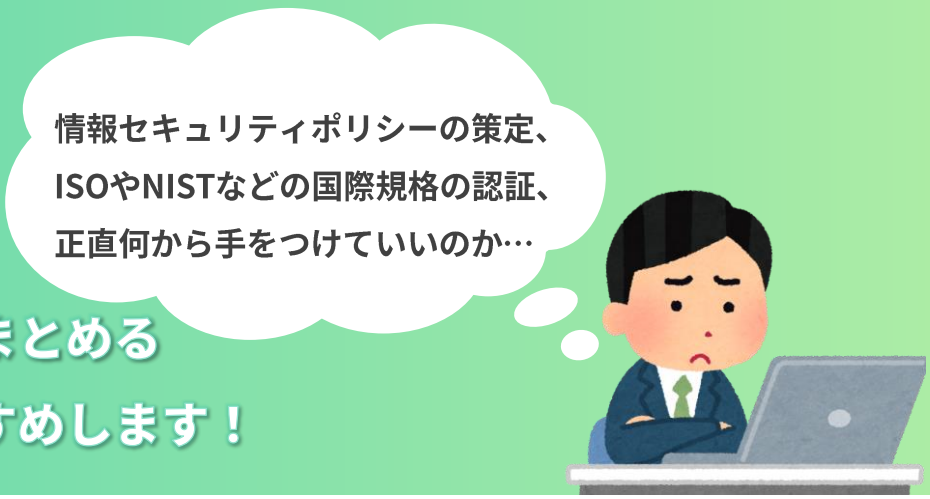
UserLock®

社内ネットワークのセキュリティポリシーをまとめる情シスご担当者様におすすめします！



情報セキュリティポリシーの策定は多くの企業にとって緊急の課題の１つとなっていますが、社内の情報システムのご担当者だけで多くの課題に対処する場合、リソースと時間がかかります。このようなセキュリティポリシーの基本となるのはユーザーログインの管理です。1つの指標となるISOやNISTなどのセキュリティに関する国際規格においても、ユーザーログインに関して細かく規定がされています。「UserLock」はこのユーザーログインをセキュアかつ簡単に管理できるソリューションです。

情報セキュリティの国際標準「ISO 27001」

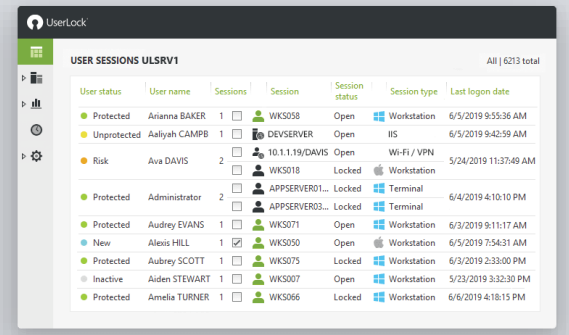
ISO 27001は国際標準化団体「ISO」の定める情報セキュリティの世界的な「スタンダード」です。情報の管理と構成、アクセスの制限、制御、または監視とその責任はISO 27001（またセキュリティ制御の詳細を規定するISO 27002）の要素となっており、UserLockを使用することで、これらの多くの要件に対処することが可能です。

米国の情報セキュリティの基準「NIST 800-53」

2002年に制定された米国の連邦情報セキュリティ管理法（FISMA）のコンプライアンスに準拠するため、NIST Special Publication 800-53「連邦情報システムおよび組織のセキュリティおよびプライバシー管理」という情報セキュリティの標準化が設定されています。UserLockはこの中でも優先度の高いセキュリティ要項に対応しています。

UserLockでログイン管理のコンプライアンス

「UserLock」は、ユーザーを一元管理するActive Directoryと連携してユーザーのログインを簡単に管理できるログイン見える化ソリューションです。さまざまなログイン管理に関するセキュリティ機能により、国際基準のコンプライアンスを実現します。



▶ ISO 27001に規定されるコンプライアンスに対応する

ISO 27001のアクセス・ログインに関する規定

■セクションA9：アクセスコントロール

ユーザーは使用が明確に許可されているネットワークおよびネットワークサービスへのアクセスのみが提供され、安全なログオン手順によるアクセスコントロールと、アクセスコントロールポリシーに従って制限を行う必要があります。

