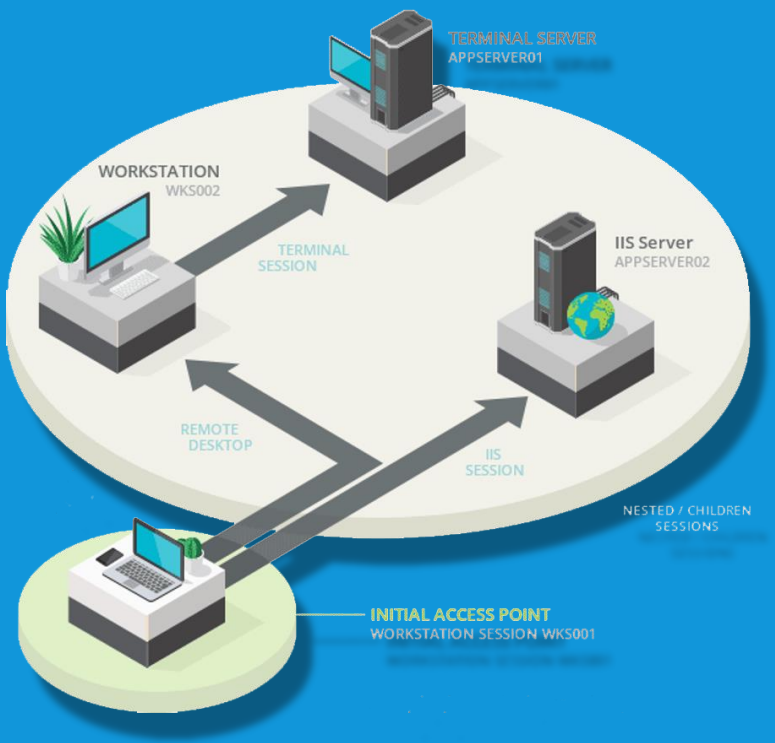
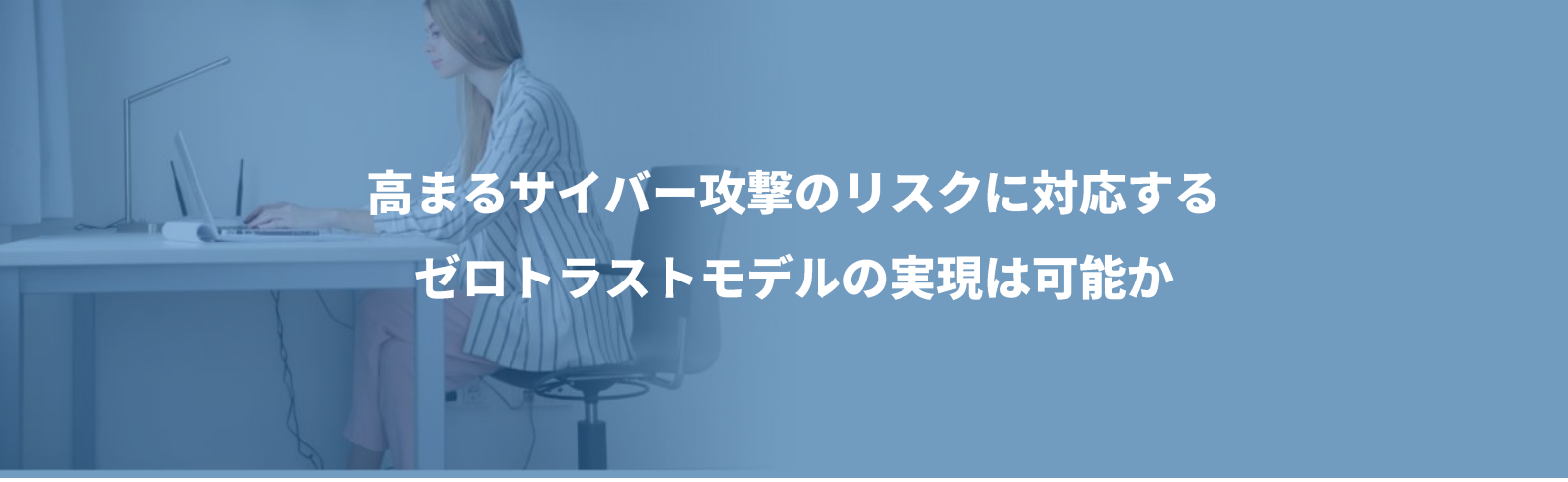
UserLock® ホワイトペーパー

# ゼロトラストモデルに興味がある人必見！
# 今あるActive Directoryに後付け可能な
# 不正ログイン対策ソリューション




OCEANBRIDGE



# 高まるサイバー攻撃のリスクに対応する
# ゼロトラストモデルの実現は可能か

## 境界防御モデルとゼロトラストモデル

昨今のコロナ禍でのリモートワークの拡大やAI技術を用いたサイバー攻撃の高度化などにより、IT・セキュリティを取り巻く状況は激変しています。

それに伴い、従来の「境界防御モデル」と呼ばれる社内と社外の境界を強固にして脅威を防ぐことが難しくなっており、今後はすべてのネットワーク・デバイス・ユーザーが安全ではないという視点に立ったセキュリティ対策、いわゆる「ゼロトラストモデル」の実現が求められます。

