X-point

SSO 連携サービス
導入・設定ガイド

2024/11/18 版

ATLED

はじめに

◆本書の目的
本書は、X-point と他システムをシングル・サインオン環境で利用する為に必要なシステムの設定、管理方法について説明しています。本書をよくお読み頂いた上で設定作業を行ってください。

◆対象とする読者
本書は「X-point」のシステム管理者を対象としています。システム管理者とは「X-point」を運用するにあたり必要な設定および基本データの作成、維持管理を行なう本システムの管理権限を持つユーザを指します。

◆対応バージョン（2024/08/18 時点）

X-point	備考
X-point v3.9	連携対象のシステムが SSL（https）を利用する場合、 「セキュリティ基本サービス」が必須になります。 「SSO 連携サービス」が必須となります。

！注意事項

※ サードパーティーCooke が利用できない場合は本機能のガジェット表示を利用する事はできません。
但し、Chrome/Edge/Firefox ブラウザで Storage Access API が利用できる場合、ブラウザ操作者がコンテンツ使用を許可する事で本機能のガジェットが利用可能になります。許可指定の要否はガジェットを利用する際に行われ、ユーザによる使用許可の設定が必要であると判断された場合にガジェット表示位置に確認画面が表示されます。表示が許可された場合は 30 日以内に再利用する限り継続してガジェットが表示されます。30 日以内の利用が無い場合は再度コンテンツ使用の許可を求める表示が行われます。
なお、ブラウザ側で許可を受け付けない設定が行われている場合は変更できない事を示す表示が行われガジェット表示は行われません、ガジェット表示ができるように設定の変更を行ってください。

【設定項目】2024/11/18 時点
Chrome ・・・ 設定＞プライバシーとセキュリティ＞サードパーティーCookie
Edge ・・・ 設定＞Cookie とサイトのアクセス許可＞
保存された Cookie とデータ＞Cookie とサイトのデータ管理と削除
Firefox ・・・ 設定＞プライバシーとセキュリティ＞強化トラッキング防止機能

◆製品名について
本書中、「X-point サーバー」は「X-point」と表記しています。
また、各製品の名称は対応バージョンを省略してある箇所もありますのでご了承ください。

◆商標について

目次／索引

1. SSO連携サービス設定の概要

SSO 連携設定を行う事により、別システム内のメニューより X-point への移動の際にログイン認証（パスワード入力）をする事なく利用できるようになります。

！注意事項

※　HTTP の GET・POST パラメータや Cookie の情報を利用した連携方法です。
※　X-point の 1 ドメインと連携できる外部システムは 1 システムのみとなります。
※　SSO 連携の方向は「外部システム」から「X-point」のみで、「X-point」から「外部システム」への連携は実現できません。