■セクションA12：運用セキュリティ

ユーザーアクティビティ、例外、障害、情報セキュリティのイベントを記録したイベントログの作成と保持、そして定期的なレビューを行う必要があります。

これらの規定を満たすUserLockの機能

通常のログインやリモートデスクトップ接続で、二段階認証を簡単に導入にできます。

パスワードのリトライや正規ルールではないログイン試行などを含むアクセスイベントの監査レポートを提供します。

ログインを端末やIPアドレスなどで制限してグループ全体を一元的に管理します。

▶ NIST 800-53コンプライアンスに対応し、データを安全に保護

NIST 800-53のアクセス・ログインに関する規定

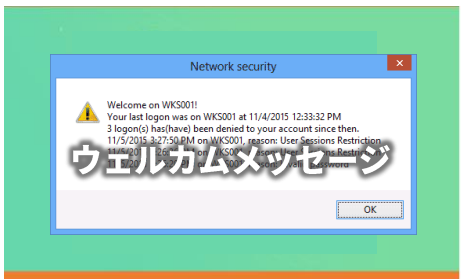
■AC-9：ログイン履歴の通知

情報システムは、システムへのログイン（アクセス）成功時に、最終ログイン（アクセス）の日時、最終ログイン（アクセス）以前のログイン（アクセス）失敗回数、最終ログイン（アクセス）の場所をユーザーに通知する必要があります。

■AC-10：同時ログインの制御

情報システムは、各アカウントへの同時ログインの制限を実行する必要があります。

これらの規定を満たすUserLockの機能



ログイン時に、ユーザーに以前の接続イベントの履歴を含むウェルカムメッセージを表示することができます。

多重ログインはセキュリティ上の問題の要因となります。同一アカウントの同時ログインを制限します。

すべてのユーザーのログイン状況をモニタリングして、ログインの挙動に関してアラートを設定することも可能です。

医療・保険

導入事例 UserLock

ヘルスケア産業は患者の個人情報を保護するセキュリティと同時に、最高の医療を患者に提供するためのアクセシビリティを兼ね備えたアクセスコントロールが求められます。

▶ CMSセキュリティ要件に定義される同時ログインの制限

米国の健康保険機関が連邦政府との契約する際、米国保健福祉省内の連邦機関であるCMS（メディケア・メディケイドサービスセンター）の規定するセキュリティ要件の遵守が必須要件となります。その中に「ユーザーはいかなる場合も1つのワークステーションのみにログオンすること」と規定されています。

CMS要件　■AC-10：同時セッションの制御

AC-10: Concurrent Session Control		
Control		
The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.		
Guidance		
The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: AC-10.1		
Assessment Objective		
Determine if:		

情報システムにおいては、各システムのアカウントへの同時セッション（ログイン）数は1つに制限されなければなりません。同時アプリケーション/プロセスセッションの数は、職務の遂行に必要なセッション数に制限されており、複数の同時アプリケーション/プロセスセッションを必要とする場合、セキュリティ計画書に文書化する必要があります。

▶ UserLockを使用した同時ユーザーログインの管理

ある米国の医療保険機関では、UserLockを導入し、CMSの規定する1人のユーザーによる複数端末へのログイン、また複数のユーザーによる１つの端末へのログインを制限する機能を実装しました。さらにそれぞれの拠点のPCの利用状況を確認し、長期間にわたって使用されていない状態にあるPCを不足している拠点に移すなど、拠点ごとの資産活用の最適化にも役立てています。

▶ すべてのユーザーのネットワークアクセスの管理と保護

これによりこの医療保険機関は連邦政府との契約に必須となるコンプライアンス要件を満たすことを実現しました。外部機関による監査レビューにおいても、UserLockの機能により3年に渡り継続して要件を満たしています。

この医療保険機関によれば、UserLockのメリットは使いやすいインターフェイスやレポート機能だけではなく、リアルタイムで提供される配信情報とアラートにより、ユーザーアカウントへのアクセスが最大となるピークタイムのトラッキングといった部分でも活用されています。このような情報は、パッチを適用する時期や、実装時に障害があった場合、影響が最小限に抑えられる時間帯の予測にも活用できるため、ヘルプデスク部門と共有することを検討しています。

OCEANBRIDGE
つかえるITを、世界から。

株式会社オーシャンブリッジ
〒 107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F
https://www.isdecisions.jp/
userlock@oceanbridge.jp