HITACHI
Inspire the Next

2024年度第2回 学認SP研究会

大学でのSP調達の実態とSPコミュニティの立ち上げ

2025年3月19日

株式会社 日立製作所
公共システム事業部　公共基盤ソリューション本部
プラットフォームソリューション第二部
河本　竜司

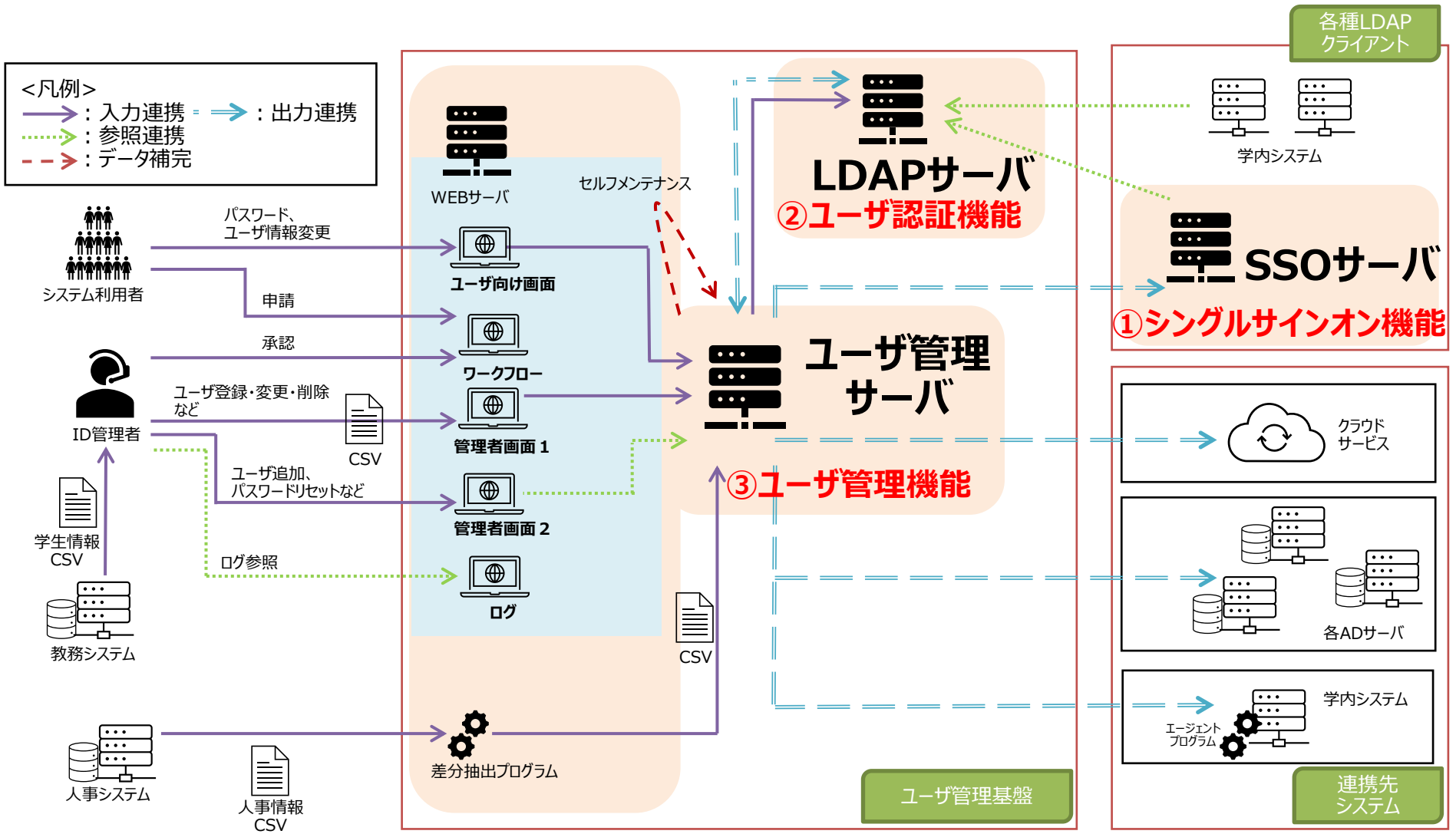
HITACHI
Inspire the Next

目次

1. 大学様のユーザ管理システムの概要

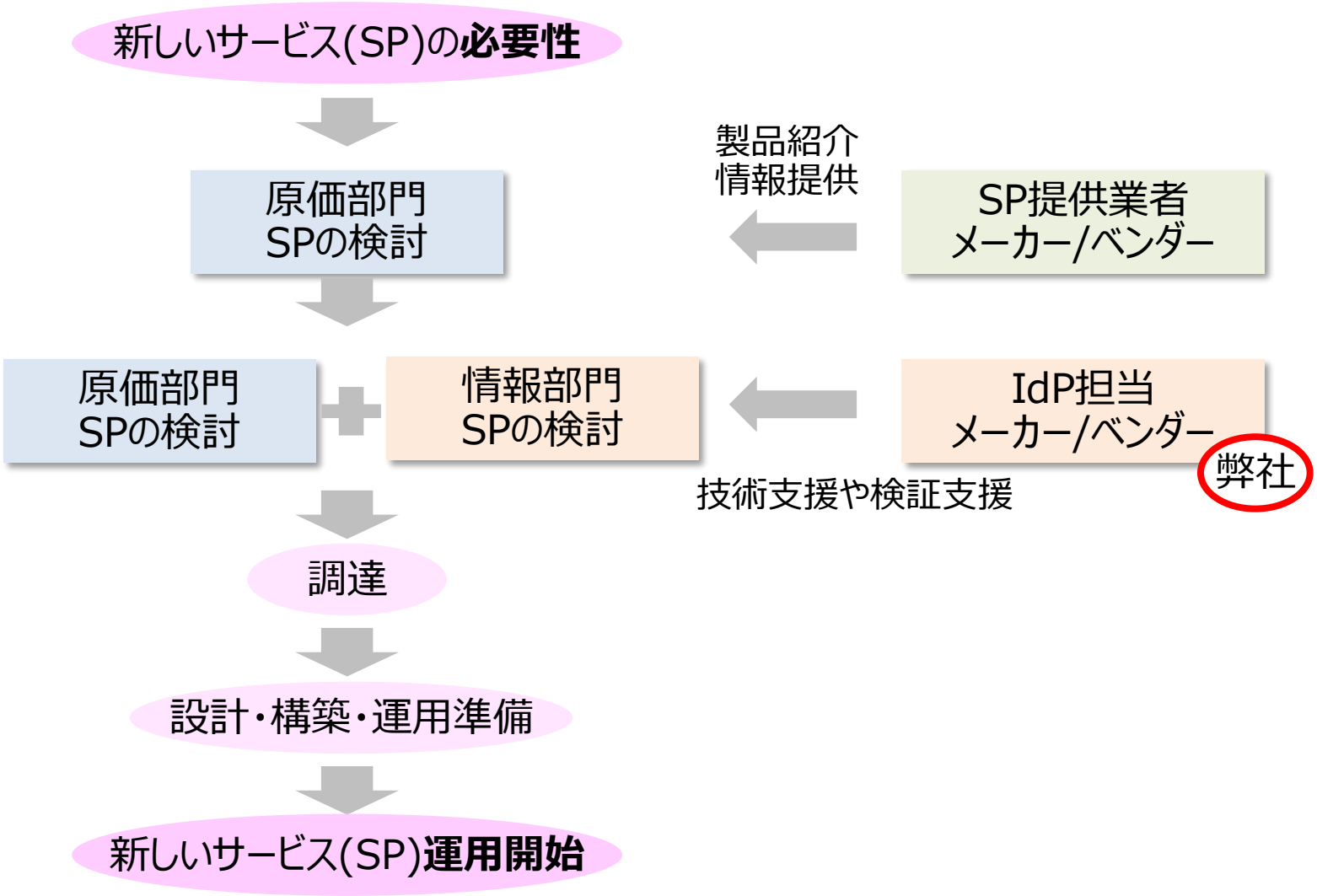
1.大学様のユーザ管理システムの概要

ユーザ管理システム(UA)は３つの機能で構成
①シングルサインオン機能(SSO認証)　②ユーザ認証機能(LDAP認証)　③ユーザ管理機能



2．新しいサービス(SP)の検討から運用開始までの流れ

2.新しいサービス(SP)の検討から運用開始までの流れ



3．[検討] SAMLは難しい

3. [検討] SAMLは難しい（1）

HITACHI
Inspire the Next

1. SAMLって何？

Security Assertion Markup Language

IdP（Identity Provider)

SP（Service Provider）

2. 用語の不統一

用語	類義語
entityID	Audience URI
	Identifier
	SSO ID プロバイダー
	オーディエンス
Assertion Consumer Service URL	Single Sign on URL
	SSO URL