しかし、ゼロトラストモデルの実現を考えた場合、企業・組織はあらゆるレイヤーにおいて、**様々なソリューションを新規導入・網羅しようとすると、膨大なコスト・運用の負荷・技術的なキャッチアップの負荷**が懸念されます。

## 既存IT資産を活かしてセキュリティを高める

無条件で究極のセキュリティを目指すのであれば、様々なソリューションを新規導入・網羅することは理想的なアプローチの1つですが、多くの企業にとってそれは現実的ではありません。ではどう対応すれば良いでのしょうか。

そもそも、昨今の複雑なIT活用において、「ゼロトラストモデル」はユーザー×アプリケーション×デバイスといった、すべてのパターンを監視するという考え方ですが、抑えるべきポイントは結局のところ、「認証とアクセス管理」です。また、「境界防御モデル」で懸念されるポイントは社内ネットワーク（＝信用できる領域）が不正アクセスにより侵されたら、無防備になってしまうということです。

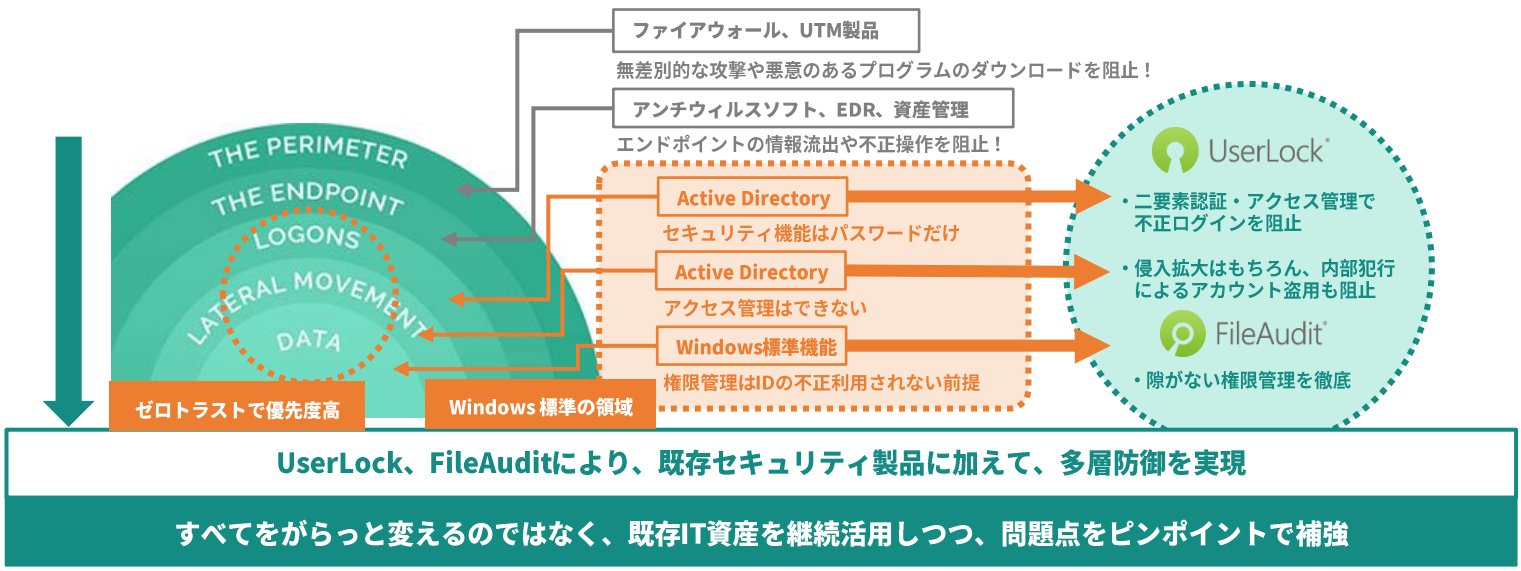
このことから、例えば多くの企業で構築されている「境界防御モデル」に沿ったITインフラのセキュリティ課題をピンポイントで強化することができれば、既存IT資産をそのまま活かすことができ、既述の「膨大なコスト・運用の負荷・技術的なキャッチアップ」の問題を解消し、セキュリティレベルを大きく向上できるのではないでしょうか。つまり、それは**実現性と費用対効果を兼ね備えた現実的なアプローチ**と言えます。


## 「No Logon, No Access」を実現するソリューション

そのようなコンセプトをもとに、ビジネス展開や製品開発を進めているのが、IS Decisions社です。同社は“No Logon, No Access：ログインされなければ、アクセスされない”という考えをもとに、比較的低コストで、導入・利用が容易で、強固な認証と柔軟なアクセス制御を実現できる「UserLock」を提供しています。

