Project

PERSPECTIVES

SSO プロジェクトを成功させる 7つのルール

15 年間におよぶ経験に基づき、本ホワイト ペーパーでは、シングル サインオン（SSO）の展開を成功させるための実践方法と避けるべき落とし穴について説明します。

EVIDIAN
A Bull Group Company

企業における SSO の展開

シングル サインオン（SSO）は、ユーザーの生産性を高め、セキュリティを強化し、ヘルプデスクのコストを削減し、組織による法規制順守を助けます。

しかし、SSO プロジェクトはそれほど簡単に実現できるものではありません。迅速な展開、プロジェクトの目的の達成、ユーザーのプロジェクトへの参加を確実に行う準備が十分にできていなければなりません。

15 年近くの間、Evidian とパートナーは何百もの SSO プロジェクトを実現してきました。これらのプロジェクトから学んだ教訓を、このドキュメントで説明いたします。これらのプロジェクトを成功に導いた「黄金律」（下記 1.～7.）の大部分は、技術面よりも、プロジェクト組織に関わるものだとお気付きいただけるでしょう。

1. プロジェクトの目的を明確に定義し共有する
2. プロジェクトが法規制順守（コンプライアンス）を助けることを実証する
3. ユーザーが積極的にプロジェクトに関与できるよう促す
4. 既存の手順とポリシーに配慮する
5. シンプルなアーキテクチャーを実現する
6. 定期的に数値指標を公開する
7. 目的達成を評価し、アイデンティティ管理への拡張を計画する

シングル サインオンとは?

シングル サインオン（SSO）により、例えばパスワードや USB トークン、生体認証-指紋リーダーがあれば指などの認証方法のうちの 1つで、全てのアプリケーションへのアクセスが可能です。

通常、シングル サインオンでは、コンピュータ上でユーザーに代わってアプリケーション パスワードを入力するソフトウェア アプリケーションを使用します。

Web アプリケーションのみを使用しているか、「シン クライアント」モードで作業している場合、SSO ソフトウェアはサーバーにホストされ、リモートからパスワードを入力します。この場合、ローカルのソフトウェア アプリケーションは不要です。

1. プロジェクトの目的を明確に定義し共有する

要約

成功した SSO プロジェクトの目的は、いずれも以下の例のようにたいへん明確です。

- ヘルプデスク コストの削減
- ユーザー（医者、営業、トレーダー、他）の生産性向上
- 重要なアプリケーションへのアクセス制御によるセキュリティ強化
- 法律と規則（ 医療上の秘密事項、PCI DSS、他）の順守

一般的に、各 SSO プロジェクトには、1 つないし 2 つの主要目的と、これに従属する綿密な目的があります。期待する具体的な成果を書き出して明確にすることが重要です。SSO ターゲットプラン、つまり、期待する具体的な成果を明確化することで、プロジェクト参加者が公式コメントを受けやすくなります。社内、社外の関係者は、平等な権限で、この計画を決めるための現場の意思を表明しやすくなります。関係者とは、例えば、社外のシステム インテグレータや、社内の経理部、社内管理部、業務部などです。

なぜ重要か?

目的を明確に定義してコストを見積もれば、プロジェクトの経過を継続的に管理部門からのサポートを保持でき、プロジェクト関係者にとって後の参考になります。

外部のサービス プロバイダーが、現在のビジネスの優先分野に集中して仕事をすること、あるいは確かに達成できる提案を行うことが可能になるでしょう。ビジネスの目的によっては、他よりもずっと適したツールや方法があります。

業務部や他部署と一緒に期待される利益を判断することで、彼らの参加を確保できます。こうして、プロジェクトの実現とユーザーの参加を促します。

事例

ある製薬会社がシングル サインオンの導入を希望しました。具体的な目的は US regulation 21 CFR Part 11（FDA:食品医薬品局が公布した連邦規則第21章第11条、電子記録・電子署名に関する規則）を順守することでした。このためには、電子文書を米国食品医薬品局に提出し、担当者によって正当性を立証されて署名される必要があります。

当初この会社では、Web アプリケーションだけに SSO ソリューションを導入する予定でした (セキュアな SSO 「ポータル」 が 1 つだけ必要になる)。 しかし、プロジェクト関係者は作業チームとともに慣例に従った目的を見直している間に、ドキュメントの完全性に関する多数のリスクが「クライアント サーバー」アプリケーションからもたらされることに気づきました。