2. 汎用SSO の利用

2.1. 前提条件

1.　ブラウザ環境

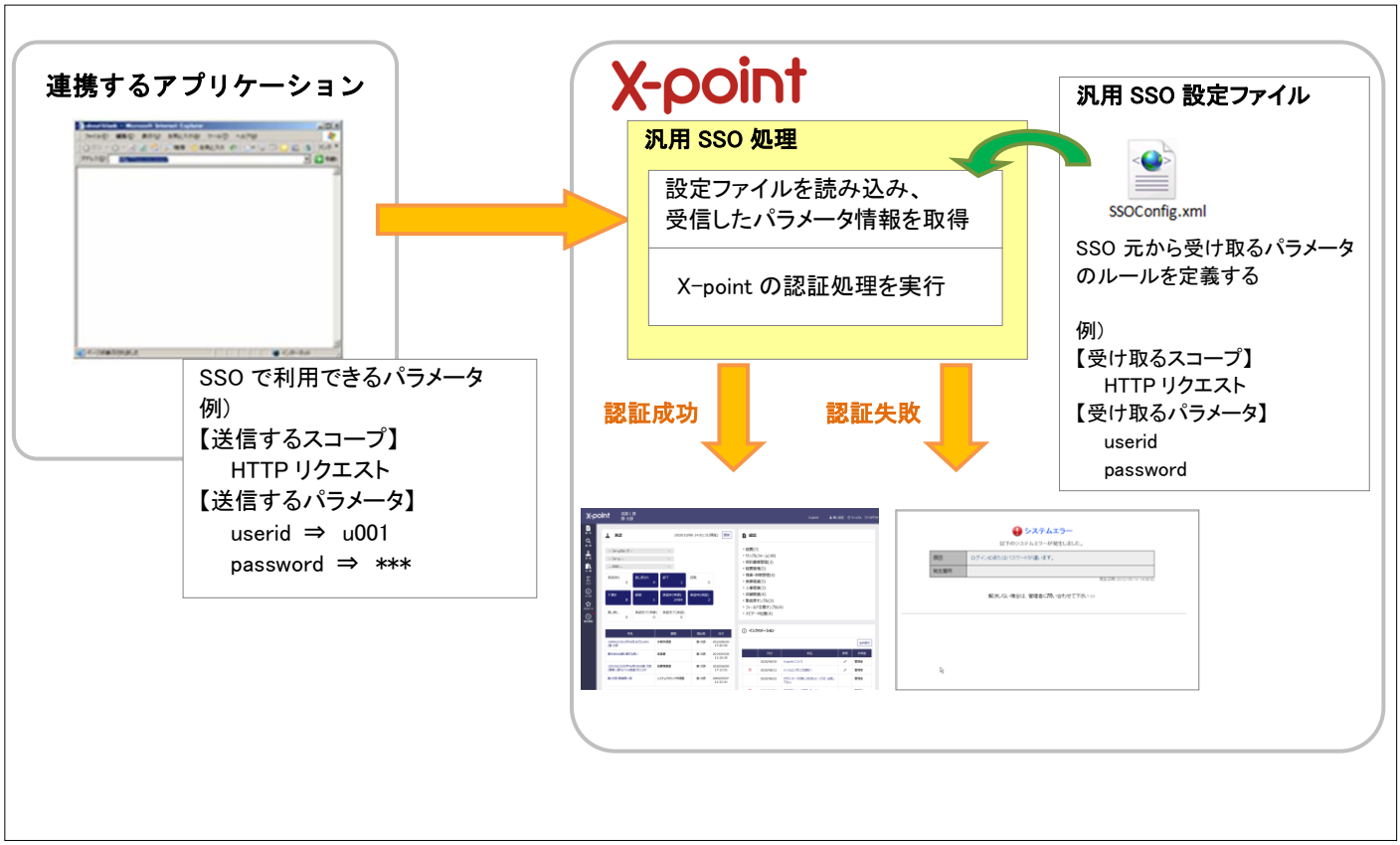
SSO する外部システムと X-point の両環境でサポートされているブラウザを使用してください。

2.2. 連携の仕組み

汎用 SSO の仕組みを利用する場合、提供される機能は以下のようになります。

・他システムより指定されたドメインに、指定されたユーザ ID でログインしユーザサイト画面を表示させることができます。
・X-point に渡すログインするアカウントは、X-point に登録されているログイン ID に対応していればログインできます。
・X-point のログイン画面利用を制限することができます。
・X-point にパスワード(クリアテキスト)で渡す場合には、パスワード認証を実施することができます。

▼連携イメージ



2.3. 汎用 SSO の仕様

汎用 SSO を利用する連携を行う際の仕様について説明します。

2.3.1. X-point 側ドメイン一つに対してひとつの連携先が指定可能

X-point と SSO 連携できる WEB システムは 1 ドメインに対し 1 システムのみ指定できます。
複数の外部システムからの連携を指定した場合も、X-point に設定できる連携元への戻り先は一つしか指定できません。
また、複数の外部システムからの SSO 連携を行う場合は、リファラーによる連携元のチェックを OFF にするか、正規表現を用いて表現する必要があります。

2.3.2. 同期すべきユーザ情報

汎用 SSO による連携は X-point の「ログイン ID」により行われます。そのため、連携元の外部システムから SSO を実行する際に送信するログイン ID は X-point 側に登録されているログイン ID と同期していなければなりません。
パスワードは、パスワード認証が“有”である場合に限り同期する必要があります。

2.3.3. X-point 側のパスワード

SSO 連携では X-point 側でパスワード認証を行うか否か指定することができます。
パスワード認証“無”に設定した場合は「ログイン ID」のみが一致すれば X-point を利用できるようになります。パスワード“有”に設定した場合は、「ログイン ID」、「パスワード」の両方が一致している必要があります。

