EAGLE EYE NETWORKS

クラウド映像監視
シングルサインオン

シングルサインオンとは？

SAML 2.0認証でのシングルサインオン（SSO）は、複数のアプリケーションや Web サイト間のアクセス管理を合理化し、セキュリティと利便性を向上させます。ユーザーが１組のユーザ認証情報（クレデンシャル情報）でログインすると、信頼できる第3の企業/機関により検証され、アクセスが与えられます。

平均 １人につき **55** 個のクレデンシャル情報を持っている

パスワード入力や再設定に費やした平均**時間**（年間） **10.9**

出典: Ponemon Instituteによる"(Yubico) 2019 State of Password and Authentication Security Behaviors Report"(CPOマガジン）。LastPassによる2019年パスワードセキュリティレポート。

クラウドアプリケーションとユーザーディレクトリの統合

問題点：多くの企業では、LDAP または Active Directory が、ネットワークや Web アプリケーションなどのオンプレミスにあるリソースに認証後、アクセス許可するための「信頼できる情報」として機能しています。新しいアプリケーションが追加されれば、その分固有のユーザー認証情報（クレデンシャル）が追加されます。管理者にとって管理が煩雑になるという状況になりかねません。

解決策：SSOを利用することで、Eagle Eye Cloud VMSと企業のLDAPやActive Directoryとの間に単一の認証統合ポイントが提供されるため、複数のディレクトリを管理する必要がなくなります。

SSOの利点

SSO認証を採用する企業のメリット

- リスクのあるクレデンシャルが少なくなるため、サイバーセキュリティ対策が向上します。
- Eagle EyeCloud VMSのクレデンシャルを個別に保存してセキュリティ対策を施す必要がないため、ユーザーが使いやすくなります。
- 標準化することにより、ベンダーやプラットフォーム特有のアーキテクチャに関連する障壁がなくなります。
- 企業において各従業員が1つのクレデンシャルで複数のアプリケーションにアクセスできることにより、管理コストを削減し、生産性を高めることができます。