3. 誰が使えるようにする？

ユーザ、グループ、権限管理

ユーザ登録や更新、削除

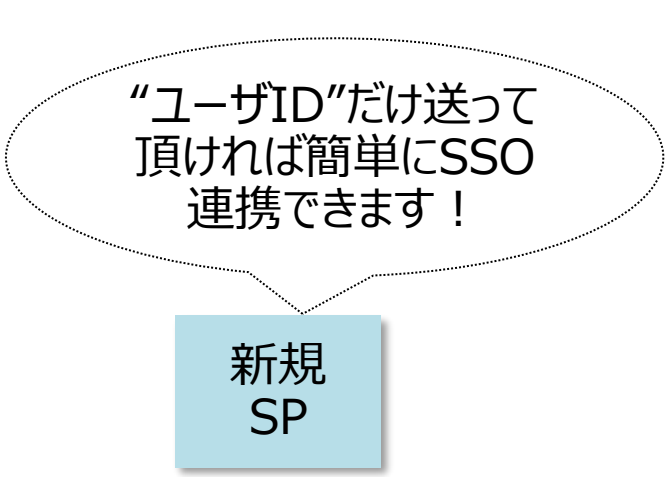
3．[検討] SAMLは難しい（２）

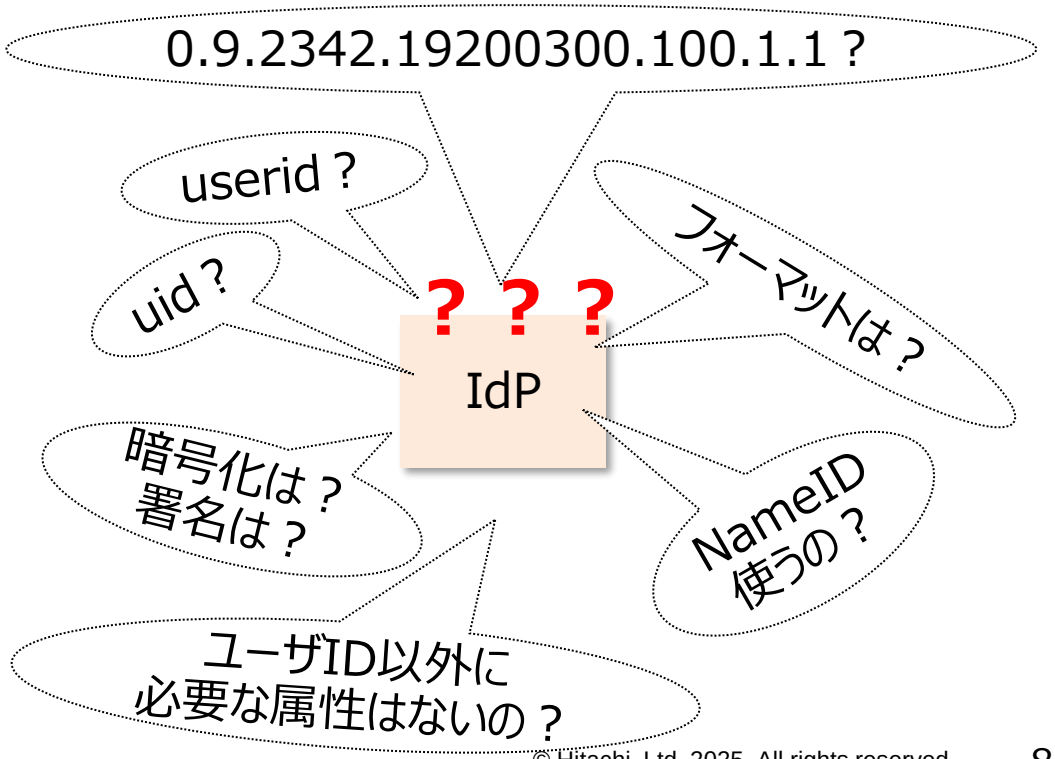
HITACHI
Inspire the Next

４．SAML連携実装のための設定方法が分かりにくい

・SPメーカ/ベンダ様の情報だけでIdP側の設定ができない

・IdPサーバとして、Shibboleth以外にも多数あり、
SPメーカ/ベンダ様でも汎用的な設定マニュアルを作れない





3．[検討] SAMLは難しい（３）

HITACHI
Inspire the Next