Evidian とインテグレーション サービス プロバイダーは、クライアント サーバー アプリケーション用に Enterprise SSO ソリューション一式を導入することを勧めました。この方法は Web アプリケーションにも対応するので、当初の機能の目的は、実際のビジネスの目的とともに達成されました。

2. プロジェクトが法規制順守を助けることを実証する

要約

SSO プロジェクトの主な目的が運営上のこと、例えば生産性やコスト削減のためであっても、社内の管理部門と連絡を取ることは有効です。SSO ソリューションによって、会社は法規制順守の目的を果たしたり、既存の管理手続きを簡略化したりすることができます。

法規制順守の目的は、IT システムにおける完全性、機密性、可用性を向上させることです。SSO はコンプライアンス担当者にさらに以下の成果をもたらします。

- 完全性：SSO は、例えば財源のような重要なリソースへのアクセスを、役割上必要な人物のみに制限します。
- 機密性：個人データ（医療情報、支払情報等）を管理するアプリケーションは、SSO で保護されます。アクセス ログは中央のポイントで保存されます。
- 可用性：パスワードを忘れてしまっても、ユーザーが事前に回答した質問に正しく答えられるならば、コンピュータとアプリケーションを使用できます。さらに、SSO が既存のディレクトリを使用するなら、既存のバックアップ システム等も利用できます。

なぜ重要か?

社内の管理部門に、相談だけの理由でプロジェクトに参加してもらうのであっても、この取り組みへの信頼性を増すことができます。規制の順守とは、明らかな目的を管理することです。なぜなら、順守しないと会社に多大な影響を及ぼすからです。

また、社内の管理部門は、初期の段階でプロジェクト展開に関する意見を述べることで、後に役立ちそうな提案を行えます。SSO を展開する方法は、彼らが監査業務をよりうまく行うのに役立ちます。

事例

ブラジルの大手通信会社では、SSO を展開することで、ユーザーの生産性を向上させ、サーベンス・オクスリー法（SOX 法）に適合することを希望しました。この米国の法律の狙いは、財務報告の完全性を確証することです。

このプロジェクトの準備期間中に、Evidian と現地のパートナーは、クライアントの社内管理部門とだけではなく、外部の監査人とも打合せをしました。打合せを行うことで、当初ははっきりしなかったニーズが明らかになりました。

例えば、監査人は統合されたデータを見て、管理手続きを検証します。そのため、監査人はこの SSO データに変更がなく、データの基が体系的に文書化されているかどうかを質問しました。

最終的に、プロジェクト チームは集められた情報を検証するための手続きをまとめました。こうして、毎年のアクセス手続きの監査を数日間短縮することができました。

3. ユーザーが積極的にプロジェクトに関与できるよう促す

要約

従業員は SSO の主要な関係者です。彼らから意見を求めて展開プロセスに取り入れることはたいへん重要です。管理職から意見を求めるだけでは、不十分です!

したがって、最も影響のある部類の従業員を特定する必要があります。彼らは、SSO のような目新しいものを警戒するかもしれませんが、いったん納得すれば推進者になるでしょう。彼らの意見から、展開期間中のユーザーの反応が予測できるようになります。

- SSO から最も恩恵を受ける人物の特定
- 「パイロット（試験）」ユーザーとのデモを含んだ定例会議
- リリースに先立つ、パイロット ユーザーへの SSO ソリューションのテストの提案
- ユーザーの 1 部が SSO を彼らの コンピュータへの「スパイ」とみなす可能性の認識
- ユーザーに技術的な利点ではなく、ビジネス上の利点を示す

なぜ重要か?

従業員は、SSO がもたらす利点を通常すぐに理解します。したがって、彼らをプロジェクトの推進者に変えることができます。SSO ユーザーは、たいてい最大の支持者になります。

一方で、ユーザーの意見は、事前に障害を検出し、修正することに役立ちます。例えば、気をつけるべき重要なアプリケーション、ローカルでの要件、見過ごされるニーズを特定できます。

事例

フランスのある病院では、健康管理スタッフ用にシングル サインオンの展開を希望しました。病院において、パスワード入力に割かれる時間は、健康管理サービスの質に影響を及ぼします。健康管理スタッフはスマートカードを用いてアプリケーションにシングル サインオンすることで、患者の看護により時間を割けるようになります。

プロジェクト チームは、健康管理スタッフの代表たちにデモを見せて、部署でテストを行いました。

チームは、情報システムを制約が多く厄介なものだとみなす数名の医師たちが、制約ができるだけ少ないシステムを望んでいることを確認しました。その一方で、医師達はアプリケーションがすぐに立ち上がることと、アクセスが記録されることを、歓迎しました。また、看護師達は検査用台車のコンピュータ上への SSO アクセスにすぐに順応しました。

