

NIST (米国標準規格) SP800-171に 対応できていますか？



アクセス制御



識別と認証



身元確認と
認証

UserLockは優先度の高い3つの
セキュリティ管理策に対応しています！

✔ NISTとは？

NIST (National Institute of Standards and Technology) は、米国の工業規格の標準を所管し、連邦政府の調達に関する技術標準などを定めている機関です。NISTの「SP800シリーズ」は幅広い領域に渡りコンピューターシステムの**セキュリティ**や**対策基準**が記載された重要なガイドラインとして、米国の多数企業が本格的に採用を始めています。

SP 800-171と SP 800-53の違い

「SP 800-53」は連邦政府機関が保有する**機密情報 (CI)** を保護する規定として先にまとめられ、「SP800-171」は機密情報以外の重要情報 (CUI) を取り扱う民間企業や組織に対して遵守を求める事項として新たに制定されたガイドラインとなっています。

令和4年、日本では防衛省が**NIST SP800-171をベース**にした「防衛産業サイバーセキュリティ基準」を発表し、翌年には中央省庁や独立行政法人の委託先企業に対し、同基準に沿った**セキュリティ対策の義務化**を行う旨を明らかにしました。

今後、日本のインフラ産業や他産業での調達要件としてNIST SP800-171への準拠が標準となる可能性は高く、サイバーセキュリティにおける自社の活動水準や製品の安全性を国際レベルに引き上げ、**信頼性と競争力を高めよう**とする企業の動きが活発化しています。

日本でも
NIST SP800-171
対応の重要性が
高まっています！



NIST SP800-171の重要な要件に対応し、 認証・予防・確認の観点から包括的なITガバナンスを実現します！

アクセス制御

多重ログイン制御

同一アカウントの同時ログインを制限できます



ユーザーの強制ログオフ

不審なログインの強制ログオフや放置されたセッションを一掃できます



接続方式によるログイン制限

Windowsログイン、VPN、IISなどの接続方式による多彩なログイン制御が可能

識別と認証

ログイン状況の監視

全ユーザーのログイン状況を監視し、特定の挙動に関してアラートを発せられます

履歴・監査レポート

パスワードの再試行など、ログイン及びアクセスイベントに関するレポートを作成します

ログイン時間の制限



ログインできる時間帯、曜日、上限時間などを簡単に設定できます

身元確認と認証

多要素認証(MFA)

ActiveDirectoryとシームレスに連携し、Windowsログイン、RDP、IISセッション等に多要素認証を付加できます。クラウド環境でも簡単・迅速に導入可能です



リモートデスクトップ接続制御

許可されたIP/マシン名からのみリモートデスクトップ(RDP)接続を許可します

今なら無料で体験できます！

- 30日間お好きなだけ
- 本製品と同様の機能 ご利用できます

お申込みはこちら



専門の技術部エンジニアが
インストールや初期設定などの
ご要望・ご相談を承ります

＼ まずはお気軽にお問合せください ／

Email: userlock@oceanbridge.jp



お問合せフォーム：
<https://www.isdecisions.jp/contact>



UserLock 国内総代理店
株式会社オーシャンブリッジ

<http://www.oceanbridge.jp/>
E-mail: userlock@oceanbridge.jp

〒107-0051 東京都港区元赤坂一丁目5番12号
住友不動産元赤坂ビル7階
TEL: 03-6809-0967

お問合せはこちら