下図は社内ネットワークと情報資産のセキュリティ侵害ステップを示しています。多くの企業では、社内ネットワークや情報資産を守るために、「THE PREMIMETER(境界)」にはファイアウォール、UTMを、「THE ENDPOINT(エンドポイント)」にはアンチウィルスソフト、EDR、資産管理を導入されていますが、「認証とアクセス管理」に相当する「LOGONS」以降にはWindows標準機能のみで構成されているケースが多く、「ゼロトラストモデル」の考え方においては、防御・対策が十分ではありません。この領域を補強するのがUserLockとFileAuditです。

## 社内のネットワークや情報資産に対するセキュリティ侵害ステップ




UserLock、FileAuditにより、既存セキュリティ製品に加えて、多層防御を実現

すべてをがらっと変えるのではなく、既存IT資産を継続活用しつつ、問題点をピンポイントで補強

OceanBridge

## UserLockの主な機能・特長

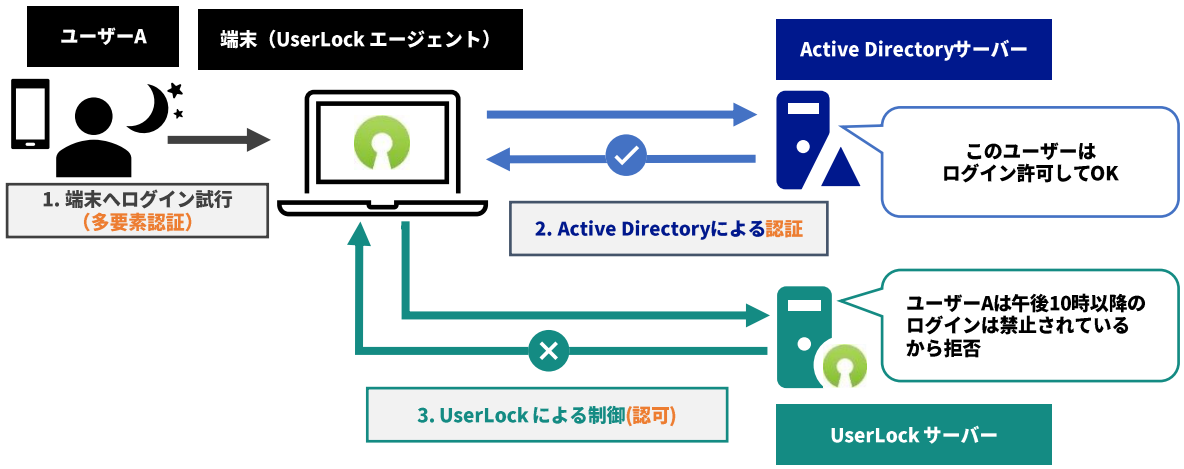
**1．社外・社内脅威からネットワークを守るセキュリティ強化**
昨今、セキュリティインシデントが多発しているID/パスワードによる認証の脆弱性を解決する二要素認証と共に、接続元・時間・接続種類、同時ログイン数などによる柔軟なアクセス制御を実現します。更に、不審なアクセスを検知した場合、その対応としてアラートや各種アクションを支援します。

**2．各種コンプライアンス遵守への対応**
ネットワーク全体に対するアクセスを俯瞰的に制御・管理することができ、各種コンプライアンス（GDPR、PCI DSS、ISO 27001、HIPAA、NIST、SOX、CCPA等）に対応する際に、企業・組織が取り決めたルールに基づき、実際の現場で運用できる仕組みを提供します。

**3．導入しやすいユニークな仕組み**
新たなID認証に仕組みを設計、導入することなく、既存の資産であるオンプレミスActive Directoryを活用し、足りない機能をUserLockが補うというユニークな仕組みにより、コスト・運用負荷・技術キャッチアップ負荷を軽減します。

**4．多数の導入実績**
グローバルでは既に3,500社以上の導入実績があり、136ヶ国以上で利用されています。日本国内ではオーシャンブリッジの正式リリース前から、製造業・金融業・IT業・教育などを中心に既に多くの導入実績があり、安心して導入していただけます。

## Active Directoryと連携するUserLockの仕組み

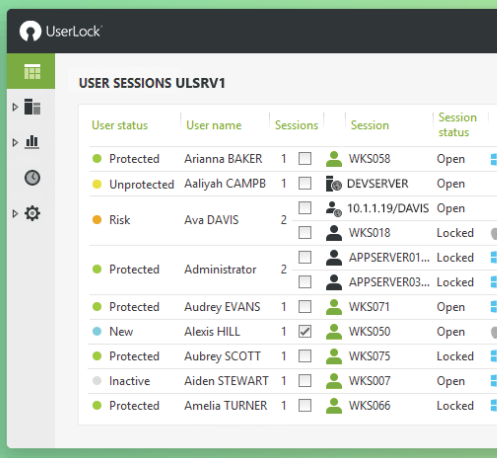



## 今後の展開

**・クラウドアプリへの対応**
今回のリリースではオンプレミス環境に特化したバージョンを提供開始しますが、オンプレミスActive Directory認証によるクラウドアプリケーション（Microsoft365、Google、SalesForce、BOX、Dropbox、その他（SAML2.0対応）など）へのシングルサインオン（SSO）に対応した新バージョンを今後近い将来に提供する予定です。

# 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