しかし、救急科の医師達は、認証用のスマートカードの組織的な利用を拒否しました。これにより、アクセススピードは遅れました。

救急部署には、猶予期間と診療の流動性に基づく特有のセキュリティ ポリシーを採用することで、問題は解決されました。この部署へのアクセスはスマートカードで物理的に制御されるため、スピードとセキュリティを兼ね備えることが可能になりました。

4. 既存の手順とポリシーに配慮する

要約

SSO は単なる「技術プロジェクト」ではありません。企業およびその中の層の日々の業務を変える可能性があります。変化の大部分はプラスのものです。

しかし、SSO を取り入れるために、管理職が自分達のやり方を変えなければならないと気づくとき、問題点がいくつか浮かび上がることがあります。例えば、アプリケーションへのアクセスを許可する方法が変わる可能性があります。

したがって、これらの変更を最小限に抑えることを確実にし、変更がやむを得ないものであるときには予め予測しておく必要があります。うまいことに、各組織が自分たちのニーズに従って、徐々にあるフェーズを計画していけます。

なぜ重要か?

SSO 展開を十分に準備し、現場の管理職や事業部長が参加すると、成功の確率が高まります。

一般的に、管理職側のやる気のなさは、惰性という問題ではありません。彼らが皆、同じプライオリティとスケジュールを持っているわけではないからです。例えば、経理部や営業部では、年度末近くに新しいツールをインストールすることを敬遠します。

SSO により手順が簡略化され、1 画面から全アプリケーションへのアクセスを管理できるようになっても、ローカル管理者は訓練を受ける必要があります。その上、手順が法律上の理由で存在する場合には、既に文書化、監査されているものなので、変更にはコストがかかります。

事例

ある事業会社は 70,000 台以上のコンピュータに SSO を展開することを希望しました。この事業部と現場の管理職達は SSO プロジェクトを支持しました。しかし、管理者達の優先順位は異なり、各自が個別に実現しなければならないタスクを持っていることが、明らかになりました 。

管理職のうち 2、3 人だけがアプリケーション アクセスの管理方法をすぐに変更することに同意しました。mySAP のようないくつかのアプリケーションは、金融セキュリティの法律に従い、SSO に組み込まれる前にテスト対象とする必要がありました。

解決方法: すぐに SSO に組み入れるべき 10 から 20 個の基本アプリケーションを、各現場と組織で決めることでした。mySAP のようなアプリケーションは、組織の既存のやり方を尊重して、この基本アプリケーションのリストから当初は除外されていました。「SSO モードへ切り替える」決定は、各部署が行いました。

同様に、SSO ではアクセス管理の方法を変更するとは限りません。最初のステップは、既にあるアカウントへのアクセスを自動化するだけです。こうして、SSO はスムーズに展開されました。各組織は、日程とオプション（統合すべきアプリケーション、統合時期、アクセス権の管理方法）を自由に選択できました。

5. シンプルなアーキテクチャーを実現する

要約

プロジェクトは、コストが低く、現在の IT 環境にうまく適合しているなら成功する可能性があがります。したがって、アーキテクチャーはできるだけ単純にすべきで、もっと複雑に、ということではありません。

SSO ソリューション自体は、課題の一部でしかありません。ユーザーについての、信頼できる最新のリストも必要になります。各ユーザーがスムーズに仕事するためには、SSO 情報（暗号化パスワード、許可されたアプリケーションのリスト、他）は各メインサイトで使用可能でないとなりません。

また、これらの要件は、複雑なソリューションに役立つとは限りません。既存のディレクトリ、サーバー、およびネットワーク リソースを使用することで、プロジェクトはインストール中と使用期間中に、かなりの節約ができます。

なぜ重要か?

プロジェクトのコストと複雑さをコントロールすることは、成功につながります。投資に対する速やかな利益を、簡単に示せるでしょう。

もし、すでにユーザー アイデンティティ リポジトリ（LDAP ディレクトリ）があり、このリソースを用いれられるのであれば、既存のユーザー更新手順から恩恵を受けられます。

同様に、「アプライアンス」によって数百ユーザーに対する迅速な展開が可能になります。しかし、ユーザー データの参照先がいくつかの場所に分かれている場合は、これらのアプライアンスと関連するサポートを増やす必要があるかもしれません。既存のローカル データベースを用いることによって、部員の実務とスキルを生かせます。