5．”SAML対応”製品を選んでいるはずなのに

”SAML対応”となっている製品/サービス/システムであっても
いざSAML連携設定をしてみるとうまくいかない

6．”SAML未対応”製品が必要な場合

学内のIdP(SSO)で利用している多要素認証を活用したいが
SAML対応をどうしよう（リバースプロキシの活用）

7．ヒューマンエラー

・用語が分かりにくい、不統一なため、設定に向けて人から人への
　設定意図が上手く伝わらない
・誤記（メタデータや設定の構文間違い）

8．運用の手間がかかる

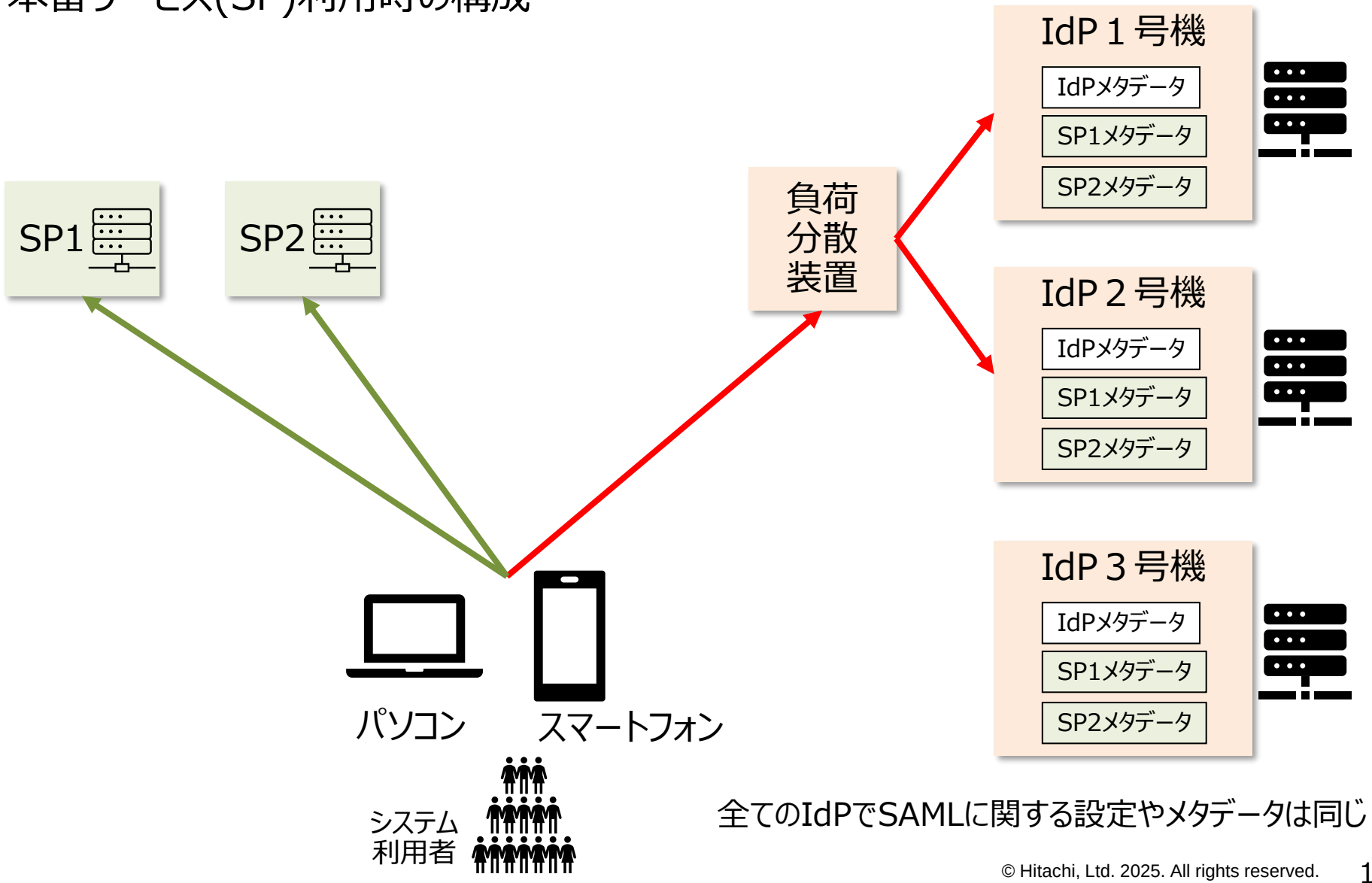
証明書更新など

４．[検証] SP-IdPのSAML連携検証環境

4．[検証] SP-IdPのSAML連携検証環境(1)