2.3.4. eFormMaker から X-point への接続

シングルサインオンする際にパスワード認証“無”に指定されている場合、フォーム管理者が eFormMaker の【動作環境設定】から接続する際に利用するパスワードを設定する必要があります。
eFormMaker に接続するユーザのパスワードは、X-point フロントサイトの【個人設定】からパスワードに変更しておく必要があります。

2.3.5. 通知メールからの書類表示

通知メールの書類 URL から書類を開くためには、X-point にログインしている必要があります。ログアウトまたはタイムアウト状態の場合は、X-point へ SSO 連携を行うなどして、ログイン状態にすると通知メールから書類が開けるようになります。

注意事項
X-point へのログイン許可が行われていない場合、管理者サイトのメールテンプレート設定で、書類を表示する URL は設定しないでください。設定されていても通知メールから書類を表示することはできません。

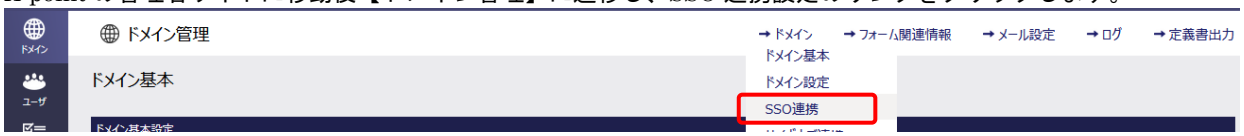
※　X-point をログアウト状態であっても通知メールの書類 URL を選択するとログイン画面が表示されますが、単独ログインができないため書類を表示することができません。

