UserLock® ホワイトペーパー

総務省が規定する地方公共団体向けの情報セキュリティに関するガイドラインに準拠するアクセス制御とは

OCEANBRIDGE

既存のWindows環境を変えず、二要素認証などの認証強化とアクセス管理機能を簡単導入

総務省が規定する地方公共団体向けの情報セキュリティに関するガイドラインとは

地方公共団体は、住民の個人情報のみならず、企業の機密情報も保有しており、このような個人情報や機密情報は、地方公共団体の使用する情報システムやネットワークを経由して行政サービスに活用されています。

当然ながら地方公共団体は、住民生活や地域の社会経済活動を保護するため、情報セキュリティ対策を講じて、保有する情報資産を守り、業務を継続することが必要となります。

さらには、近年の情報漏えいやサイバー攻撃の増加といった社会的な背景から、対策レベルを一段階強化する必要があるため、総務省は『地方公共団体における情報セキュリティポリシーに関するガイドライン』(以下、ガイドライン)を改定し、現在必要とされる情報セキュリティポリシーの詳細をまとめています。

そして、このガイドラインに準拠するための対応が、各地方公共団体で求められているのです。

ガイドラインの技術的セキュリティのポイントとなるアクセス制御

このガイドラインの６項の技術的セキュリティの中でも「アクセス制御」は不正アクセス対策として重要な項目の１つとなります。具体的には下記の４つの制御、管理機能を実現することが求められます。

- **利用時間や利用時間帯によるアクセス制御**
- **特権による接続時間の制限**
- **IPアドレスによる端末の制限**
- **同一主体による複数アクセスの制限**

これらの４つの要件は『政府機関等の対策基準策定のためのガイドライン』にも記載されており政府機関等でも同様の対策が必要とされています。

しかし、これらのアクセス制御を実現するためにはどうすればよいのでしょうか。
もし大規模なシステム変更が必要になると、導入のコストや運用面での担当者の負担が大きくなってしまう場合が多く、課題となってしまいます。そこで導入の際に重要なポイントは下記の3点です。

- **既存のWindows環境を変更する必要がない**
- **必要な機能だけを追加できる**
- **導入が簡単でコスト面でも大きな負担とならない**

ログイン管理ツール「UserLock」（ユーザーロック）であれば、上記の条件を満たし、必要なアクセス制御を実現することが可能になります。

OCEANBRIDGE

UserLockとは

UserLockは、社内ネットワーク（LAN）に接続しているユーザーと端末を一元管理する『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。使いやすいインターフェイスと多要素認証や、端末・接続方式のログイン制御など、さまざまな機能により、簡単にセキュアなログイン管理を実現します。

ガイドラインに準拠したアクセス制御を実現するUserLockの４つの機能

利用時間や利用時間帯によるアクセス制御

UserLockはログインが継続している時間や、アクセスする時間帯によるアクセス制御可能です。昨今においては、サイバーセキュリティの高度化、さらにAI技術の活用が進み、ウィルスが社内ネットワーク内に潜伏し、従業員がアクセスしていない夜間帯を狙って攻撃する、というようなインシデントも起こっております。リアルタイムでの監視が難しい場面で効果を発揮します。

IPアドレスによる端末の制限

UserLockは許可された端末、または許可されたIPアドレスなどでログイン制限をかけてグループ全体を一元的に管理することが可能です。例えば、社内規定で指定されている端末からのみログインが可能、といったセキュリティポリシーに沿った運用を行うことが可能です。情報セキュリティ関連のコンプライアンスに準拠した運用を行う場合にもご活用いただけます。

特権による接続時間の制限

管理者権限など、強い権限を持つ特権IDがハイジャックされた場合、ネットワーク全体にとって大きなセキュリティリスクとなります。そのような特権IDが、ログインしたまま長時間のセッション放置になっている場合、直ちにネットワーク接続を強制終了できる措置は重要になります。UserLockは放置されたセッションに対して自動ログオフすることが可能です。

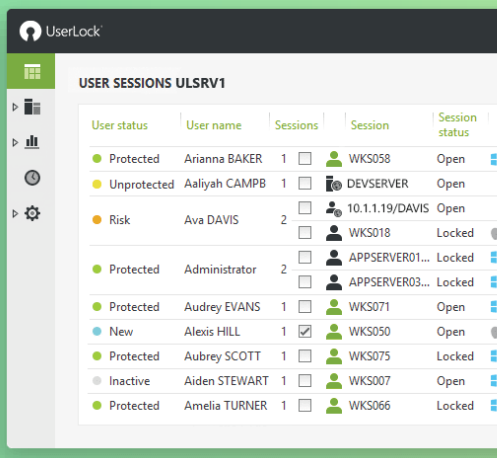
同一主体による複数アクセスの制限

UserLockは同一アカウントの複数ログインの制限を可能にします。
１つのアカウント情報での同時ログインを制限することで、本人以外の不正アクセスの防止だけでなく、社内間のアカウント使い回しや、隠れ共有といったセキュリティリスクの防止して、コンプライアンスの向上を実現します。
また、この機能はWindows Serverや他システムでは提供されていない、ユニークな機能となります。

OCEANBRIDGE

UserLock®

UserLockは、社内ネットワーク（LAN）に接続しているユーザーと端末を一元管理する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。
使いやすいインターフェイスと、さまざまな機能で簡単にセキュアなログイン管理を実現します。



UserLockの主な特長と機能

二段階認証の簡単導入

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。

多重ログインの制限

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。

ログイン端末の制限

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。

ログイン時間の設定

ログイン可能な時間帯や曜日、上限時間の設定など、個別の業務形態、時間に合わせた運用を行うことが可能です。

接続方式によるログイン制限

Wi-Fi、VPN、IISなどのさまざまな接続方式によるログインの制御が行えます。。

ログイン状況の監視

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。

強制ユーザーログオフ

社内ネットワークやリモート接続上で不審なログインや放置されたログインなどを強制的にログオフできます。

ログイン履歴の監査レポート

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。

フル機能を無料で30日間お試しいただける体験版もご用意しております。
下記サイト、またはuserlock@oceanbridge.jp (UserLock担当)まで
お気軽にお問い合わせください。

■製品情報サイト　：https://www.isdecisions.jp/userlock/
■体験版お申込み　：https://www.isdecisions.jp/trial
■製品お問い合わせ：https://www.isdecisions.jp/contact

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