を受け入れている。
- CVE® Programのパートナーであるアクロニスは、CVE Numbering Authority（CNA）で、開示されたサイバーセキュリティの脆弱性をすべてのアクロニス製品のCVEレコードとして公開する責任がある。セキュリティに関する勧告とアップデートに関する情報は、Acronis Security Advisory Database（アクロニスセキュリティアドバイザリーデータベース）を参照のこと。



インシデント管理

Acronis のセキュリティオペレーションチームとネットワークオペレーションセンター (NOC) がインシデントの特定と対応をリードし、問題の根本原因を特定し、適切な内部インシデント応当チームにそのインシデントのトリアージを依頼する。

インシデント応当チームは、セキュリティおよびコンプライアンス部門、データセンター運用部門、アーキテクチャおよび製品開発チーム、ならびに広報およびコミュニケーションチームの代表者を含む、精鋭グループで構成される。

すべての対応時間は、内部のService Level Agreement (SLA)目標 (99.9% の可用性) 、法的および契約上の義務によって決定される。

インシデントのタイプと深刻度に基づいて、Acronis は複数のエスカレーションパスを策定している。グローバルまたは重大レベルのインシデントは、Acronis の幹部によってエスカレーションおよび管理される。

Acronis のインシデント管理文化は、一般に認知されたベストプラクティスに基づいている。インシデントの処理には 7 つのステージが存在する。

準備: 適切なセキュリティコントロールが整備され、最新の状態に維持される。インシデント対応計画が策定され、すべての担当チームに連絡が与えられる。インシデントと新たな実装後にユーザと IT スタッフに教育を提供し、インシデントに対応するために迅速かつ正確に対応できるようにトレーニングを実施する。

特定: ネットワークオペレーションセンター (NOC) が 24 時間 365 日、システムイベントを監視し、疑わしいイベントを検出する。SOC (セキュリティオペレーションセンター) が情報セキュリティイベントがインシデントであるかどうか、およびその範囲 (いずれのネットワーク、システム、アプリケーション、ホスト、データセンターが影響を受けているか) を迅速に初回トライアージおよび分析することで、NOC をサポートする場合もある。初期分析は、インシデントの封じ込めやその影響のより深い分析など、後続のアクティビティの優先順位を決定するためにチームに十分な情報を提供することを目的とする。情報セキュリティイベントに関する情報は、さまざまなチャネルと Acronis 監視システムを通じて収集される。

封じ込め: このステージは、各インシデントの処理の過程において、またインシデントが Acronis のリソースやカスタマーのデータに影響を及ぼす前段階において、重要である。チームは問題の範囲、影響、影響を受けたシステムおよびカスタマーを特定する。封じ込めステージの重要な部分は、意思決定 (システムのシャットダウンや特定の機能の無効化など) である。

根絶: チームはインシデントの原因と問題の根本原因を発見するために調査を行い、マルウェアの削除や侵害されたアカウントの無効化などの除去処理を開始する。一部のインシデントについては、根絶が不要であるか、または復元中に実行される場合がある。

復元: 復元には、クリーンなバックアップからシステムを復元する、システムをゼロから再構築する、汚染されたファイルをクリーンなバージョンに置き換える、パッチをインストールする、パスワードを変更する、境界ネットワークのセキュリティを強化するなどのアクションが含まれる場合がある。復元フェーズのその他の目標は、将来の同様のインシデントの発生を防止することである。このため、NOC チームは、弱点や再発の兆候を検出するために、すべての環境を監視する。

教訓: チームはインシデントとその対応を分析し、再発防止のための推奨事項と将来の対応計画を作成する。

通知: 内外の連絡により、すべてのチームとカスタマーがインシデントのトライアージの重要なステージごとに影響と解決手順を理解し、状況を把握できるようにする。

事業継続およびディザスタリカバリ

多くの破壊的脅威がいつでも発生し得る状況であり、あらゆる拠点で事業活動に不利な影響を及ぼす可能性がある。Acronis は、リスクおよびビジネスインパクト分析の一環として、Acronis のすべての拠点（オフィスおよびデータセンター）、重要なプロセスおよびシステムにおいて、潜在的な脅威を幅広く検討している。

Acronis は、以下を目的として、包括的な事業継続およびディザスタリカバリ計画を策定する重要性を認識している。

- 従業員の安全を確保する。
- 重要なビジネスプロセスと技術（内部およびカスタマー向け）の継続を確保する。
- Acronis がカスタマーにサービスを中断することなく提供できるよう確保する。

潜在的な破壊的イベントが発生した場合に適切な対応とサービスの可用性を確保するために、Acronis は内部の事業継続およびディザスタリカバリ計画を定期的に見直し、更新している。特定の資産に関連する大半の潜在的な脅威に対するシナリオに従って、ディザスタリカバリ計画のテストが少なくとも毎年 1 回実施される。同時に、これらのテストシナリオは、サービスを実行する責任者によって決定されたさまざまな脅威の結果としてサービスの提供を停止することに関して調整される。テスト計画は情報セキュリティ委員会によって 1 年間承認され、次のいずれかの方法で実施される。

- チェックリスト。
- 構造化されたウォークスルー。
- シミュレーション。
- 中断。

Acronis は、世界中にコロケーション型データセンターを複数運用するためのパートナーシップを確立している。これらの施設は、設備、電力、冷却に関する厳格な基準とコンプライアンス要件を満たしており、ミッションクリティカルなデータを保護するために最適な状態とアップタイムを維持している。さらに、Acronis は、最も普遍的な破壊的イベントの発生率を低減または完全に排除するために、データセンターのロケーションについて厳しい要件を設けている。

Acronis はバックアップに対するバックアップを現在実行していない。その代わりとして、Acronis は単一障害点を排除するために冗長インフラストラクチャを活用している。当社のバックアップ戦略とディザスタリカバリ計画は、サービスの復元に焦点を置いている。

Acronis は、各従業員、部門、およびベンダに対して、以下に対するコミットメントを求める。

- 事業継続計画の目標のサポート。
- 事業継続およびディザスタリカバリ計画のレビュー、構築、テストおよび拡張。
- Acronis の資産、ミッション、存続可能性の保護。

サプライヤー関係管理

サプライヤーは、あらゆるビジネスにとって不可欠な一部である。一方で、企業内でどれほど厳格に資産が保護されていたとしても、サードパーティを利用する場合には、信頼性を確認する必要がある。

Acronis のベンダ選定プロセスでは、最初にサードパーティに対する基準を定義する。ビジネス要件に加えて、セキュリティとデータ保護の要件、およびカスタマーの要件の両方を考慮している。

Acronis はサードパーティの復処理者、データセンター、またはサービスプロバイダーと契約する前に、サードパーティがデータアクセスのレベルに応じた適切な水準のセキュリティおよびプライバシーを提供できることを確認するために、綿密なベンダ評価を実施する。第三者との契約には、セキュリティ、プライバシー、機密保持要件に関する情報が含まれており、Acronis は各契約期間中、第三者のセキュリティ制御、サービス提供、契約要件の遵守の定期的な監視およびレビューを行う。

詳細情報

Acronis のサイバーセキュリティとコンプライアンスの状況に関する詳細情報については、以下を参照のこと。

トラストセンター | PRIVACY（プライバシー） | 法律