2.4. X-point 側の設定

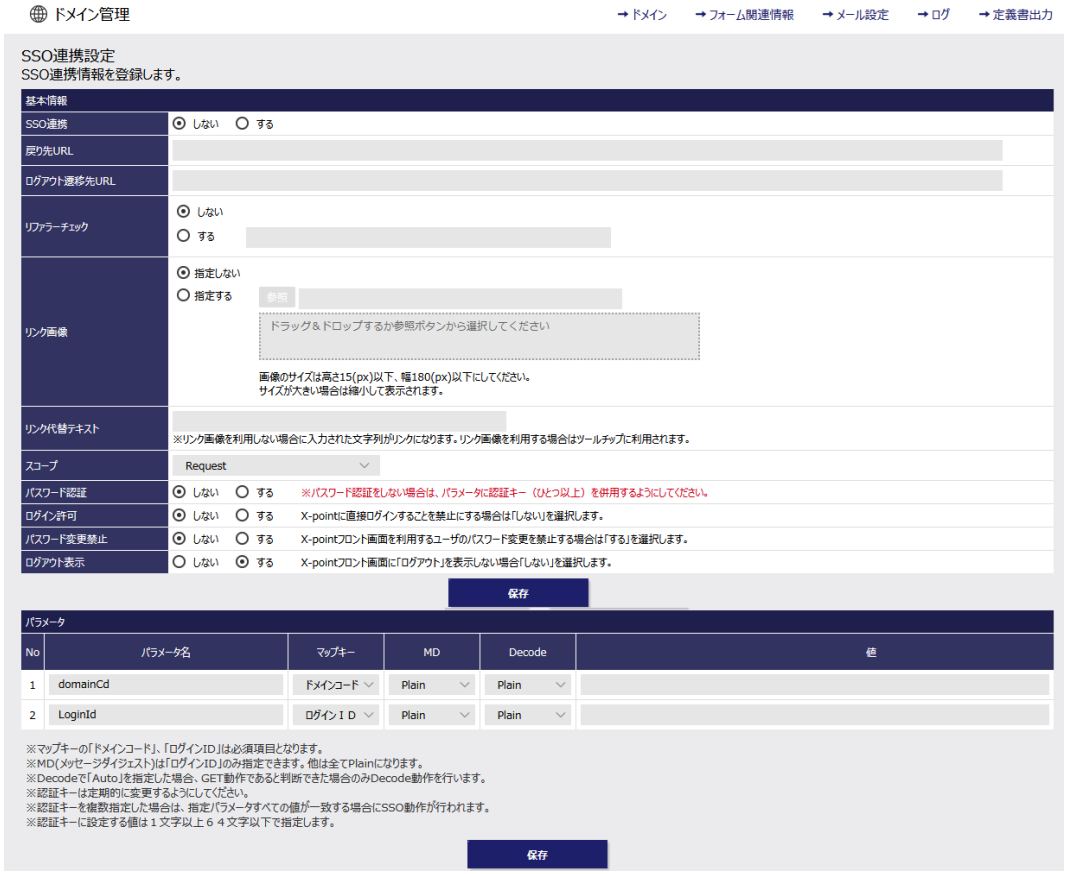
2.4.1. 設定情報の新規登録

他システムと SSO 連携を行う際の設定情報を登録します。
ドメイン管理権限を持つユーザで管理サイトにログインし、[ドメイン]→[メイン設定変更]より SSO 連携設定画面に遷移します。

1） X-point の管理者サイトに移動後【ドメイン管理】に遷移し、SSO 連携設定のリンクをクリックします。



【SSO 連携設定画面】



＜基本情報＞

【SSO 連携】
SSO 連携機能を使用する・使用しないを指定します。

【戻り先 URL】
X-point から連携先に戻る際の URL を指定します。
指定した URL は、X-point を利用する際に画面上部の【個人設定】左側に表示される画像もしくはテキストをクリックした際の遷移先となります。URL の指定を省略すると連携先に戻るためのリンク（もしくはアイコン）は表示されません。

【ログアウト遷移先 URL】
X-point のユーザフロント画面を表示している際、【ログアウト】をクリックした後に遷移する URL を指定します。
連携している製品の TOP 画面に遷移させるか、連携している製品も一緒にログオフできるような URL を指定します。
何も指定しない場合は、X-point の通常ログオフ画面が表示されます。

【リファラーチェック】
「する」が選択されている場合に遷移元 URL のチェックが設定されているチェックパターンと一致するか判断を行い、不一致の場合はログイン許可されません。

!注意事項

- 基本的には遷移するためのリンクが埋め込まれたページを表示する際に指定する URL を指定しますが、プロキシーサーバ等のリファラーを書き換える機能を持つ製品やリファラー自体を消す製品が存在しますので、X-point が実際に受け取ることができる URL を設定します。
- 判定用のリファラー文字列には正規表現を指定することができます。
  正規表現は Java 言語仕様（java.util.regex.Pattern）に準拠しており、主な利用可能パターンは以下の表に示すようになります。

構　文		マッチ対象
文字	[abc]	a、b、または c（単純クラス）
	[^abc]	a、b、c 以外の文字（否定）
	[a-zA-Z]	a ～ z または A ～ Z（範囲）
	[a-d[m-p]]	a ～ d、または m ～ p: [a-dm-p]（結合）
	[a-z&&[def]]	d、e、f（交差）
	[a-z&&[^bc]]	b と c を除く a ～ z: [ad-z]（減算）
	[a-z&&[^m-p]]	m ～ p を除く a ～ z: [a-lq-z]（減算）
定義済みの文字クラス	.	任意の文字（行末記号とマッチする場合もある）
	¥d	数字: [0-9]
	¥D	数字以外: [^0-9]
	¥w	単語構成文字: [a-zA-Z_0-9]
	¥W	非単語文字: [^¥w]
POSIX 文字クラス	¥p{Lower}	小文字の英字: [a-z]
	¥p{Upper}	大文字の英字: [A-Z]
	¥p{ASCII}	すべての ASCII 文字: [¥x00-¥x7F]
	¥p{Alpha}	英字: [¥p{Lower}¥p{Upper}]
	¥p{Digit}	10 進数字: [0-9]
	¥p{Alnum}	英数字: [¥p{Alpha}¥p{Digit}]
最長一致数量子	X? X	1 回または 0 回
	X* X	0 回以上
	X+ X	1 回以上
	X{n} X	n 回
	X{(n,} X	n 回以上
	X{n,m} X	n 回以上、m 回以下

