RESOURCE CENTER

パスワード管理が企業のISO 27001認証取得をいかに支援するか

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/how-password-management-helps-companies-achieve-iso-27001-certification/

bitwarden

ISO 27001とは何か？

更新：3月27001日現在、Bitwardenはデータセキュリティを取り巻くISO 27001のコントロールセットに準拠し、ISO 27001認証を取得しています。

国際規格であるISO27001は、データ管理を含む情報セキュリティマネジメントシステム（ISMS）を構築、維持、発展させるための基礎を定めたものです。ISO 27001への準拠または認証取得を目指す企業は、ISO 27001パスワード管理をツールセットに加えることを検討すべきである。

国際標準化機構（ISO）は、世界的な技術・工業・商業規格を開発・発行する世界的なグループです。最後に更新されたのは2022年10月で、ISMSのためのISO 27001規格は、93の管理セットからなるデータ・セキュリティの枠組みを提供している。ISO 27001の認証を取得するためには、企業はこれらすべてに準拠していることを証明する必要がある。

> ISO 27001企業として認証されるには、93の管理セットを遵守する必要があります。

ISO 27001の認証プロセスは、企業のデータ・セキュリティ方針と手順、およびそれらの適用方法を審査する独立認証機関による監査で構成される。そのプロセスは長いものになりますが、ISO 27001の認証審査に合格することは、貴社が潜在的な脅威を特定するためのセキュリティ・リスク・アセスメントを実施し、データ侵害から保護するためのセキュリティ管理策を導入していることを示します。

目次

ISO 27001認証とコンプライアンスのメリット

ISO 27001の認証は、強固な情報セキュリティ管理を証明するものであるため、企業は顧客を引き付け、維持する上で競争上の優位性を得ることができる。認証はまた、サプライヤーや、情報がどのように管理され保護されているかに関心を持つその他の利害関係者を惹きつけ、引き留めることもできる。

監査プロセスの準備だけでも、既存のISO 27001ポリシーを強化し、内部システム、構造、日々のビジネスプロセスを改善することができる。リスクマネジメントプロセスは、企業がCCPAやGDPRなどのデータ保護法をよりよく遵守し、コンプライアンス違反による罰金や、回避可能なデータ漏洩による評判の低下を回避するのにも役立つ。

セキュリティ監査に合格するためにサイバーセキュリティ対策を強化する方法については、こちらをご覧ください。

ISO 27001の管理セット

93のコントロールセットは附属書Aに含まれており、4つの大きなテーマに分類されている。ISO 27001認証を取得するためには、企業はこれらの管理体制に準拠していることを証明する必要がある。カテゴリーは以下の通り：

- 組織的統制（37の統制）
- 人コントロール（8人）
- フィジカルコントロール（14コントロール）
- 技術的コントロール（34コントロール）

旧バージョンのISOには、14のカテゴリーに分けられた114のコントロールが含まれていた。そのバージョンには、安全なログオンとパスワード管理システムに関する文言も含まれていた。

セキュア・ログオン・コントロールは、「アクセス・コントロール・ポリシーが要求する場合、システムおよびアプリケーションへのアクセスは、セキュア・ログオン・プロシージャによって制御されるべきである」と規定している。パスワード・マネージャーを使えば、ユーザーはログインにもう1つのセキュリティ・レイヤーを追加し、2要素認証をサポートするすべてのウェブサイトの管理と統合を支援する1つの場所を持てるという利点がある。

パスワード管理システムの管理には、「パスワードの質を保証するために、パスワード管理システムは協力的でなければならない」と記されていた。ISOは、ユーザーが強力でユニークなパスワードを作成でき、コラボレーションのための安全な共有機能を提供するパスワードマネージャーの使用を推奨している。

> パスワード・マネージャーは、パスワードの強度を確立し、2FAを実施し、イベント・ログを使用してユーザーの活動を監視する。これらの機能はすべて、企業がISOアクセス制御、個人情報保護、およびエンドポイント保護の要件を満たすために達成しなければならない。

ISO 27001の最新版は、附属書A 5.17でパスワード管理を取り上げている。パスワードマネージャーを採用することで満たすことができる、あるいはサポートすることができる附属書Aの追加要件は数多くある。すべてを網羅しているわけではないが、例えば以下のようなものがある：

- **附属文書A 5.3、職務の分離**：相反する職務および相反する責任分野は分離されなければならない。
- **附属書A 5.14「情報の移転**組織内及び組織と他者との間のあらゆる種類の移転設備について，情報移転の規則，手順，又は協定を定めなければならない。
- **附属書A 5.15「アクセス管理」**：情報及びその他の関連資産への物理的及び論理的アクセスを管理するための規則は、ビジネス及び情報セキュリティの要求事項に基づいて確立され、実施されなければならない。

- **付属文書 A 5.16「ID 管理」**：ID の全ライフサイクルを管理しなければならない。
- **附属書 A 5.17「認証情報」**：認証情報の割当ておよび管理は、認証情報のベストプラクティスの取扱いに関する要員へのアドバイスを含む管理プロセスによって管理されるものとする。
  - この基準に関する詳細な入門書は、安全なパスワードを作成する機能を含め、パスワードの管理に関するアドバイスとともにパスワードの推奨事項を示している。さらに、この目的は、組織が弱い、広く使用されている、または危殆化したクレデンシャルを避けることを推奨する。