事例

英国の病院では、総勢 5,000 人の健康管理および管理スタッフ用に、SSO の展開を希望しました。目的は、ヘルプデスクのコストを削減し、健康管理スタッフのカードに基づくアクセスをセキュア化することでした。もちろん、臨床用アプリケーションの高い可用性は、病院の環境には不可欠です。

アプライアンス ベースの SSO ソリューションが展開されつつありました。また一方で、病院では、組織の大きさと複雑さから生じる、性能と信頼度についての問題に気づいていました。保守と交換を考慮すると、運用コストは計画していたものより高くなり、高い可用性が保証されないことに、病院は気づいていました。

そのためこの病院は、アーキテクチャーを変更し、既存のアクティブ ディレクトリを使用することを選択しました。このディレクトリは SSO データ自体を格納することができ、新しいハードウェアは必要ありませんでした。

こうして、SSO データは各サイトのユーザーの近くで使用可能になり、SSO はより速くなりました。SSO ソリューションの高可用性は、ディレクトリの可用性なのです。また、緊急対策とバックアップ手順は既に存在しています（ディレクトリ用に使用されているものです）。

6. 定期的に数値指標を公開する

要約

他のプロジェクトと同様に、SSO プロジェクトも、経過報告書とともに文書化します。しかし、SSO は IT の範疇を超えて見えるものです。報告書は技術者でない人たちにとっても理解可能で、納得できる指標を含んだものでないとなりません。例えば：

- SSO ソリューションがインストールされたコンピュータの台数、関係するユーザーの人数
- ヘルプデスクへの問い合わせと解決した問題の数
- 集めた監査データの大きさと範囲、アクティブにされたセキュリティ機能
- ユーザー満足度の指標 (サーベイ、他)
- アプリケーションのアカウント数 (合計と 1 ユーザー当たり)
- SSO がカバーするアプリケーション数
- 自動ログインの数と省けた時間の概算

技術的な点は、当然重要です。しかし、レポートは情報共有と管理用のツールとなります。自動監査ツールは必要な指標を集めます。これにより解析と最適化の作業が容易になります。したがって、SSO への投資による迅速な利益を示すことが簡単になります。

なぜ重要か?

レポートはプロジェクトのステータスの可視化を可能にします。今までみてきたように、運用管理者、財務管理者、監査役、その他の信頼を得る必要があります。彼らは客観的な結果を期待するので、きちんと提供する必要があります。

関係部署が積極的に参加すれば、展開は容易になります。最初の現場と部署でソリューションがインストールされたら、その結果の事実と数値は他の部署を納得させるものとなります。SSO の展開が終了するとき、今後のフェーズ、または他のプロジェクトをスピードアップするのに十分な信頼を得ることになるでしょう。

事例

国際銀行のフランス支店で、パスワードの増加がセキュリティホールを作っていて、多すぎるパスワードが 1,200 人の従業員を閉口させていることに、セキュリティ部門が気づいていました。そこで、支店は生体認証を用いた SSO プロジェクトを開始しました。ゴーサインを得るための重要な根拠は、ヘルプデスクのコストを期待通りに減らすことでした。

展開には、通常のレポートが添えられました。ヘルプデスクは外注されていたため、問い合わせの進展を測ることは容易でした。設置を定期的に評価することで、プロジェクト チームは予想以上にさまざまな構成があることに気づきました。彼らは、ユーザーに生体認証に慣れてもらうことと、SSO で明らかになったパスワードの共有のような現状の問題を是正することに、時間を割くことに決めました。

このフォローアップのおかげで、予算を超えることなく、SSO は後方業務から高い評価を得ました。実用的な教訓を学んだことで、このツールを海外に普及させるよう親会社を説得しました。

7. 目的達成を評価し、アイデンティティ管理への拡張を計画する

要約

SSO プロジェクトの最後に、目的を達成できたか評価することは有益です。強力な認証、および新規アプリケーションの統合のような未決の課題のいくつかは、将来のプロジェクトにつながります。

Evidian は、SSO がより大がかりなアイデンティティ管理プロジェクトへの優れた第 1 歩であることに気づいています。数ヵ月後には、役に立つ SSO の動作履歴データベースを得ることになるでしょう。こうして、アプリケーションのどのアカウントが実際に誰によって使われたかが、わかります。

なぜ重要か?