- 指定されたリファラ文字列は、行頭に「^」、行末に「$」が自動的に追加され処理が行われます。
  つまり、比較の際は指定文字列の前後に必ず“^”と“$”が追加され指定文字列の全体一致で動作します。
  「https://nnn.nnn.nnn.nnn/xpoint/abc/.*」を指定した場合は「^https://nnn.nnn.nnn.nnn/xpoint/abc/.*$」で比較動作し「https://nnn.nnn.nnn.nnn/xpoint/abc/」で始まるリファラと同意になります。
- ブラウザの仕様により、HTTPS ページから HTTP ページへのリンクではリファラーヘッダーが送信されません。リファラーチェックを実施する際はプロトコルを一致させる必要があります。

【リンク画像】
「指定する」が選択されている場合に参照ボタンが有効になります。参照ボタンを押下して任意の画像ファイルを指定します。指定した画像は、X-point を利用する際に画面上部の 【個人設定】左側に表示されます。

【リンク代替テキスト】
リンク画像を利用しない場合に入力された文字列がリンクになります。指定した文字列は、X-point を利用する際に画面上部の【個人設定】左側に表示されます。リンク画像を利用する場合は画像のツールチップとして設定されます。

【スコープ】
SSO のための値を Request|Cookie|HTTP ヘッダーのいずれより取得するか指定します。

!注意事項

スコープに“Cookie”を指定する場合、連携元が発行する Cookie が X-point 側でも受け取れるように発行の範囲を設定してください。指定が適切に行われない場合、X-point が情報を取得できません。

(例)アクセス URL が https://renkei.domain.jp/sso_renkei/ から、https://xpoint.domain.jp/xpoint/ に連携する場合、Cookie が有効となるように domain.jp を有効範囲として指定しなければなりません。

【パスワード認証】
パスワード認証の有無を指定します。
「なし」を指定するとドメインへの SSO 連携を行なう際にパスワード認証を行ないません。
通常「なし」に指定しますが、連携元よりユーザ ID、パスワードが渡される場合でパスワード認証を実施する必要がある場合に「あり」を指定します。

【ログイン許可】
X-point のログイン画面からログインを許可するかの有無を指定します。
「なし」を指定するとログイン画面からこのドメインへのログインができなくなります。
連携するグループウェアからの利用のみを許可するような場合に、ログイン許可“しない”に設定すると X-point 単独での利用を禁止することができます。

【パスワード変更禁止】
フロント画面のユーザプロファイル画面でパスワード変更操作の許可を指定します。パスワード変更を許可する場合は“する”を指定します。
パスワード変更の禁止は連携元のシステムでパスワードを管理し、X-point 側ではログインのみを受け付ける場合に指定します。なお、X-point 側でパスワード変更を許可しても連携先のシステムに設定されているパスワードは変更されません。

【ログアウト表示】
フロント画面の上部に“ログアウト”メニューを表示するか否かを指定します。ログアウト遷移先 URL を指定できないような場合、X-point をログオフしても連携元のシステムからログオフされない為、SSO 動作の際に自動的にログインできてしまい、ログオフ操作が意味を持たない場合などに指定します。
ログアウト遷移先を指定することで、連携先のシステムからのログアウトもできるような場合に“する”を指定すると効果的です。

＜パラメータ＞

【パラメータ名】
スコープで指定した場所から、どのようなキー名で値を取り出すかを指定します。

！注意事項
・パラメータ名には同一の名称を指定することはできません。
・連携するシステム毎に設定するキー名を変更することができます。
・ドメインコード、ログイン ID の指定は必須です。省略することはできません。

【マップキー】
連携元から取り出した値をどのようなキーで X-point に渡すかを指定します。

！注意事項
・マップキーには同一のキーを指定することはできません。
・X-point と SSO 連携する場合は「ドメインコード」と「ログイン ＩＤ」は必須になります。

【MD】
受け取るパラメータ値がハッシュ値である場合にハッシュ関数のタイプを指定します。
平文以外で受取る事ができるパラメータは“ログイン ID”のみです。

！注意事項
・ユーザ数が多いシステムで、平文以外を利用すると SSO 連携時にシステムに対する負荷が高くなります。
・ユーザ数が多い場合は極力平文で利用するようにしてください。
X-point では仕様上の制限により、パスワードを平文以外で受信することができません。

【Decde】
受信したパラメータの値を URLDecode する・しないを指定します。

・Plain　・・　decode を行いません。
・Auto　・・　値を受け取った際に GET タイプの Action であると判断すると Decode を行います。
・Decode　・・　必ず decode を行います。