HITACHI
Inspire the Next

本番サービス(SP)利用時の構成

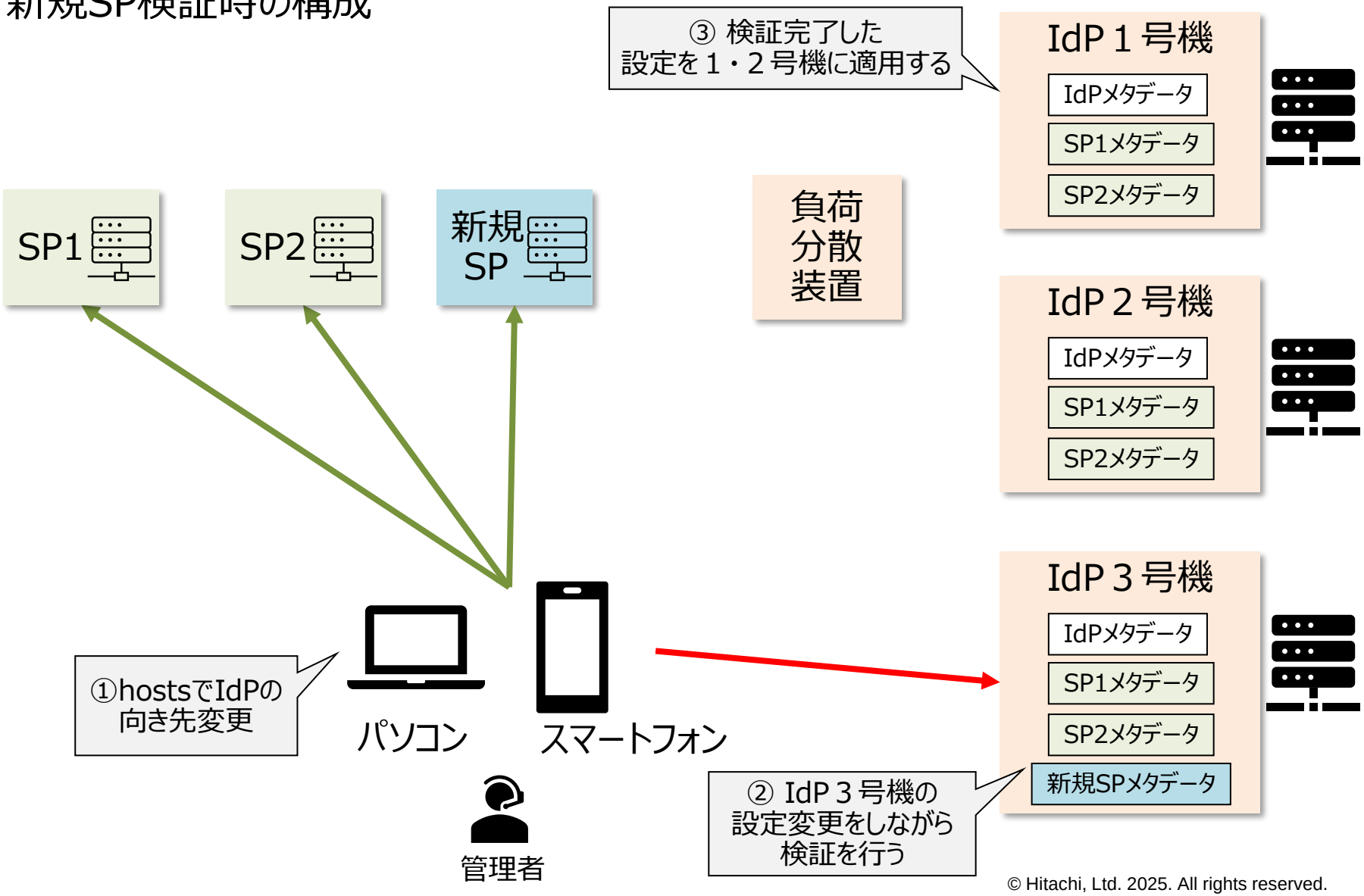


全てのIdPでSAMLに関する設定やメタデータは同じ

4. [検証] SP-IdPのSAML連携検証環境(2)