SSO プロジェクトの成功は、アイデンティティとアクセス管理の拡張を提案する良い機会でもあります。理由は簡単です。アプリケーションがどのように使用されるかがわかるので、現実的なセキュリティ ポリシーを定義することができます。実施前に、結果を予測できます。

同様に、アカウント “プロビジョニング” を実現できるようになり、承認されたワークフローの制御下で自動更新できるのです。アカウント パスワードは、SSO ソリューションに送られます。

よって、ユーザーはセキュリティ ポリシーに自然と従うことになります。アカウントは、社内の従業員の状況によって、自動的に作成されたり、消去されたりします。

事例

ヨーロッパの大手鉄道会社が、80 個のアプリケーションに対して 150,000 を超えるユーザー、すなわち百万以上のアプリケーション アカウントを管理するセキュリティ ポリシーの実現を希望しました。

この会社は全アカウントの調査を開始しました。しかし、これは実現不可能で、コストがかかり過ぎる事がわかりました。また、これらのアカウントを得ることは、予想していたよりもずっと困難でした。アカウント “sch002” は誰が使用しているか？、どうすればわかるか？、特定の従業員か？、チーム全体か？、誰も使っていないか？、 会社はこの方法では何千人月ものコストがかかることに、すぐに気づきました。

代わりに、会社は実際に使用されているアカウントを自動的に調べることに決めました。Evidian SSO はこの課題を実行しました。3 ヶ月間、この会社は実際に使用されている情報システム上で、楽々と情報を集めました。ユーザーがアカウントにアクセスするたびに、情報が集中データベースに記録されました。

次の段階で、会社はこのデータベースと、アプリケーション用に公開された全アカウント リストを比較しました。こうして、不要になったアカウントの除去と、具体的な基盤上でのセキュリティ ポリシーの構築が可能になりました。

SSO プロジェクトの実現

SSO プロジェクトはそれぞれ異なりますが、全般的なパターンは同じです。数百以上のコンピュータ上に展開するには、システム インテグレータによるサービスを利用しなければなりません。

1- モデル

納入業者を決める前に、代表的なアプリケーションをもつコンピュータのいくつかに、製品をインストールしてテストしてもらうよう頼み、「SSO ツールはインストールが容易であるか？、アプリケーションを統合できるか？、全コンピュータに展開する際に規模を上げることができるか？」を確認すべきです。

2- 計画

以下によりプロジェクトのスケジュールを立てられます。

- 機能に関する目的と固有費用について文書化。
- システム インテグレータとの社内の相談役リストの作成と、代表ユーザーの選択。
- サイトのリスト、統合するアプリケーション、および特定要件の調査。

3- 試験フェーズ

このフェーズは重要です。代表部署で試験を行う必要があります。例えば、30 日間、100 ユーザーについて製品をテストします。このフェーズは、最も一般的なアプリケーションに関して SSO ソリューションを構成するのに用います。詳細な評価を行うことと、通常の展開のためにここから教訓を得る必要があります。

4- 展開

最初に、信頼できる完全なユーザー ディレクトリを持っていることを確認する必要があります。そうでない場合には、この情報のソースを作成し、最新の状態にしておくことが可能なツールがあります。

次に、フェーズ毎を原則として、例えば部署単位に、SSO クライアントをコンピュータにインストールします。その部署のユーザーに告知して、何人かにはトレーニング セッションを提案します。次の部署に展開を実施する前に、ヘルプデスクに必ず来る質問への回答を用意する時間を与える必要があります。

管理職はプロジェクトの進捗と達成結果を確認するために、定期的に実情を報告する必要があります。

5- 評価

プロジェクトの最後に展開による作用を評価します。処理すべき残りのポイントを確認し、実行計画に記述する必要があります。

これは、アクセス ポリシー マネジメントやアプリケーション アカウント プロビジョニングなどの次のフェーズを計画する良い機会になります。

お問い合わせ先　：
EVIDIAN-BULL JAPAN 株式会社
〒150-8512 東京都渋谷区桜丘町 26-1
セルリアンタワー15 階
Tel 03-5456-7691 FAX 03-5456-5511

mailto: info@evidian.com
http://www.evidian.co.jp

© 2013 Evidian
The information contained in this document represents the view of Evidian on the issues discussed at the date of publication. Because Evidian must respond to changing market conditions, it should not be interpreted as a commitment on the part of Evidian, and Evidian cannot guarantee the accuracy of any information presented after the date of publication. This is for informational purposes only. EVIDIAN MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. We acknowledge the rights of the proprietors of trademarks mentioned in this book.

This white paper is printed on paper combining 40% eco-certified fibers from sustainable forests management and 60% recycled fibers in line with current environment standards (ISO 14001). IMPRIM'VERT®

39 J2 33LV 01 – Duplicopy – 2013