【値】
取得した値が空だった場合のデフォルト値を指定します。

＜パラメータの設定方法＞

連携動作の際、連携対象のシステムより受信するパラメータ名を設定します。パラメータ名は任意に指定できますが、何のデータを指し示すものかをマップキーで指定します。指定可能なパラメータは最大８つになります。

マップキー	区分	説　明
ドメインコード	必須	ドメインコードを受け取るパラメータ名称を指定します。 指定された値が X-point に登録されているドメインコードと一致する必要があります。 【指定例】 domainCd=xpoint
ログイン ID	必須	ログイン先のログイン ID を指定します。 指定された値が X-point に登録されているユーザのログイン ID と一致する必要があります。 【指定例】 LoginId=user01
パスワード	－	パスワード認証を“する”に設定した場合、パスワードを受け取るパラメータ名を指定します。 受信するパスワードは PLAN(平文)である必要があります。 【指定例】 Passwd=passwd01
ポートレット	－	連携対象のシステムにガジェットを表示する場合に、連携システム側で指定します。 指定可能なガジェットタイプは formLibrary,finder,wkfl,bookmark,information,queryChart の６つです。 1. formLibrary ・・・ 提出ガジェット 2. finder ・・・ 検索ガジェット 3. wkfl ・・・ 承認ガジェット 4. bookmark ・・・ ブックマークガジェット 5. information ・・・ ドメインインフォメーションガジェット 6. queryChart ・・・ グラフガジェット 【指定例】 Forward=wkfl 注：グラフガジェット(queryChart)の場合、ガジェットタイプに”-” (ハイフン)で区切って表示対象のグラフのクエリコードを指定する必要があります。 (例： Forward=queryChart-query1) クエリコードは X-point 管理者サイト/クエリ管理/クエリプロパティ画面から確認できます。
認証キー１～４	－	連携動作を行う際に双方でキーの一致を確認するパラメータを指定します。 値に指定されている文字列が、連携元と X-point 側で完全一致する必要があります。 複数の認証キーが指定されている場合は、指定したキー全てが一致しなければなりません。 値に全角文字は使用できません。 【指定例】 Authkey1=abcdefghijklmn