HITACHI
Inspire the Next

新規SP検証時の構成



5．[調達] SP調達仕様書の作成

5. [調達] SP調達仕様書の作成

HITACHI
Inspire the Next

SP調達に際してIdP(シングルサインオンシステム)との連携に関する仕様書を作成

O.シングルサインオン(SSO)システムとの連携

O.1. 本学のSSOシステムとSAML2.0を使った連携が可能なこと。
製品/システム標準でSAML2.0対応をしていない場合は
webサーバ(apache、IIS等）に Shibboleth SPやmod_auth_mellonなどの
SAML機能を組み込みSAML連携すること

O.2. 本学のSSOシステムではSAML IdPとして
Shibboleth IdPとの連携実績が無い場合は
Shibboleth IdPとの連携実績が無い場合、

O.3. 「認可」機能を有する場合は「認可」判
例１）IdPが送出する属性値をもとに例え
例２）SP側のユーザ管理情報（データベ

O.4. SAMLを使ったSSO連携にあたり、SPメ
別紙「SPヒアリングシート」へ必要事項

O.5. SPメタデータの更新運用を踏まえて下記
（１）SPメタデータの内容更新する際の

O.6. IdPメタデータの更新運用を踏まえて下記事項を明示すること。
（１）SP側にIdPメタデータを取り込む方法を具体的に明示すること。
例）
・GUI画面にIdPメタデータ(XMLファイル)をアップロード
・サーバ内にIdPメタデータ(XMLファイル)をコピー
・IdPメタデータ内の情報を個別にGUI画面に転記する、など
（２）新しいIdPメタデータをSP側に自動で取り込む仕組みの有無
本学では最新のIdPメタデータをweb(https)で公開しており
webサイトからダウンロードしSP側に自動で取り込む機能を
有しているかを明示すること。
（３）SP側に新しいIdPメタデータを取り込む際のSP側のサービス停止の要否
（４）IdP側のサーバ証明書更新時はIdPメタデータ(XMLファイル)内に新旧サーバ証明書を
並記してSP側へ提供している。SP側ではIdPの新旧サーバ証明書の
並記に対応しているか明示すること。

(例)SPヒアリングシート

項番	項目			値	説明
1	設定	連携対象SPの情報	SPのEntityID	[redacted]	EntityIDとはIdP,SPにつける固有のIDです。 任意の文字列を使用することが可能ですが、URN,URL形式のものが一般的です。 EntityIDの例: [redacted] urn:federation:MicrosoftOnline
2			SPで使用する属性	uid	アプリケーション(SP)が使用する認証情報として属性を定義します。 SPで定義した属性を元にIdPもその属性を使用します。
3			Responseの暗号化 あり／なし	あり	IdPがSPに対して送信するSAMLResponseを暗号化するかどうかを決めていただきます。
4			Assertionの暗号化 あり／なし	あり	IdPとSP間で送受信するSAMLアサーションを暗号化するかどうかを決めていただきます。
5			Responseの署名 あり／なし	なし	SPが自身のサーバ証明書を使用してIdPから受け取ったSAMLResponseが署名されたものであるか検証します。
6			Assertionの署名 あり／なし	なし	IdPとSP間で自身のサーバ証明書をそれぞれ使用して受け取ったSAMLアサーションが署名されたものであるか検証します。
7			NameIDの使用有無	あり	NameIDとはIdPとSP間で共有するユーザ識別子です。
8			NameIDで使用する属性 ※1	uid	
9			NameIDのフォーマット ※1	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	
10			NameIDの暗号化 あり／なし ※1	あり	NameIDの暗号化を行うか決めていただきます。

※1 項番6「NameIDの使用有無」で「なし」を選択した場合は記述は不要です。

HITACHI
Inspire the Next

6．まとめ

6.まとめ

新規SPの検討から本番稼働にあたり
諸組織様での対応のご負担が高い状況をご報告させて頂きました。

SPコミュニティ

でのサポートを是非よろしくお願いいたします。

- Apacheは、Apache Software Foundationの登録商標または商標です。
- IIS（Internet Information Services）は、米国Microsoft Corporationの登録商標です。
- Shibbolethは、Internet2®の登録商標です。
- AzureADは、Microsoft Corporationの登録商標です。
- OpenAMは、ForgeRock Inc.の登録商標です。
- Oktaは、Okta, Inc.の登録商標です。Oktaの商標には、Okta、Auth0、およびOktaとAuth0のロゴが含まれます。これらの商標は、米国および他の国々で登録されています。
- その他記載の製品名、会社名は、各社の商標または登録商標です。


HITACHI
Inspire the Next