この基準を踏まえると、組織は、公開、再利用、脆弱、または漏洩した可能性のあるパスワードについて報告し、実用的な洞察を得ることを可能にするパスワード管理システムを導入するのが理想的である。

- **附属書A 5.34「個人識別情報（PII）のプライバシーと保護**組織は，適用される法令及び契約上の要求事項に従って，プライバシーの保護及びPIIの保護に関する要求事項を特定し，満たさなければならない。
- **附属書 A 8.1「ユーザーエンドポイント機器」**：ユーザ・エンドポイント・デバイスに保存され、ユーザ・エンドポイント・デバイスによって処理され、又はユーザ・エンドポイント・デバイスを介してアクセス可能な情報は、保護されなければならない。
- **付属書 A 8.4、ソースコードへのアクセス**：ソースコード、開発ツール、ソフトウェア・ライブラリへの読み書きアクセスは、適切に管理されなければならない。
- **附属書 A 8.5「安全な認証」**：安全な認証技術および手順は、情報アクセス制限およびアクセス制御に関するトピック固有ポリシーに基づいて実装されなければならない。
  - この目的は、システムに安全にログインするための多要素認証の使用に重点を置く。パスワード・マネージャーを使えば、ユーザーはログインにもう1つのセキュリティ・レイヤーを追加でき、2要素認証（2FA）をサポートするすべてのウェブサイトの管理と統合を支援する1つの場所を持てるという利点がある。この目的はまた、パスワードは常に秘密にしておくべきであることを強調し、完全に暗号化されたパスワード保管庫を強く訴えている。

パスワード管理システムは、組織が非アクティブな2FAで保管庫内のアイテムを識別することを可能にする。

- **附属書A 8.11「データマスキング**データマスキングは、アクセス制御に関する組織のトピック別ポリシー及びその他の関連するトピック別ポリシー、並びに適用される法規制を考慮したビジネス要件に従って使用されなければならない。
- **付属文書 A 8.12、データ漏洩**：データ漏洩防止対策は、機密情報を処理、保管、または伝送するシステム、ネットワーク、およびその他の機器に適用されなければならない。

ご存知でしたか？

Bitwarden は、強固なサイバーセキュリティの実践を促進し、従業員が保護の弱いアカウントを特定できるようにするVault

Health Reports を提供しています。

ISO recommends using a that enables users to create strong and unique passwords and offers secure sharing capabilities for collaboration.

パスワード・マネージャーを活用してISO 27001認証を取得

パスワード管理システムは、上記の附属書Aの数多くの要件をサポートし、全体的な管理セットに含まれる多くの要件をサポートする。

ユーザーは、認証情報を秘密にし、強力でユニークなパスワードを生成するなどの パスワードのベストプラクティスを適用し、
エンドツーエンドの暗号化で機密情報を保護するパスワード・マネージャーを使用して パスワードを安全に共有することができます。
特定の機密情報や重要情報の閲覧者を制限することで、パスワード管理者は職務を分離し、インサイダーの脅威を制限することもできる。

パスワード・マネージャーを使用する組織は、パスワード強度の要件を設定し、二要素認証（2FA）を実施し、イベント・
ログを使用してユーザーの行動を監視する。これらはすべて、企業がISOのアクセス制御、個人情報保護、
およびエンドポイント保護の要件を満たすために達成しなければならない機能である。評判の良いパスワード・マネージャーのほとんどは、
SSOの統合も容易にしており、管理者がアクセスや認証プロセスを管理するのに必要なツールを備えている。この機能は、
ISOの安全な認証要件を満たすのに役立つ。

ISO 27001認証をサポートするパスワード・マネージャーを評価する場合、組織は、そのソフトウェアがSOC2タイプ2コンプライアンス、
GDPRコンプライアンス、データ・プライバシー・フレームワーク、HIPAAなどのエンタープライズ・
グレードのセキュリティおよびコンプライアンス基準に従っているかどうかを評価する必要がある。企業は、エンド・ツー・
エンドのゼロ知識暗号化を提供するソリューションを選択すべきである。

Bitwardenを開始する

Bitwarden ISO 27001準拠のパスワードマネージャを活用して、情報セキュリティマネジメントシステムのISO
27001規格を満たすことに関心がありますか？今すぐBitwardenの企業向け無料トライアルを開始しましょう！

ケーススタディ：

インベントリー・ハイブ（Inventory Hive）は、ビットワーデンのISO 27001認証を取得した。

Bitwarden Secrets ManagerとBitwarden Password Managerの両方により、Titanom
Technologiesはサイバーセキュリティの回復力を実証し、ISO 27001認証の取得を検討することができます。

"I want to set guidelines on the password generator about how strong the password must be. That's very important right now for us to achieve the ISO 27001 certification."

Jannis Morgenstern, head of IT at Titanom Technologies