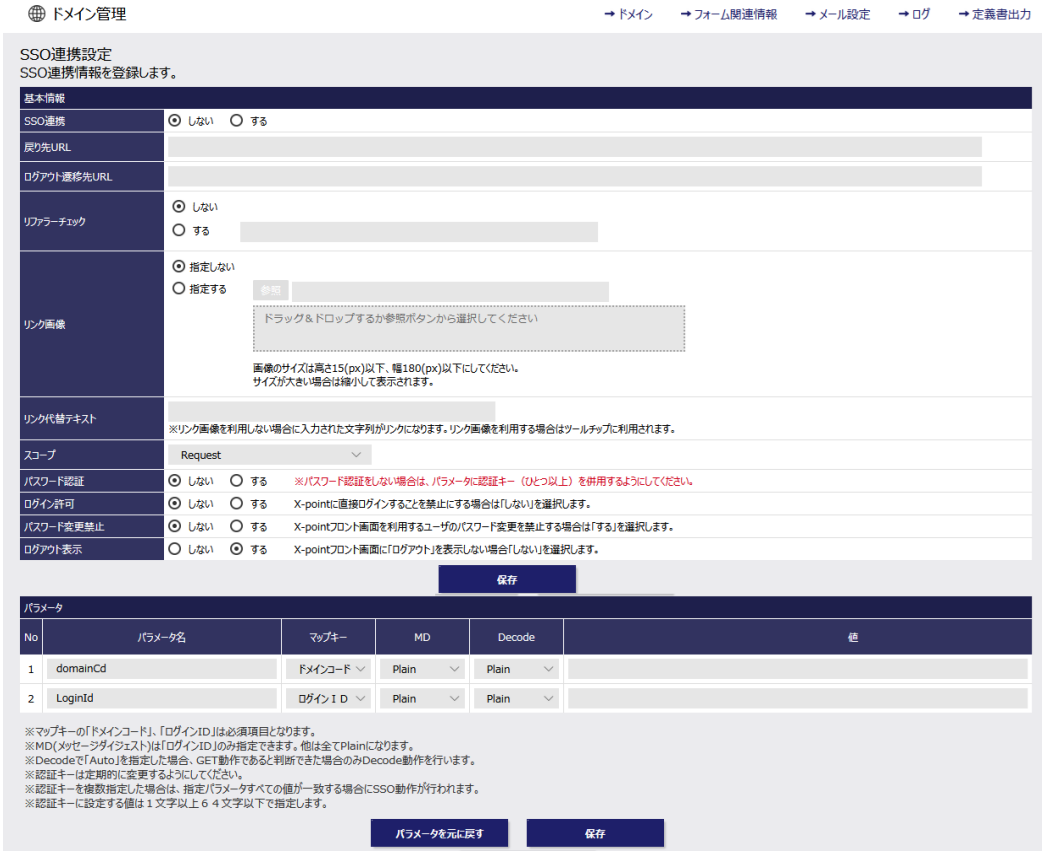
【＋】ボタンを押下するとパラメータの入力欄が１行追加されます。

【🗑】ボタンを押下するとボタンを押下した入力欄が１行削除されます。

２）【保存】ボタンを押下して設定を保存します。

2.4.2. 設定の更新

登録済みの SSO 連携設定を更新します。操作方法は新規登録の場合と同じです。



初期表示時に登録済みの設定ファイルの内容が表示されます。
【パラメータを元に戻す】ボタンを押下すると修正内容を破棄し登録されている内容に戻します。

2.5. 連携する外部システム側の設定

2.5.1. URL リンクよる SSO 連携

連携する外部システムに、X-point へのリンクを作成します。
連携する外部システムのリンクの作成方法に基づき、ログインに必要な情報を X-point に渡すリンクを作成してください。

＜ SSO 連携のリンク URL ＞

X-point で SSO 連携が動作するための URI は「/ssologin.do」です。

https://[ホスト名].atledcloud.jp/xpoint/ssologin.do

この URI に、連携情報のパラメータを指定します。

【例】ドメインコードとログイン ID を GET メソッドで X-point に引き渡す場合
https://example.atledcloud.jp/xpoint/ssologin.do**?domainCd=xpoint&LoginId=u001**

※ パスワード認証を行う場合「&Passwd={パスワード}」を追加します。

＜ 設定例 ＞
連携する外部システムの HTML ページに、SSO 連携のリンク URL を設置します。
連携 URL には、ログオンするドメインコード、ユーザ ID（パスワード認証有の場合はパスワード）を指定します。

【例】<A>タグを利用してドメインコードとログイン ID を「GET」で X-point に引き渡す場合

```
<a href="{SSO 連携のリンク URL}">X-point</a>
```

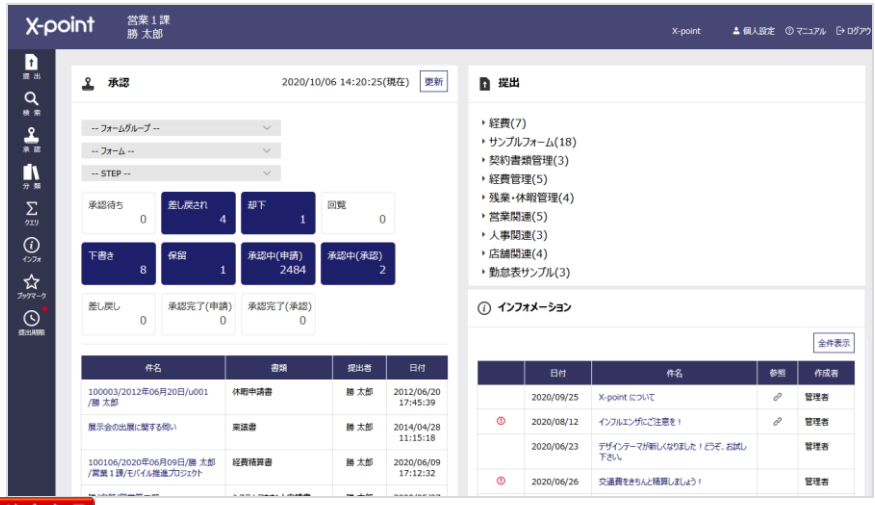
X-point

【例】<FORM>タグを利用してドメインコードとログイン ID を「POST」で X-point に引き渡す場合
通常、POST で渡すとブラウザのアドレス欄にパラメータが表示されません。

```
<form name='A' action="{SSO 連携のリンク URL}" method="post">
 <input type="hidden" name="domainCd" value="xxxx">
 <input type="hidden" name="LoginId" value="xxxx">
 <input type="submit" value="Go X-point">
</form>
```

Go X-point

【連携後の X-point の画面イメージ】



！注意事項

- X-point でドメインコードが修正された場合はパラメータのドメインコードの修正が必要になります。

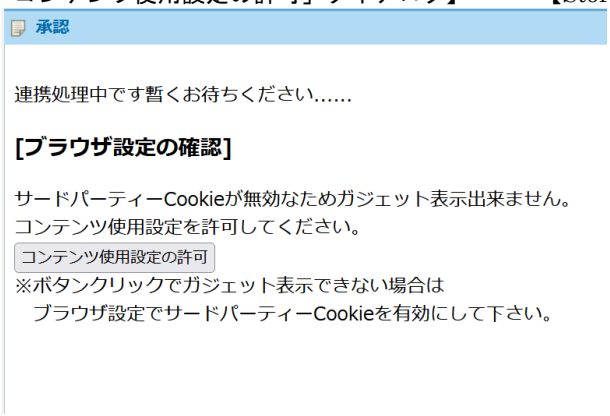
2.5.2. サードパーティーCookie が利用できない場合の動作

サードパーティーCookie が利用できない設定であるブラウザではポートを表示する事ができません。
但し、Chrome／Edge／Firefox ブラウザで Storage Access API が利用できる場合は、ブラウザ操作者がコンテンツ使用を許可する事で本機能のガジェットを利用する事が可能になります。
コンテンツ使用の許可はポートを表示する一連の動作に組み込まれています。

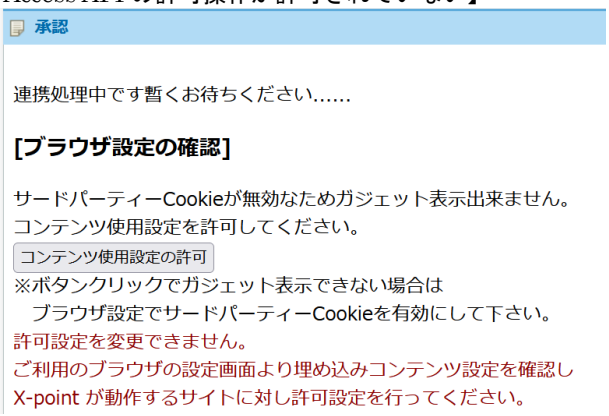
【許可動作の流れ】

1. Office・ガルーンから X-point のガジェット表示機能を呼び出す
2. サードパーティーCookie の利用が許可されている ⇒ ガジェットを表示して終了
3. Storage Access API の利用が許可されている ⇒ ガジェットを表示して終了
4. ガジェット位置に「コンテンツ使用設定の許可」ダイアログが表示される
5. ユーザが「コンテンツ使用設定の許可」をクリックする（必ず“人”が操作します）
6. ブラウザ設定で Storage Access API の許可操作が許されている ⇒ ガジェットを表示して終了
7. ブラウザ設定が Storage Access API の許可操作を許していない ⇒ ガジェットの表示は出来ません

【「コンテンツ使用設定の許可」ダイアログ】



【Storage Access API の許可操作が許可されていない】



Storage Access API の利用が許可されるとガジェットが表示されるようになります。
複数のガジェットを表示する画面の場合は、一つのガジェットで許可を行うと他のガジェットも自動的に許可されます。

※ 自動で許可されない場合は、画面全体を再表示してください。

表示が許可された場合は 30 日以内に再利用する限り継続してガジェットが表示され表示の度に延長されます。30 日以内の利用が無い場合は再度コンテンツ使用の許可を求める表示が行われます。

■改訂履歴

改版	改版内容
2021 年 10 月 1 日版	初版リリース
2024 年 11 月18 日版	サードパーティーCookie が利用できない場合の動作を追記